



使用者指南

# AWS Audit Manager



# AWS Audit Manager: 使用者指南

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

什麼是 AWS Audit Manager ? .....	1
功能 AWS Audit Manager .....	1
定價 AWS Audit Manager .....	2
您第一次使用 Audit Manager 嗎? .....	2
更多 AWS Audit Manager 資源 .....	3
理解概念和術語 .....	3
A .....	3
C .....	5
D .....	8
E .....	10
F .....	13
R .....	14
S .....	15
了解證據收集 .....	16
證據收集頻率 .....	17
控制項範例 .....	18
自動化控制 (Security Hub) .....	19
自動化控制 (AWS Config) .....	20
自動化控制項 (API 呼叫) .....	22
自動化控制 (CloudTrail) .....	23
手動控制 .....	25
具有混合資料來源的控制項 .....	26
AWS 服務 整合 .....	28
第三方 GRC 整合 .....	29
了解第三方整合 .....	30
支援的第三方 GRC 產品 .....	31
將 Audit Manager 證據整合至您的 GRC 系統 .....	32
必要條件 .....	33
步驟 1 : 啟用 Audit Manager .....	33
步驟 2 : 設定權限 .....	34
步驟 3 : 地圖控制項 .....	37
步驟 4 : 保持映射更新 .....	39
步驟 5 : 建立評估 .....	41
步驟 6. 收集證據 .....	41

定價 .....	42
其他資源 .....	42
支援的架構 .....	44
ACSC 基本八項 .....	45
什麼是基本八項？ .....	45
使用此架構 .....	46
後續步驟 .....	46
其他資源 .....	47
ACSC ISM .....	47
什麼是 ACSC ISM？ .....	47
使用此架構 .....	47
後續步驟 .....	48
其他資源 .....	48
AWS Audit Manager 示例框架 .....	48
什麼是示 AWS Audit Manager 例框架？ .....	49
使用此架構 .....	49
後續步驟 .....	50
AWS Control Tower 護欄 .....	50
什麼是 AWS Control Tower？ .....	50
使用此架構 .....	50
後續步驟 .....	51
其他資源 .....	51
AWS 生成式 AI 最佳實務 .....	52
Amazon 基岩的 AWS 生成 AI 最佳實務是什麼？ .....	52
使用此架構 .....	54
在 Amazon Bedrock 中手動驗證提示 .....	55
後續步驟 .....	57
其他資源 .....	58
AWS License Manager .....	58
什麼是 AWS License Manager？ .....	58
使用此架構 .....	59
後續步驟 .....	59
其他資源 .....	59
AWS 基礎安全性最佳做法 .....	60
什麼是 AWS 基礎安全最佳實務標準？ .....	60
使用此架構 .....	61

後續步驟 .....	61
其他資源 .....	61
AWS 營運最佳實務 .....	62
什麼是 AWS 基礎安全性最佳做法標準？ .....	62
使用此架構 .....	62
後續步驟 .....	63
其他資源 .....	63
AWS 架構良好的框架 WAF V10 .....	63
什麼是 AWS Well-Architected 的框架？ .....	63
使用此架構 .....	64
後續步驟 .....	64
其他資源 .....	61
CCCS 中型雲端控制設定檔 .....	65
什麼是中華基督教服務中心？ .....	65
使用此架構 .....	66
後續步驟 .....	67
獨聯體 AWS 基準 v.1.2 .....	67
什麼是 CIS？ .....	67
使用此架構 .....	68
後續步驟 .....	74
其他資源 .....	75
獨聯體 AWS 基準 v.1.3 .....	75
什麼是 AWS 獨聯體基準？ .....	75
使用這些架構 .....	76
後續步驟 .....	77
其他資源 .....	77
獨聯體 AWS 基準 v.1.4 .....	78
什麼是獨聯體 AWS 基準？ .....	78
使用這些架構 .....	79
後續步驟 .....	80
其他資源 .....	80
CIS 控制項 v7.1 IG1 .....	80
什麼是 CIS 控制項？ .....	81
使用此架構 .....	82
後續步驟 .....	82
其他資源 .....	83

獨聯體關鍵安全控制系統 8.0 版 .....	83
什麼是 CIS 控制項？ .....	83
使用此架構 .....	84
後續步驟 .....	85
其他資源 .....	85
安全性 FedRAMP 準控制項 r4 .....	85
什麼是 FedRAMP？ .....	85
使用此架構 .....	85
後續步驟 .....	86
其他資源 .....	86
GDPR .....	87
什麼是 GDPR？ .....	87
使用此架構 .....	87
後續步驟 .....	108
其他資源 .....	108
格爾巴 .....	108
什麼是綠色環球菌 (GLBA)？ .....	108
使用此架構 .....	108
後續步驟 .....	109
標題 21 CFR 第 11 部分 .....	109
甚麼是 CFR 第 11 部分的標題 21？ .....	110
使用此架構 .....	110
後續步驟 .....	111
其他資源 .....	111
歐盟 GMP 附件 11, V1 .....	111
什麼是歐盟 GMP 附件 11？ .....	111
使用此架構 .....	112
後續步驟 .....	113
HIPAA 安全性規則：2003 年 2 月 .....	113
什麼是 HIPAA 和 HIPAA 安全規則 2003？ .....	113
使用此架構 .....	114
後續步驟 .....	115
其他資源 .....	115
HIPAA 全方位最終規則 .....	115
什麼是 HIPAA 和 HIPAA Final Omnibus 安全規則？ .....	116
使用此架構 .....	114

後續步驟 .....	117
其他資源 .....	117
ISO/IEC 27001:2013 .....	117
什麼是 ISO/IEC 27001 ? .....	118
使用此架構 .....	118
後續步驟 .....	119
其他資源 .....	119
尼斯特 SP .....	119
什麼是尼斯特 .....	120
使用此架構 .....	120
後續步驟 .....	121
其他資源 .....	121
NIST CSF V1.1 .....	121
什麼是 NIST 網路安全架構 ? .....	122
使用此架構 .....	122
後續步驟 .....	123
其他資源 .....	123
尼斯特 SP .....	124
什麼是 NIST SP 800-171? .....	124
使用此架構 .....	124
後續步驟 .....	125
其他資源 .....	125
PCI DSS V3.2.1 .....	126
什麼是 PCI DSS ? .....	126
使用此架構 .....	126
後續步驟 .....	127
其他資源 .....	127
PCI DSS v4 .....	128
什麼是 PCI DSS ? .....	128
使用此架構 .....	129
後續步驟 .....	130
其他資源 .....	130
SSE -18 系統管理系統 2 .....	130
什麼是 SOC 2 ? .....	131
使用此架構 .....	131
後續步驟 .....	132

其他資源 .....	132
支援的資料來源 .....	133
重點 .....	133
後續步驟 .....	136
AWS Config .....	136
重點 .....	136
支援的 AWS Config 受管規則 .....	137
透過 Audit Manager 使用自訂規則 .....	149
其他資源 .....	149
AWS Security Hub .....	149
重點 .....	150
支援的 Security Hub 控制項 .....	161
其他資源 .....	184
AWS API 呼叫 .....	184
重點 .....	185
自訂控制項資料來源支援的 API 呼叫 .....	186
AWS License Manager API 呼叫 .....	195
其他資源 .....	196
AWS CloudTrail .....	196
其他資源 .....	197
設定 .....	198
必要條件 .....	198
註冊一個 AWS 帳戶 .....	199
建立具有管理權限的使用者 .....	199
新增必要許可 .....	200
後續步驟 .....	201
啟用 Audit Manager .....	201
必要條件 .....	202
程序 .....	202
後續步驟 .....	206
建議 .....	206
重點 .....	206
推薦功能 .....	206
建議整合 .....	207
後續步驟 .....	211
開始使用 .....	212



Audit Manager 教學 .....	212
稽核擁有者教學課程：建立評估 .....	213
必要條件 .....	213
程序 .....	213
其他資源 .....	215
委派教學課程：檢閱控制集 .....	216
必要條件 .....	216
程序 .....	216
其他資源 .....	220
使用 儀表板 .....	221
儀表板概念和術語 .....	221
儀表板元素 .....	223
評估篩選器 .....	223
每日快照 .....	223
依控制項網域分組的具不合規證據的控制項 .....	224
後續步驟 .....	226
其他資源 .....	227
評估 .....	228
重點 .....	228
其他資源 .....	228
建立評估 .....	229
必要條件 .....	229
程序 .....	230
後續步驟 .....	232
其他資源 .....	233
尋找評估 .....	233
必要條件 .....	233
程序 .....	233
後續步驟 .....	234
其他資源 .....	234
檢閱評估 .....	234
重點 .....	234
其他資源 .....	235
評估詳細資訊 .....	235
評估控制細節 .....	242
證據資料夾詳細 .....	247

證據詳情 .....	251
編輯評估 .....	254
必要條件 .....	254
程序 .....	254
後續步驟 .....	256
其他資源 .....	256
添加手動證據 .....	256
重點 .....	257
其他資源 .....	257
從 S3 匯入證據 .....	258
從瀏覽器上傳證據 .....	260
輸入文字作為證據 .....	264
支援檔案格式 .....	266
準備評估報告 .....	267
重點 .....	267
其他資源 .....	267
將證據添加至評估報告 .....	268
從評估報告中移除證據 .....	269
產生評估報告 .....	270
變更評估控制狀態 .....	272
必要條件 .....	272
程序 .....	272
後續步驟 .....	274
變更評估狀態 .....	274
必要條件 .....	275
程序 .....	275
後續步驟 .....	277
刪除評估 .....	277
必要條件 .....	277
程序 .....	277
其他資源 .....	279
委派 .....	280
重點 .....	280
其他資源 .....	280
適用稽核擁有者 .....	281
重點 .....	281

其他資源 .....	281
委派控制集 .....	281
尋找代表團 .....	283
刪除委派 .....	284
對於委派人 .....	285
重點 .....	285
其他資源 .....	286
查看通知 .....	286
審核控制項和證據 .....	287
編輯評論 .....	289
將控制項標示為已檢閱 .....	289
將控制項集送交給稽核擁有者 .....	290
評估報告 .....	292
瞭解資料夾結構 .....	292
瀏覽評估報告 .....	293
檢閱評估報告區段 .....	293
封面 .....	294
概觀頁面 .....	294
目錄頁 .....	295
控制項頁面 .....	296
證據摘要頁面 .....	297
證據詳細資訊頁 .....	298
驗證評估報告 .....	299
其他資源 .....	299
證據搜尋工具 .....	300
重點 .....	300
了解證據查找器如何與 CloudTrail 湖泊合作 .....	300
後續步驟 .....	301
其他資源 .....	301
搜尋證據 .....	301
必要條件 .....	301
程序 .....	301
後續步驟 .....	305
其他資源 .....	305
檢視您的搜尋結果 .....	305
必要條件 .....	306

程序 .....	306
後續步驟 .....	309
其他資源 .....	309
匯出搜尋結果 .....	309
必要條件 .....	310
程序 .....	310
其他資源 .....	314
篩選和分組選項 .....	314
篩選器參考資料 .....	314
分組參考 .....	318
範例使用案例 .....	318
使用案例 1：尋找不合規的證據並進行委派 .....	319
使用案例 2：找出合規證據 .....	319
使用案例 3：執行證據資源的快速預覽 .....	320
下載中心 .....	322
瀏覽下載中心 .....	322
正在下載檔案 .....	323
刪除檔案 .....	324
其他資源 .....	324
架構程式庫 .....	326
重點 .....	326
其他資源 .....	326
尋找框架 .....	327
必要條件 .....	327
程序 .....	327
後續步驟 .....	328
其他資源 .....	328
檢閱架構 .....	328
必要條件 .....	329
程序 .....	329
後續步驟 .....	332
其他資源 .....	332
建立自訂架構 .....	332
重點 .....	332
其他資源 .....	333
從頭開始創建 .....	333

製作可編輯的副本 .....	335
編輯自訂架構 .....	337
必要條件 .....	337
程序 .....	338
後續步驟 .....	339
其他資源 .....	339
共享自訂架構 .....	339
重點 .....	340
其他資源 .....	340
概念和術語 .....	340
傳送共享要求 .....	348
回應共享要求 .....	353
刪除共享要求 .....	357
刪除自訂架構 .....	358
必要條件 .....	358
程序 .....	358
其他資源 .....	359
控制項程式庫 .....	360
重點 .....	360
其他資源 .....	360
尋找控制項 .....	361
必要條件 .....	361
程序 .....	361
後續步驟 .....	362
其他資源 .....	363
檢閱控制項 .....	363
.....	363
通用控制 .....	363
核心控制 .....	366
標準控制 .....	369
自訂控制項 .....	373
建立自訂控制項 .....	377
.....	378
重點 .....	378
其他資源 .....	378
從頭開始創建 .....	379

製作可編輯的副本 .....	384
編輯自訂控制項 .....	388
必要條件 .....	388
程序 .....	388
後續步驟 .....	392
其他資源 .....	392
變更證據收集頻率 .....	392
刪除自訂控制項 .....	395
必要條件 .....	395
程序 .....	396
其他資源 .....	397
設定 .....	398
程序 .....	398
後續步驟 .....	398
設定您的資料加密設定 .....	399
必要條件 .....	399
程序 .....	399
其他資源 .....	400
新增委派管理員 .....	400
必要條件 .....	401
程序 .....	401
後續步驟 .....	402
其他資源 .....	402
變更委派管理員 .....	402
必要條件 .....	403
程序 .....	404
後續步驟 .....	405
其他資源 .....	405
移除委派的管理員 .....	406
必要條件 .....	406
程序 .....	406
其他資源 .....	408
設定您的預設稽核擁有者 .....	408
程序 .....	408
其他資源 .....	409
設定您的預設評估報告目標 .....	409

必要條件 .....	409
程序 .....	411
其他資源 .....	412
設定 Audit Manager 通知 .....	412
必要條件 .....	412
程序 .....	412
其他資源 .....	413
啟用證據搜尋工具 .....	413
必要條件 .....	414
程序 .....	414
後續步驟 .....	415
其他資源 .....	415
確認證據搜尋器的狀態 .....	415
必要條件 .....	415
程序 .....	415
後續步驟 .....	418
其他資源 .....	418
停用證據搜尋工具 .....	418
必要條件 .....	418
程序 .....	419
其他資源 .....	420
設定證據搜尋器的預設匯出目的地 .....	420
必要條件 .....	420
程序 .....	421
通知 .....	424
其他資源 .....	424
故障診斷 .....	425
故障排除評估和證據收集 .....	425
我建立了一個評估，但還看不到任何證據 .....	426
我的評估不會從中收集合規性檢查證據 AWS Security Hub .....	426
我在 Security Hub 中禁用了安全控制。Audit Manager 是否會收集該安全性控制的符合性檢 查證據？ .....	428
我Suppressed在安全中心中設置了發現的狀態。Audit Manager 是否會收集有關該發現項目 的合規性檢查 .....	428
我的評估不會從中收集合規性檢查證據 AWS Config .....	428
我的評估不會從 AWS CloudTrail中收集使用者活動證據 .....	430

我的評估不會收集 AWS API 呼叫的組態資料證據 .....	430
常見的控制項不會收集任何自動化證據 .....	430
我的證據是以不同的時間間隔產生的，我不確定它的收集頻率 .....	431
我先停用再重新啟用 Audit Manager，導致我既有的評估不再進行收集證據 .....	433
在我的評估詳細資料頁面上，系統會提示我重新建立評估 .....	433
資料來源和證據來源有什麼區別？ .....	433
我的評估建立失敗 .....	434
如果我從組織中移除範圍內的帳戶，會發生什麼情況？ .....	434
我看不到評估範圍內的服務 .....	434
我無法編輯評估範圍內的服務 .....	434
範圍內的服務和資料來源類型有什麼不同？ .....	435
<b>疑難排解評估報告 .....</b>	<b>436</b>
我的評估報告無法產生 .....	436
我按照上面的檢查清單進行操作，但我的評估報告仍然無法生成 .....	437
當我嘗試生成報告時，出現存取被拒絕的錯誤 .....	438
我無法解壓縮評估報告 .....	438
當我在報告中選擇證據名稱時，系統沒有將我重導向到該證據的詳細資訊 .....	439
我的評估報告產生停留進行中狀態，我不確定這對我的計費有何影響 .....	439
其他資源 .....	439
<b>控制項和控制組疑難排解 .....</b>	<b>439</b>
我在評估中看不到任何控制項或控制集 .....	440
我無法將手動證據上傳到控制項 .....	440
如果控制項顯示「可用更換」，這代表什麼意思？ .....	441
我需要多個 AWS Config 規則作為單個控件的數據源 .....	441
我的資料來源無法使用自訂規則選項 .....	441
自訂規則的下拉式清單為空 .....	441
我看不到我想要使用的自訂規則 .....	441
我看不到要使用的受管規則 .....	443
我想共享一個自訂架構，但它具有使用自訂 AWS Config 規則作為資料來源的控制項 .....	445
在 AWS Config 中更新自訂規則時會發生什麼情況？ .....	446
<b>疑難排解儀表板 .....</b>	<b>447</b>
我的儀表板上沒有任何資料 .....	447
我無法再看到評估的儀表板資料 .....	448
無法使用 CSV 下載選項 .....	448
嘗試下載 CSV 檔案時看不到下載的檔案 .....	448
儀表板遺失特定控制項或控制項域 .....	448



每日快照顯示每天的證據數量都不相同。這正常嗎？ .....	449
疑難排解委派管理員 AWS Organizations .....	449
我無法在 Audit Manager 設定委派系統管理員帳戶 .....	449
建立評估時，我無法在範圍內的帳戶看到組織中的帳戶 .....	450
當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤 .....	450
如果我取消成員帳戶與組織的連結，Audit Manager 會發生什麼情況？ .....	451
如果我將成員帳戶重新連結至組織，會發生什麼情況？ .....	451
如果我將成員帳戶從一個組織移到另一個組織，會發生什麼情況？ .....	451
證據搜尋工具疑難排解 .....	451
我無法啟用證據搜尋工具 .....	452
我已啟用證據搜尋工具，但在搜尋結果中看不到過去的證據 .....	453
我無法停用證據搜尋工具 .....	453
我的搜尋查詢失敗 .....	454
我無法從搜尋結果中產生多個評估報告 .....	455
我無法在搜尋結果中加入特定證據 .....	456
在評估報告中，並未包含所有來自證據搜尋工具的查找結果 .....	456
我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗 .....	456
其他資源 .....	459
我的 CSV 匯出失敗 .....	459
我無法從搜尋結果中匯出特定證據 .....	461
我無法一次匯出多個 CSV 檔案 .....	461
疑難排解框 .....	461
在我的自定義框架詳細信息頁面上，系統提示我重新創建自定義框架 .....	462
我無法製作自定義框架的副本或使用它來創建評估 .....	464
我傳送的共享要求狀態顯示為失敗 .....	464
我的共享要求旁邊有一個藍點。這代表什麼意思？ .....	465
我的共享框架具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？ .....	467
我更新了共享架構中使用的自訂規則。我需要採取任何動作嗎？ .....	468
針對通知進行故障診斷 .....	469
我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知 .....	469
我指定了 FIFO 主題，但沒有依預期順序收到通知 .....	470
疑難排解權限和存取 .....	470
我按照 Audit Manager 設定程序進行操作，但我沒有足夠的 IAM 權限 .....	470
我指定某人為稽核擁有者，但他們仍然無法完整存取評估。為什麼？ .....	470
我無法在 Audit Manager 中執行動作 .....	471

我想允許我以外的人員存 AWS 帳戶 取我的 Audit Manager 資源 .....	471
我看到「拒絕存取」錯誤，儘管有必要的 Audit Manager 權限 .....	472
其他資源 .....	472
標記資源 .....	474
支援的資源 .....	474
標籤限制 .....	475
在 Audit Manager 中管理標籤 .....	475
配額 .....	477
預設 Audit Manager 配額 .....	477
管理您的配額 .....	478
其他資源 .....	479
安全 .....	480
資料保護 .....	480
刪除 Audit Manager 資料 .....	481
靜態加密 .....	482
傳輸中加密 .....	483
金鑰管理 .....	483
身分與存取管理 .....	484
物件 .....	484
使用身分驗證 .....	485
使用政策管理存取權 .....	487
如何與 IAM AWS Audit Manager 搭配使用 .....	489
身分型政策範例 .....	497
預防跨服務混淆代理人 .....	513
AWS 受管理政策 .....	514
故障診斷 .....	547
使用服務連結角色 .....	549
法規遵循驗證 .....	562
恢復能力 .....	563
基礎架構安全 .....	563
VPC 端點 (AWS PrivateLink) .....	564
AWS Audit Manager VPC 端點的考量 .....	564
為 AWS Audit Manager 建立介面 VPC 端點 .....	564
建立 VPC 端點原則 AWS Audit Manager .....	564
日誌記錄和監控 .....	565
使用 Amazon 監控 EventBridge .....	566

---

CloudTrail 日誌 .....	569
組態與漏洞 .....	572
使用 Audit Manager AWS CloudFormation .....	573
Audit Manager 和 AWS CloudFormation 範本 .....	573
進一步了解 AWS CloudFormation .....	573
搭配 AWS SDK 使用 Audit Manager .....	574
禁用 AWS Audit Manager .....	575
程序 .....	575
後續步驟 .....	577
其他資源 .....	577
文件歷史紀錄 .....	578
.....	dlxxxvii

# 什麼是 AWS Audit Manager ？

歡迎使用 AWS Audit Manager 用使用者指南。

AWS Audit Manager 協助您持續稽核您的 AWS 使用情況，以簡化風險管理方式，以及遵循法規與產業標準的方式。Audit Manager 會自動化證據收集，讓您更容易評估您的政策、程序和活動 (也稱為控制項) 是否有效運作。進行稽核時，Audit Manager 可協助您管理控制項的利益相關者檢閱。這意味著您能在減少手動工作情況下，將稽核報告準備就緒。

Audit Manager 提供預建架構，可針對特定的合規標準或法規來建構和自動化評估。架構包括一個預組的控制集，其中包含說明和測試程序。這些控制項會根據指定的合規標準或法規的要求進行分組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

您可以從任何架構建立評估。建立評估時，Audit Manager 會自動執行資源評估。這些評量會收集您 AWS 帳戶定義的稽核範圍內的資料。所收集的資料會自動轉換為易於稽核的證據。然後會附加到相關控制項，以協助您證明安全性、變更管理、業務持續性和軟體授權方面的合規性。證據收集程序為持續過程，並從您建立評估時開始。完成稽核後，不再需要 Audit Manager 來收集證據，您可以停止收集證據。如需執行此操作，請將評估狀態變更為非作用中。

## Audit Manager 功能

使用 AWS Audit Manager，您可以執行下列工作：

- 快速入門 — 從支援各種合規標準和法規的預建架構中進行選擇，以[建立您的第一個評估](#)。然後，啟動自動證據收集以審核您的 AWS 服務使用情況。
- 上傳和管理來自混合式或多雲端環境的證據 — 除了 Audit Manager 從您的 AWS 環境收集的證據之外，您還可以[上傳](#)並集中管理來自內部部署或多雲端環境的證據。
- 支援常見的合規標準和法規 — 選擇其中一個 [AWS Audit Manager 標準架構](#)。這些架構為常見的合規標準和法規提供預建的控制項映射。這些措施包括 CIS 基準測試、PCI DSS、GDPR、HIPAA、SOC2、GxP 以及營運最佳實務。AWS
- 監控您的有效評估 — 使用 Audit Manager [儀表板](#)來檢視有效評估的分析資料，並快速分辨需要修正的不合規證據。
- 搜尋證據 — 使用此[證據搜尋工具](#)功能快速尋找與您的搜尋查詢相關的證據。您可以從搜尋結果中產生評估報告，或以 CSV 格式匯出搜尋結果。
- 建立自訂控制項 — [從頭開始建立您自己的控制項，或製作現有標準控制項或自訂控制項的可編輯副本](#)。您也可以使用自訂控制項功能來建立風險評估問題，並將這些問題的回覆儲存為手動證據。

- 將您的企業控制項對應至預先定義的 AWS 資料來源群組 — 選擇代表您目標的通用控制項，並使用這些控制項[建立自訂控制項](#)，以收集符合性需求組合的證據。
- 建立自訂架構 — [根據您對內部稽核的特定需求，使用標準或自訂控制項建立自己的架構](#)。
- 共用自訂架構 — 與其他人[共用您的自訂 Audit Manager 程式架構](#) AWS 帳戶，或將其複製到您自己帳戶 AWS 區域 下的另一個架構。
- 支援跨團隊協同 — 將[控制集委派](#)給主題專家，他們可以檢閱相關證據、新增評論，並更新各控制項狀態。
- 為稽核者建立報告 — [產生評估報告](#)，摘要針對稽核收集的相關證據，並連結至包含詳細證據的資料夾。
- 確保證據完整性 — 將[證據存放](#)在安全的位置，保持不變。

### Note

AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。AWS Audit Manager 因此，透過收集的證據可能不包含稽核所需的所有有關您 AWS 使用情況的資訊。AWS Audit Manager 不是法律顧問或合規專家的替代品。

## Audit Manager 定價

如需定價的詳細資訊，請參閱[AWS Audit Manager 定價](#)。

## 您第一次使用 Audit Manager 嗎？

若您第一次使用 Audit Manager，建議您閱讀以下章節：

1. [理解 AWS Audit Manager 概念和術語](#)— 瞭解 Audit Manager 中使用的關鍵概念和術語，例如評估、架構和控制項。
2. [了解如何 AWS Audit Manager 收集證據](#)— 瞭解 Audit Manager 如何收集證據以進行資源評估。
3. [使用建議 AWS Audit Manager 的設定進行設定](#)— 瞭解 Audit Manager 的設定需求。
4. [開始使用 AWS Audit Manager](#)— 依照教學課程建立您的第一個 Audit Manager 評估。
5. [AWS Audit Manager API 參考](#) — 熟悉 Audit Manager API 動作和資料類型。

## 更多 Audit Manager 資源

探索下列資源以進一步了解 Audit Manager。

- [收集證據和管理審計數據 AWS Audit Manager](#)
- [跨三線模型整合 \(第 2 部分\)：將一 AWS Config 致性套件轉換為AWS 管理與治理部落格中的 AWS Audit Manager 評估](#)

## 理解 AWS Audit Manager 概念和術語

為了協助您入門，本頁面定義了術語和解釋了 AWS Audit Manager 的一些重要概念。

### A

|B| | | |G|H|I|J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

### 評估

您可以使用 Audit Manager 評估來自動收集與稽核相關的證據。

評估是以架構為基礎，架構是與稽核相關的一組控制項。您可以從標準架構或自訂架構建立評估。標準架構包含支援特定合規標準或法規的預建控制集。相反地，自訂架構包含控制項，您可以根據特定稽核需求自訂和分組。使用架構作為起點，您可以建立評估，以指 AWS 帳戶 定要包含在稽核範圍中的內容。

當您建立評估時，Audit Manager 會 AWS 帳戶 根據架構中定義的控制項，自動開始評估您中的資源。接著，收集相關證據並將其轉換為易於稽核的格式。執行此操作後，它會將證據附加到評估中的控制項中。當需要進行稽核時，您或您選擇的委派代表可以檢閱收集的證據，然後將其新增至評估報告中。此評估報告可協助您證明您的控制項如期運作。

證據收集程序為持續過程，會在您建立評估時開始。您可以將評估狀態變更為非作用中，以停止證據收集。或者，您可以在控制層級停止證據收集。您可以將評估中的特定控制項狀態變更為非作用中來執行此操作。

如需有關建立與管理評估的說明，請參閱 [管理評估 AWS Audit Manager](#)。

### 評估報告

評估報告是由 Audit Manager 評估產生的最終文件。這些報告為您總結稽核收集的相關證據。它們連結到相關證據文件夾。資料夾會根據評估中所指定的控制項來命名和組織。對於每項評估，您可以檢閱 Audit Manager 收集的證據，並決定要在評估報告中包含哪些證據。

如需進一步了解評估報告，請參閱 [評估報告](#)。如需了解如何產生評估報告，請參閱 [準備評估報告 AWS Audit Manager](#)。

## 評估報告目的地

評估報告目的地是 Audit Manager 儲存您的評估報告的預設 S3 儲存貯體。如需進一步了解，請參閱 [設定您的預設評估報告目標](#)。

## 稽核

稽核是對您組織的資產、營運或業務完整性進行獨立檢查。資訊技術 (IT) 稽核會特別檢查組織資訊系統內的控制項。IT 稽核的目標是判斷資訊系統是否保護資產並有效運作，以及維護資料完整性。所有這些對於滿足合規標準或法規規定的監管要求至關重要。

## 稽核擁有者

稽核擁有者一詞會根據前後關聯性而有兩種不同的意義。

在 Audit Manager 的前後關聯性中，稽核擁有者是管理評估及其相關資源的使用者或角色。此 Audit Manager 角色的職責包括建立評估、檢閱證據以及產生評估報告。Audit Manager 是一項協作服務，當其他利益關係者參與其評估時，稽核擁有者將受益匪淺。例如，您可以將其他稽核擁有者新增至您的評估，以共享管理任務。或者，如果您是稽核擁有者，且需要協助解譯為控制項所收集的證據，您可以 [將該控制集委派](#)給在該領域擁有專業知識的利益關係者。這樣的人被稱為委派代表角色。

在商業術語中，稽核擁有者是協調和監督其公司的稽核準備工作，並向稽核人員提供證據的人。一般而言，這是控管、風險和合規 (GRC) 專業人員，例如合規官員或 GDPR 資料保護官。GRC 專業人員擁有管理稽核準備的專業知識和權力。具體來說，他們了解合規需求，並可以分析、解譯和準備報告資料。不過，其他業務角色也可以承擔稽核擁有者的 Audit Manager 角色，不僅是由 GRC 專業人員來擔任。例如，您可以選擇由以下團隊之一的技術專家進行設定和管理 Audit Manager 評估：

- SecOps
- 資訊科技/DevOps
- 安全營運中心 / 事件回應
- 相關團隊負責擁有、開發、修復和部署雲端資產，以及了解組織雲端基礎架構

您在 Audit Manager 評估中，選擇指定誰作為稽核擁有者，這很大程度上取決於您的組織。這同時取決於您如何架構安全性作業，以及其稽核細節。在 Audit Manager 中，同一個人可以在一項評估中擔任稽核擁有者角色，在另一個評估中擔任委派代表角色。

無論您選擇如何使用 Audit Manager，都可以使用稽核擁有者 / 委派角色管理整個組織的職責分離，並將特定的 IAM 政策授予每位使用者。透過這兩個步驟的方法，Audit Manager 可確保您完全掌控個別評估的所有細節。如需詳細資訊，請參閱 [中使用者角色的建議政策 AWS Audit Manager](#)。

## AWS 受管理來源

AWS 託管來源是為您 AWS 維護的證據來源。

每個 AWS 受管理的來源都是預先定義的資料來源群組，可對應至特定的通用控制項或核心控制項。當您使用通用控制項做為證據來源時，您會自動收集支援該通用控制項的所有核心控制項的證據。您也可以使用個別核心控制項做為證據來源。

每當受 AWS 管理的來源更新時，相同的更新都會自動套用至使用該 AWS 受管理來源的所有自訂控制項。這表示您的自訂控制項會針對該證據來源的最新定義收集證據。這可協助您確保在雲端合規環境變更時持續遵循法規遵循。

另請參閱：[customer managed source](#)、[evidence source](#)。

## C

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

## Changelog

Audit Manager 會針對評估中的每個控制項追蹤該控制項的使用者活動。您可以檢閱與特定控制項相關之活動的稽核記錄。如需有關在變更記錄檔中擷取哪些使用者活動的詳細資訊，請參閱 [Changelog 索引標籤](#)。

## 雲端合規

雲端合規是雲端交付的系統必須符合雲端客戶所面臨的標準的一般原則。

## 共同控制

請參閱 [control](#)。

## 合規監管

合規監管是由當局規定的法律、規則或其他命令，通常用於規範行為。一個範例是 GDPR。

## 合規標準

合規標準是一套結構化的準則，詳細說明組織維持與既定法規、規範或立法一致的過程。範例包括 PCI DSS 和 HIPAA。



## 控制項

控制項是為資訊系統或組織規定的保護或對策。控制項旨在保護您資訊的機密性、完整性和可用性，並符合一組定義的要求。它們可確保您的資源如預期運作、資料可靠，而且您的組織遵守適用的法律和法規。

在 Audit Manager 中，控制項還可以代表供應商風險評估問卷中的一個問題。在這種情況下，控制項是一個特定的問題，詢問有關組織的安全性和合規性狀況的資訊。

控制項會在 Audit Manager 評估中處於有效狀態時持續收集證據。您也可以手動將證據新增至任何控制項。每個證據都是一條記錄，可幫助您證明是否符合控制項的要求。

Audit Manager 提供下列類型的控制項：

控制類型	描述
共同控制	<p>您可以將共同的控制項視為可協助您達成控制目標的動作。由於通用控制項並非針對任何合規標準，因此可協助您收集可支援一系列重疊合規義務的證據。</p> <p>例如，假設有一個稱為數據分類和處理的控制目標。為了達成此目標，您可以實作稱為存取控制的通用控制項，以監控和偵測資源的未經授權存取。</p> <ul style="list-style-type: none"> <li>自動化通用控制項會為您收集證據。它們由一個或多個相關核心控制項的群組組成。反過來，這些核心控制項都會自動從預先定義的 AWS 資料來源群組收集相關證據。AWS 為您管理這些基礎資料來源，並在法規和標準變更以及識別新資料來源時更新這些資料來源。</li> <li>手動通用控制要求您上傳自己的證據。這是因為它們通常需要提供實體記錄，或關於發生在您 AWS 環境之外的事件的詳細資料。因此，通常沒有 AWS 資料來源可以產生證據來支援手動通用控制項的需求。</li> </ul> <p>您無法編輯通用控制項。不過，當您<a href="#">建立自訂控制項時</a>，您可以使用任何通用控制項做為證據來源。</p>
核心控制	<p>這是您 AWS 環境的規範準則。您可以將核心控制項視為可協助您符合共同控制項需求的動作。</p> <p>例如，假設您使用稱為「存取控制」的通用控制項來監控資源的未經授權存取。若要支援此通用控制項，您可以在 S3 儲存貯體中使用稱為「封鎖公用讀取存取」的核心控制項。</p>

控制類型	描述
	<p>由於核心控制項並非特定於任何合規標準，因此它們會收集可支援一系列重疊合規義務的證據。每個核心控制項都使用一或多個資料來源來收集有關特定資料的證據 AWS 服務。AWS 為您管理這些基礎資料來源，並在法規和標準變更以及識別新資料來源時更新這些資料來源。</p> <p>您無法編輯核心控制項。不過，當您<a href="#">建立自訂控制項時</a>，您可以使用任何核心控制項做為證據來源。</p>
標準控制	<p>這是 Audit Manager 提供的預先建置控制項。</p> <p>您可以使用標準控制項來協助您針對特定合規標準進行稽核準備。每個標準控制項都與 Audit Manager <a href="#">framework</a> 中的特定標準相關，並收集證據供您用來證明是否符合該架構。標準控制項會從 AWS 管理的基礎資料來源收集證據。每當法規和標準發生變化以及識別新的資料來源時，這些資料來源都會自動更新。您無法編輯標準控制項。但是，您可以<a href="#">製作任何標準控制項的可編輯副本</a>。</p>
自訂控制	<p>這是您在 Audit Manager 中建立的控制項，以符合您的特定規範遵循需求。</p> <p>您可以從頭開始建立自訂控制項，或建立現有標準控制項的可編輯複本。建立自訂控制項時，您可以定義特<a href="#">evidence source</a>定的控制項，以決定 Audit Manager 從何處收集證據。建立自訂控制項之後，您可以編輯該控制項或將其新增至自訂架構。您也可以<a href="#">製作任何自訂控制項的可編輯副本</a>。</p>

## 控制網域

您可以將控制網域視為控制項類別，並非特定於任何合規性標準。控制網域的一個範例是資料保護。

出於簡單的組織目的，控制項通常依網域分組。每個網域都有多個目標。

控制項網域群組是 [Audit Manager 儀表板](#) 最強大的功能之一。Audit Manager 會強調顯示評估中具有不合規證據的控制項，並依控制項網域進行分組。這可讓您在準備稽核時，將修復工作集中在特定主題領域上。

## 控制目標

控制目標描述了落在其下方的共同控制項的目標。每個目標都可以有多個共同的控制項。如果這些通用控制項已成功實作，它們會協助您達成目標。

每個控制目標都屬於控制域之下。例如，資料保護控制網域可能具有名為「資料分類和處理」的控制目標。若要支援此控制目標，您可以使用稱為「存取控制」的通用控制項來監控和偵測資源的未經授權存取。

## 核心控制

請參閱[control](#)。

## 自訂控制

請參閱[control](#)。

## 客戶管理來源

客戶管理的來源是您定義的證據來源。

在 Audit Manager 中建立自訂控制項時，您可以使用此選項建立您自己的個別資料來源。這使您可以靈活地從業務特定資源（例如自定義 AWS Config 規則）收集自動證據。如果您想要將手動證據新增至自訂控制項，也可以使用此選項。

當您使用客戶管理的來源時，您必須負責維護您建立的所有資料來源。

另請參閱：[AWS managed source](#)、[evidence source](#)。

## D

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

## 資料來源

Audit Manager 會使用資料來源收集控制項的證據。資料來源具有下列屬性：

- 資料來源類型定義 Audit Manager 從哪一種類型的資料來源收集證據。
  - 對於自動證據，類型可以是AWS Security HubAWS Config AWS CloudTrail、或 AWS API 呼叫。
  - 如果您上傳自己的證據，則類型為「手動」。
  - Audit Manager API 會將資料 [source](#) Type 稱為來源類型。
- 資料來源對應是指定資料來源類型從何處收集證據的關鍵字。
  - 例如，這可能是 CloudTrail 事件的名稱或 AWS Config 規則的名稱。
  - Audit Manager API 會將資料來源對應稱為來[源](#)關鍵字。

- 資料來源名稱會標示資料來源類型和對映的配對。
- 對於標準控制項，Audit Manager 會提供預設名稱。
- 對於自定義控件，您可以提供自己的名稱。
- Audit Manager API 會將資料來源名稱稱為 [sourceName](#)。

單一控制項可以有許多資料來源類型和多個映射項目。例如，一個控制項可能會從混合的資料來源類型 (例如 AWS Config 和 Security Hub) 收集證據。另一個控件可能具有 AWS Config 作為其唯一的數據源類型，多個 AWS Config 規則作為映射。

下表列出自動化資料來源類型，並顯示一些映射項目的範例。

Data source type (資料來源類型)	說明	映射範例
AWS Security Hub	<p>使用此資料來源類型可擷取資源安全狀態的快照。</p> <p>Audit Manager 會使用 Security Hub 控制項的名稱作為映射關鍵字，並直接從安全性中心報告該安全檢查的結果。</p>	EC2.1
AWS Config	<p>使用此資料來源類型可擷取資源安全狀態的快照。</p> <p>Audit Manager 會使用 AWS Config 規則的名稱作為對應關鍵字，並直接從中報告該規則檢查的結果 AWS Config。</p>	SNS_ENCRYPTED_KMS
AWS CloudTrail	<p>使用此資料來源類型可追蹤稽核中所需的特定使用者活動。</p> <p>Audit Manager 會使用 CloudTrail 事件的名稱做為對應關鍵字，並從 CloudTrail 記錄中收集相關的使用者活動。</p>	CreateAccessKey

Data source type (資料來源類型)	說明	映射範例
AWS API 呼叫	<p>使用此資料來源類型，透過 API 呼叫特定資源組態建立快照 AWS 服務。</p> <p>Audit Manager 會使用 API 呼叫的名稱作為映射關鍵字，並收集 API 回應。</p>	kms_ListKeys

## 委派代表

委派人是具有有限權限的 AWS Audit Manager 使用者。委派代表通常在多個不同領域具備專業的業務或技術專長。例如，這些專業知識可能涵蓋資料保留政策、培訓計劃、網路基礎結構或身分管理等領域。委派代表可幫助稽核擁有者檢閱其專業領域內的控制項所收集到的證據。委派代表可以檢閱控制集及其相關證據，以及新增評論、上傳其他證據，並更新您指派給他們檢閱的各控制項狀態。

稽核擁有者會指派特定控制集給委派代表，而非整個評估。因此，委派代表對評估的存取權限有限。如需關於委派控制集的說明，請參閱 [中的代表團 AWS Audit Manager](#)。

## E

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

## 證據

證據是包含證明是否符合控制項要求所需資訊的記錄。證據的範例包括使用者調用的變更活動，以及系統組態快照集。

Audit Manager 中主要分為兩種證據類型：自動化證據和手動證據。

證據類型	描述
自動化證據	<p>這是 Audit Manager 自動收集的證據。自動化證據包括以下三種類別：</p> <ol style="list-style-type: none"> <li>1. 符合性檢查 — 符合性檢查的結果是從 AWS Security Hub AWS Config、或兩者擷取。</li> </ol>

證據類型	描述
	<p>符合性檢查的範例包括安全中心針對 PCI DSS 控制項的安全性檢查結果，以及 HIPAA 控制項的 AWS Config 規則評估。</p> <p>如需詳細資訊，請參閱 <a href="#">AWS Config 規則 支持 AWS Audit Manager</a> 及 <a href="#">AWS Security Hub 支援的控制項 AWS Audit Manager</a>。</p> <p>2. 使用者活動 — 會在活動發生時從 CloudTrail 記錄擷取變更資源配置的使用者活動。</p> <p>使用者活動的範例包括路由表更新、Amazon RDS 執行個體備份設定變更，以及 S3 儲存貯體加密政策變更。</p> <p>如需詳細資訊，請參閱 <a href="#">AWS CloudTrail 支援的事件名稱 AWS Audit Manager</a>。</p> <p>3. 組態資料 — 資源組態的快照會直接從 AWS 服務的每日、每週或每月擷取。</p> <p>組態快照的範例包括 VPC 路由表的路由清單、Amazon RDS 執行個體備份設定以及 S3 儲存貯體加密政策。</p> <p>如需詳細資訊，請參閱 <a href="#">AWS 支援的 API 呼叫 AWS Audit Manager</a>。</p>
手動證據	<p>這是您自行新增至 Audit Manager 的證據。新增自己的證據有以下三種方法：</p> <ol style="list-style-type: none"> <li>1. 從 Amazon S3 匯入檔案</li> <li>2. 從瀏覽器上傳檔案</li> <li>3. 輸入風險評估問題的文字回覆</li> </ol> <p>如需詳細資訊，請參閱 <a href="#">在中添加手動證據 AWS Audit Manager</a>。</p>

自動化證據收集會在您建立評估時啟動。這是一個持續的程序，Audit Manager 會根據證據類型和基礎資料來源，以不同的頻率收集證據。如需詳細資訊，請參閱 [了解如何 AWS Audit Manager 收集證據](#)。

如需關於檢閱評估中證據的說明，請參閱 [檢閱中的證據 AWS Audit Manager](#)。

## 證據來源

證據來源定義控制項從何處收集證據。它可以是個別資料來源，也可以是對應至通用控制項或核心控制項的預先定義資料來源群組。

建立自訂控制項時，您可以從 AWS 受管理來源、客戶管理來源或兩者收集證據。

### Tip

我們建議您使用 AWS 受管理的來源。每當受 AWS 管理的來源更新時，相同的更新都會自動套用至使用這些來源的所有自訂控制項。這表示您的自訂控制項一律會針對該證據來源的最新定義收集證據。這可協助您確保在雲端合規環境變更時持續遵循法規遵循。

另請參閱：[AWS managed source](#)、[customer managed source](#)。

## 證據收集方法

控制項可以透過兩種方式收集證據。

證據收集方法	描述
自動化	自動化控制項會自動從 AWS 資料來源收集證據。自動化證據可以幫助您證明對此控制項的完全或部分合規性。
手動	手動控制要求您 <a href="#">上傳自己的證據</a> ，以證明是否符合控制。

### Note

您可以將手動證據附加到任何自動化控制項。在許多情況下，需要結合自動化和手動證據來證明控制項完全合規。雖然 Audit Manager 可以提供有用且相關的自動化證據，但某些自動化證據可能只會顯示部分合規性。在這種情況下，您可以用自己的證據來補充 Audit Manager 提供自動化證據。

例如：

- [AWS 生成人工智慧最佳實務架構 v2](#) 包含一個名為的控制項 Error analysis。此控制項需要您分辨在模型使用中何時偵測到不準確性。並要求您進行徹底的錯誤分析，以了解根本原因並採取糾正措施。

- 為了支援此控制項，Audit Manager 會收集自動證據，以顯示是否已針對您的評估執行 AWS 帳戶 位置啟用 CloudWatch 警示。您可以使用此證據來證明對控制項的部分合規，以證明您的警報和檢查已正確配置。
  - 為了證明完全合規，您可以用手動證據補充自動化證據。例如，您可以上傳顯示錯誤分析過程、升級和報告的閾值，以及根本原因分析結果的策略或程序。您可以使用此手動證據來證明建立的策略已到位，並在出現提示時採取了糾正措施。
- 如需更詳細的範例，請參閱[混合資料來源的控制項](#)。

## 匯出目的地

匯出目的地是預設 S3 儲存貯體，Audit Manager 會儲存您從證據搜尋工具匯出的檔案。如需詳細資訊，請參閱 [設定證據搜尋器的預設匯出目的地](#)。

## F

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

## 架構

Audit Manager 架構會針對特定標準或風險治理原則，建構並自動化評估。這些架構包含一組預先建置或客戶定義的控制項，可協助您將 AWS 資源對應至這些控制項的需求。

Audit Manager 中有兩種類型的架構。

框架類型	描述
標準框架	這是一個預先構建的框架，基於各種合規性標準和法規的 AWS 最佳實踐。  您可以使用標準架構協助針對特定合規性標準或法規 (例如 PCI DSS 或 HIPAA) 進行稽核準備。
自定義框架	這是您定義為 Audit Manager 使用者的自訂架構。  您可以使用自訂架構，根據您的特定 GRC 需求協助稽核準備工作。

如需有關建立與管理架構的說明，請參閱 [使用框架庫來管理框架 AWS Audit Manager](#)。



**Note**

AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。AWS Audit Manager 因此，透過收集的證據可能不包含稽核所需的所有有關您 AWS 使用情況的資訊。AWS Audit Manager 不是法律顧問或合規專家的替代品。

## 架構共享

您可以使用[共享自定義框架 AWS Audit Manager](#)此功能在 AWS 帳戶 和區域之間快速共用您的自訂架構。如果共享自訂架構，您可以建立共享要求。接著，收件者有 120 天的時間接受或拒絕要求。當他們接受時，Audit Manager 會將共享的自訂架構複製到其架構程式庫中。除了複製自訂架構之外，Audit Manager 也會複製該架構中包含的所有自訂控制集和控制項。這些自訂控制項會新增至收件者的控制項程式庫。Audit Manager 不會複製標準架構或控制項。這是因為這些資源在每個帳戶和區域中，已預設為可用。

## R

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

## 資源

資源是在稽核中評估的實體或資訊資產。AWS 資源範例包括 Amazon EC2 執行個體、Amazon RDS 執行個體、Amazon S3 儲存貯體和 Amazon VPC 子網路。

## 資源評估

資源評估是評估個別資源的程序。此評估基於控制項的需求。當評估處於有效狀態時，Audit Manager 會針對評估範圍內的每個獨立資源執行資源評估。資源評估會執行下列任務：

1. 收集證據，包括資源配置，事件日誌和調查結果
2. 將證據轉換並映射到控制項
3. 儲存和追蹤證據的歷程，以實現完整性

## 資源合規性

資源合規性是指在收集合規檢查證據時，對資源進行評估的狀態。

Audit Manager 會針對使用 AWS Config 和 Security Hub 做為資料來源類型的控制項收集符合性檢查證據。證據收集期間，可能會評估多個資源。因此，單一合規檢查證據可以包含一或多個資源。

您可以使用證據搜尋工具中的資源合規性篩選器來搜索資源層級的合規狀態。搜尋完成後，您就可以預覽符合搜尋條件的資源。

在證據搜尋工具中，資源合規有三種可能的值：

Value	描述
不符合規定	<p>這是指具有合規性檢查問題的資源。</p> <p>如果 Security Hub 報告資源的失敗結果，或 AWS Config 報告不合規的結果，就會發生這種情況。</p>
相容性	<p>這是指沒有符合性檢查問題的資源。</p> <p>如果 Security Hub 報告資源的「通過」結果，或報 AWS Config 告「合規」結果，就會發生這種情況。</p>
不確定的	<p>這是指符合性檢查不可用或不適用的資源。</p> <p>如果 AWS Config 或 Security Hub 是基礎資料來源類型，但這些服務未啟用，就會發生這種情況。</p> <p>如果基礎資料來源類型不支援合規性檢查 (例如手動證據、AWS API 呼叫或 CloudTrail)，也會發生這種情況。</p>

## S

|B| | | |G|H|I|J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

### 服務範圍

Audit Manager AWS 服務 會管理您評估範圍內的哪些項目。如果您有較舊的評估，可能是您過去手動指定範圍內的服務。在 2024 年 6 月 4 日之後，您無法手動指定或編輯範圍內的服務。

範圍內的服務是 AWS 服務 指您的評估會收集有關的證據。當服務包含在評估範圍內時，Audit Manager 會評估該服務的資源。一些範例資源包括如下：

- Amazon EC2 執行個體
- S3 儲存貯體
- IAM 使用者或角色

- DynamoDB 資料表
- 網路元件，例如 Amazon 虛擬私有雲端 (VPC)、安全群組或網路存取控制清單 (ACL) 表

例如，如果 Amazon S3 是範圍內的服務，Audit Manager 可以收集有關 S3 儲存貯體的證據。收集的確切證據由控件確定 [data source](#)。例如，如果資料來源類型為 AWS Config，而資料來源對映是 AWS Config 規則 (例如 s3-bucket-public-write-prohibited)，則 Audit Manager 會收集該規則評估的結果作為證據。

#### Note

請記住，範圍內的服務與數據源類型不同，數據源類型也可以是 AWS 服務 其他類型。如需詳細資訊，請參閱 [範圍內的服務和資料來源類型有什麼不同？](#) 本指南的「疑難排解」一節中的。

## 標準控制

請參閱 [control](#)。

## 了解如何 AWS Audit Manager 收集證據

中的每個主動評估都 AWS Audit Manager 會自動收集來自一系列資料來源的證據。在每項評估中，您可以定義哪個 AWS 帳戶 Audit Manager 將收集證據，而稽核管理員則會管理範圍內的哪 AWS 服務 些項目。這些服務和帳戶中的每一個都包含您擁有和使用的多個資源。Audit Manager 中的證據收集涉及對每個範圍內資源的評估。這稱為資源評估。

下列步驟說明 Audit Manager 如何為各資源評估收集證據：

### 1. 從資料來源評估資源

啟動收集證據時，Audit Manager 會從資料來源對範圍內的資源進行評估。它會擷取組態快照集、相關符合性檢查結果或使用者活動來達成此目的。然後執行分析，以判斷此資料支援哪個控制項。資源評估的結果將被保存，並轉換為證據。如需有關不同證據類型的詳細資訊，請參閱 [evidence](#) 本指南的 AWS Audit Manager 概念與術語一節。

### 2. 將評估結果轉換為證據

資源評估的結果包含從該資源擷取的原始資料，以及指示資料支援哪些控制項的中繼資料。Audit Manager 會將原始資料轉換為易於稽核的格式。接著，轉換後的資料和中繼資料會儲存為 Audit Manager 證據，再附加至控制項。

### 3. 將證據附加至相關控制項

Audit Manager 會讀取證據中繼資料。然後會將儲存的證據附加至評估中的相關控制項。附加的證據會在 Audit Manager 中顯示。如此一來，就完成了資源評估的週期。

#### Note

視控制項組態而定，在某些情況下，相同的證據可以附加至來自多個 Audit Manager 評估的多個控制項。當相同的證據附加到多個控制項時，Audit Manager 只會測量一次資源評估。這是因為相同的證據只會收集一次。然而，Audit Manager 評估中的一個控制項可以有來自多個資料來源的多項證據。

## 證據收集頻率

證據收集程序為持續過程，會在您建立評估時開始。Audit Manager 會以不同頻率從多個資料來源收集證據。因此，對於收集證據的頻率沒有 one-size-fits-all 答案。證據收集的頻率取決於證據類型及其資料來源，如下所述。

- 符合性檢查 — Audit Manager 會從 AWS Security Hub 和收集此證據類型 AWS Config。
  - 對於 Security Hub，證據收集遵循 Security Hub 檢查的時間表。如需有關 Security Hub 檢查排程的詳細資訊，請參閱 AWS Security Hub 使用指南中的[執行安全檢查排程](#)。如需 Audit Manager 支援之 Security Hub 檢查的詳細資訊，請參閱[AWS Security Hub 支援的控制項 AWS Audit Manager](#)。
  - 對於 AWS Config，證據收集遵循 AWS Config 規則中定義的觸發程序。如需有關 AWS Config 規則觸發的詳細資訊，請參閱 AWS Config 使用指南中的[觸發類型](#)。如需有關「Audit Manager」AWS Config 規則 所支援的詳細資訊，請參閱[AWS Config 規則 支持 AWS Audit Manager](#)。
- 使用者活動 — Audit Manager 會以持續的方式從 AWS CloudTrail 中收集此證據類型。這個頻率是連續的，因為使用者活動可以在一天中的任何時間發生。如需詳細資訊，請參閱[AWS CloudTrail 支援的事件名稱 AWS Audit Manager](#)。
- 組態資料 — Audit Manager 使用對 Amazon EC2、Amazon S3 或 IAM AWS 服務 等其他人的描述 API 呼叫來收集此證據類型。您可以選擇要呼叫的 API 動作。您也可以在 Audit Manager 中將頻率設定為每日、每週或每月。您可以在控制項資源庫中建立或編輯控制項時，指定此頻率。如需關於編輯與建立控制項的說明，請參閱[使用控制項程式庫管理控制項 AWS Audit Manager](#)。如需 Audit Manager 支援之 API 呼叫的詳細資訊，請參閱[AWS 支援的 API 呼叫 AWS Audit Manager](#)。

無論資料來源的證據收集頻率為何，只要控制項和評估處於有效狀態，就會自動收集新證據。

# AWS Audit Manager 控制項範例

您可以檢閱此頁面上的範例，進一步了解控制項在 AWS Audit Manager 的運作方式。

在 Audit Manager 中，控制項可以自動從四種資料來源類型收集證據：

1. AWS CloudTrail— 從 CloudTrail 日誌中捕獲用戶活動並將其導入為用戶活動證據
2. AWS Security Hub— 從 Security Hub 收集發現並將其導入為合規性檢查證據
3. AWS Config— 從中收集規則評估 AWS Config 並將其導入為合規性檢查證據
4. AWS API 呼叫 — 從 API 呼叫擷取資源快照，並將其匯入為組態資料證據

許多控制項會使用這些資料來源的預先定義分組來收集證據。這些資料來源群組稱為 [AWS 受管理來源](#)。每個 AWS Managed 來源代表一個共同的控制項或核心控制項。這可讓您有效率地將合規要求對應至相關的資料來源群組，這些資料來源已由中 AWS 的 [業界認證評估機構驗證](#) 和維護。或者，您可以使用上述四種資料來源類型來定義自己的資料來源。這使您可以靈活地上傳手動證據，或從業務特定資源（例如自定義 AWS Config 規則）收集自動證據。

此頁面上的範例顯示控制項如何從每個個別資料來源類型收集證據。它們描述了控制項的外觀、Audit Manager 如何從資料來源收集證據，以及您可以採取以證明合規性的後續步驟。

## Tip

我們建議您啟用 AWS Config 和 Security Hub，以便在 Audit Manager 中獲得最佳體驗。當您啟用這些服務時，Audit Manager 可以使用 Security Hub 發現項目並 AWS Config 規則 產生自動化的證據。

- [啟用 AWS Security Hub](#) 之後，請確定您同時 [啟用所有安全性標準](#)，並 [開啟合併的控制項調查結果設定](#)。此步驟可確認 Audit Manager 能匯入所有支援的合規標準的調查結果。
- [啟用](#) 之後 AWS Config，請確定您同時 [啟用相關 AWS Config 規則](#) 或 [部署與稽核相關的合規性標準的一致性套件](#)。此步驟可確保 Audit Manager 可以針對您啟用的所有支援 AWS Config 規則 項目匯入發現項目。

以下為每種控制項類型的範例：

## 主題

- [用 AWS Security Hub 作資料來源類型的自動化控制項](#)

- [用 AWS Config 作資料來源類型的自動化控制項](#)
- [使用 AWS API 呼叫做為資料來源類型的自動化控制項](#)
- [用 AWS CloudTrail 作資料來源類型的自動化控制項](#)
- [手動控制](#)
- [具有混合資料來源類型的控制項 \(自動和手動\)](#)

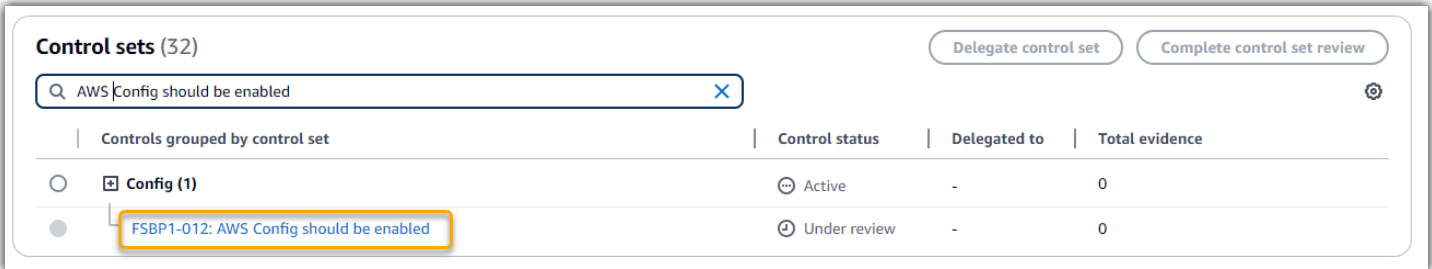
## 用 AWS Security Hub 作資料來源類型的自動化控制項

此範例顯示用 AWS Security Hub 作資料來源類型的控制項。這是取自 [AWS 基礎安全性最佳作法 \(FSBP\) 架構](#) 的標準控制項。Audit Manager 程式會使用此控制項來產生證據，協助您的 AWS 環境符合 FSBP 需求。

### 控制項細節範例

- 控制項名稱 — FSBP1-012: AWS Config should be enabled
- 控制集 — Config. 這是與組態管理相關的 FSBP 控制項的框架特定群組。
- 證據來源 — 個別資料來源
- 資料來源類型 — AWS Security Hub
- 證據類型 — 合規檢查

在下列範例中，此控制項位於從 FSBP 架構建立的 Audit Manager 評估中。



The screenshot shows the AWS Audit Manager console interface. At the top, there are buttons for 'Delegate control set' and 'Complete control set review'. Below is a search bar with the text 'AWS Config should be enabled'. A table displays control sets grouped by control set. The table has columns for 'Controls grouped by control set', 'Control status', 'Delegated to', and 'Total evidence'. One control set is highlighted in orange: 'FSBP1-012: AWS Config should be enabled'.

Controls grouped by control set	Control status	Delegated to	Total evidence
Config (1)	Active	-	0
FSBP1-012: AWS Config should be enabled	Under review	-	0

評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

### 這個控制項可以做什麼

此控制項需要在您使用安全性中心的所有 AWS 區域 位置啟用此控制項。AWS Config Audit Manager 可以使用此控制項來檢查您的 IAM 政策是否過於廣泛，無法符合 FSBP 要求。更具體地說，它可以檢

查您的客戶受管 IAM 政策是否具有包含以下萬用字元陳述式的管理員存取權："Effect": "Allow" 和 "Action": "\*" 超過 "Resource": "\*"。

## Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項評估您的範圍內資源。它會使用控制項設定中指定的資料來源來執行此作業。在此範例中，您的 IAM 政策是資源和 Security Hub，AWS Config 是資料來源類型。Audit Manager 會尋找特定安全中心檢查 ([IAM.1](#)) 的結果，然後使用 AWS Config 規則來評估您的 IAM 政策 ([iam-policy-no-statements-with-admin-access](#))。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會針對使用安全中樞作為資料來源類型的控制項產生合規檢查證據。此證據包含直接從 Security Hub 報告的合規檢查結果。
3. Audit Manager 會將儲存的證據附加至評估中名為 FSBP1-012: AWS Config should be enabled 的控制項。

## 如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，Audit Manager 可能會顯示來自 Security Hub 的失敗裁決。如果您的 IAM 政策包含萬用字元 (\*) 且範圍太廣而無法符合控制項，就可能發生這種情況。在這種情況下，您可以更新 IAM 政策，使其不允許完整的管理權限。為實現這一點，您可以決定使用者需要執行哪些任務，然後打造讓使用者只執行這些任務的政策。此更正動作有助於使您的 AWS 環境符合 FSBP 需求。

當您的 IAM 政策符合控制項時，請將控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

## 用 AWS Config 作資料來源類型的自動化控制項

此範例顯示用 AWS Config 作資料來源類型的控制項。這是取自 [AWS Control Tower 防護機制架構](#) 的標準控制項。Audit Manager 使用此控制項產生證據，協助您的 AWS 環境符合 AWS Control Tower 護欄。

### 控制項細節範例

- 控制項名稱 — CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets
- 控制集 — 此控制項屬於 Disallow public access 控制集。這是與存取管理相關的控制項群組。

- 證據來源 — 個別資料來源
- 資料來源類型 — AWS Config
- 證據類型 — 合規檢查

在下列範例中，此控制項位於從「AWS Control Tower 護欄」架構建立的「Audit Manager」評估中。

Controls grouped by control set	Control status	Delegated to	Total evidence
○ <b>Disallow public access (4)</b>	☰ Active	-	0
● <b>CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets</b>	🕒 Under review	-	0

評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

Audit Manager 可以使用此控制項來檢查 S3 儲存貯體政策的存取層級是否太寬鬆而無法滿足需 AWS Control Tower 求。更具體地說，它可以檢查封鎖公開存取功能設定、儲存貯體策略和儲存貯體存取控制清單 (ACL)，以確認您的儲存貯體不允許公開寫入存取權。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的 S3 儲存貯體是資源，而 AWS Config 是資料來源類型。Audit Manager 會尋找特定 AWS Config 規則 ([s3-bucket-public-write-prohibited](#)) 的結果，以評估評估範圍內的每個 S3 儲存貯體的設定、政策和 ACL。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會針對用 AWS Config 作資料來源類型的控制項產生符合性檢查證據。此證據包含直接從中報告的合規性檢查的結果 AWS Config。
3. Audit Manager 會將儲存的證據附加至評估中名為 CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性



將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，Audit Manager 可能會顯示 AWS Config 指出 S3 儲存貯體不合規的裁決。假如其中一個 S3 儲存貯體具有不限制公用政策的封鎖公開存取功能設定，且使用中的政策允許公開寫入存取權，就可能發生這種情況。如需修正此問題，您可以更新封鎖公開存取設定以限制公共策略。或者，您可以使用不允許公開寫入存取權的不同儲存貯體政策。此更正動作有助於使您的 AWS 環境 AWS Control Tower 符合需求。

當您確認 S3 儲存貯體存取層級符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

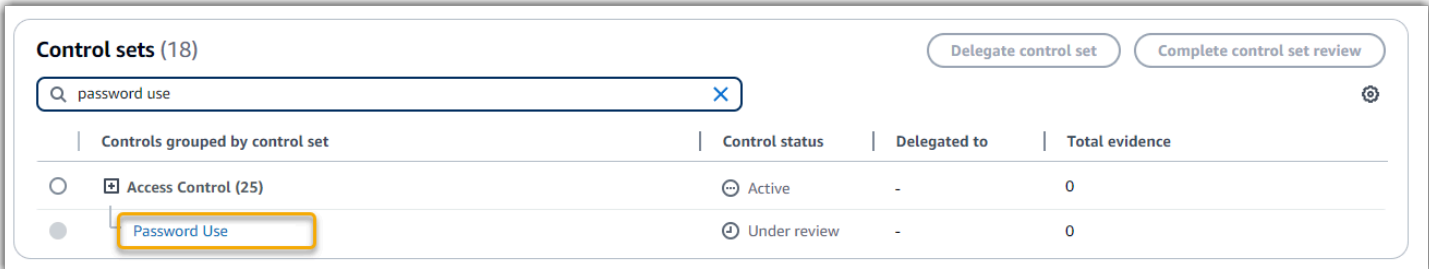
## 使用 AWS API 呼叫做為資料來源類型的自動化控制項

此範例顯示使用 AWS API 呼叫做為資料來源類型的自訂控制項。Audit Manager 會使用此控制項產生證據，協助您的 AWS 環境符合您的特定需求。

### 控制項細節範例

- 控制項名稱 — Password Use
- 控制組 — 此控制項屬於稱為 Access Control 的控制集。這是與身分識別和存取管理相關的控制項群組。
- 證據來源 — 個別資料來源
- 資料來源類型 — AWS API 呼叫
- 證據類型 — 配置資料

在下列範例中，此控制項位於從自訂架構建立的 Audit Manager 評估中。



Control sets (18)		Delegate control set	Complete control set review
Q password use			
Controls grouped by control set	Control status	Delegated to	Total evidence
<input type="radio"/> Access Control (25)	Active	-	0
<input checked="" type="radio"/> Password Use	Under review	-	0

評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

### 這個控制項可以做什麼

Audit Manager 可以使用此自訂控制項，來協助您確保擁有足夠的存取控制項策略。此控制項要求您在選擇和使用密碼時遵循良好的安全實踐。Audit Manager 可以擷取位於評估範圍內的 IAM 主體的所有密碼政策清單，協助您驗證此問題。

Audit Manager 如何收集此控制項的證據

Audit Manager 採取下列步驟來收集此自訂控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的資料來源評估範圍內的資源。在這種情況下，您的 IAM 主體是資源，AWS API 呼叫是資料來源類型。Audit Manager 會尋找特定 IAM API 呼叫 ([GetAccountPasswordPolicy](#)) 的結果。接著會傳回評估範圍內 AWS 帳戶的密碼政策。
2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會為使用 API 呼叫作為資料來源的控制項產生組態資料證據。此證據包含從 API 回應擷取的原始資料，以及指示資料支援哪些控制項的其他中繼資料。
3. Audit Manager 會將儲存的證據附加至評估中名為 Password Use 的自訂控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看證據是否充分或是否需要進行任何修補。

在此範例中，您可以檢閱證據以查看來自 API 呼叫的回應。[GetAccountPasswordPolicy](#) 回應會說明帳戶中使用者密碼的複雜性需求和強制輪替期間。您可以使用此 API 回應作為證據，以顯示您已針對評估範圍內的具有足夠 AWS 帳戶的密碼存取控制政策。如果需要，您也可以新增評論至控制項，以為相關政策提供其他見解。

當您對 IAM 主體的密碼政策符合自訂控制項感到滿意時，您可以將控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

## 用 AWS CloudTrail 作資料來源類型的自動化控制項

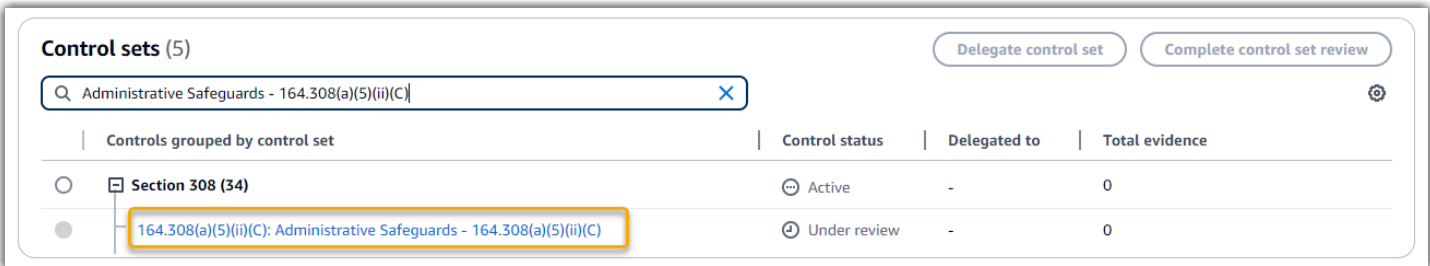
此範例顯示用 AWS CloudTrail 作資料來源類型的控制項。這是從 [HIPAA 安全規則 2003 框架採取的標準控制](#)。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合 HIPAA 需求。

控制項細節範例

- 控制項名稱 — 164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)

- 控制集 — 此控制項屬於稱為Section 308的控制集。這是與系統管理保護措施相關的 HIPAA 控制項的框架特定群組。
- 證據來源 — AWS 託管來源 ( 核心控制 )
- 基礎資料來源類型 — AWS CloudTrail
- 證據類型 — 使用者活動

以下是從 HIPAA 架構建立的 Audit Manager 評估中顯示的控制項：



Controls grouped by control set	Control status	Delegated to	Total evidence
<input type="radio"/> Section 308 (34)	Active	-	0
<input checked="" type="radio"/> 164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)	Under review	-	0

評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

這個控制項可以做什麼

此控制要求您具備監控程序以偵測未經授權的存取。未經授權存取的範例是有人在未啟用多重要素驗證 (MFA) 的情況下登入主控台。Audit Manager 提供證據，證明您已將 Amazon CloudWatch 設定為監控未啟用 MFA 的管理主控台登入請求，以協助您驗證此控制項。

Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的證據來源評估您的範圍內資源。在此情況下，控制項會使用數個核心控制項做為證據來源。

每個核心控制項都是由個別資料來源組成的受管理群組。在我們的例子中，這些核心控件之一 (Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled) 用 CloudTrail 作數據源。CloudTrail 是資料來源類型，Amazon CloudWatch 警示是評估的資源。

Audit Manager 會使用 monitoring\_EnableAlarmActions 關鍵字來檢閱您的 CloudTrail 記錄，以尋找啟用由記錄的動作的 CloudWatch 警示 CloudTrail。然後，它會傳回評估範圍內相關事件的記錄。

2. 資源評估的結果將被保存，並轉換為易於稽核的證據。Audit Manager 會針對用 CloudTrail 作資料來源類型的控制項產生使用者活動證據。此證據包含從 Amazon 擷取的原始資料 CloudWatch，以及指示資料支援哪些控制項的其他中繼資料。
3. Audit Manager 會將儲存的證據附加至評估中名為 164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C) 的控制項。

如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看是否需要進行任何修復。

在此範例中，您可以檢閱證據，以查看由 CloudTrail 記錄的警示啟用事件。您可以使用此日誌作為證據，以顯示您有足夠的監視程序來偵測何時在未啟用 MFA 的情況下進行主控台登入。如果需要，您也可以新增評論至控制項，為相關政策提供其他見解。例如，如果記錄檔顯示多個沒有 MFA 的登入，您可以新增說明如何修正問題的註解。定期監控主控台登入狀況，可協助您避免因不一致和不當登入嘗試而產生的安全問題。反過來，此最佳做法有助於使您的 AWS 環境符合 HIPAA 要求。

當您確認監控程序符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

## 手動控制

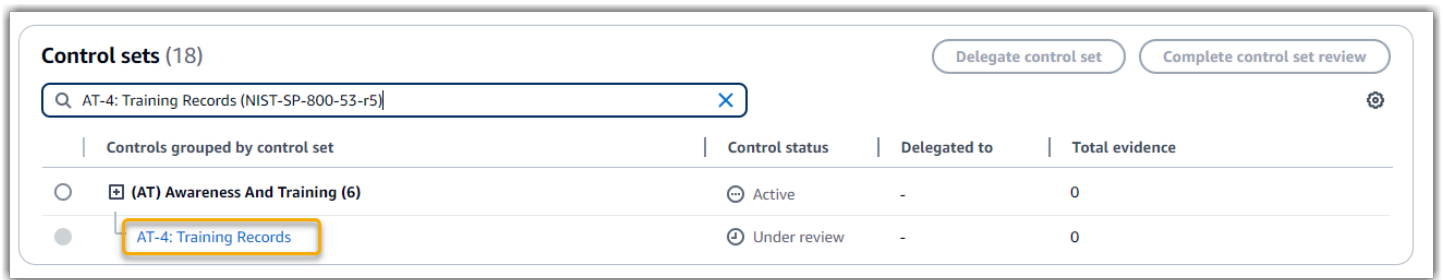
某些控制項不支援自動化證據收集。除了觀察、訪談和雲端中未產生的其他事件之外，這包括依賴提供實體記錄和簽名的控制項。在這些情況下，您可以手動上傳證據以證明您滿足控制項的要求。

此範例顯示 Audit Manager 不會收集自動化證據的手動控制項。這是取自 [NIST 800-53 \(Rev. 5\) 架構](#) 的標準控制項。您可以使用 Audit Manager 上傳並儲存證明此控制項的合規證據。

### 控制項細節範例

- 控制項名稱 — AT-4: Training Records
- 控制集 — (AT) Awareness and training. 這是與訓練相關的 NIST 控制項的框架特定群組。
- 證據來源 — 資料來源
- 基礎資料來源類型 — 手動
- 證據類型 — 手動

這是在 Audit Manager 評估中顯示的控制項，該評估是根據 NIST 800-53 (Rev. 5) Low-Moderate-High 架構所建立：



評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

### 這個控制項可以做什麼

您可以使用此控制項來協助您確保您的人員接受適當層級的安全性和隱私權訓練。具體來說，您可以證明您已根據所有員工的角色記錄了所有員工的安全性和隱私權訓練活動。您也可以顯示證明每個人都會保留訓練記錄。

### 如何手動上傳此控制項的證據

若要上傳補充自動化證據的手動證據，請參閱[中的上傳手動證據 AWS Audit Manager](#)。Audit Manager 會將上傳的證據附加至評估中名為 AT-4: Training Records 的控制項。

### 如何使用 Audit Manager 來證明對此控制項的合規性

如果您有支援此控制項的文件，您可以將其上傳為手動證據。例如，您可以上傳人力資源部門發行給員工的強制性角色訓練材料的最新副本。

就像使用自動化控制項一樣，您可以將手動控制項委派給可協助您檢閱證據的利益關係者 (或在此情況下提供)。例如，當您檢閱此控制項時，您可能發現只有部分符合其需求。如果您沒有面對面培訓的任何出勤跟踪副本，則可能是這種情況。您可以將控制權委派給 HR 利益相關者，然後他們可以上傳參加培訓的員工清單。

如果您滿意自己符合控制項，可以將其標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

## 具有混合資料來源類型的控制項 (自動和手動)

在許多情況下，需要結合自動化和手動證據來滿足控制項。雖然 Audit Manager 可以提供與控制項相關的自動化證據，但您可能需要使用您自己識別和上傳的手動證據來補充此資料。

此範例顯示使用手動證據和自動證據組合的控制項。這是取自 [NIST 800-53 \(Rev. 5\) 架構](#) 的標準控制項。Audit Manager 使用此控制項來產生證據，協助您的 AWS 環境符合 NIST 需求。

## 控制項細節範例

- 控制項名稱 — Personnel Termination
- 控制集 —(PS) Personnel Security (10). 這是 NIST 控制項的框架特定群組，與在組織系統上執行硬體或軟體維護的個人相關。
- 證據來源 — AWS 受管理 (核心控制) 和個別資料來源 (手動)
- 基礎資料來源類型 — AWS API 呼叫, AWS CloudTrail, AWS Config, 手動
- 證據類型 — 配置數據，用戶活動，合規性檢查，手動證據)

這是在 Audit Manager 評估中顯示的控制項，該評估是根據 NIST 800-53 (Rev. 5) 架構所建立：

Controls grouped by control set	Control status	Delegated to	Total evidence
(PS) Personnel Security (10)	Active	-	236
PS-4: Personnel Termination	Under review	-	87

評估會顯示控制狀態。它還顯示了迄今為止為此控制收集了多少證據。您可以從這裡委派控制集以供檢閱，或自行檢閱。選擇控制項名稱會開啟詳細資訊頁面，其中包含詳細資訊，包括該控制項的證據。

### 這個控制項可以做什麼

您可以使用此控制項來確認您是否在員工終止時保護組織資訊。具體而言，您可以證明您已停用系統存取權，並撤銷個人的認證。此外，您可以證明所有已終止的個人都參加了退出面試，其中包括對您組織的相關安全協議的討論。

### Audit Manager 如何收集此控制項的證據

Audit Manager 會採取下列步驟來收集此控制項的證據：

1. Audit Manager 會針對每個控制項，使用控制項設定中指定的證據來源評估您的範圍內資源。

在此情況下，控制項會使用數個核心控制項做為證據來源。反過來，這些核心控制項都會從個別資料來源 (AWS API 呼叫和 AWS Config) 收集相關證據。AWS CloudTrail Audit Manager 會使用這些資料來源類型，針對相關 API 呼叫、CloudTrail 事件和 AWS Config 規則評估您的 IAM 資源 (例如群組、金鑰和政策)。

2. 資源評估的結果將被保存，並轉換為易於稽核的證據。此證據包含從每個資料來源擷取的原始資料，以及指示資料支援哪些控制項的其他中繼資料。

3. Audit Manager 會將儲存的證據附加至評估中名為 Personnel Termination 的控制項。

### 如何手動上傳此控制項的證據

若要上傳補充自動化證據的手動證據，請參閱[中的上傳手動證據 AWS Audit Manager](#)。Audit Manager 會將上傳的證據附加至評估中名為 Personnel Termination 的控制項。

### 如何使用 Audit Manager 來證明對此控制項的合規性

將證據附加到控制項後，您或您選擇的委派代表可以檢閱證據，以查看證據是否充分或是否需要進行任何修補。例如，當您檢閱此控制項時，您可能會發現只有部分符合其需求。如果您有證據證明訪問被撤銷，但沒有任何退出面試的副本，則可能是這種情況。您可以將控制權委派給 HR 利益相關者，然後他們可以上傳退出面試文書的副本。或者，如果稽核期間沒有員工終止，您可以留下註解，說明為何控制項沒有附加簽署的文書工作。

當您確認自己符合控制項時，可以將該控制項標記為已檢閱，並將證據新增至您的評估報告。然後，您可以與稽核人員共用此報告，以證明控制項正在如預期般運作。

## 與相關集成 AWS 服務

AWS Audit Manager 與多個集成 AWS 服務 以自動收集您可以包含在評估報告中的證據。

### AWS Security Hub

AWS Security Hub 使用根據 AWS 最佳實務和業界標準的自動安全檢查來監控您的環境。啟用 Security Hub 後，Audit Manager 會直接從 Security Hub 報告安全檢查結果，以擷取資源安全狀態的快照。如需有關 Security Hub 的詳細資訊，請參閱[什麼是 AWS Security Hub ?](#) 在《AWS Security Hub 使用者指南》中。

### AWS CloudTrail

AWS CloudTrail 協助您監控對帳戶中資 AWS 源進行的呼叫。其中包括 AWS 管理主控台、AWS CLI 和其他呼叫 AWS 服務。Audit Manager 會 CloudTrail 直接從中收集記錄資料，並將處理的記錄檔轉換為使用者活動證據。如需有關的詳細資訊 CloudTrail，請參閱[什麼是 AWS CloudTrail ?](#) 在《AWS CloudTrail 使用者指南》中。

### AWS Config

AWS Config 提供您中 AWS 資源組態的詳細檢視 AWS 帳戶。這包含資源彼此之間的關係和之前的組態方式的資訊。Audit Manager 會直接從中報告發現項目，以擷取資源安全狀況的快照 AWS Config。如需有關的詳細資訊 AWS Config，請參閱[什麼是 AWS Config ?](#) 在《AWS Config 使用者指南》中。

## AWS License Manager

AWS License Manager 簡化將軟體廠商授權帶入雲端的程序。在建置雲端基礎架構時 AWS，您可以透過重新利用現有的授權庫存以與雲端資源搭配使用，以節省成本。Audit Manager 提供 License Manager 架構，協助您準備稽核。此架構與 License Manager 整合，可根據客戶定義的授權規則彙總授權使用資訊。如需有關 License Manager 的詳細資訊，請參閱[什麼是 AWS License Manager？](#) 在《AWS License Manager 使用者指南》中。

## AWS Control Tower

AWS Control Tower 針對雲端基礎架構強制執行預防性和偵探護欄。Audit Manager 提供 AWS Control Tower 護欄架構，協助您進行稽核準備工作。此架構包含以來自的護欄為基礎的所有 AWS Config 規則。AWS Control Tower 如需有關的詳細資訊 AWS Control Tower，請參閱[什麼是 AWS Control Tower？](#) 在《AWS Control Tower 使用者指南》中。

## AWS Artifact

AWS Artifact 是一個自助式稽核人工因素擷取入口網站，提供依需求存取 AWS 基礎結構的合規性文件和認證。AWS Artifact 提供證據以證明 AWS 雲端基礎架構符合合規性要求。相反地，可 AWS Audit Manager 協助您收集、檢閱和管理證據，以證明您的 AWS 服務使用方式符合規定。如需有關的詳細資訊 AWS Artifact，請參閱[什麼是 AWS Artifact？](#) 在《AWS Artifact 使用者指南》中。您可以在中下載[AWS 報告清單](#) AWS Management Console。

## Amazon EventBridge

Amazon 可 EventBridge 協助您自動化 AWS 服務 並自動回應系統事件，例如應用程式可用性問題或資源變更。您可以使用 EventBridge 規則來偵測 Audit Manager 事件並對其做出回應。根據您建立的規則，當事件符合您在規則中指定的值時，EventBridge 叫用一或多個目標動作。根據事件的類型，您可能想要傳送通知、擷取事件資訊，採取修正動作、啟動事件，或採取其他動作。如需詳細資訊，請參閱[AWS Audit Manager 使用 Amazon 監控 EventBridge](#)。

如需特定規範遵循 AWS 服務 方案範圍的清單，請參閱[合規性計劃範圍AWS 服務](#)中的。如需更多一般資訊，請參閱[AWS 合規計劃](#)。

## 與第三方 GRC 產品的整合

AWS Audit Manager 支援與此頁面上列出的第三方合作夥伴 GRC 產品整合。

如果您的公司使用混合雲端模式或多雲端模式，您很可能使用 GRC 產品來管理來自那些環境的證據。當該產品與 Audit Manager 整合時，您可以將您 AWS 使用情況的相關證據直接提取到 GRC 環境中。這樣能在您準備稽核時，為您提供一個集中的位置來檢閱和修復證據，從而簡化您管理合規的方式。



閱讀此頁面，了解可從 Audit Manager 擷取證據的第三方廠商 GRC 產品概述。您也可以查看您能直接在這些產品中執行哪些 Audit Manager API 動作的參考資料。

## 主題

- [了解第三方整合如何與 Audit Manager 配合](#)
- [與 Audit Manager 整合的第三方 GRC 合作夥伴產品](#)

## 了解第三方整合如何與 Audit Manager 配合

GRC 合作夥伴可以使用 Audit Manager 公用 API，將其產品與 Audit Manager 整合。有了這項整合，您可以將 GRC 環境中的企業控制項對應至 Audit Manager 提供的通用控制項。

### Tip

您可以將企業控制項對應至任何類型的 [Audit Manager 控制項](#)。不過，我們建議您使用一般控制項。當您對應至代表您目標的通用控制項時，Audit Manager 會從由管理的預先定義資料來源群組收集證據 AWS。這意味著您不必成為 AWS 專家，即可知道哪些資料來源為您的目標收集相關證據。

完成此一次性控制項映射練習後，您可以直接在 GRC 產品中建立 Audit Manager 評估。此動作會開始收集有關您 AWS 使用情況的證據。然後，您可以查看此 AWS 證據以及從混合式環境中收集的其他證據，所有這些證據都在您的企業控制項的相同內容中。

當您將 Audit Manager 整合與第三方 GRC 產品時，請謹記以下幾點：

- 所有[支援 Audit Manager 的 AWS 區域](#) 都可以整合。
- 您在 GRC 合作夥伴產品中建立的任何 Audit Manager 理員資源也會反映在 Audit Manager 中。
- 除了第三方 GRC 產品的定價外，您還需要遵守 [AWS Audit Manager 定價](#)。
- Audit Manager 收集的證據是不可變的。在第三方 GRC 產品中，證據的呈現方式與 Audit Manager 主控台顯示的方式完全相同。不過，如果您使用第三方整合，您或許可以在報告中提供其他內容，藉此增強此證據。
- [適用於 Audit Manager 的相同配額](#) 也適用於第三方 GRC 產品。例如，每個 AWS 帳戶最多可以有 100 個有效的 Audit Manager 評估。無論您是在 Audit Manager 主控台還是在第三方 GRC 產品中建立評估，都會套用此帳戶層級配額。大多數 Audit Manager 配額 (但不是全部) 都會列在 Service Quotas 主控台下的 AWS Audit Manager 命名空間下。如需要增加配額，請參閱 [管理您的 Audit Manager 配額](#)。

如果您有合規解決方案，並且有興趣與 Audit Manager 整合，請傳送電子郵件至 [auditmanager-partners@amazon.com](mailto:auditmanager-partners@amazon.com)。

## 與 Audit Manager 整合的第三方 GRC 合作夥伴產品

下列第三方 GRC 產品可以擷取 Audit Manager 的證據。

### MetricStream

若要使用此整合，請聯絡以 [MetricStream](#) 取得 MetricStream GRC 軟體的存取和購買。

MetricStream 企業 GRC 解決方案以 MetricStream 平台為基礎，可針對整個企業的 GRC 活動和流程提供全面且協同合作的方法。從 Audit Manager 擷取證據後 MetricStream，您可以主動從 AWS 環境中識別不合規的證據，並與內部部署資料來源或其他雲端合作夥伴的證據一起進行檢閱。這為您提供了一種方便且集中的方式，以便在準備稽核時檢閱並改善雲端安全性和合規狀態。

透過 MetricStream 與 Audit Manager 整合，您可以執行下列 API 作業。

任務	API 操作
Audit Manager 整合設定	<ul style="list-style-type: none"> <li>• <a href="#">GetAccountStatus</a></li> <li>• <a href="#">GetOrganizationAdminAccount</a></li> <li>• <a href="#">GetSettings</a></li> </ul>
Audit Manager 資源檢閱	<ul style="list-style-type: none"> <li>• <a href="#">GetAssessment</a></li> <li>• <a href="#">GetAssessmentFramework</a></li> <li>• <a href="#">GetControl</a></li> <li>• <a href="#">ListAssessmentFrameworks</a></li> <li>• <a href="#">ListControls</a></li> </ul>
Audit Manager 資源建立	<ul style="list-style-type: none"> <li>• <a href="#">CreateAssessment</a></li> <li>• <a href="#">CreateAssessmentFramework</a></li> </ul>
Audit Manager 資源更新	<ul style="list-style-type: none"> <li>• <a href="#">UpdateAssessment</a></li> <li>• <a href="#">UpdateAssessmentControl</a></li> <li>• <a href="#">UpdateAssessmentStatus</a></li> </ul>
管理證據	<ul style="list-style-type: none"> <li>• <a href="#">StartQuery</a>(AWS CloudTrail API)</li> </ul>

任務	API 操作
	<ul style="list-style-type: none"><li>• <a href="#">GetQueryResults</a>(AWS CloudTrail API)</li></ul>
Audit Manager 資源刪除	<ul style="list-style-type: none"><li>• <a href="#">DeleteAssessmentFramework</a></li></ul>

### 相關 MetricStream 連結

- [AWS Marketplace 鏈接](#)
- [產品連結](#)
- [產品定價](#)

## 將 Audit Manager 證據整合至您的 GRC 系統

身為企業客戶，您可能擁有跨越多個資料中心的資源，包括其他雲端廠商和內部部署環境。要從這些環境中收集證據，您可以使用第三方 GRC ( 治理，風險和合規性 ) 解決方案，例如 MetricStream CyberGRC 或 RSA Archer。或者，您可以使用自己內部開發的專有 GRC 系統。

本教學課程說明如何將內部或外部 GRC 系統與 Audit Manager 整合。這項整合可讓廠商收集其客戶 AWS 使用情況和組態的相關證據，並將該證據直接從 Audit Manager 傳送至 GRC 應用程式。如此一來，您就可以在多個環境中集中管理合規報告。

對於本教程的目的：

1. 廠商是指擁有與 Audit Manager 整合之 GRC 應用程式的實體或公司。
2. 客戶是使用的實體或公司 AWS，也使用內部或外部 GRC 應用程式。

### Note

在某些情況下，GRC 應用程序由同一家公司擁有和使用。在這個案例中，廠商是擁有 GRC 應用程式的群組或小組，而客戶是使用 GRC 應用程式的小組或群組。

此教學課程會讓您了解如何執行以下操作：

- [步驟 1：啟用 Audit Manager](#)
- [步驟 2：設定權限](#)

- [步驟 3. 將企業控制項對應至 Audit Manager 控制項](#)
- [步驟 4. 保持您的控制對應更新](#)
- [步驟 5：建立評估](#)
- [步驟 6. 開始收集證據](#)

## 必要條件

開始之前，請確定您符合下列條件：

- 您有執行中的基礎結構 AWS。
- 您使用內部 GRC 系統，或者您使用廠商提供的第三方 GRC 軟體。
- 您已完成[設定 Audit Manager](#) 所需的所有[先決條件](#)。
- 你很熟悉[理解 AWS Audit Manager 概念和術語](#)。

要記住的一些限制：

- Audit Manager 是一個區域 AWS 服務。您必須在執行 AWS 工作負載的每個區域分別設定 Audit Manager。
- Audit Manager 不支援將來自多個區域的證據彙總到單一區域。如果您的資源跨越多個 AWS 區域，則必須在 GRC 系統中彙總證據。
- Audit Manager 具有您可以建立的資源數目的預設配額。如有需要，您可以要求增加這些預設配額。如需詳細資訊，[請參閱 AWS Audit Manager](#)。

## 步驟 1：啟用 Audit Manager

### 誰完成此步驟

客戶

### 您需要執行的事項

首先啟用 Audit Manager AWS 帳戶。如果您的帳戶是組織的一部分，您可以使用您的管理帳戶啟用 Audit Manager，然後指定稽核管理員的委派管理員。

### 程序

若要啟用 Audit Manager

遵循指示[啟用 Audit Manager](#)。針對您要收集證據的所有區域重複設定程序。

### Tip

如果您使用 AWS Organizations，強烈建議您在此步驟中設定委派管理員。當您在 Audit Manager 中使用委派的系統管理員帳戶時，您可以使用證據尋找器在組織中的所有成員帳戶中搜尋證據。

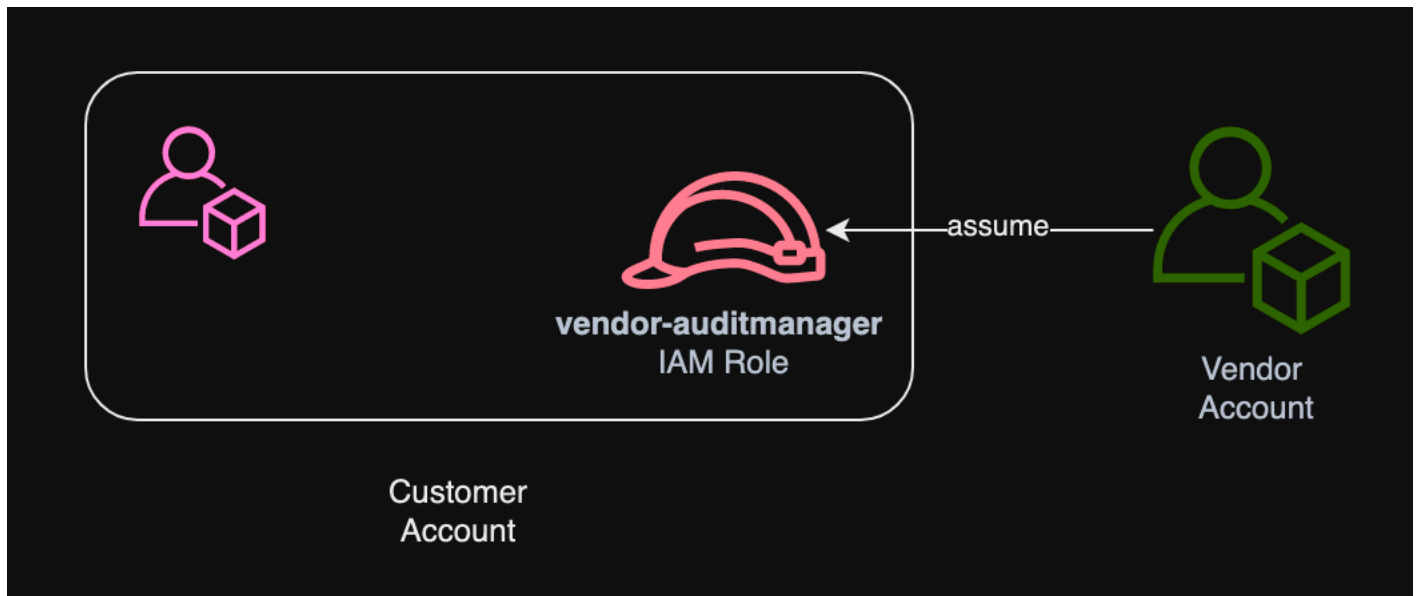
## 步驟 2：設定權限

### 誰完成此步驟

客戶

### 您需要執行的事項

在此步驟中，客戶會為其帳戶建立 IAM 角色。然後，客戶授予以供應商權限以擔任該角色。



### 程序

若要建立客戶帳戶的角色

請按照 IAM 使用者指南的 [為 IAM 使用者建立角色](#) 中的指示進行操作。

- 在角色建立工作流程的步驟 8 中，選擇建立策略，然後輸入角色的策略。

角色至少必須具有下列權限：

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
    }
  ]
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "KmsAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      },
      "StringLike" : {
        "kms:ViaService" : "auditmanager.*.amazonaws.com"
      }
    }
  }
},
{
  "Sid" : "SNSAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TagAccess",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
}
```

```
]
}
```

- 在角色建立工作流程的步驟 11 中，輸入 vendor-auditmanager 「角色」名稱。

### 允許供應商帳戶擔任角色

遵循 IAM [使用者指南中授與使用者切換角色的權限](#)中的指示。

- 政策聲明必須包含 Allow 對 sts:AssumeRole action。
- 它還必須在資源元素中包含角色的 Amazon 資源名稱 (ARN)。
- 以下是您可以使用的政策聲明示例。

在此原則中，請以廠商的 AWS 帳戶 ID 取代 #####。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::account-id:role/vendor-auditmanager"
  }
}
```

## 步驟 3。將企業控制項對應至 Audit Manager 控制項

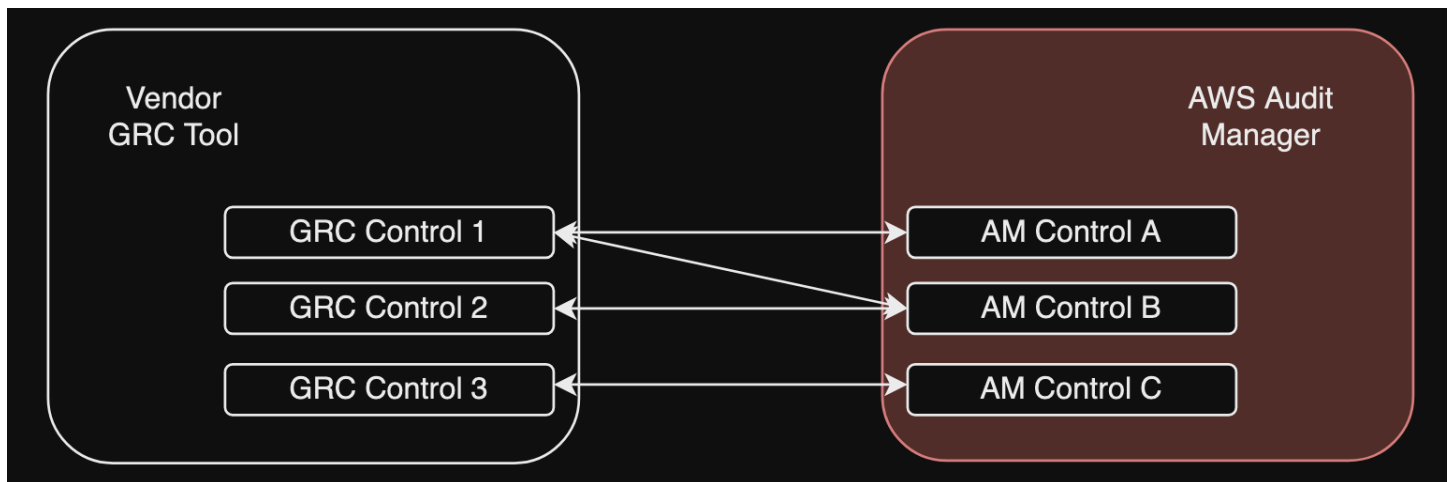
### 誰完成此步驟

客戶

### 您需要執行的事項

供應商會維護精選的企業控制項清單，供客戶在評估中使用。若要與 Audit Manager 整合，廠商必須建立一個介面，讓客戶能夠將其企業控制項對應至對應的 Audit Manager 控制項。您可以對映至 [common control](#) s (偏好) 或 [standard control](#) s。在供應商的 GRC 應用程式中開始任何評估之前，您必須先完成此對應。





### 選項 1：將企業控制項對應至通用控制項 (建議)

這是將企業控制項對映至 Audit Manager 的建議方式。這是因為常見的控制項與一般業界標準密切一致。這樣可以更輕鬆地將它們映射到您的企業控制項。

透過這種方法，供應商會建立一個介面，讓客戶能夠在其企業控制項與 Audit Manager 提供的對應通用控制項之間執行一次性對映。廠商可以使用 [ListControlsListCommonControls](#)、和 [GetControl](#) API 作業向客戶顯示此資訊。客戶完成對映練習後，供應商可以使用這些對映在 Audit Manager 中 [建立自訂控制項](#)。

下面是一個常見的控制映射的例子：

假設您有名為 Asset Management。此企業控制項會對應至 Audit Manager (Asset performance management 和 Asset maintenance scheduling) 中的兩個通用控制項。在這種情況下，您必須在 Audit Manager 中建立自訂控制項 (我們將其命名 enterprise-asset-management)。然後，Asset performance management 並將 Asset maintenance scheduling 其作為證據來源添加到新的自定義控件中。這些證據來源會從預先定義的 AWS 資料來源群組收集支援證據。這為您提供了一種有效的方法來識別對應到企業控制項需求的 AWS 資料來源。

### 程序

若要尋找可對應至的可用通用控制項

依照下列 [步驟尋找 Audit Manager 中可用的通用控制項](#) 清單。

### 建立自訂控制項

1. 請依照下列 [步驟建立符合您企業控制項](#) 的自訂控制項。

當您在自訂控制項建立工作流程的步驟 2 中指定證據來源時，請執行下列動作：

- 選擇AWS 託管來源作為證據來源。
- 選取 [使用符合法規遵循目標的通用控制項]。
- 選擇最多五個常用控制項作為企業控制的證據來源。

2. 針對所有企業控制項重複此工作，並在 Audit Manager 中為每個控制項建立對應的自訂控制項。

## 選項 2：將企業控制項對應至標準控制項

Audit Manager 提供大量預先建置的標準控制項。您可以在企業控制項與這些標準控制項之間執行一次性對應。識別對應於企業控制項的標準控制項之後，您可以直接將這些標準控制項新增至自訂架構。如果您選擇此選項，則不需要在 Audit Manager 中建立任何自訂控制項。

### 程序

#### 尋找可對映至的可用標準控制項的步驟

遵循下列步驟，在「[Audit Manager](#)」中尋找可用標準控制項的清單。

#### 若要建立自訂架構

1. 請依照下列步驟在 Audit Manager 中[建立自訂架構](#)。

當您在架構建立程序的步驟 2 中指定控制項集時，請納入對應至企業控制項的標準控制項。

2. 對所有企業控制項重複此工作，直到您已將所有對應的標準控制項納入自訂架構中為止。

## 步驟 4. 保持您的控制對應更新

### 誰完成此步驟

廠商、客戶

### 您需要執行的事項

Audit Manager 會持續更新通用控制項和標準控制項，以確保它們使用最新的可用 AWS 資料來源。這表示對應控制項是一次性工作：將標準控制項新增至自訂架構後，不需要管理標準控制項，而且在將它們新增為自訂控制項中的證據來源之後，也不需要管理通用控制項。每當更新通用控制項時，相同的更新都會自動套用至使用該通用控制項做為證據來源的所有自訂控制項。

但是，隨著時間的推移，您可能會使用新的通用控制項和標準控制項作為證據來源。考慮到這一點，廠商和客戶應該建立工作流程，以定期從 Audit Manager 擷取最新的通用控制項和標準控制項。然後，您可以複查企業控制項與 Audit Manager 控制項之間的對映，並視需要更新對映。

如果您的企業控制項已對應至通用控制項

在對映程序期間，您建立了自訂控制項。您可以使用 Audit Manager 來編輯這些自訂控制項，以便它們使用最新可用的通用控制項作為證據來源。自訂控制項更新生效後，您現有的評估會自動針對更新的自訂控制項收集證據。不需要建立新的架構或評估。

程序

若要尋找可對應至的最新通用控制項

遵循下列步驟，在「Audit Manager」中[尋找可用的一般控制項](#)。

編輯自訂控制項

1. 依照下列步驟在 [Audit Manager](#) 中編輯自訂控制項。

當您在編輯工作流程的步驟 2 中更新證據來源時，請執行下列動作：

- 選擇AWS 託管來源作為證據來源。
- 選取 [使用符合法規遵循目標的通用控制項]。
- 選擇您要用作自訂控制項的證據來源的新通用控制項。

2. 針對您要更新的所有企業控制項重複此工作。

如果您的企業控制項已對應至標準控制項

在此情況下，廠商必須建立包含最新可用標準控制項的新自訂架構，然後使用此新架構建立新的評估。建立新評估後，您可以將舊評估標記為非作用中。

程序

尋找您可以對應至的最新標準控制項的步驟

遵循下列步驟，在「Audit Manager」中[尋找可用的標準控制項](#)。

若要建立自訂架構並新增最新的標準控制項

請依照下列步驟在 Audit Manager 中[建立自訂架構](#)。

當您在架構建立工作流程的步驟 2 中指定控制項集時，請包含新的標準控制項。

若要建立評估

在 GRC 應用程式中建立評估。

若要將評估的狀態變更為非作用中

依照下列步驟[變更 Audit Manager 中評估的狀態](#)。

## 步驟 5：建立評估

誰完成此步驟

GRC 應用程式，提供供應商的意見

您需要執行的事項

身為客戶，您不需要直接在 Audit Manager 中建立評估。當您針對 GRC 應用模組中的某些控制項開始評估時，GRC 應用模組會在「Audit Manager 程式」中為您建立對應的資源。首先，GRC 應用模組會使用您建立的對映來識別相關「Audit Manager 程式」控制項。接下來，它會使用控制項資訊為您建立自訂架構。最後，它會使用新建立的自訂架構在 Audit Manager 中建立評估。

在 Audit Manager 中建立評估也需要一個[範圍](#)。此範圍會列出客戶要執行評估的 AWS 帳戶 位置並收集證據的清單。客戶必須直接在 GRC 應用程式中定義此範圍。

身為廠商，您需要儲存對assessmentId應至 GRC 應用程式中啟動之評估的對應。

這assessmentId是從「Audit Manager 擷取證據的必要條件。

若要尋找評估 ID

1. 使用此[ListAssessments](#)作業可在 Audit Manager 中檢視您的評量。您可以使用 [status](#) 參數來檢視作用中的評量。

```
aws auditmanager list-assessments --status ACTIVE
```

2. 在回應中，識別您要儲存在 GRC 應用程式中的評估，並記下assessmentId.

## 步驟 6. 開始收集證據

誰完成此步驟

## AWS Audit Manager，以供應商提供的意見

### 您需要執行的事項

建立評估後，最多需要 24 小時才能開始收集證據。此時，您的企業控制項現在會主動收集 Audit Manager 評估的證據。

我們建議您使用[證據搜尋器](#)功能，在 Audit Manager 中快速查詢和尋找證據。如果您以委派管理員的身分使用證據搜尋工具，您可以在組織中的所有成員帳戶中搜尋證據。使用篩選條件和分組的組合，您可以逐步縮小搜尋查詢的範圍。例如，如果您想要系統健全狀況的高階檢視，請擴大搜尋範圍，並依據評估、日期範圍和資源合規性進行篩選。如果您的目標是修復特定資源，則可以縮小搜尋範圍，以針對特定控制項或資源 ID 的證據作為目標。定義篩選條件後，您可以先分組並預覽相符的搜尋結果，然後再建立評估報告。

### 啟用證據搜尋工具

- 依照指示從 Audit Manager 設定[啟用證據搜尋工具](#)。

啟用證據搜尋工具之後，您可以決定從 Audit Manager 取得證據以進行評估。您也可以擷取評估中特定控制項的證據，並將證據儲存在對應至企業控制項的 GRC 應用程式中。您可以使用下列 Audit Manager API 作業來擷取證據：

- [GetEvidence](#)
- [GetEvidenceByEvidenceFolder](#)
- [GetEvidenceFolder](#)
- [GetEvidenceFoldersByAssessment](#)
- [GetEvidenceFoldersByAssessmentControl](#)

## 定價

無論您是廠商還是客戶，此整合設定都不會產生任何額外費用。客戶需要支付在 Audit Manager 中收集的證據的費用。如需定價的詳細資訊，請參閱[AWS Audit Manager 定價](#)。

## 其他資源

您可以檢閱下列資源，深入了解本教學課程中所介紹的概念：

- [評估](#) — 瞭解管理評量的概念和工作。

- [控制項程式庫](#) — 瞭解管理自訂控制項的概念和工作。
- [架構程式庫](#) — 瞭解管理自訂架構的概念和工作。
- [證據查找器](#)-了解如何導出 CSV 文件或從查詢結果中生成評估報告。
- [下載中心](#)-瞭解如何從 Audit Manager 下載評量報告和 CSV 匯出。

# 支援的架構 AWS Audit Manager

當您探索中的架構程式庫時 AWS Audit Manager，您會發現完整的預先建置標準架構清單，可協助您簡化合規性工作。這些預先建置的架構是以各種法規遵循標準和法規的 AWS 最佳實務為基礎。無論您是否需要針對 HIPAA、PCI DSS、SOC 2 或更多項目評估環境，都可以使用這些架構協助您進行稽核準備。

下列清單提供可用架構的概觀，以便您輕鬆識別符合特定需求的架構。請花點時間檢閱清單，並熟悉與組織需求最相關的架構。開啟任何頁面以查看該架構的概觀，並瞭解如何使用它來建立評估，並開始在 Audit Manager 中收集證據。

## 主題

- [ACSC 基本八項](#)
- [阿克斯科會 ISM 二零二三年三月二日](#)
- [AWS Audit Manager 示例框架](#)
- [AWS Control Tower 護欄](#)
- [AWS 生成人工智慧最佳實務架構 v2](#)
- [AWS License Manager](#)
- [AWS 基礎安全性最佳做法](#)
- [AWS 營運最佳實務](#)
- [AWS 架構良好的框架 WAF V10](#)
- [CCCS 中型雲端控制](#)
- [獨聯體 AWS 基準 V1.2.0](#)
- [獨聯體 AWS 基準 V1.3.0](#)
- [獨聯體 AWS 基準測試 v1.4.0](#)
- [独联体控制 7.1 版](#)
- [獨聯體關鍵安全控制系統 8.0 版](#)
- [安全性 FedRAMP 準控制項 r4](#)
- [GDPR](#)
- [金融服務業現代化法 \(GLBA\)](#)
- [標題 21 CFR 第 11 部分](#)

- [歐盟 GMP 附件 11, V1](#)
- [HIPAA 安全性規則：2003 年 2 月](#)
- [HIPAA 全方位最終規則](#)
- [ISO/IEC 27001:2013 Annex A](#)
- [第五修訂版](#)
- [NIST 網路安全架構 1.1 版](#)
- [尼斯特第二版](#)
- [PCI DSS V3.2.1](#)
- [PCI DSS V4.0](#)
- [SSE -18 系統管理系統 2](#)

## ACSC 基本八項

AWS Audit Manager 提供預先構建的標準框架，支持澳大利亞網路安全中心 (ACSC) 基本八。

### 主題

- [什麼是 ACSC 基本八？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 ACSC 基本八？

ACSC 是澳大利亞政府的網路安全主要機構。為了防範網路威脅，ACSC 建議組織根據 ACSC 紓解網路安全事件的策略實施八項基本紓解策略作為基準。這個基準線被稱為基本八項，使得對手更難破壞系統。

由於基本八項概述了一組最低限度的預防措施，因此您的組織需要在您的環境保證的情況下實施其他措施。此外，儘管基本八項可以幫助減輕大多數網路威脅，但它不會減輕所有網路威脅。因此，需要考慮其他紓解策略和安全控制措施，包括紓解網路安全事件的策略和資訊安全手冊(ISM) 中的策略。

[基本八項](#)由 [ACSC](#) 是根據[知識共享署名 4.0 國際許可許](#)可和版權資訊可以在 [ACSC 找到](#) | 版權。© 2022 年澳大利亞聯邦。



## 使用此架構

您可以在中使用基本八標準架構 AWS Audit Manager 來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據基本八項要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據基本八項架構中定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
澳大利亞網絡安全中心 ( ACSC ) 基本八	144	49	3

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_ASCS-Essential-Eight.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不是用來驗證您的系統是否符合「基本八」控制項。此外，他們不能保證您將通過 ACSC 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在「Audit Manager」框架庫的「標準框架」選項卡下找到「基本八」框架。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [ACSC 基本八項](#)

## 阿克斯科會 ISM 二零二三年三月二日

AWS Audit Manager 提供預先建置的標準架構，以支援澳洲網路安全中心 (ACSC) 資訊安全手冊 (ISM)。

### 主題

- [什麼是 ACSC ISM ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 ACSC ISM ?

