



的加密最佳做法和功能 AWS 服務

AWS 規定指引



AWS 規定指引: 的加密最佳做法和功能 AWS 服務

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

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

Table of Contents

簡介	1
目標對象	1
關於 AWS 密碼編譯服務	3
一般加密最佳實務	4
資料分類	4
加密傳輸中的資料	4
靜態資料加密	5
AWS 服務的加密最佳實務	6
AWS CloudTrail	6
Amazon DynamoDB	7
Amazon EC2 和 Amazon EBS	8
Amazon ECR	9
Amazon ECS	10
Amazon EFS	11
Amazon EKS	12
AWS Encryption SDK	13
AWS KMS	14
AWS Lambda	16
Amazon RDS	17
AWS Secrets Manager	18
Amazon S3	19
Amazon VPC	20
資源	22
文件歷史紀錄	23
詞彙表	24
#	24
A	24
B	27
C	28
D	31
E	34
F	36
G	37
H	37

I	38
L	40
M	41
O	44
P	47
Q	49
R	49
S	52
T	54
U	56
V	56
W	56
Z	57
.....	lviii

AWS 服務的加密最佳實務和功能

庫爾特·庫馬爾，Amazon Web Services

2024 年九月 ([文件歷史記錄](#))

加密是在數位時代保護敏感資料的基本網路安全工具。隨著企業越來越依賴資料來推動其營運 (包括生成式 AI 部署)，透過強大的加密實務來保護這些寶貴資訊，是全方位資料保護策略的重要組成部分。本指南可協助您瞭解加密原則和提 AWS 供的加密功能。

現代網路安全威脅包括數據洩露的風險，即未經授權訪問您的信息資產導致數據丟失的時候。資料是每個組織獨有的商業資產。它可以包括客戶資訊、業務計畫、設計文件或程式碼。保護企業意味著保護資料。

即使發生外洩，資料加密也能協助保護您的業務資料。它提供了防止意外洩露的防禦層。若要存取 AWS 雲端中的加密資料，使用者需要使用金鑰進行解密的許可，並且需要使用資料所在服務的許可。如果沒有這兩個許可，使用者將無法解密和檢視資料。

一般而言，您可以加密三種類型的資料。傳輸中的資料是在您的網路中主動移動的資料，例如在網路資源之間移動。靜態資料是靜止且處於休眠狀態的資料，例如儲存中的資料。範例包括區塊儲存、物件儲存、資料庫、存檔和物聯網 (IoT) 裝置。使用中的資料是指應用程式或服務正在積極處理或使用的資料。透過在使用時保護資料安全，組織可協助降低意外揭露的風險。

本指南討論加密傳輸中資料和靜態資料的考量和最佳做法。它還會檢閱許多可用的加密功能和控制項 AWS 服務。您可以在 AWS 雲端 環境中的服務層級實作這些加密建議。

目標對象

本指南可供公共和私營部門的小型、中型和大型組織使用。無論您的組織處於評估和實作資料保護策略的初始階段，還是旨在增強現有安全控制，本指南中概述的建議最適合下列受眾：

- 為企業制定政策的執行官，例如首席執行官 (CEOs)，技術長 (CTOs)，首席信息官 (CIOs) 和首席信息安全官 (CISOs)
- 負責制定技術標準的技術官，例如技術副總裁和總監
- 負責下列事項的企業利害關係人和應用程式擁有者：
 - 評估風險狀態、資料分類和保護需求
 - 監控既定組織標準的合規情況

- 合規、內部稽核和治理官，負責監控合規政策的遵守情況，包括法定和自願合規管轄範圍

關於 AWS 密碼編譯服務

加密演算法是將純文字訊息轉換為加密密文的公式或程序。如果您不熟悉加密或其術語，我們建議您在繼續本指南之前閱讀[關於資料加密](#)和[密碼編譯概念](#)。

AWS 密碼編譯服務依賴安全的開放原始碼加密演算法。這些演算法經過公共標準機構和學術研究審查。部分 AWS 工具和服務強制使用特定演算法。在其他服務中，您可以在多個可用演算法與金鑰長度之間選擇，也可以使用建議的預設值。

本節說明 AWS 工具和服務支援的部分演算法。根據金鑰運作方式，其分為對稱和非對稱兩個類別：

- 對稱加密使用相同的金鑰來加密和解密資料。AWS 服務 支援進階加密標準 (AES) 和三重資料加密標準 (3DES 或 TDES)，這是兩種廣泛使用的對稱演算法。如需詳細資訊，請參閱《AWS 密碼編譯服務和工具指南》中的[對稱演算法](#)。
- 非對稱加密使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰的存取應受到嚴格限制。AWS 服務 通常支援 RSA 和橢圓曲線密碼編譯 (ECC) 非對稱演算法。如需詳細資訊，請參閱《AWS 密碼編譯服務和工具指南》中的[非對稱演算法](#)。

AWS 密碼編譯服務符合廣泛的密碼編譯安全標準，因此您可以遵守政府或專業法規。如需 AWS 服務遵守的資料安全標準的完整清單，請參閱[AWS 合規計畫](#)。如需有關密碼編譯工具和服務的詳細資訊，請參閱[AWS 密碼編譯服務和工具](#)。

一般加密最佳實務

本節提供在中加密資料時套用的 AWS 雲端建議。這些一般加密最佳作法並非特定於 AWS 服務。本節包含下列主題：

- [資料分類](#)
- [加密傳輸中的資料](#)
- [靜態資料加密](#)

資料分類

資料分類是根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。[資料分類](#)是 AWS Well-Architected 架構中安全性支柱的一個組成部分。類別可能包括高度機密、機密、非機密和公有，但分類層及其名稱可能因組織而異。如需有關資料分類程序、考量和模型的詳細資訊，請參閱[資料分類](#) (AWS 白皮書)。

將資料分類後，您可以根據每個類別所需的保護層級為您的組織建立加密策略。例如，您的組織可能會決定高度機密的資料應使用非對稱加密，且公有資料不需要加密。如需有關設計加密策略的詳細資訊，請參閱[為靜態資料建立企業加密策略](#)。雖然該指南中的技術考量事項和建議特定於靜態資料，但您也可以使用分階段方法為傳輸中的資料建立加密策略。

加密傳輸中的資料

通 AWS 區域 過 AWS 全球網絡之間傳輸的所有數據在離開 AWS 安全設施之前，在物理層自動加密。可用區域之間的所有流量都會加密。

以下是在 AWS 雲端中對傳輸中的資料進行加密時的一般最佳實務：

- 根據您的資料分類、組織要求以及任何適用的法規或合規標準，為傳輸中的資料定義組織加密政策。我們強烈建議您對分類為高度機密或機密的傳輸中的資料進行加密。您的政策也可能視需要指定其他類別的加密，例如非機密或公有資料。
- 對傳輸中的資料進行加密時，我們建議使用已核准的密碼編譯演算法、區塊加密模式和金鑰長度，如加密政策中定義。
- 使用下列其中一種方法，加密企業網路和 AWS 雲端 基礎架構內資訊資產與系統之間的流量：
 - [AWS Site-to-Site VPN](#) 連線
 - [AWS Site-to-Site VPN](#) 和 [AWS Direct Connect](#) 連接的組合，它提供了一個 IPsec-加密的私人連接

- AWS Direct Connect 支援 Sec MAC urity (MACsec) 的連線，可將資料從公司網路加密到該 AWS Direct Connect 位置
- 根據最低權限原則識別加密金鑰的存取控制政策。最低權限是授予使用者執行工作職能所需的最低存取權的安全最佳實務。如需套用最低權限權限的詳細資訊，請參閱[中的安全性最佳做法IAM](#)和原則的[最佳做法](#)。IAM

靜態資料加密

所有 AWS 資料儲存服務，例如 Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System (AmazonEFS)，都提供加密靜態資料的選項。[加密是使用 256 位元進階加密標準 \(AES-256\) 區塊加密和 AWS 密碼編譯服務，例如 \(\) 或。AWS Key Management ServiceAWS KMSAWS CloudHSM](#)

您可以根據資料分類、加密需求或阻止您使用加密的技術限制等因素，使用用戶端 end-to-end 加密或伺服器端 end-to-end 加密來加密資料：

- 用戶端加密是在目標應用程式或服務接收資料之前在本機加密資料的行為。AWS 服務 收到加密的資料，但在加密或解密中未扮演任何角色。對於用戶端加密，您可以使用 AWS KMS、[AWS Encryption SDK](#) 或其他第三方加密工具或服務。
- 伺服器端加密是指接收資料的應用程式或服務在目的地加密資料的行為。對於伺服器端加密，您可以使 AWS KMS 用整個儲存區塊的加密。您也可以使用其他協力廠商加密工具或服務，[LUKS](#)例如在作業系統 (OS) 層級加密 Linux 檔案系統。

以下是在 AWS 雲端中對靜態資料進行加密時的一般最佳實務：

- 根據您的資料分類、組織要求以及任何適用的法規或合規標準，為靜態資料定義組織加密政策。如需詳細資訊，請參閱[為靜態資料建立企業加密策略](#)。我們強烈建議您對分類為高度機密或機密的靜態資料進行加密。您的政策也可能視需要指定其他類別的加密，例如非機密或公有資料。
- 對靜態資料進行加密時，我們建議使用已核准的密碼編譯演算法、區塊加密模式和金鑰長度。
- 根據最低權限原則識別加密金鑰的存取控制政策。

AWS 服務的加密最佳實務

本節包含下列項目的最佳做法和建議 AWS 服務：

- [AWS CloudTrail](#)
- [Amazon DynamoDB](#)
- [Amazon 彈性計算雲 \(AmazonEC2 \) 和 Amazon 彈性區塊商店 \(AmazonEBS \)](#)
- [Amazon 彈性容器註冊表 \(AmazonECR \)](#)
- [Amazon 彈性容器服務 \(AmazonECS \)](#)
- [Amazon Elastic File System \(AmazonEFS \)](#)
- [Amazon Elastic Kubernetes Service \(Amazon \) EKS](#)
- [AWS Encryption SDK](#)
- [AWS Key Management Service \(AWS KMS\)](#)
- [AWS Lambda](#)
- [Amazon Relational Database Service \(AmazonRDS \)](#)
- [AWS Secrets Manager](#)
- [Amazon Simple Storage Service \(Amazon S3\)](#)
- [Amazon Virtual Private Cloud \(AmazonVPC \)](#)

