使用者指南

AWS Security Hub

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

AWS Security Hub: 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 Security Hub？ 1
安全中心的優點 1
存取 Security Hub 2
相關服務 3
Security Hub 免費試用、使用和定價 3
檢視用量詳細資訊與預估成本 4
定價詳情 4
術語與概念 5
先決條件和建議 10
與整合 AWS Organizations 10
使用中央配置 10
配置 AWS Config 11
啟用 AWS Config 11
在中開啟資源記錄 AWS Config 12
啟用 Security Hub 14
驗證必要的權限 14
透過 Organizations 整合啟用 Security Hub 14
手動啟用 Security Hub 15
多帳戶啟用腳本 17
啟用 Security Hub 後的後續步驟 17
中央配置 18
中央組態的優點 18
誰應該使用中央配置？ 19
中央組態術語和概念 19
開始使用中央配置 23
中央組態的先決條件 24
啟動集中配置 25
選擇管理類型 27
指定自我管理帳戶的設定 28
選擇帳戶和 OU 的管理類型 28
組態原則的運作方式 30
政策考量 30
組態原則的類型 31
通過應用和繼承來關聯政策 32

測試組態原則 33
建立和關聯組態原則 34
檢視組態原則 38
組態的關聯狀態 41
關聯失敗的常見原因 42
更新組態原則 43
刪除和取消關聯組態原則 46
刪除組態原則 47
取消設定與帳戶和 OU 的關聯 48
上下文中的配置 50
在內容中配置安全性標準 50
在內容中配置安全性控制 50
停止使用中央配置 51
管理管理員和成員帳戶 54
透過 AWS Organizations 管理帳戶 54
透過邀請手動管理帳戶 55
管理帳戶 AWS Organizations 55
整合 Security Hub AWS Organizations 56
在新帳戶中自動啟用安全中心 61
在新帳戶中手動啟用安全中心 63
取消組織成員帳戶的關聯 65
停用與整合 AWS Organizations 66
應邀管理帳戶 68
新增和邀請成員帳戶 69
回應邀請 72
取消關聯成員帳戶 74
刪除成員帳戶 75
取消與管理員帳戶的關聯 76
過渡到 AWS Organizations 78
帳號允許的動作 79
限制與建議 84
成員帳戶的數目上限 84
帳戶和區域 84
管理員與成員關係的限制 84
跨服務協調管理員帳戶 85
帳戶動作對 Security Hub 資料的影響 85

Security Hub 已停用 85
取消與管理員帳戶關聯的成員帳戶 86
已從組織中移除成員帳戶 86
帳戶被暫停 86
帳戶已關閉 87
跨區域彙總 88
跨區域彙總的運作方式 88
彙總新資料並將更新複製到資料 89
決定要彙總資料的帳戶 90
中央組態與跨區域彙總 90
啟用跨區域彙總 91
啟用跨區域彙總 (主控台) 91
啟用跨區域彙總 (Security Hub API、 AWS CLI) 92
檢視跨區域彙總設定 92
檢視跨區域彙總組態 (主控台) 93
檢視目前的跨區域彙總組態 (Security Hub API、 AWS CLI) 93
更新組態 93
更新跨區域彙總組態 (主控台) 94
更新跨區域彙總組態 (Security Hub API、 AWS CLI) 94
停止跨區域彙總 95
停止跨區域彙總 (主控台) 95
停止跨區域彙總 (Security Hub API、 AWS CLI) 96
問題清單 97
建立及更新發現項目 97
使用 BatchImportFindings 98
使用 BatchUpdateFindings 102
檢視跨區域搜尋結果彙總 107
檢視尋找清單與詳細資訊 107
篩選和分組發現項目 (主控台) 108
檢視發現項目詳細資料 111
對發現採取行動 116
設定發現項目的工作流程狀態 116
將問題清單傳送至自訂動作 118
問題清單格式 119
ASFF 語法 119
合併與出貨預付 199

售後範例 250
深入分析 394
檢視和篩選深入解析清單 394
檢視洞見結果和問題清單 395
檢視分析結果並對其採取處理行動 (主控台) 395
檢視見解結果 (Security Hub API、AWS CLI) 396
檢視見解結果的發現項目 (主控台) 396
受管的洞見 397
自訂洞見 407
建立自訂分析 (主控台) 408
建立自訂分析 (程式設計) 409
修改自訂分析 (主控台) 410
修改自訂分析 (程式設計) 411
從受管理的分析 (主控台) 建立新的自訂分析 413
刪除自訂分析 (主控台) 413
刪除自訂分析 (程式設計) 414
自動化 416
自動化規則 416
自動化規則如何運作 417
可用的規則條件和規則動作 418
建立自動化規則 424
檢視自動化規則 429
編輯自動化規則 430
刪除自動化規則 434
自動化規則範例 435
自動化回應與補救 442
EventBridge 整合類型 443
EventBridge 事件格式 445
設定自動傳送發現項目的規則 447
配置和使用自訂動作 452
產品整合 457
管理產品整合 457
檢視和篩選整合清單 (主控台) 458
檢視產品整合的相關資訊 (資訊 Security Hub API、AWS CLI) 458
啟用整合 459
停用和啟用從整合接收問題清單的流程 (主控台) 459

從整合停用發現項目的流程 (Security Hub API,AWS CLI) 460
啟用來自整合的發現項目流程 (Security Hub API、AWS CLI) 460
檢視整合傳送的問題清單 461
AWS 服務 整合 461
與 Security Hub 的AWS服務整合概觀 462
AWS將發現項目傳送至 Security Hub 的服務 463
AWS從 Security Hub 接收發現項目的服務 476
第三方產品整合 478
與 Security Hub 的第三方整合概觀 479
將發現項目傳送至 Security Hub 的第三方整 488
從 Security Hub 接收發現的第三方整合 504
第三方整合，可將發現項目傳送至 Security Hub 並從中接收發現 510
使用自訂產品整合 511
傳送自訂安全產品問題清單的需求與建議 512
從自訂產品更新問題清單 513
自訂整合範例 513
標準和控制 514
適用於標準和控制的 IAM 許可 514
安全檢查和分數 515
AWS Config 規則和安全檢查 516
控制項發現項目所需 AWS Config 資源 517
執行安全檢查的排程 546
產生及更新控制項發現項 547
法規遵循狀態和控制狀態 558
決定安全分數 560
標準參考 562
AWS FSBP 562
獨聯體 AWS 基金會基準 V1.2.0 和 1.4.0 版 574
尼斯特 SP 587
PCI DSS 600
服務管理標準 602
檢視和管理安全性標準 613
啟用和停用標準 614
檢視標準的詳細資訊 620
啟用和停用特定標準中的控制項 624
控制項參考 630

AWS 帳戶 控制 686
AWS Certificate Manager 控制 688
API Gateway 控制項 690
AWS AppSync 控制 695
Athena 控制 697
AWS Backup 控制 698
CloudFormation 控制 698
CloudFront 控制 699
CloudTrail 控制 707
CloudWatch 控制 713
CodeBuild 控制 753
AWS Config 控制 757
AWS DMS 控制 759
Amazon DocumentDB 控件 763
控制項 767
Amazon ECR 控制 771
Amazon ECS 控制 773
Amazon EC2 控制項 780
Amazon EC2 Auto Scaling 控制 801
Amazon EC2 Systems Manager 控制 807
Amazon EFS 控制 810
Amazon EKS 控制 813
ElastiCache 控制 816
Elastic Beanstalk 控制 821
Elastic Load Balancing 控制 823
Amazon EMR 控制 835
彈性搜索控件 837
EventBridge 控制 843
Amazon FSx 控制 845
GuardDuty 控制 846
IAM 控制 847
Kinesis 控制 870
AWS KMS 控制 871
Lambda 控制項 874
Amazon Macie 控制 878
Amazon MSK 控制 880

Amazon MQ 控制 881
Neptune 控制 883
Network Firewall 控制 890
OpenSearch 服務控制 895
AWS Private Certificate Authority 控制 902
Amazon RDS 控制 903
Amazon Redshift 控制 926
53 號路線控制 933
Amazon S3 控制 933
SageMaker 控制 954
Secrets Manager 控制 956
Amazon SNS 控制 960
Amazon SQS 控制 963
Step Functions 控制 963
AWS WAF 控制 964
檢視和管理安全性控制 971
合併控制項檢視 971
控制項的整體安全分數 972
控制類別 973
在所有標準中啟用和停用控制項 976
在啟用的標準中自動啟用新控制項 979
自訂控制參數 985
您可能想要停用的控制項 1001
檢視控制項的詳細資訊 1004
篩選和排序控制項 1007
檢視控制項發現項目並採取動作 1008
Dashboard (儀表板) 1028
摘要儀表板的可用小器具 1028
窗口小部件默認顯示 1028
窗口小部件默認隱藏 1030
篩選「摘要」儀表板 1030
建立和儲存篩選器集 1031
更新或刪除過濾器集 1032
自訂摘要控制面板 1032
建立資源 CloudFormation 1034
Security Hub 和 AWS CloudFormation 範本 1034

進一步了解 AWS CloudFormation 1034
訂閱 Security Hub 通告 1036
Amazon SNS 訊息格式 1041
安全 1044
資料保護 1044
身分識別和存取權管理 1045
物件 1046
使用身分驗證 1046
使用政策管理存取權 1049
Security Hub 如何與 IAM 搭配使用 1051
身分型政策範例 1060
服務連結角色 1066
AWS 受管理政策 1069
疑難排解 1078
法規遵循驗證 1081
恢復能力 1082
基礎設施安全性 1082
VPC 端點 (AWS PrivateLink) 1083
安全中心 VPC 端點的考量 1083
建立安全中心的介面 VPC 端點 1083
建立安全性中樞的 VPC 端點原則 1083
共用子網路 1084
記錄 API 呼叫 1085
安全中心資訊 CloudTrail 1085
範例：Security Hub 記錄檔項目 1086
標記資源 1088
標記基本面 1088
在 IAM 政策中使用標籤 1089
將標籤新增至資源 1090
檢閱資源的標籤 1092
編輯資源的標籤 1094
移除資源的標籤 1095
配額 1097
最大配額 1097
費率配額 1097
Security Hub 區域限制 1098

跨區域彙總限制 1098
各區域整合的可用性 1098
在中國（北京）和中國（寧夏）支持的集成 1098
AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 支援的整合 1099
各區域標準的可用性 1100
各區域控制項的可用性 1101
控制區域限制 1101
美國東部 (俄亥俄) 1102
美國東部 (維吉尼亞北部) 1103
美國西部 (加利佛尼亞北部) 1103
美國西部 (奧勒岡) 1104
非洲 (開普敦) 1105
亞太區域 (香港) 1107
亞太區域 (海德拉巴) 1108
亞太區域 (雅加達) 1114
亞太區域 (墨爾本) 1119
亞太區域 (孟買) 1124
亞太區域 (大阪) 1125
亞太區域 (首爾) 1130
亞太區域 (新加坡) 1131
亞太區域 (雪梨) 1132
亞太區域 (東京) 1132
加拿大 (中部) 1133
加拿大西部 (卡加利) 1134
中國 (北京) 1142
中國 (寧夏) 1145
歐洲 (法蘭克福) 1149
歐洲 (愛爾蘭) 1149
歐洲 (倫敦) 1150
歐洲 (米蘭) 1151
Europe (Paris) 1153
歐洲 (西班牙) 1154
歐洲 (斯德哥爾摩) 1161
歐洲 (蘇黎世) 1162
以色列 (特拉維夫) 1168
Middle East (Bahrain) 1175

中東 (阿拉伯聯合大公國) 1176
南美洲 (聖保羅) 1182
AWS GovCloud (美國東部) 1183
AWS GovCloud (美國西部) 1189
停用 Security Hub 1196
控制變更記錄 1198
文件歷史紀錄 1222
..... mcclxxiv

什麼是 AWS Security Hub？

AWSSecurity Hub 為您提供中安全性狀態的全面檢視，AWS並協助您根據安全性產業標準和最佳做法來評估您的AWS環境。

Security Hub 會收集和支援的協力廠商產品之間AWS 帳戶的安全性資料AWS 服務，並協助您分析安全性趨勢並找出最優先順序的安全性問題。

為了協助您管理組織的安全性狀態，Security Hub 支援多種安全性標準。其中包括由開發的AWS基礎安全性最佳實務 (FSBP) 標準AWS，以及外部合規架構，例如網際網路安全中心 (CIS)、支付卡產業資料安全標準 (PCI DSS)，以及美國國家標準與技術研究所 (NIST)。每個標準都包含數個安全控制，每個控制都代表安全性最佳實務。Security Hub 會針對安全性控制執行檢查，並產生控制發現項目，協助您根據安全性最佳實務來評估合規性。

除了產生控制發現之外，Security Hub 還會收到來自其他 AWS 服務 (例如亞馬遜 GuardDuty、Amazon Inspector 和 Amazon Macie) 的發現結果，以及支援的第三方產品。這為您提供了一個單一窗格，解決各種與安全性相關的問題。您也可以將 Security Hub 發現項目傳送給其他AWS服務和支援的協力廠商產品。

Security Hub 提供的自動化功能可協助您分類和修復安全性問題。例如，您可以使用自動化規則，在安全性檢查失敗時自動更新重大發現項目。您也可以利用與 Amazon 的整合 EventBridge 來觸發特定發現項目的自動回應。

主題

- 安全中心的優點
- 存取 Security Hub
- 相關服務
- Security Hub 免費試用和定價

安全中心的優點

以下是 Security Hub 協助您監控整個AWS環境中的合規性和安全性狀態的一些關鍵方式。

可讓您更輕易地收集和排列問題清單的優先順序

Security Hub 可減少收集整合式和合AWS作夥伴產品跨帳戶的安全發現項目AWS 服務並排定優先順序的工作。Security Hub 使用AWS安全性尋找格式 (ASFF) (標準尋找格式) 來處理尋找資料。這

樣就不需要以多種格式管理來自眾多來源的發現項目。Security Hub 也會關聯不同提供者的發現項目，協助您排定最重要的項目的優先順序。

根據最佳實務和標準自動進行安全檢查

Security Hub 會根據AWS最佳實務和業界標準，自動執行連續的帳戶層級組態和安全性檢查。Security Hub 使用這些檢查的結果來計算安全分數，並識別需要注意的特定帳戶和資源。

合併帳戶與提供者問題清單的檢視

Security Hub 會整合帳戶和提供者產品之間的安全發現項目，並在 Security Hub 主控台上顯示結果。您也可以透過安全中心 API 或 SDK 擷取發現項目。AWS CLI透過全面檢視您目前的安全狀態，您可以發現趨勢、識別潛在問題，並採取必要的補救措施。

能夠自動尋找更新和補救

您可以建立根據您定義的條件修改或隱藏發現項目的自動化規則。Security Hub 還支持與 Amazon 的集成 EventBridge。若要自動修復特定發現項目，您可以定義產生搜尋結果時要採取的自訂動作。例如，您可以設定自訂動作，將問題清單傳送到售票系統或自動化修補系統。

存取 Security Hub

Security Hub 在大多數情況下都可用AWS 區域。如需目前提供安全中樞的區域清單，請參閱 AWS AWS 一般參考. 如需管理您的帳戶AWS 區域的相關資訊AWS 帳戶，請參閱AWS Account Management參考指南中的「指定AWS 區域您的帳戶可以使用的項目」。

在每個區域中，您可以透過下列任一方式存取和使用資訊安全中心：

Security Hub 主控台

這AWS Management Console是一個基於瀏覽器的介面，您可以使用它來建立和管理AWS資源。作為該主控台的一部分，Security Hub 主控台可讓您存取您的 Security Hub 帳戶、資料和資源。您可以使用 Security Hub 主控台來執行 Security Hub 工作：檢視發現項目、建立自動化規則、建立彙總區域等等。

Security Hub API

Security Hub API 可讓您以程式設計方式存取您的 Security Hub 帳戶、資料和資源。透過 API，您可以將 HTTPS 要求直接傳送至 Security Hub。如需 API 的相關資訊，請參閱 AWSSecurity Hub API 參考。

AWS CLI

使用AWS CLI，您可以在系統的命令列上執行命令，以執行 Security Hub 工作。在某些情況下，使用命令列可能比使用主控台更快、更方便。如果您想要建置執行工作的指令碼，指令列也很有用。如需安裝與使用 AWS CLI 的詳細資訊，請參閱 AWS Command Line Interface 使用者指南。

AWS SDK

AWS提供包含各種程式設計語言和平台 (例如 Java、Go、Python、C++ 和 .NET) 的程式庫和範例程式碼的開發套件。SDK 提供方便、以程式設計方式存取安全中心及其他您偏好AWS 服務的語言。他們還處理諸如密碼編譯簽名請求，管理錯誤以及自動重試請求等任務。如需有關安裝和使用 AWS SDK 的詳細資訊，請參閱建置在其上AWS的工具。

> **Important**
>
> Security Hub 只會偵測並整合您啟用 Security Hub 之後所產生的發現項目。它不會追溯偵測並整合您啟用 Security Hub 之前產生的安全性發現項目。
> Security Hub 只會在您帳戶中啟用資訊安全中心的區域中接收和處理發現項目。
> 若要完全符合 CIS AWS 基準測試安全性檢查，您必須在所有支援的AWS區域啟用資訊安全中心。

相關服務

為了進一步保護您的AWS環境，請考慮使用其他與安全AWS 服務中心結合使用。

如需其他AWS 服務傳送或接收 Security Hub 發現項目的清單，請參閱AWS 服務與 AWS Security Hub 的整合。

Security Hub 使用服務連結規則AWS Config來執行大部分控制項的安全性檢查。您必須在AWS Config中啟用AWS Config並記錄資源，Security Hub 才能產生大部分的控制項發現項目。如需詳細資訊，請參閱 配置 AWS Config。

Security Hub 免費試用和定價

當您第一次啟用安全中心時，該帳戶會自動註冊 30 天的安全性中心免費試用。AWS 帳戶

當您在免費試用期間使用 Security Hub 時，會向您收取使用 Security Hub 與之互動的其他服務 (例如 AWS Config項目) 的使用費用。只有 Security Hub 標準啟動的AWS Config規則，就不會向您收取費用。

在您的免費試用期結束之前，您不需要支付使用 Security Hub 的費用。

> **Note**
>
> 中國 (北京) 地區不支援安全中心免費試用。

檢視用量詳細資訊與預估成本

Security Hub 提供使用資訊，包括使用 Security Hub 的預估 30 天費用。使用情況詳細資訊包括免費試用的剩餘時間。使用資訊可協助您瞭解 Security Hub 在免費試用期結束後的費用。免費試用期結束後，也可以使用使用信息。

若要顯示使用資訊 (主控台)

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在功能窗格中，選擇 [設定] 下的 [使用]。

預估的每月費用是根據您帳戶的 Security Hub 使用量，以進行 30 天期間預計的發現項目和安全檢查。

使用資訊和估計費用僅適用於目前帳戶和目前區域。在彙總區域中，使用量資訊和預估成本不包含連結的區域。如需連結區域的更多資訊，請參閱the section called “跨區域彙總的運作方式”。

定價詳情

如需 Security Hub 如何針對擷取的發現項目和安全性檢查收費用的詳細資訊，請參閱 Security Hub 定價。

術語與概念

本主題說明AWS安全性中樞中協助您開始使用的重要概念。

帳戶

包含您 AWS 資源的標準 Amazon Web Services (AWS) 帳戶。您可以使用您AWS的帳戶登入並啟用 Security Hub。

帳戶可以邀請其他帳戶啟用 Security Hub，並在 Security Hub 中與該帳戶建立關聯。接受成員邀請為選擇性。如果邀請被接受，該帳戶將成為管理員帳戶，而新增的帳戶是成員帳戶。管理員帳戶可以檢視其成員帳戶中的發現項目。

如果您已註冊AWS Organizations，則您的組織會指定組織的 Security Hub 管理員帳戶。Security Hub 系統管理員帳戶可以啟用其他組織帳戶做為成員帳戶。

帳戶不能同時是管理員帳戶和成員帳戶。一個帳戶只能有一個管理員帳戶。

如需詳細資訊，請參閱管理管理員和成員帳戶。

管理員帳戶

Security Hub 中的一個帳戶，被授與檢視關聯成員帳戶發現項目的存取權。

帳戶會以下列其中一種方式成為系統管理員帳戶：

- 該帳戶會邀請其他帳戶在安全性中心中與該帳戶建立關聯。當這些帳戶接受邀請時，他們就會成為成員帳戶，而邀請帳戶就會成為他們的管理員帳戶。
- 該帳戶由組織管理帳戶指定為 Security Hub 系統管理員帳戶。Security Hub 系統管理員帳戶可以將任何組織帳戶啟用為成員帳戶，也可以邀請其他帳戶成為成員帳戶。

一個帳戶只能有一個管理員帳戶。帳戶不能同時是管理員帳戶和成員帳戶。

聚總區域

設定彙總區域可讓您在單一窗格AWS 區域中檢視多個安全發現項目。

聚總區域是您檢視與管理搜尋結果的「區域」。搜尋結果會從連結區域彙總至聚總區域。發現項目的更新會跨區域複寫。

在彙總區域中，「安全性」標準、「見解」和「發現項目」頁面包含來自所有連結區域的資料。

請參閱 跨區域彙總。

存檔的問題清單

將 RecordState 設為 ARCHIVED 的問題清單。封存發現項目表示尋找項目提供者認為該發現項目已不再相關。記錄狀態與工作流程狀態不同，工作流程狀態會追蹤發現項目的調查狀態。

尋找提供者可以使用 Security Hub API 的BatchImportFindings作業來封存他們所建立的發現項目。如果控制項已停用或刪除關聯的資源，Security Hub 會根據下列其中一項準則，自動封存控制項的發現項目。

- 發現結果不會在三到五天內更新（請注意，這是最好的努力，並不能保證）。
- 會傳回相關聯的AWS Config評估NOT_APPLICABLE。

根據預設，已封存的發現項目會從 Security Hub 主控台的發現項目清單中排除。您可以更新篩選條件以包含已封存的問題清單。

Security Hub API 的GetFindings作業會傳回使用中和封存的發現項目。您可以包含記錄狀態的篩選條件。

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS 安全問題清單格式 (ASFF)

Security Hub 彙總或產生之發現項目內容的標準化格式。AWS安全性尋找項目格式可讓您使用 Security Hub 來檢視和分析安全AWS性服務、協力廠商解決方案或 Security Hub 本身因執行安全性檢查而產生的發現項目。如需詳細資訊，請參閱AWS 安全性搜尋結果格式 (ASFF)。

控制項

為資訊系統或組織規定的一種保護或應對措施，旨在保護其資訊的機密性、完整性和可用性，並符合一組定義的安全需求。安全性標準與控制項集合相關聯。

術語安全控制是指具有跨標準的單一控制項 ID 和標題的控制項。術語標準控制項是指具有標準特定控制項 ID 和標題的控制項。目前，Security Hub 僅支援AWS GovCloud (US) Region和中國區域的標準控制項。所有其他區域都支援安全性控制。

自訂動作

用於將所選發現項目傳送至的 Security Hub 機制 EventBridge。會在安全性中心中建立自訂動作。然後將其連結至 EventBridge 規則。規則會定義一個要在接收到與自訂動作 ID 建立關聯的問題清單時，所要採取的特定動作。例如，您可以使用自訂動作來將特定問題清單，或是一小組問題清單傳送至回應或修補工作流程。如需詳細資訊，請參閱the section called “建立自訂動作 (主控台)”。

委派的管理員帳戶 (Organizations)

在組織中，服務的委派管理員帳戶能夠管理組織服務的使用情況。

在資訊安全中心中，Security Hub 系統管理員帳戶也是 Security Hub 的委派系統管理員帳戶。當組織管理帳戶第一次指定 Security Hub 系統管理員帳戶時，Security Hub 會呼叫組 Organizations，將該帳戶設為委派的系統管理員帳戶。

接著，組織管理帳戶必須選擇委派的系統管理員帳戶做為所有區域中的 Security Hub 系統管理員帳戶。

問題清單

安全檢查或安全性相關偵測的可觀察記錄。Security Hub 會在完成控制項的安全性檢查之後產生一個發現項目。這些稱為控制項發現項目。發現結果也可能來自第三方產品整合。

如需有關安全中心中發現項目的詳細資訊，請參閱問題清單。

> **Note**
>
> 問題清單會在最近更新 90 天後刪除，如果沒有更新，則在建立日期 90 天後刪除。若要存放超過 90 天的發現項目，您可以在將發現項目路由 EventBridge 到 Amazon S3 儲存貯體中設定規則。

跨區域彙總

將發現項目、見解、控制合規狀態和安全分數從連結的區域彙總到彙總區域。然後，您可以從彙總區域檢視所有資料，並從彙總區域更新發現項目和見解。

請參閱 跨區域彙總。

尋找攝入

從其他AWS服務和協力廠商合作夥伴提供者將發現項目匯入 Security Hub。

尋找擷取事件包括新發現項目和現有發現項目的更新。

Insight

彙總陳述式和選用篩選條件定義的相關問題清單集合。該洞見會識別需要注意和介入的安全區域。Security Hub 提供了一些您無法修改的受管理（預設）見解。您也可以建立自訂 Security Hub 深入解析，以追蹤您的AWS環境和使用方式獨有的安全性問題。如需詳細資訊，請參閱深入分析。

連結區域

啟用跨區域彙總時，連結的區域是將發現項目、見解、控制符合性狀態和安全分數彙總至彙總區域的區域。

在連結的區域中，「搜尋結果」與「見解」頁面僅包含來自該區域的發現項目。

請參閱 跨區域彙總。

成員帳戶

已授與管理員帳戶權限以檢視其發現項目並對其採取動作的帳戶。

帳戶會以下列其中一種方式成為會員帳戶：

- 該帳戶接受來自其他帳戶的邀請。
- 若為組織帳戶，Security Hub 系統管理員帳戶會將該帳戶啟用為成員帳戶。

相關要求

映射到控制的一組產業或法規要求。

規則

用於評定是否有遵守控制的一組自動化條件。規則受到評估時，可能會通過或失敗。如果評估無法判斷規則通過或失敗，則規則會處於警告狀態。如果無法評估規則，則規則會處於不可用狀態。

安全檢查

針對單一資源對規則進行特定 point-in-time 評估，導致通過、失敗、警告或無法使用的狀態。執行安全檢查會產生問題清單。

Security Hub 管理員帳戶

管理組織 Security Hub 成員資格的組織帳戶。

組織管理帳戶會在每個區域中指定安全性中樞系統管理員帳戶。組織管理帳戶必須在所有區域中選擇相同的 Security Hub 系統管理員帳戶。

安全性中樞系統管理員帳戶也是 Organizations 中安全性中樞的委派系統管理員帳戶。

Security Hub 系統管理員帳戶可以將任何組織帳戶啟用為成員帳戶。安全中心管理員帳戶也可以邀請其他帳戶成為成員帳戶。

安全標準

針對指定特性主題發佈的陳述式，通常可測量且為控制項形式，必須予以滿足或加以存檔以確保合規性。安全標準可以是以法規框架、最佳實務或內部公司政策為基礎。控制項可能與安全性中樞中的一個或多個支援的標準相關聯。若要深入了解安全性中心中的安全性標準，請參閱標準和控制。

嚴重性

指派給 Security Hub 控制項的嚴重性可識別控制項的重要性。控制項的嚴重性可以是「嚴重」、「高」、「中」、「低」或「資訊」。指派給控制項發現項目的嚴重性等於控制項本身的嚴重性。若要瞭解 Security Hub 如何將嚴重性指派給控制項，請參閱指派嚴重性給控制項發現。

工作流程狀態

調查問題清單的狀態。使用 `Workflow.Status` 屬性追蹤。

最初的工作流程狀態為 `NEW`。如果您通知資源擁有者對搜尋結果採取動作，您可以將工作流程狀態設定為 `NOTIFIED`。如果搜尋結果不是問題，且不需要任何動作，請將工作流程狀態設定為 `SUPPRESSED`。檢閱並修正尋找項目後，請將工作流程狀態設定為 `RESOLVED`。

依預設，大多數的搜尋結果清單只包含工作流程狀態為 `NEW` 或 `NOTIFIED` 的搜尋結果。控制的問題清單也會包含在 `RESOLVED` 的問題清單中。

對於 `GetFindings` 操作，您可以包含工作流程狀態的篩選條件。

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Security Hub 主控台提供設定發現項目工作流程狀態的選項。客戶 (或 SIEM、票證、事件管理或 SOAR 工具代表客戶更新來自問題清單提供者的問題清單) 也可以用 `BatchUpdateFindings` 來更新工作流程狀態。

先決條件和建議

下列必要條件和建議可協助您開始使用 AWS Security Hub。

與整合 AWS Organizations

AWS Organizations 是一項全域帳戶管理服務，可讓管理 AWS 員整合並集中管理多個組織單位 AWS 帳戶 和組織單位 (OU)。它提供帳戶管理和合併帳單功能，旨在支援預算、安全性和合規性需求。它不收取額外費用，並與多個集成 AWS 服務，包括 Security Hub GuardDuty，Amazon 和 Amazon Macie。

為了協助自動化和簡化帳戶管理，我們強烈建議您整合 Security Hub 和 AWS Organizations. 如果您有多個使用資訊 Security Hub 的 Organizations AWS 帳戶 ，則可以與組織整合。

如需啟動整合的指示，請參閱整合 Security Hub AWS Organizations。

使用中央配置

當您整合 Security Hub 和組織時，您可 Organizations 選擇使用稱為中央組態的功能，為您的組織設定和管理 Security Hub。我們強烈建議您使用中央組態，因為它可讓系統管理員自訂組織的安全性涵蓋範圍。在適當情況下，委派的系統管理員可允許成員帳戶設定自己的安全性涵蓋範圍設定。

中央組態可讓委派的系統管理員跨帳戶、OU 和區域設定 Security Hub。委派的系統管理員會藉由建立組態原則來設定 Security Hub。在組態原則中，您可以指定下列設定：

- Security Hub 是否已啟用或停用
- 啟用和停用哪些安全標準
- 啟用和停用哪些安全控制項
- 是否自訂選取控制項的參數

身為委派的系統管理員，您可以為整個組織建立單一組態原則，或為各種帳戶和 OU 建立不同的組態原則。例如，測試帳戶和生產帳戶可以使用不同的配置策略。

使用組態原則的成員帳戶和 OU 會集中管理，且只能由委派的系統管理員進行設定。委派的系統管理員可以將特定的成員帳戶和 OU 指定為自我管理，讓成員能夠依區域設定自己的設定。

若要深入瞭解中央規劃，請參閱安全中心中的集中配置。

配置 AWS Config

AWS Security Hub 使用服務連結 AWS Config 規則對大多數控制項執行安全性檢查。

若要支援這些控制項， AWS Config 必須在每 AWS 區域 個已啟用 Security Hub 的所有帳戶 (包括系統管理員帳戶和成員帳戶) 上啟用。此外，對於每個已啟用的標準，都 AWS Config 必須配置為記錄啟用控制項所需的資源。

我們建議您在啟用 Security Hub 標準之 AWS Config 前，先開啟中的資源記錄。如果 Security Hub 嘗試在資源記錄關閉時執行安全性檢查，則檢查會傳回錯誤。

Security Hub 不會 AWS Config 為您管理。如果您已 AWS Config 啟用，則可以透過 AWS Config 主控台或 API 設定其設定。

如果您啟用標準但尚未啟用 AWS Config，Security Hub 會嘗試根據下列排程建立 AWS Config 規則：

- 在您啟用標準的當天
- 啟用標準的第二天
- 啟用標準後 3 天
- 啟用標準後的 7 天 (之後每 7 天連續一次)

如果您使用中央組態，Security Hub 也會在您重新套用啟用一或多個標準的組態原 AWS Config 則時嘗試建立規則。

啟用 AWS Config

如果 AWS Config 尚未啟用，您可以使用下列其中一種方式啟用它：

- 主控台或 AWS CLI — 您可以 AWS Config 使用 AWS Config 主控台或手動啟用 AWS CLI。請參閱開AWS Config 發人員指南 AWS Config中的開始使用。
- AWS CloudFormation 範本 — 如果您想要在大量帳號 AWS Config 上啟用，可以 AWS Config 使用 [啟用] CloudFormation 範本啟用 AWS Config。若要存取此範本，請參閱《AWS CloudFormation 使用指南》中的範AWS CloudFormation StackSets 例範本。
- Github 腳本 — Security Hub 提供了一個GitHub 腳本，可為跨區域的多個帳戶啟用 Security Hub。如果您尚未與組織整合，或您的帳戶不屬於組織，則此指令碼非常有用。當您使用此指令碼來啟用 Security Hub 時，它也會自動啟 AWS Config 用這些帳戶。

如需啟用 AWS Config 以協助您執行 Security Hub 安全性檢查的詳細資訊，請參閱最 AWS Config 佳化 AWS Security Hub 以有效管理雲端安全性狀態。

在中開啟資源記錄 AWS Config

當您以預設設定開啟中 AWS Config 的資源記錄時，它會記錄所有支援的區域資源類型，這些資源會 AWS Config 探索其執行 AWS 區域 中的所有支援類型。您也可以設定 AWS Config 為記錄支援的全域資源類型。您只需要在單一區域中記錄全域資源 (如果您使用中央設定，我們建議這是您的家區域)。

如果您使用啟 CloudFormation StackSets 用 AWS Config，我們建議您執行兩個不同的功能 StackSets。執行一個， StackSet 以在單一區域中記錄所有資源，包括全域資源。執行一秒鐘， StackSet 以記錄除其他區域中的全域資源以外的所有資源。

您也可以使用「快速設定」功能 AWS Systems Manager，快速設定 AWS Config 跨帳戶和區域的資源記錄。在「快速設定」程序期間，您可以選擇要記錄全域資源的「區域」。若要取得更多資訊，請AWS Config 參閱《AWS Systems Manager 使用指南》中的〈規劃記錄

安全控制項Config.1會在未記錄全域資源的區域中產生失敗的發現項目。這是預期的，您可以使用自動化規則來隱藏這些發現項目。

如果您使用多帳戶指令碼來啟用 Security Hub，它會自動啟用所有區域中所有資源 (包括全域資源) 的資源記錄。然後，您可以更新組態，以便僅在單一區域中記錄全域資源。如需詳細資訊，請參閱AWS Config 開發人員指南中的選取哪些資源 AWS Config 記錄。

若要讓 Security Hub 準確地報告依賴 AWS Config 規則之控制項的發現項目，您必須啟用相關資源的記錄功能。如需控制項及其相關 AWS Config 資源的清單，請參閱AWS Config 產生控制項發現項所需的資源。AWS Config 可讓您在連續記錄和每日記錄資源狀態變更之間進行選擇。如果您選擇每日記錄，如果資源狀態發生變更，則會在每 24 小時期間結束時 AWS Config 傳送資源組態資料。如果沒有變更，則不會傳送任何資料。這可能會延遲產生變更觸發控制項的 Security Hub 發現項目，直到 24 小時期間完成為止。

> **Note**
>
> 若要在安全性檢查後產生新的發現項目並避免發現過時，您必須擁有足夠的權限供附加至組態記錄程式的 IAM 角色，才能評估基礎資源。

成本考量

有關與資源記錄相關的費用的詳細信息，請參閱AWS Security Hub 定價和AWS Config 定價。

Security Hub 可能會透過更新 AWS Config 組態項目來影響您的`AWS::Config::ResourceCompliance`組態記錄程式成本。每當與 AWS Config 規則相關聯的 Security Hub 控制項變更符合性狀態、啟用或停用，或具有參數更新時，都可能會發生更新。如果您僅將 AWS Config 設定記錄程式用於 Security Hub，而且不會將此設定項目用於其他用途，建議您在 AWS Config 主控台或關閉其記錄 AWS CLI。這可以降低您的 AWS Config 成本。您不需要記錄`AWS::Config::ResourceCompliance`安全檢查即可在安全中心中工作。

啟用 Security Hub

有兩種方法可以通過與AWS Organizations或手動集成來啟用AWS安全中心。

我們強烈建議您在多帳戶和多區域環境中與 Organizations 整合。如果您有獨立帳戶，則必須手動設定 Security Hub。

驗證必要的權限

註冊 Amazon Web Services (AWS) 之後，您必須啟用 Security Hub 才能使用其功能和功能。若要啟用資 Security Hub，您必須先設定權限，以便存取 Security Hub 主控台和 API 作業。您或您的管理AWS員可以使用 AWS Identity and Access Management (IAM) 將呼叫的AWS受管政策附加`AWSSecurityHubFullAccess`到 IAM 身分。

若要透過 Organizations 整合來啟用和管理 Security Hub，您也應該附加名為的AWS受管理原則`AWSSecurityHubOrganizationsAccess`。

如需詳細資訊，請參閱AWSAWS Security Hub 的受管理原則。

透過 Organizations 整合啟用 Security Hub

若要開始使用 Security HubAWS Organizations，組織的AWS Organizations管理帳戶會將帳戶指定為組織的 Security Hub 委派系統管理員帳戶。Security Hub 會在目前區域中的委派系統管理員帳戶中自動啟用。

選擇您偏好的方法，然後依照步驟指定委派的管理員。

Security Hub console

若要在上線時指定 Security Hub 委派的系統管理員

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 選擇 [移至 Security Hub]。系統會提示您登入 Organizations 管理帳戶。
3. 在 [指定委派管理員] 頁面的 [委派管理員帳戶] 區段中，指定委派管理員帳戶。建議您選擇您為其他AWS安全性和規範遵循服務設定的相同委派管理員。
4. 選擇設定委派管理員。

Security Hub API

從 Organizations 管理帳戶叫用 `EnableOrganizationAdminAccount`API。提供 Security Hub 委派系統管理員帳戶的AWS 帳戶識別碼。

AWS CLI

從 Organizations 管理帳戶執行`enable-organization-admin-account`命令。提供 Security Hub 委派系統管理員帳戶的AWS 帳戶識別碼。

範例命令：

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

如需與 Organizations 整合的詳細資訊，請參閱整合 Security Hub AWS Organizations。

指定委派的系統管理員之後，我們建議您繼續使用中央設定來設定 Security Hub。控制台會提示您這樣做。透過使用中央設定，您可以簡化為組織啟用和設定 Security Hub 的程序，並確保您的組織擁有足夠的安全性涵蓋範圍。

中央設定可讓委派的系統管理員跨多個組織帳戶和區域自訂 Security Hub，而不是依區域設定。您可以為整個組織建立組態原則，或為不同帳戶和 OU 建立不同的組態原則。這些原則會指定在關聯帳戶中是否啟用或停用 Security Hub，以及啟用哪些安全性標準和控制項。

委派管理員可以將帳戶指定為集中管理或自我管理的帳戶。集中管理的帳戶只能由委派的系統管理員設定。自我管理帳戶可以指定自己的設定。

如果您不使用中央設定，委派的系統管理員可以設定 Security Hub 的能力更有限。如需詳細資訊，請參閱管理帳戶 AWS Organizations。

手動啟用 Security Hub

如果您擁有獨立帳戶或未與之整合，則必須手動啟用 Security Hub AWS Organizations。獨立帳戶無法與整合，AWS Organizations且必須使用手動啟用。

當您手動啟用 Security Hub 時，您可以指定 Security Hub 系統管理員帳戶，並邀請其他帳戶成為成員帳戶。當潛在成員帳戶接受邀請時，就會建立管理員與成員關係。

選擇您偏好的方法，然後按照步驟啟用 Security Hub。當您從主控台啟用 Security Hub 時，您也可以選擇啟用支援的安全性標準。

Security Hub console

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 當您第一次開啟 Security Hub 主控台時，請選擇 [移至 Security Hub]。
3. 在歡迎頁面上，[安全性標準] 區段會列出 Security Hub 支援的安全性標準。

   選取標準的勾選方塊以啟用標準，然後清除勾選方塊將其停用。

   您可以隨時啟用或停用標準，或是其個別的控制項。如需有關管理安全性標準和控制項的資訊，請參閱 Security Hub 中的AWS安全性控制項和標準。
4. 選擇 Enable Security Hub (啟用 Security Hub)。

Security Hub API

調用該 EnableSecurityHubAPI。當您從 API 啟用 Security Hub 時，它會自動啟用下列預設安全性標準：

- AWS 基礎安全最佳實務
- 互聯網安全中心（CIS）AWS基準基準 v1.2.0

如果您不希望啟用這些標準，請將 `EnableDefaultStandards` 設為 `false`。

您也可以使用`Tags`參數將標籤值指派給 Hub 資源。

AWS CLI

執行 enable-security-hub 命令。若要啟用預設標準，請包括`--enable-default-standards`。若要不啟用預設標準，請包括`--no-enable-default-standards`。預設安全性標準如下：

- AWS 基礎安全最佳實務
- 互聯網安全中心（CIS）AWS基準基準 v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

範例

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

多帳戶啟用腳本

> **Note**
>
> 我們建議您使用中央設定來啟用和設定多個帳戶和區域的 Security Hub，而不是這個指令碼。

中的 Security Hub 多帳戶啟用指令碼 GitHub可讓您跨帳戶和區域啟用 Security Hub。該腳本還可以自動發送邀請到成員帳戶並啟用AWS Config的過程。

此指令碼會自動啟用所有區域中所有資源 (包括全域資源) 的資源記錄。它不會將全球資源記錄限制在單一區域。

有一個對應的腳本可以跨帳戶和區域禁用 Security Hub。

啟用 Security Hub 後的後續步驟

啟用 Security Hub 之後，我們建議您啟用對您的安全性需求很重要的安全性標準和安全性控制項。啟用控制項之後，Security Hub 會開始執行安全性檢查並產生控制項發現項目。您也可以利用 Security Hub 與其他AWS 服務及第三方解決方案之間的整合，在 Security Hub 中查看其發現項目。

安全中心中的集中配置

中央配置是一項 Security Hub 功能，可幫助您跨多個AWS 帳戶和AWS 區域. 若要使用中央設定，您必須先整合 Security Hub 和AWS Organizations. 您可以建立組織並指定組織的委派 Security Hub 系統管理員帳戶，以整合服務。

從委派的 Security Hub 系統管理員帳戶中，您可以指定如何在組織帳戶和組織單位 (OU) 跨區域設定 Security Hub 服務、安全性標準和安全性控制項。您只需幾個步驟即可從一個主要區域 (稱為「地區」) 設定這些設定。如果您不使用中央設定，則必須在每個帳戶和區域中分別設定 Security Hub。

當您使用中央組態時，委派的系統管理員可以選擇要設定的帳戶和 OU。如果委派的系統管理員將成員帳戶或 OU 指定為自我管理，則該成員可以在每個區域中個別設定自己的設定。如果委派的系統管理員將成員帳戶或 OU 指定為集中管理，則只有委派的系統管理員可以跨區域設定成員帳戶或 OU。您可以將組織中的所有帳戶和 OU 指定為集中管理、全部自行管理或兩者的組合。

若要設定集中管理的帳戶，委派的系統管理員會使用 Security Hub 組態原則。組態原則可讓委派的系統管理員指定是否啟用或停用 Security Hub，以及啟用和停用哪些標準和控制項。它們也可以用來自定義某些控件的參數。

組態原則會在主區域和所有連結的區域中生效。委派的管理員會在開始使用中央組態之前，指定組織的主「區域」和「連結的區域」。委派的系統管理員可以為整個組織建立單一組態原則，或建立多個組態原則來設定不同帳戶和 OU 的變數設定。

本節提供中央組態的概觀。

中央組態的優點

集中配置的優點包括：

簡化安全中樞服務和功能的組態

當您使用中央組態時，Security Hub 會引導您完成為組織設定安全性最佳做法的程序。它也會自動將產生的組態原則部署到指定的帳戶和 OU。如果您有現有的 Security Hub 設定 (例如自動啟用新的安全性控制項)，您可以使用這些設定做為組態原則的起點。此外，Security Hub 主控台上的 [組態] 頁面會顯示設定原則的即時摘要，以及哪些帳戶和 OU 使用每個原則。

跨帳戶和區域進行設定

您可以使用集中設定跨多個帳戶和區域設定 Security Hub。這有助於確保組織的每個部分都維持一致的組態和適當的安全性涵蓋範圍。

適應不同帳戶和 OU 中的不同配置

透過集中設定，您可以選擇以不同方式設定組織的帳戶和 OU。例如，您的測試帳戶和生產帳戶可能需要不同的配置。您也可以建立涵蓋新帳戶加入組織時的組態策略。

防止配置漂移

當使用者變更與委派管理員的選擇衝突的服務或功能時，就會發生組態偏移。中央配置可防止這種漂移。當您將帳戶或 OU 指定為集中管理時，只能由組織的委派系統管理員進行設定。如果您偏好使用特定帳戶或 OU 來設定自己的設定，可以將其指定為自我管理。

誰應該使用中央配置？

對於包含多個 Security Hub 帳戶的AWS環境而言，中央組態最有利。它旨在幫助您集中管理多個帳戶的 Security Hub。

您可以使用中央組態來設定 Security Hub 服務、安全性標準和安全性控制。您也可以使用它來自定義某些控件的參數。如需標準和控制項的資訊，請參閱安全控制和安 AWS 全中心的標準。

中央組態術語和概念

瞭解下列重要術語和概念可協助您使用 Security Hub 中央組態。

中央配置

Security Hub 功能可協助組織委派的 Security Hub 系統管理員帳戶設定 Security Hub 服務、安全性標準，以及跨多個帳戶和區域的安全性控制。若要設定這些設定，委派的系統管理員會針對其組織中的集中管理帳戶建立和管理 Security Hub 組態原則。自我管理帳戶可以在每個區域中個別設定自己的設定。若要使用集中設定，您必須整合 Security Hub 和AWS Organizations.