ACSC 是澳大利亞政府的網路安全主要機構。ACSC 生產 ISM，它作為一組網路安全原則的功能。這些原則的目的是提供有關組織如何保護其系統和資料免受網路威脅的策略指導。這些網路安全原則分為四個關鍵活動：管理、保護、偵測和回應。組織應要能夠證明其組織內部正在遵守網路安全原則。ISM 適用於資訊安全長、資訊長、網路安全專業人員和資訊技術經理。

ISM 框架由 ACSC 根據 [創用 CC 姓名標示 4.0 國際授權](#) 條款提供，版權信息可在 [ACSC](#) | 版權所有。© 2022 年澳大利亞聯邦。

## 使用此架構

您可以使用中的 ACSC ISM 標準架構 AWS Audit Manager 來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 ACSC ISM 需求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 ACSC ISM 架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，

您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
澳大利亞網絡安全中心 ( ACSC ) 信息安全手冊 ( ISM ) 2023 年 3 月 2 日	557	320	22

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_ACSC-ISM-02-March-2023.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用於驗證您的系統是否符合 ACSC 資訊安全手冊控制項。此外，他們不能保證您將通過 ACSC 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到 ACSC ISM 架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [ACSC 資訊安全手冊](#)

## AWS Audit Manager 示例框架

AWS Audit Manager 提供預先建置的範例架構，協助您開始進行稽核準備。

## 主題

- [什麼是示 AWS Audit Manager 例框架？](#)
- [使用此架構](#)
- [後續步驟](#)

## 什麼是示 AWS Audit Manager 例框架？

AWS Audit Manager 範例架構是一個簡單的架構，可用來在 Audit Manager 中開始使用。相較之下，Audit Manager 提供的其他一些預先打造架構要大得多，而且包含許多控制項。透過使用範例架構，而不是這些較大的架構，您可以更輕鬆地檢閱和探索架構的範例。此架構中的控制項是以一系列 AWS Config 規則和 AWS API 呼叫為基礎。

## 使用此架構

您可以使用此架構來協助您開始使用 Audit Manager。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用 AWS Audit Manager 範例架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。接下來，它會收集相關證據，然後將其附加到評估中的控制項。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
Amazon Web Services (AWS) Audit Manager 示例框架	5	0	3

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_AWS-Audit-Manager-Sample-Framework.zip](#) 檔案。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## AWS Control Tower 護欄

AWS Audit Manager 提供預先建立的 AWS Control Tower 護欄架構，協助您進行稽核準備。

### 主題

- [什麼是 AWS Control Tower ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS Control Tower ?

AWS Control Tower 是一項管理和治理服務，可用來瀏覽建立多帳戶 AWS 環境所涉及的設定程序和治理需求。

使用 AWS Control Tower，您只需按幾下滑鼠即可佈建符合公司或整個組織政策的新 AWS 帳戶政策。AWS Control Tower 代表您建立協調流程層，結合並整合其他 [AWS 服務](#) 數個功能。這些服務包括 AWS Organizations AWS IAM Identity Center、和 AWS 服務目錄。其有助於簡化設置、管理多重帳戶，打造既安全又合規的 AWS 環境。

AWS Control Tower 護欄框架包含所有以來自 AWS Config 規則的護欄為基礎的。AWS Control Tower

## 使用此架構

您可以使用 AWS Control Tower 防護機制架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據以中 AWS Config 規則的護欄為基礎的來群組。AWS Control Tower 您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 AWS Control Tower 稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 AWS Control Tower 護欄架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS Control Tower 護欄框架的詳細信息如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
AWS Control Tower 護欄	14	0	5

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_AWS-Control-Tower-Guardrails.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合 AWS Control Tower 護欄。因此，其無法保證您會通過稽核。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到 [AWS Control Tower 護欄] 架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [AWS Control Tower 服務頁面](#)
- [AWS Control Tower 使用者指南](#)

# AWS 生成人工智慧最佳實務架構 v2

## Note

2024 年 6 月 11 日，將此架構 AWS Audit Manager 升級為新版本的 AWS 生成式人工智慧最佳實務架構 v2。除了支援 Amazon 基岩的最佳實務外，v2 還可讓您收集證據，證明您正在遵循 Amazon 上的最佳實務。SageMaker 不再支援 AWS 生成 AI 最佳實務架構 v1。如果您先前已從 v1 架構建立評估，您現有的評估將會繼續運作。不過，您無法再從 v1 架構建立新評估。我們鼓勵您使用 v2 升級的框架來代替。

AWS Audit Manager 提供預先建置的標準架構，協助您深入瞭解 Amazon 基岩和 Amazon SageMaker 上的生成 AI 實作如何依照建 AWS 議的最佳實務進行運作。

Amazon Bedrock 是一項全受管服務，可透過 API 使用 Amazon 和其他首席人工智慧公司的 AI 模型。使用 Amazon Bedrock，您可以搭配組織資料私下調整現有模型。這可讓您利用基礎模型 (FM) 和大型語言模型 (LLM) 安全地打造應用程式，而不會影響資料隱私。如需詳細資訊，請參閱 Amazon Bedrock 使用者指南中的 [什麼是 Amazon Bedrock?](#)。

Amazon SageMaker 是全受管的機器學習 (ML) 服務。透過 SageMaker，資料科學家和開發人員可以針對需要深度自訂和模型微調的延伸使用案例，建置、訓練和部署機器學習模型。SageMaker 提供受管理的 ML 演算法，以便在分散式環境中針對極大型資料有效執行。透過內建支援您自己的演算法和架構，SageMaker 提供彈性的分散式訓練選項，以適應您的特定工作流程。如需詳細資訊，請參閱 [什麼是 Amazon SageMaker?](#) 在 Amazon 用 SageMaker 戶指南。

## 主題

- [Amazon 基岩的 AWS 生成 AI 最佳實務是什麼?](#)
- [使用此架構幫助您進行稽核準備](#)
- [在 Amazon Bedrock 中手動驗證提示](#)
- [後續步驟](#)
- [其他資源](#)

## Amazon 基岩的 AWS 生成 AI 最佳實務是什麼?

生成式 AI 是指 AI 的一個分支，其重心是讓機器產出內容。生成式 AI 模型的設計目的，是要產生與訓練範例非常相似的輸出。這會建立 AI 可以模仿人類對話、產生創意內容、分析大量資料，將通常由人

類完成的程序自動化的情境。生成式 AI 的快速成長，帶來非常可觀的創新技術。在此同時，要如何以負責任的方式使用生成式 AI 並符合治理要求，在這些方面帶來了新的挑戰。

AWS 致力於為您提供所需的工具和指導，以負責任的方式建置和管理應用程式。為了協助您達成此目標，Audit Manager 已與 Amazon 基岩合作，並 SageMaker 建立 AWS 生成人工智慧最佳實務架構 v2。此架構為您提供專門建置的工具，用於在 Amazon 基岩和 Amazon 上監控和改善生成 AI 專案的治理。SageMaker 您可以使用此架構中的最佳實務，針對模型使用情況提高控制力與可見性，並隨時瞭解模型行為。

該框架中的控件是與 AI 專家、合規從業人員、安全保證專家合作開發的 AWS，並獲得德勤的意見。每個自動控制項都會對應至 Audit Manager 從中收集證據的 AWS 資料來源。您可以根據以下八個原則，使用收集到的證據來評估您的生成式 AI 實施：

1. 負責 — 針對生成式 AI 模型的部署和使用，制定並遵守道德條件
2. 安全 — 建立清楚的參數和道德界限，以防止產生有害或有問題的輸出
3. 公平 — 考慮並尊重 AI 系統如何影響使用者的不同子群
4. 永續 — 力求更高的效率和更永續的能源
5. 韌性 — 維持完整性和可用性機制，以確保 AI 系統可靠地運行
6. 隱私 — 確保敏感資料不遭竊或暴露
7. 準確 — 打造精確、可靠且穩健的 AI 系統
8. 安全 — 防止未經授權人士存取生成式 AI 系統

## 範例

假設您的應用程式使用 Amazon Bedrock 提供的第三方基礎模型。您可以使用 AWS 生成 AI 最佳實務架構來監控此模型的使用情況。透過使用此架構，您可以收集證據，證明您的使用方式符合生成式 AI 最佳實務。這為您提供了穩定持續的方法，用來追蹤模型的使用情況和權限，標記敏感資料以及收到任何意外揭露的警報。例如，此架構中的特定控制項可以收集證據，協助您證明您已針對下列項目實作機制：

- 紀錄新資料的來源，性質，品質和處理，以確保透明度並幫助故障排除或審核 (負責)
- 使用預先定義的效能指標定期評估模型，以確保模型符合準確性和安全性基準 (安全)
- 使用自動化監控工具，即時偵測和警示潛在的偏見成果或行為 (公平)
- 不論是否由您產生模型，都會評估、識別和紀錄模型使用情況以及可重複使用現有模型的案例 (永續)
- 如果發生無意的 PII 外洩或意外揭露 (隱私)，設定通知程序



- 建立人工智慧系統的即時監控，並針對任何異常或中斷設定警示 (韌性)
- 偵測不準確性，並進行徹底的錯誤分析以瞭解根本原因 (準確)
- 對 AI 模型的輸入和輸出數據實施 end-to-end 加密，以達到最低行業標準 (安全)

## 使用此架構幫助您進行稽核準備

### Note

- 如果您是 Amazon 基岩或 SageMaker 客戶，則可以直接在 Audit Manager 中使用此架構。請務必在您執行生成式 AI 模型和應用程式的 AWS 帳戶和區域中使用此架構並執行評估。
- 如果您想要加密 Amazon 基岩或使 SageMaker 用自己的 KMS 金鑰的 CloudWatch 日誌，請確定 Audit Manager 可以存取該金鑰。若要這麼做，您可以在稽核管理員[設定您的資料加密設定](#)設定中選擇客戶管理的金鑰。
- 此框架使用 Amazon 基岩[ListCustomModels](#)操作來產生有關您自訂模型使用情況的證據。此 API 作業目前僅在美國東部 (維吉尼亞北部) 和美國西部 (奧勒岡) AWS 區域支援。因此，您可能無法在亞太區域 (東京)、亞太區域 (新加坡) 或歐洲 (法蘭克福) 區域看到自訂模型使用的證據。

您可以使用此架構協助您準備稽核，瞭解 Amazon 基岩和 SageMaker 其包括一個預先建置的控制集，其中包含說明和測試程序。這些控制項會根據生成式 AI 最佳實務來分組為不同控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集證據，以協助您監視預期原則的遵循情形。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 AWS 生成 AI 最佳實務架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱	AWS Audit Manager	控制集數	自動化控制項數量	手動控制項數量
AWS 生成人工智慧最佳實務架構 v2		8	71	39

**i** Tip

若要深入瞭解自動化和手動控制項，請參閱 [Audit Manager 概念與術語](#)，以取得將手動證據新增至部分自動化控制項最佳時機範例的建議。

若要檢閱在此標準架構中用來做為控制資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ ConfigDataSourceMappings \\_ AWS-產生-AI 最佳作法- 框架 V2](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用於驗證您的系統是否符合生成 AI 最佳實務。此外，他們無法保證您會通過有關生成 AI 使用情況的稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 在 Amazon Bedrock 中手動驗證提示

您可能有不同的提示集，您需要針對特定模型進行評估。在此情況下，您可以使用 `InvokeModel` 操作來評估每個提示，並收集回應作為手動證據。

### 使用 `InvokeModel` 操作

若要開始使用，請建立預先定義的提示清單。您將使用這些提示來驗證模型的回應。請確定您的提示清單具有您要評估的所有使用案例。例如，您可能會收到提示，提示您可以用來驗證模型回應是否不會洩露任何個人身分識別資訊 (PII)。

建立提示清單後，請使用 Amazon Bedrock 提供的 [InvokeModel](#) 操作來測試每個提示。然後，您可以收集模型對這些提示的回應，並在 Audit Manager 評估中將 [此資料作為手動證據上傳](#)。

`InvokeModel` 操作有三種不同的使用方法。

#### 1. HTTP 請求

您可以使用郵差等工具來建立 HTTP 要求呼叫，`InvokeModel` 並儲存回應。

**i** Note

Postman 是由第三方公司開發。它不是由開發或支持 AWS。若要進一步了解如何使用 Postman 或需 Postman 相關問題的協助，請參閱 Postman 網站的 [支援中心](#)。

## 2. AWS CLI

您可以使用 AWS CLI 來執行[叫用模型](#)命令。如需指示和詳細資訊，請參閱 Amazon Bedrock 使用者指南中的[在模型上執行推論](#)。

下面的例子演示了如何 AWS CLI 使用提示生成文本 ##### 和人造### V2 模型。該示例在響應中返回多達 300 個令牌，並將響應保存到文件 `invoke-model-output.txt`：

```
aws bedrock-runtime invoke-model \  
  --model-id anthropic.claude-v2 \  
  --body '{"prompt": "\n\nHuman:story of two dogs\n\nAssistant:",  
  "max_tokens_to_sample" : 300}' \  
  --cli-binary-format raw-in-base64-out \  
  invoke-model-output.txt
```

## 3. 自動化驗證

您可以使用 CloudWatch Synthetics 金絲雀來監視模型響應。使用此解決方案，您可以驗證預先定義的提示清單的 InvokeModel 結果，然後使用 CloudWatch 來監視這些提示的模型行為。

要開始使用此解決方案，您必須首先[建立一個 Synthetics 金絲雀](#)。建立金絲雀後，您可以使用下列程式碼片段來驗證您的提示和模型的回應。

```
const invokeModel = async function () {  
  log.info("Starting Bedrock::Invoke.");  
  
  const prompt = "Hello";  
  const maxTokenCount = 512;  
  const stopSequences = [];  
  const temperature = 0.5;  
  const topP = 0.5;  
  
  const modelId = "amazon.titan-tg1-large";  
  
  var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:  
"us-west-2"});  
  const param = {  
    body: {  
      "inputText": prompt,  
      "textGenerationConfig": {  
        "maxTokenCount": maxTokenCount,  
        "stopSequences": stopSequences,  
        "temperature": temperature,
```

```

        "topP": topP
      }
    },
    modelId: modelId
  };
  const response = await bedrockRuntime.invokeModel(param);
  return "Successfully completed Bedrock::Invoke.";
};

```

### Note

或者，您也可以使用 Lambda 函數執行此指令碼。如果您選擇這個做法，則需要先[建立 Lambda 函數](#)。

## 範例提示

您可以使用這些範例提示作為測試模型回應的起點。在下列範例中，將#####取代為您自己的資料，以反映您的特定測試使用案例。

如需測試模型回應中的不適當內容

```

"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age, religion, or other protected class>"

```

如需在模型回應中測試 PII

```

"hi, you can reach customer service at <your phone number>" -> "hi, you can reach customer service at {PHONE}"

```

如需在模型回應中測試褻瀆

```

"<abusive or derogatory insult>" -> "***** ** ***** **"
"Hello, <offensive name>" -> "Hello, *****"

```

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱[在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [Amazon Bedrock](#)
- [Amazon Bedrock 使用者指南](#)
- [Amazon SageMaker](#)
- [Amazon SageMaker 用戶指南](#)
- [將負責任的 AI 從理論轉變為實踐](#)
- [保護消費者並促進創新 — AI 法規與建立負責任人工智慧的信任](#)
- [負責任地使用機器學習指南](#)

## AWS License Manager

AWS Audit Manager 提供預先建置的 AWS License Manager 架構，協助您進行稽核準備。

### 主題

- [什麼是 AWS License Manager ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS License Manager ?

有了 AWS License Manager，您可以跨內部部署環境集中管理來自各種軟體廠商 (例如 Microsoft、SAP、Oracle 或 IBM) AWS 的軟體授權。將所有軟體授權集中在同一個位置，可提供更好的控制力和可見性，並可能協助您限制超額授權，並降低不合規和錯誤報告問題的風險。

此 AWS License Manager 架構與 License Manager 整合，可根據客戶定義的授權規則彙總授權使用資訊。

## 使用此架構

您可以使用AWS License Manager架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據客戶定義的授權規則進行分組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它根據 AWS License Manager 框架中定義的控件執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

框 AWS License Manager 架的詳細信息如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
AWS License Manager	27	0	6

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合授權規則。因此，他們無法保證您會透過授權使用稽核。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱[在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

### 授權管理器連結

- [AWS License Manager 服務頁面](#)
- [AWS License Manager 使用者指南](#)

## 授權管理員 API

在此架構中，Audit Manager 會使用自訂活動呼叫 `GetLicenseManagerSummary` 來收集證據。`GetLicenseManagerSummary` 活動會呼叫下列三個 License Manager API：

1. [ListLicenseConfigurations](#)
2. [ListAssociationsForLicenseConfiguration](#)
3. [ListUsageForLicenseConfiguration](#)

然後，傳回的資料會轉換成證據，並附加至評估中的相關控制項。

例如，假設您使用兩個授權產品 (2017 年版 SQL 服務和 Oracle 資料庫企業版)。首先，`GetLicenseManagerSummary` 活動會呼叫 [ListLicenseConfigurations](#) API，該 API 會提供您帳戶中授權設定的詳細資料。接下來，它通過調用 [ListUsageForLicenseConfiguration](#) 和為每個許可證配置添加其他上下文數據 [ListAssociationsForLicenseConfiguration](#)。最後，它將授權組態資料轉換為證據，並將其附加到架構中的對應控制項 (4.5 - 2017 SQL 伺服器客戶管理授權和 3.0.4 - Oracle 資料庫企業版客戶管理授權)。如果您使用的授權產品未涵蓋架構中任何控制項，則該授權組態資料會附加至下列控制項的證據：5.0 - 其他授權的客戶管理授權。

## AWS 基礎安全性最佳做法

AWS Audit Manager 提供預先建置的標準架構，以支援 AWS 基礎安全性最佳作法。

### 主題

- [什麼是 AWS 基礎安全最佳實務標準？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS 基礎安全最佳實務標準？

AWS 基礎安全性最佳做法標準是一組控制項，可偵測您部署的帳戶和資源何時偏離安全性最佳作法。

您可以使用此標準來持續評估所有工作負載 AWS 帳戶 和工作負載，並快速找出偏離最佳實務的區域。標準提供了可採取動作和規範式的引導，讓您了解如何改善和維護組織的安全狀態。

控制項包含橫跨多個 AWS 服務的最佳實務。系統會為每個控制項指派一個類別，以反映其套用的安全性功能。如需詳細資訊，請參閱 AWS Security Hub 使用者指南的 [控制類別](#)。

## 使用此架構

您可以使用 AWS 基礎安全性最佳做法架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項 AWS 會根據基礎安全性最佳作法需求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您 AWS 帳戶和服務中的資源。它會根據基 AWS 礎安全性最佳做法架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

AWS 基礎安全性最佳做法架構詳細資料如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
AWS 基礎安全性最佳做法	146	0	31

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 AWS 基礎安全性最佳作法。此外，他們無法保證您會通過 AWS 基礎安全性最佳做法稽核。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- AWS 使 AWS Security Hub 用 [者指南中的基本安全性最佳做法標準](#)



- AWS Security Hub 使用者指南中的[控制項類別](#)

## AWS 營運最佳實務

AWS Audit Manager 提供預先建置的 AWS 作業最佳實務 (OBP) 架構，協助您進行稽核準備。

此架構提供了 AWS 基礎安全性最佳作法標準的控制項子集。這些控制項可做為基準檢查，以偵測您部署的帳戶和資源是否偏離了安全最佳實務。

### 主題

- [什麼是 AWS 基礎安全性最佳做法標準？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS 基礎安全性最佳做法標準？

您可以使用AWS 基礎安全最佳實務標準來評估您的帳戶和工作負載，並快速找出偏離最佳實務的區域。標準提供了可採取動作和規範式的引導，讓您了解如何改善和維護組織的安全狀態。

控制項包含橫跨多個 AWS 服務的最佳實務。系統會為每個控制項指派一個類別，以反映其套用的安全性功能。如需詳細資訊，請參閱AWS Security Hub 使用者指南的[控制類別](#)。

## 使用此架構

您可以使用AWS 操作最佳實務架構，協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 AWS 作業最佳實務要求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

AWS 營運最佳作法架構詳細資料如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
AWS 營運最佳實務	0	51	20

此架構中的控制項並不用於驗證您的系統是否符合 AWS 營運最佳實務。因此，其無法保證您會通過 AWS 操作最佳實務的稽核。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

此架構僅包含手動控制項。這些手動控制不會自動收集證據。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- AWS 使 AWS Security Hub 用 [者指南中的基本安全性最佳做法標準](#)
- AWS Security Hub 使用者指南中的 [控制項類別](#)

## AWS 架構良好的框架 WAF V10

AWS Audit Manager 提供預先建置的標準架構，支援 AWS Well-Architected 的架構第 10 版。

### 主題

- [什麼是 AWS Well-Architected 的框架？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS Well-Architected 的框架？

[AWS Well-Architected](#) 是一種架構，可協助您針對應用程式和工作負載打造安全、高效能、具彈性且有效率的基礎架構。AWS Well-Architected 是以六個支柱 (卓越營運、安全性、可靠性、效能效率、成本最佳化和永續性) 為中心而打造的，其可為您和您的合作夥伴提供一致的方法，來評估架構並實作可擴展的設計。

## 使用此架構

您可以使用 AWS Well-Architected 的架構來協助您為稽核做好準備。此架構說明在雲端中設計和執行工作負載的重要概念、設計原則和結構方面的最佳實務。在 AWS Well-Architected 的六大支柱中，AWS Audit Manager 為安全性和可靠性提供預先建置架構和控制項的支柱。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它根據 AWS Well-Architected 的框架中定義的控件來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
Amazon Web Services ( AWS ) 結構良好的框架 ( WAF ) v10	44	290	6

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_AWS-Well-Architected-Framework-WAF-v10.zip](#) 檔案。

此架構中的控制項，並非為了驗證您的系統是否合規而設計。因此，其無法保證您會通過稽核。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [AWS Well-Architected](#)
- [AWS Well-Architected 的框架文檔](#)

## CCCS 中型雲端控制

AWS Audit Manager 提供預先建置的標準架構，支援加拿大網路安全中心 (CCCS) 中型雲端控制。

### 主題

- [什麼是中華基督教服務中心？](#)
- [使用此架構](#)
- [後續步驟](#)

## 什麼是中華基督教服務中心？

CCCS 是加拿大網路安全專家指導、服務和支援的權威來源。CCCS 為加拿大政府、工業界和公眾提供此專業知識。全國各地的加拿大公共部門組織都依賴他們對雲端服務供應商的嚴格評估，以做出明智的雲端採購決策。

CCCS 中型雲端控制設定檔於 2020 年 5 月，取代加拿大 PROTECTED B/中等完整性/中等可用性 (PBMM) 設定檔的使用。如果您的組織使用公有雲服務來支援具有中等機密性、完整性和可用性 (AIC) 要求的業務活動，則 CCCS 中型雲端安全控制設定檔適合您使用。具有中等 AIC 要求的工作負載，代表未經授權揭露、修改或對業務活動所使用的資訊或服務的訪問，可以合理預期會對個人或組織造成嚴重傷害，或對一組個人群體造成有限的傷害。這些傷害程度的範例如下：

- 對年度利潤的重大影響
- 失去主要客戶
- 商譽損失
- 明確違反合規
- 數百人或成千上萬人的隱私侵犯
- 影響程式效能
- 導致精神障礙或疾病

- 破壞
- 聲譽受損
- 個人財務困難

## 使用此架構

您可以使用 CCCS 中型雲端控制的 AWS Audit Manager 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CCCS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用此架構做為起點，您可以建立 Audit Manager 評估，並開始收集與 CCCS Medium Cloud Control 稽核相關的證據。在評估中，您可以指 AWS 帳戶 定要包含在稽核範圍中的項目。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 CCCS 中型雲端控制架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
加拿大網絡安全中心 ( CCCS ) 中等雲端控制	258	95	175

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_AuditManager\\_ConfigDataSourceMappings\\_CCCS-Medium-Cloud-Control.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 CCCS 中型雲端控制需求。此外，他們不能保證您將通過 CCCS 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 獨聯體 AWS 基準 V1.2.0

AWS Audit Manager 提供了兩個預構建的框架，支持互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.2.0。

### Note

- 如需支援 v1.3.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準 V1.3.0](#)。
- 如需支援 v1.4.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準測試 v1.4.0](#)。

### 主題

- [什麼是 CIS ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 CIS ?

獨聯體國家是一家開發 [獨聯體 AWS 基準基準](#) 的非營利組織。此基準測試可作為一組的安全性組態最佳作法 AWS。這些業界公認的最佳做法超越了現有的高階安全性指引，因為它們為您提供了清晰、step-by-step 實作和評估程序。

如需詳細資訊，請參閱 AWS 安全部落格上的 CIS AWS 基準基準部落格 [文章](#)。

### CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護貴組織使用的特定系統。CIS 控制項是組織層級系統的基本最佳實務指南，以協助防範已知的網路攻擊媒介。

## 範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

示例：獨聯體 AWS 基準測試 v1.2.0-確保為「根用戶」帳戶啟用了 MFA。

此建議提供有關如何檢查此問題以及如何在 AWS 環境的 root 帳戶上設定此項目的規範性指引。

- CIS 控制項則是為組織整體提供的建議。它們不是針對單一供應商產品。

範例：CIS v7.1-針對所有系統管理存取使用多因素驗證

此控制項描述預期要在組織內套用的項目。它不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

## 使用此架構

您可以在中使用 CIS AWS 基準 v1.2 架構 AWS Audit Manager 來協助您為 CIS 稽核做好準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.2.0 , 第一級	35	1	4
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.2.0 , 第一級和第二級	48	1	4

**i** Tip

若要檢閱用來做為這些標準架構之資料來源對映的 AWS Config 規則清單，請下載下列檔案：

1. [AuditManager\\_ConfigDataSourceMappings\\_ 思維系統-AWS-基準標記-V1.2.0,-Level-1.zip](#)
2. [AuditManager\\_ConfigDataSourceMappings\\_ 思維系統-AWS-基準標記-V1.2.0,-Level-1-and-2.zip](#)

這些架構中的控制項並非用於驗證您的系統是否符合 CIS AWS Benchmark 最佳實務。此外，他們不能保證您會通過獨聯體審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到這些架構。

## 使用這些架構的先決條件

CIS AWS 基準 v1.2 框架中的許多控件都用 AWS Config 作數據源類型。若要支援這些控制項，您必須在每個已[啟用](#) Audit Manager AWS 區域的所有帳號 AWS Config 上啟用。您也必須確定已啟用特定 AWS Config 規則，且這些規則已正確設定。

需要以下 AWS Config 規則和參數才能收集正確的證據並獲取 CIS AWS 基準 v1.2 的準確合規狀態。如需如何啟用或配置規則的指示，請參閱[使用 AWS Config 受管規則](#)。

必要的 AWS Config 規則	必要參數
<a href="#">ACCESS_KEYS_ROTATED</a>	<b>maxAccessKeyAge</b> <ul style="list-style-type: none"> <li>• 沒有輪換的最大天數。</li> <li>• 類型：Int</li> <li>• 預設：90 天</li> <li>• 合規要求：最多 90 天</li> </ul>
<a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a>	不適用
<a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a>	不適用



必要的 AWS Config 規則	必要參數
<a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a>	不適用
<a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a>	不適用
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>MaxPasswordAge</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼過期前的天數。</li> <li>類型：int</li> <li>預設：90</li> <li>合規要求：最多 90 天</li> </ul>
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>MinimumPasswordLength</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼的長度下限。</li> <li>類型：int</li> <li>預設：14</li> <li>合規要求：至少 14 字元</li> </ul>
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>PasswordReusePrevention</b> (選用)</p> <ul style="list-style-type: none"> <li>允許重複使用的密碼次數。</li> <li>類型：int</li> <li>預設：24</li> <li>合規要求：重複使用前至少經過 24 個密碼</li> </ul>
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>RequireLowercaseCharacters</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼至少必須包含一個小寫字元。</li> <li>類型：布林值</li> <li>預設：True</li> <li>合規要求：至少有一個小寫字元</li> </ul>

必要的 AWS Config 規則	必要參數
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>RequireNumbers</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼至少必須包含一個數字。</li> <li>類型：布林值</li> <li>預設：True</li> <li>合規要求：至少有一個數字字元</li> </ul>
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>RequireSymbols</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼至少必須包含一個符號。</li> <li>類型：布林值</li> <li>預設：True</li> <li>合規要求：至少有一個符號字元</li> </ul>
<a href="#">IAM_PASSWORD_POLICY</a>	<p><b>RequireUppercaseCharacters</b> (選用)</p> <ul style="list-style-type: none"> <li>密碼至少必須包含一個大寫字元。</li> <li>類型：布林值</li> <li>預設：True</li> <li>合規要求：至少有一個大寫字元</li> </ul>
<a href="#">IAM_POLICY_IN_USE</a>	<p><b>policyARN</b></p> <ul style="list-style-type: none"> <li>要檢查的 IAM 政策 ARN。</li> <li>類型：字串</li> <li>合規要求：建立 IAM 角色以管理事件 AWS。</li> </ul> <p><b>policyUsageType</b> (選用)</p> <ul style="list-style-type: none"> <li>指定應將政策連接到使用者、群組或角色。</li> <li>類型：字串</li> <li>有效值：IAM_USER   IAM_GROUP   IAM_ROLE   ANY</li> <li>預設值：ANY</li> <li>合規要求：將信任政策連結到建立的 IAM 角色</li> </ul>

必要的 AWS Config 規則	必要參數
<a href="#">IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS</a>	不適用
<a href="#">IAM_ROOT_ACCESS_KEY_CHECK</a>	不適用
<a href="#">IAM_USER_NO_POLICES_CHECK</a>	不適用
<a href="#">IAM_USER_UNUSED_CREDENTIALS_CHECK</a>	<b>maxCredentialUsageAge</b> <ul style="list-style-type: none"> <li>無法使用憑證的最大天數。</li> <li>類型：Int</li> <li>預設：90 天</li> <li>合規要求：90 天以上</li> </ul>
<a href="#">INCOMING_SSH_DISABLED</a>	不適用
<a href="#">MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS</a>	不適用
<a href="#">MULTI_REGION_CLOUD_TRAIL_ENABLED</a>	不適用

必要的 AWS Config 規則	必要參數
<a href="#">RESTRICTED_INCOMING_TRAFFIC</a>	<p><b>blockedPort1</b> (選用)</p> <ul style="list-style-type: none"><li>• 已封鎖的 TCP 連接埠號碼。</li><li>• 類型：int</li><li>• 預設：20</li><li>• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入</li></ul> <p><b>blockedPort2</b> (選用)</p> <ul style="list-style-type: none"><li>• 已封鎖的 TCP 連接埠號碼。</li><li>• 類型：int</li><li>• 預設：21</li><li>• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入</li></ul> <p><b>blockedPort3</b> (選用)</p> <ul style="list-style-type: none"><li>• 已封鎖的 TCP 連接埠號碼。</li><li>• 類型：int</li><li>• 預設：3389</li><li>• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入</li></ul> <p><b>blockedPort4</b> (選用)</p> <ul style="list-style-type: none"><li>• 已封鎖的 TCP 連接埠號碼。</li><li>• 類型：int</li><li>• 預設：3306</li><li>• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入</li></ul> <p><b>blockedPort5</b> (選用)</p> <ul style="list-style-type: none"><li>• 已封鎖的 TCP 連接埠號碼。</li><li>• 類型：int</li><li>• 預設：4333</li></ul>

必要的 AWS Config 規則	必要參數
	<ul style="list-style-type: none"> <li>• 合規要求：確保沒有安全群組允許在封鎖的連接埠上進行傳入</li> </ul>
<a href="#"><u>ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</u></a>	不適用
<a href="#"><u>ROOT_ACCOUNT_MFA_ENABLED</u></a>	不適用
<a href="#"><u>S3_BUCKET_LOGGING_ENABLED</u></a>	<p><b>targetBucket</b> (選用)</p> <ul style="list-style-type: none"> <li>• 儲存伺服器存取日誌的目標 S3 儲存貯體。</li> <li>• 類型：字串</li> <li>• 合規要求：啟用日誌</li> </ul> <p><b>targetPrefix</b> (選用)</p> <ul style="list-style-type: none"> <li>• 儲存伺服器存取日誌的 S3 儲存貯體的字首。</li> <li>• 類型：字串</li> <li>• 合規要求：識別用於 CloudTrail 記錄的 S3 儲存貯體</li> </ul>
<a href="#"><u>S3_BUCKET_PUBLIC_READ_PROHIBITED</u></a>	不適用
<a href="#"><u>VPC_DEFAULT_SECURITY_GROUP_CLOSED</u></a>	不適用
<a href="#"><u>VPC_FLOW_LOGS_ENABLED</u></a>	<p><b>trafficType</b> (選用)</p> <ul style="list-style-type: none"> <li>• 流程日誌的 trafficType 。</li> <li>• 類型：字串</li> <li>• 合規要求：已啟用流程日誌</li> </ul>

## 後續步驟

如需使用這些架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂這些架構以支援您的特定需求的指示，請參閱[在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [獨聯體 AWS 基金會基準 v1.2.0](#)
- [CIS AWS Foundations Benchmark AWS 安全部落格貼文](#)

## 獨聯體 AWS 基準 V1.3.0

AWS Audit Manager 提供了兩個支持 CIS AWS 基準測試 v1.3 的預構建標準框架。

### Note

- 如需支援 v1.2.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準 V1.2.0](#)。
- 如需支援 v1.4.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準測試 v1.4.0](#)。

## 主題

- [什麼是 AWS 獨聯體基準？](#)
- [使用這些架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 AWS 獨聯體基準？

獨聯體公司開發了[獨聯體 AWS 基準測試 v1.3.0](#)，這是一套安全配置的最佳實踐。AWS 這些業界公認的最佳做法超越了現有的高階安全性指引，因為它們為 AWS 使用者提供了清晰、step-by-step 實作和評估程序。

如需詳細資訊，請參閱 AWS 安全部落格上的 CIS AWS 基準基準部落格[文章](#)。

CIS AWS Benchmark v1.3.0 提供了為子集配置安全選項的 AWS 服務指導，並著重於基礎，可測試和架構不可知的設置。本文件部分特定 Amazon Web Services 範圍包含以下項目：

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (預設)

## CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準套用的設定可保護貴組織使用的系統。CIS 控制項是基本最佳實務指南，供組織遵循以協助防範已知的網路攻擊媒介。

### 範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

示例：獨聯體 AWS 基準測試 v1.3.0-確保為「根用戶」帳戶啟用了 MFA

此建議提供有關如何檢查此問題以及如何在 AWS 環境的 root 帳戶上設定此項目的規範性指引。

- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。

範例：CIS v7.1-針對所有系統管理存取使用多因素驗證

此控制項會說明組織內預期套用的項目，但不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

## 使用這些架構

您可以在中使用 CIS AWS 基準 v1.3 框架 AWS Audit Manager 來幫助您為 CIS 審核做準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜

尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.3.0 , 第一級	36	1	5
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.3.0 , 第一級和第二級	54	1	5

#### Tip

若要檢閱用來做為這些標準架構之資料來源對映的 AWS Config 規則清單，請下載下列檔案：

1. [AuditManager\\_ ConfigDataSourceMappings \\_ 思維系統-AWS-基準標記-V1.3.0,-Level-1.zip](#)
2. [AuditManager\\_ ConfigDataSourceMappings \\_ 思維系統-AWS-基準標記-V1.3.0,-Level-1-and-2.zip](#)

這些架構中的控制項並非用於驗證您的系統是否符合 CIS AWS Benchmark 最佳實務。此外，他們不能保證您會通過獨聯體審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到這些架構。

## 後續步驟

如需使用這些架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂這些架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [CIS AWS Foundations BenchmarkAWS 安全部落格貼文](#)



# 獨聯體 AWS 基準測試 v1.4.0

AWS Audit Manager 提供兩個預先構建的標準框架，支持互聯網安全中心 ( CIS ) AWS 基準測試 v1.4.0。

## Note

- 如需支援 v1.2.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準 V1.2.0](#)。
- 如需支援 v1.3.0 之 Audit Manager 架構的相關資訊，請參閱 [獨聯體 AWS 基準 V1.3.0](#)。

## 主題

- [什麼是獨聯體 AWS 基準？](#)
- [使用此架構支援您進行稽核準備](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是獨聯體 AWS 基準？

CIS AWS 基準測試 v1.4.0 針對 Amazon Web Services 子集設定安全選項提供規範指導。其將基礎、可測試和體系結構不可知的設定做為重點。本文件部分特定 Amazon Web Services 範圍包含以下項目：

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

## CIS 基準和 CIS 控制項之間的區別

CIS 基準是針對供應商產品的安全性最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護正在使用的系統。CIS 控制項是基本最佳實務指南，供組織遵循以協助防範已知的網路攻擊媒介。

### 範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

示例：獨聯體 AWS 基準測試 v1.3.0-確保為「根用戶」帳戶啟用了 MFA

此建議提供有關如何檢查此問題以及如何在 AWS 環境的 root 帳戶上設定此項目的規範性指引。

- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。

範例：CIS v7.1-針對所有系統管理存取使用多因素驗證

此控制項描述預期要在組織內套用的項目。然而，它不會說明您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

## 使用此架構支援您進行稽核準備

您可以在中使用 CIS AWS 基準測試 v1.4.0 架構 AWS Audit Manager 來協助您為 CIS 稽核做好準備。您也可以根據特定需求自訂這些架構和他們的控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.4.0，第一級	37	1	5

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準測試 v1.4.0 , 第一級和第二級	57	1	5

### Tip

若要檢閱用來做為這些標準架構之資料來源對映的 AWS Config 規則清單，請下載下列檔案：

1. [AuditManager\\_ConfigDataSourceMappings\\_ 思維系統-AWS-基準標記-V1.4.0,-Level-1.zip](#)
2. [AuditManager\\_ConfigDataSourceMappings\\_ 思維系統-AWS-基準標記-V1.4.0,-Level-1-and-2.zip](#)

這些架構中的控制項並不是用來驗證您的系統是否符合 CIS AWS 基準測試 v1.4.0。此外，他們不能保證您會通過獨聯體審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到這些架構。

## 後續步驟

如需使用這些架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂這些架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- Center for Internet Security 的 [CIS 基準](#)
- [CIS AWS Foundations BenchmarkAWS 安全部落格貼文](#)

## 独联体控制 7.1 版

AWS Audit Manager 提供了一個預先構建的標準框架，支持互聯網安全中心 ( CIS ) v7.1 實施組 1。

**Note**

如需有關 CIS V8 iG1 以及支援此標準的 AWS Audit Manager 架構的資訊，請參閱。[獨聯體關鍵安全控制系統 8.0 版](#)

**主題**

- [什麼是 CIS 控制項？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 CIS 控制項？

CIS 控制是一組優先順序的動作，共同形成了一 defense-in-depth 組最佳實踐。這些最佳實務行動可紓解針對系統和網路的最普遍的網路攻擊。Implementation Group 1 通常是針對資源與網路安全專業知識有限的組織所設計，其在子控制項的實施部分需要進一步協助。

### CIS 控制項和 CIS 基準之間的區別

CIS 控制項是基本最佳實務指南，組織可遵循這些指南防範已知的網路攻擊媒介。CIS 基準是針對供應商產品的安全最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護使用的系統。

### 範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。
  - 示例：獨聯體 AWS 基準測試 v1.2.0-確保為「根用戶」帳戶啟用了 MFA
  - 此建議提供有關如何檢查此問題以及如何在 AWS 環境的 root 帳戶上設定此項目的規範性指引。
- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。
  - 範例：CIS v7.1-針對所有系統管理存取使用多因素驗證
  - 此控制項描述預期要在組織內套用的項目。它不會告知您應該如何將其應用於正在執行的系統和工作負載中 (無論它們位於何處)。

## 使用此架構

您可以使用 CIS 控制項 v7.1 IG1 架構來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CIS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 CIS Controls v7.1 IG1 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

CIS 控制項 v7.1 IG1 架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
互聯網安全中心 (獨聯體) 7.1 版, IG1	31	12	18

### Tip

若要檢閱在此標準架構中用作資料來源對映的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_CIS- V7.1-IG1.zip](#) 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 控制項所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [CIS 控制項 v7.1 IG1](#)

## 獨聯體關鍵安全控制系統 8.0 版

AWS Audit Manager 提供預先建置的標準架構，支援 CIS 重要安全性控制 8.0 版實作群組 1。

### Note

如需 CIS 7.1、IG1 以及支援此標準之 AWS Audit Manager 架構的相關資訊，請參閱。[独联体控制 7.1 版](#)

### 主題

- [什麼是 CIS 控制項？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 CIS 控制項？

CIS 關鍵安全控制 (CIS Controls) 是一套優先級的保護措施，可紓解針對系統和網路的最普遍的網路攻擊。它們被映射並引用到多款法律、監管和政策架構中。CIS 控制項 v8 已進行增強，以跟上現代系統和軟體的步伐。轉向雲端運算、虛擬化、行動化 work-from-home、外包以及改變攻擊者策略，促使更新發生。此項更新支援企業移至完全雲端和混合式環境時的安全性。

### CIS 控制項和 CIS 基準之間的區別

CIS 控制項是基本最佳實務指南，組織可遵循這些指南防範已知的網路攻擊媒介。CIS 基準是針對供應商產品的安全最佳實務指南。從操作系統到雲端服務和網路裝置，基準測試套用的設定可保護使用的系統。

### 範例

- CIS 基準是一系列的方案。它們通常會參考可在廠商產品中檢閱和配置的特定設定。

- 示例：獨聯體 AWS 基準測試 v1.2.0-確保為「根用戶」帳戶啟用了 MFA
- 此建議提供有關如何檢查此問題以及如何在 AWS 環境的 root 帳戶上設定此項目的規範性指引。
- CIS 控制項適用於您的組織整體，而不是只針對單一供應商產品。
  - 範例：CIS v7.1-針對所有系統管理存取使用多因素驗證
  - 此控制項描述預期要在組織內套用的項目。它不會告知您應該如何將其應用於正在執行的系統和工作負載中（無論它們位於何處）。

## 使用此架構

您可以使用 CIS v8 IG1 框架來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CIS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它根據 CIS v8 框架中定義的控件執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
獨聯體關鍵安全控制系統 8.0 版 (獨聯體 8.0 版)	38	18	15

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_CIS- v8.0-IG1.zip](#) 檔案。

此架構中的控制項，並非為了驗證您的系統是否符合 CIS 控制項所設計。此外，他們無法保證您會透過 CIS 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [CIS 控制項 v8](#)

## 安全性 FedRAMP 準控制項 r4

AWS Audit Manager 提供預先建置的標準架構，支援聯邦風險與授權管理計畫 (FedRAMP) 安全基準控制項 r4。

### 主題

- [什麼是 FedRAMP ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 FedRAMP ?

聯邦 FedRAMP 成立於 2011 年。其為美國聯邦政府施行和使用雲端服務，提供符合成本效益、以風險評估為基礎的方法。FedRAMP 讓聯邦機構能夠使用現代雲端技術，並著重於聯邦資訊的安全性和保護性。

如需 FedRAMP 仲裁基準控制項的詳細資訊，請參閱 [FedRAMP 基礎安全性測試案例程序範本](#)。

## 使用此架構

您可以使用 FedRAMP r4 架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 FedRAMP r4 需求分組到控制集中。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。



使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

FedRAMP 基礎架構的詳細資料如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
聯邦風險與授權管理計畫 (FedRAMP) 安全基準控制項 r4, 中等	234	91	17

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_FedRAMP-Security-Baseline-Controls-r4-Moderate.zip](#) 檔案。

這個架構中的控制項並不是用來驗證您的系統是否符合 FedRAMP r4。此外，他們無法保證您會透過 FedRAMP 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [AWS FedRAMP 的規範遵循頁面](#)
- [AWS FedRAMP 部落格文章](#)

# GDPR

AWS Audit Manager 提供預先建置的標準架構，以支援 2016 年《一般資料保護規則》(GDPR)。

此架構僅包含手動控制項。這些手動控制不會自動收集證據。不過，如果您想要自動收集 GDPR 下的某些控制項的證據，您可以使用 Audit Manager 中的自訂控制功能。如需詳細資訊，請參閱 [使用此架構](#)。

## 主題

- [什麼是 GDPR ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 GDPR ?

GDPR 是歐洲隱私權法，於 2018 年 5 月 25 日成為強制執行。GDPR 取代了歐盟資料保護指令，也稱為 [95/46/EC 指令](#)。它旨在協調整個歐盟 (EU) 的資料保護法律。其透過實施在整個歐盟成員國具有約束力的單一資料保護法，以實現這項目標。

GDPR 適用於在歐盟設立的所有組織，以及處理歐盟資料當事人提供商品或服務，或歐盟境內行為相關的歐盟資料主體個人資料的組織 (無論它們是否在歐盟建立)。個人資料是任何與已識別或可識別的自然人有關的任何資訊。

您可以在 Audit Manager 的框架庫頁面中找到 GDPR 框架。如需詳細資訊，請參閱 [一般資料保護規則 \(GDPR\) 中心](#)。

## 使用此架構

您可以使用 Audit Manager 中的 GDPR 2016 框架來幫助您為審計做好準備。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
2016 年一般資料保護條例	0	378	10

您可以在 [Audit Manager] 的 [標準架構] 索引標籤下找到 GDPR 2016 架構。 [使用框架庫來管理框架](#)  
[AWS Audit Manager](#) 此標準架構僅包含手動控制項。

### Note

如果您想要自動化 GDPR 的證據收集作業，可以使用 Audit Manager 來為 GDPR [建立自己的自訂控制項](#)。下表提供有關可在自訂控制項中對應至 GDPR 要求的 AWS 資料來源的建議。雖然下列某些資料來源已對應至多個控制項，但請記住，每次資源評估只需支付一次費用。下列建議使用 AWS Config 和 AWS Security Hub 做為資料來源。若要成功從這些資料來源收集證據，請確定您已按照指示[啟用 AWS Config 和 AWS Security Hub 設定](#) AWS 帳戶。以這種方式設定這兩項服務之後，每次針對指定 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 都會收集證據。

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條 設計與預 設的資料 保護 1	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> <li>AWS CloudTrail 桶不公開</li> <li>顯示具備 Allow:*:* 的所有政策，並列出所有使用這些政策的主體和服務</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">IAM_ROOT_ACCESS_KEY_CHECK</a></li> <li><a href="#">ROOT_ACCOUNT_MFA_ENABLED</a></li> <li><a href="#">ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">ACCESS_KEYS_ROTATED</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• <a href="#">IAM_PASSWORD_POLICY</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li>• <a href="#">CloudWatch1</a></li> <li>• 1.1 (<a href="#">IAM.20</a>)</li> <li>• 1.10 (<a href="#">IAM.16</a>)</li> <li>• 1.11 (<a href="#">IAM.17</a>)</li> <li>• 1.12 (<a href="#">IAM.4</a>)</li> <li>• 1.13 (<a href="#">IAM.9</a>)</li> <li>• 1.14 (<a href="#">IAM.6</a>)</li> <li>• 1.16 (<a href="#">IAM.2</a>)</li> <li>• 1.2 (<a href="#">IAM.5</a>)</li> <li>• 1.20 (<a href="#">IAM.18</a>)</li> <li>• 1.22 (<a href="#">IAM.1</a>)</li> <li>• 1.3 (<a href="#">IAM.8</a>)</li> <li>• 1.4 (<a href="#">IAM.3</a>)</li> <li>• 1.5 (<a href="#">IAM.11</a>)</li> <li>• 1.6 (<a href="#">IAM.12</a>)</li> <li>• 1.7 (<a href="#">IAM.13</a>)</li> <li>• 1.8 (<a href="#">IAM.14</a>)</li> <li>• 1.9 (<a href="#">IAM.15</a>)</li> <li>• <a href="#">CloudTrail1</a></li> <li>• 2.2 (<a href="#">CloudTrail.4</a>)</li> <li>• 2.3 (<a href="#">CloudTrail.6</a>)</li> <li>• 2.4 (<a href="#">CloudTrail.5</a>)</li> <li>• 2.5 (<a href="#">Config.1</a>)</li> <li>• 2.6 (<a href="#">CloudTrail.7</a>)</li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"><li>• <a href="#">CloudTrail2</a></li><li>• 2.8 (<a href="#">KMS.4</a>)</li><li>• 2.9 (<a href="#">EC2.6</a>)</li><li>• <a href="#">CloudWatch</a></li><li>• 3.10 (<a href="#">CloudWatch. 10</a>)</li><li>• 3.11 (<a href="#">CloudWatch. 11</a>)</li><li>• 3.12 (<a href="#">CloudWatch. 12</a>)</li><li>• 3.13 (<a href="#">CloudWatch. 13</a>)</li><li>• 3.14 (<a href="#">CloudWatch. 14</a>)</li><li>• <a href="#">Config.1</a></li></ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條 設計與預 設的資料 保護 2	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> <li>AWS CloudTrail 桶不公開</li> <li>顯示具備 Allow:*:* 的所有政策，並列出所有使用這些政策的主體和服務</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">IAM_ROOT_ACCESS_KEY_CHECK</a></li> <li><a href="#">ROOT_ACCOUNT_MFA_ENABLED</a></li> <li><a href="#">ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">ACCESS_KEYS_ROTATED</a></li> <li><a href="#">IAM_PASSWORD_POLICY</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">CloudWatch1</a></li> <li>1.1 (<a href="#">IAM.20</a>)</li> <li>1.10 (<a href="#">IAM.16</a>)</li> <li>1.11 (<a href="#">IAM.17</a>)</li> <li>1.12 (<a href="#">IAM.4</a>)</li> <li>1.13 (<a href="#">IAM.9</a>)</li> <li>1.14 (<a href="#">IAM.6</a>)</li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• 1.16 (<a href="#">IAM.2</a>)</li> <li>• 1.2 (<a href="#">IAM.5</a>)</li> <li>• 1.20 (<a href="#">IAM.18</a>)</li> <li>• 1.22 (<a href="#">IAM.1</a>)</li> <li>• 1.3 (<a href="#">IAM.8</a>)</li> <li>• 1.4 (<a href="#">IAM.3</a>)</li> <li>• 1.5 (<a href="#">IAM.11</a>)</li> <li>• 1.6 (<a href="#">IAM.12</a>)</li> <li>• 1.7 (<a href="#">IAM.13</a>)</li> <li>• 1.8 (<a href="#">IAM.14</a>)</li> <li>• 1.9 (<a href="#">IAM.15</a>)</li> <li>• <a href="#">CloudTrail1</a></li> <li>• 2.2 (<a href="#">CloudTrail.4</a>)</li> <li>• 2.3 (<a href="#">CloudTrail.6</a>)</li> <li>• 2.4 (<a href="#">CloudTrail.5</a>)</li> <li>• 2.5 (<a href="#">Config.1</a>)</li> <li>• 2.6 (<a href="#">CloudTrail.7</a>)</li> <li>• <a href="#">CloudTrail2</a></li> <li>• 2.8 (<a href="#">KMS.4</a>)</li> <li>• 2.9 (<a href="#">EC2.6</a>)</li> <li>• <a href="#">CloudWatch</a></li> <li>• 3.10 (<a href="#">CloudWatch. 10</a>)</li> <li>• 3.11 (<a href="#">CloudWatch. 11</a>)</li> <li>• 3.12 (<a href="#">CloudWatch. 12</a>)</li> <li>• 3.13 (<a href="#">CloudWatch. 13</a>)</li> <li>• 3.14 (<a href="#">CloudWatch. 14</a>)</li> <li>• <a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 25 條 設計與預 設的資料 保護 3	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> <li>AWS CloudTrail 桶不公開</li> <li>顯示具備 Allow:*:* 的所有政策，並列出所有使用這些政策的主體和服務</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">IAM_ROOT_ACCESS_KEY_CHECK</a></li> <li><a href="#">ROOT_ACCOUNT_MFA_ENABLED</a></li> <li><a href="#">ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">ACCESS_KEYS_ROTATED</a></li> <li><a href="#">IAM_PASSWORD_POLICY</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">CloudWatch1</a></li> <li>1.1 (<a href="#">IAM.20</a>)</li> <li>1.10 (<a href="#">IAM.16</a>)</li> <li>1.11 (<a href="#">IAM.17</a>)</li> <li>1.12 (<a href="#">IAM.4</a>)</li> <li>1.13 (<a href="#">IAM.9</a>)</li> <li>1.14 (<a href="#">IAM.6</a>)</li> </ul>



控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• 1.16 (<a href="#">IAM.2</a>)</li> <li>• 1.2 (<a href="#">IAM.5</a>)</li> <li>• 1.20 (<a href="#">IAM.18</a>)</li> <li>• 1.22 (<a href="#">IAM.1</a>)</li> <li>• 1.3 (<a href="#">IAM.8</a>)</li> <li>• 1.4 (<a href="#">IAM.3</a>)</li> <li>• 1.5 (<a href="#">IAM.11</a>)</li> <li>• 1.6 (<a href="#">IAM.12</a>)</li> <li>• 1.7 (<a href="#">IAM.13</a>)</li> <li>• 1.8 (<a href="#">IAM.14</a>)</li> <li>• 1.9 (<a href="#">IAM.15</a>)</li> <li>• <a href="#">CloudTrail1</a></li> <li>• 2.2 (<a href="#">CloudTrail.4</a>)</li> <li>• 2.3 (<a href="#">CloudTrail.6</a>)</li> <li>• 2.4 (<a href="#">CloudTrail.5</a>)</li> <li>• 2.5 (<a href="#">Config.1</a>)</li> <li>• 2.6 (<a href="#">CloudTrail.7</a>)</li> <li>• <a href="#">CloudTrail2</a></li> <li>• 2.8 (<a href="#">KMS.4</a>)</li> <li>• 2.9 (<a href="#">EC2.6</a>)</li> <li>• <a href="#">CloudWatch</a></li> <li>• 3.10 (<a href="#">CloudWatch. 10</a>)</li> <li>• 3.11 (<a href="#">CloudWatch. 11</a>)</li> <li>• 3.12 (<a href="#">CloudWatch. 12</a>)</li> <li>• 3.13 (<a href="#">CloudWatch. 13</a>)</li> <li>• 3.14 (<a href="#">CloudWatch. 14</a>)</li>   <li>• <a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條 處理活動 之紀錄 1	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_ENABLED</a></li> <li><a href="#">ELB_LOGGING_ENABLED</a></li> <li><a href="#">CLOUDTRAIL_SECURITY_TRAIL_ENABLED</a></li> <li><a href="#">REDSHIFT_CLUSTER_CONFIGURATION_CHECK</a></li> <li><a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條 處理活動 之紀錄 2	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_ENABLED</a></li> <li><a href="#">ELB_LOGGING_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條 處理活動 之紀錄 3	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> <li>AWS CloudTrail 桶不公開</li> <li>顯示具備 Allow:*:* 的所有政策，並列出所有使用這些政策的主體和服務</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_ENABLED</a></li> <li><a href="#">ELB_LOGGING_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條 處理活動 之紀錄 4	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> <li>AWS CloudTrail 桶不公開</li> <li>顯示具備 Allow:*:* 的所有政策，並列出所有使用這些政策的主體和服務</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_ENABLED</a></li> <li><a href="#">ELB_LOGGING_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 30 條 處理活動 之紀錄 5	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>顯示期間內的所有根帳號事件</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li><a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li><a href="#">VPC_FLOW_LOGS_ENABLED</a></li> <li><a href="#">CMK_BACKING_KEY_ROTATION_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_ENABLED</a></li> <li><a href="#">ELB_LOGGING_ENABLED</a></li> <li><a href="#">CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</a></li> </ul> <p>選擇 AWS Security Hub 作為資料來源類型，然後選取下列 Security Hub 控制項作為資料來源對應：</p> <ul style="list-style-type: none"> <li><a href="#">Config.1</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條 處理之安 全性 1	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>• 顯示所有服務的靜態資料加密</li> <li>• 顯示所有服務的傳輸中的資料加密</li> <li>• 已為 Amazon S3 啟用 MFA 刪除功能</li> <li>• 所有 Amazon Inspector 掃描</li> <li>• 顯示未啟用 Amazon Inspector 的所有執行個體</li> <li>• 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器</li> <li>• AWS CloudTrail 靜態加密</li> <li>• Amazon CloudWatch 警報 AWS Config 顯示所有更改和所有註釋設置</li> <li>• 所有根活動</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li>• <a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li>• <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a></li> <li>• <a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li>• <a href="#">CLOUDWATCH_LOG_GROUP_ENCRYPTED</a></li> <li>• <a href="#">EFS_ENCRYPTED_CHECK</a></li> <li>• <a href="#">ELASTICSEARCH_ENCRYPTED_AT_REST</a></li> <li>• <a href="#">ENCRYPTED_VOLUMES</a></li> <li>• <a href="#">RDS_STORAGE_ENCRYPTED</a></li> <li>• <a href="#">REDSHIFT_CLUSTER_CONFIGURATION_CHECK</a></li> <li>• <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• <a href="#"><u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SNS_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_SNAPSHOT_ENCRYPTED</u></a></li> <li>• <a href="#"><u>S3_DEFAULT_ENCRYPTION_KMS</u></a></li> <li>• <a href="#"><u>DAX_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>EKS_SECRETS_ENCRYPTED</u></a></li> <li>• <a href="#"><u>RDS_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>REDSHIFT_BACKUP_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_IN_BACKUP_PLAN</u></a></li> <li>• <a href="#"><u>WAF_CLASSIC_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>WAFV2_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_ACM_CERTIFICATE_REQUIRED</u></a></li> <li>• <a href="#"><u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u></a></li> <li>• <a href="#"><u>REDSHIFT_REQUIRE_TLS_SSL</u></a></li> <li>• <a href="#"><u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u></a></li> <li>• <a href="#"><u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u></a></li> <li>• <a href="#"><u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_TLS_HTTPS_LISTENERS_ONLY</u></a></li> <li>• <a href="#"><u>ACM_CERTIFICATE_EXPIRATION_CHECK</u></a></li> <li>• <a href="#"><u>API_GW_CACHE_ENABLED_AND_ENCRYPTED</u></a></li> </ul>



控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條 處理之安 全性 2	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>• 顯示所有服務的靜態資料加密</li> <li>• 顯示所有服務的傳輸中的資料加密</li> <li>• 已為 Amazon S3 啟用 MFA 刪除功能</li> <li>• 所有 Amazon Inspector 掃描</li> <li>• 顯示未啟用 Amazon Inspector 的所有執行個體</li> <li>• 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器</li> <li>• AWS CloudTrail 靜態加密</li> <li>• Amazon CloudWatch 警報 AWS Config 顯示所有更改和所有註釋設置</li> <li>• 所有根活動</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li>• <a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li>• <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a></li> <li>• <a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li>• <a href="#">CLOUDWATCH_LOG_GROUP_ENCRYPTED</a></li> <li>• <a href="#">EFS_ENCRYPTED_CHECK</a></li> <li>• <a href="#">ELASTICSEARCH_ENCRYPTED_AT_REST</a></li> <li>• <a href="#">ENCRYPTED_VOLUMES</a></li> <li>• <a href="#">RDS_STORAGE_ENCRYPTED</a></li> <li>• <a href="#">REDSHIFT_CLUSTER_CONFIGURATION_CHECK</a></li> <li>• <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• <a href="#"><u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SNS_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_SNAPSHOT_ENCRYPTED</u></a></li> <li>• <a href="#"><u>S3_DEFAULT_ENCRYPTION_KMS</u></a></li> <li>• <a href="#"><u>DAX_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>EKS_SECRETS_ENCRYPTED</u></a></li> <li>• <a href="#"><u>RDS_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>REDSHIFT_BACKUP_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_IN_BACKUP_PLAN</u></a></li> <li>• <a href="#"><u>WAF_CLASSIC_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>WAFV2_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_ACM_CERTIFICATE_REQUIRED</u></a></li> <li>• <a href="#"><u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u></a></li> <li>• <a href="#"><u>REDSHIFT_REQUIRE_TLS_SSL</u></a></li> <li>• <a href="#"><u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u></a></li> <li>• <a href="#"><u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u></a></li> <li>• <a href="#"><u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_TLS_HTTPS_LISTENERS_ONLY</u></a></li> <li>• <a href="#"><u>ACM_CERTIFICATE_EXPIRATION_CHECK</u></a></li> <li>• <a href="#"><u>API_GW_CACHE_ENABLED_AND_ENCRYPTED</u></a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條 處理之安 全性 3	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>• 顯示所有服務的靜態資料加密</li> <li>• 顯示所有服務的傳輸中的資料加密</li> <li>• 已為 Amazon S3 啟用 MFA 刪除功能</li> <li>• 所有 Amazon Inspector 掃描</li> <li>• 顯示未啟用 Amazon Inspector 的所有執行個體</li> <li>• 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器</li> <li>• AWS CloudTrail 靜態加密</li> <li>• Amazon CloudWatch 警報 AWS Config 顯示所有更改和所有註釋設置</li> <li>• 所有根活動</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li>• <a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li>• <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a></li> <li>• <a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li>• <a href="#">CLOUDWATCH_LOG_GROUP_ENCRYPTED</a></li> <li>• <a href="#">EFS_ENCRYPTED_CHECK</a></li> <li>• <a href="#">ELASTICSEARCH_ENCRYPTED_AT_REST</a></li> <li>• <a href="#">ENCRYPTED_VOLUMES</a></li> <li>• <a href="#">RDS_STORAGE_ENCRYPTED</a></li> <li>• <a href="#">REDSHIFT_CLUSTER_CONFIGURATION_CHECK</a></li> <li>• <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• <a href="#"><u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SNS_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_SNAPSHOT_ENCRYPTED</u></a></li> <li>• <a href="#"><u>S3_DEFAULT_ENCRYPTION_KMS</u></a></li> <li>• <a href="#"><u>DAX_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>EKS_SECRETS_ENCRYPTED</u></a></li> <li>• <a href="#"><u>RDS_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>REDSHIFT_BACKUP_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_IN_BACKUP_PLAN</u></a></li> <li>• <a href="#"><u>WAF_CLASSIC_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>WAFV2_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_ACM_CERTIFICATE_REQUIRED</u></a></li> <li>• <a href="#"><u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u></a></li> <li>• <a href="#"><u>REDSHIFT_REQUIRE_TLS_SSL</u></a></li> <li>• <a href="#"><u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u></a></li> <li>• <a href="#"><u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u></a></li> <li>• <a href="#"><u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_TLS_HTTPS_LISTENERS_ONLY</u></a></li> <li>• <a href="#"><u>ACM_CERTIFICATE_EXPIRATION_CHECK</u></a></li> <li>• <a href="#"><u>API_GW_CACHE_ENABLED_AND_ENCRYPTED</u></a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
第 32 條 處理之安 全性 4	第 4 章 - 控制方 與處理 方	<p>您可以在中<a href="#">建立支援此 GDPR 控制項</a> AWS Audit Manager 的自訂控制項。</p> <p>當您<a href="#">指定控制項詳細資訊</a>時，請在測試資訊下輸入下列內容：</p> <ul style="list-style-type: none"> <li>• 顯示所有服務的靜態資料加密</li> <li>• 顯示所有服務的傳輸中的資料加密</li> <li>• 已為 Amazon S3 啟用 MFA 刪除功能</li> <li>• 所有 Amazon Inspector 掃描</li> <li>• 顯示未啟用 Amazon Inspector 的所有執行個體</li> <li>• 顯示正在使用 HTTPS (SSL) 接聽的所有負載平衡器</li> <li>• AWS CloudTrail 靜態加密</li> <li>• Amazon CloudWatch 警報 AWS Config 顯示所有更改和所有註釋設置</li> <li>• 所有根活動</li> </ul> <p><a href="#">設定控制項資料來源</a>時，建議您將下列所有項目納入資料來源：</p> <p>選擇 AWS Config 作為資料來源類型，然後選取下列 AWS Config 管理規則作為資料來源對映：</p> <ul style="list-style-type: none"> <li>• <a href="#">CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</a></li> <li>• <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a></li> <li>• <a href="#">CLOUD_TRAIL_ENCRYPTION_ENABLED</a></li> <li>• <a href="#">CLOUDWATCH_LOG_GROUP_ENCRYPTED</a></li> <li>• <a href="#">EFS_ENCRYPTED_CHECK</a></li> <li>• <a href="#">ELASTICSEARCH_ENCRYPTED_AT_REST</a></li> <li>• <a href="#">ENCRYPTED_VOLUMES</a></li> <li>• <a href="#">RDS_STORAGE_ENCRYPTED</a></li> <li>• <a href="#">REDSHIFT_CLUSTER_CONFIGURATION_CHECK</a></li> <li>• <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a></li> </ul>

控制項名稱	控制集	建議控制項資料來源映射項目
		<ul style="list-style-type: none"> <li>• <a href="#"><u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u></a></li> <li>• <a href="#"><u>SNS_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTED_KMS</u></a></li> <li>• <a href="#"><u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_SNAPSHOT_ENCRYPTED</u></a></li> <li>• <a href="#"><u>S3_DEFAULT_ENCRYPTION_KMS</u></a></li> <li>• <a href="#"><u>DAX_ENCRYPTION_ENABLED</u></a></li> <li>• <a href="#"><u>EKS_SECRETS_ENCRYPTED</u></a></li> <li>• <a href="#"><u>RDS_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>REDSHIFT_BACKUP_ENABLED</u></a></li> <li>• <a href="#"><u>RDS_IN_BACKUP_PLAN</u></a></li> <li>• <a href="#"><u>WAF_CLASSIC_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>WAFV2_LOGGING_ENABLED</u></a></li> <li>• <a href="#"><u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_ACM_CERTIFICATE_REQUIRED</u></a></li> <li>• <a href="#"><u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u></a></li> <li>• <a href="#"><u>REDSHIFT_REQUIRE_TLS_SSL</u></a></li> <li>• <a href="#"><u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u></a></li> <li>• <a href="#"><u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u></a></li> <li>• <a href="#"><u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u></a></li> <li>• <a href="#"><u>ELB_TLS_HTTPS_LISTENERS_ONLY</u></a></li> <li>• <a href="#"><u>ACM_CERTIFICATE_EXPIRATION_CHECK</u></a></li> <li>• <a href="#"><u>API_GW_CACHE_ENABLED_AND_ENCRYPTED</u></a></li> </ul>

建立新的自訂控制項之後，您可以將其新增至自訂 GDPR 架構。您可以從自訂 GDPR 架構建立評估。如此一來，Audit Manager 就可以自動收集您新增的自訂控制項的證據。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [一般資料保護規範 \(GDPR\) 中心](#)
- [AWS GDPR 部落格文章](#)

## 金融服務業現代化法 (GLBA)

AWS Audit Manager 提供支持格拉姆-里奇-比利利法案 ( GLBA ) 的預構建框架。

### 主題

- [什麼是綠色環球菌 \(GLBA\) ?](#)
- [使用此架構](#)
- [後續步驟](#)

## 什麼是綠色環球菌 (GLBA) ?

GLBA ( 或 GLB 法案 ) ，也稱為 1999 年的金融服務現代化法案，是美國制定的聯邦法律，旨在控制金融機構處理個人私人信息的方式。這個動作是由三個區段組成。首先是財務隱私規則，其規定了私人財務資訊的收集與揭露。第二個是保障規則，其規定金融機構必須實施安全計劃以保護此類資訊。第三個是禁止預編，即禁止進行預編的行動 ( 利用假訪問取得私人資訊 ) 。該法案還要求金融機構向客戶提供書面的隱私通知，以解釋他們的資訊共享做法。

## 使用此架構

您可以使用 GLBA 2016 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 GLBA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用 GLBA 架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 GLBA 稽核相關的證據。在評估中，您可以指 AWS 帳戶 定要包含在稽核範圍中的項目。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 GLBA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
金融服務業現代化法 (GLBA)	0	120	16

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 GLBA 標準。此外，他們不能保證您會通過 GLBA 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到 GLBA 架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 標題 21 CFR 第 11 部分

AWS Audit Manager 提供預先構建的標準框架，支持聯邦法規 (CFR) 第 11 部分第 21 部，電子記錄；電子簽名-範圍和應用程序 2023 年 5 月 24 日。

### 主題

- [甚麼是 CFR 第 11 部分的標題 21？](#)
- [使用此架構](#)
- [後續步驟](#)



- [其他資源](#)

## 甚麼是 CFR 第 11 部分的標題 21？

GxP 是指適用於生產食品和醫療產品的生命科學組織之法規和準則。屬於這種情況的醫療產品包括藥品、醫療設備和醫療軟體應用程式。GxP 要求的總體目的，是確保食品和醫療產品的消費者安全。這也是為了確保用於制定產品相關安全決策的資料完整性。

在美國，GxP 法規由美國食品和藥物管理局 (FDA) 執行，並包含在聯辦法規 (21 CFR) 標題 21 中。在 21 CFR 內，第 11 部分包含建立、修改、維護、封存、擷取或分發電子記錄和電子簽名以支援 GXP 規範活動的電腦系統的要求。第 11 部分的創建目的是允許 FDA 監管的生命科學組織採用新的信息技術，同時提供框架以確保電子 GxP 數據值得信賴和可靠。

如需針對 GxP 系統使用 AWS 雲端的全方位方法，請參閱在 GxP 系統中[使用 AWS 產品的注意事項](#)白皮書。

## 使用此架構

您可以使用標題 21 CFR 第 11 部分框架來幫助您準備審核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 CFR 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它根據標題 21 CFR 第 11 部分框架中定義的控件執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
標題 21 聯辦法規 (CFR) 第 11 部，電子記錄；電子簽名-適用範圍和應用 2023 年 5 月 24 日	17	8	2

**i** Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_Title-21-CFR-Part-11.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合 GxP 規範。此外，他們無法保證您會透過稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [AWS GxP 的相容性頁面](#)
- [在 GxP 系統中使用 AWS 產品的注意事項](#)

## 歐盟 GMP 附件 11, V1

AWS Audit Manager 提供一個預先建立的框架，以支持《歐盟藥品管制規則》-第 4 冊：人類和獸醫用藥品的良好生產規範 ( GMP ) -附件 11。EudraLex

### 主題

- [什麼是歐盟 GMP 附件 11？](#)
- [使用此架構](#)
- [後續步驟](#)

## 什麼是歐盟 GMP 附件 11？

歐盟 GMP 附件 11 框架是歐洲相當於美國的第 21 號 CFR 第 11 部分框架。本附件適用於所有形式的電腦化系統，其用於優良生產規範 (GMP) 受管活動的一部分。電腦化系統是一組軟體和硬體元件，合

併共同實現特定功能。應用程式應進行驗證，且 IT 基礎架構應該符合資格。當電腦化系統取代手動操作，產品品質、製程控制或品質保證不會因此而降低。該過程的整體風險不應增加。

Annex 11 是歐洲 GMP 指導方針的一部分，並定義了製藥行業組織使用的電腦化系統參考條款。Annex 11 的功能就像檢查清單，使歐洲監管機構能夠制定與藥品和醫療設備相關的電腦化系統之要求。由歐洲委員會委員會制定的準則不是從 FDA 那麼遠 (標題 21 CFR 部分 11)。Annex 11 明訂電子紀錄及電子簽章應考慮管理的條件。

## 使用此架構

您可以使用歐盟 GMP 附件 11 框架來幫助您為審計做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據歐盟 GMP 要求分為控制組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。這是基於歐盟 GMP 附件 11 框架所界定的管制措施。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
EudraLex -歐洲聯盟藥用產品 管制規則-第四冊：人類及獸醫 用藥品的良好生產規範-附件 11	15	17	3

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_EudraLex-GMP-Volume-4-Annex-11.zip](#) 檔案。

此架構中的控制並非用於驗證您的系統是否符合歐盟 GMP 附件 11 要求。此外，他們不能保證您將通過歐盟 GMP 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## HIPAA 安全性規則：2003 年 2 月

AWS Audit Manager 提供預先建立的標準架構，以支援《Health 保險流通與責任法案》(HIPAA) 安全規則：2003 年 2 月。

### Note

如需有關 HIPAA Final Omnibus 安全規則 2013 以及支援此標準的 Audit Manager 架構的資訊，請參閱 [HIPAA 全方位最終規則](#)。

### 主題

- [什麼是 HIPAA 和 HIPAA 安全規則 2003 ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 HIPAA 和 HIPAA 安全規則 2003 ?

HIPAA 是一項協助美國員工在轉換或失去工作時保留醫療保險的立法。該法案亦旨在推廣電子健康紀錄，透過改善資料互通，改善美國醫療系統的效率 and 品質。

隨著電子醫療紀錄的使用日益增加，HIPAA 還納入受保護醫療資訊 (PHI) 之安全性和隱私權保障的條款。PHI 包括一系列非常廣泛的個人身份健康和健康相關資料。這包括保險和帳單資訊、診斷資料、臨床照護資料，以及實驗室結果，例如影像和測試結果。

美國健康與公共服務部於 2003 年 2 月發布了最終版的 [安全規則](#)。為了讓受保護的電子健康資訊之機密性、完整性和可用性得到保障，因此設立此國家標準之規則。

HIPAA 規則適用於涵蓋的實體。這些包括醫院、醫療服務提供者、雇主贊助的健康計劃、研究設施以及直接處理患者和患者資料的保險公司。保護 PHI 的 HIPAA 要求也延伸到商業夥伴。

有關 HIPAA 和 HITECH 如何保護健康資訊的更多相關內容，請參閱美國衛生和公共服務部的[健康資訊隱私網頁](#)。

越來越多的醫療保健提供者、付款人和 IT 專業人員正在使用以 AWS 公用事業為基礎的雲端服務來處理、儲存和傳輸受保護的醫療資訊 (PHI)。AWS 使受 HIPAA 約束的涵蓋實體及其業務夥伴能夠使用安全 AWS 環境來處理、維護和儲存受保護的健康資訊。

如需有關如何使用 AWS 處理和儲存健康狀態資訊的指示，請參閱在[Amazon Web Services 上架構 HIPAA 安全性與合規性](#)白皮書。

## 使用此架構

您可以使用 HIPAA 安全規則 2003 來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 HIPAA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 HIPAA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱	AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
《Health 保險流通與責任法案》(HIPAA) 安全規則：2003 年 2 月		45	40	5

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_HIPAA-Security-Rule-Feb-2003.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 HIPAA 標準。此外，他們不能保證您會通過 HIPAA 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- 來自美國衛生與公共服務部的 [健康資訊隱私權](#)
- 美國衛生與公共服務部的 [安全規則](#)
- [Amazon Web Services 上的 HIPAA 安全與合規架構](#)
- [AWS HIPAA 的法規遵循頁面](#)

## HIPAA 全方位最終規則

AWS Audit Manager 提供預先建立的標準架構，支援《Health 保險可攜性與責任法案》(HIPAA) 綜合性最終規則。

### Note

如需 HIPAA 安全性規則 2003 與支援此標準之 AWS Audit Manager 架構的相關資訊，請參閱 [HIPAA 安全性規則：2003 年 2 月](#)

### 主題

- [什麼是 HIPAA 和 HIPAA Final Omnibus 安全規則？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 HIPAA 和 HIPAA Final Omnibus 安全規則？

HIPAA 是幫助美國工人在改變或失去工作時保留醫療保險的立法。該法案亦旨在推廣電子健康紀錄，透過改善資料互通，改善美國醫療系統的效率 and 品質。

隨著電子醫療紀錄的使用日益增加，HIPAA 還納入受保護醫療資訊 (PHI) 之安全性和隱私權保障的條款。PHI 包括一系列非常廣泛的個人身份健康和健康相關資料。這包括保險和帳單資訊、診斷資料、臨床照護資料，以及實驗室結果，例如影像和測試結果。

HIPAA Final Omnibus 安全規則於 2013 年生效，其對所有先前通過的規則追加了不少更新。安全性、隱私權、違規通知和強制執行規則的修改，旨在增強資料分享的機密性和安全性。

HIPAA 規則適用於涵蓋的實體。這些包括醫院、醫療服務提供者、雇主贊助的健康計劃、研究設施以及直接處理患者和患者資料的保險公司。作為綜合更新的一部分，許多適用於涵蓋實體的 HIPAA 規則，現在也適用於商業夥伴。

有關 HIPAA 和 HITECH 如何保護健康資訊的更多相關內容，請參閱美國衛生和公共服務部的[健康資訊隱私網頁](#)。

越來越多的醫療保健提供者、付款人和 IT 專業人員正在使用以 AWS 公用事業為基礎的雲端服務來處理、儲存和傳輸受保護的醫療資訊 (PHI)。AWS 使受 HIPAA 約束的涵蓋實體及其業務夥伴能夠使用安全 AWS 環境來處理、維護和儲存受保護的健康資訊。如需有關如何使用 AWS 處理和儲存健康狀態資訊的指示，請參閱在[Amazon Web Services 上架構 HIPAA 安全性與合規性](#)白皮書。

### 使用此架構

您可以使用 HIPAA 綜合性最終規則框架來幫助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 HIPAA 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 HIPAA 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
Health 保險可攜性與責任法案 (HIPAA) 綜合性最終規則	45	29	5

**i** Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_HIPAA-Omnibus-Final-Rule.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 HIPAA 標準。此外，他們不能保證您會通過 HIPAA 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- 來自美國衛生與公共服務部的 [健康資訊隱私權](#)
- 美國衛生與公共服務部的 [Omnibus HIPAA Rulemaking](#)
- [Amazon Web Services 上的 HIPAA 安全與合規架構](#)
- [AWS HIPAA 的法規遵循頁面](#)

## ISO/IEC 27001:2013 Annex A

AWS Audit Manager 提供預先建立的標準架構，支援國際標準化組織 (ISO)/國際電工委員會 (IEC) 27001:2013 附件 A。

### 主題



- [什麼是 ISO/IEC 27001:2013 Annex A ?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 ISO/IEC 27001:2013 Annex A ?

國際電工委員會 ( IEC ) 和國際標準化組織 ( ISO ) 都是獨立的非政府組 not-for-profit 織，他們制定和發布完全同意的國際標準。

ISO/IEC 27001:2013 Annex A 是一項安全管理標準，其指出遵循 ISO/IEC 27002 最佳實務指引的安全管理最佳做法，以及完整的安全控制措施。此國際標準規定了如何在組織中建立、實施、維護和持續改善資訊安全管理系統的要求。這些標準包括針對您的組織需求量身打造的資訊安全風險評估和處理要求。此國際標準中的要求是通用的，旨在適用於所有組織，無論其類型、規模或性質。

## 使用此架構

您可以使用 ISO/IEC 27001:2013 附件 A 的 AWS Audit Manager 架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 ISO/IEC 27001:2013 Annex A 要求，分為控制組。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用此架構作為起點，您可以建立 Audit Manager 評估，並開始收集與 ISO/IEC 27001:2013 Annex A 稽核相關的證據。在評估中，您可以指 AWS 帳戶 定要包含在稽核範圍中的項目。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 ISO/IEC 27001:2013 Annex A 架構中所定義的控制項來執行此操作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
國際標準化組織 (ISO)/國際電工委員會 (IEC)	61	53	35

**i** Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_ISO-IEC-270012013-Annex-A.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合此國際標準。此外，他們不能保證您將通過 ISO/IEC 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager [使用框架庫來管理框架 AWS Audit Manager](#) 的標準架構索引標籤下，找到 ISO/IEC 27001:2013 Annex A 架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- 如需有關此國際標準的詳細資訊，請參閱 ANSI 網路商店中的 [ISO/IEC 27001:2013](#)。

## 第五修訂版

AWS Audit Manager 提供預先建置的架構，支援 NIST 800-53 第 5 版：資訊系統與 Organizations 的安全性與隱私權控制。

**i** Note

- 如需支援 NIST SP 800-171 之 Audit Manager 架構的相關資訊，請參閱 [尼斯特第二版](#)
- 如需支援 NIST CSF 之 Audit Manager 架構的相關資訊，請參閱 [NIST 網路安全架構 1.1 版](#)

## 主題

- [什麼是尼斯特](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是尼斯特

[美國國家標準與技術研究所 \(NIST\)](#) 成立於 1901 年，現為美國商務部的一員。NIST 是美國最古老的物理科學實驗室之一。美國國會成立了該機構，以改善當時二流的測量基礎設施。該基礎設施是美國工業競爭力的一大挑戰，當時落後於英國和德國等其他經濟強國。

NIST SP 800-53 安全控制通常適用於美國聯邦資訊系統。這些通常必須經過正式評估和授權程序的系統。此過程確保對資訊和資訊系統的機密性、完整性和可用性有全面防護。這是根據系統的安全類別和影響層級 (低、中或高) 以及風險判定而定。當您從 NIST SP 800-53 安全控制類別中選擇安全控制時，即會根據這些安全控制要求來評估系統。

NIST SP 800-53 架構代表 NIST SP 800-53 修訂版 5 針對聯邦資訊系統與 Organizations 的建議安全控制中所定義的安全性控制項與相關評估程序。如需 NIST SP 800-53 架構與最新出版的 NIST 特別出版品 SP 800-53 修訂版 5 之間的内容中所述的任何差異，請參閱 [NIST 電腦安全資源中心](#) 所提供的官方已發佈文件。

## 使用此架構

您可以使用 NIST SP 800-53 架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 NIST SP 800-53 架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
NIST 800-53 第五版：適用於資訊系統和 Organizations 的安全性與隱私權控制	634	373	20

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_NIST-800-53-Rev-5.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合 NIST 標準。此外，他們不能保證您會通過 NIST 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [國家標準技術研究所 \(NIST\)](#)
- [NIST 電腦安全資源中心](#)
- [AWS NIST 的合規性頁面](#)

## NIST 網路安全架構 1.1 版

AWS Audit Manager 提供支援 NIST 網路安全架構 (CSF) 1.1 版的預先建置架構。

### Note

- 如需支援 NIST SP 800-53 之 Audit Manager 架構的相關資訊，請參閱。[第五修訂版](#)
- 如需支援 NIST SP 800-171 之 Audit Manager 架構的相關資訊，請參閱。[尼斯特第二版](#)

## 主題

- [什麼是 NIST 網路安全架構？](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 NIST 網路安全架構？

[美國國家標準與技術研究所 \(NIST\)](#) 成立於 1901 年，現為美國商務部的一員。NIST 是美國最古老的物理科學實驗室之一。美國國會成立了該機構，以改善當時二流的測量基礎設施。該基礎設施是美國工業競爭力的一大挑戰，落後於英國和德國等其他經濟強國。

美國依賴關鍵基礎設施的可靠運作。網路安全威脅利用關鍵基礎設施系統日益增加的複雜性和互聯性。它們將美國的安全、經濟以及公共安全和健康置於風險之中。類似於財務和聲譽風險，網路安全風險影響公司的盈利能力。它可以提高成本並影響收入。它可能損害組織的創新能力，以及獲得和維持客戶的能力。最終，網路安全可以擴大組織的整體風險管理。

NIST 網路安全架構 (CSF) 受到全球各國政府和產業的支援，作為任何組織使用的建議基準，無論產業或規模大小。NIST 網路安全架構包含三個主要元件：架構核心、設定檔和實作層。架構核心包含所需的網路安全活動和成果，分為 23 個類別，涵蓋組織的廣泛網路安全目標。概況包含了組織對其組織需求和目標，風險偏好和資源的調整，以及使用架構核心所需結果的資源的獨特一致性。實施層描述了組織的網路安全風險管理實踐展現出架構核心中所定義的特色。

## 使用此架構

您可以使用 NIST CSF 1.1 版來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST CSF 要求分組成控制集。Audit Manager 目前支援架構核心元件。Audit Manager 不支援此架構中的設定檔和實作元件。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 NIST CSF 中定義的控制項來執行此動

作。當您需要進行稽核時，您 (或您選擇的委派人員) 可以檢閱 Audit Manager 收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
NIST 網路安全架構 (CSF) 1.1 版	49	59	22

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_NIST-CSF-v1.1.zip](#) 檔案。

Audit Manager 提供的控制項並不用於驗證您的系統是否符合 NIST CSF。此外，他們無法保證您會透過 NIST 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [國家標準技術研究所 \(NIST\)](#)
- [NIST 電腦安全資源中心](#)
- [AWS NIST 的合規性頁面](#)
- [NIST 網路安全架構-與雲端中的 NIST CSF 保持一致 AWS](#)

# 尼斯特第二版

AWS Audit Manager 提供預先建置的標準架構，支援 NIST 800-171 修訂版 2：保護非聯邦系統與 Organizations 中受控制的非機密資訊。

## Note

- 如需支援 NIST SP 800-53 之 Audit Manager 架構的相關資訊，請參閱。[第五修訂版](#)
- 如需支援 NIST CSF 之 Audit Manager 架構的相關資訊，請參閱。[NIST 網路安全架構 1.1 版](#)

## 主題

- [什麼是 NIST SP 800-171?](#)
- [使用此架構](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 NIST SP 800-171?

NIST SP 800-171 專注於保護非聯邦系統和組織中受控制的未分類資訊 (CUI) 的機密性。它提出實現此目標的具體安全要求。NIST 800-171 是一份出版物，概述在網路上處理 CUI 的非聯邦組織所需的安全標準和策略。於 2015 年 6 月由[美國國家標準技術研究院 \(NIST\)](#) 首次出版。NIST 是一家美國政府機構，發布多項標準和出版物，以加強公共和私營部門的網路安全抗禦能力。NIST SP 800-171 已定期收到更新，以配合新興的網路威脅和不斷變化的技術。於 2020 年 2 月發布最新版本 (修訂版 2)。

NIST SP 800-171 中的網路安全控制措施可保護政府承包商和分包商的 IT 網路中的 CUI。它定義了政府承包商在其網路處理或儲存 CUI 時必須遵守的做法和程序。NIST SP 800-171 僅適用於承包商網路中存在 CUI 的那些部分。

## 使用此架構

您可以使用 NIST SP 800-171 架構來協助您為稽核做好準備。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 NIST 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。它會根據 NIST SP 800-171 架構中定義的控制項來執行此作業。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
NIST 800-171 修訂版 2：保護非聯邦系統與 Organizations 中受控制的非機密資訊	81	29	14

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManager\\_ConfigDataSourceMappings\\_NIST-800-171-Rev-2.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 NIST 800-171 的規定。此外，他們無法保證您會透過 NIST 之稽核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控制項。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [國家標準技術研究所 \(NIST\)](#)
- [NIST 電腦安全資源中心](#)



- [AWS NIST 的合規性頁面](#)

## PCI DSS V3.2.1

AWS Audit Manager 提供支援支付卡產業資料安全標準 (PCI DSS) v3.2.1 的預建標準架構。

### Note

如需 PCI DSS v4 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 [PCI DSS V4.0](#)。

### 主題

- [什麼是 PCI DSS ?](#)
- [使用此架構幫助您進行稽核準備](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 PCI DSS ?

PCI DSS 是一個專有的信息安全標準。它由 [PCI 安全標準委員會管理](#)，該委員會由美國運通，發現金融服務，JCB 國際，全 MasterCard 球和 Visa Inc. PCI DSS 適用於存儲，處理或傳輸持卡人數據 (CHD) 或敏感身份驗證數據 (SAD) 的實體。這包括但不受限於商家、處理者、收單銀行、發行者 and 服務提供者。PCI DSS 受卡片品牌所規範，且由支付卡產業安全標準委員會管理。

AWS 通過 PCI DSS 第一級服務供應商認證，這是可用評估的最高等級。合規評估由獨立且經過認證的安全評估員 (QSA) Coalfire Systems Inc. 進行。您可以透過以下方式取得 PCI DSS 合規證明 (AOC) 和責任摘要。AWS Artifact 這是一個自助入口網站，可隨選存取 AWS 合規報告。登入 [AWS 管理主控台](#)，或 [AWS Artifact 在開始使用中深入](#) 了解 AWS Artifact。

您可以從 [PCI 安全標準委員會文件庫](#) 下載 PCI DSS 標準。

## 使用此架構幫助您進行稽核準備

您可以使用 PCI DSS V3.2.1 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 PCI DSS 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 PCI DSS V3.2.1 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
支付卡產業資料安全標準 (PCI DSS) v3.2.1	168	116	15

#### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_PCI-DS-DS-v3.2.1.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 PCI DSS 標準。此外，他們不能保證您會通過 PCI DSS 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [PCI 安全標準委員會](#)
- [PCI 安全標準委員會文件庫](#)。

- [AWS PCI DSS 的合規性頁面](#)

## PCI DSS V4.0

AWS Audit Manager 提供支援支付卡產業資料安全標準 (PCI DSS) v4.0 的預建架構。

### Note

如需 PCI DSS v3.2.1 以及支援此功能的 Audit Manager 架構之相關資訊，請參閱 [PCI DSS V3.2.1](#)。

### 主題

- [什麼是 PCI DSS ?](#)
- [使用此架構幫助您進行稽核準備](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 PCI DSS ?