的加密最佳做法 AWS CloudTrail

[AWS CloudTrail](#) 可協助您稽核 AWS 帳戶的監管、合規、操作和風險。

請考慮此服務的下列加密最佳實務：

- CloudTrail 應使用客戶管理的日誌進行加密 AWS KMS key。選擇與接收日誌檔案的 S3 儲存貯體位於同一區域的KMS金鑰。如需詳細資訊，請參閱[更新軌跡以使用KMS金鑰](#)。
- 作為額外的安全層，啟用追蹤的日誌檔案驗證。這可協助您判斷記錄檔在 CloudTrail 傳送之後是否已修改、刪除或未變更。如需指示，請參閱[啟用的記錄檔完整性驗證 CloudTrail](#)。
- 使用介面VPC端點 CloudTrail 來啟用與其他資源通訊，VPCs而不會遍歷公用網際網路。如需詳細資訊，請參閱[AWS CloudTrail 搭配介面VPC端點使用](#)。
- 將aws:SourceArn條件金鑰新增至KMS金鑰原則，以確保僅針對特定追蹤或追蹤 CloudTrail 使用 KMS金鑰。如需詳細資訊，請參閱[設 AWS KMS key 定 CloudTrail](#)。

- 在中 AWS Config，實作受[cloud-trail-encryption-enabled](#) AWS 管規則以驗證和強制執行記錄檔加密。
- 如果設定 CloudTrail 為透過 Amazon 簡單通知服務 (AmazonSNS) 主題傳送通知，請在 CloudTrail 政策聲明中新增 `aws:SourceArn` (或選擇性`aws:SourceAccount`) 條件金鑰，以防止未經授權的帳戶存取SNS主題。如需詳細資訊 [Amazon 請參SNS閱 CloudTrail](#)。
- 如果您正在使用 AWS Organizations，請建立一個組織追蹤，以記錄該組織 AWS 帳戶中的所有事件。這包括組織中的管理帳戶和所有成員帳戶。如需詳細資訊，請參閱[為組織建立追蹤](#)。
- 建立[適用於所有 AWS 區域](#)儲存公司資料的追蹤，以記錄這些區域中的 AWS 帳戶活動。AWS 啟動新區域時，CloudTrail 會自動包含新區域並記錄該區域中的事件。

Amazon DynamoDB 的加密最佳實務

[Amazon DynamoDB](#) 是全受管的無SQL資料庫服務，可提供快速、可預測且可擴展的效能。靜態 DynamoDB 加密可保護加密表格中的資料，包括其主索引、本機和全域次要索引、串流、全域表格、備份和 DynamoDB Accelerator (DAX) 叢集，每當資料儲存在耐久媒體中。

根據資料分類要求，可以透過實作伺服器端或用戶端加密來維護資料機密性和完整性：

對於伺服器端加密，當您建立新資料表時，您可以使用 AWS KMS keys 加密資料表。您可以使用 AWS 擁有的金鑰、AWS 受控金鑰或客戶管理金鑰。我們建議使用客戶受管金鑰，因為您的組織可以完全控制金鑰，並且當您使用此金鑰類型時，資料表層級加密金鑰、DynamoDB 資料表、本機和全域次要索引以及串流都使用相同的金鑰進行加密。如需這些金鑰類型的詳細資訊，請參閱[客戶金鑰和 AWS 金鑰](#)。

Note

您可以隨時在 AWS 擁有的金鑰、AWS 受管金鑰和客戶管理金鑰之間切換。

對於用戶端加密和 end-to-end 保護靜態和傳輸中的資料，您可以使用 [Amazon DynamoDB 加密用戶端](#)。除了保護項目屬性值機密性的加密之外，DynamoDB Encryption Client 也會簽署項目。這透過啟用偵測對項目的未授權變更 (包括新增或刪除屬性)，或用一個加密值替換另一個加密值，來提供完整性保護。

請考慮此服務的下列加密最佳實務：

- 將停用或排程刪除金鑰的許可限制為僅需要執行這些任務的人員。這些狀態可避免所有使用者和 DynamoDB 服務可在資料表上加密或解密資料，以及執行讀取和寫入操作。

- 雖然 DynamoDB 依預設會使用加密傳輸中的資料，但建議HTTPS使用其他安全性控制。您可以使用下列任一選項：
 - AWS Site-to-Site VPN 連接使IPsec用加密。
 - AWS Direct Connect 建立私人連接的連接。
 - AWS Direct Connect 與IPsec加密私人 AWS Site-to-Site VPN 連接的連接連接。
 - 如果只需要從虛擬私有雲 (VPC) 內存取 DynamoDB，您可以使用VPC閘道端點，並僅允許中的資源存VPC取它。這樣可防止流量周遊公有網際網路。
- 如果您使用的是VPC端點，請將與端點關聯的端點IAM策略和策略限制為僅授權的使用者、資源和服務。如需詳細資訊，請參閱[使用政策控制 DynamoDB 端點的存取和使用端點IAM策略控制對服務的存取](#)。
- 您可以根據加密政策，在應用程式層級對需要加密的資料實作資料欄層級資料加密。
- 設定叢DAX集以在設定叢集時加密靜態資料，例如快取中的資料、組態資料和記錄檔。您無法在現有叢集上啟用靜態加密。此伺服器端加密有助於保護資料，防止透過基礎儲存進行未經授權的存取。DAX靜態加密會自動整AWSKMS合，以管理用於加密叢集的單一服務預設金鑰。如果在建立加密DAX叢集時不存在服務預設金鑰，則 AWS KMS 會自動建立新的 AWS 受管理金鑰。如需詳細資訊，請參閱[靜DAX態加密](#)。

Note

客戶管理的金鑰無法搭配DAX叢集使用。

- 設定DAX叢集以在設定叢集時加密傳輸中的資料。您無法在現有叢集上啟用傳輸中加密。DAX用TLS來加密應用程式與叢集之間的要求和回應，並使用叢集的 x509 憑證來驗證叢集的身分識別。如需詳細資訊，請參閱[傳輸中DAX加密](#)。
- 在中 AWS Config，實作受[dax-encryption-enabled](#) AWS 管規則以驗證和維護DAX叢集的加密。

Amazon EC2 和 Amazon 的加密最佳實踐 EBS

[Amazon 彈性運算雲 \(AmazonEC2\)](#) 在 AWS 雲端。您可以視需要啟動任意數量的虛擬伺服器，，並快速進行擴展或縮減。[Amazon 彈性區塊存放區 \(AmazonEBS\)](#) 提供用於執行個體的區塊層級儲存磁碟區。EC2

請考慮這些服務的下列加密最佳實務：

- 使用適當的資料分類鍵和值來標記所有EBS磁碟區。這可協助您根據您的原則判斷並實作適當的安全性與加密需求。

- 根據您的加密原則和技術可行性，針對執行個體之間或EC2執行個體與內部部署網路之間EC2傳輸中的資料設定加密。
- 加密EC2執行個體的開機EBS磁碟區和資料磁碟區。加密的EBS磁碟區會保護下列資料：
 - 磁碟區內的待用資料
 - 所有在磁碟區和執行個體間移動的資料
 - 所有從磁碟區建立的快照
 - 所有從那些快照建立的磁碟區

[如需詳細資訊，請參閱EBS加密的運作方式。](#)

- 預設為目前帳戶的EBS磁碟區啟用加密功能 AWS 區域。這會強制加密任何新EBS磁碟區和快照複本。它對現有EBS磁碟區或快照沒有任何影響。如需詳細資訊，請參閱[預設啟用加密](#)。
- 加密 Amazon 執行個體的執行個EC2體存放根磁碟區。這有助於保護與作業系統一起儲存的組態檔案和資料。如需詳細資訊，請參閱[如何使用 Amazon EC2 執行個體存放區加密保護靜態資料](#) (AWS 部落格文章)
- 在中 AWS Config，實作[加密磁碟區](#)規則以自動化檢查，以驗證並強制執行適當的加密組態。

Amazon 的加密最佳實踐 ECR

[Amazon 彈性容器登錄 \(Amazon ECR\)](#) 是安全、可擴展且可靠的受管容器映像登錄服務。

Amazon 將圖像ECR存儲在亞馬遜ECR管理的 Amazon S3 存儲桶中。每個 Amazon ECR 儲存庫都有一個加密組態，這是在建立儲存庫時設定的。根據預設，Amazon ECR 會使用伺服器端加密搭配 Amazon S3 受管 (SSE-S3) 加密金鑰。如需詳細資訊，請參閱[靜態加密](#) (Amazon ECR 文件)。

請考慮此服務的下列加密最佳實務：

- 不要將預設伺服器端加密與 Amazon S3 受管 (SSE-S3) 加密金鑰搭配使用，而是使用存放在其中的客戶受管KMS金鑰。AWS KMS此金鑰類型提供最細緻的控制選項。

Note

該KMS密鑰必須存在於與儲存庫 AWS 區域 相同的位置。

- 佈建儲存庫時，請勿撤銷 Amazon 預設ECR建立的授權。這可能會影響功能，例如存取資料、加密推送至儲存庫的新映像，或在提取映像時將其解密。

- 用 AWS CloudTrail 於記錄 Amazon ECR 傳送到的請求 AWS KMS。日誌項目包含加密內容金鑰，可使其更容易識別。
- 設定 Amazon ECR 政策以控制來自特定 Amazon VPC 端點或特定端點的存取VPCs。實際上，這將隔離對特定 Amazon ECR 資源的網路存取，僅允許從特定VPC資源進行存取。透過與 Amazon VPC 端點建立虛擬私人網路 (VPN) 連線，您可以加密傳輸中的資料。
- Amazon ECR 支持基於資源的政策。使用這些原則，您可以根據來源 IP 位址或特定 IP 位址來限制存取 AWS 服務。