首頁地區

委派系統管理員藉由建立及管理組態原AWS 區域則，從中集中設定 Security Hub。組態原則會在主區域和所有連結的區域中生效。

本地區域也作為 Security Hub 彙總區域，從連結的區域接收發現項目、見解和其他資料。

2019 年 3 月 20 日或之後AWS推出的區域稱為選擇加入區域。選擇加入的區域不能是主要區域，但可以是連結的區域。如需選擇加入區域的清單，請參閱《AWS帳戶管理參考指南》中的啟用和停用區域之前的考量事項。

連結區域

一個AWS 區域可以從主區域配置的。組態原則是由委派管理員在首頁區域中建立的。這些政策會在首頁「區域」和所有連結的區域中生效。您必須至少指定一個連結的區域，才能使用中央組態。

鏈接的區域還將發現結果，見解和其他數據發送到主區域。

2019 年 3 月 20 日或之後AWS推出的區域稱為選擇加入區域。您必須先為帳戶啟用此類區域，才能套用組態原則。Organizations 管理帳戶可以為成員帳戶啟用選擇加入區域。如需詳細資訊，請參閱《AWS 區域帳戶管理參考指南》中的「指定您的AWS帳戶可以使用的項目」

Security Hub 組態原則

委派系統管理員可針對集中管理的帳戶設定的 Security Hub 設定集合。其中包含：

- 是否啟用或停用 Security Hub。
- 是否啟用一個或多個安全標準。
- 在啟用的標準中啟用哪些安全控制項。委派的系統管理員可以提供應啟用的特定控制項清單來執行此操作，而 Security Hub 會停用所有其他控制項 (包括釋放時的新控制項)。或者，委派的系統管理員可以提供應停用的特定控制項清單，而 Security Hub 會啟用所有其他控制項 (包括釋放時的新控制項)。
- (可選) 自訂已啟用標準中選取的已啟用控制項的參數。

組態原則會在至少與一個帳戶、組織單位 (OU) 或根目錄關聯之後，在主區域及所有連結的區域中生效。

在 Security Hub 主控台上，委派的系統管理員可以選擇 Security Hub 建議的組態原則或建立自訂組態原則。使用 Security Hub API 和AWS CLI委派的系統管理員只能建立自訂組態原則。委派的系統管理員最多可以建立 20 個自訂組態原則。

在建議的組態原則 Security Hub、AWS基礎安全性最佳作法 (FSBP) 標準，以及所有現有和新的 FSBP 控制項都會啟用。接受參數的控制項使用預設值。建議的組態原則適用於整個組織。

若要將不同的設定套用至組織，或將不同的組態原則套用至不同的帳戶和 OU，請建立自訂組態原則。

本機組態

整合 Security Hub 和之後，組織的預設組態類型AWS Organizations。透過本機組態，委派的系統管理員可以選擇在目前區域中的新組織帳戶中自動啟用 Security Hub 和預設安全性標準。如果委派管理員自動啟用預設標準，屬於這些標準的所有控制項也會自動啟用新組織帳戶的預設參數。這些

設定不適用於現有帳戶，因此在帳戶加入組織後可能會有組態偏差。停用屬於預設標準一部分的特定控制項，以及規劃其他標準和控制項，必須分別在每個帳戶和區域中完成。

本機設定不支援使用設定原則。若要使用組態原則，您必須切換到中央組態。

手動帳戶管理

如果您未與 Security Hub 整合，AWS Organizations或者您擁有獨立帳戶，則必須在每個區域中個別指定每個帳戶的設定。手動帳號管理不支援使用設定原則。

中央設定 API

只有 Security Hub 委派安全中心系統管理員可以在主區域中使用的資訊安全中心作業，以管理集中管理帳戶的組態原則。這些操作包括：

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

帳戶特定的 API

可用來啟用或停用安全中樞、標準和控制項的安全性中樞作業。 account-by-account 這些操作在每個單獨的區域中使用。

自我管理帳戶可以使用帳戶特定的操作來配置自己的設置。集中管理的帳戶無法在本地區和連結區域中使用下列帳戶特定作業。在這些區域中，只有委派的系統管理員可以透過中央組態作業和組態原則來設定集中管理的帳戶。

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`

- EnableSecurityHub
- UpdateStandardsControl

但是，若要檢查其帳戶的狀態，集中管理帳戶的擁有者可以使用任何Get或Describe作業。

如果您使用本機設定或手動帳號管理，而非集中設定，則可以使用這些帳戶特定的作業。

組織單位 (OU)

在AWS Organizations和 Security Hub 中，一組的容器AWS 帳戶。組織單位 (OU) 也可以包含其他 OU，可讓您建立類似上下顛倒樹狀結構的階層，父 OU 位於頂端，而 OU 的分支則向下延伸，以樹狀結尾的帳戶結尾。一個 OU 只能有一個父項，而每個組織帳戶只能是一個 OU 的成員。

您可以在AWS Organizations或中管理 OU AWS Control Tower。如需詳細資訊，請參閱使用指南中的「管理組織單位」或「AWS Organizations使用指南」AWS Control Tower AWS Control Tower 中的「管理組織與帳戶」。

委派的管理員可以將組態原則與特定帳戶或 OU 產生關聯，或將組態原則與根建立關聯，以涵蓋組織中的所有帳戶和 OU。

集中管理

只有委派管理員才能使用組態原則跨區域設定的帳戶、OU 或根目錄。

委派的系統管理員帳戶會指定是否集中管理帳戶。委派的系統管理員也可以將帳戶的狀態從集中管理變更為自我管理，或其他方式。

自我管理

管理其本身 Security Hub 設定的帳戶、OU 或根目錄。自我管理帳戶會使用帳戶特定作業，在每個區域中個別設定 Security Hub。這與集中管理的帳戶不同，只有委派系統管理員才能透過組態原則跨區域進行設定。

委派的系統管理員帳戶會指定帳戶是否為自我管理。委派的系統管理員帳戶也可以將帳戶的狀態從自我管理變更為集中管理，或其他方式。

委派的系統管理員可以將自我管理的行為套用至帳戶或 OU。或者，帳戶或 OU 可以從父項繼承自我管理的行為。委派的系統管理員帳戶本身可以是自我管理的帳戶。

組態原則關聯

設定原則與帳號、組織單位 (OU) 或根目錄之間的連結。當原則關聯存在時，帳號、OU 或根使用組態原則所定義的設定。在以下任一情況下都存在關聯：

- 當委派的系統管理員直接將組態原則套用至帳戶、OU 或根目錄時
- 當帳號或 OU 從父 OU 或根目錄繼承組態原則時

關聯存在，直到套用或繼承不同的組態為止。

套用的組態原則

一種組態原則關聯類型，委派的管理員會直接將組態原則套用至目標帳戶、OU 或根目錄。目標是以組態原則所定義的方式設定，而且只有委派管理員可以變更其組態。如果套用至 root，則組態原則會影響組織中未透過應用程式或從最近父項繼承使用不同組態的所有帳戶和 OU。

委派的系統管理員也可以將自我管理的組態套用至特定帳戶、OU 或根目錄。

繼承的組態原則

一種組態原則關聯類型，其中帳戶或 OU 會採用最接近的父 OU 或根目錄的組態。如果設定原則未直接套用至帳戶或 OU，則會繼承最接近父系的組態。政策的所有元素都會繼承。換句話說，帳戶或 OU 無法選擇只繼承部分原則。如果最接近的父系是自我管理的，子帳戶或 OU 會繼承父項的自我管理行為。

繼承不能覆蓋應用的配置。也就是說，如果設定原則或自我管理的設定直接套用至帳戶或 OU，它會使用該組態，而且不會繼承父項的組態。

根目錄

在AWS Organizations和 Security Hub，組織中的頂層父節點。如果委派的系統管理員將組態原則套用至 root，則該原則會與組織中的所有帳戶和 OU 產生關聯，除非他們透過應用程式或繼承使用不同的原則，或指定為自我管理。如果系統管理員將根指定為自我管理，則組織中的所有帳戶和 OU 都會自我管理，除非他們透過應用程式或繼承使用組態原則。如果根目錄為自我管理且目前沒有組態策略存在，則組織中的所有新帳號都會保留其目前的設定。

加入組織的新帳戶會屬於根帳戶，直到它們被指派給特定 OU 為止。如果新帳戶未指派給 OU，除非委派系統管理員將其指定為自我管理帳戶，否則它會繼承根組態。

開始使用中央配置

AWS Security Hub委派的系統管理員帳戶可以使用中央設定，為多個帳戶和組織單位 (OU) 設定 Security Hub、標準和控制項AWS 區域。

本節說明中央組態的先決條件以及如何開始使用它。

中央組態的先決條件

在您開始使用中央組態之前，您必須先整合 Security Hub，AWS Organizations並指定主區域。如果您使用 Security Hub 主控台，這些必要條件會包含在中央設定的選擇加入工作流程中。

與 Organizations 整合

您必須整合 Security Hub 和組 Organizations，才能使用集中設定。

若要整合這些服務，請先在 [組織] 中建立組 Organizations。然後，您可以從 Organizations 管理帳戶指定 Security Hub 委派的系統管理員帳戶。如需說明，請參閱整合 Security Hub AWS Organizations。

請確定您已在您預定的本地區域中指定委派的管理員。當您開始使用中央組態時，相同的委派管理員也會在所有連結的區域中自動設定。Organizations 管理帳戶無法設定為委派的管理員帳戶。

> **Important**
>
> 當您使用中央設定時，您無法使用安全中心主控台或 Security Hub API 來變更或移除委派的系統管理員帳戶。如果組 Organizations 管理帳戶使用 AWS Organizations API 來變更或移除 Security Hub 委派的系統管理員，Security Hub 會自動停止中央設定。您的配置策略也會取消關聯並刪除。成員帳戶會保留在委派管理員變更或移除之前所擁有的組態。

指定居住地區

您必須指定「主區域」才能使用中央組態。「首頁區域」是指委派管理員從中設定組織的「區域」。

若要使用中央組態，您必須至少指定一個可從主區域設定的連結區域。

> **Note**
>
> 本地區域不能是AWS已指定為選擇加入區域的地區。選擇加入的區域預設為停用。如需選擇加入區域的清單，請參閱《AWS帳戶管理參考指南》中的啟用和停用區域之前的考量事項。

委派的系統管理員只能從主區域建立和管理組態原則。組態原則會在主區域和所有連結的區域中生效。您無法建立僅套用至這些區域的子集，而不適用於其他區域的組態原則。

主區域也是您的 Security Hub 彙總區域，可從連結的區域接收發現項目、見解和其他資料。

如果您已經為跨區域彙總設定彙總區域，則這是中央組態的預設本地區域。您可以在開始使用中央配置之前更改主地區域，方法是刪除當前的發現項目彙總器並在您想要的主區域中創建一個新的地區。發現項目彙總器是指定本地區域和連結區域的 Security Hub 資源。

若要指定主區域，請依照設定彙總區域的步驟執行。如果您已經有一個主區域，則可以調用 GetFindingAggregatorAPI 以查看有關它的詳細信息，包括當前鏈接到該地區的區域。

啟動集中配置

選擇您偏好的方法，並依照下列步驟開始為您的組織使用中央組態。

Security Hub console

若要集中設定您的組織

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 在功能窗格中，選擇 [設定] 和 [設定]。然後，選擇啟動中央配置。

   如果您要上線至 Security Hub，請選擇 [移至 Security Hub]。
3. 在 [指定委派管理員] 頁面上，選取您的委派管理員帳戶或輸入其帳戶 ID。如果適用，建議您選擇您為其他AWS安全性和規範遵循服務設定的相同委派管理員。選擇設定委派管理員。
4. 在「集中化組織」頁面的「區域」區段中，選取您的首頁「地區」。您必須登入所在地區才能繼續。如果您已經為跨區域彙總設定彙總區域，它會顯示為本地區域。若要變更主要地區，請選擇 「編輯區域設定」。然後，您可以選擇首選的主地區域並返回此工作流程。
5. 選取至少一個「地區」以連結至本地區域。選擇性地選擇是否要將 future 支援的區域自動連結至本位目錄「區域」。您在此選取的區域可由委派的系統管理員從主區域設定。設定原則會在您的家用區域和所有連結的區域中生效。
6. 選擇確認並繼續。
7. 您現在可以使用中央規劃。繼續依照主控台提示建立您的第一個設定原則。如果您尚未準備好建立設定原則，請選擇 [我還沒準備好進行設定]。您可以稍後在導覽窗格中選擇 [設定] 和 [組態] 來建立原則。如需建立組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

Security Hub API

若要集中設定 Security Hub

1. 使用委派管理員帳戶的認證，從主區域叫用 UpdateOrganizationConfigurationAPI。

2. 將AutoEnable欄位設定為false。
3. 將物件中的ConfigurationType欄位設OrganizationConfiguration定為CENTRAL。此動作會產生下列影響：
   - 在所有連結的區域中，將呼叫帳戶指定為 Security Hub 委派的系統管理員。
   - 在所有連結的區域中，啟用委派管理員帳戶中的安全性中樞。
   - 針對使用 Security Hub 且屬於組織的新帳戶和現有帳戶，指定呼叫帳戶為 Security Hub 委派系統管理員。這發生在首頁「區域」和所有連結的區域中。只有在新組織帳戶與啟用 Security Hub 的組態原則相關聯時，呼叫帳戶才會設定為委派的系統管理員。只有在已啟用 Security Hub 的情況下，呼叫帳戶才會設定為現有組織帳戶的委派管理員。
   - false在所有連結的區域中設AutoEnable定為，並設定AutoEnableStandards為NONE在主「區域」和所有連結的區域中。當您使用中央設定時，這些參數與家用和連結的區域無關，但您可以透過使用組態原則，在組織帳戶中自動啟用 Security Hub 和預設安全性標準。
4. 您現在可以使用中央規劃。委派的系統管理員可以建立組態原則，以在您的組織中設定 Security Hub。如需建立組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

API 請求示例：

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

若要集中設定 Security Hub

1. 使用委派管理員帳戶的認證，從主區域執行update-organization-configuration命令。
2. 納入 no-auto-enable 參數。
3. 將物件中的ConfigurationType欄位設organization-configuration定為CENTRAL。此動作會產生下列影響：
   - 在所有連結的區域中，將呼叫帳戶指定為 Security Hub 委派的系統管理員。
   - 在所有連結的區域中，啟用委派管理員帳戶中的安全性中樞。

- 針對使用 Security Hub 且屬於組織的新帳戶和現有帳戶，指定呼叫帳戶為 Security Hub 委派系統管理員。這發生在首頁「區域」和所有連結的區域中。只有在新組織帳戶與啟用 Security Hub 的組態原則相關聯時，呼叫帳戶才會設定為委派的系統管理員。只有在已啟用 Security Hub 的情況下，呼叫帳戶才會設定為現有組織帳戶的委派管理員。
- 在所有連結的區域no-auto-enable中將自動啟用選項設定為，並NONE在主區域和所有連結的區域中設定auto-enable-standards為。當您使用中央設定時，這些參數與家用和連結的區域無關，但您可以透過使用組態原則，在組織帳戶中自動啟用 Security Hub 和預設安全性標準。

4. 您現在可以使用中央規劃。委派的系統管理員可以建立組態原則，以在您的組織中設定 Security Hub。如需建立組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

範例命令：

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

組織帳戶和 OU 的管理類型

當您使用中央設定時，AWS Security Hub委派的系統管理員可以將每個組織帳戶和組織單位 (OU) 指定為集中管理或自我管理。帳戶或 OU 的管理類型會決定您可以如何指定及變更其 Security Hub 設定。

自我管理的帳戶或 OU 可以在每AWS 區域個帳戶中分別設定自己的安全性中樞設定。委派的系統管理員無法為自我管理的帳戶或 OU 設定 Security Hub 設定，而且組態原則無法與其產生關聯。相反地，只有委派的系統管理員可以針對主區域和連結區域中的集中管理帳戶和 OU 設定 Security Hub 設定。組態原則可與集中管理的帳戶和 OU 產生關聯。

委派的系統管理員可以在自我管理和集中管理之間切換帳戶或 OU 的狀態。根據預設，當您透過安全中心 API 啟動集中設定時，所有帳戶和 OU 都會自我管理。在主控台中，管理類型取決於您的第一個設定原則。您與第一個原則相關聯的帳戶和 OU 會集中管理。其他帳戶和 OU 預設為自我管理。

如果您將組態原則與自我管理帳戶相關聯，則該策略會覆寫自我管理的指定。帳戶會進行集中管理，並採用組態策略中反映的設定。

子帳戶和 OU 可以從自我管理的父項繼承自我管理的行為，與子帳戶和 OU 可以從集中管理的父項繼承組態原則的方式相同。如需詳細資訊，請參閱 通過應用和繼承來關聯政策。

自我管理的帳戶或 OU 無法繼承父節點或根節點的組態原則。例如，如果您希望組織中的所有帳戶和 OU 都從根目錄繼承組態原則，則必須將自我管理節點的管理類型變更為集中管理。

指定自我管理帳戶的設定

自我管理帳戶必須在每個區域中個別設定自己的設定。

自我管理帳戶的擁有者可以在每個區域中叫用下列 API 來設定其設定：

- `EnableSecurityHub`並啟`DisableSecurityHub`用或停用 Security Hub 服務
- `BatchEnableStandards`並啟`BatchDisableStandards`用或停用標準
- `BatchUpdateStandardsControlAssociations`或啟`UpdateStandardsControl`用或停用控制項

如需安全中心 API 動作的說明，請參閱 AWS Security HubAPI 參考。

自我管理帳戶也可以使用 Security Hub 主控台，或AWS CLI在每個區域中設定其設定。

自我管理的帳戶無法叫用任何與 Security Hub 組態原則和原則關聯相關的 API。只有委派的系統管理員可以呼叫中央組態 API，並使用組態原則來設定集中管理的帳戶。

選擇帳戶和 OU 的管理類型

選擇您偏好的方法，然後依照步驟將帳戶或 OU 指定為集中管理或自我管理。

Security Hub console

若要選擇帳戶或 OU 的管理類型

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 選擇 Configuration (組態)。
3. 在 [組織] 索引標籤上，選取目標帳戶或 OU。選擇編輯。
4. 如果您要委派管理員設定目標帳戶或 OU，請在 [定義組態] 頁面上，針對 [管理類型] 選擇 [集中管理]。然後，如果您要將現有的組態原則與目標產生關聯，請選擇「套用特定原則」。如果您希望目標繼承其最近父項的組態，請選擇「從我的組織繼承」。如果您希望帳戶或 OU 設定自己的設定，請選擇 [自我管理]。
5. 選擇下一步。檢閱您的變更，然後選擇 [儲存]。

Security Hub API

若要選擇帳戶或 OU 的管理類型

1. 從主區域中的安全中心委派系統管理員帳戶叫用 StartConfigurationPolicyAssociationAPI。
2. 針對ConfigurationPolicyIdentifier欄位，SELF_MANAGED_SECURITY_HUB如果您希望帳戶或 OU 控制其自己的設定，請提供此欄位。如果您希望委派管理員控制帳戶或 OU 的設定，請提供相關組態政策的 Amazon 資源名稱 (ARN) 或 ID。
3. 針對Target欄位，提供您要變更其管理類型之目標的識別碼、OU ID 或根 ID。AWS 帳戶這會將自我管理的行為或指定的組態原則與目標產生關聯。目標的子帳戶可能會繼承自我管理的行為或組態策略。

指定自我管理帳戶的 API 請求範例：

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

若要選擇帳戶或 OU 的管理類型

1. 從主區域中的安全中心委派系統管理員帳戶執行start-configuration-policy-association命令。
2. 針對configuration-policy-identifier欄位，SELF_MANAGED_SECURITY_HUB如果您希望帳戶或 OU 控制其自己的設定，請提供此選項。如果您希望委派管理員控制帳戶或 OU 的設定，請提供相關組態政策的 Amazon 資源名稱 (ARN) 或 ID。
3. 針對target欄位，提供您要變更其管理類型之目標的識別碼、OU ID 或根 ID。AWS 帳戶這會將自我管理的行為或指定的組態原則與目標產生關聯。目標的子帳戶可能會繼承自我管理的行為或組態策略。

指定自我管理帳戶的指令範例：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Security Hub 組態原則的運作方式

委派的系統管理員帳戶可以建立組AWS Security Hub態原則，以設定組織中的 Security Hub、安全性標準和安全性控制。建立組態原則之後，委派的管理員可以將其與帳戶、組織單位 (OU) 或根建立關聯。委派管理員也可以檢視、編輯或刪除組態原則。

政策考量

在 Security Hub 中建立組態原則之前，請考慮下列詳細資料。

- 配置策略必須關聯才能生效 — 建立配置策略之後，您可以將其與一個或多個帳戶、組織單位 (OU) 或根建立關聯。組態原則可透過直接應用程式或從父 OU 繼承，與帳戶或 OU 產生關聯。
- 一個帳號或 OU 只能與一個組態原則產生關聯 — 為了避免衝突的設定，一個帳號或 OU 只能在任何指定時間與一個組態原則產生關聯。或者，帳戶或 OU 也可以是自我管理的。
- 配置策略已完成 — 配置策略提供完整的設置規格。例如，子女帳戶無法接受某個策略中某些控制項的設定，以及另一個策略中其他控制項的設定。當您將策略與子帳戶相關聯時，請確保策略指定了您希望子帳戶使用的所有設定。
- 無法還原設定原則 — 在將組態原則與帳戶或 OU 產生關聯之後，就無法還原設定原則。例如，如果您將停用 CloudWatch 控制項的組態策略與特定帳號產生關聯，然後解除該策略的關聯，則該帳戶中的 CloudWatch 控制項會繼續停用。若要再次啟用 CloudWatch 控制項，您可以將帳戶與啟用控制項的新策略建立關聯。或者，您可以將帳戶變更為自我管理，並啟用帳戶中的每個 CloudWatch 控制項。
- 組態原則會在您的主區域和所有連結區域中生效 — 設定政策會影響主區域和所有連結區域中的所有關聯帳戶。您無法建立只在部分這些區域中生效的設定原則，而不會在其他區域中生效。例外情況是涉及全域資源的控制項。

  2019 年 3 月 20 日或之後AWS推出的區域稱為選擇加入區域。您必須為帳戶啟用此類區域，組態政策在該處生效之前。Organizations 管理帳戶可以為成員帳戶啟用選擇加入區域。如需啟用選擇加入區域的指示，請參閱《帳戶管理參考指南》中AWS 區域的「指定帳戶可以使用的AWS帳戶」。

  如果您的原則設定的控制項無法在主區域或一或多個連結的區域使用，Security Hub 會略過無法使用的區域中的控制項組態，但會在可用控制項的區域中套用設定。
- 組態政策是資源 — 組態政策具有 Amazon 資源名稱 (ARN) 和通用唯一識別碼 (UUID)，做為資源。ARN 使用下列格式：`arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*。自我管理的組態沒有 ARN。自我管理組態的 UUID 為。`SELF_MANAGED_SECURITY_HUB`

組態原則的類型

每個組態原則都會指定下列設定：

- 啟用或停用 Security Hub。
- 啟用一或多個安全標準。
- 指出在已啟用的標準中啟用哪些安全性控制。您可以提供應啟用的特定控制項清單，而 Security Hub 會停用所有其他控制項，包括發行時的新控制項。或者，您可以提供應停用的特定控制項清單，而 Security Hub 會啟用所有其他控制項，包括發行時的新控制項。
- (可選) 為已啟用的標準中選取的啟用控制項自訂參數。

中央設定原則不包含AWS Config錄製程式設定。您必須分別啟用AWS Config並開啟必要資源的記錄，Security Hub 才能產生控制項發現項目。如需詳細資訊，請參閱 配置 AWS Config。

如果您使用中央組態，Security Hub 會自動停用與所有區域 (主區域除外) 中涉及全域資源的控制項。其他控制項會在所有可用的區域中啟用。若要將這些控制項的發現項目限制為只有一個「區域」，您可以更新記AWS Config錄器設定，並關閉所有區域中的全域資源記錄，但本地區域除外。如需涉及全域資源的控制項清單，請參閱處理全球資源的控制項。

建議的組態原則

第一次在 Security Hub 主控台中建立組態原則時，您可以選擇安全中心建議的原則。

建議的原則會啟用 Security Hub、AWS基礎安全性最佳作法 (FSBP) 標準，以及所有現有和新的 FSBP 控制項。接受參數的控制項使用預設值。建議的策略適用於 root (所有帳戶和 OU，新的和現有的)。建立組織的建議策略之後，您可以從委派的系統管理員帳戶修改它。例如，您可以啟用其他標準或控制項，或停用特定的 FSBP 控制項。如需修改組態原則的指示，請參閱更新 Security Hub 組態原則。

自訂組態原則

委派系統管理員最多可以建立 20 個自訂組態原則，而非建議的原則。您可以將單一自訂原則與整個組織產生關聯，或是使用不同帳戶和 OU 的不同自訂原則建立關聯。對於自訂組態原則，您可以指定所需的設定。例如，您可以建立自訂政策來啟用 FSBP、網際網路安全中心 (CIS) AWS 基準測試 v1.4.0，以及除 Amazon Redshift 控制項以外的所有標準控制項。您在自訂組態原則中使用的資料粒度等級取決於整個組織中預定的安全性涵蓋範圍。

> **Note**
>
> 您無法將停用 Security Hub 的設定原則與委派的系統管理員帳戶建立關聯。這種策略可以與其他帳戶相關聯，但會略過與委派管理員的關聯。委派的管理員帳戶會保留其目前的組態。

建立自訂組態原則之後，您可以透過更新組態原則來反映建議的組態，以切換至建議的組態原則。不過，在建立第一個原則之後，您看不到在 Security Hub 主控台中建立建議的組態原則的選項。

通過應用和繼承來關聯政策

當您第一次選擇加入中央組態時，您的組織沒有關聯，且其行為方式與選擇加入之前的行為相同。然後委派的系統管理員可以在組態原則或自我管理行為與帳戶、OU 或根目錄之間建立關聯。可以通過應用程序或繼承來建立關聯。

從委派的系統管理員帳戶中，您可以直接將組態原則套用至帳戶、OU 或根目錄。或者，委派的系統管理員也可以將自我管理的指定直接套用至帳戶、OU 或根目錄。

如果沒有直接應用程式，帳戶或 OU 會繼承具有組態原則或自我管理行為的最接近父系的設定。如果最近的父項與組態原則相關聯，則子項會繼承該原則，且只能由主區域中的委派管理員進行設定。如果最接近的父系是自我管理的，則子系會繼承自我管理的行為，並且能夠在每個父項中指定自己的設定。AWS 區域

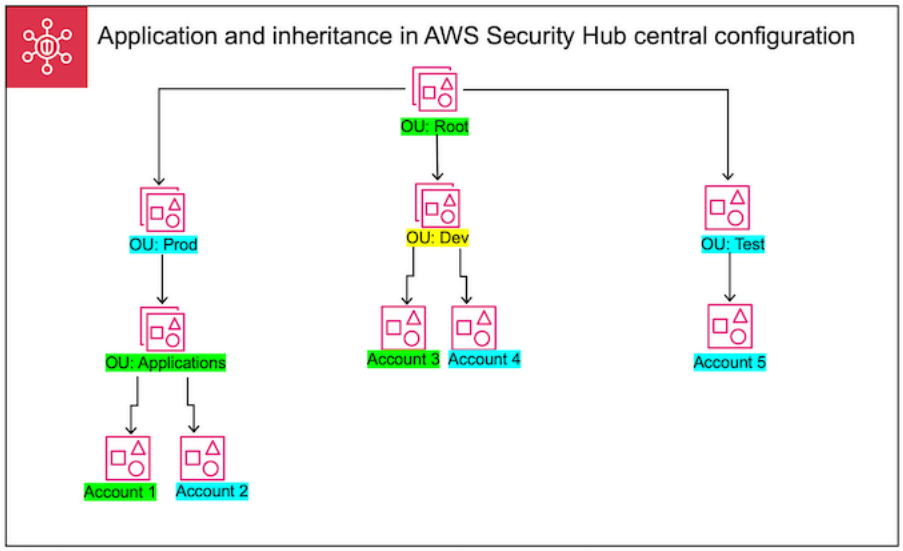
應用程序優先於繼承。換句話說，繼承不會覆寫委派系統管理員直接套用至帳戶或 OU 的組態原則或自我管理指定。

如果您直接將組態策略套用至自我管理的帳戶，則該策略會覆寫自我管理的指定。帳戶會進行集中管理，並採用組態策略中反映的設定。

我們建議您直接將設定原則套用至根目錄。如果您將策略套用至根目錄，則加入組織的新帳號將自動繼承根策略，除非您將這些帳號與不同的策略產生關聯或將其指定為自我管理。

在指定時間，只能透過應用程式或繼承與帳戶或 OU 建立關聯一個組態原則。這是為了防止衝突的設定而設計。

下圖說明原則應用程式和繼承在中央組態中的運作方式。



在此範例中，以綠色反白顯示的節點具有已套用的組態原則。以藍色反白顯示的節點沒有套用的組態原則。以黃色反白顯示的節點已指定為自我管理。每個帳戶和 OU 都使用下列組態：

- OU: 根 (綠色) — 此 OU 使用已套用至其的組態原則。
- OU: Prod (藍色) — 此 OU 會繼承 OU: 根目錄的組態原則。
- OU：應用程式 (綠色) — 此 OU 使用已套用的組態原則。
- 帳戶 1 (綠色) — 此帳戶使用已套用的組態策略。
- 帳戶 2 (藍色) — 此帳戶會繼承 OU: 應用程式的組態策略。
- OU: dev (黃色) — 此 OU 是自我管理的。
- 帳戶 3 (綠色) — 此帳戶使用已套用的組態策略。
- 帳戶 4 (藍色) — 此帳戶會繼承 OU: dev 的自我管理行為。
- OU：測試 (藍色) — 此帳戶會從 OU: root 繼承組態策略。
- 帳號 5 (藍色) — 此帳戶會從 OU: Root 繼承組態原則，因為其直接父系 OU: test 與組態策略沒有關聯。

測試組態原則

若要測試組態原則的效果，您可以將其與單一帳戶或 OU 產生關聯，然後再在整個組織中更廣泛地建立關聯。

若要測試組態原則

1. 建立自訂設定原則，但不要將其套用至任何帳戶。確認 Security Hub 啟用、標準和控制項的指定設定正確無誤。
2. 將設定原則套用至沒有任何子帳戶或 OU 的測試帳戶或 OU。
3. 確認測試帳戶或 OU 在您的本地區域和所有連結的區域中以預期的方式使用組態原則。您也可以確認組織中的所有其他帳戶和 OU 都保持自我管理，並且可以在每個區域中變更自己的設定。

在單一帳戶或 OU 中測試組態原則之後，您可以將其與其他帳戶和 OU 建立關聯。如需有關策略建立與關聯的指示，請參閱建立和關聯安全性中樞組態原則。已套用帳戶的子系會繼承策略，除非它們是自我管理的，或是套用不同的設定原則。您也可以視需要編輯組態原則並建立其他組態原則。

建立和關聯安全性中樞組態原則

委派的管理員帳戶可以建立組AWS Security Hub態原則，並將其與組織帳戶、組織單位 (OU) 或根建立關聯。

如果這是您第一次建立組態原則，建議您先檢閱Security Hub 組態原則的運作方式。

選擇您偏好的存取方法，然後按照步驟建立和關聯組態原則。使用 Security Hub 主控台時，您可以同時將組態原則套用至多個帳戶或 OU。使用 Security Hub API 時AWS CLI，或者，您可以將組態原則套用至每個要求中只有一個帳戶或 OU。

Security Hub console

若要建立並關聯組態原則

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在瀏覽窗格中，選擇 [組態] 和 [原則] 索引標籤。然後，選擇 [建立原則]。
3. 在 [設定組織] 頁面上，如果這是您第一次建立組態原則，您會在 [組態類型] 下看到三個選項。如果您已建立至少一個設定原則，則只會看到 [自訂原則] 選項。

   - 選擇 [在整個組織中使用AWS建議的 Security Hub 組態]，以使用我們建議的原則。建議的原則會在所有組織帳戶中啟用安全性中樞、啟用AWS基礎安全性最佳作法 (FSBP) 標準，並啟用所有新的和現有的 FSBP 控制項。控制項使用預設參數值。
   - 選擇 [我尚未準備好設定]，以便稍後建立設定原則。

- 選擇 [自訂原則] 以建立自訂組態原則。指定是否要啟用或停用 Security Hub、要啟用哪些標準，以及要在這些標準中啟用哪些控制項。或者，為支援自訂參數的一個或多個已啟用控制項指定自訂參數值。

4. 在 [帳戶] 區段中，選擇您要套用組態原則的目標帳戶、OU 或根目錄。

   - 如果您要將組態策略套用至根目錄，請選擇 [所有帳號]。這包括組織中沒有套用或繼承其他原則的所有帳戶和 OU。
   - 如果您要將組態策略套用至特定帳戶或 OU，請選擇 [特定帳戶]。輸入帳號 ID，或從組織結構中選取帳戶和 OU。您最多可以指定 15 個要套用策略的帳戶或 OU。若要指定較大的數字，請在建立後編輯策略，並將其套用至其他帳戶。
   - 選擇僅委派管理員，將組態原則套用至目前委派的管理員帳戶。

5. 選擇下一步。
6. 在 [檢閱並套用] 頁面上，檢閱您的組態原則詳細資料。然後，選擇 [建立原則並套用]。在您的首頁「區域」和「連結的區域」中，此動作會覆寫與此組態政策相關聯之帳戶的現有組態設定。帳戶可以透過應用程式與組態策略相關聯，或從父節點繼承。已套用目標的子帳戶和 OU 會自動繼承此組態原則，除非特別排除、自我管理或使用不同的組態原則。

Security Hub API

若要建立並關聯組態原則

1. 從主區域中的安全中心委派系統管理員帳戶叫用 CreateConfigurationPolicyAPI。
2. 針對Name，提供組態原則的唯一名稱。(選擇性) 提供組態原則的說明。Description
3. 針對ServiceEnabled欄位，指定是否要在此設定原則中啟用或停用 Security Hub。
4. 針對EnabledStandardIdentifiers欄位，指定您要在此組態原則中啟用的 Security Hub 標準。
5. 針對SecurityControlsConfiguration物件，指定您要在此組態原則中啟用或停用的控制項。選擇EnabledSecurityControlIdentifiers表示指定的控制項已啟用。其他屬於已啟用標準 (包括新發行的控制項) 的一部分的控制項會停用。選擇DisabledSecurityControlIdentifiers表示指定的控制項已停用。其他屬於已啟用標準 (包括新發行的控制項) 的一部分的控制項會啟用。
6. 或者，針對SecurityControlCustomParameters欄位指定您要自訂參數的已啟用控制項。提CUSTOM供ValueType欄位和欄位的自訂參數Value值。該值必須是正確的數據類型，並且在 Security Hub 指定的有效範圍內。僅選取控制項支援自訂參數值。如需詳細資訊，請參閱自訂控制參數。

7. 若要將您的設定原則套用至帳戶或 OU，請從主區域中的 Security Hub 委派系統管理員帳戶叫用 StartConfigurationPolicyAssociationAPI。
8. 對於該ConfigurationPolicyIdentifier欄位，請提供政策的 Amazon 資源名稱 (ARN) 或識別碼。這個 ARN 和識別碼是由 CreateConfigurationPolicy API 傳回。
9. 針對Target欄位，請提供您要套用此組態原則的 OU、帳戶或根 ID。您只能在每個 API 請求中提供一個目標。所選目標的子帳戶和 OU 會自動繼承此組態原則，除非它們是自我管理或使用不同的組態原則。

建立設定原則的 API 要求範例：

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
```

```
    }
}
```

關聯組態原則的 API 要求範例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

若要建立並關聯組態原則

1. 從主區域中的安全中心委派系統管理員帳戶執行create-configuration-policy命令。
2. 針對name，提供組態原則的唯一名稱。(選擇性) 提供組態原則的說明。description
3. 針對ServiceEnabled欄位，指定是否要在此設定原則中啟用或停用 Security Hub。
4. 針對EnabledStandardIdentifiers欄位，指定您要在此組態原則中啟用的 Security Hub 標準。
5. 在SecurityControlsConfiguration欄位中，指定您要在此組態原則中啟用或停用的控制項。選擇EnabledSecurityControlIdentifiers表示指定的控制項已啟用。其他屬於已啟用標準 (包括新發行的控制項) 的一部分的控制項會停用。選擇DisabledSecurityControlIdentifiers表示指定的控制項已停用。會啟用套用至已啟用標準的其他控制項 (包括新發行的控制項)。
6. 或者，針對SecurityControlCustomParameters欄位指定您要自訂參數的已啟用控制項。提CUSTOM供ValueType欄位和欄位的自訂參數Value值。該值必須是正確的數據類型，並且在 Security Hub 指定的有效範圍內。僅選取控制項支援自訂參數值。如需詳細資訊，請參閱自訂控制參數。
7. 若要將您的組態原則套用至帳戶或 OU，請從主區域中的 Security Hub 委派系統管理員帳戶執行start-configuration-policy-association命令。
8. 對於該configuration-policy-identifier欄位，請提供組態政策的 Amazon 資源名稱 (ARN) 或識別碼。此 ARN 和 ID 由create-configuration-policy命令返回。

9. 針對target欄位，請提供您要套用此組態原則的 OU、帳戶或根 ID。每次執行命令時，您只能提供一個目標。所選目標的子系會自動繼承此組態原則，除非它們是自行管理或使用不同的組態原則。

建立組態原則的範例命令：

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

關聯組態原則的範例命令：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

該 StartConfigurationPolicyAssociation API 返回一個名為的字段AssociationStatus。此欄位會告訴您原則關聯是處於擱置中狀態，或處於成功或失敗的狀態。狀態可能需要 24 小時才會從SUCCESS或PENDING變更FAILURE。如需關聯狀態的詳細資訊，請參閱組態的關聯狀態。

檢視 Security Hub 組態原則

委派的管理員帳戶可以檢視組織的組AWS Security Hub態原則及其詳細資料。

選擇您偏好的方法，然後按照步驟檢視您的組態原則。

Console

若要檢視組態原則

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 選擇 [原則] 索引標籤以檢視組態原則的概觀。
4. 選取組態原則，然後選擇「檢視詳細資料」以查看其他詳細資訊。

API

若要檢視組態原則

若要檢視所有設定原則的摘要清單，請從您主區域的 Security Hub 委派系統管理員帳戶叫用 `ListConfigurationPolicies`API。您可以提供可選的分頁參數

API 請求示例：

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

若要檢視特定組態原則的詳細資料，請從您主區域的 Security Hub 委派系統管理員帳戶叫用 `GetConfigurationPolicy`API。提供您要查看其詳細資料之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。

API 請求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

若要檢視所有設定原則及其關聯的摘要清單，請從您主區域中的 Security Hub 委派系統管理員帳戶叫用 ListConfigurationPolicyAssociationsAPI。或者，您可以提供分頁參數，或依特定原則 ID、關聯類型或關聯狀態篩選結果。

API 請求示例：

```
{
    "AssociationType": "APPLIED"
}
```

若要檢視特定帳戶、OU 或根帳戶的關聯，請從您主區域中的 Security Hub 委派系統管理員帳戶叫用GetConfigurationPolicyAssociation或 BatchGetConfigurationPolicyAssociationsAPI。對於Target，請提供帳號、OU ID 或根識別碼。

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

若要檢視組態原則

若要檢視所有設定原則的摘要清單，請從主區域的 Security Hub 委派系統管理員帳戶執行list-configuration-policies命令。

範例命令：

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

若要檢視特定組態原則的詳細資料，請從您的主區域中的 Security Hub 委派系統管理員帳戶執行get-configuration-policy命令。提供您要查看其詳細資料之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。

```
aws securityhub --region us-east-1 get-configuration-policy \
```

```
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

若要檢視所有設定原則及其帳戶關聯的摘要清單，請從您主區域的 Security Hub 委派系統管理員帳戶執行list-configuration-policy-associations命令。或者，您可以提供分頁參數，或依特定原則 ID、關聯類型或關聯狀態篩選結果。

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

若要檢視特定帳戶的關聯，請從您的主區域中的 Security Hub 委派系統管理員帳戶執行get-configuration-policy-association或batch-get-configuration-policy-associations命令。對於target，請提供帳號、OU ID 或根識別碼。

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

組態的關聯狀態

下列中央設定 API 作業會傳回名為的欄位AssociationStatus：

- BatchGetConfigurationPolicyAssociations
- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

當基礎組態是組態原則以及自我管理行為時，都會傳回此欄位。

的值會AssociationStatus告訴您原則關聯為擱置中，還是處於成功或失敗的狀態。狀態可能需要 24 小時才會從SUCCESS或PENDING變更FAILURE。父 OU 或根目錄的關聯狀態取決於其子系的狀態。如果所有子項的關聯狀態為SUCCESS，則父項的關聯狀態為SUCCESS。如果一或多個子項的關聯狀態為FAILED，則父項的關聯狀態為FAILED。

的值AssociationStatus也取決於所有區域。如果主「區域」和所有連結區域中的關聯成功，則的值AssociationStatus為SUCCESS。如果這些區域中的一或多個關聯失敗，則的值AssociationStatus為FAILED。

下列行為也會影響的值AssociationStatus：

- 如果目標是父 OU 或根目錄，則目標具有AssociationStatusSUCCESS或FAILED僅當所有子系都具有SUCCESS或FAILED狀態時。如果子帳戶或 OU 的關聯狀態在您第一次將父項與設定產生關聯後變更 (例如，新增或移除連結的區域)，則除非您再次呼叫 StartConfigurationPolicyAssociation API，否則該變更不會更新父項的關聯狀態。
- 如果目標是帳戶，則該目標具有AssociationStatusSUCCESS或FAILED僅當關聯在主「區域」和所有連結的區域FAILED中產生SUCCESS或結果時才會有帳戶。如果在您第一次將目標帳戶與組態產生關聯後，目標帳戶的關聯狀態變更 (例如，新增或移除連結的區域時)，則其關聯狀態會更新。不過，除非您再次呼叫 StartConfigurationPolicyAssociation API，否則變更不會更新父項的關聯狀態。

如果您新增連結的區域，Security Hub 會複寫位於PENDINGSUCCESS、或新區域中FAILED狀態的現有關聯。

關聯失敗的常見原因

組態原則關聯可能會因下列常見原因而失敗：

- 組 Organ@@ izations 管理帳戶不是成員 — 如果您想要將組態原則與組 Organizations 管理帳戶建立關聯，則該帳戶必須已啟用 Security Hub。這會使管理帳戶成為組織中的成員帳戶。
- AWS Config未啟用或正確設定 — 若要在組態原則中啟用標準，AWS Config必須啟用並設定為記錄相關資源。
- 必須與委派的系統管理員帳戶建立關聯 — 您只能在登入委派的管理員帳戶時，將原則與目標帳戶和 OU 產生關聯。
- 必須從本地區域建立關聯 — 您只能在登入本地區域時，將原則與目標帳戶和 OU 產生關聯。
- 未啟用選擇加入區域 — 如果成員帳戶或連結區域中的 OU 是委派系統管理員尚未啟用的選擇加入區域，則原則關聯會失敗。從委派的系統管理員帳戶啟用 [區域] 後，您可以重試。
- 成員帳號已暫停 — 如果您嘗試將策略與暫停的成員帳戶建立關聯，則策略關聯會失敗。

更新 Security Hub 組態原則

委派的系統管理員帳戶可視需要更新AWS Security Hub組態原則。委派的系統管理員可以更新原則設定、與策略相關聯的帳戶或 OU，或兩者都更新。更新策略設定後，與組態策略相關聯的帳戶會自動開始使用更新的策略。

與建立組態原則時類似，您可以更新下列原則設定：

- 啟用或停用 Security Hub。
- 啟用一或多個安全性標準。
- 指出在已啟用的標準中啟用哪些安全性控制。您可以提供應啟用的特定控制項清單，而 Security Hub 會停用所有其他控制項，包括發行時的新控制項。或者，您可以提供應停用的特定控制項清單，而 Security Hub 會啟用所有其他控制項，包括釋放控制項時的新控制項。
- (可選) 為已啟用的標準中選取的啟用控制項自訂參數。

選擇您偏好的方法，然後按照步驟更新配置策略。

Console

若要更新組態原則

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 選擇 Policies (政策) 標籤。
4. 選取您要編輯的組態原則，然後選擇 [編輯]。如果需要，請編輯策略設定。如果您要保持原則設定不變，請保持此區段不變。
5. 選擇「下一步」。如果需要，請編輯原則關聯。如果要保持原則關聯不變，請保持此段落不變。
6. 選擇下一步。
7. 檢閱您的變更，然後選擇 [儲存並套用]。在您的首頁「區域」和「連結的區域」中，此動作會覆寫與此組態政策相關聯之帳戶的現有組態設定。帳戶可以透過應用程式與組態策略相關聯，或從父節點繼承。

API

若要更新組態原則

1. 若要更新組態原則中的設定，請從主區域中的 Security Hub 委派系統管理員帳戶叫用 UpdateConfigurationPolicyAPI。
2. 提供您要更新之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。
3. 為下的欄位提供更新的值ConfigurationPolicy。或者，您也可以提供更新的原因。
4. 若要新增此組態原則的新關聯，請從主區域中的 Security Hub 委派系統管理員帳戶叫用 StartConfigurationPolicyAssociationAPI。若要移除一或多個目前的關聯，請從主區域中的 Security Hub 委派系統管理員帳戶叫用 StartConfigurationPolicyDisassociationAPI。
5. 在ConfigurationPolicyIdentifier欄位中，提供您要更新其關聯之組態原則的 ARN 或 ID。
6. 針對Target欄位，提供您要關聯或取消關聯的帳戶、OU 或根 ID。此動作會覆寫指定 OU 或帳號之前的原則關聯。

> **Note**
>
> 當您呼叫 UpdateConfigurationPolicy API 時，Security Hub 會執行EnabledStandardIdentifiers、EnabledSecurityControlIdentifiers、DisabledSe位的完整清單取代。每次呼叫此 API 時，請提供您要啟用的完整標準清單，以及您要啟用或停用和自訂參數的控制項完整清單。

更新配置策略的 API 請求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
```

```
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

若要更新組態原則

1. 若要更新組態原則中的設定，請從主區域中的 Security Hub 委派系統管理員帳戶執行update-configuration-policy命令。
2. 提供您要更新之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。
3. 為下的欄位提供更新的值`configuration-policy`。或者，您也可以提供更新的原因。
4. 若要新增此組態原則的新關聯，請從主區域中的 Security Hub 委派系統管理員帳戶執行start-configuration-policy-association命令。若要移除一或多個目前的關聯，請從主區域中的 Security Hub 委派系統管理員帳戶執行start-configuration-policy-disassociation命令。
5. 在`configuration-policy-identifier`欄位中，提供您要更新其關聯之組態原則的 ARN 或 ID。

6. 針對target欄位，提供您要關聯或取消關聯的帳戶、OU 或根 ID。此動作會覆寫指定 OU 或帳號之前的原則關聯。

> **Note**
>
> 當您執行命update-configuration-policy令時，Security Hub 會執行EnabledStandardIdentifiers、EnabledSecurityControlIdentifiers、DisabledSe位的完整清單取代。每次執行此命令時，請提供您要啟用的完整標準清單，以及您要啟用或停用和自訂參數的控制項完整清單。

更新配置策略的示例命令：

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

該 StartConfigurationPolicyAssociation API 返回一個名為的字段AssociationStatus。此欄位會告訴您原則關聯處於擱置中狀態，或處於成功或失敗的狀態。狀態可能需要 24 小時才會從SUCCESS或PENDING變更FAILURE。如需關聯狀態的詳細資訊，請參閱組態的關聯狀態。

刪除和取消關聯 Security Hub 組態原則

委派的系統管理員帳戶可以刪除組AWS Security Hub態原則。或者，委派的管理員帳戶可以保留組態原則，但會將其與特定帳戶或組織單位 (OU) 取消關聯。

下節將說明這兩個選項。

刪除組態原則

當您刪除組態原則時，您的組織將不再存在該設定原則。目標帳戶、OU 和組織根目錄無法再使用組態原則。與已刪除組態策略關聯的目標會繼承最近父項的組態原則，或者如果最近的父項是自我管理的，則會變成自我管理的。如果您想讓目標使用不同的組態，可以將目標與新的組態原則產生關聯。如需詳細資訊，請參閱建立和關聯安全性中樞組態原則。