支付卡產業資料安全標準 (PCI DSS) 是一項全球標準，提供保護付款資料的技術與作業要求基準。PCI DSS v4.0 是此標準的下一代演進。

PCI DSS 的開發目的是鼓勵和強化支付卡帳戶資料的安全性。它也促進全球廣泛採用一致的資料安全措施。它提供了以保護帳戶資料為目的而設計的技術和操作要求之基準。雖然這套標準的設計重心是放在具有支付卡帳戶資料的環境，但您也可以使用 PCI DSS 來防範威脅並保護支付生態系統中的其他要素。

PCI 安全標準委員會 (PCI SSC) 在 PCI DSS v3.2.1 和 v4.0 之間引進了許多更動。這些更新分為三大類別：

1. 不斷變化的要求 – 更動的部分可確保該標準在面對新興威脅和技術時可以與時俱進，也能滿足支付產業帶來的各種變化。範例包含全新或修改的要求或測試程序，或移除某項要求。
2. 說明或指導 – 更新了措辭、解釋、定義、其他指導或指示，以增進對特定主題的瞭解或提供進一步資訊或指導。

3. 結構或格式 – 內容的重組，包含將各項要求予以組合、分離和重新編號，以便與內容一致。

## 使用此架構幫助您進行稽核準備

### Note

此標準架構使用來自 Security Hub 的合併控制項做為資料來源。若要順利從合併控制項收集證據，請確定您已開啟 Security Hub 中的合併控制項調查結果設定。如需有關使用 Security Hub 做為資料來源類型的詳細資訊，請參閱 [AWS Audit Manager 支援的 AWS Security Hub 控制項](#)。

您可以使用 PCI DSS V4.0 架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 PCI DSS V4.0 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據 PCI DSS V4.0 架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱 AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
支付卡產業資料安全標準 (PCI DSS) v4.0	175	105	15

### Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_PCI-DS-DS-v4.0.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並非用來驗證您的系統是否符合 PCI DSS 標準。此外，他們不能保證您會通過 PCI DSS 審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [PCI DSS v4.0 Resource Hub](#)
- [PCI 安全標準委員會](#)
- [PCI 安全標準委員會文件庫](#)。
- [AWS PCI DSS 的合規性頁面](#)
- [支付卡產業資料安全標準 \(PCI DSS\) v4.0 的合規性指南 AWS](#)

## SSE -18 系統管理系統 2

AWS Audit Manager 提供預先建置的標準架構，支援服務 Organizations 控制項 (SOC) 報告 2 第 18 號證明標準聲明 (SSAE)。

### 主題

- [什麼是 SOC 2?](#)
- [使用此架構幫助您進行稽核準備](#)
- [後續步驟](#)
- [其他資源](#)

## 什麼是 SOC 2？

SOC 2 由 [美國註冊會計師協會 \(AICPA\)](#) 定義，是在審計過程中產生的一組報告的名稱。其目的是供服務組織 (向其他組織提供資訊系統服務的組織) 使用，將這些資訊系統的 [內部控制項](#) 驗證報表發布給這些服務使用者。這些報告著重於五個類別的控制項，稱為信任服務原則。

AWS SOC 報告是獨立的第三方檢查報告，展示如何 AWS 實現關鍵合規性控制和目標。這些報告的目的是幫助您和您的稽核員瞭解為支援營運和法規遵循而建立的 AWS 控制措施。這裡有五個 AWS SOC 報告：

- AWS SOC 1 報告，可供 AWS 客戶使用 [AWS Artifact](#)。
- AWS SOC 2 安全性、可用性和機密性報告，可供 AWS 客戶從 [AWS Artifact](#)。
- AWS SOC 2 安全性、可用性和機密性報告可供 AWS 客戶取得 [AWS Artifact](#)(範圍僅包括 Amazon DocumentDB)。
- AWS SOC 2 隱私權第一類報告，可供 AWS 客戶使用 [AWS Artifact](#)。
- AWS SOC 3 安全性、可用性和機密性報告，[以白皮書形式公開提供](#)。

## 使用此架構幫助您進行稽核準備

您可以使用此架構來協助您準備稽核。此架構包含預先打造的控制集合，其中包含說明和測試程序。這些控制項會根據 SOC 2 要求分組成控制集。您也可以根據特定需求自訂架構和控制項，以支援內部稽核。

使用架構作為起點，您可以建立 Audit Manager 評估，並開始收集與您的稽核相關的證據。建立評估之後，Audit Manager 會開始評估您的 AWS 資源。其根據架構中定義的控制項來執行此動作。需要進行稽核時，您或您選擇的委派代表可以檢閱 Audit Manager 所收集的證據。您也可以瀏覽這些評估中的證據資料夾，並選擇要包含在評估報告中的證據。或者，如果您啟用了證據搜尋工具，您就可以搜尋特定證據並以 CSV 格式匯出，或者從搜尋結果建立評估報告。不論何種方式，您都可以使用此評估報告來顯示您的控制項正在按預期運作。

架構的詳細資訊如下：

框架名稱	AWS Audit Manager	自動化控制項數量	手動控制項數量	控制集數
關於證明參與標準 (SSAE) 第 18 號的聲明，服務 Organizations 控制 (SOC) 報告 2		46	15	20

**i** Tip

若要檢閱在此標準架構中用作資料來源對應的 AWS Config 規則，請下載 [AuditManagerConfigDataSourceMappings\\_SSAE-編號 -18-SOC-報表 -2.zip](#) 檔案。

此 AWS Audit Manager 架構中的控制項並不用於驗證您的系統是否符合標準。此外，他們不能保證您會通過審核。AWS Audit Manager 不會自動檢查需要手動證據收集的程序控件。

您可以在 Audit Manager 中架構程式庫的 [標準架構] 索引標籤下找到此架構。

## 後續步驟

如需使用此架構建立評估方式的說明，請參閱 [在中建立評估 AWS Audit Manager](#)。

如需如何自訂此架構以支援您的特定需求的指示，請參閱 [在中製作現有框架的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [AWS SOC 的合規性頁面](#)

## 自動化證據的支援資料來源類型

在中建立自訂控制項時 AWS Audit Manager，您可以設定控制項以從下列資料來源類型收集自動證據：

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API 呼叫

每種資料來源類型都提供不同的功能，可用於擷取使用者活動記錄、符合性發現項目、資源組態等。

在本章中，您可以瞭解這些自動化資料來源類型，以及 Audit Manager 支援的特定 AWS Security Hub 控制項、AWS Config 規則和 AWS API 呼叫。

### 重點

下表概述了每種自動資料來源類型的概觀。

Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解秘訣
AWS CloudTrail	追蹤特定使用者活動。	持續。	從 <a href="#">支援的事件名稱</a> 清單中選取。	Audit Manager 會根據您選擇的關鍵字篩選 CloudTrail 記錄。結果會匯入為使用者活動證據。	<a href="#">我的評估不會從 AWS CloudTrail 中收集使用者</a>



Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解訣
AWS Config	透過報告發現項目來擷取資源安全狀況的快照 AWS Config。	根據 AWS Config 規則中定義的觸發程序。	選擇規則類型，然後選取規則。 <ul style="list-style-type: none"> <li>對於受管規則，請從<a href="#">支援的受管規則關鍵字</a>清單中選取。</li> <li>對於自訂規則，請從<a href="#">可用規則</a>清單中選取。</li> </ul>	Audit Manager 會直接從取得此規則的發現項目 AWS Config。結果會匯入為合規檢查證據。	<a href="#">活動證據</a>  <a href="#">我的評估不會從中收集合規性檢查證據</a> <a href="#">AWS Config</a>  <a href="#">AWS Config 整合問題</a>

Data source type (資料來源類型)	說明	證據收集頻率	如需使用此資料來源類型.....	當此控制項在評估中處於使用中狀態時...	相關的疑難排解秘訣
AWS Security Hub	透過 Security Hub 報告調查結果，擷取資源安全狀況的快照。	根據 Security Hub 的檢查排程。	從 <a href="#">支援的 Security Hub 控制識別碼</a> 清單中選取。	Audit Manager 會直接從 Security Hub 取得安全檢查的結果。結果會匯入為合規檢查證據。	<a href="#">我的評估不會從中收集合規性檢查證據</a> <a href="#">AWS Security Hub</a>
AWS API 呼叫	透過指定的 API 呼叫，直接擷取資源組態的快照 AWS 服務。	每日、每週或每月。	從 <a href="#">支援的 API 呼叫</a> 清單中選取，然後選取您偏好的頻率。	Audit Manager 會根據您的指定頻率進行 API 呼叫。系統會將回應匯入為組態資料證據。	<a href="#">我的評估不會收集 AWS API 呼叫的組態資料證據</a>

 Tip

您可以建立自訂控制項，使用上述資料來源的預先定義分組來收集證據。這些資料來源群組稱為[AWS 受管理來源](#)。每個 AWS 受管理的來源代表一個共同的控制項或核心控制項，以符合常

見的合規性要求。這為您提供了一種將合規要求映射到相關 AWS 數據源組的有效方法。若要查看可用的一般控制項，請參閱[尋找可用的控制項 AWS Audit Manager](#)。或者，您可以使用上述四種資料來源類型來定義自己的自訂資料來源。這使您可以靈活地上傳手動證據，或從業務特定資源（例如自定義 AWS Config 規則）收集自動證據。

## 後續步驟

若要深入瞭解可在自訂控制項中使用的特定資料來源，請參閱下列頁面。

- [AWS Config 規則 支持 AWS Audit Manager](#)
- [AWS Security Hub 支援的控制項 AWS Audit Manager](#)
- [AWS 支援的 API 呼叫 AWS Audit Manager](#)
- [AWS CloudTrail 支援的事件名稱 AWS Audit Manager](#)

## AWS Config 規則 支持 AWS Audit Manager

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

除了受管規則之外，您還可以將自訂規則映射至控制項資料來源。

### 內容

- [重點](#)
- [支援的 AWS Config 受管規則](#)
- [搭配 Audit Manager 使用 AWS Config 自訂規則](#)
- [其他資源](#)


### 重點

- Audit Manager 不會從[服務連結 AWS Config 規則](#)中收集證據，但來自一致性套件和來源的服務連結規則除外。AWS Organizations

- Audit Manager 不會為您管理 AWS Config 規則。開始收集證據之前，建議您先檢閱目前的 AWS Config 規則參數。然後，根據所選架構的要求來驗證這些參數。如果需要，您可以[更新 AWS Config 中的規則參數](#)，使其符合架構需求。這將有助於確保您的評估為該架構收集正確的合規檢查證據。

例如，假設您正在為 CIS v1.2.0 建立評估。此架構具有名為「[確保 IAM 密碼政策](#)」的控制項，[長度至少需要 14 或更高](#)。在中 AWS Config，[iam-password-policy](#)規則具有檢查密碼長度的 `MinimumPasswordLength` 參數。此參數的預設值為 14 字元。因此，該規則符合控制項的需求。如果您沒有使用預設參數值，請確保您使用的值等於或大於 CIS v1.2.0 的 14 個字元要求。您可以在 [AWS Config 文件](#) 中找到每個受管規則的預設參數詳細資訊。

- 如果您需要驗證 AWS Config 規則是受管規則還是自訂規則，可以使用 [AWS Config 主控台](#) 執行此操作。從左側導覽功能表中選擇規則，然後在表格中尋找規則。如果是受管規則，類型欄會顯示 AWS 受管規則。

	Name	Remediation action	Type	Compliance
<input type="radio"/>	<a href="#">account-part-of-organizations</a>	Not set	AWS managed	 Compliant

## 支援的 AWS Config 受管規則

稽核 AWS Config 管理員支援下列受管理規則。當您為自訂控制項設定資料來源時，您可以使用下列任何一個受管規則識別碼關鍵字。如需有關下列任何受管規則的詳細資訊，請從清單中選擇項目，或參閱 AWS Config 使用者指南中的 [AWS Config 受管規則](#)。

### Tip

當您在建立自訂控制項期間在 Audit Manager 主控台中選擇受管規則時，請確定您尋找下列其中一個規則識別碼關鍵字，而非規則名稱。如需規則名稱和規則識別碼之間的差異，以及如何尋找受管規則識別碼的詳細資訊，請參閱本使用手冊的 [疑難排解](#) 一節。

### 支援 AWS Config 受管規則關鍵字

- [ACCESS\\_KEYS\\_ROTATED](#)
- [ACCOUNT\\_PART\\_OF\\_ORGANIZATIONS](#)
- [ACM\\_CERTIFICATE\\_EXPIRATION\\_CHECK](#)
- [ACM\\_CERTIFICATE\\_RSA\\_CHECK](#)

## 支援 AWS Config 受管規則關鍵字

- [ALB\\_DESYNC\\_MODE\\_CHECK](#)
- [ALB\\_HTTP\\_DROP\\_INVALID\\_HEADER\\_ENABLED](#)
- [ALB\\_HTTP\\_TO\\_HTTPS\\_REDIRECTION\\_CHECK](#)
- [ALB\\_WAF\\_ENABLED](#)
- [API\\_GW\\_ASSOCIATED\\_WITH\\_WAF](#)
- [API\\_GW\\_CACHE\\_ENABLED\\_AND\\_ENCRYPTED](#)
- [API\\_GW\\_ENDPOINT\\_TYPE\\_CHECK](#)
- [API\\_GW\\_EXECUTION\\_LOGGING\\_ENABLED](#)
- [API\\_GW\\_SSL\\_ENABLED](#)
- [API\\_GW\\_XRAY\\_ENABLED](#)
- [API\\_GWV2\\_ACCESS\\_LOGS\\_ENABLED](#)
- [API\\_GWV2\\_AUTHORIZATION\\_TYPE\\_CONFIGURED](#)
- [APPROVED\\_AMIS\\_BY\\_ID](#)
- [APPROVED\\_AMIS\\_BY\\_TAG](#)
- [APPSYNC\\_ASSOCIATED\\_WITH\\_WAF](#)
- [APPSYNC\\_CACHE\\_ENCRYPTION\\_AT\\_REST](#)
- [APPSYNC\\_LOGGING\\_ENABLED](#)
- [AURORA\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [AURORA\\_MYSQL\\_BACKTRACKING\\_ENABLED](#)
- [AURORA\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [AUTOSCALING\\_CAPACITY\\_REBALANCING](#)
- [AUTOSCALING\\_GROUP\\_ELB\\_HEALTHCHECK\\_REQUIRED](#)
- [AUTOSCALING\\_LAUNCH\\_CONFIG\\_HOP\\_LIMIT](#)
- [AUTOSCALING\\_LAUNCH\\_CONFIG\\_PUBLIC\\_IP\\_DISABLED](#)
- [AUTOSCALING\\_LAUNCHCONFIG\\_REQUIRES\\_IMDSV2](#)
- [AUTOSCALING\\_LAUNCH\\_TEMPLATE](#)
- [AUTOSCALING\\_MULTIPLE\\_AZ](#)
- [AUTOSCALING\\_MULTIPLE\\_INSTANCE\\_TYPES](#)
- [BACKUP\\_PLAN\\_MIN\\_FREQUENCY\\_AND\\_MIN\\_RETENTION\\_CHECK](#)

## 支援 AWS Config 受管規則關鍵字

- [BACKUP\\_RECOVERY\\_POINT\\_ENCRYPTED](#)
- [BACKUP\\_RECOVERY\\_POINT\\_MANUAL\\_DELETION\\_DISABLED](#)
- [BACKUP\\_RECOVERY\\_POINT\\_MINIMUM\\_RETENTION\\_CHECK](#)
- [BEANSTALK\\_ENHANCED\\_HEALTH\\_REPORTING\\_ENABLED](#)
- [CLB\\_DESYNC\\_MODE\\_CHECK](#)
- [CLB\\_MULTIPLE\\_AZ](#)
- [CLOUD\\_TRAIL\\_CLOUD\\_WATCH\\_LOGS\\_ENABLED](#)
- [CLOUD\\_TRAIL\\_ENABLED](#)
- [CLOUD\\_TRAIL\\_ENCRYPTION\\_ENABLED](#)
- [CLOUD\\_TRAIL\\_LOG\\_FILE\\_VALIDATION\\_ENABLED](#)
- [CLOUDFORMATION\\_STACK\\_DRIFT\\_DETECTION\\_CHECK](#)
- [CLOUDFORMATION\\_STACK\\_NOTIFICATION\\_CHECK](#)
- [CLOUDFRONT\\_ACCESSLOGS\\_ENABLED](#)
- [CLOUDFRONT\\_ASSOCIATED\\_WITH\\_WAF](#)
- [CLOUDFRONT\\_CUSTOM\\_SSL\\_CERTIFICATE](#)
- [CLOUDFRONT\\_DEFAULT\\_ROOT\\_OBJECT\\_CONFIGURED](#)
- [CLOUDFRONT\\_NO\\_DEPRECATED\\_SSL\\_PROTOCOLS](#)
- [CLOUDFRONT\\_ORIGIN\\_ACCESS\\_IDENTITY\\_ENABLED](#)
- [CLOUDFRONT\\_ORIGIN\\_FAILOVER\\_ENABLED](#)
- [CLOUDFRONT\\_S3\\_ORIGIN\\_ACCESS\\_CONTROL\\_ENABLED](#)
- [CLOUDFRONT\\_S3\\_ORIGIN\\_NON\\_EXISTENT\\_BUCKET](#)
- [CLOUDFRONT\\_SECURITY\\_POLICY\\_CHECK](#)
- [CLOUDFRONT\\_SNI\\_ENABLED](#)
- [CLOUDFRONT\\_TRAFFIC\\_TO\\_ORIGIN\\_ENCRYPTED](#)
- [CLOUDFRONT\\_VIEWER\\_POLICY\\_HTTPS](#)
- [CLOUDTRAIL\\_S3\\_DATAEVENTS\\_ENABLED](#)
- [CLOUDTRAIL\\_SECURITY\\_TRAIL\\_ENABLED](#)
- [CLOUDWATCH\\_ALARM\\_ACTION\\_CHECK](#)
- [CLOUDWATCH\\_ALARM\\_ACTION\\_ENABLED\\_CHECK](#)

## 支援 AWS Config 受管規則關鍵字

- [CLOUDWATCH\\_ALARM\\_RESOURCE\\_CHECK](#)
- [CLOUDWATCH\\_ALARM\\_SETTINGS\\_CHECK](#)
- [CLOUDWATCH\\_LOG\\_GROUP\\_ENCRYPTED](#)
- [CMK\\_BACKING\\_KEY\\_ROTATION\\_ENABLED](#)
- [CODEBUILD\\_PROJECT\\_ARTIFACT\\_ENCRYPTION](#)
- [CODEBUILD\\_PROJECT\\_ENVIRONMENT\\_PRIVILEGED\\_CHECK](#)
- [編碼生成\\_項目\\_恩瓦爾\\_AWSCRED\\_CHECK](#)
- [CODEBUILD\\_PROJECT\\_LOGGING\\_ENABLED](#)
- [CODEBUILD\\_PROJECT\\_S3\\_LOGS\\_ENCRYPTED](#)
- [CODEBUILD\\_PROJECT\\_SOURCE\\_REPO\\_URL\\_CHECK](#)
- [CODEDEPLOY\\_AUTO\\_ROLLBACK\\_MONITOR\\_ENABLED](#)
- [CODEDEPLOY\\_EC2\\_MINIMUM\\_HEALTHY\\_HOSTS\\_CONFIGURED](#)
- [CODEDEPLOY\\_LAMBDA\\_ALLATONCE\\_TRAFFIC\\_SHIFT\\_DISABLED](#)
- [CODEPIPELINE\\_DEPLOYMENT\\_COUNT\\_CHECK](#)
- [CODEPIPELINE\\_REGION\\_FANOUT\\_CHECK](#)
- [CUSTOM\\_SCHEMA\\_REGISTRY\\_POLICY\\_ATTACHED](#)
- [CW\\_LOGGROUP\\_RETENTION\\_PERIOD\\_CHECK](#)
- [DAX\\_ENCRYPTION\\_ENABLED](#)
- [DB\\_INSTANCE\\_BACKUP\\_ENABLED](#)
- [DESIRED\\_INSTANCE\\_TENANCY](#)
- [DESIRED\\_INSTANCE\\_TYPE](#)
- [DMS\\_REPLICATION\\_NOT\\_PUBLIC](#)
- [DYNAMODB\\_AUTOSCALING\\_ENABLED](#)
- [DYNAMODB\\_IN\\_BACKUP\\_PLAN](#)
- [DYNAMODB\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [DYNAMODB\\_PITR\\_ENABLED](#)
- [DYNAMODB\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [DYNAMODB\\_TABLE\\_ENCRYPTED\\_KMS](#)
- [DYNAMODB\\_TABLE\\_ENCRYPTION\\_ENABLED](#)

## 支援 AWS Config 受管規則關鍵字

- [DYNAMODB\\_THROUGHPUT\\_LIMIT\\_CHECK](#)
- [EBS\\_IN\\_BACKUP\\_PLAN](#)
- [EBS\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [EBS\\_OPTIMIZED\\_INSTANCE](#)
- [EBS\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [EBS\\_SNAPSHOT\\_PUBLIC\\_RESTORABLE\\_CHECK](#)
- [EC2\\_CLIENT\\_VPN\\_NOT\\_AUTHORIZE\\_ALL](#)
- [識別碼 : EC2\\_EBS\\_ENCRYPTION\\_BY\\_DEFAULT](#)
- [EC2\\_IMDSV2\\_CHECK](#)
- [EC2\\_INSTANCE\\_DETAILED\\_MONITORING\\_ENABLED](#)
- [EC2\\_INSTANCE\\_MANAGED\\_BY\\_SSM](#)
- [EC2\\_INSTANCE\\_MULTIPLE\\_ENI\\_CHECK](#)
- [EC2\\_INSTANCE\\_NO\\_PUBLIC\\_IP](#)
- [EC2\\_INSTANCE\\_PROFILE\\_ATTACHED](#)
- [EC2\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [EC2\\_LAUNCH\\_TEMPLATE\\_PUBLIC\\_IP\\_DISABLED](#)
- [EC2\\_MANAGEDINSTANCE\\_APPLICATIONS\\_BLACKLISTED](#)
- [EC2\\_MANAGEDINSTANCE\\_APPLICATIONS\\_REQUIRED](#)
- [EC2\\_MANAGEDINSTANCE\\_ASSOCIATION\\_COMPLIANCE\\_STATUS\\_CHECK](#)
- [EC2\\_MANAGEDINSTANCE\\_INVENTORY\\_BLACKLISTED](#)
- [EC2\\_MANAGEDINSTANCE\\_PATCH\\_COMPLIANCE\\_STATUS\\_CHECK](#)
- [EC2\\_MANAGEDINSTANCE\\_PLATFORM\\_CHECK](#)
- [EC2\\_NO\\_AMAZON\\_KEY\\_PAIR](#)
- [EC2\\_PARAVIRTUAL\\_INSTANCE\\_CHECK](#)
- [EC2\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [EC2\\_SECURITY\\_GROUP\\_ATTACHED\\_TO\\_ENI](#)
- [EC2\\_SECURITY\\_GROUP\\_ATTACHED\\_TO\\_ENI\\_PERIODIC](#)
- [EC2\\_STOPPED\\_INSTANCE](#)
- [EC2\\_TOKEN\\_HOP\\_LIMIT\\_CHECK](#)



## 支援 AWS Config 受管規則關鍵字

- [EC2\\_TRANSIT\\_GATEWAY\\_AUTO\\_VPC\\_ATTACH\\_DISABLED](#)
- [EC2\\_VOLUME\\_INUSE\\_CHECK](#)
- [ECR\\_PRIVATE\\_IMAGE\\_SCANNING\\_ENABLED](#)
- [ECR\\_PRIVATE\\_LIFECYCLE\\_POLICY\\_CONFIGURED](#)
- [ECR\\_PRIVATE\\_TAG\\_IMMUTABILITY\\_ENABLED](#)
- [ECS\\_已啟用\\_AWSVPC\\_NETWORKING\\_\( \)](#)
- [ECS\\_CONTAINER\\_INSIGHTS\\_ENABLED](#)
- [ECS\\_CONTAINERS\\_NONPRIVILEGED](#)
- [ECS\\_CONTAINERS\\_READONLY\\_ACCESS](#)
- [ECS\\_FARGATE\\_LATEST\\_PLATFORM\\_VERSION](#)
- [ECS\\_NO\\_ENVIRONMENT\\_SECRETS](#)
- [ECS\\_TASK\\_DEFINITION\\_LOG\\_CONFIGURATION](#)
- [ECS\\_TASK\\_DEFINITION\\_MEMORY\\_HARD\\_LIMIT](#)
- [ECS\\_TASK\\_DEFINITION\\_NONROOT\\_USER](#)
- [ECS\\_TASK\\_DEFINITION\\_PID\\_MODE\\_CHECK](#)
- [ECS\\_TASK\\_DEFINITION\\_USER\\_FOR\\_HOST\\_MODE\\_CHECK](#)
- [EFS\\_ACCESS\\_POINT\\_ENFORCE\\_ROOT\\_DIRECTORY](#)
- [EFS\\_ACCESS\\_POINT\\_ENFORCE\\_USER\\_IDENTITY](#)
- [EFS\\_ENCRYPTED\\_CHECK](#)
- [EFS\\_IN\\_BACKUP\\_PLAN](#)
- [EFS\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [EFS\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [EIP\\_ATTACHED](#)
- [EKS\\_CLUSTER\\_LOGGING\\_ENABLED](#)
- [EKS\\_CLUSTER\\_OLDEST\\_SUPPORTED\\_VERSION](#)
- [EKS\\_CLUSTER\\_SUPPORTED\\_VERSION](#)
- [EKS\\_ENDPOINT\\_NO\\_PUBLIC\\_ACCESS](#)
- [EKS\\_SECRETS\\_ENCRYPTED](#)
- [ELASTIC\\_BEANSTALK\\_LOGS\\_TO\\_CLOUDWATCH](#)

## 支援 AWS Config 受管規則關鍵字

- [ELASTIC\\_BEANSTALK\\_MANAGED\\_UPDATES\\_ENABLED](#)
- [ELASTICACHE\\_AUTO\\_MINOR\\_VERSION\\_UPGRADE\\_CHECK](#)
- [ELASTICACHE\\_RBAC\\_AUTH\\_ENABLED](#)
- [ELASTICACHE\\_REDIS\\_CLUSTER\\_AUTOMATIC\\_BACKUP\\_CHECK](#)
- [ELASTICACHE\\_REPL\\_GRP\\_AUTO\\_FAILOVER\\_ENABLED](#)
- [ELASTICACHE\\_REPL\\_GRP\\_ENCRYPTED\\_AT\\_REST](#)
- [ELASTICACHE\\_REPL\\_GRP\\_ENCRYPTED\\_IN\\_TRANSIT](#)
- [ELASTICACHE\\_REPL\\_GRP\\_REDIS\\_AUTH\\_ENABLED](#)
- [ELASTICACHE\\_SUBNET\\_GROUP\\_CHECK](#)
- [ELASTICACHE\\_SUPPORTED\\_ENGINE\\_VERSION](#)
- [ELASTICSEARCH\\_ENCRYPTED\\_AT\\_REST](#)
- [ELASTICSEARCH\\_IN\\_VPC\\_ONLY](#)
- [ELASTICSEARCH\\_LOGS\\_TO\\_CLOUDWATCH](#)
- [ELASTICSEARCH\\_NODE\\_TO\\_NODE\\_ENCRYPTION\\_CHECK](#)
- [ELB\\_ACM\\_CERTIFICATE\\_REQUIRED](#)
- [ELB\\_CROSS\\_ZONE\\_LOAD\\_BALANCING\\_ENABLED](#)
- [ELB\\_CUSTOM\\_SECURITY\\_POLICY\\_SSL\\_CHECK](#)
- [ELB\\_DELETION\\_PROTECTION\\_ENABLED](#)
- [ELB\\_LOGGING\\_ENABLED](#)
- [ELB\\_PREDEFINED\\_SECURITY\\_POLICY\\_SSL\\_CHECK](#)
- [ELB\\_TLS\\_HTTPS\\_LISTENERS\\_ONLY](#)
- [ELBV2\\_ACM\\_CERTIFICATE\\_REQUIRED](#)
- [ELBV2\\_MULTIPLE\\_AZ](#)
- [EMR\\_KERBEROS\\_ENABLED](#)
- [EMR\\_MASTER\\_NO\\_PUBLIC\\_IP](#)
- [ENCRYPTED\\_VOLUMES](#)
- [FMS\\_SHIELD\\_RESOURCE\\_POLICY\\_CHECK](#)
- [FMS\\_WEBACL\\_RESOURCE\\_POLICY\\_CHECK](#)
- [FMS\\_WEBACL\\_RULEGROUP\\_ASSOCIATION\\_CHECK](#)

## 支援 AWS Config 受管規則關鍵字

- [FSX\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [FSX\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [GUARDDUTY\\_ENABLED\\_CENTRALIZED](#)
- [GUARDDUTY\\_NON\\_ARCHIVED\\_FINDINGS](#)
- [IAM\\_CUSTOMER\\_POLICY\\_BLOCKED\\_KMS\\_ACTIONS](#)
- [IAM\\_GROUP\\_HAS\\_USERS\\_CHECK](#)
- [IAM\\_INLINE\\_POLICY\\_BLOCKED\\_KMS\\_ACTIONS](#)
- [IAM\\_NO\\_INLINE\\_POLICY\\_CHECK](#)
- [IAM\\_PASSWORD\\_POLICY](#)
- [IAM\\_POLICY\\_BLACKLISTED\\_CHECK](#)
- [IAM\\_POLICY\\_IN\\_USE](#)
- [IAM\\_POLICY\\_NO\\_STATEMENTS\\_WITH\\_ADMIN\\_ACCESS](#)
- [IAM\\_POLICY\\_NO\\_STATEMENTS\\_WITH\\_FULL\\_ACCESS](#)
- [IAM\\_ROLE\\_MANAGED\\_POLICY\\_CHECK](#)
- [IAM\\_ROOT\\_ACCESS\\_KEY\\_CHECK](#)
- [IAM\\_USER\\_GROUP\\_MEMBERSHIP\\_CHECK](#)
- [IAM\\_USER\\_MFA\\_ENABLED](#)
- [IAM\\_USER\\_NO\\_POLICIES\\_CHECK](#)
- [IAM\\_USER\\_UNUSED\\_CREDENTIALS\\_CHECK](#)
- [INCOMING\\_SSH\\_DISABLED](#)
- [INSTANCES\\_IN\\_VPC](#)
- [KINESIS\\_STREAM\\_ENCRYPTED](#)
- [INTERNET\\_GATEWAY\\_AUTHORIZED\\_VPC\\_ONLY](#)
- [KMS\\_CMK\\_NOT\\_SCHEDULED\\_FOR\\_DELETION](#)
- [LAMBDA\\_CONCURRENCY\\_CHECK](#)
- [LAMBDA\\_DLQ\\_CHECK](#)
- [LAMBDA\\_FUNCTION\\_PUBLIC\\_ACCESS\\_PROHIBITED](#)
- [LAMBDA\\_FUNCTION\\_SETTINGS\\_CHECK](#)
- [LAMBDA\\_INSIDE\\_VPC](#)

## 支援 AWS Config 受管規則關鍵字

- [LAMBDA\\_VPC\\_MULTI\\_AZ\\_CHECK](#)
- [MACIE\\_STATUS\\_CHECK](#)
- [MFA\\_ENABLED\\_FOR\\_IAM\\_CONSOLE\\_ACCESS](#)
- [MQ\\_AUTOMATIC\\_MINOR\\_VERSION\\_UPGRADE\\_ENABLED](#)
- [MQ\\_CLOUDWATCH\\_AUDIT\\_LOGGING\\_ENABLED](#)
- [MQ\\_NO\\_PUBLIC\\_ACCESS](#)
- [MULTI\\_REGION\\_CLOUD\\_TRAIL\\_ENABLED](#)
- [NACL\\_NO\\_UNRESTRICTED\\_SSH\\_RDP](#)
- [NETFW\\_LOGGING\\_ENABLED](#)
- [NETFW\\_MULTI\\_AZ\\_ENABLED](#)
- [NETFW\\_POLICY\\_DEFAULT\\_ACTION\\_FRAGMENT\\_PACKETS](#)
- [NETFW\\_POLICY\\_DEFAULT\\_ACTION\\_FULL\\_PACKETS](#)
- [NETFW\\_POLICY\\_RULE\\_GROUP\\_ASSOCIATED](#)
- [NETFW\\_STATELESS\\_RULE\\_GROUP\\_NOT\\_EMPTY](#)
- [NLB\\_CROSS\\_ZONE\\_LOAD\\_BALANCING\\_ENABLED](#)
- [NO\\_UNRESTRICTED\\_ROUTE\\_TO\\_IGW](#)
- [OPENSEARCH\\_ACCESS\\_CONTROL\\_ENABLED](#)
- [OPENSEARCH\\_AUDIT\\_LOGGING\\_ENABLED](#)
- [OPENSEARCH\\_DATA\\_NODE\\_FAULT\\_TOLERANCE](#)
- [OPENSEARCH\\_ENCRYPTED\\_AT\\_REST](#)
- [OPENSEARCH\\_HTTPS\\_REQUIRED](#)
- [OPENSEARCH\\_IN\\_VPC\\_ONLY](#)
- [OPENSEARCH\\_LOGS\\_TO\\_CLOUDWATCH](#)
- [OPENSEARCH\\_NODE\\_TO\\_NODE\\_ENCRYPTION\\_CHECK](#)
- [RDS\\_AUTOMATIC\\_MINOR\\_VERSION\\_UPGRADE\\_ENABLED](#)
- [RDS\\_CLUSTER\\_DEFAULT\\_ADMIN\\_CHECK](#)
- [RDS\\_CLUSTER\\_DELETION\\_PROTECTION\\_ENABLED](#)
- [RDS\\_CLUSTER\\_IAM\\_AUTHENTICATION\\_ENABLED](#)
- [RDS\\_CLUSTER\\_MULTI\\_AZ\\_ENABLED](#)

## 支援 AWS Config 受管規則關鍵字

- [RDS\\_DB\\_SECURITY\\_GROUP\\_NOT\\_ALLOWED](#)
- [RDS\\_ENHANCED\\_MONITORING\\_ENABLED](#)
- [RDS\\_IN\\_BACKUP\\_PLAN](#)
- [RDS\\_INSTANCE\\_DEFAULT\\_ADMIN\\_CHECK](#)
- [RDS\\_INSTANCE\\_DELETION\\_PROTECTION\\_ENABLED](#)
- [RDS\\_INSTANCE\\_IAM\\_AUTHENTICATION\\_ENABLED](#)
- [RDS\\_INSTANCE\\_PUBLIC\\_ACCESS\\_CHECK](#)
- [RDS\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [RDS\\_LOGGING\\_ENABLED](#)
- [RDS\\_MULTI\\_AZ\\_SUPPORT](#)
- [RDS\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [RDS\\_SNAPSHOT\\_ENCRYPTED](#)
- [RDS\\_SNAPSHOTS\\_PUBLIC\\_PROHIBITED](#)
- [RDS\\_STORAGE\\_ENCRYPTED](#)
- [REDSHIFT\\_BACKUP\\_ENABLED](#)
- [REDSHIFT\\_REQUIRE\\_TLS\\_SSL](#)
- [REDSHIFT\\_CLUSTER\\_CONFIGURATION\\_CHECK](#)
- [REDSHIFT\\_CLUSTER\\_MAINTENANCESETTINGS\\_CHECK](#)
- [識別符](#) : REDSHIFT\_CLUSTER\_PUBLIC\_ACCESS\_CHECK
- [REDSHIFT\\_AUDIT\\_LOGGING\\_ENABLED](#)
- [REDSHIFT\\_CLUSTER\\_KMS\\_ENABLED](#)
- [REDSHIFT\\_DEFAULT\\_ADMIN\\_CHECK](#)
- [REDSHIFT\\_DEFAULT\\_DB\\_NAME\\_CHECK](#)
- [REDSHIFT\\_ENHANCED\\_VPC\\_ROUTING\\_ENABLED](#)
- [REQUIRED\\_TAGS](#)
- [RESTRICTED\\_INCOMING\\_TRAFFIC](#)
- [ROOT\\_ACCOUNT\\_HARDWARE\\_MFA\\_ENABLED](#)
- [ROOT\\_ACCOUNT\\_MFA\\_ENABLED](#)
- [S3\\_ACCOUNT\\_LEVEL\\_PUBLIC\\_ACCESS\\_BLOCKS\\_PERIODIC](#)

## 支援 AWS Config 受管規則關鍵字

- [S3\\_ACCOUNT\\_LEVEL\\_PUBLIC\\_ACCESS\\_BLOCKS](#)
- [S3\\_BUCKET\\_ACL\\_PROHIBITED](#)
- [識別符](#) : S3\_BUCKET\_BLACKLISTED\_ACTIONS\_PROHIBITED
- [識別碼](#) : S3\_BUCKET\_DEFAULT\_LOCK\_ENABLED
- [S3\\_BUCKET\\_LEVEL\\_PUBLIC\\_ACCESS\\_PROHIBITED](#)
- [S3\\_BUCKET\\_LOGGING\\_ENABLED](#)
- [S3\\_BUCKET\\_POLICY\\_GRANTEE\\_CHECK](#)
- [S3\\_BUCKET\\_POLICY\\_NOT\\_MORE\\_PERMISSIVE](#)
- [S3\\_BUCKET\\_PUBLIC\\_READ\\_PROHIBITED](#)
- [S3\\_BUCKET\\_PUBLIC\\_WRITE\\_PROHIBITED](#)
- [S3\\_BUCKET\\_REPLICATION\\_ENABLED](#)
- [S3\\_BUCKET\\_SERVER\\_SIDE\\_ENCRYPTION\\_ENABLED](#)
- [S3\\_BUCKET\\_SSL\\_REQUESTS\\_ONLY](#)
- [S3\\_BUCKET\\_VERSIONING\\_ENABLED](#)
- [S3\\_DEFAULT\\_ENCRYPTION\\_KMS](#)
- [S3\\_EVENT\\_NOTIFICATIONS\\_ENABLED](#)
- [S3\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [S3\\_LIFECYCLE\\_POLICY\\_CHECK](#)
- [S3\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [S3\\_VERSION\\_LIFECYCLE\\_POLICY\\_CHECK](#)
- [SAGEMAKER\\_ENDPOINT\\_CONFIGURATION\\_KMS\\_KEY\\_CONFIGURED](#)
- [SAGEMAKER\\_NOTEBOOK\\_INSTANCE\\_INSIDE\\_VPC](#)
- [SAGEMAKER\\_NOTEBOOK\\_INSTANCE\\_KMS\\_KEY\\_CONFIGURED](#)
- [SAGEMAKER\\_NOTEBOOK\\_INSTANCE\\_ROOT\\_ACCESS\\_CHECK](#)
- [SAGEMAKER\\_NOTEBOOK\\_NO\\_DIRECT\\_INTERNET\\_ACCESS](#)
- [SECRETSMANAGER\\_ROTATION\\_ENABLED\\_CHECK](#)
- [SECRETSMANAGER\\_SCHEDULED\\_ROTATION\\_SUCCESS\\_CHECK](#)
- [SECRETSMANAGER\\_SECRET\\_PERIODIC\\_ROTATION](#)
- [SECRETSMANAGER\\_SECRET\\_UNUSED](#)

## 支援 AWS Config 受管規則關鍵字

- [SECRETSMANAGER\\_USING\\_CMK](#)
- [SECURITY\\_ACCOUNT\\_INFORMATION\\_PROVIDED](#)
- [SECURITYHUB\\_ENABLED](#)
- [SERVICE\\_VPC\\_ENDPOINT\\_ENABLED](#)
- [SES\\_MALWARE\\_SCANNING\\_ENABLED](#)
- [SHIELD\\_ADVANCED\\_ENABLED\\_AUTORENEW](#)
- [SHIELD\\_DRT\\_ACCESS](#)
- [SNS\\_ENCRYPTED\\_KMS](#)
- [SNS\\_TOPIC\\_MESSAGE\\_DELIVERY\\_NOTIFICATION\\_ENABLED](#)
- [SSM\\_DOCUMENT\\_NOT\\_PUBLIC](#)
- [STEP\\_FUNCTIONS\\_STATE\\_MACHINE\\_LOGGING\\_ENABLED](#)
- [STORAGEGATEWAY\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [STORAGEGATEWAY\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [SUBNET\\_AUTO\\_ASSIGN\\_PUBLIC\\_IP\\_DISABLED](#)
- [VIRTUALMACHINE\\_LAST\\_BACKUP\\_RECOVERY\\_POINT\\_CREATED](#)
- [VIRTUALMACHINE\\_RESOURCES\\_PROTECTED\\_BY\\_BACKUP\\_PLAN](#)
- [VPC\\_DEFAULT\\_SECURITY\\_GROUP\\_CLOSED](#)
- [VPC\\_FLOW\\_LOGS\\_ENABLED](#)
- [VPC\\_NETWORK\\_ACL\\_UNUSED\\_CHECK](#)
- [VPC\\_PEERING\\_DNS\\_RESOLUTION\\_CHECK](#)
- [識別符](#) : [VPC\\_SG\\_OPEN\\_ONLY\\_TO\\_AUTHORIZED\\_PORTS](#)
- [VPC\\_VPN\\_2\\_TUNNELS\\_UP](#)
- [WAF\\_CLASSIC\\_LOGGING\\_ENABLED](#)
- [WAF\\_GLOBAL\\_RULEGROUP\\_NOT\\_EMPTY](#)
- [WAF\\_GLOBAL\\_RULE\\_NOT\\_EMPTY](#)
- [WAF\\_GLOBAL\\_WEBACL\\_NOT\\_EMPTY](#)
- [WAF\\_REGIONAL\\_RULEGROUP\\_NOT\\_EMPTY](#)
- [WAF\\_REGIONAL\\_RULE\\_NOT\\_EMPTY](#)
- [WAF\\_REGIONAL\\_WEBACL\\_NOT\\_EMPTY](#)

## 支援 AWS Config 受管規則關鍵字

- [WAFV2\\_LOGGING\\_ENABLED](#)
- [WAFV2\\_RULEGROUP\\_NOT\\_EMPTY](#)
- [WAFV2\\_WEBACL\\_NOT\\_EMPTY](#)

## 搭配 Audit Manager 使用 AWS Config 自訂規則

您可以使用 AWS Config 自訂規則做為稽核報告的資料來源。當控制項具有對應至 AWS Config 規則的資料來源時，Audit Manager 會新增 AWS Config 規則所建立的評估。

您可以使用的自訂規則取決於 AWS 帳戶 您登入 Audit Manager 時使用的規則。如果您可以在中存取自訂規則 AWS Config，則可以在「Audit Manager」中將其用作資料來源對映。

- 對於個人 AWS 帳戶 — 您可以使用您在帳戶中創建的任何自定義規則。
- 對於屬於組織的帳戶 — 您可以使用任何成員層級的自訂規則。或者，您可以在 AWS Config 中使用任何可用的組織層級自訂規則。

將自訂規則對應為控制項的資料來源之後，您可以將該控制項新增至 Audit Manager 中的自訂架構。

## 其他資源

- 若要尋找此資料來源類型問題的說明，請參閱[我的評估不會從中收集合規性檢查證據 AWS Config](#)和[AWS Config 整合問題](#)。
- 若要使用此資料來源類型建立自訂控制項，請參閱[在中建立自訂控制項 AWS Audit Manager](#)。
- 若要建立使用自訂控制項的自訂架構，請參閱[在中建立自訂架構 AWS Audit Manager](#)。
- 若要將您的自訂控制項新增至現有的自訂架構，請參閱[編輯自訂架構 AWS Audit Manager](#)。
- 若要在中建立自訂規則 AWS Config，請參閱AWS Config 開發人員指南 [AWS Config](#)中的〈[開發自訂規則](#)〉。

## AWS Security Hub 支援的控制項 AWS Audit Manager

您可以使用 Audit Manager 擷取 Security Hub 發現項目作為稽核的證據。當您建立或編輯自訂控制項時，您可以指定一或多個 Security Hub 控制項做為證據收集的資料來源對應。Security Hub 會根據這些控制項執行符合性檢查，而 Audit Manager 會將結果報告為符合性檢查證據。



## 內容

- [重點](#)
- [支援的 Security Hub 控制項](#)
- [其他資源](#)

## 重點

- Audit Manager 不會從 [Security Hub 心建立的服務連結 AWS Config 規則](#) 收集證據。
- 2022 年 11 月 9 日，Security Hub 推出了與網際網路安全中心 (CIS) AWS 基準指標 1.4.0 版要求相符的自動安全檢查，第 1 級和第 2 級 (CIS v1.4.0)。在 Security Hub 中，除了 [CIS v1.2.0 標準](#) 外，還支援 [CIS v 1.4.0 標準](#)。
- 建議您在 Security Hub 中開啟 [合併控制項調查結果](#) 設定 (如果尚未開啟)。如果您在 2023 年 2 月 23 日當天或之後啟用資 Security Hub，此設定預設為開啟。

啟用合併調查結果時，Security Hub 會針對每個安全檢查產生單一調查結果 (即使相同檢查適用於多個標準)。每個 Security Hub 調查結果都會做為 Audit Manager 中一項獨立資源評估來收集。因此，合併的調查結果會導致 Audit Manager 針對 Security Hub 調查結果執行的獨立資源評估總計減少。因此，使用合併的調查結果可以降低 Audit Manager 的使用成本，而不會犧牲證據品質和可用性。如需定價的詳細資訊，請參閱 [AWS Audit Manager 定價](#)。

### 開啟或關閉合併調查結果時的證據範例

下列範例顯示，Audit Manager 如何根據您的 Security Hub 設定收集和提供證據的比較。

When consolidated findings is turned on

假設您已經在安全中心啟用了以下三個安全標準：AWS FSBP，PCI DSS 和獨聯體基準測試 v1.2.0。

- [這三個標準都使用相同的控制項 \(IAM.4\) 與相同的基礎 AWS Config 規則 \(iam-root-access-key-check\)。](#)
- 由於已開啟合併的發現項目設定，因此 Security Hub 會針對此控制項產生一個尋找項目。
- Security Hub 會將合併的調查結果傳送給 Audit Manager 以進行此控制項。
- 合併的調查結果會被視為 Audit Manager 中的一項獨立資源評估。因此，您的評估中會新增一份證據。

此處提供範例說明該證據的範例：

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/finding/09876543-p0o9-i8u7-y6t5-098765432109",
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-west-2",
  "GeneratorId": "security-control/IAM.4",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-10-25T11:32:24.861Z",
  "LastObservedAt": "2023-11-02T11:59:19.546Z",
  "CreatedAt": "2023-10-25T11:32:24.861Z",
  "UpdatedAt": "2023-11-02T11:59:15.127Z",
  "Severity": {
    "Label": "INFORMATIONAL",
    "Normalized": 0,
    "Original": "INFORMATIONAL"
  },
  "Title": "IAM root user access key should not exist",
  "Description": "This AWS control checks whether the root user access key is available.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-check-000270f5",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:iam::111122223333:root",
  }
}
```

```

    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
  },
  "Resources": [{
    "Type": "AwsAccount",
    "Id": "AWS:::Account:111122223333",
    "Partition": "aws",
    "Region": "us-west-2"
  }],
  "Compliance": {
    "Status": "PASSED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/1.12"
    ],
    "SecurityControlId": "IAM.4",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    },
    {
      "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
    }
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "RESOLVED"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "INFORMATIONAL",
    "Original": "INFORMATIONAL"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2023-11-02T11:59:20.980Z"
}

```

## When consolidated findings is turned off

假設您已經在安全中心啟用了以下三個安全標準：AWS FSBP，PCI DSS 和獨聯體基準測試 v1.2.0。

- [這三個標準都使用相同的控制項 \(IAM.4\) 與相同的基礎 AWS Config 規則 \(iam-root-access-key-check\)。](#)
- 由於已關閉合併的調查結果設定，Security Hub 會針對每個已啟用的標準 (在本例中為三個調查結果)，針對每個安全檢查產生個別的調查結果。
- Security Hub 會針對此控制項，傳送三個獨立的標準特定調查結果給 Audit Manager。
- 這三個調查結果計數為 Audit Manager 中的三個獨特資源評估 因此，三項獨立的證據新增至您的評估中。

此處提供範例說明該證據的範例。請注意，在此範例中，下列三個承載中的每一項都具有相同的安全控制 ID (*SecurityControlId*:"IAM.4")。因此，當下列調查結果從 Security Hub 傳入時，在 Audit Manager (IAM.4) 中收集此證據的評估控制會收到三個不同的證據。

### IAM.4 的證據 (FSBP)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
    "findings":[
      {
        "SchemaVersion":"2018-10-08",
        "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-a78f-3cbe9402d17d",
        "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
        "ProductName":"Security Hub",
```

```

    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
    ],
    "FirstObservedAt": "2020-10-05T19:18:47.848Z",
    "LastObservedAt": "2023-11-01T14:12:04.106Z",
    "CreatedAt": "2020-10-05T19:18:47.848Z",
    "UpdatedAt": "2023-11-01T14:11:53.720Z",
    "Severity": {
      "Product": 0,
      "Label": "INFORMATIONAL",
      "Normalized": 0,
      "Original": "INFORMATIONAL"
    },
    "Title": "IAM.4 IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key
is available.",
    "Remediation": {
      "Recommendation": {
        "Text": "For information on how to correct this issue, consult the
AWS Security Hub controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
      }
    },
    "ProductFields": {
      "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
      "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
      "ControlId": "IAM.4",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
      "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-67cbb1c4",
      "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
      "StandardsControlArn": "arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
      "aws/securityhub/ProductName": "Security Hub",
      "aws/securityhub/CompanyName": "AWS",

```

```

        "Resources:0/Id":"arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
    },
    "Resources":[
        {
            "Type":"AwsAccount",
            "Id":"AWS:::Account:111122223333",
            "Partition":"aws",
            "Region":"us-west-2"
        }
    ],
    "Compliance":{
        "Status":"PASSED",
        "SecurityControlId":"IAM.4",
        "AssociatedStandards":[
            {
                "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
            }
        ]
    },
    "WorkflowState":"NEW",
    "Workflow":{
        "Status":"RESOLVED"
    },
    "RecordState":"ACTIVE",
    "FindingProviderFields":{
        "Severity":{
            "Label":"INFORMATIONAL",
            "Original":"INFORMATIONAL"
        },
        "Types":[
            "Software and Configuration Checks/Industry and Regulatory
Standards/AWS-Foundational-Security-Best-Practices"
        ]
    },
    "ProcessedAt":"2023-11-01T14:12:07.395Z"
}
]
}
}

```

## IAM.4 的證據 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
    "findings":[
      {
        "SchemaVersion":"2018-10-08",
        "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
        "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
        "ProductName":"Security Hub",
        "CompanyName":"AWS",
        "Region":"us-west-2",
        "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.12",
        "AwsAccountId":"111122223333",
        "Types":[
          "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
        ],
        "FirstObservedAt":"2020-10-05T19:18:47.775Z",
        "LastObservedAt":"2023-11-01T14:12:07.989Z",
        "CreatedAt":"2020-10-05T19:18:47.775Z",
        "UpdatedAt":"2023-11-01T14:11:53.720Z",
        "Severity":{
          "Product":0,
          "Label":"INFORMATIONAL",
          "Normalized":0,

```

```

    "Original": "INFORMATIONAL"
  },
  "Title": "1.12 Ensure no root user access key exists",
  "Description": "The root user is the most privileged user in an AWS
account. AWS Access Keys provide programmatic access to a given AWS account. It is
recommended that all access keys associated with the root user be removed.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the
AWS Security Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "1.12",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
    "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-67cbb1c4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:iam::111122223333:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:111122223333",
      "Partition": "aws",
      "Region": "us-west-2"
    }
  ],
  "Compliance": {
    "Status": "PASSED",

```



```

        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [
            {
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            }
        ],
        "WorkflowState": "NEW",
        "Workflow": {
            "Status": "RESOLVED"
        },
        "RecordState": "ACTIVE",
        "FindingProviderFields": {
            "Severity": {
                "Label": "INFORMATIONAL",
                "Original": "INFORMATIONAL"
            },
            "Types": [
                "Software and Configuration Checks/Industry and Regulatory
Standards/CIS AWS Foundations Benchmark"
            ]
        },
        "ProcessedAt": "2023-11-01T14:12:13.436Z"
    }
]
}
}

```

## PCI DSS 的證據

```

{
  "version": "0",
  "id": "12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type": "Security Hub Findings - Imported",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2023-10-27T18:55:59Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
}

```

```

"detail":{
  "findings":[
    {
      "SchemaVersion":"2018-10-08",
      "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
      "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
      "ProductName":"Security Hub",
      "CompanyName":"AWS",
      "Region":"us-west-2",
      "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
      "AwsAccountId":"111122223333",
      "Types":[
        "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
      ],
      "FirstObservedAt":"2020-10-05T19:18:47.788Z",
      "LastObservedAt":"2023-11-01T14:12:02.413Z",
      "CreatedAt":"2020-10-05T19:18:47.788Z",
      "UpdatedAt":"2023-11-01T14:11:53.720Z",
      "Severity":{
        "Product":0,
        "Label":"INFORMATIONAL",
        "Normalized":0,
        "Original":"INFORMATIONAL"
      },
      "Title":"PCI.IAM.1 IAM root user access key should not exist",
      "Description":"This AWS control checks whether the root user access key
is available.",
      "Remediation":{
        "Recommendation":{
          "Text":"For information on how to correct this issue, consult the
AWS Security Hub controls documentation.",
          "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
      },
      "ProductFields":{
        "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
        "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
        "ControlId":"PCI.IAM.1",
        "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",

```

```

    "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
    "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
    "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
    "aws/securityhub/ProductName":"Security Hub",
    "aws/securityhub/CompanyName":"AWS",
    "Resources:0/Id":"arn:aws:iam::111122223333:root",
    "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
  },
  "Resources":[
    {
      "Type":"AwsAccount",
      "Id":"AWS:::Account:111122223333",
      "Partition":"aws",
      "Region":"us-west-2"
    }
  ],
  "Compliance":{
    "Status":"PASSED",
    "RelatedRequirements":[
      "PCI DSS 2.1",
      "PCI DSS 2.2",
      "PCI DSS 7.2.1"
    ],
    "SecurityControlId":"IAM.4",
    "AssociatedStandards":[
      {
        "StandardsId":"standards/pci-dss/v/3.2.1"
      }
    ]
  },
  "WorkflowState":"NEW",
  "Workflow":{
    "Status":"RESOLVED"
  },
  "RecordState":"ACTIVE",
  "FindingProviderFields":{
    "Severity":{
      "Label":"INFORMATIONAL",
      "Original":"INFORMATIONAL"
    }
  },

```

```

        "Types": [
            "Software and Configuration Checks/Industry and Regulatory
Standards/PCI-DSS"
        ]
    },
    "ProcessedAt": "2023-11-01T14:12:05.950Z"
}
]
}
}
}

```

## 支援的 Security Hub 控制項

Audit Manager 目前支援下列 Security Hub 控制項。當您為自訂控制項設定資料來源時，您可以使用下列任何一個特定於標準的控制項 ID 關鍵字。

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
CIS v1.2.0	1.2	<a href="#">IAM.5</a>
CIS v1.2.0	1.3	<a href="#">IAM.8</a>
CIS v1.2.0	1.4	<a href="#">IAM.3</a>
CIS v1.2.0	1.5	<a href="#">IAM.11</a>
CIS v1.2.0	1.6	<a href="#">IAM.12</a>
CIS v1.2.0	1.7	<a href="#">IAM.13</a>
CIS v1.2.0	1.8	<a href="#">IAM.14</a>
CIS v1.2.0	1.9	<a href="#">IAM.15</a>
CIS v1.2.0	1.10	<a href="#">IAM.16</a>

安全標準	Audit Manager 支援的關鍵字  (Security Hub 中 的標準控制項識 別碼)	相關控制項文件  ( Security Hub 中對應的安全控制 ID )
CIS v1.2.0	1.11	<a href="#">IAM.17</a>
CIS v1.2.0	1.12	<a href="#">IAM.4</a>
CIS v1.2.0	1.13	<a href="#">IAM.9</a>
CIS v1.2.0	1.14	<a href="#">IAM.6</a>
CIS v1.2.0	1.16	<a href="#">IAM.2</a>
CIS v1.2.0	1.20	<a href="#">IAM.18</a>
CIS v1.2.0	1.22	<a href="#">IAM.1</a>
CIS v1.2.0	2.1	<a href="#">CloudTrail.1</a>
CIS v1.2.0	2.2	<a href="#">CloudTrail.4</a>
CIS v1.2.0	2.3	<a href="#">CloudTrail.6</a>
CIS v1.2.0	2.4	<a href="#">CloudTrail.5</a>
CIS v1.2.0	2.5	<a href="#">Config.1</a>
CIS v1.2.0	2.6	<a href="#">CloudTrail.7</a>
CIS v1.2.0	2.7	<a href="#">CloudTrail.2</a>
CIS v1.2.0	2.8	<a href="#">KMS.4</a>
CIS v1.2.0	2.9	<a href="#">EC2.6</a>
CIS v1.2.0	3.1	<a href="#">CloudWatch.2</a>
CIS v1.2.0	3.2	<a href="#">CloudWatch.3</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
CIS v1.2.0	3.3	<a href="#">CloudWatch.1</a>
CIS v1.2.0	3.4	<a href="#">CloudWatch.4</a>
CIS v1.2.0	3.5	<a href="#">CloudWatch.5</a>
CIS v1.2.0	3.6	<a href="#">CloudWatch.6</a>
CIS v1.2.0	3.7	<a href="#">CloudWatch.7</a>
CIS v1.2.0	3.8	<a href="#">CloudWatch.8</a>
CIS v1.2.0	3.9	<a href="#">CloudWatch.9</a>
CIS v1.2.0	3.10	<a href="#">CloudWatch.10</a>
CIS v1.2.0	3.11	<a href="#">CloudWatch.11</a>
CIS v1.2.0	3.12	<a href="#">CloudWatch.12</a>
CIS v1.2.0	3.13	<a href="#">CloudWatch.13</a>
CIS v1.2.0	3.14	<a href="#">CloudWatch.14</a>
CIS v1.2.0	4.1	<a href="#">EC2.13</a>
CIS v1.2.0	4.2	<a href="#">EC2.14</a>
CIS v1.2.0	4.3	<a href="#">EC2.2</a>
PCI DSS	PCI。 AutoScaling.1	<a href="#">AutoScaling.1</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
PCI DSS	PCI。 CloudTrail.1	<a href="#">CloudTrail.1</a>
PCI DSS	PCI。 CloudTrail.2	<a href="#">CloudTrail.2</a>
PCI DSS	PCI。 CloudTrail.3	<a href="#">CloudTrail.3</a>
PCI DSS	PCI。 CloudTrail.4	<a href="#">CloudTrail.4</a>
PCI DSS	PCI。 CodeBuild.1	<a href="#">CodeBuild.1</a>
PCI DSS	PCI。 CodeBuild.2	<a href="#">CodeBuild.2</a>
PCI DSS	PCI.Config.1	<a href="#">Config.1</a>
PCI DSS	PCI.CW.1	<a href="#">CloudWatch.1</a>
PCI DSS	PCI.DMS.1	<a href="#">DMS.1</a>
PCI DSS	PCI.EC2.1	<a href="#">EC2.1</a>
PCI DSS	PCI.EC2.2	<a href="#">EC2.2</a>
PCI DSS	PCI.EC2.3	<a href="#">EC2.3</a>
PCI DSS	PCI.EC2.4	<a href="#">EC2.12</a>
PCI DSS	PCI.EC2.5	<a href="#">EC2.13</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
PCI DSS	PCI.EC2.6	<a href="#">EC2.6</a>
PCI DSS	PCI.ELBv2.1	<a href="#">ELB.1</a>
PCI DSS	PCI.ES.1	<a href="#">ES.1</a>
PCI DSS	PCI.ES.2	<a href="#">ES.2</a>
PCI DSS	PCI。 GuardDuty.1	<a href="#">GuardDuty.1</a>
PCI DSS	PCI.IAM.1	<a href="#">IAM.1</a>
PCI DSS	PCI.IAM.2	<a href="#">IAM.2</a>
PCI DSS	PCI.IAM.3	<a href="#">IAM.3</a>
PCI DSS	PCI.IAM.4	<a href="#">IAM.4</a>
PCI DSS	PCI.IAM.5	<a href="#">IAM.9</a>
PCI DSS	PCI.IAM.6	<a href="#">IAM.6</a>
PCI DSS	PCI.IAM.7	<a href="#">PCI.IAM.7</a>
PCI DSS	PCI.IAM.8	<a href="#">PCI.IAM8.</a>
PCI DSS	PCI.KMS.1	<a href="#">PCI.KMS.4</a>
PCI DSS	PCI.Lambda.1	<a href="#">Lambda.1</a>
PCI DSS	PCI.Lambda.2	<a href="#">Lambda.3</a>



安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
PCI DSS	PCI.Opensearch.1	<a href="#">Opensearch.1</a>
PCI DSS	PCI.Opensearch.2	<a href="#">Opensearch.2</a>
PCI DSS	PCI.RDS.1	<a href="#">RDS.1</a>
PCI DSS	PCI.RDS.2	<a href="#">RDS.2</a>
PCI DSS	PCI.Redshift.1	<a href="#">Redshift.1</a>
PCI DSS	PCI.S3.1	<a href="#">S3.1</a>
PCI DSS	PCI.S3.2	<a href="#">S3.2</a>
PCI DSS	PCI.S3.3	<a href="#">S3.3</a>
PCI DSS	PCI.S3.4	<a href="#">S3.4</a>
PCI DSS	PCI.S3.5	<a href="#">S3.5</a>
PCI DSS	PCI.S3.6	<a href="#">S3.1</a>
PCI DSS	PCI.SageMaker.1	<a href="#">SageMaker.1</a>
PCI DSS	PCI.SSM.1	<a href="#">SSM.1</a>
PCI DSS	PCI.SSM.2	<a href="#">SSM.2</a>
PCI DSS	PCI.SSM.3	<a href="#">SSM.3</a>
AWS 基礎安全性最佳做法	Account.1	<a href="#">Account.1</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	帳戶 .2	<a href="#">帳戶 .2</a>
AWS 基礎安全性最佳做法	ACM.1	<a href="#">ACM.1</a>
AWS 基礎安全性最佳做法	ACM.2	<a href="#">ACM.2</a>
AWS 基礎安全性最佳做法	APIGateway.1	<a href="#">APIGateway.1</a>
AWS 基礎安全性最佳做法	APIGateway.2	<a href="#">APIGateway.2</a>
AWS 基礎安全性最佳做法	APIGateway.3	<a href="#">APIGateway.3</a>
AWS 基礎安全性最佳做法	APIGateway.4	<a href="#">APIGateway.4</a>
AWS 基礎安全性最佳做法	APIGateway.5	<a href="#">APIGateway.5</a>
AWS 基礎安全性最佳做法	APIGateway.8	<a href="#">APIGateway.8</a>
AWS 基礎安全性最佳做法	APIGateway.9	<a href="#">APIGateway.9</a>
AWS 基礎安全性最佳做法	AppSync.2	<a href="#">AppSync.2</a>
AWS 基礎安全性最佳做法	AppSync.5	<a href="#">AppSync.5</a>
AWS 基礎安全性最佳做法	雅典娜 .1	<a href="#">雅典娜 .1</a>
AWS 基礎安全性最佳做法	AutoScaling.1	<a href="#">AutoScaling.1</a>
AWS 基礎安全性最佳做法	AutoScaling.2	<a href="#">AutoScaling.2</a>
AWS 基礎安全性最佳做法	AutoScaling.3	<a href="#">AutoScaling.3</a>
AWS 基礎安全性最佳做法	AutoScaling.4	<a href="#">AutoScaling.4</a>
AWS 基礎安全性最佳做法	Autoscaling.5	<a href="#">Autoscaling.5</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	AutoScaling.6	<a href="#">AutoScaling.6</a>
AWS 基礎安全性最佳做法	AutoScaling.9	<a href="#">AutoScaling.9</a>
AWS 基礎安全性最佳做法	Backup. 1	<a href="#">Backup. 1</a>
AWS 基礎安全性最佳做法	CloudFormation.1	<a href="#">CloudFormation.1</a>
AWS 基礎安全性最佳做法	CloudFront.1	<a href="#">CloudFront.1</a>
AWS 基礎安全性最佳做法	CloudFront.2	<a href="#">CloudFront.2</a>
AWS 基礎安全性最佳做法	CloudFront.3	<a href="#">CloudFront.3</a>
AWS 基礎安全性最佳做法	CloudFront.4	<a href="#">CloudFront.4</a>
AWS 基礎安全性最佳做法	CloudFront.5	<a href="#">CloudFront.5</a>
AWS 基礎安全性最佳做法	CloudFront.6	<a href="#">CloudFront.6</a>
AWS 基礎安全性最佳做法	CloudFront.7	<a href="#">CloudFront.7</a>
AWS 基礎安全性最佳做法	CloudFront.8	<a href="#">CloudFront.8</a>
AWS 基礎安全性最佳做法	CloudFront.9	<a href="#">CloudFront.9</a>
AWS 基礎安全性最佳做法	CloudFront.10	<a href="#">CloudFront.10</a>
AWS 基礎安全性最佳做法	CloudFront.12	<a href="#">CloudFront.12</a>
AWS 基礎安全性最佳做法	CloudFront.13	<a href="#">CloudFront.13</a>
AWS 基礎安全性最佳做法	CloudTrail.1	<a href="#">CloudTrail.1</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	CloudTrail.2	<a href="#">CloudTrail.2</a>
AWS 基礎安全性最佳做法	CloudTrail.3	<a href="#">CloudTrail.3</a>
AWS 基礎安全性最佳做法	CloudTrail.4	<a href="#">CloudTrail.4</a>
AWS 基礎安全性最佳做法	CloudTrail.5	<a href="#">CloudTrail.5</a>
AWS 基礎安全性最佳做法	CloudTrail.6	<a href="#">CloudTrail.6</a>
AWS 基礎安全性最佳做法	CloudTrail.7	<a href="#">CloudTrail.7</a>
AWS 基礎安全性最佳做法	CloudWatch.1	<a href="#">CloudWatch.1</a>
AWS 基礎安全性最佳做法	CloudWatch.2	<a href="#">CloudWatch.2</a>
AWS 基礎安全性最佳做法	CloudWatch.3	<a href="#">CloudWatch.3</a>
AWS 基礎安全性最佳做法	CloudWatch.4	<a href="#">CloudWatch.4</a>
AWS 基礎安全性最佳做法	CloudWatch.5	<a href="#">CloudWatch.5</a>
AWS 基礎安全性最佳做法	CloudWatch.6	<a href="#">CloudWatch.6</a>
AWS 基礎安全性最佳做法	CloudWatch.7	<a href="#">CloudWatch.7</a>
AWS 基礎安全性最佳做法	CloudWatch.8	<a href="#">CloudWatch.8</a>
AWS 基礎安全性最佳做法	CloudWatch.9	<a href="#">CloudWatch.9</a>
AWS 基礎安全性最佳做法	CloudWatch.10	<a href="#">CloudWatch.10</a>
AWS 基礎安全性最佳做法	CloudWatch.11	<a href="#">CloudWatch.11</a>
AWS 基礎安全性最佳做法	CloudWatch.12	<a href="#">CloudWatch.12</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	CloudWatch.13	<a href="#">CloudWatch.13</a>
AWS 基礎安全性最佳做法	CloudWatch.14	<a href="#">CloudWatch.14</a>
AWS 基礎安全性最佳做法	CloudWatch.15	<a href="#">CloudWatch.15</a>
AWS 基礎安全性最佳做法	CloudWatch.16	<a href="#">CloudWatch.16</a>
AWS 基礎安全性最佳做法	CloudWatch.17	<a href="#">CloudWatch.17</a>
AWS 基礎安全性最佳做法	CodeBuild.1	<a href="#">CodeBuild.1</a>
AWS 基礎安全性最佳做法	CodeBuild.2	<a href="#">CodeBuild.2</a>
AWS 基礎安全性最佳做法	CodeBuild.3	<a href="#">CodeBuild.3</a>
AWS 基礎安全性最佳做法	CodeBuild.4	<a href="#">CodeBuild.4</a>
AWS 基礎安全性最佳做法	CodeBuild.5	<a href="#">CodeBuild.5</a>
AWS 基礎安全性最佳做法	Config.1	<a href="#">Config.1</a>
AWS 基礎安全性最佳做法	DMS.1	<a href="#">DMS.1</a>
AWS 基礎安全性最佳做法	公升 .6	<a href="#">公司 .6</a>
AWS 基礎安全性最佳做法	毫升 .7	<a href="#">公司 .7</a>
AWS 基礎安全性最佳做法	公升 .8	<a href="#">公司 .8</a>
AWS 基礎安全性最佳做法	數位 .9	<a href="#">公司 .9</a>
AWS 基礎安全性最佳做法	DocumentDB	<a href="#">DocumentDB</a>
AWS 基礎安全性最佳做法	DocumentDB	<a href="#">DocumentDB</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	DocumentDB	<a href="#">DocumentDB 3</a>
AWS 基礎安全性最佳做法	DocumentDB 4	<a href="#">DocumentDB 4</a>
AWS 基礎安全性最佳做法	DocumentDB 5	<a href="#">DocumentDB 5</a>
AWS 基礎安全性最佳做法	DynamoDB.1	<a href="#">DynamoDB.1</a>
AWS 基礎安全性最佳做法	DynamoDB.2	<a href="#">DynamoDB.2</a>
AWS 基礎安全性最佳做法	DynamoDB.3	<a href="#">DynamoDB.3</a>
AWS 基礎安全性最佳做法	DynamoB.4	<a href="#">DynamoB.4</a>
AWS 基礎安全性最佳做法	DynamoB.6	<a href="#">DynamoB.6</a>
AWS 基礎安全性最佳做法	EC2.1	<a href="#">EC2.1</a>
AWS 基礎安全性最佳做法	EC2.2	<a href="#">EC2.2</a>
AWS 基礎安全性最佳做法	EC2.3	<a href="#">EC2.3</a>
AWS 基礎安全性最佳做法	EC2.4	<a href="#">EC2.4</a>
AWS 基礎安全性最佳做法	EC2.6	<a href="#">EC2.6</a>
AWS 基礎安全性最佳做法	EC2.7	<a href="#">EC2.7</a>
AWS 基礎安全性最佳做法	EC2.8	<a href="#">EC2.8</a>
AWS 基礎安全性最佳做法	EC2.9	<a href="#">EC2.9</a>
AWS 基礎安全性最佳做法	EC2.10	<a href="#">EC2.10</a>
AWS 基礎安全性最佳做法	EC2.12	<a href="#">EC2.12</a>

安全標準	Audit Manager 支援的關鍵字  (Security Hub 中 的標準控制項識 別碼)	相關控制項文件  ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	EC2.13	<a href="#">EC2.13</a>
AWS 基礎安全性最佳做法	EC2.14	<a href="#">EC2.14</a>
AWS 基礎安全性最佳做法	EC2.15	<a href="#">EC2.15</a>
AWS 基礎安全性最佳做法	EC2.16	<a href="#">EC2.16</a>
AWS 基礎安全性最佳做法	EC2.17	<a href="#">EC2.17</a>
AWS 基礎安全性最佳做法	EC2.18	<a href="#">EC2.18</a>
AWS 基礎安全性最佳做法	EC2.19	<a href="#">EC2.19</a>
AWS 基礎安全性最佳做法	EC2.20	<a href="#">EC2.20</a>
AWS 基礎安全性最佳做法	EC2.21	<a href="#">EC2.21</a>
AWS 基礎安全性最佳做法	EC2.22	<a href="#">EC2.22</a>
AWS 基礎安全性最佳做法	EC2.23	<a href="#">EC2.23</a>
AWS 基礎安全性最佳做法	EC2.24	<a href="#">EC2.24</a>
AWS 基礎安全性最佳做法	EC2.25	<a href="#">EC2.25</a>
AWS 基礎安全性最佳做法	EC2.28	<a href="#">EC2.28</a>
AWS 基礎安全性最佳做法	EC2.51	<a href="#">EC2.51</a>
AWS 基礎安全性最佳做法	ECR.1	<a href="#">ECR.1</a>
AWS 基礎安全性最佳做法	ECR.2	<a href="#">ECR.2</a>
AWS 基礎安全性最佳做法	ECR.3	<a href="#">ECR.3</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	ECS.1	<a href="#">ECS.1</a>
AWS 基礎安全性最佳做法	ECS.2	<a href="#">ECS.2</a>
AWS 基礎安全性最佳做法	ECS.3	<a href="#">ECS.3</a>
AWS 基礎安全性最佳做法	ECS.4	<a href="#">ECS.4</a>
AWS 基礎安全性最佳做法	ECS.5	<a href="#">ECS.5</a>
AWS 基礎安全性最佳做法	ECS.8	<a href="#">ECS.8</a>
AWS 基礎安全性最佳做法	等 .9	<a href="#">ECS.9</a>
AWS 基礎安全性最佳做法	ECS.10	<a href="#">ECS.10</a>
AWS 基礎安全性最佳做法	ECS.12	<a href="#">ECS.12</a>
AWS 基礎安全性最佳做法	EFS.1	<a href="#">EFS.1</a>
AWS 基礎安全性最佳做法	EFS.2	<a href="#">EFS.2</a>
AWS 基礎安全性最佳做法	EFS.3	<a href="#">EFS.3</a>
AWS 基礎安全性最佳做法	EFS.4	<a href="#">EFS.4</a>
AWS 基礎安全性最佳做法	EKS.1	<a href="#">EKS.1</a>
AWS 基礎安全性最佳做法	EKS.2	<a href="#">EKS.2</a>
AWS 基礎安全性最佳做法	EKS.8	<a href="#">EK.8</a>
AWS 基礎安全性最佳做法	ElastiCache.1	<a href="#">ElastiCache.1</a>
AWS 基礎安全性最佳做法	ElastiCache.2	<a href="#">ElastiCache.2</a>



安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	ElastiCache.3	<a href="#">ElastiCache.3</a>
AWS 基礎安全性最佳做法	ElastiCache.4	<a href="#">ElastiCache.4</a>
AWS 基礎安全性最佳做法	ElastiCache.5	<a href="#">ElastiCache.5</a>
AWS 基礎安全性最佳做法	ElastiCache.6	<a href="#">ElastiCache.6</a>
AWS 基礎安全性最佳做法	ElastiCache.7	<a href="#">ElastiCache.7</a>
AWS 基礎安全性最佳做法	ElasticBeanstalk.1	<a href="#">ElasticBeanstalk.1</a>
AWS 基礎安全性最佳做法	ElasticBeanstalk.2	<a href="#">ElasticBeanstalk.2</a>
AWS 基礎安全性最佳做法	ElasticBeanstalk.3	<a href="#">ElasticBeanstalk.3</a>
AWS 基礎安全性最佳做法	ELB.1	<a href="#">ELB.1</a>
AWS 基礎安全性最佳做法	ELB.2	<a href="#">ELB.2</a>
AWS 基礎安全性最佳做法	ELB.3	<a href="#">ELB.3</a>
AWS 基礎安全性最佳做法	ELB.4	<a href="#">ELB.4</a>
AWS 基礎安全性最佳做法	ELB.5	<a href="#">ELB.5</a>
AWS 基礎安全性最佳做法	ELB.6	<a href="#">ELB.6</a>
AWS 基礎安全性最佳做法	ELB.7	<a href="#">ELB.7</a>
AWS 基礎安全性最佳做法	ELB.8	<a href="#">ELB.8</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	ELB.9	<a href="#">ELB.9</a>
AWS 基礎安全性最佳做法	ELB.10	<a href="#">ELB.10</a>
AWS 基礎安全性最佳做法	ELB.12	<a href="#">ELB.12</a>
AWS 基礎安全性最佳做法	ELB.13	<a href="#">ELB.13</a>
AWS 基礎安全性最佳做法	ELB.14	<a href="#">ELB.14</a>
AWS 基礎安全性最佳做法	精靈 .16	<a href="#">ELB.16</a>
AWS 基礎安全性最佳做法	ELBv2.1	<a href="#">ELB.1</a>
AWS 基礎安全性最佳做法	EMR.1	<a href="#">EMR.1</a>
AWS 基礎安全性最佳做法	EMR.2	<a href="#">EMR.2</a>
AWS 基礎安全性最佳做法	ES.1	<a href="#">ES.1</a>
AWS 基礎安全性最佳做法	ES.2	<a href="#">ES.2</a>
AWS 基礎安全性最佳做法	ES.3	<a href="#">ES.3</a>
AWS 基礎安全性最佳做法	ES.4	<a href="#">ES.4</a>
AWS 基礎安全性最佳做法	ES.5	<a href="#">ES.5</a>
AWS 基礎安全性最佳做法	ES.6	<a href="#">ES.6</a>
AWS 基礎安全性最佳做法	ES.7	<a href="#">ES.7</a>
AWS 基礎安全性最佳做法	ES.8	<a href="#">ES.8</a>
AWS 基礎安全性最佳做法	EventBridge.3	<a href="#">EventBridge3.</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	EventBridge.4	<a href="#">EventBridge.4</a>
AWS 基礎安全性最佳做法	FSX.1	<a href="#">FSX.1</a>
AWS 基礎安全性最佳做法	GuardDuty.1	<a href="#">GuardDuty.1</a>
AWS 基礎安全性最佳做法	IAM.1	<a href="#">IAM.1</a>
AWS 基礎安全性最佳做法	IAM.2	<a href="#">IAM.2</a>
AWS 基礎安全性最佳做法	IAM.3	<a href="#">IAM.3</a>
AWS 基礎安全性最佳做法	IAM.4	<a href="#">IAM.4</a>
AWS 基礎安全性最佳做法	IAM.5	<a href="#">IAM.5</a>
AWS 基礎安全性最佳做法	IAM.6	<a href="#">IAM.6</a>
AWS 基礎安全性最佳做法	IAM.7	<a href="#">IAM.7</a>
AWS 基礎安全性最佳做法	IAM.8	<a href="#">IAM .8</a>
AWS 基礎安全性最佳做法	IAM.9	<a href="#">IAM.9</a>
AWS 基礎安全性最佳做法	我的 .10	<a href="#">亞姆 .10</a>
AWS 基礎安全性最佳做法	IAM.11	<a href="#">IAM.11</a>
AWS 基礎安全性最佳做法	IAM.12	<a href="#">IAM.12</a>
AWS 基礎安全性最佳做法	IAM.13	<a href="#">IAM.13</a>
AWS 基礎安全性最佳做法	IAM.14	<a href="#">IAM.14</a>
AWS 基礎安全性最佳做法	IAM.15	<a href="#">IAM.15</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	IAM.16	<a href="#">IAM.16</a>
AWS 基礎安全性最佳做法	IAM.17	<a href="#">IAM.17</a>
AWS 基礎安全性最佳做法	IAM.18	<a href="#">IAM.18</a>
AWS 基礎安全性最佳做法	我的 .19	<a href="#">亞姆 .19</a>
AWS 基礎安全性最佳做法	IAM.21	<a href="#">IAM.21</a>
AWS 基礎安全性最佳做法	我的 .22	<a href="#">家居安 .22</a>
AWS 基礎安全性最佳做法	Kinesis.1	<a href="#">Kinesis.1</a>
AWS 基礎安全性最佳做法	KMS.1	<a href="#">KMS.1</a>
AWS 基礎安全性最佳做法	KMS.2	<a href="#">KMS.2</a>
AWS 基礎安全性最佳做法	KMS.3	<a href="#">KMS.3</a>
AWS 基礎安全性最佳做法	KMS.4	<a href="#">KMS.4</a>
AWS 基礎安全性最佳做法	Lambda.1	<a href="#">Lambda.1</a>
AWS 基礎安全性最佳做法	Lambda.2	<a href="#">Lambda.2</a>
AWS 基礎安全性最佳做法	Lambda.3	<a href="#">Lambda.3</a>
AWS 基礎安全性最佳做法	Lambda.5	<a href="#">Lambda.5</a>
AWS 基礎安全性最佳做法	馬賽 .1	<a href="#">馬賽 .1</a>
AWS 基礎安全性最佳做法	每米 5 米	<a href="#">每米 5 米</a>
AWS 基礎安全性最佳做法	每克里數	<a href="#">每小米</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	毫克 .1	<a href="#">莫斯科</a>
AWS 基礎安全性最佳做法	MSK.2	<a href="#">麥斯克</a>
AWS 基礎安全性最佳做法	海王星 1 號	<a href="#">海王星 1 號</a>
AWS 基礎安全性最佳做法	海王星 2	<a href="#">海王星 .2</a>
AWS 基礎安全性最佳做法	海王星 .3	<a href="#">海王星 .3</a>
AWS 基礎安全性最佳做法	海王星 .4	<a href="#">海王星 .4</a>
AWS 基礎安全性最佳做法	海王星 .5	<a href="#">海王星 .5</a>
AWS 基礎安全性最佳做法	海王星 .6	<a href="#">海王星 .6</a>
AWS 基礎安全性最佳做法	海王星 .7	<a href="#">海王星 .7</a>
AWS 基礎安全性最佳做法	海王星 .8	<a href="#">海王星 .8</a>
AWS 基礎安全性最佳做法	海王星 .9	<a href="#">海王星 .9</a>
AWS 基礎安全性最佳做法	NetworkFirewall.1	<a href="#">NetworkFirewall.1</a>
AWS 基礎安全性最佳做法	NetworkFirewall.2	<a href="#">NetworkFirewall.2</a>
AWS 基礎安全性最佳做法	NetworkFirewall.3	<a href="#">NetworkFirewall.3</a>
AWS 基礎安全性最佳做法	NetworkFirewall.4	<a href="#">NetworkFirewall.4</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	NetworkFirewall.5	<a href="#">NetworkFirewall.5</a>
AWS 基礎安全性最佳做法	NetworkFirewall.6	<a href="#">NetworkFirewall.6</a>
AWS 基礎安全性最佳做法	NetworkFirewall.9	<a href="#">NetworkFirewall.9</a>
AWS 基礎安全性最佳做法	Opensearch.1	<a href="#">Opensearch.1</a>
AWS 基礎安全性最佳做法	Opensearch.2	<a href="#">Opensearch.2</a>
AWS 基礎安全性最佳做法	Opensearch.3	<a href="#">Opensearch.3</a>
AWS 基礎安全性最佳做法	Opensearch.4	<a href="#">Opensearch.4</a>
AWS 基礎安全性最佳做法	Opensearch.5	<a href="#">Opensearch.5</a>
AWS 基礎安全性最佳做法	Opensearch.6	<a href="#">Opensearch.6</a>
AWS 基礎安全性最佳做法	Opensearch.7	<a href="#">Opensearch.7</a>
AWS 基礎安全性最佳做法	Opensearch.8	<a href="#">Opensearch.8</a>
AWS 基礎安全性最佳做法	打開搜索 .10	<a href="#">打開搜索 .10</a>
AWS 基礎安全性最佳做法	PCA.1	<a href="#">PCA.1</a>
AWS 基礎安全性最佳做法	RDS.1	<a href="#">RDS.1</a>
AWS 基礎安全性最佳做法	RDS.2	<a href="#">RDS.2</a>
AWS 基礎安全性最佳做法	RDS.3	<a href="#">RDS.3</a>

安全標準	Audit Manager 支援的關鍵字  (Security Hub 中 的標準控制項識 別碼)	相關控制項文件  ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	RDS.4	<a href="#">RDS.4</a>
AWS 基礎安全性最佳做法	RDS.5	<a href="#">RDS.5</a>
AWS 基礎安全性最佳做法	RDS.6	<a href="#">RDS.6</a>
AWS 基礎安全性最佳做法	RDS.7	<a href="#">RDS.7</a>
AWS 基礎安全性最佳做法	RDS.8	<a href="#">RDS.8</a>
AWS 基礎安全性最佳做法	RDS.9	<a href="#">RDS.9</a>
AWS 基礎安全性最佳做法	RDS.10	<a href="#">RDS.10</a>
AWS 基礎安全性最佳做法	RDS.11	<a href="#">RDS.11</a>
AWS 基礎安全性最佳做法	RDS.12	<a href="#">RDS.12</a>
AWS 基礎安全性最佳做法	RDS.13	<a href="#">RDS.13</a>
AWS 基礎安全性最佳做法	RDS.14	<a href="#">RDS.14</a>
AWS 基礎安全性最佳做法	RDS.15	<a href="#">RDS.15</a>
AWS 基礎安全性最佳做法	RDS.16	<a href="#">RDS.16</a>
AWS 基礎安全性最佳做法	RDS.17	<a href="#">RDS.17</a>
AWS 基礎安全性最佳做法	RDS.18	<a href="#">RDS.18</a>
AWS 基礎安全性最佳做法	RDS.19	<a href="#">RDS.19</a>
AWS 基礎安全性最佳做法	RDS.20	<a href="#">RDS.20</a>
AWS 基礎安全性最佳做法	RDS.21	<a href="#">RDS.21</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	RDS.22	<a href="#">RDS.22</a>
AWS 基礎安全性最佳做法	RDS.23	<a href="#">RDS.23</a>
AWS 基礎安全性最佳做法	RDS.24	<a href="#">RDS.24</a>
AWS 基礎安全性最佳做法	RDS.25	<a href="#">RDS.25</a>
AWS 基礎安全性最佳做法	RDS.26	<a href="#">RDS.26</a>
AWS 基礎安全性最佳做法	RDS.27	<a href="#">RDS.27</a>
AWS 基礎安全性最佳做法	RDS.34	<a href="#">RDS.34</a>
AWS 基礎安全性最佳做法	RDS.35	<a href="#">RDS.35</a>
AWS 基礎安全性最佳做法	Redshift.1	<a href="#">Redshift.1</a>
AWS 基礎安全性最佳做法	Redshift.2	<a href="#">Redshift.2</a>
AWS 基礎安全性最佳做法	Redshift.3	<a href="#">Redshift.3</a>
AWS 基礎安全性最佳做法	Redshift.4	<a href="#">Redshift.4</a>
AWS 基礎安全性最佳做法	Redshift.6	<a href="#">Redshift.6</a>
AWS 基礎安全性最佳做法	Redshift.7	<a href="#">Redshift.7</a>
AWS 基礎安全性最佳做法	Redshift.8	<a href="#">Redshift.8</a>
AWS 基礎安全性最佳做法	Redshift.9	<a href="#">Redshift.9</a>
AWS 基礎安全性最佳做法	Redshift.10	<a href="#">Redshift.10</a>
AWS 基礎安全性最佳做法	香港路線	<a href="#">香港路線</a>



安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	S3.1	<a href="#">S3.1</a>
AWS 基礎安全性最佳做法	S3.2	<a href="#">S3.2</a>
AWS 基礎安全性最佳做法	S3.3	<a href="#">S3.3</a>
AWS 基礎安全性最佳做法	S3.4	<a href="#">S3.4</a>
AWS 基礎安全性最佳做法	S3.5	<a href="#">S3.5</a>
AWS 基礎安全性最佳做法	S3.6	<a href="#">S3.6</a>
AWS 基礎安全性最佳做法	S3.7	<a href="#">S3.7</a>
AWS 基礎安全性最佳做法	S3.8	<a href="#">S3.8</a>
AWS 基礎安全性最佳做法	S3.9	<a href="#">S3.9</a>
AWS 基礎安全性最佳做法	S3.11	<a href="#">S3.11</a>
AWS 基礎安全性最佳做法	S3.12	<a href="#">S3.12</a>
AWS 基礎安全性最佳做法	S3.13	<a href="#">S3.13</a>
AWS 基礎安全性最佳做法	S3.14	<a href="#">S3.14</a>
AWS 基礎安全性最佳做法	S3.15	<a href="#">S3.15</a>
AWS 基礎安全性最佳做法	S3.17	<a href="#">S3.17</a>
AWS 基礎安全性最佳做法	S3.19	<a href="#">S3.19</a>
AWS 基礎安全性最佳做法	S3.19	<a href="#">S3.20</a>
AWS 基礎安全性最佳做法	SageMaker.1	<a href="#">SageMaker.1</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	SageMaker.2	<a href="#">SageMaker.2</a>
AWS 基礎安全性最佳做法	SageMaker.3	<a href="#">SageMaker.3</a>
AWS 基礎安全性最佳做法	SecretsMa nager.1	<a href="#">SecretsManager.1</a>
AWS 基礎安全性最佳做法	SecretsMa nager.2	<a href="#">SecretsManager.2</a>
AWS 基礎安全性最佳做法	SecretsMa nager.3	<a href="#">SecretsManager.3</a>
AWS 基礎安全性最佳做法	SecretsMa nager.4	<a href="#">SecretsManager.4</a>
AWS 基礎安全性最佳做法	SNS.1	<a href="#">SNS.1</a>
AWS 基礎安全性最佳做法	SNS.2	<a href="#">SNS.2</a>
AWS 基礎安全性最佳做法	SQS.1	<a href="#">SQS.1</a>
AWS 基礎安全性最佳做法	SSM.1	<a href="#">SSM.1</a>
AWS 基礎安全性最佳做法	SSM.2	<a href="#">SSM.2</a>
AWS 基礎安全性最佳做法	SSM.3	<a href="#">SSM.3</a>
AWS 基礎安全性最佳做法	SSM.4	<a href="#">SSM.4</a>
AWS 基礎安全性最佳做法	StepFunctions.1	<a href="#">StepFunctions.1</a>
AWS 基礎安全性最佳做法	WAF.1	<a href="#">WAF.1</a>

安全標準	Audit Manager 支援的關鍵字 (Security Hub 中的標準控制項識別碼)	相關控制項文件 ( Security Hub 中對應的安全控制 ID )
AWS 基礎安全性最佳做法	WAF.2	<a href="#">WAF.2</a>
AWS 基礎安全性最佳做法	WAF.3	<a href="#">WAF.3</a>
AWS 基礎安全性最佳做法	WAF.4	<a href="#">WAF.4</a>
AWS 基礎安全性最佳做法	WAF.6	<a href="#">WAF.6</a>
AWS 基礎安全性最佳做法	WAF.7	<a href="#">WAF.7</a>
AWS 基礎安全性最佳做法	WAF.8	<a href="#">WAF.8</a>
AWS 基礎安全性最佳做法	WAF.10	<a href="#">WAF.10</a>
AWS 基礎安全性最佳做法	WAF.11	<a href="#">WAF.11</a>
AWS 基礎安全性最佳做法	WAF.12	<a href="#">WAF.12</a>

## 其他資源

- 若要尋找有關此資料來源類型之證據收集問題的說明，請參閱[我的評估不會從中收集合規性檢查證據 AWS Security Hub](#)。
- 若要使用此資料來源類型建立自訂控制項，請參閱[在中建立自訂控制項 AWS Audit Manager](#)。
- 若要建立使用自訂控制項的自訂架構，請參閱[在中建立自訂架構 AWS Audit Manager](#)。
- 若要將您的自訂控制項新增至現有的自訂架構，請參閱[編輯自訂架構 AWS Audit Manager](#)。

## AWS 支援的 API 呼叫 AWS Audit Manager

您可以使用 Audit Manager 擷取 AWS 環境的快照作為稽核的證據。建立或編輯自訂控制項時，您可以指定一或多個 AWS API 呼叫做為證據收集的資料來源對應。然後，Audit Manager 會對相關的項目進行 API 呼叫 AWS 服務，並為您的 AWS 資源收集組態詳細資料的快照集。

Audit Manager 會擷取 API 呼叫範圍內的每個資源組態快照，並轉換成證據。如此一來，每個資源都會獲得一個證據，而不是每個 API 呼叫使用一個證據。

例如，如果 `ec2_DescribeRouteTables` API 呼叫從五個路由表擷取組態快照，則單一 API 呼叫總共會獲得五個證據。每個證據都是個別路由表組態的快照。

## 主題

- [重點](#)
- [自訂控制項資料來源支援的 API 呼叫](#)
- [AWS License Manager 標準架構中使用的 API 呼叫](#)
- [其他資源](#)

## 重點

### 編頁 API 呼叫

許多人 AWS 服務 收集和存儲大量數據。因此，當 `list`、`describe`、或 `get` API 呼叫嘗試傳回您的資料時，可能會有很多結果。如果資料量太大而無法在單次回應中全部顯示，則可以透過編頁功能將結果分為更易於管理的部分。這會將結果劃分為資料的「分頁」，使回應更容易處理。

其中 [自訂控制項資料來源支援的 API 呼叫](#) 一些已分頁。這代表它們會先傳回部分結果，並要求後續請求傳回整個結果集。舉例來說，Amazon RDS [DescribeDBInstances](#) 單次作業最多可傳回 100 個執行個體，如需傳回下一頁結果，則需要後續請求。

自 2023 年 3 月 8 日起，Audit Manager 支援分頁 API 呼叫做為證據收集的資料來源。以前，如果使用分頁的 API 呼叫做為資料來源，則 API 回應中僅傳回您的資源子集（最多 100 個結果）。現在，Audit Manager 會多次呼叫分頁的 API 作業，並取得每個結果頁面，直至傳回所有資源為止。接下來，Audit Manager 會針對每個資源擷取組態快照集，並將其儲存為證據。由於您的完整資源集現在已在 API 回應中擷取，因此您可能會注意到 2023 年 3 月 08 日之後收集的證據量有所增加。

Audit Manager 會自動為您處理 API 呼叫分頁。如果您對使用分頁的 API 呼叫建立自訂控制項並作為資料來源，則不需要指定任何分頁參數。

## 自訂控制項資料來源支援的 API 呼叫

在自訂控制項中，您可以使用下列 API 呼叫中的任何一個作為資料來源。然後，Audit Manager 可以使用這些 API 呼叫來收集有關您使用 AWS 情況的證據。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">acm_GetAccountConfiguration</a>	收集與您 AWS 帳戶關聯的帳戶組態選項的快照。
<a href="#">acm_ListCertificates</a>	擷取憑證 ARN 和網域名稱的清單。
<a href="#">自動縮放 _ DescribeAutoScalingGroups</a>	收集有關 Auto Scaling 組的快照 AWS 帳戶。
<a href="#">備份 _ ListBackupPlans</a>	擷取您中所有使用中備份計畫的清單 AWS 帳戶。
<a href="#">基岩 _ GetModelInvocationLoggingConfiguration</a>	收集目前組態值的快照，以便在您 AWS 帳戶的。
<a href="#">雲前 _ ListDistributions</a>	擷取. 中所有發行版的清單 AWS 帳戶。
<a href="#">雲徑 _ DescribeTrails</a>	收集一或多個線索 (與您 AWS 帳戶的目前區域關聯) 的設定之快照。
<a href="#">雲徑 _ ListTrails</a>	檢索您的 AWS 帳戶。
<a href="#">雲觀察 _ DescribeAlerts</a>	收集用於您 AWS 帳戶的警報之組態快照。
<a href="#">配置 _ DescribeConfigRules</a>	檢索有關 AWS Config 規則的詳細信息。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">配置 _ DescribeDeliveryChannels</a>	收集您 AWS 帳戶中的交付管道之組態快照。
<a href="#">直接連接 _ DescribeDirectConnectGateways</a>	擷取所有 AWS Direct Connect 閘道的清單。
<a href="#">直接連接 _ DescribeVirtualGateways</a>	擷取 AWS 帳戶所擁有的虛擬私有閘道清單。
<a href="#">文件資料庫 _ DescribeCertificates</a>	收集您 AWS 帳戶的憑證清單。
<a href="#">文件描述 ClusterParameterGroups</a>	收集您 AWS 帳戶的 DBClusterParameterGroup 描述之清單。
<a href="#">docdb_DescribeDBInstances</a>	收集您 AWS 帳戶的已佈建 Amazon DynamoDB 執行個體之相關資訊。
<a href="#">雲觀察 _ DescribeAlerts</a>	收集有關您的 AWS 帳戶。
<a href="#">雲徑 _ DescribeTrails</a>	收集與您相關聯的一或多個軌跡的設定快照 AWS 帳戶。
<a href="#">動力 b_ DescribeTable</a>	<p>收集您 AWS 帳戶中 DynamoDB 資料表的組態快照。</p> <p>使用此 API 做為資料來源時，您不需要提供特定 DynamoDB 表格的名稱。相反地，Audit Manager 會使用 ListTables 作業來列出您的所有表格。然後，Audit Manager 會針對列出的每個表格執行 DescribeTable 作業，以產生該資源的證據。</p>
<a href="#">動力 b_ ListBackups</a>	擷取與您 AWS 帳戶關聯的 DynamoDB 備份清單。
<a href="#">動力 b_ ListTables</a>	擷取與您 AWS 帳戶 和目前端點關聯的所有資料表名稱的清單。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">ec2_DescribeAddresses</a>	收集彈性 IP 地址的快照。
<a href="#">ec2_DescribeCustomerGateways</a>	收集 VPN 客戶閘道的快照。
<a href="#">ec2_DescribeEgressOnlyInternetGateways</a>	收集僅限輸出網際網路閘道的快照。
<a href="#">ec2_DescribeFlowLogs</a>	收集流量日誌的快照。
<a href="#">ec2_DescribeInstances</a>	收集執行個體的快照。
<a href="#">ec2_DescribeInternetGateways</a>	收集網際網路閘道的快照。
<a href="#">ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations</a>	收集您的虛擬介面群組與本機閘道路由表之間的關聯說明 AWS 帳戶。
<a href="#">ec2_DescribeLocalGateways</a>	收集本機閘道的快照。
<a href="#">ec2_DescribeLocalGatewayVirtualInterfaces</a>	收集本機閘道虛擬介面的快照。
<a href="#">ec2_DescribeNATGateways</a>	收集 NAT 閘道的快照。
<a href="#">ec2_DescribeNetworkAcls</a>	收集網路 ACL 的快照。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">ec2_DescribeRouteTables</a>	收集路由表的快照。
<a href="#">ec2_DescribeSecurityGroups</a>	收集安全群組的快照。
<a href="#">ec2_DescribeSecurityGroupRules</a>	收集一或多個安全群組規則的快照。
<a href="#">ec2_DescribeTransitGateways</a>	收集運輸閘道的快照。
<a href="#">ec2_DescribeVolumes</a>	收集 VPC 端點的快照。
<a href="#">ec2_DescribeVpcs</a>	收集 VPC 的快照。
<a href="#">ec2_DescribeVpcEndpoints</a>	收集 VPC 端點的快照。
<a href="#">ec2_DescribeVpcEndpointConnections</a>	收集 VPC 端點連線到 VPC 端點服務的快照，包括任何等待您接受的端點。
<a href="#">ec2_DescribeVpcEndpointServiceConfigurations</a>	收集您 AWS 帳戶的 VPC 端點服務組態的快照集。
<a href="#">ec2_DescribeVpcPeeringConnections</a>	收集 VPN 連線的快照。
<a href="#">ec2_DescribeVpnConnections</a>	收集 VPN 連線的快照。
<a href="#">ec2_DescribeVpnGateways</a>	收集虛擬私有閘道的快照。



支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">ec2_GetEbsDefaultKmsKeyId</a>	為您 AWS 帳戶 目前區域中 AWS KMS key 的 EBS 加密收集預設快照。
<a href="#">ec2_GetEbsEncryptionByDefault</a>	說明是否在目前區域中為您的 AWS 帳戶 預設啟用 EBS 加密。
<a href="#">Ecs_DescribeClusters</a>	收集 ECS 叢集的快照。
<a href="#">eks_DescribeAddonVersions</a>	收集您附加元件版本的快照。
<a href="#">彈性_DescribeCacheClusters</a>	收集已佈建叢集的快照。
<a href="#">彈性_DescribeServiceUpdates</a>	收集 Amazon 服務更新的快照 ElastiCache。
<a href="#">彈性檔案系統_DescribeAccessPoints</a>	收 Amazon EFS 的 AWS 帳戶。
<a href="#">彈性檔案系統_DescribeFileSystems</a>	收集 Amazon EFS 檔案系統的快照。
<a href="#">彈性負載平衡v2_DescribeLoadBalancers</a>	收集您 AWS 帳戶的。
<a href="#">elasticloadbalancingv2_DescribeSSLPolicies</a>	收集您用於 SSL 交涉的政策快照。
<a href="#">彈性負載平衡v2_DescribeTargetGroups</a>	收集 ELB 目標群組的快照。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">彈性試管 _ ListSecurityConfigurations</a>	擷取您 AWS 帳戶可見的安全性組態清單，及其建立日期和時間，以及名稱。
<a href="#">活動資訊 _ ListConnections</a>	檢索您的 Amazon EventBridge 連接列表 AWS 帳戶。
<a href="#">活動資訊 _ ListEventBuses</a>	擷取您的 Amazon EventBridge 事件匯流排清單 AWS 帳戶，包括預設事件匯流排、自訂事件匯流排和合作夥伴事件匯流排。
<a href="#">活動資訊 _ ListEventSources</a>	擷取已與您 AWS 帳戶共用的合作夥伴事件來源清單。
<a href="#">活動資訊 _ ListRules</a>	檢索您的 Amazon EventBridge 規則列表。
<a href="#">火管 _ ListDeliveryStreams</a>	擷取交付串流的清單。
<a href="#">FSX _ DescribeFileSystems</a>	收集您 AWS 帳戶所擁有的檔案系統之快照。
<a href="#">守衛 _ ListDetectors</a>	<code>detectorIds</code> 為您的 Amazon GuardDuty 偵測器資源擷取清單。
<a href="#">iam _ GenerateCredentialReport</a>	產生 AWS 帳戶的憑證報告。
<a href="#">iam _ GetAccountPasswordPolicy</a>	收集您 AWS 帳戶的密碼政策之快照。
<a href="#">iam _ GetAccountSummary</a>	收集您 AWS 帳戶中 IAM 實體用量和 IAM 配額的快照。
<a href="#">iam _ ListGroups</a>	擷取 IAM 群組清單，這些群組與您的 AWS 帳戶。
<a href="#">我的身份證 ListOpen ConnectProviders</a>	擷取在您 AWS 帳戶中定義的 IAM OpenID Connect (OIDC) 供應商資源物件的清單。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">iam_ListPolicies</a>	擷取您 AWS 帳戶中可用的所有受管政策清單，包含您自己的客戶定義受管政策和所有 AWS 受管政策。
<a href="#">iam_ListRoles</a>	擷取 IAM 角色的清單，這些角色與您的 AWS 帳戶。
<a href="#">iam_ListSAMLProviders</a>	擷取在您 AWS 帳戶中 IAM 內定義的 SAML 供應商資源物件的清單。
<a href="#">iam_ListUsers</a>	擷取您中的 IAM 使用者清單 AWS 帳戶。
<a href="#">iam_MFA 设备 ListVirtual</a>	擷取您 AWS 帳戶中定義的虛擬 MFA 裝置清單。
<a href="#">卡夫卡_ListClusters</a>	擷取您的 AWS 帳戶
<a href="#">卡夫卡_ListKafka Versions</a>	擷取您 AWS 帳戶中 Apache Kafka 版本物件的清單。
<a href="#">運動_ListStreams</a>	擷取 Kinesis 資料串流的清單。
<a href="#">kms_GetKeyPolicy</a>	<p>Audit Manager 會使用此 API 來收集您 AWS KMS keys 中 AWS 帳戶的金鑰政策之快照。</p> <p>當您使用此 API 作為資料來源時，您不需要提供特定的名稱 AWS KMS key。相反地，Audit Manager 會使用 ListKeys 作業來列出您所有的 KMS 金鑰。然後，Audit Manager 會針對列出的每個 KMS 金鑰執行 GetKeyPolicy 作業，以產生該資源的證據。</p>
<a href="#">kms_GetKeyRotationStatus</a>	<p>Audit Manager 使用此 API 來收集您 AWS KMS keys 的 AWS 帳戶。</p> <p>當您使用此 API 作為資料來源時，您不需要提供特定的名稱 AWS KMS key。相反地，Audit Manager 會使用 ListKeys 作業來列出您所有的 KMS 金鑰。然後，Audit Manager 會針對列出的每個 KMS 金鑰執行 GetKeyRotationStatus 作業，以產生該資源的證據。</p>
<a href="#">kms_ListKeys</a>	擷取 AWS KMS keys 中的清單 AWS 帳戶。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">羊巴達 _ ListFunctions</a>	使用每個函數的特定版本組態 AWS 帳戶，擷取您中的 Lambda 函數清單。
<a href="#">rds_DescribeDatabaseDBClusters</a>	收集您的. 中現有 Amazon Aurora 資料庫叢集和異地同步備份資料庫叢集的 AWS 帳戶快照。
<a href="#">rds_DescribeDBInstances</a>	收集您 AWS 帳戶中已佈建 RDS 執行個體的快照。
<a href="#">rds_DescribeDBInstanceAutomatedBackups</a>	收集您中目前和已刪除執行個體的備份快照 AWS 帳戶。
<a href="#">rds_DescribeDBSecurityGroups</a>	收集您 SecurityGroups 的 AWS 帳戶。
<a href="#">紅色的 _ DescribeClusters</a>	收集您 AWS 帳戶中已佈建 Amazon Redshift 叢集的快照。
<a href="#">s3_GetBucketEncryption</a>	<p>收集顯示 S3 儲存貯體預設加密組態的快照。</p> <p>使用此 API 做為資料來源時，您不需要提供特定的 S3 儲存貯體的名稱。相反地，Audit Manager 會使用 ListBuckets 作業來列出您的所有儲存貯體。然後，Audit Manager 會針對列出的每個儲存貯體執行 GetBucketEncryption 作業，以產生該資源的證據。</p> <p>Audit Manager 只能 AWS 區域 為在您的評估中建立的值區提供加密狀態。如果您需要查看跨多個 S3 儲存貯體的加密狀態 AWS 區域，建議您在每個擁有 S3 儲存貯體的 AWS 區域 位置建立評估。</p>
<a href="#">s3_ListBuckets</a>	擷取 AWS 帳戶. 中的 S3 儲存貯體清單
<a href="#">下垂機 _ ListAlgorithms</a>	擷取. 中的機器學習演算法清單 AWS 帳戶。
<a href="#">下垂機 _ ListDomains</a>	擷取您的網域清單 AWS 帳戶。

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">下垂機 _ ListEndpoints</a>	擷取. 中的端點清單 AWS 帳戶。
<a href="#">下垂機 _ ListEndpointConfigs</a>	擷取 AWS 帳戶. 中的端點組態清單
<a href="#">下垂機 _ ListFlowDefinitions</a>	擷取. 中的流程定義清單 AWS 帳戶。
<a href="#">下垂機 _ ListHumanTaskUis</a>	擷取. 中的人工作業介面清 AWS 帳戶單
<a href="#">下垂機 _ ListLabelingJobs</a>	擷取您中的標籤工作清單 AWS 帳戶。
<a href="#">下垂機 _ ListModels</a>	擷取您中的模型清單 AWS 帳戶。
<a href="#">下垂機 _ ListModelBiasJobDefinitions</a>	擷取您中的模型偏差工作定義清單 AWS 帳戶。
<a href="#">下垂機 _ ListModelCards</a>	擷取您的 AWS 帳戶.
<a href="#">下垂機 _ ListModelQualityJobDefinitions</a>	在中擷取模型品質監視工作定義的清單 AWS 帳戶。
<a href="#">下垂機 _ ListMonitoringAlerts</a>	擷取指定監督排程的警示清單。
<a href="#">下垂機 _ ListMonitoringSchedules</a>	擷取. 中所有監視排程的清單 AWS 帳戶。
<a href="#">下垂機 _ ListTrainingJobs</a>	擷取您中的訓練工作清單 AWS 帳戶。
<a href="#">下垂機 _ ListUserProfile</a>	擷取您的 AWS 帳戶.

支援的 API 呼叫	Audit Manager 如何使用此 API 收集證據
<a href="#">秘書經理 _ ListSecrets</a>	擷取儲存在您的密碼清單 AWS 帳戶，不包括標記為要刪除的密碼。
<a href="#">sns_ ListTopics</a>	擷取您中的 SNS 主題清單 AWS 帳戶。
<a href="#">平方米 _ ListQueue S</a>	擷取您 AWS 帳戶中的 SQS 佇列清單。
<a href="#">WAF-區域 _ ListWebAcls</a>	為您擷取的 <a href="#">WebACLSummary</a> 件清單。AWS 帳戶
<a href="#">WAF-區域 _ ListRules</a>	擷取您的 <a href="#">RuleSummary</a> 物件清單 AWS 帳戶。
<a href="#">waf_ ListRuleGroups</a>	擷取您中規則群組的 <a href="#">RuleGroupSummary</a> 物件清單 AWS 帳戶。
<a href="#">waf_ ListRules</a>	擷取您的 <a href="#">RuleSummary</a> 物件清單 AWS 帳戶。
<a href="#">waf_ ListWebAcls</a>	為您擷取的 <a href="#">WebACLSummary</a> 件清單。AWS 帳戶

## AWS License Manager 標準架構中使用的 API 呼叫

在 [AWS License Manager](#) 標準架構中，Audit Manager 會使用自訂活動呼叫 `GetLicenseManagerSummary` 來收集證據。此活動會呼叫下列三個 License Manager API：

- [ListLicenseConfigurations](#)
- [ListAssociationsForLicenseConfiguration](#)
- [ListUsageForLicenseConfiguration](#)

然後，傳回的資料會轉換成證據，並附加至評估中的相關控制項。

### 範例

假設您使用兩個授權產品（2017 年版 SQL 服務和 Oracle 資料庫企業版）。首先，`GetLicenseManagerSummary` 活動會呼叫 [ListLicenseConfigurations](#) API，該 API 會提供您帳戶中授權設定的詳細資料。接下來，它通過調用 [ListUsageForLicenseConfiguration](#) 和為每個許可證配

置添加其他上下文數據 [ListAssociationsForLicenseConfiguration](#)。最後，它將授權組態資料轉換為證據，並將其附加到架構中的對應控制項 (4.5 - 2017 SQL 伺服器客戶管理授權和 3.0.4 - Oracle 資料庫企業版客戶管理授權)。

如果您使用的授權產品未涵蓋架構中任何控制項，則該授權組態資料會附加至下列控制項的證據：5.0 - 其他授權的客戶管理授權。

## 其他資源

- 若要尋找有關此資料來源類型之證據收集問題的說明，請參閱 [我的評估不會收集 AWS API 呼叫的組態資料證據](#)。
- 若要使用此資料來源類型建立自訂控制項，請參閱 [在中建立自訂控制項 AWS Audit Manager](#)。
- 若要建立使用自訂控制項的自訂架構，請參閱 [在中建立自訂架構 AWS Audit Manager](#)。
- 若要將您的自訂控制項新增至現有的自訂架構，請參閱 [編輯自訂架構 AWS Audit Manager](#)。

## AWS CloudTrail 支援的事件名稱 AWS Audit Manager

您可以使用 Audit Manager 擷取 AWS CloudTrail [管理事件](#)和[全域服務事件](#)，作為稽核的證據。建立或編輯自訂控制項時，您可以指定一或多個 CloudTrail 事件名稱做為證據收集的資料來源對應。然後，Audit Manager 會根據您選擇的關鍵字篩選 CloudTrail 記錄檔，並將結果匯入為使用者活動證據。

### Note

Audit Manager 僅擷取管理事件和全域服務事件。資料事件和洞見事件無法作為證據。如需有關不同類型 CloudTrail 事件的詳細資訊，請參閱《AWS CloudTrail 使用指南》中的 [CloudTrail 概念](#)。

除了上述情況之外，Audit Manager 不支援下列 CloudTrail 事件：

- kms\_GenerateDataKey
- kms\_Decrypt
- sts\_AssumeRole
- 动力视频 \_ GetDataEndpoint
- 动力视频 \_ GetSignalingChannelEndpoint

- 动力视频 \_ DescribeSignalingChannel
- 动力视频 \_ DescribeStream

自 2023 年 5 月 11 日起，Audit Manager 不再支援唯讀 CloudTrail 事件做為證據收集的關鍵字。我們總共刪除了 3,135 個唯讀關鍵字。由於客戶和 AWS 服務 兩者都對 API 進行讀取呼叫，因此唯讀事件會很雜亂。因此，唯讀關鍵字會收集許多不可靠或與稽核無關的證據。唯讀關鍵字包括 ListDescribe、和 Get API 呼叫 (例如 [GetObject](#) , [ListBuckets](#)適用於 Amazon S3)。如果您使用這些關鍵字之一來收集證據，則無需執行任何作業。系統已自動從 Audit Manager 主控台和您的評估中移除關鍵字，而且不會再為這些關鍵字收集證據。

## 其他資源

- 若要尋找有關此資料來源類型之證據收集問題的說明，請參閱[我的評估不會從 AWS CloudTrail中收集使用者活動證據](#)。
- 若要使用此資料來源類型建立自訂控制項，請參閱[在中建立自訂控制項 AWS Audit Manager](#)。
- 若要建立使用自訂控制項的自訂架構，請參閱[在中建立自訂架構 AWS Audit Manager](#)。
- 若要將您的自訂控制項新增至現有的自訂架構，請參閱[編輯自訂架構 AWS Audit Manager](#)。



# 使用建議 AWS Audit Manager 的設定進行設定

開始使用 Audit Manager 之前，請務必完成下列設定工作。

本章將引導您完成必要條件、帳戶設定、使用者權限，以及啟用和設定 Audit Manager 具有建議功能和整合的必要步驟。完成這些工作後，您就可以使用 Audit Manager，並開始簡化稽核和合規工作。

## 內容

- [設定的先決條件 AWS Audit Manager](#)
  - [註冊一個 AWS 帳戶](#)
  - [建立具有管理權限的使用者](#)
  - [新增存取和啟用 Audit Manager 所需的許可](#)
  - [後續步驟](#)
- [啟用 AWS Audit Manager](#)
  - [必要條件](#)
  - [程序](#)
  - [後續步驟](#)
- [啟用建議的功能 AWS 服務 和 AWS Audit Manager](#)
  - [重點](#)
  - [設定建議的 Audit Manager 功能](#)
  - [設定與其他建議的整合 AWS 服務](#)
  - [後續步驟](#)

## 設定的先決條件 AWS Audit Manager

在使用之前 AWS Audit Manager，您必須確定已正確設定 AWS 帳戶 和使用者權限。

本頁概述建立 AWS 帳戶 (如有需要)、設定管理使用者，以及授與存取和啟用 Audit Manager 所需權限的必要步驟。

## 任務

1. [註冊一個 AWS 帳戶](#)
2. [建立具有管理權限的使用者](#)

### 3. [新增存取和啟用 Audit Manager 所需的許可](#)

#### Important

如果您已使用 AWS 和 IAM 進行設定，則可以略過任務 1 和 2。但是，您必須完成任務 3，以確保您具有設定 Audit Manager 所需的權限。

## 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建 AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

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

## 建立具有管理權限的使用者

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

保護您的 AWS 帳戶根使用者

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

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

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

## 建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

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

## 以具有管理權限的使用者身分登入

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

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

## 指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

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

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

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

## 新增存取和啟用 Audit Manager 所需的許可

您必須向使用者授予啟用 Audit Manager 所需的許可。對於需要稽核管理員完整存取權限的使用者，請使用受[AWSAuditManagerAdministratorAccess](#)管理的策略。這是您的中可用的 AWS 受管理策略 AWS 帳戶，它是 Audit Manager 員的建議策略。

**i** Tip

作為安全性最佳做法，建議您開始使用 AWS 受管理的原則，然後轉向最低權限的權限。AWS 受管理的原則會授與許多常見使用案例的權限。但請記住，由於 AWS 受管政策可供所有 AWS 客戶使用，因此他們可能不會針對您的特定使用案例授與最低權限權限。因此，我們建議您定義使用案例的[客戶管理政策](#)，以便進一步減少許可。如需詳細資訊，請參閱 AWS Identity and Access Management IAM 使用者指南中的[AWS 受管政策](#)。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 [建立權限合集](#) 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南 的 [為第三方身分提供者 \(聯合\) 建立角色](#) 中的指示進行操作。

- IAM 使用者：

- 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 [為 IAM 使用者建立角色](#) 中的指示進行操作。
- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的 [新增許可到使用者 \(主控台\)](#) 中的指示。

## 後續步驟

既然您已設定 AWS 帳戶 並授與必要權限，就可以啟用 Audit Manager 了。如需 step-by-step 指示，請參閱[啟用 AWS Audit Manager](#)。

## 啟用 AWS Audit Manager

現在您已完成設定 Audit Manager 的先決條件，您可以在 AWS 環境中啟用該服務。

在此頁面上，您將學習如何使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager 理員 API 啟用稽核管理員。選擇最適合您需求的方法，然後依照對應的步驟啟動並執行 Audit Manager。

## 必要條件

請確保您已完成中描述的所有任務[設定的先決條件 AWS Audit Manager](#)。

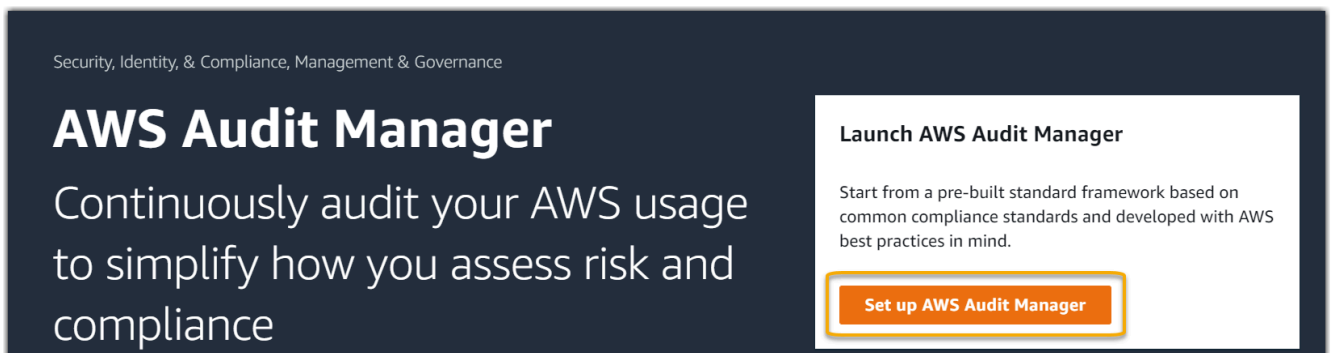
## 程序

您可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來啟用 Audit Manager。  
AWS Management Console

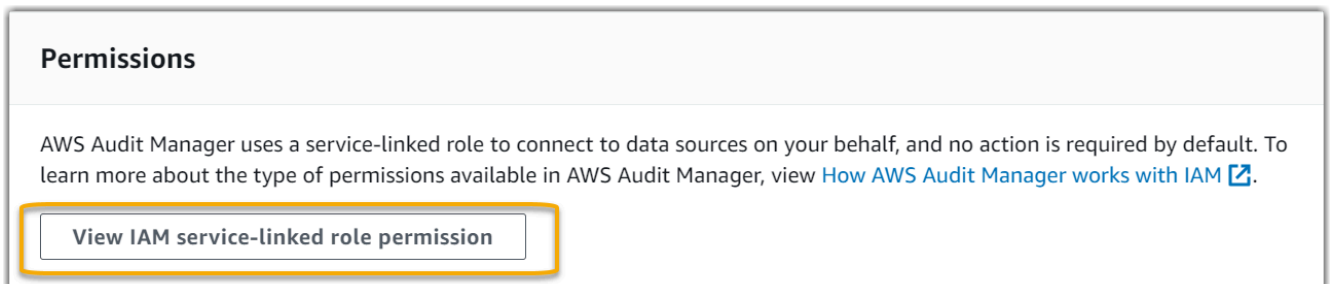
Audit Manager console

如需使用主控台來啟用 Audit Manager

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 使用 IAM 身分的憑證登入。
3. 選擇 Set up (設定) AWS Audit Manager。



4. 在權限中，無須採取任何動作。這是因為 Audit Manager 使用[服務連結角色](#)代表您連線到資料來源。您可以選擇查看 IAM 服務連結角色權限，以查看服務連結角色。



5. 在 [資料加密] 下，預設選項是讓 Audit Manager 建立和管理，以安全地儲存資料。AWS KMS key

### Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)

如果您想要使用自己的客戶管理金鑰來加密 Audit Manager 中的資料，請選取自訂加密設定 (進階) 旁邊的核取方塊。然後，您可選擇現有 KMS 金鑰或 [建立新的金鑰](#)。

### Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)  
To use the default key, clear this option.

Choose an AWS KMS key  
This key will be used for encryption instead of the default key.

- (選擇性) 如果您希望 Audit Manager 針對多個帳戶執行評估，您可以在委派管理員-選擇性下指定委派管理員帳戶。如需詳細資訊和建議事項，請參閱[啟用和設定 AWS Organizations \(選擇性\)](#)。

### Delegated administrator - optional

For AWS Audit Manager to support multiple accounts in your organization, you must specify a delegated administrator. Use this setting to add or remove the delegated AWS Audit Manager administrator for your organization. [Learn more](#)

Delegated administrator account ID

- (選用) 在 AWS Config — 選用底下，我們建議您啟 AWS Config 用最佳體驗。這可讓 Audit Manager 使用 AWS Config 規則產生證據。如需指示和建議的設定，請參閱[啟用和設定 AWS Config \(選擇性\)](#)。

### AWS Config - optional

Allow AWS Audit Manager to access [AWS Config](#) and generate evidence from AWS Config rules. Enabling AWS Config incurs charges.

Enable AWS Config 

- (選擇性) 在 Security Hub — 選擇性部分中，我們建議您啟用 Security Hub 以獲得最佳體驗。這可讓 Audit Manager 使用 Security Hub 檢查產生證據。如需指示和建議的設定，請參閱[啟用和設定 AWS Security Hub \(選擇性\)](#)。

### Security Hub - optional

Allow AWS Audit Manager to access [Security Hub](#) and generate evidence from security findings. Enabling Security Hub incurs charges.

Enable Security Hub 

- 選擇 **完成設定** 以完成設定程序。

Complete setup

## AWS CLI

若要使用啟用 Audit Manager AWS CLI

在命令列中，使用下列設定參數執行[註冊帳戶](#)命令：

- `--kms-key`(選擇性) — 使用此參數可使用您自己的客戶管理金鑰來加密 Audit Manager 資料。如果您未在此處指定選項，Audit Manager 會代表您建立和管理 AWS KMS key 資料的安全儲存。
- `--delegated-admin-account`(選擇性) — 使用此參數可為 Audit Manager 指定組織的委派管理員帳戶。如果您未在此處指定選項，則不會註冊委派管理員。

輸入範例 ( 用自己的資訊替換##### )：

```
aws auditmanager register-account \
```

```
--kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
--delegated-admin-account 111122224444
```

輸出範例：