Amazon 的加密最佳實踐 ECS

[Amazon 彈性容器服務 \(AmazonECS\)](#) 是一種快速且可擴展的容器管理服務，可協助您在叢集上執行、停止和管理容器。

使用 AmazonECS，您可以使用下列任何一種方法來加密傳輸中的資料：

- 建立服務網格。使用 AWS App Mesh，設定已部署的 [Envoy Proxy](#) 和網狀端點 (例如[虛擬節點](#)或[虛擬閘道](#)) 之間的TLS連線。您可以使用TLS來自 AWS Private Certificate Authority 或客戶提供的憑證。如需詳細資訊和逐步解說，請參閱在 [AWS App Mesh 使用 AWS Certificate Manager \(ACM\) 或客戶提供的憑證 \(AWS 部落格文章\)](#) 中啟用服務之間的流量加密。
- 如果支援，請使用[AWS 硝基隔離區](#)。AWS 硝基隔離區是 Amazon 的一EC2項功能，可讓您從 Amazon 執行個體建立隔離的執行環境 (稱為隔離區)。EC2其旨在協助保護您最敏感的資料。此外，[ACM對於 Nitro Enclaves](#)，您可以在具有 Nitro Enclaves 的 Amazon EC2 實例上運行的 Web 應用程序和 Web 服務器使用公共和私有 SSL AWS /TLS證書。如需詳細資訊，請參閱 [AWS Nitro Enclaves — 用於處理機密資料的隔離EC2環境](#) (AWS 部落格文章)。
- 搭配應用程式負載平衡器使用伺服器名稱指示 (SNI) 通訊協定。您可以在應用程式負載平衡器的單一HTTPS接聽程式後部署多個應用程式。每個接聽程式都有自己的TLS憑證。您可以由提供的憑證 ACM，也可以使用自我簽署憑證。[應用程式負載平衡器](#)和 [Network Load Balancer](#) 都支援SNI。如需詳細資訊，請參閱[應用程式負載平衡器現在 Support 使用智慧選取的多個TLS憑證 SNI](#) (AWS 部落格文章)。
- 為了提高安全性和靈活性 AWS Private Certificate Authority，請使用與 Amazon ECS 任務部署TLS憑證。如需詳細資訊，請參閱[維護TLS容器第 2 部分：使用 AWS Private CA](#) (部AWS 部落格文章)。
- 通過使用[秘密發現服務 TLS](#) (特使TLS) 或託管在 () 中的證書在 [App Mesh](#) 中實現相互 ACM ([mGitHub](#)) 。

請考慮此服務的下列加密最佳實務：

- 在技術可行的情況下，為了增強安全性，請在中設定 [Amazon ECS 界面VPC端點](#) AWS PrivateLink。透過VPN連線存取這些端點會加密傳輸中的資料。
- 安全地存儲敏感材料，例如API密鑰或數據庫憑據。您可以將這些參數作為加密參數儲存在 Parameter Store (AWS Systems Manager的功能) 中。不過，我們建議您使用這項服務，AWS Secrets Manager 因為這項服務可讓您自動輪換密碼、產生隨機密碼，以及跨越共用密碼 AWS 帳戶。
- 為了協助降低環境變數資料外洩的風險，我們建議您使用秘密存放區CSI驅動程式的 [AWS Secrets Manager 和 Config 提供者](#) (GitHub)。此驅動程式可讓您將儲存在 Secrets Manager 中的機密和儲存在 Parameter Store 中的參數顯示為掛載在 Kubernetes Pod 中的檔案。

Note

AWS Fargate 不支援。

- 如果您的資料中心或網路上的外部第三方中的使用者或應用程式直接向其發出HTTPSAPI要求 AWS 服務，請使用從 AWS Security Token Service (AWS STS) 取得的臨時安全登入資料來簽署這些要求。

Amazon 的加密最佳實踐 EFS

[Amazon Elastic File System \(AmazonEFS\)](#) 可協助您在 AWS 雲端。

請考慮此服務的下列加密最佳實務：

- 在中 AWS Config，實作受 [efs-encrypted-check](#) AWS 管規則。此規則會檢查 Amazon EFS 是否設定為使用加密檔案資料 AWS KMS。
- 透過建立 Amazon CloudWatch 警示來監控CreateFileSystem事EFS件的 CloudTrail 日誌，並在建立未加密的檔案系統時觸發警示，對 Amazon 檔案系統強制執行加密。如需詳細資訊，請參閱 [逐步解說：在靜態 Amazon EFS 檔案系統上執行加密](#)。
- 使用掛載 [輔助程EFS式掛載](#) 檔案系統。這會在用戶端和 Amazon EFS 服務之間設定並維護 TLS 1.2 通道，並透過此加密通路由所有網路檔案系統 (NFS) 流量。下列指令會實作傳輸中加密TLS的使用。

```
sudo mount -t efs -o tls file-system-id:/ /mnt/efs
```

如需詳細資訊，請參閱 [使用 EFS mount 輔助程式掛載EFS檔案系統](#)。

- 使用 AWS PrivateLink，實作介面VPC端點，在VPCs和 Amazon 之間建立私有連線EFSAPI。透過端點之間的VPN連線傳輸中的資料會加密。如需詳細資訊，請參閱[AWS 服務 使用介面VPC端點](#)存取。
- 在以IAM身為基礎的原則中使用elasticfilesystem:Encrypted條件金鑰，以防止使用者建立未加密的EFS檔案系統。如需詳細資訊，請參閱[使用IAM來強制建立加密檔案系統](#)。
- KMS應使用以資源為基礎的金鑰原則，為最低權限存取設定用於EFS加密的金鑰。
- 使用EFS檔案系統策略中的aws:SecureTransport條件金鑰，在連線至EFS檔案系統時強制TLS對用NFS戶端使用。如需詳細資訊，請參閱[使用 Amazon Elastic File System 加密檔案資料中的傳輸中資料 \(AWS 白皮書\)](#)。

Amazon 的加密最佳實踐 EKS

[Amazon Elastic Kubernetes Service \(AmazonEKS\)](#) 可協助您在上執行 Kubernetes，AWS 而無需安裝或維護自己的 Kubernetes 控制平面或節點。在 Kubernetes 中，密碼可協助您管理敏感資訊，例如使用者憑證、密碼或金鑰。API根據預設，這些密碼會以未加密方式儲存在API伺服器的基礎資料存放區 (稱為 `etcd`) 中。任何具有API存取權或存取權的使用者都`etcd`可以擷取或修改密碼。此外，任何有權在命名空間中建立 Pod 的人都可以使用該存取權來讀取該命名空間中的任何機密。您可以使用 AWS 受管金鑰或客戶受管金鑰 AWS KMS keys，在 Amazon EKS 中將這些靜態密鑰加密。使用的另一種方法`etcd`是使用 [AWS Secret 和 Config 提供程序 \(ASCP\)](#) (GitHub 存儲庫)。ASCP IAM與以資源為基礎的政策整合，以限制和限制僅在叢集內特定 Kubernetes 網繭中對機密的存取。

您可以搭配 Kubernetes 使用下列 AWS 儲存服務：

- 對於 Amazon 彈性區塊商店 (AmazonEBS)，您可以使用樹內存儲驅動程序或 [Amazon EBS CSI 驅動程序](#)。兩者都包括用於加密磁碟區和提供客戶受管金鑰的參數。
- 對於 Amazon Elastic File System (AmazonEFS)，您可以使用 [Amazon EFS CSI 驅動程式](#)並支援動態和靜態佈建。

請考慮此服務的下列加密最佳實務：

- 如果您使用的是 `etcd` (依預設儲存未加密的機密物件)，請執行下列操作以協助保護機密：
 - [加密機密靜態資料](#) (Kubernetes 文件)。
 - 透過限制讀取和寫入密碼的角色型存取控制 (RBAC) 規則啟用或設定授權。限制建立新機密或取代現有機密的許可。如需詳細資訊，請參閱[授權概觀](#) (Kubernetes 文件)。

- 如果您在 Pod 中定義多個容器，且只有其中一個容器需要存取機密，請定義磁碟區掛載，以便其他容器無法存取該機密。以磁碟區掛載的機密會具現化為 tmpfs 磁碟區，並在刪除 Pod 時自動從節點中移除。您也可以使用環境變數，但我們不建議使用此方法，因為環境變數的值可能會出現在日誌中。如需詳細資訊，請參閱[機密](#) (Kubernetes 文件)。
- 如果可能，避免授予對命名空間內的機密的 watch 和 list 請求的存取權。在 Kubernetes 中 API，這些要求非常強大，因為它們可讓用戶端檢查該命名空間中每個密碼的值。
- 僅允許叢集管理員存取 etcd，包括唯讀存取權。
- 如果有多個 etcd 執行個體，請確定使用 etcdTLS 於對 etcd 等之間的通訊。
- 如果您正在使用 ASCP，請執行下列動作以協助保護機密：
 - 使用[服務帳戶的 IAM 角色](#)來限制僅授權網繭的秘密存取權。
 - 透過使用加密[提供者 \(GitHub 儲存庫\)](#)來使用客戶管理的金鑰實作信封 AWS 加密，以啟用 Kubernetes 密碼的加密。KMS
- 建立 Amazon 指 CloudWatch 標篩選器和警示，以針對管理員指定的操作傳送警示，例如秘密刪除或在待刪除期間使用秘密版本。如需詳細資訊，請參閱[根據異常偵測建立警報](#)。

的加密最佳做法 AWS Encryption SDK

[AWS Encryption SDK](#) 是開放原始碼的用戶端加密程式庫。它使用行業標準和最佳實踐來支持多種[編程語言](#)的實施和互操作性。AWS Encryption SDK 使用安全、經過驗證的對稱金鑰演算法來加密資料，並提供符合密碼編譯最佳作法的預設實作。如需詳細資訊，請參閱[AWS Encryption SDK 中的支援演算法套件](#)。

的主要功能之一 AWS Encryption SDK 是支援加密使用中的資料。通過採用 encrypt-then-use 方法，您可以在應用程序邏輯處理敏感數據之前對其進行加密。即使應用程式本身受到安全性事件的影響，這有助於保護資料免於遭受可能的暴露或竊改。

請考慮此服務的下列最佳實務：

- 遵循 [AWS Encryption SDK 的最佳實務](#) 中的所有建議。
- 選取一或多個包裝金鑰，以協助保護您的資料金鑰。如需詳細資訊，請參閱[選取包裝金鑰](#)。
- 將 KeyId 參數傳遞給 [ReEncrypt](#) 作業，以協助防止使用不受信任的 KMS 金鑰。如需詳細資訊，請參閱[改善用戶端加密：明確 KeyIds 和金鑰承諾](#) (AWS 部落格文章)。
- 搭配使用時 AWS Encryption SDK AWS KMS，請使用本機 KeyId 篩選。如需詳細資訊，請參閱[改善用戶端加密：明確 KeyIds 和金鑰承諾](#) (AWS 部落格文章)。

- 對於流量大量需要加密或解密的應用程式，或者如果您的帳戶超出 AWS KMS [請求配額](#)，[您](#)可以使用 AWS Encryption SDK。請注意資料金鑰快取的下列最佳實務：
 - 設定[快取安全閾值](#)以限制每個已快取資料金鑰可使用的時間長度，以及依據每個資料金鑰可以保護的資料數量。如需設定這些閾值時的建議，請參閱[設定快取安全閾值](#)。
 - 將本機快取限制為實現特定應用程式使用案例效能改進所需的最小資料金鑰數。如需設定本機快取限制的指示和範例，請參閱[使用資料金鑰快取：Step-by-step](#)。