我們建議至少建立一個組態原則，並將其與組織產生關聯，以提供適當的安全性涵蓋範圍。

刪除組態策略之前，您必須先取消策略與帳號、OU 或目前套用的根目錄的關聯。

選擇您偏好的方法，然後依照步驟刪除組態原則。

Console

若要刪除組態原則

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 選擇 Policies (政策) 標籤。選取您要刪除的組態原則，然後選擇刪除。如果組態原則仍與任何帳戶或 OU 相關聯，系統會提示您先取消原則與這些目標的關聯，然後才能刪除原則。
4. 檢閱確認訊息。輸入**`confirm`**，然後選擇「刪除」。

API

若要刪除組態原則

從主區域中的安全中心委派系統管理員帳戶叫用 DeleteConfigurationPolicyAPI。

提供您要刪除之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。如果您收到`ConflictException`錯誤訊息，組態原則仍會套用至組織中的帳戶或 OU。若要解決此錯誤，請先取消設定原則與這些帳戶或 OU 的關聯，然後再嘗試刪除它。

刪除配置策略的 API 請求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

```
}
```

AWS CLI

若要刪除組態原則

從主區域中的安全中心委派系統管理員帳戶執行delete-configuration-policy命令。

提供您要刪除之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。如果您收到`ConflictException`錯誤訊息，組態原則仍會套用至組織中的帳戶或 OU。若要解決此錯誤，請先取消設定原則與這些帳戶或 OU 的關聯，然後再嘗試刪除它。

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

取消設定與帳戶和 OU 的關聯

在委派的系統管理員帳戶中，您可以取消目標帳戶、OU 或根目前套用至該帳戶或自我管理組態的組態原則之間的關聯。您只能將目標與套用的組態取消關聯，而不能取消與繼承組態的關聯。若要變更繼承的組態，您可以將組態原則或自我管理行為套用至受影響的帳戶或 OU。您也可以將新的組態原則 (包括您想要的修改) 套用至最接近的父項。

解除關聯不會刪除設定原則。策略會保留在您的帳戶中，因此您可以將其與組織中的其他目標產生關聯。解除關聯完成時，受影響的目標會繼承最接近父系的組態原則或自我管理行為。如果沒有可繼承的組態，目標會保留其在解除關聯之前的設定，但會變成自我管理。

選擇您偏好的方法，然後依照步驟取消帳戶、OU 或根目前設定的關聯。

Console

取消帳戶或 OU 與其目前組態的關聯

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。

3. 在 [組 Organ izations] 索引標籤上，選取您要取消與其目前組態關聯的帳號、OU 或根目錄。選擇編輯 。
4. 如果您希望委派的管理員能夠將原則直接套用至目標，請在「定義組態」頁面上選擇「管理」的「套用原則」。如果您希望目標繼承其最近父項的組態，請選擇繼承。在其中一種情況下，委派的管理員會控制目標的設定值。如果您希望帳戶或 OU 控制自己的設定，請選擇 [自我管理]。
5. 檢閱變更後，請選擇 [下一步] 和 [套用]。如果這些組態與您目前的選擇衝突，此動作會覆寫範圍內任何帳戶或 OU 的現有組態。

API

取消帳戶或 OU 與其目前組態的關聯

1. 從主區域中的安全中心委派系統管理員帳戶叫用 StartConfigurationPolicyDisassociationAPI。
2. 對於`ConfigurationPolicyIdentifier`，請提供您要取消關聯之組態政策的 Amazon 資源名稱 (ARN) 或 ID。提`SELF_MANAGED_SECURITY_HUB`供此欄位以取消自我管理行為的關聯。
3. 針對`Target`，提供您要與此組態原則中斷關聯的帳戶、OU 或根目錄。

取消配置策略關聯的 API 請求示例：

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

取消帳戶或 OU 與其目前組態的關聯

1. 從主區域中的安全中心委派系統管理員帳戶執行start-configuration-policy-disassociation命令。
2. 對於`configuration-policy-identifier`，請提供您要取消關聯之組態政策的 Amazon 資源名稱 (ARN) 或 ID。提`SELF_MANAGED_SECURITY_HUB`供此欄位以取消自我管理行為的關聯。
3. 針對`target`，提供您要與此組態原則中斷關聯的帳戶、OU 或根目錄。

取消設定原則關聯的範例命令：

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

標準或控制項環境中的中央組態

您可以從 AWS Security Hub 主控台的 [組態] 頁面或特定安全性標準或安全性控制項的內容中使用中央組態。在內容中使用此功能可讓您以與現有工作流程整合的方式，在整個組織中配置標準和控制項。此外，當您檢視發現項目時，您可以探索哪些標準和控制項與您的環境最相關，並同時進行設定。

內容中的組態只能在 Security Hub 主控台上使用。您必須以程式設計方式呼叫 UpdateConfigurationPolicyAPI，以變更組織中特定標準或控制項的設定方式。

在內容中配置安全性標準

依照下列步驟，透過中央組態在前後關聯中配置安全性標準。

若要在內容中配置安全性標準 (僅限主控台)

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在導覽窗格中，選擇 [安全性標準]。
3. 針對您要設定的標準，選擇「設定」。您也可以選擇特定的標準，然後從標準詳細資料頁面中選擇「設定」。主控台會列出您現有的 Security Hub 組態原則 (組態原則)，以及此標準的狀態。
4. 選擇要在每個組態原則中啟用或停用標準的選項。
5. 完成變更後，請選擇 [下一步]。
6. 檢閱您的變更，然後選擇「套用」。此動作會影響與組態原則相關聯的所有帳號和 OU。您的設定會在本地區和所有連結的區域中生效。

在內容中配置安全性控制

依照下列步驟，透過中央組態設定內容中的安全性控制。

若要在內容中設定安全性控制項 (僅限主控台)

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在導覽窗格中，選擇 [控制項]。
3. 選擇特定控制項，然後選擇 [設定]。主控台會列出您目前的設定原則，以及每個控制項的狀態。
4. 選擇啟用或停用每個組態原則中控制項的選項。您也可以選擇自訂控制項參數。
5. 完成變更後，請選擇 [下一步]。
6. 檢閱您的變更，然後選擇「套用」。此動作會影響與組態原則相關聯的所有帳號和 OU。您的設定會在本地區和所有連結的區域中生效。

停止使用中央配置

當您停止使用中央組態時AWS Security Hub，委派的系統管理員將喪失跨多個組織單位 (OU) 和設定 Security Hub AWS 帳戶、安全性標準和安全性控制的能力AWS 區域。相反地，組織帳戶必須在每個區域中個別設定自己的大部分設定。

> **Important**
>
> 在停止使用中央設定之前，您必須先取消帳戶和 OU 與其目前組態的關聯，無論這是組態原則還是自我管理行為。
> 您也必須先刪除組態原則，才能停止使用中央設定。

當您停止中央規劃時，會發生下列變更：

- 委派的管理員無法再為組織建立組織的組態原則。
- 已套用或繼承組態原則的帳戶會保留其目前的設定，但會成為自我管理。
- 您的組織會切換至本機組態。在本機組態下，必須在每個組織帳戶和區域中分別設定大多數 Security Hub 設定。委派的系統管理員可以選擇自動啟用 Security Hub、預設安全性標準，以及屬於新組織帳戶預設標準一部分的所有控制項。默認標準是基AWS礎安全性最佳實踐（FSBP）和互聯網安全中心（CIS）AWS基準基準 v1.2.0。這些設定只會在目前的「區域」中生效，而且只會影響新的組織帳戶。委派的系統管理員無法變更哪些預設標準。本機設定不支援在 OU 層級使用組態原則或組態。

當您停止使用中央組態時，委派管理員帳戶的識別碼會保持不變。您的本地區域和連結的區域也會保持不變（您的主區域現在稱為彙總區域，可用於尋找彙總）。

選擇您偏好的方法，然後按照步驟停止使用中央配置並切換到本地配置。

Security Hub console

停止使用中央組態

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 在「概觀」區段中，選擇 「編輯」。
4. 在 [編輯組織組態] 方塊中，選擇 [本機組態]。如果您還沒有，系統會提示您取消關聯並刪除目前的設定原則，然後才能停止中央設定。指定為自我管理的帳戶或 OU 必須與其自我管理組態中斷關聯。您可以在主控台中執行此操作，方法是將每個自我管理帳戶的管理類型或 OU 變更為 [集中管理] 和 [從我的組織繼承]。
5. 選擇性地選取新組織帳戶的本機組態預設設定。
6. 選擇 Confirm (確認) 。

Security Hub API

停止使用中央組態

1. 調用該 UpdateOrganizationConfigurationAPI。
2. 將物件中的`ConfigurationType`欄位設`OrganizationConfiguration`定為`LOCAL`。如果您有現有的組態原則或原則關聯，API 會傳回錯誤。若要取消設定原則的關聯，請呼叫 `StartConfigurationPolicyDisassociation` API。若要刪除設定原則，請呼叫 `DeleteConfigurationPolicy` API。
3. 如果您想要在新組織帳戶中自動啟用 Security Hub，請將`AutoEnable`欄位設定為`true`。根據預設，此欄位的值為`false`，而且不會在新的組織帳戶中自動啟用 Security Hub。選擇性地，如果您要在新組織帳戶中自動啟用預設安全性標準，請將`AutoEnableStandards`欄位設定為`DEFAULT`。這是默認值。如果您不想在新組織帳戶中自動啟用預設安全性標準，請將`AutoEnableStandards`欄位設定為`NONE`。

API 請求示例：

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

停止使用中央組態

1. 執行 update-organization-configuration 命令。
2. 將物件中的ConfigurationType欄位設organization-configuration定為LOCAL。如果您有現有的組態原則或原則關聯，命令會傳回錯誤。若要取消設定原則的關聯，請執行命start-configuration-policy-disassociation令。若要刪除組態原則，請執行delete-configuration-policy命令。
3. 如果您想要在新的組織帳戶中自動啟用安全性中樞，請包含auto-enable參數。根據預設，此參數的值為no-auto-enable，而且不會在新的組織帳戶中自動啟用 Security Hub。選擇性地，如果您要在新組織帳戶中自動啟用預設安全性標準，請將auto-enable-standards欄位設定為DEFAULT。這是默認值。如果您不想在新組織帳戶中自動啟用預設安全性標準，請將auto-enable-standards欄位設定為NONE。

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

管理管理員和成員帳戶

如果您的AWS環境有多個帳戶，您可以將使用 AWS Security Hub 的帳戶視為成員帳戶，並將其與單一系統管理員帳戶建立關聯。管理員可以監控您的整體安全狀況，並對成員帳戶採取允許的處理行動。管理員還可以大規模執行各種帳戶管理和管理任務，例如監控估計的使用成本和評估帳戶配額。

您可以通過兩種方式將成員帳戶與管理員建立關聯，方法是將 Security Hub 與 Security Hub 中的成員資格邀請整合AWS Organizations或手動傳送和接受成員資格邀請。

透過 AWS Organizations 管理帳戶

AWS Organizations是一項全球帳戶管理服務，可讓管理AWS員整合和管理多個帳戶AWS 帳戶。它提供帳戶管理和合併帳單功能，旨在支援預算、安全性和合規性需求。它不收取額外費用，並且與多個集成AWS 服務，包括 AWS Security Hub，Amazon Macie 和 Amazon GuardDuty。如需詳細資訊，請參閱《AWS Organizations 使用者指南》https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html。

當您整合 Security Hub 和時AWS Organizations，Organizations 管理帳戶會指定 Security Hub 委派的系統管理員。Security Hub 會自動在指定資訊安全中心的委派系統管理員帳戶AWS 區域中啟用。

指定委派的系統管理員之後，我們建議您使用中央設定來管理 Security Hub 中的帳戶。這是自訂 Security Hub 並確保組織適當安全性涵蓋範圍的最有效方法。

中央設定可讓委派的系統管理員跨多個組織帳戶和區域自訂 Security Hub，而不是依區域設定。您可以為整個組織建立組態原則，或為不同帳戶和 OU 建立不同的組態原則。這些原則會指定在關聯帳戶中是否啟用或停用 Security Hub，以及啟用哪些安全性標準和控制項。

委派管理員可以將帳戶指定為集中管理或自我管理的帳戶。集中管理的帳戶只能由委派的系統管理員設定。自我管理帳戶可以指定自己的設定。

如果您未選擇加入中央設定，委派的系統管理員可以設定 Security Hub 的能力更有限，稱為本機組態。在本機組態下，委派的系統管理員可以在目前區域的新組織帳戶中，自動啟用 Security Hub 和預設安全性標準。但是，現有帳戶不會使用這些設定，因此在帳戶加入組織後可能會發生設定偏差。

除了這些新帳戶設定之外，本機組態是帳戶特定且特定於區域的設定。每個組織帳戶必須分別在每個區域中設定 Security Hub 服務、標準和控制項。本機設定也不支援使用設定原則。

透過邀請手動管理帳戶

如果您擁有獨立帳戶或未與 Organizations 整合，則必須在 Security Hub 中透過邀請手動管理成員帳戶。獨立帳戶無法與 Organizations 整合，因此必須以手動方式進行管理。如果您 future 新增其他帳戶，建議您整合AWS Organizations並使用中央設定。

當您使用手動帳戶管理時，您可以指定帳戶做為 Security Hub 管理員。管理員帳戶可以查看成員帳戶中的數據，並對成員帳戶發現項目採取某些操作。Security Hub 系統管理員邀請其他帳戶成為成員帳戶，而當潛在成員帳戶接受邀請時，就會建立系統管理員與成員關係。

手動帳號管理不支援使用設定原則。如果沒有組態原則，系統管理員就無法針對不同帳戶設定變數設定，以集中自訂 Security Hub。相反地，每個組織帳戶都必須在每個區域中個別啟用和設定 Security Hub。這可能會使您更加困難和耗時，以確保您使用 Security Hub 的所有帳戶和區域都有足夠的安全性涵蓋範圍。這也可能導致配置偏移，因為成員帳戶可以指定自己的設置，而無需管理員輸入。

若要透過邀請管理帳戶，請參閱應邀管理帳戶。

管理帳戶 AWS Organizations

您可以 AWS Security Hub 與組織中的帳戶整合 AWS Organizations，然後管理安全中心。

若要將 Security Hub 與整合 AWS Organizations，請在中建立組織 AWS Organizations。組 Organizations 管理帳戶會將一個帳戶指定為組織的 Security Hub 委派系統管理員。委派的系統管理員接著可以為組織中的其他帳戶啟用 Security Hub、將這些帳戶新增為 Security Hub 成員帳戶，並對成員帳戶採取允許的動作。Security Hub 委派的系統管理員可以啟用和管理最多 10,000 個成員帳戶的 Security Hub。

委派管理員的組態能力範圍取決於您是否使用中央組態。啟用中央設定後，您不需要在每個成員帳戶和 AWS 區域. 委派的系統管理員可以在指定的成員帳戶和組織單位 (OU) 跨區域強制執行特定的 Security Hub 設定。

Security Hub 委派的系統管理員帳戶可以對成員帳戶執行下列動作：

- 如果使用中央組態，請透過建立 Security Hub 組態原則來集中設定成員帳戶和 OU 的 Security Hub。組態原則可用來啟用和停用 Security Hub、啟用和停用標準，以及啟用和停用控制項。
- 加入組織時，自動將新帳戶視為 Security Hub 成員帳戶。如果您使用中央組態，與 OU 相關聯的組態原則會包含屬於 OU 一部分的現有帳戶和新帳戶。
- 將現有的組織帳戶視為「Security Hub」成員帳戶。如果您使用中央規劃，這會自動發生。

- 取消屬於組織的成員帳戶的關聯。如果您使用中央設定，則只有在將成員帳戶指定為自我管理後，才能將其取消關聯。或者，您可以將停用 Security Hub 的組態原則與特定的集中管理成員帳戶建立關聯。

如需委派管理員可對成員帳戶執行的動作完整清單，請參閱帳號允許的動作。

本節中的主題說明如何將 Security Hub 與整合，以 AWS Organizations 及如何管理組織中帳戶的安全性中樞。在相關的情況下，每個部分都會識別中央組態使用者的管理優點和差異。

主題

- 整合 Security Hub AWS Organizations
- 在新的組織帳戶中自動啟用安全中心
- 在新的組織帳戶中手動啟用安全中心
- 取消成員帳戶與組織的關聯
- 停用 Security Hub 整合 AWS Organizations

整合 Security Hub AWS Organizations

若要整合 AWS Security Hub 和 AWS Organizations，您可 Organizations 在 [組織] 中建立組織，並使用組織管理帳戶來指定委派的 Security Hub 系統管理員帳戶。委派的系統管理員接著可以為成員帳戶啟用 Security Hub、檢視成員帳戶中的資料，以及對成員帳戶執行其他允許的動作。

如果您使用中央組態，則委派的系統管理員也可以建立 Security Hub 組態原則，以指定如何在組織帳戶中設定 Security Hub 服務、標準和控制項。

建立組織

組織是您建立用來合併的實體，以 AWS 帳戶 便您可以將它們當作單一單位來管理。

您可以使用 AWS Organizations 主控台或使用其中一個 SDK API 中的 AWS CLI 命令來建立組織。如需詳細指示，請參閱《AWS Organizations 使用指南》中的「建立組織」。

您可以用 AWS Organizations 來集中檢視和管理組織內的所有帳戶。組織具有一個管理帳戶，以及零個或多個成員帳戶。您可以使用階層式的樹狀結構來組織帳戶，其頂端有根，而組織單位 (OU) 則位於根目錄下。每個帳戶都可以直接位於根目錄下，或放置在階層中的其中一個 OU 中。OU 是特定帳戶的容器。例如，您可以建立包含與財務作業相關之所有帳戶的財務 OU。

選擇委派 Security Hub 系統管理員的建議

如果您有手動邀請程序中的系統管理員帳戶，而且正在使用轉換至帳戶管理 AWS Organizations，則 Security Hub 建議您將該帳戶指定為委派的 Security Hub 系統管理員。

您不應將組織管理帳戶指定為委派的 Security Hub 系統管理員。這是因為有權存取組織管理帳戶以管理帳單的使用者，可能與需要存取 Security Hub 進行安全性管理的使用者不同。

我們建議跨區域使用相同的委派管理員。如果您選擇加入中央設定，Security Hub 會自動在您的主區域和任何連結的區域中指定相同的委派系統管理員。

驗證設定委派 Security Hub 系統管理員的權限

若要指定和移除委派的 Security Hub 系統管理員帳戶，組織管理帳戶必須具有 Security Hub 中的`EnableOrganizationAdminAccount`和`DisableOrganizationAdminAccount`動作的權限。Organizations 管理帳戶也必須具有 Organizations 的管理權限。

若要授與所有必要的權限，請將下列 Security Hub 受管政策附加至組織管理帳戶的 IAM 主體：

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

指定委派的 Security Hub 系統管理員

若要指定委派的 Security Hub 系統管理員帳戶，您可以使用 Security Hub 主控台、Security Hub API 或 AWS CLI。Security Hub AWS 區域 只會在目前設定委派的系統管理員，而且您必須在其他區域中重複此動作。如果您開始使用中央組態，則 Security Hub 會自動在主區域和連結的區域中設定相同的委派系統管理員。

組織管理帳戶不需要啟用安全性中樞，即可指定委派的安全中心系統管理員帳戶。

我們建議組織管理帳戶不是委派的 Security Hub 系統管理員帳戶。不過，如果您確實選擇組織管理帳戶做為 Security Hub 委派的系統管理員，則管理帳戶必須啟用 Security Hub。如果管理帳戶未啟用 Security Hub，您必須手動為其啟用 Security Hub。無法為組織管理帳戶自動啟用 Security Hub。

> **Note**
>
> 您必須使用下列其中一種方法指定委派的 Security Hub 系統管理員。使用 Organizations API 指定委派的 Security Hub 系統管理員並不會反映在資訊安全中心中。
> 選擇您偏好的方法，然後按照步驟指定委派的 Security Hub 系統管理員帳戶。

Security Hub console

在上線時指定委派的 Security Hub 系統管理員

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 選擇 [移至 Security Hub]。系統會提示您登入組織管理帳戶。
3. 在 [指定委派管理員] 頁面的 [委派管理員帳戶] 區段中，指定委派管理員帳戶。我們建議您選擇您為其他 AWS 安全性和規範遵循服務設定的相同委派管理員。
4. 選擇設定委派管理員。系統會提示您登入委派的系統管理員帳戶 (如果您尚未登入)，以便使用中央設定繼續上線。如果您不想啟動中央設定，請選擇 [取消]。您的委派管理員已設定，但您尚未使用中央設定。

從 [設定] 頁面指定委派的 Security Hub 管理員

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在 [安全性中心] 瀏覽窗格中，選擇 [設定]。然後選擇一般。
3. 如果目前已指派 Security Hub 管理員帳戶，則必須先移除目前帳戶，才能指定新帳戶。

   若要移除目前帳戶，請選擇 [委派管理員] 底下的 [移除]。
4. 輸入您要指定為 Security Hub 系統管理員帳戶之帳戶的帳戶識別碼。

   您必須在所有區域中指定相同的安全性中樞系統管理員帳戶。如果您指定的帳戶與其他區域中指定的帳戶不同，則主控台會傳回錯誤訊息。
5. 選擇委派。

Security Hub API

從組織管理帳戶叫用 EnableOrganizationAdminAccountAPI。提供委派 Security Hub 系統管理員帳戶的 AWS 帳戶 識別碼。

AWS CLI

從組織管理帳戶執行enable-organization-admin-account命令。提供委派 Security Hub 系統管理員帳戶的 AWS 帳戶 識別碼。

範例命令：

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

移除委派的 Security Hub 管理員

> **Warning**
>
> 當您使用中央設定時，您無法使用安全中心主控台或 Security Hub API 來變更或移除委派的系統管理員帳戶。如果組織管理帳戶使用 AWS Organizations 主控台或 AWS Organizations API 來變更或移除委派的 Security Hub 系統管理員，Security Hub 會自動停止集中設定，並刪除您的組態原則和原則關聯。成員帳戶會保留委派系統管理員變更或移除前所擁有的組態。

只有組織管理帳戶可以移除委派的 Security Hub 系統管理員帳戶。

若要變更委派的 Security Hub 系統管理員，您必須先移除目前委派的系統管理員帳戶，然後指定新的系統管理員帳戶。

如果您使用 Security Hub 主控台移除一個區域中的委派系統管理員，則會在所有區域中自動移除該委派系統管理員。

Security Hub API 只會從發出 API 呼叫或命令的區域移除委派的 Security Hub 系統管理員帳戶。您必須在其他區域中重複此動作。

如果您使用 Organizations API 移除委派的 Security Hub 系統管理員帳戶，則會在所有區域中自動移除該帳戶。

移除委派的 Security Hub 系統管理員 (Organizations API， AWS CLI)

您可以使用 Organizations 移除所有區域中委派的 Security Hub 系統管理員。

如果您使用中央組態來管理帳戶，則移除委派的管理員帳戶會導致刪除您的組態原則和原則關聯。成員帳戶會保留在委派管理員變更或移除之前所擁有的組態。不過，移除的委派系統管理員帳戶無法再管理這些帳戶。它們成為自我管理帳戶，必須在每個區域中單獨配置。

選擇您偏好的方法，然後依照指示移除委派的 Security Hub 系統管理員帳戶 AWS Organizations。

AWS Organizations API

移除委派的 Security Hub 系統管理員

調用該 DeregisterDelegatedAdministratorAPI。提供委派系統管理員帳戶的帳戶識別碼，以及 Security Hub 的服務主體，也就是說`securityhub.amazonaws.com`。

AWS CLI

移除委派的 Security Hub 系統管理員

執行 deregister-delegated-administrator 命令。提供委派系統管理員帳戶的帳戶識別碼，以及 Security Hub 的服務主體，也就是說securityhub.amazonaws.com。

```
aws organizations deregister-delegated-administrator --account-id <admin account ID>
 --service-principal <Security Hub service principal>
```

範例

```
aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

移除委派的 Security Hub 系統管理員 (Security Hub 主控台)

您可以使用 Security Hub 主控台來移除所有區域中委派的安全中樞系統管理員。

移除委派的 Security Hub 系統管理員帳戶時，成員帳戶會與已移除的委派 Security Hub 系統管理員帳戶中斷關聯。

Security Hub 仍在成員帳戶中啟用。在新的 Security Hub 管理員啟用成員帳戶之前，它們會成為獨立帳戶。

如果組織管理帳戶不是 Security Hub 中已啟用的帳戶，請使用 [歡迎使用安全性中心] 頁面上的選項。

從 [歡迎使用 Security Hub] 頁面移除委派的 Security Hub 系統管理員帳戶

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 選擇 [移至 Security Hub]。
3. 在委派管理員下，選擇移除。

如果組織管理帳戶是 Security Hub 中已啟用的帳戶，請使用 [設定] 頁面 [一般] 索引標籤上的選項。

若要從 [設定] 頁面移除委派的 Security Hub 系統管理員帳戶

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在 [安全性中心] 瀏覽窗格中，選擇 [設定]。然後選擇一般。
3. 在委派管理員下，選擇移除。

移除委派的 Security Hub 系統管理員 (Security Hub API， AWS CLI)

您可以使用 Security Hub API 或 Security Hub 作業 AWS CLI 來移除委派的 Security Hub 系統管理員。當您使用其中一種方法移除委派管理員時，只會在發出 API 呼叫或命令的區域中將其移除。安全中心不會更新其他區域，也不會移除中的委派系統管理員帳戶 AWS Organizations。

選擇您偏好的方法，然後依照下列步驟移除具有 Security Hub 的委派安全中心系統管理員帳戶。

Security Hub API

移除委派的 Security Hub 系統管理員

使用組織管理帳戶的認證呼叫 DisableOrganizationAdminAccountAPI。提供委派 Security Hub 系統管理員帳戶的帳戶識別碼。

AWS CLI

移除委派的 Security Hub 系統管理員

使用組織管理帳戶的認證，執行disable-organization-admin-account命令。提供委派 Security Hub 系統管理員帳戶的帳戶識別碼。

```
aws securityhub disable-organization-admin-account --admin-account-id <admin account
 ID>
```

範例

```
aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

在新的組織帳戶中自動啟用安全中心

當新帳戶加入您的組織時，這些帳戶會新增至 AWS Security Hub 主控台 [帳戶] 頁面上的清單中。針對組織帳戶，類型為依組織。根據預設，新帳戶在加入組織時不會成為 Security Hub 成員。他們的狀態為非成員。委派的系統管理員帳戶可以自動將新帳戶新增為成員，並在這些帳戶加入組織時在這些帳戶中啟用 Security Hub。

> **Note**
>
> 雖然 AWS 區域 有許多區域預設為使用中狀態 AWS 帳戶，但您必須手動啟用某些區域。這些區域在本文件中稱為選擇加入區域。若要在選擇加入區域的新帳戶中自動啟用 Security Hub，

該帳戶必須先啟用該區域。只有帳戶擁有者可以啟用選擇加入區域。如需有關選擇加入區域的詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用的項目。

根據您使用中央規劃 (建議) 還是本端規劃，此程序會有所不同。

自動啟用新組織帳號 (集中配置)

如果您使用中央組態，您可以建立已啟用 Security Hub 的組態原則，在新的和現有的組織帳戶中自動啟用 Security Hub。然後，您可以將原則與組織根目錄或特定組織單位 (OU) 產生關聯。

如果您將已啟用 Security Hub 的組態原則與特定 OU 產生關聯，則屬於該 OU 的所有帳戶 (現有和新增) 中都會自動啟用 Security Hub。不屬於 OU 的新帳戶是自我管理的，而且不會自動啟用 Security Hub。如果您將啟用 Security Hub 的組態原則與根目錄建立關聯，則會在加入組織的所有帳戶 (現有和新增) 中自動啟用 Security Hub。例外情況是，如果帳戶透過應用程式或繼承使用不同的策略，或是自我管理。

在您的組態原則中，您也可以定義應在 OU 中啟用哪些安全性標準和控制項。若要針對已啟用的標準產生控制項發現項目，OU 中的帳號必須已 AWS Config 啟用並設定為記錄必要的資源。如需有關 AWS Config 錄製的詳細資訊，請參閱啟用和設定 AWS Config。

如需建立組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

自動啟用新組織帳戶 (本機組態)

當您使用本機設定並開啟自動啟用時，Security Hub 會將新的組織帳戶新增為成員，並在目前的區域中啟用 Security Hub。其他地區不受影響。此外，開啟自動啟用並不會在現有組織帳戶中啟用 Security Hub，除非這些帳戶已新增為成員帳戶。

開啟自動啟用後，當他們加入組織時，目前區域中的新帳戶也會自動啟用預設安全性標準。默認標準是基 AWS 礎安全性最佳實踐（FSBP）和互聯網安全中心（CIS） AWS 基準基準 v1.2.0。您無法變更預設標準。如果您想要在整個組織中啟用其他標準，或針對特定帳戶和 OU 啟用標準，建議您使用中央組態。

若要針對預設標準 (以及其他已啟用的標準) 產生控制項搜尋結果，您組織中的科目必須已 AWS Config 啟用並設定為記錄必要的資源。如需有關 AWS Config 錄製的詳細資訊，請參閱啟用和設定 AWS Config。

選擇您偏好的方法，然後按照步驟在新的組織帳戶中自動啟用 Security Hub。這些指示只有在您使用本機組態時才適用。

Security Hub console

若要自動啟用新的組織帳戶做為 Security Hub 成員

1. 開啟主 AWS Security Hub 控台，網址為 https://console.aws.amazon.com/securityhub/。

   Sign 正在使用委派系統管理員帳戶的認證。
2. 在 [Security Hub] 瀏覽窗格的 [設定] 下，選擇 [組態]。
3. 在「帳戶」區段中，開啟「自動啟用帳戶」。

Security Hub API

若要自動啟用新的組織帳戶做為 Security Hub 成員

從委派的系統管理員帳戶叫用 UpdateOrganizationConfigurationAPI。將AutoEnable欄位設定為true以在新組織帳戶中自動啟用安全性中樞。

AWS CLI

若要自動啟用新的組織帳戶做為 Security Hub 成員

從委派的系統管理員帳戶執行update-organization-configuration命令。包含auto-enable參數以在新的組織帳戶中自動啟用安全中心。

```
aws securityhub update-organization-configuration --auto-enable
```

在新的組織帳戶中手動啟用安全中心

如果您未在新的組織帳戶中自動啟用 Security Hub，當他們加入組織時，您可以將這些帳戶新增為成員，並在他們加入組織後手動啟用 Security Hub。您也必須手動啟用安全性中樞 AWS 帳戶 ，您先前已取消與組織的關聯。

> **Note**
>
> 如果您使用中央配置，則此部分不適用於您。如果您使用中央設定，您可以建立組態原則，以便在指定的成員帳戶和組織單位 (OU) 中啟用 Security Hub。您也可以在這些帳戶和 OU 中啟用特定標準和控制項。

如果帳戶已經是不同組織內的成員帳戶，您就無法在帳戶中啟用 Security Hub。

您也無法在目前暫停的帳戶中啟用安全性中樞。如果您嘗試在暫停的帳戶中啟用服務，帳戶狀態會變更為 [帳戶已暫停]。

- 如果該帳戶未啟用 Security Hub，則會在該帳戶中啟用安全性中心。除非您關閉默認安全標準，否則 AWS 基 AWS 礎安全性最佳實踐（FSBP）標準和 CIS 基準測試 v1.2.0 也會在帳戶中啟用。

  此情況的例外是「Organizations」管理帳戶。無法在 Organizations 管理帳戶中自動啟用 Security Hub。您必須先在 Organizations 管理帳戶中手動啟用 Security Hub，才能將其新增為成員帳戶。
- 如果帳戶已啟用 Security Hub，Security Hub 不會對帳戶進行任何其他變更。它只能啟用成員資格。

若要讓 Security Hub 產生控制項發現項目，成員帳戶必須已 AWS Config 啟用並設定為記錄必要的資源。如需詳細資訊，請參閱啟用並設定 AWS Config。

選擇您偏好的方法，然後依照步驟將組織帳戶啟用為 Security Hub 成員帳戶。

Security Hub console

手動將組織帳戶啟用為 Security Hub 成員

1. 開啟主 AWS Security Hub 控台，網址為 https://console.aws.amazon.com/securityhub/。

   使用委派系統管理員帳戶的認證登入。
2. 在 [Security Hub] 瀏覽窗格的 [設定] 下，選擇 [組態]。
3. 在 [帳號] 清單中，選取您要啟用的每個組織帳戶。
4. 選擇「動作」，然後選擇「新增成員」。

Security Hub API

手動將組織帳戶啟用為 Security Hub 成員

從委派的系統管理員帳戶叫用 `CreateMembers`API。對於要啟用的每個帳戶，請提供帳戶 ID。

與手動邀請程序不同，當您呼叫`CreateMembers`以啟用組織帳戶時，不需要傳送邀請。

AWS CLI

手動將組織帳戶啟用為 Security Hub 成員

從委派的系統管理員帳戶執行`create-members`命令。對於要啟用的每個帳戶，請提供帳戶 ID。

與手動邀請程序不同，當您執行`create-members`以啟用組織帳戶時，不需要傳送邀請。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

範例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

取消成員帳戶與組織的關聯

若要停止接收及檢視來自 AWS Security Hub 成員帳戶的發現項目，您可以取消成員帳戶與組織的關聯。

> **Note**
>
> 如果您使用中央規劃，解除關聯的運作方式不同。您可以建立一個組態原則，停用一或多個集中管理的成員帳戶中的 Security Hub。之後，這些帳戶仍然是組織的一部分，但不會產生 Security Hub 發現項目。如果您使用中央設定，但也有手動邀請的成員帳戶，則可以取消一或多個手動邀請帳戶的關聯。

使用管理的成員帳戶 AWS Organizations 無法取消其帳戶與系統管理員帳戶的關聯。只有管理員帳戶可以取消成員帳戶的關聯。

取消成員帳戶的關聯並不會關閉帳戶。而是從組織中移除成員帳戶。取消關聯的成員帳戶會變成獨立帳戶， AWS 帳戶 該帳戶不再由與 Security Hub 整合 AWS Organizations管理。

選擇您偏好的方法，然後按照步驟取消成員帳戶與組織的關聯。

Security Hub console

若要取消成員帳戶與組織的關聯

1. 開啟主 AWS Security Hub 控台，網址為 https://console.aws.amazon.com/securityhub/。

   使用委派系統管理員帳戶的認證登入。
2. 在功能窗格的 [設定] 下，選擇 [組態]。

3. 在「帳戶」區段中，選取您要取消關聯的帳戶。如果您使用中央設定，您可以選取手動邀請的帳戶，以取消與索引標籤的關聯。Invitation accounts僅當您使用中央規劃時，此頁籤才可見。
4. 選擇 [動作]，然後選擇 [取消帳戶關聯]。

Security Hub API

若要取消成員帳戶與組織的關聯

從委派的系統管理員帳戶叫用 DisassociateMembersAPI。您必須提供成員帳戶的 AWS 帳戶 ID 才能取消關聯。若要檢視成員帳戶清單，請呼叫 ListMembersAPI。

AWS CLI

若要取消成員帳戶與組織的關聯

從委派的系統管理員帳戶執行 > disassociate-members 命令。您必須提供成員帳戶的 AWS 帳戶 ID 才能取消關聯。若要檢視成員帳戶清單，請執行 > list-members 命令。

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

範例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

您也可以使用 AWS Organizations 控制台 AWS CLI、或 AWS SDK 取消成員帳戶與組織的關聯。如需詳細資訊，請參閱《使用指南》中的〈從組織中移除成員帳AWS Organizations 戶〉。

停用 Security Hub 整合 AWS Organizations

與組 AWS Organizations 織整合之後 AWS Security Hub，「組 Organizations」管理帳戶隨後可以停用整合。身為 Organizations 管理帳戶的使用者，您可以在中停用 Security Hub 的受信任存取權限來執行此操作 AWS Organizations。

當您停用 Security Hub 的受信任存取時，會發生下列情況：

- Security Hub 失去其作為中受信任服務的狀態 AWS Organizations。
- 安全中心委派的系統管理員帳戶會失去所有安全性中樞成員帳戶的安全性中樞設定、資料和資源的存取權 AWS 區域。

- 如果您使用的是中央組態，Security Hub 會自動停止為您的組織使用它。您的組態原則和原則關聯都會遭到刪除。帳戶會保留在您停用受信任存取之前所擁有的組態。
- 所有 Security Hub 成員帳戶都會成為獨立帳戶，並保留其目前的設定。如果已針對一或多個區域中的成員帳戶啟用 Security Hub，則會繼續為這些區域中的帳戶啟用安全性中樞。啟用的標準和控制項也不會變更。您可以在每個帳戶和地區分別變更這些設定。不過，帳戶不再與任何區域中委派的系統管理員相關聯。

如需停用受信任服務存取之結果的其他資訊，請參閱《使用AWS Organizations 者指南》 AWS 服務中的「 AWS Organizations 與其他」搭配使用。

若要停用受信任的存取，您可以使用 AWS Organizations 主控台、Organizations API 或 AWS CLI. 只有 Organizations 管理帳戶的使用者可以停用 Security Hub 的信任服務存取權。如需有關所需權限的詳細資訊，請參閱《AWS Organizations 使用指南》中的「停用受信任存取所需的權限」。

停用受信任的存取之前，我們建議您與組織的委派系統管理員合作，以停用成員帳戶中的 Security Hub，並清除這些帳戶中的 Security Hub 資源。

選擇您偏好的方法，然後依照步驟停用 Security Hub 的受信任存取權。

Organizations console

若要停用 Security Hub 的受信任存取

1. AWS Management Console 使用 AWS Organizations 管理帳戶的認證登入。
2. 開啟「Organizations」主控台，位於 https://console.aws.amazon.com/organizations/。
3. 在導覽窗格中，選擇服務。
4. 在 [整合式服務] 下，選擇AWS Security Hub。
5. 選擇停用受信任的存取。
6. 確認您要停用受信任的存取。

Organizations API

若要停用 Security Hub 的受信任存取

調用 AWS Organizations API 的禁用AWSServiceAccess操作。對於`ServicePrincipal`參數，請指定 Security Hub 服務主體 (`securityhub.amazonaws.com`)。

AWS CLI

若要停用 Security Hub 的受信任存取

執行 AWS Organizations API 的disable-aws-service-access命令。對於`service-principal`參數，請指定 Security Hub 服務主體 (`securityhub.amazonaws.com`)。

範例：

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

應邀管理帳戶

您可以通過兩種方式集中管理多個AWS Security Hub帳戶，方法是將 Security Hub 與AWS Organizations或手動發送和接受會員邀請集中管理。如果您擁有獨立帳戶或未與 Organizations 整合，則必須使用手動程序。在手動帳戶管理中，安全性中心系統管理員會邀請帳戶成為成員。當潛在成員接受邀請時，就會建立管理員與成員關係。Security Hub 系統管理員帳戶可以管理多達 1,000 個以邀請為基礎的成員帳戶的 Security Hub 心。

> **Tip**
>
> 如果您在 Security Hub 中建立以邀請為基礎的組織，您可以隨後轉換為改用AWS Organizations。如果您有多個會員帳戶，我們建議您透過管理帳戶AWS Organizations。

發現項目與其他資料的跨區域彙總可供您透過手動邀請程序邀請的帳戶使用。不過，當您使用手動邀請程序AWS 區域時，您必須分別在每個成員帳戶中分別設定 Security Hub 設定。

您也必須針對不屬於您組織的帳戶使用以邀請為基礎的手動程序。例如，您可能不會在組織中包含測試帳戶。或者，您可能想要將來自多個組織的帳戶合併到單一 Security Hub 系統管理員帳戶下。Security Hub 系統管理員帳戶必須傳送邀請至屬於其他組織的帳戶。

在 Security Hub 主控台的 [組態] 頁面上，透過邀請新增的帳戶會列在 [邀請帳戶] 索引標籤中。如果您使用安全中心中的集中配置，但也邀請組織外的帳戶，您可以在此索引標籤中檢視來自邀請型帳戶的發現項目。不過，Security Hub 系統管理員無法透過使用組態原則設定跨區域的邀請型帳戶。

本節中的主題說明如何透過邀請管理成員帳戶。

主題

- 新增和邀請成員帳戶
- 回應成為會員帳戶的邀請
- 取消關聯成員帳戶
- 刪除成員帳戶
- 取消與管理員帳戶的關聯
- 轉換AWS Organizations為帳戶管理

新增和邀請成員帳戶

您的帳戶會成為接受邀請之帳戶的AWS Security Hub管理員。

當您接受來自其他帳戶的邀請時，您的帳戶會成為成員帳戶，而該帳戶會成為您的管理員。

如果您的帳戶是管理員帳戶，則無法接受成為會員帳戶的邀請。

新增成員帳戶包含下列步驟：

1. 管理員帳戶會將成員帳戶新增至其成員帳戶清單。
2. 管理員帳戶會傳送邀請至成員帳戶。
3. 會員帳戶接受邀請。

新增會員帳戶

透過 Security Hub 主控台，您可以將帳戶新增至您的成員帳戶清單。在 Security Hub 主控台中，您可以個別選取帳戶，或上傳包含帳戶資訊的`.csv`檔案。

對於每個帳戶，您必須提供帳戶 ID 和電子郵件地址。電子郵件地址應該是帳戶安全性問題時要聯絡的電子郵件地址。它不用於驗證帳戶。

選擇您偏好的方式，然後依照步驟新增會員帳戶。

Security Hub console

將帳戶新增至您的成員帳戶清單

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

使用管理員帳戶的憑據登錄。

2. 在左側窗格中，選擇 Settings (設定)。
3. 在 [設定] 頁面上，選擇 [帳戶]，然後選擇 [新增帳戶]。然後，您可以個別新增帳戶，或上傳包含帳號清單的.csv檔案。
4. 若要選取帳戶，請執行下列其中一個動作：

   - 若要個別新增帳戶，請在 [輸入帳戶] 底下，輸入要新增之帳戶的帳戶 ID 和電子郵件地址，然後選擇 [新增]。

     對每個帳戶重複此過程。

   - 若要使用逗號分隔值 (.csv) 檔案新增多個帳戶，請先建立檔案。該文件必須包含要添加的每個帳戶的帳戶 ID 和電子郵件地址。

     在您的.csv清單中，每行必須顯示一個帳戶。.csv檔案的第一行必須包含標頭。在標題中，第一列是**Account ID**，第二列是**Email**。

     後續每行都必須包含要新增帳戶的有效帳戶 ID 和電子郵件地址。

     以下是在文字編輯器中檢視.csv檔案的範例。

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     在試算表程式中，欄位會顯示在不同的欄中。基礎格式仍以逗號分隔。您必須將帳戶 ID 格式化為非十進位數字。例如，帳戶識別碼 444455556666 無法格式化為 444455556666.0。另外，請確保數字格式不會從帳戶 ID 中刪除任何前導零。

     若要選取檔案，請在主控台上選擇 [上傳清單 (.csv)]。然後選擇「瀏覽」。

     選取檔案後，請選擇 [新增帳戶]。
5. 完成新增帳戶後，在 [要新增的帳戶] 下，選擇 [下一步]。

Security Hub API

將帳戶新增至您的成員帳戶清單

從管理員帳戶叫用 CreateMembersAPI。對於要添加的每個成員帳戶，您必須提供 AWS 帳戶 ID。

AWS CLI

將帳戶新增至您的成員帳戶清單

從管理員帳戶執行`create-members`命令。對於要添加的每個成員帳戶，您必須提供 AWS 帳戶 ID。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

範例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

邀請會員帳戶

新增成員帳戶後，您會傳送邀請至該成員帳戶。您也可以重新傳送邀請給您與管理員取消關聯的帳戶。

Security Hub console

邀請潛在會員帳戶

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用管理員帳戶的憑據登錄。
2. 在功能窗格中，選擇 [設定]，然後選擇 [帳戶]。
3. 對於要邀請的帳戶，請在「狀態」欄中選擇「邀請」。
4. 系統提示您確認時，請選擇「邀請」。

> **Note**
>
> 若要重新傳送已取消關聯之帳戶的邀請，請在 [帳戶] 頁面上選取每個已取消關聯的 在 [動作] 中，選擇 [重新傳送邀

Security Hub API

邀請潛在會員帳戶

從管理員帳戶叫用 InviteMembersAPI。對於每個要邀請的帳戶，您必須提供 AWS 帳戶 ID。

AWS CLI

邀請潛在會員帳戶

從管理員帳戶執行invite-members命令。對於每個要邀請的帳戶，您必須提供 AWS 帳戶 ID。

```
aws securityhub invite-members --account-ids <accountIDs>
```

範例

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

回應成為會員帳戶的邀請

您可以接受或拒絕成為會員帳戶的邀請。

接受邀請後，您的帳戶就AWS Security Hub會成為會員帳戶。傳送邀請的帳戶會成為您的 Security Hub 系統管理員帳戶。系統管理員帳戶使用者可以在 Security Hub 中檢視您的成員帳戶的發現項目。

如果您拒絕邀請，您的帳戶會在管理員帳戶的成員帳戶清單上標示為已撤銷。

您只能接受一個成為會員帳戶的邀請。

您必須先啟用 Security Hub，才能接受或拒絕邀請。

請記住，所有 Security Hub 帳戶都必須已AWS Config啟用並設定，才能記錄所有資源。如需需求的詳細資訊AWS Config，請參閱啟用和設定AWS Config。

接受邀請

選擇您偏好的方式，然後按照步驟接受成為會員帳戶的邀請。

Security Hub console

接受會員邀請

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 在功能窗格中，選擇 [設定]，然後選擇 [帳戶]。

3. 在 [系統管理員帳戶] 區段中，開啟 [接受]，然後選擇 [接受邀請]。

Security Hub API

接受會員邀請

調用該 AcceptAdministratorInvitationAPI。您必須提供邀請識別碼和管理員帳戶的 AWS 帳戶 ID。若要擷取有關邀請的詳細資料，請使用ListInvitations作業。

AWS CLI

接受會員邀請

執行 accept-administrator-invitation 命令。您必須提供邀請識別碼和管理員帳戶的 AWS 帳戶 ID。若要擷取有關邀請的詳細資料，請執行list-invitations命令。

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

範例

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> 安全中心主控台會繼續使用AcceptInvitation。它最終將更改為使用AcceptAdministratorInvitation。任何專門控制此功能存取權的 IAM 政策都必須繼續使用AcceptInvitation。您也應該新增AcceptAdministratorInvitation至您的原則，以確保主控台開始使用之後有正確的權限AcceptAdministratorInvitation。

拒絕邀請

您可以拒絕成為會員帳戶的邀請。當您在 Security Hub 主控台中拒絕邀請時，您的帳戶會在系統管理員帳戶的成員帳戶清單上標示為已退出。

拒絕邀請時，您必須登入收到邀請的成員帳戶。

選擇您偏好的方式，然後按照步驟拒絕成為會員帳戶的邀請。

Security Hub console

拒絕會員邀請

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 在功能窗格中，選擇 [設定]，然後選擇 [帳戶]。
3. 在「管理員帳戶」區段中，選擇「拒絕邀請」。

Security Hub API

拒絕會員邀請

調用該 DeclineInvitationsAPI。您必須提供發出邀請的管理員帳戶 AWS 帳戶 ID。若要檢視邀請的相關資訊，請使用ListInvitations作業。

AWS CLI

拒絕會員邀請

執行 decline-invitations 命令。您必須提供發出邀請的管理員帳戶 AWS 帳戶 ID。若要檢視邀請的相關資訊，請執行list-invitations指令。

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

範例

```
aws securityhub decline-invitations --account-ids "123456789012"
```

取消關聯成員帳戶

AWS Security Hub管理員帳戶可以取消成員帳戶的關聯，以停止接收和檢視該帳戶的發現項目。您必須先取消成員帳戶的關聯，才能刪除該帳戶。

當您取消關聯成員帳戶時，該帳戶會保留在狀態為「已移除 (已取消關聯)」的成員帳戶清單中。您的帳戶會從成員帳戶的管理員帳戶資訊中移除。

若要繼續接收帳戶的發現項目，您可以重新傳送邀請。要完全刪除會員帳戶，您可以刪除會員帳戶。

選擇您偏好的方法，然後按照步驟取消受手動邀請的成員帳戶與管理員帳戶的關聯。

Security Hub console

取消與手動邀請成員帳戶的關聯

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用管理員帳戶的憑據登錄。
2. 在功能窗格的 [設定] 下，選擇 [組態]。
3. 在「帳戶」區段中，選取您要取消關聯的帳戶。
4. 選擇 [動作]，然後選擇 [取消帳戶關聯]。

Security Hub API

取消與手動邀請成員帳戶的關聯

從管理員帳戶叫用 DisassociateMembersAPI。您必須提供要取消關聯之成員帳戶的 AWS 帳戶 ID。若要檢視成員帳戶清單，請使用此ListMembers作業。

AWS CLI

取消與手動邀請成員帳戶的關聯

從管理員帳戶執行disassociate-members命令。您必須提供要取消關聯之成員帳戶的 AWS 帳戶 ID。若要檢視成員帳戶清單，請執行list-members命令。

```
aws securityhub disassociate-members --account-ids <accountIds>
```

範例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

刪除成員帳戶

AWS Security Hub身為管理員帳戶，您可以刪除透過邀請加入的成員帳戶。您必須先取消已啟用帳戶的關聯，才能刪除該帳戶。

當您刪除成員帳戶時，該帳戶會從清單中完全移除。要恢復帳戶的會員資格，您必須添加並再次邀請它，就像它是一個全新的會員帳戶一樣。

您無法刪除屬於組織且使用與整合進行管理的帳戶AWS Organizations。

選擇您偏好的方式，然後按照步驟刪除手動邀請的會員帳戶。

Security Hub console

刪除手動邀請的會員帳戶

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   使用管理員帳戶登入。
2. 在瀏覽窗格中，選擇 [設定]，然後選擇 [組態]。
3. 選擇 [邀請帳戶] 索引標籤。然後，選取要刪除的帳號。
4. 選擇動作，然後選擇刪除。只有在您取消帳戶關聯時，此選項才可用。您必須先取消成員帳戶的關聯，才能刪除該帳戶。

Security Hub API

刪除手動邀請的會員帳戶

從管理員帳戶叫用 DeleteMembersAPI。您必須提供要刪除之成員帳戶的 AWS 帳戶 ID。若要擷取成員帳戶清單，請叫用 ListMembersAPI。

AWS CLI

刪除手動邀請的會員帳戶

從管理員帳戶執行delete-members命令。您必須提供要刪除之成員帳戶的 AWS 帳戶 ID。若要擷取成員帳戶清單，請執行list-members命令。

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

範例

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

取消與管理員帳戶的關聯

如果您的帳戶是透過邀請加入AWS Security Hub成員帳戶，您可以取消該成員帳戶與管理員帳戶的關聯。取消關聯成員帳戶後，Security Hub 不會將發現項目從帳戶傳送至系統管理員帳戶。

使用與整合管理的成員帳戶AWS Organizations無法取消其帳戶與系統管理員帳戶的關聯。只有 Security Hub 委派的系統管理員可以取消與 Organizations 所管理之成員帳戶的關聯。

當您取消與管理員帳戶的關聯時，您的帳戶會保留在系統管理員帳戶的成員清單中，且狀態為 [已撤銷]。不過，系統管理員帳戶不會收到您帳戶的任何發現項目。

取消您自己與管理員帳戶的關聯後，成為成員的邀請仍然存在。您 future 來可以再次接受邀請。

Security Hub console

取消與管理員帳戶的關聯

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 在功能窗格中，選擇 [設定]，然後選擇 [帳戶]。
3. 在 [系統管理員帳戶] 區段中，關閉 [接受]，然後選擇 [更新]。

Security Hub API

取消與管理員帳戶的關聯

調用該 DisassociateFromAdministratorAccountAPI。

AWS CLI

取消與管理員帳戶的關聯

執行 disassociate-from-administrator-account 命令。

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> 安全中心主控台會繼續使用DisassociateFromMasterAccount。它最終將更改為使用DisassociateFromAdministratorAccount。任何專門控制此功能存取權的 IAM 政策都必須繼續使用DisassociateFromMasterAccount。您也應該新增DisassociateFromAdministratorAccount至您的原則，以確保主控台開始使用之後有正確的權限DisassociateFromAdministratorAccount。

轉換AWS Organizations為帳戶管理

在中手動管理帳戶時AWS Security Hub，您必須邀請潛在會員帳戶，並在每個帳戶中分別配置每個成員帳戶AWS 區域。

透過整合 Security Hub 和AWS Organizations，您就可以免除傳送邀請的需求，並進一步掌控 Security Hub 在組織中設定和自訂的方式。

您可以使用組合方法來使用AWS Organizations整合，但也可以手動邀請組織外部的帳戶。不過，我們建議您只使用「Organizations」整合。集中設定是一項可協助您跨多個帳戶和區域管理 Security Hub 的功能，只有在您與組 Organizations 整合時才能使用。

本節說明如何從以邀請為基礎的手動帳戶管理轉換為管理帳戶。AWS Organizations

整合 Security Hub AWS Organizations

首先，您必須整合 Security Hub 和AWS Organizations.