```
{  
  "status": "ACTIVE"  
}
```

若要取得有關 AWS CLI 和安裝 AWS CLI 工具的更多資訊，請參閱《AWS Command Line Interface 使用指南》中的以下內容。

- [AWS 命令列介面使用者指南](#)
- [取得設定 AWS Command Line Interface](#)

## Audit Manager API

如需使用 Audit Manager API 啟用 Audit Manager

使用具有下列設定參數的 [RegisterAccount](#) 作業：

- [KMSKey](#) (選擇性) — 使用此參數可使用您自己的客戶管理金鑰來加密 Audit Manager 資料。如果您未在此處指定選項，Audit Manager 會代表您建立和管理 AWS KMS key 資料的安全儲存。
- [delegatedAdminAccount](#) (選擇性) — 使用此參數可為稽核管理員指定組織的委派管理員帳戶。如果您未指定，則不會註冊委派管理員。

輸入範例 ( 用自己的資訊替換##### )：

```
{  
  "kmsKey": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
  "delegatedAdminAccount": "111122224444"  
}
```

輸出範例：

```
{
```



```
"status": "ACTIVE"  
}
```

## 後續步驟

啟用 Audit Manager 之後，我們建議您設定一些建議的功能和整合，以獲得最佳體驗。如需詳細資訊，請參閱 [啟用建議的功能 AWS 服務 和 AWS Audit Manager](#)。

## 啟用建議的功能 AWS 服務 和 AWS Audit Manager

現在，您已經啟用了 AWS Audit Manager，是時候設置推薦的功能和集成以充分利用該服務。

### 重點

為了在 Audit Manager 中獲得最佳體驗，建議您設定下列功能並啟用下列 AWS 服務。

#### 任務

- [設定建議的 Audit Manager 功能](#)
- [設定與其他建議的整合 AWS 服務](#)
  - [啟用和設定 AWS Config \(選擇性\)](#)
  - [啟用和設定 AWS Security Hub \(選擇性\)](#)
  - [啟用和設定 AWS Organizations \(選擇性\)](#)

## 設定建議的 Audit Manager 功能

在您啟用 Audit Manager 之後，建議您啟用證據搜尋工具功能。

[證據搜尋工具](#)提供了一種在 Audit Manager 之中搜尋證據的強大方法。您可以使用證據搜尋工具快速查詢證據，不須一頭栽進證據資料夾，想辦法找出您要查找的內容。如果您以委派管理員的身分使用證據搜尋工具，您可以在組織中的所有成員帳戶中搜尋證據。

使用篩選條件和分組的組合，您可以逐步縮小搜尋查詢的範圍。例如，如果您想要系統健全狀況的高階檢視，請擴大搜尋範圍，並依據評估、日期範圍和資源合規性進行篩選。如果您的目標是修復特定資源，則可以縮小搜尋範圍，以針對特定控制項或資源 ID 的證據作為目標。定義篩選條件後，您可以先分組並預覽相符的搜尋結果，然後再建立評估報告。

## 設定與其他建議的整合 AWS 服務

為了在 Audit Manager 中獲得最佳體驗，我們強烈建議您啟用下列項目 AWS 服務：

- AWS Organizations— 您可以使用 Organizations 對多個帳戶執行 Audit Manager 評估，並將證據合併到委派管理員帳戶中。
- AWS Security Hub和 AWS Config— 啟用這些功能時 AWS 服務，它們可以用作 Audit Manager 評估中控制項的資料來源類型。然後，Audit Manager 可以直接從這些服務報告合規檢查的結果。

### Important

啟用 AWS Config、Security Hub 和 Organizations 是選擇性建議。不過，如果您確實啟用這些服務，則需要進行下列設定。

### 啟用和設定 AWS Config ( 選擇性 )

Audit Manager 中的許多控制項都用 AWS Config 作資料來源類型。若要支援這些控制項，您必須在每個已啟用 Audit Manager AWS 區域的所有帳號 AWS Config 上啟用。如果 Audit Manager 嘗試收集用 AWS Config 作資料來源類型之控制項的證據，且未啟用相關 AWS Config 規則，則不會收集這些控制項的證據。

Audit Manager 不會 AWS Config 為您管理。您可以按照以下步驟啟用 AWS Config 和配置其設定。

### Important

啟用 AWS Config 是選擇性的建議。但是，如果啟用 AWS Config，則需要以下設定。

### 要 AWS Config 與 Audit Manager 整合的工作

- [步驟 1：啟用 AWS Config](#)
- [步驟 2：AWS Config 設定要與 Audit Manager 搭配使用的設定](#)

### 步驟 1：啟用 AWS Config

您可以使 AWS Config 用 AWS Config 控制台或 API 啟用。如需指示，請參閱AWS Config 開發人員指南中的[AWS Config入門](#)。

## 步驟 2：AWS Config 設定要與 Audit Manager 搭配使用的設定

啟用之後 AWS Config，請務必[同時針對與稽核相關的AWS Config 規範標準啟用規則或部署一致性套件](#)。此步驟可確保 Audit Manager 可以針對您啟用的 AWS Config 規則匯入調查結果。

啟用 AWS Config 規則後，建議您檢閱該規則的參數。然後，您應該根據所選合規性架構的要求來驗證這些參數。如果需要，您可以[更新 AWS Config 中的規則參數](#)，確保其符合架構需求。這將有助於確保您的評估為該給定架構收集正確的合規檢查證據。

例如，假設您正在為 CIS v1.2.0 建立評估。此架構包含一個名為 [1.4 — 確保存取金鑰每 90 天或更短的時間輪換一次](#)的控制項。在中 AWS Config，[access-keys-rotated](#)規則具有預設值為 90 天的maxAccessKeyAge參數。因此，該規則符合控制項的需求。如果您不使用預設值，請確保您使用的值等於或大於 CIS v1.2.0 的 90 天要求。

您可以在 [AWS Config 文件](#)中找到每個受管規則的預設參數詳細資訊。如需有關如何配置規則的指示，請參閱[使用 AWS Config 受管規則](#)。

### 啟用和設定 AWS Security Hub（選擇性）

Audit Manager 中的許多控制項會使用 Security Hub 做為資料來源類型。若要支援這些控制項，您必須在每個已啟用 Audit Manager 的區域中的所有帳戶上啟用 Security Hub。如果 Audit Manager 嘗試收集使用 Security Hub 做為資料來源類型之控制項的證據，且未啟用相關的 Security Hub 標準，則不會針對這些控制項收集任何證據。

Audit Manager 不會為您管理 Security Hub。您可以按照以下步驟啟用 Security Hub 並配置其設定。

#### Important

啟用 Security Hub 是選擇性建議。不過，如果您確實啟用 Security Hub，則需要下列設定。

### 要 AWS Security Hub 與 Audit Manager 整合的工作

- [步驟 1：啟用 AWS Security Hub](#)
- [步驟 2：設定您的 Security Hub 設定，以便與 Audit Manager 搭配使用](#)
- [步驟 3：設定組 Organizations 的「組織」設定](#)

## 步驟 1：啟用 AWS Security Hub

您可以使用主控台或 API 以啟用 Security Hub。如需指示，請參閱AWS Security Hub 使用者指南中的[設定 AWS Security Hub](#)。

## 步驟 2：設定您的 Security Hub 設定，以便與 Audit Manager 搭配使用

在您可以啟用 Security Hub 後，請確認執行下列作業：

- [啟用 AWS Config 和設定資源記錄](#) — Security Hub 使用服務連結 AWS Config 規則來執行控制項的大部分安全性檢查。若要支援這些控制項，AWS Config 必須啟用並設定為記錄您在每個已啟用標準中啟用之控制項所需的資源。
- [啟用所有安全標準](#) — 此步驟可確保「Audit Manager」可以針對所有支援的符合性標準匯入發現項
- [開啟 Security Hub 的合併控制項調查結果設定](#) - 如果您在 2023 年 2 月 23 日或之後啟用 Security Hub，則預設會開啟此設定。

### Note

當您啟用合併的調查結果時，Security Hub 會針對每個安全檢查產生單一調查結果 (即使跨多個標準使用相同的檢查也是如此)。每個 Security Hub 調查結果都會做為 Audit Manager 中一項獨立資源評估來收集。因此，合併的調查結果會導致 Audit Manager 針對 Security Hub 調查結果執行的獨立資源評估總計減少。因此，使用合併的調查結果通常有效降低 Audit Manager 使用成本。如需有關使用 Security Hub 做為資料來源類型的詳細資訊，請參閱[AWS Security Hub 支援的控制項 AWS Audit Manager](#)。如需 Audit Manager 定價的詳細資訊，請參閱[AWS Audit Manager 定價](#)。

## 步驟 3：設定組 Organizations 的「組織」設定

如果您使用 AWS Organizations 並且想要從您的成員帳戶收集 Security Hub 證據，則還必須在 Security Hub 中執行下列步驟。

設定您組織的 Security Hub 設定

1. 請登入 AWS Management Console 並開啟 AWS Security Hub 主控台，[網址為 https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/)。
2. 使用您的 AWS Organizations 管理帳戶，將帳戶指定為 Security Hub 的委派系統管理員。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的[指定 Security Hub 管理員帳戶](#)。

**Note**

確認您在 Security Hub 中使用的委派管理員帳戶與您在 Audit Manager 中使用的帳戶相同。

3. 使用您的 Organizations 委派管理員帳戶，移至 設定、帳戶，選取所有帳戶，然後選取 自動註冊 將其新增為成員。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的[啟用組織中的成員帳戶](#)。
4. AWS Config 為組織的每個成員帳戶啟用。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的[啟用組織中的成員帳戶](#)。
5. 為組織的每個成員帳戶啟用 PCI DSS 安全標準。C AWS IS 基準標準和基 AWS 礎最佳做法標準已預設啟用。如需詳細資訊，請參閱AWS Security Hub 使用者指南中的[啟用安全標準](#)。

### 啟用和設定 AWS Organizations (選擇性)

Audit Manager 透過與整合支援多個帳戶 AWS Organizations。Audit Manager 可以對多個帳戶執行評估，並將證據合併到委派管理員帳戶中。委派管理員擁有建立及管理以組織做為信任區域之 Audit Manager 資源的許可。只有管理帳戶可以指定委派管理員。

**Important**

啟用 AWS Organizations 是選擇性的建議。但是，如果啟用 AWS Organizations，則需要以下設定。

### 要 AWS Organizations 與 Audit Manager 整合的工作

- [步驟 1：建立或加入組織](#)
- [步驟 2：啟用您組織中的所有功能](#)
- [步驟 3：為 Audit Manager 指定委派管理員](#)

#### 步驟 1：建立或加入組織

如果您 AWS 帳戶 不是組織的一部分，您可以建立或加入組織。如需指示，請參閱AWS Organizations 使用者指南中的[建立和管理組織](#)。

## 步驟 2：啟用您組織中的所有功能

下一步，必須啟用您組織中的所有功能。如需指示，請參閱AWS Organizations 使用者指南中的[啟用組織中的所有功能](#)。

## 步驟 3：為 Audit Manager 指定委派管理員

建議您使用 Organizations 管理帳戶啟用 Audit Manager 管理員，然後指定委派管理員。之後，您可以使用委派管理員帳戶登入並執行評估。根據最佳實務，建議您僅使用委派管理員帳戶來建立評估，而不是使用管理帳戶。

若要在啟用稽核管理員之後新增或變更委派的管理員，請參閱[新增委派管理員](#)和[變更委派管理員](#)。

## 後續步驟

現在，您已經使用建議的設定設定設定來設定稽核管理員，就可以開始使用該服務了。

- 若要開始進行第一次評估，請參閱[稽核擁有者教學課程：建立評估](#)。
- 若要在 future 更新您的設定，請參閱[檢閱及設定您的 AWS Audit Manager 設定](#)。

# 開始使用 AWS Audit Manager

您可以使用本節中的自學 step-by-step 課程來瞭解如何使用執行工作 AWS Audit Manager。

## Tip

以下教學課程按受眾進行分類。根據您身為稽核擁有者或委派代表的角色不同，選擇適合您的教學課程。

- 稽核擁有者是負責建立及管理評估的 Audit Manager 使用者。在商業世界中，稽核擁有者通常是治理、風險管理和法規遵循 (GRC) 專業人員。不過，在 Audit Manager 的前後關聯中，SecOps 或 DevOps 專案團隊的個人也可能會假設稽核擁有者的使用者角色。稽核擁有者可以向主題專家 (也稱為委派代表) 要求協助，以檢閱特定控制項並驗證證據。稽核擁有者必須要有必要授權，才可管理評估。
- 委派代表是具有專業技術或業務專業知識的主題專家。雖然他們不擁有或管理稽核管理員評估，但他們仍然可以對其做出貢獻。委派代表協助稽核擁有者完成任務，例如驗證屬於其專業領域的控制項的證據。委派代表在 Audit Manager 中具有有限的權限。這是因為稽核擁有者委派特定控制集以供檢閱，而不是委派整個評估。

如需有關這些角色和其他 Audit Manager 概念的詳細資訊，請參閱本指南的[audit owner](#)和[理解 AWS Audit Manager 概念和術語](#)節 [delegate](#) 中的。

如需每個角色建議 IAM 授權的詳細資訊，請參閱 [中使用者角色的建議政策 AWS Audit Manager](#)。

## Audit Manager 教學

### [建立評估](#)

對象：稽核擁有者

概觀：按照 step-by-step 說明創建您的第一個評估並快速啟動和運行。本教學課程將逐步引導您如何使用標準架構建立評估，並開始自動收集證據。

### [檢閱控制集](#)

對象：委派代表

概觀：檢閱屬於您專業領域的控制項的證據，以協助稽核擁有者。瞭解如何檢閱控制集及其相關證據、新增註解、上傳證據，以及更新控制項的狀態。

## 稽核擁有者教學課程：建立評估

本自學課程提供的簡介 AWS Audit Manager。在本自學課程中，您將使用建立評估 [AWS Audit Manager 示例框架](#)。藉由建立評估，您可以啟動該架構中控制項的持續自動化證據收集程序。

### Note

AWS Audit Manager 協助收集與驗證符合特定合規性框架和法規相關的證據。不過，這不會評估您的合規狀態。AWS Audit Manager 因此，透過收集的證據可能不包含稽核所需的所有有關您 AWS 使用情況的資訊。AWS Audit Manager 不是法律顧問或合規專家的替代品。

## 必要條件

開始此自學課程之前，請確定您符合下列條件：

- 您已完成 [使用建議 AWS Audit Manager 的設定進行設定](#) 中描述的所有先決條件。您必須使用 AWS 帳戶和 AWS Audit Manager 主控台才能完成本教學課程。
- 您的 IAM 身分會被授與適當的授權，以便在 AWS Audit Manager 中建立和管理評估。授與這些權限的兩個建議政策是 [授予使用者 AWS Audit Manager 的完整管理員存取權](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。
- 您對 Audit Manager 的術語和功能已經很熟悉了。如需一般概觀，請參閱 [什麼是 AWS Audit Manager ?](#) 和 [理解 AWS Audit Manager 概念和術語](#)。

## 程序

### 任務

- [步驟 1：指定評估詳細資訊](#)
- [步驟 2：AWS 帳戶 在範圍內指定](#)
- [步驟 3：指定稽核擁有者](#)
- [步驟 4：檢閱和建立](#)



## 步驟 1：指定評估詳細資訊

第一步，請選取架構並提供評估的基本資訊。

### 指定評估詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 選擇啟動 AWS Audit Manager。
3. 在畫面頂端的綠色橫幅中，選擇 [從架構開始]。
4. 選擇您要的架構，然後選擇從架構建立評估。在本教學課程中，請使用 AWS Audit Manager 範例架構。
5. 在評估名稱下，輸入評估的名稱。
6. (選擇性) 在評估說明下，輸入評估的說明。
7. 在評估報告目標下，選擇您要儲存評估報告的 S3 儲存貯體。
8. 在 [架構] 下，確認已選取 [AWS Audit Manager 範例架構]。
9. (選擇性) 在「標籤」下，選擇「新增標籤」，將標籤與您的評估產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的，在搜尋此評估時，可用作搜尋條件。
10. 選擇下一步。

## 步驟 2：AWS 帳戶 在範圍內指定

接下來，指定您要包含在評估範圍中的 AWS 帳戶。

AWS Audit Manager 與整合 AWS Organizations，因此您可以跨多個帳戶執行 Audit Manager 員評估，並將證據合併到委派的管理員帳戶中。如需在 Audit Manager 中啟用組織 (如果尚未啟用)，請參閱本指南設定頁面上的 [啟用和設定 AWS Organizations \(選擇性\)](#)。

### Note

Audit Manager 在評估範圍內最多可支援 200 個帳戶。如果您嘗試包含超過 200 個帳戶，則評估建立可能會失敗。

### 指定範圍內帳戶

1. 在下方 AWS 帳戶，選 AWS 帳戶 取您要包含在評估範圍中的項目。

- 如果您在 Audit Manager 中啟用了 Organizations，則會列出多個帳戶。
- 如果您未在 Audit Manager 中啟用 Organizations，則只會列出您目前的帳戶。

## 2. 選擇下一步。

### 步驟 3：指定稽核擁有者

在此步驟中，您可以指定評估的稽核擁有者。稽核擁有者是工作場所中負責管理稽核管理員評估的個 DevOps 人 (通常來自 GRC 或團隊)。SecOps 我們建議他們使用 [AWSAuditManagerAdministratorAccess](#) 政策。

#### 如需指定稽核擁有者

1. 在稽核擁有者底下，選擇要進行評估的稽核擁有者。若要尋找其他稽核擁有者，請使用搜尋列來依名稱或搜尋 AWS 帳戶。
2. 選擇下一步。

### 步驟 4：檢閱和建立

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，選擇 [建立評估] 以開始收集持續的證據。

建立評估之後，系統會繼續收集證據，直到您 [變更評估狀態](#) 為非作用中為止。或者，您可以 [變更控制項狀態](#) 為非作用中，來停止特定控制項收集證據。

#### Note

建立評估後 24 小時即可取得自動證據。Audit Manager 會自動從多個資料來源收集證據，而證據收集的頻率根據證據類型而定。如需詳細資訊，請參閱本指南中的 [證據收集頻率](#)。

## 其他資源

我們建議您繼續進一步了解本課程中介紹的概念和工具。請檢閱下列資源以繼續：

- [複查評估詳細資料 AWS Audit Manager](#)— 向您介紹評量詳細資訊頁面，您可以在其中探索評量的不同元件。

- [管理評估 AWS Audit Manager](#) — 以本教學課程為基礎，並提供有關管理評估的概念和工作的深入資訊。在本章中，我們特別建議您查看以下主題：
  - 如何從不同架構[建立評估](#)
  - 如何[檢閱評估中的證據](#)並[產生評估報告](#)
  - 如何[變更評估狀態](#)或[刪除評估](#)
- [使用框架庫來管理框架 AWS Audit Manager](#)— 介紹架構程式庫，並說明如何按照自己特定的合規需求[建立自訂架構](#)。
- [使用控制項程式庫管理控制項 AWS Audit Manager](#)— 介紹控制項程式庫，並說明如何[建立自訂控制項](#)以在自訂架構中使用。
- [理解 AWS Audit Manager 概念和術語](#)— 提供 Audit Manager 中使用的概念和術語的定義。
- [影片] [收集證據並使用以下方式管理稽核資料 AWS Audit Manager](#) — 顯示本教學課程中所述的評估建立程序，以及其他工作，例如檢閱控制項和產生評估報告。

## 委派教學課程：檢閱控制集

本教學課程說明如何檢閱由 AWS Audit Manager 中的稽核擁有者與您共用的控制集。

稽核擁有者使用 Audit Manager 來建立評估，並收集該評估中控制項的證據。有時，稽核擁有者在驗證控制集的證據時，可能會遇到問題或需要協助。在此情況下，稽核擁有者可以委派主題專家對控制集進行檢閱。

作為委派代表，您可以幫助稽核擁有者檢閱收集到的屬於您專業領域的控制項證據。

### 必要條件

在您開始教學課程之前，請務必先達成以下條件：

- 您 AWS 帳戶 已設定完成。若要完成此自學課程，您必須同時使用 AWS 帳戶 和 Audit Manager 主控台。如需詳細資訊，請參閱 [使用建議 AWS Audit Manager 的設定進行設定](#)。
- 您對 Audit Manager 的術語和功能已經很熟悉了。如需 Audit Manager 的一般概觀，請參閱 [什麼是 AWS Audit Manager ?](#) 和 [理解 AWS Audit Manager 概念和術語](#)。

## 程序

### 任務

- [步驟 1：檢視您的通知](#)
- [步驟 2：檢閱控制集及其相關證據](#)
- [步驟 3。添加手動證據 \(可選\)](#)
- [步驟 4. 針對控制項新增評論 \(選擇性\)](#)
- [步驟 5：將控制項標示為已檢閱 \(選擇性\)](#)
- [步驟 6. 將已檢閱的控制集提交至稽核擁有者](#)

## 步驟 1：檢視您的通知

首先登入 Audit Manager，您可以在其中存取通知，以查看已委派給您以供檢閱的控制集。

### 檢視您的通知

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇通知。
3. 在通知頁面上，檢閱已委派給您的控制集清單。通知表包含以下資訊：

名稱	描述
日期	委派控制集的日期。
評估	與控制集相關聯的評估名稱。您可以選擇評估名稱，開啟評估詳細資料頁面。
控制集	委託給您進行複查的控制集名稱。
來源	委派控制項集給您的使用者或角色。
Description	稽核擁有者提供的檢閱指示。

#### Tip

您也可以訂閱 SNS 主題，以便在控制集指派給您以供檢閱時接收電子郵件警示。如需詳細資訊，請參閱 [通知 AWS Audit Manager](#)。

## 步驟 2：檢閱控制集及其相關證據

下一個步驟是檢閱稽核擁有者委派給您的控制集。透過檢查這些控制項及其證據，您可以確定是否需要對控制項採取任何其他動作。其他動作可包括手動上傳其他證據以證明合規性，或留下有關該控制項的註解。

### 如需檢閱控制集

1. 在通知頁面上，檢閱委派給您的控制集清單。然後找出您要檢閱的評估，並選擇相關評估的名稱。
2. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
3. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。然後，選擇控制項名稱以開啟控制項詳細資訊頁面。
4. (選擇性) 選擇更新控制項狀態以變更控制項的狀態。審核正在進行中時，您可以將狀態標記為「審核中」。
5. 檢閱 [證據] 資料夾、[詳細資料]、[證據來源]、[註解] 和 [變更記錄檔] 索引標籤中的控制項 若要瞭解這些索引標籤中的每個索引標籤，以及如何瞭解它們包含的資料，請參閱[檢閱中的評估控制 AWS Audit Manager](#)。

### 如需檢閱控制項的證據

1. 在控制項詳細資訊頁面中，選擇證據資料夾索引標籤。
2. 導覽至證據資料夾表，會顯示包含該控制項之證據的資料夾清單。這些資料夾是根據收集該資料夾內證據的日期來組織和命名的。
3. 選擇證據資料夾的名稱以將其開啟。從這裡，您可以檢閱該日期收集之所有證據的摘要。若要瞭解此資訊，請參閱[檢閱中的證據資料夾 AWS Audit Manager](#)。
4. 從證據資料夾摘要頁面，瀏覽至證據表格。在時間欄位下方，選擇要開啟的明細項目，並檢閱當時收集的證據詳細資訊。若要瞭解此資訊，請參閱[檢閱中的證據 AWS Audit Manager](#)。

## 步驟 3。添加手動證據 ( 可選 )

雖然會 AWS Audit Manager 自動收集許多控制項的證據，但在某些情況下，您可能需要提供其他證據。在這些情況下，您可以手動添加自己的證據，以幫助您證明是否符合該控制。

### 若要將手動證據新增至控制項

有幾種方法可以將手動證據添加到控制項中。您可以從 Amazon S3 匯入檔案、從瀏覽器上傳檔案或輸入文字回應。如需每種方法的指示，請參閱[在中添加手動證據 AWS Audit Manager](#)。

## 步驟 4. 針對控制項新增評論 (選擇性)

您可以為審核的任何控制項新增評論。稽核擁有者可以看見這些評論。例如，您可以留下評論以提供狀態更新，並確認您已修正該控制項的任何問題。

若要將評論加入至控制項

1. 在通知頁面上，檢閱委派給您的控制集清單。尋找您要為其留下評論之控制集，然後選擇相關評估的名稱。
2. 選擇控制項索引標籤，向下捲動至控制集表格，然後選取控制項名稱加以開啟。
3. 選擇評論索引標籤。
4. 在傳送評論底下，在文字方塊中輸入您的評論。
5. 選擇「提交注釋」以添加您的評論。然後，您的註解會顯示在頁面的先前評論章節下，還會顯示與此控制項相關的任何其他註解。

## 步驟 5：將控制項標示為已檢閱 (選擇性)

變更控制項狀態是選擇性的。不過，建議您在完成該控制項的審核時，將每個控制項的狀態變更為已審核。無論個別控制項的狀態為何，您仍然可以將控制項提交至稽核擁有者。

如需將控制項標記為已審核

1. 在通知頁面上，檢閱委派給您的控制集清單。尋找包含您要標示為已檢閱之控制項的控制集。然後，選擇相關評估的名稱以開啟評估詳細資料頁面。
2. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
3. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。選擇控制項名稱以開啟控制項詳細資訊頁面。
4. 選擇更新控制項狀態，並將狀態變更為已審核。
5. 在出現的快顯視窗中，選擇更新控制項狀態，確認您已完成審核的控制項。

## 步驟 6. 將已檢閱的控制集提交至稽核擁有者

檢閱完所有控制項後，請將控制集提交回稽核擁有者，讓他們知道您已完成檢閱。

## 如需將已檢閱的控制集提交至擁有者

1. 在通知頁面上，檢閱指派給您的控制集清單。搜尋您要提交至稽核擁有者的控制集，然後選擇相關評估的名稱。
2. 向下捲動至控制集表格，選取要提交至稽核擁有者的控制集，然後選擇提交以供審閱。
3. 在出現的快顯視窗中，您可以先新增關於該控制集的任何高階評論，然後再選擇提交以供審核。

將控制項提交至稽核擁有者之後，他們可以檢視您為其留下的任何評論。

## 其他資源

您可以繼續進一步了解本教學課程中介紹的概念。以下是一些推薦的資源：

- [複查評估詳細資料 AWS Audit Manager](#) 向您介紹評量詳細資訊頁面，您可以在其中探索 Audit Manager 評估的不同元件。
- [檢閱中的評估控制 AWS Audit Manager](#) 和 [檢閱中的證據 AWS Audit Manager](#) 提供定義以協助您瞭解評估中的控制項和證據。
- [理解 AWS Audit Manager 概念和術語](#) — 提供 Audit Manager 中使用的概念和術語的定義。

# 使用 Audit Manager 儀表板

使用 Audit Manager 儀表板，您可以在使用中的評估中以圖像顯示不合規的證據。這是一種方便快捷的方式，可以監控您的評估、隨時掌握資訊並主動修復問題。儀表板在預設設定下，會以由上而下彙總的方式，檢視提供所有使用中的評估。使用此檢視，您可以直觀地找出評估中的問題，而無需先篩選大量個別證據。

儀表板是您登入 Audit Manager 主控台時看到的第一個畫面。它包含兩個小工具，顯示與您最相關的資料和關鍵績效指標 (KPI)。使用評估篩選器，您可以調整此資料，以專注在特定評估的 KPI。您可以從該處檢閱控制項網域群組，以分辨哪些控制項具有最不合規的證據。然後，您可以探索基礎控制項，以檢查和修復問題。

## Note

如果您是第一次使用 Audit Manager，或者您沒有任何使用中的評估，則儀表板中不會顯示任何資料。若要開始使用，請[建立評估](#)。這將開始持續收集證據。24 小時後，彙總的證據資料將開始顯示在儀表板中。您可以閱讀以下各節，以了解如何理解和解釋此資料。

本頁面涵蓋下列主題：

### 主題

- [儀表板概念和術語](#)
- [儀表板元素](#)
- [後續步驟](#)
- [其他資源](#)

## 儀表板概念和術語

本節說明開始使用 Audit Manager 儀表板前需要瞭解的重要事項。

### 許可和可見性

[稽核擁有者](#)和[代理人](#)都可以存取儀表板。這表示這兩個角色都可以在您的 AWS 帳戶存取相同的資訊，可讓您的所有團隊專注在相同的 KPI 和目標。



## 篩選條件

Audit Manager 提供一個頁面層級 [the section called “評估篩選器”](#)，您可以將其套用至儀表板上的所有小工具。

## 不合規證據

儀表板會強調顯示評估中具有 [合規檢查證據](#) 和 不合規結果的控制項。符合性檢查證據與使用 AWS Config 或 AWS Security Hub 做為資料來源類型的控制項有關。針對此證據類型，Audit Manager 會直接從這些服務回報合規檢查的結果。如果安全中樞回報失敗結果，或者如果 AWS Config 報告不合規的結果，則 Audit Manager 會將證據歸類為不合規。

## 不確定證據

如果合規檢查無法使用或不適用，則證據為不確定。因此，無法進行合規評估。如果控制項使用 AWS Config 或 AWS Security Hub 做為資料來源類型，但您未啟用這些服務，就會發生這種情況。如果控制項使用不支援相容性檢查的資料來源類型，例如手動證據、AWS API 呼叫或 AWS CloudTrail。

如果在主控台裡，證據的合規檢查狀態為不適用，則在儀表板中將分類為不確定。

## 合規證據

如果合規檢查沒有回報任何問題，則證據將會是合規。如果 Security Hub 報告「通過」結果或 AWS Config 報告「合規」結果，就會發生這種情況。

## 控制項網域

儀表板介紹控制項網域的概念。您可以將控制項網域視為控制項的一般類別，不特定於任何一個架構。控制項網域群組是儀表板最強大的功能之一。Audit Manager 會強調顯示評估中具有不合規證據的控制項，並依控制項網域進行分組。使用此功能，您可以在準備稽核時，將修復工作集中在特定主題網域上。

### Note

控制項網域與控制集不同。控制集是一種特定於架構的控制項群組，通常由管理機構定義。例如，PCI DSS 架構有一個名為需求 8：識別和驗證對系統元件的存取的控制組。此控制集屬於身分與存取管理的控制項網域下。

## 資料的最終一致性

儀表板資料最終是一致的。這代表當您從儀表板讀取資料時，儀表板可能不會立即反映最近完成寫入或更新作業的結果。如果您在幾個小時內再次檢查，儀表板應該會反映最新的資料。

## 已刪除和非使用中評估的資料

儀表板會顯示使用中評估的資料。如果您在檢視儀表板的同一天刪除評估，或將其狀態變更為非使用中，則該評估的資料會如下所示。

- 非使用中評估 — 如果 Audit Manager 在您將評估變更為非使用中之前收集了評估的證據，則該證據資料會包含在儀表板當天的計數。
- 已刪除的評估 — 如果 Audit Manager 在您刪除之前收集了評估的證據，則該證據資料不會包含在儀表板當天的計數中。

## 儀表板元素

以下幾節涵蓋儀表板的不同元件。

### 主題

- [評估篩選器](#)
- [每日快照](#)
- [依控制項網域分組的具不合規證據的控制項](#)

## 評估篩選器

您可以使用評估篩選器來專注於特定的使用中評估。

依預設，儀表板會顯示所有使用中評估的彙總資料。如果您要檢視特定評估的資料，請套用評估篩選器。這是適用於儀表板上所有小工具的頁面層級篩選器。



如需套用評估篩選器，請從儀表板頂端的下拉式清單中選取評估。此清單會顯示最多 10 項使用中的評估。最近建立的評估會先顯示出來。如果您有許多使用中的評估，您可以開始輸入評估名稱以快速找到評估。選取評估後，儀表板僅顯示該評估的資料。

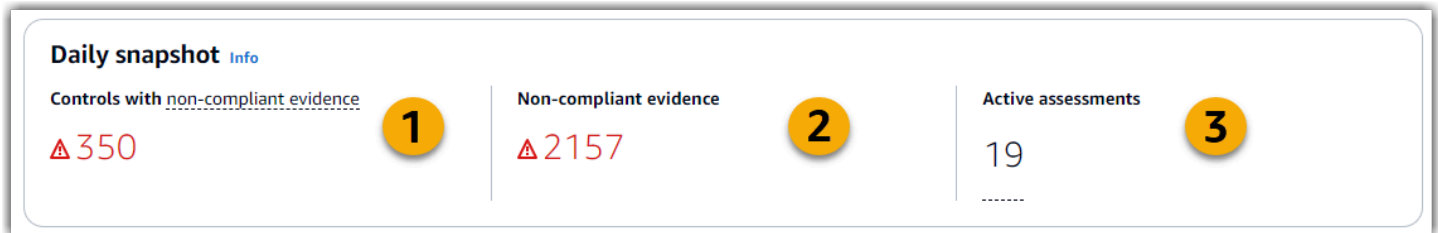
## 每日快照

這項小工具會顯示使用中評估目前合規性狀態的快照。

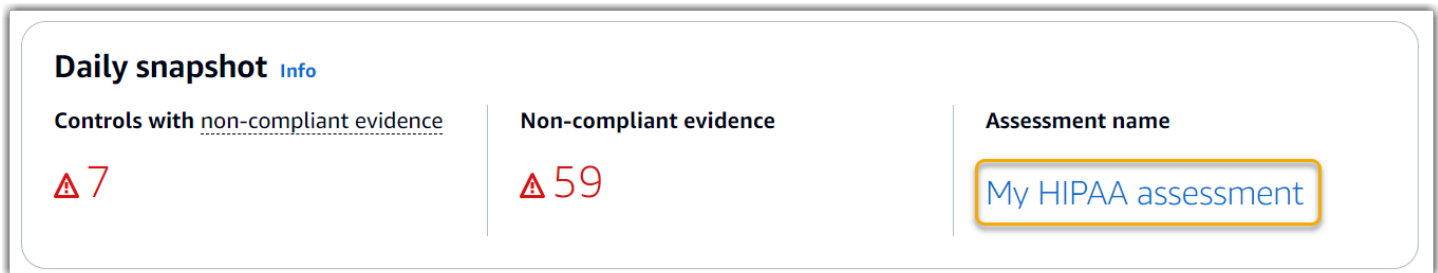
每日快照會顯示儀表板頂端當天收集的最新資料。使用國際標準時間 (UTC) 表示儀表板上的日期與時間。重要的是，這些資料是依據該時間點的每日統計。它們不是迄今為止的總和。

預設情況下，每日快照會顯示所有使用中評估的下列資料：

1. 具有不合規證據的控制項 - 與不合規證據相關聯的控制項總數。
2. 不符合規定的證據-符合性檢查證據的總量與不合規的結論。
3. 使用中評估 - 您使用中評估的總數。選擇此數字以查看這些評估的連結。



每日快照資料會根據您套用的[the section called “評估篩選器”](#)資料而變更。當您指定評估時，資料僅反映該評估的每日計數。在此情況下，每日快照會顯示您指定之評估的名稱。您可以選擇評估的名稱來開啟它。

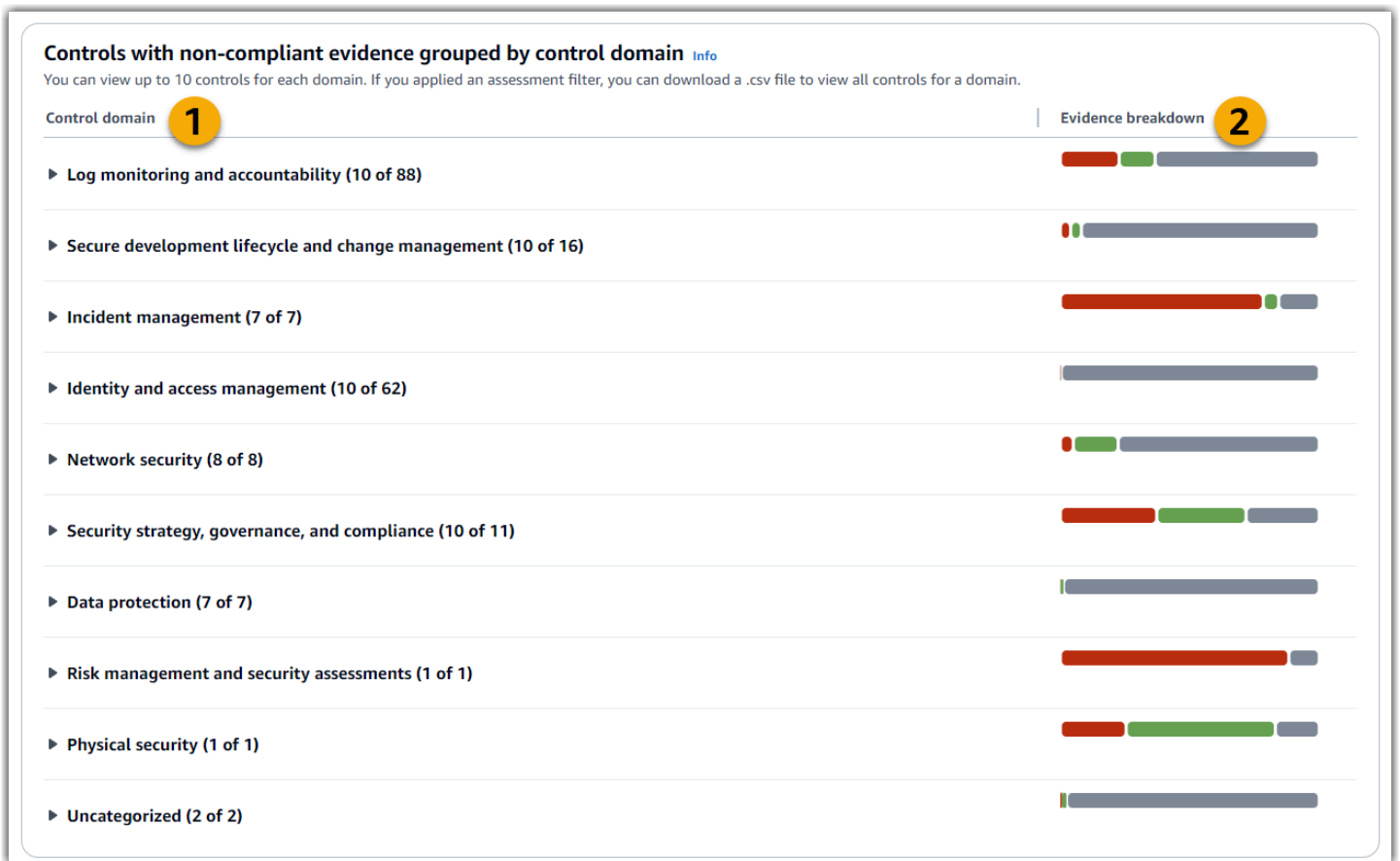


## 依控制項網域分組的具不合規證據的控制項

您可以使用此小工具來分辨哪些控制項具有最不相容的證據。

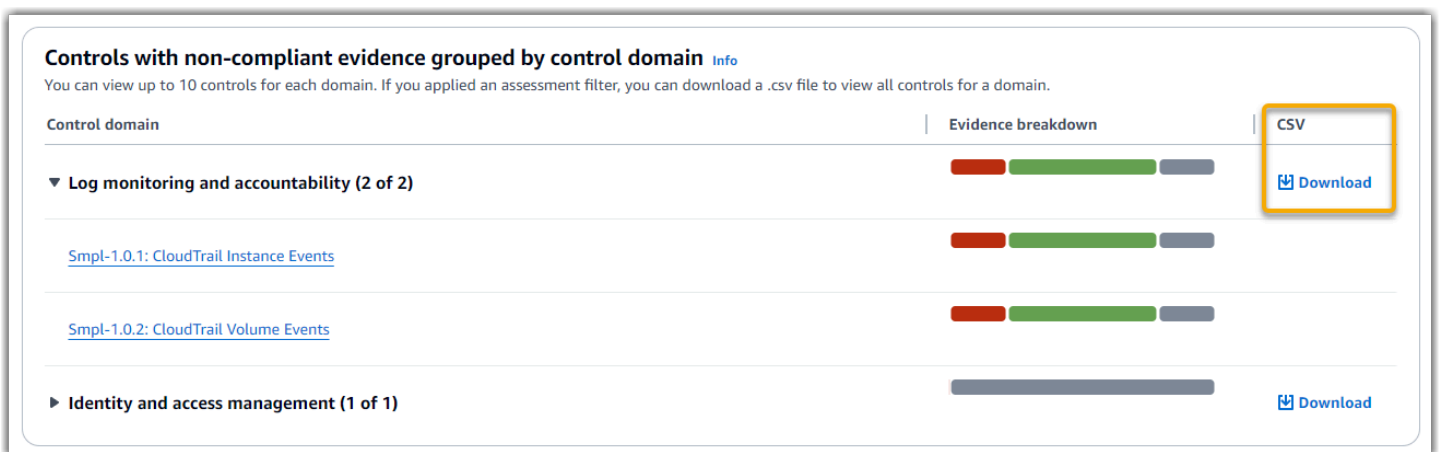
預設情況下，小工具會顯示您所有使用中評估的下列資料：

1. 控制項網域 — 與您的使用中評估相關的[control domains](#)清單。
2. 證據分類 — 顯示證據合規狀態分類的條形圖。



如需展開控制項網域，請選擇其名稱旁邊的箭頭。展開後，主控台最多會針對每個網域顯示 10 個控制項。這些控制項會根據不合規證據的最高總數來排名。

此小工具中的資料會根據您套用的 [the section called “評估篩選器”](#) 而變更。當您指定評估時，您只能看到該評估的資料。此外，您也可以為評估中的每個可用控制網域下載 CSV 檔案。



.csv 檔案包含網域中與不合規證據相關聯的控制項完整清單。下列範例顯示含有虛構化值的 CSV 資料欄。

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AssessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefg-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

最後，當您套用評估篩選時，每個網域下的控制項名稱都將變為超連結。選擇任何控制項，以開啟指定評估中的控制項詳細資訊頁面。

**Controls with non-compliant evidence grouped by control domain** [Info](#)

You can view up to 10 controls for each domain. If you applied an assessment filter, you can download a .csv file to view all controls for a domain.

Control domain	Evidence breakdown	CSV
<p>▼ Log monitoring and accountability (2 of 2)</p> <p><a href="#">Smpl-1.0.1: CloudTrail Instance Events</a></p> <p><a href="#">Smpl-1.0.2: CloudTrail Volume Events</a></p>		<p><a href="#">Download</a></p>
<p>► Identity and access management (1 of 1)</p>		<p><a href="#">Download</a></p>

### Tip

使用控制項詳細資訊頁面做為起點，您可以從一個詳細資訊層級移至下一個層級。

1. 控制項詳細資訊頁面-在此頁面上，會**證據資料夾索引標籤**列出 Audit Manager 為該控制項收集的每日證據資料夾。如需更多詳細資訊，請選擇一個資料夾。
2. 證據文件夾- 接下來，您可以查看該文件夾中的證據**證據資料夾摘要**和列表。如需更多詳細資訊，請選擇個別證據項目。
3. 個人證據 - 最後，您可以瀏覽**個人證據詳細資訊**。這是最細微層級的證據資料。

## 後續步驟

以下是您可以在查看儀表板後，所執行的一些後續步驟。

- 下載 CSV 檔案 — 尋找您要關注的評估和控制網域，並[下載含有不合規證據的相關控制項的完整清單](#)。
- 檢閱控制項 — 分辨需要修正的控制項之後，您可以[檢閱控制項](#)。
- 委派控制項以供檢閱 — 如果您需要協助檢閱控制項，您可以[委派控制集以供檢閱](#)。
- 編輯您的評估 — 如果您想要變更使用中評估的範圍，您可以[編輯評估](#)。
- 更新評估狀態 — 如果您想停止收集評估的證據，可以將評估狀態變更為非作用中。

## 其他資源

若要尋找常見問題和問題的解答，請參閱[儀表板問題疑難排解](#)本指南的「疑難排解」一節。

# 管理評估 AWS Audit Manager

Audit Manager 評估以架構為基礎，而架構是控制項群組。使用架構作為起點，您可以建立評估，以收集該架構中控制項的證據。在評估中，您也可以定義稽核範圍。這包括指定您 AWS 帳戶 要收集證據的證據。

## 重點

您可以從任何架構建立評估。您也可以使用 Audit Manager 所提供的[標準架構](#)。或者，您可以透過自己構建的[自訂架構](#)建立評估。標準架構包含支援特定合規標準或法規的預建控制集。相反地，自訂架構包含控制項，您可以根據自己的需求自訂和分組。

證據收集屬於持續過程，自您建立評估起開始。當需要進行稽核時，您或委派人員可以[檢閱此證據](#)，然後[將其新增至評估報告](#)。

### Note

AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。AWS Audit Manager 因此，透過收集的證據可能不包含稽核所需的所有有關您 AWS 使用情況的資訊。AWS Audit Manager 不是法律顧問或合規專家的替代品。

## 其他資源

若要在稽核管理員中建立和管理評量，請遵循此處概述的程序。

- [在中建立評估 AWS Audit Manager](#)
- [尋找您的評估 AWS Audit Manager](#)
- [檢閱評估 AWS Audit Manager](#)
  - [複查評估詳細資料 AWS Audit Manager](#)
  - [檢閱中的評估控制 AWS Audit Manager](#)
  - [檢閱中的證據資料夾 AWS Audit Manager](#)
  - [檢閱中的證據 AWS Audit Manager](#)
- [編輯評量 AWS Audit Manager](#)

- [變更評估控制項的狀態 AWS Audit Manager](#)
- [在中將評估的狀態變更為非作用中 AWS Audit Manager](#)
- [在中添加手動證據 AWS Audit Manager](#)
  - [從 Amazon S3 匯入手動證據檔案](#)
  - [從瀏覽器上傳手動證據檔案](#)
  - [輸入任意格式文字回應作為手動辨識](#)
  - [手動證據支援的檔案格式](#)
- [準備評估報告 AWS Audit Manager](#)
  - [將證據添加至評估報告](#)
  - [從評估報告中移除證據](#)
  - [產生評估報告](#)
  - [從下載中心下載評估報告](#)
  - [瀏覽評估報告並探索其內容](#)
  - [驗證評估報告](#)
  - [刪除評估報告](#)
  - [從您的證據查找器搜索結果生成評估報告](#)
- [刪除中的評估 AWS Audit Manager](#)

## 在中建立評估 AWS Audit Manager

本主題建立在[稽核擁有者教學課程：建立評估](#)。您可以在此頁面上找到詳細說明，向您展示如何從架構建立評估。請依照下列步驟建立評估，並開始持續收集證據。

### 必要條件

開始此自學課程之前，請確定您符合下列條件：

- 您已完成 [使用建議 AWS Audit Manager 的設定進行設定](#) 中描述的所有先決條件。您必須使用 AWS 帳戶 和 Audit Manager 主控台來完成本教學課程。
- 您的 IAM 身分具有適當的許可，可在稽核管理員中建立和管理評估。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。



# 程序

## 任務

- [步驟 1：指定評估詳細資訊](#)
- [步驟 2：AWS 帳戶 在範圍內指定](#)
- [步驟 3：指定稽核擁有者](#)
- [步驟 4：檢閱和建立](#)

## 步驟 1：指定評估詳細資訊

首先選擇一個架構並提供評估的基本資訊。

### 指定評估詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇 評估，然後選擇建立評估。
3. 在名稱下，輸入評估的名稱。
4. (選擇性) 在說明下，輸入評估的說明。
5. 在評估報告目標下，選取您要儲存評估報告的 S3 儲存貯體。

#### Tip

預設評估報告目的地是根據您的[評估設定而定](#)。如果您願意，您可以建立並使用多個 S3 儲存貯體，協助您針對不同的評估組織評估報告。

6. 在 [選取架構] 下，選取您要從中建立評估的架構。您也可以使用搜尋列，依名稱、合規標準或法規來查詢架構。

#### Tip

要了解有關框架的更多信息，請選擇框架名稱以查看框架詳細信息頁面。

7. (選擇性) 在「標籤」下，選擇「新增標籤」，將標籤與評估產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的，在搜尋此評估時，可用作搜尋條件。
8. 選擇下一步。

**Note**

請務必確保您的評估會針對特定架構收集正確的證據。在開始收集證據之前，我們建議您先檢閱所選架構的需求。然後，根據您目前的 AWS Config 規則參數驗證這些需求。如需確保規則參數符合架構需求，您可以在 [AWS Config 中更新規則](#)。

例如，假設您正在為 CIS v1.2.0 建立評估。此架構包含一個名為 [1.9 — 確保 IAM 密碼政策的長度至少需要 14 或更高的控制項](#)。在中 AWS Config，[iam-password-policy](#) 規則具有檢查密碼長度的 `MinimumPasswordLength` 參數。此參數的預設值為 14 字元。因此，該規則符合控制項的需求。如果您沒有使用預設參數值，請確保您使用的值等於或大於 CIS v1.2.0 的 14 個字元要求。您可以在 [AWS Config 文件](#) 中找到每個受管規則的預設參數詳細資訊。

## 步驟 2：AWS 帳戶 在範圍內指定

您可以指定 AWS 帳戶 要在評估範圍內的多個。Audit Manager 透過與 AWS Organizations 整合來支援多個帳戶。這表示 Audit Manager 員評估可以在多個帳戶上執行，而收集的證據會合併到委派的管理員帳戶中。如需在 Audit Manager 中啟用 Organizations，請參閱 [啟用和設定 AWS Organizations \(選擇性\)](#)。

**Note**

Audit Manager 在評估範圍內最多可支援 200 個帳戶。如果您嘗試包含超過 200 個帳戶，則評估建立可能會失敗。

### 若要 AWS 帳戶 在範圍內指定

1. 在下方 AWS 帳戶，選 AWS 帳戶 取您要包含在評估範圍中的項目。
  - 如果您在 Audit Manager 中啟用了 Organizations，則會顯示多個帳戶。您可以從清單中選擇一或多個帳戶。或者，您也可以使用帳戶名稱、ID 或電子郵件搜尋帳戶。
  - 如果您未在 Audit Manager 中啟用 Organizations，則只會列出您目前 AWS 帳戶 的組織。
2. 選擇下一步。

**Note**

當範圍內的帳戶從組織中移除時，Audit Manager 不會再為該帳戶收集證據。但是，該帳戶仍會繼續顯示在您的評估中的 AWS 帳戶 索引標籤下。若要從範圍內的帳戶清單中移除該帳戶，

請[編輯評估](#)。已移除帳戶在編輯期間不再顯示於清單中，您可以在不包含該帳戶的範圍內儲存您的變更。

### 步驟 3：指定稽核擁有者

在此步驟中，您可以指定評估的稽核擁有者。稽核擁有者是工作場所中負責管理稽核管理員評估的個 DevOps 人 (通常來自 GRC 或團隊)。SecOps 我們建議他們使用 [AWSAuditManagerAdministratorAccess](#) 政策。

如需指定稽核擁有者

1. 在稽核擁有者下，檢閱目前的稽核擁有者清單。稽核擁有者一欄會顯示使用者 ID 和角色。此 AWS 帳戶欄會顯示該稽核擁有者 AWS 帳戶的。
2. 核取方塊已選擇的稽核擁有者會包含在您的評估中。清除任何稽核擁有者的核取方塊，即可將其從評估中移除。您可以使用搜尋列，按名稱或 AWS 帳戶搜尋尋找其他稽核擁有者。
3. 完成時，選擇下一步。

### 步驟 4：檢閱和建立

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，請選擇 建立評估。

該動作意味著評估證據持續收集過程的開始。建立評估之後，系統會繼續收集證據，直到您[變更評估狀態](#)為非作用中為止。或者，您可以將控制項[狀態變更為非作用中](#)，來停止特定控制項的證據收集。

#### Note

自動證據在您的評估建立後 24 小時內即可使用。Audit Manager 會自動從多個資料來源收集證據，而證據收集的頻率根據證據類型而定。如需進一步了解，請參閱本指南中的 [證據收集頻率](#)。

## 後續步驟

若要稍後重新檢視您的評估，請參閱[尋找您的評估 AWS Audit Manager](#)。您可以依照下列步驟找出您的評估，以便檢視、編輯或繼續處理評估。

## 其他資源

如需 Audit Manager 中評估問題的解決方案，請參閱[疑難排解評估和證據收集問題](#)。

## 尋找您的評估 AWS Audit Manager

在中建立評量之後 AWS Audit Manager，您可以在 Audit Manager 主控台的評估頁面上找到評量。

在此頁面中，您可以對評量執行各種動作。例如，您可以檢視評量詳細資料、編輯評估組態或刪除不再需要的評量。此外，評量頁面也是建立新評量的起點。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 以程式設計方式檢視評量。

## 必要條件

下列程序假設您先前已建立至少一個評估。如果您尚未建立評估，按照下列步驟操作時將不會看到任何結果。

確保您的 IAM 身分具有適當的許可，以便在中查看評估 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、稽 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視您的評量。

### Audit Manager console

若要在 Audit Manager 主控台上檢視您的評量

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估查看評估清單。
3. 選擇任何評估名稱以檢視該評估的詳細資訊。

### AWS CLI

如需檢視您的評估 (CLI)

如需在 Audit Manager 中檢視評估，請執行[list-assessments](#)命令。您可以使用 `--status` 子指令來檢視作用中或非作用中的評量。

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

## Audit Manager API

若要使用 API 檢視您的評量

若要在 Audit Manager 中檢視評量，請使用[ListAssessments](#)作業。您可以使用 `status` 屬性來檢視作用中或非作用中的評估。

有關詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用 `ListAssessments` 操作和參數的資訊。

## 後續步驟

當您準備好探索評估的內容時，請按照中的步驟操作[檢閱評估 AWS Audit Manager](#)。此頁面將引導您完成評估詳細信息，並解釋您在此處看到的信息。

在評量頁面中，您也可以[編輯評估](#)、[刪除評估](#)或[建立評估](#)。

## 其他資源

如需 Audit Manager 中評估問題的解決方案，請參閱[疑難排解評估和證據收集問題](#)。

## 檢閱評估 AWS Audit Manager

在 Audit Manager 中建立評估之後，您可以隨時開啟並檢閱您的評估。

## 重點

當您準備好探索評估時，您可以逐步深入了解詳細資料，並透過提高精細程度來檢閱您的評估。

1. 評估詳細資料 — 首先檢閱評估的整體詳細資料。在此頁面上，您可以檢閱評量名稱、說明、範圍和其他詳細資訊。這會為您提供評估的高階概觀。
2. 評估控制詳細資料 — 接下來，透過檢閱每個評估控制項的詳細資訊，深入了解評估。這將使您能夠了解每個控制項的特定需求和目標。
3. 證據資料夾詳細資訊 — 對於每個評估控制項，您可以檢閱包含指定控制項之證據的對應證據資料夾。這些資料夾會組織與每個控制項相關的支援證據。
4. 證據詳細資訊 — 最後，進一步向下鑽研以檢閱每個資料夾中的個別證據。這可能包括設定快照、使用者活動記錄、合規性發現項目，或手動上傳的證據，例如文件和螢幕擷取畫面。檢閱此證據可協助您瞭解組織如何滿足控制項的需求。

透過執行這些步驟，您可以徹底探索評估、瞭解其元件，以及檢閱支援組織合規性工作的證據。

## 其他資源

若要開始在 Audit Manager 中檢閱評量，請遵循此處概述的程序。

- [複查評估詳細資料 AWS Audit Manager](#)
- [檢閱中的評估控制 AWS Audit Manager](#)
- [檢閱中的證據資料夾 AWS Audit Manager](#)
- [檢閱中的證據 AWS Audit Manager](#)

## 複查評估詳細資料 AWS Audit Manager

當您需要檢閱評估的詳細資料時，您會在評估詳細資料頁面上找到這些資訊分為數個區段。這些部分可幫助您輕鬆訪問和了解任務的相關信息。

### 內容

- [必要條件](#)
- [程序](#)
  - [評估詳細資料段](#)
  - [控制項索引標籤](#)
  - [評估報告選擇索引標籤](#)
  - [AWS 帳戶 標籤](#)

- [AWS 服務 標籤](#)
- [稽核擁有者索引標籤](#)
- [標籤索引標籤](#)
- [Changelog 索引標籤](#)
- [後續步驟](#)
- [其他資源](#)

## 必要條件

下列程序假設您先前已建立至少一個評估。如果您尚未建立評估，按照下列步驟操作時將不會看到任何結果。

確保您的 IAM 身分具有適當的許可，以便在中查看評估 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

若要開啟和檢閱評量詳細資訊頁面

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估查看評估清單。
3. 選擇評估名稱來開啟評估。
4. 使用下列資訊作為參考，檢閱評估詳細資料。

評量詳細資訊頁面的區段

- [評估詳細資料段](#)
- [控制項索引標籤](#)
- [評估報告選擇索引標籤](#)
- [AWS 帳戶 標籤](#)
- [AWS 服務 標籤](#)
- [稽核擁有者索引標籤](#)
- [標籤索引標籤](#)

## • [Changelog 索引標籤](#)

### 評估詳細資料段

您可以使用「評量詳細資料」區段來查看評量的摘要。

在評估詳細資料區段中，您可以檢閱下列資訊：

名稱	描述
1. Description	評定的描述。
2. 合規性類型	評估支援的合規標準或法規。
3. 評估報告目的地	Audit Manager 儲存評估報告的 S3 儲存貯體。
4. 證據總數	為此評估收集的證據項目總數。
5. 評估報告選擇	被選中包括在評估報告中的證據項目的數量。
6. Date created (建立日期)	評估的建立日期。
7. 上次更新	上次編輯評估的日期。
8. 狀態	評估的狀態。 <ul style="list-style-type: none"> <li>• 作用中-評估目前正在收集證據。</li> <li>• 非作用中-評估不再收集證據。</li> </ul>

### 控制項索引標籤

您可以使用此標籤來查看評估中控制項的相關資訊。



在 [控制狀態摘要] 底下，您可以檢閱下列資訊：

名稱	描述
總控制	此評估中的控制項總數。
已審閱	稽核擁有者或委託人審核的控制項數目。
正在審查中	目前正在檢閱的控制項數目。
非作用中	不再主動收集證據的控制項數量

在「控制集」表格中，您可以複查依控制集群組的控制項清單。您可以展開或折疊每個控制集中的控制項。如果您正在尋找特定控制項，也可以依名稱搜尋。

在此表格中，您可以檢閱下列資訊：

名稱	描述
按控制組分組的控制項	控制集的名稱。
控制狀態	<p>控制項的狀態。</p> <ul style="list-style-type: none"> <li>審核中表示此控制項未審核完成。此控制項仍在收集證據，您可以新增手動證據。這是預設狀態。</li> <li>已檢閱表示已檢閱此控制項的證據。仍在收集證據，您可以添加手動證據。</li> <li>非作用中表示已停止此控制項的自動證據收集。您無法再新增手動證據。</li> </ul>
委派給	此控制項的複查者 (如果已指派給委託人進行審核)。
證據總數	針對此控制項收集的證據項目數目。

### 評估報告選擇索引標籤

您可以使用此標籤來查看將包含在評估報告中的證據。證據會依據證據資料夾分組，這些資料夾會根據建立日期進行組織。

您可以瀏覽這些資料夾，並選擇要包含在評估報告中的證據。如需有關如何將證據新增至評估報告的指示，請參閱[將證據添加至評估報告](#)。

在本節中，您可以檢閱下列資訊：

名稱	描述
證據文件夾	證據資料夾的名稱。資料夾根據收集證據的日期來命名。
選取的證據	包含在評估報告中的資料夾中的證據項目數目。
控制項名稱	與此證據資料夾相關聯的控制項名稱。

### AWS 帳戶 標籤

您可以使用此索引標籤 **AWS 帳戶** 來查看評估範圍內的內容。

在本節中，您可以檢閱下列資訊：

名稱	描述
帳戶 ID	AWS 帳戶的 ID。
Account name (帳戶名稱)	AWS 帳戶的名稱。
電子郵件	與 AWS 帳戶相關聯的電子郵件地址。

### AWS 服務 標籤

您可能會或可能不會在評估中看到此標籤。

如果未顯示 AWS 服務 標籤 (理想狀態)

如果您沒有看到此索引標籤，則 Audit Manager AWS 服務 正在管理您評估範圍內的哪些標籤。

Audit Manager 會檢查您的評估控制項及其資料來源，然後將此資訊對應至對應 AWS 服務的來源，藉此推斷此範圍。每當評估的基礎資料來源變更時，Audit Manager 會視需要自動更新範圍，以反映正確的範圍 AWS 服務。這可確保您的評估收集有關您 AWS 環境中所有相關服務的準確而全面的證據。

## 如果顯示 AWS 服務 標籤

如果您確實看到此標籤，則「Audit Manager」不會管理您評估範圍內的哪 AWS 服務 些標籤。

在此情況下，您會看到下列有關您定義之範圍內之服務的資訊：

名稱	描述
AWS 服務	AWS 服務的名稱。
類別	服務類別，例如計算或資料庫。
Description	AWS 服務的描述。

Audit Manager 會針對此表格中的服務執行資源評估。例如，如果列出了 Amazon S3，則 Audit Manager 可以收集有關 S3 儲存貯體的證據。收集的確切證據由控件確定 [data source](#)。例如，如果資料來源類型為 AWS Config，而資料來源對映是 AWS Config 規則 (例如 s3-bucket-public-write-prohibited)，則 Audit Manager 會收集該規則評估的結果作為證據。如需詳細資訊，請參閱本指南中的 [範圍內的服務和資料來源類型有什麼不同？](#)。

如果您的評估透過標準架構在主控台中建立的，Audit Manager 會為您選擇服務，並根據架構的需求映射其資料來源。如果標準框架只包含手動控件，則不 AWS 服務 在範圍內。

### Note

下次您編輯評估或變更評估中的其中一個自訂控制項時，Audit Manager 會為您接管範圍內的服務管理。發生這種情況時，該 AWS 服務標籤會從您的評估中移除。

## 稽核擁有者索引標籤

您可以使用此索引標籤來查看評估的稽核擁有者。

在本節中，您可以檢閱下列資訊：

名稱	描述
稽核擁有者	稽核擁有者的名稱。
AWS 帳戶	稽核擁有者的 AWS 帳戶 識別碼。

## 標籤索引標籤

您可以使用此索引標籤來查看評估的標籤。這些標籤會繼承自用來建立評估的架構。如需有關 Audit Manager 中標籤的詳細資訊，請參閱 [標記 AWS Audit Manager 資源](#)。

在本節中，您可以檢閱下列資訊：

名稱	描述
索引鍵	標籤的金鑰，例如合規標準、法規或類別。
Value	標籤的值。

## Changelog 索引標籤

您可以使用此標籤來查看評估的使用者活動。

在本節中，您可以檢閱下列資訊：

名稱	描述
日期	活動的日期。
使用者	執行動作的使用者。
Action	發生的動作，例如正在建立的評估。
類型	變更的物件類型，例如評估。
Resource	受變更影響的資源，例如建立評估的來源架構。

## 後續步驟

若要繼續檢閱評估的內容，請遵循中的步驟[檢閱中的評估控制 AWS Audit Manager](#)。此頁面將引導您完成評估控制詳細資訊，並說明您在此處看到的資訊。

## 其他資源

- [在我的評估詳細資料頁面上，系統會提示我重新建立評估](#)

- [我在評估中看不到任何控制項或控制集](#)
- [我看不到評估範圍內的服務](#)

## 檢閱中的評估控制 AWS Audit Manager

當您需要檢閱評估中的控制項時，您會在評估控制項詳細資料頁面上找到分為數個區段的資訊。這些部分可幫助您輕鬆訪問和了解任務的相關信息。

### 內容

- [必要條件](#)
- [程序](#)
  - [控制項詳情區段](#)
  - [證據資料夾索引標籤](#)
  - [詳細資訊索引標籤](#)
  - [證據來源標籤](#)
  - [評論索引標籤](#)
  - [Changelog 索引標籤](#)
- [後續步驟](#)
- [其他資源](#)

### 必要條件

下列程序假設您先前已建立至少一個評估。如果您尚未建立評估，按照下列步驟操作時將不會看到任何結果。

確保您的 IAM 身分具有適當的許可，以便在中查看評估 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

#### 開啟和檢閱評量控制項詳細資訊頁面

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估，然後選擇要開啟的評估名稱。

3. 在評估頁面上，選擇控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱來開啟。
4. 使用下列資訊作為參考，檢閱評估控制詳細資訊。

### 評估控制項詳細資訊頁面的區段

- [控制項詳情區段](#)
- [證據資料夾索引標籤](#)
- [詳細資訊索引標籤](#)
- [證據來源標籤](#)
- [評論索引標籤](#)
- [Changelog 索引標籤](#)

### 控制項詳情區段

您可以使用「控制項詳細資訊」區段來查看評估控制項的摘要。

在本節中，您可以檢閱下列資訊：

名稱	描述
Description	為此控制項提供的描述。
控制狀態	<p>控制項的狀態。</p> <ul style="list-style-type: none"> <li>• 審核中 — 尚未審核控制項。此控制項仍在收集證據，您可以新增手動證據。這是預設狀態。</li> <li>• 已檢閱 — 檢閱此控制項的證據。仍在收集證據，您可以添加手動證據。</li> <li>• 非作用中 — 停止此控制項的自動化證據收集。您無法再新增手動證據。</li> </ul>

### 證據資料夾索引標籤

您可以使用此索引標籤來查看針對此控制項收集的證據。每天都會組織成資料夾。您也可以從這裡執行下列動作：

- 檢閱證據資料夾 — 若要查看任何證據資料夾的詳細資料，請選擇超連結的資料夾名稱。

- 將證據資料夾新增至評估報告 — 若要包含證據資料夾，請選取該資料夾，然後選擇 [新增至評估報告]。
- 從評估報告中移除證據資料夾 — 若要排除資料夾，請選取該資料夾，然後選擇從評估報告中移除。
- 新增手動辨識-如需指示，請參閱[在中添加手動證據 AWS Audit Manager](#)。

在本節中，您可以檢閱下列資訊：

名稱	描述
證據文件夾	證據資料夾的名稱。根據收集或手動添加證據的日期來命名。
合規性檢查	證據資料夾中的問題數目。這個數字代表直接從 AWS Security Hub、AWS Config 或兩者報告的安全性問題總數。  如果您看到 [不適用]，表示您沒有 Security Hub 或 AWS Config 已啟用，或是證據來自不同的資料來源類型。
證據總數	資料夾內的證據項目總數。
評估報告選擇	包含在評估報告中的資料夾中的證據項目數目。

#### Tip

如果您看不到您要尋找的證據資料夾，請將下拉式篩選條件變更為 [全時]。否則，依預設，您會看到最近七天的資料夾。

### 詳細資訊索引標籤

在本節中，您可以檢閱下列資訊：

名稱	描述
測試資訊	測試控制項是否如預期運作的建議程序。
行動計劃	如果需要修正控制項，建議採取的動作。

## 證據來源標籤

您可以使用此標籤來查看評估控制項從何處收集證據。證據來源可以包括以下任何一項：

名稱	描述
通用控制	<p>這些是收集證據以支持評估控制的常見控制措施。</p> <p>通用控制項使用為您 AWS 管理的基礎資料來源收集證據。對於列出的每個通用控制項，Audit Manager 會收集所有支援核心控制項的相關證據。選擇通用控制項以查看相關的核心控制項。</p>
核心控制	<p>這些是收集證據以支持評估控制的核心控制。</p> <p>核心控制項會使用為您 AWS 管理的預先定義資料來源群組來收集證據。選擇核心控制項以查看基礎資料來源。</p>
資料來源	<p>這些是收集證據以支援評估控制的個別資料來源。</p> <ul style="list-style-type: none"> <li>• 名稱 — 資料來源的名稱。</li> <li>• 類型 — 證據來源的資料來源類型。 <ul style="list-style-type: none"> <li>• 如果 Audit Manager 收集證據，則類型可以是 AWS Security Hub、AWS Config、AWS CloudTrail、或 AWS API 呼叫。</li> <li>• 如果您上傳自己的證據，則類型為「手動」。說明會指出所需的手動證據是檔案上傳還是文字回應。</li> </ul> </li> <li>• 映射 — 用於收集證據的特定關鍵字。 <ul style="list-style-type: none"> <li>• 如果類型為 AWS Config，則對映為 AWS Config 規則 (例如 SNS_ENCRYPTED_KMS )</li> <li>• 如果類型為 AWS Security Hub，則對應為 Security Hub 控制項 (例如 EC2.1)。</li> <li>• 如果類型是 AWS API 呼叫，則對應為 API 呼叫 (例如 kms_ListKeys )。</li> <li>• 如果類型為 AWS CloudTrail，則對映為 CloudTrail 事件 (例如 CreateAccessKey )。</li> </ul> </li> <li>• 頻率 — Audit Manager 為 AWS API 呼叫資料來源收集證據的頻率。</li> </ul>



## 評論索引標籤

在此選項卡中，您可以添加有關控件及其證據的註釋。您也可以查看先前留言的清單。

- 在發送評論下，您可以輸入文字，然後選擇提交評論，為控制項新增評論。
- 在既往評論下，您可以檢視既往評論的清單，以及評論的發佈日期和關聯的使用者 ID。

## Changelog 索引標籤

您可以使用此索引標籤來查看評估控制項的使用者活動。AWS CloudTrail中的稽核記錄日誌也提供了相同的資訊。透過直接在 Audit Manager 中擷取的使用者活動，您可以輕鬆檢閱指定控制項的稽核記錄活動。

在本節中，您可以檢閱下列資訊：

名稱	描述
日期	活動的日期和時間，以國際標準時間 (UTC) 表示。
使用者	執行活動的使用者或角色。
Action	發生的動作，例如正在建立的評估。
類型	變更的物件類型，例如評估。
Resource	受變更影響的資源，例如建立評估的來源架構。

Audit Manager 會透過 changelog 追蹤下列使用者活動：

- 建立評估
- 編輯評估
- 完成評估
- 刪除評估
- 委派需要檢閱的控制集
- 將已檢閱的控制集送交回稽核擁有者
- 上傳手動證據

- [更新控制項狀態](#)
- [產生評估報告](#)

## 後續步驟

若要繼續檢閱您的評估，請遵循中的步驟[檢閱中的證據資料夾 AWS Audit Manager](#)。本頁將引導您瀏覽證據文件夾，並向您展示如何了解所看到的信息。

## 其他資源

- [我在評估中看不到任何控制項或控制集](#)

## 檢閱中的證據資料夾 AWS Audit Manager

當您的評估收集證據時，Audit Manager 會將其組織到資料夾中，以方便您使用。當您需要查看證據文件夾時，您會發現這些信息分為幾個部分。

### 內容

- [必要條件](#)
- [程序](#)
  - [證據資料夾摘要](#)
  - [證據表](#)
- [後續步驟](#)
- [其他資源](#)

## 必要條件

下列程序假設您先前已建立至少一個評估。如果您尚未建立評估，按照下列步驟操作時將不會看到任何結果。

確保您的 IAM 身分具有適當的許可，以便在中查看評估 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

請記住，評估最多需要 24 小時才能開始收集自動證據。如果您的評估還沒有證據，當您按照以下步驟操作時，您將不會看到任何結果。

## 程序

若要開啟和檢閱證據資料夾

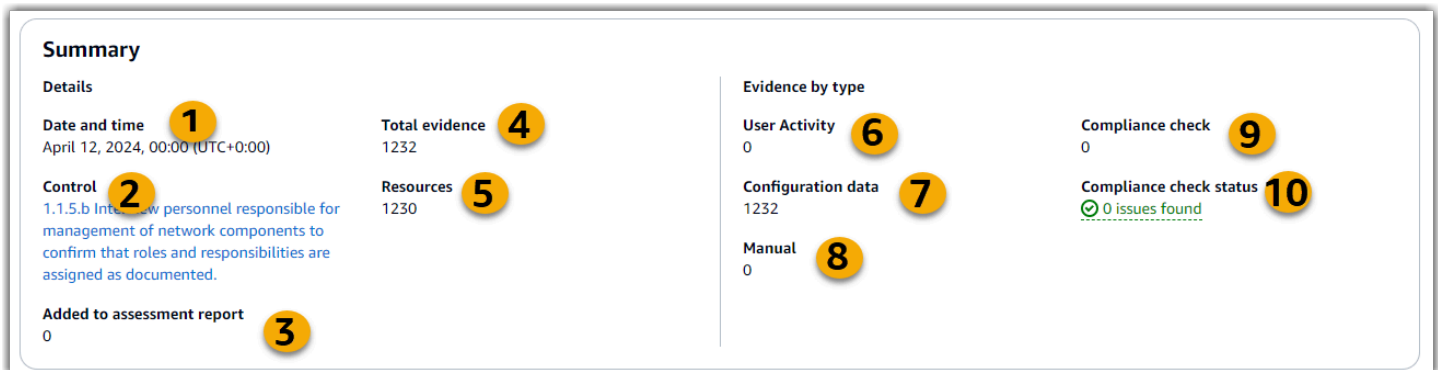
1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在瀏覽窗格中，選擇評估，然後選擇評估。
3. 在評估頁面中，選擇「控制項」標籤，向下捲動至「控制項」表格，然後選擇評量控制項。
4. 在評估控制頁面中，選擇證據資料夾標籤。
5. 在「證據」資料夾表格中，選擇證據資料夾的名稱。
6. 使用下列資訊作為參考來檢閱證據資料夾。

證據資料夾頁面的區段

- [證據資料夾摘要](#)
- [證據表](#)

證據資料夾摘要

您可以使用頁面的 [摘要] 區段來查看證據資料夾中證據的高階概觀。要進一步了解不同證據類型，請參閱[證據](#)。



在本節中，您可以檢閱下列資訊：

名稱	描述
1. 日期和時間	建立證據資料夾的時間和日期。這以國際標準時間 (UTC) 表示。
2. 控制項	與證據資料夾相關的控制項名稱。

名稱	描述
3. 已新增至評估報告	被選中包括在評估報告中的證據項目的數量。
4. 證據總數	證據資料夾中證據項目的總數。
5. 資源	收集此 AWS 資料夾中的證據時，評估的資源總數。
6. 使用者活動	屬於使用者活動類別的證據項目數量。此證據是從 AWS CloudTrail 記錄檔收集的。
7. 組態資料	屬於組態資料類別的證據項目數目。此證據是從擷取其他設定快照的 API 呼叫中收集的 AWS 服務。
8. 手動	屬於手動類別的證據項目數量。此證據是手動新增的。
9. 合規性檢查	符合性檢查類別的證據項目數目。這些證據是從 AWS Config AWS Security Hub、或兩者收集的。
10. 合規性檢查狀態	直接從 AWS Security Hub、AWS Config 或兩者報告的問題總數。

## 證據表

您可以使用「證據」表格來查看證據資料夾中包含的證據。您也可以從這裡表格執行下列動作：

- 檢閱個別證據 — 若要查看任何證據的詳細資料，請在「時間」欄下選擇超連結的證據名稱。
- 將證據新增至評估報告 — 若要包含證據，請選取該證據，然後選擇 [新增至評估報告]。
- 從評估報告中移除證據 — 若要排除證據，請選取該證據，然後選擇「從評估報告中移除」。
- 新增手動辨識-如需指示，請參閱[在中添加手動證據 AWS Audit Manager](#)。

在此表格中，您可以檢閱下列資訊：

名稱	描述
Time (時間)	指定收集證據的時間。這也作為證據的名稱。時間以國際標準時間 (UTC) 表示。
合規性檢查	屬於相容性檢查類別之證據的評估狀態。

名稱	描述
	<ul style="list-style-type: none"> <li>如需從安全中樞收集的證據，則會直接從 Security Hub 全中心回報「通過」或「失敗」結果。</li> <li>對於從中收集的證據 AWS Config，則會直接從中報告「合規」或「不合規」結果。AWS Config</li> <li>如果顯示不適用，表示您未啟用 AWS Config 或 Security Hub，或證據來自不同的資料來源類型。</li> </ul>
各類證據	<p>證據的類型。</p> <ul style="list-style-type: none"> <li>合規性檢查證據是從 AWS Config 或收集的 AWS Security Hub。</li> <li>用戶活動證據是從中收集的 AWS CloudTrail。</li> <li>組態資料證據是從 API 呼叫收集到其他的 AWS 服務。</li> <li>手動證據是您手動新增的證據。</li> </ul>
資料來源	從中收集證據的資料來源。
事件名稱	叫用證據收集的事件名稱。
事件來源	識別與事件相關 AWS 服務的服務主體。
資源	收集證據時評估的資源數量。
評估報告選擇	<p>指出證據是否包含在評估報告中。</p> <ul style="list-style-type: none"> <li>如需包含證據，請選擇證據，然後選擇新增至評估報告。</li> <li>如需排除證據，請選擇證據，然後選擇從評估報告中移除。</li> </ul>

## 後續步驟

當您準備好探索資料夾中的個別證據時，請按照中的步驟操作[檢閱中的證據 AWS Audit Manager](#)。本頁將引導您了解證據詳細信息以及如何解釋您在此處看到的信息。

## 其他資源

- 如需 Audit Manager 中證據問題的解決方案，請參閱[疑難排解評估和證據收集問題](#)。

## 檢閱中的證據 AWS Audit Manager

當您需要查看特定證據時，請按照此頁面上的說明進行操作。您會發現證據詳細信息分為幾個部分。

### 內容

- [必要條件](#)
- [程序](#)
  - [Summary](#)
  - [Attributes](#)
  - [包含的資源](#)
- [其他資源](#)

### 必要條件

下列程序假設您先前已建立至少一個評估。如果您尚未建立評估，按照下列步驟操作時將不會看到任何結果。

確保您的 IAM 身分具有適當的許可，以便在中查看評估 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

請記住，評估最多需要 24 小時才能開始收集自動證據。如果您的評估還沒有證據，當您按照以下步驟操作時，您將不會看到任何結果。

### 程序

若要開啟和檢閱證據詳細資料頁面

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在瀏覽窗格中，選擇評估，然後選擇評估。
3. 在評估頁面中，選擇「控制項」標籤，向下捲動至「控制項」表格，然後選擇控制項。
4. 在控制項詳細資訊頁上，選擇證據資料夾索引標籤。
5. 在「證據」資料夾表格中，選擇證據資料夾的名稱。
6. 在「時間」欄下選擇證據名稱，以開啟證據詳細資料頁面。

## 7. 使用以下信息作為參考來查看證據詳細信息。

### 證據詳細資料頁面的區段

- [Summary](#)
- [Attributes](#)
- [包含的資源](#)

### Summary

您可以使用「摘要」區段來查看證據的概觀。

**Summary** 11  Include in assessment report

**Evidence ID** 1  
15dd9e4a-19ba-3fad-b2be-810585f4e6a6

**Date and time** 2  
April 12, 2024, 00:00 (UTC+0:00)

**Compliance check** 3  
Inconclusive

**Data source mapping** 4  
listPolicies

**Data source** 5  
AWS API calls

**Account ID** 6  
[REDACTED]

**IAM ID** 7  
-

**Assessment** 8  
PCI DSS V3.2.1 Assessment [\[link\]](#)

**Control** 9  
1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. [\[link\]](#)

**Evidence folder name** 10  
2024-04-12 [\[link\]](#)

在本節中，您可以檢閱下列資訊：

名稱	描述
1. 證據識別碼	證據的唯一識別碼。
2. 日期和時間	收集證據的時間和日期。這以國際標準時間 (UTC) 表示。
3. 合規性檢查	符合性檢查證據的評估狀態。 <ul style="list-style-type: none"> <li>對於從中收集的證據 AWS Security Hub，會直接從中報告「通過」或「失敗」結果 AWS Security Hub。</li> <li>對於從中收集的證據 AWS Config，則會直接從中報告「合規」或「不合規」結果。AWS Config</li> <li>如果顯示不適用，則表示兩件事之一。要么你沒有 AWS Security Hub 或 AWS Config 啟用。或者，證據來自不同的數據源。</li> </ul>
4. 資料來源對映	用來收集證據的對應關鍵字。

名稱	描述
5. Data source type (資料來源類型)	從中收集證據的資料來源類型。
6. 帳戶 ID	AWS 帳戶 這是與證據有關的。
7. 身分識別碼	相關使用者或角色 (如果適用)。
8. 評估	與證據相關聯的評估名稱。
9. 控制項	與證據相關聯的控制項名稱。
10. 證據資料夾名稱	包含證據的證據資料夾名稱。
11. 包括在評估報告	可讓您在評估報告中包含或排除證據的開關。

## Attributes

您可以使用「屬性」表來詳細查看證據屬性。

在此表格中，您可以檢閱下列資訊：

名稱	描述
屬性名稱	屬性的索引鍵。
Value	屬性的值。在某些情況下，JSON 檔案的連結會提供更多資訊。

## 包含的資源

您可以使用「包含的資源」表格來查看經過評估以產生此證據的資源。

在本節中，您可以檢閱下列資訊：

名稱	描述
ARN	資源的 Amazon Resource Name (ARN)。ARN 可能不適用於所有證據類型。



名稱	描述
支援合規	<p>資源的評估狀態。</p> <ul style="list-style-type: none"> <li>對於從收集的證據 AWS Security Hub，「通過」或「失敗」結果會直接從 Security Hub 報告。</li> <li>對於從中收集的證據 AWS Config，則會直接從中報告「合規」或「不合規」結果。AWS Config</li> <li>如果顯示不適用，表示您未啟用 AWS Config 或 Security Hub，或證據來自不同的資料來源。</li> </ul>
Value	有關資源評估的詳細資訊。在某些情況下，JSON 檔案的連結會提供更多資訊。

## 其他資源

- 如需 Audit Manager 中證據問題的解決方案，請參閱[疑難排解評估和證據收集問題](#)。

## 編輯評量 AWS Audit Manager

您可能會遇到需要在中編輯現有評量的情況 AWS Audit Manager。或許您的稽核範圍已變更，需要更新評估中 AWS 帳戶 包含的內容。或者，由於人事變更，您可能需要修訂指派給評鑑的稽核擁有者清單。在這種情況下，您可以編輯您的活動評估並進行必要的調整，而不會中斷您的證據收集。

以下頁面概述編輯評量詳細資料、變更範圍 AWS 帳戶 內、更新稽核擁有者，以及檢閱和儲存變更的步驟。

### 必要條件

下列程序假設您先前已建立至少一個評估，且該評估處於使用中狀態。

確保您的 IAM 身分具有適當的許可，可在中編輯評估 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager管理存取權](#)。

### 程序

#### 任務

- [步驟 1：編輯評估詳細資訊](#)
- [步驟 2：AWS 帳戶 在範圍內編輯](#)
- [步驟 3：編輯稽核擁有者](#)
- [步驟 4：檢視並儲存](#)

## 步驟 1：編輯評估詳細資訊

請依照下列步驟編輯評估的詳細資訊。

如需編輯評估

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估。
3. 選擇評估，然後選擇編輯。
4. 在「編輯評估詳細資料」下，視需要編輯評估詳細資料。
5. 選擇下一步。

## 步驟 2：AWS 帳戶 在範圍內編輯

在此步驟中，您可以變更評估中包含的帳戶。Audit Manager 在評估範圍內最多可支援 200 個帳戶。

AWS 帳戶 在範圍內編輯

1. 若要新增 AWS 帳戶，請選取帳戶名稱旁邊的核取方塊。
2. 若要移除 AWS 帳戶，請清除帳戶名稱旁的核取方塊。
3. 選擇下一步。

### Note

若要編輯稽核管理員的委派管理員，請參閱[變更委派管理員](#)。

## 步驟 3：編輯稽核擁有者

在此步驟中，您可以變更評估中包含的稽核擁有者。

## 如需編輯稽核擁有者

1. 若要新增稽核擁有者，請選取帳戶名稱旁邊的核取方塊。
2. 若要移除稽核擁有者，請清除帳戶名稱旁邊的核取方塊。
3. 選擇下一步。

## 步驟 4：檢視並儲存

檢閱評估的資訊。如需變更步驟的資訊，請選擇編輯。完成後，請選擇儲存變更確認您的編輯。

完成編輯後，對評估的變更將在次日 00:00 UTC 生效。

## 後續步驟

當您不再需要收集特定評估控制項的證據時，您可以變更該控制項的狀態。如需說明，請參閱[變更評估控制項的狀態 AWS Audit Manager](#)。

當您不再需要收集整個評估的證據時，您可以將評估狀態變更為非作用中。如需說明，請參閱[在中將評估的狀態變更為非作用中 AWS Audit Manager](#)。

## 其他資源

- 如需 Audit Manager 中評估問題的解決方案，請參閱[疑難排解評估和證據收集問題](#)。
- 如需有關為何無法再編輯範圍內的服務的詳細資訊，請參閱本指南[我無法編輯評估範圍內的服務的「疑難排解」](#)一節。

## 在中添加手動證據 AWS Audit Manager

Audit Manager 可以自動收集多個控制項的證據。但是，某些控制項可能需要無法自動收集的證據。在這種情況下，您可以手動添加自己的證據。

請考量下列範例：

- 某些控制項與提供實體記錄 (例如簽名) 或非雲端產生事件 (例如觀察和訪談) 有關。在這些情況下，您可以手動添加文件作為證據。例如，如果控制項需要有關組織結構的資訊，您可以上傳公司組織圖的副本作為手動證據。

- 某些控制項代表供應商風險評估問題。風險評估問題可能需要文件作為證據 (例如組織圖)。或者，它可能只需要一個簡單的文字回應 (例如職位列表)。對於後者，您可以回答問題並將您的回復保存為手動證據。

您也可以使用手動上傳功能來管理來自多個環境的證據。如果您的公司使用混合雲端模型或多雲端模式，您可以上傳來自內部部署環境、雲端託管環境或 SaaS 應用程式的證據。這可讓您將證據儲存在 Audit Manager 評估的結構中，以組織您的證據 (不限來源)，其中每項證據都映射至特定控制項。

## 重點

在 Audit Manager 中將手動證據新增至您的評量時，您有三種方法可供選擇。

1. 從 Amazon S3 匯入檔案- 當您將證據檔案存放在 S3 儲存貯體 (例如文件、報告或稽核管理員無法自動收集的其他成品) 時，此方法非常理想。透過直接從 S3 匯入這些檔案，您可以將此手動證據與自動收集的證據無縫整合。
2. 從瀏覽器上傳檔案- 如果您的電腦或網路本機儲存了證據檔案，您可以使用此方法手動將其上傳到 Audit Manager。當您需要包含實體記錄 (例如掃描的文件或影像)，而這些記錄在您的 AWS 環境中無法使用數位格式時，此方法特別有用。
3. 新增自由格式文字作為證據- 在某些情況下，您需要提供的證據不是檔案的形式，而是文字回應或說明。此方法可讓您將任意格式文字直接輸入 Audit Manager。這在回應供應商風險評估問題時特別有用。

## 其他資源

- 如需有關如何將手動證據新增至評估控制項的指示，請參閱下列資源。請記住，您一次只能使用一種方法。
  - [從 Amazon S3 匯入手動證據檔案](#)
  - [從瀏覽器上傳手動證據檔案](#)
  - [輸入任意格式文字回應作為手動辨識](#)
- 若要瞭解您可以使用哪些檔案格式，請參閱[手動證據支援的檔案格式](#)。
- 若要進一步瞭解 Audit Manager 中不同類型的證據，請參閱[evidence](#)本指南的概念與術語一節中的。
- 如需疑難排解協助，請參閱[我無法將手動證據上傳到控制項](#)。

## 從 Amazon S3 匯入手動證據檔案

您可以手動將證據檔案從 Amazon S3 儲存貯體匯入您的評估中。這使您可以用額外的輔助材料補充自動收集的證據。

### 必要條件

- 一個手動證據檔案的最大支援 100 MB。
- 您必須使用其中一個[手動證據支援的檔案格式](#)。
- 每個控制項每天最多 AWS 帳戶 可以手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。
- 當控制項處於非作用中狀態時，您無法添加手動證據至該控制項。若要新增手動證據，您必須先將[控制狀態變更](#)為「審核中」或「已審核」。
- 確保您的 IAM 身分具有管理中評估的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來匯入檔案。

#### AWS console

在 Audit Manager 主控台上從 S3 匯入檔案

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估，然後選擇評估。
3. 選擇 [控制項] 索引標籤，向下捲動至 [控制項集]，然後選擇控制項。
4. 在證據資料夾索引標籤上，選擇添加手動證據，然後選擇從 S3 匯入檔案。
5. 在下一頁，輸入證據的 S3 URI。您可以瀏覽至 [Amazon S3 主控台](#) 中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。
6. 選擇上傳。

## AWS CLI

在下列程序中，將#####取代為您自己的資訊。

若要從中的 S3 匯入檔案 AWS CLI

1. 執行 [list-assessments](#) 命令查看評估清單。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 [get-assessment](#) 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

另外，找到控制集和您要向其上上傳證據的控制項，並記下 ID。

3. 執行 [batch-import-evidence-to-assessment-control](#) 命令搭配下列參數：

- `--assessment-id` — 使用步驟 1 中的評估 ID。
- `--control-set-id` — 使用步驟 2 中的控制集 ID。
- `--control-id` — 使用步驟 2 中的控制項 ID。
- `--manual-evidence` — 使用 `s3ResourcePath` 作為手動證據類型，並指定證據的 S3 URI。您可以瀏覽至 [Amazon S3 主控台](#) 中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://DOC-EXAMPLE-BUCKET/EXAMPLE-FILE.extension
```

## Audit Manager API

若要使用 API 從 S3 匯入檔案

1. 呼叫 [ListAssessments](#) 操作查看您的評估清單。另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 呼叫 [GetAssessment](#) 操作並指定步驟 1 的評估 ID。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。
3. 搭配下列參數呼叫 [BatchImportEvidenceToAssessmentControl](#) 操作：
  - [assessmentId](#) — 使用步驟 1 中的評估 ID。
  - [controlSetId](#) — 使用步驟 2 中的控制集 ID。
  - [controlId](#) — 使用步驟 2 中的控制項 ID。
  - [manualEvidence](#) — 使用 `s3ResourcePath` 作為手動證據類型，並指定證據的 S3 URI。您可以瀏覽至 [Amazon S3 主控台](#) 中的物件，然後選擇複製 S3 URI 以尋找 S3 URI。

如需詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

新增並檢閱評估的證據後，您可以產生評估報告。如需詳細資訊，請參閱 [準備評估報告 AWS Audit Manager](#)。

## 其他資源

若要瞭解您可以使用哪些檔案格式，請參閱 [手動證據支援的檔案格式](#)。

## 從瀏覽器上傳手動證據檔案

您可以從瀏覽器手動將證據檔案上傳至 Audit Manager 評估。這使您可以額外的輔助材料補充自動收集的證據。

### 必要條件

- 一個手動證據檔案的最大支援 100 MB。
- 您必須使用其中一個 [手動證據支援的檔案格式](#)。
- 每個控制項每天最多 AWS 帳戶 可以手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。
- 當控制項處於非作用中狀態時，您無法添加手動證據至該控制項。若要新增手動證據，您必須先將 [控制狀態變更](#) 為「審核中」或「已審核」。

- 確保您的 IAM 身分具有管理中評估的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 上傳檔案。

### AWS console

在 Audit Manager 主控台上從瀏覽器上傳檔案的步驟

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估，然後選擇評估。
3. 在 [控制項] 索引標籤上，向下捲動至 [控制組]，然後選擇控制項。
4. 在「證據」資料夾標籤中，選擇「新增手動證據」。
5. 選擇從瀏覽器上傳檔案。
6. 選擇您要上傳的檔案。
7. 選擇上傳。

### AWS CLI

在下列程序中，將#####取代為您自己的資訊。

若要在瀏覽器中上傳檔案 AWS CLI

1. 執行 [list-assessments](#) 命令查看評估清單。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 [get-assessment](#) 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```



另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 執行 `get-evidence-file-upload-url` 命令並指定您要上傳的檔案。

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

此外，記下預先簽章的 URL 和 `evidenceFileName`。

4. 使用步驟 3 中的預先簽署 URL，從瀏覽器上傳檔案。此動作會將您的檔案上傳到 Amazon S3，並將其儲存為可附加至評估控制項的物件。在下面的步驟中，您將使用 `evidenceFileName` 參數引用新建立的物件。

#### Note

當您使用預先簽署的 URL 上傳檔案時，Audit Manager 會使用伺服器端加密功能來保護和儲存您的 AWS Key Management Service 資料。為此，當您使用預先簽署的 URL 上傳檔案時，您必須在請求中使用 `x-amz-server-side-encryption` 標頭。如果您使用的是 AWS KMS key 在稽核管理員 [設定您的資料加密設定](#) 設定中管理的客戶，請務必在請求中也包含 `x-amz-server-side-encryption-aws-kms-key-id` 標頭。如果請求中沒有 `x-amz-server-side-encryption-aws-kms-key-id` 標頭，Amazon S3 會假設您想要使用 AWS 受管金鑰。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密使用 [金 AWS Key Management Service 鑰 \(SSE-KMS\) 保護資料](#)。

5. 執行 `batch-import-evidence-to-assessment-control` 命令搭配下列參數：

- `--assessment-id` — 使用步驟 1 中的評估 ID。
- `--control-set-id` — 使用步驟 2 中的控制集 ID。
- `--control-id` — 使用步驟 2 中的控制項 ID。
- `--manual-evidence` — 使用 `evidenceFileName` 作為手動證據類型，並指定步驟 3 中的證據檔案名稱。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence evidenceFileName=fileName.extension
```

## Audit Manager API

### 使用 API 從瀏覽器上傳檔案

1. 呼叫 [ListAssessments](#) 操作。另外，找到您要向其上傳證據的評估，並記下評估 ID。
2. 呼叫 [GetAssessment](#) 操作並指定步驟 1 的 `assessmentId`。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。
3. 呼叫 [GetEvidenceFileUploadUrl](#) 操作並指定您要上傳的 `fileName`。此外，記下預先簽署的 URL 和 `evidenceFileName`。
4. 使用步驟 3 中的預先簽署 URL，從瀏覽器上傳檔案。此動作會將您的檔案上傳到 Amazon S3，並將其儲存為可附加至評估控制項的物件。在下面的步驟中，您將使用 `evidenceFileName` 參數引用新建立的物件。

#### Note

當您使用預先簽署的 URL 上傳檔案時，Audit Manager 會使用伺服器端加密功能來保護和儲存您的 AWS Key Management Service 資料。為此，當您使用預先簽署的 URL 上傳檔案時，您必須在請求中使用 `x-amz-server-side-encryption` 標頭。如果您使用的是 AWS KMS key 在稽核管理員 [設定您的資料加密設定](#) 設定中管理的客戶，請務必在請求中也包含 `x-amz-server-side-encryption-aws-kms-key-id` 標頭。如果請求中沒有 `x-amz-server-side-encryption-aws-kms-key-id` 標頭，Amazon S3 會假設您想要使用 AWS 受管金鑰。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密使用 [金 AWS Key Management Service \(SSE-KMS\) 保護資料](#)。

5. 搭配下列參數呼叫 [BatchImportEvidenceToAssessmentControl](#) 操作：
  - [assessmentId](#) — 使用步驟 1 中的評估 ID。
  - [controlSetId](#) — 使用步驟 2 中的控制集 ID。
  - [controlId](#) — 使用步驟 2 中的控制項 ID。
  - [manualEvidence](#) — 使用 `evidenceFileName` 作為手動證據類型，並指定步驟 3 中的證據檔案名稱。

如需詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

收集並檢閱評估的證據後，您可以產生評估報告。如需詳細資訊，請參閱 [準備評估報告 AWS Audit Manager](#)。

## 其他資源

若要瞭解您可以使用哪些檔案格式，請參閱 [手動證據支援的檔案格式](#)。

## 輸入任意格式文字回應作為手動辨識

您可以輸入任意格式文字並將該文字儲存為證據，以提供評估控制項的其他上下文和支援資訊。這使您可以手動記錄未通過自動證據收集捕獲的詳細信息。

例如，您可以使用 Audit Manager 建立自訂控制項，以代表供應商風險評估問卷中的問題。在此情況下，每個控制項的名稱都是特定問題，會要求您提供有關組織安全性和規範遵循狀況的資訊。若要記錄您對特定供應商風險評估問題的回應，您可以輸入文字回應，並將其儲存為控制項的手動證據。

## 必要條件

- 當控制項處於非作用中狀態時，您無法添加手動證據至該控制項。若要新增手動證據，您必須先將 [控制狀態變更](#) 為「審核中」或「已審核」。
- 確保您的 IAM 身分具有管理中評估的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、稽 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來輸入文字回應。

### AWS console

若要在 Audit Manager 主控台上輸入文字回應

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估，然後選擇評估。
3. 選擇 [控制項] 索引標籤，向下捲動至 [控制項集]，然後選擇控制項。

4. 在「證據」資料夾標籤中，選擇「新增手動證據」。
5. 選擇 [輸入文字回應]。
6. 在出現的快顯視窗中，輸入純文字格式的回應。
7. 選擇確認。

## AWS CLI

在下列程序中，將#####取代為您自己的資訊。

若要輸入文字回應 AWS CLI

1. 執行 [list-assessments](#) 命令。

```
aws auditmanager list-assessments
```

另外，找到您要向其上傳證據的評估，並記下評估 ID。

2. 執行 [get-assessment](#) 命令並指定步驟 1 的評估 ID。

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。

3. 執行 [batch-import-evidence-to-assessment-control](#) 命令搭配下列參數：

- `--assessment-id` — 使用步驟 1 中的評估 ID。
- `--control-set-id` — 使用步驟 2 中的控制集 ID。
- `--control-id` — 使用步驟 2 中的控制項 ID。
- `--manual-evidence` — 使用 `textResponse` 作為手動證據類型，然後輸入要保存為手動證據的文字。

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter text here"
```

## Audit Manager API

使用 API 輸入文字回應

1. 呼叫 [ListAssessments](#) 操作。另外，找到您要向其上傳證據的評估，並記下評估 ID。
2. 呼叫 [GetAssessment](#) 操作並指定步驟 1 的 `assessmentId`。另外，找到控制集和您要向其上傳證據的控制項，並記下 ID。
3. 搭配下列參數呼叫 [BatchImportEvidenceToAssessmentControl](#) 操作：
  - [assessmentId](#) — 使用步驟 1 中的評估 ID。
  - [controlSetId](#) — 使用步驟 2 中的控制集 ID。
  - [controlId](#) — 使用步驟 2 中的控制項 ID。
  - [manualEvidence](#) — 使用 `textResponse` 作為手動證據類型，然後輸入要保存為手動證據的文字。

如需詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

收集並檢閱評估的證據後，您可以產生評估報告。如需詳細資訊，請參閱 [準備評估報告 AWS Audit Manager](#)。

## 手動證據支援的檔案格式

下表列出並說明您可以將其作為手動證據上傳的檔案類型。對於每種檔案類型，表格也會列出支援的副檔名。

檔案類型	描述	支援的檔案副檔名
壓縮或存檔	GNU Zip 壓縮的封存檔和 ZIP 壓縮的封存檔	.gz, .zip
文件	常見的文件檔案，例如 PDF 和 Microsoft Office 檔案	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx

檔案類型	描述	支援的檔案副檔名
映像	圖像和圖形檔案	.jpeg, .jpg, .png, .svg
文字	其他非二進位文字檔案，例如純文字文件和標記語言檔案	.cer, .csv, .html, .jmx, .json, .md, .out, .rtf, .txt, .xml, .yaml, .yml

## 其他資源

檢閱下列頁面，瞭解可將自己的證據新增至評估控制項的不同方式。

- [從 Amazon S3 匯入手動證據檔案](#)
- [從瀏覽器上傳手動證據檔案](#)
- [輸入任意格式文字回應作為手動辨識](#)

## 準備評估報告 AWS Audit Manager

收集並檢閱評估的證據後，您可以產生評估報告。評估報告會概述您的評估，並提供包含相關證據的組織資料夾集的連結。

### 重點

新收集的證據不會自動出現在評估報告中。這表示您可以控制要包含在報告中的證據。選取要包含的證據後，您可以產生最終評估報告，以便與稽核人員共用。

產生評估報告時，會將其放置在您選擇作為評估報告目的地的 S3 儲存貯體中。您也可以從「Audit Manager」的下載中心下載評估報告。

### 其他資源

如需有關評量報告及其管理方式的詳細資訊，請參閱下列資源。

- [將證據添加至評估報告](#)
- [從評估報告中移除證據](#)
- [產生評估報告](#)

- [下載評估報告](#)
- [瀏覽評估報告並探索其內容](#)
- [驗證評估報告](#)
- [刪除評估報告](#)
- [從您的證據查找器搜索結果生成評估報告](#)
- [設定您的預設評估報告目標](#)
- [評估報告問題疑難排解](#)

## 將證據添加至評估報告

您必須至少在評估報告中添加一項證據，才能產生評估報告。您可以新增整個證據資料夾，也可以從資料夾中新增特定證據項目。

### 程序

要在評估報告中包括證據，請按照以下步驟操作。

#### 如需將證據添加至評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估，然後選擇評估。
3. 在「控制項」標籤上，向下捲動至「控制項集」表，然後選擇含有您要包含在評估報告中之證據的控制項。
4. 選擇將證據添加至評估報告的方式。
  - a. 如需添加整個證據資料夾，請向下捲動至證據資料夾，選擇您要添加的資料夾，然後選擇添加至評估報告。

#### Tip

如果您看不到要尋找的資料夾，請將下拉式清單篩選條件變更為所有時間。否則，依預設，您會看到最近七天的資料夾。

如果添加至評估報告呈灰色，表示證據資料夾已添加至評估報告。

- b. 如需添加特定證據，請選擇證據資料夾以開啟其內容。從清單中選擇一個或多個項目，然後選擇添加至評估報告。

 Tip

如果添加至評估報告顯示為灰色，請確定您已選擇證據旁的核取方塊，然後再試一次。

5. 將證據添加至評估報告後，會出現綠色的成功橫幅。選擇在評估報告中檢視證據查看將包含在評估報告中的證據。
  - 或者，您可以導覽回您的評估並選擇評估報告選擇索引標籤，查看將包含在評估報告中的證據。

## 後續步驟

如果您需要從評估報告中移除證據，請參閱[從評估報告中移除證據](#)。

當您準備好產生評估報告時，請參閱[產生評估報告](#)。

## 其他資源

若要尋找常見問題和問題的解答，請參閱[評估報告問題疑難排解](#)本指南的「疑難排解」一節。

## 從評估報告中移除證據

如果您需要從評估報告中移除證據，請按照下列步驟操作。您可以移除整個證據資料夾，也可以從資料夾中移除特定證據。

### 程序

如需從評估報告中移除證據

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估，然後選擇評估的名稱來將其開啟。
3. 在控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱將其開啟。
4. 選擇您要從評估報告中移除證據的方式。



- a. 如需移除整個證據資料夾，請向下捲動至證據資料夾，選擇您要移除的資料夾，然後選擇從評估報告中移除。

**i** Tip

如果您看不到要尋找的資料夾，請將下拉式清單篩選條件變更為所有時間。否則，依預設，您會看到最近七天的資料夾。

如果從評估報告中移除顯示為灰色，表示證據資料夾已從評估報告中移除。

- b. 如需移除特定證據，請選擇證據資料夾以開啟其內容。從清單中選擇一個或多個項目，然後選擇從評估報告中移除。

**i** Tip

如果從評估報告中移除顯示為灰色，請確定您已選擇證據旁的核取方塊，然後再試一次。

5. 將證據添加至評估報告後，會出現綠色的成功橫幅。選擇在評估報告中檢視證據查看將包含在評估報告中的證據。
  - 或者，您可以導覽回您的評估並選擇評估報告選擇索引標籤，查看將包含在評估報告中的證據。

## 後續步驟

當您準備好產生評估報告時，請參閱[產生評估報告](#)。

## 其他資源

若要尋找常見問題和問題的解答，請參閱[評估報告問題疑難排解](#)本指南的「疑難排解」一節。

## 產生評估報告

當您準備好產生評估報告時，請依照下列步驟操作。

### 必要條件

您必須至少在評估報告中添加一項證據，才能產生評估報告。您可以添加整個證據資料夾，也可以添加資料夾中的單項證據。

為確保成功產生評估報告，請檢閱 [評估報告目的地的組態提示](#)。

## 程序

### 產生評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇評估。
3. 選擇您要為其產生評估報告的評估的名稱。
4. 選擇評估報告選擇索引標籤，然後選擇產生評估報告。

#### Tip

如果產生評估報告顯示為灰色，表示尚未將證據添加至評估報告。

5. 在快顯視窗中，提供評估報告的名稱和描述，並檢閱評估報告詳細資訊。
6. 選擇產生評估報告，數分鐘後便會產生評估報告。
7. 您可以從 Audit Manager 主控台的下載中心頁面，找到並下載評估報告。
  - 或者，您可以前往評估報告目的地 S3 儲存貯體，然後從該處下載評估報告。

## 後續步驟

產生評估報告後，您可以進一步了解以下資訊：

- 尋找並下載您的評估報告 — 了解如何從 [下載中心](#) 或 [Amazon S3](#) 下載評估報告。
- 探索您的評估報告 — 了解如何 [導覽評估報告並探索其內容](#)。
- 驗證您的評估報告 — 瞭解如何使用 [ValidateAssessmentReportIntegrity](#) API 作業來驗證您的評估報告。
- 刪除不需要的評估報告 — 了解如何從 [下載中心](#) 或 [Amazon S3](#) 刪除不需要的報告。
- 從證據查找器生成評估報告 — 了解如何 [從證據查找器搜索結果中生成評估報告](#)。

## 其他資源

若要尋找常見問題和問題的解答，請參閱 [評估報告問題疑難排解](#) 本指南的「疑難排解」一節。

## 變更評估控制項的狀態 AWS Audit Manager

您可以在使用中的評估中變更評量控制項的狀態。更新控制項的狀態可讓您追蹤其進度，並指出何時檢閱控制項，讓您的評估井然有序 up-to-date。

### 必要條件

下列程序假設您先前已建立評估，且其目前狀態為作用中狀態。

確保您的 IAM 身分具有管理中評估的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來更新評估控制項狀態。

#### Note

將控制項狀態變更為已檢閱該操作不可變更。將控制項的狀態設定為已檢閱之後，就無法再變更該控制項的狀態或還原為先前的狀態。

#### Audit Manager console

在 Audit Manager 主控台上變更評估控制狀態

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估。
3. 選擇評估名稱來開啟評估。
4. 在評估頁面上，選擇控制項索引標籤，向下捲動至控制集表格，然後選擇控制項名稱來開啟。
5. 選擇頁面右上角的 [更新控制項狀態]，然後選擇狀態：

狀態	描述
正在審查中	如果您尚未檢閱控制項，請選擇此狀態。

狀態	描述
已審閱	如果您已完成此控制項的證據複查，並且想要繼續收集或新增證據，請選擇此狀態。
非作用中	如果您要停止收集此控制項的自動證據，請選擇此狀態。

- 選擇 [更新控制狀態] 以確認您的選擇。

## AWS CLI

若要變更評估控制狀態 AWS CLI

- 運行[列表評估](#)命令。

```
aws auditmanager list-assessments
```

執行後，傳回評估清單。尋找包含您要更新之控制項的評估，並記下評估 ID。

- 執行取[得評估](#)命令，並從步驟 1 指定評估 ID。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