如需詳細資訊，請參閱 [AWS Encryption SDK：如何判斷資料金鑰快取是否適合您的應用程式](#) (AWS 部落格文章)。

的加密最佳做法 AWS Key Management Service

[AWS Key Management Service \(AWS KMS\)](#) 可協助您建立和控制加密金鑰，以協助保護您的資料。AWS KMS 與大多數其他可 AWS 服務 以加密數據的集成。如需完整清單，請參閱[與AWS 服務 整合 AWS KMS](#)。AWS KMS 還與整合 AWS CloudTrail 以記錄KMS金鑰的使用，以滿足稽核、法規和法規遵循需求。

KMS索引鍵是中的主要資源 AWS KMS，它們是加密金鑰的邏輯表示法。有三種主要類型的KMS鍵：

- 客戶管理的金KMS鑰是您建立的金鑰。
- AWS 代管金KMS鑰是代表您在帳戶中 AWS 服務 建立的金鑰。
- AWS 擁有的金KMS鑰是 AWS 服務 擁有和管理的金鑰，可用於多個金鑰 AWS 帳戶。

如需有關這些金鑰類型的詳細資訊，請參閱[客戶金鑰和 AWS 金鑰](#)。

在中 AWS 雲端，策略用於控制誰可以存取資源和服務。例如，在 AWS Identity and Access Management (IAM) 中，以身分識別為基礎的政策會定義使用者、使用者群組或角色的許可，以資源為基礎的政策附加至資源 (例如 S3 儲存貯體)，並定義允許存取哪些主體、支援的動作以及必須符合的任何其他條件。與IAM原則類似，AWS KMS 使用[金鑰原則](#)來控制KMS金鑰的存取。每個KMS金鑰都必須有一個金鑰原則，而且每個金鑰只能有一個金鑰原則。定義允許或拒絕金鑰存取的原則時，請注意下列事KMS項：

- 您可以控制客戶受管金鑰的金鑰原則，但無法直接控制 AWS 受管理金鑰或 AWS 擁有金鑰的金鑰原則。
- 關鍵政策允許 AWS KMS API 授予對 AWS 帳戶。除非金鑰原則明確允許，否則您無法使用原IAM則來允許存取KMS金鑰。未經金鑰原則的許可，允許權限的IAM策略不會生效。如需詳細資訊，請參閱[允許IAM原則允許存取KMS金鑰](#)。

- 您可以使用IAM策略拒絕對客戶管理的金鑰的存取，而無需金鑰政策的對應許可。
- 設計多區域金鑰的金鑰IAM原則和原則時，請考量下列事項：
 - 金鑰政策不是多區域金鑰的[共用屬性](#)，且不會在相關的多區域金鑰之間複製或同步。
 - 使用 CreateKey 和 ReplicateKey 動作建立多區域金鑰時，將套用[預設金鑰政策](#)，除非在請求中指定了金鑰政策。
 - 您可以實作條件索引鍵，例如 [aws: RequestedRegion](#)，將許可限制為特定 AWS 區域。
 - 您可以使用授予來允許多區域主要金鑰或複本金鑰的許可。不過，單一授權無法用來允許多個金鑰的權限，即使這些KMS金鑰是相關的多區域金鑰也一樣。

使用 AWS KMS 和建立金鑰原則時，請考慮下列加密最佳做法和其他安全性最佳做法：

- 請遵守下列資源中的建議，以取得 AWS KMS 最佳實務：
 - [AWS KMS 補助金的最佳做法](#) (AWS KMS 文檔)
 - [IAM政策的最佳做法](#) (AWS KMS 文件)
- 根據職責分離最佳實務，為管理金鑰的人員和使用金鑰的人員維護個別身分：
 - 建立和刪除金鑰的管理員角色不應具有使用金鑰的能力。
 - 部分服務可能只需要加密資料，而不應授予使用金鑰解密資料的能力。
- 金鑰政策應永遠遵循最低權限的模型。請勿在中kms:*的動作IAM或金鑰原則中使用，因為這會將主參與者權限授予管理和使用金鑰。
- 在金鑰原則中使用 [kms: ViaService](#) 條件金鑰，將客戶受管金鑰的使用限制為特定 AWS 服務 金鑰。
- 如果您可以在金鑰類型之間進行選擇，則優先客戶受管金鑰，因為其會提供最精細的控制選項，包括下列選項：
 - [管理身分驗證和存取控制](#)
 - [啟用和停用金鑰](#)
 - [輪換 AWS KMS keys](#)
 - [標記金鑰](#)
 - [建立別名](#)
 - [刪除 AWS KMS keys](#)
- AWS KMS 管理和修改權限必須明確拒絕未核准的主參與者，而且任何未經授權主體的 allow 陳述式中都不應存在 AWS KMS 修改權限。如需詳細資訊，請參閱[適用於 AWS Key Management Service 的動作、資源和條件鍵](#)。

- 為了偵測KMS金鑰的未經授權使用情況，請在中 [AWS Config實作-kms iam-customer-policy-blocked-動作和-kms 動作規則。iam-inline-policy-blocked](#)這可防止主參與者對所有資源使用 AWS KMS 解密動作。
- 在中實作服務控制原則 (SCPs)，AWS Organizations 以防止未經授權的使用者或角色直接以指令或透過主控台的方式刪除KMS金鑰。如需詳細資訊，請參閱[使用SCPs做為預防性控制項](#) (AWS 部落格文章)。
- 在日誌中 CloudTrail 記錄 AWS KMS API呼叫。這會記錄相關的事件屬性，例如發出的請求內容、發出請求的來源 IP 地址以及發出請求的人。如需詳細資訊，請參閱[使用記錄 AWS KMS API呼叫 AWS CloudTrail](#)。
- 如果您使用[加密上下文](#)，它不應該包含任何敏感信息。CloudTrail 將加密內容儲存在純JSON文字檔案中，任何有權存取包含資訊的 S3 儲存貯體的人都可以檢視這些內容。
- 監控客戶受管金鑰的使用情況時，設定事件以在偵測特定動作 (例如建立金鑰、更新客戶受管金鑰政策或匯入金鑰材料) 時通知您。也建議您實作自動回應，例如停用金鑰或執行組織政策規定的任何其他事件回應動作的 AWS Lambda 函數。
- [多區域金鑰](#)建議用於特定案例，例如合規、災難復原或備份。多區域金鑰的安全屬性與單一區域金鑰顯著不同。授權建立、管理和使用多區域金鑰時，採用下列建議：
 - 允許委託人只將多區域金鑰複寫至需要的 AWS 區域中。
 - 只將多區域金鑰的許可授予需要這些金鑰的委託人，並且僅為需要這些金鑰的任務授予。

的加密最佳做法 AWS Lambda

[AWS Lambda](#) 是一項運算服務，可協助您執行程式碼，無需佈建或管理伺服器。若要保護您的環境變數，可以使用伺服器端加密來保護您的靜態資料，並使用用戶端加密來保護傳輸中的資料。

請考慮此服務的下列加密最佳實務：

- Lambda 永遠使用 AWS KMS key提供靜態伺服器端加密。根據預設，Lambda 會使用 AWS 受管金鑰。我們建議您使用客戶受管金鑰，因為您可以完全控制此金鑰，包括管理、輪換和稽核。
- 對於需要加密的傳輸中資料，請啟用輔助程式，以確保環境變數已在用戶端加密，以便在傳輸過程中使用偏好的KMS金鑰進行保護。如需詳細資訊，請參閱[保護環境變數](#)中的傳輸中安全。
- 儲存敏感或重要資料的 Lambda 函數環境變數應在傳輸過程中進行加密，以協助保護動態傳遞至函數的資料 (通常是存取資訊) 免遭未經授權的存取。
- 若要防止使用者檢視環境變數，請在IAM原則中的使用者權限或拒絕存取預設金鑰、客戶管理金鑰或所有金鑰的金鑰原則中新增陳述式。如需詳細資訊，請參閱[使用 AWS Lambda 環境變數](#)。

Amazon 的加密最佳實踐 RDS

[Amazon Relational Database Service \(AmazonRDS\)](#) 可協助您在中設定、操作和擴展關聯式資料庫 (DB) AWS 雲端。靜態加密的資料包括資料庫執行個體的基礎儲存體、其自動化備份、僅供讀取複本，以及快照。

以下是可用來加密資料RDS庫執行個體中靜態資料的方法：

- 您可以使 AWS KMS keys用 AWS 受管金鑰或客戶受管金鑰來加密 Amazon RDS 資料庫執行個體。如需詳細資訊，請參閱本指南中的 [AWS Key Management Service](#)。
- Amazon RDS 適用於 Oracle 和 Amazon 的SQL伺服器RDS支援使用透明資料加密 (TDE) 來加密資料庫執行個體。如需詳細資訊，請參閱 [Oracle 通透資料加密或SQL伺服器中的通透資料加密 Support](#)。

您可以同時使用TDE和KMS金鑰來加密資料庫執行個體。但是，這可能會稍微影響資料庫的效能，您必須分別管理這些金鑰。

以下是您可以用來加密往返資料庫執行個體或從資料RDS庫執行個體傳輸的資料的方法：

- 對於執行 Maria RDS DB、Microsoft SQL 伺服器、我SQL的、甲骨文或 Postgre 的 Amazon 資料庫執行個體SQL，您可以使用SSL來加密連線。如需詳細資訊，請參閱[使用SSL/TLS加密資料庫執行個體的連線](#)。
- Amazon RDS 版 Oracle 也支援 Oracle 原生網路加密 (NNE)，該加密功能會在資料庫執行個體進出資料時加密資料。NNE和SSL加密不能同時使用。如需詳細資訊，請參閱 [Oracle 原生網路加密](#)。

請考慮此服務的下列加密最佳實務：

- RDS為了處理、存放或SQL傳輸需要加密的資料，RDS請使用傳RDS輸加密功能連線到 Amazon 或 Amazon 以進行 Postgre 資料SQL庫執行個體進行連線加密。您可以在參數群組中將 `rds.force_ssl` 參數設定為 1 來實作此操作。如需詳細資訊，請參閱[使用參數群組](#)。Amazon 版 Oracle 使RDS用 Oracle 資料庫原生網路加密。
- RDS資料庫執行個體加密的客戶管理金鑰應該僅用於此目的，不得與任何其他金鑰搭配使用 AWS 服務。
- 在加密RDS資料庫執行個體之前，請先建立KMS金鑰需求。執行個體使用的金鑰以後無法變更。例如，在您的加密政策中，根據您的業務需求定義 AWS 受管理金鑰或客戶管理金鑰的使用和管理標準。