您可以透過完成下列步驟來整合這些服務：

- 在中建立組織AWS Organizations。如需指示，請參閱《AWS Organizations使用指南》中的「建立組織」。
- 從 Organizations 管理帳戶中，指定 Security Hub 委派的系統管理員帳戶。

> **Note**
>
> 組織管理帳戶無法設定為 DA 帳戶。

如需詳細說明，請參閱 整合 Security Hub AWS Organizations。

完成上述步驟後，即表示您授與中的 Security Hub 受信任存取權限AWS Organizations。這也會為委派的系統管理員帳戶啟AWS 區域用目前的安全中樞。

委派的系統管理員可以在 Security Hub 中管理組織，主要是將組織的帳戶新增為 Security Hub 成員帳戶。系統管理員也可以存取這些帳戶的特定 Security Hub 設定、資料和資源。

當您使用組織轉換為帳戶管理時，以邀請為基礎的帳戶不會自動成為 Security Hub 成員。只有您新增至新組織的帳戶才能成為 Security Hub 成員。

中央配置與本地配置

啟用整合後，您可以管理「Organizations」的帳戶。如需相關資訊，請參閱 管理帳戶 AWS Organizations。帳戶管理會根據您組織的組態類型而有所不同。

您的組織有兩種可能的組態類型：本端和中央。您的預設組態類型為本機組態。若要查看您目前的組態類型，請在 Security Hub 主控台的導覽窗格中選擇 [設定]，然後選擇 [組態]。您也可以叫用 `DescribeOrganizationConfiguration`API 來檢視您的組態類型。

在本機組態下，委派的系統管理員帳戶可以選擇在新帳戶加入組織時自動啟用 Security Hub 和預設安全性標準。這些新帳號設定會在目前的「地區」中生效。其他安全性中樞設定必須由每個區域中的每個成員帳戶個別設定。

我們建議使用中央配置而不是本地配置。在中央組態下，委派的系統管理員帳戶可以建立 Security Hub 組態原則，以便跨多個區域生效，並在組織的各種帳戶和組織單位 (OU) 中指定 Security Hub 功能。您可以將單一組態原則套用至整個組織，或將不同的組態原則套用至不同的帳戶和 OU。例如，您可以在生產帳戶中啟用一組標準和控制項，並在測試帳戶中啟用不同的一組標準和控制項。DA 可以根據需要編輯配置策略。

如需中央組態如何運作的詳細資訊，請參閱安全中心中的集中配置。

如需從本端規劃切換到中央規劃的指示，請參閱開始使用中央配置。

帳號允許的動作

管理員和成員帳戶可以存取下表中所述的AWS Security Hub動作。在表中，這些值具有以下含義：

- 任何 — 帳戶可針對同一管理員下的任何成員帳戶執行動作。
- 目前 — 帳戶只能為自己 (您目前登入的帳戶) 執行動作。
- 破折號 — 指示帳號無法執行動作。

如表格中所述，允許的動作會根據您是否整合，以AWS Organizations及組織使用的組態類型而有所不同。如需中央規劃和本端規劃之間差異的資訊，請參閱透過 AWS Organizations 管理帳戶。

Security Hub 不會將成員帳戶發現項目複製到系統管理員帳戶中。在 Security Hub 中，所有發現項目都會擷取至特定帳戶的特定區域。在每個區域中，管理員帳戶都可以檢視和管理該區域中其成員帳戶的發現項目。

如果您設定彙總區域，管理員帳戶可以檢視並管理複製至聚總區域之連結區域的成員帳戶發現項目。如需跨區域彙總的詳細資訊，請參閱跨區域彙總。

此表格反映管理員和成員帳戶的預設權限。您可以使用自訂 IAM 政策進一步限制對 Security Hub 功能和功能的存取。如需指引和範例，請參閱將 IAM 政策與使用者角色調整的部落格文章。AWS Security Hub

如果您與組 Organizations 整合並使用中央組態，則允許的動作

如果您與組 Organizations 整合並使用中央設定，系統管理員和成員帳戶可以存取 Security Hub 動作，如下所示。

動作	Security Hub 委派管理員帳戶	集中管理的會員帳戶	自行管理會員帳戶
建立和管理 Security Hub 組態原則	適用於自我和集中管理帳戶	–	–
檢視組織帳戶	任何	–	–
取消關聯成員帳戶	任何	–	–
刪除會員帳號	任何非組織帳戶	–	–
停用 Security Hub	適用於往來帳戶和集中管理帳戶	–	Current
檢視發現項目與尋找項目	任何	Current	Current
更新發現	任何	Current	Current
檢視洞察結果	任何	Current	Current
檢視控制項詳情	任何	Current	Current
開啟或關閉合併的控制項發現項目	任何	–	–
啟用和停用標準	適用於往來帳戶和集中管理帳戶	–	Current

動作	Security Hub 委派管理員帳戶	集中管理的會員帳戶	自行管理會員帳戶
啟用和停用控制項	適用於往來帳戶和集中管理帳戶	–	Current
啟用和停用整合	Current	Current	Current
設定跨區域彙總	任何	–	–
選擇主地區和連結區域	任何（必須停止並重新啟動中央配置才能更改主區域）	–	–
設定自訂動作	Current	Current	Current
設定自動化規則	任何	–	–
設定自訂見解	Current	Current	Current

如果您與組 Organizations 整合並使用本機組態，則允許的動作

如果您與組 Organizations 整合並使用本機組態，系統管理員和成員帳戶可以存取 Security Hub 動作，如下所示。

動作	Security Hub 委派管理員帳戶	成員帳戶
建立和管理 Security Hub 組態原則	–	–
檢視組織帳戶	任何	–
取消關聯成員帳戶	任何	–
刪除會員帳號	–	–
停用 Security Hub	–	目前 (如果帳戶與委派管理員取消關聯)

動作	Security Hub 委派管理員帳戶	成員帳戶
檢視發現項目與尋找項目	任何	Current
更新發現	任何	Current
檢視洞察結果	任何	Current
檢視控制項詳情	任何	Current
開啟或關閉合併的控制項發現項目	任何	–
啟用和停用標準	Current	Current
在新組織帳戶中自動啟用安全中樞和預設標準	目前帳戶與新組織帳戶	–
啟用和停用控制項	Current	Current
啟用和停用整合	Current	Current
設定跨區域彙總	任何	–
設定自訂動作	Current	Current
設定自動化規則	任何	–
設定自訂見解	Current	Current

邀請型帳號允許的動作

如果您使用以邀請為基礎的方法手動管理帳戶，而不是與整合，系統管理員和成員帳戶可以存取 Security Hub 動作，如下所示。AWS Organizations

動作	Security Hub 管理員帳戶	成員帳戶
建立和管理 Security Hub 組態原則	–	–

動作	Security Hub 管理員帳戶	成員帳戶
檢視組織帳戶	任何	–
取消關聯成員帳戶	任何	Current
刪除會員帳號	任何	–
停用 Security Hub	目前 (如果沒有已啟用的成員帳戶)	目前 (如果帳號與管理員帳戶取消關聯)
檢視發現項目與尋找項目	任何	Current
更新發現	任何	Current
檢視洞察結果	任何	Current
檢視控制項詳情	任何	Current
開啟或關閉合併的控制項發現項目	任何	–
啟用和停用標準	Current	Current
在新組織帳戶中自動啟用安全中樞和預設標準	–	–
啟用和停用控制項	Current	Current
啟用和停用整合	Current	Current
設定跨區域彙總	任何	–
設定自訂動作	Current	Current
設定自動化規則	任何	–
設定自訂見解	Current	Current

帳戶管理的限制和建議

下節概述了在中管理成員帳戶時要記住的一些限制和建議 AWS Security Hub。

成員帳戶的數目上限

如果您使用與整合 AWS Organizations，則 Security Hub 最多可支援每個委派系統管理員帳戶中每個帳戶 10,000 個成員帳戶 AWS 區域。如果您手動啟用和管理安全中心，則 Security Hub 支援每個區域中每個系統管理員帳戶最多 1,000 個成員帳戶邀請。

帳戶和區域

各組織成員資格

如果您將 Security Hub 與整合 AWS Organizations，Organizations 管理帳戶可以為 Security Hub 指定委派的系統管理員 (DA) 帳戶。組織管理帳戶無法在組 Organizations 中設定為 DA。雖然安全中心允許這樣做，但我們建議 Organizations 管理帳戶不應該是 DA。

我們建議您在所有地區選擇相同的 DA 帳戶。如果您使用中央組態，則 Security Hub 會在您為組織設定安全中心的所有區域中設定相同的 DA 帳戶。

我們也建議您在 AWS 安全性和合規性服務中選擇相同的 DA 帳戶，以協助您在單一管理窗格中管理與安全性相關的問題。

邀請成員資格

對於透過邀請建立的成員帳戶，系統管理員與成員帳戶關聯只會在邀請寄出來源的地區建立。系統管理員帳戶必須在您想要使用它的每個區域中啟用安全性中樞。然後，管理員帳戶會邀請每個帳戶成為該地區的會員帳戶。

管理員與成員關係的限制

> **Note**
>
> 如果您使用與 Security Hub 整合 AWS Organizations，但尚未手動邀請任何成員帳戶，則本節不適用於您。

帳戶不能同時是管理員帳戶和成員帳戶。

一個成員帳戶只能與一個管理員帳戶關聯。如果組織帳戶已由 Security Hub 系統管理員帳戶啟用，則該帳戶無法接受來自其他帳戶的邀請。如果帳戶已接受邀請，則該組織的 Security Hub 管理員帳戶無法啟用該帳戶。它也無法接收來自其他帳戶的邀請。

對於手動邀請程序，可選擇是否接受成員資格邀請。

跨服務協調管理員帳戶

Security Hub 彙總了來自各種 AWS 服務的發現，例如 Amazon GuardDuty，Amazon Inspector 和 Amazon Macie。Security Hub 還允許用戶從 GuardDuty 發現中進行轉置，以在 Amazon Detective 中開始調查。

不過，您在這些其他服務中設定的系統管理員與成員關係不會自動套用至 Security Hub。Security Hub 建議您針對所有這些服務使用與系統管理員帳戶相同的帳戶。此管理員帳戶應該是負責安全工具的帳戶。相同的帳戶也應該是的彙總帳戶。 AWS Config

例如， GuardDuty 管理員帳戶 A 的使用者可以在 GuardDuty 主控台上看到 GuardDuty成員帳戶 B 和 C 的發現項目。如果帳戶 A 接著啟用安全性中樞，帳戶 A 的使用者不會在 Security Hub 中自動看到帳戶 B 和 C 的 GuardDuty發現項目。這些帳戶也需要 Security Hub 管理員與成員關係。

若要這麼做，請將帳戶 A 設為 Security Hub 系統管理員帳戶，並啟用帳戶 B 和 C 成為 Security Hub 成員帳戶。

帳戶動作對 Security Hub 資料的影響

這些帳號動作會對AWS Security Hub資料產生下列影響。

Security Hub 已停用

如果您使用中央組態，委派的系統管理員 (DA) 可以建立 Security Hub 組態原則，以AWS Security Hub在特定帳戶和組織單位 (OU) 中停用。在此情況下，安全性中樞會停用指定的帳戶和您本地區域和任何連結的區域中的 OU。

如果不使用中央設定，您必須在每個啟用 Security Hub 的帳戶和區域中個別停用安全中心。

如果系統管理員帳戶中已停用 Security Hub，則系統管理員帳戶不會產生新的發現項目。如果在 DA 帳戶中停用 Security Hub，您也無法使用中央設定。現有的問題清單會在 90 天後刪除。

與其他項目的整AWS 服務合已移除。

已啟用的安全性標準和控制項會停用。

其他 Security Hub 資料和設定 (包括自訂動作、深入解析和第三方產品訂閱) 都會保留。

取消與管理員帳戶關聯的成員帳戶

當成員帳戶與系統管理員帳戶取消關聯時，系統管理員帳戶會失去檢視成員帳戶中發現項目的權限。不過，這兩個帳戶仍會啟用 Security Hub。

如果您使用中央設定，DA 無法為與 DA 帳戶取消關聯的成員帳戶設定安全性中樞。

為管理員帳戶定義的自訂設定或整合不會套用至前一個成員帳戶的發現項目。例如，取消關聯帳戶後，管理員帳戶中可能會有一個自訂動作作為 Amazon EventBridge 規則中的事件模式。但是，此自定義操作不能在成員帳戶中使用。

在 Security Hub 系統管理員帳戶的 [帳戶] 清單中，已移除的帳戶的狀態為 [已取消關聯]。

已從組織中移除成員帳戶

從組織中移除成員帳戶時，Security Hub 系統管理員帳戶會失去檢視成員帳戶中發現項目的權限。不過，在這兩個帳戶中，仍會啟用安全性中樞，這兩個帳戶的設定與移除前的設定相同。

如果您使用中央設定，則無法在成員帳戶從委派系統管理員所屬的組織中移除 Security Hub 之後設定該帳戶。不過，除非您手動變更，否則帳戶會保留移除之前的設定。

在 Security Hub 系統管理員帳戶的 [帳戶] 清單中，已移除的帳戶的狀態為 [已刪除]。

帳戶被暫停

當帳戶在中暫停時AWS，帳戶會失去檢視其在 Security Hub 中發現項目的權限。不會針對該帳戶產生新的發現項目。暫停帳戶的系統管理員帳戶可以檢視現有的帳戶發現項目。

對於組織帳戶，成員帳戶狀態也可以變更為 [帳戶已暫停]。如果帳戶在系統管理員帳戶嘗試啟用帳戶的同時遭到暫停，就會發生這種情況。帳戶已暫停帳戶的系統管理員帳戶無法檢視該帳戶的發現項目。否則，暫停狀態不會影響會員帳戶狀態。

如果您使用中央組態，如果委派的系統管理員嘗試將組態原則與暫停的帳戶建立關聯，則原則關聯會失敗。

90 天後，帳戶將被終止或重新激活。當帳戶重新啟用時，其 Security Hub 權限會還原。如果成員帳戶狀態為 [帳戶已暫停]，則系統管理員帳戶必須手動啟用帳戶。

帳戶已關閉

當關閉AWS 帳戶時，Security Hub 響應關閉如下。

Security Hub 會保留帳戶的發現項目 90 天，自帳戶關閉的有效日期起。在 90 天期限結束時，Security Hub 會永久刪除帳戶的所有發現項目。

- 若要保留發現項目超過 90 天，您可以使用自訂動作搭配 EventBridge 規則，將發現項目存放在 Amazon S3 儲存貯體中。只要安全中心保留發現項目，當您重新開啟已關閉的帳戶時，Security Hub 會還原帳戶的發現項目。
- 如果帳戶是 Security Hub 系統管理員帳戶，則會以系統管理員身分移除該帳戶，並移除所有成員帳戶。如果該帳戶是成員帳戶，則會從 Security Hub 系統管理員帳戶中取消關聯，並以成員身分移除。
- 如需詳細資訊，請參閱帳 B AWSilling and Cost Management 使用指南中的關閉帳戶。

> **Important**
>
> 對於 AWS GovCloud (US) 區域的客戶：
>
> - 在關閉帳戶前，請先備份政策資料和其他帳戶資源，然後刪除。在您關閉帳戶後，您將沒有存取這些的權限。

跨區域彙總

透過跨區域彙總，您可以彙總發現項目、尋找更新、見解、控制合規狀態，以及從多個區域到單一彙總區域的安全分數。然後，您可以從彙總區域管理所有這些資料。

> **Note**
>
> 在中 AWS GovCloud (US)，只有發現項目、尋找更新和深入解析才支援跨區域彙總。 AWS GovCloud (US)具體而言，您只能彙總 AWS GovCloud (美國東部) 和 (美國西部) 之間的發現項目、尋找更新和 AWS GovCloud 深入解析。在中國地區，跨區域彙總僅支援跨中國區域的搜尋結果、尋找更新和見解。具體而言，您只能彙總中國（北京）和中國（寧夏）之間的調查結果，發現更新和見解。

假設您將美國東部 (維吉尼亞北部) 設定為彙總區域，將美國西部 (奧勒岡) 和美國西部 (加利佛尼亞北部) 設定為連結的區域。當您檢視美國東部 (維吉尼亞北部) 的「發現項目」頁面時，您會看到來自全部三個區域的發現項目。這些發現項目的更新也會反映在所有三個區域中。

必須在每個區域中修改控制項的啟用狀態。如果已在連結的區域中啟用控制項，但在聚總區域中停用，您可以從聚總區域查看控制項的相容性狀態，但您無法從聚總區域啟用或停用該控制項。

若要檢視跨區域安全分數和合規狀態，請將下列許可新增至使用 Security Hub 的 IAM 角色：

- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

跨區域彙總的運作方式

跨區域彙總是由獨立帳戶與管理員帳戶設定。成員帳戶從其管理員帳戶繼承跨區域彙總組態。

當成員帳戶與管理員帳戶中斷關聯時，會停止該成員帳戶的跨區域彙總。即使該帳戶在成為會員帳戶之前已啟用跨區域彙總，也是如此。

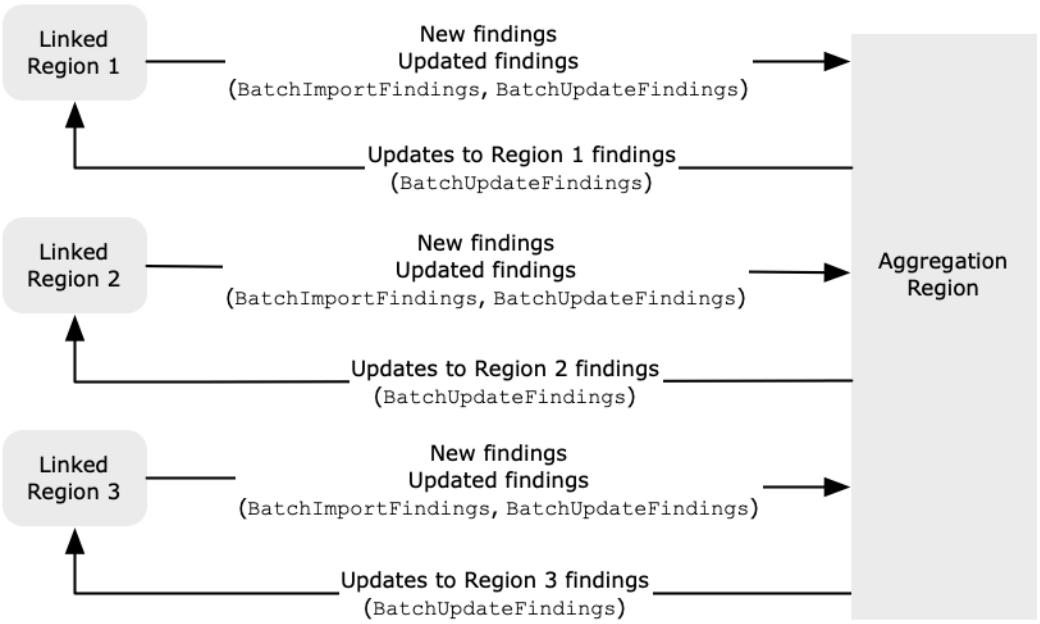
跨區域彙總是以「區域」與「連結區域」的彙總為基礎。

彙總新資料並將更新複製到資料

啟用跨區域彙總時，Security Hub 會在連結的區域和彙總區域之間彙總下列資料：

- 問題清單
- 深入分析
- 控制符合性狀態
- 安全分數

除了先前清單中的新資料之外，Security Hub 也會在連結的區域和彙總區域之間複寫此資料的更新。連結區域中發生的更新會複寫到彙總區域。彙總區域中發生的更新會複寫回連結的區域。



如果彙總 [區域] 和 [連結的區域] 中發生衝突的更新，則會使用最新的更新。

跨區域彙總不會增加 Security Hub 的成本。當 Security Hub 複寫新資料或更新時，不會向您收費。

在聚總區域中，「彙總」頁面提供跨連結區域之有效發現項目的檢視表。如需詳細資訊，請參閱依嚴重性檢視發現項目的跨區域摘要。分析發現項目的其他「摘要」頁面面板也會顯示來自跨連結區域的資訊。

彙總區域中的安全分數是透過比較傳遞的控制項數目與所有連結區域中啟用的控制項數目來計算。此外，如果至少在一個連結的 [區域] 中啟用控制項，則會在彙總 [區域] 的 [安全性] 標準詳細資料頁面上看到控制項。標準詳細資料頁面上控制項的符合性狀態反映了跨連結區域的發現項目。如果在一或多個

連結的區域中與控制項相關聯的安全性檢查失敗，該控制項的符合性狀態會在彙總「區域」的標準詳細資料頁面上顯示為「失敗」。安全檢查的數目包括來自所有連結區域的發現項目。

決定要彙總資料的帳戶

Security Hub 只會彙總帳戶已啟用 Security Hub 之區域的資料。不會根據跨區域彙總組態為帳戶自動啟用 Security Hub。

若要瞭解中央組態如何影響跨區域彙總，請參閱中央組態與跨區域彙總。

當系統管理員帳戶設定跨區域彙總時，Security Hub 會在連結的區域中識別該管理員帳戶的成員帳戶。

在每個連結的區域中，該管理員帳戶的每個成員帳戶都會繼承跨區域彙總組態。Security Hub 會將其發現項目、見解、控制狀態和安全分數彙總至彙總區域。

如果彙總區域中的成員帳戶不是連結區域中的成員帳戶，則 Security Hub 不會從該區域彙總該帳戶的資料。

如果您計劃使用跨區域彙總，並擁有多個管理員帳戶，我們建議您採用下列最佳作法：

- 每個管理員帳戶在區域中都有相同的成員帳戶。
- 每個管理員帳戶都有不同的成員帳戶。
- 每個管理員帳戶使用不同的彙總區域。

中央組態與跨區域彙總

中央配置是 Security Hub 中的一項選擇加入功能，如果您與 AWS Organizations之整合，則可以使用該功能。如果您使用中央設定，委派的系統管理員帳戶可以為組織中的帳戶和組織單位 (OU) 設定 Security Hub 服務、標準和控制項。若要設定帳戶和 OU，委派的系統管理員會建立 Security Hub 組態原則。組態原則可用來定義是否啟用或停用 Security Hub，以及啟用哪些標準和控制項。委派的系統管理員會將組態原則與特定帳戶、OU 或根 (整個組織) 產生關聯。

委派的管理員只能從彙總區域建立和管理組織的組態原則。此外，組態原則會在彙總區域和所有連結的區域中生效。您無法建立僅套用於某些連結區域的設定原則，而不適用於其他連結的區域。在中央配置中，聚合區域被稱為主區域。為了進行中央配置，相同的區域必須作為本地區域，並且為了跨區域彙總而言，作為彙總區域。如需跨區域彙總的相關資訊，請參閱跨區域彙總。

若要使用中央組態，您必須指定主區域和至少一個連結的區域。

變更跨區域彙總設定可能會影響您的組態原則。當您新增連結的區域時，您的設定政策會在該區域中生效。如果「地區」是選擇加入的區域，則必須啟用「地區」，您的組態政策才能在該處生效。相反地，當您移除連結的區域時，該區域的設定政策不會再生效。在該區域中，帳戶會維護移除連結區域時的設定。您可以更改這些設置，但必須在每個帳戶和地區分別進行更改。

如果您移除或變更主 [地區]，您的組態原則和原則關聯都會遭到刪除。您無法再在任何區域中使用集中設定或建立組態原則。帳號會維護變更或移除主要區域之前的設定。您可以隨時變更這些設定，但由於您不再使用中央設定，因此必須在每個帳戶和區域中分別修改設定。如果您指定新的本地區域，則可以使用中央組態並再次建立組態原則。

如需中央規劃的更多資訊，請參閱安全中心中的集中配置。

啟用跨區域彙總

您必須從要指定為彙總區域 AWS 區域 的「跨區域」啟用「跨區域」彙總。

您無法使用預設為停用的「區域」作為彙總區域。如需預設為停用的區域清單，請參閱在中啟用區域AWS 一般參考。

啟用跨區域彙總 (主控台)

啟用跨區域彙總時，您可以選擇連結的區域。您也可以選擇在 Security Hub 開始支援新區域且您已選擇加入新區域時，是否要自動連結新區域。

啟用跨區域彙總

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 使用選 AWS 區域 取器登入您要用作彙總「區域」的「區域」。
3. 在 [安全性中心] 瀏覽功能表中，選擇 [設定]，然後選取 [
4. 針對尋找聚總，選擇設定發現項目聚總。

   依預設，彙總「區域」設定為「無彙總區域」。
5. 在「聚總區域」下，選取將目前區域指定為彙總區域的選項。
6. 或者，對於「連結區域」，選取要從中彙總資料的區域。
7. 若要在 Security Hub 支援的情況下自動彙總來自分割區中新區域的資料，並且您選擇加入這些資料，請選取 [連結 future 區域]。
8. 選擇 儲存。

啟用跨區域彙總 (Security Hub API、 AWS CLI)

您可以使用 Security Hub API 來啟用跨區域彙總。

若要從 Security Hub API 啟用跨區域彙總，您可以建立搜尋結果彙總工具。您必須從要用作彙總「區域」的「區域」建立搜尋結果彙總工具。

若要建立尋找結果彙總器 (Security Hub API， AWS CLI)

- Security Hub API：從您要用作彙總區域的「區域」中，使用此CreateFindingAggregator作業。對於RegionLinkingMode，您可以從下列選項中選擇：
  - ALL_REGIONS— Security Hub 彙總來自所有區域的資料。Security Hub 也會在新區域受到支援的情況下彙總資料，而且您選擇加入這些資料。
  - ALL_REGIONS_EXCEPT_SPECIFIED— Security Hub 會彙總所有區域的資料，但您要排除的區域除外。Security Hub 也會在新區域受到支援的情況下彙總資料，而且您選擇加入這些資料。用Regions於提供要從彙總排除的區域清單。
  - SPECIFIED_REGIONS— Security Hub 從選定的區域清單彙總資料。Security Hub 不會自動彙總來自新區域的資料。用Regions來提供要彙總的地區清單。
- AWS CLI：在命令列中執行 create-finding-aggregator 命令。使用空格分隔每個區域。

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-
linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --
regions <Region list>
```

在下列範例中，已針對選取的區域設定跨區域彙總。彙總區域為美國東部 (維吉尼亞北部)。連結的區域是美國西部 (加利佛尼亞北部) 和美國西部 (奧勒岡)。

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

檢視跨區域彙總設定

您可以從任何區域檢視目前的跨區域彙總組態。組態包括彙總區域、連結的區域，以及是否自動連結新區域。

檢視跨區域彙總組態 (主控台)

「設定」頁面的「區域」頁籤會顯示目前的跨區域彙總組態。您可以從任何區域檢視組態。成員帳戶也可以檢視管理員帳戶所設定的跨區域組態。

如果未啟用跨區域彙總，則「區域」頁標會顯示啟用跨區域彙總的選項。請參閱 the section called “啟用跨區域彙總”。只有管理員帳戶和獨立帳戶才能啟用跨區域彙總。

如果已啟用跨區域聚總，則「區域」頁標會顯示下列資訊：

- 聚合區域
- 是否要從 Security Hub 支援且您選擇加入的新區域，自動彙總發現項目、見解、控制狀態和安全分數
- 連結區域的清單

檢視目前的跨區域彙總組態 (Security Hub API、 AWS CLI)

您可以使用 Security Hub API 或 AWS CLI 檢視目前的跨區域彙總組態。您可以從任何區域檢視跨區域彙總組態。

若要檢視目前的跨區域彙總組態 (Security Hub API， AWS CLI)

- Security Hub API：使用 `GetFindingAggregator`API。當您提出要求時，您必須提供尋找結果彙總器 ARN。要獲得發現聚合器 ARN，請使用. `ListFindingAggregators`
- AWS CLI：在命令列中執行 `get-finding-aggregator` 命令。要獲得發現聚合器 ARN，請使用. `list-finding-aggregators`

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

更新跨區域彙總組態

您可以更新跨區域彙總組態，以變更目前彙總區域的連結 AWS 區域 。您也可以變更是否要從新區域自動彙總發現項目、見解、控制狀態和安全分數。

在中啟用區域之前，不會針對選擇加入區域實作跨區域彙總變更。 AWS 帳戶在 2019 年 3 月 20 日或之後 AWS 推出的區域為選擇加入「地區」。

當您停止從連結的區域彙總資料時，Security Hub 不會從彙總區域移除任何現有的彙總資料。

您無法使用更新程序來變更聚總區域。若要變更彙總區域，您必須執行下列動作：

1. 停止跨區域彙總。請參閱 the section called “停止跨區域彙總”。
2. 變更至您要成為新彙總區域的「區域」。
3. 啟用跨區域彙總。請參閱 the section called “啟用跨區域彙總”。

更新跨區域彙總組態 (主控台)

您必須從目前的彙總區域更新跨區域彙總組態。

在彙總區域以 AWS 區域 外，「發現項目」聚總面板會顯示一則訊息，告知您必須在彙總「區域」中編輯組態。選擇此訊息以顯示連結，以切換作業選項至聚總區域。

若要變更目前彙總區域的連結區域

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 變更為目前彙總區域。
3. 在資訊安全中心導覽功能表中，選擇 [設定]，然後選擇 [地區]
4. 在尋找彙總下，選擇編輯。
5. 在「連結區域」下，更新選取的連結區域。
6. 如果需要，請變更是否選取「連結 future 區域」。此設定會決定 Security Hub 是否會在新增區域支援時自動連結新區域，並且您選擇加入這些區域。
7. 選擇 儲存。

更新跨區域彙總組態 (Security Hub API、 AWS CLI)

您可以使用 Security Hub API 或 AWS CLI 更新跨區域彙總組態。您必須從目前的彙總區域更新跨區域彙總。

您可以變更區域連結模式。如果連結模式為`ALL_REGIONS_EXCEPT_SPECIFIED`或`SPECIFIED_REGIONS`，您可以變更已排除或包含區域的清單。

當您變更排除或包含的區域清單時，您必須提供包含更新的完整清單。例如，假設您目前彙總來自美國東部 (俄亥俄) 的發現項目，並且想要彙總來自美國西部 (奧勒岡) 的發現項目。撥打電話時

UpdateFindingAggregator，您會提供一份同時包含美國東部 (俄亥俄) 和美國西部 (奧勒岡) 的Regions清單。

若要更新跨區域彙總 (Security Hub API， AWS CLI)

- Security Hub API：使用 UpdateFindingAggregatorAPI 操作。若要識別發現項目彙總器，您必須提供尋找結果彙總器 ARN。要獲得發現聚合器 ARN，請使用. ListFindingAggregators

  您可以提供「區域」連結模式，以及已更新的排除或包含的區域清單。
- AWS CLI：在命令列中執行 update-finding-aggregator 命令。使用空格分隔每個區域。

```
aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
 ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

  在下列範例中，所選區域的跨區域彙總組態變更為彙總。此命令會從目前的彙總區域 (美國東部 (維吉尼亞北部) 執行。連結的區域是美國西部 (加利佛尼亞北部) 和美國西部 (奧勒岡)。

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
 arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
west-2
```

停止跨區域彙總

如果您不想再彙總資料或想要變更彙總區域，請停止跨區域彙總。

當您停止跨區域彙總時，Security Hub 會停止彙總資料。它不會從彙總區域移除任何現有的彙總資料。

停止跨區域彙總 (主控台)

您必須停止目前彙總區域的跨區域彙總。

在聚總區域以外的區域中，「搜尋結果」聚總面板會顯示一則訊息，告知您必須在聚總區域中編輯組態。選擇此訊息以顯示切換至聚總區域的連結。

若要停止跨區域彙總

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

2. 變更為目前彙總區域。
3. 在資訊安全中心導覽功能表中，選擇 [設定]，然後選擇 [地區]
4. 在尋找彙總下，選擇編輯。
5. 在「聚總區域」下，選擇「無聚總區域」。
6. 選擇 儲存。
7. 在確認對話方塊的確認欄位中輸入**Confirm**。
8. 選擇確認。

停止跨區域彙總 (Security Hub API、 AWS CLI)

您可以使用 Security Hub API 停止跨區域彙總。您必須停止聚總「區域」的「跨區域」彙總。

若要停止跨區域彙總 (Security Hub API， AWS CLI)

- Security Hub API：使用DeleteFindingAggregator操作。若要識別要刪除的尋找項目彙總器，請提供尋找結果彙總器 ARN。要獲得發現聚合器 ARN，請使用. ListFindingAggregators
- AWS CLI：在命令列中執行 delete-finding-aggregator 命令。

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

AWS 安全中心的發現項目

AWS Security Hub 消除了處理來自多個提供者的大量發現項目的複雜性。它減少了管理和提高所有資源和工作負載的 AWS 帳戶安全性所需的工作量。

Security Hub 會從下列來源接收發現項目。

- 與您啟用的 AWS 安全服務整合。請參閱the section called “AWS 服務 整合”。
- 與您啟用第三方產品的整合。請參閱the section called “第三方產品整合”。
- 您設定的自訂整合。請參閱the section called “使用自訂產品整合”。
- Security Hub 會檢查已啟用的控制項。請參閱the section called “產生及更新控制項發現項”。

Security Hub 會使用稱為「 AWS 安全性搜尋結果格式」的標準發現項目格式來消耗 如需問題清單格式的詳細資訊，請參閱 the section called “問題清單格式”。

Security Hub 會將整合式產品的發現項目建立關聯，以排定最重要的優先順序。

問題清單提供者可以更新問題清單，來反映問題清單的其他案例。您可以更新問題清單，提供您調查及其結果的詳細資訊。

Security Hub 也可讓您彙總跨區域的發現項目，以便您可以從單一位置檢視所有發現項目。請參閱跨區域彙總。

主題

- 建立及更新發現項目 AWS Security Hub
- 按嚴重性檢視發現項目的跨區域摘要
- 檢視尋找項目清單與詳細資訊 AWS Security Hub
- 針對中的發現採取行動 AWS Security Hub
- AWS 安全性搜尋結果格式 (ASFF)

建立及更新發現項目 AWS Security Hub

在中 AWS Security Hub，發現項目可能來自下列其中一種尋找結果提供者類型。

- 與其他 AWS 服務啟用的整合
- 與第三方提供者的啟用整合

- 安全中心中已啟用的控制項

在建立問題清單後，問題清單提供者和客戶便可以更新問題清單。

- 問題清單提供者可以使用 BatchImportFindings API 操作來更新問題清單的一般資訊。問題清單提供者只能更新其建立的問題清單。
- 客戶使用 BatchUpdateFindingsAPI 作業將調查的狀態反映為發現項目。BatchUpdateFindings也可以代表客戶使用售票、事件管理、協調流程、補救或 SIEM 工具。

  從 Security Hub 主控台，客戶可以管理發現項目的工作流程狀態，並將發現項目傳送至自訂動作。請參閱the section called “對發現採取行動”。

Security Hub 也會自動更新和刪除發現項目。

如果在過去 90 天內沒有更新，所有發現都會自動刪除。

如果您啟用跨區域彙總，則 Security Hub 會自動將連結區域中的新發現項目彙總至彙總區域。Security Hub 也會將更新複寫到發現項目。連結區域中發生的更新會複寫到彙總區域。彙總區域中發生的更新會複寫到原始的連結區域。如需跨區域彙總的詳細資訊，請參閱跨區域彙總。

主題

- 使用 BatchImportFindings 建立和更新問題清單
- 使用 BatchUpdateFindings 更新問題清單

使用 BatchImportFindings 建立和更新問題清單

問題清單提供者可以使用 BatchImportFindings API 操作來建立新的問題清單和更新其建立問題清單的資訊。問題清單提供者無法更新其未建立的問題清單。

客戶、SIEM、票證工具和 SOAR 工具可以使用 BatchUpdateFindings 來進行與其處理來自問題清單提供者問題清單相關的更新。請參閱the section called “使用 BatchUpdateFindings”。

每當 AWS Security Hub 收到創建或更新發現的BatchImportFindings請求時，它都會自動在 Amazon 中生成Security Hub Findings - Imported事件 EventBridge。請參閱the section called “自動化回應與補救”。

帳戶和批次大小的要求

BatchImportFindings必須由下列其中一項呼叫：

- 與發現項目相關聯的帳戶。關聯帳戶的識別碼是發現項目AwsAccountId屬性的值。
- 允許列出正式 Security Hub 合作夥伴整合的帳戶。

Security Hub 只能接受針對已啟用 Security Hub 的帳戶尋找更新。同時也必須啟用問題清單提供者。如果 Security Hub 停用，或未啟用尋找項目提供者整合，則會在FailedFindings清單中傳回發現項目，並顯示錯InvalidAccess誤。

BatchImportFindings每個批次最多可接受 100 個發現項目，每個搜尋結果最多可接受 240 KB，每個批次最多可接受 6 MB 的發現項目。每個區域的節流速率限制為每個帳戶 10 TPS，突發為 30 TPS。

決定是要建立或更新問題清單

若要判斷是否要建立或更新發現項目，Security Hub 會檢查ID欄位。如果 ID 的值與現有問題清單不相符，則會建立新的問題清單。

如果ID不符合現有的發現項目，則 Security Hub 會檢查更新的UpdatedAt欄位。

- 如果UpdatedAt在更新上與現有發現項目相符或之前UpdatedAt發生，則會忽略更新。
- 如果更新上的 UpdatedAt 在現有問題清單上的 UpdatedAt 之後發生，則會更新現有問題清單。

的受限屬性 BatchImportFindings

對於現有的發現項目，尋找提供者無法使用BatchImportFindings來更新下列屬性和物件。這些屬性只能使用更新BatchUpdateFindings。

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub 會忽略中BatchImportFindings針對這些屬性和物件的任何內容。客戶或其他代表他們行事的供應商會用BatchUpdateFindings來更新他們。

使用 FindingProviderFields

尋找提供者也不應使用BatchImportFindings來更新下列屬性。

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

相反地，尋找提供者會使用FindingProviderFields物件來提供這些屬性的值。

範例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

對於BatchImportFindings請求，Security Hub 處理頂層屬性中的值，FindingProviderFields如下所示。

(偏好) 在中**BatchImportFindings**提供屬性的值 **FindingProviderFields**，但不提供對應頂層屬性的值。

例如，BatchImportFindings提供FindingProviderFields.Confidence，但不提供Confidence。這是BatchImportFindings請求的首選選項。

安全中心會更新中的屬性值FindingProviderFields。

只有當屬性尚未由BatchUpdateFindings更新時，它才會將值複寫到頂層屬性。

BatchImportFindings提供頂層屬性的值，但不提供中對應屬性的值**FindingProviderFields**。

例如，BatchImportFindings提供Confidence，但不提供FindingProviderFields.Confidence。

Security Hub 會使用值來更新中的屬性FindingProviderFields。它會覆寫任何現有的值。

只有當屬性尚未由更新時，Security Hub 才會更新頂層屬性BatchUpdateFindings。

BatchImportFindings提供最上層屬性和中對應屬性的值**FindingProviderFields**。

例如，同時BatchImportFindings提供Confidence和FindingProviderFields.Confidence。

對於新發現項目，Security Hub 會使用中的值FindingProviderFields來填入中的最上層屬性和對應屬性FindingProviderFields。它不會使用提供的頂層屬性值。

對於現有的發現項目，Security Hub 會使用這兩個值。但是，只有當屬性尚未由更新時，它才會更新頂層屬性值BatchUpdateFindings。

使用來自的batch-import-findings命令 AWS CLI

在中 AWS Command Line Interface，您可以使用命batch-import-findings令來建立或更新發現項目。

您可以將每個發現項目提供為 JSON 物件。

範例

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
```

```
                "Partition": "aws",
                "Region": "us-west-1",
                "Type": "AwsCloudTrailTrail"
            }
        ],
        "SchemaVersion": "2018-10-08",
        "Title": "CloudTrail trail vulnerability",
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

使用 BatchUpdateFindings 更新問題清單

此BatchUpdateFindings動作可用來更新與客戶從尋找提供者處理搜尋結果相關的資訊。客戶可以使用它，也可以由代表客戶工作的 SIEM，票務，事件管理或 SOAR 工具使用。您可以使用BatchUpdateFindings來更新「 AWS 安全性搜尋結果格式」(ASFF) 中的特定欄位。

您無法使用BatchUpdateFindings來建立新的發現項目。您可以使用它一次最多更新 100 個發現項目。

每當 Security Hub 收到更新發現的BatchUpdateFindings請求時，它會自動在 Amazon 中生成一個Security Hub Findings - Imported事件 EventBridge。請參閱the section called “自動化回應與補救”。

BatchUpdateFindings 不會變更問題清單的 UpdatedAt 欄位。UpdatedAt 只會反映問題清單提供者最近一次的更新。

的可用欄位 BatchUpdateFindings

管理員帳號可以使用 > BatchUpdateFindings 來更新其帳戶或其成員帳戶的發現項目。成員帳戶可以使用 > BatchUpdateFindings 來更新其帳戶的發現項目。

客戶只能使用 > BatchUpdateFindings 來更新下列欄位和物件。

- Confidence
- Criticality

- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

依預設，管理員和成員帳戶可以存取上述所有欄位和欄位值。Security Hub 也提供內容索引鍵，可讓您限制對欄位和欄位值的存取。

例如，您可能只允許將成員帳戶設定Workflow.Status為RESOLVED。或者，您可能不想允許更改會員帳戶Severity.Label。

設定存取權 BatchUpdateFindings

您可以設定 IAM 政策，以限制使BatchUpdateFindings用更新欄位和欄位值的存取權。

在限制存取的陳述式中BatchUpdateFindings，使用下列值：

- Action 是 securityhub:BatchUpdateFindings
- Effect 是 Deny
- 對於Condition，您可以根據下列項目拒絕BatchUpdateFindings要求：
  - 發現項目包括特定欄位。
  - 搜尋結果包括特定欄位值。

條件索引鍵

這些是用於限制訪問的條件鍵。BatchUpdateFindings

「退回」欄位

ASFF 欄位的條件索引鍵如下：