在回應中，尋找您要更新的控制項，並記下控制項 ID 及其控制集識別碼。

- 執行命[update-assessment-control](#)令並指定下列參數：

- assessment-id— 控制項所屬的評估。
- control-set-id— 控制項所屬的控制項集。
- control-id— 您要更新的控制項。
- control-status— 將此值設定為UNDER\_REVIEWREVIEWED、或INACTIVE。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager update-assessment-control --assessment-id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

## Audit Manager API

### 使用 API 變更評估控制狀態

1. 使用[ListAssessments](#)操作。

在回應中，尋找包含您要更新之控制項的評量，並記下評估 ID。

2. 使用[GetAssessment](#)作業並指定步驟 1 中的評估 ID。

在回應中，尋找您要更新的控制項，並記下控制項 ID 及其控制集識別碼。

3. 使用[UpdateAssessmentControl](#)作業並指定下列參數：

- [assessmentId](#)— 控制項所屬的評估。
- [controlSetId](#)— 控制項所屬的控制項集。
- [controlId](#)您要更新的控制項。
- [controlStatus](#)— 將此值設定為UNDER\_REVIEWREVIEWED、或INACTIVE。

如需有關這些 API 作業的詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

當您準備好變更評估狀態時，請參閱[在中將評估的狀態變更為非作用中 AWS Audit Manager](#)。

## 在中將評估的狀態變更為非作用中 AWS Audit Manager

當您不再需要收集評估的證據時，您可以將評估狀態變更為非作用中。當評估的狀態變更為非作用中時，評估就會停止收集證據。因此，針對該評估，您不會再產生任何費用。

除了停止證據收集之外，Audit Manager 還可以對非作用中評估內的控制項進行下列變更：

- 所有控制集都變更為已檢閱狀態。
- 處於審核中狀態的所有控制項變更為已審核
- 非作用中評估的委派人員無法再檢視或編輯其控制項和控制集。

## 必要條件

下列程序假設您先前已建立評估，且其目前狀態為作用中狀態。

確保您的 IAM 身分具有管理中評估的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、稽核管 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來更新評估狀態。

### Warning

此動作不可復原。我們建議您謹慎進行，並確認您確實希望將評估標記為非作用中。當評估處於非作用中狀態時，您只有唯讀存取權。這表示您仍然可以檢閱先前收集的證據並產生評估報告。然而，您無法編輯非作用中的評估、新增註解或上傳任何手動證據。

## Audit Manager console

若要在 Audit Manager 主控台上將評估狀態變更為非作用中

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估。
3. 選擇評估名稱來開啟評估。
4. 在頁面右上角選擇更新評估狀態，然後選擇非作用中。
5. 在快顯視窗中選擇更新狀態，以確認您要將狀態變更為非作用中。

評估及其控制項的變更會在大約一分鐘後生效。

## AWS CLI

若要將評估狀態變更為非作用中 AWS CLI

1. 首先，識別您要更新的評估。為此，執行 [list-assessments](#) 命令。

```
aws auditmanager list-assessments
```

執行後，傳回評估清單。找到您要停用的評估，並記下評估 ID。

2. 接下來，運行 [update-assessment-status](#) 命令並指定以下參數：
  - `--assessment-id` — 使用此參數可指定您要停用的評估。
  - `--status` – 將此值設定為 `INACTIVE`。

在下列範例中，將 `#####` 取代之為您自己的資訊。

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-  
cdef-EXAMPLE11111 --status INACTIVE
```

評估及其控制項的變更會在大約一分鐘後生效。

## Audit Manager API

使用 API 將評估狀態變更為非作用中

1. 使用此 [ListAssessments](#) 作業尋找您要停用的評估，並記下評估 ID。
2. 使用 [UpdateAssessmentStatus](#) 作業並指定下列參數：
  - [assessmentId](#) — 使用此參數可指定您要停用的評估。
  - [status](#) — 將此值設定為 `INACTIVE`。

評估及其控制項的變更會在大約一分鐘後生效。

如需有關這些 API 作業的詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

當您確定不再需要非使用中的評估時，可以刪除評估來清除 Audit Manager 環境。如需說明，請參閱[刪除中的評估 AWS Audit Manager](#)。

## 刪除中的評估 AWS Audit Manager

當您不再需要評估時，可以將其從 Audit Manager 環境中刪除。這可讓您清理工作區，並專注於與目前工作和優先順序相關的評量。

### Tip

如果您的目標是降低成本，請考慮將[評估狀態變更為非作用中](#)，而不是將其刪除。此動作會停止證據收集，並將您的評估置於唯讀狀態，您可以在其中檢閱先前收集的證據。非作用中的評估不會產生任何費用。

## 必要條件

下列程序假設您先前已建立評估。

確保您的 IAM 身分具有適當的許可，可以刪除中的評估 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 刪除評估。

### Warning

此動作會永久刪除您的評估及其收集的所有證據。您無法復原此資料。因此，我們建議您謹慎行事，並確定您真的要刪除您的評估。



## Audit Manager console

若要刪除稽核管理員主控台上的評估

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估。
3. 選擇您要刪除的評估，然後選擇刪除。

## AWS CLI

若要刪除中的評估 AWS CLI

1. 首先，確定您要刪除的評估。為此，執行 [list-assessments](#) 命令。

```
aws auditmanager list-assessments
```

執行後，傳回評估清單。找到您要刪除的評估，並記下評估 ID。

2. 接下來，使用 [delete-assessment](#) 命令，並指定要刪除的評估 `--assessment-id`。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111
```

## Audit Manager API

若要使用 API 刪除評估

1. 使用此 [ListAssessments](#) 作業尋找您要刪除的評量。

此外，記下評估 ID。

2. 使用 [DeleteAssessment](#) 作業並指定您要刪除之評估的評估 ID。

有關此 API 操作的更多資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一項特定語言 AWS 軟體開發套件中使用這些操作和參數的資訊。

## 其他資源

如需 Audit Manager 中資料保留的相關資訊，請參閱[刪除 Audit Manager 資料](#)。

# 中的代表團 AWS Audit Manager

當您瀏覽中的評估程序時 AWS Audit Manager，您可能會遇到需要主題專家協助以檢閱和驗證所收集的證據的情況。這是代表團的概念發揮作用的地方。

## 重點

委派可讓**稽核擁有者**將特定控制集指派給**委託人** — 在相關領域具有專業知識的個人。透過使用委派功能，您可以確保每個控制項的證據均由適當的人員徹底評估。這有助於您簡化審核流程，並提高評估的整體準確性和可靠性。無論您是需要有關解釋技術證據、澄清合規性要求，還是獲得特定領域的更深入見解的指導，代表團都能讓您與主題專家有效地協作。

在高層次上，委託過程如下：

1. 稽核擁有者會在其評估中選擇控制項集，並委派該控制項集以供審核。
2. 委派人會對這些控制項及其證據進行審核，完成後將控制項集回傳給稽核擁有者。
3. 稽核擁有者會被通知審核已完成，並檢查委派人對審核的控制項是否有任何備註。

### Note

AWS 帳戶 可以是稽核擁有者，也可以是不同的委託人 AWS 區域。

## 其他資源

您可以使用本章的下列各節，進一步瞭解如何在中管理委派作業 AWS Audit Manager。

- [瞭解稽核擁有者的不同委派作業](#)
  - [委派要檢閱的控制集 AWS Audit Manager](#)
  - [尋找並檢閱您所傳送的委託 AWS Audit Manager](#)
  - [在中刪除已完成的委託 AWS Audit Manager](#)
- [瞭解委派的不同委派工作](#)
  - [查看您的委派請求通知](#)

- [審核委派的控制集及其相關證據](#)
- [在控制集檢閱期間新增有關控制項的註解](#)
- [將控制項標示為檢閱 AWS Audit Manager](#)
- [將已檢閱的控制集送交回稽核擁有者](#)

## 瞭解稽核擁有者的不同委派作業

身為中的稽核擁有者 AWS Audit Manager，您必須負責管理評估並確保組織內的合規性。雖然您具備治理、風險和法規遵循方面的專業知識，但有時候您可能遇到問題或需要主題專家的協助，才能檢閱和解釋特定的技術證據或控制。這是 Audit Manager 中的委派功能變得有用的地方。

### 重點

建立委派可讓您將評估中的控制集指派給具有相關領域專業知識或技術專業知識的其他 Audit Manager 使用者 (稱為委派)。然後，這些委派人員可以複查指派的控制集、分析收集的證據、視需要提供註解或其他證據，以及更新個別控制項的狀態。

委派處理可運用組織內的集體專業知識，簡化控制項的複查與驗證。它可確保每個控制項都由最合格的人員進行徹底評估，從而提高評估的準確性和可靠性。

### 其他資源

下列各節將引導您完成與以稽核擁有者身分管理委託相關聯的不同工作。這包括如何委派控制集、追蹤委託狀態以及管理已完成的委託。透過有效地使用委派，您可以與主題專家協同合作、運用他們的專業知識，並在 Audit Manager 中維護全面且明智的稽核流程。

- [委派要檢閱的控制集 AWS Audit Manager](#)
- [尋找並檢閱您所傳送的委託 AWS Audit Manager](#)
- [在中刪除已完成的委託 AWS Audit Manager](#)

## 委派要檢閱的控制集 AWS Audit Manager

當您需要主題專家的協助時，您可以選擇 AWS 帳戶 要協助您的項目，然後將控制集委派給他們進行審核。

## 必要條件

確保您的 IAM 身分具有在中建立委派的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用下列任一程序以委派控制集。

### 從評估頁面委派控制集

#### 從評估頁面委派一個控制集

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇評估。
3. 選擇包含您要委派的控制集評估名稱。
4. 在評估頁面中，選擇控制項索引標籤。這會顯示評估中的控制項狀態摘要和控制項清單。
5. 選取控制集，然後選擇委派控制集。
6. 在委派選取下，會顯示使用者和角色的清單。選擇使用者或角色，或使用搜尋列以尋找使用者或角色。
7. 在委派詳細資訊下，審核控制集名稱和評估名稱。
8. (選擇性) 在評論下，新增附有指示的評論，以協助委派完成其審核任務。請勿在您的評論中包含任何敏感資訊。
9. 選擇委派控制集。
10. 綠色成功橫幅可確認控制集委派成功。選擇檢視委派來查看委派請求。您也可以在主控台左側導覽窗格中選擇 [委派]，隨時檢視委託。AWS Audit Manager

### 從委派頁面委派一個控制集

#### 從委派頁面委派一個控制集

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇委派。
3. 在委派頁面中，選擇 建立委派。

4. 在選擇評估與控制集下，指定您要委派的評估和控制集。
5. 在委託選擇下，您將看到用戶和角色的清單。選擇使用者或角色，或使用搜尋列以尋找使用者或角色。
6. (選擇性) 在評論下，新增附有指示的評論，以協助委派完成其審核任務。請勿在您的評論中包含任何敏感資訊。
7. 選擇 建立委派。
8. 綠色成功橫幅可確認控制集委派成功。選擇檢視委派來查看委派請求。您也可以在主控台左側導覽窗格中選擇 [委派]，隨時檢視委託。AWS Audit Manager

委派控制集進行審核之後，委派人會收到通知，然後可以開始複查控制集。委派人的遵循流程在[瞭解委派的的不同委派工作](#)中有所描述。

## 後續步驟

若要稍後重新審視您的委派，請參閱[尋找並檢閱您所傳送的委託 AWS Audit Manager](#)。

## 尋找並檢閱您所傳送的委託 AWS Audit Manager

您可以隨時存取委託清單，方法是選擇「Audit Manager」左側導覽窗格中的 [委託]。[委託] 頁面包含使用中和已完成委託的清單。

委託完成後，您會在 Audit Manager 中收到通知。您也可能會收到來自委託人的評論和評論。下列程序說明如何在 Audit Manager 中檢查委託完成後，以及如何檢視委派可能為您留下的任何註解。

## 必要條件

請確定您的 IAM 身分具有適當的許可，以檢視中的委派 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

請依照下列步驟尋找並檢閱您先前建立的委託。

### 檢視已完成的委託並檢查評論

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。

2. 在導覽窗格中，選擇委派。
3. 檢閱 [委派] 頁面，其中包含含下列資訊的表格：

名稱	描述
委派給	您委派控制項集的對象。AWS 帳戶
日期	委派控制集的日期。
狀態	委派的目前狀態。
評估	包含評量詳細資訊頁面連結的評量名稱。
控制集	委派要複查之控制集的名稱。

4. 尋找委派人已審核並送交給您的評估與控制集，然後選擇要開啟的評估名稱。
5. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
6. 在 [依控制項集分組的控制項] 底下，尋找您所委派之控制集的名稱。
7. 展開控制項集的名稱以顯示其控制項，然後選擇控制項名稱以開啟控制項詳細資訊頁面。
8. 選擇評論索引標籤，以檢視委派人針對特定控制項新增的任何備註。
9. 如果您滿意控制集的檢閱已完成，請選取控制集，然後選擇 [完成控制集檢閱]。

#### Important

Audit Manager 會持續收集證據。因此，在委派完成對控制項的檢閱後，可能會收集其他新證據。

如果您只想在評估報告中使用已審核過的證據，則可以參考控制項審核的時間戳記，來確定何時審核證據。您可以在控制項詳細資訊頁 [Changelog 索引標籤](#) 面上找到此時間戳記。接著，您可以使用此時間戳記來分辨要新增至評估報告的證據。

## 後續步驟

若要在委派完成後刪除，而您不再需要它，請參閱 [在中刪除已完成的委託 AWS Audit Manager](#)。

## 在中刪除已完成的委託 AWS Audit Manager

在某些情況下，您可能會建立委派，但之後不再需要協助審核該控制集。發生這種情況時，您可以在 Audit Manager 中刪除作用中的委派。您也可以刪除不再想在委託頁面上看到的已完成委託。

## 必要條件

請確定您的 IAM 身分具有適當的許可，可在中刪除委派 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

### 刪除委派

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇委派。
3. 在委派頁面上，選取您要取消的委派，然後選擇移除委派。
4. 在出現的快顯視窗中，選擇刪除來確認您的選擇。

## 瞭解委派的不同委派工作

身為中的委派 AWS Audit Manager，您在評估程序期間支援稽核擁有者方面扮演重要角色。雖然[稽核擁有者](#)負責管理評估並確保整體合規性，但他們有時可能需要主題專家的協助，以檢閱和解釋超出其專業領域的特定技術證據。在這種情況下，您的知識和技能變得非常寶貴。

## 重點

委派功能可讓稽核擁有者指派特定控制集給您以供檢閱，並深入瞭解您的專業業務或技術專業知識。這種協同合作方法不僅可以提高評估的準確性和可靠性，還可以簡化審核流程，使稽核擁有者能夠專注於他們的核心職責，同時您將精力集中在您的專業知識最有價值的領域上。

身為委派人，您可能會收到來自稽核擁有者的要求，以檢閱與指定控制集相關聯的證據。您可以協助稽核擁有者，方法是審核控制集及其相關證據、新增評論、上傳其他證據，以及更新您審核的各控制項狀態。



### Note

稽核擁有者委派特定控制集以供審核，而非整個評估。因此，委派代表對評估的存取權限有限。委派可以審核證據、新增評論、上傳手動證據，以及更新控制項集中每個控制項的控制項狀態。如需有關 Audit Manager 中角色和許可的詳細資訊，請參閱 [中使用者角色的建議政策 AWS Audit Manager](#)。

## 其他資源

在以下各節中，您可以進一步瞭解與以委派身分管理委派相關聯的任務。這包括如何檢視內送委派請求、複查指定的控制集、提供附註與其他證據，以及如何將複查的控制項提交回稽核擁有者。

- [查看您的委派請求通知](#)
- [審核委派的控制集及其相關證據](#)
- [在控制集檢閱期間新增有關控制項的註解](#)
- [將控制項標示為檢閱 AWS Audit Manager](#)
- [將已檢閱的控制集送交回稽核擁有者](#)

## 查看您的委派請求通知

當稽核擁有者請求您協助審核控制集時，您會收到通知，通知您委派給您的控制集。

### 必要條件

確保您的 IAM 身分具有適當的許可，可以在中查看通知 AWS Audit Manager。授與這些權限的兩個建議政策是 [授予使用者 AWS Audit Manager 的完整管理員存取權](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。


### 程序

若要檢視您的通知

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇通知。

3. 在通知頁面上，檢閱已委派給您進行審核的控制集清單。此表格包含以下資訊：

名稱	描述
日期	委派控制集的日期。
評估	與控制集相關聯的評估名稱。
控制集	控制集的名稱。
來源	委派控制項集給您的使用者或角色。
Description	稽核擁有者所提供的指示。

 Tip

您也可以訂閱 SNS 主題，以便在控制集委派給您以供檢閱時接收電子郵件提醒。如需詳細資訊，請參閱 [通知 AWS Audit Manager](#)。

## 後續步驟

當您準備好開始檢閱委派給您的控制項時，請參閱 [審核委派的控制集及其相關證據](#)。

## 審核委派的控制集及其相關證據

您可以透過檢閱稽核擁有者委託給您的控制集來協助他。

您可以檢查這些控制項及其相關證據，以判斷是否需要任何其他動作。此類額外動作可能包括 [手動上傳其他證據](#) 以證明合規性，或 [留下評論](#) 以說明您遵循的修正步驟。

## 必要條件

請確定您的 IAM 身分具有適當的許可，以檢視中的控制項集 AWS Audit Manager。授與這些權限的兩個建議政策是 [授予使用者 AWS Audit Manager 的完整管理員存取權](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

### 如需檢閱控制集

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇通知。
3. 在 [通知] 頁面上，您可以看到已委派給您的控制集清單。分辨您要檢閱的控制集，並選擇相關評估的名稱，以開啟評估詳細資訊頁面。
4. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
5. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。
6. 選擇控制項名稱以開啟控制項詳細資訊頁面。
7. (選擇性) 選擇更新控制項狀態以變更控制項的狀態。審核正在進行時，您可以將狀態標示為審核中。
8. 檢閱 [證據] 資料夾、[詳細資料]、[資料來源]、[註解] 和 [變更記錄檔] 索引標籤中的控制項
  - 若要瞭解這些索引標籤中的每個索引標籤，以及如何瞭解它們包含的資料，請參閱[檢閱中的評估控制 AWS Audit Manager](#)。

### 如需檢閱控制項的證據

1. 在控制項詳細資訊頁面中，選擇證據資料夾索引標籤。
2. 導覽至「證據」資料夾表格，以查看包含該控制項之證據的資料夾清單。這些資料夾是根據收集證據的日期來組織和命名。
3. 選擇證據資料夾的名稱以將其開啟。然後，查看在該日期收集的所有證據摘要。
  - 此摘要包括直接從 AWS Security Hub、AWS Config 或兩者報告的符合性檢查問題總數。
  - 若要瞭解有關此資訊的更多資訊，請參閱[檢閱中的證據資料夾 AWS Audit Manager](#)。
4. 從證據資料夾摘要頁面，瀏覽至證據表格。在「時間」欄下，選擇要開啟的證據。
5. 查看證據的詳細信息。
  - 若要瞭解有關此資訊的更多資訊，請參閱[檢閱中的證據 AWS Audit Manager](#)。

## 後續步驟

在某些情況下，您可能需要提供其他證據來證明合規性。在這些情況下，您可以手動上傳證據。如需說明，請參閱[在中添加手動證據 AWS Audit Manager](#)。

如果您要針對委派給您的一或多個控制項留下註解，請參閱[在控制集檢閱期間新增有關控制項的註解](#)。

## 在控制集檢閱期間新增有關控制項的註解

您可以為審核的任何控制項新增評論。稽核擁有者可以看見這些評論。

### 必要條件

請確定您的 IAM 身分具有適當的許可，可將註解新增至中的評估控制 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

若要將評論加入至控制項

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇通知。
3. 在通知頁面上，檢閱委派給您的控制集清單。
4. 尋找包含您要為其留下註解的控制項集，然後選擇相關評量的名稱以開啟評估。
5. 選擇控制項索引標籤，向下捲動至控制集表格，然後選取控制項名稱加以開啟。
6. 選擇評論索引標籤。
7. 在傳送評論底下，在文字方塊中輸入您的評論。
8. 選擇送交評論以新增您的評論。然後，您的註解會顯示在頁面的「上一個註解」區段下，以及與此控制項相關的任何其他註解。

## 後續步驟

完成控制項的檢閱後，請依照中的步驟執行[將控制項標示為檢閱 AWS Audit Manager](#)。

## 將控制項標示為檢閱 AWS Audit Manager

您可以透過更新控制集內個別控制項的狀態，以表明審核進度。

變更控制項狀態是選擇性的。不過，建議您在完成該控制項的審核時，將每個控制項的狀態變更為已審核。無論個別控制項的狀態為何，您仍然可以將控制項送交回稽核擁有者。

## 必要條件

確保您的 IAM 身分具有適當的許可，以更新中的評估控制狀態 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

如需將控制項標記為已審核

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇通知。
3. 在通知頁面上，檢閱委派給您的控制集清單。
4. 尋找您要標示為已複查的控制集，然後選擇相關評估的名稱以開啟評估。
5. 在評估詳細資訊頁面的控制項索引標籤下，向下捲動至控制集表格。
6. 在依控制集分組的控制項欄位下，展開控制集名稱以顯示其控制項。
7. 選擇控制項名稱以開啟控制項詳細資訊頁面。
8. 選擇更新控制項狀態，並將狀態變更為已審核。
9. 在出現的快顯視窗中，選擇更新控制項狀態，確認您已完成審核的控制項。

## 後續步驟

若要完成委派程序，請參閱[將已檢閱的控制集送交回稽核擁有者](#)。

## 將已檢閱的控制集送交回稽核擁有者

在檢閱控制項集、新增註解或其他證據，以及更新個別控制項的狀態之後，您會達到一個重要步驟 — 將已檢閱的控制項集提交回稽核擁有者。提交已審核的控制項集會標示委派任務的完成情況，並可讓稽核擁有者將您的見解和建議納入整體評估中。

## 必要條件

確保您的 IAM 身分具有適當的許可，可將審核的控制集提交回中的稽核擁有者 AWS Audit Manager。授與這些權限的兩個建議政策是[授予使用者 AWS Audit Manager 的完整管理員存取權](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

請遵循下列步驟，將控制項集提交給稽核擁有者。

若要將已審核的控制集送交回稽核擁有者，請執行

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇通知。
3. 檢閱委派給您的控制集清單。搜尋您要送交回稽核擁有者的控制集，然後選擇相關評估的名稱。
4. 向下捲動至控制集表格，選取要送交給稽核擁有者的控制集，然後選擇提交以供審核。
5. 在出現的快顯視窗中，您可以先新增評論，然後再選擇送出以供審核。

# 評估報告

評估報告總結了針對評估收集的選定證據。它還包含指向 PDF 檔案的連結，其中包含有關每項證據的詳細資訊。評估報告的具體內容、組織和命名慣例取決於您在[產生報告時選擇的](#)參數。

評估報告可協助您選擇和編譯與稽核相關的證據。但是，他們不會評估證據本身的合規性。相反地，Audit Manager 只會提供選定證據的詳細資訊作為您可與稽核人員共用的輸出。

## 內容

- [瞭解評估報告資料夾結構](#)
- [瀏覽評估報告](#)
- [檢閱評估報告的各個部分](#)
  - [封面](#)
  - [概觀頁面](#)
    - [報告摘要](#)
    - [評估摘要](#)
  - [目錄頁](#)
  - [控制項頁面](#)
    - [控制項摘要](#)
    - [收集的證據](#)
  - [證據摘要頁面](#)
  - [證據詳細資訊頁](#)
- [驗證評估報告](#)
- [其他資源](#)

## 瞭解評估報告資料夾結構

當您下載評估報告時，Audit Manager 會產生一個 zip 資料夾。這包含您的評估報告和巢狀子資料夾中的相關證據檔案。

zip 資料夾的結構如下所示：

- 評估資料夾 (範例：myAssessmentName-a1b2c3d4) — 根資料夾。

- 評估報告資料夾 (範例：reportName-a1b2c3d4e5f6g7) — 您可以在其中找到 AssessmentReportSummary .pdf、digest.txt 和 README.txt 檔案的子資料夾。
- 控制項證據資料夾 (範例：controlName-a1b2c3d4e5f6g) — 依相關控制項將證據檔案分組的子資料夾。
- 資料來源證據資料夾 (範例：CloudTrail,Security Hub) — 依資料來源類型將證據檔案分組的子資料夾。
  - 日期證據資料夾 (範例：2022-07-01) — 依證據收集日期將證據檔案分組的子資料夾。
  - 證據檔案 — 包含單個證據詳細資訊的檔案。

## 瀏覽評估報告

首先開啟 zip 資料夾，然後導覽下一層級至評估報告資料夾。在這裡，您可以找到評估報告 PDF 和 README.txt 檔案。

您可以檢閱 README.txt 檔案，了解 zip 資料夾的結構和內容。它還提供有關每個檔案命名慣例的參考資訊。如果您要尋找特定項目，這項資訊可協助您直接導覽至子資料夾或證據檔案。

否則，如需瀏覽證據並找到所需資訊，請開啟評估報告 PDF。其提供報告的高階概觀，以及建立報告所依據評估的摘要。

接下來，使用目錄 (TOC) 瀏覽報表。您可以選擇 TOC 中的任何超連結控制項，直接跳至該控制項的摘要。

當您準備好檢閱控制項的證據詳細資訊時，您可以選擇超連結的證據名稱來執行此操作。對於自動化證據，超連結會開啟一個新的 PDF 檔案，其中包含有關該證據的詳細資訊。對於手動證據，超連結會將您帶到包含證據的 S3 儲存貯體。

### Tip

每個頁面頂端的頁面導覽路徑導覽會在您瀏覽控制項和證據時，在評估報告中顯示您目前的位置。選擇超連結目錄，隨時導覽回目錄。

## 檢閱評估報告的各個部分

請使用下列資訊來進一步了解評估報告的各個區段。



**Note**

當您在下列區段中的任何屬性旁看到連字號 (-) 時，表示該屬性的值為 null，即值不存在。

- [封面](#)
- [概觀頁面](#)
- [目錄頁](#)
- [控制項頁面](#)
- [證據摘要頁面](#)
- [證據詳細資訊頁](#)

## 封面

封面包含評估報告的名稱。它也會顯示產生報表的日期和時間，以及產生報表之使用者的帳戶 ID。

封面的格式如下。Audit Manager 會以報告相關資訊取代####。

*Assessment report name*

Report generated on *MM/DD/YYYY* at *HH:MM:SS AM/PM UCT* by *AccountID*

## 概觀頁面

概觀頁面有兩個部分：報告本身的摘要，以及正在報告的評估摘要。

### 報告摘要

本區段總結評估報告。

名稱	描述
報告名稱	報告名稱。
Description	稽核擁有者產生報告時所輸入的描述。
產生日期	產生報告的日期。時間以國際標準時間 (UTC) 表示。

名稱	描述
包含的總控制	報告中包含並收集證據的控制項數目。這是評估中控制項總數的子集。
AWS 帳戶 包括	報告中包 AWS 帳戶 含並收集了證據的數量。這是評估總數 AWS 帳戶 的子集。
評估報告選擇	選取要包含在報告中的證據項目數。包含報告中發現的合規檢查問題總數。

## 評估摘要

本區段總結報告相關的評估。

名稱	描述
評估名稱	產生報告的評估名稱。
狀態	產生報告時的評估狀態。
評估地區	在中建立評估的。 AWS 區域
AWS 帳戶 在範圍內	這些清 AWS 帳戶 單在評估範圍內。
框架名稱	建立評估的來源架構名稱。
稽核擁有者	評估稽核擁有者的使用者或角色。
上次更新	上次更新評估的日期。時間以 UTC 表示。

## 目錄頁

目錄會顯示評估報告的完整目錄。目錄根據評估中包含的控制集進行分組和組織。控制項會列在其各自的控制集之下。

選擇目錄中的任何項目，直接導覽至報告的該區段。您可以選擇控制集，也可以直接前往控制項。

## 控制項頁面

控制項頁面有兩個部分：控制項本身的摘要，以及針對控制項收集的證據摘要。

### 控制項摘要

此區段包含下列資訊：

名稱	描述
控制項名稱	控制項的名稱。
Description	控制項的描述。
控制集	控制項所屬控制項集的名稱。
測試資訊	此控制項的建議測試程序。
行動計劃	如果控制項未完成，建議執行的動作。
評估報告選擇	評估報告中包含與此控制項相關的證據項目數目。這包括針對此控制項的證據找到的合規檢查問題數量。

### 收集的證據

本區段顯示針對控制項收集的證據。證據會依據資料夾分組，這些資料夾會依據證據收集日期進行組織與命名。每個證據資料夾名稱旁邊是該資料夾的合規檢查問題總數。

每個證據資料夾名稱下方都有超連結的證據名稱清單。

- 自動化證據名稱以證據收集時間戳記開頭，後跟服務代碼、事件名稱 (最多 20 個字元)、帳戶 ID 和 12 個字元的唯一 ID。

例如：21-30-24\_IAM\_CreateUser\_111122223333\_a1b2c3d4e5f6

對於自動化證據，超連結名稱會開啟一個新的 PDF 檔案，其中包含摘要和進一步的詳細資訊。

- 手動證據名稱以證據上傳時間戳記開頭，後跟 manual 標籤、帳戶 ID 和 12 個字元的唯一 ID。還包括檔案名稱的前 10 個字元和副檔名 (最多 10 個字元)。

例如：00-00-00\_manual\_111122223333\_a1b2c3d4e5f6\_myimage.png

對於手動證據，超連結名稱會將您帶到包含該證據的 S3 儲存貯體。

每個證據名稱旁邊是該項目的合規檢查的結果。

- 對於從 AWS Security Hub 或收集的自動證據 AWS Config，報告合規，不合規或不確定的結果。
- 對於從 AWS CloudTrail 和 API 調用收集的自動證據，以及所有手動證據，將顯示不確定的結果。

## 證據摘要頁面

證據摘要頁面包含下列資訊。

名稱	描述
ID	證據的唯一識別碼。
收集日期	建立或上載證據的日期。
Description	證據的描述，包括帳戶 ID 和資料來源類型。
評估名稱	產生報告的評估名稱。
框架名稱	建立評估的來源架構名稱。
控制項名稱	證據支援的控制項名稱。
控制集名稱	相關控制項所屬之控制項集的名稱。
控制項說明	證據支援之控制項的描述。
測試資訊	控制項的建議測試程序。
行動計劃	如果控制未滿足，建議執行的操作。
AWS 區域	與證據相關聯的地區名稱。
身分識別碼	與證據相關聯之使用者或角色的 ARN。
AWS 帳戶	與證據相關聯的身份證 AWS 帳戶 件。

名稱	描述
AWS 服務	與證據相關聯的名稱。 AWS 服務
事件名稱	證據事件的名稱。
Event time (事件時間)	證據事件發生的時間。
資料來源	從那裡收集或上傳證據。資料來源類型可以是「AWS Config Security Hub」、「AWS API 呼叫」或「手動」。 CloudTrail
各类证据	<p>證據的類別</p> <ul style="list-style-type: none"> <li>• 合規性檢查證據是從 AWS Config 或 Security Hub 收集。</li> <li>• 用戶活動證據是從 CloudTrail 日誌中收集的。</li> <li>• 組態資料證據是從其他快照收集的 AWS 服務。</li> <li>• 手動證據是您手動上傳的證據。</li> </ul>
合規性檢查狀態	<p>屬於相容性檢查類別之證據的評估狀態。</p> <ul style="list-style-type: none"> <li>• 對於從 AWS Security Hub 或收集的自動證據 AWS Config，報告合規，不合規或不確定的結果。</li> <li>• 對於從 AWS CloudTrail 和 API 調用收集的自動證據，以及所有手動證據，將顯示不確定的結果。</li> </ul>

## 證據詳細資訊頁

證據詳細資訊頁會顯示證據的名稱和證據詳細資訊表。此表提供證據每個元素的詳細明細，以便您了解資料並驗證資料是否正確。根據證據的資料來源，證據詳細資訊頁的內容會有所不同。

### Tip

每個頁面頂端的頁面導覽路徑導覽會在您瀏覽證據詳細資訊時，顯示您目前的位置。選擇證據摘要以隨時瀏覽回證據摘要。

## 驗證評估報告

當您產生評估報告時，Audit Manager 會產生名為 `digest.txt` 的報告檔案檢查總和。您可以使用此檔案來驗證報告的完整性，並確保在建立報告後未修改任何證據。它包含具有簽章和雜湊 (如果報告存檔的任何部分變更，則無效) 的 JSON 對象。

若要驗證評估報告的完整性，請使用 Audit Manager 提供的 [ValidateAssessmentReportIntegrity](#) API。

## 其他資源

若要尋找常見問題和問題的解答，請參閱 [評估報告問題疑難排解](#) 本指南的「疑難排解」一節。

# 證據搜尋工具

證據搜尋工具為 Audit Manager 中的證據提供了強而有力的搜尋方式。您現在可以使用證據搜尋工具快速查詢證據，而無須一頭栽進證據資料夾，想方設法找到您要尋找的內容。如果您以委派管理員的身分使用證據搜尋工具，您可以在組織中的所有成員帳戶中搜尋證據。

使用篩選條件和分組的組合，您可以逐步縮小搜尋查詢的範圍。例如，如果您想要系統健全狀況的高階檢視，請擴大搜尋範圍，並依據評估、日期範圍和資源合規性進行篩選。如果您的目標是修復特定資源，則可以縮小搜尋範圍，以針對特定控制項或資源 ID 的證據作為目標。定義篩選條件後，您可以先分組並預覽相符的搜尋結果，然後再建立評估報告。

若要使用證據搜尋工具，您必須從 Audit Manager 設定中啟用此功能。

## 重點

### 了解證據查找器如何與 CloudTrail 湖泊合作

證據搜尋工具使用 [AWS CloudTrail Lake](#) 的查詢和儲存功能。在開始使用證據查找器之前，了解更多有關 CloudTrail Lake 的工作原理會很有幫助。

CloudTrail Lake 將資料彙總到支援強大 SQL 查詢的單一、可搜尋的事件資料存放區。這表示您可以在整個組織和自訂時間範圍內搜尋資料。使用證據搜尋工具，您可以直接在 Audit Manager 主控台中使用此搜尋功能。

當您要求啟用證據搜尋工具時，Audit Manager 會代表您建立事件資料存放區。啟用證據搜尋工具之後，您日後的所有 Audit Manager 證據都會擷取至事件資料存放區，以供證據搜尋工具搜尋查詢使用。啟用證據搜尋工具後，我們還會使用過去兩年的有用證據資料回填新建立的事件資料存放區。如果您以委派系統管理員的身分使用證據搜尋工具，我們將回填您的組織中的所有成員帳戶的資料。

您的所有證據資料(無論是回填資料還是新資料)都會在事件資料存放區中保留 2 年。您可以隨時變更預設的保留期間。如需指示，請參閱《AWS CloudTrail 使用指南》中的[更新事件資料存放區](#)。您可以在事件資料存放區中保留事件資料最長 7 年，即 2555 天。

#### Note

將新證據資料新增至事件資料存放區時，資料儲存和擷取會產生 CloudTrail Lake 費用。對於 CloudTrail Lake 查詢，您可以隨時付費。這表示您在證據搜尋工具中進行的每次搜尋查詢，都需要支付掃描資料的費用。

如需 CloudTrail Lake 定價的詳細資訊，請參閱[AWS CloudTrail 定價](#)。

## 後續步驟

若要開始使用，請從 Audit Manager 設定中啟用證據搜尋工具。如需說明，請參閱[啟用證據搜尋工具](#)。

## 其他資源

- [尋找證據, 在, 證據, 發現者](#)
- [在證據搜尋工具中檢視結果](#)
- [證據搜尋器的篩選和分組選項](#)
- [證據查找器的示例用例](#)
- [證據搜尋工具問題疑難排解](#)

## 尋找證據, 在, 證據, 發現者

您可以使用證據查找器執行有針對性的搜索，並快速顯示相關證據以供審查。

在此頁面上，您將瞭解如何依評估、日期範圍、資源合規性狀態和其他屬性等條件篩選搜尋。套用這些篩選條件可將搜尋範圍縮小為您需要的證據。您也可以按特定欄位對結果進行分組，以更好地分析模式。

### 必要條件

請確定您已完成在 Audit Manager 設定中啟用證據搜尋工具的步驟。如需說明，請參閱[啟用證據搜尋工具](#)。

此外，請確保您具有在證據查找器中執行搜索查詢的權限。如需您可以使用的權限原則範例，請參閱[允許使用者在證據搜尋工具中執行搜索查詢](#)。

### 程序

請依照下列步驟在 Audit Manager 主控台中搜尋證據。



1. [執行搜尋查詢](#)
2. [停止進行中的搜尋查詢 \(選用\)](#)
3. [編輯搜尋查詢的篩選條件 \(選用\)](#)

### Note

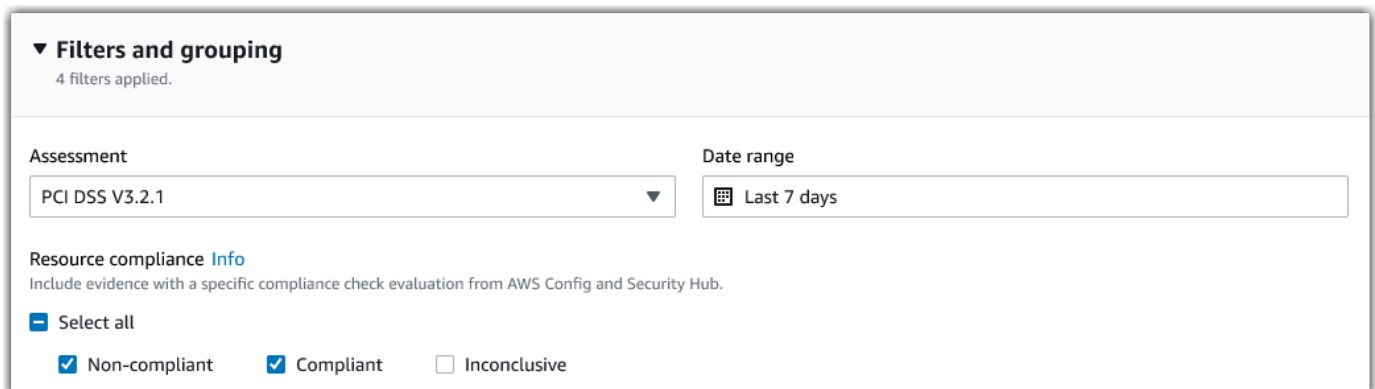
您也可以使用 CloudTrail API 查詢證據資料。如需詳細資訊，請參閱 AWS CloudTrail API 參考 [StartQuery](#) 中的。如果您偏好使用 AWS CLI，請參閱「使用 AWS CloudTrail 者指南」中的「[啟動查詢](#)」。

## 執行搜尋查詢

請按照以下步驟，在證據搜尋工具中執行搜尋查詢。

### 要搜尋證據

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇證據搜尋工具。
3. 接下來，套用篩選條件以縮小搜尋範圍。
  - a. 針對評估，選擇評估。
  - b. 在日期範圍選取範圍。
  - c. 針對資源合規性，選取評估狀態。



▼ Filters and grouping  
4 filters applied.

Assessment: PCI DSS V3.2.1

Date range: Last 7 days

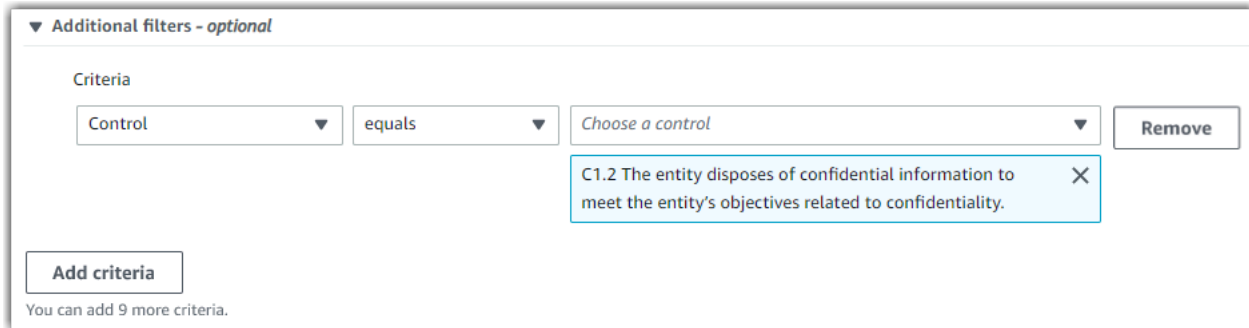
Resource compliance [Info](#)  
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

Select all

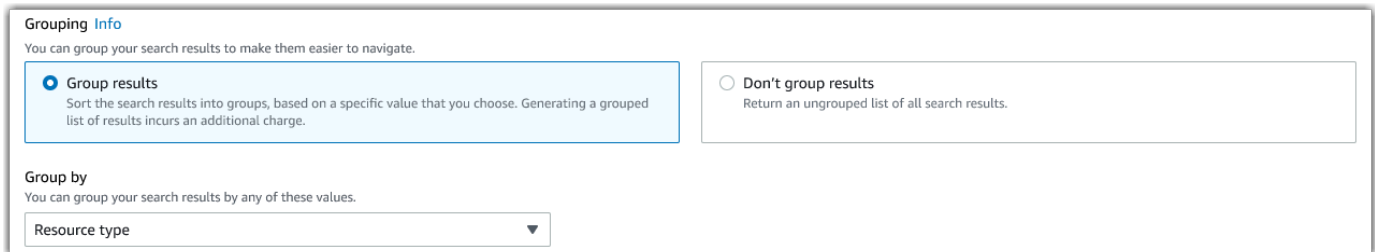
Non-compliant    Compliant    Inconclusive

4. (選用) 選擇其他篩選條件 - 選用以進一步縮小搜尋範圍。

- a. 選擇新增條件，選取條件，然後為該條件選取一或多個值。
- b. 繼續以相同的方式提出更多篩選條件。
- c. 若要移除不想要的篩選條件，請選擇移除



5. 在分組底下，指定是否要將搜尋結果分組。
  - a. 如果想對結果進行分組，請選取一個值作為分組結果依據。
  - b. 如果您不想對結果進行分組，請繼續執行步驟 6。



6. 選擇 Search (搜尋)。



您的搜尋可能需要幾分鐘的時間，視您擁有的證據資料量而定。在搜尋過程中，您可以隨時離開證據搜尋工具。備妥搜尋結果時，即會出現閃光列通知您。

## 停止搜尋查詢

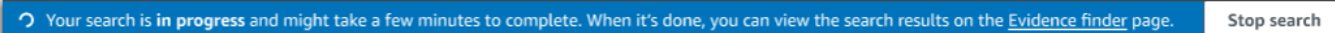
如果您因為任何理由而想要停止搜尋查詢，請依照下列步驟執行。

**Note**

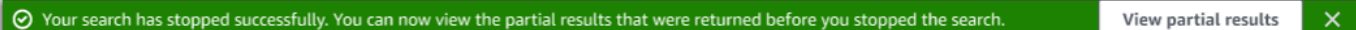
停止搜尋查詢仍可能會產生費用。停止搜尋查詢之前，即會依掃描的證據資料量向您收取費用。停止後，您可以檢視傳回的部分結果。

若要停止進行中的搜尋查詢

1. 在螢幕上方的藍色進度閃光列中，選擇停止搜尋。



2. (選用) 檢閱停止搜尋查詢之前傳回的部分結果。
  - a. 如果您在證據搜尋工具頁面上，螢幕上會顯示部分結果。
  - b. 如果您離開證據搜尋工具，請在綠色確認閃光列中選擇檢視部分結果。



## 編輯搜尋篩選條件

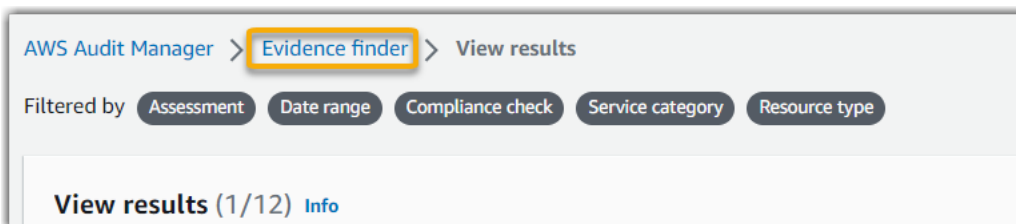
請依照下列步驟返回最近的搜尋查詢，並視需要調整篩選條件。

**Note**

您編輯篩選條件並選擇搜尋時，這即會啟動新的搜尋查詢。

若要編輯最近的搜尋查詢

1. 在檢視結果頁面中，從頁面導覽路徑導覽選單中選取證據搜尋工具。



2. 選擇篩選條件和分組以展開篩選條件選項。

## Evidence finder Info

Evidence finder quickly retrieves and groups the evidence that's relevant to your search. To get started, apply filters to narrow the scope of your search. Then, choose how you want to group the results.

► **Filters and grouping**  
4 filters applied.

3. 接下來，編輯篩選條件或開始新的搜尋。
  - a. 若要編輯篩選條件，請調整或移除目前的篩選條件和分組選項。
  - b. 若要重新開始，請選擇清除篩選條件，然後套用您選擇的篩選條件和分組選項。



4. 完成後，請選擇搜尋。



## 後續步驟

搜尋完成後，您可以檢視符合搜尋條件的結果。如需說明，請參閱[在證據搜尋工具中檢視結果](#)。

## 其他資源

- [證據搜尋器的篩選和分組選項](#).
- [證據查找器的示例用例](#).
- [證據搜尋工具問題疑難排解](#).

## 在證據搜尋工具中檢視結果

搜尋完成後，您可以檢視符合搜尋條件的結果。

請記住，在收集證據時可能會評估多個資源。因此，證據可能包含一個或多個相關資源。在證據搜尋工具中，結果會顯示在資源層級，每個資源有一個資料列。您可以預覽每個資源的摘要，而無需離開頁面。

檢閱搜尋結果後，您可以產生包含該證據的評估報告。您也可以將搜尋結果匯出為逗號分隔值 (CSV) 檔案。

### Important

我們建議您將證據搜尋工具保持開啟狀態，直到您完成搜尋結果的探索為止。當您瀏覽離開檢視結果表格時，系統會捨棄您的搜尋結果。如有需要，您可以在 CloudTrail 主控台中[檢視您最近的搜尋結果](https://console.aws.amazon.com/cloudtrail/)：<https://console.aws.amazon.com/cloudtrail/>。在這裡，您的搜尋查詢結果將保留七天。但請記住，您無法從 CloudTrail 主控台的搜尋結果產生評估報告。

## 必要條件

下列程序假設您已按照下列步驟在證據尋找器中執行搜尋。

## 程序

請按照以下步驟在證據查找器中查看您的搜索結果。

### 任務

- [步驟 1. 檢視分組結果](#)
- [步驟 2. 檢視搜尋結果](#)
  - [管理您的檢視偏好](#)
  - [預覽資源摘要](#)

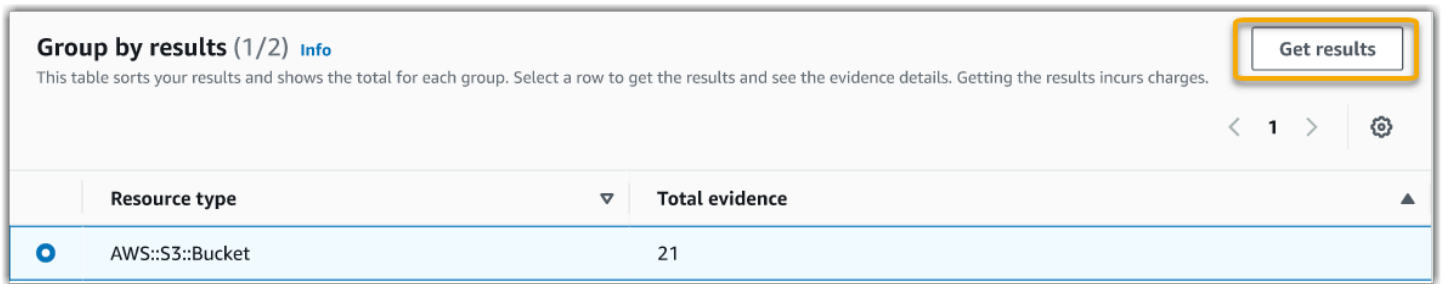
## 步驟 1. 檢視分組結果

如果您將結果分組，則可以在深入研究證據之前查看分組。

### Note

如果您沒有將結果分組，證據搜尋工具不會顯示按結果分組表格。相反地，您會直接前往檢視結果表格。

您可以使用按結果分組表格，瞭解相符證據的廣度，以及它在特定維度之間的分佈方式。結果會依您選取的值分組。例如，如果您按資源類型分組，則表格會顯示 AWS 資源類型的清單。證據總計欄會顯示每個資源類型的相符結果數目。



若要取得群組的結果

1. 從按結果分組表格中，選取您要取得之結果的列。
2. 選擇取得結果。這會啟動新的搜尋查詢，並將您重新導向至檢視結果表格，您可以在其中查看該群組的結果。

## 步驟 2. 檢視搜尋結果

檢視結果表格會顯示您的搜尋結果。您可以在此處管理檢視偏好設定並預覽資源摘要。

管理您的檢視偏好

您的檢視偏好設定會控制您在結果頁面上看到的內容。

要管理您的檢視偏好設定

1. 選擇檢視結果表頂端的設定圖示 (#)。
2. 視需要檢視和變更下列設定：

設定	描述
選擇可見的表格欄	使用切換選項可變更要顯示的欄。
頁面大小	選取一個選項按鈕，指定每個頁面上顯示的結果數目。
Wrap text (文字自動換行)	選取此勾選方塊可折繞長行文字，以提高可讀性。

3. 選擇確認以儲存偏好設定。

## 預覽資源摘要

您可以預覽與搜尋查詢相符的證據的相關資源。這可協助您判斷搜尋查詢是否傳回預期的結果，或者您是否需要調整篩選條件並重新執行搜尋查詢。

請記住，證據可以有一個或多個相關資源。證據搜尋工具將在資源層級顯示結果（每個資源佔一行）。

### Note

證據搜尋工具會傳回自動和手動證據的結果。但是，您只能預覽自動證據的資源摘要。這是因為 Audit Manager 不會針對手動證據執行資源評估，因此沒有可用的資源摘要。

若要查看有關手動證據的詳細資料，請選擇證據名稱以開啟證據詳細資料頁面。如果您從證據搜尋工具結果中生成評估報告，則評估報告中包含手動證據詳細資訊。

## 要預覽資源摘要

1. 選取結果旁的選項按鈕。這會在目前頁面上開啟資源摘要面板。
2. （選擇性）若要查看相關證據的完整詳細資料，請選擇證據名稱。
3. （選擇性）使用水平線 (=) 拖曳資源摘要窗格並調整大小。
4. 選擇 (x) 以關閉資源摘要窗格。

Evidence <a href="#">↗</a>	Resource ARN	Resource compliance	Date and time
<input type="radio"/> 22615e944-a8b2-4cb0-85e4-d853ea94347b	arn:aws:iam:us-west-1:██████████:policyName	<span style="color: red;">⚠ Non-compliant</span>	August 10, 2022, 7:30 (UTC+00:00)
<input checked="" type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1:██████████:trail/AWSOrganizationMaster	<span style="color: green;">✔ Compliant</span>	August 10, 2022, 7:30 (UTC+00:00)
<input type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1:██████████:trail/	<span style="color: green;">✔ Compliant</span>	August 10, 2022, 7:30 (UTC+00:00)

**99615e944-a8b2-4cb0-85e4-d853ea94350d** ✕

**Resource summary**

Resource ARN arn:aws:iam:us-west-1:██████████:policyName	Data source type AWS Config	Assessment <a href="#">PCI DSS V3.2.1</a>
Resource Type AWS::S3::Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Control domain Identity and access management
Resource compliance <span style="color: red;">⚠ Non-compliant</span>	Account ID ██████████	Control <a href="#">7.2.1 Confirm that access control systems are in place on all system components.</a>
Date and time August 10, 2022, 7:30 (UTC+00:00)		

## 後續步驟

檢閱搜尋結果後，您可以從中產生評估報告，或將其匯出為 CSV 檔案。如需說明，請參閱[從證據查找器導出搜索結果](#)。

## 其他資源

- [證據搜尋器的篩選和分組選項](#)
- [證據查找器的示例用例](#)
- [證據搜尋工具問題疑難排解](#)

## 從證據查找器導出搜索結果

檢閱完搜尋結果後，您可以根據這些結果產生評估報告。或者，您可以將證據查找器搜索結果導出為 CSV 文件。



## 必要條件

下列程序假設您已按照步驟[執行搜尋](#)，並在證據尋找器中檢閱搜尋結果。

## 程序

### 內容

- [從搜尋結果產生評估報告](#)
- [將搜尋結果匯出為 CSV 檔案](#)
  - [匯出結果後檢視結果](#)

## 從搜尋結果產生評估報告

對搜尋結果滿意後，您可以產生評估報告。

### 要從搜尋結果產生評估報告

1. 在檢視結果表格頂端，選擇產生評估報告。
2. 輸入評估報告的名稱和說明，並檢閱評估報告詳細資訊。
3. 選擇產生評估報告。

您的評估報告需要幾分鐘的時間才會產生。發生這種情況時，您可以離開證據搜尋工具，等待綠色的成功通知提醒您報告已準備就緒。然後，您可以前往 Audit Manager 下載中心並[下載您的評估報告](#)。

### Note

Audit Manager 僅使用搜尋結果中的證據來產生一次性報告。此報告不包含[從評估頁面手動新增至報告](#)的任何證據。

限制適用於評估報告中包含多少項證據。如需詳細資訊，請參閱[證據搜尋工具問題疑難排解](#)。

## 將搜尋結果匯出為 CSV 檔案

您可能需要可攜式版本的證據搜尋工具搜尋結果。在這種情況下，您可以將搜尋結果匯出為 CSV 檔案。

匯出搜尋結果後，七天內 CSV 檔案仍可在 Audit Manager 下載中心取得。CSV 檔案的副本也會傳送到您偏好的 S3 儲存貯體中，這稱為匯出目的地。您的 CSV 檔案會保留在此儲存貯體中，直到您刪除該檔案為止。

Audit Manager 使用 [CloudTrail Lake](#) 功能從證據搜尋工具匯出和傳送 CSV 檔案。下列因素定義了 CSV 匯出程序的運作方式：

- 您的所有搜尋結果都包含在 CSV 檔案中。如果您只想在評估報告中包含特定的搜尋結果，建議您[編輯您的搜尋篩選器](#)。如此一來，您就可以縮小結果範圍，僅針對您要匯出的證據。
- CSV 檔案會以壓縮的 GZIP 格式匯出。預設 CSV 檔案名稱為 `queryID/result.csv.gz`，其中 `queryID` 是搜尋查詢的 ID。
- CSV 匯出的檔案大小上限為 1 TB。如果您要匯出超過 1 TB 的資料，您的結果會分割為多個檔案。每個 CSV 檔案都會命名為 `result_#.csv.gz`。您取得的 CSV 檔案數量取決於搜尋結果的總大小。例如，匯出 2 TB 的資料會提供兩個查詢結果檔案：`result_1.csv.gz` 和 `result_2.csv.gz`。
- 除了 CSV 檔案之外，還會將 JSON 簽署檔案傳送到您的 S3 儲存貯體。此檔案可做為總和驗證碼，以驗證 CSV 檔案中的資訊是否正確。若要深入了解，請參閱 AWS CloudTrail 開發人員指南中的 [CloudTrail sign 檔案結構](#)。若要判斷查詢結果在傳送後是否已修改、刪除或未變更，您可以使用 CloudTrail 查詢結果完整性驗證。如需指示，請參閱 AWS CloudTrail 開發人員指南中的 [驗證已儲存的查詢結果](#)。

#### Note

證據搜尋工具預覽或 CSV 匯出中，目前不包含手動證據文字回覆。若要檢視文字回應數據，請在證據搜尋工具結果中選擇手動證據名稱以開啟證據詳細資訊頁面。如果您需要在 Audit Manager 主控台以外檢視文字回應資料，建議您根據證據搜尋工具結果產生評估報告。所有手動證據詳細資料，包括文字回應，都包含在評估報告中。

## 首次匯出結果

首次匯出搜尋結果時，請依照下列步驟進行。此程序為您提供指定未來所有匯出的預設匯出目的地選項。如果您不想立即儲存預設的匯出目的地，您可以稍後透過[更新匯出目的地設定](#)來進行操作。

### ⚠ Important

開始之前，請確定您有可用的 S3 儲存貯體作為匯出目的地。您可以使用其中一個現有的 S3 儲存貯體，也可以在 [Amazon S3 中建立新儲存貯體](#)。此外，您的 S3 儲存貯體必須具有必要的許可政策，才能 CloudTrail 將匯出檔案寫入該儲存貯體。更具體地說，值區政策必須包含 `s3:PutObject` 動作和值區 ARN，並將其列 CloudTrail 為服務主體。我們提供您可以使用的 [範例權限策略](#)。關於如何將此政策附加到 S3 儲存貯體的指南，請參閱 [使用 Amazon S3 主控台新增儲存貯體政策](#)。

如需更多秘訣，請參閱 [匯出目的地的組態提示](#)。如果您在匯出 CSV 檔案時遇到任何問題，請參閱 [csv-exports](#)。

### 匯出搜尋結果 ( 首次執行體驗 )

1. 在檢視結果表格頂端，選擇匯出 CSV。
2. 指定您要匯出檔案的 S3 儲存貯體。
  - 選擇瀏覽 S3 以從儲存貯體清單中選取。
  - 或者，您也可以使用以下格式輸入儲存貯體 URI：`s3://bucketname/prefix`

### 💡 Tip

為確保目的地儲存貯體有序組織，您可以為 CSV 匯出建立選用資料夾。若要這麼做，請在資源 URI 方塊中的值加上斜線 (/) 和字首 (例如，`/evidenceFinderExports`)。然後，Audit Manager 會在將 CSV 檔案新增至儲存貯體時包含此字首，而 Amazon S3 會產生字首指定的路徑。如需在 Amazon S3 中首碼的詳細資訊，請參閱在 Amazon 簡易儲存服務使用者指南中的 [在 Amazon S3 主控台編組物件](#)。

3. ( 選擇性 ) 如果您不想將此儲存貯體預設為匯出目的地，請取消選取在我的證據搜尋工具設定中，將此儲存貯體預設為匯出目的地的核取方塊。
4. 選擇 Export (匯出)。

儲存匯出目的地後，匯出結果

將預設 S3 儲存貯體儲存為匯出目的地後，您可以繼續執行下列步驟。

## 匯出搜尋結果(儲存預設匯出目的地後)

1. 在檢視結果表格頂端，選擇匯出 CSV。
2. 在出現的提示中，檢閱將儲存匯出檔案的預設 S3 儲存貯體。
  - a. (選擇性) 若要繼續使用此儲存貯體並隱藏此訊息，請勾選 **不要再提醒我** 方塊。
  - b. (選擇性) 若要變更儲存貯體，請依照程序[更新匯出目的地設定](#)。
3. 選擇確認。

視您要匯出的資料量而定，匯出程序可能需要幾分鐘的時間才能完成。您可以在匯出過程中離開證據搜尋工具。當您離開證據搜尋工具時，您的搜尋作業將停止，搜尋結果也會自主控台移除。不過，CSV 匯出程序會在背景中繼續執行。CSV 檔案將包含符合您查詢的完整搜尋結果集。

## 匯出結果後檢視結果

若要尋找您的 CSV 檔案並檢查其狀態，請前往 Audit Manager [Audit Manager 下載中心](#)。匯出的檔案準備就緒後，[您可以從下載中心下載 CSV 檔案](#)。

您也可以匯出目的地 S3 儲存貯體中找到，並下載 CSV 檔案。

## 在 Amazon S3 主控台中尋找 CSV 檔案和簽署檔案

1. 開啟 [Amazon S3 主控台](#)。
2. 選擇您在匯出 CSV 檔案時，指定的匯出目的地儲存貯體。
3. 瀏覽物件階層，直到找出 CSV 檔案和簽署檔案。CSV 檔案的副檔名為 `.csv.gz`，而簽署檔案的副檔名為 `.json`。

您將瀏覽與下列範例類似的物件階層，但使用不同的匯出目的地儲存貯體名稱、帳戶 ID、日期和查詢 ID。

```
All Buckets
  Export_Destination_Bucket_Name
    AWSLogs
      Account_ID;
        CloudTrail-Lake
          Query
            YYYY
              MM
                DD
```

Query\_ID

## 其他資源

- [證據搜尋工具問題疑難排解](#)
- [設定證據搜尋器的預設匯出目的地](#)

## 證據搜尋器的篩選和分組選項

在此頁面上，您可以看到可用於證據查找器的過濾器 and 分組選項列表。

### 篩選器參考資料

您可以使用下列篩選器來尋找符合特定條件的證據，例如評估、控制或 AWS 服務。

#### 主題

- [必要篩選器](#)
- [其他篩選條件 \(選擇性\)](#)
- [結合篩選器](#)

### 必要篩選器

使用這些篩選條件，開始對評估中的證據進行高階概觀。

篩選器名稱	描述	備註
評估	傳回特定評估的證據。	您只能依據一個評估進行篩選。
日期範圍	傳回特定時段的證據。	<p>或者，您可以使用相對範圍來定義相對於今天日期的範圍 (例如，<b>Last 30 days</b>)。</p> <p>或者，您可以使用絕對範圍來指定特定的日期範圍 (例如，<b>June 27th - July 4th</b>)。</p>
支援合規	傳回具有特定合規檢查評估的資源。	Audit Manager 會針對使用 AWS Config 和 Security Hub 做為資料來源類型的控制項收集 <a href="#">符合性檢查證據</a> 。請記住，在收集證據時可能會評估多種資源。

篩選器名稱	描述	備註
		<p>因此，單一合規檢查證據可以包含一或多個資源。您可以使用此篩選器來探索資源層級的合規狀態。</p> <p>您可以選擇以下其中一個選項：</p> <ul style="list-style-type: none"> <li>• 不合規 — 此篩選器會尋找具有合規檢查問題的資源。如果 Security Hub 報告失敗結果或報告不合規的結果，就會發生這種情況。AWS Config</li> <li>• 合規 — 此篩選器會尋找不具有合規檢查問題的資源。如果 Security Hub 報告「通過」結果或報告「合規」結果，就會發生這種情況。AWS Config</li> <li>• 不確定 — 此篩選器會尋找合規檢查不可用或不適用的資源。如果資源使用 AWS Config 或安全中樞做為基礎資料來源類型，但這些服務未啟用，就會發生這種情況。如果資源使用不支援符合性檢查的基礎資料來源類型 (例如手動證據、AWS API 呼叫或 CloudTrail)，也會發生這種情況。</li> </ul>

## 其他篩選條件 ( 選擇性 )

使用這些篩選條件來縮小搜尋查詢的範圍。例如，使用服務查看與 Amazon S3 相關的所有證據。使用資源類型將範圍縮小至 S3 儲存貯體。或者，使用資源 ARN 以特定 S3 儲存貯體為目標。

您可以使用下列一或多個條件建立其他篩選器。

條件名稱	描述	何時使用此條件
帳戶 ID	向下鑽取 AWS 帳戶。	使用此條件來尋找與特定 AWS 帳戶相關的證據。
控制項	依控制項名稱進行深層探勘。	使用此條件來尋找與特定控制項相關的證據。
控制項域	依控制項網域進行深層探勘。	當您準備稽核時，請使用此條件，將重點放在特定主題領域。如果您要查詢從標準架構建立的評估，則可以依控制項網域進行篩選。

條件名稱	描述	何時使用此條件
		控制項網域的範例包括身分識別與存取管理、記錄與監控，以及網路管理。
Data source type (資料來源類型)	依資料來源的類型進行深層探勘。	<p>使用此條件可將結果限縮於特定資料來源。</p> <p>將值設定為Manual，以尋找您手動上傳的證據。或者，您可以根據自動證據的來源（例如AWS Config、CloudTrail、Security Hub或AWS API calls）過濾自動證據。</p>
事件名稱	依事件名稱進行深層探勘。	<p>使用此條件可將重點放在與證據相關的特定事件上。事件是AWS帳戶中活動的記錄。</p> <p>例如，您可以搜尋API呼叫的名稱，例如用於設定權限的IAM AttachRolePolicy 作業。或者，搜尋CloudTrail關鍵字，例如使用者登入您的帳戶CloudTrail時所記錄的ConsoleLogin事件。</p>
資源ARN	按Amazon Resource Name (ARN)進行深層探勘。	使用此條件來尋找與特定AWS資源相關的證據。
Resource Type (資源類型)	依資源類型進行深層探勘。	使用此條件專注於正在評估的資源類型，例如Amazon EC2執行個體或S3儲存貯體。
服務	按AWS服務名稱向下鑽取。	使用此條件尋找與特定相關的證據AWS服務，例如Amazon EC2、Amazon S3或AWS Config。
服務目錄	按AWS服務類別向下鑽研。	<p>使用此條件可將重點放在的特定類別上AWS服務。</p> <p>範例包括安全性、身分識別與合規性、資料庫和存放區。</p>

## 結合篩選器

## 條件行為

當您指定多個條件時，Audit Manager 會將 AND 運算子套用到您的選定內容。這表示所有條件都會分組為單一查詢，且結果必須符合所有組合的條件。

## 範例

在下列篩選器設定中，證據搜尋工具會針對呼叫 **MySOC2Assessment** 的評估，傳回過去 7 天內不合規的資源。此外，結果與 IAM 政策和指定控制項有關。

Assessment: MySOC2Assessment | Date range: Last 7 days

Resource compliance [Info](#)  
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

Select all  
 Non-compliant  Compliant  Inconclusive

Additional filters - optional

Criteria

Control equals Choose a control Remove  
7.2.1 Confirm that access control systems are in place on all system components. X

and Resource type contains Enter text Remove  
AWS::IAM::Policy X

Add criteria

## 條件值行為

當您指定多個條件值時，這些值會與 OR 運算子連結。證據搜尋工具會傳回符合任何這些條件值的結果。

## 範例

在下列篩選器設定中，證據搜尋工具會傳回來自 AWS CloudTrail AWS Config、或的搜尋結果 AWS Security Hub。

and Data source type equals Choose a data source type Remove  
AWS CloudTrail X AWS Config X AWS SecurityHub X



## 分組參考

您可以將搜尋結果分組，以加快瀏覽速度。分組顯示搜尋結果的廣度，以及它們在特定維度中的分佈方式。

您可以使用以下任一分組的數值。

分組依據	描述
帳戶 ID	依據分組結果 AWS 帳戶。
控制項	依控制項名稱分組結果。
Data source type (資料來源類型)	依證據來源的資料來源類型分組結果。
事件名稱	依事件名稱分組結果。
資源 ARN	依 Amazon Resource Name (ARN) 分組結果。
Resource Type (資源類型)	依資源類型分組結果。
服務	依 AWS 服務 名稱分組結果。
服務目錄	按 AWS 服務 類別分組結果。

## 證據查找器的示例用例

證據搜尋工具可以幫助您處理多種使用範例。此頁面提供了一些範例，並建議您可以在每個案例中使用的搜尋篩選器。

### 主題

- [使用案例 1：尋找不合規的證據並進行委派](#)
- [使用案例 2：找出合規證據](#)
- [使用案例 3：執行證據資源的快速預覽](#)

## 使用案例 1：尋找不合規的證據並進行委派

如果您是合規官、資料保護官或監督稽核準備工作的 GRC 專業人員，則此使用案例非常理想。

當您監管組織的合規性狀況時，您可能會仰賴合作夥伴團隊來協助您修復問題。您可以使用證據搜尋工具來幫助您為合作夥伴團隊組織工作。

透過應用篩選器，您可以一次專注於一個區域的證據。此外，您還可以與您合作的每個合作夥伴團隊的責任和範圍保持一致。透過這種方式執行目標搜尋，您可以使用搜尋結果來分辨每個主題領域，瞭解實際需要補救的內容。然後，您可以將不合規的證據委託給對應的合作夥伴團隊進行補救。

對於此工作流程，請按照步驟[搜尋證據](#)。使用下列篩選器尋找不合規的證據。

```
Assessment | <assessment name>  
Date range | <date range>  
Resource compliance | Non-compliant
```

接下來，為您要關注的區域應用其他篩選器。例如，使用服務類別篩選器尋找與 IAM 相關的不合規資源。然後，與擁有組織 IAM 資源的團隊共用這些結果。或者，如果您要查詢從標準架構建立的評估，您可以使用控制項網域篩選器來尋找與身分識別和存取管理網域相關的不合規證據。

```
Control domain | <domain that you're focusing on>  
or  
Service category | <AWS ## category that you're focusing on>
```

找到所需證據後，請按照以下步驟從搜尋結果產生評估報告。如需說明，請參閱[從搜尋結果產生評估報告](#)。您可以與合作夥伴團隊共享此報告，他們可以將其用作補救檢查清單。

## 使用案例 2：找出合規證據

如果您在擁有和修復雲端資產的 IT/或其他角色中 SecOps 工作 DevOps，則此使用案例非常理想。

作為稽核的一部分，系統可能會要求您修正您擁有的資源的問題。完成這項工作之後，您可以使用證據搜尋工具來驗證您的資源是否合規。

對於此工作流程，請按照步驟[搜尋證據](#)。使用下列篩選器尋找合規的證據。

```
Assessment | <assessment name>  
Date range | <date range>
```

Resource compliance | **Compliant**

接下來，應用其他篩選器以縮小範圍至僅剩下您負責的證據。視您的擁有權範圍而定，視需要進行目標搜尋。下列篩選範例是從最廣到最精確的順序排列。選擇適合您的選項，並以您自己的值取代 `<#####>`。

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS ## that you own>
Service | <a specific AWS ## that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

如果您負責相同條件的多個實例（例如，您擁有多個 AWS 服務），則可以按該值對[結果進行分組](#)。這項行動將為您提供與每個 AWS 服務證據相符的總證據。然後，您可以取得您擁有之服務的結果。

## 使用案例 3：執行證據資源的快速預覽

此使用案例適合所有 Audit Manager 客戶。

以前，檢閱個別證據詳細資料非常耗時。如果您想要預覽證據，您必須直接前往該評估，然後瀏覽深層巢狀的證據資料夾。現在，證據搜尋工具提供了一種預覽此資訊的便捷方法。對於符合搜尋查詢的每個證據項目，您可以預覽該證據的個別資源。

若要開始使用，請按照步驟[搜尋證據](#)。接著，選取結果旁的選項按鈕以檢視目前頁面中的資源摘要。您可以預覽與證據項目相關的每個個別資源。若要查看任何資源的完整證據詳細資料，請選擇證據名稱。如需詳細資訊，請參閱[預覽資源摘要](#)。

Evidence	Resource ARN	Resource compliance	Date and time
<input type="radio"/> <a href="#">22615e944-a8b2-4cb0-85e4-d853ea94347b</a>	<code>arn:aws:iam:us-west1:██████████:policyName</code>	Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
<input checked="" type="radio"/> <a href="#">99615e944-a8b2-4cb0-85e4-d853ea94350d</a>	<code>arn:aws:cloudtrail:us-west-1:██████████:trail/AWSOrganizationMaster</code>	Compliant	August 10, 2022, 7:30 (UTC+00:00)
<input type="radio"/> <a href="#">99615e944-a8b2-4cb0-85e4-d853ea94350d</a>	<code>arn:aws:cloudtrail:us-west-1:██████████:trail/</code>	Compliant	August 10, 2022, 7:30 (UTC+00:00)

**99615e944-a8b2-4cb0-85e4-d853ea94350d** ✕

### Resource summary

<b>Resource ARN</b> <code>arn:aws:iam:us-west1:██████████:policyName</code>	<b>Data source type</b> AWS Config	<b>Assessment</b> <a href="#">PCI DSS V3.2.1</a>
<b>Resource Type</b> AWS::S3::Bucket	<b>Data source mapping</b> S3_BUCKET_PUBLIC_READ_PROHIBITED	<b>Control domain</b> Identity and access management
<b>Resource compliance</b> Non-compliant	<b>Account ID</b> ██████████	<b>Control</b> 7.2.1 Confirm that access control systems are in place on all system components.
<b>Date and time</b> August 10, 2022, 7:30 (UTC+00:00)		

# Audit Manager 下載中心

您可以在下載中心找到並管理所有可下載的 Audit Manager 檔案。當您產生評估報告或匯出證據搜尋工具的搜尋結果時，檔案會出現在下載中心中。

## 內容

- [瀏覽下載中心](#)
- [正在下載檔案](#)
- [刪除檔案](#)
- [其他資源](#)

## 瀏覽下載中心

請依照下列步驟在下載中心瀏覽檔案。

### 在下載中心尋找檔案

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇下載中心。
3. 選擇評估報告標籤以檢視可供下載的評估報告。
  - 此標籤會顯示您產生的評估報告。在您刪除評估報告之前，您可在下載中心獲取評估報告。
  - 如需查看評估報告的最新狀態，請選擇重新整理圖示 (#) 以重新載入表格。評估報告表格中的每一列都會顯示報告的名稱、建立日期，以及下列其中一種狀態：

狀態	描述
In progress (正在進行)	Audit Manager 正在產生評估報告。
備妥	您可以下載評估報告。
錯誤	無法產生評估報告。在此情況下，Audit Manager 會顯示描述錯誤的訊息。

狀態	描述
	如需如何解決這些錯誤的相關資訊，請參閱 <a href="#">評估報告問題疑難排解</a> 。

#### 4. 選擇 [匯出] 索引標籤以檢視可供下載的 CSV 匯出。

- 此標籤會顯示您過去七天匯出的證據搜尋結果。CSV 檔案會在七天後從下載中心中移除，但仍可在[匯出目的地](#) S3 儲存貯體中使用。如需有關如何在 S3 目的地儲存貯體中尋找證據搜尋工具 CSV 匯出的說明，請參閱 [匯出結果後檢視結果](#)。
- 如需查看 CSV 報告的最新狀態，請選擇重新整理圖示 (#) 以重新載入表格。匯出表格中的每一列都會顯示檔案名稱、匯出日期以及下列其中一種狀態：

狀態	描述
In progress (正在進行)	Audit Manager 正在準備 CSV 檔案。
備妥	匯出成功，檔案可供您下載。
錯誤	匯出失敗。在此情況下，Audit Manager 會顯示描述錯誤的訊息。  如需如何解決這些錯誤的相關資訊，請參閱 <a href="#">csv-exports</a> 。

#### Note

請記住，匯出索引標籤也可能會顯示您直接在 AWS CloudTrail Lake 中執行的查詢的 CSV 檔案。這包括在 CloudTrail 控制台中或使用 CloudTrail API 進行的查詢。CloudTrail 如果您查詢 Audit Manager 事件資料存放區，而您選擇將結果儲存到 Amazon S3，則匯出會顯示在此索引標籤上。

## 正在下載檔案

請依照下列步驟從下載中心中下載檔案。

## 如需下載檔案

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇下載中心。
3. 選擇評估報告索引標籤或匯出索引標籤。
4. 選擇您要下載的檔案，然後選擇下載。

如需有關如何直接從 S3 目的地儲存貯體下載檔案的指示，請參閱 Amazon Simple Storage Service (Amazon S3) 使用者指南中的 [下載物件](#)。

## 刪除檔案

請依照下列步驟刪除下載中心中不再需要的任何評估報告。

### Note

目前不支援從下載中心刪除 CSV。CSV 匯出會在七天後自動從下載中心中移除。

## 刪除評估報告

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇下載中心。
3. 選擇評估報告索引標籤。
4. 選擇您要刪除的評估報告，然後選擇刪除。

如果您想要從 S3 目的地儲存貯體刪除評估報告或 CSV 匯出，建議您直接在 Amazon S3 中完成此任務。如需指示，請參閱 Amazon Simple Storage Service (Amazon S3) 使用者指南中的 [刪除 Amazon S3 物件](#)。

## 其他資源

- [設定證據搜尋器的預設匯出目的地](#)

- [設定您的預設評估報告目標](#)
- [評估報告問題疑難排解](#)
- [疑難排解 CSV 匯出問題](#)
- [從 Amazon S3 下載對象](#)
- [刪除 Amazon S3 對象](#)



# 使用框架庫來管理框架 AWS Audit Manager

您可以在中的框架庫中找到和管理框架 AWS Audit Manager。

架構決定哪些控制項會在一段時間內在某個環境中測試。它會針對指定的合規性標準或法規，定義控制項及其資料來源的映射項目。它也可用來建構和自動化 Audit Manager 評估。您可以使用框架作為起點來審核您的使用 AWS 服務 情況並開始自動化證據收集。

## 重點

在框架庫中，框架分為以下幾類。

- 標準架構是由 AWS 提供之預先定義的架構。這些架構以不同合規性標準和法規 (例如 GDPR 和 HIPAA) 的 AWS 最佳實務為基礎。標準架構包括根據架構支援的合規性標準或法規，組織到控制集中的控制項。

您可以檢視標準架構的內容，但無法編輯或刪除它們。不過，您可以建立任何標準架構的可編輯副本，以建立符合特定需求的新架構。

- 自定義框架是您創建的框架。您可以從頭開始建立自訂架構，或製作現有架構的可編輯副本。您可以使用自訂架構，以符合特定需求的方式將控制項組織到控制集中。

您可以從標準架構或自訂架構建立評估。

### Note

AWS Audit Manager 協助收集與驗證符合特定合規標準和法規相關的證據。不過，這不會評估您的合規狀態。AWS Audit Manager 因此，透過收集的證據可能不包含稽核所需的所有有關您 AWS 使用情況的資訊。AWS Audit Manager 不是法律顧問或合規專家的替代品。

## 其他資源

若要在稽核管理員中建立和管理架構，請遵循此處概述的程序。

- [尋找可用的架構 AWS Audit Manager](#)
- [檢閱框架 AWS Audit Manager](#)

- [在中建立自訂架構 AWS Audit Manager](#)
  - [從頭開始創建自定義框架 AWS Audit Manager](#)
  - [在中製作現有框架的可編輯副本 AWS Audit Manager](#)
- [編輯自訂架構 AWS Audit Manager](#)
- [刪除中的自定義框架 AWS Audit Manager](#)
- [共享自定義框架 AWS Audit Manager](#)
  - [架構共享概念和術語](#)
  - [發送共享自定義框架的請求 AWS Audit Manager](#)
  - [回應共用要求 AWS Audit Manager](#)
  - [刪除共用要求 AWS Audit Manager](#)
- [支援的架構 AWS Audit Manager](#)

## 尋找可用的架構 AWS Audit Manager

您可以在 [Audit Manager] 主控台的 [架構程式庫] 頁面上找到所有可用的架構。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視所有可用的架構。

### 必要條件

請確定您的 IAM 身分具有適當的許可，以檢視中的架構 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

#### Audit Manager console

若要在 Audit Manager 主控台上檢視可用架構

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇架構程式庫。
3. 選擇標準架構索引標籤或自訂架構索引標籤，瀏覽可用的標準和自訂架構。

## AWS CLI

若要檢視中的可用架構 AWS CLI

若要在 Audit Manager 中檢視架構，請使用指[list-assessment-frameworks](#) 令並指定 `--framework-type`。或者，您可以擷取標準架構的清單。或者，您也可以擷取自訂架構的清單。

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

## Audit Manager API

若要使用 API 檢視可用架構

使用該[ListAssessmentFrameworks](#) 操作並指定 [框架](#) 類型。或者，您可以傳回標準架構的清單。或者，您也可以傳回自訂架構的清單。

有關詳細資訊，請選擇先前的任一連結，在 AWS Audit Manager API 參考資料中閱讀更多資訊。這包括有關如何在其中一個特定語言 SDK 中使用 `ListAssessmentFrameworks` 操作和參數的信息 AWS。

## 後續步驟

當您準備好探索架構的詳細資訊時，請依照中的步驟操作[檢閱框架 AWS Audit Manager](#)。此頁面將引導您完成框架詳細信息，並解釋您在此處看到的信息。

在框架庫頁面中，您還可以[創建](#)，[編輯](#)，[刪除](#)或[共享](#)自定義框架。

## 其他資源

如需 Audit Manager 中架構問題的解決方案，請參閱[疑難排解架構問](#)。

## 檢閱框架 AWS Audit Manager

您可以使用 Audit Manager 主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱架構的詳細資料。

## 必要條件

請確定您的 IAM 身分具有適當的許可，以檢視中的架構 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

### Audit Manager console

在 Audit Manager 主控台上檢視架構詳細資料

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇架構程式庫以查看可用架構的清單。
3. 選擇標準架構索引標籤或自訂架構索引標籤，瀏覽可用的架構。
4. 選擇架構名稱以開啟。
5. 使用下列資訊作為參考，檢閱架構詳細資訊。

### 架構詳細資訊章節

本節說明架構的概觀。在本節中，您可以檢閱下列資訊：

名稱	描述
Description	框架的描述 ( 如果有提供 )。
框架類型	指定框架是標準框架還是自定義框架。
合規性類型	該框架支持的合規標準或法規。

如果您正在查看自定義框架，則還可以查看以下詳細信息：

名稱	描述
創建者	建立自訂架構的帳戶。
Date created (建立日期)	建立自訂架構的日期。

名稱	描述
上次更新	上次編輯此架構的日期。

### 控制項索引標籤

此索引標籤會列出架構中的控制項，並依控制集分組。在此標籤上，您可以檢閱下列資訊：

名稱	描述
按控制組分組的控制項	選擇樹狀檢視圖示以查看屬於每個控制集的控制項。
類型	指定控制項是標準控制項還是自訂控制項。
資料來源	指定「Audit Manager」從中收集該架構控制項之證據的資料來源。

### 標籤頁

這個索引標籤會列出與架構相關聯的標籤。在此標籤上，您可以檢閱下列資訊：

名稱	描述
索引鍵	標籤鍵 (例如，符合性標準、法規或類別)。
Value	標籤值。

## AWS CLI

若要檢視框架詳細資料 AWS CLI

- 若要識別您要檢閱的架構，請執行 `list-assessment-frameworks` 命令並指定 `--framework-type`。或者，您可以擷取標準架構的清單。或者，您也可以擷取自訂架構的清單。

在下列範例中，將 `#####` 取代為 `Custom` 或 `Standard`。

```
aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
```

回應返回架構列表。找到您要檢閱的架構，並記下架構 ID 和 Amazon Resource Name (ARN)。

- 若要取得架構詳細資料，請執行 [get-assessment-framework](#) 命令並指定 `--framework-id`。

在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

 Tip

架構詳細資訊會以 JSON 格式傳回。若要瞭解此資料，請參閱《AWS CLI 指令參考》中的 [get-assessment-framework 輸出](#)。

- 若要查看架構的標籤，請使用指 [list-tags-for-resource](#) 令並指 `--resource-arn` 定架構的。

在下列範例中，將 `#####` 取代為您自己的資訊：

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如需有關 Audit Manager 中標籤的詳細資訊，請參閱 [標籤 AWS Audit Manager 資源](#)。

## Audit Manager API

若要使用 API 檢視架構詳細資料

- 若要識別您要檢閱的架構，請使用此 [ListAssessmentFrameworks](#) 作業並指定 [Framework Type](#)。或者，您可以傳回標準架構的清單。或者，您也可以傳回自訂架構的清單。

在回應中找到您要檢閱的架構，並記下架構 ID 和 Amazon Resource Name (ARN)。

- 要獲取框架詳細信息，請使用 [GetAssessmentFramework](#) 操作。在要求中，指定您從步驟 1 取得的 [架構 ID](#)。

**i** Tip

架構詳細資訊會以 JSON 格式傳回。若要瞭解此資料，請參閱 AWS Audit Manager API 參考中的 [GetAssessmentFramework 回應元素](#)。

- 若要查看架構的標籤，請使用此 [ListTagsForResource](#) 作業。在請求中，指定從步驟 1 獲得的架構 [resourceArn](#)。

如需 Audit Manager 中標籤的詳細資訊，請參閱 [標記 AWS Audit Manager 資源](#)。

如需有關這些 API 作業的詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

在架構詳細資訊頁面中，您可以 [從架構建立評估](#)，或 [製作架構的可編輯副本](#)。

如果您正在檢閱自訂架構，也可以 [編輯](#)、[刪除](#) 或 [共用](#) 架構。

## 其他資源

- [在我的自定義框架詳細信息頁面上，系統提示我重新創建自定義框架](#)
- [我無法製作自定義框架的副本或使用它來創建評估](#)

## 在中建立自訂架構 AWS Audit Manager

您可以使用自訂架構，以符合特定需求的方式將控制項組織到控制集中。

## 重點

在 Audit Manager 中建立自訂架構時，您有兩種方法可供選擇：

- 從頭開始創建自定義框架-這使您可以靈活地從乾淨的石板開始，並根據您的規範定義框架的各個方面。當您的需求明顯偏離現有的標準架構，或者當您需要納入組織專屬的專屬控制集時，此方法特別有益。

2. 製作現有框架的可編輯副本-這種方法可讓您利用現有框架的結構和內容，同時提供自定義框架以滿足您的特定需求的自由。從建立的基礎開始，您可以簡化建立自訂架構的程序，將您的努力集中在針對組織的獨特需求量身打造。

無論您選擇哪種方法，建立自訂架構都需要執行一系列步驟，例如指定架構詳細資料、定義控制項集，以及在完成架構建立之前檢閱架構。在此過程中，您可以合併組織的特定控制集，以確保自訂架構能正確反映您的 GRC 需求。

## 其他資源

如需如何建立自訂架構的指示，請參閱下列資源。

- [從頭開始創建自定義框架 AWS Audit Manager](#)
- [在中製作現有框架的可編輯副本 AWS Audit Manager](#)

## 從頭開始創建自定義框架 AWS Audit Manager

如果組織的合規性需求與中可用的預先建置標準架構不一致 AWS Audit Manager，您可以從頭開始建立自己的自訂架構。

本頁概述了如何根據您的特定需求建立自訂架構的步驟。

### 必要條件

請確定您的 IAM 身分具有在中建立自訂架構的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager管理存取權](#)。

### 程序

#### 任務

- [步驟 1：指定架構詳細資訊](#)
- [步驟 2：指定控制集](#)
- [步驟 3：檢閱及建立架構](#)

#### 步驟 1：指定架構詳細資訊

首先指定有關自定義框架的詳細信息。



## 指定架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導航窗格中，選擇框架庫，然後選擇創建自定義框架。
3. 在框架詳細信息下，輸入名稱，合規類型（可選）和框架的描述（也是可選的）。輸入 PCI\_DSS 或 GDPR 之類的合規性類型意味著您可以在稍後使用此關鍵字搜索框架。
4. 在標籤下，選擇新增標籤，將標籤與架構產生關聯。您可以指定每一個標籤的金鑰和值。標籤索引鍵是必要的。在框架庫中搜索此框架時，您可以將其用作搜索條件。
5. 選擇下一步。

## 步驟 2：指定控制集

接下來，您可以指定要新增至架構的控制項，以及要如何組織這些控制項。首先將控制集新增至架構，然後將控制項新增至控制集。

### Note

當您使用主控 AWS Audit Manager 台建立自訂架構時，您最多可以為每個架構新增 10 個控制集。

使用 Audit Manager API 建立自訂架構時，您可以建立 10 個以上的控制集。若要新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的 [CreateAssessmentFrameworkAPI](#)。

## 指定控制集的步驟

1. 在控制集名稱下，輸入控制集的名稱。
2. 在 [新增控制項] 下，使用 [控制項類型] 下拉式清單選取兩種控制項類型之一：[標準控制項] 或 [自訂控制項]
3. 根據您在上一個步驟中選取的選項，會顯示標準控制項或自訂控制項的清單。選取一或多個控制項，然後選擇 [新增] 以控制項集。
4. 在出現的快顯視窗中，選擇 [新增至控制集]。
5. 複查顯示在 [選取的控制項] 清單中的控制項。
  - 若要新增更多控制項，請重複步驟 2 至 4。
  - 若要移除不想要的控制項目，請選取一或多個控制項，然後選擇 [移除]

- 若要新增控制集，請選擇 [新增控制集]。
- 若要移除不想要的控制集，請選擇 [移除控制集]。
- 完成新增控制項集和控制項之後，請選擇下一步。

### 步驟 3：檢閱及建立架構

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂架構。

### 後續步驟

建立新的自訂架構之後，您可以從架定義立評估。如需詳細資訊，請參閱 [在中建立評估 AWS Audit Manager](#)。

若要稍後重新造訪您的自訂架構，請參閱 [尋找可用的架構 AWS Audit Manager](#)。您可以依照下列步驟找出自訂架構，以便檢視、編輯、共用或刪除它。

### 其他資源

如需 Audit Manager 中架構問題的解決方案，請參閱 [疑難排解架構問](#)。

## 在中製作現有框架的可編輯副本 AWS Audit Manager

您可以使用現有架構作為起點，並製作可編輯的副本，而不是從頭開始建立自訂架構。執行此操作時，現有框架仍保留在框架庫中，並使用您的特定設置創建一個新的自定義框架。

您可以製作任何現有架構的可編輯副本。它可以是標準架構或自訂架構。

### 必要條件

請確定您的 IAM 身分具有在中建立自訂架構的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

#### 任務

- [步驟 1：指定架構詳細資訊](#)
- [步驟 2：指定控制集](#)

## • 步驟 3：檢閱及建立架構

### 步驟 1：指定架構詳細資訊

除標籤外，所有架構詳細資訊都是從原始架構繼承的。視需要檢閱和修改這些詳細資訊。

#### 指定架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導覽窗格中，選擇架構程式庫。
3. 選擇您要用作起點的架構，選擇 [建立自訂架構]，然後選擇 [製作複本]。
4. 在出現的快顯視窗中，輸入新自訂架構的名稱，然後選擇 [繼續]。
5. 在框架詳細信息下，查看框架的名稱，合規性類型和描述，並根據需要進行更改。合規類型應指出合規標準，或與您架構相關聯的法規。您可以使用此關鍵字來搜索架構。
6. 在標籤下，選擇新增標籤，將標籤與架構產生關聯。您可以指定每一個標籤的金鑰和值。標籤鍵是強制性的，當您在框架庫中搜索此框架時，可以用作搜索條件。
7. 選擇下一步。

### 步驟 2：指定控制集

控制集是從原始架構結轉的。視需要新增更多控制項或移除現有控制項，以變更目前的組態。

#### Note

當您使用 Audit Manager 主控台建立自訂架構時，您最多可以為每個架構新增 10 個控制集。使用 Audit Manager API 建立自訂架構時，您可以新增 10 個以上的控制集。若要新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的 [CreateAssessmentFrameworkAPI](#)。

#### 指定控制集的步驟

1. 在 [控制集名稱] 下，視需要變更控制集的名稱。
2. 在 [新增控制項] 底下，使用下拉式清單選取兩種控制項類型之一來新增控制項：[標準控制項] 或 [自訂控制項]。
3. 根據您在上一個步驟中選取的選項，會顯示標準控制項或自訂控制項的清單。選取一或多個控制項，然後選擇 [新增] 以控制項集。

4. 在出現的快顯視窗中，選擇 [新增至控制集]。
5. 複查顯示在 [選取的控制項] 清單中的控制項。
  - 若要新增更多控制項，請重複步驟 2 至 4。
  - 若要移除不想要的控制項目，請選取一或多個控制項，然後選擇 [移除]
6. 若要新增控制項集至架構，請選擇 [新增控制項集]。
7. 若要移除不想要的控制集，請選擇 [移除控制集]。
8. 完成新增控制項集和控制項之後，請選擇下一步。

### 步驟 3：檢閱及建立架構

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂架構。

### 後續步驟

建立新的自訂架構之後，您可以從架定義立評估。如需詳細資訊，請參閱 [在中建立評估 AWS Audit Manager](#)。

若要稍後重新造訪您的自訂架構，請參閱 [尋找可用的架構 AWS Audit Manager](#)。您可以依照下列步驟找出自訂架構，以便檢視、編輯、共用或刪除它。

### 其他資源

如需 Audit Manager 中架構問題的解決方案，請參閱 [疑難排解架構問](#)。

## 編輯自訂架構 AWS Audit Manager

您可能需要在合規性需求變更時修改中 AWS Audit Manager 的自訂架構。

本頁概述編輯自訂架構詳細資料和控制項集的步驟。

### 必要條件

下列程序假設您先前已建立自訂架構。

請確定您的 IAM 身分具有適當的許可，可在中編輯自訂架構 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

# 程序

## 任務

- [步驟 1：編輯架構詳細資訊](#)
- [步驟 2：編輯控制集](#)
- [步驟 3。檢閱並儲存](#)

## 步驟 1：編輯架構詳細資訊

首先查看和編輯現有的架構詳細資訊。

如要編輯架構詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導航窗格中，選擇架構程式庫，然後選擇自訂架構選項卡。
3. 選擇您要停止的機群，選擇動作，然後選擇停止。
  - 或者，打開自定義框架，然後選擇框架詳細信息頁面右上角的編輯。
4. 在框架詳細信息下，查看框架的名稱，合規性類型和描述，並進行任何必要的更改。
5. 選擇下一步。

### Tip

要編輯架構的標籤，請打開架構並選擇架構 [標籤選項卡](#)。您可以在這裡檢視和編輯與架構相關聯的標籤。

## 步驟 2：編輯控制集

接下來，檢閱並編輯架構中的控制項和控制集。

### Note

當您使用主控 AWS Audit Manager 台編輯自訂架構時，您最多可以為每個架構新增 10 個控制集。

使用 Audit Manager API 編輯自訂架構時，您可以新增 10 個以上的控制集。若要新增超過主控台目前允許的控制集，請使用 Audit Manager 提供的 [UpdateAssessmentFrameworkAPI](#)。

## 編輯控制集的步驟

1. 在控制集名稱底下，視需要檢閱及編輯控制集的名稱。
2. 在 [新增控制項] 下，使用 [控制項類型] 下拉式清單選取兩種控制項類型之一：[標準控制項] 或 [自訂控制項]
3. 根據您在上一個步驟中選擇的選項，會顯示標準控制項或自訂控制項的清單。選取一或多個控制項，然後選擇 [新增] 以控制項集。
4. 在出現的快顯視窗中，選擇「新增」。
5. 複查和編輯顯示在 [選取的控制項] 清單中的控制項。
  - 若要新增更多控制項，請重複步驟 2 至 4。
  - 若要移除不想要的控制項，請選取一或多個控制項，然後選擇「從控制集移除」
6. 若要新增控制項集至架構，請選擇 [新增控制項集]。
7. 若要移除不想要的控制集，請選擇 [移除控制集]。
8. 完成新增控制項集和控制項之後，請選擇下一步。

## 步驟 3。檢閱並儲存

檢閱架構的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇儲存變更。

## 後續步驟

當您確定不再需要自訂架構時，可以刪除架構來清理 Audit Manager 環境。如需說明，請參閱[刪除中的自定義框架 AWS Audit Manager](#)。

## 其他資源

如需 Audit Manager 中架構問題的解決方案，請參閱[疑難排解架構問](#)。

## 共享自定義框架 AWS Audit Manager

您可以使用的架構共用功能，快速複寫您建立的 AWS Audit Manager 自訂架構。您可以與其他人共用您的自訂架構 AWS 帳戶，或將您的架構複製到您自己帳戶 AWS 區域下的另一個架構。接著，收件者可以存取您的自訂架構，並使用它來建立評估。他們可以做到這一點，而不必為該架構重複任何配置工作。

## 重點

如果共享自訂架構，您可以建立共享要求。接下來，共享要求的收件者有 120 天的時間接受或拒絕要求。當他們接受共享要求時，Audit Manager 會將共享的自訂架構複寫到其架構程式庫中。除了複寫自訂架構之外，Audit Manager 也會複寫屬於該架構的所有自訂控制集和自訂控制項。接著，這些自訂控制項會新增至收件者的控制項程式庫。Audit Manager 不會複寫標準架構或控制項。依預設，這些功能可在啟用 Audit Manager 的所有 AWS 帳戶和區域中使用。

架構共享功能僅適用於付費層。不過，共享自訂架構或接受共享要求不會產生額外費用。若要進一步了解的定價 AWS Audit Manager，請參閱定[AWS Audit Manager 價頁面](#)。

### Important

如果標準架構被指定為不符合共用資格，則您不得共用衍生自標準架構的自訂架構 AWS，除非您已取得標準架構擁有者的許可。若要瞭解哪些標準架構不符合共享資格及更多內容，請參閱[架構共享資格](#)。

## 其他資源

若要進一步了解如何在 Audit Manager 中共用自訂架構，請參閱下列資源。

- [架構共享概念和術語](#)
- [發送共享自定義框架的請求 AWS Audit Manager](#)
- [回應共用要求 AWS Audit Manager](#)
- [刪除共用要求 AWS Audit Manager](#)

## 架構共享概念和術語

瞭解下列重要概念後，您可以更充分地運用 AWS Audit Manager 自訂架構共享功能。

## 重點

### 寄件者

這是共享請求的創建者以及自定義框架的存在 AWS 帳戶 位置。寄件者可以與任何 AWS 帳戶，或者，他們將自定義框架複製到自己帳戶 AWS 區域 下支持的任何內容。

### 收件人

這是共享架構的消費者。收件人可以接受或拒絕寄件者的共享要求。

#### Note

收件者可以是委派系統管理員帳戶。不過，您無法與 AWS Organizations 管理帳戶共用自訂架構。

### 架構資格

您只能共享自訂架構。默認情況下，標準框架已經存在於所有 AWS 帳戶 和啟用的 AWS 區域 AWS Audit Manager 位置。此外，您共享的自訂架構不得包含敏感資料。這包括在架構本身中找到的資料、其控制集，以及屬於自訂架構一部分的任何自訂控制項。

#### Important

由提供的一些標準框架 AWS Audit Manager 包含受許可協議約束的受版權保護的材料。自訂架構可能包含衍生自這些架構的內容。如果標準架構被指定為不符合共用資格，則您不得共用衍生自標準架構的自訂架構 AWS，除非您已取得標準架構擁有者的許可。若要瞭解哪些標準架構符合共享資格，請參閱下表。

標準架構名稱	符合分享資格的自訂版本
<a href="#">澳大利亞網絡安全中心 (ACSC) 基本八</a>	 是



標準架構名稱	符合分享資格的自訂版本
<a href="#">澳大利亞網絡安全中心 ( ACSC ) 信息安全手冊 ( ISM ) 2023 年 3 月 2 日</a>	 是
<a href="#">Amazon Web Services ( AWS ) Audit Manager 示例框架</a>	 是
<a href="#">AWS Control Tower 防護機制</a>	 是
<a href="#">AWS 生成人工智慧最佳實務架構 v2</a>	 是
<a href="#">AWS License Manager</a>	 是
<a href="#">AWS 基礎安全性最佳做法</a>	 是
<a href="#">AWS 營運最佳作法</a>	 是

標準架構名稱	符合分享資格的自訂版本
<a href="#"><u>Amazon Web Services ( AWS ) 結構良好的框架 ( WAF ) v10</u></a>	 是
<a href="#"><u>加拿大網絡安全中心 ( CCCS ) 中等雲端控制</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.2.0 , 第一級</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.2.0 , 第一級和第二級</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.3.0 , 第一級</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.3.0 , 第一級和第二級</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.4.0 , 第一級</u></a>	 否
<a href="#"><u>互聯網安全中心 ( CIS ) Amazon Web Services ( AWS ) 基準 v1.4.0 , 第一級和第二級</u></a>	 否

標準架構名稱	符合分享資格的自訂版本
<a href="#">互聯網安全中心 (獨聯體) 7.1 版, IG1</a>	 是
<a href="#">獨聯體關鍵安全控制系統 8.0 版 ( 獨聯體 8.0 版 ) , IG1</a>	 否
<a href="#">聯邦風險與授權管理計畫 (FedRAMP) 安全基準控制項 r4, 中等</a>	 是
<a href="#">2016 年一般資料保護條例</a>	 是
<a href="#">金融服務業現代化法 (GLBA)</a>	 是
<a href="#">標題 21 聯邦法規 ( CFR ) 第 11 部, 電子記錄; 電子簽名-適用範圍和應用 2023 年 5 月 24 日</a>	 是
<a href="#">EudraLex -歐洲聯盟藥用產品管制規則-第四冊：人類及獸醫用藥品的良好生產規範-附件 11</a>	 是

標準架構名稱	符合分享資格的自訂版本
<a href="#">《Health 保險流通與責任法案》(HIPAA) 安全規則：2003 年 2 月</a>	 是
<a href="#">Health 保險可攜性與責任法案 (HIPAA) 綜合性最終規則</a>	 是
<a href="#">國際標準化組織 (ISO)/國際電工委員會 (IEC)</a>	 否
<a href="#">NIST 800-53 第五版：適用於資訊系統和 Organizations 的安全性與隱私權控制</a>	 是
<a href="#">NIST 網路安全架構 (CSF) 1.1 版</a>	 是
<a href="#">NIST 800-171 修訂版 2：保護非聯邦系統與 Organizations 中受控制的非機密資訊</a>	 是
<a href="#">支付卡產業資料安全標準 (PCI DSS) v3.2.1</a>	 否

標準架構名稱	符合分享資格的自訂版本
<a href="#">支付卡產業資料安全標準 (PCI DSS) v4.0</a>	 否
<a href="#">關於證明參與標準 (SSAE) 第 18 號的聲明，服務 Organizations 控制 (SOC) 報告 2</a>	 否

## 分享要求

如果共享自訂架構，您可以建立共享要求。共享要求會指定收件者，並通知他們有可用的自訂架構。收件者有 120 天的時間可以接受或拒絕來回應共享要求。如果 120 天內未採取任何動作，則共享要求就會過期，且收件者無法將自訂架構新增至其架構程式庫。寄件者和收件者可以從架構程式庫的共享要求頁面檢視共享要求，並針對共享要求採取動作。

## 共享要求狀態

共享要求可以有下列任何一種狀態。

狀態	描述
Active (作用中)	這表示已成功傳送給收件者並等待其回應的共用要求。
即將到期	這表示未來 30 天內到期的共用要求。
共享	這表示收件者接受的共用要求。
非作用中	這表示共用要求在收件者採取動作之前已撤銷、拒絕或過期。
複製	這表示正在複寫至收件者架構程式庫的已接受共用要求。
失敗	這表示未成功傳送給收件者的共用要求。

## 分享要求通知

Audit Manager 會在收到共享要求時通知收件者。當共享要求即將在接下來 30 天的某個時間到期時，收件者和寄件者都會收到通知。

- 若為收件者，已接收狀態為有效或即將到期的請求旁會出現一個藍色的通知點。收件者可以透過接受或拒絕共享要求來解決通知。
- 對寄件者而言，已傳送的要求旁會出現藍色通知圓點，狀態為即將到期。收件者接受或拒絕要求時，解決通知。否則，要求在到期後會自動消失。此外，寄件者可以透過撤銷共享要求來解決通知。

### 寄件者所有權

寄件者會維護他們共享的自訂架構完整存取權。他們可以在共享要求到期前，隨時透過[撤銷共享要求](#)來取消有效的共享要求。不過，收件者接受共享要求後，寄件者便無法再撤銷收件者對該自訂架構的存取權。這是因為當收件者接受要求時，Audit Manager 會在收件者的架構程式庫中建立自訂架構的獨立副本。

除了複寫寄件者的自訂架構之外，Audit Manager 也會複寫屬於該架構的所有自訂控制集和自訂控制項。不過，Audit Manager 不會複製任何附加至自訂架構的標籤。

### 收件者所有權

收件者可以完整存取他們接受的自訂架構。當收件者接受要求時，Audit Manager 會將自訂架構複寫到其架構程式庫的自訂架構索引標籤。接下來，收件者可以使用與任何其他自訂架構相同的方式來管理共享自訂架構。收件者可以共享從其他寄件者獲得的自訂架構。收件者無法封鎖寄件者傳送共享要求。

### 共享架構到期

當寄件者建立共享要求時，Audit Manager 會將要求設定為在 120 天後過期。收件者可以在要求到期之前接受並取得共享架構的存取權。如果收件者在此期間不接受，共享要求就會過期。在此之後，過期共享要求的紀錄仍會保留在其歷史紀錄中。過期共享架構的快照會以一年效期 TTL 存在於 S3 儲存貯體，以供稽核之用。

寄件者可以在共享要求到期前，隨時選擇[撤銷共享要求](#)。

### 共享架構資料儲存和備份

當您建立共用請求時，Audit Manager 會將自訂架構的快照儲存在美國東部 (維吉尼亞北部) AWS 區域。Audit Manager 也會將相同快照的備份儲存在美國西部 (奧勒岡) AWS 區域。

當發生下列其中一個事件時，Audit Manager 會刪除快照和備份快照：

- 寄件者撤銷共享要求。
- 收件者拒絕共享要求。
- 收件者遇到錯誤且未成功接受共享要求。
- 共享要求會在收件者回應要求之前過期。

當寄件者[重新傳送共享要求](#)時，快照會取代為與自訂架構最新版本相對應的更新版本。

當收件者接受共用要求時，快照會 AWS 帳戶 根據共用要求中指 AWS 區域 定的快照複製到其中。

## 共享架構版本控制

當您共用自訂架構時，Audit Manager 會在指定的 AWS 帳戶 和 [區域] 中建立該架構的獨立副本。這表示您應該牢記以下幾點：

- 收件者接受的共享架構，是建立共享要求時該架構的快照。如果您在傳送共享要求後更新原始自訂架構，則不會自動更新要求。若要共享已更新架構的最新版本，您可以[重新傳送共享要求](#)。此新快照的到期日為重新共享日期起 120 天。
- 當您與另一個人共享自定義框架，AWS 帳戶 然後從框架庫中刪除它時，共享的自定義框架仍保留在收件者的框架庫中。
- 當您將自定義框架共享給您帳戶 AWS 區域 下的另一個框架，然後在第一個中刪除該自定義框架時 AWS 區域，自定義框架將保留在第二個區域中。
- 當您在接受共享自訂架構之後刪除它時，任何複寫為自訂架構一部分的自訂控制項，都會保留在您的控制項程式庫中。

## 其他資源

- [發送共享自定義框架的請求 AWS Audit Manager](#)
- [回應共用要求 AWS Audit Manager](#)
- [刪除共用要求 AWS Audit Manager](#)
- [疑難排解架構問](#)

## 發送共享自定義框架的請求 AWS Audit Manager

本教學課程說明如何在 AWS 帳戶 和之間共用您的自訂架構 AWS 區域。

當您共享自訂架構時，Audit Manager 會建立架構的快照，並將共享要求傳送給收件者。收件者有 120 天的時間接受共享架構。當他們接受共享要求時，Audit Manager 會將共享的自訂架構複寫到 AWS 區域指定的架構程式庫中。如果您想要在自己的帳戶下將自訂架構複製到其他區域，請使用以下教學課程，並輸入您自己的 AWS 帳戶 ID 作為收件者帳戶 ID。