- 授權存取客戶管理的金KMS鑰時，請在原則中使用條件金鑰，遵循最低權限原則。IAM例如，若要允許客戶受管金鑰僅用於源自 Amazon 的請求RDS，請使用帶有`rds.<region>.amazonaws.com`值的 [kms: ViaService 條件金鑰](#)。此外，您可以使用 [Amazon RDS 加密環境](#) 中的金鑰或值做為使用客戶受管金鑰的條件。
- 強烈建議您為加密的RDS資料庫執行個體啟用備份。Amazon RDS 可能會失去對資料庫執行個體 KMS金鑰的存取權，例如KMS金鑰未啟用或KMS金鑰的RDS存取權被撤銷時。如果發生此情況，則加密的資料庫執行個體將進入可復原狀態七天。如果資料庫執行個體在七天後未重新取得對金鑰的存取權，則資料庫將變得最終無法存取，必須從備份還原。如需詳細資訊，請參閱[加密資料庫執行個體](#)。
- 如果僅供讀取複本與其加密的資料庫執行個體位於相同 AWS 區域，則必須使用相同的KMS金鑰來加密兩者。
- 在中 AWS Config，實作[rds-storage-encrypted](#) AWS 受管規則以驗證和強制執行資料RDS庫執行個體的加密，以及驗證和強制執行RDS資料庫快照集加密的[rds-snapshots-encrypted](#)規則。
- 用 AWS Security Hub 於評估您的 Amazon RDS 資源是否遵循安全最佳實務。如需詳細資訊，請參閱 [Amazon 的 Security Hub 控制項RDS](#)。

的加密最佳做法 AWS Secrets Manager

[AWS Secrets Manager](#)透過API呼叫 Secrets Manager 以程式設計方式擷取密碼，協助您取代程式碼中的硬式編碼認證 (包括密碼)。Secrets Manager 與 AWS KMS 整合，可使用受 AWS KMS key。此整合使用永遠不會保留 AWS KMS 未加密的加密金鑰來保護儲存的密碼。您也可以定義金KMS鑰的自訂權限，以稽核產生、加密和解密保護已儲存密碼之資料金鑰的作業。如需詳細資訊，請參閱 [AWS Secrets Manager](#)中的[機密加密和解密](#)。

請考慮此服務的下列加密最佳實務：

- 在金鑰原則中，使用 [kms: ViaService](#) 條件金鑰，透過指派值，將金鑰的使用限制為僅限來自 Secrets Manager 的要求`secretsmanager.<region>.amazonaws.com`。
- 為了獲得額外的安全性，請根據業務需求，使用 [Secrets Manager 加密內容](#) 中的金鑰或值作為使用金KMS鑰的條件，方法是建立下列項目：
 - IAM或金鑰原則中的[字串條件運算子](#)
 - 授權中的[授予限制條件](#)
- 在中 AWS Config，實作受[secretsmanager-using-cmk](#) AWS 管規則，以確認 Secrets Manager 中的所有密碼均使用 AWS 受管KMS金鑰或客戶管理KMS金鑰加密。
- 若要確保密碼符合定義的循環原則，請實作下列 AWS Config 規則：

- [secretsmanager-rotation-enabled-check](#)— 檢查是否針對秘密管理員中儲存的密碼設定輪換。
- [secretsmanager-scheduled-rotation-success-check](#) — 檢查密碼是否已成功輪替。AWS Config 還檢查上次旋轉的日期是否在配置的旋轉頻率內。
- [secretsmanager-secret-periodic-rotation](#)— 檢查是否在指定的天數內輪替密碼。
- [secretsmanager-secret-unused](#)— 檢查是否在指定天數內存取密碼。
- 用 AWS CloudTrail 於記錄 Secrets Manager 和非API事件的所有API呼叫，例如輪替開始、循環成功、循環失敗以及已排程的密碼刪除。如需詳細資訊，請參 [AWS Secrets Manager 閱使用 AWS CloudTrail](#)。
- 使用 [Amazon](#) 設 EventBridge 定某些 Secrets Manager 作業的警示，例如刪除機密、輪替密碼，或嘗試使用排定要刪除的密碼。您可以選擇觸發提醒的操作。該警報可以是 Amazon 簡單通知服務 (AmazonSNS) 主題，可傳送電子郵件或簡訊給訂閱者，也可以是記錄操作詳細資訊以供日後檢閱的 AWS Lambda 功能。

Amazon S3 的加密最佳實務

[Amazon Simple Storage Service \(Amazon S3\)](#) 是一種雲端型物件儲存服務，可協助您儲存、保護和擷取任何數量的資料。

對於 Amazon S3 中的伺服器端加密，有以下三個選項：

- [使用 Amazon S3 受管加密金鑰 \(SSE-S3\) 進行伺服器端加密](#)
- [伺服器端加密 AWS Key Management Service \(SSE-KMS\)](#)
- [使用客戶提供的加密金鑰 \(SSE-C\) 進行伺服器端](#)

Amazon S3 使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，做為 Amazon S3 中每個儲存貯體的加密基礎層級。從 2023 年 1 月 5 日起，所有上傳到 Amazon S3 的新物件都會自動加密，無需額外費用，也不會影響效能。S3 儲存貯體預設加密組態和新物件上傳的自動加密狀態可用於 AWS CloudTrail 日誌、S3 庫存、S3 儲存鏡頭、Amazon S3 主控台，以及 AWS Command Line Interface (AWS CLI) 和中的其他 Amazon S3 API 回應標頭 AWS SDKs。如需詳細資訊，請參閱 [預設加密FAQ](#)。

如果在上傳時使用伺服器端加密物件，請將標 `x-amz-server-side-encryption` 頭新增至請求，告知 Amazon S3 使用 SSE-S3 KMS、SSE-或-SSE C 加密物件。以下是標 `x-amz-server-side-encryption` 頭的可能值：

- AES256，可通知 Amazon S3 使用 Amazon S3 受管金鑰。

- `aws:kms`，這會告訴 Amazon S3 使用 AWS KMS 受管金鑰。
- 將值設為 `True` 或 `False` 用於 SSE-C

如需詳細資訊，請參閱 [Defense-in-depth 要求 1：靜態和傳輸期間資料必須加密](#)，請參閱 [如何使用儲存貯體政策和套用深度防禦以協助保護 Amazon S3 資料](#) (AWS 部落格文章)。

對於 Amazon S3 中的 [用戶端加密](#)，有以下兩個選項：

- 一個密鑰存儲在 AWS KMS
- 儲存在應用程式內的金鑰

請考慮此服務的下列加密最佳實務：

- 在中 AWS Config，實作 [bucket-server-side-encryption 啟用 s3](#) 的 AWS 受管規則，以驗證和強制執行 S3 儲存貯體加密。
- 部署 Amazon S3 儲存貯體政策，以驗證所有正在上傳的物件是否都使用 `s3:x-amz-server-side-encryption` 條件進行加密。如需詳細資訊，請參閱 [使用 SSE-S3 保護資料](#) 中的範例儲存貯體政策和 [新增儲存貯體政策中的](#) 指示。
- 使用 S3 儲存貯體政策上的 `aws:SecureTransport` 條件，僅允許透過 HTTPS (TLS) 加密連線。如需詳細資訊，請參閱 [我應該使用哪些 S3 儲存貯體政策來符合 s3- AWS Config 規則 bucket-ssl-requests-only ?](#)
- 在中 AWS Config，實作 [s3-bucket-ssl-requests-only](#) AWS 受管規則以要求使用請求 SSL。
- 在您需要授予 Amazon S3 物件的跨帳戶存取權時，使用客戶受管金鑰。設定金鑰政策，以允許透過其他 AWS 帳戶存取。

Amazon 的加密最佳實踐 VPC

[Amazon Virtual Private Cloud \(AmazonVPC\)](#) 可協助您將 AWS 資源啟動到已定義的虛擬網路中。此虛擬網路與您在自己的資料中心中操作的傳統網路相似，且具備使用 AWS 可擴展基礎設施的優勢。

請考慮此服務的下列加密最佳實務：

- 加密企業網路內的資訊資產與系統之間的流量，並 VPCs 使用下列其中一種方式：
 - AWS Site-to-Site VPN 連接
 - AWS Site-to-Site VPN 和 AWS Direct Connect 連接的組合，它提供了一個 IPsec-加密的私人連接

- AWS Direct Connect 支援 Sec MAC urity (MACsec) 的連線，可將資料從公司網路加密到該 AWS Direct Connect 位置
- 使用中 AWS PrivateLink 的VPC端點將您的端點私密連接VPCs到支持，AWS 服務 而無需使用互聯網閘道。您可以使用 AWS Direct Connect 或 AWS VPN 服務來建立此連線。您VPC與其他服務之間的流量不會離開 AWS 網路。如需詳細資訊，請參閱[存取 AWS 服務 透過 AWS PrivateLink](#)。
- 設定僅允許來自與[安全通訊協定相關聯之連接埠的流量的安全群組規則](#)，例如HTTPS超過 TCP /443。定期稽核安全群組及其規則。

資源

- [建立靜態資料的企業加密策略](#) (AWS 規範指南)
- AWS Key Management Service(AWS KMS 文件) [的安全性最佳做法](#)
- [如何 AWS 服務 使用 AWS KMS](#) (AWS KMS 文檔)
- [安全支柱：數據保護](#) (AWS Well-Architected 的框架)

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關 future 更新的通知，您可以訂閱[RSS摘要](#)。

變更	描述	日期
AWS 服務 更新	我們更新了 Amazon Elastic Kubernetes Service (Amazon) ， AWS Encryption SDK Amazon 關係數據庫服務 (AmazonEKS) 和亞馬遜簡單存儲服務 (亞馬遜 S3RDS) 的信息和建議。	2024年9月4日
初次出版	—	2022 年 12 月 2 日

AWS 規定指引詞彙

以下是 AWS 規範性指引所提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora Postgre SQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Relational Database Service 服務 (AmazonRDS)，適用於 AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的內部部署 Oracle 資料庫移轉至中 EC2 執行個體上的 Oracle 資料庫 AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V 應用程式移轉至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱以 [屬性為基礎的存取控制](#)。

抽象的服務

請參閱[受管理服務](#)。

ACID

請參閱[原子性、一致性、隔離性、耐用性](#)。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它比[主動-被動遷移](#)更具彈性，但需要更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