```
securityhub:ASFFSyntaxPath/<fieldName>
```

*<fieldName>*以 ASFF 欄位取代。設定存取權時BatchUpdateFindings，請在 IAM 政策中包含一或多個特定的 ASFF 欄位，而不是父級欄位。例如，若要限制對Workflow.Status欄位的存取，您必須包含 securityhub:ASFFSyntaxPath/Workflow.Status在原則中，而不是Workflow父層級欄位。

不允許對欄位進行所有更新

為了防止用戶對特定字段進行任何更新，請使用如下條件：

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

例如，下列陳述式表示BatchUpdateFindings無法用來更新工作流程狀態。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

不允許特定欄位值

為了防止用戶將字段設置為特定值，請使用如下條件：

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
               }
}
```

例如，下列陳述式表示BatchUpdateFindings無法用來設定Workflow.Status為SUPPRESSED。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

您也可以提供不允許的值清單。

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
               }
}
```

例如，下列陳述式表示BatchUpdateFindings無法用Workflow.Status來設定為RESOLVED或SUPPRESSED。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

使用來自的 batch-update-findings命令 AWS CLI

在中 AWS Command Line Interface，您可以使用命batch-update-findings令來更新發現項目。

針對每個要更新的發現項目，您都會提供產生發現項目之產品的尋找項目 ID 和 ARN。

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

當您提供要更新的屬性時，您可以使用 JSON 格式或捷徑格式。

以下是使用 JSON 格式之Note物件的更新範例：

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

以下是使用快捷方式格式的相同更新：

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

命 AWS CLI 令參考提供每個欄位的 JSON 和捷徑語法。

下列 > batch-update-findings 範例會更新兩個發現項目，以新增附註、變更嚴重性標籤並加以解決。

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

這是相同的例子，但使用快捷方式而不是 JSON。

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

按嚴重性檢視發現項目的跨區域摘要

在「摘要」頁面上，「依區域分類的搜尋結果」會彙總區域每個嚴重度的作用中發現項目數目 計數只包含工作流程狀態為NEW或的發現項目NOTIFIED。

啟用跨區域聚總之前，「依區域的搜尋結果」只會彙總目前「區域」的搜尋結果。它提供設定跨區域彙總的連結。

啟用跨區域聚總之後，「依區域的搜尋結果」只會顯示在聚總區域中。它不會顯示在連結的區域中。此小組會摘要所有連結區域的發現項目。

根據預設，清單只會顯示具有相符發現項目的連結區域。若要顯示所有連結的區域，包括沒有相符發現項目的連結區域，請選擇「所有連結的區域」。若只要顯示具有相符搜尋結果的連結區域，請選擇含搜尋結果的連結區域。

當您選擇「區域」的嚴重性值時，便會顯示「發現項目」清單。清單會依選取的區域和嚴重性進行篩選。此外，也會篩選清單，以顯示工作流程狀態為NEW或的作用中發現項目NOTIFIED。

檢視尋找項目清單與詳細資訊 AWS Security Hub

在 AWS Security Hub 瀏覽窗格中，[控制項] 頁面會顯示 Security Hub 中可用的控制項合併清單。請參閱the section called “檢視和管理安全性控制”。

在 [安全性標準] 頁面上，您可以瀏覽至特定標準，並檢視目前在標準中啟用之控制項的發現項目清單。請參閱the section called “檢視和管理安全性標準”。

在「見解」頁面上，您可以檢視相符分析結果的發現項目清單。請參閱the section called “檢視洞見結果和問題清單”。

在「發現項目」頁面上，您可以檢視在一或多個標準中啟用的已啟用產品整合和控制項中的發現項目清單。Security Hub 還會跟踪 90 天的查找歷史記錄。

在「整合」頁面上，您可以檢視其他 AWS 服務或第三方整合所產生的發現項目清單。請參閱the section called “檢視整合傳送的問題清單”。

您也可以使用 `GetFindings` API 操作來擷取篩選後的問題清單。

如果您啟用跨區域彙總，則可以檢視跨區域的控制項狀態、安全分數、見解和發現項目。在彙總區域中，「控制項」、「安全性」標準、「發現項目」和「見解」頁面包含來自彙總區域和連結區域的資料。在其他區域中，這些頁面只包含來自該區域的發現項目。如需如何設定跨區域彙總的相關資訊，請參閱跨區域彙總。

主題

- 篩選和分組發現項目 (主控台)
- 檢視發現項目詳細資料

篩選和分組發現項目 (主控台)

當您從「發現項目」頁面、「整合」頁面或「見解」頁面顯示發現項目清單時，一律會根據記錄狀態和工作流程狀態篩選清單。這是用於洞察或集成的過濾器的補充。

記錄狀態指出問題清單處於作用中還是已存檔狀態。尋找項目提供者可以封存搜尋結果。 AWS Security Hub 如果刪除關聯的資源，也會自動封存控制項的發現項目。根據預設，問題清單只會顯示作用中的問題清單。

工作流程狀態指出問題清單的調查狀態。工作流程狀態只能由 Security Hub 客戶或代表客戶操作的系統更新。根據預設，問題清單只會顯示工作流程狀態為 NEW 或 NOTIFIED 的問題清單。預設控制項的問題清單也會包含 RESOLVED 問題清單。

如果您已啟用尋找彙總，則可以在「發現項目」和「見解」頁面上，依「區域」篩選發現項目。

如需使用控制項尋找清單的資訊，請參閱〈〉the section called “篩選和排序發現項目”。

新增篩選條件

如要變更清單的範圍，您可以新增篩選條件。

您最多可以篩選 10 個屬性。對於每個屬性，您最多可以提供 20 個篩選值。

篩選尋找項目清單時，Security Hub 會將 AND 邏輯套用至篩選器集合。換句話說，只有當問題清單符合所有提供的篩選條件時，才會相符。例如，如果您新增 GuardDuty 為產品名稱的篩選器，並新增`AwsS3Bucket`為資源類型的篩選器，則符合的發現項目必須符合這兩個條件。

不過，Security Hub 會將 OR 邏輯套用至使用相同屬性但不同值的篩選器。例如，您將兩者 GuardDuty 和 Amazon Inspector 器添加為產品名稱的過濾器值。在這種情況下，發現匹配，如果它是由 GuardDuty 或 Amazon Inspector 生成的。

將篩選條件新增到問題清單

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 若要顯示發現項目清單，請執行下列任一項作業：

- 在 [安全中心] 瀏覽窗格中，選擇 [發現項目]
- 在 [資訊 Security Hub] 瀏覽窗格中，選擇 [見解] 選擇一個洞察力。然後在結果清單上，選擇深入解析結果。
- 在 [安全性中心] 功能窗格中，選擇 [整合]。選擇「查看整合的發現項目」。

3. 選擇「新增篩選器」方塊。
4. 在功能表中的「篩選器」下，選擇一個篩選器。

   請注意，當您依 [公司名稱] 或 [產品名稱] 篩選時，Security Hub 會使用頂層`CompanyName`和`ProductName`欄位。API 會使用中的值`ProductFields`。
5. 選擇篩選條件比對類型。

   對於字串篩選器，您可以從下列比較選項中選擇：

   - is — 尋找與篩選器值完全相符的值。
   - 開頭為 — 尋找以篩選值開頭的值。
   - is not — 尋找與篩選值不相符的值。
   - 不開頭為 — 尋找不以篩選值開頭的值。

   對於數字篩選，您可以選擇是提供單一數字 (簡單) 還是數字範圍 (範圍)。

   對於日期或時間篩選器，您可以選擇是從目前的日期和時間 (滾動視窗) 或特定日期範圍 (固定範圍) 提供時間長度。

   新增多個篩選器具有下列互動：

   - is 並以篩選器開頭由 OR 連接。如果值包含任何篩選值，則相符。例如，如果您指定「嚴重性」標籤為「嚴重」，而「嚴重性」標籤為「高」，則結果會同時包含嚴重性和高嚴重性發現項
   - 不是也不是以篩選器開頭，由 AND 加入。只有當值不包含任何這些篩選值時，才符合該值。例如，如果您指定「嚴重性」標籤不是「低」且「嚴重性」標籤不是「中」，則結果不會包含低或中嚴重性發現項目。

   如果您在欄位上有篩選器，則不能在同一欄位上使用 is not 或不以篩選器開頭。
6. 指定篩選條件值。

   請注意，對於字串篩選器，篩選值是區分大小寫的。

例如，對於來自 Security Hub 的發現項目，產品名稱為「Security Hub」。如果您使用 EQUALS 運算子查看來自 Security Hub 的發現項目，您必須輸入**`Security Hub`**作為篩選器值。如果您輸入 **`security hub`**，則不會顯示任何問題清單。

同樣地，如果您使用 PREFIX 運算子，並輸入**`Sec`**，則會顯示 Security Hub 發現項目。如果您輸入**`sec`**，則不會顯示「Security Hub」發現項目。

7. 選擇套用。

分組問題清單

除了變更篩選器之外，您還可以根據所選屬性的值來分組發現項目。

當您將發現項目分組時，發現項目清單會取代為相符發現項目中所選屬性的值清單。對於每個值，清單會顯示符合其他篩選準則的發現項目數目。

例如，如果您依 AWS 帳戶 ID 將發現項目分組，您會看到帳戶識別碼清單，以及每個帳戶的相符發現項目數目。

請注意，Security Hub 只能顯示 100 個值。如果群組值超過 100，您只會看到前 100 個。

當您選擇屬性值時，會顯示該值的相符發現項目清單。

在問題清單中分組問題清單

1. 在尋找項目清單中，選擇 [新增篩選器] 方塊。
2. 在選單中，選擇位於 Grouping (分組) 下方的 Group by (分組依據)。
3. 在清單中，選擇要用於分組的屬性。
4. 選擇套用。

變更篩選器值或群組屬性

針對現有篩選條件，您可以變更篩選條件值。您也可以變更群組屬性。

例如，您可以變更 Record state (記錄狀態) 篩選條件，尋找 `ARCHIVED` 問題清單，而非 `ACTIVE` 問題清單。

編輯篩選條件或群組屬性的步驟

1. 在篩選的發現項目清單上，選擇篩選或群組屬性。

2. 在「分組依據」中，選擇新屬性，然後選擇「套用」。
3. 對於篩選器，請選擇新值，然後選擇「套用」。

刪除篩選器或群組屬性

若要刪除篩選或群組屬性，請選擇 x 圖示。

清單會自動更新以反映變更。當您移除分組屬性時，清單會從欄位值清單變回發現項目清單。

檢視發現項目詳細資料

從 Security Hub 主控台上的尋找項目清單中，您可以顯示尋找項目的詳細資料面板。詳細資料面板包含過去 90 天內發現項目的歷史記錄。您還可以以編程方式查找詳細信息並查找歷史記錄。

檢視尋找項目詳細資料 (主控

請依照下列步驟檢視 Security Hub 主控台上的尋找詳細資料。

檢視發現項目詳細資料面板 (主控台)

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 若要顯示發現項目清單，請執行下列任一項作業：
   - 在 [安全中心] 瀏覽窗格中，選擇 [發現項目]
   - 在 [資訊 Security Hub] 瀏覽窗格中，選擇 [見解] 選擇一個洞察力。然後在結果清單上，選擇深入解析結果。
   - 在 [安全性中心] 功能窗格中，選擇 [整合]。選擇「查看整合的發現項目」。
3. 選取尋找結果標題。

發現項目詳細資料面板頂端包含發現項目的概觀資訊，包括帳戶、嚴重性、日期和狀態。如果您與整合， AWS Organizations 且登入的帳戶是組織成員帳戶，則詳細資料面板會包含該帳戶名稱。對於手動邀請而非透過 Organizations 整合邀請的成員帳戶，詳細資料面板僅包含帳號 ID。發現項目詳細資訊面板也包含下列資訊：

- Detective 調查包含一個鏈接，可以進一步調查 Detective 中的發現。這僅適用於從其他收到的 Security Hub 發現項目 AWS 服務。
- 弱點詳細資訊包含有關弱點來源和受影響套件的資訊。這是針對單一弱點的可擴充區段，以及針對多個弱點進行分頁的區段。本節僅適用於 Amazon Inspector 傳送至 Security Hub 的發現項目。

- 類型和相關發現項目包含有關發現項目類型的資訊。
- 參數會顯示安全性控制項目前的參數值。Security Hub 會在對控制項進行安全性檢查時使用這些參數值。
- 資源包含發現項目所涉及之資源的相關資訊。本節還包括與發現項目相關的應用程式的名稱和 Amazon 資源名稱 (ARN)。如果您已建立應用程式，並將應用程式標籤新增至尋找項目所涉及的資源，則此發現項目只會包含應用程式中繼 我們建議您在中建立應用程式並新增標籤AWS Service Catalog AppRegistry。
- 修正會顯示控制項發現項目。它提供指示的連結，以修正觸發發現項目的問題。
- 尋找提供者欄位會顯示尋找項目提供者的可信度、重要性、相關發現項目、嚴重性和尋找項目類型的值。

在發現項目詳細資料面板中，您可以檢視更多詳細資料，並將欄位值新增至篩選條件。

- 若要顯示發現項目的完整 JSON，請選擇尋找項目 ID。從 Finding JSON (問題清單 JSON) 中，您可以將問題清單 JSON 下載到檔案。
- 若要將欄位值新增至發現項目清單篩選器，請選擇欄位旁邊的搜尋圖示。
- 對於以 AWS Config 規則為基礎的發現項目，若要顯示適用規則的清單，請選擇「規則」。
- 選擇「操作記錄」面板，檢視最多 90 天的尋找歷史記錄。

擷取尋找項目詳細資訊 (程式化)

選擇您偏好的方法，並依照下列步驟，以程式設計方式取得 Security Hub 發現項目清單。您可以指定篩選器，將發現項目清單縮小為特定子集。

下列索引標籤包含擷取發現項目的幾種語言指示。如需其他語言的支援，請參閱建置所在的工具 AWS。

> **Note**
>
> 當您篩選`CompanyName`或時`ProductName`，Security Hub 會使用中的值`ProductFields`。它不使用頂層`CompanyName`和`ProductName`欄位。

Security Hub API

1. 執行 `GetFindings`。

2. 選擇性地植入Filters參數，以縮小您要擷取的發現項目範圍。
3. 您可以選擇性地植入MaxResults參數，將發現項目限制為指定的數目，以及將發現項目分頁的NextToken參數。
4. 選擇性地植入SortCriteria參數，以依特定欄位排序發現項目。

如果您已啟用跨區域彙總，並從彙總區域呼叫此 API，則結果會包含彙總和連結區域的發現項目。

AWS CLI

1. 在命令列中，執行get-findings命令。
2. 選擇性地植入filters參數，以縮小您要擷取的發現項目範圍。
3. 您可以選擇性地植入max-items參數，將發現項目限制為指定的數目，以及將發現項目分頁的page-size參數。
4. 選擇性地植入sort-criteria參數，以依特定欄位排序發現項目。

```
get-findings --filters <filter criteria JSON> --sort-criteria <sort criteria> --
page-size <findings per page> --max-items <maximum number of results>
```

範例

```
aws securityhub get-findings --filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

如果您已啟用跨區域彙總，並從彙總區域呼叫此 API，則結果會包含彙總和連結區域的發現項目。

PowerShell

1. 使用指Get-SHUBFinding令程式。
2. 選擇性地植入Filter參數，以縮小您要擷取的發現項目範圍。

範例

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
```

```
"XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
"EQUALS"; Value = 'FAILED'}}
```

尋找歷史

尋找歷程記錄是一項 Security Hub 功能，可讓您追蹤過去 90 天內對發現項目所做的變更。它可用於作用中和已封存的發現項目。「尋找項目歷程記錄」提供一段時間內對發現項目所做的變更不可變的追蹤，包括變更的內容、發生時間以及由哪位使用者所做的變更。

特別是，您可以追蹤對中欄位所做的變更AWS 安全性搜尋結果格式 (ASFF)。Security Hub 會追蹤您手動和使用自動化規則進行的變更。

查找歷史記錄可在 Security Hub 主控台、API 和 AWS CLI.

如果您已登入 Security Hub 系統管理員帳戶，您可以尋找系統管理員帳戶和所有成員帳戶的歷程記錄。

選擇您喜歡的方法，然後按照以下步驟獲取查找歷史記錄。

Security Hub console

檢視尋找項目記錄 (主控台)

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在左側導覽窗格中，選擇「發現項目」。
3. 選取發現項目。在顯示的面板中，選擇「操作記錄」標籤。

Security Hub API

1. 視需要使用適當的篩選器來執行 `GetFindings`，以識別您要檢視其歷史記錄的發現項目。API 回應會為您提供`ProductArn`和用`Id`於發現項目。在第三個步驟中，您需要這些欄位的值。
2. 執行 `GetFindingHistory`。
3. 使用`ProductArn`和`Id`欄位識別您要取得歷史記錄的發現項目。如需這些欄位的詳細資訊，請參閱AwsSecurityFindingIdentifier。每個請求只能取得一個搜尋結果的歷史記錄。
4. 提供`StartTime`與的值，`EndTime`將尋找歷史記錄限制在特定期間內。
5. 提供一個值，`MaxResults`以將尋找歷史記錄限制為特定數目的結果。如果未提供，API 回應會傳回尋找歷史記錄的前 100 個結果。

6. 提供一個值，NextToken以檢視發現項目的下 100 個結果 (如果適用)。在您的初始 API 請求中，的值NextToken應該是NULL。

API 請求示例：

```
{
"FindingIdentifier": {
  "ProductArn": "arn:aws:securityhub:us-west-2:123456789012:product/123456789012/
default",
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"MaxResults": 2,
"StartTime": "2021-09-30T15:53:35.573Z",
"EndTime": "2021-09-31T15:53:35.573Z"
}
```

AWS CLI

1. 視需要使用適當的篩選器執行get-findings命令，以識別您要檢視其歷史記錄的發現項目。回應會給你ProductArn和Id發現。在第三個步驟中，您需要這些欄位的值。
2. 執行 get-finding-history 命令。
3. 使用ProductArn和Id欄位識別您要取得歷史記錄的發現項目。如需這些欄位的詳細資訊，請參閱AwsSecurityFindingIdentifier。每個請求只能取得一個搜尋結果的歷史記錄。
4. 提供start-time與的值，end-time將尋找歷史記錄限制在特定期間內。
5. 提供一個值，max-results以將尋找歷史記錄限制為特定數目的結果。如果未提供，則該命令返回查找歷史記錄的前 100 個結果。
6. 提供一個值，next-token以檢視發現項目的下 100 個結果 (如果適用)。在您的初始請求中，的值next-token應為NULL。

   範例命令：