## 必要條件

在您開始教學課程之前，請務必先達成以下條件：

- 您已熟悉 Audit Manager 的[架構共享概念和術語](#)。
- 您要共享的自訂架構須為[可供共享](#)，並存在於您 AWS Audit Manager 環境的架構程式庫中。
- 收件者已 AWS Audit Manager 在您 AWS 區域 要共用自訂架構的位置啟用。
- 收件者不是 AWS Organizations 管理帳戶。
- 您的 IAM 身分具有適當的許可，可在中共用自訂架構 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

### Tip

在開始之前，請記下您要與其共用自訂架構的 AWS 帳戶 ID。如果您的目標是將框架複製到您帳戶 AWS 區域 下的另一個框架，則這可以是您自己的帳戶 ID。教學步驟 2 您需要這個資訊。

## 程序

### 任務

- [步驟 1：確定您要共享的自訂架構](#)
- [步驟 2：傳送共享要求](#)
- [步驟 3：檢視您傳送的要求](#)
- [步驟 4 \(選用\)：撤銷共用請求](#)

### 步驟 1：確定您要共享的自訂架構

首先確定您要共享的自訂架構。您可以在 Audit Manager 的架構程式庫頁面上找到所有可用的自訂架構清單。

### Important

不要共享包含敏感資料的自訂架構。這包括在架構本身中找到的資料、其控制集，以及屬於自訂架構一部分的任何自訂控制項。如需詳細資訊，請參閱[架構合格服務](#)。

### 若要檢視可用的自訂架構

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。



2. 在導覽窗格中，選擇架構程式庫。
3. 選擇自訂架構索引標籤。此步驟將顯示可用的自訂架構清單。您可以選擇任何架構名稱來查看該自訂架構的詳細資訊。

## 步驟 2：傳送共享要求

下一步，指定收件者，並傳送自訂架構的共享要求給他們。在共享請求過期之前，接收方有 120 天的時間對共享要求做出回應。

### 若要傳送共享要求

1. 從架構程式庫的自訂架構選項卡中，選擇架構的名稱以打開詳細資訊頁面。從這裡選擇動作，然後選擇共享自訂架構。
  - 或者，從架構程式庫的清單中選取自訂架構，選擇動作，然後選擇共用自訂架構。根據自訂架構的大小，Audit Manager 準備共享要求可能需要幾秒鐘的時間。
2. 檢閱對話方塊中顯示的通知。
  - 如果您不確定是否可以共享自訂架構，請參閱[架構資格](#)以取得進一步指引。
  - 如果您的架構具有使用自訂 AWS Config 規則做為資料來源的控制項，建議您聯絡收件者，讓他們知道。接著收件者可以在的執行個體中建立並啟用相同的 AWS Config 規則 AWS Config。如需詳細資訊，請參閱 [我的共享框架具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？](#)。
3. 輸入 **agree**，然後選擇同意繼續。
4. 在下個畫面上，執行下列操作：
  - 在AWS 帳戶下方輸入收件者的帳戶 ID。這可以是您自己的帳戶 ID。
  - 在AWS 區域下方，從下拉式清單中選取收件人的區域。
  - (選用) 在傳送給收件者的訊息下方，輸入有關您要共用之自訂架構的選擇性評論。
  - 在自訂架構詳細資料底下，檢閱詳細資料以確認您要共用此架構。
5. 選擇共用。

#### Note

請謹記以下幾點：

- 當您與另一個架構共用自訂架構時 AWS 帳戶，該架構只會複寫到指定的架構 AWS 區域。接受共享要求後，收件者就可以視需要跨區域複寫架構。
- 共用自訂架構時 AWS 區域，最多可能需要 10 分鐘的時間來處理共用要求動作。傳送跨區域共享要求之後，建議您稍後再回來查看，以確認您的共享要求已成功傳送。
- 當您傳送共享要求時，Audit Manager 會在建立共享要求時擷取自訂架構的快照。如果您在傳送共享要求後更新自訂架構，則不會自動更新要求。如果共享已更新架構的最新版本，您可以[重新傳送共享要求](#)。此新快照的到期日為重新共享日期起 120 天。

### 步驟 3：檢視您傳送的要求

您可以選取已傳送要求索引標籤，查看您傳送的所有共用要求清單。您可以視需要篩選此清單。例如，您可以套用篩選器，只顯示未來 30 天內到期的要求。

#### 若要檢視和篩選已傳送的要求

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已傳送請求標籤。
3. (選用) 套用篩選條件，調整顯示的已傳送要求。您可以透過尋找 全部狀態 下拉式清單，並將篩選器變更為下列其中一項來執行此操作。

狀態	描述
Active (作用中)	此篩選器會顯示等待收件者回應的共用要求。
即將到期	此篩選器會顯示未來 30 天內到期的共用要求。
共享	此篩選器會顯示收件者所接受的共用要求。共享自訂架構現在存在於收件者的架構程式庫中。
非作用中	此篩選器會顯示在收件者採取動作前遭拒、撤銷或過期的共用要求。選擇非有效一詞以檢視更多詳細資料。
複製	這表示正在複寫至收件者架構程式庫的已接受共用要求。
失敗	此篩選器會顯示未成功傳送給收件者的共用要求。選擇失敗一詞以檢視更多詳細資料。

**Note**

處理共享要求最多需要 15 分鐘的時間。因此，如果傳送共用要求給收件者時發生錯誤，失敗狀態可能不會立即顯示。建議您稍後再回來查看，以確認您的共享要求已成功傳送。

**步驟 4 (選用)：撤銷共用請求**

如果您需要在有效的共享要求到期前取消該要求，您可以隨時撤銷要求。此為選擇性步驟。如果您不採取任何動作，收件者就無法在到期日之後接受共享要求。

**撤銷共享要求**

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已傳送請求標籤。
3. 選取您要撤銷的架構，然後選擇撤銷要求。
4. 在出現的快顯視窗中，選擇撤銷。

**Note**

您只能撤銷狀態為作用中或即將到期之共用要求的存取權。收件者接受共享要求後，您可以不再撤銷收件者對該自訂架構的存取權。這是因為自訂架構的複本現在存在於收件者的架構程式庫中。

共用架構時 AWS 區域，最多可能需要 10 分鐘的時間來處理共用要求動作。撤銷跨區域共享要求之後，建議您稍後再回來查看，以確認您的共享要求已成功撤銷。

**後續步驟****為更新架構重新傳送共享要求**

傳送自訂架構的共享要求後，可能會遇到該架構更新的情形。但這麼一來，共享要求並不會自動更新，架構的最新版本也不會被沿用。不過，如果其狀態為有效、已共享或即將到期，您就可以更新現有的共享要求。若要這麼做，您可以重新傳送具有與現有要求相同的詳細資料集的新共享要求。在新的共享要求中，包含相同的自訂架構 ID、收件者帳戶 ID 和收件者 AWS 區域。您也可以提供新共享要求的新備註。

當您重新傳送共享要求時，請謹記下列事項：

- 要成功更新，新請求必須使用相同的自訂架構 ID。其必須指定與現有要求相同的收件人帳戶 ID 和區域。
- 如果自訂架構的名稱已變更，更新後的共享要求會顯示最新的名稱。
- 如果您提供新的備註，更新後的共享要求會顯示最新的備註。
- 當您重新傳送共享要求時，到期日會延長六個月。

### 為更新架構重新傳送共享要求

1. 從架構程式庫的自訂架構選項卡中，選擇要共享的架構的名稱。這將打開架構詳細資訊頁面。
2. 選擇 [動作]，然後選擇 [共用自訂架構]
3. 檢閱對話方塊中顯示的通知，輸入 **agree**，然後選擇同意以繼續。
4. 在下個畫面上，執行下列操作：
  - 在 AWS 帳戶 下方輸入您在現有共享要求中指定的相同帳戶 ID。
  - 在 AWS 區域 下方，選擇您在現有共享要求中指定的相同區域。
  - (選用) 在給收件者的訊息下，輸入有關更新之自訂架構的選擇性評論。
  - 在自訂架構詳細資料底下，檢閱詳細資料以確認您要重新傳送共用要求。
5. 選擇共用以重新傳送並更新共用要求。

## 其他資源

若要尋找共用自訂架構時可能遇到的問題的解決方案，請參閱[疑難排解架構問](#)。

## 回應共用要求 AWS Audit Manager

本教學課程說明當您收到自訂架構的共享要求時應採取的動作。Audit Manager 會在您收到共享要求時通知您。當共享要求即將在接下來 30 天的某個時間到期時，您也會收到通知提醒。

## 必要條件

在開始之前，我們建議您先進一步了解 Audit Manager [架構共享概念和術語](#)。

## 程序

### 任務

- [步驟 1：檢查收到的要求通知](#)

- [步驟 2：對要求採取行動](#)
- [步驟 3：查看收到要求的歷史紀錄](#)

### 步驟 1：檢查收到的要求通知

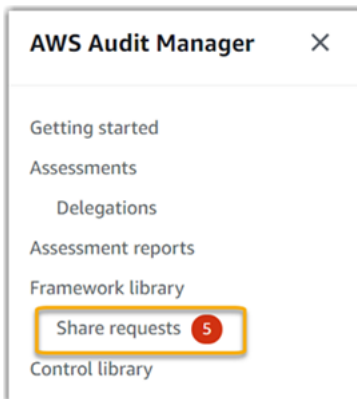
首先檢查您的共享要求通知。[已接收的要求] 索引標籤會顯示您從其他人收到的共用要求清單 AWS 帳戶。等待回覆的要求會以藍點顯示。您也可以篩選此檢視，只顯示未來 30 天內到期的要求。

若要檢視收到的要求

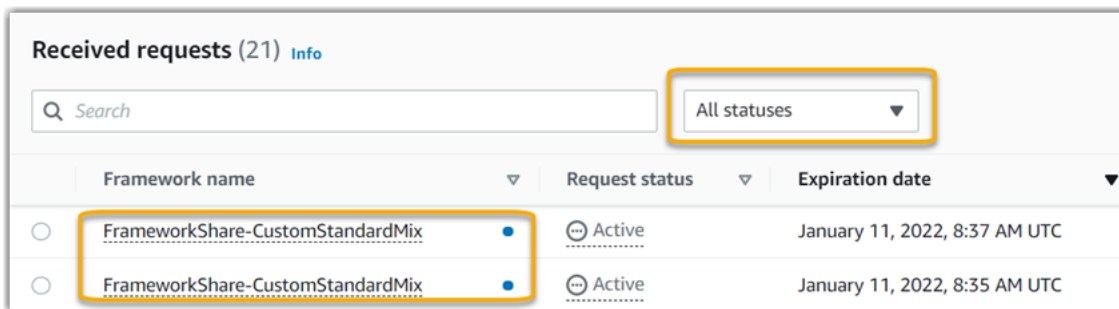
1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。



3. 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要您處理的共享要求數目。



4. 選擇共享要求。依預設，此頁面會在已接收的要求索引標籤上開啟。
5. 尋找帶有藍點的項目，以找出需要執行動作的共享要求。



6. (選擇性) 若只要檢視未來 30 天內到期的要求，請尋找所有狀態下拉式清單，然後選取即將到期。

## 步驟 2：對要求採取行動

您必須透過接受或拒絕共享要求來採取行動，才能刪除藍點通知。

### 接受共享架構

當您接受共享要求時，Audit Manager 會將原始架構的快照，複寫到架構程式庫的自訂架構索引標籤中。Audit Manager 會使用您在 [Audit Manager 設定](#) 中指定的 KMS 金鑰，複寫並加密新的自訂架構。

### 接受共享要求

1. 開啟共用請求頁面，並確定您正在檢視已接收要求索引標籤。
2. (選用) 從篩選器下拉式清單中，選取有效或即將到期。
3. (選用) 選擇架構名稱以檢視共用請求的詳細資訊。這包括架構說明、架構中的控制項數目，以及來自寄件者的訊息等資訊。
4. 選取您要接受的共用要求，選擇動作，然後選擇接受。

在您接受共享要求後，共享自訂架構狀態會變更為複寫中並新增至您的架構程式庫。如果架構包含自訂控制項，這些控制項將在此時添加到您的控制項庫中。

當架構複寫完成時，狀態會變更為已共享。自訂架構已準備好可供使用時，會有成功橫幅通知您。

#### Tip

當您接受自訂架構時，它只會複製到您當前的架構 AWS 區域。您可能希望新的共享架構在您的 AWS 帳戶所有區域都能使用。如果是這樣，在您接受共享請求後，您可以根據需要將[架構共享](#)給您帳戶下的其他區域。

### 拒絕共享架構

當您拒絕共享要求時，Audit Manager 不會將該自訂架構新增至您的架構程式庫。不過，已拒絕共用要求的紀錄會保留在已接收要求索引標籤中，狀態為非作用中。

### 若要拒絕共享要求

1. 開啟共用請求頁面，並確定您正在檢視已接收要求索引標籤。
2. (選用) 從篩選器下拉式清單中，選取有效或即將到期。

3. (選用) 選擇架構名稱以檢視共用請求的詳細資訊。這包括架構說明、架構中的控制項數目，以及來自寄件者的訊息等資訊。
4. 選取您要拒絕的共用要求，選擇動作，然後選擇拒絕。
5. 在出現的對話方塊中，選擇刪除以確認您的選擇。

**i** Tip

如果您改變主意並希望在拒絕後存取共享架構，請要求寄件者傳送新的共享要求給您。

**i** Note

跨 AWS 區域共享架構時，最多可能需要 10 分鐘來處理共享要求動作。在跨區域共享要求採取動作之後，建議您稍後再回來查看，以確認共享要求已成功接收或拒絕。

### 步驟 3：查看收到要求的歷史紀錄

接受或拒絕共用架構後，您可以返回共用要求頁面查看您的共用要求紀錄。您可以視需要篩選此清單。例如，您可以套用篩選器，只顯示已接受的要求。

若要檢視共享要求的紀錄：

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側瀏覽窗格中，選擇共享要求。
3. 選擇已接收的請求標籤。
4. 找到「全部狀態」下拉式清單，然後選取下列其中一個篩選條件：

名稱	描述
Active (作用中)	此篩選器會顯示您尚未接受或拒絕的共用要求。
即將到期	此篩選器會顯示未來 30 天內到期的共用要求。
共享	此篩選器會顯示您接受的共用要求。共享架構現在可以在您的架構程式庫中使用。

名稱	描述
非作用中	此篩選器會顯示已拒絕或過期的共用要求。
失敗	此篩選器會顯示未成功傳送的共用要求。選擇失敗一詞以檢視更多詳細資料。

## 後續步驟

接受共享自訂架構後，您可以在架構程式庫的自訂架構選項卡中找到它。您現在可以使用該架構來建立評估。如需進一步了解，請參閱[在中建立評估 AWS Audit Manager](#)。

有關如何編輯新自定義框架的說明，請參閱[編輯自訂架構 AWS Audit Manager](#)。

## 其他資源

若要尋找可能遇到之問題的解決方案，請參閱[疑難排解架構問](#)。

## 刪除共用要求 AWS Audit Manager

當您不再需要共用請求時，可以將其從 Audit Manager 環境中刪除。這可讓您清理工作區，並專注於與目前工作和優先順序相關的請求。

當您刪除共享要求時，只會刪除要求本身。共享架構本身仍保留在您的架構程式庫中。

## 必要條件

下列程序假設您先前已傳送或接收共用要求。您無法刪除狀態為有效或複寫狀態的共享要求。

請確定您的 IAM 身分具有適當的許可，可在中刪除共用請求 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager管理存取權](#)。

## 程序

### 刪除共享要求

1. 在瀏覽窗格中，選擇共享要求。
2. 選擇已發送請求或已接收請求標籤。
3. 選取您不再需要的架構，然後選擇刪除。



4. 在出現的快顯視窗中，選擇刪除。

## 其他資源

若要尋找可能遇到之問題的解決方案，請參閱[疑難排解架構問](#)。

## 刪除中的自定義框架 AWS Audit Manager

當您不再需要自訂架構時，可以將其從 Audit Manager 環境中刪除。這可讓您清理工作區，並專注於與目前工作和優先順序相關的自訂架構。

## 必要條件

下列程序假設您先前已建立自訂架構。

請確定您的 IAM 身分具有適當的許可，可在中刪除自訂架構 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、稽 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 刪除自訂架構。

### Note

刪除自訂架構並不會影響從架構刪除前建立的任何現有評估。

### Audit Manager console

若要刪除 Audit Manager 主控台上的自訂架構

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側導航窗格中，選擇架構程式庫，然後選擇自訂架構選項卡。
3. 選取您要刪除的架構，選擇動作，然後選擇刪除。
  - 或者，您也可以開啟自訂架構，然後選擇架構摘要頁面右上角的動作、刪除。

4. 在快顯視窗中，選擇刪除以確認刪除。

## AWS CLI

### 若要刪除自訂架構 AWS CLI

1. 首先，識別您要刪除的自訂架構。若要執行此操作，請執行[list-assessment-frameworks](#)命令並指定`--framework-type`為Custom。

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

回應返回自訂架構的列表。找到您要刪除的自訂架構，並記下架構 ID。

2. 接下來，運行[delete-assessment-framework](#)命令並指定要刪除的框架。`--framework-id`

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

## Audit Manager API

### 若要使用 API 刪除自訂架構

1. 使用該[ListAssessmentFrameworks](#)操作並將[框架類型](#)指定為Custom。從回應中，找到要刪除的自訂架構，並記下架構 ID。
2. 使用該[DeleteAssessmentFramework](#)操作刪除框架。在要求中，使用[架構 ID](#)參數來指定您要刪除的架構。

如需有關這些 API 作業的詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 其他資源

如需 Audit Manager 中資料保留的相關資訊，請參閱[刪除 Audit Manager 資料](#)。

# 使用控制項程式庫管理控制項 AWS Audit Manager

您可以從中的控制項程式庫存取和管理控制項 AWS Audit Manager。

## 重點

在控制項資源庫中，控制項分為下列品類。

- 一般控制項會收集支援多重疊相容性標準的證據。自動化通用控制項包含一或多個相關[核心控制項](#)，每個控制項都會從預先定義的資料來源群組收集支援證據。這為您提供了一種有效的方法來識別對應到您的合規要求產品組合的 AWS 資料來源。每個自動化通用控制項的基礎資料來源均由[AWS 安全保證服務](#)的業界認證評估機構驗證和維護。
- 標準控制項會收集證據以支援特定的合規性標準。您可以檢視標準控制項的詳細資料，但無法編輯或刪除它們。不過，您可以建立任何標準控制項的可編輯複本，以建立符合特定需求的新控制項。
- 自訂控制項是您擁有和定義的控制項。建立自訂控制項時，建議您選擇代表目標的通用控制項，並將其用作證據來源。因此，您的自訂控制項可以收集與這些通用控制項相關的所有證據。您也可以使用核心控制項做為證據來源，或使用您自己定義的其他來源。完成後，將自訂控制項新增至自訂架構，然後建立評估以開始收集證據。

## 其他資源

若要在稽核管理員中建立和管理控制項，請遵循此處概述的程序。

- [尋找可用的控制項 AWS Audit Manager](#)
- [檢閱中的控制項 AWS Audit Manager](#)
  - [檢閱共同控制項](#)
  - [檢閱核心控制項](#)
  - [複查標準控制項](#)
  - [檢閱自訂控制項](#)
- [在中建立自訂控制項 AWS Audit Manager](#)
  - [從頭開始創建自定義控件 AWS Audit Manager](#)
  - [在中製作控制項的可編輯副本 AWS Audit Manager](#)
- [編輯中的自訂控制項 AWS Audit Manager](#)

- [變更控制項收集證據的頻率](#)
- [刪除中的自訂控制項 AWS Audit Manager](#)
- [自動化證據的支援資料來源類型](#)
  - [AWS Config 規則 支持 AWS Audit Manager](#)
  - [AWS Security Hub 支援的控制項 AWS Audit Manager](#)
  - [AWS 支援的 API 呼叫 AWS Audit Manager](#)
  - [AWS CloudTrail 支援的事件名稱 AWS Audit Manager](#)

## 尋找可用的控制項 AWS Audit Manager

您可以在 Audit Manager 主控台的 [控制項程式庫] 頁面上找到所有可用的控制項。

您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢視所有可用的控制項。

### 必要條件

請確定您的 IAM 身分具有適當的許可，可在中檢視控制項 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

#### Audit Manager console

若要在 Audit Manager 主控台上檢視可用控制項

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選擇索引標籤以瀏覽可用的控制項。
  - 選擇「一般」以查看由提供的一般控制項 AWS。
  - 選擇「標準」以查看由提供的標準控制項 AWS。
  - 選擇 [自訂] 以查看您建立的自訂控制項。

## AWS CLI

若要在中尋找共用控制項 (AWS CLI)

執行命[list-common-controls](#)令以查看常用控制項的清單。

```
aws controlcatalog list-common-controls
```

您也可以使用選用common-control-filter屬性來傳回具有特定目標的一般控制項清單。

在下列範例中，將#####取代為您自己的資訊。

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

若要尋找其他類型的控制項 AWS CLI

執行[清單控制項](#)指令，並指定--control-type為CustomStandard、或。Core

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager list-controls --control-type Type
```

## Audit Manager API

若要使用 API 尋找通用控制項

使用此[ListCommonControls](#)作業查看可用通用控制項的清單。您也可以使用選用commonControlFilter屬性來傳回具有特定目標的控制項清單。

若要使用 API 尋找其他類型的控制項

使用該[ListControls](#)操作並將[控制類型](#)指定為CustomStandard、或Core。

如需詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

當您準備好探索控制項的詳細資料時，請依照中的步驟操作[檢閱中的控制項 AWS Audit Manager](#)。此頁面將引導您完成控制項詳細資訊，並說明您在此處看到的資訊。

您也可以從控制項程式庫頁面[建立自訂控制項](#)、[編輯自訂控制項](#)或[刪除自訂控制項](#)。

## 其他資源

如需控制 Audit Manager 中問題的解決方案，請參閱 [控制項和控制集問題疑難排解](#)

## 檢閱中的控制項 AWS Audit Manager

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱控制項的詳細資訊。

若要開始在 Audit Manager 中檢閱控制項，請遵循此處概述的程序。

- [檢閱共同控制項](#)
- [檢閱核心控制項](#)
- [複查標準控制項](#)
- [檢閱自訂控制項](#)

## 檢閱共同控制項

當您需要檢閱控制項的詳細資料時，您會在控制項詳細資料頁面上找到組織成數個區段的資訊。這些章節可協助您輕鬆存取和瞭解該控制項的相關資訊。

### 必要條件

確保您的 IAM 身分具有適當的許可，以檢視 Audit Manager 中的通用控制項。更明確地說，您需要下列權限才能檢視 Control Catalog 所提供的一般控制項、控制項目標及 AWS 控制項網域：

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

授與這些權限的建議策略是 [AWSAuditManagerAdministratorAccess](#)。

### 程序

您可以使用 Audit Manager 主控台、控 AWS 制目錄 API 或 AWS Command Line Interface (AWS CLI) 來檢閱通用控制項。

## Audit Manager console

在 Audit Manager 主控台上檢視一般控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選擇「一般」以查看由提供的一般控制項 AWS。
4. 選擇任何一般控制項名稱，即可檢視該控制項的詳細資訊。
5. 使用下列資訊作為參考，檢閱一般控制項詳細資訊。

### 概述部分

本節說明常見控制項。

### 證據來源標籤

此標籤包含下列資訊：

名稱	描述
核心控制	<p>這些是收集證據以支持共同控制的核心控制項。</p> <ul style="list-style-type: none"><li>• 當您收集此共同控制項的證據時，您會自動收集此處列出的所有核心控制項的證據。當這些核心控制項中的每一個都成功實作時，這有助於證明您符合共用控制項的需求。</li><li>• 每個核心控制項都使用預先定義的資料來源分組來收集 AWS 服務。AWS 為您管理這些資料來源。這意味著每當法規和標準發生變化以及識別新的數據源時，它們都會自動更新。選擇任何核心控制項以查看基礎資料來源。</li></ul>

### 相關需求標籤

當您收集此通用控制項的證據時，相同的證據可協助您證明是否符合此索引標籤上所列之相關標準控制項的需求。選擇任何標準控制項以查看更多詳細資訊。

**Note**

- 共同控制項可能會產生證據，證明只有部分符合標準控制項。您可能需要其他證據才能證明完全符合標準控制。
- 此時，「相關需求」頁標只會顯示相關的標準控制項。雖然通用控制項可以與一或多個自訂控制項相關，但這些關聯不會顯示在此索引標籤中。

## AWS CLI

若要檢視中的一般控制項詳細資訊 AWS CLI

1. 執行命 [list-common-controls](#) 令以查看可用的通用控制項清單。當您使用此作業時，您可以套用選擇性 `common-control-filter` 來查看具有特定目標的一般控制項。

```
aws controlcatalog list-common-controls
```

2. 在回應中，識別您要檢閱的通用控制項，並記下其詳細資訊。

## AWS Control Catalog API

若要使用 API 檢視一般控制項詳細資料

1. 使用此 [ListCommonControls](#) 作業查看可用通用控制項的清單。使用此作業時，您可以套用選用項目 `commonControlFilter` 來查看具有特定目標的控制項清單。
2. 在回應中，識別您要檢閱的控制項，並記下其詳細資訊。

如需有關這些 API 作業的詳細資訊，請選擇此程序中的連結，以閱讀 AWS 控制目錄 API 參考中的詳細資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

您可以選擇代表目標的通用控制項，並使用它們做為建置組塊來建立自訂控制項。每個自動通用控制項都會對應至 Audit Manager 為您處理的預先定義 AWS 資料來源群組。這意味著您不必成為 AWS 專家，即可知道哪些資料來源為您的目標收集相關證據。此外，您不必自行維護這些資料來源對應。

如需如何建立使用通用控制項做為證據來源的自訂控制項的指示，請參閱 [在中建立自訂控制項 AWS Audit Manager](#)。



## 其他資源

- [檢閱核心控制項](#)
- [複查標準控制項](#)
- [檢閱自訂控制項](#)

## 檢閱核心控制項

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱 Audit Manager 核心控制項的詳細資料。

### 必要條件

請確定您的 IAM 身分具有適當的許可，可在中檢視控制項 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

#### Audit Manager console

在稽核管理員主控台上檢視核心控制項詳細資料

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選擇「一般」以查看由提供的一般控制項 AWS。
4. 尋找符合您使用案例的通用控制項。
5. 選擇一般控制項名稱旁的樹狀檢視圖示。這會顯示支援一般控制項的核心控制項。
6. 選擇您要檢閱的核心控制項名稱。
7. 使用下列資訊作為參考，檢閱核心控制項詳細資料。

#### 概述部分

本節說明核心控制項，並列出其從中收集證據的[資料來源類型](#)。

#### 證據來源標籤

此標籤包含下列資訊：

名稱	描述
資料來源	<p>這些是核心控制項從中收集證據的 AWS 受管資料來源。每當法規和標準發生變化以及識別新的資料來源時，這些資料來源都會自動更新。</p> <ul style="list-style-type: none"> <li>• 映射 — 用於收集證據的特定關鍵字。 <ul style="list-style-type: none"> <li>• 如果類型為 AWS Config，則對映為 AWS Config 規則 (例如 SNS_ENCRYPTED_KMS )。</li> <li>• 如果類型為 AWS Security Hub，則對應為 Security Hub 控制項 (例如 EC2.1)。</li> <li>• 如果類型是 AWS API 呼叫，則對應為 API 呼叫 (例如 kms_ListKeys )。</li> <li>• 如果類型為 AWS CloudTrail，則對映為 CloudTrail 事件 (例如 CreateAccessKey )。</li> </ul> </li> <li>• 類型 — 證據來源的資料來源類型。 <ul style="list-style-type: none"> <li>• 如果 Audit Manager 收集證據，則類型可以是 AWS Security Hub、AWS Config、AWS CloudTrail、或 AWS API 呼叫。</li> <li>• 如果您上傳自己的證據，則類型為「手動」。說明會指出所需的手動證據是檔案上傳還是文字回應。</li> </ul> </li> <li>• 頻率 — Audit Manager 為 AWS API 呼叫資料來源收集證據的頻率。</li> </ul>

## 詳細資訊索引標籤

此標籤包含下列資訊：

名稱	描述
指示	描述如何測試和修復控制項的方向。
測試資訊	建議的測試程序。
行動計劃	如果您需要修復控制項，建議採取的動作。

## AWS CLI

若要檢視核心控制項詳細資料 AWS CLI

1. 請依照下列步驟[尋找控制項](#)。確保將設置 `--control-type` 為 `Core`，並根據需要應用任何可選過濾器。

```
aws auditmanager list-controls --control-type Core
```

2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 和 Amazon 資源名稱 (ARN)。
3. 執行取[得控制](#)命令並指定。 `--control-id` 在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

### Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解這些資料，請參閱《AWS CLI 命令參考》中的 [get-control 輸出](#)。

4. 若要查看標籤詳細資料，請執行[list-tags-for-resource](#)命令並指定 `--resource-arn`。在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

## Audit Manager API

若要使用 API 檢視核心控制項詳細資料

1. 請依照下列步驟[尋找控制項](#)。請務必將 `ControlType` 設定為 `Core`，並視需要套用任何選用的濾鏡。
2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 和 Amazon 資源名稱 (ARN)。
3. 使用 [GetControl](#) 操作並指定您在步驟 2 中記下的 [控制 L id](#)。

**i** Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解此資料，請參閱 AWS Audit Manager API 參考資料中的[GetControl 回應元素](#)。

4. 若要查看標籤詳細資料，請使用[ListTagsForResource](#)作業並指定您在步驟 2 中記下的 [resourceArn](#)。

如需有關這些 API 作業的詳細資訊，請選擇此程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

您可以選擇代表目標的核心控制項，並使用它們做為建置組塊來建立自訂控制項。每個自動化核心控制項都會對應至 Audit Manager 為您處理的預先定義 AWS 資料來源群組。這意味著您不必成為 AWS 專家，即可知道哪些資料來源為您的目標收集相關證據。此外，您不必自行維護這些資料來源對應。

如需如何建立使用核心控制項做為證據來源的自訂控制項的指示，請參閱[在中建立自訂控制項 AWS Audit Manager](#)。

## 其他資源

- [檢閱共同控制項](#)
- [複查標準控制項](#)
- [檢閱自訂控制項](#)

## 複查標準控制項

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱標準控制項的詳細資訊。

## 必要條件

請確定您的 IAM 身分具有適當的許可，可在中檢視控制項 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱標準控制項的詳細資訊。

### Audit Manager console

在 Audit Manager 主控台上檢視標準控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選擇「標準」以查看由提供的標準控制項 AWS。
4. 選擇任何標準控制項名稱，以檢視該控制項的明細。
5. 使用下列資訊作為參考，複查標準控制項詳細資訊。

### 概述部分

本節說明標準控制項，並列出其用來收集證據的[資料來源類型](#)。

### 證據來源標籤

此標籤包含下列資訊：

名稱	描述
核心控制	<p>這些是收集證據以支持標準控制項的核心控制項。</p> <p>每個核心控制項都使用預先定義的資料來源分組來收集 AWS 服務。這些資料來源由您管理 AWS，並在法規和標準變更以及識別新資料來源時自動更新。選擇任何核心控制項以查看基礎資料來源。</p>
資料來源	<p>這些是收集證據以支援標準控制項的其他 AWS 受管資料來源。</p> <ul style="list-style-type: none"><li>• 映射 — 用於收集證據的特定關鍵字。<ul style="list-style-type: none"><li>• 如果類型為 AWS Config，則對映為 AWS Config 規則 (例如 SNS_ENCRYPTED_KMS )。</li><li>• 如果類型為 AWS Security Hub，則對應為 Security Hub 控制項 (例如 EC2.1)。</li></ul></li></ul>

名稱	描述
	<ul style="list-style-type: none"> <li>• 如果類型是 AWS API 呼叫，則對應為 API 呼叫 (例如 kms_ListKeys )。</li> <li>• 如果類型為 AWS CloudTrail，則對映為 CloudTrail 事件 (例如 CreateAccessKey )。</li> <li>• 類型 — 證據來源的資料來源類型。 <ul style="list-style-type: none"> <li>• 如果 Audit Manager 收集證據，則類型可以是 AWS Security Hub AWS Config、AWS CloudTrail、或 AWS API 呼叫。</li> <li>• 如果您上傳自己的證據，則類型為「手動」。說明會指出所需的手動證據是檔案上傳還是文字回應。</li> </ul> </li> <li>• 頻率 — Audit Manager 為 AWS API 呼叫資料來源收集證據的頻率。</li> </ul>

## 詳細資訊索引標籤

此標籤包含下列資訊：

名稱	描述
指示	描述如何測試和修復控制項的方向。
測試資訊	建議的測試程序。
行動計劃	如果您需要修復控制項，建議採取的動作。
Tags (標籤)	與控制項相關聯的標籤。
索引鍵	標籤鍵 (例如，符合性標準、法規或類別)。
Value	標籤值。

## AWS CLI

若要檢視標準控制項詳細資訊 AWS CLI

1. 請依照下列步驟[尋找控制項](#)。確保將設置 `--control-type` 為 `Standard`，並根據需要應用任何可選過濾器。

```
aws auditmanager list-controls --control-type Standard
```

2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 和 Amazon 資源名稱 (ARN)。
3. 執行取[得控制](#)命令並指定。 `--control-id` 在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

### Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解此資料，請參閱《命令參考》中的 [AWS CLI get-control 輸出](#)

4. 若要查看標籤詳細資料，請執行[list-tags-for-resource](#)命令並指定 `--resource-arn`。在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

## Audit Manager API

若要使用 API 檢視標準控制項詳細資料

1. 請依照下列步驟[尋找控制項](#)。請務必將 `ControlType` 設定為 `Standard`，並視需要套用任何選用的濾鏡。
2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 和 Amazon 資源名稱 (ARN)。
3. 使用 [GetControl](#) 操作並指定您在步驟 2 中記下的 [控制 L id](#)。

**i** Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解此資料，請參閱 AWS Audit Manager API 參考資料中的 [GetControl 回應元素](#)。

4. 若要查看標籤詳細資料，請使用 [ListTagsForResource](#) 作業並指定您在步驟 2 中記下的 [resourceArn](#)。

如需有關這些 API 作業的詳細資訊，請選擇此程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

您可以將標準控制項新增至任何自訂架構。如需說明，請參閱 [在中建立自訂架構 AWS Audit Manager](#)。

您也可以自訂任何標準控制項，使其符合您的需求。如需說明，請參閱 [在中製作控制項的可編輯副本 AWS Audit Manager](#)。

## 其他資源

- [檢閱共同控制項](#)
- [檢閱核心控制項](#)
- [檢閱自訂控制項](#)

## 檢閱自訂控制項

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱自訂控制項的詳細資料。

## 必要條件

請確定您的 IAM 身分具有適當的許可，可在中檢視控制項 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。



## 程序

您可以使用稽核管理員主控台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 來檢閱自訂控制項的詳細資料。

### Audit Manager console

在 Audit Manager 主控台上檢視自訂控制項詳細資料

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選擇 [自訂] 以查看您建立的自訂控制項。
4. 選擇任何自訂控制項名稱，即可檢視該控制項的詳細資料。
5. 使用下列資訊做為參考，檢閱自訂控制項詳細資料。

### 概述部分

本節說明自訂控制項，並列出其用來收集證據的[資料來源類型](#)。它還提供有關控制項何時建立和上次更新的資訊。

### 證據來源標籤

此索引標籤會顯示自訂控制項從何處收集證據。其包含下列資訊：

名稱	描述
通用控制	這些是收集證據以支持自定義控件的常見控件。  通用控制項使用為您 AWS 管理的基礎資料來源收集證據。對於列出的每個通用控制項，Audit Manager 會收集所有支援核心控制項的相關證據。選擇通用控制項以查看相關的核心控制項。
核心控制	這些是收集證據以支持自定義控件的核心控件。  核心控制項會使用為您 AWS 管理的預先定義資料來源群組來收集證據。選擇核心控制項以查看基礎資料來源。
資料來源	這些是收集證據以支援自訂控制項的資料來源。

名稱	描述
	<div data-bbox="618 212 1507 428" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b></p> <p>這些資料來源不是由您管理的 AWS。您有責任維護它們。</p> </div> <ul style="list-style-type: none"> <li>• <b>名稱</b> — 資料來源的名稱。</li> <li>• <b>類型</b> — 證據來源的資料來源類型。 <ul style="list-style-type: none"> <li>• 如果 Audit Manager 收集證據，則類型可以是 AWS Security Hub AWS Config、AWS CloudTrail、或 AWS API 呼叫。</li> <li>• 如果您上傳自己的證據，則類型為「手動」。說明會指出所需的手動證據是檔案上傳還是文字回應。</li> </ul> </li> <li>• <b>映射</b> — 用於收集證據的特定關鍵字。 <ul style="list-style-type: none"> <li>• 如果類型為 AWS Config，則對映為 AWS Config 規則 (例如 SNS_ENCRYPTED_KMS )。</li> <li>• 如果類型為 AWS Security Hub，則對應為 Security Hub 控制項 (例如 EC2.1)。</li> <li>• 如果類型是 AWS API 呼叫，則對應為 API 呼叫 (例如 kms_ListKeys )。</li> <li>• 如果類型為 AWS CloudTrail，則對映為 CloudTrail 事件 (例如 CreateAccessKey )。</li> </ul> </li> <li>• <b>頻率</b> — Audit Manager 為 AWS API 呼叫資料來源收集證據的頻率。</li> </ul>

## 詳細資訊索引標籤

此標籤包含下列資訊：

名稱	描述
指示	描述如何測試和修復控制項的方向。

名稱	描述
測試資訊	建議的測試程序。
行動計劃	如果您需要修復控制項，建議採取的動作。
Tags (標籤)	與控制項相關聯的標籤。
索引鍵	標籤鍵 (例如，符合性標準、法規或類別)。
Value	標籤值。

## AWS CLI

若要檢視自訂控制項詳細資料 AWS CLI

1. 請依照下列步驟[尋找控制項](#)。確保將設置 `--control-type` 為 `Custom`，並根據需要應用任何可選過濾器。

```
aws auditmanager list-controls --control-type Custom
```

2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 和 Amazon 資源名稱 (ARN)。
3. 執行取[得控制](#)命令並指定。 `--control-id` 在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

### Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解這些資料，請參閱《AWS CLI 命令參考》中的 [get-control 輸出](#)。

4. 若要查看控制項的標籤，請使用指[list-tags-for-resource](#)令並指定 `--resource-arn`。在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

## Audit Manager API

使用 API 檢視自訂控制項詳細資料

1. 請依照下列步驟[尋找控制項](#)。請務必將 [ControlType](#) 設定為 Custom，並視需要套用任何選用的濾鏡。
2. 在回應中，識別您要檢閱的控制項，並記下控制 ID 及其 Amazon 資源名稱 (ARN)。
3. 使用 [GetControl](#) 操作並指定您在步驟 2 中記下的 [控制 L id](#)。

### Tip

控制項詳細資訊會以 JSON 格式傳回。若要協助您瞭解此資料，請參閱 AWS Audit Manager API 參考資料中的 [GetControl 回應元素](#)。

4. 若要查看控制項的標籤，請使用 [ListTagsForResource](#) 作業並指定您在步驟 2 中記下的控制項 [resourceArn](#)。

如需有關這些 API 作業的詳細資訊，請選擇此程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

您可以將自訂控制項新增至任何自訂架構。如需說明，請參閱 [在中建立自訂架構 AWS Audit Manager](#)。

您也可以 [編輯自訂控制項](#)、[製作自訂控制項的可編輯副本](#)，或 [刪除不再需要的自訂控制項](#)。

## 其他資源

- [檢閱共同控制項](#)
- [檢閱核心控制項](#)
- [複查標準控制項](#)

## 在中建立自訂控制項 AWS Audit Manager

您可以使用自訂控制項來收集符合特定合規需求的證據。

就像標準控制項一樣，啟用的自訂控制項會在您的評估中持續收集證據。您也可以將手動證據新增至您建立的任何自訂控制項。每個證據都會成為記錄，協助您證明是否符合自訂控制項的需求。

若要開始使用，以下是如何使用自訂控制的範例：

將您的企業控制項對應至預先定義的 AWS 資料來源群組

您可以使用通用控制項作為證據來源，將您的企業控制項加入 Audit Manager。選擇代表您目標的通用控制項，並使用這些控制項做為建置區塊，以建立控制項，以收集符合性需求產品組合的證據。每個自動通用控制項都會對應至預先定義的資料來源群組。這意味著您不必成為 AWS 專家，即可知道哪些資料來源為您的目標收集相關證據。而當您使用通用控制項做為證據來源時，您不再需要維護資料來源對應，因為 Audit Manager 會為您處理此項目。

建立供應商風險評估問題

您可以使用自訂控制項來支援管理供應商風險評估的方式。您建立的每個控制項，都可以代表個別的風險評估問題。例如，控制項名稱可以是問題，您可以上傳檔案或輸入文字回應作為手動證據來提供答案。

## 重點

在 Audit Manager 中建立自訂控制項時，您有兩種方法可供選擇：

1. 從頭開始建立控制項-此方法提供最大的彈性，並可讓您根據您的確切需求量身打造控制項。這是一個很好的選擇，當你有一個特定的合規性要求沒有被現有的控制項充分覆蓋。當您需要將組織的企業控制項對應至預先定義的 AWS 資料來源群組，或是要將廠商風險評估問題建立為個別控制項時，此方法特別有用。
2. 建立現有控制項的可編輯副本-如果現有的標準控制項或自訂控制項部分符合您的需求，您可以建立該控制項的可編輯副本。如果您只需要對現有控制項進行較小的變更，則此方法會更有效率。如果您想要調整一些屬性，使控制項符合您的特定需求，這是一個不錯的選擇。例如，您可以變更控制項使用 API 呼叫來收集證據的頻率，然後變更控制項的名稱以反映這一點。

## 其他資源

如需如何建立自訂控制項的指示，請參閱下列資源。

- [從頭開始創建自定義控件 AWS Audit Manager](#)
- [在中製作控制項的可編輯副本 AWS Audit Manager](#)

## 從頭開始創建自定義控件 AWS Audit Manager

如果您組織的合規性需求與中可用的預先建置標準控制項不一致 AWS Audit Manager，您可以從頭開始建立自己的自訂控制項。

本頁概述建立根據您的特定需求量身打造的自訂控制項的步驟。

### 必要條件

請確定您的 IAM 身分具有在中建立自訂控制項的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

要從 AWS Config 和 Security Hub 成功收集證據，請確保您執行以下操作：

- [啟用 AWS Config](#)，然後套用 [AWS Config 與 Audit Manager 搭配使用的必要設定](#)
- [啟用 Security Hub](#)，然後套用 [必要的設定，以便搭配 Audit Manager 使用 Security Hub](#)

然後，每次針對指定 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 就可以收集證據。

### 程序

#### 任務

- [步驟 1：指定控制項詳細資訊](#)
- [步驟 2：指定證據來源](#)
- [步驟 3 \(選擇性\)：定義行動計劃](#)
- [步驟 4：檢閱並建立控制項](#)

#### 步驟 1：指定控制項詳細資訊

首先指定自訂控制項的詳細資訊。

#### Important

強烈建議您不要將敏感的識別資訊放入任意格式表單欄位，例如「控制項詳細資料」或「測試資訊」。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

## 如需指定控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中選取控制項資料庫，然後選取建立自訂控制項。
3. 在控制項詳細資訊下，輸入下列有關控制項的資訊。
  - 控制項 — 輸入好記的名稱、標題或風險評估問題。此值可協助您分辨控制項程式庫中的控制項。
  - 說明（選擇性） — 輸入詳細資訊，協助其他人瞭解控制項的目標。此說明會顯示在控制項詳細資訊頁面上。
4. 在測試資訊下，輸入測試控制項的建議步驟。
5. 在標籤下，選擇新增標籤，將標籤與控制項產生關聯。您可以指定一個索引鍵，為此控制項支援的相容性架構標籤提供最適合的說明。標籤索引鍵是必要的，當您在控制項程式庫中搜尋此控制項時，可用來做為搜尋條件。
6. 選擇下一步。

### 步驟 2：指定證據來源

接下來，指定一些證據來源。證據來源可決定您的自訂控制項從何處收集證據。您可以使用 AWS 受管來源、客戶管理來源，或兩者兼而有之。

#### Tip

我們建議您使用 AWS 受管理的來源。每當受 AWS 管理的來源更新時，相同的更新都會自動套用至使用這些來源的所有自訂控制項。這表示您的自訂控制項會針對該證據來源的最新定義收集證據。

如果您不確定要選擇哪些選項，請參閱下列範例和我們的建議。

您的角色	您的目標	推薦的證據來源
GRC 專業	我想收集特定網域或目標的證據	AWS 管理 ( <a href="#">common control</a> ) 使用對映至特定通用控制項的預先定義資料來源群組。

您的角色	您的目標	推薦的證據來源
技術專家	我想收集有關我負責的 AWS 資源的證據	AWS 管理 ( <a href="#">core control</a> ) 使用對映至 AWS 需求的預先定義資料來源群組。
技術專家	我想使用自訂 AWS Config 規則來收集證據	客戶管理 (自動化 <a href="#">data source</a> ) 使用自訂資料來源收集特定的自動化證據。
GRC 專業	我想收集證據，例如文件和文本回復	客戶管理 (手動 <a href="#">data source</a> ) 使用自訂資料來源上傳您自己的手動證據。

### 若要指定受 AWS 管理的來源 (建議)

我們建議您從選擇一個或多個常用控制項開始。當您選擇代表目標的共同控制項時，Audit Manager 會收集所有支援核心控制項的相關證據。如果您想要收集有關 AWS 環境的目標證據，也可以選擇個別的核心控制項。

### 若要指定 AWS 受管理的來源

1. 前往頁面的 AWS 受管理來源區段。
2. 若要新增通用控制項，請依照下列步驟執行：
  - a. 選取 [使用符合法規遵循目標的通用控制項]。
  - b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 2。您最多可以新增五個常用控制項。
3. 若要移除一般控制項，請選擇控制項名稱旁邊的 X。
4. 若要新增核心控制項，請依照下列步驟執行：
  - a. 選取 [使用符合規範 AWS 準則的核心控制項]。
  - b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 4。您最多可以新增 50 個核心控制項。
5. 若要移除核心控制項，請選擇控制項名稱旁邊的 X。



6. 若要新增客戶管理的資料來源，請遵循下列步驟。否則請選擇 Next (下一步)。 /

若要指定客戶管理的來源

若要從資料來源收集自動證據，您必須選擇資料來源類型和資料來源對映。這些詳細資料會對應到您的 AWS 使用情況，並告知 Audit Manager 從何處收集證據。如果您想提供自己的證據，則應改為選擇手動資料來源。

**Note**

您必須負責維護在此步驟中建立的資料來源對應。

若要指定客戶管理的來源

1. 前往頁面的「客戶管理來源」區段。
2. 選取「使用資料來源」以收集手動或自動證據。
3. 選擇新增。
4. 請選擇下列其中一個選項：
  - 選擇 AWS API 呼叫，然後選擇 API 呼叫和證據收集頻率。
  - 選擇AWS CloudTrail 事件，然後選擇事件名稱。
  - 選擇AWS Config 受管規則，然後選擇規則識別碼。
  - 選擇AWS Config 自訂規則，然後選擇規則識別碼。
  - 選擇「AWS Security Hub 控制」，然後選擇「Security Hub」控制項。
  - 選擇「手動資料來源」，然後選擇一個選項：
    - 檔案上傳 — 如果控制項需要文件作為證據，請使用此選項。
    - 文字回應 — 如果控制項需要風險評估問題的答案，請使用此選項。

**Tip**

如需有關自動資料來源類型和疑難排解秘訣的資訊，請參閱[自動化證據的支援資料來源類型](#)。

如果您需要與專家一起驗證資料來源設定，請立即選擇「手動資料來源」。這樣，您就可以建立控制項並立即將其新增至架構，然後視需要[編輯控制項](#)。

5. 在 [資料來源名稱] 下，提供描述性名稱。
6. (選擇性) 在其他詳細資訊下，輸入資料來源說明和疑難排解說明。
7. 選擇新增資料來源。
8. (選擇性) 若要新增其他資料來源，請選擇「新增」，然後重複步驟 1-7。您最多可以新增 100 個資料來源。
9. 若要移除資料來源，請從表格中選取資料來源，然後選擇「移除」。
10. 完成時，選擇下一步。

### 步驟 3 (選擇性)：定義行動計劃

接下來，指定需要修正此控制項時要採取的動作。

#### Important

我們強烈建議您不要將敏感的識別資訊放入任意格式欄位 (例如「行動計劃」) 中。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

### 定義行動計劃

1. 在標題下，輸入行動計劃的描述性標題。
2. 在「指示」下，輸入行動計劃的詳細指示。
3. 選擇下一步。

### 步驟 4：檢閱並建立控制項

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇建立自訂控制項。

### 後續步驟

建立新的自訂控制項之後，您可以將其新增至自訂架構。如需進一步了解，請參閱 [在中建立自訂架構 AWS Audit Manager](#) 和 [編輯自訂架構 AWS Audit Manager](#)。

將自訂控制項新增至自訂架構後，您可以建立評估並開始收集證據。如需進一步了解，請參閱 [在中建立評估 AWS Audit Manager](#)。

若要稍後重新造訪您的自訂控制項，請參閱[尋找可用的控制項 AWS Audit Manager](#)。您可以依照下列步驟找出自訂控制項，以便檢視、編輯或刪除它。

## 其他資源

如需在 Audit Manager 中控制問題的解決方案，請參閱[控制項和控制集問題疑難排解](#)。

## 在中製作控制項的可編輯副本 AWS Audit Manager

您可以使用現有的標準控制項或自訂控制項做為起點，並製作符合您需求的可編輯副本，而不是從頭開始建立自訂控制項。當您執行此操作時，現有的標準控制項會保留在控制項程式庫中，而且會使用您的自訂設定建立新的控制項。

### 必要條件

請確定您的 IAM 身分具有在中建立自訂架構的適當許可 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

要從 AWS Config 和 Security Hub 成功收集證據，請確保您執行以下操作：

- [啟用 AWS Config](#)，然後套用[AWS Config 與 Audit Manager 搭配使用的必要設定](#)。
- [啟用 Security Hub](#)，然後套用[必要的設定，以便搭配 Audit Manager 使用 Security Hub](#)。

然後，每次針對指定 AWS Config 規則或 Security Hub 控制項進行評估時，Audit Manager 就可以收集證據。

## 程序

### 任務

- [步驟 1：指定控制項詳細資訊](#)
- [步驟 2：指定證據來源](#)
- [步驟 3：\(選擇性\)：定義行動計劃](#)
- [步驟 4：檢閱並建立控制項](#)

### 步驟 1：指定控制項詳細資訊

控制項詳細資訊內容擷取自原始控制項。視需要檢閱和修改這些詳細資訊。

**⚠ Important**

強烈建議您不要將敏感的識別資訊放入任意格式表單欄位，例如「控制項詳細資料」或「測試資訊」。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

**如需指定控制項詳細資訊**

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中，選擇控制程式庫。
3. 選取您要變更的標準控制項或自訂控制項，然後選擇 [製作複本]。
4. 指定控制項的新名稱，然後選擇「繼續」。
5. 在控制項詳細資訊底下，視需要自訂控制項詳情。
6. 在「測試資訊」下，視需要變更指示。
7. 在標籤下，視需要自訂標籤。
8. 選擇下一步。

**步驟 2：指定證據來源**

證據來源是繼承自原始控制項。您可以視需要變更、新增或移除證據來源。

若要指定受 AWS 管理的來源 (建議)

**💡 Tip**

我們建議您從選擇一個或多個常用控制項開始。如果您有更精細的合規性需求，也可以選擇一個或多個特定的核心控制項。

若要指定 AWS 受管理的來源

1. 在受AWS 管理的來源下，檢閱目前的選取項目，並視需要進行變更。
2. 若要新增通用控制項，請依照下列步驟執行：
  - a. 選取 [使用符合法規遵循目標的通用控制項]。

- b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 2。您最多可以新增五個常用控制項。
3. 若要移除一般控制項，請選擇控制項名稱旁邊的 X。
4. 若要新增核心控制項，請依照下列步驟執行：
  - a. 選取 [使用符合規範 AWS 準則的核心控制項]。
  - b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 4。您最多可以新增 50 個核心控制項。
5. 若要移除核心控制項，請選擇控制項名稱旁邊的 X。
6. 若要編輯客戶管理的資料來源，請遵循下列步驟。否則請選擇 Next (下一步)。

#### 若要指定客戶管理的來源

若要從資料來源收集自動證據，您必須選擇資料來源類型和資料來源對映。這些詳細資料會對應到您的 AWS 使用情況，並告知 Audit Manager 從何處收集證據。如果您想提供自己的證據，則應改為選擇手動資料來源。

#### Note

您必須負責維護在此步驟中建立的資料來源對應。

#### 若要指定客戶管理的來源

1. 在「客戶管理來源」下，檢閱目前的資料來源，並視需要進行變更。
2. 若要移除資料來源，請從表格中選取資料來源，然後選擇「移除」。
3. 若要新增資料來源，請依照下列步驟執行：
  - a. 選取「使用資料來源」以收集手動或自動證據。
  - b. 選擇新增。
  - c. 請選擇下列其中一個選項：
    - 選擇 AWS API 呼叫，然後選擇 API 呼叫和證據收集頻率。
    - 選擇 AWS CloudTrail 事件，然後選擇事件名稱。
    - 選擇 AWS Config 受管規則，然後選擇規則識別碼。

- 選擇AWS Config 自訂規則，然後選擇規則識別碼。
- 選擇「AWS Security Hub 控制」，然後選擇「Security Hub」控制項。
- 選擇「手動資料來源」，然後選擇一個選項：
  - 檔案上傳 — 如果控制項需要文件作為證據，請使用此選項。
  - 文字回應 — 如果控制項需要風險評估問題的答案，請使用此選項。

 Tip

如需有關自動資料來源類型和疑難排解秘訣的資訊，請參閱[自動化證據的支援資料來源類型](#)。

如果您需要與專家一起驗證資料來源設定，請立即選擇「手動資料來源」。這樣，您就可以建立控制項並立即將其新增至架構，然後視需要[編輯控制項](#)。

- d. 在 [資料來源名稱] 下，提供描述性名稱。
  - e. (選擇性) 在其他詳細資訊下，輸入資料來源說明和疑難排解說明。
  - f. 選擇新增資料來源。
  - g. (選擇性) 若要新增其他資料來源，請選擇「新增」，然後重複步驟 3。您最多可以新增 100 個資料來源。
4. 完成時，選擇下一步。

### 步驟 3：(選擇性)：定義行動計劃

行動計劃會繼承自原始控制項。您可以視需要編輯此行動計劃。

 Important

我們強烈建議您不要將敏感的識別資訊放入任意格式欄位 (例如「行動計劃」) 中。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

### 若要指定指示

1. 在「標題」下，檢閱標題並視需要進行變更。
2. 在「指示」下，檢閱指示並視需要進行變更。
3. 選擇下一步。

## 步驟 4：檢閱並建立控制項

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。完成時，請選擇建立自訂控制項。

### 後續步驟

建立新的自訂控制項之後，您可以將其新增至自訂架構。如需進一步了解，請參閱 [在中建立自訂架構 AWS Audit Manager](#) 和 [編輯自訂架構 AWS Audit Manager](#)。

將自訂控制項新增至自訂架構後，您可以建立評估並開始收集證據。如需進一步了解，請參閱 [在中建立評估 AWS Audit Manager](#)。

若要稍後重新造訪您的自訂控制項，請參閱 [尋找可用的控制項 AWS Audit Manager](#)。您可以依照下列步驟找出自訂控制項，以便檢視、編輯或刪除它。

### 其他資源

如需在 Audit Manager 中控制問題的解決方案，請參閱 [控制項和控制集問題疑難排解](#)。

## 編輯中的自訂控制項 AWS Audit Manager

您可能需要在合規性需求變更時修改中 AWS Audit Manager 的自訂控制項。

本頁概述編輯自訂控制項詳細資訊、證據來源和行動計劃指示的步驟。

### 必要條件

下列程序假設您先前已建立自訂控制項。

請確定您的 IAM 身分具有適當的許可，可在中編輯自訂控制項 AWS Audit Manager。授與這些權限的兩個建議政策是 [AWSAuditManagerAdministratorAccess](#) 和 [授予使用者 AWS Audit Manager 管理存取權](#)。

### 程序

請依照下列步驟編輯自訂控制項。

#### Note

當您編輯控制項時，您的變更會套用至控制項處於作用中狀態的所有評量。在所有這些評估中，Audit Manager 會根據最新的控制定義自動開始收集證據。

## 任務

- [步驟 1：編輯控制項詳細資訊](#)
- [步驟 2：編輯證據來源](#)
- [步驟 3：編輯行動計劃](#)

### 步驟 1：編輯控制項詳細資訊

視需要檢閱和編輯控制項詳細資料。

#### Important

強烈建議您不要將敏感的識別資訊放入任意格式表單欄位，例如「控制項詳細資料」或「測試資訊」。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

若要編輯控制項詳細資訊

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在功能窗格中，選擇 [控制項庫]，然後選擇 [自訂] 索引標籤。
3. 選取您要編輯的控制項，並選擇編輯。
4. 在控制項詳細資訊底下，視需要編輯控制項詳細資訊。
5. 在「測試資訊」下，視需要編輯描述。
6. 選擇下一步。

### 步驟 2：編輯證據來源

接下來，您可以編輯、移除或新增控制項的證據來源。

#### Note

當您編輯控制項以包含更多或更少的證據來源時，這可能會影響您的控制項在任何有效評估中收集的證據量。例如，如果您新增證據來源，您可能會注意到 Audit Manager 會執行比以前更多的資源評估，並收集更多的證據。如果您刪除證據來源，則您的控制權可能會收集較少的證據。



如需有關資源評估和定價的詳細資訊，請參閱[AWS Audit Manager 定價](#)。

### 若要編輯 AWS 受管理的來源

#### 若要編輯 AWS 受管理的來源

1. 在受AWS 管理的來源下，檢閱目前的選取項目，並視需要進行變更。
2. 若要新增通用控制項，請依照下列步驟執行：
  - a. 選取 [使用符合法規遵循目標的通用控制項]。
  - b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 2。您最多可以新增五個常用控制項。
3. 若要移除一般控制項，請選擇控制項名稱旁邊的 X。
4. 若要新增核心控制項，請依照下列步驟執行：
  - a. 選取 [使用符合規範 AWS 準則的核心控制項]。
  - b. 從下拉式清單中選擇一般控制項。
  - c. (選擇性) 視需要重複步驟 4。您最多可以新增 50 個核心控制項。
5. 若要移除核心控制項，請選擇控制項名稱旁邊的 X。
6. 若要新增客戶管理的資料來源，請遵循下列步驟。否則請選擇 Next (下一步)。

#### 若要編輯客戶管理的來源

#### Note

您必須負責維護在此步驟中編輯的資料來源對應。

#### 若要編輯客戶管理的來源

1. 在「客戶管理來源」下，檢閱目前的資料來源，並視需要進行變更。
2. 若要移除資料來源，請從表格中選取資料來源，然後選擇「移除」。
3. 若要新增資料來源，請依照下列步驟執行：
  - a. 選取「使用資料來源」以收集手動或自動證據。

- b. 選擇新增。
- c. 請選擇下列其中一個選項：
  - 選擇 AWS API 呼叫，然後選擇 API 呼叫和證據收集頻率。
  - 選擇 AWS CloudTrail 事件，然後選擇事件名稱。
  - 選擇 AWS Config 受管規則，然後選擇規則識別碼。
  - 選擇 AWS Config 自訂規則，然後選擇規則識別碼。
  - 選擇「AWS Security Hub 控制」，然後選擇「Security Hub」控制項。
  - 選擇「手動資料來源」，然後選擇一個選項：
    - 檔案上傳 — 如果控制項需要文件作為證據，請使用此選項。
    - 文字回應 — 如果控制項需要風險評估問題的答案，請使用此選項。

 Tip


如需有關自動資料來源類型和疑難排解秘訣的資訊，請參閱[自動化證據的支援資料來源類型](#)。

如果您需要與專家一起驗證資料來源設定，請立即選擇「手動資料來源」。這樣，您就可以建立控制項並立即將其新增至架構，然後視需要[編輯控制項](#)。

- d. 在 [資料來源名稱] 下，提供描述性名稱。
  - e. (選擇性) 在其他詳細資訊下，輸入資料來源說明和疑難排解說明。
  - f. 選擇新增資料來源。
  - g. (選擇性) 若要新增其他資料來源，請選擇「新增」，然後重複步驟 3。您最多可以新增 100 個資料來源。
4. 完成時，選擇下一步。

### 步驟 3：編輯行動計劃

接下來，檢閱並編輯選用的行動計劃。

 Important

我們強烈建議您不要將敏感的識別資訊放入任意格式欄位 (例如「行動計劃」) 中。如果您建立內含敏感資訊的自訂控制項，您不得共用包含這些控制項的任何自訂架構。

## 若要編輯行動計劃

1. 在標題下，視需要編輯標題。
2. 在「指示」下，視需要編輯指示。
3. 選擇下一步。

## 步驟 4：檢視並儲存

檢閱控制項的資訊。如需變更步驟的資訊，請選擇編輯。

完成時，請選擇儲存變更。

### Note

編輯控制項之後，變更會在包含控制項的所有使用中評估中生效，如下所示：

- 對於以 AWS API 呼叫做為資料來源類型的控制項，變更會在次日的 00:00 UTC 生效。
- 之於所有其他控制項，變更會立即生效。

## 後續步驟

當您確定不再需要自訂控制項時，可以刪除該控制項來清除 Audit Manager 環境。如需說明，請參閱[刪除中的自訂控制項 AWS Audit Manager](#)。

## 其他資源

如需在 Audit Manager 中控制問題的解決方案，請參閱[控制項和控制集問題疑難排解](#)。

## 變更控制項收集證據的頻率

AWS Audit Manager 可以從各種數據源收集證據。證據收集的頻率取決於控制項使用的資料來源類型。

下列各章節提供關於每個控制項資料來源類型的證據收集頻率相關資訊，及其變更方式 (如果適用)。

### 主題

- [重點](#)

- [AWS API 呼叫的組態快照](#)
- [AWS Config 合規檢查](#)
- [安全中心的合規檢查](#)
- [使用者活動日誌 AWS CloudTrail](#)

## 重點

- 針對 AWS API 呼叫，Audit Manager 會使用對其他人 AWS 服務的描述 API 呼叫來收集證據。您可以直接在 Audit Manager 中指定證據收集頻率（僅適用於自訂控制項）。
- 對於 AWS Config，「Audit Manager」會直接從中報告符合性檢查的結果 AWS Config。頻率會遵循 AWS Config 規則中定義的觸發程序。
- 針對 AWS Security Hub，Audit Manager 會直接從 Security Hub 回報合規檢查的結果。頻率會遵循 Security Hub 的檢查排程。
- 對於 AWS CloudTrail，Audit Manager 會持續收集來自的證據 CloudTrail。您無法變更此證據類型的頻率。

## AWS API 呼叫的組態快照

### Note

以下內容僅適用於自訂控制項。您無法變更標準控制項的證據收集頻率。

如果自訂控制項使用 AWS API 呼叫做為資料來源類型，您可以依照下列步驟在 Audit Manager 中變更證據收集頻率。

使用 API 呼叫資料來源變更自訂控制項的證據收集頻率

1. 開啟 AWS Audit Manager 主控台，[網址為 https://console.aws.amazon.com/auditmanager/home](https://console.aws.amazon.com/auditmanager/home)。
2. 在功能窗格中，選擇 [控制項資料庫]，然後選擇 [自訂] 索引標籤。
3. 選擇您要編輯的自訂控制項，並選擇編輯。
4. 在編輯控制項詳細資訊頁面上，選擇下一步。
5. 在「客戶管理來源」下，尋找您要更新的 API 呼叫資料來源。
6. 從表格中選取資料來源，然後選擇「移除」。

7. 選擇新增。
8. 選擇 AWS API 呼叫。
9. 選擇您在步驟 5 中移除的相同 API 呼叫，然後選取偏好的證據收集頻率。
10. 在 [資料來源名稱] 下，提供描述性名稱。
11. ( 選擇性 ) 在其他詳細資訊下，輸入資料來源說明和疑難排解說明。
12. 選擇下一步。
13. 在編輯行動計劃頁面上，選擇下一步。
14. 在 [檢閱和更新] 頁面上，檢閱自訂控制項的資訊。如需變更步驟的資訊，請選擇編輯。
15. 完成時，請選擇儲存變更。

編輯控制項之後，變更會在包含控制項的所有作用中評估中，次日 00:00 UTC 生效。

## AWS Config 合規檢查

### Note

以下內容適用於使用 AWS Config 規則 做為資料來源使用的標準控制項和自訂控制項。

如果控制項用 AWS Config 作資料來源類型，您無法直接在 Audit Manager 中變更證據收集頻率。這是因為頻率遵循 AWS Config 規則中定義的觸發程序。

有兩種類型的觸發器 AWS Config 規則：

1. 組態變更- AWS Config 在建立、變更或刪除特定類型的資源時，執行規則的評估。
2. 週期性-以您選擇的頻率 AWS Config 執行規則評估 (例如，每 24 小時)。

若要深入瞭解的觸發器 AWS Config 規則，請參閱開發 AWS Config 人員指南中的 [觸發器類型](#)。

如需如何管理的指示 AWS Config 規則，請參閱 [管理 AWS Config 規則](#)。

## 安全中心的合規檢查

### Note

以下內容適用於使用 Security Hub 檢查做為資料來源的標準控制項和自訂控制項。

如果控制項使用 Security Hub 做為資料來源類型，您無法直接在 Audit Manager 中變更證據收集頻率。這是因為頻率遵循 Security Hub 的檢查排程。

- 定期檢查會在最近一次執行後的 12 小時內自動執行。您無法變更其週期性。
- 變更觸發檢查會在關聯資源變更狀態時執行。即使資源未變更狀態，變更觸發檢查的時間也會每 18 小時重新整理一次更新。這有助於指出控制是否仍已啟用。一般而言，Security Hub 會盡可能地使用變更觸發規則。

若要深入瞭解，請參閱AWS Security Hub 使用指南中的[執行安全檢查的排程](#)。

## 使用者活動日誌 AWS CloudTrail

### Note

以下內容適用於使用 AWS CloudTrail 使用者活動日誌做為資料來源的標準控制項和自訂控制項。

您無法變更使用活動記錄 CloudTrail 做為資料來源類型之控制項的證據收集頻率。Audit Manager 會以連續的方式收集此證據類型。CloudTrail 頻率是連續的，因為使用者活動可能在一天中的任何時間發生。

## 刪除中的自訂控制項 AWS Audit Manager

如果您建立了自訂控制項，但不再需要它，您可以將其從 Audit Manager 環境中刪除。這可讓您清理工作區，並專注於與目前工作和優先順序相關的自訂控制項。

### 必要條件

下列程序假設您先前已建立自訂控制項。

請確定您的 IAM 身分具有適當的許可，以刪除中的自訂控制項 AWS Audit Manager。授與這些權限的兩個建議政策是[AWSAuditManagerAdministratorAccess](#)和[授予使用者 AWS Audit Manager 管理存取權](#)。

## 程序

您可以使用稽核管理員主控台、稽 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 刪除自訂控制項。

### Important

當您刪除自訂控制項時，此動作會從目前相關的任何自訂架構或評估中移除控制項。因此，Audit Manager 將停止收集在您所有評估中該自訂控制項的證據。這包括您先前在刪除自訂控制項之前建立的評估。

### Audit Manager console

刪除 Audit Manager 主控台上的自訂控制項

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在導覽窗格中選取控制項資料庫，然後選取建立自訂控制項標籤。
3. 選取您要刪除的控制項，然後選擇刪除。
4. 在出現的快顯視窗中，選擇刪除以確認刪除。

### AWS CLI

若要刪除中的自訂控制項 AWS CLI

1. 首先，找出您要刪除的自訂控制項。為此，請執行 [list-controls](#) 指令，並指定 `--control-type` 為 Custom。

```
aws auditmanager list-controls --control-type Custom
```

回應會傳回自訂控制項。找到您要刪除的控制項，並記下控制項 ID。

2. 接下來，執行 [刪除控制項](#) 指令，並使用 `--control-id` 參數來指定要刪除的控制項。

在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111
```

## Audit Manager API

若要使用 API 刪除自訂控制項

1. 使用該[ListControls](#)操作並將[控制類型](#)指定為Custom。從回應中找到您要刪除的控制項並記下控制項 ID。
2. 使用此[DeleteControl](#)作業刪除自訂控制項。在要求中，使用[controlId](#)參數來指定您要刪除的控制項。

如需有關這些 API 作業的詳細資訊，請選擇上一個程序中的任何連結，以在 AWS Audit Manager API 參考中閱讀更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 其他資源

如需 Audit Manager 中資料保留的相關資訊，請參閱[刪除 Audit Manager 資料](#)。



# 檢閱及設定您的 AWS Audit Manager 設定

您可以隨時檢閱和設定您的 AWS Audit Manager 設定，以確保這些設定符合您的特定需求。

本章將引導您完成存取、檢閱和調整 Audit Manager 設定的程序 step-by-step。繼續進行操作，您將了解如何變更一般設定、評估設定和證據搜尋器設定，以配合不斷演進的合規目標和業務需求。

## 程序

若要開始使用，請依照下列步驟檢視 Audit Manager 設定。您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來檢視 Audit Manager 設定。

若要檢視您的設定

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇符合您目標的標籤。
  - 一般設定-選擇此標籤可檢閱和更新您的一般 Audit Manager 設定。
  - 評估設定-選擇此標籤可檢閱和更新評估的預設設定。
  - 證據搜尋器設定-選擇此標籤以檢視和更新您的證據搜尋器設定。

## 後續步驟

若要針對您的使用案例自訂 Audit Manager 設定，請遵循此處概述的程序。

- 一般設定
  - [設定您的資料加密設定](#)
  - [新增委派管理員](#)
  - [變更委派管理員](#)
  - [移除委派的管理員](#)
  - [禁用 AWS Audit Manager](#)
- 評估設定

- [設定您的預設稽核擁有者](#)
- [設定您的預設評估報告目標](#)
- [設定 Audit Manager 通知](#)
- 證據搜尋器設定
  - [啟用證據搜尋工具](#)
  - [確認證據搜尋器的狀態](#)
  - [設定證據搜尋器的預設匯出目的地](#)
  - [停用證據搜尋工具](#)

## 設定您的資料加密設定

您可以在中選擇加密資料的方式 AWS Audit Manager。Audit Manager 會自動 AWS 受管金鑰 為資料的安全儲存建立唯一的資料。依預設，您的 Audit Manager 資料會使用此 KMS 金鑰加密。不過，如果您想要自訂資料加密設定，您可以指定自己的對稱加密客戶管理金鑰。使用您自己的 KMS 金鑰 可為您提供更多彈性，包括能夠建立、旋轉和停用金鑰。

### 必要條件

如果您提供客戶管理的金鑰，該金鑰必須與您的評估 AWS 區域 相同，才能成功產生評估報告並匯出證據搜尋結果。

### 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來更新資料加密設定。

#### Note

如果您變更 Audit Manager 資料加密設定，這些變更會套用至您建立的任何新評估。這包括您依據新評估建立的任何評估報告和證據搜尋工具匯出。

這些變更不會套用至您在變更加密設定之前，已建立的現有評估。除現有的評估報告和 CSV 匯出外，還包括您依據現有評估建立的新評估報告和 CSV 匯出。現有的評估及其所有評估報告和 CSV 匯出都將繼續使用舊有的 KMS 金鑰。如果產生評估報告的 IAM 身分無法使用舊有 KMS 金鑰，則在金鑰政策層級授予許可。

## Audit Manager console

若要在 Audit Manager 主控台上更新資料加密設定

1. 從一般設定索引標籤，前往資料加密區段。
2. 如需使用 Audit Manager 提供的預設 KMS 金鑰，請清除自訂加密設定 (進階) 核取方塊。
3. 如需使用客戶受管金鑰，請選擇自訂加密設定 (進階) 核取方塊。您可選擇現有 KMS 金鑰或建立新的金鑰。

## AWS CLI

若要更新您的資料加密設定 AWS CLI

執行[更新設定](#)命令，並使用 `--kms-key` 參數來指定您自己的客戶受管金鑰。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

## Audit Manager API

使用 API 更新您的資料加密設定

呼叫[UpdateSettings](#)作業，並使用 [KMSKey](#) 參數來指定您自己的客戶管理金鑰。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 其他資源

- 如需有關如何建立金鑰的說明，請參閱AWS Key Management Service 使用者指南中的[建立金鑰](#)。
- 如需如何在金鑰原則層級授與權限的指示，請參閱 AWS Key Management Service 開發人員指南中的[允許其他帳戶中的使用者使用 KMS 金鑰](#)。

## 新增委派管理員

如果您使用 AWS Organizations 且想要啟用的多帳戶支援 AWS Audit Manager，您可以將組織中的成員帳戶指定為 Audit Manager 的委派管理員。

如果您想要在多個「Audit Manager 員」中使用 AWS 區域，則必須在每個區域中個別指定委派的管理員帳戶。在 Audit Manager 設定中，您應該在所有區域中使用相同的委派管理員帳戶。

## 必要條件

請注意下列定義委派管理員如何在 Audit Manager 中運作的因素。

- 您的帳戶必須屬於組織帳戶。
- 指定委派管理員之前，您必須先[啟用組織中的所有功能](#)。此外，您必須[設定組織的 Security Hub 設定](#)。如此一來，Audit Manager 就可以從您的成員帳戶收集 Security Hub 證據。
- 委派的管理員帳戶必須具有您在設定 Audit Manager 員時提供的 KMS 金鑰的存取權。
- 您無法在 Audit Manager AWS Organizations 管理員中以委派的系統管理員身分使用您的管理帳戶。

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來新增委派管理員。

### Note

在 Audit Manager 設定中新增委派管理員後，您的管理帳戶將無法再在 Audit Manager 中建立其他評估。此外，針對管理帳戶建立的任何現有評估，系統會停止證據收集。Audit Manager 會收集證據並附加至委派管理員帳戶，委派管理員是管理組織評估的主要帳戶。

### Audit Manager console

若要在稽核管理員主控台上新增委派的管理員

1. 從一般設定索引標籤，前往委派管理員區段。
2. 在委派管理員帳戶 ID 項下，輸入委派管理員的帳戶 ID。
3. 選擇委派。

## AWS CLI

若要在中新增委派管理員 AWS CLI

執行[register-organization-admin-account](#)命令並使用--admin-account-id參數來指定委派管理員的帳戶 ID。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

## Audit Manager API

使用 API 新增委派管理員

呼叫[RegisterOrganizationAdminAccount](#)作業，並使用[adminAccountId](#)參數來指定委派系統管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 後續步驟

若要變更委派管理員帳戶，請參閱[變更委派管理員](#)。

若要移除委派管理員帳戶，請參閱[移除委派的管理員](#)。

## 其他資源

- [建立和管理組織](#)
- [委派系統管理員與 AWS Organizations 相關問題疑難排解](#)

## 變更委派管理員

在中變更委派管理員 AWS Audit Manager 需要兩個步驟。首先，您必須移除目前委派的系統管理員帳戶。然後，您可以將新帳戶新增為委派管理員。

請依照此頁面上的步驟變更您的委派管理員。

內容

- [必要條件](#)
  - [移除目前帳戶之前](#)
  - [在您添加新帳戶之前](#)
- [程序](#)
- [後續步驟](#)
- [其他資源](#)

## 必要條件

### 移除目前帳戶之前

移除目前委派的系統管理員帳戶之前，請記住下列考量事項：

- **證據搜尋工具清除工作**-如果目前委派的管理員 (帳戶 A) 已啟用證據搜尋工具，您必須先執行清理工作，才能將帳戶 B 指派為新的委派管理員。

在您使用管理帳戶移除帳戶 A 之前，請確定帳戶 A 已登入 Audit Manager 並停用證據搜尋工具。停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。

如果未完成此工作，事件資料存放區會保留在帳戶 A 中。在此情況下，我們建議原始委派管理員使用 CloudTrail Lake 手動[刪除事件資料存放區](#)。

為了確保您最終不會產生多個事件資料存放區，有必要進行此清理任務。在您移除或變更委派的管理員帳戶後，Audit Manager 會忽略未使用的事件資料存放區。但是，如果您未刪除未使用的事件資料存放區，則事件資料存放區會繼續向 CloudTrail Lake 產生儲存費用。

- **資料刪除**-當您移除稽核管理員的委派系統管理員帳戶時，不會刪除該帳戶的資料。如果您想要刪除委派管理員帳戶的資源資料，則必須先單獨執行該任務，然後才能移除帳戶。您可以在 Audit Manager 主控台中執行這項操作。或者，您可以使用 Audit Manager 提供的其中一項 API 刪除操作。如需可用刪除操作的清單，請參閱[刪除 Audit Manager 資料](#)。

目前，Audit Manager 不提供刪除特定委派管理員證據的選項。相反地，當您註銷 Audit Manager 管理帳戶時，我們會在註銷時對目前的委派管理員帳戶執行清除任務。

### 在您添加新帳戶之前

在您新增新的委派系統管理員帳戶之前，請記住下列考量事項：

- 新帳戶必須是組織的一部分。
- 在指定新的委派管理員之前，您必須先[啟用組織中的所有功能](#)。此外，您必須[設定組織的 Security Hub 設定](#)。如此一來，Audit Manager 就可以從您的成員帳戶收集 Security Hub 證據。
- 委派的管理員帳戶必須具有您在設定 Audit Manager 員時提供的 KMS 金鑰的存取權。
- 您無法在 Audit Manager AWS Organizations 管理員中以委派的系統管理員身分使用您的管理帳戶。

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來變更委派的管理員。

### Warning

當您變更委派管理員時，您可以繼續存取先前在舊有委派管理員帳戶下收集的證據。不過，Audit Manager 會停止收集證據，並停止將證據附加至舊有委派管理員帳戶。

## Audit Manager console

若要在稽核管理員主控台上變更目前的委派管理員

1. (選用) 如果目前委派管理員 (帳戶 A) 已啟用證據搜尋工具，請執行下列清除任務：
  - 將帳戶 B 指派為新的委派管理員之前，請確定帳戶 A 登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除帳戶 A 啟用證據搜尋工具時建立的事件資料存放區。如果您未完成此步驟，則帳戶 A 必須移至 CloudTrail Lake 並手動[刪除事件資料存放區](#)。否則，事件資料存放區會保留在帳戶 A 中，並繼續產生 CloudTrail Lake 儲存費用。
2. 從一般設定索引標籤，前往委派管理員區段並選擇移除。
3. 在出現的快顯視窗中，選擇移除以確認移除。
4. 在委派管理員帳戶 ID 項下，輸入新委派管理員帳戶 ID。
5. 選擇委派。

## AWS CLI

若要變更目前的委派管理員 AWS CLI

首先，使用 `--admin-account-id` 參數執行 [deregister-organization-admin-account](#) 命令，以指定目前委派管理員的帳戶 ID。

在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

然後，使用 `--admin-account-id` 參數執行 [register-organization-admin-account](#) 命令，以指定新委派管理員的帳戶 ID。

在下列範例中，將 `#####` 取代為您自己的資訊。

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

## Audit Manager API

使用 API 變更目前委派的管理員

首先，呼叫 [DeregisterOrganizationAdminAccount](#) 作業，並使用 `adminAccountId` 參數來指定目前委派管理員的帳戶 ID。

然後，呼叫 [RegisterOrganizationAdminAccount](#) 作業，並使用 `adminAccountId` 參數來指定新委派系統管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 後續步驟

若要移除委派管理員帳戶，請參閱 [移除委派的管理員](#)。

## 其他資源

- [建立和管理組織](#)
- [委派系統管理員與 AWS Organizations 相關問題疑難排解](#)



## 移除委派的管理員

移除委派的系統管理員帳戶會停止該帳戶的進一步證據收集，但您仍可保留先前收集之證據的存取權。

如果您需要移除 Audit Manager 的委派管理員帳戶，您可以依照此頁面上的必要步驟執行。請仔細遵循先決條件和程序，因為它們涉及清理資源，以避免不必要的存儲成本。

### 必要條件

從稽核管理員移除委派的系統管理員帳戶之前，請記住下列考量事項：

#### 證據搜尋工具清理任務

如果目前委派的管理員已啟用證據搜尋工具，您需要執行清除工作。

在您使用管理帳戶移除目前委派的系統管理員之前，請確定目前委派的系統管理員帳戶已登入 Audit Manager 並停用證據搜尋工具。停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。

如果此任務未完成，則事件資料存放區會保留在帳戶中。在此情況下，建議原始委派管理員使用 CloudTrail Lake 手動[刪除事件資料存放區](#)。

為了確保您最終不會產生多個事件資料存放區，有必要進行此清理任務。在您移除或變更委派的管理員帳戶後，Audit Manager 會忽略未使用的事件資料存放區。但是，如果您未刪除未使用的事件資料存放區，則事件資料存放區會繼續向 CloudTrail Lake 產生儲存費用。

#### 資料刪除

當您移除 Audit Manager 的委派管理員帳戶時，不會刪除該帳戶的資料。如果您想要刪除委派管理員帳戶的資源資料，則必須先單獨執行該任務，然後才能移除帳戶。您可以在 Audit Manager 主控台中執行這項操作。或者，您可以使用 Audit Manager 提供的其中一項 API 刪除操作。如需可用刪除操作的清單，請參閱[刪除 Audit Manager 資料](#)。

目前，Audit Manager 不提供刪除特定委派管理員證據的選項。相反地，當您註銷 Audit Manager 管理帳戶時，我們會在註銷時對目前的委派管理員帳戶執行清除任務。

### 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 來移除委派管理員。

**⚠ Warning**

當您移除委派管理員時，您可以繼續存取先前在該委派管理員帳戶下收集的證據。不過，Audit Manager 會停止收集證據，並停止將證據附加至舊有委派管理員帳戶。

## Audit Manager console

若要在稽核管理員主控台上移除目前的委派管理員

1. (選用) 如果目前委派管理員 已啟用證據搜尋工具，請執行下列清除任務：

- 確定目前委派管理員帳戶登入 Audit Manager 並停用證據搜尋工具。

停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。如果此步驟未完成，委派的系統管理員帳戶必須使用 CloudTrail Lake 手動[刪除事件資料存放區](#)。否則，事件資料存放區會保留在其帳戶中，並繼續產生 CloudTrail Lake 儲存費用。

2. 從一般設定索引標籤，前往委派管理員區段並選擇移除。
3. 在出現的快顯視窗中，選擇移除以確認移除。

## AWS CLI

停用證據搜尋工具會自動刪除啟用證據搜尋工具時帳戶中建立的事件資料存放區。如果此步驟未完成，委派的系統管理員帳戶必須使用 CloudTrail Lake 手動[刪除事件資料存放區](#)。否則，事件資料存放區會保留在其帳戶中，並繼續產生 CloudTrail Lake 儲存費用。

若要移除目前的委派管理員 AWS CLI

執行[deregister-organization-admin-account](#)命令並使用 `--admin-account-id` 參數來指定委派管理員的帳戶 ID。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

## Audit Manager API

使用 API 移除目前委派的管理員

呼叫 [DeregisterOrganizationAdminAccount](#) 作業，並使用 [adminAccountId](#) 參數來指定委派系統管理員的帳戶 ID。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 其他資源

- [委派系統管理員與 AWS Organizations 相關問題疑難排解](#)

## 設定您的預設稽核擁有者

您可以使用此設定來指定在 Audit Manager 中具有評量的主要存取權限的預 [audit owner](#) 設值。

### 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來更新此設定。

#### Audit Manager console

您可以從表格中 AWS 帳戶 列出的項目中進行選擇，或使用搜尋列來尋找其他項目 AWS 帳戶。

若要在稽核管理員主控台上更新預設 Audit Manager 擁有者

1. 從評估設定索引標籤，前往預設稽核擁有者區段，然後選擇編輯。
2. 如需新增預設稽核擁有者，請選擇稽核擁有者下方帳戶名稱旁的核取方塊。
3. 如需移除預設稽核擁有者，請清除稽核擁有者下方帳戶名稱旁的核取方塊。
4. 完成後，選擇儲存。

#### AWS CLI

若要更新您的預設稽核擁有者 AWS CLI

執行 [update-settings](#) 命令，並使用 `--default-process-owners` 參數來指定稽核擁有者。

在下列範例中，將 `#####` 取代為您自己的資訊。請注意，`roleType` 只能是 `PROCESS_OWNER`。

```
aws auditmanager update-settings --default-process-owners
roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

## Audit Manager API

使用 API 更新您的預設稽核擁有者

呼叫 [UpdateSettings](#) 作業並使用 [defaultProcessOwners](#) 參數來指定預設稽核擁有者。請注意，roleType 只能是 PROCESS\_OWNER。

## 其他資源

- 如需稽核擁有者的詳細資訊，請參閱本指南概念與術語區段中的 [稽核擁有者](#)。

## 設定您的預設評估報告目標

當您產生評估報告時，Audit Manager 會將報告發佈到您選擇的 S3 儲存貯體。此 S3 儲存貯體稱為 [assessment report destination](#)。您可以選擇 Audit Manager 將評估報告存放在其中的 S3 儲存貯體。

## 必要條件

### 評估報告目的地的組態提示

為確保成功產生評估報告，我們建議您針對評估報告目標使用下列設定。

#### 相同區域儲存貯體

我們建議您使用與您的評估處於相同 AWS 區域的 S3 儲存貯體。當您使用相同區域儲存貯體和評估時，您的評估報告最多可包含 22,000 個證據項目。相反地，當您使用跨區域儲存貯體和評估時，只能包含 3,500 個證據項目。

#### AWS 區域

您 AWS 區域的客戶受管金鑰 (如果提供的話) 必須與評估區域和評估報告目標 S3 儲存貯體相符。如需如何變更 KMS 金鑰的指示，請參閱 [設定您的資料加密設定](#)。如需支援的 Audit Manager 區域清單，請參閱 Amazon Web Services 一般參考中的 [AWS Audit Manager 端點和配額](#)。

## S3 儲存貯體加密

如果您的評估報告目的地具有需要進行 [SSE-KMS](#) 伺服器端加密 (SSE) 的儲存貯體政策，則該儲存貯體政策中使用的 KMS 金鑰必須與您在 Audit Manager 資料加密設定中設定的 KMS 金鑰相符。如果您未在 Audit Manager 設定中設定 KMS 金鑰，且您的評估報告目的地儲存貯體政策需要 SSE，請確定儲存貯體政策允許 [SSE-S3](#)。如需如何設定用於資料加密之 KMS 金鑰的指示，請參閱[設定您的資料加密設定](#)。

### 跨帳戶 S3 儲存貯體

Audit Manager 主控台不支援將跨帳戶 S3 儲存貯體用作評估報告目的地。您可以使用 AWS CLI 或其中一個 AWS SDK 來指定跨帳戶儲存貯體做為評估報告目的地，但為了簡單起見，我們建議您不要這麼做。如果您選擇將跨帳戶 S3 儲存貯體用作評估報告目的地，請考慮以下幾點。

- 根據預設，S3 物件 (例如評估報告) 由上 AWS 帳戶 傳物件所擁有。您可以使用 [S3 物件擁有權](#) 設定更改該預設行為，以便由具有 bucket-owner-full-control 標準存取控制清單 (ACL) 的帳戶寫入的任何新物件自動為儲存貯體擁有者所有。

我們雖不要求，但建議您對跨帳戶儲存貯體設定進行下列變更。進行這些變更可確保儲存貯體擁有者完全控制您發佈至其儲存貯體的評估報告。

- [將 S3 儲存貯體的物件擁有權](#) 設定為首選儲存貯體擁有者，而非預設物件寫入器
- [新增儲存貯體政策](#) 以確保上傳至該儲存貯體的物件具有 bucket-owner-full-control ACL
- 如需允許 Audit Manager 在跨帳戶 S3 儲存貯體中發佈報告，您必須將下列 S3 儲存貯體政策新增至評估報告目的地。以您自己的資訊取代 #####。此政策中的 Principal 元素是擁有評估並建立評估報告的使用者或角色。Resource 指定發佈報告的跨帳戶 S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow cross account assessment report publishing",
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
      },
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
```

```
        "s3:PutObjectAcl",
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
    ]
}
]
```

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來更新此設定。

### Audit Manager console

在 Audit Manager 主控台上更新預設評估報告目標

1. 從評估設定索引標籤，前往評估報告目的地區段。
2. 若要使用現有的 S3 儲存貯體，請從下拉式功能表中選取儲存貯體名稱。
3. 若要建立新的 S3 儲存貯體，請選擇 [建立新儲存貯體]。
4. 完成後，選擇儲存。

### AWS CLI

若要更新您的預設評估報告目標 AWS CLI

執行 [update-settings](#) 命令，並使用 `--default-assessment-reports-destination` 參數來指定 S3 儲存貯體。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager update-settings --default-assessment-reports-destination
destinationType=S3,destination=s3://DOC-EXAMPLE-DESTINATION-BUCKET
```

### Audit Manager API

使用 API 更新預設評估報告目標

呼叫 [UpdateSettings](#) 作業，並使用 [defaultAssessmentReports目的地](#) 參數來指定 S3 儲存貯體。

## 其他資源

- [建立值區](#)
- [評估報告](#)

## 設定 Audit Manager 通知

您可以設定 Audit Manager，將通知傳送至您選擇的 Amazon SNS 主題。如果您已訂閱該 SNS 主題，則每當您登入 Audit Manager 時，都會直接收到通知。

請按照本頁的步驟進行操作，瞭解如何根據您的偏好檢視和更新通知設定。您可以使用標準 SNS 主題或 FIFO (first-in-first-out) SNS 主題。雖然 Audit Manager 支援傳送通知至 FIFO 主題，但無法保證郵件的傳送順序。

## 必要條件

如果您想要使用您不擁有的 Amazon SNS 主題，則必須為此設定 AWS Identity and Access Management (IAM) 政策。具體而言，您必須將其設定為允許從 Amazon Resource Name (ARN) 發佈至主題。如需您可以使用的範例原則，請參閱 [範例 1 \(SNS 主題的許可\)](#)。

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來更新此設定。

### Audit Manager console

在 Audit Manager 主控台上更新通知設定

1. 從評估設定索引標籤，前往通知區段。
2. 如需使用現有的 SNS 主題，請從下拉式選單選擇主題名稱。
3. 如需建立新的 SNS 主題，請選擇新清單。
4. 完成後，選擇儲存。

## AWS CLI

若要更新您的通知設定 AWS CLI

執行 [update-settings](#) 命令，並使用 `--sns-topic` 參數來指定 S3 主題。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-  
assessment-topic
```

## Audit Manager API

使用 API 更新通知設定

呼叫 [UpdateSettings](#) 作業，並使用 `snsTopic` 參數來指定 SNS 主題。

## 其他資源

- 如需有關如何建立 Amazon SNS 主題的資訊，請參閱 Amazon SNS 使用者指南中的 [建立 Amazon SNS 主題](#)。
- 如需可用來允許 Audit Manager 傳送通知給 Amazon SNS 主題的範例政策，請參閱 [範例 1 \(SNS 主題的許可\)](#)
- 如需深入了解在 Audit Manager 中調用通知的動作清單，請參閱 [通知 AWS Audit Manager](#)。
- 如需 Audit Manager 中通知問題的解決方案，請參閱 [通知問題疑難排解](#)。

## 啟用證據搜尋工具

您可以在 Audit Manager 中啟用證據搜尋器功能，以便在您的 AWS 帳戶。如果您是稽核管理員的委派系統管理員，您可以搜尋組織中所有成員帳戶的證據。

請按照以下步驟學習如何啟用證據查找器。請密切注意先決條件，因為您需要特定權限才能在 CloudTrail Lake 中建立和管理此功能的事件資料存放區。



## 必要條件

### 啟用證據搜尋工具所需的許可

若要啟用證據搜尋工具，您需要在 CloudTrail Lake 中建立和管理事件資料存放區的權限。若要使用此功能，您需要執行 CloudTrail Lake 查詢的權限。如需您可以使用的權限原則範例，請參閱[範例 4 \(啟用證據搜尋工具的許可\)](#)。

如果您需要權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 系統管理員，則可以複製所需的權限聲明，並[將其附加到 IAM 政策](#)。

## 程序

### 請求啟用證據搜尋工具

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來完成此工作。

#### Note

您必須在每個要搜索證據的 AWS 區域 位置啟用證據查找器。

### Audit Manager console

要求在 Audit Manager 主控台上啟用證據搜尋工具

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 從證據搜尋工具設定索引標籤，前往證據搜尋工具區段。
3. 選擇 [必要的權限原則]，然後選取 [檢視 CloudTrail 湖泊權限]，以檢視必要的證據尋找 如果您尚未獲得這些許可，您可以複製此政策聲明並[將其附加到 IAM 政策](#)。
4. 選擇 啟用。
5. 在快顯視窗中，選擇請求啟用。

### AWS CLI

要求啟用證據查找器 AWS CLI

使用 `--evidence-finder-enabled` 參數執行 [update-settings](#) 命令。

```
aws auditmanager update-settings --evidence-finder-enabled
```

## Audit Manager API

使用 API 要求啟用證據搜尋工具

呼叫 [UpdateSettings](#) 作業並使用 [evidenceFinderEnabled](#) 參數。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 後續步驟

請求啟用證據搜尋工具後，您可以查看要求的狀態。如需說明，請參閱 [確認證據搜尋器的狀態](#)。

## 其他資源

- [證據搜尋工具](#)
- [證據搜尋工具問題疑難排解](#)

## 確認證據搜尋器的狀態

提交啟用證據搜尋器的請求後，啟用此功能並建立事件資料存放區最多需要 10 分鐘。建立事件資料存放區後，所有新證據都會擷取至事件資料存放區。

啟用證據搜尋工具並建立事件資料存放區後，我們還會使用您過去兩年內的證據回填新建立的事件資料存放區。此程序會自動執行，最多持續 7 天。

請按照此頁面上的步驟檢查並了解啟用證據查找器的請求狀態。

## 必要條件

確保按照以下步驟啟用證據查找器。如需說明，請參閱 [啟用證據搜尋工具](#)。

## 程序

您可以使用 Audit Manager 主控台、AWS CLI、或 Audit Manager API 來檢查證據搜尋工具的目前狀態。

## Audit Manager console

在 Audit Manager 主控台上查看證據搜尋工具的目前狀態

1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 在左側的導覽窗格中，選擇設定。
3. 在 啟用證據搜尋工具 — 選用項下，檢閱目前的狀態。

每個狀態的定義如下：

狀態	描述
未啟用證據搜尋工具	您尚未成功啟用證據查找器。
您已要求啟用證據搜尋器	您的請求正在等待建立的事件資料存放區。
已啟用證據搜尋工具	已建立事件資料倉庫。您現在可以使用證據搜尋工具。  根據您擁有的證據量，使用您過去的證據資料回填新的事件資料存放區最多需要七天時間。藍色資訊窗格表示資料回填正在進行中。在此期間，隨時開始探索證據搜尋工具。但是，請記住，在回填完成之前，部分資料不可用。
您已要求停用證據搜尋器	您的請求正在等待刪除的事件資料存放區。
證據查找器已被禁用	證據搜尋工具已永久停用，且事件資料儲存區已刪除。

## AWS CLI

要查看證據查找器的當前狀態 AWS CLI

執行 [get-settings](#) 命令，`--attribute` 參數設置為 `EVIDENCE_FINDER_ENABLEMENT`。

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

其會傳回下列資訊。

```
enablementStatus
```

此屬性顯示證據搜尋工具的目前狀態。

- `ENABLE_IN_PROGRESS` — 您請求啟用證據搜尋工具。目前正在建立事件資料存放區以支援證據搜尋工具的查詢。
- `ENABLED` — 已建立事件資料存放區，並啟用證據搜尋工具。我們建議您等待七天，直到事件資料存放區回填您過去的證據資料。您可以在此期間使用證據搜尋工具，但在回填完成之前，部分資料不可用。
- `DISABLE_IN_PROGRESS` — 您請求停用證據搜尋工具，並且您的請求需待事件資料存放區刪除方可通過。
- `DISABLED` — 您永久停用證據搜尋工具，並刪除事件資料存放區。在此之後，您將無法重新啟用證據搜尋工具。

### backfillStatus

此屬性顯示證據資料回填的目前狀態。

- `NOT_STARTED` — 回填尚未開始。
- `IN_PROGRESS` — 回填正在進行中。最多需要七天的時間完成，具體取決於證據資料的數量。
- `COMPLETED` — 回填已完成。現在，您可以查詢既往所有證據。

## Audit Manager API

使用 API 查看證據查找器的當前狀態

在將 `attribute` 參數設定為 `EVIDENCE_FINDER_ENABLEMENT` 的情況下呼叫作業 `GetSettings`。其會傳回下列資訊。

### enablementStatus

此屬性顯示證據搜尋工具的目前狀態。

- `ENABLE_IN_PROGRESS` — 您請求啟用證據搜尋工具。目前正在建立事件資料存放區以支援證據搜尋工具的查詢。
- `ENABLED` — 已建立事件資料存放區，並已啟用證據搜尋工具。我們建議您等待七天，直到事件資料存放區回填您過去的證據資料。您可以在此期間使用證據搜尋工具，但在回填完成之前，部分資料不可用。
- `DISABLE_IN_PROGRESS` — 您已請求停用證據搜尋工具 — 您的請求需待事件資料存放區刪除方可通過。

- **DISABLED** — 您永久停用證據搜尋工具，並刪除事件資料存放區。在此之後，您將無法重新啟用證據搜尋工具。

## backfillStatus

此屬性顯示證據資料回填的目前狀態。

- **NOT\_STARTED** 意味著回填尚未開始。
- **IN\_PROGRESS** 表示回填正在進行中。最多需要七天的時間完成，具體取決於證據資料的數量。
- **COMPLETED** 表示回填已完成。現在，您可以查詢既往所有證據。

如需詳細資訊，請參閱 Audit Manager API 參考[evidenceFinderEnablement](#)中的。

## 後續步驟

成功啟用證據查找器後，您可以開始使用該功能。我們建議您等待七天，直到事件資料存放區回填您過去的證據資料。您可以在此期間使用證據查找器，但是在回填完成之前，並非所有數據都可以使用。

要開始使用證據查找器，請參閱[尋找證據, 在, 證據, 發現者](#)。

## 其他資源

- [證據搜尋工具問題疑難排解](#)

## 停用證據搜尋工具

如果您不想再使用證據搜尋器，您可以隨時停用此功能。

請按照以下步驟了解如何禁用證據查找器。請密切注意先決條件，因為您需要特定的權限才能刪除啟用證據查找器時建立的 CloudTrail Lake 中的事件資料存放區。

## 必要條件

### 停用證據搜尋工具所需的許可

若要停用證據搜尋工具，您需要刪除 CloudTrail Lake 中事件資料存放區的權限。如需您可以使用的範例政策，請參閱[停用證據搜尋工具的許可](#)。

如果您需要權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 管理員，則可以[將所需的許可聲明附加到 IAM 政策](#)。

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來完成此工作。

### Warning

停用證據搜尋工具會刪除 Audit Manager 建立的 CloudTrail Lake 事件資料存放區。因此，您無法重新啟用該功能。如需在停用證據搜尋工具後重新使用證據搜尋工具，您必須[停用 AWS Audit Manager](#)，然後完全[重新啟用](#)該服務。

### Audit Manager console

若要在 Audit Manager 主控台上停用證據尋找器

1. 在 Audit Manager 設定頁面的證據搜尋工具區段中，選擇停用。
2. 在出現的快顯視窗中，輸入 **Yes** 確認您的決定。
3. 選擇請求停用。

### AWS CLI

若要停用中的證據搜尋工具 AWS CLI

使用 `--no-evidence-finder-enabled` 參數執行 [update-settings](#) 命令。

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

### Audit Manager API

若要使用 API 停用證據搜尋工具

呼叫 [UpdateSettings](#) 作業並使用 [evidenceFinderEnabled](#) 參數。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用此操作和參數的資訊。

## 其他資源

- [證據搜尋工具問題疑難排解](#)

## 設定證據搜尋器的預設匯出目的地

當您在證據搜尋工具中執行查詢時，您可以將搜尋結果匯出為逗號分隔值 (CSV) 檔案。使用此設定可選擇 Audit Manager 儲存匯出檔案的預設 S3 儲存貯體。

### 必要條件

您的 S3 儲存貯體必須具有必要的許可政策，才能 CloudTrail 將匯出檔案寫入該儲存貯體。更具體地說，值區政策必須包含 `s3:PutObject` 動作和值區 ARN，並將其列 CloudTrail 為服務主體。

- 如需您可以使用的權限原則範例，請參閱[範例 3 \(匯出目的地許可\)](#)。
- 如需將此政策附加到 S3 儲存貯體的指示，請參閱[使用 Amazon S3 主控台新增儲存貯體政策](#)。
- 如需更多提示，請參閱[匯出目的地的組態提示](#)。

### 匯出目的地的組態提示。

為確保檔案成功匯出，建議您驗證匯出目的地的下列組態。

#### AWS 區域

您 AWS 區域的客戶管理金鑰 (如果您提供的話) 必須符合您評估的區域。關於如何變更 KMS 金鑰的說明，請參閱 [Audit Manager 資料加密設定](#)。

#### 跨帳戶 S3 儲存貯體

Audit Manager 主控台不支援將跨帳戶 S3 儲存貯體用作匯出目的地。您可以使用 AWS CLI 或其中一個 AWS SDK 指定跨帳戶儲存貯體，但為了簡單起見，我們建議您不要這麼做。如果您選擇將跨帳戶 S3 儲存貯體用作匯出目的地，請考慮以下幾點。

- 根據預設，S3 物件 (例如 CSV 匯出) 由上傳物件所擁有。AWS 帳戶 您可以使用 [S3 物件擁有權](#) 設定更改該預設行為，以便由具有 `bucket-owner-full-control` 標準存取控制清單 (ACL) 的帳戶寫入的任何新物件自動為儲存貯體擁有者所有。

我們雖不要求，但建議您對跨帳戶儲存貯體設定進行下列變更。進行這些變更可確保儲存貯體擁有者完全控制您發佈至其儲存貯體的匯出檔案。

- 將 [S3 儲存貯體的物件擁有權](#) 設定為首選儲存貯體擁有者，而非預設物件寫入器
- [新增儲存貯體政策](#) 以確保上傳至該儲存貯體的物件具有 bucket-owner-full-control ACL
- 如需允許 Audit Manager 將檔案匯出至跨帳戶 S3 儲存貯體，您必須將下列 S3 儲存貯體政策新增至匯出目的地儲存貯體。以您自己的資訊取代 #####。此政策中的 Principal 元素是擁有評估和匯出檔案的使用者或角色。Resource 指定匯出檔案的跨帳戶 S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow cross account file exports",
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
      },
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
      ]
    }
  ]
}
```

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或稽 Audit Manager API 來更新此設定。



## Audit Manager console

在 Audit Manager 主控台上更新匯出目的地設定

1. 從證據搜尋工具設定索引標籤，前往匯出目的地區段。
2. 請選擇下列其中一個選項：
  - 如需移除目前的 S3 儲存貯體，請選擇移除清除您的設定。
  - 請繼續執行步驟 3，進行預設 S3 儲存貯體的首次儲存。
3. 指定您要儲存匯出檔案的 S3 儲存貯體。
  - 選擇瀏覽 S3，從儲存貯體清單中進行選擇。
  - 或者，您也可以使用以下格式輸入儲存貯體 URI：**s3://bucketname/prefix**

### Tip

為確保目的地儲存貯體有序組織，您可以為 CSV 匯出建立選用資料夾。若要這麼做，請在資源 URI 方塊中的值加上斜線 (/) 和字首 (例如，/**evidenceFinderCSVExports**)。然後，Audit Manager 會在將 CSV 檔案新增至儲存貯體時包含此字首，而 Amazon S3 會產生字首指定的路徑。如需在 Amazon S3 中首碼的詳細資訊，請參閱在 Amazon 簡易儲存服務使用者指南中的[在 Amazon S3 主控台編組物件](#)。

4. 完成後，選擇儲存。

如需有關建立 S3 儲存貯體的說明，請參閱 Amazon S3 使用者指南中的[建立儲存貯體](#)。

## AWS CLI

若要更新您的匯出目的地設定 AWS CLI

執行 [update-settings](#) 命令，並使用 `--default-export-destination` 參數來指定 S3 儲存貯體。

在下列範例中，將#####取代為您自己的資訊。