聚合函數

此SQL函數會在一組資料列上運作，並計算群組的單一傳回值。彙總函式的範例包括SUM和MAX。

AI

請參閱[人工智慧](#)。

AIOps

請參閱[人工智慧作業](#)。

匿名化

永久刪除資料集中個人資訊的程序。匿名化可以幫助保護個人隱私。匿名資料不再被視為個人資料。

反模式

一種常用的解決方案，用於重複發生的問題，其中解決方案是適得其反，無效，或者比替代方案效果低。

應用控制

一種安全性方法，只允許使用核准的應用程式，以協助保護系統免受惡意軟體的攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是[產品組合探索和分析程序](#)的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱[什麼是人工智慧？](#)

人工智能操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何 AIOps 在 AWS 移轉策略中使用的詳細資訊，請參閱[作業整合指南](#)。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性，一致性，隔離性，持久性 () ACID

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

以屬性為基礎的存取控制 () ABAC

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請[參閱](#) [AWS Identity and Access Management \(IAM\) 文件](#) AWS 中的「」。

授權資料來源

儲存資料主要版本的位置，被認為是最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以便處理或修改資料，例如匿名化、編輯或將其虛擬化。

可用區域

一個獨立的位置，與其他 AWS 區域 可用區域中的故障隔離，並為相同區域中的其他可用區域提供廉價、低延遲的網路連線能力。

AWS 雲端採用架構 (AWS CAF)

指導方針和最佳做法的架構，可協 AWS 助組織制定有效率且有效的計畫，以順利移轉至雲端。AWS CAF 將指引組織到六個重點領域中，稱為「觀點」：商業、人員、治理、平台、安全性和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。針對此觀點，AWS CAF 提供人員開發、訓練和通訊的指引，協助組織為成功採用雲端做好準備。如需詳細資訊，請參閱[AWS CAF 網站](#)和[AWS CAF 白皮書](#)。

AWS 工作負載資格架構 (AWS WQF)

可評估資料庫移轉工作負載、建議移轉策略並提供工作預估的工具。AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

壞機器人

旨在破壞或對個人或組織造成傷害的[機器人](#)。

BCP

請參閱[業務連續性規劃](#)。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以使用 Amazon Detective 的行為圖表來檢查失敗的登入嘗試、可疑 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的[行為圖中的資料](#)。

大端序系統

首先儲存最高有效位元組的系統。另請參閱「[位元順序](#)」。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

建立兩個獨立但相同環境的部署策略。您可以在一個環境中執行目前的應用程式版本 (藍色)，而在另一個環境 (綠色) 中執行新的應用程式版本。此策略可協助您以最小的影響快速回復。

機器人

透過網際網路執行自動化工作並模擬人類活動或互動的軟體應用程式。某些漫遊器是有用的或有益的，例如用於索引 Internet 上信息的網絡爬蟲。其他一些機器人 (稱為不良機器人) 旨在破壞或對個人或組織造成傷害。

殭屍網絡

受**惡意軟件**感染並受到單一方（稱為**機器人牧民**或**機器人操作員**）控制的**機器人網絡**。殭屍網絡是擴展**機器人**及其影響的最著名機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為**功能分支**。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱[關於分支](#) (GitHub 文件)。

防碎玻璃訪問

在特殊情況下，並透過核准的程序，使用者可以快速取得他 AWS 帳戶 們通常沒有存取權限的存取權。如需詳細資訊，請參閱 AWS Well-Architected 指南中的[實作防破玻璃程序](#)指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和**綠地**策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值（例如，銷售、客戶服務或營銷）。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在[AWS上執行容器化微服務](#)白皮書的[圍繞業務能力進行組織](#)部分。

業務連續性規劃 (BCP)

一種解決破壞性事件（如大規模遷移）對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱[AWS 雲端採用架構](#)。

金絲雀部署

向最終用戶發行版本的緩慢和增量版本。當您有信心時，您可以部署新版本並完全取代目前的版本。

CCoE

請參閱[雲端卓越中心](#)。

CDC

請參閱[變更資料擷取](#)。

更改數據捕獲 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更改的中繼資料的程序。您可以將其用CDC於各種目的，例如稽核或複寫目標系統中的變更，以維護同步化。

混沌工程

故意引入故障或破壞性事件來測試系統的彈性。您可以使用 [AWS Fault Injection Service \(AWS FIS\)](#) 執行實驗來 stress 您的 AWS 工作負載並評估其回應。

CI/CD

請參閱[持續整合和持續交付](#)。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的[CCoE文章](#)。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲計算通常連接到[邊緣計算](#)技術。

雲端運作模式

在 IT 組織中，這是用來建置、成熟和最佳化一或多個雲端環境的作業模型。如需詳細資訊，請參閱[建立您的雲端作業模型](#)。

採用雲端階段

組織移轉至下列四個階段時通常會經歷 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 — 進行基礎投資以擴展雲端採用率 (例如，建立 landing zone、定義 CCoE、建立營運模式)
- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段是 Stephen Orban 在 AWS 雲端 企業策略部落格部落格文章 [「邁向雲端優先的旅程與採用階段」](#) 中所定義的。如需其與 AWS 移轉策略之間關聯的詳細資訊，請參閱 [移轉準備指南](#)。

CMDB

請參閱 [組態管理資料庫](#)。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲儲存庫包括 GitHub 或 AWS CodeCommit。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料。查詢此類資料時，通常可以接受慢速查詢。將此資料移至效能較低且成本較低的儲存層或類別可降低成本。

計算機視覺 (CV)

一個 [AI](#) 領域，它使用機器學習來分析和從數字圖像和視頻等視覺格式中提取信息。例如，提 AWS Panorama 供將 CV 添加到現場部署攝像機網絡的設備，Amazon 為 CV SageMaker 提供圖像處理算法。

配置漂移

對於工作負載，組態會從預期的狀態變更。這可能會導致工作負載變得不合規，而且通常是漸進且無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常會 CMDB 在移轉的產品組合探索和分析階段使用資料。

一致性套件

AWS Config 規則和補救動作的集合，您可以組合這些動作來自訂合規性和安全性檢查。您可以使用範本，將一致性套件部署為 AWS 帳戶和區域中的單一YAML實體，或跨組織部署。如需詳細資訊，請參閱文件中的[AWS Config 一致性套件](#)。

持續整合和持續交付 (CI/CD)

自動化軟體發程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱[持續交付的優點](#)。CD 也可表示持續部署。如需詳細資訊，請參閱[持續交付與持續部署](#)。

CV

請參閱[電腦視覺](#)。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected 架構中安全性支柱的一個組成部分。如需詳細資訊，請參閱[資料分類](#)。

資料漂移

生產資料與用來訓練 ML 模型的資料之間有意義的變化，或輸入資料隨著時間的推移有意義的變化。資料漂移可降低 ML 模型預測中的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

透過集中式管理和控管，提供分散式、分散式資料擁有權的架構架構。

資料最小化

僅收集和處理絕對必要的數據的原則。在中執行資料最小化 AWS 雲端可降低隱私權風險、成本和分析碳足跡。

資料周長

您 AWS 環境中的一組預防性護欄，可協助確保只有受信任的身分正在存取來自預期網路的受信任資源。若要取得更多資訊，請參閱 [〈在上建立資料周長〉](#) AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

數據來源

在整個生命週期中追蹤資料來源和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧 (例如分析) 的資料管理系統。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫操作語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱 [資料庫定義語言](#)。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

defense-in-depth

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。在上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層加入多個控制項，以協助保護資源。例如，— defense-in-depth 種方法可能會結合多因素驗證、網路分段和加密。

委派的管理員

在中 AWS Organizations，相容的服務可以註冊成 AWS 員帳戶，以管理組織的帳戶並管理該服務的權限。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的 [可搭配 AWS Organizations 運作的服務](#)。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 [環境](#)。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS 上實作安全控制中的 [偵測性控制](#)。

發展價值流映射 (DVSM)

用於識別限制並排定優先順序，對軟體開發生命週期中的速度和品質產生不利影響的程序。DVSM 擴展了最初為精益生產實踐而設計的價值流映射過程。它著重於創造和通過軟件開發過程中移動價值所需的步驟和團隊。

數字雙胞胎

真實世界系統的虛擬表現法，例如建築物、工廠、工業設備或生產線。數位雙胞胎支援預測性維護、遠端監控和生產最佳化。

維度表

在 [star 結構描述](#) 中，較小的資料表包含事實資料表中定量資料的相關資料屬性。維度表格屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標籤。

災難

防止工作負載或系統在其主要部署位置達成其業務目標的事件。這些事件可能是自然災害、技術故障或人為行為造成的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您使用的策略和程序，將因 [災難](#) 造成的停機時間和資料遺失降到最低。如需詳細資訊，請參閱 AWS Well-Architected [的架構中的雲端中的工作負載的災難復原](#) [AWS：雲端復原](#)。

DML

請參閱[資料庫操作語言](#)。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需如何使用網域導向設計搭配絞死程式圖案的詳細資訊，請參閱[現代化舊版 Microsoft .ASP.NET \(ASMX \) 通過使用容器和 Amazon 網API關逐步增量的 Web 服務](#)。

博士

請參閱[災難復原](#)。

漂移檢測

追蹤基線組態的偏差。例如，您可以用 AWS CloudFormation 來[偵測系統資源中的漂移](#)，也可以用 AWS Control Tower 來[偵測 landing zone 中可能會影響法規遵循治理要求的變更](#)。

DVSM

請參閱[開發價值流映射](#)。

E

EDA

請參閱[探索性資料分析](#)。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與[雲計算](#)相比，邊緣計算可以減少通信延遲並縮短響應時間。

加密

一種計算過程，將純文本數據（這是人類可讀的）轉換為密文。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱[服務端點](#)。

端點服務

您可以在虛擬私有雲 (VPC) 中託管以與其他使用者共用的服務。您可以建立端點服務，AWS PrivateLink 並將權限授與其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 主體。這些帳戶或主體可以透過建立介面端點私下連線到您的 VPC 端點服務。如需詳細資訊，請參閱 Amazon 虛擬私有雲端 ([Amazon VPC](#)) 文件中的[建立端點服務](#)。

企業資源規劃 (ERP)

自動化和**管理**企業關鍵業務流程 (例如會計和專案管理) 的系統。[MES](#)

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的[信封加密](#)。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如，AWS CAF 安全史詩包括身分識別和存取管理、偵探控制、基礎架構安全性、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱[計畫實作指南](#)。

ERP

請參閱[企業資源規劃](#)。

探索性資料分析 () EDA

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。EDA通過計算摘要統計和創建數據可視化來執行。

F

事實表

[星型架構](#)中的中央表格。它存儲有關業務運營的定量數據。事實資料表通常包含兩種類型的資料欄：包含計量的資料欄，以及包含維度表格外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來減少開發生命週期的理念。這是敏捷方法的關鍵組成部分。