```
aws securityhub --region us-west-2 \
get-finding-history
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 --start-time "2021-09-30T15:53:35.573Z" --end-time
 "2021-09-31T15:53:35.573Z"
```

針對中的發現採取行動 AWS Security Hub

AWS Security Hub 可讓您追蹤發現項目的調查目前狀態。

您也可以將發現項目傳送至自訂動作以進行處理。

主題

- 設定發現項目的工作流程狀態
- 將問題清單傳送至自訂動作

設定發現項目的工作流程狀態

工作流程狀態會追蹤調查發現項目的進度。工作流程狀態是個別查找項目的特定狀態。它不會影響新發現的產生。例如，將「搜尋結果」的工作流程狀態設定為SUPPRESSED或RESOLVED不會阻 AWS Security Hub 止針對相同問題產生新的發現項目。

工作流程狀態包含下列值：

NEW

檢閱發現項目之前的初始狀態。

從整合式擷取的發現項目 AWS 服務，例如 AWS Config，具有NEW其初始狀態。

NEW在下列情況下，Security Hub 也會將工作流程狀態從NOTIFIED或RESOLVED重設為：

- RecordState從變更ARCHIVED為ACTIVE。
- Compliance.Status從變更PASSED為FAILEDWARNING、或NOT_AVAILABLE。

這些更改意味著需要進行額外的調查。

NOTIFIED

指出您已向資源擁有者告知嚴重性問題。當您不是資源擁有者，且需要資源擁有者介入以解決安全問題時，可以使用此狀態。

如果發生下列任一情況，那么工作流程狀態會自動從變更NOTIFIED為NEW：

- RecordState從變更ARCHIVED為ACTIVE。
- Compliance.Status從變更PASSED為FAILEDWARNING、或NOT_AVAILABLE。

SUPPRESSED

表示您已檢閱發現項目，但不相信需要採取任何動作。

如果從變更為，則SUPPRESSED搜尋結果的工作流程狀態不會RecordState變ARCHIVED更ACTIVE。

RESOLVED

問題清單已檢閱並進行修補，目前視為已解決。

RESOLVED除非發生下列其中一種情況，否則發現項目仍會

- RecordState從變更ARCHIVED為ACTIVE。
- Compliance.Status從變更PASSED為FAILEDWARNING、或NOT_AVAILABLE。

在這些情況下，工作流程狀態會自動重設為NEW。

對於來自控制項的發現項目，如果Compliance.Status是PASSED，則 Security Hub 會自動將工作流程狀態設定為RESOLVED。

設定發現項目的工作流程狀態

選擇您偏好的方法，並依照步驟設定一或多個發現項目的工作流程狀態。

若要自動更新特定發現項目的工作流程狀態，請參閱自動化規則。

Security Hub console

若要設定發現項目的工作流程狀態

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 若要顯示發現項目清單，請執行下列任一項作業：
   - 在 [安全中心] 瀏覽窗格中，選擇 [發現項目]
   - 在 [資訊 Security Hub] 瀏覽窗格中，選擇 [見解] 選擇一個洞察力。然後在結果清單上，選擇深入解析結果。
   - 在 [安全性中心] 功能窗格中，選擇 [整合]。選擇「查看整合的發現項目」。
   - 在 [安全中心] 瀏覽窗格中，選擇 [安全性標準]。選擇檢視結果以顯示控制項清單。然後，選取控制項以查看該控制項的發現項目清單。
3. 在尋找項目清單中，選取您要更新之每個發現項目的核取方塊。

4. 在列表的頂端，選擇狀態對于「工作流程」狀態。

Security Hub API

調用該 BatchUpdateFindingsAPI。提供產生發現項目之產品的尋找項目識別碼和 ARN。您可以通過調用 GetFindingsAPI 獲取這些詳細信息。

AWS CLI

執行 batch-update-findings 命令。提供產生發現項目之產品的尋找項目識別碼和 ARN。您可以透過執行get-findings命令取得這些詳細資訊。

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

範例

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

將問題清單傳送至自訂動作

您可以建立 AWS Security Hub 自訂動作，透過 Amazon 將 Security Hub 自動化 EventBridge。針對自訂動作，事件類型為 Security Hub Findings - Custom Action。

如需建立自訂動作的詳細資訊和詳細步驟，請參閱 the section called “自動化回應與補救”。

設定自訂動作之後，您可以將問題清單傳送至該動作。

將發現項目傳送至自訂動作 (主控台)

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 若要顯示發現項目清單，請執行下列任一項作業：
   - 在 [安全中心] 瀏覽窗格中，選擇 [發現項目]
   - 在 [資訊 Security Hub] 瀏覽窗格中，選擇 [見解] 選擇一個洞察力。然後在結果清單上，選擇深入解析結果。

- 在 [安全性中心] 功能窗格中，選擇 [整合]。選擇「查看整合的發現項目」。
- 在 [安全中心] 瀏覽窗格中，選擇 [安全性標準]。選擇檢視結果以顯示控制項清單。然後選擇控制項名稱。

3. 在尋找項目清單中，選取要傳送至自訂動作之每個發現項目的核取方塊。

   您一次最多可以傳送 20 個問題清單。

4. 在「動作」中，選擇自訂動作。

AWS 安全性搜尋結果格式 (ASFF)

AWS Security Hub 會從安全性服務和第三方產品整合中取用、彙總、組織和優先順序處 AWS 理發現項目。Security Hub 會使用稱為「 AWS 安全性尋找結果格式」(ASFF) 的標準發現項目格式來處理這些發現項目，這樣就不需要耗時的資料轉換工作。然後，相互關聯所有產品的問題清單，排定最重要幾個的優先順序。

主題

- AWS 安全性發現格式 (ASFF) 語法
- 合併對 ASFF 欄位與值的影響
- 售後範例

AWS 安全性發現格式 (ASFF) 語法

此頁面提供「 AWS 安全性發現項目格式」(ASFF) 中發現項目的完整 JSON 大綱。格式衍生自 JSON 結構描述。選擇連結的物件名稱，以檢視該物件的範例發現項目。您可以將 Security Hub 發現項目與此處顯示的資源和範例進行比較，以協助您解譯發現項目。

若要檢視必要 ASFF 屬性的摘要，請參閱the section called “必要的頂層屬性”。

若要檢視其他最上層 ASFF 屬性的描述，請參閱the section called “選用的頂層屬性”。

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
```

```
        "Api": "string",
        "CallerType": "string",
        "DomainDetails": {
         "Domain": "string"
        },
        "FirstSeen": "string",
        "LastSeen": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
         "City": {
```

```
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "RemotePortDetails": {
         "Port": number,
         "PortName": "string"
        }
       },
       "PortProbeAction": {
        "Blocked": boolean,
        "PortProbeDetails": [{
         "LocalIpDetails": {
          "IpAddressV4": "string"
         },
         "LocalPortDetails": {
          "Port": number,
          "PortName": "string"
         },
         "RemoteIpDetails": {
          "City": {
           "CityName": "string"
          },
          "Country": {
           "CountryCode": "string",
           "CountryName": "string"
          },
          "GeoLocation": {
           "Lat": number,
           "Lon": number
```

```
        },
        "IpAddressV4": "string",
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       }
      }]
     }
    },
    "AwsAccountId": "string",
    "AwsAccountName": "string",
    "CompanyName": "string",
    "Compliance": {
     "AssociatedStandards": [{
      "StandardsId": "string"
     }],
     "RelatedRequirements": ["string"],
     "SecurityControlId": "string",
     "SecurityControlParameters": [
      {
       "Name": "string",
       "Value": ["string"]
      }
    ],
     "Status": "string",
     "StatusReasons": [
      {
       "Description": "string",
       "ReasonCode": "string"
      }
     ]
    },
    "Confidence": number,
    "CreatedAt": "string",
    "Criticality": number,
    "Description": "string",
    "FindingProviderFields": {
     "Confidence": number,
     "Criticality": number,
     "RelatedFindings": [{
      "ProductArn": "string",
```

```
      "Id": "string"
     }],
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Types": ["string"]
    },
    "FirstObservedAt": "string",
    "GeneratorId": "string",
    "Id": "string",
    "LastObservedAt": "string",
    "Malware": [{
     "Name": "string",
     "Path": "string",
     "State": "string",
     "Type": "string"
    }],
    "Network": {
     "DestinationDomain": "string",
     "DestinationIpV4": "string",
     "DestinationIpV6": "string",
     "DestinationPort": number,
     "Direction": "string",
     "OpenPortRange": {
      "Begin": integer,
      "End": integer
     },
     "Protocol": "string",
     "SourceDomain": "string",
     "SourceIpV4": "string",
     "SourceIpV6": "string",
     "SourceMac": "string",
     "SourcePort": number
    },
    "NetworkPath": [{
     "ComponentId": "string",
     "ComponentType": "string",
     "Egress": {
      "Destination": {
       "Address": ["string"],
       "PortRanges": [{
        "Begin": integer,
```

```
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       },
       "Ingress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       }
      }],
      "Note": {
       "Text": "string",
       "UpdatedAt": "string",
       "UpdatedBy": "string"
      },
      "PatchSummary": {
       "FailedCount": number,
       "Id": "string",
       "InstalledCount": number,
       "InstalledOtherCount": number,
       "InstalledPendingReboot": number,
       "InstalledRejectedCount": number,
       "MissingCount": number,
       "Operation": "string",
```

```
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
     "Region": "string",
     "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
     }],
     "Remediation": {
      "Recommendation": {
       "Text": "string",
       "Url": "string"
      }
     },
     "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
       "DetailedResultsLocation": "string",
       "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
         "Detections": [{
          "Arn": "string",
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
```

```
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
```

```
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
```

```
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
         "TimeOfDay": "string",
         "TimeZone": "string"
        },
        "PubliclyAccessible": boolean,
        "SecurityGroups": [
         "string"
        ],
        "StorageType": "string",
        "SubnetIds": [
         "string",
         "string"
        ],
        "Users": [{
         "Username": "string"
        }]
       },
       "AwsApiGatewayRestApi": {
        "ApiKeySource": "string",
        "BinaryMediaTypes": [" string"],
        "CreatedDate": "string",
        "Description": "string",
```

```
        "EndpointConfiguration": {
         "Types": ["string"]
        },
        "Id": "string",
        "MinimumCompressionSize": number,
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "CacheClusterEnabled": boolean,
        "CacheClusterSize": "string",
        "CacheClusterStatus": "string",
        "CanarySettings": {
         "DeploymentId": "string",
         "PercentTraffic": number,
         "StageVariableOverrides": [{
          "string": "string"
         }],
         "UseStageCache": boolean
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
```

```
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
          "string": "string"
        },
        "WebAclArn": "string"
      },
      "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
          "AllowCredentials": boolean,
          "AllowHeaders": ["string"],
          "AllowMethods": ["string"],
          "AllowOrigins": ["string"],
          "ExposeHeaders": ["string"],
          "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
      },
      "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
          "DataTraceEnabled": boolean,
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
```

```
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
         },
         {
          "AuthenticationType": "string"
         }
         ],
         "ApiId": "string",
         "Arn": "string",
         "AuthenticationType": "string",
         "Id": "string",
         "LogConfig": {
          "CloudWatchLogsRoleArn": "string",
          "ExcludeVerboseContent": boolean,
          "FieldLogLevel": "string"
         },
         "Name": "string",
         "XrayEnabled": boolean
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
        "Name": "string",
```

```
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
```

```
        }
       }
      },
      "AwsAutoScalingLaunchConfiguration": {
       "AssociatePublicIpAddress": boolean,
       "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
         "DeleteOnTermination": boolean,
         "Encrypted": boolean,
         "Iops": number,
         "SnapshotId": "string",
         "VolumeSize": number,
         "VolumeType": "string"
        },
        "NoDevice": boolean,
        "VirtualName": "string"
       }],
       "ClassicLinkVpcId": "string",
       "ClassicLinkVpcSecurityGroups": ["string"],
       "CreatedTime": "string",
       "EbsOptimized": boolean,
       "IamInstanceProfile": "string"
      },
      "ImageId": "string",
      "InstanceMonitoring": {
       "Enabled": boolean
      },
      "InstanceType": "string",
      "KernelId": "string",
      "KeyName": "string",
      "LaunchConfigurationName": "string",
      "MetadataOptions": {
       "HttpEndPoint": "string",
       "HttpPutReponseHopLimit": number,
       "HttpTokens": "string"
      },
      "PlacementTenancy": "string",
      "RamdiskId": "string",
      "SecurityGroups": ["string"],
      "SpotPrice": "string",
      "UserData": "string"
     },
     "AwsBackupBackupPlan": {
```

```
      "BackupPlan": {
       "AdvancedBackupSettings": [{
        "BackupOptions": {
         "WindowsVSS":"string"
        },
        "ResourceType":"string"
       }],
       "BackupPlanName": "string",
       "BackupPlanRule": [{
        "CompletionWindowMinutes": integer,
        "CopyActions": [{
         "DestinationBackupVaultArn": "string",
         "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
         }
        }],
        "Lifecycle": {
         "DeleteAfterDays": integer
        },
        "RuleName": "string",
        "ScheduleExpression": "string",
        "StartWindowMinutes": integer,
        "TargetBackupVault": "string"
       }]
      },
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "VersionId": "string"
    },
     "AwsBackupBackupVault": {
      "AccessPolicy": {
       "Statement": [{
        "Action": ["string"],
        "Effect": "string",
        "Principal": {
         "AWS": "string"
        },
        "Resource": "string"
       }],
       "Version": "string"
      },
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
```

```
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
```

```
        "ResourceRecord": {
         "Name": "string",
         "Type": "string",
         "Value": "string"
        },
        "ValidationDomain": "string",
        "ValidationEmails": ["string"],
        "ValidationMethod": "string",
        "ValidationStatus": "string"
       }],
       "ExtendedKeyUsages": [{
        "Name": "string",
        "OId": "string"
       }],
       "FailureReason": "string",
       "ImportedAt": "string",
       "InUseBy": ["string"],
       "IssuedAt": "string",
       "Issuer": "string",
       "KeyAlgorithm": "string",
       "KeyUsages": [{
        "Name": "string"
       }],
       "NotAfter": "string",
       "NotBefore": "string",
       "Options": {
        "CertificateTransparencyLoggingPreference": "string"
       },
       "RenewalEligibility": "string",
       "RenewalSummary": {
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "RenewalStatus": "string",
        "RenewalStatusReason": "string",
```

```
        "UpdatedAt": "string"
       },
       "Serial": "string",
       "SignatureAlgorithm": "string",
       "Status": "string",
       "Subject": "string",
       "SubjectAlternativeNames": ["string"],
       "Type": "string"
      },
      "AwsCloudFormationStack": {
       "Capabilities": ["string"],
       "CreationTime": "string",
       "Description": "string",
       "DisableRollback": boolean,
       "DriftInformation": {
        "StackDriftStatus": "string"
       },
       "EnableTerminationProtection": boolean,
       "LastUpdatedTime": "string",
       "NotificationArns": ["string"],
       "Outputs": [{
        "Description": "string",
        "OutputKey": "string",
        "OutputValue": "string"
       }],
       "RoleArn": "string",
       "StackId": "string",
       "StackName": "string",
       "StackStatus": "string",
       "StackStatusReason": "string",
       "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
       "CacheBehaviors": {
        "Items": [{
         "ViewerProtocolPolicy": "string"
        }]
       },
       "DefaultCacheBehavior": {
        "ViewerProtocolPolicy": "string"
       },
       "DefaultRootObject": "string",
       "DomainName": "string",
       "Etag": "string",
```

```
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
          }
         }]
        },
        "Status": "string",
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
         "CloudFrontDefaultCertificate": boolean,
```

```
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "SnsTopicArn": "string",
       "SnsTopicName": "string",
       "TrailArn": "string"
      },
      "AwsCloudWatchAlarm": {
       "ActionsEnabled": boolean,
       "AlarmActions": ["string"],
       "AlarmArn": "string",
       "AlarmConfigurationUpdatedTimestamp": "string",
       "AlarmDescription": "string",
       "AlarmName": "string",
       "ComparisonOperator": "string",
       "DatapointsToAlarm": number,
       "Dimensions": [{
        "Name": "string",
        "Value": "string"
       }],
       "EvaluateLowSampleCountPercentile": "string",
       "EvaluationPeriods": number,
       "ExtendedStatistic": "string",
       "InsufficientDataActions": ["string"],
       "MetricName": "string",
       "Namespace": "string",
       "OkActions": ["string"],
       "Period": number,
```

```
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
       },
       "AwsCodeBuildProject": {
        "Artifacts": [{
         "ArtifactIdentifier": "string",
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Name": "string",
         "NamespaceType": "string",
         "OverrideArtifactName": boolean,
         "Packaging": "string",
         "Path": "string",
         "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
```

```
        "Type": "string"
       },
       "LogsConfig": {
        "CloudWatchLogs": {
         "GroupName": "string",
         "Status": "string",
         "StreamName": "string"
        },
        "S3Logs": {
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Status": "string"
        }
       },
       "Name": "string",
       "ServiceRole": "string",
       "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
       },
       "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
       }
      },
      "AwsDmsEndpoint": {
       "CertificateArn": "string",
       "DatabaseName": "string",
       "EndpointArn": "string",
       "EndpointIdentifier": "string",
       "EndpointType": "string",
       "EngineName": "string",
       "KmsKeyId": "string",
       "Port": integer,
       "ServerName": "string",
       "SslMode": "string",
       "Username": "string"
      },
      "AwsDmsReplicationInstance": {
       "AllocatedStorage": integer,
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZone": "string",
```

```
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
        }],
        "BillingModeSummary": {
          "BillingMode": "string",
          "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
          "Backfilling": boolean,
```

```
        "IndexArn": "string",
        "IndexName": "string",
        "IndexSizeBytes": number,
        "IndexStatus": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        },
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        }
       }],
       "GlobalTableVersion": "string",
       "ItemCount": number,
       "KeySchema": [{
        "AttributeName": "string",
        "KeyType": "string"
       }],
       "LatestStreamArn": "string",
       "LatestStreamLabel": "string",
       "LocalSecondaryIndexes": [{
        "IndexArn": "string",
        "IndexName": "string",
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        }
       }],
       "ProvisionedThroughput": {
        "LastDecreaseDateTime": "string",
        "LastIncreaseDateTime": "string",
```

```
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
       },
       "Replicas": [{
        "GlobalSecondaryIndexes": [{
         "IndexName": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         }
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
```

```
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
       "SessionTimeoutHours": "integer",
       "SplitTunnel": boolean,
       "TransportProtocol": "string",
       "VpcId": "string",
       "VpnPort": integer
      },
      "AwsEc2Eip": {
       "AllocationId": "string",
       "AssociationId": "string",
       "Domain": "string",
       "InstanceId": "string",
       "NetworkBorderGroup": "string",
       "NetworkInterfaceId": "string",
       "NetworkInterfaceOwnerId": "string",
       "PrivateIpAddress": "string",
       "PublicIp": "string",
       "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
       "IamInstanceProfileArn": "string",
       "ImageId": "string",
```

```
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
         "HttpEndpoint": "string",
         "HttpProtocolIpv6": "string",
         "HttpPutResponseHopLimit": number,
         "HttpTokens": "string",
         "InstanceMetadataTags": "string"
        },
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
```

```
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
       "IsDefault": boolean,
       "NetworkAclId": "string",
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2NetworkInterface": {
       "Attachment": {
        "AttachmentId": "string",
        "AttachTime": "string",
```

```
        "DeleteOnTermination": boolean,
        "DeviceIndex": number,
        "InstanceId": "string",
        "InstanceOwnerId": "string",
        "Status": "string"
       },
       "Ipv6Addresses": [{
        "Ipv6Address": "string"
       }],
       "NetworkInterfaceId": "string",
       "PrivateIpAddresses": [{
        "PrivateDnsName": "string",
        "PrivateIpAddress": "string"
       }],
       "PublicDnsName": "string",
       "PublicIp": "string",
       "SecurityGroups": [{
        "GroupId": "string",
        "GroupName": "string"
       }],
       "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
       "AssociationSet": [{
        "AssociationState": {
         "State": "string"
        },
        "Main": boolean,
        "RouteTableAssociationId": "string",
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
```

```
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
```

```
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
       },
       "AwsEc2TransitGateway": {
        "AmazonSideAsn": number,
        "AssociationDefaultRouteTableId": "string",
        "AutoAcceptSharedAttachments": "string",
        "DefaultRouteTableAssociation": "string",
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
       },
```

```
      "AwsEc2Volume": {
       "Attachments": [{
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "InstanceId": "string",
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
       "KmsKeyId": "string",
       "Size": number,
       "SnapshotId": "string",
       "Status": "string",
       "VolumeId": "string",
       "VolumeScanStatus": "string",
       "VolumeType": "string"
      },
      "AwsEc2Vpc": {
       "CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "DhcpOptionsId": "string",
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlockState": "string",
        "Ipv6CidrBlock": "string"
       }],
       "State": "string"
      },
      "AwsEc2VpcEndpointService": {
       "AcceptanceRequired": boolean,
       "AvailabilityZones": ["string"],
       "BaseEndpointDnsNames": ["string"],
       "ManagesVpcEndpoints": boolean,
       "GatewayLoadBalancerArns": ["string"],
       "NetworkLoadBalancerArns": ["string"],
       "PrivateDnsName": "string",
       "ServiceId": "string",
       "ServiceName": "string",
       "ServiceState": "string",
       "ServiceType": [{
```

```
        "ServiceType": "string"
       }]
      },
      "AwsEc2VpcPeeringConnection": {
       "AccepterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "ExpirationTime": "string",
       "RequesterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
```

```
      },
      "AwsEc2VpnConnection": {
       "Category": "string",
       "CustomerGatewayConfiguration": "string",
       "CustomerGatewayId": "string",
       "Options": {
        "StaticRoutesOnly": boolean,
        "TunnelOptions": [{
         "DpdTimeoutSeconds": number,
         "IkeVersions": ["string"],
         "OutsideIpAddress": "string",
         "Phase1DhGroupNumbers": [number],
         "Phase1EncryptionAlgorithms": ["string"],
         "Phase1IntegrityAlgorithms": ["string"],
         "Phase1LifetimeSeconds": number,
         "Phase2DhGroupNumbers": [number],
         "Phase2EncryptionAlgorithms": ["string"],
         "Phase2IntegrityAlgorithms": ["string"],
         "Phase2LifetimeSeconds": number,
         "PreSharedKey": "string",
         "RekeyFuzzPercentage": number,
         "RekeyMarginTimeSeconds": number,
         "ReplayWindowSize": number,
         "TunnelInsideCidr": "string"
        }]
       },
       "Routes": [{
        "DestinationCidrBlock": "string",
        "State": "string"
       }],
       "State": "string",
       "TransitGatewayId": "string",
       "Type": "string",
       "VgwTelemetry": [{
        "AcceptedRouteCount": number,
        "CertificateArn": "string",
        "LastStatusChange": "string",
        "OutsideIpAddress": "string",
        "Status": "string",
        "StatusMessage": "string"
       }],
       "VpnConnectionId": "string",
       "VpnGatewayId": "string"
      },
```

```
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
       },
       "RepositoryName": "string",
       "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
       "ActiveServicesCount": number,
       "CapacityProviders": ["string"],
       "ClusterArn": "string",
       "ClusterName": "string",
       "ClusterSettings": [{
        "Name": "string",
        "Value": "string"
       }],
       "Configuration": {
        "ExecuteCommandConfiguration": {
         "KmsKeyId": "string",
         "LogConfiguration": {
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
         },
         "Logging": "string"
        }
       },
       "DefaultCapacityProviderStrategy": [{
```

```
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "RegisteredContainerInstancesCount": number,
       "RunningTasksCount": number,
       "Status": "string"
      },
      "AwsEcsContainer": {
       "Image": "string",
       "MountPoints": [{
        "ContainerPath": "string",
        "SourceVolume": "string"
       }],
       "Name": "string",
       "Privileged": boolean
      },
      "AwsEcsService": {
       "CapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "Cluster": "string",
       "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
         "Enable": boolean,
         "Rollback": boolean
        },
        "MaximumPercent": number,
        "MinimumHealthyPercent": number
       },
       "DeploymentController": {
        "Type": "string"
       },
       "DesiredCount": number,
       "EnableEcsManagedTags": boolean,
       "EnableExecuteCommand": boolean,
       "HealthCheckGracePeriodSeconds": number,
       "LaunchType": "string",
       "LoadBalancers": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "LoadBalancerName": "string",
```

```
        "TargetGroupArn": "string"
       }],
       "Name": "string",
       "NetworkConfiguration": {
        "AwsVpcConfiguration": {
         "AssignPublicIp": "string",
         "SecurityGroups": ["string"],
         "Subnets": ["string"]
        }
       },
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "PlacementStrategies": [{
        "Field": "string",
        "Type": "string"
       }],
       "PlatformVersion": "string",
       "PropagateTags": "string",
       "Role": "string",
       "SchedulingStrategy": "string",
       "ServiceArn": "string",
       "ServiceName": "string",
       "ServiceRegistries": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "Port": number,
        "RegistryArn": "string"
       }],
       "TaskDefinition": "string"
      },
      "AwsEcsTask": {
       "CreatedAt": "string",
       "ClusterArn": "string",
       "Group": "string",
       "StartedAt": "string",
       "StartedBy": "string",
       "TaskDefinitionArn": "string",
       "Version": number,
       "Volumes": [{
        "Name": "string",
        "Host": {
         "SourcePath": "string"
```

```
        }
       }],
       "Containers": [{
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       }]
      },
      "AwsEcsTaskDefinition": {
       "ContainerDefinitions": [{
        "Command": ["string"],
        "Cpu": number,
        "DependsOn": [{
         "Condition": "string",
         "ContainerName": "string"
        }],
        "DisableNetworking": boolean,
        "DnsSearchDomains": ["string"],
        "DnsServers": ["string"],
        "DockerLabels": {
         "string": "string"
        },
        "DockerSecurityOptions": ["string"],
        "EntryPoint": ["string"],
        "Environment": [{
         "Name": "string",
         "Value": "string"
        }],
        "EnvironmentFiles": [{
         "Type": "string",
         "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
         "Hostname": "string",
         "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
```

```
          },
          "Type": "string"
        },
        "HealthCheck": {
          "Command": ["string"],
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
          "Capabilities": {
            "Add": ["string"],
            "Drop": ["string"]
          },
          "Devices": [{
            "ContainerPath": "string",
            "HostPath": "string",
            "Permissions": ["string"]
          }],
          "InitProcessEnabled": boolean,
          "MaxSwap": number,
          "SharedMemorySize": number,
          "Swappiness": number,
          "Tmpfs": [{
            "ContainerPath": "string",
            "MountOptions": ["string"],
            "Size": number
          }]
        },
        "LogConfiguration": {
          "LogDriver": "string",
          "Options": {
            "string": "string"
          },
          "SecretOptions": [{
            "Name": "string",
            "ValueFrom": "string"
          }]
        },
```

```
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
         "CredentialsParameter": "string"
        },
        "ResourceRequirements": [{
         "Type": "string",
         "Value": "string"
        }],
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
         "HardLimit": number,
         "Name": "string",
         "SoftLimit": number
        }],
        "User": "string",
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
        "WorkingDirectory": "string"
```

```
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
         "DeviceName": "string",
         "DeviceType": "string"
        }],
        "IpcMode": "string",
        "Memory": "string",
        "NetworkMode": "string",
        "PidMode": "string",
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "ProxyConfiguration": {
         "ContainerName": "string",
         "ProxyConfigurationProperties": [{
          "Name": "string",
          "Value": "string"
         }],
         "Type": "string"
        },
        "RequiresCompatibilities": ["string"],
        "Status": "string",
        "TaskRoleArn": "string",
        "Volumes": [{
         "DockerVolumeConfiguration": {
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
```

```
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
       },
       "AwsEfsAccessPoint": {
        "AccessPointId": "string",
        "Arn": "string",
        "ClientToken": "string",
        "FileSystemId": "string",
        "PosixUser": {
         "Gid": "string",
         "SecondaryGids": ["string"],
         "Uid": "string"
        },
        "RootDirectory": {
         "CreationInfo": {
          "OwnerGid": "string",
          "OwnerUid": "string",
          "Permissions": "string"
         },
         "Path": "string"
        }
       },
       "AwsEksCluster": {
        "Arn": "string",
        "CertificateAuthorityData": "string",
        "ClusterStatus": "string",
        "Endpoint": "string",
        "Logging": {
         "ClusterLogging": [{
          "Enabled": boolean,
          "Types": ["string"]
         }]
        },
        "Name": "string",
        "ResourcesVpcConfig": {
         "EndpointPublicAccess": boolean,
```

```
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
```

```
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "ElasticsearchClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "ElasticsearchVersion": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
       "LogPublishingOptions": {
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
```

```
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VPCOptions": {
        "AvailabilityZones": [
         "string"
        ],
        "SecurityGroupIds": [
         "string"
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
```

```
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                       "Key": "string",
                       "Value": "string"
                   }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
```

```
        "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
          "SubnetId": "string",
          "ZoneName": "string"
        },
        "CanonicalHostedZoneId": "string",
        "CreatedTime": "string",
        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
          "Key": "string",
          "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
          "Code": "string",
          "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
      },
      "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
```

```
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
              "Status": "string"
            }
          },
          "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
```

```
          "EbsVolumes": {
           "Status": "string"
          }
         },
         "ServiceRole": "string"
        }
       }
      },
      "AwsIamAccessKey": {
       "AccessKeyId": "string",
       "AccountId": "string",
       "CreatedAt": "string",
       "PrincipalId": "string",
       "PrincipalName": "string",
       "PrincipalType": "string",
       "SessionContext": {
        "Attributes": {
         "CreationDate": "string",
         "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
         "AccountId": "string",
         "Arn": "string",
         "PrincipalId": "string",
         "Type": "string",
         "UserName": "string"
        }
       },
       "Status": "string"
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupId": "string",
       "GroupName": "string",
       "GroupPolicyList": [{
        "PolicyName": "string"
       }],
       "Path": "string"
      },
      "AwsIamPolicy": {
```

```
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
```

```
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
```

```
      "AwsLambdaFunction": {
       "Architectures": [
        "string"
       ],
       "Code": {
        "S3Bucket": "string",
        "S3Key": "string",
        "S3ObjectVersion": "string",
        "ZipFile": "string"
       },
       "CodeSha256": "string",
       "DeadLetterConfig": {
        "TargetArn": "string"
       },
       "Environment": {
        "Variables": {
         "Stage": "string"
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
       "FunctionName": "string",
       "Handler": "string",
       "KmsKeyArn": "string",
       "LastModified": "string",
       "Layers": {
        "Arn": "string",
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
       "Runtime": "string",
       "Timeout": integer,
       "TracingConfig": {
        "Mode": "string"
       },
       "Version": "string",
       "VpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
```

```
        "MasterArn": "string",
        "MemorySize": number
      },
      "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
          "string"
        ],
        "CreatedDate": "string",
        "Version": number
      },
      "AwsMskCluster": {
        "ClusterInfo": {
          "ClientAuthentication": {
            "Sasl": {
              "Scram": {
                "Enabled": boolean
              },
              "Iam": {
                "Enabled": boolean
              }
            },
            "Tls": {
              "CertificateAuthorityArnList": [],
              "Enabled": boolean
            },
            "Unauthenticated": {
              "Enabled": boolean
            }
          },
          "ClusterName": "string",
          "CurrentVersion": "string",
          "EncryptionInfo": {
            "EncryptionAtRest": {
              "DataVolumeKMSKeyId": "string"
            },
            "EncryptionInTransit": {
              "ClientBroker": "string",
              "InCluster": boolean
            }
          },
          "EnhancedMonitoring": "string",
          "NumberOfBrokerNodes": integer
        }
      },
```

```
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
```

```
        "RuleGroup": {
         "RulesSource": {
          "RulesSourceList": {
           "GeneratedRulesType": "string",
           "Targets": ["string"],
           "TargetTypes": ["string"]
          },
          "RulesString": "string",
          "StatefulRules": [{
           "Action": "string",
           "Header": {
            "Destination": "string",
            "DestinationPort": "string",
            "Direction": "string",
            "Protocol": "string",
            "Source": "string",
            "SourcePort": "string"
           },
           "RuleOptions": [{
            "Keyword": "string",
            "Settings": ["string"]
           }]
          }],
          "StatelessRulesAndCustomActions": {
           "CustomActions": [{
            "ActionDefinition": {
             "PublishMetricAction": {
              "Dimensions": [{
               "Value": "string"
              }]
             }
            },
            "ActionName": "string"
           }],
           "StatelessRules": [{
            "Priority": number,
            "RuleDefinition": {
             "Actions": ["string"],
             "MatchAttributes": {
              "DestinationPorts": [{
               "FromPort": number,
               "ToPort": number
              }],
              "Destinations": [{
```

```
            "AddressDefinition": "string"
           }],
           "Protocols": [number],
           "SourcePorts": [{
            "FromPort": number,
            "ToPort": number
           }],
           "Sources": [{
            "AddressDefinition": "string"
           }],
           "TcpFlags": [{
            "Flags": ["string"],
            "Masks": ["string"]
           }]
          }
         }
        }]
       }
      },
      "RuleVariables": {
       "IpSets": {
        "Definition": ["string"]
       },
       "PortSets": {
        "Definition": ["string"]
       }
      }
     },
     "RuleGroupArn": "string",
     "RuleGroupId": "string",
     "RuleGroupName": "string",
     "Type": "string"
    },
    "AwsOpenSearchServiceDomain": {
     "AccessPolicies": "string",
     "AdvancedSecurityOptions": {
      "Enabled": boolean,
      "InternalUserDatabaseEnabled": boolean,
      "MasterUserOptions": {
       "MasterUserArn": "string",
       "MasterUserName": "string",
       "MasterUserPassword": "string"
      }
     },
```

```
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
```

```
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
```

```
        "DbClusterOptionGroupName": "string",
        "Status": "string"
       }],
       "DbClusterParameterGroup": "string",
       "DbClusterResourceId": "string",
       "DbSubnetGroup": "string",
       "DeletionProtection": boolean,
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Endpoint": "string",
       "Engine": "string",
       "EngineMode": "string",
       "EngineVersion": "string",
       "HostedZoneId": "string",
       "HttpEndpointEnabled": boolean,
       "IamDatabaseAuthenticationEnabled": boolean,
       "KmsKeyId": "string",
       "MasterUsername": "string",
       "MultiAz": boolean,
       "Port": integer,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ReaderEndpoint": "string",
       "ReadReplicaIdentifiers": ["string"],
       "Status": "string",
       "StorageEncrypted": boolean,
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRdsDbClusterSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZones": ["string"],
       "ClusterCreateTime": "string",
       "DbClusterIdentifier": "string",
       "DbClusterSnapshotAttributes": [{
        "AttributeName": "string",
        "AttributeValues": ["string"]
```

```
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
      },
      "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
          "RoleArn": "string",
          "FeatureName": "string",
          "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
          "DbParameterGroupName": "string",
          "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
          "DbSubnetGroupArn": "string",
          "DbSubnetGroupDescription": "string",
```

```
        "DbSubnetGroupName": "string",
        "SubnetGroupStatus": "string",
        "Subnets": [{
         "SubnetAvailabilityZone": {
          "Name": "string"
         },
         "SubnetIdentifier": "string",
         "SubnetStatus": "string"
        }],
        "VpcId": "string"
       },
       "DeletionProtection": boolean,
       "Endpoint": {
        "Address": "string",
        "Port": number,
        "HostedZoneId": "string"
       },
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Engine": "string",
       "EngineVersion": "string",
       "EnhancedMonitoringResourceArn": "string",
       "IAMDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LatestRestorableTime": "string",
       "LicenseModel": "string",
       "ListenerEndpoint": {
        "Address": "string",
        "HostedZoneId": "string",
        "Port": number
       },
       "MasterUsername": "admin",
       "MaxAllocatedStorage": number,
       "MonitoringInterval": number,
       "MonitoringRoleArn": "string",
       "MultiAz": boolean,
       "OptionGroupMemberships": [{
```

```
        "OptionGroupName": "string",
        "Status": "string"
       }],
       "PendingModifiedValues": {
        "AllocatedStorage": number,
        "BackupRetentionPeriod": number,
        "CaCertificateIdentifier": "string",
        "DbInstanceClass": "string",
        "DbInstanceIdentifier": "string",
        "DbSubnetGroupName": "string",
        "EngineVersion": "string",
        "Iops": number,
        "LicenseModel": "string",
        "MasterUserPassword": "string",
        "MultiAZ": boolean,
        "PendingCloudWatchLogsExports": {
         "LogTypesToDisable": ["string"],
         "LogTypesToEnable": ["string"]
        },
        "Port": number,
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "StorageType": "string"
       },
       "PerformanceInsightsEnabled": boolean,
       "PerformanceInsightsKmsKeyId": "string",
       "PerformanceInsightsRetentionPeriod": number,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
       }],
       "PromotionTier": number,
       "PubliclyAccessible": boolean,
       "ReadReplicaDBClusterIdentifiers": ["string"],
       "ReadReplicaDBInstanceIdentifiers": ["string"],
       "ReadReplicaSourceDBInstanceIdentifier": "string",
       "SecondaryAvailabilityZone": "string",
       "StatusInfos": [{
        "Message": "string",
        "Normal": boolean,
```

```
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcSecurityGroups": [{
        "VpcSecurityGroupId": "string",
        "Status": "string"
       }]
      },
      "AwsRdsDbSecurityGroup": {
       "DbSecurityGroupArn": "string",
       "DbSecurityGroupDescription": "string",
       "DbSecurityGroupName": "string",
       "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
```

```
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
```

```
        "ParameterGroupName": "string"
       }],
       "ClusterPublicKey": "string",
       "ClusterRevisionNumber": "string",
       "ClusterSecurityGroups": [{
        "ClusterSecurityGroupName": "string",
        "Status": "string"
       }],
       "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "string",
        "ManualSnapshotRetentionPeriod": number,
        "RetentionPeriod": number,
        "SnapshotCopyGrantName": "string"
       },
       "ClusterStatus": "string",
       "ClusterSubnetGroupName": "string",
       "ClusterVersion": "string",
       "DBName": "string",
       "DeferredMaintenanceWindows": [{
        "DeferMaintenanceEndTime": "string",
        "DeferMaintenanceIdentifier": "string",
        "DeferMaintenanceStartTime": "string"
       }],
       "ElasticIpStatus": {
        "ElasticIp": "string",
        "Status": "string"
       },
       "ElasticResizeNumberOfNodeOptions": "string",
       "Encrypted": boolean,
       "Endpoint": {
        "Address": "string",
        "Port": number
       },
       "EnhancedVpcRouting": boolean,
       "ExpectedNextSnapshotScheduleTime": "string",
       "ExpectedNextSnapshotScheduleTimeStatus": "string",
       "HsmStatus": {
        "HsmClientCertificateIdentifier": "string",
        "HsmConfigurationIdentifier": "string",
        "Status": "string"
       },
       "IamRoles": [{
        "ApplyStatus": "string",
        "IamRoleArn": "string"
```

```
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
```

```
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
         "Id": "string",
         "Name": "string",
         "Config": {
          "Comment": "string"
         }
        },
        "NameServers": ["string"],
        "QueryLoggingConfig": {
         "CloudWatchLogsLogGroupArn": {
          "CloudWatchLogsLogGroupArn": "string",
          "Id": "string",
          "HostedZoneId": "string"
         }
        },
        "Vpcs": [
         {
          "Id": "string",
          "Region": "string"
         }
        ]
       },
       "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
```

```
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
               "Value": "string"
              },
              "Type": "string"
             }
            ],
            "Type": "string"
           }
          },
          "Id": "string",
          "NoncurrentVersionExpirationInDays": number,
          "NoncurrentVersionTransitions": [{
           "Days": number,
           "StorageClass": "string"
          }],
          "Prefix": "string",
```

```
          "Status": "string",
          "Transitions": [{
           "Date": "string",
           "Days": number,
           "StorageClass": "string"
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
         "RoutingRules": [{
          "Condition": {
           "HttpErrorCodeReturnedEquals": "string",
           "KeyPrefixEquals": "string"
          },
```

```
          "Redirect": {
           "HostName": "string",
           "HttpRedirectCode": "string",
           "Protocol": "string",
           "ReplaceKeyPrefixWith": "string",
           "ReplaceKeyWith": "string"
          }
         }]
        },
        "CreatedAt": "string",
        "ObjectLockConfiguration": {
         "ObjectLockEnabled": "string",
         "Rule": {
          "DefaultRetention": {
           "Days": integer,
           "Mode": "string",
           "Years": integer
          }
         }
        },
        "OwnerAccountId": "string",
        "OwnerId": "string",
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
```

```
        "VersionId": "string"
      },
      "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
          "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
```

```
        "Endpoint": "string",
        "Protocol": "string"
       },
       "TopicName": "string"
      },
      "AwsSqsQueue": {
       "DeadLetterTargetArn": "string",
       "KmsDataKeyReusePeriodSeconds": number,
       "KmsMasterKeyId": "string",
       "QueueName": "string"
      },
      "AwsSsmPatchCompliance": {
       "Patch": {
        "ComplianceSummary": {
         "ComplianceType": "string",
         "CompliantCriticalCount": integer,
         "CompliantHighCount": integer,
         "CompliantInformationalCount": integer,
         "CompliantLowCount": integer,
         "CompliantMediumCount": integer,
         "CompliantUnspecifiedCount": integer,
         "ExecutionType": "string",
         "NonCompliantCriticalCount": integer,
         "NonCompliantHighCount": integer,
         "NonCompliantInformationalCount": integer,
         "NonCompliantLowCount": integer,
         "NonCompliantMediumCount": integer,
         "NonCompliantUnspecifiedCount": integer,
         "OverallSeverity": "string",
         "PatchBaselineId": "string",
         "PatchGroup": "string",
         "Status": "string"
        }
       }
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
```

```
        },
        "TracingConfiguration": {
         "Enabled": boolean
        }
       },
       "AwsWafRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
       },
       "AwsWafRegionalRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
```

```
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
```

```
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       }],
       "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
       }
```

```
      },
      "AwsWafWebAcl": {
       "DefaultAction": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "ExcludedRules": [{
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }],
       "WebAclId": "string"
      },
      "AwsWafv2WebAcl": {
       "Arn": "string",
       "Capacity": number,
       "CaptchaConfig": {
        "ImmunityTimeProperty": {
         "ImmunityTime": number
        }
       },
       "DefaultAction": {
        "Block": {}
       },
       "Description": "string",
       "ManagedbyFirewallManager": boolean,
       "Name": "string",
       "Rules": [{
        "Action": {
         "RuleAction": {
          "Block": {}
         }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
```

```
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
       },
       "Id": "string",
       "Partition": "string",
       "Region": "string",
       "ResourceRole": "string",
       "Tags": {
        "string": "string"
       },
       "Type": "string"
      }],
      "SchemaVersion": "string",
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
```

```
    },
    "Sample": boolean,
    "SourceUrl": "string",
    "Threats": [{
     "FilePaths": [{
      "FileName": "string",
      "FilePath": "string",
      "Hash": "string",
      "ResourceId": "string"
     }],
     "ItemCount": number,
     "Name": "string",
     "Severity": "string"
    }],
    "ThreatIntelIndicators": [{
     "Category": "string",
     "LastObservedAt": "string",
     "Source": "string",
     "SourceUrl": "string",
     "Type": "string",
     "Value": "string"
    }],
    "Title": "string",
    "Types": ["string"],
    "UpdatedAt": "string",
    "UserDefinedFields": {
     "string": "string"
    },
    "VerificationState": "string",
    "Vulnerabilities": [{
     "CodeVulnerabilities": [{
      "Cwes": [
       "string",
       "string"
      ],
      "FilePath": {
       "EndLine": integer,
       "FileName": "string",
       "FilePath": "string",
       "StartLine": integer
      },
      "SourceArn":"string"
     }],
     "Cvss": [{
```

```
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

合併對 ASFF 欄位與值的影響

Security Hub 提供兩種合併類型：

- 合併控制項檢視 (永遠開啟；無法關閉) — 每個控制項在標準上都有單一識別碼。Security Hub 主控台的 [控制項] 頁面會顯示跨標準的所有控制項。
- 合併控制項發現項目 (可開啟或關閉) — 開啟合併控制項發現項目時，即使跨多個標準共用檢查，Security Hub 仍會產生單一發現項目以進行安全檢查。這是為了減少發現噪音。如果您在 2023 年 2 月 23 日或之後啟用 Security Hub，預設會為您開啟合併控制項發現項目。否則，預設會關閉此功能。不過，只有在系統管理員帳戶中開啟 Security Hub 成員帳戶時，才會開啟整合控制項發現項目。如果管理員帳戶中的功能已關閉，則會在成員帳戶中關閉該功能。如需開啟此功能的指示，請參閱開啟合併的控制項結果。

這兩個功能都會對控制中的尋找欄位和值進行變更AWS 安全性搜尋結果格式 (ASFF)。本節總結了這些變更。

合併的控制項檢視 — ASFF 變更

合併的控制項檢視功能引入了下列變更，以控制 ASFF 中的搜尋欄位與值。

如果您的工作流程不依賴這些控制項尋找欄位的值，則不需要採取任何動作。

如果您的工作流程依賴這些控制項尋找欄位的特定值，請更新工作流程以使用目前值。

「退回」欄位	合併控制項檢視前的範例值	合併控制項檢視之後的範例值，以及變更說明
合規性。 SecurityControlId	不適用 (新欄位)	EC2.2 引入跨標準的單一控制項 ID。 `ProductFields.RuleId` 仍然為 CIS v1.2.0 控件提供基於標準的控制 ID。 `ProductFields.ControlId` 仍然為其他標

「退回」欄位	合併控制項檢視前的範例值	合併控制項檢視之後的範例值，以及變更說明
		準中的控制項提供基於標準的控制項 ID。
合規性。 AssociatedStandards	不適用 (新欄位)	[{」StandardsId「:「標準/aws-foundational-security-best-練習/V/1.0.0」}] 顯示啟用控制項的標準。
ProductFields。 ArchivalReasons：0 /說明	不適用 (新欄位)	「發現項目處於「已封存」狀態，因為已開啟或關閉合併的控制項發現項目。這會導致在產生新的發現項目時封存處於先前狀態的發現項目。」 說明 Security Hub 為何封存現有的發現項目。
ProductFields。 ArchivalReasons：0/ ReasonCode	不適用 (新欄位)	「合併 _ 控制 _ 尋找 _ 更新」 提供 Security Hub 封存現有發現項目的原因。

「退回」欄位	合併控制項檢視前的範例值	合併控制項檢視之後的範例值，以及變更說明
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此欄位不再參考標準。
補救. 建議. 文字	「如需如何修正此問題的指示，請參閱 AWS Security Hub PCI DSS 文件。」	「如需如何修正此問題的指示，請參閱 AWS Security Hub 控制項說明文件。」 此欄位不再參考標準。
補救建議網址	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此欄位不再參考標準。

合併的控制項結果 — ASFF 變更

如果您開啟合併的控制項搜尋結果，您可能會受到下列變更的影響，以控制 ASFF 中的搜尋欄位與值。這些變更是先前針對合併控制項檢視所描述的變更之外的其他變更。

如果您的工作流程不依賴這些控制項尋找欄位的值，則不需要採取任何動作。

如果您的工作流程依賴這些控制項尋找欄位的特定值，請更新工作流程以使用目前值。

> **Note**
>
> AWS 2.0.0 版的自動化安全回應支援整合的控制項發現項目。如果您使用此版本的解決方案，則可以在開啟合併的控制項發現項目時維護工作流程。

「退回」欄位	開啟合併控制項發現項目之前的範例值	開啟合併控制項發現項目之後的值範例，以及變更說明
GeneratorId	aws-foundational-security-best-練習/V/1.0.0/Config	安全控制/Config。1 此欄位不再參考標準。
Title	設定 1 應該啟 AWS Config 用	AWS Config 應該啟用 此欄位不再參考特定於標準的資訊。
Id	安全管理系統:安全集線器:歐盟-中央:1:123456789012: 訂閱/PCI-DS/V/3.2.1/PCI.5 /尋找/亞6A26-A156-48F0-9403-115983E5A956	安全管理系統:安全中心:歐盟-中央 1:123456789012: 安全性控制 /Iam.9 /尋找/查找/A156-48f0-9403-115983e5a956 此欄位不再參考標準。
ProductFields.ControlId	PCI.EC2.2	已移除。請參閱`Compliance.SecurityControlId`。 此欄位會被移除，以支持單一、不可知的控制項 ID。
ProductFields.RuleId	1.3	已移除。請參閱`Compliance.SecurityControlId`。 此欄位會被移除，以支持單一、不可知的控制項 ID。

「退回」欄位	開啟合併控制項發現項目之前的範例值	開啟合併控制項發現項目之後的值範例，以及變更說明
描述	此 PCI DSS 控制項會檢查目前帳戶和區域中 AWS Config 是否已啟用。	此 AWS 控制項會檢查目前科目與區域中 AWS Config 是否已啟用。 此欄位不再參考標準。

嚴重性	「嚴重性」：{
	
	「產品介紹」：90,
	
	「標籤」：「嚴重」，
	
	「標準化」：90，
	
	「原創」：「嚴重」
	
	}
		「嚴重性」：{
		
		「標籤」：「嚴重」，
		
		「標準化」：90，
		
		「原創」：「嚴重」
		
		}
		
		Security Hub 不再使用 [產品] 欄位來描述發現項目的嚴重性。

類型	[「軟體與組態檢查/產業與法規標準 /PCI-DSS」]	["軟體與組態檢查/產業與法規標準"] 此欄位不再參考標準。
合規性。 RelatedRequirements	["零件數據資料管理系統 10.5.2」， 「PCI DSS 11.5」]	[「投資卡付款式直接輸入資料系統 3.2.1/10.5.2」， 「支援資料輸入資料直接儲存系統 3.2.1/11.5」， 「獨聯體 AWS 基金會基準 v1.2.0/2.5」] 此欄位顯示所有啟用標準中的相關需求。

「退回」欄位	開啟合併控制項發現項目之前的範例值	開啟合併控制項發現項目之後的值範例，以及變更說明
CreatedAt	2022-05-05 噸	2022-09-25 噸 格式保持不變，但是當您開啟合併的控制項發現項目時，會重設值。
FirstObservedAt	2022-05-07 噸 18:13.138	2022-09-28 噸 格式保持不變，但是當您開啟合併的控制項發現項目時，會重設值。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	已移除。請參閱`Remediation.Recommendation.Url` 。
ProductFields.StandardsArn	ARN: AWN: 安全集線器::: 標準/-實踐/V/1.0.0 aws-foundational-security-best	已移除。請參閱`Compliance.AssociatedStandards` 。
ProductFields.StandardsControlArn	ARN: AWN: 安全性中樞:美國東部-1：123456789012：控制/-實踐/V/1.0.0/Config .1 aws-foundational-security-best	已移除。Security Hub 產生一個發現項目，以便跨標準進行安全檢查。
ProductFields.StandardsGuideArn	ARN: AWN: 安全集線器::: 規則//V/1.2.0 cis-aws-foundations-benchmark	已移除。請參閱`Compliance.AssociatedStandards` 。
ProductFields.StandardsGuideSubscriptionArn	安全中心:安全性中樞:美國東部-2:12456789012: 訂閱//V/1.2.0 cis-aws-foundations-benchmark	已移除。Security Hub 產生一個發現項目，以便跨標準進行安全檢查。
ProductFields.StandardsSubscriptionArn	坐標:AWN: 安全中心:美國東部-1:123456789012: 訂閱/-練習/V/1.0.0 aws-foundational-security-best	已移除。Security Hub 產生一個發現項目，以便跨標準進行安全檢查。

「退回」欄位	開啟合併控制項發現項目之前的範例值	開啟合併控制項發現項目之後的值範例，以及變更說明
ProductFields.aw/ 安全集線器/FindingId	ARN: aws: 安全集線器:我們東部 -1:: 產品/AWS/安全集線器/架構:AWS: 安全集線器:我們東-1:123456789012: 訂閱/-實踐 /V/1.0.0/Config .1/尋找/751c2173-7372-4E12-8656-A52DFD67 aws-foundational-security-best	ARN: aws: 安全性中樞:我們東部-1: 產品/AWS/安全集線器/應用程式:AWS: 安全性中樞:我們東-1:123456789012: 安全性控制/Config .1/尋找/751C2173-7372-4e12-8656-A5210DF1D67 此欄位不再參考標準。

開啟合併的控制項搜尋結果後，客戶提供的 ASFF 欄位值

如果您開啟合併的控制項發現項目，Security Hub 會跨標準產生一個發現項目，並封存原始發現項目 (每個標準的個別發現項目)。若要檢視已封存的發現項目，您可以造訪 Security Hub 主控台的 [發現項目] 頁面，並將 [記錄] 狀態篩選器設定為 [已封存]，或使用 `GetFindings`API 動作。您在 Security Hub 主控台或使用 BatchUpdateFindingsAPI 所做的原始發現項目所做的更新將不會保留在新的發現項目中 (如果需要，您可以參考封存的發現項目來復原此資料)。

客戶提供的 ASFF 欄位	開啟合併控制項發現項目之後的變更說明
可信度	重置為空狀態。
危急性	重置為空狀態。
注意	重置為空狀態。
RelatedFindings	重置為空狀態。
嚴重性	發現項目的預設嚴重性 (符合控制項的嚴重性)。
類型	重置為與標準無關的值。
UserDefinedFields	重置為空狀態。
VerificationState	重置為空狀態。

客戶提供的 ASFF 欄位	開啟合併控制項發現項目之後的變更說明
工作流程	新的失敗發現項目的預設值為NEW。新傳遞的發現項目的預設值為RESOLVED。

開啟整合控制項發現項目之前和之後的產生器 ID

以下是開啟合併控制項發現項目時控制項的產生器 ID 變更清單。這些適用於截至 2023 年 2 月 15 日 Security Hub 支援的控制項。

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/1.1 cis-aws-foundations-benchmark	安全控制/.1 CloudWatch
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/1.1 cis-aws-foundations-benchmark	安全性控制/IAM.20
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/1.10 cis-aws-foundations-benchmark	安全性控制/IAM.16
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.11 cis-aws-foundations-benchmark	安全性控制/IAM.17
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.12 cis-aws-foundations-benchmark	安全性控制/IAM.4
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.13 cis-aws-foundations-benchmark	安全性控制/IAM.9
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.14 cis-aws-foundations-benchmark	安全性控制/IAM.6
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.16 cis-aws-foundations-benchmark	安全性控制/IAM.2
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.2 cis-aws-foundations-benchmark	安全性控制/IAM.5

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.20 cis-aws-foundations-benchmark	安全性控制/IAM.18
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.22 cis-aws-foundations-benchmark	安全性控制 /IAM。1
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/1.3 cis-aws-foundations-benchmark	安全性控制/IAM.8
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.4 cis-aws-foundations-benchmark	安全性控制 /IAM3
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.5 cis-aws-foundations-benchmark	安全性控制/IAM.11
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.6 cis-aws-foundations-benchmark	安全性控制/IAM.12
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.7 cis-aws-foundations-benchmark	安全性控制/IAM.13
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.8 cis-aws-foundations-benchmark	安全性控制/IAM.14
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/1.9 cis-aws-foundations-benchmark	安全性控制/IAM.15
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.1 cis-aws-foundations-benchmark	安全控制/.1 CloudTrail
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.2 cis-aws-foundations-benchmark	安全控制 /.4 CloudTrail
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/2.3 cis-aws-foundations-benchmark	安全控制 /.6 CloudTrail
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/2.4 cis-aws-foundations-benchmark	安全控制 /.5 CloudTrail

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.5 cis-aws-foundations-benchmark	安全控制/Config。1
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.6 cis-aws-foundations-benchmark	安全控制 /.7 CloudTrail
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.7 cis-aws-foundations-benchmark	安全控制/.2 CloudTrail
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/2.8 cis-aws-foundations-benchmark	安全性控制/KMS.4
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/2.9 cis-aws-foundations-benchmark	安全性控制 /EC2.6
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.1 cis-aws-foundations-benchmark	安全控制/.2 CloudWatch
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/3.2 cis-aws-foundations-benchmark	安全控制/.3 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.3 cis-aws-foundations-benchmark	安全控制/.1 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.4 cis-aws-foundations-benchmark	安全控制 /.4 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.5 cis-aws-foundations-benchmark	安全控制 /.5 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.6 cis-aws-foundations-benchmark	安全控制 /.6 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.7 cis-aws-foundations-benchmark	安全控制 /.7 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.8 cis-aws-foundations-benchmark	安全控制 /.8 CloudWatch

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.9 cis-aws-foundations-benchmark	安全控制 /.9 CloudWatch
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/3.10 cis-aws-foundations-benchmark	安全控制 /.10 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.11 cis-aws-foundations-benchmark	安全控制 /.11 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.12 cis-aws-foundations-benchmark	安全控制 /.12 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.13 cis-aws-foundations-benchmark	安全控制 /.13 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/3.14 cis-aws-foundations-benchmark	安全控制 /.14 CloudWatch
ARN: AWN: 安全性集線器:: 規則///V/1.2.0/規則/4.1 cis-aws-foundations-benchmark	安全性控制/EC2.13
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/4.2 cis-aws-foundations-benchmark	安全控制/EC2.14
ARN: AWN: 安全集線器:: 規則///V/1.2.0/規則/4.3 cis-aws-foundations-benchmark	安全性控制/EC2.2
cis-aws-foundations-benchmark/V/1.4.0/1.10	安全性控制/IAM.5
cis-aws-foundations-benchmark/V/1.4.0/1.14	安全性控制 /IAM3
cis-aws-foundations-benchmark/V/1.4.0/1.16	安全性控制 /IAM。1
cis-aws-foundations-benchmark/V/1.4.0/1.17	安全性控制/IAM.18
cis-aws-foundations-benchmark/V/1.4.0/1.4	安全性控制/IAM.4
cis-aws-foundations-benchmark/V/1.4.0/1.5	安全性控制/IAM.9

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
cis-aws-foundations-benchmark/V/1.4.0/1.6	安全性控制/IAM.6
cis-aws-foundations-benchmark/V/1.4.0/1.7	安全控制/.1 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/1.8	安全性控制/IAM.15
cis-aws-foundations-benchmark/V/1.4.0/1.9	安全性控制/IAM.16
cis-aws-foundations-benchmark/V/1.4.0/2.1.2	安全控制 /S3.5
cis-aws-foundations-benchmark/V/1.4.0/2.1.5.1	安全控制 /S3.1
cis-aws-foundations-benchmark/V/1.4.0/2.1.5.2	安全控制 /S3.8
cis-aws-foundations-benchmark/V/1.4.0/2.2.1	安全控制/EC2.7
cis-aws-foundations-benchmark/V/1.4.0/2.3.1	安全控制 /RDS.3
cis-aws-foundations-benchmark/V/1.4.0/3.1	安全控制/.1 CloudTrail
cis-aws-foundations-benchmark/V/1.4.0/3.2	安全控制 /.4 CloudTrail
cis-aws-foundations-benchmark/V/1.4.0/3.4	安全控制 /.5 CloudTrail
cis-aws-foundations-benchmark/V/1.4.0/3.5	安全控制/Config。1
cis-aws-foundations-benchmark/V/1.4.0/3.6	安全控制 /S3.9
cis-aws-foundations-benchmark/V/1.4.0/3.7	安全控制/.2 CloudTrail
cis-aws-foundations-benchmark/V/1.4.0/3.8	安全性控制/KMS.4
cis-aws-foundations-benchmark/V/1.4.0/3.9	安全性控制 /EC2.6
cis-aws-foundations-benchmark/V/1.4.0/4.3	安全控制/.1 CloudWatch
cis-aws-foundations-benchmark/V/4.0/4.4	安全控制 /.4 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.5	安全控制 /.5 CloudWatch

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
cis-aws-foundations-benchmark/V/1.4.0/4.6	安全控制 /.6 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.7	安全控制 /.7 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.8	安全控制 /.8 CloudWatch
cis-aws-foundations-benchmark/V/4.0/4.9	安全控制 /.9 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.10	安全控制 /.10 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.11	安全控制 /.11 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.12	安全控制 /.12 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.13	安全控制 /.13 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/4.14	安全控制 /.14 CloudWatch
cis-aws-foundations-benchmark/V/1.4.0/5.1	安全控制/EC2.21
cis-aws-foundations-benchmark/V/1.4.0/5.3	安全性控制/EC2.2
aws-foundational-security-best-練習/V/1.0.0/帳戶	安全控制/帳戶。1
aws-foundational-security-best-練習/V /1.0.0/ ACM1	安全性控制/ACM.1
aws-foundational-security-best-練習/V/1.0.0/ APIGATI.1	安全控制/管理方式。1
aws-foundational-security-best-練習/V/1.0.0/ APGATI.2	安全控制/管理方式。2
aws-foundational-security-best-練習/V/1.0.0/ APGATI.3	安全控制/管理方式 3
aws-foundational-security-best-練習/V/1.0.0/ APGATI.4	安全控制/安全管理 4

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/APGATI.5	安全控制/安全管理。5
aws-foundational-security-best-練習/V/1.0.0/apigate.8	安全控制/安全管理 .8
aws-foundational-security-best-練習/V/1.0.0/apigate.9	安全控制/安全管理 .9
aws-foundational-security-best-練習/V /1.0.0/AutoScaling	安全控制/.1 AutoScaling
aws-foundational-security-best-練習/V /1.0.0/AutoScaling	安全控制/.2 AutoScaling
aws-foundational-security-best-練習/V /1.0.0/AutoScaling	安全控制/.3 AutoScaling
aws-foundational-security-best-練習/V /1.0.0/ .4 AutoScaling	安全控制 /.4 AutoScaling
aws-foundational-security-best-練習/V/1.0.0/ 自動縮放 .5	安全控制/自動調整規模。5
aws-foundational-security-best-練習/V /1.0.0/ .6 AutoScaling	安全控制 /.6 AutoScaling
aws-foundational-security-best-練習/V /1.0.0/ .9 AutoScaling	安全控制 /.9 AutoScaling
aws-foundational-security-best-練習/V /1.0.0/CloudFormation	安全控制/.1 CloudFormation
aws-foundational-security-best-練習/V /1.0.0/CloudFront	安全控制/.1 CloudFront
aws-foundational-security-best-練習/V /1.0.0/CloudFront	安全控制/.2 CloudFront

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/ CloudFront	安全控制/.3 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .4 CloudFront	安全控制 /.4 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .5 CloudFront	安全控制 /.5 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .6 CloudFront	安全控制 /.6 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .7 CloudFront	安全控制 /.7 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .8 CloudFront	安全控制 /.8 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ .9 CloudFront	安全控制 /.9 CloudFront
aws-foundational-security-best-練習/V/1.0.0/.10 CloudFront	安全控制 /.10 CloudFront
aws-foundational-security-best-練習/V/1.0.0/.12 CloudFront	安全控制 /.12 CloudFront
aws-foundational-security-best-練習/V /1.0.0/ CloudTrail	安全控制/.1 CloudTrail
aws-foundational-security-best-練習/V /1.0.0/ CloudTrail	安全控制/.2 CloudTrail
aws-foundational-security-best-練習/V /1.0.0/ .4 CloudTrail	安全控制 /.4 CloudTrail
aws-foundational-security-best-練習/V /1.0.0/ .5 CloudTrail	安全控制 /.5 CloudTrail

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/ CodeBuild	安全控制/.1 CodeBuild
aws-foundational-security-best-練習/V /1.0.0/ CodeBuild	安全控制/.2 CodeBuild
aws-foundational-security-best-練習/V /1.0.0/ CodeBuild	安全控制/.3 CodeBuild
aws-foundational-security-best-練習/V /1.0.0/ .4 CodeBuild	安全控制 /.4 CodeBuild
aws-foundational-security-best-練習/V /1.0.0/ .5 CodeBuild	安全控制 /.5 CodeBuild
aws-foundational-security-best-練習/V/1.0.0/ Config	安全控制/Config。1
aws-foundational-security-best-練習/V/1.0.0/數位公升 1	安全控制/DMS1
aws-foundational-security-best-練習/V/1.0.0/動態。1	安全控制/動態。1
aws-foundational-security-best-練習/V/1.0.0/動態 .2	安全控制/動態 .2
aws-foundational-security-best-練習/V/1.0.0/動態 .3	安全控制/動態 .3
aws-foundational-security-best-練習/V/1.0.0/ EC2.1	安全性控制 /EC2.1
aws-foundational-security-best-練習/V /1.0.0/ EC2.3	安全性控制/EC2.3
aws-foundational-security-best-練習/V /1.0.0/ EC2.4	安全性控制/EC2.4

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/EC2.6	安全性控制 /EC2.6
aws-foundational-security-best-練習/V /1.0.0/EC2.7	安全控制/EC2.7
aws-foundational-security-best-練習/V /1.0.0/EC2.8	安全性控制/EC2.8
aws-foundational-security-best-練習/V /1.0.0/EC2.9	安全控制/EC2.9
aws-foundational-security-best-練習/V/1.0.0/EC2.10	安全控制/EC2.10
aws-foundational-security-best-練習/V/1.0.0/EC2.15	安全控制/EC2.15
aws-foundational-security-best-練習/V/1.0.0/EC2.16	安全控制/EC2.16
aws-foundational-security-best-練習/V/1.0.0/EC2.17	安全控制/EC2.17
aws-foundational-security-best-練習/V/1.0.0/EC2.18	安全控制/EC2.18
aws-foundational-security-best-練習/V/1.0.0/EC2.19	安全控制/EC2.19
aws-foundational-security-best-練習/V /1.0.0/EC2.2	安全性控制/EC2.2
aws-foundational-security-best-練習/V/1.0.0/EC2.20	安全控制/EC2.20
aws-foundational-security-best-練習/V/1.0.0/EC2.21	安全控制/EC2.21

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/EC2.22	安全控制/EC2.22
aws-foundational-security-best-練習/V/1.0.0/EC2.23	安全控制/EC2.23
aws-foundational-security-best-練習/V/1.0.0/EC2.24	安全控制/EC2.24
aws-foundational-security-best-練習/V/1.0.0/EC2.25	安全控制/EC2.25
aws-foundational-security-best-練習/V/1.0.0/ecr.1	安全性控制 /ECr.1
aws-foundational-security-best-練習/V/1.0.0/ecr.2	安全控制 /EC.2
aws-foundational-security-best-練習/V/1.0.0/ecr.3	安全控制 /ECR3
aws-foundational-security-best-練習/V/1.0.0/EC.1	安全控制 /EC.1
aws-foundational-security-best-練習/V/1.0.0/EC.10	安全控制 /EC.10
aws-foundational-security-best-練習/V/1.0.0/EC.12	安全控制 /EC.12
aws-foundational-security-best-練習/V/1.0.0/EC.2	安全性控制/EC.2
aws-foundational-security-best-練習/V/1.0.0/EC.3	安全控制 /EC.3
aws-foundational-security-best-練習/V/1.0.0/EC.4	安全控制 /EC.4

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/EC.5	安全控制 /EC.5
aws-foundational-security-best-練習/V/1.0.0/EC.8	安全控制 /EC.8
aws-foundational-security-best-練習/V/1.0.0/EF.1	安全控制
aws-foundational-security-best-練習/V /1.0.0/EF.2	安全控制
aws-foundational-security-best-練習/V /1.0.0/EPS3	安全控制
aws-foundational-security-best-練習/V/1.0.0/EPS4	安全控制
aws-foundational-security-best-練習/V /1.0.0/EK.	安全控制/EK.2
aws-foundational-security-best-練習/V /1.0.0/ElasticBeanstalk	安全控制/.1 ElasticBeanstalk
aws-foundational-security-best-練習/V /1.0.0/ElasticBeanstalk	安全控制/.2 ElasticBeanstalk
aws-foundational-security-best-練習/V/1.0.0/ElbV2.1	安全控制系統 (ELB.1)
aws-foundational-security-best-練習/V/1.0.0/Elb.2	安全控制系統 (ELB.2)
aws-foundational-security-best-練習/V/1.0.0/Elb.3	安全控制系統 /ELB.3
aws-foundational-security-best-練習/V/1.0.0/Elb.4	安全控制系統 /ELB.4

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/Elb.5	安全控制系統 /ELB.5
aws-foundational-security-best-練習/V/1.0.0/Elb.6	安全控制系統 /ELB.6
aws-foundational-security-best-練習/V /1.0.0/Elb.7	安全控制系統 /ELB.7
aws-foundational-security-best-練習/V/1.0.0/Elb.8	安全控制系統 /ELB.8
aws-foundational-security-best-練習/V /1.0.0/Elb.9	安全控制系統 /ELB.9
aws-foundational-security-best-練習/V /1.0.0/Elb.10	安全控制系統
aws-foundational-security-best-練習/V /1.0.0/Elb.11	安全控制系統
aws-foundational-security-best-練習/V /1.0.0/Elb.12	安全控制系統 (ELB.12)
aws-foundational-security-best-練習/V /1.0.0/Elb.13	安全控制系統 (ELB.13)
aws-foundational-security-best-練習/V /1.0.0/Elb.14	安全控制系統 (ELB.14)
aws-foundational-security-best-練習/V/1.0.0/EMR.1	安全性控制 /EMr.1
aws-foundational-security-best-練習/V/1.0.0/es.1	安全控制 /ES.1
aws-foundational-security-best-練習/V/1.0.0/es.2	安全控制 /ES.2

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/.3	安全控制 /.3
aws-foundational-security-best-練習/V/1.0.0/.4	安全控制 /.4
aws-foundational-security-best-練習/V /1.0.0/.5	安全性控制 /.5
aws-foundational-security-best-練習/V/1.0.0/.6	安全性控制 /.6
aws-foundational-security-best-練習/V/1.0.0/.7	安全控制 /.7
aws-foundational-security-best-練習/V/1.0.0/.8	安全控制 /.8
aws-foundational-security-best-練習/V /1.0.0/ GuardDuty	安全控制/.1 GuardDuty
aws-foundational-security-best-練習/V/1.0.0/ Iam.1	安全性控制 /IAM。1
aws-foundational-security-best-練習/V/1.0.0/ IAM.2	安全性控制/IAM.2
aws-foundational-security-best-實踐/V/1.0.0/ IAM	安全性控制/IAM.21
aws-foundational-security-best-練習/V/1.0.0/ IAM.3	安全性控制 /IAM3
aws-foundational-security-best-實踐/V/1.0.0/ IAM	安全性控制/IAM.4
aws-foundational-security-best-練習/V/1.0.0/ IAM	安全性控制/IAM.5
aws-foundational-security-best-實踐/V/1.0.0/ IAM.6	安全性控制/IAM.6
aws-foundational-security-best-實踐/V/1.0.0/ IAM.7	安全性控制/IAM.7

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/IAM	安全性控制/IAM.8
aws-foundational-security-best-練習/V/1.0.0/運 Kinesis .1	安全控制 Kinesis 1
aws-foundational-security-best-練習/V /1.0.0/公里1	安全性控制/KMS.1
aws-foundational-security-best-練習/V /1.0.0/公里.2	安全性控制/KMS.2
aws-foundational-security-best-練習/V /1.0.0/公里.3	安全性控制/KMS.3
aws-foundational-security-best-練習/V/1.0.0/Lambda .1	安全控制/Lambda 本 1
aws-foundational-security-best-練習/V/1.0.0/Lambda。	安全控制/Lambda 本。2
aws-foundational-security-best-練習/V/1.0.0/Lambda .5	安全控制 Lambda 本 5
aws-foundational-security-best-練習/V /1.0.0/NetworkFirewall	安全控制/.3 NetworkFirewall
aws-foundational-security-best-練習/V /1.0.0/ .4 NetworkFirewall	安全控制 /.4 NetworkFirewall
aws-foundational-security-best-練習/V /1.0.0/ .5 NetworkFirewall	安全控制 /.5 NetworkFirewall
aws-foundational-security-best-練習/V /1.0.0/ .6 NetworkFirewall	安全控制 /.6 NetworkFirewall
aws-foundational-security-best-練習 /V/1.0.0/打開搜索.1	安全性控制/開放搜尋。1

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習 /V/1.0.0/開放搜索.2	安全控制/開放搜尋 2
aws-foundational-security-best-練習 /V/1.0.0/開放搜索.3	安全性控制/開放搜尋 3
aws-foundational-security-best-練習 /V/1.0.0/打開搜索.4	安全控制/開放搜尋 4
aws-foundational-security-best-練習 /V/1.0.0/打開搜索 .5	安全控制/開放搜索 .5
aws-foundational-security-best-練習 /V/1.0.0/打開搜索 .6	安全控制/開放搜索 .6
aws-foundational-security-best-練習 /V/1.0.0/打開搜索 .7	安全控制/開放搜尋 .7
aws-foundational-security-best-練習 /V/1.0.0/打開搜索 .8	安全控制/開放搜尋 .8
aws-foundational-security-best-練習/V/1.0.0/R.1	安全控制 /RDS.1
aws-foundational-security-best-練習/V/1.0.0/RD.10	安全控制 /RDS.10
aws-foundational-security-best-練習/V/1.0.0/RDS.11	安全性控制/RDS.11
aws-foundational-security-best-練習/V/1.0.0/RD.12	安全性控制/RDS.12
aws-foundational-security-best-練習/V/1.0.0/RD.13	安全性控制/RDS.13
aws-foundational-security-best-練習/V/1.0.0/RD.14	安全性控制/RDS.14

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/R.15	安全性控制/RDS.15
aws-foundational-security-best-練習/V/1.0.0/RD.16	安全性控制/RDS.16
aws-foundational-security-best-練習/V/1.0.0/RD.17	安全性控制/RDS.17
aws-foundational-security-best-練習/V/1.0.0/R.18	安全控制/RDS.18
aws-foundational-security-best-練習/V/1.0.0/R.19	安全性控制/RDS.19
aws-foundational-security-best-練習/V/1.0.0/RD.2	安全控制 /RDS.2
aws-foundational-security-best-練習/V/1.0.0/RD.20	安全控制/RDS.20
aws-foundational-security-best-練習/V/1.0.0/RD.21	安全控制/RDS.21
aws-foundational-security-best-練習/V/1.0.0/RD.22	安全性控制/RDS.22
aws-foundational-security-best-練習/V/1.0.0/RDS.23	安全性控制/RDS.23
aws-foundational-security-best-練習/V/1.0.0/R.24	安全性控制/RDS.24
aws-foundational-security-best-練習/V/1.0.0/R.25	安全性控制/RDS.25
aws-foundational-security-best-練習/V/1.0.0/R.3	安全控制 /RDS.3

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/R.4	安全性控制/RDS.4
aws-foundational-security-best-練習/V/1.0.0/R.5	安全控制 /RDS.5
aws-foundational-security-best-練習/V/1.0.0/R.6	安全控制 /RDS.6
aws-foundational-security-best-練習/V/1.0.0/R.7	安全控制 /RDS.7
aws-foundational-security-best-練習/V/1.0.0/RD.8	安全性控制/RDS.8
aws-foundational-security-best-練習/V/1.0.0/RD.9	安全性控制/RDS.9
aws-foundational-security-best-練習/V/1.0.0/Redshift 1	安全控制/Redshift 1
aws-foundational-security-best-練習/V/1.0.0/Redshift。	安全控制/Redshift 2
aws-foundational-security-best-練習/V/1.0.0/Redshift 3	安全控制/Redshift 3
aws-foundational-security-best-練習/V/1.0.0/Redshift 動。4	安全控制/Redshift 4
aws-foundational-security-best-練習/V/1.0.0/Redshift 動。6	安全控制/Redshift。6
aws-foundational-security-best-練習/V/1.0.0/Redshift 動 .7	安全控制/Redshift。7
aws-foundational-security-best-練習/V/1.0.0/Redshift 動 .8	安全控制/Redshift。8
aws-foundational-security-best-練習/V/1.0.0/Redshift 動。9	安全控制/Redshift 9

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V/1.0.0/S3.1	安全控制 /S3.1
aws-foundational-security-best-練習/V/1.0.0/S3.10	安全性控制
aws-foundational-security-best-練習/V /1.0.0/S3.11	安全性控制
aws-foundational-security-best-練習/V/1.0.0/S3.12	安全性控制
aws-foundational-security-best-練習/V/1.0.0/S3.13	安全性控制
aws-foundational-security-best-練習/V /1.0.0/S3.2	安全控制 /S3.2
aws-foundational-security-best-練習/V/1.0.0/S3.3	安全控制 /S3.3
aws-foundational-security-best-練習/V/1.0.0/S3.5	安全控制 /S3.5
aws-foundational-security-best-練習/V/1.0.0/S3.6	安全控制 /S3.6
aws-foundational-security-best-練習/V/1.0.0/S3.8	安全控制 /S3.8
aws-foundational-security-best-練習/V/1.0.0/S3.9	安全控制 /S3.9
aws-foundational-security-best-練習/V /1.0.0/SageMaker	安全控制/.1 SageMaker
aws-foundational-security-best-練習/V /1.0.0/SageMaker	安全控制/.2 SageMaker

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/ SageMaker	安全控制/.3 SageMaker
aws-foundational-security-best-練習/V /1.0.0/ SecretsManager	安全控制/.1 SecretsManager
aws-foundational-security-best-練習/V /1.0.0/ SecretsManager	安全控制/.2 SecretsManager
aws-foundational-security-best-練習/V /1.0.0/ SecretsManager	安全控制/.3 SecretsManager
aws-foundational-security-best-練習/V /1.0.0/ .4 SecretsManager	安全控制 /.4 SecretsManager
aws-foundational-security-best-練習/V /1.0.0/ SN.1	安全性控制/SN.1
aws-foundational-security-best-練習/V /1.0.0/ SN.2	安全性控制/SN.2
aws-foundational-security-best-練習/V/1.0.0/平方米 1	安全性控制/SQ.1
aws-foundational-security-best-練習/V/1.0.0/ SSM.1	安全性控制 /SSM。1
aws-foundational-security-best-練習/V/1.0.0/ SSM.2	安全性控制 /SSM 2
aws-foundational-security-best-練習/V/1.0.0/ SSM.3	安全性控制 /SSM3
aws-foundational-security-best-練習/V/1.0.0/ SSM	安全性控制/SSM4
aws-foundational-security-best-練習/V/1.0.0/波1	安全性控制/WAF.1

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
aws-foundational-security-best-練習/V /1.0.0/波2	安全性控制/WAF.2
aws-foundational-security-best-練習/V/1.0.0/波3	安全性控制/WAF.3
aws-foundational-security-best-練習/V/1.0.0/wa.4	安全性控制 /WAF.4
aws-foundational-security-best-練習/V/1.0.0/wa.6	安全性控制 /WAF.6
aws-foundational-security-best-練習/V/1.0.0/W.7	安全性控制 /WAF.7
aws-foundational-security-best-練習/V/1.0.0/W.8	安全性控制 /WAF.8
aws-foundational-security-best-練習/V /1.0.0/波10	安全性控制/WAF.10
PCI-DS/V/3.2.1/PCI。 AutoScaling.1	安全控制/.1 AutoScaling
PCI-DS/V/3.2.1/PCI。 CloudTrail.1	安全控制/.2 CloudTrail
PCI-DS/V/3.2.1/PCI。 CloudTrail.2	安全控制/.3 CloudTrail
PCI-DS/V/3.2.1/PCI。 CloudTrail.3	安全控制 /.4 CloudTrail
PCI-DS/V/3.2.1/PCI。 CloudTrail.4	安全控制 /.5 CloudTrail
PCI-DS/V/3.2.1/PCI。 CodeBuild.1	安全控制/.1 CodeBuild
PCI-DS/V/3.2.1/PCI。 CodeBuild.2	安全控制/.2 CodeBuild
PCI-DS/V/3.2.1/PCI.配置.1	安全控制/Config。1
PCI-DS/V/3.2.1/PCI.1	安全控制/.1 CloudWatch
PCI-DS/V/3.2.1/PCI.1	安全控制/DMS1

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
PCI-DS/V/3.2.1/PCI.ec2.1	安全性控制 /EC2.1
PCI-DS/V/3.2.1/PCI.ec2.2	安全性控制/EC2.2
PCI-DS/V/3.2.1/PCI.ec2.4	安全控制/EC2.12
PCI-DS/V/3.2.1/PCI.ec2.5	安全性控制/EC2.13
PCI-DS/V/3.2.1/PCI.ec2.6	安全性控制 /EC2.6
PCI-DS/V/3.2.1/PCI.ELBV2.1	安全控制系統 (ELB.1)
PCI-DS/V/3.2.1/PCI.1	安全控制 /ES.2
PCI-DS/V/3.2.1/PCI.E.	安全控制 /ES.1
PCI-DS/V/3.2.1/PCI。 GuardDuty.1	安全控制/.1 GuardDuty
PCI-DS/V/3.2.1/PCIA.1	安全性控制/IAM.4
PCI-DS/V/3.2.1/PCIAM.2	安全性控制/IAM.2
PCI-DS/V/3.2.1/PCIAM.3	安全性控制 /IAM。1
PCI-DS/V/3.2.1/PCI.4	安全性控制/IAM.6
PCI-DS/V/3.2.1/PCIAM.5	安全性控制/IAM.9
PCI-DS/V/3.2.1/PCIAM.6	安全性控制/IAM.19
PCI-DS/V/3.2.1/PCI.7	安全性控制/IAM.8
PCI-DS/V/3.2.1/PCI.8	安全性控制/IAM.10
PCI-DS/V/3.2.1/PCI.KM.1	安全性控制/KMS.4
PCI-DS/V/3.2.1/PCI.Lambda	安全控制/Lambda 本 1
PCI-DS/V/3.2.1/PCI.Lambda	安全控制/Lambda 3

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
PCI-DS/V/3.2.1/PCI 開放搜索 1	安全控制/開放搜尋 2
PCI-DS/V/3.2.1/PCI.開放搜索.2	安全性控制/開放搜尋。1
PCI-DS/V/3.2.1/PCI..1	安全控制 /RDS.1
PCI-DS/V/3.2.1/PCI.rds.2	安全控制 /RDS.2
PCI-DS/V/3.2.1/PCI.	安全控制/Redshift 1
PCI-DS/V/3.2.1/PCI.S3.1	安全控制 /S3.3
PCI-DS/V/3.2.1/PCI.S3.2	安全控制 /S3.2
PCI-DS/V/3.2.1/PCI.S3.3	安全控制 /S3.7
PCI-DS/V/3.2.1/PCI.S3.5	安全控制 /S3.5
PCI-DS/V/3.2.1/PCI.S3.6	安全控制 /S3.1
PCI-DS/V/3.2.1/PCI。 SageMaker.1	安全控制/.1 SageMaker
PCI-DSS/V/3.2.1/PCI.S	安全性控制 /SSM 2
PCI-DS/V/3.2.1/PCI.S.	安全性控制 /SSM3
PCI-DSS/V/3.2.1/PCI.S.	安全性控制 /SSM。1
service-managed-aws-control-塔/V /1.0.0/英尺	安全性控制/ACM.1
service-managed-aws-control-塔/V/1.0.0/APGATEW.1	安全控制/管理方式。1
service-managed-aws-control-塔/V/1.0.0/APGATE.2	安全控制/管理方式。2
service-managed-aws-control-塔/V/1.0.0/APGATE.3	安全控制/管理方式 3

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V/1.0.0/APGATE.4	安全控制/安全管理 4
service-managed-aws-control-塔/V/1.0.0/APGATE.5	安全控制/安全管理。5
service-managed-aws-control-塔/V /1.0.0/AutoScaling	安全控制/.1 AutoScaling
service-managed-aws-control-塔/V /1.0.0/AutoScaling	安全控制/.2 AutoScaling
service-managed-aws-control-塔/V /1.0.0/AutoScaling	安全控制/.3 AutoScaling
service-managed-aws-control-塔/V /1.0.0/ .4 AutoScaling	安全控制 /.4 AutoScaling
service-managed-aws-control-塔/V/1.0.0/自動縮放 .5	安全控制/自動調整規模。5
service-managed-aws-control-塔/V /1.0.0/ .6 AutoScaling	安全控制 /.6 AutoScaling
service-managed-aws-control-塔/V /1.0.0/ .9 AutoScaling	安全控制 /.9 AutoScaling
service-managed-aws-control-塔/V /1.0.0/CloudTrail	安全控制/.1 CloudTrail
service-managed-aws-control-塔/V /1.0.0/CloudTrail	安全控制/.2 CloudTrail
service-managed-aws-control-塔/V /1.0.0/ .4 CloudTrail	安全控制 /.4 CloudTrail
service-managed-aws-control-塔/V /1.0.0/ .5 CloudTrail	安全控制 /.5 CloudTrail

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/ CodeBuild	安全控制/.1 CodeBuild
service-managed-aws-control-塔/V /1.0.0/ CodeBuild	安全控制/.2 CodeBuild
service-managed-aws-control-塔/V /1.0.0/ .4 CodeBuild	安全控制 /.4 CodeBuild
service-managed-aws-control-塔/V /1.0.0/ .5 CodeBuild	安全控制 /.5 CodeBuild
service-managed-aws-control-塔/V /1.0.0/公分1	安全控制/DMS1
service-managed-aws-control-塔/V/1.0.0/動態 B.1	安全控制/動態。1
service-managed-aws-control-塔/V /1.0.0/動態 .2	安全控制/動態 .2
service-managed-aws-control-塔/V /1.0.0/EC 2.1	安全性控制 /EC2.1
service-managed-aws-control-塔/V /1.0.0/EC 2.2	安全性控制/EC2.2
service-managed-aws-control-塔/V /1.0.0/EC 2.3	安全性控制/EC2.3
service-managed-aws-control-塔/V /1.0.0/EC 2.4	安全性控制/EC2.4
service-managed-aws-control-塔/V /1.0.0/EC 2.6	安全性控制 /EC2.6
service-managed-aws-control-塔/V /1.0.0/EC 2.7	安全控制/EC2.7

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/EC2.8	安全性控制/EC2.8
service-managed-aws-control-塔/V /1.0.0/EC2.9	安全控制/EC2.9
service-managed-aws-control-塔/V /1.0.0/EC2.10	安全控制/EC2.10
service-managed-aws-control-塔/V /1.0.0/EC2.15	安全控制/EC2.15
service-managed-aws-control-塔/V /1.0.0/EC2.16	安全控制/EC2.16
service-managed-aws-control-塔/V /1.0.0/EC2.17	安全性控制/EC2.17
service-managed-aws-control-塔/V /1.0.0/EC2.18	安全控制/EC2.18
service-managed-aws-control-塔/V /1.0.0/EC2.19	安全控制/EC2.19
service-managed-aws-control-塔/V /1.0.0/EC2.20	安全控制/EC2.20
service-managed-aws-control-塔/V /1.0.0/EC2.21	安全控制/EC2.21
service-managed-aws-control-塔/V /1.0.0/EC2.22	安全控制/EC2.22
service-managed-aws-control-塔/V/1.0.0/ecr.1	安全性控制 /ECr.1
service-managed-aws-control-塔/V/1.0.0/ecr.2	安全控制 /ECR2
service-managed-aws-control-塔/V/1.0.0/ecr.3	安全性控制 /ECR3

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/EC.1	安全控制 /EC.1
service-managed-aws-control-塔/V /1.0.0/EC.2	安全性控制/EC.2
service-managed-aws-control-塔/V /1.0.0/EC.3	安全控制 /EC.3
service-managed-aws-control-塔/V /1.0.0/EC.4	安全控制 /EC.4
service-managed-aws-control-塔/V /1.0.0/EC.5	安全控制 /EC.5
service-managed-aws-control-塔/V /1.0.0/EC.8	安全控制 /EC.8
service-managed-aws-control-塔/V /1.0.0/EC .10	安全控制 /EC.10
service-managed-aws-control-塔/V /1.0.0/EC .12	安全控制 /EC.12
service-managed-aws-control-塔/V /1.0.0/EPS1	安全控制
service-managed-aws-control-塔/V /1.0.0/EPS2	安全控制
service-managed-aws-control-塔/V /1.0.0/EF.3	安全控制
service-managed-aws-control-塔/V /1.0.0/EPS4	安全控制
service-managed-aws-control-塔/V /1.0.0/ek.2	安全控制/EK.2
service-managed-aws-control-塔/V /1.0.0/Elb.2	安全控制系統 (ELB.2)
service-managed-aws-control-塔/V /1.0.0/Elb.3	安全控制系統 /ELB.3
service-managed-aws-control-塔/V /1.0.0/Elb.4	安全控制系統 /ELB.4
service-managed-aws-control-塔/V /1.0.0/Elb.5	安全控制系統 /ELB.5
service-managed-aws-control-塔/V /1.0.0/Elb.6	安全控制系統 /ELB.6
service-managed-aws-control-塔/V /1.0.0/Elb.7	安全控制系統 /ELB.7

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/Elb.8	安全控制系統 /ELB.8
service-managed-aws-control-塔/V /1.0.0/Elb.9	安全控制系統 /ELB.9
service-managed-aws-control-塔/V /1.0.0/Elb.10	安全控制系統 /ELB.10
service-managed-aws-control-塔/V /1.0.0/Elb.12	安全控制系統 (ELB.12)
service-managed-aws-control-塔/V /1.0.0/Elb.13	安全控制系統 (ELB.13)
service-managed-aws-control-塔/V /1.0.0/Elb.14	安全控制系統 (ELB.14)
service-managed-aws-control-塔/V /1.0.0/易爾B2.1	安全控制系統 /ELB2.1
service-managed-aws-control-塔/V/1.0.0/emr.1	安全性控制 /EMr.1
service-managed-aws-control-塔/V /1.0.0/ES.1	安全控制 /ES.1
service-managed-aws-control-塔/V /1.0.0/ES.2	安全控制 /ES.2
service-managed-aws-control-塔/V /1.0.0/.3	安全控制 /.3
service-managed-aws-control-塔/V /1.0.0/.4	安全控制 /.4
service-managed-aws-control-塔/V /1.0.0/.5	安全性控制 /.5
service-managed-aws-control-塔/V /1.0.0/.6	安全性控制 /.6
service-managed-aws-control-塔/V /1.0.0/.7	安全性控制 /.7
service-managed-aws-control-塔/V /1.0.0/.8	安全性控制 /.8
service-managed-aws-control-塔/V /1.0.0/ElasticBeanstalk	安全控制/.1 ElasticBeanstalk

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/ ElasticBeanstalk	安全控制/.2 ElasticBeanstalk
service-managed-aws-control-塔/V /1.0.0/ GuardDuty	安全控制/.1 GuardDuty
service-managed-aws-control-塔/V /1.0.0/Iam.1	安全性控制 /IAM 1
service-managed-aws-control-塔/V /1.0.0/Iam.2	安全性控制/IAM.2
service-managed-aws-control-塔/V/1.0.0/Iam.3	安全性控制 /IAM3
service-managed-aws-control-塔/V /1.0.0/Iam.4	安全性控制/IAM.4
service-managed-aws-control-塔/V /1.0.0/Iam.5	安全性控制/IAM.5
service-managed-aws-control-塔/V /1.0.0/Iam.6	安全性控制/IAM.6
service-managed-aws-control-塔/V /1.0.0/Iam.7	安全性控制/IAM.7
service-managed-aws-control-塔/V /1.0.0/Iam.8	安全性控制/IAM.8
service-managed-aws-control-塔/V /1.0.0/亞姆 .21	安全性控制/IAM.21
service-managed-aws-control-塔樓/V /1.0.0/Ki nesis 力.1	安全控制 Kinesis 1
service-managed-aws-control-塔/V /1.0.0/公里 .1	安全性控制/KMS.1
service-managed-aws-control-塔/V /1.0.0/公里 .2	安全性控制/KMS.2
service-managed-aws-control-塔/V /1.0.0/公里 .3	安全性控制/KMS.3
service-managed-aws-control-塔/V /1.0.0/La mbda .1	安全控制/Lambda 本 1

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/Lambda 2	安全控制/Lambda 本。2
service-managed-aws-control-塔/V /1.0.0/Lambda .5	安全控制 Lambda 本 5
service-managed-aws-control-塔/V /1.0.0/NetworkFirewall	安全控制/.3 NetworkFirewall
service-managed-aws-control-塔/V /1.0.0/ .4 NetworkFirewall	安全控制 /.4 NetworkFirewall
service-managed-aws-control-塔/V /1.0.0/ .5 NetworkFirewall	安全控制 /.5 NetworkFirewall
service-managed-aws-control-塔/V /1.0.0/ .6 NetworkFirewall	安全控制 /.6 NetworkFirewall
service-managed-aws-control-塔/V/1.0.0/打開搜索.1	安全性控制/開放搜尋。1
service-managed-aws-control-塔/V/1.0.0/打開搜索.2	安全控制/開放搜尋 2
service-managed-aws-control-塔/V/1.0.0/打開搜索.3	安全性控制/開放搜尋 3
service-managed-aws-control-塔/V/1.0.0/打開搜索.4	安全控制/開放搜尋 4
service-managed-aws-control-塔/V/1.0.0/打開搜索.5	安全控制/開放搜索 .5
service-managed-aws-control-塔/V/1.0.0/打開搜索 .6	安全控制/開放搜索 .6
service-managed-aws-control-塔/V/1.0.0/打開搜索.7	安全控制/開放搜尋 .7

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V/1.0.0/打開搜索.8	安全控制/開放搜尋 .8
service-managed-aws-control-塔/V /1.0.0/R.1	安全控制 /RDS.1
service-managed-aws-control-塔/V /1.0.0/R.2	安全控制 /RDS.2
service-managed-aws-control-塔/V /1.0.0/R.3	安全控制 /RDS.3
service-managed-aws-control-塔/V /1.0.0/R.4	安全性控制/RDS.4
service-managed-aws-control-塔/V /1.0.0/R.5	安全控制 /RDS.5
service-managed-aws-control-塔/V /1.0.0/R.6	安全控制 /RDS.6
service-managed-aws-control-塔/V /1.0.0/R.8	安全性控制/RDS.8
service-managed-aws-control-塔/V /1.0.0/R.9	安全性控制/RDS.9
service-managed-aws-control-塔/V /1.0.0/R.10	安全控制 /RDS.10
service-managed-aws-control-塔/V /1.0.0/R.11	安全性控制/RDS.11
service-managed-aws-control-塔/V /1.0.0/R.13	安全性控制/RDS.13
service-managed-aws-control-塔/V /1.0.0/R.17	安全性控制/RDS.17
service-managed-aws-control-塔/V /1.0.0/R.18	安全控制/RDS.18
service-managed-aws-control-塔/V /1.0.0/R.19	安全性控制/RDS.19
service-managed-aws-control-塔/V /1.0.0/R.20	安全控制/RDS.20
service-managed-aws-control-塔/V /1.0.0/R.21	安全控制/RDS.21
service-managed-aws-control-塔/V /1.0.0/RDS.22	安全性控制/RDS.22
service-managed-aws-control-塔/V /1.0.0/R.23	安全性控制/RDS.23

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/R.25	安全性控制/RDS.25
service-managed-aws-control-塔樓/V/1.0.0/Redshift .1	安全控制/Redshift 1
service-managed-aws-control-塔/V /1.0.0/Redshift。	安全控制/Redshift 2
service-managed-aws-control-塔/V /1.0.0/Redshift .4	安全控制/Redshift 4
service-managed-aws-control-塔/V /1.0.0/Redshift .6	安全控制/Redshift。6
service-managed-aws-control-塔/V /1.0.0/Redshift .7	安全控制/Redshift。7
service-managed-aws-control-塔/V /1.0.0/Redshift .8	安全控制/Redshift。8
service-managed-aws-control-塔/V /1.0.0/Redshift .9	安全控制/Redshift 9
service-managed-aws-control-塔/V /1.0.0/S3.1	安全性控制 /S3.1
service-managed-aws-control-塔/V /1.0.0/S3.2	安全性控制 /S3.2
service-managed-aws-control-塔/V /1.0.0/S3.3	安全性控制 /S3.3
service-managed-aws-control-塔/V /1.0.0/S3.5	安全性控制 /S3.5
service-managed-aws-control-塔/V /1.0.0/S3.6	安全性控制 /S3.6
service-managed-aws-control-塔/V /1.0.0/S3.8	安全控制 /S3.8
service-managed-aws-control-塔/V /1.0.0/S3.9	安全性控制 /S3.9
service-managed-aws-control-塔/V /1.0.0/S3.10	安全控制

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/S3.11	安全性控制 /3.11
service-managed-aws-control-塔/V /1.0.0/S3.12	安全性控制
service-managed-aws-control-塔/V /1.0.0/S3.13	安全控制
service-managed-aws-control-塔/V /1.0.0/ SageMaker	安全控制/.1 SageMaker
service-managed-aws-control-塔/V /1.0.0/ SecretsManager	安全控制/.1 SecretsManager
service-managed-aws-control-塔/V /1.0.0/ SecretsManager	安全控制/.2 SecretsManager
service-managed-aws-control-塔/V /1.0.0/ SecretsManager	安全控制/.3 SecretsManager
service-managed-aws-control-塔/V /1.0.0/ .4 SecretsManager	安全控制 /.4 SecretsManager
service-managed-aws-control-塔/V /1.0.0/SN.1	安全性控制/SN.1
service-managed-aws-control-塔/V /1.0.0/sn.2	安全性控制/SN.2
service-managed-aws-control-塔/V /1.0.0/平方米	安全性控制/SQ.1
service-managed-aws-control-塔/V /1.0.0/SSM.1	安全性控制/SSM.1
service-managed-aws-control-塔/V /1.0.0/SSM.2	安全性控制/SSM.2
service-managed-aws-control-塔/V /1.0.0/SSM.3	安全性控制 /SSM3
service-managed-aws-control-塔/V/1.0.0/SSM.4	安全性控制/SSM4

開啟合併控制項發現項目之前的產生器 ID	開啟合併控制項發現項目之後的產生器 ID
service-managed-aws-control-塔/V /1.0.0/波2	安全性控制/WAF.2
service-managed-aws-control-塔/V /1.0.0/波3	安全性控制/WAF.3
service-managed-aws-control-塔/V /1.0.0/波4	安全性控制 /WAF.4

合併如何影響控制 ID 和標題

整合的控制項檢視與整合控制項發現結果可將控制項 ID 和標題標準化。安全控制 ID 和安全控制標題是指這些與標準無關的值。下表顯示安全控制 ID 和標題與標準特定控制 ID 和標題的對應。屬於 AWS 基礎安全性最佳作法 (FSBP) 標準之控制項的 ID 和標題會保持不變。

無論帳戶中的合併控制項發現項目是開啟還是關閉，Security Hub 主控台都會顯示安全控制 ID 和安全控制標題。不過，只有在帳戶中開啟合併控制項發現項目時，Security Hub 發現項目才會包含安全性控制 ID 和安全控制標題。如果帳戶中已關閉合併控制項發現項目，Security Hub 發現項目會包含特定於標準的控制 ID 和標題。如需合併如何影響控制項發現項目的詳細資訊，請參閱樣本控制結果。

對於屬於服務管理標準一部分的控制項： AWS Control Tower，當合併的控制項發現項目開啟時，會從發現項目的控制項 ID 和標題中移除前置詞CT.。

若要在此表格上執行您自己的指令碼，請將其下載為 .csv 檔案。

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	1.1 避免使用根用戶	[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報
CIS v1.2.0	1.1 避免使用根用戶	[IAM.20] 避免使用根用戶
CIS v1.2.0	1.10 確保 IAM 密碼政策防止密碼重複使用	[IAM.16] 確保 IAM 密碼政策防止密碼重複使用
CIS v1.2.0	1.11 確保 IAM 密碼政策在 90 天或更短的時間內過期	[IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期
CIS v1.2.0	1.12 確保根用戶訪問密鑰不存在	[IAM.4] IAM 根使用者存取金鑰不應存在

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	1.13 確定已為根使用者啟用 MFA	[IAM.9] 應該為根用戶啟用 MFA
CIS v1.2.0	1.14 確定已為根使用者啟用硬體 MFA	[IAM.6] 應為根使用者啟用硬體 MFA
CIS v1.2.0	1.16 確保 IAM 政策僅附加到群組或角色	[IAM.2] IAM 使用者不應附加 IAM 政策
CIS v1.2.0	1.2 確保為擁有主控台密碼的所有 IAM 使用者啟用多因素身份驗證 (MFA)	[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
CIS v1.2.0	1.20 確保已建立支援角色來管理事件 AWS Support	[IAM.18] 確保已建立支援角色來管理事件 AWS Support
CIS v1.2.0	1.22 確保未建立允許完整「*: *」管理權限的 IAM 政策	[IAM.1] IAM 政策不應允許完整的「*」管理特權
CIS v1.2.0	1.3 確定停用 90 天 (含) 以上未使用的登入資料	[IAM.8] 應移除未使用的 IAM 使用者登入資料
CIS v1.2.0	1.4 確保每 90 天或更短期限輪換存取金鑰	[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
CIS v1.2.0	1.5 確保 IAM 密碼政策至少需要一個大寫字母	[IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母
CIS v1.2.0	1.6 確保 IAM 密碼政策至少需要一個小寫字母	[IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母
CIS v1.2.0	1.7 確保 IAM 密碼政策至少需要一個符號	[IAM.13] 確保 IAM 密碼政策至少需要一個符號
CIS v1.2.0	1.8 確保 IAM 密碼政策至少需要一個數字	[IAM.14] 確保 IAM 密碼政策至少需要一個數字
CIS v1.2.0	1.9 確保 IAM 密碼政策的密碼長度下限為 14 或更高	[IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	2.1 確保 CloudTrail 所有區域均啟用	[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤
CIS v1.2.0	2.2 確定已啟用 CloudTrail 記錄檔驗證	[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證
CIS v1.2.0	2.3 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取	[CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
CIS v1.2.0	2.4 確保跟 CloudTrail 踪與 CloudWatch 日誌集成	[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合
CIS v1.2.0	2.5 確保 AWS Config 已啟用	???
CIS v1.2.0	2.6 確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌	[CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌
CIS v1.2.0	2.7 確保 CloudTrail 記錄檔在靜態時使用 KMS CMK 加密	[CloudTrail.2] CloudTrail 應啟用靜態加密
CIS v1.2.0	2.8 確定輪換客戶建立的 CMK	[KMS.4] AWS KMS 按鍵旋轉應該已啟用
CIS v1.2.0	2.9 確定所有 VPC 中皆已啟用 VPC 流程記錄	[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
CIS v1.2.0	3.1 確定未經授權的 API 呼叫中存在日誌指標篩選條件和警示	[CloudWatch.2] 確保未經授權的 API 調用存在日誌指標過濾器和警報
CIS v1.2.0	3.10 確定安全群組變更存在日誌指標篩選條件和警示	[CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	3.11 確定網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示	[CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示
CIS v1.2.0	3.12 確定網路閘道變更存在日誌指標篩選條件和警示	[CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示
CIS v1.2.0	3.13 確定路由表變更存在日誌指標篩選條件和警示	[CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報
CIS v1.2.0	3.14 確定 VPC 變更存在日誌指標篩選條件和警示	[CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報
CIS v1.2.0	3.2 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報	[CloudWatch.3] 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報
CIS v1.2.0	3.3 確保針對 root 用戶的使用存在日誌指標過濾器和警報	[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報
CIS v1.2.0	3.4 確定存在 IAM 政策變更的記錄指標篩選器和警示	[CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報
CIS v1.2.0	3.5 確保存在 CloudTrail 配置變更的日誌指標過濾器和警報	[CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報
CIS v1.2.0	3.6 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報	[CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報
CIS v1.2.0	3.7 確定停用或排定刪除客戶建立的 CMK，存在日誌指標篩選條件和警示	[CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰
CIS v1.2.0	3.8 確定 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	[CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	3.9 確保存在 AWS Config 配置更改的日誌指標過濾器和警報	[CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報
CIS v1.2.0	4.1 確保無安全群組允許從 0.0.0.0/0 輸入連接埠 22	[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
CIS v1.2.0	4.2 確保無安全群組允許從 0.0.0.0/0 輸入連接埠 3389	[EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
CIS v1.2.0	4.3 確保每個 VPC 的預設安全群組都會限制所有流量	[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
独联体	1.10 確保為擁有主控台密碼的所有 IAM 使用者啟用多因素身份驗證 (MFA)	[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
独联体	1.14 確保每 90 天或更短時間旋轉一次存取金鑰	[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
独联体	1.16 確保未附加允許完整「*: *」管理權限的 IAM 政策	[IAM.1] IAM 政策不應允許完整的「*」管理特權
独联体	1.17 確保已建立支援角色來管理事件 AWS Support	[IAM.18] 確保已建立支援角色來管理事件 AWS Support
独联体	1.4 確定根使用者帳號存取金鑰不存在	[IAM.4] IAM 根使用者存取金鑰不應存在
独联体	1.5 確定已為根使用者帳號啟用 MFA	[IAM.9] 應該為根用戶啟用 MFA
独联体	1.6 確定已為根使用者帳戶啟用硬體 MFA	[IAM.6] 應為根使用者啟用硬體 MFA
独联体	1.7 不再使用 root 使用者進行管理和日常工作	[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

標準	標準控制項 ID 和標題	安全控制 ID 和標題
独联体	1.8 確保 IAM 密碼政策的長度下限為 14 或更高	[IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高
独联体	1.9 確保 IAM 密碼政策防止重複使用密碼	[IAM.16] 確保 IAM 密碼政策防止密碼重複使用
独联体	2.1.2 確保 S3 儲存貯體政策設定為拒絕 HTTP 請求	[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求
独联体	2.1.5.1 S3 區塊公用存取設定應該已啟用	[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
独联体	2.1.5.2 S3 區塊公開存取設定應在儲存貯體層級啟用	[S3.8] S3 通用存儲桶應阻止公共訪問
独联体	2.2.1 確定已啟用 EBS 磁碟區加密	[EC2.7] 應啟用 EBS 預設加密
独联体	2.3.1 確定已啟用 RDS 執行個體的加密	[RDS.3] RDS 資料庫執行個體應啟用靜態加密
独联体	3.1 確保 CloudTrail 所有區域均已啟用	[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤
独联体	3.2 確定已啟用 CloudTrail 記錄檔驗證	[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證
独联体	3.4 確保跟 CloudTrail 踪與 CloudWatch 日誌集成	[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合
独联体	3.5 確保 AWS Config 所有區域均已啟用	[Config 1] AWS Config 應該被啟用
独联体	3.6 確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌	[CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌

標準	標準控制項 ID 和標題	安全控制 ID 和標題
独联体	3.7 確保使用 KMS CMK 在靜態時加密 CloudTrail 記錄	[CloudTrail.2] CloudTrail 應啟用靜態加密
独联体	3.8 確定已啟用客戶建立的 CMK 輪替	[KMS.4] AWS KMS 按鍵旋轉應該已啟用
独联体	3.9 確定已在所有 VPC 中啟用虛擬私人雲端流程記錄	[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
独联体	4.4 確定存在 IAM 政策變更的記錄指標篩選器和警示	[CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報
独联体	4.5 確保存在 CloudTrail 配置更改的日誌指標過濾器和警報	[CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報
独联体	4.6 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報	[CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報
独联体	4.7 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶建立的 CMK	[CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰
独联体	4.8 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示	[CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示
独联体	4.9 確保存在 AWS Config 配置更改的日誌指標過濾器和警報	[CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報
独联体	4.10 確定安全性群組變更存在記錄指標篩選器和警示	[CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報
独联体	4.11 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示	[CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示

標準	標準控制項 ID 和標題	安全控制 ID 和標題
独联体	4.12 確定網路閘道變更存在記錄指標篩選器和警示	[CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示
独联体	4.13 確保路由表更改存在日誌指標過濾器和警報	[CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報
独联体	4.14 確定 VPC 變更存在記錄指標篩選器和警示	[CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報
独联体	5.1 確保沒有網路 ACL 允許從 0.0.0/0 輸入到遠端伺服器管理連接埠	[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
独联体	5.3 確保每個 VPC 的默認安全組限制所有流量	[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
PCI DSS v3.2.1	PCI。 AutoScaling.1 與負載平衡器關聯的自動調度資源群組應使用負載平衡器健康狀態檢	[AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
PCI DSS v3.2.1	PCI。 CloudTrail.1 CloudTrail 日誌應使用 AWS KMS CMK 進行靜態加密	[CloudTrail.2] CloudTrail 應啟用靜態加密
PCI DSS v3.2.1	PCI。 CloudTrail.2 CloudTrail 應該啟用	[CloudTrail.3] CloudTrail 應該被啟用
PCI DSS v3.2.1	PCI。 CloudTrail.3 應啟用 CloudTrail 日誌文件驗證	[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證
PCI DSS v3.2.1	PCI。 CloudTrail.4 跟 CloudTrail 踪應該與 Amazon CloudWatch 日誌集成	[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合
PCI DSS v3.2.1	PCI。 CodeBuild.1 CodeBuild GitHub 或比特桶源存儲庫網址應該使用 OAuth	[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	PCI。 CodeBuild.2 CodeBuild 項目環境變量不應包含純文本憑據	[CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
PCI DSS v3.2.1	設定 1 應該啟 AWS Config 用	[Config 1] AWS Config 應該被啟用
PCI DSS v3.2.1	PCI.CW.1 針對「root」使用者的使用，應該存在記錄度量篩選器和警示	[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service 複寫執行個體不應為公用	[DMS.1] Database Migration Service 複製執行個體不應該是公用的
PCI DSS v3.2.1	EBS 快照不應該可公開還原	[EC2.1] Amazon EBS 快照不應公開還原
PCI DSS v3.2.1	PCI.EC2.2 VPC 預設安全性群組應禁止輸入和輸出流量	[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
PCI DSS v3.2.1	應移除未使用的 EC2 EIP	[EC2.12] 應移除未使用的 Amazon EC2 EIP
PCI DSS v3.2.1	安全性群組不應允許從 0.0.0.0/0 輸入至連接埠 22	[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
PCI DSS v3.2.1	應該在所有虛擬私人雲端中啟用虛擬私人雲端流程記錄	[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
PCI DSS v3.2.1	應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS	[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
PCI DSS v3.2.1	PCI.ES.1 彈性搜尋網域應該位於 VPC 中	[ES.2] 彈性搜索域名不應公開訪問
PCI DSS v3.2.1	PCI.ES.2 彈性搜尋網域應啟用靜態加密	[ES.1] 彈性搜尋網域應啟用靜態加密

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	PCI。 GuardDuty.1 GuardDuty 應該啟用	[GuardDuty.1] GuardDuty 應該啟用
PCI DSS v3.2.1	IAM 根使用者存取金鑰不應存在	[IAM.4] IAM 根使用者存取金鑰不應存在
PCI DSS v3.2.1	身分與存取權管理使用者不應附加身分與存取權管理政策	[IAM.2] IAM 使用者不應附加 IAM 政策
PCI DSS v3.2.1	PCI.IAM.3 身分與存取權管理政策不應允許完整的「*」管理權限	[IAM.1] IAM 政策不應允許完整的「*」管理特權
PCI DSS v3.2.1	應該為根使用者啟用 PCI.IAM.4 硬體 MFA	[IAM.6] 應為根使用者啟用硬體 MFA
PCI DSS v3.2.1	應該為根使用者啟用虛擬 MFA	[IAM.9] 應該為根用戶啟用 MFA
PCI DSS v3.2.1	應為所有身分與存取權管理使用者啟用 PCI.IAM.6 MFA	[IAM.19] 應為所有 IAM 使用者啟用 MFA
PCI DSS v3.2.1	如果未在預先定義的天數內使用 PCI.IAM.7 IAM 使用者登入資料，則應停用	[IAM.8] 應移除未使用的 IAM 使用者登入資料
PCI DSS v3.2.1	適用於 IAM 使用者的 PCI.IAM.8 密碼政策應具有強式組態	[IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config
PCI DSS v3.2.1	應該啟用客戶主金鑰 (CMK) 輪換	[KMS.4] AWS KMS 按鍵旋轉應該已啟用
PCI DSS v3.2.1	Lambda 函數應該禁止公共訪問	[Lambda 1] Lambda 函數政策應該禁止公共訪問
PCI DSS v3.2.1	Lambda 函數應該位於 VPC 中	[Lambda 3] Lambda 函數應該在 VPC 中
PCI DSS v3.2.1	OpenSearch 網域應該位於虛擬私人 VPC	[打開搜索 .2] OpenSearch 域名不應該是公開訪問

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	EBS 快照不應該可公開還原	OpenSearch 網域應啟用靜態加密功能
PCI DSS v3.2.1	RDS 快照應該是私有的	[RDS.1] RDS 快照應該是私有的
PCI DSS v3.2.1	PCI.RDS.2 RDS 資料庫執行個體應該禁止公開存取	[RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI。1 Amazon Redshift 集群應禁止公共訪問	[紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
PCI DSS v3.2.1	PCI.S3.1 S3 儲存貯體應該禁止公用寫入存取	[S3.3] S3 通用存儲桶應該阻止公共寫入訪問
PCI DSS v3.2.1	PCI.S3.2 S3 儲存貯體應該禁止公用讀取存取	[S3.2] S3 通用存儲桶應該阻止公共讀取訪問
PCI DSS v3.2.1	PCI.S3.3 S3 儲存貯體應該已啟用跨區域複寫	[S3.7] S3 一般用途儲存貯體應使用跨區域複寫
PCI DSS v3.2.1	PCI.S3.5 S3 儲存貯體應該要求使用安全通訊端層	[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求
PCI DSS v3.2.1	應該啟用 PCI.S3.6 S3 區塊公開存取設定	[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
PCI DSS v3.2.1	PCI。 SageMaker.1 Amazon SageMaker 筆記本實例不應該直接訪問互聯網	[SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
PCI DSS v3.2.1	安裝修補程式後，由系統管理員管理的 PCI.SSM.1 EC2 執行個體應具有「合規」的修補程式合規狀態	[SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	由系統管理員管理的 PCI.SSM.2 EC2 執行個體應具有「合規」的關聯合規性狀態	[SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
PCI DSS v3.2.1	EC2 執行個體應由下列項目管理：AWS Systems Manager	[SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager

更新合併的工作流程

如果您的工作流程不依賴任何控制項尋找欄位的特定格式，則不需要採取任何動作。

如果您的工作流程依賴表格中註明的任何控制項尋找欄位的特定格式，您應該更新工作流程。例如，如果您建立了針對特定控制 ID 觸發動作的 Amazon E CloudWatch vents 規則 (例如，在控制項 ID 等於 CIS 2.7 時叫用 AWS Lambda 函數)，請更新規則以使用該控制項的`Compliance.SecurityControlId`欄位 CloudTrail .2。

如果您使用任何已變更的控制項尋找欄位或值建立自訂見解，請更新這些見解以使用目前的欄位或值。

售後範例

下列各節包含「 AWS 安全性搜尋結果格式」(ASFF) 中必要與選用屬性的範例，以及 ASFF 支援的每個資源範例。

主題

- 必要的頂層屬性
- 選用的頂層屬性
- Resources

必要的頂層屬性

Security Hub 中的所有發現項目都需要 AWS 安全性發現項目格式 (ASFF) 中的下列頂層屬性。如需有關這些必要屬性的詳細資訊，請參閱 AWS Security Hub API 參考AwsSecurityFinding中的。

AwsAccountId

發現項目套用的 AWS 帳戶 ID。

範例