```
aws auditmanager update-settings --default-export-destination
destinationType=S3,destination=DOC-EXAMPLE-DESTINATION-BUCKET
```

如需有關如何建立 S3 儲存貯體的說明，請參閱 AWS CLI 命令參考中的 [create-bucket](#)。

## Audit Manager API

使用 API 更新匯出目的地設定

呼叫作 [UpdateSettings](#) 業並使用 [defaultExportDestination](#) 參數來指定 S3 儲存貯體。

如需有關如何建立 S3 儲存貯體的指示，請參閱 Amazon S3 API 參考 [CreateBucket](#) 中的。

# 通知 AWS Audit Manager

AWS Audit Manager 可以通過 [Amazon 簡單通知服務 \(亞馬遜 SNS\)](#) 通知您有關用戶操作的信息。

發生下列其中一個動作時，Audit Manager 會傳送通知：

- 稽核擁有者委派控制集以供檢閱
- 委派人員將已檢閱的控制集交回稽核擁有者。
- 稽核擁有者完成控制集的檢閱。

## 其他資源

- 若要在 Audit Manager 中配置通知，請參閱[設定 Audit Manager 通知](#)。
- 若要尋找常見問題和問題的解答，請參閱[通知問題疑難排解](#)本指南的「疑難排解」一節。

# 疑難排解常見問題 AWS Audit Manager

使用時 AWS Audit Manager，您可能會遇到某些需要疑難排解的問題或挑戰。無論您是面臨設定評估、收集證據或服務的任何其他方面的挑戰，您都可以使用本疑難排解指南尋找我們的建議，協助您快速有效地解決常見問題。

我們鼓勵您查看下面的主題列表，找到最符合您案例的主題，然後按照提供的指引重新回到正軌。透過遵循提供的疑難排解步驟，您可以獨立解決問題，並繼續利用 Audit Manager 的完整功能。不過，如果此處未涵蓋您的具體問題，或是您在遵循建議的步驟後仍無法解決問題，我們建議您聯絡以取得 [AWS Support](#) 進一步協助。

## 主題

- [疑難排解評估和證據收集問題](#)
- [評估報告問題疑難排解](#)
- [控制項和控制集問題疑難排解](#)
- [儀表板問題疑難排解](#)
- [委派系統管理員與 AWS Organizations 相關問題疑難排解](#)
- [證據搜尋工具問題疑難排解](#)
- [疑難排解架構問](#)
- [通知問題疑難排解](#)
- [權限和存取問題疑難排解](#)

## 疑難排解評估和證據收集問題

請參考此頁面提供的資訊來解決 Audit Manager 中的常見評估和證據收集問題。

### 證據收集問題

- [我建立了一個評估，但還看不到任何證據](#)
- [我的評估不會從中收集合規性檢查證據 AWS Security Hub](#)
- [我的評估不會從中收集合規性檢查證據 AWS Config](#)
- [我的評估不會從 AWS CloudTrail 中收集使用者活動證據](#)
- [我的評估不會收集 AWS API 呼叫的組態資料證據](#)

- [常見的控制項不會收集任何自動化證據](#)
- [我的證據是以不同的時間間隔產生的，我不確定它的收集頻率](#)
- [我先停用再重新啟用 Audit Manager，導致我既有的評估不再進行收集證據](#)
- [在我的評估詳細資料頁面上，系統會提示我重新建立評估](#)
- [資料來源和證據來源有什麼區別？](#)

## 評估問題

- [我的評估建立失敗](#)
- [如果我從組織中移除範圍內的帳戶，會發生什麼情況？](#)
- [我看不到評估範圍內的服務](#)
- [我無法編輯評估範圍內的服務](#)
- [範圍內的服務和資料來源類型有什麼不同？](#)

## 我建立了一個評估，但還看不到任何證據

如果您看不到任何證據，可能是您在建立評估後尚未等待至少 24 小時，或是發生設定錯誤。

我們建議您檢查以下內容：

1. 確認自建立評估以來已過 24 小時。建立評估 24 小時後，即可使用自動證據。
2. 請確定您使用的 Audit Manager AWS 區域 與您預期看到的證據相同。AWS 服務
3. 如果您希望看到 AWS Config 和的合規性檢查證據 AWS Security Hub，請確定 AWS Config 和 Security Hub 主控台都顯示這些檢查的結果。AWS Config 和 Security Hub 結果應顯示在中使 AWS 區域 用 Audit Manager 的相同。

如果您仍然無法在評估中看到證據，並且不是由於上述任一問題所造成，請查看此頁面描述的其他潛在原因。

## 我的評估不會從中收集合規性檢查證據 AWS Security Hub

如果您沒有看到 AWS Security Hub 控制項的合規性檢查證據，這可能是由於下列其中一個問題所致。

### AWS Security Hub 中缺少配置

如果您在啟用 AWS Security Hub 時遺漏了某些設定步驟，可能會導致此問題。

若要修正此問題，請確定您已使用 Audit Manager 的必要設定啟用 Security Hub。如需說明，請參閱[啟用和設定 AWS Security Hub \(選擇性\)](#)。

您的 **ControlMappingSource** 中的一個 Security Hub 控制項名稱輸入不正確

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 Security Hub 控制項做為證據收集的[資料來源映射項目](#)。若要執行此操作，請輸入控制 ID 做為 [keywordValue](#)。

如果您沒有看到 Security Hub 控制項的合規檢查證據，可能是因為 keywordValue 在您的 ControlMappingSource 中輸入不正確。keywordValue 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識該規則。因此，您可能無法如預期收集該控制項的合規檢查證據。

若要修正此問題，請[更新自訂控制項](#)並修訂 keywordValue。Security Hub 關鍵字正確格式各不相同。為了獲得精確度，請參考的清單[支援的 Security Hub 控制項](#)。

**AuditManagerSecurityHubFindingsReceiver** Amazon EventBridge 規則丟失

啟用 Audit Manager 時，系統會在 Amazon 中自動建立並啟用名為 AuditManagerSecurityHubFindingsReceiver 的規則 EventBridge。此規則可讓 Audit Manager 收集 Security Hub 調查結果作為證據。

如果您使用 Security Hub 的 AWS 區域位置未列出並啟用此規則，則 Audit Manager 無法收集該區域的安全中心發現項目。

若要解決此問題，請前往[EventBridge 主控台](#)並確認您的 AWS 帳戶。

AuditManagerSecurityHubFindingsReceiver 如果規則不存在，建議您[停用 Audit Manager](#)，然後重新啟用服務。如果此動作無法解決問題，或停用 Audit Manager 不是可選選項，請[聯絡 AWS Support](#) 尋求協助。

由 Security Hub 建立的服務連結 AWS Config 規則

請記住，Audit Manager 不會從 [Security Hub 建立的服務連結 AWS Config 規則](#) 中收集證據。這是由 Security Hub 服務啟用和控制的特定受管理 AWS Config 規則類型。Security Hub 會在您的 AWS 環境中建立這些服務連結規則的執行個體，即使相同規則的其他執行個體已經存在也是如此。因此，為防止證據重複，Audit Manager 不支援從服務連結規則收集證據。

## 我在 Security Hub 中禁用了安全控制。Audit Manager 是否會收集該安全性控制的符合性檢查證據？

Audit Manager 不會收集已停用安全性控制的證據。

如果您在 Security Hub 中將安全性控制的狀態設定為 [\[停用\]](#)，則不會針對目前帳戶和 [區域] 中的該控制項執行安全性檢查。因此，Security Hub 中沒有可用的安全性發現項目，而且 Audit Manager 不會收集任何相關證據。

透過遵守您在 Security Hub 中設定的停用狀態，Audit Manager 可確保您的評估能夠準確反映與您環境相關的作用中安全性控制和發現項目，不包括您故意停用的任何控制項。

## 我 **Suppressed** 在安全中心中設置了發現的狀態。Audit Manager 是否會收集有關該發現項目的合規性檢查

Audit Manager 會針對隱藏搜尋結果的安全控制收集證據。

如果您在 Security Hub 中將尋找項目的工作流程狀態設定為 [隱藏](#)，這表示您已檢閱此尋找項目，且不相信需要執行任何動作。在 Audit Manager 中，這些隱藏的發現項目會作為證據收集，並附加至您的評估。證據詳細資料會顯示直接從 Security Hub SUPPRESSED 報告的評估狀態。

此方法可確保您的 Audit Manager 評估能夠準確呈現 Security Hub 的發現項目，同時還可讓您瞭解任何可能需要在稽核中進一步檢閱或考量的隱藏發現項目。

## 我的評估不會從中收集合規性檢查證據 AWS Config

如果您沒有看到規則的合 AWS Config 規性檢查證據，這可能是由於下列其中一個問題所致。


在您的 **ControlMappingSource** 中規則識別碼輸入錯誤

當您使用 Audit Manager API 建立自訂控制項時，您可以將 AWS Config 規則指定為證據收集的 [資料來源對應](#)。您指定的 [keywordValue](#) 取決於規則的類型。

如果您沒有看到規則的合 AWS Config 規性檢查證據，可能 keywordValue 是您的 ControlMappingSource。keywordValue 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識規則。因此，您可能無法如預期收集該規則的合規檢查證據。

若要修正此問題，請 [更新自訂控制項](#) 並修訂 keywordValue。

- 對於自訂規則，請確定 keywordValue 具有 Custom\_ 字首，後面接著自訂規則名稱。自訂規則名稱的格式可能會有所差異。為確保正確性，請造訪 [AWS Config 控制台](#) 以驗證您的自訂規則名稱。
- 對於受管規則，請確定 keywordValue 是 ALL\_CAPS\_WITH\_UNDERSCORES 中的規則識別碼。例如 CLOUDWATCH\_LOG\_GROUP\_ENCRYPTED。如需準確性，請參考 [支援的受管規則關鍵字清單](#)。

 Note

對於某些受管規則，規則識別碼與規則名稱不同。例如，[受限制 ssh](#) 的規則識別碼為 INCOMING\_SSH\_DISABLED。請務必使用規則識別碼，而不是規則名稱。若要尋找規則識別碼，請從 [受管規則清單](#) 中選擇規則，然後找到其識別碼值。

### 此規則為服務連結 AWS Config 規則

您可以使用 [受管規則](#) 和 [自訂規則](#) 作為證據收集的資料來源映射項目。但是，Audit Manager 不會從大多數 [服務連結規則](#) 中收集證據。

Audit Manager 只會從下列兩種類型收集證據的服務連結規則：

- 一致性套件中的服務連結規則
- 服務連結規則 AWS Organizations

Audit Manager 不會從其他服務連結規則收集證據，特別是任何具有 Amazon Resource Name (ARN) 且包含下列字首的規則：arn:aws:config:\*:\*:config-rule/aws-service-rule/...

Audit Manager 無法從大多數服務連結 AWS Config 規則中收集證據的原因，是為了防止評估中出現重複的證據。服務連結規則是一種特定類型的受管規則，可讓其他人在您 AWS 服務的帳戶中建立 AWS Config 規則。例如，[某些 Security Hub 控制項會使用 AWS Config 服務連結規則來執行安全性檢查](#)。對於每個使用服務連結 AWS Config 規則的 Security Hub 控制項，Security Hub 會在您的 AWS 環境中建立必要 AWS Config 規則的執行個體。即使您帳戶中已存在原始規則，也會發生這種情況。因此，為避免從同一規則中重複收集相同證據，Audit Manager 會忽略服務連結規則，而不會從中收集證據。

### AWS Config 未啟用

AWS Config 必須在您的 AWS 帳戶。以這種方式進行設定 AWS Config 之後，每次執行 AWS Config 規則評估時，Audit Manager 都會收集證據。請確定您已 AWS Config 在您的 AWS 帳戶。如需指示，請參閱 [啟用和設定 AWS Config](#)。



在您設定評估之前，AWS Config 規則評估了資源組態

如果您的 AWS Config 規則設定為評估特定資源的組態變更，您可能會在中看到評估 AWS Config 與 Audit Manager 中的證據不相符。如果規則評估發生在您在 Audit Manager 評估中設定控制項之前，就會發生這種情況。在此情況下，直到基礎資源再次變更狀態並觸發規則的重新評估，Audit Manager 才會產生證據。

因應措施是您可以導覽至 AWS Config 主控台當中的規則，然後[手動重新評估規則](#)。這將調用與該規則相關之所有資源的新評估。

## 我的評估不會從 AWS CloudTrail 中收集使用者活動證據

當您使用 Audit Manager API 建立自訂控制項時，您可以指定 CloudTrail 事件名稱作為證據收集的[資料來源對應](#)。若要執行此操作，請將事件名稱輸入為 `keywordValue`。

如果您沒有看到 CloudTrail 事件的使用者活動證據，可能 `keywordValue` 是您的 `ControlMappingSource`。 `keywordValue` 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識事件名稱。因此，您可能無法依預期收集該事件的使用者活動證據。

若要修正此問題，請[更新自訂控制項](#)並修訂 `keywordValue`。請確保事件寫入為 `serviceprefix_ActionName`。例如 `cloudtrail_StartLogging`。如需準確性，請參閱[服務授權參考](#)中的 AWS 服務 字首和動作名稱。

## 我的評估不會收集 AWS API 呼叫的組態資料證據

當您使用 Audit Manager API 建立自訂控制項時，您可以將 AWS API 呼叫指定為證據收集的[資料來源對應](#)。若要執行此作業，您可以將 API 呼叫輸入為 `keywordValue`。

如果您沒有看到 AWS API 呼叫的組態資料證據，可能 `keywordValue` 是您的 `ControlMappingSource`。 `keywordValue` 會區分大小寫。如果輸入不正確，Audit Manager 可能無法辨識 API 呼叫。因此，您可能無法按預期收集該 API 呼叫的組態資料證據。

若要修正此問題，請[更新自訂控制項](#)並修訂 `keywordValue`。請確保 API 呼叫寫入為 `serviceprefix_ActionName`。例如 `iam_ListGroups`。為了獲得精確度，請參考的清單[AWS 支援的 API 呼叫 AWS Audit Manager](#)。

## 常見的控制項不會收集任何自動化證據

檢閱通用控制項時，您可能看到下列訊息：此通用控制項不會從核心控制項收集自動證據。

這表示目前沒有任何 AWS 受管理的證據來源可以支援此通用控制項。因此，[證據來源] 索引標籤是空的，且不會顯示核心控制項。

當通用控制項未收集自動化證據時，就稱為手動通用控制項。手動通用控制項通常需要提供實體記錄和簽章，或者關於 AWS 環境外發生的事件的事實資料。因此，通常沒有 AWS 資料來源可以產生支援控制項需求的證據。

如果通用控制項是手動的，您仍然可以將其用作自訂控制項的證據來源。唯一的區別是，共同的控制不會自動收集任何證據。相反，您需要手動上傳自己的證據以支持共同控制的要求。

若要將證據新增至手動共用控制

#### 1. 建立自訂控制項

- 依照下列步驟[建立](#)或[編輯](#)自訂控制項。
- 當您在步驟 2 中指定證據來源時，請選擇手動通用控制項作為證據來源。

#### 2. 建立自訂架構

- 依照下列步驟[建立](#)或[編輯](#)自訂架構。
- 當您在步驟 2 中指定控制項集時，請加入新的自訂控制項。

#### 3. 建立評估

- 按照以下步驟從您的自定義框架[創建評估](#)。
- 在這一點上，手動共同控制現在是主動評估控制中的證據來源。

#### 4. 上傳手動證據

- 請按照以下步驟將[手動證據添加](#)到評估中的控制項中。

#### Note

隨著 future 可用的 AWS 資料來源越多，可 AWS 能會更新通用控制項，將核心控制項納入為證據來源。在這種情況下，如果通用控制項是一或多個作用中評估控制項中的證據來源，您將自動從這些更新中獲益。您無需進一步設置，您將開始收集支持共同控制的自動證據。

## 我的證據是以不同的時間間隔產生的，我不確定它的收集頻率

Audit Manager 評估中的控制項會映射至各種資料來源。每個資料來源都有不同的證據收集頻率。因此，對於收集證據的頻率沒有 one-size-fits-all 答案。某些資料來源會評估合規性，而其他資料來源僅擷取資源狀態和變更資料，不涉及合規性判斷。

以下是不同資料來源類型的摘要，以及收集證據的頻率。

Data source type (資料來源類型)	說明	證據收集頻率	此控制項在評估中處於作用中狀態時
AWS CloudTrail	追蹤特定使用者活動。	持續性	Audit Manager 會根據您選擇的關鍵字篩選 CloudTrail 記錄。已處理的日誌檔會匯入為使用者活動證據。
AWS Security Hub	透過 Security Hub 報告調查結果，擷取資源安全狀況的快照。	根據 Security Hub 檢查的排程計劃 (通常約每 12 小時進行一次)	Audit Manager 會直接從 Security Hub 擷取安全性調查結果。調查結果會匯入為合規檢查證據。
AWS Config	透過報告發現項目來擷取資源安全狀況的快照 AWS Config。	根據規則中定義的設定 AWS Config 定	Audit Manager 會直接從中擷取規則評估 AWS Config。評估結果會匯入為合規檢查證據。
AWS API 呼叫	透過指定的 API 呼叫，直接擷取資源組態的快照 AWS 服務。	每日、每週或每月	Audit Manager 會根據您的指定頻率進行 API 呼叫。系統會將回應匯入為組態資料證據。

無論證據收集頻率如何，只要評估處於活動狀態，系統都會自動收集新證據。如需詳細資訊，請參閱 [證據收集頻率](#)。

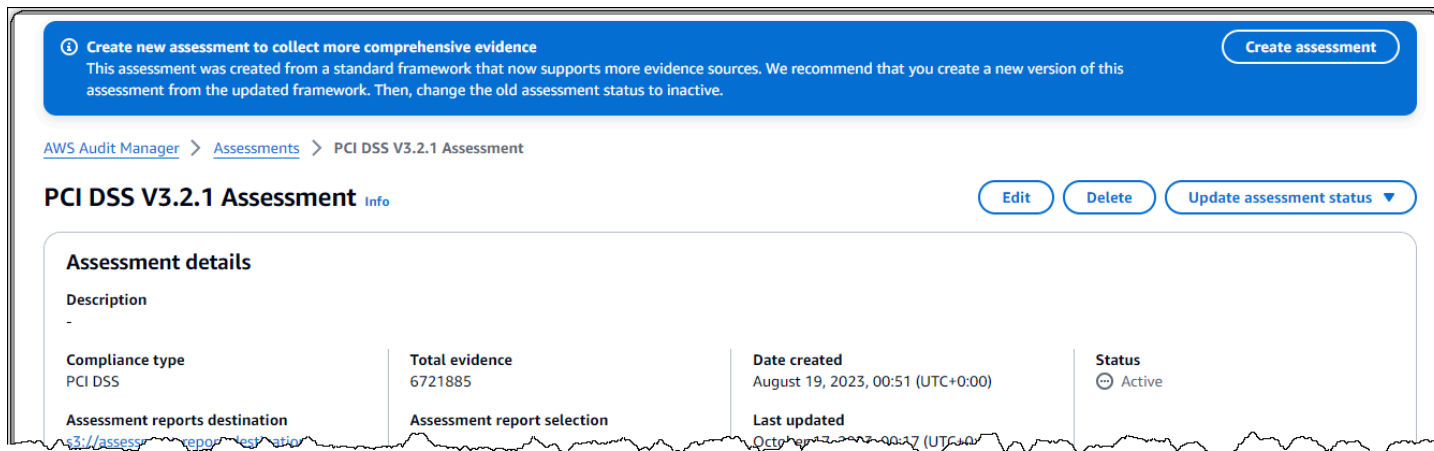
如需了解詳細資訊，請參閱 [自動化證據的支援資料來源類型](#) 和 [變更控制項收集證據的頻率](#)。

## 我先停用再重新啟用 Audit Manager，導致我既有的評估不再進行收集證據

當您停用 Audit Manager 並選擇不刪除資料時，您現有的評估會進入休眠狀態，並停止收集證據。這表示當您重新啟用 Audit Manager 時，您先前建立的評估仍可使用。但是，它們不會自動恢復收集證據。

如需重新開始收集既有評估的證據，請[編輯評估](#)並選擇儲存，而不進行任何變更。

## 在我的評估詳細資料頁面上，系統會提示我重新建立評估



如果您看到「建立新評估以收集更全面的證據」的訊息，表示「Audit Manager」現在會針對建立評估的來源提供標準架構的新定義。

在新的架構定義中，架構的所有標準控制項現在都可以從[AWS 受管理的來源](#)收集證據。這表示每當針對一般或核心控制項的基礎資料來源有更新時，Audit Manager 就會自動將相同的更新套用至所有相關的標準控制項。

若要從這些受 AWS 管理的來源中受益，我們[建議您從更新的架構建立新的評估](#)。執行此操作之後，您可以將舊的評估狀態變更為非作用中。此動作有助於確保您的新評估會收集來自 AWS 受管理來源的最準確、最全面的證據。如果您不採取任何行動，您的評估會繼續使用舊的架構和控制項定義來收集與之前完全相同的證據。

## 資料來源和證據來源有什麼區別？

證據來源決定從何處收集證據。這可以是個別資料來源，也可以是對應至核心控制項或共用控制項的預先定義資料來源群組。

資料來源是最精細的證據來源類型。資料來源包含下列詳細資訊，告知 Audit Manager 要從何處收集證據資料：

- [資料來源類型](#) (例如, AWS Config)
- [資料來源對映](#) (例如, 特定 AWS Config 規則, 例如s3-bucket-public-write-prohibited)

## 我的評估建立失敗

如果您的評估建立失敗, 可能是因為您在評估範圍中選取了太多 AWS 帳戶。如果您使用的是 AWS Organizations, Audit Manager 員在單一評估範圍內最多可支援 200 個成員帳戶。如果超過此數量, 評估建立可能會失敗。因應措施是, 您可以進行多次評估, 每次評估使用範圍內不同帳戶來執行。

## 如果我從組織中移除範圍內的帳戶, 會發生什麼情況?

當範圍內的帳戶從組織中移除時, Audit Manager 不會再為該帳戶收集證據。但是, 該帳戶仍會繼續顯示在您的評估中的 AWS 帳戶 索引標籤下。若要從範圍內的帳戶清單中移除該帳戶, 請[編輯評估](#)。已移除帳戶在編輯期間不再顯示於清單中, 您可以在不包含該帳戶的範圍內儲存您的變更。

## 我看不到評估範圍內的服務

如果您沒有看到此 AWS 服務索引標籤, 這表示範圍內的服務是由稽核管理員為您管理。當您建立新評估時, 稽核管理員會從該時間點開始為您管理範圍內的服務。

如果您有較舊的評估, 可能是您先前在評估中看到此標籤。但是, 當發生下列任一事件時, Audit Manager 會自動從您的評估中移除此標籤, 並接管範圍內的服務管理:

- 您可以編輯評估
- 您可以編輯評估中使用的其中一個自訂控制項

Audit Manager 會檢查您的評估控制項及其資料來源, 然後將此資訊對應至對應 AWS 服務的資訊, 藉此推斷範圍內的服務。如果您的評估基礎資料來源變更, 我們會根據需要自動更新範圍, 以反映正確的服務。這可確保您的評估收集有關您 AWS 環境中所有相關服務的準確而全面的證據。

## 我無法編輯評估範圍內的服務

[編輯評量 AWS Audit Manager](#) 工作流程不再具有「編輯」服務步驟。這是因為 Audit Manager 現在 AWS 服務 會管理您評估範圍內的哪些項目。

如果您有較舊的評估, 建立評估時, 可能是手動定義範圍內的服務。但是, 您無法繼續編輯這些服務。當發生下列任一事件時, Audit Manager 會自動接管評估範圍內的服務管理:

- 您可以編輯評估
- 您可以編輯評估中使用的其中一個自訂控制項

Audit Manager 會檢查您的評估控制項及其資料來源，然後將此資訊對應至對應 AWS 服務的資訊，藉此推斷範圍內的服務。如果您的評估基礎資料來源變更，我們會根據需要自動更新範圍，以反映正確的服務。這可確保您的評估收集有關您 AWS 環境中所有相關服務的準確而全面的證據。

## 範圍內的服務和資料來源類型有什麼不同？

A [service in scope](#) 是包 AWS 服務 含在評估範圍內的。當一項服務在範圍內時，Audit Manager 會收集您使用該服務及其資源的相關證據。

### Note

Audit Manager AWS 服務 會管理您評估範圍內的哪些項目。如果您有較舊的評估，可能是您過去手動指定範圍內的服務。往後，您無法指定或編輯範圍內的服務。

[資料來源類型](#) 會指出從何處收集證據。如果您上傳自己的證據，則資料來源類型為手動。如果由 Audit Manager 收集證據，則資料來源可以是下列四種類型之一：

1. AWS Security Hub — 從 Security Hub 報告發現項目，擷取資源安全狀況的快照。
2. AWS Config — 透過報告發現項目來擷取資源安全狀況的快照 AWS Config。
3. AWS CloudTrail — 追蹤資源的特定使用者活動。
4. AWS API 呼叫 — 直接透過 API 呼叫特定資源設定擷取快照 AWS 服務。

這裡有兩個例子來說明範圍內的服務，以及資料來源類型之間的差異。

### 範例 1

假設您想收集名為 4.1.2 — 禁止對 S3 儲存貯體進行公開寫入存取的控制項證據。此控制項會檢查 S3 儲存貯體政策的存取層級。對於此控制項，Audit Manager 會使用特定 AWS Config 規則 ([s3-bucket-public-write-prohibited](#)) 來尋找 S3 儲存貯體的評估。在此範例中，下列情況成立：

- [service in scope](#) 是 Amazon S3
- 正在評估的 [資源](#) 是您的 S3 儲存貯體

- [資料來源類型](#)為 AWS Config
- [資料來源對映](#)是特定 AWS Config 規則 (s3-bucket-public-write-prohibited)

## 範例 2

假設您想收集名為 164.308(a)(5)(ii)(C) 的 HIPAA 控制項的證據。此控制項需要監控程序來偵測不適當的登入。針對此控制項，Audit Manager 會使用 CloudTrail 記錄檔來尋找所有 [AWS 管理主控台登入事件](#)。在此範例中，下列情況成立：

- 該 [service in scope](#) 是 IAM
- 正在評估的 [資源](#) 是您的使用者
- [資料來源類型](#) 為 CloudTrail
- [資料來源對映](#) 是特定 CloudTrail 事件 (ConsoleLogin)

## 評估報告問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的評估報告問題。

### 主題

- [我的評估報告無法產生](#)
- [我按照上面的檢查清單進行操作，但我的評估報告仍然無法生成](#)
- [當我嘗試生成報告時，出現存取被拒絕的錯誤](#)
- [我無法解壓縮評估報告](#)
- [當我在報告中選擇證據名稱時，系統沒有將我重導向到該證據的詳細資訊](#)
- [我的評估報告產生停留進行中狀態，我不確定這對我的計費有何影響](#)
- [其他資源](#)

## 我的評估報告無法產生

您的評估報告可能因為多種因素，未能成功產生。您可以透過檢查常見原因來對此問題進行故障排除。請使用下列清單來開始。

1. 檢查您的任何 AWS 區域 信息是否不匹配：
  - a. 您 AWS 區域 的客戶管理金鑰是否與您 AWS 區域 的評估相符？

如果您為 Audit Manager 資料加密提供了自己的 KMS 金鑰，則該金鑰必須與您的評估 AWS 區域相同。若要解決此問題，請將 KMS 金鑰變更為與評估位於相同區域的金鑰。如需如何變更 KMS 金鑰的指示，請參閱[設定您的資料加密設定](#)。

b. 您 AWS 區域的客戶受管金鑰是否與 S3 儲存貯體相符？AWS 區域

如果您為 Audit Manager 資料加密提供了自己的 KMS 金鑰，則該金鑰必須與您用 AWS 區域作評估報告目標的 S3 儲存貯體位於相同的 S3 儲存貯體中。為解決此問題，您可以變更 KMS 金鑰或 S3 儲存貯體，使它們與您的評估位於相同區域。如需如何變更 KMS 金鑰的指示，請參閱[設定您的資料加密設定](#)。如需如何變更 S3 儲存貯體的指示，請參閱[設定您的預設評估報告目標](#)。

2. 檢查您用作評估報告目的地的 S3 儲存貯體的權限：

a. 產生評估報告的 IAM 實體是否具有對 S3 儲存貯體所需的權限？

IAM 實體必須擁有 S3 儲存貯體的所需權限，才能在該儲存貯體中發佈報表。我們提供您可以使用的[範例政策](#)。

b. S3 儲存貯體是否有需要使用 [SSE-KMS](#) 的伺服器端加密 (SSE) 的儲存貯體政策？

如果是，則該儲存貯體原則中使用的 KMS 金鑰必須與 Audit Manager 資料加密設定中指定的 KMS 金鑰相符。如果您未在 Audit Manager 設定中設定 KMS 金鑰，且 S3 儲存貯體政策需要 SSE，請確定儲存貯體政策允許 [SSE-S3](#)。如需如何變更 KMS 金鑰的指示，請參閱[設定您的資料加密設定](#)。如需如何變更 S3 儲存貯體的指示，請參閱[設定您的預設評估報告目標](#)。

如果您仍然無法成功產生評估報告，請查看本頁上的下述問題。

## 我按照上面的檢查清單進行操作，但我的評估報告仍然無法生成

Audit Manager 會限制您可以新增至評估報告的證據數量。此限制取決於您 AWS 區域的評估、用作評估報告目標的 S3 儲存貯體區域，以及您的評估是否使用受管的客戶 AWS KMS key。

1. 相同區域報告的上限為 22,000 (S3 儲存貯體和評估都在同一個 AWS 區域的情況下)
2. 跨區域報告的上限為 3,500 (S3 儲存貯體和評估在不同 AWS 區域的情況下)
3. 如果評估使用客戶管理的 KMS 金鑰，則上限為 3,500

如果您嘗試產生包含多於此證據的報告，作業可能會失敗。

因應措施是，您可以產生多個評估報告，而不是一份較大的評估報告。透過這種方式，您可以將評估中的證據匯出到更易於管理的批次中。



## 當我嘗試生成報告時，出現存取被拒絕的錯誤

如果您的評估是由委派的系統管理員帳戶建立，並且 Audit Manager 設定中指定的 KMS 金鑰不屬於該帳戶，您將會收到 `access denied` 錯誤訊息。若要避免此錯誤，當您指定 Audit Manager 的委派系統管理員時，請確定委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。

如果您沒有用作評估報告目的地的 S3 儲存貯體的寫入權限，您也可能會收到 `access denied` 錯誤訊息。

若您收到 `access denied` 錯誤訊息，請確定您符合下列要求：

- 您在 Audit Manager 設定中的 KMS 金鑰將權限授予委派系統管理員。您可以依照 AWS Key Management Service 開發人員指南中，[允許其他帳戶中的使用者使用 KMS 金鑰](#) 中的指南進行設定。如需如何在 Audit Manager 中檢閱和變更加密設定的指示，請參閱[設定您的資料加密設定](#)。
- 您擁有一個權限策略，該策略可授予您對用作評估報告目的地的 S3 儲存貯體的寫入存取權限。更具體地說，您的許可政策包含一個 `s3:PutObject` 動作、指定 S3 儲存貯體的 ARN，並包含用於加密評估報告的 KMS 金鑰。如需您可以使用的範例原則，請參閱[範例 2 \(評估報表目的地許可\)](#)。

### Note

如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括您依據新評估所建立的任何評估報告。

這些變更不會套用至您在變更加密設定之前，已建立的現有評估。出了現有的評估報告之外，這還包括了您根據現有評估建立的新評估報告。現有的評估及其所有評估報告都將繼續使用舊有的 KMS 金鑰。如果產生評估報告的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

## 我無法解壓縮評估報告

如果您無法在 Windows 上解壓縮評估報告，Windows 檔案總管可能無法解壓縮，因為其檔案路徑有數個巢狀資料夾或長名稱。這是因為，在 Windows 檔案命名系統下，資料夾路徑、檔案名稱和副檔名不能超過 259 個字元。否則，會導致 `Destination Path Too Long` 錯誤。

為解決此問題，請嘗試將 zip 檔案移至其目前位置的上層資料夾。然後，您可以再次嘗試從那裡解壓縮它。或者，您也可以嘗試縮短 zip 檔案的名稱，或將其解壓縮到較短文件路徑的其他位置。

## 當我在報告中選擇證據名稱時，系統沒有將我重導向到該證據的詳細資訊

如果您在瀏覽器中操作評估報告，或使用作業系統上安裝的預設 PDF 閱讀器，可能會發生此問題。某些瀏覽器和系統預設的 PDF 閱讀器不允許開啟相對連結。這表示，雖然在評估報告摘要 PDF 中的超連結可能有效 (例如目錄中的超連結控制項名稱)，但當您嘗試從評估摘要 PDF 導覽至獨立的證據詳細資料 PDF 時，超連結將被忽略。

如果您遇到此問題，建議您使用專用的 PDF 閱讀器來閱覽您的評估報告。為了獲得可靠的使用體驗，我們建議您安裝並使用 Adobe Acrobat Reader，您可以在 [Adobe 官網](#) 下載該服務。其他 PDF 閱讀器也可以使用，但 Adobe Acrobat Reader 已被證明可以與 Audit Manager 評估報告穩定且可靠地運作。

## 我的評估報告產生停留進行中狀態，我不確定這對我的計費有何影響

產生評估報告不會影響計費。我們只會根據您的評估收集的證據向您收取費用。如需定價的詳細資訊，請參閱 [AWS Audit Manager 定價](#)。

## 其他資源

下列頁面提供從證據搜尋工具產生評估報告的疑難排解指南：

- [我無法從搜尋結果中產生多個評估報告](#)
- [我無法在搜尋結果中加入特定證據](#)
- [在評估報告中，並未包含所有來自證據搜尋工具的查找結果](#)
- [我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗](#)

## 控制項和控制集問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中控制項的常見問題。

### 一般問題

- [我在評估中看不到任何控制項或控制集](#)
- [我無法將手動證據上傳到控制項](#)
- [如果控制項顯示「可用更換」，這代表什麼意思？](#)

### AWS Config 整合問題

- [我需要多個 AWS Config 規則作為單個控件的數據源](#)

- [當我設定控制項資料來源時，無法使用自訂規則選項](#)
- [自訂規則選項可用，但下拉式清單中沒有顯示任何規則](#)
- [一些自訂規則可用，但我看不到我想要使用的規則](#)
- [我看不到要使用的受管規則](#)
- [我想共享一個自定義框架，但它具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？](#)
- [在 AWS Config 中更新自訂規則時會發生什麼情況？我需要在 Audit Manager 中採取任何動作嗎？](#)

## 我在評估中看不到任何控制項或控制集

簡而言之，若要檢視評估的控制項，您必須被指定為該評估的稽核擁有者。此外，您還需要必要的 IAM 權限，才能檢視和管理相關 Audit Manager 資源。

如果您需要存取評估中的控制項，請要求該評估的一位稽核擁有者將您指定為稽核擁有者。您可以在[建立](#)或[編輯](#)評估時指定稽核擁有者。

同樣請確保您具備管理評估的所需權限。我們建議稽核擁有者使用[AWSAuditManagerAdministratorAccess](#)策略。如果您需要 IAM 權限相關協助，請聯絡您的管理員或[AWS 支援人員](#)。有關如何將政策附加到 IAM 身分的更多資訊，請參閱 IAM 使用者指南中的[向使用者新增權限](#)和[新增及移除 IAM 身分權限](#)。

## 我無法將手動證據上傳到控制項

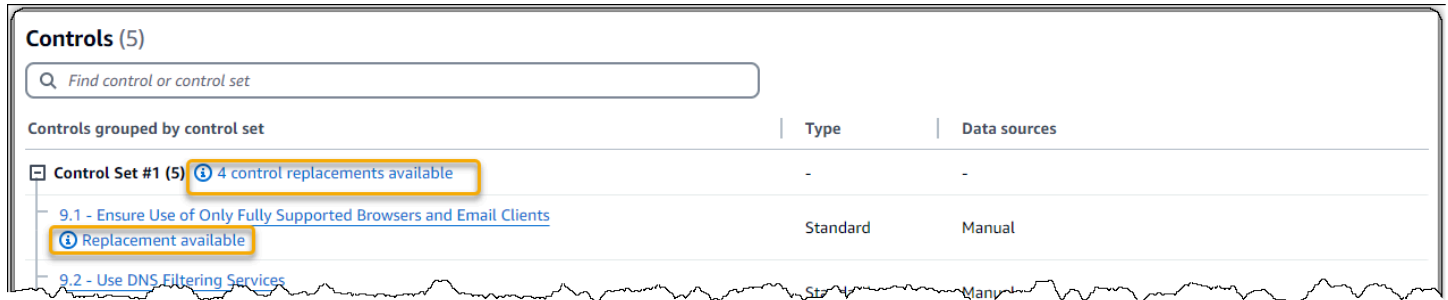
如果您無法手動將證據上傳至控制項，可能是因為控制項處於非作用中狀態。

若要將手動證據上傳至控制項，您必須先將控制項狀態變更為審核中或已審核。如需說明，請參閱[變更評估控制項的狀態](#) [AWS Audit Manager](#)。

### Important

每個控制項每天最多只 AWS 帳戶 能手動上傳 100 個證據檔案至控制項。超過這個每日配額，會導致該控制項的任何額外手動上傳失敗。如果您需要將大量手動證據上傳至單一控制項，請在數天內分批上傳證據。

## 如果控制項顯示「可用更換」，這代表什麼意思？



如果您看到此訊息，表示自訂架構中的一或多個標準控制項可使用更新的控制項定義。我們建議您取代這些控制項，以便您可以從 Audit Manager 現在提供的改良的證據來源中獲益。

如需如何繼續操作的指示，請參閱[在我的自定義框架詳細信息頁面上](#)，系統提示我重新創建自定義框架。

### 我需要使用多個 AWS Config 規則作為單個控件的數據源

您可以將受管規則和自訂規則的組合用於單一控制項。若要這麼做，請為控制項定義多個證據來源，然後為每個證據來源選取偏好的規則類型。您可以為單一自訂控制項定義多達 100 個客戶管理的資料來源。

### 當我設定控制項資料來源時，無法使用自訂規則選項

這表示您沒有檢視您的 AWS 帳戶 或組織的自訂規則的權限。更具體地說，您沒有在 Audit Manager 主控台中執行 [DescribeConfigRules](#) 作業的權限。

若要解決此問題，請聯絡您的 AWS 管理員以取得協助。如果您就是 AWS 管理員，可以透過 [管理您的 IAM 政策](#) 為使用者或群組提供權限。

### 自訂規則選項可用，但下拉式清單中沒有顯示任何規則

這表示您的 AWS 帳戶 或組織中沒有啟用和使用任何自訂規則。

如果您在中還沒有任何自訂規則 AWS Config，您可以建立規則。如需指示，請參閱 AWS Config 開發人員指南中的 [AWS Config 自訂規則](#)。

若您預期看到自訂規則，請參閱下述疑難排解項目。

### 一些自訂規則可用，但我看不到我想要使用的規則

如果您看不到預期查找的自訂規則，可能是下列問題之一所致。

## 您的帳戶已從規則中排除

您使用的委派系統管理員帳戶可能已從規則中排除。

您組織的管理帳戶 (或其中一個 AWS Config 委派管理員帳戶) 可以使用 AWS Command Line Interface (AWS CLI) 建立自訂組織規則。當進行此操作時，他們可以指定 [要排除的帳戶列表](#)，使這些帳戶不受該規則約束。如果您的帳戶在此清單中，則 Audit Manager 中無法使用該規則。

若要解決此問題，請聯絡您的 AWS Config 管理員以取得協助。如果您是 AWS Config 系統管理員，則可以執行 [put-organization-config-rule](#) 命令來更新排除帳戶的清單。

## 規則未在 AWS Config 中成功建立和啟用

也有可能未成功建立和啟用自訂規則。如果在 [建立規則時發生錯誤](#)，或未 [啟用](#) 該規則，則該規則不會顯示在 Audit Manager 的可用規則清單中。

如需協助您解決此問題，建議您聯絡 AWS Config 管理員。

## 此規則為受管規則

如果您在自訂規則的下拉式清單中找不到您要尋找的規則，則該規則可能是受管規則。

您可以使用 [AWS Config 主控台](#) 來驗證規則是否為受管規則。若要這麼做，請在左側導覽功能表中選擇規則，然後在表格中查找規則。如果規則是受管規則，類型欄會顯示 AWS 受管。

	Name	Remediation action	Type	Compliance
<input type="radio"/>	<a href="#">account-part-of-organizations</a>	Not set	AWS managed	<span style="color: green;">✔</span> Compliant

確認它是受管規則之後，請返回 Audit Manager 並選取受管規則作為規則類型。然後，在受管規則的下拉式清單中，尋找受管規則識別碼關鍵字。

AWS Config rule type [Info](#)

Select a rule type to view a list of the available rules.

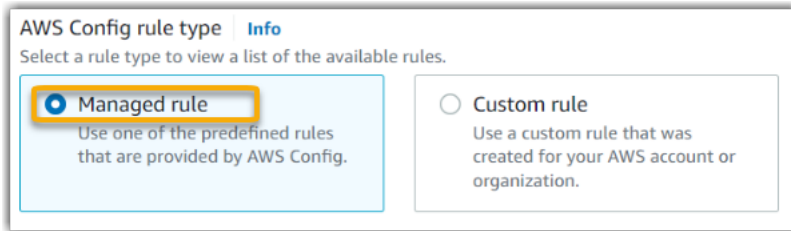
**Managed rule**  
Use one of the predefined rules that are provided by AWS Config.

**Custom rule**  
Use a custom rule that was created for your AWS account or organization.

**Managed rule**  
For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

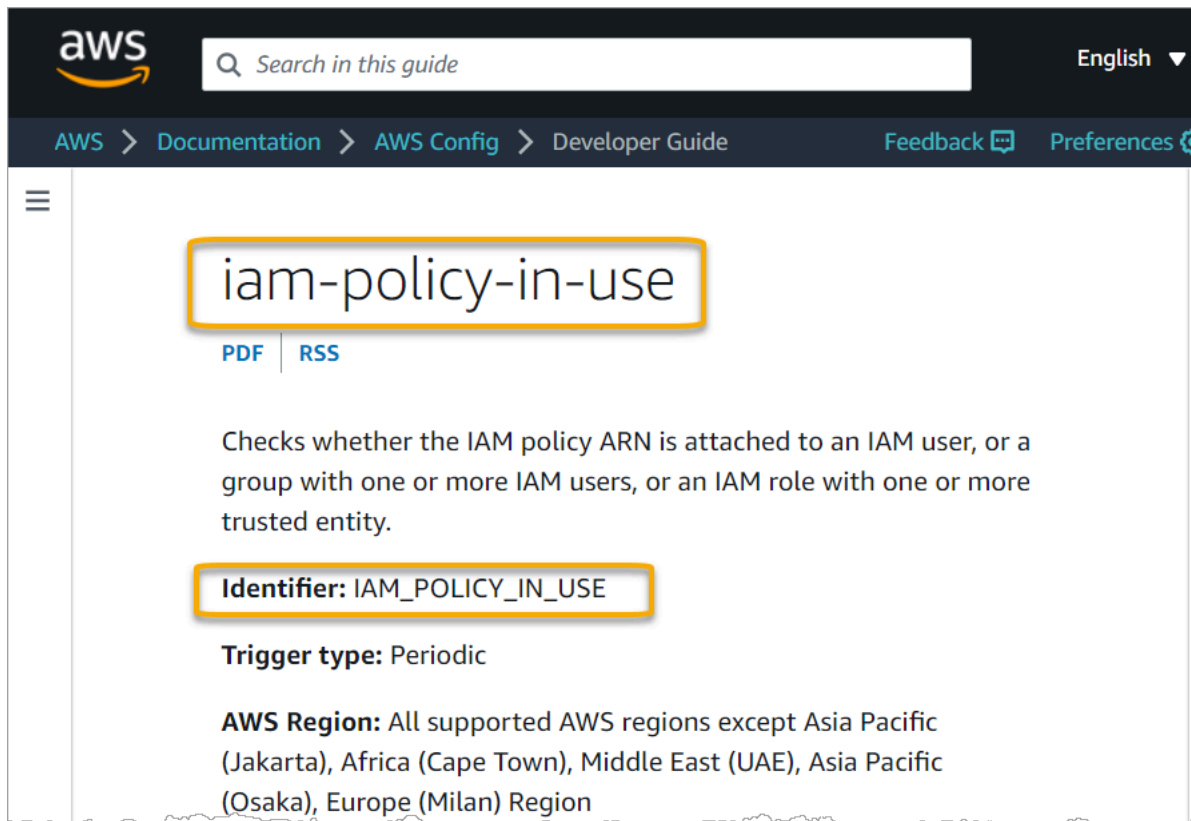
## 我看不到要使用的受管規則

在您從 Audit Manager 主控台的下拉式清單中選取規則之前，請確定已選取受管規則作為規則類型。

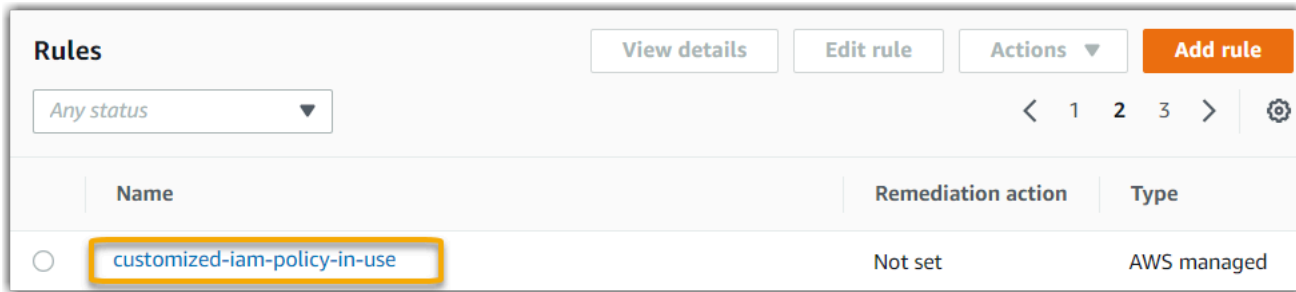


如果您仍然看不到預期尋找的受管規則，可能是您正在尋找規則名稱。相反地，您必須尋找規則識別碼。

如果您使用的是預設受管規則，其名稱和識別碼會類似。名稱以小寫字母表示，並使用破折號 (例如，iam-policy-in-use)。識別碼為大寫，並使用底線 (例如，IAM\_POLICY\_IN\_USE)。若要尋找預設受管規則的識別碼，請檢閱[支援的 AWS Config 受管規則關鍵字清單](#)，然後追蹤您要使用之規則的連結。這會帶您前往該受管規則的 AWS Config 文件集。從這裡，您可以看到名稱和識別碼。在 Audit Manager 下拉式清單中尋找識別碼關鍵字。



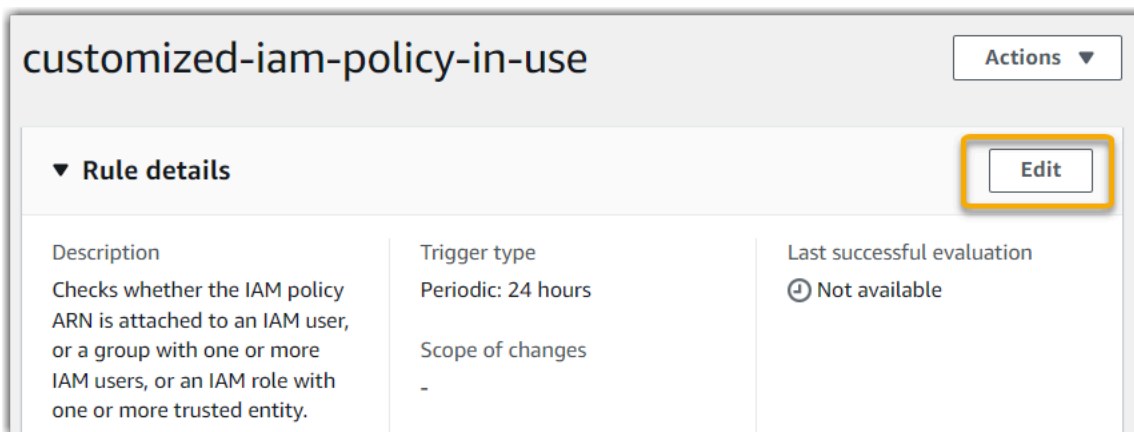
如果您使用自訂受管規則，可以使用主[AWS Config 控制台](#)尋找規則識別碼。舉例來說，假設您想要使用名為 `customized-iam-policy-in-use` 的受管規則。若要尋找此規則的識別碼，請移至 AWS Config 主控台，選擇左側導覽功能表中的 [規則]，然後選擇表格中的規則。



The screenshot shows the 'Rules' section of the AWS Config console. At the top, there are buttons for 'View details', 'Edit rule', 'Actions', and 'Add rule'. Below these is a filter dropdown set to 'Any status' and a pagination control showing pages 1, 2, and 3. A table lists the rules with columns for 'Name', 'Remediation action', and 'Type'. The rule 'customized-iam-policy-in-use' is highlighted with a yellow box. Its remediation action is 'Not set' and its type is 'AWS managed'.

Name	Remediation action	Type
customized-iam-policy-in-use	Not set	AWS managed

選擇編輯以開啟有關受管規則的詳細資料。



The screenshot shows the 'Rule details' page for the 'customized-iam-policy-in-use' rule. At the top right, there is an 'Actions' dropdown menu with an 'Edit' button highlighted in yellow. Below this, the 'Rule details' section is expanded, showing three columns of information: 'Description', 'Trigger type', and 'Last successful evaluation'. The 'Description' column contains text about checking IAM policy ARNs. The 'Trigger type' column shows 'Periodic: 24 hours' and 'Scope of changes' as '-'. The 'Last successful evaluation' column shows a clock icon and 'Not available'.

Description	Trigger type	Last successful evaluation
Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.	Periodic: 24 hours Scope of changes -	⌚ Not available

在詳細資訊一節下，您可以找到從 (IAM\_POLICY\_IN\_USE) 建立的受管規則的來源識別碼。

## Edit rule

### Details

**Name**  
A unique name for the rule. 128 characters max. No special characters or spaces.

customized-iam-policy-in-use

**Description**

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

**Managed rule name**

IAM\_POLICY\_IN\_USE

您現在可以返回 Audit Manager 主控台，並從下拉式清單中選取相同的識別碼關鍵字。

AWS Config rule type [Info](#)

Select a rule type to view a list of the available rules.

**Managed rule**  
Use one of the predefined rules that are provided by AWS Config.

**Custom rule**  
Use a custom rule that was created for your AWS account or organization.

**Managed rule**  
For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

IAM\_POLICY\_IN\_USE

我想共享一個自定義框架，但它具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？

是的，收件人可以收集這些控制的證據，但需要幾個步驟來實現這一目標。

若要讓 Audit Manager 使用 AWS Config 規則作為資料來源對應來收集證據，必須符合下列條件。同樣適用於受管理規則和自訂規則。

1. 規則必須存在於收件者的 AWS 環境中
2. 必須在收件者的 AWS 環境中啟用規則



請記住，您的帳戶中的自定義 AWS Config 規則可能不存在於收件人的 AWS 環境中。此外，當收件者接受共享要求時，Audit Manager 不會在其帳戶中重新建立您的任何自訂規則。若要讓收件者使用您的自訂規則作為資料來源對應來收集證據，他們必須在執行個體中建立相同的自訂規則 AWS Config。收件者[建立](#)並[啟用](#)規則後，Audit Manager 可以從該資料來源收集證據。

我們建議您與收件者通訊，讓他們知道是否需要在其 AWS Config 執行個體中建立任何自訂規則。

## 在 AWS Config 中更新自訂規則時會發生什麼情況？我需要在 Audit Manager 中採取任何動作嗎？

### 針對 AWS 環境中的規則更新

如果您更新 AWS 環境中的自訂規則，則不需要在 Audit Manager 中執行任何動作。Audit Manager 會依照下表所述偵測和處理規則更新。偵測到規則更新時，Audit Manager 不會另行通知。

案例	Audit Manager 會做什麼	您需要執行的事項
自訂規則會在您的執行個體中更新 AWS Config	Audit Manager 會繼續使用更新的規則定義報告該規則的調查結果。	不需採取任何動作。
自訂規則會在您的執行個體中刪除 AWS Config	Audit Manager 會停止報告已刪除規則的調查結果。	不需採取任何動作。  如果需要，您可以 <a href="#">編輯自訂控制項</a> ，使用已刪除規則作為資料來源映射項目。這樣做有助於透過移除已刪除的規則，來清除資料來源設定。否則，刪除的規則名稱會保留為未使用的資料來源映射項目。

### 適用於 AWS 環境外部的規則更新

如果在您的 AWS 環境之外更新了自訂規則，則 Audit Manager 不會偵測規則更新。如果您使用共享的自訂架構，這將是需要考慮的因素。這是因為，在這個案例中，寄件者和收件者各自在不同的 AWS 環境中工作。下表提供適用於此方案的建議作法。

您的角色	案例	建議的動作
寄件者	<ul style="list-style-type: none"> <li>您共享使用自訂規則作為資料來源映射項目的架構。</li> <li>共用架構之後，您就更新或刪除了中的其中一個規則 AWS Config。</li> </ul>	通知收件者您的更新。如此一來，他們就可以套用相同的更新，並與最新的規則定義保持同步。
收件人	<ul style="list-style-type: none"> <li>您接受使用自訂規則做為資料來源映射項目的共享架構。</li> <li>在的執行個體中重新建立自訂規則之後 AWS Config，寄件者就會更新或刪除其中一個規則。</li> </ul>	在您自己的 AWS Config 執行個體中進行對應的規則更新。

## 儀表板問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的儀表板問題。

### 主題

- [我的儀表板上沒有任何資料](#)
- [我無法再看到評估的儀表板資料](#)
- [無法使用 CSV 下載選項](#)
- [嘗試下載 CSV 檔案時看不到下載的檔案](#)
- [儀表板遺失特定控制項或控制項域](#)
- [每日快照顯示每天的證據數量都不相同。這正常嗎？](#)

### 我的儀表板上沒有任何資料

如果 [每日快照](#) Widget 中的數字顯示連字號 (-)，表示沒有可用的資料。您必須至少有一個作用中的評估，才能在儀表板中查看資料。若要開始使用，請[建立評估](#)。24 小時後，您的評估數據將開始顯示在儀表板中。

**Note**

如果每日快照小工具中的數字顯示為零(0)，表示您作用中的評估(或您選取的評估)沒有不合規的證據。

## 我無法再看到評估的儀表板資料

Audit Manager 不會顯示使用舊版標準架構建立之評估的儀表板資料。您可以從最新版本的標準架構重新建立評估來解決此問題。

當 Audit Manager 於 2024 年 6 月 6 日啟動通用控制項程式庫時，我們更新了所有標準架構。在新的框架定義中，框架的所有標準控件現在都可以從 [AWS managed sources](#) 收集證據。這表示每當針對一般或核心控制項的基礎資料來源有更新時，Audit Manager 就會自動將相同的更新套用至所有相關的標準控制項。

每次自動更新這些資料來源對映時，您不需要建立新評估。建立新評估是一次性活動，我們建議您在通用控制項啟動後完成。

若要查看儀表板上的深入解析資料，請從標準架構的更新版本建立新的評估。建立新評估之後，您可以將 [舊評估的狀態變更為非作用中](#)。

## 無法使用 CSV 下載選項

此選項只適用於個別評估。請確定已套用 [評估篩選器](#) 至儀表板，然後再試一次。請記住，您一次只能下載一個 CSV 檔案。

## 嘗試下載 CSV 檔案時看不到下載的檔案

如果控制項域包含大量控制項，則 Audit Manager 產生 CSV 檔案時可能會有短暫的延遲。文件生成後，它會開始自動下載。

如果您仍然看不到下載的檔案，請確定您的網際網路連線正常運作，而且您使用的是最新版本的網頁瀏覽器。此外，請檢查您最近的下載文件夾。檔案會下載至瀏覽器所決定的預設位置。如果這樣無法解決您的問題，請嘗試使用其他瀏覽器下載檔案。

## 儀表板遺失特定控制項或控制項域

這可能表示您作用中的評估(或指定的評估)沒有該控制項或控制項域的任何相關資料。

只有當下列兩個條件都符合時，控制項域才會顯示在儀表板上：

- 您作用中的評估(或指定的評估)至少包含一個與該域相關的控制項
- 該域內至少有一個控制項，在儀表板頂端的日期有收集證據

只有當控制項在儀表板頂部的日期收集證據時，控制項才會顯示在域內。

## 每日快照顯示每天的證據數量都不相同。這正常嗎？

並非每天都會收集所有證據。Audit Manager 評估中的控制項會對應至不同的資料來源，而且每個控制項都可以有不同的證據收集排程。因此，每日快照每天顯示的證據數量不同是很正常的。如需詳細資訊，請參閱 [證據收集頻率](#)。

## 委派系統管理員與 AWS Organizations 相關問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的委派系統管理員問題。

### 主題

- [我無法在 Audit Manager 設定委派系統管理員帳戶](#)
- [建立評估時，我無法在範圍內的帳戶看到組織中的帳戶](#)
- [當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤](#)
- [如果我取消成員帳戶與組織的連結，Audit Manager 會發生什麼情況？](#)
- [如果我將成員帳戶重新連結至組織，會發生什麼情況？](#)
- [如果我將成員帳戶從一個組織移到另一個組織，會發生什麼情況？](#)

## 我無法在 Audit Manager 設定委派系統管理員帳戶

雖然支援多個委派管理員 AWS Organizations，但 Audit Manager 只允許一名委派管理員。如果您嘗試在 Audit Manager 中指定多個委派系統管理員，您會收到下列錯誤訊息：

- 主控台：You have exceeded the allowed number of delegated administrators for the delegated service
- CLI：An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 111111111111 from 222222222222 to 333333333333

在 Audit Manager 中，選擇一個要擔任委派系統管理員的帳戶。請務必先在組織內註冊此委派系統管理員帳戶，然後在 Audit Manager [新增與委派系統管理員相同的帳戶](#)。

## 建立評估時，我無法在範圍內的帳戶看到組織中的帳戶

如果您希望 Audit Manager 評估包含組織中的多個帳戶，則必須指定委派系統管理員。

請確認您已為 Audit Manager 配置委派系統管理員帳戶。如需說明，請參閱[新增委派管理員](#)。

需要謹記的一些事項：

- 您無法在 Audit Manager AWS Organizations 管理員中以委派的系統管理員身分使用您的管理帳戶。
- 如果您要啟用多個 Audit Manager 員 AWS 區域，則必須在每個區域中個別指定委派的管理員帳戶。在 Audit Manager 設定中，為所有區域指定相同的委派系統管理員帳戶。
- 當您指定 Audit Manager 的委派系統管理員時，請確保委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。若要瞭解如何檢閱和變更加密設定，請參閱[設定您的資料加密設定](#)。

## 當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤

如果您的評估是由委派的系統管理員帳戶建立，並且 Audit Manager 設定中指定的 KMS 金鑰不屬於該帳戶，您將會收到 access denied 錯誤訊息。若要避免此錯誤，當您指定 Audit Manager 的委派系統管理員時，請確定委派系統管理員帳戶具有您設定 Audit Manager 時所提供的 KMS 金鑰的存取權限。

如果您沒有用作評估報告目的地的 S3 儲存貯體的寫入權限，您也可能會收到 access denied 錯誤訊息。

若您收到 access denied 錯誤訊息，請確定您符合下列要求：

- 您在 Audit Manager 設定中的 KMS 金鑰將權限授予委派系統管理員。您可以依照 AWS Key Management Service 開發人員指南中，[允許其他帳戶中的使用者使用 KMS 金鑰](#)中的指南進行設定。如需如何在 Audit Manager 中檢閱和變更加密設定的指示，請參閱[設定您的資料加密設定](#)。
- 您擁有一個權限策略，該策略可授予您評估報告目的地的寫入存取權限。更具體地說，您的許可政策包含一個 s3:PutObject 動作、指定 S3 儲存貯體的 ARN，並包含用於加密評估報告的 KMS 金鑰。如需您可以使用的範例原則，請參閱[範例 2 \(評估報表目的地許可\)](#)。

**Note**

如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括您依據新評估所建立的任何評估報告。

這些變更不會套用至您在變更加密設定之前，已建立的現有評估。出了現有的評估報告之外，這還包括了您根據現有評估建立的新評估報告。現有的評估及其所有評估報告都將繼續使用舊有的 KMS 金鑰。如果產生評估報告的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

## 如果我取消成員帳戶與組織的連結，Audit Manager 會發生什麼情況？

當您取消組織成員帳戶的連結時，Audit Manager 會收到有關此事件的通知。然後，Audit Manager 會自動從現有評估範圍中的帳戶清單中移除此 AWS 帳戶。當您指定新評估的範圍後，取消連結的帳戶將不會再出現在符合資格的 AWS 帳戶清單中。

當 Audit Manager 從評估範圍中的帳戶中移除取消連結的成員帳戶時，系統不會通知您這項變更。此外，取消連結的成員帳戶也不會收到通知，得知帳戶已不再啟用 Audit Manager。

## 如果我將成員帳戶重新連結至組織，會發生什麼情況？

當您將成員帳戶重新連結至組織時，該帳戶不會自動新增至您現有 Audit Manager 評估的範圍。但是，當您在評估範圍內指定帳戶 AWS 帳戶時，重新連結的成員帳戶現在會顯示為符合資格。

- 對於現有評估，您可以手動編輯評估範圍，以新增重新連結的成員帳戶。如需說明，請參閱[步驟 2：AWS 帳戶在範圍內編輯](#)。
- 對於新的評估，您可以在評估設定期間新增重新連結的帳戶。如需說明，請參閱[步驟 2：AWS 帳戶在範圍內指定](#)。

## 如果我將成員帳戶從一個組織移到另一個組織，會發生什麼情況？

如果成員帳戶已在組織 1 中啟用 Audit Manager 然後移轉至組織 2，不會因此啟用組織 2 的 Audit Manager。

## 證據搜尋工具問題疑難排解

請參考此頁面提供的資訊，解決 Audit Manager 中常見的證據搜尋工具問題。

## 一般證據搜尋工具問題

- [我無法啟用證據搜尋工具](#)
- [我已啟用證據搜尋工具，但在搜尋結果中看不到過去的證據](#)
- [我無法停用證據搜尋工具](#)
- [我的搜尋查詢失敗](#)

## 證據搜尋工具評估報告問題

- [我無法從搜尋結果中產生多個評估報告](#)
- [我無法在搜尋結果中加入特定證據](#)
- [在評估報告中，並未包含所有來自證據搜尋工具的查找結果](#)
- [我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗](#)
- [其他資源](#)

## 證據搜尋工具 CSV 匯出問題

- [我的 CSV 匯出失敗](#)
- [我無法從搜尋結果中匯出特定證據](#)
- [我無法一次匯出多個 CSV 檔案](#)

## 我無法啟用證據搜尋工具

無法啟用證據搜尋工具的常見原因如下：

### 您缺少權限

如果您是第一次嘗試啟用證據查找器，請確保您具有[啟用證據查找器的必要權限](#)。這些權限可讓您建立和管理 CloudTrail Lake 中的事件資料存放區，這對於支援證據搜尋器搜尋查詢是必要的。許可還允許您在證據搜尋工具中執行搜尋查詢。

如果您需要權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 管理員，則可以複製所需的權限聲明並[將其附加到 IAM 政策](#)。

### 您正在使用組織管理帳戶

請記住，您無法使用管理帳戶來啟用證據搜尋工具。以委派系統管理員帳戶身分登入，然後重試。

## 您之前已停用證據搜尋工具

目前不支援重新啟用證據搜尋工具。如果您之前已停用證據搜尋工具，則無法再次啟用它。

## 我已啟用證據搜尋工具，但在搜尋結果中看不到過去的證據

當您啟用證據搜尋工具時，您過去的所有證據資料，最多需要 7 天才能存取使用。

在這 7 天期間，事件資料存放區會回填您過去兩年的證據資料。這意味著，如果您在啟用證據搜尋工具後立即使用操作，則在完成回填之前，無法獲取完整的搜尋結果。

如需如何檢查資料回填狀態的指示，請參閱[確認證據搜尋器的狀態](#)。

## 我無法停用證據搜尋工具

這可能由以下其中一個原因造成。

### 您缺少權限

如果您嘗試禁用證據查找器，請確保您具有[禁用證據查找器的所需權限](#)。這些權限可讓您更新和刪除 CloudTrail Lake 中的事件資料儲存區，這對於停用證據搜尋工具是必要的。

如果您需要權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 管理員，則可以複製所需的權限聲明並[將其附加到 IAM 政策](#)。

### 啟用證據搜尋工具的要求仍在進行中

當您要求啟用證據搜尋工具時，我們會建立一個事件資料存放區，以支援證據搜尋工具查詢。建立事件資料存放區時，您無法停用證據搜尋工具。

若要繼續，請等到事件資料存放區建立完成，然後再試一次。如需詳細資訊，請參閱[確認證據搜尋器的狀態](#)。

### 您已要求停用證據搜尋工具

當您要求停用證據搜尋工具時，我們會刪除用於證據搜尋工具查詢的事件資料存放區。如果您在刪除事件資料存放區時再次嘗試停用證據搜尋工具，您會收到錯誤訊息。

在這種情況下，不需要採取任何動作。等待事件資料存放區刪除。一旦完成，證據搜尋工具將被禁用。如需詳細資訊，請參閱[確認證據搜尋器的狀態](#)。



## 我的搜尋查詢失敗

失敗的搜尋查詢可能由以下其中一項原因造成。

### 您缺少權限

驗證使用者是否具備執行搜尋查詢和存取搜尋結果的[所需權限](#)。具體而言，您需要下列 CloudTrail 動作的權限：

- [StartQuery](#)
- [DescribeQuery](#)
- [CancelQuery](#)
- [GetQueryResults](#)

如果您需要權限方面的協助，請聯絡您的 AWS 管理員。如果您是 AWS 管理員，則可以複製所需的權限聲明並[將其附加到 IAM 政策](#)。

### 您的查詢數目已達上限

您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會導致 `MaxConcurrentQueriesException` 錯誤。如果您收到這個錯誤訊息，請稍候一分鐘讓部分查詢完成，然後再次執行查詢。

### 您的查詢陳述式有驗證錯誤

如果您使用 API 或 CLI 來執行 CloudTrail 湖泊 [StartQuery](#) 作業，請確定您的 `queryStatement` 是有效的。如果查詢陳述式有驗證錯誤、語法不正確或不支援的關鍵字，這會導致 `InvalidQueryStatementException`。

如需有關撰寫查詢的詳細資訊，請參閱 AWS CloudTrail 使用指南中的[建立或編輯查詢](#)。

如需有效語法的範例，請檢閱下列可用來查詢 Audit Manager 事件資料存放區的查詢陳述式範例。

#### 範例 1：調查證據及其合規狀態

此範例會在指定日期範圍內，尋找帳戶中所有評估中具有任何合規狀態的證據。

```
SELECT eventData.evidenceId, eventData.resourceArn,  
eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02  
00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

#### 範例 2：判斷控制項的不合規證據

此範例會尋找特定評估和控制項在指定日期範圍內的所有不合規證據。

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN ('NON_COMPLIANT', 'FAILED', 'WARNING') AND eventData.controlId IN ('aa11bb22-cc33-dd44-ee55-ff66gg77hh88')
```

### 範例 3：按名稱計算證據

此範例會列出指定日期範圍內評估的總證據，並依名稱分組，並依證據計數排序。

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY eventData.eventName ORDER BY totalEvidence DESC
```

### 範例 4：依資料來源和服務探索證據

此範例會尋找特定資料來源和服務在指定日期範圍內的所有證據。

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND eventData.dataSource IN ('AWS API calls')
```

### 範例 5：依資料來源和控制項域探索合規證據

此範例尋找特定控制項域的合規證據，其中證據來自非 AWS Config 的資料來源。

```
SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN ('PASSED', 'COMPLIANT') AND eventData.controlDomainName IN ('Logging and monitoring', 'Data security and privacy') AND eventData.dataSource NOT IN ('AWS Config')
```

## 其他 API 異常狀況

[StartQuery](#) API 可能由於其他幾個原因而失敗。如需可能錯誤和說明的完整清單，請參閱 AWS CloudTrail API 參考中的 [StartQuery 錯誤](#)。

## 我無法從搜尋結果中產生多個評估報告

此錯誤是由於同時執行過多 CloudTrail Lake 查詢所造成的。

如果您將搜尋結果分組，並嘗試針對群組結果中的每個明細項目立即產生評估報告，就會發生此錯誤。當您取得搜尋結果並產生評估報告時，每個動作都會觸發一次查詢。您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。

若要避免發生此錯誤，請確保您沒有一次產生過多的評估報告。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。如果您收到此錯誤訊息，請等待幾分鐘，讓進行中的評估報告完成。

您可以從 Audit Manager 主控台的下載中心頁面，檢查評估報告的狀態。報告完成後，在證據搜尋工具中返回您的分組結果。然後，您可以繼續取得結果，並為每個明細項目產生評估報告。

## 我無法在搜尋結果中加入特定證據

您的所有搜尋結果都包含在評估報告中。您無法從搜尋結果集中選擇性地新增個別列。

如果您只想在評估報告中包含特定的搜尋結果，建議您[編輯目前的搜尋篩選器](#)。如此一來，您就可以縮小結果範圍，僅鎖定您要包含在報告中的證據。

## 在評估報告中，並未包含所有來自證據搜尋工具的查找結果

當您產生評估報告時，您可以新增的證據數量有限。此限制取決於您 AWS 區域的評估、用作評估報告目標的 S3 儲存貯體區域，以及您的評估是否使用受管的客戶 AWS KMS key。

1. 相同區域報告的上限為 22,000 (S3 儲存貯體和評估都在同一個 AWS 區域的情況下)
2. 跨區域報告的上限為 3,500 (S3 儲存貯體和評估在不同 AWS 區域的情況下)
3. 如果評估使用客戶管理的 KMS 金鑰，則上限為 3,500

如果您超過此限制，報告仍會建立。不過，Audit Manager 只會將前 3,500 或 22,000 個證據項目新增至報告。

若要避免發生此問題，建議您[編輯目前的搜尋篩選器](#)。如此一來，您就可以針對較少量的證據來減少搜尋結果。如果需要，您可以重複此方法並產生多個評估報告，而不是一個較大的報告。

## 我想從搜尋結果中產生評估報告，但我的查詢陳述式執行失敗

如果您使用的是 [CreateAssessmentReport](#) API，且您的查詢陳述式傳回驗證例外狀況，請查看下表以取得如何修正此問題的指引。

**Note**

即使查詢陳述式在中運作 CloudTrail，相同的查詢對於在 Audit Manager 中產生評估報告可能無效。這是因為兩個服務之間的查詢驗證有些差異。

子句	問題	解決方案	備註
SELECT	SELECT 子句包含一個列名	移除 SELECT 子句並替換為 SELECT eventJson。	僅支援 SELECT eventJson。  此驗證由 Audit Manager 處理。
FROM	FROM 子句包含無效的事件資料存放區 ID 或  提供的事件資料存放區 ID 與 Audit Manager 設定中的事件資料存放區 ID 不符	移除子句 FROM 並替換為 FROM <i>edsID</i> ，其中的值 edsID 與 Audit Manager 設定中指定的事件資料存放區 ID 相符。  您可以從 Audit Manager 設定中擷取事件資料存放區的 ARN。如需詳細資訊，請參閱 AWS Audit Manager API 參考 <a href="#">GetSettings</a> 中的。	此驗證由 Audit Manager 處理。
GROUP BY	查詢中存在一個 GROUP BY 子句	移除 GROUP BY 子句。	此驗證由 Audit Manager 處理。
HAVING	查詢中存在一個 HAVING 子句	移除 HAVING 子句。	此驗證由 Audit Manager 處理。
LIMIT	LIMIT 子句包含的值超過允許的最大限制	如果 LIMIT 子句存在，請確保其值等於或小於支援的最大限制： <ul style="list-style-type: none"> <li>對於同區域報表，上限為 22,000</li> <li>對於跨區域報表，上限為 3,500</li> </ul>	在主控台中，可傳回的證據結果數量沒有限制。不過，產生評估報告時，您可以包含的證據數量會有限制。

子句	問題	解決方案	備註
		<ul style="list-style-type: none"> <li>對於相關評估使用客戶管理的報表 AWS KMS key，上限為 3,500</li> </ul>	<p>如果您的查詢陳述式中未提供任何 LIMIT 值，則會套用預設的最大限制。</p> <p>此驗證由 Audit Manager 處理。</p>
ORDER BY	ORDER BY 子句包含 SELECT 子句中不存在的 <a href="#">彙總函數</a> 或 <a href="#">別名</a>	請確保 ORDER BY 子句不包含任何使用 <a href="#">彙總函數</a> 或 <a href="#">別名</a> 的條件。	此驗證由 CloudTrail <a href="#">StartQuery API 處理</a> 。
WHERE	<p>WHERE 子句包含多個 assessmentId</p> <p>或</p> <p>WHERE 子句包含一個 assessmentId，其與您的 createAssessmentReport 要求的 assessmentId 不相符。</p> <p>或</p> <p>WHERE 子句包含一個不支援的列名</p>	<p>請確定您只指定一個 assessmentId，而且它符合您在 createAssessmentReport API 要求中指定的 <a href="#">assessmentId 參數</a>。</p> <p>移除任何不支援的欄位名稱。</p>	此驗證由 CloudTrail <a href="#">StartQuery API 處理</a> 。

## 範例

下列範例說明如何在呼叫 [CreateAssessmentReport](#) 作業時使用 queryStatement 參數。使用這些查詢之前，請先用您自己的 edsId 和 assessmentId 值取代 #####。

### 範例 1：建立報表（適用相同區域限制）

此範例會建立一個報告，其中包含在 2022 年 1 月 22 日至 23 日之間建立之 S3 儲存貯體的結果。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

### 範例 1：建立報表 (適用跨區域限制)

此範例會建立一個報告，其中包含指定事件資料存放區和評估的所有結果，但未指定日期範圍。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

### 範例 3：建立報告 (在預設限制下)

此範例會建立一個報告，其中包含指定事件資料存放區和評估的所有結果，其上限低於預設最大值。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

## 其他資源

下列頁面提供關於評估報告的一般疑難問題排解指南：

- [評估報告問題疑難排解](#)

## 我的 CSV 匯出失敗

您的 CSV 匯出失敗原因有很多種可能性。您可以透過檢查常見原因來對此問題進行故障排除。

首先，請確認您符合使用 CSV 匯出功能的必要條件：

您已成功啟用證據搜尋工具

如果您尚未[啟用證據搜尋工具](#)，則無法執行搜尋查詢並匯出搜尋結果。

事件資料存放區的回填已完成

如果您在啟用證據搜尋工具後立即使用證據搜尋工具，並且[證據回填](#)仍在進行中，則可能會有一些結果無法使用。若要檢查回填狀態，請參閱[確認證據搜尋器的狀態](#)。

您的搜尋查詢成功

Audit Manager 無法匯出失敗查詢的結果。若要疑難排解失敗的查詢，請參閱 [我的搜尋查詢失敗](#)。

確認符合先決條件後，請使用下列檢查清單來檢查潛在問題：

1. 檢查您搜尋查詢的狀態：
  - a. 查詢是否已取消？證據搜尋工具會顯示在取消查詢之前處理的部分結果。不過，Audit Manager 不會將部分結果匯出到 S3 儲存貯體或下載中心。
  - b. 查詢是否已執行超過一個小時？執行時間超過一小時的查詢可能會逾時。證據搜尋工具會顯示在查詢逾時之前處理的部分結果。但是，Audit Manager 不會匯出部分結果。若要避免逾時，您可以減少掃描的證據量，以指[編輯搜尋篩選條件](#)定較窄的時間範圍。
2. 檢查匯出目的地的 S3 儲存貯體名稱和 URI：
  - a. 指定的儲存貯體是否存在？如果您手動輸入儲存貯體 URI，請確保沒有錯誤輸入任何內容。當 Audit Manager 嘗試將 CSV 檔案匯出到 Amazon S3 時，錯字或不正確的 URI 可能會導致 RESOURCE\_NOT\_FOUND 錯誤。
3. 檢查匯出目的地的 S3 儲存貯體權限：
  - a. 您有 S3 儲存貯體的寫入權限嗎？您必須擁有用作匯出目的地的 S3 儲存貯體寫入權限。更具體地說，IAM 許可政策必須包含 s3:PutObject 動作和值區 ARN，並列 CloudTrail 為服務主體。我們提供您可以使用的[範例政策](#)。
4. 檢查您的任何 AWS 區域 信息是否不匹配：
  - a. 您 AWS 區域 的客戶管理金鑰是否與您 AWS 區域 的評估相符？如果您為資料加密提供了客戶管理金鑰，則該金鑰必須與您的評估 AWS 區域 相同。如需如何變更 KMS 金鑰的指示，請參閱[設定您的資料加密設定](#)。
5. 檢查委派管理員的帳戶權限：
  - a. Audit Manager 設定中的客戶管理金鑰，是否會將權限授與委派系統管理員？如果您使用委派系統管理員帳戶，並指定了用於資料加密的客戶管理金鑰，請確定委派系統管理員擁有該 KMS 金鑰的存取權。如需指示，請參閱 AWS Key Management Service 開發人員指南中的[允許其他帳戶中的使用者使用 KMS 金鑰](#)。若要在 Audit Manager 中檢閱和變更您的加密設定，請參閱[設定您的資料加密設定](#)。

#### Note

如果您變更 Audit Manager 資料加密設定，這些變更會套用至您未來建立的新評估。這包括從新的評估匯出的任何 CSV 檔案。

這些變更不會套用至您在變更加密設定之前，已建立的現有評估。除了現有的 CSV 匯出之外，這還包括基於現有評估匯出的新 CSV。現有的評估及其所有 CSV 報告都將繼續使用舊有

的 KMS 金鑰。如果匯出 CSV 檔案的 IAM 身分沒有使用舊有 KMS 金鑰的權限，您可以在金鑰政策層級授予權限。

## 我無法從搜尋結果中匯出特定證據

您的所有搜尋結果都包含在結果中。

如果您只想在 CSV 檔案中包含特定的搜尋結果，建議您[編輯目前的搜尋篩選器](#)。如此一來，您就可以縮小結果範圍，僅鎖定您要匯出的證據。

## 我無法一次匯出多個 CSV 檔案

此錯誤是由於同時執行過多 CloudTrail Lake 查詢所造成的。

如果您將搜尋結果分組，並嘗試針對群組結果中的每個行項目立即匯出 CSV 檔案，就會發生此錯誤。當您在取得搜尋結果時同步匯出 CSV 檔案，這些動作都會引發一次查詢。您一次最多可以執行 5 個查詢。如果您同時執行的查詢數目已達上限，則會返回 `MaxConcurrentQueriesException` 錯誤。

若要避免發生此錯誤，請確保您沒有一次匯出太多 CSV 檔案。

若要解決此錯誤，請等待進行中的 CSV 匯出完成。大多數匯出動作需要幾分鐘的時間。不過，如果您要匯出非常大量的資料，則可能需要長達一個小時才能完成匯出作業。在匯出過程中，您可以隨時離開證據搜尋工具。

您可以從 Audit Manager 主控台的下載中心檢查匯出狀態。匯出的檔案準備就緒後，返回證據搜尋工具中的分組結果。然後，您可以繼續取得結果，並匯出每個明細項目的 CSV 檔案。

## 疑難排解架構問

您可以使用此頁面上的資訊來解決 Audit Manager 中常見的架構問題。

### 一般框架問題

- [在我的自定義框架詳細信息頁面上，系統提示我重新創建自定義框架](#)
- [我無法製作自定義框架的副本或使用它來創建評估](#)

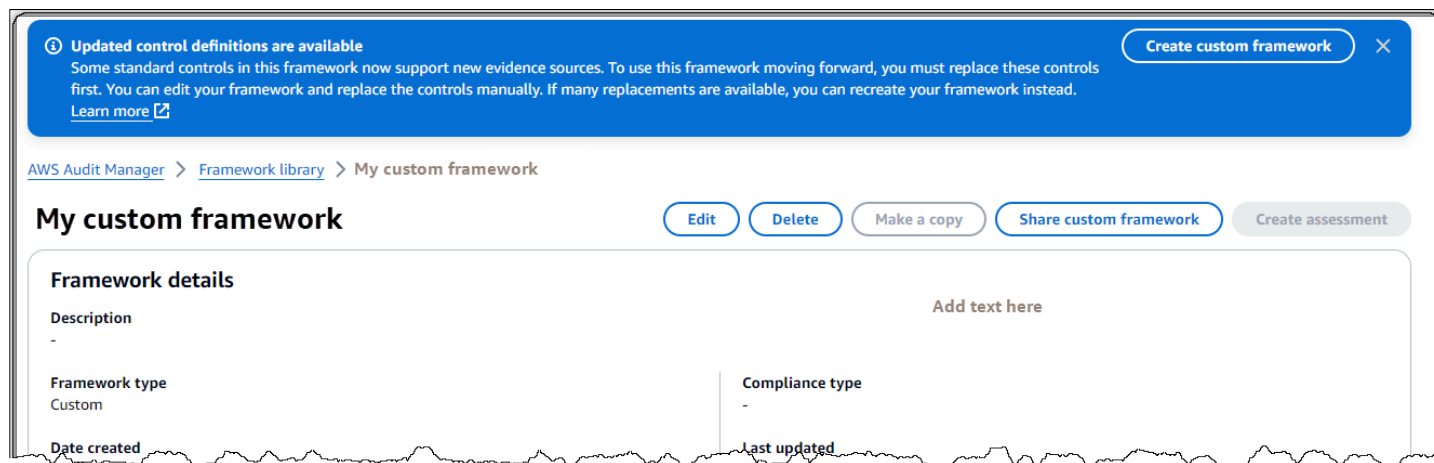
### 框架共享問題

- [我傳送的共享要求狀態顯示為失敗](#)



- [我的共享要求旁邊有一個藍點。這代表什麼意思？](#)
- [我的共享框架具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？](#)
- [我更新了共享架構中使用的自訂規則。我需要採取任何動作嗎？](#)

在我的自定義框架詳細信息頁面上，系統提示我重新創建自定義框架



如果您看到一則訊息，指出已更新的控制項定義可用，這表示 Audit Manager 現在會針對自訂架構中的某些標準控制項提供較新的定義。

標準控制現在可以從中收集證據 [AWS managed source](#)。這表示每當 Audit Manager 更新通用控制項或核心控制項的基礎資料來源時，相同的更新都會自動套用至相關的標準控制項。這可協助您確保在雲端合規環境變更時持續遵循法規遵循。為了確保您從這些受 AWS 管理的來源中受益，我們建議您更換自訂架構中的控制項。

在您的自訂架構中，Audit Manager 會指出哪些控制項有可用的取代項目。您必須先取代這些控制項，才能複製自訂架構或從中建立評估。下次您編輯自訂架構時，我們會提示您取代這些控制項以及您想要進行的任何其他編輯。

有兩種方法可以替換自定義框架中的控件：

### 1. 重新創建自定義框架

如果大量控制項有可用的替代項目，建議您重新建立自訂架構。如果您的自定義框架基於標準框架，這可能是最好的選擇。

- 例如，假設您使用 [第五修訂版](#) 作為起點創建了自定義框架。這個標準架構有 1007 個標準控制項，而且您新增了 20 個自訂控制項。

- 在這種情況下，最有效的選擇是NIST 800-53 (Rev. 5) Low-Moderate-High在框架庫中查找並[製作該框架的可編輯副本](#)。在此過程中，您可以添加之前使用的 20 個自定義控件。因為您現在使用標準架構的最新定義做為起點，所以您的自訂架構會自動繼承所有 1007 個標準控制項的最新定義。

## 2. 編輯您的自訂架構

如果少數控制項有可用的替代項目，建議您編輯自訂架構並手動取代控制項。

- 例如，假設您從頭開始創建了自定義框架。在您的自訂架構中，您新增了 20 個您自己建立的自訂控制項，以及標準架構中的八個標[ACSC 基本八項](#) 準控制項。
- 在這種情況下，由於最多八個控制項有可用的更新，因此最有效的選項是編輯您的自訂架構，並逐一取代這些控制項。如需詳細資訊，請參閱下列程序。

### 手動取代自訂架構中的控制項

### 手動取代自訂架構中的控制項

1. 開啟 AWS Audit Manager 主控台，[網址為 https://console.aws.amazon.com/auditmanager/home](https://console.aws.amazon.com/auditmanager/home)。
2. 在左側導覽窗格中，選擇 [架構資料庫]，然後選擇 [自訂架構] 索引標籤。
3. 選擇您要停止的機群，選擇動作，然後選擇停止。
4. 在 [編輯架構詳細資料] 頁面上，選擇 [下一步]
5. 在 [編輯控制集] 頁面上，檢閱每個控制項集的名稱，以查看其任何控制項是否有可用的取代項目。
6. 選擇受影響的控制集以將其展開，並識別需要更換其控制項。

#### Tip

若要更快速地識別控制項，請**Replacement available**在搜尋方塊中輸入。

7. 選取核取方塊並選擇 [從控制集移除]，以移除受影響的控制項。
8. 重新添加相同的控件。此動作會以最新的控制項定義取代您剛移除的控制項。
  - a. 在 [新增控制項] 下，使用 [控制項類型] 下拉式清單，並選取 [標準]
  - b. 尋找剛移除之控制項的取代項目。

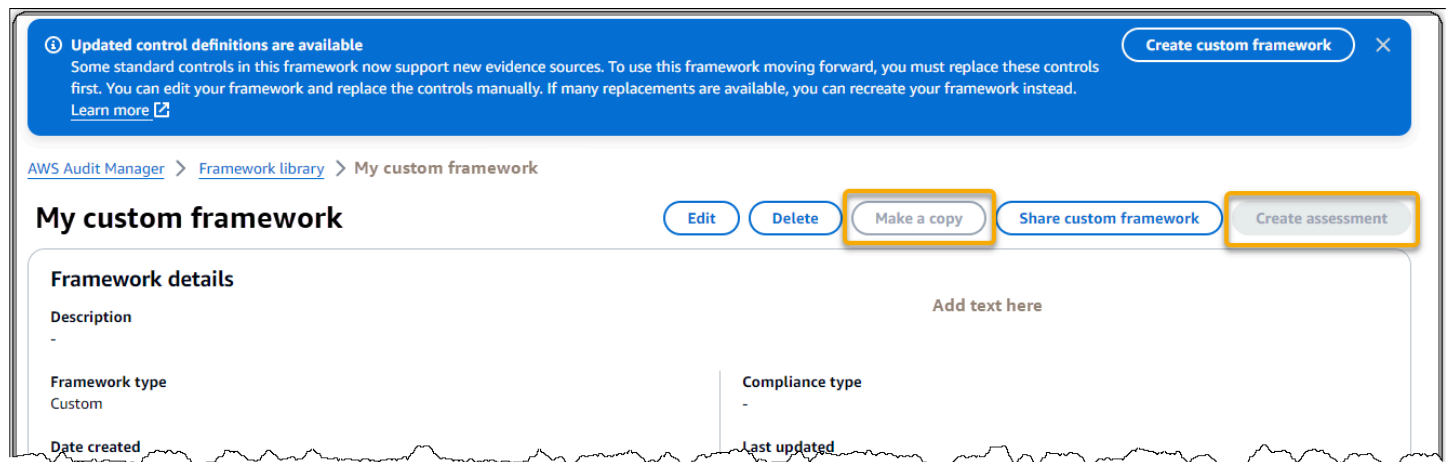
**i** Tip

在某些情況下，取代控制項名稱可能與原始控制項名稱不完全相同。在此情況下，取代控制項名稱可能與原始控制項名稱非常相似。在極少數情況下，一個控制項可能會被兩個控制項取代 (或其他方式)。

如果找不到取代控制項，建議您進行部分搜尋。若要這麼做，請輸入原始控制項名稱的一部分，或是代表您要尋找之項目的關鍵字。您也可以依照規範類型進行搜尋，進一步縮小結果清單的範圍。

- c. 選取控制項旁邊的核取方塊，然後選擇 [新增至控制集]。
  - d. 在出現的快顯視窗中，選擇「新增」以確認。
9. 視需要重複步驟 6-8，直到您取代所有控制項為止。
  10. 選擇下一步。
  11. 在 [檢閱並儲存] 頁面上，選擇 [儲存變更]。

## 我無法製作自定義框架的副本或使用它來創建評估



如果 [架構詳細資料] 頁面上無法使用 [建立副本] 和 [建立評估] 按鈕，這表示您必須取代自訂架構中的某些控制項。

如需如何繼續操作的指示，請參閱[在我的自定義框架詳細信息頁面上](#)，系統提示我重新創建自定義框架。

## 我傳送的共享要求狀態顯示為失敗

如果您嘗試共享自訂架構，但作業失敗，建議您檢查下列項目：

1. 請確定已在收件者 AWS 帳戶 和指定區域中啟用 Audit Manager。如需支援的 AWS Audit Manager 區域清單，請參閱 Amazon Web Services 一般參考中的 [AWS Audit Manager 端點和配額](#)。
2. 確保您在指定收件人帳戶時輸入了正確的 AWS 帳戶 ID。
3. 請確定您未將 AWS Organizations 管理帳戶指定為收件者。您可以與委派系統管理員共享自訂架構，但是如果您嘗試與管理帳戶共享自訂架構，則作業會失敗。
4. 如果您使用客戶管理金鑰來加密 Audit Manager 資料，請確保您的 KMS 金鑰已啟用。如果您的 KMS 金鑰已停用，而您嘗試共享自訂架構，則作業會失敗。關於如何啟用已停用 KMS 金鑰的指南，請參閱 AWS Key Management Service 開發人員指南中的 [啟用和停用金鑰](#)。

## 我的共享要求旁邊有一個藍點。這代表什麼意思？

藍點通知表示有共享要求需要您過目。

### 寄件者藍點通知

已傳送的共享要求旁會出現藍色通知圓點，且狀態為即將到期。Audit Manager 會顯示藍點通知，以便提醒收件者在共享要求到期之前對其採取行動。

若要讓藍點通知消失，收件者必須接受或拒絕要求。如果您撤銷共享要求，藍點也會消失。

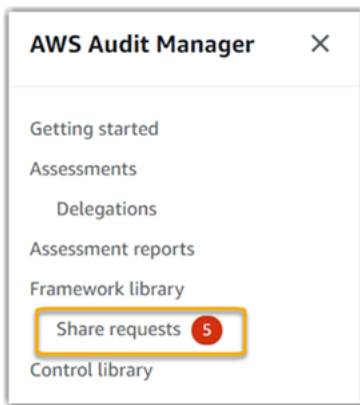
您可以使用下列程序來檢查，是否有任何即將到期的共享要求，並傳送選擇性提醒給收件者採取行動。

若要檢視已傳送要求的通知

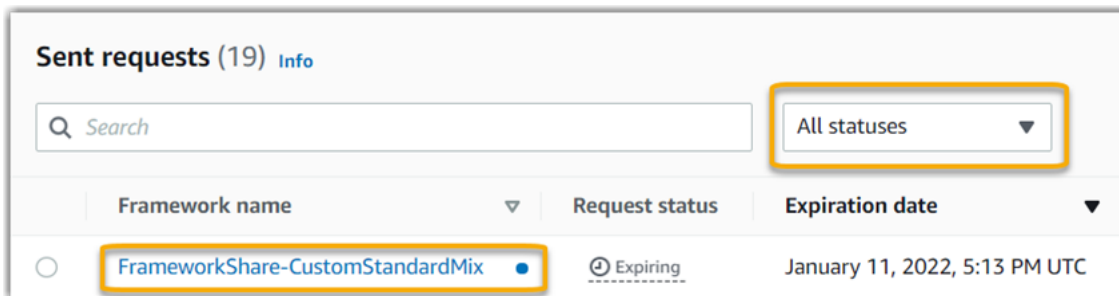
1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。



3. 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要處理的共享要求數目。



4. 選擇共享要求，然後選擇傳送要求索引標籤。
5. 尋找藍點，找出未來 30 天內到期的共享要求。或者，您也可以從所有狀態 篩選器下拉式清單中選取即將到期，檢視即將到期的共享要求。



6. (選擇性) 提醒收件者，他們需要在共享要求到期前對其採取行動。此步驟為選擇性步驟，因為 Audit Manager 會在主控台中傳送通知，以便在共享要求處於作用中或即將到期時通知收件者。但是，您也可以使用偏好的通訊管道向收件人發送自己的提醒。

### 收件者藍點通知

已傳送的共享要求旁會出現藍色通知圓點，且狀態為作用中或即將到期。Audit Manager 會顯示藍點通知，以便提醒收件者在共享請求到期之前對其採取行動。若要讓藍點通知消失，收件者必須[接受或拒絕](#)要求。如果傳送者撤銷共享要求，藍點也會消失。

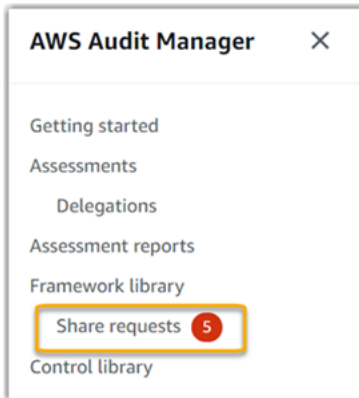
您可以使用下列程序檢查作用中和即將到期的共享要求。

### 若要檢視已接收請求的通知

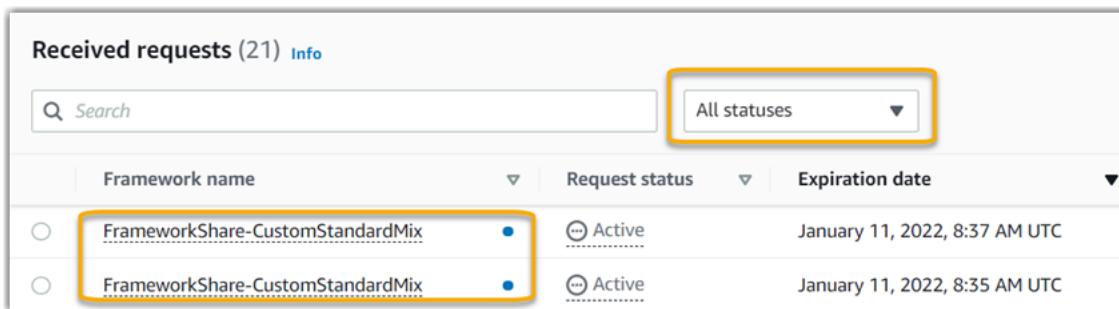
1. 開啟 AWS Audit Manager 主控台，網址為 <https://console.aws.amazon.com/auditmanager/home>。
2. 如果您有共享要求通知，Audit Manager 會在導覽功能表圖示旁邊顯示一個紅點。



- 展開瀏覽窗格，然後查看共享要求的旁邊。通知圖示會指出需要您處理的共享要求數目。



- 選擇共享要求。依預設，此頁面會在已接收的要求索引標籤上開啟。
- 尋找帶有藍點的項目，以找出需要執行動作的共享要求。



- (選擇性) 若只要檢視未來 30 天內到期的要求，請尋找所有狀態下拉式清單，然後選取即將到期。

我的共享框架具有使用自定義 AWS Config 規則作為數據源的控件。收件人可以收集這些控制項的證據嗎？

是的，收件人可以收集這些控制的證據，但需要幾個步驟來實現這一目標。

若要讓 Audit Manager 使用 AWS Config 規則作為資料來源對應來收集證據，必須符合下列條件。這些條件同時適用於受管規則和自訂規則。

- 規則必須存在於收件者的 AWS 環境中。
- 此規則必須在收件者的 AWS 環境中啟用。

請記住，您的帳戶中的 AWS Config 規則可能不存在於收件者的 AWS 環境中。此外，當收件者接受共享要求時，Audit Manager 不會在其帳戶中重新建立您的任何自訂規則。若要讓收件者使用您的自訂規則作為資料來源對應來收集證據，他們必須在執行個體中建立相同的自訂規則 AWS Config。收件者在中 [建立並啟用](#) 規則後 AWS Config，Audit Manager 可以從該資料來源收集證據。

我們建議您與收件者通訊，讓他們知道是否應在其執行個體中建立任何自訂 AWS Config 規則 AWS Config。

## 我更新了共享架構中使用的自訂規則。我需要採取任何動作嗎？

### 針對 AWS 環境中的規則更新

當您更新 AWS 環境中的自訂規則時，Audit Manager 中不需要任何動作。Audit Manager 會依照下表所述的方式偵測和處理規則更新。偵測到規則更新時，Audit Manager 不會另行通知。

案例	Audit Manager 會做什麼	您需要執行的事項
自訂規則會在您的執行個體中更新 AWS Config。	Audit Manager 會繼續使用更新的規則定義報告該規則的調查結果。	不需採取任何動作。
自訂規則會在您的執行個體中刪除 AWS Config。	Audit Manager 會停止報告已刪除規則的調查結果。	不需採取任何動作。  如果需要，您可以 <a href="#">編輯自訂控制項</a> ，使用已刪除規則作為資料來源映射項目。然後，您可以移除已刪除的規則，以清除控制項的資料來源設定。否則，刪除的規則名稱會保留為未使用的資料來源映射項目。

### 適用於 AWS 環境外部的規則更新

在收件者的 AWS 環境中，Audit Manager 不會偵測到規則更新。這是因為寄件者和收件者各自在不同的 AWS 環境中工作。下表提供適用於此方案的建議作法。

您的角色	案例	建議的動作
寄件者	<ul style="list-style-type: none"> <li>您共享使用自訂規則作為資料來源映射項目的架構。</li> <li>共用架構之後，您就更新或刪除了中的其中一個規則 AWS Config。</li> </ul>	請連絡收件者，通知他們相關更新。如此一來，他們就可以套用相同的更新，並與最新的規則定義保持同步。
收件人	<ul style="list-style-type: none"> <li>您接受使用自訂規則做為資料來源映射項目的共享架構。</li> <li>在的執行個體中重新建立自訂規則之後 AWS Config，寄件者就會更新或刪除其中一個規則。</li> </ul>	在您自己的 AWS Config 執行個體中進行對應的規則更新。

## 通知問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的通知問題。

### 主題

- [我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知](#)
- [我指定了 FIFO 主題，但沒有依預期順序收到通知](#)

## 我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知

如果您的 Amazon SNS 主題使 AWS KMS 用伺服器端加密 (SSE)，您可能會遺漏 AWS KMS 金鑰政策所需的許可。如果您沒有將一個端點訂閱至主題中，也可能無法收到通知。

如果您沒有收到通知，請確認執行下列作業：

- 您已將所需的許可政策附加至 KMS 金鑰。如需您可以使用的範例原則，請參閱[範例 2 \(添加至 SNS 主題之 KMS 金鑰的許可\)](#)。
- 您訂閱了發送通知的主題的端點。當您訂閱電子郵件端點至主題時，您會收到一封電子郵件，要求您確認訂閱。您必須確認訂閱，才能開始接收電郵通知。如需詳細資訊，請參閱 Amazon SNS 開發人員指南中的[入門](#)。



## 我指定了 FIFO 主題，但沒有依預期順序收到通知

Audit Manager 支援將通知傳送至 FIFO SNS 主題。但是，其無法保證 Audit Manager 會將通知依序傳送至您的 FIFO 主題。

## 權限和存取問題疑難排解

請參考此頁面提供的資訊來解決 Audit Manager 中常見的權限問題。

### 主題

- [我按照 Audit Manager 設定程序進行操作，但我沒有足夠的 IAM 權限](#)
- [我指定某人為稽核擁有者，但他們仍然無法完整存取評估。為什麼？](#)
- [我無法在 Audit Manager 中執行動作](#)
- [我想允許我以外的人員存 AWS 帳戶 取我的 Audit Manager 資源](#)
- [我看到「拒絕存取」錯誤，儘管有必要的 Audit Manager 權限](#)
- [其他資源](#)

## 我按照 Audit Manager 設定程序進行操作，但我沒有足夠的 IAM 權限

您用於存取 Audit Manager 的使用者、角色或群組必須具有所需的權限。除此之外，您的身份驗證政策不應設定的太嚴格。否則，主控台將無法如預期般運作。本指南提供您可以使用的範例原則 [允許啟用 Audit Manager 所需的最低許可](#)。根據您的使用案例，您可能需要更廣泛、更少限制的權限。舉例來說，我們建議稽核擁有者具備 [系統管理員存取權](#)。這樣他們就可以修改 Audit Manager 設定並管理資源，例如評估、架構、控制項和評估報告。其他使用者（例如委派人員）可能只需要 [管理存取權](#) 或 [唯讀存取權](#)。

請務必為您的使用者、角色或群組添加適當的權限。對於稽核擁有者，建議的策略為 [AWSAuditManagerAdministratorAccess](#)。對於代理人，您可以使用 [IAM 政策範例頁面上提供的管理存取範例政策](#)。您可以使用這些範例政策作為起點，並根據您的需求進行必要的變更。

我們建議您花些時間自訂權限，以滿足您的特定需求。如果您需要 IAM 權限相關協助，請聯絡您的管理員或 [AWS 支援人員](#)。

## 我指定某人為稽核擁有者，但他們仍然無法完整存取評估。為什麼？

僅將某人指定為稽核擁有者，並不會提供評估的完整存取權限。稽核擁有者還必須擁有必要的 IAM 權限才能存取和管理 Audit Manager 資源。換句話說，除了將使用者 [指定為稽核擁有者](#) 之外，您還必須

將必要的 [IAM 政策](#) 附加到該使用者上。換句話說，只要同時具備兩者，Audit Manager 確保您可以完全控制每個評估的所有細節。

#### Note

對於稽核擁有者，我們建議您使用 [AWSAuditManagerAdministratorAccess](#) 策略。如需詳細資訊，請參閱 [中使用者角色的建議政策 AWS Audit Manager](#)。

## 我無法在 Audit Manager 中執行動作

如果您沒有使用 AWS Audit Manager 主控台或 Audit Manager API 作業的必要權限，您可能會遇到 `AccessDeniedException` 錯誤訊息。

若要解決此問題，請聯絡管理員以取得協助。您的管理員是為您提供簽署憑證的人員。

## 我想允許我以外的人員存取 AWS 帳戶 取我的 Audit Manager 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 如需了解 Audit Manager 是否支援這些功能，請參閱 [如何與 IAM AWS Audit Manager 搭配使用](#)。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 [IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限](#)。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的 [提供第三方 AWS 帳戶 擁有的存取權](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。

## 我看到「拒絕存取」錯誤，儘管有必要的 Audit Manager 權限

如果您的帳戶是組織的一部分，則 Access Denied 錯誤可能是由 [服務控制策略 \(SCP\)](#) 引起的。SCP 是用來管理組織權限的原則。當 SCP 就位時，它可以拒絕所有成員帳戶的特定權限，包括您在稽核管理員中使用的委派系統管理員帳戶。

例如，如果您的組織有一個拒絕 AWS 控制目錄 API 權限的 SCP，您就無法檢視控制目錄所提供的資源。即使您具有 Audit Manager 所需的權限 (例如 [AWSAuditManagerAdministratorAccess](#) 策略)，也是如此。SCP 會明確拒絕存取控制目錄 API，覆寫受管理原則權限。

下面是這樣一個 SCP 的一個例子。有了這個 SCP，您委派的管理員帳戶就會遭拒絕存取使用 Audit Manager 中的通用控制項功能所需的一般控制項、控制目標和控制網域。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListDomains",
      ],
      "Resource": "*"
    }
  ]
}
```

若要解決這個問題，我們建議您採取下列步驟：

1. 確認 SCP 是否已附加至您的組織。如需指示，請參閱 [AWS Organizations 使用者指南中的取得組織政策的相關資訊](#)。
2. 識別 SCP 是否造成 Access Denied 錯誤。
3. 更新 SCP，以確保您委派的管理員帳戶具有 Audit Manager 員的必要存取權。如需指示，請參閱 [AWS Organizations 使用者指南中的更新 SCP](#)。

## 其他資源

下列頁面提供因缺少權限而可能導致的其他問題的疑難排解指南：

- [我在評估中看不到任何控制項或控制集](#)
- [當我設定控制項資料來源時，無法使用自訂規則選項](#)
- [當我嘗試生成報告時，出現存取被拒絕的錯誤](#)
- [當我嘗試使用委派系統管理員帳戶產生評估報告時，出現存取遭拒的錯誤](#)
- [我無法啟用證據搜尋工具](#)
- [我無法停用證據搜尋工具](#)
- [我的搜尋查詢失敗](#)
- [我在 Audit Manager 中指定了 Amazon SNS 主題，但沒有收到任何通知](#)

# 標記 AWS Audit Manager 資源

標籤是您指派或指派給 AWS 資源的 AWS 中繼資料標籤。每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義鍵與值。例如，您可以將鍵定義為 `stage`，將資源的值定義為 `test`。

標籤可協助您執行以下操作：

- 輕鬆找到您的 Audit Manager 資源。瀏覽架構程式庫和控制項程式庫時，您可以將標籤用作搜尋條件。
- 將您的資源與合規類型建立關聯。您可以使用合規特定標籤來標記多個資源，以便將這些資源與特定架構建立關聯。
- 識別和組織您的 AWS 資源。許多 AWS 服務支持標記，因此您可以為來自不同服務的資源分配相同的標籤，以指示資源是相關的。
- 追蹤您的 AWS 成本。您可以在 AWS Billing and Cost Management 儀表板上啟用這些標籤。AWS 使用標籤來分類您的成本，並提供每月成本分配報告給您。如需詳細資訊，請參閱 AWS Billing and Cost Management 使用者指南中的 [使用成本配置標籤](#)。

以下各節提供有關的標籤的詳細資訊 AWS Audit Manager。

## 內容

- [Audit Manager 中支援的資源](#)
- [標籤限制](#)
- [其他資源](#)

## Audit Manager 中支援的資源

下列 Audit Manager 資源支援標記：

- 評估
- 控制
- 架構

## 標籤限制

下列基本限制適用於 Audit Manager 資源上的標籤：

- 您可以指派給資源的標籤數量上限：50
- 索引鍵長度上限：128 個 Unicode 字元
- 數值長度上限：256 個 Unicode 字元
- 鍵與值的有效字元：a-z、A-Z、0-9、空格和下列字元：\_ . : / = + - 及 @
- 鍵和值會區分大小寫
- 不要用aws:作密鑰的前綴；它保留供 AWS 使用

## 其他資源

您可以在建立評估、架構或控制項時將標籤設定為屬性。您可以透過稽核管理員主控台、AWS Command Line Interface (AWS CLI) 和稽核管理員 API 新增、編輯和刪除標籤。如需詳細資訊，請參閱下列連結：

- 對於標記評估：
  - [在中建立評估 AWS Audit Manager](#) 和 [編輯評量 AWS Audit Manager](#) 見本指南的評估區段
  - [標籤索引標籤](#)在本指南的「檢閱評量」頁
  - [CreateAssessment](#)並[UpdateAssessment](#)在 AWS Audit Manager API 參考中
  - [TagResource](#)並[UntagResource](#)在 AWS Audit Manager API 參考中
- 對於標記框架：
  - [在中建立自訂架構 AWS Audit Manager](#) 和 [編輯自訂架構 AWS Audit Manager](#) 見本指南的架構程式庫區段
  - [Tags tab](#)在本指南的「查看框架詳細信息」頁面上
  - [CreateAssessmentFramework](#)並[UpdateAssessmentFramework](#)在 AWS Audit Manager API 參考中
  - [TagResource](#)並[UntagResource](#)在 AWS Audit Manager API 參考中
- 對於標籤控制項：
  - [在中建立自訂控制項 AWS Audit Manager](#) 和 [編輯中的自訂控制項 AWS Audit Manager](#) 見本指南的控制項程式庫區段
  - 本指南 [檢閱自訂控制項] 頁面上的章[Tags](#)節

- 本指南 [Tags](#) 「檢閱標準控制項」頁面上的章節
- [CreateControl](#)並[UpdateControl](#)在 AWS Audit Manager API 參考中
- [TagResource](#)並[UntagResource](#)在 AWS Audit Manager API 參考中

# 了解配額和限制 AWS Audit Manager

您的每個配額都 AWS 帳戶 有預設配額 (先前稱為限制) AWS 服務。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，而其他配額無法提高。

大多數 Audit Manager 配額 (但不是全部) 都會列在 Service Quotas 主控台的 AWS Audit Manager 命名空間下。如需要增加配額，請參閱 [管理您的 Audit Manager 配額](#)。

## 內容

- [預設 Audit Manager 配額](#)
- [管理您的 Audit Manager 配額](#)
- [其他資源](#)

## 預設 Audit Manager 配額

以下是 AWS 帳戶 每個區域的 AWS Audit Manager 配額。

資源	配額
評估	每個帳戶的使用中評估數量：100
評估報告	您可以新增至評估報告的證據項目數量： <ul style="list-style-type: none"><li>• 相同區域報告 (評估和評估報告目的地 S3 儲存貯體位於相同 AWS 區域)：22,000</li><li>• 跨區域報告 (評估和評估報告目的地 S3 儲存貯體位於不同 AWS 區域)：3,500</li><li>• 對於相關評估使用客戶管理的報表 AWS KMS key：3,500</li></ul>
控制	每個帳戶的自訂控制項數量：500
证据	單個手動證據檔案的大小上限：100 MB 每個控制項的每日手動證據上傳數量：100