故障隔離邊界

在中 AWS 雲端，可用區域、AWS 區域控制平面或資料平面等界限，可限制故障影響並協助改善工作負載的彈性。如需詳細資訊，請參閱[AWS 錯誤隔離邊界](#)。

功能分支

請參閱[分支](#)。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以通過各種技術計算的數值得分，例如 Shapley 加法解釋 (SHAP) 和集成漸變。如需詳細資訊，請參閱[機器學習模型可解釋性：AWS](#)。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

FGAC

請參閱[精細的存取控制](#)。

精細的存取控制 () FGAC

使用多個條件來允許或拒絕訪問請求。

閃切遷移

一種資料庫移轉方法，透過[變更資料擷取使用連續資料](#)複寫，在最短的時間內移轉資料，而不是使用階段化方法。目標是將停機時間降至最低。

G

地理阻塞

請參閱[地理限制](#)。

地理限制 (地理封鎖)

在 Amazon 中 CloudFront，防止特定國家/地區的使用者存取內容分發的選項。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的[限制內容的地理分佈](#)。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被認為是遺留的，[基於主幹的工作流程是現代的首選方法](#)。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為[棕地](#)。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位控管資源、原則和合規性的高階規則 (OUs)。預防性防護機制會強制執行政策，以確保符合合規標準。它們是透過使用服務控制原則和IAM權限界限來實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是通過使用 AWS Config，Amazon AWS Security Hub GuardDuty，AWS Trusted Advisor亞馬遜檢查 Amazon Inspector 和自定義 AWS Lambda 檢查來實現的。

H

公頃

查看[高可用性](#)。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如, Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分, 而轉換結構描述可能是一項複雜任務。[AWS 提供有助於結構描述轉換的 AWS SCT](#)。

高可用性 (HA)

工作負載在遇到挑戰或災難時持續運作的能力, 無需干預。HA 系統的設計可自動容錯移轉、持續提供高品質的效能, 以及處理不同的負載和故障, 並將效能影響降到最低。

歷史學家現代化

一種用於現代化和升級操作技術 (OT) 系統的方法, 以更好地滿足製造業的需求。歷史學家是一種類型的數據庫, 用於收集和存儲工廠中的各種來源的數據。

異質資料庫遷移

將您的來源資料庫遷移到共用相同資料庫引擎的目標資料庫 (例如, Microsoft SQL 伺服器至 Amazon RDS 伺服器版SQL伺服器)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱數據

經常存取的資料, 例如即時資料或最近的轉譯資料。此資料通常需要高效能的儲存層或類別, 才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性, 修補程式通常是在典型的 DevOps 發行工作流程之外進行。

超級護理期間

在切換後, 遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常, 此期間的長度為 1-4 天。在超級護理期間結束時, 遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

IaC

查看[基礎結構即程式碼](#)。

身分型政策

附加至一或多個IAM主參與者的原則, 可定義其在 AWS 雲端環境中的權限。

閒置應用程式

在 90 天內，平均記憶 CPU 體使用量介於 5% 到 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱[工業物聯網](#)。

不可變基礎設施

為生產工作負載部署新基礎結構的模型，而不是更新、修補或修改現有基礎結構。[不可變的基礎架構本質上比可變基礎架構更加一致、可靠且可預測](#)。如需詳細資訊，請參閱 Well-Architected 的架構中的[使用不可變基礎結構 AWS 構進行部署最佳作法](#)。

入境 (入口) VPC

在 AWS 多帳戶架構中，可接 VPC 受、檢查和路由來自應用程式外部的網路連線。[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您 VPCs 的應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

[Klaus Schwab](#) 於 2016 年推出的一個術語，指的是透過連線能力、即時資料、自動化、分析和 AI/ML 的進步來實現製造流程的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱[建立工業物聯網 \(IIoT\) 數位轉型策略](#)。

檢查 VPC

在 AWS 多帳戶架構中，集中 VPC 管理 VPCs (相同或不同 AWS 區域)、Internet 和內部部署網絡之間的網絡流量檢查。[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您的 VPCs 的應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱[什麼是 IoT ?](#)

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱[機器學習模型可解釋性 AWS](#)。

IoT

請參閱[物聯網](#)。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需將雲端作業與 ITSM 工具整合的相關資訊，請參閱[作業整合指南](#)。

ITIL

請參閱[IT 資訊庫](#)。

ITSM

請參閱[IT 服務管理](#)。

L

基於標籤的訪問控制 () LBAC

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派了一個安全性標籤值。使用者安全性標籤與資料安全性標籤之間的交集決定了使用者可以看到哪些列與欄。

登陸區域

landing zone 是一個架構良好的多帳戶 AWS 環境，具有可擴展性和安全性。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱[設定安全且可擴展的多帳戶 AWS 環境](#)。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱以[標示為基礎的存取控制](#)。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱文件IAM中的[套用最低權限權限](#)。

隨即轉移

見 [7 盧比](#)

小端序系統

首先儲存最低有效位元組的系統。另請參閱 [「位元順序」](#)。

較低的環境

請參閱[環境](#)。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱[機器學習](#)。

主要分支

請參閱[分支](#)。

惡意軟體

旨在危及計算機安全性或隱私的軟件。惡意軟件可能會破壞計算機系統，洩漏敏感信息或獲得未經授權的訪問。惡意軟體的例子包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、間諜軟體和鍵盤記錄程式。

受管理服務

AWS 服務用於 AWS 操作基礎架構層、作業系統和平台，並且您可以存取端點以儲存和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也被稱為抽象的服務。

製造執行系統 (MES)

用於跟踪，監控，記錄和控制生產過程的軟件系統，可在現場將原材料轉換為成品。

MAP

請參閱 [Migration Acceleration Program](#)。

機制

一個完整的過程，您可以在其中創建工具，推動工具的採用，然後檢查結果以進行調整。機制是一個循環，它加強和改善自己，因為它運行。如需詳細資訊，請參閱 AWS Well-Architected 的架構中 [建置機制](#)。

成員帳戶

屬於 AWS 帳戶中組織的管理帳戶以外的所有帳戶 AWS Organizations。一個帳戶一次只能是一個組織的成員。

MES

請參閱 [製造執行系統](#)。

郵件佇列遙測傳輸 (MQTT)

[以發佈/訂閱模式為基礎的輕量型 machine-to-machine \(M2M\) 通訊協定，適用於資源受限 IoT 裝置。](#)

微服務

一個小型的獨立服務，通過明確定義的溝通 APIs，通常由小型，獨立的團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱 [使用 AWS 無伺服器服務整合微服務](#)。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務通過使用輕量級通過明確定義的接口進行通信。APIs 此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱 [上 AWS 的實作微服務](#)。

Migration Acceleration Program (MAP)

提供諮詢支援、訓練和服務的 AWS 計畫，協助組織為移轉至雲端建立穩固的營運基礎，並協助抵消移轉的初始成本。MAP 包含用於以有條理的方式執行舊版移轉的移轉方法，以及一組可自動化和加速常見移轉案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 [AWS 遷移策略](#) 的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。移轉工廠團隊通常包括營運、業務分析師和擁有者、移轉工程師、開發人員和 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的 [遷移工廠的討論](#) 和 [雲端遷移工廠指南](#)。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。移轉中繼資料的範例包括目標子網路、安全性群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：EC2 使用 AWS 用應用程式遷移服務將遷移重新託管至 Amazon。

移轉組合評估 (MPA)

這是一種線上工具，可提供驗證要移轉至的商業案例的 AWS 雲端資訊。MPA 提供詳細的產品組合評估 (伺服器適當大小、定價、TCO 比較、移轉成本分析) 以及移轉規劃 (應用程式資料分析與資料收集、應用程式分組、移轉優先順序，以及波浪規劃)。所有 AWS 顧問和 APN 合作夥伴顧問均可免費使用該 [MPA 工具](#) (需要登錄)。

移轉準備程度評估 (MRA)

取得有關組織雲端準備狀態的深入解析、識別優勢和弱點，以及建立行動計劃以縮小已識別差距的程序，使用 AWS CAF。如需詳細資訊，請參閱 [遷移準備程度指南](#)。MRA 是 [AWS 移轉策略](#) 的第一階段。

遷移策略

將工作負載移轉至 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 [7 Rs](#) 項目，並參閱 [動員您的組織以加速大規模移轉](#)。

機器學習 (ML)

請參閱[機器學習](#)。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱[AWS 雲端](#)

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱[評估應用程式的現代化準備程度 AWS 雲端](#)。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱[將單一體系分解為微服務](#)。

MPA

請參閱[移轉組合評估](#)。

MQTT

請參閱[佇列遙測傳輸](#)的郵件。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」或者「這個客戶對哪種產品類別最感興趣？」

可變的基礎

更新和修改生產工作負載現有基礎結構的模型。為了提高一致性，可靠性和可預測性，AWS Well-Architected 框架建議使用[不可變的基礎結構](#)作為最佳實踐。

O

OAC

請參閱[原始存取控制](#)。

OAI

請參閱[原始存取身分](#)。

OCM

請參閱[組織變更管理](#)。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱[作業整合](#)。

OLA

請參閱[作業層級協定](#)。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱[開放程序通訊-統一架構](#)。

開放程序通訊-統一架構 (OPC-UA)

用於工業自動化的 machine-to-machine (M2M) 通訊協定。OPC-UA 提供了具有數據加密，身份驗證和授權方案的互操作性標準。

作業層級協定 () OLA

一份協議，闡明哪些功能 IT 群組承諾互相交付，以支援服務等級協議 () SLA。

操作準備審查 (ORR)

問題和相關最佳做法的檢查清單，可協助您瞭解、評估、預防或減少事件和可能的故障範圍。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的[作業準備檢閱 \(ORR\)](#)。

操作技術

可與實體環境搭配使用的硬體和軟體系統，以控制工業作業、設備和基礎設施。在製造業中，整合 OT 和資訊技術 (IT) 系統是[工業 4.0](#) 轉型的關鍵焦點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱[操作整合指南](#)。

組織追蹤

由建立的追蹤 AWS CloudTrail 記錄中組織 AWS 帳戶 中所有人的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱[CloudTrail文件中的為組織建立追蹤](#)。

組織變革管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM透過加速變更採用、解決過渡問題，以及推動文化和組織變革，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 移轉策略中，這個架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱[OCM指南](#)。

原點存取控制 (OAC)

在中 CloudFront，限制存取權限以保護 Amazon Simple Storage Service (Amazon S3) 內容的增強選項。OAC支援所有 S3 儲存貯體 AWS 區域、伺服器端加密 AWS KMS (SSE-KMS)，以及 S3 儲存貯體的動態PUT和DELETE請求。