```
"AwsAccountId": "111111111111"
```

CreatedAt

指出發現項目擷取的潛在安全性問題何時建立。

範例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub 會在最近更新 90 天後刪除發現項目，如果未發生更新，則會在建立日期後刪除 90 天。若要存放超過 90 天的發現項目，您可以在 Amazon 中設定將發現結果路由 EventBridge 到 S3 儲存貯體的規則。

描述

問題清單的描述。此欄位可以是非特定的範例文字或問題清單執行個體的特定詳細資訊。

針對 Security Hub 產生的控制項發現項目，此欄位會提供控制項的描述。

如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

範例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

產生問題清單的解決方案特定元件 (邏輯分散式單位) 識別符。

對於 Security Hub 產生的控制項發現項目，如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

範例

```
"GeneratorId": "security-control/Config.1"
```

Id

問題清單的產品特定識別符。對於 Security Hub 產生的控制項發現項目，此欄位會提供發現項目的 Amazon 資源名稱 (ARN)。

如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

範例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

由 Security Hub 產生的 Amazon 資源名稱 (ARN)，可在產品向 Security Hub 註冊後唯一識別第三方發現項目產品。

此欄位的格式為 `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*。

- 對於與 Security Hub 整合的 AWS 服務，`company-id`必須是 "aws"，而且`product-id`必須是 AWS 公用服務名稱。由於 AWS 產品和服務不與帳戶相關聯，因此 ARN 的`account-id`區段為空白。 AWS 尚未與 Security Hub 整合的服務會被視為協力廠商產品。
- 針對公有產品，`company-id` 和 `product-id` 必須是註冊時指定的 ID 值。
- 針對私有產品，`company-id` 必須是帳戶 ID。`product-id` 必須是預留的 "default" 字詞，或註冊時指定的 ID。

範例

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

資源

Resources物件會提供一組資源資料類型，用來描述發現項目所參照的 AWS 資源。

範例

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
```

```
                    "Occurrences": {
                        "Pages": [
                            {
                                "PageNumber": 1,
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                 },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
```

```
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
```

```
    "NetworkInterfaceId": "eni-e5aa89a3"
   }
   ],
   "SubnetId": "PublicSubnet",
   "Type": "i3.xlarge",
   "VirtualizationType": "hvm",
   "VpcId": "TestVPCIpv6"
  }

]
```

SchemaVersion

要格式化問題清單的結構描述版本。此欄位的值必須是 AWS識別的正式發佈版本之一。在目前版本中，「 AWS 安全性發現格式」架構版本為2018-10-08。

範例

```
"SchemaVersion": "2018-10-08"
```

嚴重性

定義發現項目的重要性。如需有關此物件的詳細資訊，請參閱 AWS Security Hub API 參考*Severity*中的。

Severity同時是尋找項目中的頂層物件，且巢狀於FindingProviderFields物件之下。

發現項目的頂層Severity物件的值應該只能由 BatchUpdateFindingsAPI 更新。

若要提供嚴重性資訊，尋找提供者應在發出 BatchImportFindingsAPI 要求FindingProviderFields時更新下方的Severity物件。
如果新發現項目的BatchImportFindings請求只提供Label或僅提供Normalized，則 Security Hub 會自動填入另一個欄位的值。 下的Product欄位FindingProviderFields已淘汰，且未填入目前的發現項目中。請改用Original欄位。

問題清單嚴重性不會將牽涉之資產或基礎資源的重要性納入考量。重要性的定義是與問題清單相關聯之資源的重要性層級。例如，與任務關鍵應用程式相關聯的資源，其重要性高於與非生產測試相關聯的資源。如果要擷取資源重要性的資訊，請使用 Criticality 欄位。

我們建議您在將搜尋結果的原生嚴重性分數轉譯為 ASFF Severity.Label 中的值時，使用下列指引。

- INFORMATIONAL— 此類別可能包括PASSEDWARNING、或NOT AVAILABLE支票或敏感資料識別的發現項目。
- LOW— 可能導致 future 妥協的結果。例如，此類別可能包括弱點、設定弱點和公開的密碼。
- MEDIUM— 表示積極的妥協，但沒有跡象表明對手完成了他們的目標的發現。例如，此類別可能包括惡意軟件活動，黑客活動和異常行為檢測。
- HIGH或 CRITICAL — 指出對手已完成其目標的發現項目，例如作用中的資料遺失或入侵，或拒絕服務。

範例

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Title

問題清單的標題。此欄位可以包含非特定的範例文字或此問題清單執行個體的特定詳細資訊。

對於控制項發現項目，此欄位會提供控制項的標題。

如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

範例

```
"Title": "AWS Config should be enabled"
```

類型

一或多個格式為 *namespace*/*category*/*classifier* 的問題清單類型，可分類問題清單。如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

Types應該只使用 BatchUpdateFindings.