資源	配額
	<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p><b>i</b> Tip</p> <p>如果您需要將大量手動證據上傳至單一控制項，建議您在數天內分批上傳證據。</p> </div>
架構	<p>每個帳戶的自訂架構數量：100</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p><b>i</b> Note</p> <p>不論架構是誰建立的，架構配額會套用至架構程式庫中所有共享的自訂架構。</p> </div>
共用自訂架構收件者	使用中的收件人帳戶數量：100
API 存取權	所有 API 的每秒交易次數 (TPS)：20 TPS

## 管理您的 Audit Manager 配額

AWS Audit Manager 與「Service Quotas」整合 AWS 服務，可讓您從中央位置檢視和管理配額。Service Quotas 可讓您輕鬆查詢 Amazon Manager 配額的值。

使用主控台來檢視 Audit Manager Service Quotas

1. 開啟 Service Quotas 主控台，網址為 <https://console.aws.amazon.com/servicequotas/>。
2. 在導覽窗格中，選擇 AWS 服務。
3. 從 AWS 服務清單中，搜尋並選取 AWS Audit Manager。
4. 在 [服務配額] 清單中，您可以看到服務配額名稱、套用的配額值 (如果有的話)、AWS 預設配額值，以及配額是否可調整。
5. 若要檢視服務配額的其他資訊 (例如說明)，請選擇配額名稱。
6. (選用) 若要請求增加配額，請選取您要增加的配額、選取 Request quota increase (請求增加配額)、輸入或選取必要資訊，然後選取 Request (請求)。

## 其他資源

如需如何管理配額的詳細資訊，[請參閱《Service Quotas 使用者指南》中的要求增加配額。](#)

如需有關 Service Quotas 的詳細資訊，請參閱[什麼是 Service Quotas？](#) 在 Service Quotas 使用指南中。

# 瞭解中的安全性和資料保護 AWS Audit Manager

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在雲 AWS 端 AWS 服務 中執行的基礎架構。AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Audit Manager，請參閱[合規計劃的 AWS 服務範圍](#)範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的資料。AWS 服務 您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Audit Manager。下列主題說明如何將 Audit Manager 設定為達到您的安全及合規目標。您也會學到如何使用其 AWS 服務 他協助您監視和保護 Audit Manager 資源的其他資源。

## 主題

- [資料保護 AWS Audit Manager](#)
- [的身分識別與存取管理 AWS Audit Manager](#)
- [符合性驗證 AWS Audit Manager](#)
- [了解彈性 AWS Audit Manager](#)
- [基礎結構安全 AWS Audit Manager](#)
- [AWS Audit Manager 和介面 VPC 端端點 \(\)AWS PrivateLink](#)
- [登錄和監控 AWS Audit Manager](#)
- [了解中的配置和漏洞分析 AWS Audit Manager](#)

## 資料保護 AWS Audit Manager

AWS [共用責任模型](#)適用於中的資料保護 AWS Audit Manager。如此模型中所述，AWS 負責保護執行所有 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用 Audit Manager 或其他人時。AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

除此之外，我們特別建議 Audit Manager 客戶在建立評估、自訂控制項、自訂架構和委派評論時，不要在自由格式欄位中包含敏感識別資訊。

## 刪除 Audit Manager 資料

有幾種方法可以刪除 Audit Manager 資料。

### 停用 Audit Manager 時的資料刪除

[停用 Audit Manager](#) 時，您可以決定是否要刪除所有 Audit Manager 資料。如果您選擇刪除資料，資料會在停用 Audit Manager 後的 7 天內刪除。刪除資料後，您就無法復原。

### 自動刪除資料

某些 Audit Manager 資料會在特定時間後自動刪除。Audit Manager 會保留以下客戶資料。

資料類型	資料保留期間	備註
證據	資料會自建立之日起保留兩年。	包括自動化證據和手動證據

資料類型	資料保留期間	備註
客戶建立的資源	資料會無限期保留	包括評估、評估報告、自訂控制項和自訂架構

## 手動刪除資料

您可以隨時刪除單項 Audit Manager 資源。如需詳細說明，請參閱下列主題：

- [刪除中的評估 AWS Audit Manager](#)
  - 另請參閱：[DeleteAssessment](#)在 AWS Audit Manager API 參考
- [刪除中的自定義框架 AWS Audit Manager](#)
  - 另請參閱：[DeleteAssessmentFramework](#)在 AWS Audit Manager API 參考
- [刪除共用要求 AWS Audit Manager](#)
  - 另請參閱：[DeleteAssessmentFrameworkShare](#)在 AWS Audit Manager API 參考
- [刪除評估報告](#)
  - 另請參閱：[DeleteAssessmentReport](#)在 AWS Audit Manager API 參考
- [刪除中的自訂控制項 AWS Audit Manager](#)
  - 另請參閱：[DeleteControl](#)在 AWS Audit Manager API 參考

如需刪除您在使用 Audit Manager 時可能已建立的其他資源資料，請參閱下列內容：

- AWS CloudTrail 使用者指南中，[刪除事件資料存放區](#)
- Amazon Simple Storage Service (Amazon S3) 使用者指南中的[刪除儲存貯體](#)

## 靜態加密

AWS 受管金鑰 為了加密靜態資料，Audit Manager 會針對其所有資料存放區和記錄使用伺服器端加密。

您的資料會以客戶管理的金鑰加密 AWS 擁有的金鑰，或根據您選取的設定而定。如果您未提供客戶管理的金鑰，Audit Manager 會使用 AWS 擁有的金鑰 來加密您的內容。Audit Manager 中的所有 DynamoDB 和 Amazon S3 服務中繼資料透過 AWS 擁有的金鑰加密。

Audit Manager 會依下列方式加密資料：

- 存放在 Amazon S3 中的服務中繼資料會 AWS 擁有的金鑰使用 SSE-KMS 加密。
- 儲存在 DynamoDB 中的服務中繼資料使用 KMS 和 AWS 擁有的金鑰進行伺服器端加密。
- 您儲存在 DynamoDB 中的內容使用客戶管理金鑰或 AWS 擁有的金鑰進行用戶端加密。KMS 金鑰根據您選擇的設定而定。
- 您存放在 Audit Manager Amazon S3 中的內容使用 SSE-KMS 加密。KMS 金鑰根據您的選擇而定，可以是客戶管理金鑰或 AWS 擁有的金鑰。
- 發佈到 S3 儲存貯體的評估報告會進行以下加密：
  - 如果您提供客戶管理金鑰，您的資料會使用 SSE-KMS 加密。
  - 如果您使用 AWS 擁有的金鑰，則您的資料會使用 SSE-S3 加密。

## 傳輸中加密

Audit Manager 會提供安全且私有的端點，以供您加密傳輸中的資料。安全和私有端點允許 AWS 保護對 Audit Manager 的 API 請求的完整性。

### 跨服務傳輸

根據預設，所有服務間通訊皆受到 Transport Layer Security (TLS) 加密的保護。

## 金鑰管理

Audit Manager 支援 AWS 擁有的金鑰和客戶受管金鑰，以加密所有 Audit Manager 資源 (儲存到帳戶中 S3 儲存貯體的評估、控制項、架構、證據和評估報告)。

建議您使用客戶管理金鑰。如此一來，您就可以檢視和管理用來保護資料的加密金鑰，包括在 AWS CloudTrail 中檢視其使用日誌。選擇客戶管理金鑰時，Audit Manager 會針對 KMS 金鑰建立一個授權，以便可以用於加密您的內容。

### Warning

刪除或禁用用於加密 Audit Manager 資源的 KMS 金鑰之後，您就再也無法解密以該 KMS 金鑰加密的資源，這表示該資料已無法復原。

在 AWS Key Management Service (AWS KMS) 中刪除 KMS 金鑰具有破壞性且具有潛在危險性。如需有關刪除 KMS 金鑰的詳細資訊，請參閱 AWS Key Management Service 使用者手冊 AWS KMS keys 中的 [刪除](#)。

當您使用稽核管理員 API 或 AWS Command Line Interface (AWS CLI) 啟用 Audit Manager Audit Manager 時，您可以指定加密設定。AWS Management Console 如需說明，請參閱[啟用 AWS Audit Manager](#)。

您可以隨時檢閱和變更您的加密設定。如需說明，請參閱[設定您的資料加密設定](#)。

如需如何設定客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 使用者指南中的[建立金鑰](#)。

## 的身分識別與存取管理 AWS Audit Manager

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員可以控制誰能完成身分驗證 (登入) 和獲得授權 (取得許可)，而得以使用 Audit Manager 資源。IAM 是您可以使用的 AWS 服務，無需額外付費。

### 主題

- [物件](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [如何與 IAM AWS Audit Manager 搭配使用](#)
- [以身分識別為基礎的原則範例 AWS Audit Manager](#)
- [預防跨服務混淆代理人](#)
- [AWS 受管理的政策 AWS Audit Manager](#)
- [疑難排解 AWS Audit Manager 身分和存取](#)
- [使用服務連結角色 AWS Audit Manager](#)

## 物件

根據您在 Audit Manager 中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 Audit Manager 服務執行工作，管理員會為您提供所需的憑證和許可。隨著您為了執行作業而使用的 Audit Manager 功能數量變多，您可能會需要額外的許可。了解存取許可的

管理方式可協助您向管理員請求正確的許可。若您無法存取 Audit Manager 中的某項功能，請參閱 [疑難排解 AWS Audit Manager 身分和存取](#)。

**服務管理員** — 如果您負責公司的 Audit Manager 資源，您可能具備 Audit Manager 的完整存取權。您的任務是判斷服務使用者應存取的 Audit Manager 功能及資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。如需進一步了解貴公司可搭配 Audit Manager 使用 IAM 的方式，請參閱 [如何與 IAM AWS Audit Manager 搭配使用](#)。

**IAM 管理員**：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 Audit Manager 存取權的詳細資訊。如需檢視您可以在 IAM 中使用的 Audit Manager 身分型政策範例，請參閱 [以身分識別為基礎的原則範例 AWS Audit Manager](#)。

## 使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 [AWS 登入 使用者指南中的如何登入您 AWS 帳戶](#)的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的 [簽署 AWS API 請求](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [多重要素驗證](#)和 IAM 使用者指南中的 [在 AWS 中使用多重要素驗證 \(MFA\)](#)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的 [需要根使用者憑證的任務](#)。



## 聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identity Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。AWS Directory Service 同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 [AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center ?](#)。

## IAM 使用者和群組

[IAM 使用者](#)是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱IAM 使用者指南中的[建立 IAM 使用者 \(而非角色\) 的時機](#)。

## IAM 角色

[IAM 角色](#)是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以[切換角色，在中暫時擔任 IAM 角色](#)。AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的[使用 IAM 角色](#)。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 [IAM 使用者指南](#)中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，

則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的[IAM 中的跨帳戶資源存取](#)。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的策略詳細資訊，請參閱[《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的[IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的[建立角色以委派許可給 AWS 服務服務](#)。
- 服務連結角色 — 服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的[利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的[建立 IAM 角色 \(而非使用者\) 的時機](#)。

## 使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS，當與身分識別或資源相關聯時，會定義其權限。AWS 當主參與者 (使用者、root 使用者或角色

工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 [JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console、AWS CLI、或 AWS API 取得角色資訊。

## 身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的 [建立 IAM 政策](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶。受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的 [在受管政策和內嵌政策間選擇](#)。

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中 [指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。AWS WAF 如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的 [存取控制清單 \(ACL\) 概觀](#)。

## 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- **許可界限** – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 [IAM 實體許可界限](#)。
- **服務控制策略 (SCP)** — SCP 是 JSON 策略，用於指定中組織或組織單位 (OU) 的最大權限。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 [SCP 運作方式](#)。
- **工作階段政策** – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的 [工作階段政策](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

## 如何與 IAM AWS Audit Manager 搭配使用

在您使用 IAM 管理 Audit Manager 的存取權之前，請了解搭配 Audit Manager 使用的 IAM 功能有哪些。

您可以搭配使用的 IAM 功能 AWS Audit Manager

IAM 功能	Audit Manager 報告
<a href="#">身分型政策</a>	是

IAM 功能	Audit Manager 報告
<a href="#">資源型政策</a>	否
<a href="#">政策動作</a>	是
<a href="#">政策資源</a>	是
<a href="#">政策條件索引鍵</a>	部分
<a href="#">ACL</a>	否
<a href="#">ABAC (政策中的標籤)</a>	是
<a href="#">臨時憑證</a>	是
<a href="#">轉送存取工作階段 (FAS)</a>	是
<a href="#">服務角色</a>	否
<a href="#">服務連結角色</a>	是

若要深入瞭解如何以 AWS Audit Manager 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的[搭配 IAM 使用的 AWS 服務](#)。

## 以身分識別為基礎的原則 AWS Audit Manager

支援身分型政策	是
---------	---

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素參考](#)。

AWS Audit Manager 會建立為稽核管理員管理員命名 `AWSAuditManagerAdministratorAccess` 的受管理策略。此政策會授予稽核管理員中的完整管理存取權。管理員可以將此政策附加至任何現有的角色或使用者，或使用此政策建立新角色。

### 中使用者角色的建議政策 AWS Audit Manager

AWS Audit Manager 可讓您使用不同的 IAM 政策，維護不同使用者之間的職責隔離，以及針對不同稽核。Audit Manager 中的兩個角色及其建議政策的定義如下。

角色	描述和建議政策
稽核擁有者	<ul style="list-style-type: none"> <li>此角色必須具有管理中 AWS Audit Manager 評量的必要權限。</li> <li>建議用於此角色的受管理策略是名 <a href="#">AWSAuditManagerAdministratorAccess</a> 為的受管理策略。您可以使用此政策作為起點，根據需要縮小這些許可的範圍。</li> </ul>
委派代表	<ul style="list-style-type: none"> <li>此角色可存取評估中委派的控制集。可以更新控制項狀態、添加評論、提交控制集以供審核，以及將證據添加至評估報告。</li> <li>建議用於此角色的政策為下列範例政策：<a href="#">授予使用者 AWS Audit Manager 管理存取權</a>。您可以使用此政策作為起點，根據您的需求進行必要的變更。</li> </ul>

### 以身分識別為基礎的原則範例 AWS Audit Manager

如需檢視 Audit Manager 身分型政策範例，請參閱 [以身分識別為基礎的原則範例 AWS Audit Manager](#)。

### 以資源為基礎的政策 AWS Audit Manager

支援以資源基礎的政策 否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中 [指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信

任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南 [中的 IAM 中的跨帳戶資源存取](#)。

## 的政策動作 AWS Audit Manager

支援政策動作 是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Audit Manager 動作清單，請參閱服務授權參考中的 [AWS Audit Manager 定義的動作](#)。

中的策略動作在動作之前 AWS Audit Manager 使用下列前置詞。

```
auditmanager
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
  "auditmanager:GetEvidenceDetails",  
  "auditmanager:GetEvidenceEventDetails"  
]
```

您也可以使用萬用字元 (\*) 來指定多個動作。例如，如需指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "auditmanager:Get*"
```

如需檢視 Audit Manager 身分型政策範例，請參閱 [以身分識別為基礎的原則範例 AWS Audit Manager](#)。

## 的政策資源 AWS Audit Manager

支援政策資源 是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示陳述式適用於所有資源。

```
"Resource": "*" 
```

若要查看 AWS Audit Manager 資源類型及其 ARN 的清單，請參閱服務授權參考中的 [AWS Audit Manager 定義的資源](#)。如需了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Audit Manager 定義的動作](#)。

Audit Manager 的評估具有以下 Amazon Resource Name (ARN) 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Audit Manager 控制集具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/  
${assessmentId}controlSet/${controlSetId}
```

Audit Manager 控制項具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

如需 ARN 格式的詳細資訊，請參閱 [Amazon Resource Name \(ARN\)](#)。



例如，如需在陳述式中指定 `i-1234567890abcdef0` 評估，請使用下列 ARN。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/i-1234567890abcdef0"
```

如需指定屬於特定帳戶的所有執行個體，請使用萬用字元 (\*)。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

有些 Audit Manager 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (\*)。

```
"Resource": "*"
```

許多 Audit Manager API 動作都涉及多個資源。例如，`ListAssessments` 傳回目前登入者可存取的評估中繼資料清單 AWS 帳戶。因此，使用者必須具有檢視評估的許可。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [  
    "resource1",  
    "resource2"
```

如需查看 Audit Manager 資源類型及其 ARN 的清單，請參閱 IAM 使用者指南中的 [AWS Audit Manager 定義的資源](#)。如需了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Audit Manager 定義的動作](#)。

部分 Audit Manager API 動作支援多個資源。例如，`GetChangeLogs` 存取 `assessmentID`、和 `controlID` 和 `controlSetId`，因此主體必須具有存取這些資源的許可。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [  
    "assessmentId",  
    "controlId",  
    "controlSetId"
```

## 的政策條件索引鍵 AWS Audit Manager

支援服務特定政策條件金鑰

部分

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用[條件運算子](#)的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯 OR 運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

當政策陳述式中的主體是 [AWS 服務主體](#) 時，強烈建議您使用政策中的 [aws:SourceArn](#) 或 [aws:SourceAccount](#) 全域條件索引鍵。您可以使用這些全域條件內容索引鍵來協助防止[混淆代理人案例](#)。下列記錄的政策示範如何使用 Audit Manager 中的 [aws:SourceArn](#) 和 [aws:SourceAccount](#) 全域條件內容索引鍵，來預防混淆代理人問題。

- [用於 Audit Manager 通知的 SNS 主題範例政策](#)
- [與 SNS 主題搭配使用的 KMS 金鑰範例政策](#)

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其使用者名稱標記時，將存取資源的許可授予該使用者。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

Audit Manager 不提供任何服務專用條件索引鍵，但它支援一些全域條件索引鍵的使用。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容金鑰](#)。

## AWS Audit Manager 中的存取控制清單 (ACL)

支援 ACL	否
--------	---

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

## 以屬性為基礎的存取控制 (ABAC) 搭配 AWS Audit Manager

支援 ABAC (政策中的標籤)	是
------------------	---

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱 IAM 使用者指南中的 [什麼是 ABAC?](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的 [使用屬性型存取控制 \(ABAC\)](#)。

如需標記 AWS Audit Manager 資源的更多資訊，請參閱 [標記 AWS Audit Manager 資源](#)。

## 使用臨時登入資料 AWS Audit Manager

支援臨時憑證 是

當您使用臨時憑據登錄時，某些 AWS 服務不起作用。如需其他資訊，包括哪些 AWS 服務與臨時登入資料 [搭配 AWS 服務使用](#)，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的 [切換至角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

## 轉寄存存取工作階段 AWS Audit Manager

支援轉寄存存取工作階段 (FAS) 是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求

AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。

## AWS Audit Manager的服務角色

支援服務角色	否
--------	---

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立角色以委派許可給 AWS 服務服務](#)。

### Warning

變更服務角色的許可有可能會讓 AWS Audit Manager 功能出現故障。只有 Audit Manager 提供指引時，才能編輯服務角色。

## 服務連結角色 AWS Audit Manager

支援服務連結角色	是
----------	---

服務連結角色是一種連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關的服務連結角色的詳細資訊 AWS Audit Manager，請參閱 [使用服務連結角色 AWS Audit Manager](#)。

## 以身分識別為基礎的原則範例 AWS Audit Manager

根據預設，使用者和角色不具備建立或修改 Audit Manager 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的 [建立 IAM 政策](#)。

如需 AWS Audit Manager 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的[適用 AWS Audit Manager 的動作、資源和條件索引鍵](#)。

## 內容

- [政策最佳實務](#)
- [允許啟用 Audit Manager 所需的最低許可](#)
- [授予使用者 AWS Audit Manager 的完整管理員存取權](#)
  - [範例 1 \(受管政策, AWSAuditManagerAdministratorAccess\)](#)
  - [範例 2 \(評估報表目的地許可\)](#)
  - [範例 3 \(匯出目的地許可\)](#)
  - [範例 4 \(啟用證據搜尋工具的許可\)](#)
  - [範例 5 \(停用證據搜尋工具的許可\)](#)
- [授予使用者 AWS Audit Manager 管理存取權](#)
- [允許使用者唯讀存取 AWS Audit Manager](#)
- [允許使用者檢視他們自己的許可](#)
- [允許 AWS Audit Manager 傳送通知給 Amazon SNS 主題](#)
  - [範例 1 \(SNS 主題的許可\)](#)
  - [範例 2 \(添加至 SNS 主題之 KMS 金鑰的許可\)](#)
- [允許使用者在證據搜尋工具中執行搜索查詢](#)

## 政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Audit Manager 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的 AWS 受管理原則。它們在您的 AWS 帳戶。建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的[AWS 受管政策](#)或[任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的[IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動

作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM Access Analyzer 政策驗證](#)。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

## 允許啟用 Audit Manager 所需的最低許可

此範例會示範如何允許不具有管理員角色的帳戶啟用 AWS Audit Manager。

### Note

我們在此提供的是基本政策，可授予啟用 Audit Manager 所需的最低許可。以下政策中的所有許可均屬必要許可。您不得省略此政策的任何部分，否則，您將無法啟用 Audit Manager。我們建議您花時間自訂權限，以滿足您的特定需求。如需任何協助，請聯絡您的管理員或 [Amazon Web Services Support](#)。

如需授予啟用 Audit Manager 所需的最低存取權，請使用下列許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "auditmanager:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
```

```

        "iam:AWSServiceName": "auditmanager.amazonaws.com"
    }
}
},
{
    "Sid": "CreateEventsAccess",
    "Effect": "Allow",
    "Action": [
        "events:PutRule"
    ],
    "Resource": "*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "events:source": [
                "aws.securityhub"
            ]
        }
    }
},
{
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
        "events:PutTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
},
{
    "Effect": "Allow",
    "Action": "kms:ListAliases",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "auditmanager.amazonaws.com"
        }
    }
}
]
}

```

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合您嘗試執行之 API 作業的動作就可以了。

## 授予使用者 AWS Audit Manager 的完整管理員存取權

下列範例原則會授與對的完整管理員存取權 AWS Audit Manager。

- [範例 1 \(受管政策, `AWSAuditManagerAdministratorAccess`\)](#)
- [範例 2 \(評估報表目的地許可\)](#)
- [範例 3 \(匯出目的地許可\)](#)
- [範例 4 \(啟用證據搜尋工具的許可\)](#)
- [範例 5 \(停用證據搜尋工具的許可\)](#)

### 範例 1 (受管政策, `AWSAuditManagerAdministratorAccess`)

該 `AWSAuditManagerAdministratorAccess` 策略包括啟用和停用 Audit Manager 的功能、變更 Audit Manager 設定的能力，以及管理所有稽核管理員資源 (例如評估、架構、控制項和評估報告) 的能力。

### 範例 2 (評估報表目的地許可)

此政策授予您存取特定 S3 儲存貯體，以及在其中添加檔案和刪除檔案的許可。因此，您可使用指定的儲存貯體作為 Audit Manager 中的評估報告目的地。

以您自己的資訊取代#####。包括用作評估報告目的地的 S3 儲存貯體，以及用於加密評估報告的 KMS 金鑰。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
    }
  ]
},
{
```



```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
]
}

```

### 範例 3 (匯出目的地許可)

下列政策允許 CloudTrail 將證據尋找器查詢結果傳遞至指定的 S3 儲存貯體。作為安全性最佳實務，IAM 全域條件金鑰 `aws:SourceArn` 有助於確保僅針對事件資料存放區 CloudTrail 寫入 S3 儲存貯體。

以您自己的資訊取代 #####，如下所示：

- 將 `DOC-EXAMPLE-DESTINATION-BUCKET` 取代為您用作匯出目的地的 S3 儲存貯體。
- 將 `[myQueryRunning##]` 取代 AWS 區域 為適合您組態的 [區域]。
- 將我的 `## AWS ## ID` 取代為使用的識別碼。CloudTrail 此 ID 可能不同於 S3 儲存貯體的 AWS 帳戶 ID。如果這是組織事件資料存放區，您必須使 AWS 帳戶 用管理帳戶。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource": [

```

```

        "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
        "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
    ],
    "Condition": {
        "StringEquals": {
            "AWS:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
    }
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
    "Condition": {
        "StringEquals": {
            "AWS:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
    }
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt*",
        "kms:GenerateDataKey*"
    ],
}

```

```

        "Resource": "*"
    }
]
}

```

#### 範例 4 (啟用證據搜尋工具的許可)

如需啟用和使用證據搜尋工具功能，則需要以下許可政策。此原則陳述式可讓 Audit Manager 建立 CloudTrail Lake 事件資料存放區並執行搜尋查詢。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageCloudTrailLakeQueryAccess",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:DescribeQuery",
        "cloudtrail:GetQueryResults",
        "cloudtrail:CancelQuery"
      ],
      "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
    },
    {
      "Sid": "ManageCloudTrailLakeAccess",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:CreateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
    }
  ]
}

```

#### 範例 5 (停用證據搜尋工具的許可)

此範例政策授予在 Audit Manager 中停用證據搜尋工具功能的許可。這涉及刪除您第一次啟用該功能時建立的事件資料存放區。

使用此政策前，請將#####取代為您的資訊。您應該指定啟用證據搜尋工具時建立的事件資料存放區的 UUID。您可以從 Audit Manager 設定中擷取事件資料存放區的 ARN。如需詳細資訊，請參閱 AWS Audit Manager API 參考[GetSettings](#)中的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DeleteEventDataStore",
        "cloudtrail:UpdateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail::event-data-store-UUID"
    }
  ]
}
```

## 授予使用者 AWS Audit Manager 管理存取權

此範例會示範如何授予非管理員 AWS Audit Manager 管理存取權。

此策略授予管理所有 Audit Manager 資源 (評估、架構和控制項) 的能力，但不授予啟用或停用 Audit Manager 或修改 Audit Manager 設定的能力。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:AssociateAssessmentReportEvidenceFolder",
        "auditmanager:BatchAssociateAssessmentReportEvidence",
        "auditmanager:BatchCreateDelegationByAssessment",
        "auditmanager:BatchDeleteDelegationByAssessment",
        "auditmanager:BatchDisassociateAssessmentReportEvidence",
        "auditmanager:BatchImportEvidenceToAssessmentControl",
        "auditmanager:CreateAssessment",
        "auditmanager:CreateAssessmentFramework",
        "auditmanager:CreateAssessmentReport",
        "auditmanager:CreateControl",
        "auditmanager>DeleteControl",
        "auditmanager>DeleteAssessment",
        "auditmanager>DeleteAssessmentFramework",
        "auditmanager>DeleteAssessmentFrameworkShare",
        "auditmanager>DeleteAssessmentReport",

```

```
"auditmanager:DisassociateAssessmentReportEvidenceFolder",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:GetAssessmentFramework",
"auditmanager:GetControl",
"auditmanager:GetServicesInScope",
"auditmanager:GetSettings",
"auditmanager:GetAssessmentReportUrl",
"auditmanager:GetChangeLogs",
"auditmanager:GetDelegations",
"auditmanager:GetEvidence",
"auditmanager:GetEvidenceByEvidenceFolder",
"auditmanager:GetEvidenceFileUploadUrl",
"auditmanager:GetEvidenceFolder",
"auditmanager:GetEvidenceFoldersByAssessment",
"auditmanager:GetEvidenceFoldersByAssessmentControl",
"auditmanager:GetInsights",
"auditmanager:GetInsightsByAssessment",
"auditmanager:GetOrganizationAdminAccount",
"auditmanager:ListAssessments",
"auditmanager:ListAssessmentReports",
"auditmanager:ListControls",
"auditmanager:ListKeywordsForDataSource",
"auditmanager:ListNotifications",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentFrameworkShareRequests",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListTagsForResource",
"auditmanager:StartAssessmentFrameworkShare",
"auditmanager:TagResource",
"auditmanager:UntagResource",
"auditmanager:UpdateControl",
"auditmanager:UpdateAssessment",
"auditmanager:UpdateAssessmentControl",
"auditmanager:UpdateAssessmentControlSetStatus",
"auditmanager:UpdateAssessmentFramework",
"auditmanager:UpdateAssessmentFrameworkShare",
"auditmanager:UpdateAssessmentStatus",
"auditmanager:ValidateAssessmentReportIntegrity"
],
"Resource": "*"

```

```
    },
    {
      "Sid": "ControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsAccess",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMAccess",
      "Effect": "Allow",
      "Action": [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3Access",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
```

```

        "Sid": "KmsAccess",
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:ListKeys",
            "kms:ListAliases"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SNSAccess",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "TagAccess",
        "Effect": "Allow",
        "Action": [
            "tag:GetResources"
        ],
        "Resource": "*"
    }
]
}

```

## 允許使用者唯讀存取 AWS Audit Manager

此原則授予評估、架構和控制等 AWS Audit Manager 資源的唯讀存取權。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:Get*",
        "auditmanager:List*"
      ],
      "Resource": "*"
    }
  ]
}

```

```
    }  
  ]  
}
```

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "ViewOwnUserInfo",  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetUserPolicy",  
        "iam:ListGroupsWithUser",  
        "iam:ListAttachedUserPolicies",  
        "iam:ListUserPolicies",  
        "iam:GetUser"  
      ],  
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]  
    },  
    {  
      "Sid": "NavigateInConsole",  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetGroupPolicy",  
        "iam:GetPolicyVersion",  
        "iam:GetPolicy",  
        "iam:ListAttachedGroupPolicies",  
        "iam:ListGroupPolicies",  
        "iam:ListPolicyVersions",  
        "iam:ListPolicies",  
        "iam:ListUsers"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```



## 允許 AWS Audit Manager 傳送通知給 Amazon SNS 主題

此範例中的政策授予 Audit Manager 傳送通知到現有 Amazon SNS 主題的許可。

- [範例 1](#) — 如果您想要接收來自 Audit Manager 的通知，請使用此範例將權限新增至您的 SNS 主題存取原則。
- [範例 2](#) — 如果您的 SNS 主題使用 AWS Key Management Service (AWS KMS) 進行伺服器端加密 (SSE)，請使用此範例將權限新增至 KMS 金鑰存取原則。

在下列政策中，取得許可的主體是 Audit Manager 服務主體，即 `auditmanager.amazonaws.com`。當政策陳述式中的主體是 [AWS 服務主體](#) 時，強烈建議您使用政策中的 [aws:SourceArn](#) 或 [aws:SourceAccount](#) 全域條件索引鍵。您可以使用這些全域條件內容索引鍵來協助防止[混淆代理人案例](#)。

### 範例 1 (SNS 主題的許可)

此政策陳述式允許 Audit Manager 將事件發佈至特定 SNS 主題。任何發佈至指定 SNS 主題的要求都必須符合政策條件。

使用此政策前，請將#####取代為您的資訊。謹記下列事項：

- 如果您在此政策中使用 `aws:SourceArn` 條件索引鍵，則該值必須是通知來源之 Audit Manager 資源的 ARN。在以下範例中，`aws:SourceArn` 使用萬用字元 (\*) 作為資源 ID。這允許對所有 Audit Manager 資源進行來自 Audit Manager 的所有請求。透過 `aws:SourceArn` 全域條件索引鍵，您可以使用 `StringLike` 或 `ArnLike` 條件運算子。最佳實務建議您使用 `ArnLike`。
- 透過 [aws:SourceAccount](#) 條件索引鍵，您可以使用 `StringEquals` 或 `StringLike` 條件運算子。最佳作法是，建議您使用 `StringEquals` 來實作最低權限。
- 如果您同時使用 `aws:SourceAccount` 和 `aws:SourceArn`，帳戶值必須顯示相同的帳戶 ID。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowAuditManagerToUseSNSTopic",
    "Effect": "Allow",
    "Principal": {
      "Service": "auditmanager.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:region:accountID:topicName",
```

```

    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountID"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
      }
    }
  }
}

```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceArn 條件索引鍵：

```

"Condition": {
  "StringLike": {
    "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
  }
}

```

透過 StringLike 條件運算子，下列替代範例僅使用 aws:SourceAccount 條件索引鍵：

```

"Condition": {
  "StringLike": {
    "aws:SourceAccount": "accountID"
  }
}

```

## 範例 2 (添加至 SNS 主題之 KMS 金鑰的許可)

政策陳述式允許 Audit Manager 使用 KMS 金鑰 [產生資料金鑰](#)，它可用來加密 SNS 主題。針對指定操作使用 KMS 金鑰的任何請求都必須滿足政策條件。

使用此政策前，請將#####取代為您的資訊。謹記下列事項：

- 如果您在此政策中使用 aws:SourceArn 條件索引鍵，則值必須是正在加密之資源的 ARN。例如，在這種情況下，它是您帳戶中的 SNS 主題。將值設定為 ARN 或具有萬用字元 (\*) 的 ARN 模式。透過 aws:SourceArn 條件索引鍵，您可以使用 StringLike 或 ArnLike 條件運算子。最佳實務建議您使用 ArnLike。
- 透過 aws:SourceAccount 條件索引鍵，您可以使用 StringEquals 或 StringLike 條件運算子。最佳作法是，建議您使用 StringEquals 來實作最低權限。如果您不知道 SNS 主題的 ARN，可以使用 aws:SourceAccount。

- 如果您同時使用 `aws:SourceAccount` 和 `aws:SourceArn`，帳戶值必須顯示相同的帳戶 ID。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowAuditManagerToUseKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "auditmanager.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:region:accountID:key/*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountID"
      }
      "ArnLike": {
        "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
      }
    }
  }
}
```

透過 `StringLike` 條件運算子，下列替代範例僅使用 `aws:SourceArn` 條件索引鍵：

```
"Condition": {
  "StringLike": {
    "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
  }
}
```

透過 `StringLike` 條件運算子，下列替代範例僅使用 `aws:SourceAccount` 條件索引鍵：

```
"Condition": {
  "StringLike": {
    "aws:SourceAccount": "accountID"
  }
}
```

```
}
```

## 允許使用者在證據搜尋工具中執行搜索查詢

下列原則授與對 CloudTrail Lake 事件資料存放區執行查詢的權限。如需使用證據搜尋工具功能，則需要此許可政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageCloudTrailLakeQueryAccess",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:DescribeQuery",
        "cloudtrail:GetQueryResults",
        "cloudtrail:CancelQuery"
      ],
      "Resource": "*"
    }
  ]
}
```

## 預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以在未經許可的情況下對其他客戶的資源採取動作。為了預防這種情況，Amazon Web Services 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源策略中使用[aws:SourceArn](#)和[aws:SourceAccount](#)全域條件前後關聯鍵字，以限制授 AWS Audit Manager 予其他服務以存取您資源的權限。

- 如果您想要僅允許一個資源與跨服務存取權相關聯，則請使用 `aws:SourceArn`。如需指定多個資源，您也可以使用萬用字元 (\*) `aws:SourceArn`。

例如，您可以使用 Amazon SNS 主題接收來自 Audit Manager 的活動通知。在此情況下，在您的 SNS 主題存取政策中，`aws:SourceArn` 的 ARN 值是作為通知來源的 Audit Manager 資源。因為您可能有多個 Audit Manager 資源，因此建議您使用萬用字元 `aws:SourceArn`。因此，您可在 SNS 主題存取政策中指定所有 Audit Manager 資源。

- 如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 `aws:SourceAccount`。
- 如果 `aws:SourceArn` 值不包含帳戶 ID (例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體 ARN)，則必須使用這兩個全域條件內容索引鍵來限制許可。
- 如果使用兩項條件，且如果 `aws:SourceArn` 值包含帳戶 ID，則在相同政策陳述式中使用 `aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須顯示相同的帳戶 ID。
- 防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 Amazon Resource Name (ARN)，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域內容條件索引鍵搭配萬用字元 (\*) 來表示 ARN 的未知部分。例如 `arn:aws:service:*:123456789012:*`。

## Audit Manager 混淆代理人支援

Audit Manager 在下列情況下會提供混淆代理人支援。下列政策範例示範如何使用 `aws:SourceArn` 和 `aws:SourceAccount` 條件索引鍵來預防混淆代理人問題。

- [範例政策：您用來接收 Audit Manager 通知的 SNS 主題](#)
- [範例政策：您用來加密 SNS 主題的 KMS 金鑰](#)

Audit Manager 不會為您 Audit Manager [設定您的資料加密設定](#) 設定中提供的客戶管理金鑰提供混淆代理人支援。如果您提供了自己的客戶管理金鑰，則無法在該 KMS 金鑰政策中使用 `aws:SourceAccount` 或 `aws:SourceArn` 條件。

## AWS 受管理的政策 AWS Audit Manager

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住，AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。AWS 當新的啟動或新 AWS 服務的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#)。

## 主題

- [AWS 受管理的策略：AWSAuditManagerAdministratorAccess](#)
- [AWS 受管理的策略：AWSAuditManagerServiceRolePolicy](#)
- [AWS Audit ManagerAWS 受管理策略的更新](#)

## AWS 受管理的策略：AWSAuditManagerAdministratorAccess

您可將 AWSAuditManagerAdministratorAccess 政策連接到 IAM 身分。

此原則會授與允許完整管理存取權的管理權限 AWS Audit Manager。此存取權包括啟用和停用 AWS Audit Manager、變更中 AWS Audit Manager 的設定以及管理所有 Audit Manager 資源 (例如評估、架構、控制項和評估報告) 的功能。

AWS Audit Manager 需要跨多個 AWS 服務的廣泛權限。這是因為與多項 AWS 服務 AWS Audit Manager 整合，可自動從評估範圍內的 AWS 帳戶和服務收集證據。

## 許可詳細資訊

此政策包含以下許可：

- `Audit Manager` — 授予主體 AWS Audit Manager 資源的完整許可。
- `Organizations` — 授予主體列出帳號和組織單位，以及註冊或取消註冊委派管理員。這是必要的，以便您可以啟用多帳戶支援，並允許 AWS Audit Manager 對多個帳戶執行評估，並將證據合併到委派的管理員帳戶中。
- `iam` — 允許主體取得和列出 IAM 中使用者，以及建立服務連結角色。這是必要的，以便您可以指定評估的稽核擁有者和代理人。此政策也允許主體刪除服務連結角色，並擷取刪除狀態。這是必要的，AWS Audit Manager 以便在您選擇停用中的服務時清除資源並刪除服務連結角色。AWS Management Console
- `s3` — 允許主體列出可用 Amazon Simple Storage Service (Amazon S3) 儲存貯體。這是必要的，以便您可以指定您要在其中存放證據報告或上傳手動證據的 S3 儲存貯體。
- `kms` — 允許主體列出和描述金鑰、列出別名以及建立授權。這是必要的，以便您可以選擇客戶管理金鑰進行資料加密。

- `sns` — 允許主體列出 Amazon SNS 中的訂閱主題。這是必要的，以便您可以指定您希望作為 AWS Audit Manager 傳送通知目的地的 SNS 主題。
- `events`— 允許主參與者列出 AWS Security Hub 及管理檢查。這是必要的，AWS Audit Manager 以能夠自動收集受監視之 AWS 服務的 AWS Security Hub 發現項目 AWS Security Hub。然後，它可以將此資料轉換為證據，以包含在您的 AWS Audit Manager 評估中。
- `tag` — 允許主體擷取已標籤化的資源。這是必要的，以便您可以在 AWS Audit Manager 中瀏覽架構、控制項和評估時使用標籤作為搜尋篩選條件。
- `controlcatalog`— 可讓主參與者列出「控制目錄」所提供的網域、目標和一般 AWS 控制項。這是必要的，以便您可以使用中的通用控制項功能 AWS Audit Manager。有了這些權限，您就可以檢視控制項程式庫中的一般 AWS Audit Manager 控制項清單，並依網域和目標篩選控制項。建立自訂控制項時，您也可以使用通用控制項做為證據來源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsAccess",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowOnlyAuditManagerIntegration",
      "Effect": "Allow",
```

```

    "Action": [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator",
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "organizations:ServicePrincipal": [
          "auditmanager.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "IAMAccess",
    "Effect": "Allow",
    "Action": [
      "iam:GetUser",
      "iam:ListUsers",
      "iam:ListRoles"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IAMAccessCreateSLR",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "auditmanager.amazonaws.com"
      }
    }
  },
  {
    "Sid": "IAMAccessManageSLR",
    "Effect": "Allow",
    "Action": [
      "iam>DeleteServiceLinkedRole",
      "iam:UpdateRoleDescription",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
  },

```



```
    "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
  },
  {
    "Sid": "S3Access",
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Sid": "KmsAccess",
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  },
  {
    "Sid": "KmsCreateGrantAccess",
    "Effect": "Allow",
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      },
      "StringLike": {
        "kms:ViaService": "auditmanager.*.amazonaws.com"
      }
    }
  },
  {
    "Sid": "SNSAccess",
    "Effect": "Allow",
    "Action": [
      "sns:ListTopics"
    ],
    "Resource": "*"
  }
}
```

```

    },
    {
      "Sid": "CreateEventsAccess",
      "Effect": "Allow",
      "Action": [
        "events:PutRule"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "events:detail-type": "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals": {
          "events:source": [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid": "EventsAccess",
      "Effect": "Allow",
      "Action": [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid": "TagAccess",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ControlCatalogAccess",

```

```
    "Effect": "Allow",
    "Action": [
      "controlcatalog:ListCommonControls",
      "controlcatalog:ListDomains",
      "controlcatalog:ListObjectives"
    ],
    "Resource": "*"
  }
]
```

## AWS 受管理的策略：AWSAuditManagerServiceRolePolicy

您不得將 AWSAuditManagerServiceRolePolicy 連接到 IAM 實體。此原則附加至服務連結角色 AWSServiceRoleForAuditManager，可 AWS Audit Manager 讓您代表執行動作。如需詳細資訊，請參閱 [使用服務連結角色 AWS Audit Manager](#)。

角色許可政策，AWSAuditManagerServiceRolePolicy，允許 AWS Audit Manager 代表您執行下列動作來收集自動化證據：

- 從下列資料來源收集資料：
  - 管理事件來源 AWS CloudTrail
  - 符合性檢查來源 AWS Config 規則
  - 符合性檢查來源 AWS Security Hub
- 使用 API 呼叫描述下列 AWS 服務的資源組態。

### Tip

如需 Audit Manager 用來從這些服務收集證據之 API 呼叫的詳細資訊，請參閱本指南中的 [自訂控制項資料來源支援的 API 呼叫](#)。

- Amazon API Gateway
- AWS Backup
- Amazon Bedrock
- AWS Certificate Manager
- Amazon CloudFront
- AWS CloudTrail

- Amazon CloudWatch
- Amazon CloudWatch 日誌
- Amazon Cognito 使用者集區
- AWS Config
- Amazon 數據 Firehose
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- Amazon OpenSearch 服務
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3

- Amazon SageMaker
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

## 許可詳細資訊

AWSAuditManagerServiceRolePolicy 允許 AWS Audit Manager 對指定的資源完成以下操作：

- acm:GetAccountConfiguration
- acm:ListCertificates
- apigateway:GET
- autoscaling:DescribeAutoScalingGroups
- backup:ListBackupPlans
- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents

- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeBackup`
- `dynamodb:DescribeContinuousBackups`
- `dynamodb:DescribeTable`
- `dynamodb:DescribeTableReplicaAutoScaling`
- `dynamodb:ListBackups`
- `dynamodb:ListGlobalTables`
- `dynamodb:ListTables`
- `ec2:DescribeAddresses`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeInstanceCreditSpecifications`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations`
- `ec2:DescribeLocalGateways`
- `ec2:DescribeLocalGatewayVirtualInterfaces`

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters

- `elasticmapreduce:ListSecurityConfigurations`
- `es:DescribeDomains`
- `es:DescribeDomain`
- `es:DescribeDomainConfig`
- `es:ListDomainNames`
- `events:DeleteRule`
- `events:DescribeRule`
- `events:DisableRule`
- `events:EnableRule`
- `events:ListConnections`
- `events:ListEventBuses`
- `events:ListEventSources`
- `events:ListRules`
- `events:ListTargetsByRule`
- `events:PutRule`
- `events:PutTargets`
- `events:RemoveTargets`
- `firehose:ListDeliveryStreams`
- `fsx:DescribeFileSystems`
- `guardduty:ListDetectors`
- `iam:GenerateCredentialReport`
- `iam:GetAccessKeyLastUsed`
- `iam:GetAccountAuthorizationDetails`
- `iam:GetAccountPasswordPolicy`
- `iam:GetAccountSummary`
- `iam:GetCredentialReport`
- `iam:GetGroupPolicy`
- `iam:GetPolicy`



- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy

- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig

- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - 此 API 動作會在可用位 AWS 帳戶 置的範圍內 service-linked-role 運作。它無法存取跨帳戶儲存貯體政策。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3>ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker>ListAlgorithms
- sagemaker>ListDomains
- sagemaker>ListEndpointConfigs
- sagemaker>ListEndpoints

- `sagemaker:ListFlowDefinitions`
- `sagemaker:ListHumanTaskUis`
- `sagemaker:ListLabelingJobs`
- `sagemaker:ListModels`
- `sagemaker:ListModelBiasJobDefinitions`
- `sagemaker:ListModelCards`
- `sagemaker:ListModelQualityJobDefinitions`
- `sagemaker:ListMonitoringAlerts`
- `sagemaker:ListMonitoringSchedules`
- `sagemaker:ListTrainingJobs`
- `sagemaker:ListUserProfiles`
- `securityhub:DescribeStandards`
- `secretsmanager:DescribeSecret`
- `secretsmanager:ListSecrets`
- `sns:ListTagsForResource`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetRule`
- `waf-regional:GetWebAcl`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListRules`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:GetRule`
- `waf:GetRuleGroup`
- `waf:ListActivatedRulesInRuleGroup`
- `waf:ListRuleGroups`

- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
```

```
"dynamodb:DescribeTable",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListTables",
"ec2:DescribeInstanceCreditSpecifications",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:GetLaunchTemplateData",
"ec2:DescribeAddresses",
"ec2:DescribeCustomerGateways",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGateways",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeTransitGateways",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetEbsEncryptionByDefault",
"ecs:DescribeClusters",
"eks:DescribeAddonVersions",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeServiceUpdates",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSslPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListSecurityConfigurations",
```

```
"events:DescribeRule",
"events:ListConnections",
"events:ListEventBuses",
"events:ListEventSources",
"events:ListRules",
"firehose:ListDeliveryStreams",
"fsx:DescribeFileSystems",
"guardduty:ListDetectors",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccessKeyLastUsed",
"iam:GetCredentialReport",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupsForUser",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListOpenIdConnectProviders",
"iam:ListPolicies",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSamlProviders",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"iam:ListPolicyVersions",
"iam:ListAccessKeys",
"iam:ListAttachedRolePolicies",
"iam:ListMfaDeviceTags",
"iam:ListMfaDevices",
"kafka:ListClusters",
"kafka:ListKafkaVersions",
"kinesis:ListStreams",
"kms:DescribeKey",
"kms:GetKeyPolicy",
```

```
"kms:GetKeyRotationStatus",
"kms:ListGrants",
"kms:ListKeyPolicies",
"kms:ListKeys",
"lambda:ListFunctions",
"license-manager:ListAssociationsForLicenseConfiguration",
"license-manager:ListLicenseConfigurations",
"license-manager:ListUsageForLicenseConfiguration",
"logs:DescribeDestinations",
"logs:DescribeExportTasks",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:DescribeResourcePolicies",
"logs:FilterLogEvents",
"logs:GetDataProtectionPolicy",
"es:DescribeDomains",
"es:DescribeDomain",
"es:DescribeDomainConfig",
"es:ListDomainNames",
"organizations:DescribeOrganization",
"organizations:DescribePolicy",
"rds:DescribeCertificates",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeLoggingStatus",
"route53:GetQueryLoggingConfig",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelCard",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeModel",
"sagemaker:DescribeTrainingJob",
```



```
"sagemaker:DescribeUserProfile",
"sagemaker:ListAlgorithms",
"sagemaker:ListDomains",
"sagemaker:ListEndpoints",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListLabelingJobs",
"sagemaker:ListModels",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelCards",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListMonitoringAlerts",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListTrainingJobs",
"sagemaker:ListUserProfiles",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:ListAllMyBuckets",
"secretsmanager:DescribeSecret",
"secretsmanager:ListSecrets",
"securityhub:DescribeStandards",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:ListQueues",
"waf-regional:GetRule",
"waf-regional:GetWebAcl",
"waf:GetRule",
"waf:GetRuleGroup",
"waf:ListActivatedRulesInRuleGroup",
"waf:ListWebAcls",
"wafv2:ListWebAcls",
"waf-regional:GetLoggingConfiguration",
"waf-regional:ListRuleGroups",
"waf-regional:ListSubscribedRuleGroups",
"waf-regional:ListWebACLs",
"waf-regional:ListRules",
"waf:ListRuleGroups",
"waf:ListRules"
],
"Resource": "*",
"Sid": "APIsAccess"
```

```
},
{
  "Sid": "S3Access",
  "Effect": "Allow",
  "Action": [
    "s3:GetBucketAcl",
    "s3:GetBucketLogging",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketTagging"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": [
        "${aws:PrincipalAccount}"
      ]
    }
  }
},
{
  "Sid": "APIGatewayAccess",
  "Effect": "Allow",
  "Action": [
    "apigateway:GET"
  ],
  "Resource": [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/restapis/*/stages"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": [
        "${aws:PrincipalAccount}"
      ]
    }
  }
},
{
  "Sid": "CreateEventsAccess",
  "Effect": "Allow",
  "Action": [
    "events:PutRule"
```

```

    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
    "Condition": {
      "StringEquals": {
        "events:detail-type": "Security Hub Findings - Imported"
      },
      "Null": {
        "events:source": "false"
      },
      "ForAllValues:StringEquals": {
        "events:source": [
          "aws.securityhub"
        ]
      }
    }
  },
  {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
      "events:DeleteRule",
      "events:DescribeRule",
      "events:EnableRule",
      "events:DisableRule",
      "events:ListTargetsByRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  }
]
}

```

## AWS Audit Manager AWS 受管理策略的更新

檢視 AWS Audit Manager 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「AWS Audit Manager [文件歷史記錄](#)」頁面上的 RSS 摘要。

變更	描述	日期
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	我們已將下列權限新增至AWSAuditManagerServiceRolePolicy。AWS	06/10/2024

變更	描述	日期
	<p>Audit Manager 現在可以執行下列動作，以收集您的 AWS 帳戶。</p> <ul style="list-style-type: none"> <li>• sagemaker:DescribeAlgorithm</li> <li>• sagemaker:DescribeDomain</li> <li>• sagemaker:DescribeEndpoint</li> <li>• sagemaker:DescribeFlowDefinition</li> <li>• sagemaker:DescribeHumanTaskUi</li> <li>• sagemaker:DescribeLabelingJob</li> <li>• sagemaker:DescribeModel</li> <li>• sagemaker:DescribeModelBiasJobDefinition</li> <li>• sagemaker:DescribeModelCard</li> <li>• sagemaker:DescribeModelQualityJobDefinition</li> <li>• sagemaker:DescribeTrainingJob</li> <li>• sagemaker:DescribeUserProfile</li> <li>• sagemaker:ListAlgorithms</li> <li>• sagemaker:ListDomains</li> <li>• sagemaker:ListEndpoints</li> <li>• sagemaker:ListFlowDefinitions</li> <li>• sagemaker:ListHumanTaskUis</li> <li>• sagemaker:ListLabelingJobs</li> <li>• sagemaker:ListModels</li> <li>• sagemaker:ListModelBiasJobDefinitions</li> <li>• sagemaker:ListModelCards</li> <li>• sagemaker:ListModelQualityJobDefinitions</li> </ul>	

變更	描述	日期
	<ul style="list-style-type: none"> <li>• sagemaker:ListMonitoringAlerts</li> <li>• sagemaker:ListMonitoringSchedules</li> <li>• sagemaker:ListTrainingJobs</li> <li>• sagemaker:ListUserProfiles</li> </ul>	
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	<p>我們已將下列權限新增至AWSAuditManagerServiceRolePolicy。AWS Audit Manager 現在可以執行下列動作，以收集您的 AWS 帳戶。</p> <ul style="list-style-type: none"> <li>• iam:ListAttachedGroupPolicies</li> <li>• iam:ListAttachedUserPolicies</li> <li>• iam:ListGroupsForUser</li> <li>• es:ListDomainNames</li> </ul> <p>我們還在策略 ( arn:aws:apigateway:*::/restapis ) 的 APIGatewayAccess 節中添加了一個新的資源。</p> <p>該策略現在不僅授予 API Gateway REST API 的階段和階段資源，而且還授予 REST API 本身的指定權限 ( 在本例中為apigateway:GET 操作 )。除了與這些 API 相關的階段和階段資源之外，此變更有效地擴展了原則的範圍，以包括擷取 API Gateway REST API 本身相關資訊的功能。</p>	05/17/2024

變更	描述	日期
<a href="#">AWSAuditManagerAdministratorAccess</a> – 更新現有政策	<p>我們將以下許可新增到 <code>AWSAuditManagerAdministratorAccess</code> :</p> <ul style="list-style-type: none"><li>• <code>controlcatalog:ListCommonControls</code></li><li>• <code>controlcatalog:ListDomains</code></li><li>• <code>controlcatalog:ListObjectives</code></li></ul> <p>此更新可讓您檢視控制項目錄所提供的控制項網域、控制項目標及一般 AWS 控制項。如果您要使用中的通用控制項功能，則需要這些權限 AWS Audit Manager。</p>	05/15/2024

變更	描述	日期
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	<p>我們已將下列權限新增至AWSAuditManagerServiceRolePolicy。AWS Audit Manager 現在可以執行下列動作，以收集您的 AWS 帳戶。</p> <ul style="list-style-type: none"> <li>• apigateway:GET</li> <li>• autoscaling:DescribeAutoScalingGroups</li> <li>• backup:ListBackupPlans</li> <li>• cloudfront:GetDistribution</li> <li>• cloudfront:GetDistributionConfig</li> <li>• cloudfront:ListDistributions</li> <li>• cloudtrail:GetTrail</li> <li>• cloudtrail:ListTrails</li> <li>• dynamodb:DescribeContinuousBackups</li> <li>• dynamodb:DescribeBackup</li> <li>• dynamodb:DescribeTableReplicaAutoScaling</li> <li>• ec2:DescribeInstanceCreditSpecifications</li> <li>• ec2:DescribeInstanceAttribute</li> <li>• ec2:DescribeSecurityGroupRules</li> <li>• ec2:DescribeVpcEndpointConnections</li> <li>• ec2:DescribeVpcEndpointServiceConfigurations</li> <li>• ec2:GetLaunchTemplateData</li> <li>• es:DescribeDomains</li> <li>• es:DescribeDomain</li> </ul>	05/15/2024

變更	描述	日期
	<ul style="list-style-type: none"> <li>• es:DescribeDomainConfig</li> <li>• iam:GetAccessKeyLastUsed</li> <li>• iam:GetGroupPolicy</li> <li>• iam:GetPolicy</li> <li>• iam:GetPolicyVersion</li> <li>• iam:GetRolePolicy</li> <li>• iam:GetUser</li> <li>• iam:GetUserPolicy</li> <li>• iam:ListAccessKeys</li> <li>• iam:ListAttachedRolePolicies</li> <li>• iam:ListMfaDeviceTags</li> <li>• iam:ListMfaDevices</li> <li>• iam:ListPolicyVersions</li> <li>• logs:GetDataProtectionPolicy</li> <li>• rds:DescribeDBInstanceAutomatedBackups</li> <li>• rds:DescribeDBClusterEndpoints</li> <li>• rds:DescribeDBClusterParameterGroups</li> <li>• redshift:DescribeClusterSnapshots</li> <li>• redshift:DescribeLoggingStatus</li> <li>• s3:GetBucketAcl</li> <li>• s3:GetBucketLogging</li> <li>• s3:GetBucketOwnershipControls</li> <li>• s3:GetBucketTagging</li> <li>• sagemaker:DescribeEndpointConfig</li> <li>• sagemaker:ListEndpointConfigs</li> <li>• secretsmanager:DescribeSecret</li> </ul>	



變更	描述	日期
	<ul style="list-style-type: none"> <li>• secretsmanager:ListSecrets</li> <li>• sns:ListTagsForResource</li> <li>• waf-regional:GetRule</li> <li>• waf-regional:GetWebAcl</li> <li>• waf-regional:ListRules</li> <li>• waf:GetRule</li> <li>• waf:GetRuleGroup</li> <li>• waf:ListRuleGroups</li> <li>• waf:ListRules</li> <li>• waf:ListWebAcls</li> <li>• wafv2:ListWebAcls</li> </ul>	
<p><a href="#">AWSAuditManagerServiceRolePolicy</a></p> <p>– 更新現有政策</p>	<p>服務連結角色現在允 AWS Audit Manager 許執行 <code>s3:GetBucketPolicy</code> 作。</p> <p>需要此 API 動作才能支援 <a href="#">AWS 生成式 AI 最佳實務架構 v1</a>。它可讓 Audit Manager 收集有關您生成式 AI 模型資料訓練資料集之政策限制的自動化證據。</p> <p>動 <code>GetBucketPolicy</code> 作會在可用位 AWS 帳戶置的範圍內 <code>service-linked-role</code> 運作。它無法存取跨帳戶儲存貯體政策。</p>	<p>12/06/2023</p>

變更	描述	日期
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	<p>我們已將下列權限新增至AWSAuditManagerServiceRolePolicy。AWS Audit Manager 現在可以執行下列動作，以收集您的 AWS 帳戶。</p> <ul style="list-style-type: none"> <li>• acm:GetAccountConfiguration</li> <li>• acm:ListCertificates</li> <li>• backup:ListRecoveryPointsByResource</li> <li>• bedrock:GetCustomModel</li> <li>• bedrock:GetFoundationModel</li> <li>• bedrock:GetModelCustomizationJob</li> <li>• bedrock:GetModelInvocationLoggingConfiguration</li> <li>• bedrock:ListCustomModels</li> <li>• bedrock:ListFoundationModels</li> <li>• bedrock:ListModelCustomizationJobs</li> <li>• cloudtrail:LookupEvents</li> <li>• cloudwatch:DescribeAlarmsForMetric</li> <li>• cloudwatch:GetMetricStatistics</li> <li>• cloudwatch:ListMetrics</li> <li>• directconnect:DescribeDirectConnectGateways</li> <li>• directconnect:DescribeVirtualGateways</li> <li>• dynamodb:ListBackups</li> <li>• dynamodb:ListGlobalTables</li> <li>• ec2:DescribeAddresses</li> </ul>	11/06/2023

變更	描述	日期
	<ul style="list-style-type: none"> <li>• ec2:DescribeCustomerGateways</li> <li>• ec2:DescribeEgressOnlyInternetGateways</li> <li>• ec2:DescribeInternetGateways</li> <li>• ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations</li> <li>• ec2:DescribeLocalGateways</li> <li>• ec2:DescribeLocalGatewayVirtualInterfaces</li> <li>• ec2:DescribeNatGateways</li> <li>• ec2:DescribeTransitGateways</li> <li>• ec2:DescribeVpcPeeringConnections</li> <li>• ec2:DescribeVpnConnections</li> <li>• ec2:DescribeVpnGateways</li> <li>• ec2:GetEbsDefaultKmsKeyId</li> <li>• ec2:GetEbsEncryptionByDefault</li> <li>• ecs:DescribeClusters</li> <li>• eks:DescribeAddonVersions</li> <li>• elasticache:DescribeCacheClusters</li> <li>• elasticache:DescribeServiceUpdates</li> <li>• elasticfilesystem:DescribeAccessPoints</li> <li>• elasticloadbalancing:DescribeLoadBalancers</li> <li>• elasticloadbalancing:DescribeSslPolicies</li> </ul>	

變更	描述	日期
	<ul style="list-style-type: none"> <li>• elasticloadbalancing:DescribeTargetGroups</li> <li>• elasticmapreduce:ListClusters</li> <li>• elasticmapreduce:ListSecurityConfigurations</li> <li>• events:ListConnections</li> <li>• events:ListEventBuses</li> <li>• events:ListEventSources</li> <li>• events:ListRules</li> <li>• firehose:ListDeliveryStreams</li> <li>• fsx:DescribeFileSystems</li> <li>• iam:GetAccountPasswordPolicy</li> <li>• iam:GetCredentialReport</li> <li>• iam:ListOpenIdConnectProviders</li> <li>• iam:ListSamlProviders</li> <li>• iam:ListVirtualMFADevices</li> <li>• kafka:ListClusters</li> <li>• kafka:ListKafkaVersions</li> <li>• kinesis:ListStreams</li> <li>• lambda:ListFunctions</li> <li>• logs:DescribeDestinations</li> <li>• logs:DescribeExportTasks</li> <li>• logs:DescribeLogGroups</li> <li>• logs:DescribeMetricFilters</li> <li>• logs:DescribeResourcePolicies</li> <li>• logs:FilterLogEvents</li> <li>• rds:DescribeCertificates</li> <li>• rds:DescribeDbClusterEndpoints</li> </ul>	

變更	描述	日期
	<ul style="list-style-type: none"> <li>• rds:DescribeDbClusterParameterGroups</li> <li>• rds:DescribeDbClusters</li> <li>• rds:DescribeDbSecurityGroups</li> <li>• redshift:DescribeClusters</li> <li>• s3:GetBucketPublicAccessBlock</li> <li>• s3:GetBucketVersioning</li> <li>• sns:ListTopics</li> <li>• sqs:ListQueues</li> <li>• waf-regional:GetLoggingConfiguration</li> <li>• waf-regional:ListRuleGroups</li> <li>• waf-regional:ListSubscribedRuleGroups</li> <li>• waf-regional:ListWebACLs</li> </ul>	
<p><a href="#">AWSAuditManagerServiceRolePolicy</a></p> <p>– 更新現有政策</p>	<p>我們將以下許可新增到 AWSAuditManagerServiceRolePolicy :</p> <ul style="list-style-type: none"> <li>• dynamodb:DescribeTable</li> <li>• dynamodb:ListTables</li> <li>• ec2:DescribeVolumes</li> <li>• kms:GetKeyPolicy</li> <li>• kms:GetKeyRotationStatus</li> <li>• kms:ListKeyPolicies</li> <li>• rds:DescribeDBInstances</li> <li>• redshift:DescribeClusters</li> <li>• s3:GetEncryptionConfiguration</li> <li>• s3:ListAllMyBuckets</li> </ul>	<p>2022 年 7 月 7 日</p>

變更	描述	日期
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	<p>服務連結角色現在允 AWS Audit Manager 許執行 <code>organizations:DescribeOrganization</code> 作。</p> <p>我們還將 <code>CreateEventsAccess</code> 資源範圍從萬用字元 (*) 縮小到特定類型的資源 (<code>arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver</code>)。</p> <p>最後，我們為 <code>Null</code> 條件索引鍵添加 <code>events:source</code> 條件運算子，以確認來源值存在且其值不為 <code>null</code>。</p>	2022 年 5 月 20 日
<a href="#">AWSAuditManagerAdministratorAccess</a> – 更新現有政策	我們已更新的金鑰條件政策， <code>events:source</code> 以反映這是多值金鑰。	04/29/2022
<a href="#">AWSAuditManagerServiceRolePolicy</a> – 更新現有政策	我們已更新的金鑰條件政策， <code>events:source</code> 以反映這是多值金鑰。	03/16/2022
AWS Audit Manager 開始追蹤變更	AWS Audit Manager 開始追蹤其 AWS 受管理策略的變更。	2021 年 6 月 5 日

## 疑難排解 AWS Audit Manager 身分和存取

請使用以下資訊來協助您診斷和修正使用 Audit Manager 和 IAM 時發生的常見問題。

### 主題

- [我沒有執行操作的授權 AWS Audit Manager](#)
- [我沒有授權執行 iam : PassRole](#)
- [我想允許我以外的人訪 AWS 帳戶 問我的 AWS Audit Manager 資源](#)

## 我沒有執行操作的授權 AWS Audit Manager

`AccessDeniedException` 當使用者沒有使用權限 AWS Audit Manager 或 Audit Manager API 作業時，就會出現錯誤。

在此情況下，管理員必須將政策更新為允許您存取。

## 我沒有授權執行 iam : PassRole

如果錯誤訊息告知您未獲得授權，無法執行 `iam:PassRole` 動作，您的政策就必須更新，允許您將角色傳遞給 Audit Manager。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 Audit Manager 中執行動作時，發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

## 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Audit Manager 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 如需了解 Audit Manager 是否支援這些功能，請參閱 [如何與 IAM AWS Audit Manager 搭配使用](#)。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 [IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限](#)。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的 [提供第三方 AWS 帳戶 擁有的存取權](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。

- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。

## 使用服務連結角色 AWS Audit Manager

AWS Audit Manager 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Audit Manager 的特殊 IAM 角色類型。服務連結角色由 Audit Manager 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓您 AWS Audit Manager 更輕鬆地設定，因為您不需要手動新增必要的權限。Audit Manager 定義其服務連結角色的許可，除非另有定義，否則僅有 Audit Manager 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

如需關於支援服務連結角色的其他服務資訊，請參閱 [可搭配 IAM 運作的 AWS 服務](#)，並尋找在服務連結角色欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

### 服務連結角色權限 AWS Audit Manager

Audit Manager 使用名為的服務連結角色 `AWSServiceRoleForAuditManager`，可存取使用或管理的 AWS 服務和資源。AWS Audit Manager

`AWSServiceRoleForAuditManager` 服務連結角色信任 `auditmanager.amazonaws.com` 服務來擔任該角色。

角色權限原則可讓 Audit Manager 收集有關您 AWS 使用情況的自動證據。[AWSAuditManagerServiceRolePolicy](#) 具體而言，它可以代表您執行以下動作。


- Audit Manager 可用 AWS Security Hub 來收集合規性檢查證據。在此情況下，「Audit Manager」會使用下列權限，直接從中報告安全性檢查結果 AWS Security Hub。然後，將結果附加到您的相關評估控制項中作為證據。
  - `securityhub:DescribeStandards`

#### Note

如需有關 Audit Manager 可描述的特定 Security Hub 控制項的詳細資訊，請參閱 [AWS Audit Manager 支援的 AWS Security Hub 控制項](#)。




- Audit Manager 可用 AWS Config 來收集合規性檢查證據。在這種情況下，Audit Manager 會使用下列權限直接從 AWS Config 中報告 AWS Config 規則評估的結果。然後，將結果附加到您的相關評估控制項中作為證據。
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

 Note

如需有關 Audit Manager 可描述哪些特定 AWS Config 規則的詳細資訊，請參閱[受支援的 AWS Config 規則 AWS Audit Manager](#)。

- Audit Manager 可用 AWS CloudTrail 來收集使用者活動證據。在此情況下，Audit Manager 會使用下列權限從 CloudTrail 記錄擷取使用者活動。然後，將活動附加到您的相關評估控制項中作為證據。
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

 Note

如需有關 Audit Manager 可描述哪些特定 CloudTrail 事件的詳細資訊，請參閱[受支援的 AWS CloudTrail 事件名稱 AWS Audit Manager](#)。

- Audit Manager 可以使用 AWS API 呼叫來收集資源組態證據。在此情況下，Audit Manager 會使用下列許可來呼叫描述下列 AWS 服務之資源組態的唯讀 API。然後，將 API 回應附加到您的相關評估控制項中作為證據。
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`

- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`
- `cloudtrail:ListTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeBackup`
- `dynamodb:DescribeContinuousBackups`
- `dynamodb:DescribeTable`
- `dynamodb:DescribeTableReplicaAutoScaling`
- `dynamodb:ListBackups`
- `dynamodb:ListGlobalTables`
- `dynamodb:ListTables`
- `ec2:DescribeAddresses`

- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ~~ecs:DescribeClusters~~
- eks:DescribeAddonVersions

- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events>DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed

- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices

- kafka:ListClusters

- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- ~~redshift:DescribeClusters~~
- redshift:DescribeClusterSnapshots

- `redshift:DescribeLoggingStatus`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketAcl`
- `s3:GetBucketLogging`
- `s3:GetBucketOwnershipControls`
- `s3:GetBucketPolicy`
  - 此 API 動作會在可用位 AWS 帳戶 置的範圍內 `service-linked-role` 運作。它無法存取跨帳戶儲存貯體政策。
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3>ListAllMyBuckets`
- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`
- `sagemaker:DescribeModel`
- `sagemaker:DescribeModelBiasJobDefinition`
- `sagemaker:DescribeModelCard`
- `sagemaker:DescribeModelQualityJobDefinition`
- `sagemaker:DescribeTrainingJob`
- `sagemaker:DescribeUserProfile`
- `sagemaker>ListAlgorithms`
- `sagemaker>ListDomains`
- `sagemaker>ListEndpointConfigs`

- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules



- waf:ListWebAcls
- wafv2:ListWebAcls

### Note

如需有關 Audit Manager 可以描述的特定 API 呼叫的詳細資訊，請參閱 [自訂控制項資料來源支援的 API 呼叫](#)。

若要檢視服務連結角色的完整權限詳細資料 `AWSServiceRoleForAuditManager`，請參閱 AWS 受管理策略參考指南 [AWSAuditManagerServiceRolePolicy](#) 中的。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。

## 建立 AWS Audit Manager 服務連結角色

您不需要手動建立一個服務連結角色。當您啟用時 AWS Audit Manager，服務會自動為您建立服務連結角色。您可以從的上架頁面或透過 API 或 AWS CLI 啟用 Audit Manager。AWS Management Console 如需詳細資訊，請參閱本使用者指南中的 [啟用 AWS Audit Manager](#)。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

## 編輯 AWS Audit Manager 服務連結角色

AWS Audit Manager 不允許您編輯 `AWSServiceRoleForAuditManager` 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的 [編輯服務連結角色](#)。

如需允許 IAM 實體編輯 `AWSServiceRoleForAuditManager` 服務連結角色的描述

將下列陳述式新增至 IAM 實體編輯服務連結角色描述所需的許可政策：

```
{
  "Effect": "Allow",
  "Action": [
    "iam:UpdateRoleDescription"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
}
```

```
"Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

## 刪除 AWS Audit Manager 服務連結角色

如果您不再需要使用 Audit Manager，我們建議您刪除 `AWSServiceRoleForAuditManager` 服務連結角色。這樣就不會有未積極監控或維護的未使用實體。然而，務必清除服務連結角色，之後才能將其刪除。

### 清除服務連結角色

您必須先確認 Audit Manager 服務連結角色沒有作用中的工作階段，並移除該角色使用的資源，之後才能使用 IAM 將其刪除。若要這麼做，請確定 Audit Manager 已全部 AWS 區域取消註冊。取消註冊後，Audit Manager 將不再使用服務連結角色。

如需有關如何取消註冊 Audit Manager 的說明，請參閱以下資源：

- 本指南中的 [禁用 AWS Audit Manager](#)
- AWS Audit Manager API 參考中的 [DeregisterAccount](#)
- [撤銷註冊-帳戶](#) 的參考 AWS CLI AWS Audit Manager

如需有關如何手動刪除 Audit Manager 資源的說明，請參閱本指南中的 [刪除 Audit Manager 資料](#)。

### 刪除 服務連結角色

您可以使用 IAM 主控台、AWS Command Line Interface (AWS CLI) 或 IAM API 來刪除服務連結角色。

#### IAM console

請依照下列步驟，在 IAM 主控台中刪除服務連結角色：

##### 刪除服務連結角色 (主控台)

1. 登入 AWS Management Console 並開啟 IAM 主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 在 IAM 主控台的導覽窗格中，選擇角色。選擇 `AWSServiceRoleForAuditManager` 旁的核取方塊，而非名稱或列本身。
3. 在頁面頂端的角色動作下選擇刪除。

4. 在確認對話方塊中，檢閱上次存取資訊，以顯示每個所選擇角色上次存取 AWS 服務的時。這可協助您確認角色目前是否作用中。如果您想要繼續進行，在文字輸入欄位中輸入 **AWSServiceRoleForAuditManager**，然後選擇刪除來提交服務連結角色以進行刪除。
5. 查看 IAM 主控台通知，監視服務連結角色刪除的進度。因為 IAM 服務連結角色刪除不同步，所以在您提交角色進行刪除之後，刪除任務可能會成功或失敗。如果任務成功，則會從清單中移除角色，而且成功訊息會出現在頁面頂端。

## AWS CLI

您可以使用的 IAM 命令 AWS CLI 來刪除服務連結角色。

### 刪除服務連結角色 (AWS CLI)

1. 輸入以下命令來列出您帳戶中的角色：

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. 因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則可以拒絕該請求。您必須從回應中擷取 `deletion-task-id`，以檢查刪除任務的狀態。

輸入下列命令，以提交服務連結角色刪除要求：

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. 使用下列命令，以檢查刪除任務的狀態：

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

刪除任務的狀態可以是 NOT\_STARTED、IN\_PROGRESS、SUCCEEDED 或 FAILED。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

## IAM API

您可以使用 IAM API 刪除服務連結角色。

## 刪除服務連結角色 (API)

1. [GetRole](#) 打電話列出您帳戶中的角色。在請求中，指定 `AWSServiceRoleForAuditManager` 為 `RoleName`。
2. 因為無法刪除正在使用或具有相關聯資源的服務連結角色，所以您必須提交刪除要求。如果不符合這些條件，則可以拒絕該請求。您必須從回應中擷取 `DeletionTaskId`，以檢查刪除任務的狀態。

若要提交服務連結角色的刪除要求，請致電 [DeleteServiceLinkedRole](#)。在請求中，指定 `AWSServiceRoleForAuditManager` 為 `RoleName`。

3. 要檢查刪除狀態，請致電 [GetServiceLinkedRoleDeletionStatus](#)。在請求中，指定 `DeletionTaskId`。

刪除任務的狀態可以是 `NOT_STARTED`、`IN_PROGRESS`、`SUCCEEDED` 或 `FAILED`。如果刪除失敗，則呼叫會傳回失敗原因，以進行疑難排解。

## 刪除 Audit Manager 服務連結角色的提示

如果 Audit Manager 正在使用該角色或具有相關聯的資源，則 Audit Manager 服務連結角色的刪除程序可能會失敗。這可能發生在下列情況中：

1. 您的帳戶仍在一個或多個 Audit Manager 中註冊 AWS 區域。
2. 您的帳戶屬於組 AWS 織，而管理帳戶或委派的管理員帳戶仍會登入 Audit Manager。

若要解決刪除失敗的問題，請先檢查您 AWS 帳戶 是否屬於組織。您可以通過調用 [DescribeOrganization](#) API 操作或導航到 AWS Organizations 控制台來完成此操作。

如果您 AWS 帳戶 是組織的一部分

1. 使用您的管理帳戶移 [除稽核管理員中所有已新增管理員 AWS 區域 的委派管理員](#)。
2. 使用您的管理帳戶在您使用該服務的所有 AWS 區域 位置取 [消註冊 Audit Manager](#)。
3. 請遵循上一個程序中的步驟，再試一次刪除服務連結角色。

如果您不 AWS 帳戶 是組織的一部分

1. 請確定您已在使用該服務的所有 AWS 區域 位置取 [消註冊 Audit Manager](#)。
2. 請遵循上一個程序中的步驟，再試一次刪除服務連結角色。

從 Audit Manager 取消註冊後，服務將停止使用服務連結角色。然後，您可以成功刪除角色。

## 支援 AWS Audit Manager 服務連結角色的區域

AWS Audit Manager 支援在所有可用服務的 AWS 區域 地方使用服務連結角色。如需詳細資訊，請參閱 [AWS 服務端點](#)。

## 符合性驗證 AWS Audit Manager

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱[AWS 服務 遵循規範計劃](#)方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱[AWS 規範計劃](#)。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載中的報告中的](#) AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- [安全性與合規性快速入門指南](#) — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- [在 Amazon Web Services 上架構 HIPAA 安全性與合規性](#) — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 應用程式。

### Note

並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 [HIPAA 資格服務參照](#)。

- [AWS 合規資源](#) — 此工作簿和指南集合可能適用於您的產業和所在地。
- [AWS 客戶合規指南](#) — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- [使用 AWS Config 開發人員指南中的規則評估資源](#) — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) — 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。

- [Amazon GuardDuty](#) — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務偵測您的工作負載、容器和資料的潛在威脅。GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- [AWS Audit Manager](#)— 這 AWS 服務有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

## 了解彈性 AWS Audit Manager

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。

透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱[AWS 全域基礎結構](#)。

## 基礎結構安全 AWS Audit Manager

AWS 稽核管理員身為受管服務，受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱[AWS 雲端安全](#) 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 AWS Audit Manager。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 [AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

您可以從任何網路位置呼叫這些 API 作業，但支 AWS Audit Manager 援以資源為基礎的存取原則，其中可能包含以來源 IP 位址為基礎的限制。您也可以使用 Audit Manager 政策來控制從特定 Amazon Virtual Private Cloud (Amazon VPC) 的端點或特定 VPC 的存取。實際上，這會將對特定 Audit Manager 資源的網路存取從網路內的特定 VPC 隔離出來 AWS 。

## AWS Audit Manager 和介面 VPC 端端點 (AWS PrivateLink)

您可以在 VPC 和 AWS Audit Manager 建立介面 VPC 端點之間建立私人連線。介面端點是由 [AWS PrivateLink](#) 提供技術支援，這項技術可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線的情況下私密地存取 Audit Manager API。VPC 中的執行個體不需要公有 IP 地址，即能與 Audit Manager API 通訊。您的 VPC 和 AWS Audit Manager 不會離開 AWS 網路之間的流量。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

### AWS Audit Manager VPC 端點的考量

在為其設定介面 VPC 端點之前 AWS Audit Manager，請務必先查看 Amazon VPC 使用者指南中的[介面端點屬性和限制](#)。

AWS Audit Manager 支援從您的 VPC 呼叫其所有 API 動作。

### 為 AWS Audit Manager 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 建立 AWS Audit Manager 服務的 VPC 端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[建立介面端點](#)。

建立 VPC 端點以 AWS Audit Manager 使用下列服務名稱：

- `com.amazonaws.region.auditmanager`

如果您為端點啟用私有 DNS，則可以 AWS Audit Manager 使用該區域的預設 DNS 名稱發出 API 要求，例如 `auditmanager.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[透過介面端點存取服務](#)。

### 建立 VPC 端點原則 AWS Audit Manager

您可以將端點政策連接至控制 AWS Audit Manager 存取權限的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。

- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 VPC 端點控制對服務的存取](#)。

範例：用於動作的 VPC 端點原則 AWS Audit Manager

以下是的端點策略範例 AWS Audit Manager。附加至端點後，此政策會針對所有資源上的所有主體，授予列出的 Audit Manager 動作的存取權限。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "auditmanager:GetAssessment",
        "auditmanager:GetServicesInScope",
        "auditmanager:ListNotifications"
      ],
      "Resource": "*"
    }
  ]
}
```

## 登錄和監控 AWS Audit Manager

監控是維持 Audit Manager 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供下列監視工具來監視 Audit Manager、在發生錯誤時報告，並在適當時採取自動動作：

- AWS CloudTrail 擷取您 AWS 帳戶 發出或代表發出的 API 呼叫和相關事件，並傳送日誌檔案至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 [AWS CloudTrail 使用者指南](#)。
- Amazon EventBridge 是一種無伺服器事件匯流排服務，可讓您輕鬆地將應用程式與各種來源的資料連接起來。EventBridge 從您自己的應用程式、Software-as-a 服務 (SaaS) 應用程式以及服務提供即時資料串流，並 AWS 將該資料路由到目標 (例如 Lambda)。這可讓您監控在服務中發生的事件，並建置事件導向的架構。如需詳細資訊，請參閱 [Amazon EventBridge 使用者指南](#)。



## AWS Audit Manager 使用 Amazon 監控 EventBridge

Amazon 可 EventBridge 協助您自動化 AWS 服務 並自動回應系統事件，例如應用程式可用性問題或資源變更。

您可以使用 EventBridge 規則來偵測 Audit Manager 事件並對其做出回應。根據您建立的規則，當事件符合您在規則中指定的值時，EventBridge 叫用一或多個目標動作。根據事件的類型，您可能會想要傳送通知、擷取事件資訊，採取修正動作、啟動事件，或採取其他動作。

例如，每當您的帳戶中發生下列 Audit Manager 事件時，您可以進行偵測：

- 稽核擁有者建立、更新或刪除評估
- 稽核擁有者委派控制集以供檢閱
- 委派人員完成其檢閱，並將已檢閱的控制集交回稽核擁有者
- 稽核擁有者更新評估控制項的狀態

可以自動觸發的動作如下：

- 使用 AWS Lambda 函數將通知傳遞給 Slack 通道。
- 將有關檢查的資料推送到 Amazon Kinesis Data Streams，以支援完整且即時的狀態監控。
- 向您的電子郵件傳送 Amazon Simple Notification Service (Amazon SNS) 主題。
- 通過 Amazon CloudWatch 警報操作獲得通知。

### Note

Audit Manager 持續傳遞事件。這表示 Audit Manager 至少會成功嘗試將事件傳遞至 EventBridge 少一次。如果事件因為 EventBridge 服務中斷而無法傳遞，則 Audit Manager 將於稍後重試最多 24 小時。

## EventBridge Audit Manager 的範例格式

下列 JSON 程式碼顯示 Audit Manager 中評估建立事件的範例。如需有關此事件中任何欄位的資訊，請參閱[事件結構參考](#)。

```
{  
  "version": "0",
```

```
"id": "55c5a6f3-6183-3989-49ec-a3c998857644",
"detail-type": "Assessment Created",
"source": "aws.auditmanager",
"account": "111122223333",
"time": "2023-07-27T00:38:33Z",
"region": "us-west-2",
"resources":
  [
    "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
  ],
"detail":
{
  "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
  "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
  "assessmentTenantId": "111122223333",
  "assessmentName": "myAssessment",
  "eventTime": 1690418289068,
  "eventName": "CREATE",
  "eventType": "ASSESSMENT",
  "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
}
```

## 建立 EventBridge 規則的先決條件

建議您在為 Audit Manager 事件建立規則之前，執行以下操作：

- 熟悉中的事件、規則和目標。EventBridge 如需詳細資訊，請參閱 [什麼是 Amazon EventBridge？](#) 在 Amazon 用 EventBridge 戶指南。
- 建立要在事件規則中使用的目標。例如，您可建立 Amazon SNS 主題，以便每當完成控制集檢閱時，您都會收到文字訊息或電子郵件。如需詳細資訊，請參閱 [EventBridge 目標](#)。

## 建立 Audit Manager 的 EventBridge 規則

請遵循下列步驟來建立在 Audit Manager 發出的事件上觸發的 EventBridge 規則。盡可能發出事件。

### 建立 Audit Manager EventBridge 規則的步驟

1. 在 <https://console.aws.amazon.com/events/> 打開 Amazon EventBridge 控制台。
2. 在導覽窗格中，選擇規則。

3. 選擇建立規則。
4. 在定義規則詳細資訊頁面中，輸入規則名稱和描述。
5. 請保留事件匯流排和規則類型的預設值，然後選擇 下一步。
6. 在 [建立事件模式] 頁面上，針對 [事件來源] 選擇AWS 事件或 EventBridge 合作夥伴事件。
7. 對於建立方法，選擇自訂模式 (JSON 編輯器)。
8. 在事件模式下，以 JSON 撰寫事件模式，並指定要用於比對的欄位。

如需比對 Audit Manager 事件，您可以使用以下簡單模式：

```
{
  "detail-type": ["Event"]
}
```

以下列其中一個支援的值取代##：

- a. 輸入 Assessment Created 以在建立評估時收到通知。
- b. 輸入 Assessment Updated 以在更新評估時收到通知。
- c. 輸入 Assessment Deleted 以在刪除評估時收到通知。
- d. 輸入 Assessment ControlSet Delegation Created 以在委派控制集進行檢閱時收到通知。
- e. 輸入 Assessment ControlSet Reviewed 以在檢閱評估控制集時收到通知。
- f. 輸入 Assessment Control Reviewed 以在檢閱評估控制項時收到通知。

 Tip

根據需要將更多欄位添加到您的事件模式中。如需有關可用欄位的詳細資訊，請參閱 [Amazon EventBridge 事件模式](#)。

9. 選擇下一步。
10. 在選擇目標頁面上，選擇您為此規則建立的目標類型，然後設定該類型所需的任何其他選項。例如，如果您選擇 Amazon SNS，請確認您的 SNS 主題設定正確，以便透過電子郵件或簡訊通知您。

**i** Tip

顯示的欄位會因選擇的服務而異。如需有關可用目標的詳細資訊，請參閱 [EventBridge 主控台中可用的目標](#)。

11. 對於許多目標類型，EventBridge 需要將事件傳送至目標的權限。在這些情況下，EventBridge 可以建立執行規則所需的 IAM 角色。
  - a. 如需自動建立 IAM 角色，請選擇 為此特定資源建立新角色。
  - b. 如需使用您早前建立的 IAM 角色，請選擇 使用現有角色。
12. (選用) 選擇新增其他目標，為此規則新增另一個目標。
13. 選擇下一步。
14. (選用) 在 設定標籤頁面，新增任何標籤，然後選擇下一步。
15. 在檢閱並建立頁面上，檢閱您的規則設定，並確定其符合您的事件監控要求。
16. 選擇建立規則。您的規則現在將監控 Audit Manager 事件，然後將這些事件傳送至您指定的目標。

## 使用記錄 AWS Audit Manager API 呼叫 CloudTrail

Audit Manager 與服務整合 CloudTrail，可提供使用者、角色或 Audit Manager AWS 服務中所採取的動作記錄的服務。CloudTrail 將 Audit Manager 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Audit Manager 主控台進行的呼叫，以及針對 Audit Manager API 操作的程式碼呼叫。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Audit Manager 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 Audit Manager 提出的請求、提出請求的 IP 位址、提出請求的人員、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 用者指南](#)。

## Audit Manager 資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶時啟用。當活動在 Audit Manager 中發生時，該活動會與事件歷程記錄中的其他 CloudTrail AWS 服務事件一起記錄在事件中。

您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱 [檢視具有事 CloudTrail 件記錄的事件](#)。

如需您的正在進行中的 AWS 帳戶事件記錄 (包括 Audit Manager 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。

此外，您可以設定其他，AWS 服務以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務與整合](#)
- [設定 Amazon SNS 通知 CloudTrail](#)
- [從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔](#)

所有 Audit Manager 動作都會記錄在 API 參考中，CloudTrail 並記錄在 [AWS Audit Manager API 參考](#)中。例如，對 `CreateControlDeleteControl`、和 `UpdateAssessmentFramework` API 作業的呼叫會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

如需詳細資訊，請參閱 [CloudTrail 使用 userIdentity 元素](#)。

## 了解 Audit Manager 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範 [CreateAssessment](#) 動作的 CloudTrail 記錄項目。

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
```

```
arn:"arn:aws:iam::accountId:user/userName",
accountId:"111122223333",
accessKeyId:"accessKeyId",
userName:"userName",
sessionContext:{
  sessionIssuer:{
  },
  webIdFederationData:{
  },
  attributes:{
    mfaAuthenticated:"false",
    creationDate:"2020-11-19T07:32:06Z"
  }
},
eventTime:"2020-11-19T07:32:36Z",
eventSource:"auditmanager.amazonaws.com",
eventName:"CreateAssessment",
awsRegion:"us-west-2",
sourceIPAddress:"sourceIPAddress",
userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
requestParameters:{
  frameworkId:"frameworkId",
  assessmentReportsDestination:{
    destination:"****",
    destinationType:"S3"
  },
  clientToken:"****",
  scope:{
    awsServices:[
      {
        serviceName:"license-manager"
      }
    ],
    awsAccounts:"****"
  },
  roles:"****",
  name:"****",
  description:"****",
  tags:"****"
},
responseElements:{
  assessment:"****"
```

```
  },
  requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
  eventID:"a782029a-959e-4549-81df-9f6596775cb0",
  readOnly:false,
  eventType:"AwsApiCall",
  recipientAccountId:"recipientAccountId"
}
```

## 了解中的配置和漏洞分析 AWS Audit Manager

配置和 IT 控制是我們的客戶 AWS 之間共同責任。如需詳細資訊，請參閱 AWS [共用的責任模型](#)。

# 建立 AWS Audit Manager 資源 AWS CloudFormation

AWS Audit Manager 與整合的服務可協助您建立資源模型並設定資源 AWS 源 AWS CloudFormation，以減少建立和管理資源和基礎架構的時間。您可以建立描述您想要的所有 AWS 資源 (例如評量) 的範本，並為您 AWS CloudFormation 佈建和設定這些資源。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定 Audit Manager 資源。描述您的資源一次，然後在多個 AWS 帳戶和區域中一遍又一遍地佈建相同的資源。

## Audit Manager 和 AWS CloudFormation 範本

如需佈建和設定 Audit Manager 與相關服務的資源，您必須了解 [AWS CloudFormation 範本](#)。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，可以使用 AWS CloudFormation 設計師來協助您開始 AWS CloudFormation 使用範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南中的 [什麼是 AWS CloudFormation 設計器？](#)。

Audit Manager 支援在中建立評量 AWS CloudFormation。如需更多詳細資訊 (包括評估的 JSON 和 YAML 範本範例)，請參閱 AWS CloudFormation 使用者指南中的 [AWS Audit Manager 資源類型參考](#)。

## 進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- [AWS CloudFormation](#)
- [AWS CloudFormation 使用者指南](#)
- [AWS CloudFormation API 參考](#)
- [AWS CloudFormation 指令行介面使用者指南](#)



## 搭 AWS Audit Manager 配 AWS SDK 使用

AWS 軟件開發套件 ( SDK ) 可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和文件，讓開發人員以偏好的語言建置應用程式。

SDK 文件	此服務特定文件	程式碼範例
<a href="#">AWS SDK for C++</a>	<a href="#">AWS SDK for C++ Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for C++ 程式碼範例</a>
<a href="#">AWS SDK for Go</a>	<a href="#">AWS SDK for Go Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for Go 程式碼範例</a>
<a href="#">AWS SDK for Java</a>	<a href="#">AWS SDK for Java 2.x Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for Java 程式碼範例</a>
<a href="#">AWS SDK for JavaScript</a>	<a href="#">AWS SDK for JavaScript Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for JavaScript 程式碼範例</a>
<a href="#">AWS SDK for .NET</a>	<a href="#">AWS SDK for .NET Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for .NET 程式碼範例</a>
<a href="#">AWS SDK for PHP</a>	<a href="#">AWS SDK for PHP Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for PHP 程式碼範例</a>
<a href="#">AWS SDK for Python (Boto3)</a>	<a href="#">AWS SDK for Python (Boto) Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for Python (Boto3) 程式碼範例</a>
<a href="#">AWS SDK for Ruby</a>	<a href="#">AWS SDK for Ruby Audit Manager 的 API 參考</a>	<a href="#">AWS SDK for Ruby 程式碼範例</a>

如需此服務專屬的範例，請參閱 [Audit Manager 使用 AWS SDK 的程式碼範例](#)。

### Note

Audit Manager 在核心版本 1.19.32 及更新版本 AWS SDK for Python (Boto3) 中提供。開始使用 SDK 之前，請確定您使用的是適當的核心版本。

# 禁用 AWS Audit Manager

如果您不想再使用此服務，您可以停用 Audit Manager。當您停用 Audit Manager 時，您也可以選擇刪除所有資料。

依預設，停用 Audit Manager 時，不會刪除您的資料。您的證據資料會自建立之日起保留兩年。您的其他 Audit Manager 資源 (包括評估、自訂控制項和自訂架構) 會無限期保留，您日後重新啟用 Audit Manager 即可使用這些資源。如需有關資料保留的詳細資訊，請參閱本指南中的[資料保護](#)。

如果您選擇刪除資料，Audit Manager 會刪除所有證據資料以及您建立的所有 Audit Manager 資源 (包括評估、自訂控制項和自訂架構)。您的所有資料都會在停用 Audit Manager 後七天內刪除。

## 主題

- [程序](#)
- [後續步驟](#)
- [其他資源](#)

## 程序

您可以使用 Audit Manager 主控台、AWS Command Line Interface (AWS CLI) 或 Audit Manager 員 API 來停用稽核管理員。

### Warning

- 當您停用 Audit Manager 時，您的存取權即會撤銷，且該服務不再收集任何現有評估的證據。除非您重新啟用 Audit Manager，否則您無法存取服務中的任何內容。
- 刪除所有資料屬於永久動作。即使您決定日後重新啟用 Audit Manager，您的資料也無法復原。

## Audit Manager console

若要在 Audit Manager 主控台上停用 Audit Manager

1. 從一般設定索引標籤，前往停用 AWS Audit Manager 區段。
2. 選擇停用。

3. 在快顯視窗中，檢閱您目前的資料保留設定。
  - a. 選擇停用 Audit Manager 繼續下一步。
  - b. 如需變更您目前的選擇，請執行下列步驟：
    - i. 選擇取消以返回設定頁面。
    - ii. 如需使用預設的資料保留設定，請關閉刪除所有資料。此選項會保留證據資料，時間為從建立之日起兩年，並無限期保留其他 Audit Manager 資源。
    - iii. 如需刪除資料，請開啟刪除所有資料。
    - iv. 選擇停用，然後選擇停用 Audit Manager 以確認您的選擇。

## AWS CLI

### 開始之前

停用 Audit Manager 之前，您可以執行 [update-settings](#) 命令設定您的首選資料保留政策。依預設，Audit Manager 會保留您的資料。如果您要請求刪除資料，請使用 `--deregistration-policy` 參數，並將 `deleteResources` 值設定為 ALL。

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

### 若要在中停用 Audit Manager AWS CLI

當您準備好停用 Audit Manager 時，請執行 [deregister-account](#) 命令。

```
aws auditmanager deregister-account
```

## Audit Manager API

### 開始之前

停用 Audit Manager 之前，您可以使用 [UpdateSettings](#) API 作業來設定偏好的資料保留原則。依預設，Audit Manager 會保留您的資料。如果要刪除數據，則可以使用該 [DeregistrationPolicy](#) 屬性請求刪除數據。

### 若要使用 API 停用 Audit Manager

當您準備好停用 Audit Manager 時，請呼叫 [DeregisterAccount](#) 作業。

如需詳細資訊，請選擇先前的連結以閱讀 Audit Manager API 參考中的更多資訊。這包括有關如何在其中一個特定語言 AWS SDK 中使用這些操作和參數的資訊。

## 後續步驟

如果您需要在停用 Audit Manager 之後重新啟用它，請遵循下列步驟讓服務重新啟動並執行。

如需在停用 Audit Manager 之後重新啟用 Audit Manager

前往 Audit Manager 服務首頁，並依照步驟將 Audit Manager 設定為新使用者。如需詳細資訊，請參閱 [使用建議 AWS Audit Manager 的設定進行設定](#)。

### Tip

- 如果您選擇在停用 Audit Manager 時刪除資料，則必須等到資料刪除後才能重新啟用服務。視您擁有的資料量而定，最多可能需要七天的時間。但是，在此之前，您可隨時嘗試重新啟用 Audit Manager。在多數情況下，資料會在短短一小時內刪除。
- 如果您在停用 Audit Manager 時選擇不刪除資料，則您現有的評估會進入休眠狀態，並因此停止收集證據。如需重新開始收集既有評估的證據，請[編輯評估](#)並選擇儲存，而不進行任何變更。

## 其他資源

- 如需 Audit Manager 中資料保留的詳細資訊，請參閱本指南中的[資料保護](#)。

# AWS Audit Manager 用戶指南的文檔歷史記錄

下表說明從 2020 年 12 月 8 日起，每個版本的「AWS Audit Manager 使用者指南」中的重要變更。

變更	描述	日期
<a href="#">支援的新架構：AWS 生成式 AI 最佳實務 v2</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">AWS 生成式 AI 最佳實務架構 v2</a> 。	2024年6月11日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2024年6月10日
<a href="#">使用通用控制項來簡化針對企業控制項執行評估的方式</a>	當您建立自訂控制項時，您現在可以使用通用控制項做為證據來源。每個通用控制項都會對應至相關 AWS 資料來源的受管理群組。這些預先定義的分組可簡化證據收集，無需識別哪些 AWS 資源需要針對指定控制項進行評估。如需如何尋找通用控制項並將其用作證據來源的詳細資訊，請參閱 <a href="#">Control 程式庫</a> 。	2024年6月6日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2024年5月17日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已更新政策 <a href="#">AWSAuditManagerAdmin</a>	2024年5月15日

	<a href="#">inistratorAccess</a> 策。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager的AWS 受管政策</a> 。	
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager的AWS 受管政策</a> 。	2024年5月15日
<a href="#">Support 其他 AWS API 呼叫</a>	您現在可以在 Audit Manager 中使用其他 AWS API 呼叫做為自訂控制項的資料來源。如需詳細資訊，請參閱 <a href="#">自訂控制項資料來源支援的 API 呼叫</a> 。	2024年5月15日
<a href="#">支援的新架構：PCI DSS V4.0</a>	新的預先建置架構現已在 AWS Audit Manager提供。如需詳細資訊，請參閱 <a href="#">PCI DSS V4.0</a> 。	2023 年 12 月 19 日
<a href="#">Support 其他 AWS API 呼叫</a>	您現在可以在 Audit Manager 中使用其他 AWS API 呼叫做為自訂控制項的資料來源。如需詳細資訊，請參閱 <a href="#">自訂控制項資料來源支援的 API 呼叫</a> 。	2023 年 12 月 7 日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager的AWS 受管政策</a> 。	2023 年 12 月 6 日
<a href="#">Support AWS Security Hub 整合的控制項發現</a>	Audit Manager 現在支援中的合併控制項 AWS Security Hub。如需詳細資訊，請參閱 <a href="#">支援的AWS Security Hub 控制項 AWS Audit Manager</a> 。	2023 年 11 月 16 日

<a href="#">與整合 MetricStream</a>	您現在可以將 Audit Manager 的證據擷取到 MetricStream。如需詳細資訊，請參閱 <a href="#">與第三方 GRC 產品的整合</a> 。	2023 年 11 月 14 日
<a href="#">新的支援架構：AWS 生成式 AI 最佳實務</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">AWS 生成式 AI 最佳實務架構 v1</a> 。	2023 年 11 月 8 日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2023 年 11 月 6 日
<a href="#">與 Amazon 集成 EventBridge</a>	您現在可以監視發生在中的事件，AWS Audit Manager 並將這些事件用作事件驅動架構的一部分。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 使用 Amazon 進行監控 EventBridge</a> 。	2023 年 8 月 18 日
<a href="#">支援風險評估和新的手動證據選項</a>	您現在可以使用自訂控制項建立流程來支援風險評估。現在，一個控制項可以代表一個風險評估問題，您可以透過上傳檔案或輸入文字作為手動證據來提供答案。如需詳細資訊，請參閱 <a href="#">建立自訂控制項</a> 和 <a href="#">新增手動證據</a> 。	2023 年 6 月 12 日
<a href="#">支援 CSV 匯出</a>	您現在可以匯出 CSV 格式的證據搜尋工具的搜尋結果。如需詳細資訊，請參閱 <a href="#">匯出搜尋結果</a> 。	2023 年 6 月 9 日

<a href="#">新支援架構：澳大利亞網路安全中心 (ACSC) 資訊安全手冊</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">澳大利亞網路安全中心 (ACSC) 資訊安全手冊</a> 。	2023 年 3 月 24 日
<a href="#">改善的評估報告</a>	我們改善了 Audit Manager 評估報告的格式和內容。如需有關如何導覽及理解評估報告的詳細資訊，請參閱 <a href="#">評估報告</a> 。	2023 年 3 月 23 日
<a href="#">支援分頁 API 呼叫</a>	AWS Audit Manager 現在支援分頁 API 呼叫做為證據收集的資料來源。如需詳細資訊，請參閱 <a href="#">分頁 API 呼叫</a> 。	2023 年 3 月 8 日
<a href="#">新支援架構：HIPAA 最終綜合安全規則 2013</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">HIPAA 最終綜合安全規則 2013</a> 。出於差異化目的，之前存在的 HIPAA 架構 (在架構程式庫中層稱為 HIPAA) 現在命名為 <a href="#">HIPAA 安全規則 2003</a> 。	2023 年 3 月 8 日
<a href="#">Support 其他 AWS API 呼叫</a>	您現在可以使用額外的九個 AWS API 呼叫做為 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱 <a href="#">自訂控制項資料來源支援的 API 呼叫</a> 。	2023 年 3 月 3 日
<a href="#">更新了指南以符合 IAM 最佳實務</a>	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 <a href="#">IAM 中的安全最佳實務</a> 。	2023 年 1 月 6 日



[新資料保留設定](#)

現在，您可以指定是否要在停用 Audit Manager 時刪除所有資料。如需詳細資訊，請參閱 [停用 AWS Audit Manager 和刪除 Audit Manager 資料](#)。

2023 年 1 月 6 日

[支援證據搜尋工具](#)

您現在可以使用證據搜尋工具對證據資料執行搜尋查詢。如需詳細資訊，請參閱 [證據搜尋工具疑難排解](#)。

2022 年 11 月 18 日

[新支援架構：澳大利亞網路安全中心 \(ACSC\) 基本八項策略](#)

新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 [澳大利亞網路安全中心 \(ACSC\) 基本八項策略](#)。

2022 年 8 月 24 日

[更新的 AWS 受管政策](#)

AWS Audit Manager 已經更新了 [AWSAuditManagerServiceRolePolicy](#)。如需詳細資訊，請參閱 [AWS Audit Manager 的 AWS 受管政策](#)。

2022 年 7 月 7 日

[更新的 AWS 受管政策](#)

AWS Audit Manager 已經更新了 [AWSAuditManagerServiceRolePolicy](#)。如需詳細資訊，請參閱 [AWS Audit Manager 的 AWS 受管政策](#)。

2022 年 5 月 20 日

[新支援架構：加拿大網路安全中心中型雲端控制設定檔](#)

新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 [加拿大網路安全中心中型雲端控制設定檔](#)。

2022 年 5 月 6 日

<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已更新政策 <a href="#">AWSAuditManagerAdministratorAccess</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2022 年 4 月 29 日
<a href="#">Support 其他 AWS Config 受管規則</a>	您現在可以使用額外的 91 個 AWS Config 受管規則做為 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱 <a href="#">搭配使用 AWS Config 受管規則 AWS Audit Manager</a> 。	2022 年 4 月 27 日
<a href="#">Support AWS Config 自訂規則</a>	您現在可以使用 AWS Config 自訂規則做為 Audit Manager 中自訂控制項的資料來源。如需詳細資訊，請參閱 <a href="#">搭配使用 AWS Config 自訂規則 AWS Audit Manager</a> 。	2022 年 4 月 27 日
<a href="#">新支援架構：ISO/IEC 27001:2013 附件 A</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">ISO/IEC 27001:2013 附件 A</a> 。	2022 年 4 月 7 日
<a href="#">更新的 AWS 受管政策</a>	AWS Audit Manager 已經更新了 <a href="#">AWSAuditManagerServiceRolePolicy</a> 。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2022 年 3 月 16 日

[新支援架構：適用於 CIS Amazon Web Services Foundations Benchmark v1.4 的 CIS 基準](#)

現在提供了兩個新的預構建框架 AWS Audit Manager：CIS Amazon Web Services 基準 v1.4，1 級和 CIS 基準測試 CIS Amazon Web Services 基準測試 v1.4，1 級和 2。如需詳細資訊，請參閱 [適用於 CIS AWS Audit Manager Foundations Benchmark v1.4.0 的 CIS 基準](#)。

2022 年 3 月 2 日

[新支援架構：CIS 控制措施 v8 IG1](#)

新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 [CIS 控制項 v8 IG1](#)。

2022 年 3 月 2 日

[AWS Audit Manager 儀表板](#)

您現在可以使用 Audit Manager 儀表板來監控您的作用中評估，並快速識別不合規的證據。如需詳細資訊，請參閱 [使用 Audit Manager 儀表板](#)。

2021 年 11 月 18 日

[自訂架構共用](#)

您現在可以與其他人共用自訂 Audit Manager 架構 AWS 帳戶，或將它們複製到您自己帳戶 AWS 區域下的另一個架構。如需詳細資訊，請參閱 [共用自訂架構](#)。

2021 年 10 月 22 日

[AWS Audit Manager 控制項的新範例](#)

您現在可以檢閱控制項範例，並瞭解 Audit Manager 如何協助您的 AWS 環境符合其需求。如需詳細資訊，請參閱 [AWS Audit Manager 控制項範例](#)。

2021 年 9 月 21 日

<a href="#">新支援架構：金融服務業現代化法 (GLBA)</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">金融服務業現代化法 (GLBA)</a> 。	2021 年 9 月 2 日
<a href="#">新增疑難排解章</a>	添加了疑難排解章節。如需詳細資訊，請參閱 <a href="#">中的疑難排解 AWS Audit Manager</a> 。	2021 年 8 月 23 日
<a href="#">新增委派章節和教學課程</a>	我們擴展了委派文件，編為新章節。如需詳細資訊，請參閱 <a href="#">中 AWS Audit Manager 的委託</a> 。我們也新增了一個新的教學課程，針對在中首次檢閱控制項集的委派 AWS Audit Manager。如需詳細資訊，請參閱 <a href="#">委派代表教學課程：檢閱控制集</a> 。	2021 年 6 月 25 日
<a href="#">新支援架構：NIST SP 800-171 Rev. 2</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">NIST SP 800-171 Rev. 2</a> 。	2021 年 6 月 17 日
<a href="#">改善的評估報告</a>	我們改善了 AWS Audit Manager 評估報告的格式和內容。有關如何導覽和理解新評估報告的詳細資訊，請參閱 <a href="#">評估報告</a> 。	2021 年 6 月 8 日
<a href="#">新的 AWS 受管理策略頁面</a>	AWS Audit Manager 已開始追蹤其受管理策略的變更。如需詳細資訊，請參閱 <a href="#">AWS Audit Manager 的 AWS 受管政策</a> 。	2021 年 5 月 6 日

<a href="#">新支援架構：NIST 網路安全架構 1.1 版</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">NIST 網路安全架構 1.1 版</a> 。	2021 年 5 月 5 日
<a href="#">支持的新框架：AWS Well-Architected</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">AWS Well-Architected</a> 。	2021 年 5 月 5 日
<a href="#">支援的新架構：AWS 基礎安全性最佳做法</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">AWS 基礎安全最佳實務</a> 。	2021 年 5 月 5 日
<a href="#">新支援架構：GxP 歐盟附件 11</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">GxP 歐盟附件 11</a> 。	2021 年 4 月 28 日
<a href="#">新支援架構：NIST 800-53 (Rev. 5) 低-中-高</a>	新的預先建置架構現已在 AWS Audit Manager 提供。如需詳細資訊，請參閱 <a href="#">NIST 800-53 (Rev. 5) 低-中-高</a> 。	2021 年 3 月 25 日
<a href="#">新支持的框架：CIS 基準基準 V1.3 的 CIS AWS Audit Manager 基準</a>	現在提供了兩個新的預構建框架 AWS Audit Manager：獨聯體基準 AWS Audit Manager 基準 v1.3.0，1 級和獨聯體基準 v1.3.0，1 級和 2 的獨聯體 AWS Audit Manager 基準測試。如需詳細資訊，請參閱 <a href="#">適用於 CIS AWS Audit Manager Foundations Benchmark v1.3.0 的 CIS 基準</a> 。	2021 年 3 月 22 日
<a href="#">初始版本</a>	AWS Audit Manager 用戶指南和 API 參考的初始版本。	2020 年 12 月 8 日

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。