原點存取識別 (OAI)

在中 CloudFront，用於限制存取以保護 Amazon S3 內容的選項。使用時OAI，CloudFront 會建立 Amazon S3 可用來進行驗證的主體。經驗證的主體只能透過特定散發存取 S3 儲存 CloudFront 貯體中的內容。另請參閱 [OAC](#)，其中提供更精細且增強的存取控制。

ORR

請參閱[作業整備檢閱](#)。

OT

請參閱[操作技術](#)。

出站 (出口) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動的網路連線。VPC[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您VPCs的應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附加至IAM主參與者的IAM管理原則，可設定使用者或角色可擁有的最大權限。如需詳細資訊，請參閱IAM文件中的[權限界限](#)。

個人身份信息 (PII)

直接查看或與其他相關數據配對時，可用於合理推斷個人身份的信息。PII包括姓名、地址和聯絡資訊的範例。

PII

請參閱[個人識別資訊](#)。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱[可編程邏輯控制器](#)

PLM

請參閱[產品生命週期管理](#)

政策

可以定義權限 (請參閱以[身分識別為基礎的策略](#))、指定存取條件 (請參閱以[資源為基礎的策略](#)) 或定義組織中所有帳戶的最大權限的物件 AWS Organizations (請參閱[服務控制策略](#))。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱[在微服務中啟用資料持久性](#)。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱[評估遷移準備程度](#)。

述詞

傳回true或的查詢條件false，通常位於子WHERE句中。

謂詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這樣可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS 上實作安全控制中的[預防性控制](#)。

委託人

中 AWS 可執行動作和存取資源的實體。此實體通常是IAM角色或使用 AWS 帳戶者的根使用者。如需詳細資訊，請參閱IAM文件中[角色術語與概念](#)中的主參與者。

隱私設計

一種系統工程方法，在整個工程過程中將隱私權納入考量。

私有託管區域

一種容器，其中包含有關您希望 Amazon Route 53 如何回應一或多VPCs個網域內網域及其子網域的DNS查詢的相關資訊。如需詳細資訊，請參閱 Route 53 文件中的[使用私有託管區域](#)。

主動控制

一種[安全控制項](#)，旨在防止部署不符合規範的資源。這些控制項會在資源佈建之前進行掃描。如果資源不符合控制項，則不會佈建該資源。如需詳細資訊，請參閱 AWS Control Tower 文件中的[控制項參考指南](#)，並參閱實作安全性[控制中的主動](#)控制 AWS。

產品生命週期管理 (PLM)

在產品的整個生命週期中管理資料和流程，從設計、開發、上市到成長與成熟度，再到下降和移除。

生產環境

請參閱[環境](#)。

可編程邏輯控制器 (PLC)

在製造業中，一台高度可靠且適應性強的計算機，可監控機器並自動化製造過程。

化名化

以預留位置值取代資料集中的個人識別碼的程序。假名化可以幫助保護個人隱私。假名化數據仍被認為是個人數據。

發布/訂閱 (發布/訂閱)

一種模式，可在微服務之間實現非同步通訊，以提高延展性和回應能力 例如，在以微服務為基礎的微服務中 [MES](#)，微服務可以將事件訊息發佈到其他微服務可訂閱的通道。系統可以在不變更發佈服務的情況下新增微服務。

Q

查詢計劃

一系列步驟，如指令，用來存取關聯式資料SQL庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI矩陣

見[負責任，負責，諮詢，通知 \(\) RACI](#)。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI矩陣

見[負責任，負責，諮詢，通知 \(\) RACI](#)。

RCAC

請參閱[列與欄存取控制](#)。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新建築師

見 [7 盧比](#)

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這決定了最後一個恢復點和服務中斷之間可接受的數據丟失。

恢復時間目標 (RTO)

服務中斷與恢復服務之間的最大可接受延遲。

重構

見 [7 盧比](#)

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 是隔離和獨立於其他的，以提供容錯能力，穩定性和彈性。如需詳細資訊，請參閱[指定 AWS 區域 您的帳戶可以使用的項目](#)。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新主持

見 [7 盧比](#)

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

見 [7 盧比](#)

再平台

見 [7 盧比](#)

買回

見 [7 盧比](#)

彈性

應用程式抵抗或從中斷中復原的能力。在規劃備援時，[高可用性](#)和[災難復原](#)是常見的考量因素。AWS 雲端如需詳細資訊，請參閱[AWS 雲端 復原力](#)。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責，負責，諮詢，通知 () 矩陣 RACI

定義移轉活動和雲端作業所涉及之所有各方的角色與責任的矩陣。矩陣名稱衍生自矩陣中定義的責任型別：負責 (R)、負責 (A)、諮詢 (C) 及通知 (I)。支撐 (S) 類型是可選的。如果包括支持，則該矩陣稱為RASCI矩陣，如果將其排除，則稱為RACI矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS 上實作安全控制中的[回應性控制](#)。

保留

見 [7 盧比](#)

退休

見 [7 盧比](#)

旋轉

定期更新[密碼](#)以使攻擊者更難以存取認證的程序。

列與欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性SQL運算式。RCAC由列權限和欄遮罩組成。

RPO

請參閱[復原點目標](#)。

RTO

請參閱[復原時間目標](#)。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML2.0

許多身份提供者 (IdPs) 使用的開放標準。此功能可啟用同盟單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 作業，而不必 IAM 為組織中的每個人建立使用者。如需有關 SAML 2.0 型聯合的詳細資訊，請參閱說明文件中的[關於 SAML 以 2.0 為基礎的 IAM 聯合](#)。

SCADA

請參閱[監督控制和資料擷取](#)。

SCP

請參閱[服務控制策略](#)。

秘密

您以加密形式儲存的機密或受限制資訊，例如密碼或使用者認證。AWS Secrets Manager 它由秘密值及其中繼資料組成。密碼值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱「[Secrets Manager 碼中有什麼內容？](#)」在 Secrets Manager 文檔中。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全性控制有四種主要類型：[預防性](#)、[偵測](#)、[回應式](#)和[主動式](#)。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全信息和事件管理 (SIEM) 系統

結合安全性資訊管理 (SIM) 與安全性事件管理 (SEM) 系統的工具與服務。SIEM 系統收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生警示。

安全回應自動化

預先定義且程式化的動作，其設計用來自動回應或修復安全性事件。這些自動化作業可做為[偵探](#)或[回應式](#)安全控制項，協助您實作 AWS 安全性最佳實務。自動回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

在其目的地的數據加密，通 AWS 服務 過接收它。

服務控制政策 (SCP)

為 AWS Organizations 中的組織的所有帳戶提供集中控制許可的政策。SCP 定義護欄或設定管理員可委派給使用者或角色的動作限制。您可以用 SCP 作允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的 [服務控制原則](#)。

服務端點

URL 的進入點的 AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 [AWS 服務端點](#)。

服務等級協議 () SLA

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務等級指示器 () SLI

對服務效能層面的測量，例如錯誤率、可用性或輸送量。

服務層級目標 () SLO

代表服務狀況的目標測量結果，由 [服務層次指示器](#) 測量。

共同責任模式

描述您在雲端安全性和合規方面共享的責任的模型。AWS 負責雲端的安全性，而您則負責雲端的安全性。如需詳細資訊，請參閱 [共同責任模式](#)。

SIEM

請參閱 [安全性資訊和事件管理系統](#)。

單點故障 (SPOF)

應用程式的單一重要元件發生故障，可能會中斷系統。

SLA

請參閱 [服務等級協議](#)。

SLI

請參閱 [服務層級指示器](#)。

SLO

請參閱 [服務等級目標](#)。

split-and-seed 模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱[中的應用程式現代化的階段化方法](#)。AWS 雲端

SPOF

請參閱[單一故障點](#)。

星型綱要

使用一個大型事實資料表來儲存交易或測量資料，並使用一或多個較小的維度表格來儲存資料屬性的資料庫組織結構。這種結構是專為在[數據倉庫](#)中使用或用於商業智能目的。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 [Martin Fowler 引入](#)，作為重寫單一系統時管理風險的方式。如需如何套用此模式的範例，請參閱[現代化舊版 Microsoft ASP.NET \(ASMX \) 通過使用容器和 Amazon 網API關逐步增量的 Web 服務](#)。

子網

您的VPC. 子網必須位於單一可用區域。

監督控制與資料擷取 () SCADA

在製造業中，使用硬體與軟體來監控實體資產與生產作業的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動以偵測潛在問題或監控效能的方式測試系統。您可以使用 [Amazon CloudWatch Synthetics](#) 來創建這些測試。

T

標籤

作為組織 AWS 資源的中繼資料的索引鍵值配對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱[標記您的 AWS 資源](#)。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱[環境](#)。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可用來互連VPCs與內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的[傳輸閘道是什麼](#)。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

授與權限給您指定的服務，以代表您在組織內 AWS Organizations 及其帳戶中執行工作。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 AWS Organizations 文件中的[AWS Organizations 與其他 AWS 服務搭配使用](#)。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

一個小 DevOps 團隊，你可以餵兩個比薩餅。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱[量化深度學習系統的不確定性](#)指南。

無差別的任務

也稱為繁重工作，是創建和操作應用程序所必需的工作，但不能為最終用戶提供直接價值或提供競爭優勢。無差異化作業的範例包括採購、維護和容量規劃。

較高的環境

請參閱[環境](#)。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC凝視

兩者之間的連線VPCs，可讓您使用私有 IP 位址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的[什麼是對VPC等互連](#)。

漏洞

會危及系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

溫暖的數據

不常存取的資料。查詢此類資料時，通常可以接受中度緩慢的查詢。

視窗功能

一種SQL函數，可對以某種方式與目前記錄相關的一組資料列執行計算。視窗函數對於處理工作非常有用，例如計算移動平均值或根據目前列的相對位置存取列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器 and 應用程式。

WORM

看到 [寫一次，多讀](#)。

WQF

請參閱 [AWS工作負載限定架構](#)

寫一次，多讀 (WORM)

一種儲存模型，可單次寫入資料並防止資料遭到刪除或修改。授權用戶可以根據需要多次讀取數據，但無法更改數據。這種數據存儲基礎設施被認為是 [不可變](#) 的。

Z

零日漏洞利用

一種利用 [零時差漏洞](#) 的攻擊，通常是惡意軟件。

零時差漏洞

生產系統中未緩解的瑕疵或弱點。威脅參與者可以利用這種類型的漏洞攻擊系統。由於攻擊，開發人員經常意識到該漏洞。

殭屍應用程式

具有平均CPU且記憶體使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。