尋找想要提供值的提供者Types應該使用下的Types屬性FindingProviderFields。

在下列清單中，頂層項目符號是命名空間，第二層項目符號是類別，第三層項目符號是分類器。我們建議尋找提供者使用定義的命名空間來協助排序和分組發現項目。定義的類別和分類器也可以使用，但這不是必需的。只有軟體和組態檢查命名空間有定義的分類器。

您可以定義命名空間/分類/分類器的部分路徑。例如，下列尋找項目類型都是有效的：

- TTP
- TTPs/Defense Evasion
- TTPS /防守避免/ CloudTrailStopped

下列清單中的策略、技術和程序 (TTP) 類別與 MITRE AT &CK MatrixTM 相符。「異常行為」命名空間反映了一般的異常行為，例如一般統計異常，並且不與特定的 TTP 保持一致。不過，您可使用異常行為和 TTP 問題清單類型來分類問題清單。

命名空間、類別和分類器的清單：

- 軟體和組態檢查
  - 漏洞
    - CVE
  - AWS 安全性最佳做法
    - 網路連線能力
    - 執行時間行為分析
  - 產業和法規標準
    - AWS 基礎安全性最佳做法
    - CIS 主機強化基準
    - 獨聯體 AWS 基礎基準
    - 精密信息系統
    - 雲端安全性聯盟控制
    - ISO 90001 控制
    - ISO 27001 控制
    - ISO 27017 控制
    - ISO 27018 控制
    - SOC 1
    - SOC 2
    - HIPAA 控制 (美國)
    - NIST 800-53 控制 (美國)
    - NIST CSF 控制 (美國)

    - IRAP 控制 (澳大利亞)
    - K-ISMS 控制 (韓國)
    - MTCS 控制 (新加坡)
    - FISC 控制 (日本)
    - 個人編號法案控制 (日本)
    - ENS 控制 (西班牙)
    - Cyber Essentials Plus 控制 (英國)
    - G-Cloud 控制 (英國)
    - C5 控制 (德國)
    - IT-Grundschutz 控制 (德國)
    - GDPR 控制 (歐洲)
    - TISAX 控制 (歐洲)
  - 修補管理
- TTP
  - 初始存取
  - 執行
  - Persistence
  - 權限提升
  - 防禦逃脫
  - 登入資料存取
  - 探索
  - 水平擴散
  - 收集
  - 命令和控制
- 效果
  - 資料曝光
  - 資料外洩
  - 資料銷毀
  - 拒絕服務
  - 資源耗用

- 異常行為
  - 應用程式
  - 網路流程
  - IP 地址
  - 使用者
  - VM
  - 容器
  - 無伺服器
  - 處理
  - 資料庫
  - 資料
- 敏感資料識別
  - PII
  - 密碼
  - 法律聲明
  - 金融
  - 安全
  - 商業

範例

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

指出尋找項目提供者上次更新發現項目記錄的時間。

此時間戳記會反映發現項目記錄上次或最近更新的時間。因此，它可能與時`LastObservedAt`間戳記不同，時間戳記反映事件或弱點是上次或最近觀察到的時間。

更新問題清單記錄時，您必須將此時間戳記更新為目前的時間戳記。建立搜尋結果記錄時，`CreatedAt`和`UpdatedAt`時間戳記必須相同。更新發現項目記錄之後，此欄位的值必須比其所包含的所有先前值更新。

請注意，UpdatedAt無法使用 BatchUpdateFindingsAPI 作業更新。您只能使用更新它BatchImportFindings。

範例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub 會在最近更新 90 天後刪除發現項目，如果未發生更新，則會在建立日期後刪除 90 天。若要存放超過 90 天的發現項目，您可以在 Amazon 中設定將發現結果路由 EventBridge 到 S3 儲存貯體的規則。

選用的頂層屬性

在「 AWS 安全性發現格式」(ASFF) 中，這些最上層屬性是選用的。如需有關這些屬性的詳細資訊，請參閱 AWS Security Hub API 參考AwsSecurityFinding中的。

動作

Action物件提供有關影響資源或對資源執行之動作的詳細資訊。

範例

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
```

```
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                    "GeoLocation": {
                        "Lon": 0,
                        "Lat": 0
                    },
                    "Organization": {
                        "AsnOrg": "ExampleASO",
                        "Org": "ExampleOrg",
                        "Isp": "ExampleISP",
                        "Asn": 64496
                    }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

發現項目適用的 AWS 帳戶 名稱。

範例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

產生發現項目之產品的公司名稱。對於基於控制的發現，公司是 AWS。

Security Hub 會自動為每個發現項目填入此屬性。您無法使用`BatchImportFindings`或更新它`BatchUpdateFindings`。例外情況是當您使用自訂整合時。請參閱the section called “使用自訂產品整合”。

當您使用 Security Hub 主控台依公司名稱篩選發現項目時，您可以使用此屬性。當您使用 Security Hub API 依公司名稱篩選發現項目時，您可以使用下的`aws/securityhub/CompanyName`屬性`ProductFields`。Security Hub 不會同步處理這兩個屬性。

範例

```
"CompanyName": "AWS"
```

合規

Compliance物件會提供與控制項相關的尋找詳細資訊。系統會針對從 Security Hub 控制項產生的發現項目，以及 AWS Config 傳送至 Security Hub 的發現項目傳回此屬性。

範例

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
```

```
  (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
  been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
  itself includes scenarios where Not Applicable is returned. The specific reason why
  Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

可信度

發現項目可準確識別其用於識別之行為或問題的可能性。

Confidence應該只使用 BatchUpdateFindings.

尋找想要提供值的提供者Confidence應該使用下的Confidence屬性FindingProviderFields。請參閱the section called “使用 FindingProviderFields”。

Confidence使用比率刻度以 0-100 的基礎進行得分。0 表示百分之零的信賴度，100 表示 100% 的信賴度。例如，基於網路流量統計偏差的資料洩漏偵測具有較低的信賴度，因為尚未驗證實際洩漏。

範例

```
"Confidence": 42
```

危急性

指定給與發現項目相關聯之資源的重要性層級。

Criticality只能通過調用 BatchUpdateFindingsAPI 操作進行更新。請勿使用更新此物件BatchImportFindings。

尋找想要提供值的提供者Criticality應該使用下的Criticality屬性FindingProviderFields。請參閱the section called “使用 FindingProviderFields”。

Criticality使用僅支援完整整數的比率刻度，以 0-100 為基礎進行評分。0 分表示不重要的基礎資源，100 分預留給最重要的資源。

對於每個資源，指定時請考慮下列事項Criticality：

- 受影響的資源是否包含敏感資料 (例如，含 PII 的 S3 儲存貯體)？
- 受影響的資源是否使對手能夠加深他們的訪問或擴展其功能以執行其他惡意活動（例如，受損的系統管理員帳戶）？

- 此資源是否為企業重要資產 (例如，若遭入侵可能造成重大收益損失的業務系統)？

您可使用下列準則：

- 支援關鍵任務系統或包含高度敏感資料的資源，可在 75—100 範圍內評分。
- 支持重要（但不是關鍵系統）或包含中等重要數據的資源可以在 25—74 範圍內進行評分。
- 為不重要的系統供電或包含非敏感資料的資源應在 0-24 範圍內進行評分。

範例

```
"Criticality": 99
```

FindingProviderFields

`FindingProviderFields`包括下列屬性：

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

您可以使`FindingProviderFields`用 `BatchImportFindings`API 操作進行更新。您無法使用更新它`BatchUpdateFindings`。

如需有關 Security Hub 如何處理來自`BatchImportFindings`對應頂層屬性的更新`FindingProviderFields`和更新的詳細資訊，請參閱the section called “使用 FindingProviderFields”。

範例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
```

```
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

指出第一次觀察到發現項目擷取的潛在安全性問題的時間。

此時間戳記會反映第一次發現事件或弱點的時間。因此，它可能與時間戳記不同，時間CreatedAt戳記反映建立此尋找結果記錄的時間。

此時間戳記在發現記錄的更新之間應該是不可變的，但如果確定更準確的時間戳記，則可以更新。

範例

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

指出安全發現項目產品最近發現項目所擷取的潛在安全性問題的時間。

此時間戳記會反映上次或最近發現事件或弱點的時間。因此，它可能與時UpdatedAt間戳記不同，時間戳記反映此尋找記錄上次或最近更新的時間。

您可以提供此時間戳記，但在第一次觀察時不需要此時間戳記。如果您在第一次觀察時提供此欄位，則時間戳記應與FirstObservedAt時間戳記相同。您應該更新此欄位，以在每次觀察到問題清單時，反映上次或最近觀察到的時間戳記。

範例

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

惡意

Malware 物件提供與問題清單相關的惡意程式清單。

範例

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

網路 (已停用)

Network物件提供有關發現項目的網路相關資訊。

此物件已淘汰。若要提供此資料，您可以將資料對映至中的資源Resources，或使用Action物件。

範例

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

此NetworkPath物件會提供與發現項目相關之網路路徑的相關資訊。中的每個項目
都NetworkPath代表路徑的一個元件。

範例

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
     }
]
```

注意

Note物件會指定使用者定義的附註，您可以加入至發現項目。

問題清單提供者可以提供問題清單的初始備註，但之後便無法新增備註。您只能使用更新註記BatchUpdateFindings。

範例

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

此PatchSummary物件會針對選取的相容性標準，提供執行處理的修補程式相容性狀態摘要。

範例

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

處理

Process物件會提供有關發現項目的程序相關詳細資訊。

範例：

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

指出 Security Hub 何時收到發現項目，並開始處理它。

這與CreatedAt和不同UpdatedAt，這是與尋找項目提供者與安全性問題和發現項目互動相關的必要時間戳記。ProcessedAt時間戳記會指出 Security Hub 何時開始處理尋找項目。處理完成後，發現項目會顯示在使用者的帳戶中。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

一種資料類型，其中安全發現項目產品可以包含其他解決方案特定詳細資料，這些詳細資料不屬於定義的 AWS 安全性發現

對於 Security Hub 控制項產生的發現項目，ProductFields包括控制項的相關資訊。請參閱the section called “產生及更新控制項發現項”。

此欄位不應包含多餘的資料，也不得包含與「 AWS 安全性發現格式」欄位衝突的資料。

aws/"前置詞僅代表 AWS 產品和服務的保留命名空間，不得與第三方整合的發現結果一起提交。

雖然非必要，但產品應該將欄位名稱格式化為 company-id/product-id/field-name，其中 company-id 和 product-id 符合問題清單 ProductArn 所提供的內容。

當 Security Hub 封存現有的發現項Archival目時，會使用參照的欄位。例如，當您停用控制項或標準，以及開啟或關閉合併控制項發現項目時，Security Hub 會封存現有的發現項目。

此欄位也可能包含標準的相關資訊，其中包括產生發現項目的控制項。

範例

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
```

```
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

提供產生發現項目的產品名稱。對於以控制項為基礎的發現項目，產品名稱為 Security Hub。

Security Hub 會自動為每個發現項目填入此屬性。您無法使用BatchImportFindings或更新它BatchUpdateFindings。例外情況是當您使用自訂整合時。請參閱the section called “使用自訂產品整合”。

當您使用 Security Hub 主控台依產品名稱篩選發現項目時，您可以使用此屬性。

當您使用 Security Hub API 依產品名稱篩選發現項目時，您可以使用下的aws/securityhub/ProductName屬性ProductFields。

Security Hub 不會同步處理這兩個屬性。

RecordState

提供發現項目的記錄狀態。

根據預設，會將服務一開始產生的問題清單視為 ACTIVE。

ARCHIVED 狀態表示問題清單應被隱藏看不到。封存的問題清單不會立即刪除。您可以搜尋、檢閱和報告這些項目。如果刪除關聯的資源、資源不存在或控制項已停用，Security Hub 會自動封存以控制項為基礎的發現項目。

RecordState用於尋找提供者，且只能由更新BatchImportFindings。您無法使用更新它BatchUpdateFindings。

若要追蹤調查項目的狀態，請使用Workflow而非RecordState。

如果記錄狀態從變更ARCHIVED為ACTIVE，且搜尋結果的工作流程狀態為NOTIFIED或RESOLVED，則 Security Hub 會自動將工作流程狀態設定為NEW。

範例

```
"RecordState": "ACTIVE"
```

區域

指定 AWS 區域 從中產生發現項目的位置。

Security Hub 會自動為每個發現項目填入此屬性。您無法使用BatchImportFindings或更新它BatchUpdateFindings。

範例

```
"Region": "us-west-2"
```

RelatedFindings

提供與目前發現項目相關的發現項目清單。

RelatedFindings應該只使用 BatchUpdateFindingsAPI 操作進行更新。您不應使用更新此物件BatchImportFindings。

針對BatchImportFindings要求，尋找提供者應該使用下的RelatedFindings物件FindingProviderFields。

若要檢視RelatedFindings屬性的說明，請參閱 AWS Security Hub API 參考*RelatedFinding*中的。

範例

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

修補

Remediation 物件可提供處理問題清單的建議修補步驟資訊。

範例

```
"Remediation": {
    "Recommendation": {
```

```
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

樣本

指定尋找項目是否為範例尋找項目。

```
"Sample": true
```

SourceUrl

SourceUrl物件會提供連結至有關尋找項目產品中目前發現項目之頁面的 URL。

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

ThreatIntelIndicator物件提供與發現項目相關的威脅情報詳細資訊。

範例

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

威脅

Threats物件會提供有關發現項目偵測到之安全威脅的詳細資訊。

範例

```
"Threats": [{
```

```
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

提供與發現項目相關聯的名稱-值字串配對清單。這些是新增到問題清單的自訂使用者定義欄位。這些欄位可透過您的特定組態自動產生。

尋找提供者不應將此欄位用於產品所產生的資料。相反地，尋找提供者可以將此ProductFields欄位用於未對應至任何標準「 AWS 安全性發現格式」欄位的資料。

這些欄位只能使用 BatchUpdateFindings 更新。

範例

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

提供發現的真實性。發現項目產品可以UNKNOWN為此欄位提供的值。如果發現項目產品的系統中存在有意義的類比，則發現項目產品應該為此欄位提供值。此欄位通常由使用者決定或動作在調查發現項目之後填入。

問題清單提供者可以提供此屬性的初始值，但之後便無法更新該值。您只能使用更新此屬性BatchUpdateFindings。

```
"VerificationState": "Confirmed"
```

漏洞

此Vulnerabilities物件會提供與發現項目相關聯的弱點清單。

範例

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
```

```
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

工作流程

Workflow 物件會提供關於問題清單調查狀態的相關資訊。

此欄位適用於客戶搭配補救、協調流程和票務工具使用。這不適用於問題清單提供者。

您只能使用更新Workflow欄位BatchUpdateFindings。客戶也只能從主控台進行更新。請參閱the section called “設定發現項目的工作流程狀態”。

範例

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (已退休)

此物件已淘汰，而且已由Workflow物件的Status欄位取代。

此欄位提供發現項目的工作流程狀態。問題清單產品可針對此欄位提供 NEW 值。如果問題清單產品系統中有意義的類比，問題清單產品可針對此欄位提供值。

範例

```
"WorkflowState": "NEW"
```

Resources

`Resources` 物件可提供問題清單中所涉及資源的相關資訊。

它包含多達 32 個資源對象的數組。

若要確定資源名稱的格式化方式，請參閱AWS 安全性發現格式 (ASFF) 語法。

如需每個資源物件的範例，請從下列清單中選取。

主題

- 資源屬性
- AwsAmazonMQ
- AwsApiGateway
- AwsAppSync
- AwsAthena
- AwsAutoScaling
- AwsBackup
- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks

- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge
- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

資源屬性

以下是「 AWS 安全性尋找格式」(ASFF) 中`Resources`物件的說明與範例。如需有關這些欄位的詳細資訊，請參閱 資源。

ApplicationArn

識別與發現項目相關之應用程式的 Amazon 資源名稱 (ARN)。

範例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

識別與發現項目相關的應用程式名稱。

範例

```
"ApplicationName": "SampleApp"
```

DataClassification

此DataClassification欄位提供在資源上偵測到之機密資料的相關資訊。

範例

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
```

```
                        "End": 10,
                        "StartColumn": 20
                    }
                ],
                "Pages": [],
                "Records": [],
                "Cells": []
            }
        },
        {
            "Count": 59,
            "Type": "EMAIL_ADDRESS",
            "Occurrences": {
                "Pages": [
                    {
                        "PageNumber": 1,
                        "OffsetRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                         },
                        "LineRange": {
                            "Start": 1,
                            "End": 100,
                            "StartColumn": 10
                        }
                    }
                ]
            }
        },
        {
            "Count": 2229,
            "Type": "URL",
            "Occurrences": {
               "LineRanges": [
                    {
                        "Start": 1,
                        "End": 13
                    }
               ]
            }
        },
        {
            "Count": 13826,
```

```
                    "Type": "NameDetection",
                    "Occurrences": {
                         "Records": [
                             {
                                 "RecordIndex": 1,
                                 "JsonPath": "$.ssn.value"
                             }
                         ]
                     }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
             {
                 "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                 "Name": "1712be25e7c7f53c731fe464f1c869b8",
                 "Count": 2,
             }
        ],
        "TotalCount": 2
    }
  }
}
```

詳細資訊

此Details欄位提供有關使用適當物件之單一資源的其他資訊。每個資源都必須在物件中的個別資源物件中Resources提供。

請注意，如果尋找項目大小超過 240 KB 的最大值，則會從尋找項目中移除Details物件。對於使用 AWS Config 規則的控制項發現項目，您可以在主控 AWS Config 台上檢視資源詳細資訊。

Security Hub 為其支援的資源類型提供一組可用的資源詳細資料。這些詳細資訊對應於Type物件的值。盡可能使用提供的類型。

例如，如果資源是 S3 儲存貯體，請Type將資源設定為，AwsS3Bucket並在AwsS3Bucket物件中提供資源詳細資訊。

該Other對象允許您提供自定義字段和值。您可以在下列情況下使用Other物件：

- 資源類型 (資源的值Type) 沒有對應的詳細資料物件。若要提供資源的詳細資訊，請使用Other物件。
- 資源類型的物件不包含您要填入的所有欄位。在此情況下，請使用資源類型的詳細資訊物件來填入可用欄位。使用Other物件填入不在類型特定物件中的欄位。
- 資源類型不是提供的類型之一。在此情況下，請Resource.Type將設定為Other，並使用Other物件來填入詳細資訊。

範例

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
```

```
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

給定資源類型的標識符。

對於由 Amazon AWS 資源名稱（ARN）識別的資源，這是 ARN。

對於缺少 ARN 的 AWS 資源，這是建立資源之 AWS 服務所定義的識別碼。

對於非AWS 資源，這是與資源相關聯的唯一識別碼。

範例

```
"Id": "arn:aws:s3:::example-bucket"
```

分區

資源所在的分割區。分割區是一組 AWS 區域。每個分區 AWS 帳戶 的範圍都是一個分區。

支援下列分割區：

- aws – AWS 區域
- aws-cn - 中國區域
- aws-us-gov – AWS GovCloud (US) Region

範例

```
"Partition": "aws"
```

區域

此資源所 AWS 區域 在位置的程式碼。如需區域代碼的清單，請參閱區域端點。

範例

```
"Region": "us-west-2"
```

ResourceRole

識別發現項目中資源的角色。資源可以是發現項目活動的目標，也可以是執行活動的實行者。

範例

```
"ResourceRole": "target"
```

標籤

處理尋找項目時與資源相關聯的 AWS 標籤清單。您只能針對具有關聯標籤的資源包括Tags屬性。如果資源沒有相關聯的標籤，請不要在問題清單中包含 Tags 屬性。

以下基本限制適用於標籤：

- 您只能在此欄位中提供 AWS 資源上存在的標籤。若要提供未在「 AWS 安全性發現格式」中定義的資料，請使用Other詳細資料分欄。
- 值限制為下列字元：A-Z、a-z、0-9、空格和.: + = @ _/-(連字號)。
- 值限制為最多 256 個字元的 AWS 標籤值長度。

範例

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Type

您要提供詳細資訊的資源類型。

盡可能使用提供的資源類型之一，例如 AwsEc2Instance 或 AwsS3Bucket。

如果資源類型不符合任何提供的資源類型，請將資源設定Type為Other，並使用Other詳細資訊子欄位填入詳細資訊。

支援的值會列在「資源」下。

範例

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

以下是AwsAmazonMQ資源的「 AWS 安全性發現格式」(ASFF) 範例。

AwsAmazonMQBroker

AwsAmazonMQBroker提供 Amazon MQ 代理程式的相關資訊，此代理程式是在 Amazon MQ 上執行的訊息代理程式環境。

下列範例顯示AwsAmazonMQBroker物件的 ASFF。若要檢視AwsAmazonMQBroker屬性的描述，請參閱 AWS Security Hub API 參考資料中的 AwsAmazonMQBroker。

範例

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
```

```
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

以下是AwsApiGateway資源之「 AWS 安全性搜尋結果格式」的範例。

AwsApiGatewayRestApi

該AwsApiGatewayRestApi物件包含 Amazon API Gateway 版本 1 中的 REST API 的相關資訊。

以下是「 AWS 安全性AwsApiGatewayRestApi發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsApiGatewayRestApi屬性的說明，請參閱 AWS Security Hub API 參考AwsApiGatewayRestApiDetails中的。

範例

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
```

```
}
```

AwsApiGatewayStage

該AwsApiGatewayStage物件提供有關第 1 版 Amazon API Gateway 階段的資訊。

以下是「 AWS 安全性AwsApiGatewayStage發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsApiGatewayStage屬性的說明，請參閱 AWS Security Hub API 參考AwsApiGatewayStageDetails中的。

範例

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
```

```
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayAPI

該AwsApiGatewayV2Api物件包含 Amazon API Gateway 中第 2 版 API 的相關資訊。

以下是「 AWS 安全性AwsApiGatewayV2Api發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsApiGatewayV2Api屬性的描述，請參閱 AWS Security Hub API 參考ApiDetails中的AwsApiGatewayV2。

範例

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
```

```
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGateway第二階段

`AwsApiGatewayV2Stage`包含 Amazon API Gateway 第 2 版階段的相關資訊。

以下是「 AWS 安全性`AwsApiGatewayV2Stage`發現項目格式」(ASFF) 中的發現項目範例。若要檢視`AwsApiGatewayV2Stage`屬性的描述，請參閱 AWS Security Hub API 參考StageDetails中的AwsApiGatewayV2。

範例

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
```

```
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```


AwsAppSync

以下是AwsAppSync資源的「 AWS 安全性發現格式」(ASFF) 範例。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi提供 AWS AppSync GraphQL API 的相關資訊，這是您應用程式的頂層建構。

下列範例顯示AwsAppSyncGraphQLApi物件的 ASFF。若要檢視AwsAppSyncGraphQLApi屬性的描述，請參閱 API 參考資料中的 AwsAppSyncGraphQL AWS Security Hub API。

範例

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

以下是AwsAthena資源的「 AWS 安全性發現格式」(ASFF) 範例。

AwsAthenaWorkGroup

AwsAthenaWorkGroup提供有關亞馬遜雅典娜工作組的資訊。工作群組可協助您區隔使用者、團隊、應用程式或工作負載。它還可以幫助您設置數據處理限制並跟踪成本。

下列範例顯示AwsAthenaWorkGroup物件的 ASFF。若要檢視AwsAthenaWorkGroup屬性的說明，請參閱 AWS Security Hub API 參考AwsAthenaWorkGroup中的。

範例

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

以下是AwsAutoScaling資源之「 AWS 安全性搜尋結果格式」的範例。

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup物件會提供有關自動縮放群組的詳細資訊。

以下是「 AWS 安全性AwsAutoScalingAutoScalingGroup發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsAutoScalingAutoScalingGroup屬性的說明，請參閱 AWS Security Hub API 參考AwsAutoScalingAutoScalingGroupDetails中的。

範例

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
```

```
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

`AwsAutoScalingLaunchConfiguration`物件提供有關啟動組態的詳細資訊。

以下是「 AWS 安全性`AwsAutoScalingLaunchConfiguration`發現項目格式」(ASFF) 中的發現項目範例。

若要檢視`AwsAutoScalingLaunchConfiguration`屬性的說明，請參閱 AWS Security Hub API 參考AwsAutoScalingLaunchConfigurationDetails中的。

範例

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
```

```
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
```

```
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

以下是AwsBackup資源之「 AWS 安全性搜尋結果格式」的範例。

AwsBackupBackupPlan

AwsBackupBackupPlan物件提供 AWS Backup 備份計畫的相關資訊。 AWS Backup 備份計畫是一種原則運算式，可定義您要備份 AWS 資源的時間和方式。

下列範例顯示AwsBackupBackupPlan物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsBackupBackupPlan屬性的說明，請參閱 AWS Security Hub API 參考AwsBackupBackupPlan中的。

範例

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
```

```
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

`AwsBackupBackupVault`物件提供有關 AWS Backup 備份儲存庫的資訊。 AWS Backup 備份保管庫是儲存和組織備份的容器。

下列範例顯示`AwsBackupBackupVault`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsBackupBackupVault`屬性的說明，請參閱 AWS Security Hub API 參考[AwsBackupBackupVault](#)中的。

範例

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

此`AwsBackupRecoveryPoint`物件提供 AWS Backup 備份的相關資訊，也稱為復原點。 AWS Backup 復原點代表指定時間內資源的內容。

下列範例顯示`AwsBackupRecoveryPoint`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsBackupBackupVault`屬性的說明，請參閱 AWS Security Hub API 參考[AwsBackupRecoveryPoint](#)中的。

範例

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

AwsCertificateManager

以下是AwsCertificateManager資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCertificateManagerCertificate

AwsCertificateManagerCertificate物件提供有關 AWS Certificate Manager (ACM) 憑證的詳細資訊。

以下是「 AWS 安全性AwsCertificateManagerCertificate發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsCertificateManagerCertificate屬性的說明，請參閱 AWS Security Hub API 參考AwsCertificateManagerCertificateDetails中的。

範例

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
```

```
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
```

```
}
```

AwsCloudFormation

以下是AwsCloudFormation資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCloudFormationStack

該AwsCloudFormationStack對象提供有關嵌套為頂層模板中資源的 AWS CloudFormation 堆棧的詳細信息。

下列範例顯示AwsCloudFormationStack物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsCloudFormationStack屬性的說明，請參閱 AWS Security Hub API 參考AwsCloudFormationStackDetails中的。

範例

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
```

```
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

以下是AwsCloudFront資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCloudFrontDistribution

該AwsCloudFrontDistribution物件提供有關 Amazon CloudFront 分發組態的詳細資訊。

以下是「 AWS 安全性AwsCloudFrontDistribution發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsCloudFrontDistribution屬性的說明，請參閱 AWS Security Hub API 參考AwsCloudFrontDistributionDetails中的。

範例

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
```

```
                            200,
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
                }
            }
        ]
    },
    "Origins": {
        "Items": [
            {
                "CustomOriginConfig": {
                    "HttpPort": 80,
                    "HttpsPort": 443,
                    "OriginKeepaliveTimeout": 60,
                    "OriginProtocolPolicy": "match-viewer",
                    "OriginReadTimeout": 30,
                    "OriginSslProtocols": {
                      "Items": ["SSLv3", "TLSv1"],
                      "Quantity": 2
                    }
                }
            },
        ]
    },
                "DomainName": "my-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
        ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
           "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
           "Certificate": "ASCAJRRE5XYF52TKRY5M4",
           "CertificateSource": "iam",
           "CloudFrontDefaultCertificate": true,
           "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
           "MinimumProtocolVersion": "TLSv1.2_2021",
```

```
            "SslSupportMethod": "sni-only"
        },
        "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

以下是AwsCloudTrail資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCloudTrailTrail

AwsCloudTrailTrail物件會提供有關 AWS CloudTrail 追蹤的詳細資訊。

以下是「 AWS 安全性AwsCloudTrailTrail發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsCloudTrailTrail屬性的說明，請參閱 AWS Security Hub API 參考AwsCloudTrailTrailDetails中的。

範例

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch

以下是AwsCloudWatch資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCloudWatchAlarm

該AwsCloudWatchAlarm物件提供有關 Amazon CloudWatch 警示的詳細資訊，這些警示會在警示變更狀態時觀察指標或執行動作。

下列範例顯示AwsCloudWatchAlarm物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsCloudWatchAlarm屬性的說明，請參閱 AWS Security Hub API 參考AwsCloudWatchAlarmDetails中的。

範例

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
```

```
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

以下是AwsCodeBuild資源之「 AWS 安全性搜尋結果格式」的範例。

AwsCodeBuildProject

AwsCodeBuildProject 物件提供了 AWS CodeBuild 專案的資訊。

以下是「 AWS 安全性AwsCodeBuildProject發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsCodeBuildProject屬性的說明，請參閱 AWS Security Hub API 參考AwsCodeBuildProjectDetails中的。

範例

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
```

```
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
       "Certificate": "string",
       "EnvironmentVariables": [
            {
                 "Name": "string",
                 "Type": "string",
                 "Value": "string"
            }
       ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
    },
    "LogsConfig": {
         "CloudWatchLogs": {
              "GroupName": "string",
              "Status": "string",
              "StreamName": "string"
         },
         "S3Logs": {
              "EncryptionDisabled": boolean,
              "Location": "string",
              "Status": "string"
         }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
    },
    "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
    }
```

```
}
```

AwsDms

以下是AwsDms資源之「 AWS 安全性搜尋結果格式」的範例。

AwsDmsEndpoint

AwsDmsEndpoint物件提供 AWS Database Migration Service (AWS DMS) 端點的相關資訊。端點提供有關資料存放區的連線、資料存放區類型和位置資訊。

下列範例顯示AwsDmsEndpoint物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsDmsEndpoint屬性的說明，請參閱 AWS Security Hub API 參考AwsDmsEndpointDetails中的。

範例

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

此AwsDmsReplicationInstance物件提供 AWS Database Migration Service (AWS DMS) 複製執行個體的相關資訊。DMS 會使用複寫執行個體連線至來源資料倉庫、讀取來源資料，以及格式化資料以供目標資料倉庫使用。

下列範例顯示AwsDmsReplicationInstance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsDmsReplicationInstance屬性的說明，請參閱 AWS Security Hub API 參考AwsDmsReplicationInstanceDetails中的。

範例

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

AwsDmsReplicationTask物件提供 AWS Database Migration Service (AWS DMS) 複製工作的相關資訊。複寫工作會將一組資料從來源端點移至目標端點。

下列範例顯示AwsDmsReplicationInstance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsDmsReplicationInstance屬性的說明，請參閱 AWS Security Hub API 參考AwsDmsReplicationInstance中的。

範例

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
```

```
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
```

```
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

以下是AwsDynamoDB資源之「 AWS 安全性搜尋結果格式」的範例。

AwsDynamoDbTable

此AwsDynamoDbTable物件提供有關亞馬遜動態資料表的詳細資訊。

以下是「 AWS 安全性AwsDynamoDbTable發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsDynamoDbTable屬性的說明，請參閱 AWS Security Hub API 參考AwsDynamoDbTableDetails中的。

範例

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
```

```
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
   ],
   "GlobalTableVersion": "V1",
   "ItemCount": 2705,
   "KeySchema": [
```

```
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
    ],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
```

```
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

以下是AwsEc2資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEc2ClientVpnEndpoint

AwsEc2ClientVpnEndpoint物件提供有關 AWS Client VPN 端點的資訊。Client VPN 端點是您建立和設定以啟用和管理用戶端 VPN 工作階段的資源。它是所有用户端 VPN 工作階段的終止點。

下列範例顯示AwsEc2ClientVpnEndpoint物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2ClientVpnEndpoint屬性的描述，請參閱 AWS Security Hub API 參考 ClientVpnEndpointDetails中的 AwsEc2。

範例

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

此AwsEc2Eip物件提供有關彈性 IP 位址的資訊。

下列範例顯示AwsEc2Eip物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2Eip屬性的描述，請參閱 AWS Security Hub API 參考EipDetails中的 AwsEc2。

範例

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

該AwsEc2Instance物件提供有關 Amazon EC2 執行個體的詳細資訊。

下列範例顯示AwsEc2Instance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2Instance屬性的描述，請參閱 AWS Security Hub API 參考InstanceDetails中的 AwsEc2。

範例

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
```

```
          "NetworkInterfaceId": "eni-e5aa89a3"
       }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

該AwsEc2LaunchTemplate物件包含指定執行個體組態資訊之 Amazon 彈性運算雲端啟動範本的詳細資訊。

下列範例顯示AwsEc2LaunchTemplate物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2LaunchTemplate屬性的描述，請參閱 AWS Security Hub API 參考 LaunchTemplateDetails中的 AwsEc2。

範例

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
```

```
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

該AwsEc2NetworkAcl物件包含有關 Amazon EC2 網路存取控制清單 (ACL) 的詳細資料。

下列範例顯示AwsEc2NetworkAcl物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2NetworkAcl屬性的描述，請參閱 AWS Security Hub API 參考NetworkAclDetails中的AwsEc2。

範例

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
```

```
        "RuleAction": "allow",
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

該AwsEc2NetworkInterface物件提供有關 Amazon EC2 網路界面的資訊。

下列範例顯示AwsEc2NetworkInterface物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2NetworkInterface屬性的描述，請參閱 AWS Security Hub API 參考NetworkInterfaceDetails中的 AwsEc2。

範例

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

該AwsEc2RouteTable物件提供有關 Amazon EC2 路由表的資訊。

下列範例顯示AwsEc2RouteTable物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2RouteTable屬性的描述，請參閱 AWS Security Hub API 參考RouteTableDetails中的 AwsEc2。

範例

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

該`AwsEc2SecurityGroup`物件描述了一個 Amazon EC2 安全群組。

下列範例顯示`AwsEc2SecurityGroup`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsEc2SecurityGroup`屬性的描述，請參閱 AWS Security Hub API 參考SecurityGroupDetails中的 AwsEc2。

範例

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
```

```
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

該AwsEc2Subnet物件提供 Amazon EC2 中子網路的相關資訊。

下列範例顯示AwsEc2Subnet物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2Subnet屬性的描述，請參閱 AWS Security Hub API 參考SubnetDetails中的 AwsEc2。

範例

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
```

```
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

此AwsEc2TransitGateway物件提供 Amazon EC2 傳輸閘道的詳細資訊，該閘道會互連虛擬私有雲端 (VPC) 和現場部署網路。

以下是「 AWS 安全性AwsEc2TransitGateway發現項目格式」(ASFF) 中的發現項目範例。若要檢視AwsEc2TransitGateway屬性的描述，請參閱 AWS Security Hub API 參考 TransitGatewayDetails中的 AwsEc2。

範例

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

該AwsEc2Volume物件提供有關 Amazon EC2 磁碟區的詳細資訊。

下列範例顯示AwsEc2Volume物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2Volume屬性的描述，請參閱 AWS Security Hub API 參考VolumeDetails中的 AwsEc2。

範例

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

該AwsEc2Vpc物件提供有關 Amazon EC2 VPC 的詳細資訊。

下列範例顯示AwsEc2Vpc物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2Vpc屬性的描述，請參閱 AWS Security Hub API 參考VpcDetails中的 AwsEc2。

範例

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
```

```
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

`AwsEc2VpcEndpointService`物件包含 VPC 端點服務之服務組態的詳細資料。

下列範例顯示`AwsEc2VpcEndpointService`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsEc2VpcEndpointService`屬性的描述，請參閱 AWS Security Hub API 參考 VpcEndpointServiceDetails中的 AwsEc2。

範例

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
```

```
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

此AwsEc2VpcPeeringConnection物件提供有關兩個 VPC 之間網路連線的詳細資訊。

下列範例顯示AwsEc2VpcPeeringConnection物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2VpcPeeringConnection屬性的描述，請參閱 AWS Security Hub API 參考 VpcPeeringConnectionDetails中的 AwsEc2。

範例

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
```

```
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEc2VpnConnection

該AwsEc2VpnConnection物件提供有關 Amazon EC2 VPN 連接的詳細資訊。

下列範例顯示AwsEc2VpnConnection物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEc2VpnConnection屬性的描述，請參閱 AWS Security Hub API 參考 VpnConnectionDetails中的 AwsEc2。

範例

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
```

```
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
   }
}
```

AwsEcr

以下是AwsEcr資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEcrContainerImage

該AwsEcrContainerImage物件提供有關 Amazon ECR 映像的資訊。

下列範例顯示AwsEcrContainerImage物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEcrContainerImage屬性的說明，請參閱 AWS Security Hub API 參考AwsEcrContainerImageDetails中的。

範例

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

此AwsEcrRepository物件提供 Amazon 彈性容器登錄存放庫的相關資訊。

下列範例顯示AwsEcrRepository物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEcrRepository屬性的說明，請參閱 AWS Security Hub API 參考AwsEcrRepositoryDetails中的。

範例

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

以下是AwsEcs資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEcsCluster

該AwsEcsCluster物件提供有關 Amazon 彈性容器服務叢集的詳細資訊。

下列範例顯示AwsEcsCluster物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEcsCluster屬性的說明，請參閱 AWS Security Hub API 參考AwsEcsClusterDetails中的。

範例

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

該AwsEcsContainer對象包含有關 Amazon ECS 容器的詳細信息。

下列範例顯示AwsEcsContainer物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEcsContainer屬性的說明，請參閱 AWS Security Hub API 參考AwsEcsContainerDetails中的。

範例

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

該`AwsEcsService`物件提供 Amazon ECS 叢集中服務的詳細資訊。

下列範例顯示`AwsEcsService`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsEcsService`屬性的說明，請參閱 AWS Security Hub API 參考AwsEcsServiceDetails中的。

範例

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
```

```
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
```

```
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

該AwsEcsTask物件提供有關 Amazon ECS 任務的詳細資訊。

下列範例顯示AwsEcsTask物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEcsTask屬性的說明，請參閱 AWS Security Hub API 參考AwsEcsTask中的。

範例

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
```

```
  }
}
```

AwsEcsTaskDefinition

`AwsEcsTaskDefinition`物件包含有關任務定義的詳細資訊。任務定義描述 Amazon 彈性容器服務任務的容器和磁碟區定義。

下列範例顯示`AwsEcsTaskDefinition`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsEcsTaskDefinition`屬性的說明，請參閱 AWS Security Hub API 參考[AwsEcsTaskDefinitionDetails](#)中的。

範例

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
```

```
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

以下是AwsEfs資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEfsAccessPoint

該AwsEfsAccessPoint物件提供有關存放在 Amazon 彈性檔案系統中的檔案的詳細資訊。

下列範例顯示AwsEfsAccessPoint物件的「 AWS 安全性發現格式」(ASFF)。
若要檢視AwsEfsAccessPoint屬性的說明，請參閱 AWS Security Hub API 參考AwsEfsAccessPointDetails中的。

範例

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
```

```
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

以下是AwsEks資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEksCluster

該AwsEksCluster物件提供有關 Amazon EKS 叢集的詳細資訊。

下列範例顯示AwsEksCluster物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEksCluster屬性的說明，請參閱 AWS Security Hub API 參考AwsEksClusterDetails中的。

範例

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
```

```
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

以下是AwsElasticBeanstalk資源之「 AWS 安全性搜尋結果格式」的範例。

AwsElasticBeanstalkEnvironment

該AwsElasticBeanstalkEnvironment對象包含有關 AWS Elastic Beanstalk 環境的詳細信息。

下列範例顯示AwsElasticBeanstalkEnvironment物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsElasticBeanstalkEnvironment屬性的說明，請參閱 AWS Security Hub API 參考AwsElasticBeanstalkEnvironmentDetails中的。

範例

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
```

```
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

以下是AwsElasticSearch資源之「 AWS 安全性搜尋結果格式」的範例。

AwsElasticSearchDomain

該AwsElasticSearchDomain對象提供有關 Amazon OpenSearch 服務域的詳細信息。

下列範例顯示AwsElasticSearchDomain物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsElasticSearchDomain屬性的說明，請參閱 AWS Security Hub API 參考AwsElasticSearchDomainDetails中的。

範例

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
```

```
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           }
    },
    "NodeToNodeEncryptionOptions": {
           "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
           "AutomatedUpdateDate": "string",
           "Cancellable": boolean,
           "CurrentVersion": "string",
           "Description": "string",
           "NewVersion": "string",
           "UpdateAvailable": boolean,
           "UpdateStatus": "string"
    },
    "VPCOptions": {
           "AvailabilityZones": [
                 "string"
           ],
           "SecurityGroupIds": [
                 "string"
           ],
           "SubnetIds": [
                 "string"
           ],
          "VPCId": "string"
    }
}
```

AwsElb

以下是AwsElb資源之「 AWS 安全性搜尋結果格式」的範例。

AwsElbLoadBalancer

`AwsElbLoadBalancer`物件包含有關 Classic Load Balancer 的詳細資訊。

下列範例顯示`AwsElbLoadBalancer`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsElbLoadBalancer`屬性的說明，請參閱 AWS Security Hub API 參考[AwsElbLoadBalancerDetails](#)中的。

範例

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
```

```
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
```

```
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

`AwsElbv2LoadBalancer` 物件提供了負載平衡器的資訊。

下列範例顯示`AwsElbv2LoadBalancer`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsElbv2LoadBalancer`屬性的描述，請參閱 AWS Security Hub API 參考LoadBalancerDetails中的 AwsElbv2。

範例

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
```

```
                    "Code": "string",
                    "Reason": "string"
                },
                "Type": "string",
                "VpcId": "string"
            }
```

AwsEventBridge

以下是AwsEventBridge資源之「 AWS 安全性搜尋結果格式」的範例。

AwsEventSchemasRegistry

該AwsEventSchemasRegistry物件提供有關 Amazon EventBridge 結構描述登錄的資訊。結構描述定義傳送至的事件結構 EventBridge。結構描述登錄是收集結構描述並以邏輯方式分組的容器。

下列範例顯示AwsEventSchemasRegistry物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEventSchemasRegistry屬性的說明，請參閱 AWS Security Hub API 參考AwsEventSchemasRegistry中的。

範例

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

該AwsEventsEndpoint物件提供有關 Amazon EventBridge 全球端點的資訊。端點可以通過使其具有區域容錯來提高應用程序的可用性。

下列範例顯示AwsEventsEndpoint物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEventsEndpoint屬性的說明，請參閱 AWS Security Hub API 參考AwsEventsEndpointDetails中的。

範例

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
```

```
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

該AwsEventsEventbus物件提供有關 Amazon EventBridge 全球端點的資訊。端點可以通過使其具有區域容錯來提高應用程序的可用性。

下列範例顯示AwsEventsEventbus物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsEventsEventbus屬性的說明，請參閱 AWS Security Hub API 參考AwsEventsEventbusDetails中的。

範例

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
```

```
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

以下是AwsGuardDuty資源之「 AWS 安全性搜尋結果格式」的範例。

AwsGuardDutyDetector

該AwsGuardDutyDetector對象提供有關 Amazon GuardDuty 檢測器的信息。檢測器是代表 GuardDuty 服務的對象。需要一個檢測器才 GuardDuty 能成為可操作。

下列範例顯示AwsGuardDutyDetector物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsGuardDutyDetector屬性的說明，請參閱 AWS Security Hub API 參考AwsGuardDutyDetector中的。

範例

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
```

```
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

以下是AwsIam資源之「 AWS 安全性搜尋結果格式」的範例。

AwsIamAccessKey

AwsIamAccessKey物件包含與發現項目相關的 IAM 存取金鑰的詳細資料。

下列範例顯示AwsIamAccessKey物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsIamAccessKey屬性的說明，請參閱 AWS Security Hub API 參考AwsIamAccessKeyDetails中的。

範例

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
```

```
                            "MfaAuthenticated": boolean
                        },
                        "SessionIssuer": {
                            "AccountId": "string",
                            "Arn": "string",
                            "PrincipalId": "string",
                            "Type": "string",
                            "UserName": "string"
                        }
                    },
                    "Status": "string"
                }
```

AwsIamGroup

`AwsIamGroup`物件包含 IAM 群組的詳細資料。

下列範例顯示`AwsIamGroup`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsIamGroup`屬性的說明，請參閱 AWS Security Hub API 參考[AwsIamGroupDetails](#)中的。

範例

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

該`AwsIamPolicy`物件代表 IAM 許可政策。

下列範例顯示AwsIamPolicy物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsIamPolicy屬性的說明，請參閱 AWS Security Hub API 參考AwsIamPolicyDetails中的。

範例

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

AwsIamRole物件包含 IAM 角色的相關資訊，包括所有角色的政策。

下列範例顯示AwsIamRole物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsIamRole屬性的說明，請參閱 AWS Security Hub API 參考AwsIamRoleDetails中的。

範例

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
```

```
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

該AwsIamUser對象提供有關用戶的信息。

下列範例顯示AwsIamUser物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsIamUser屬性的說明，請參閱 AWS Security Hub API 參考AwsIamUserDetails中的。

範例

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

以下是AwsKinesis資源之「 AWS 安全性搜尋結果格式」的範例。

AwsKinesisStream

該AwsKinesisStream物件提供有關 Amazon Kinesis Data Streams 訊。

下列範例顯示AwsKinesisStream物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsKinesisStream屬性的說明，請參閱 AWS Security Hub API 參考AwsKinesisStreamDetails中的。

範例

```
"AwsKinesisStream": {
```

```
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

以下是AwsKms資源之「 AWS 安全性搜尋結果格式」的範例。

AwsKmsKey

物AwsKmsKey件提供有關 AWS KMS key.

下列範例顯示AwsKmsKey物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsKmsKey屬性的說明，請參閱 AWS Security Hub API 參考AwsKmsKeyDetails中的。

範例

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

以下是AwsLambda資源之「 AWS 安全性搜尋結果格式」的範例。

AwsLambdaFunction

此AwsLambdaFunction物件提供有關 Lambda 函數組態的詳細資訊。

下列範例顯示AwsLambdaFunction物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsLambdaFunction屬性的說明，請參閱 AWS Security Hub API 參考AwsLambdaFunctionDetails中的。

範例

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
```

```
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

此AwsLambdaLayerVersion物件提供有關 Lambda 圖層版本的詳細資訊。

下列範例顯示AwsLambdaLayerVersion物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsLambdaLayerVersion屬性的說明，請參閱 AWS Security Hub API 參考AwsLambdaLayerVersionDetails中的。

範例

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

以下是AwsMsk資源之「 AWS 安全性搜尋結果格式」的範例。

AwsMskCluster

該AwsMskCluster物件提供有關阿帕奇卡夫卡 (Amazon MSK) 叢集的 Amazon 受管串流的資訊。

下列範例顯示AwsMskCluster物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsMskCluster屬性的說明，請參閱 AWS Security Hub API 參考AwsMskClusterDetails中的。

範例

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

以下是`AwsNetworkFirewall`資源之「 AWS 安全性搜尋結果格式」的範例。

AwsNetworkFirewallFirewall

`AwsNetworkFirewallFirewall`物件包含有關 AWS Network Firewall 防火牆的詳細資訊。

下列範例顯示AwsNetworkFirewallFirewall物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsNetworkFirewallFirewall屬性的說明，請參閱 AWS Security Hub API 參考AwsNetworkFirewallFirewallDetails中的。

範例

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

AwsNetworkFirewallFirewallPolicy物件提供有關防火牆策略的詳細資訊。防火牆策略定義網路防火牆的行為。

下列範例顯示AwsNetworkFirewallFirewallPolicy物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsNetworkFirewallFirewallPolicy屬性的說明，請參閱 AWS Security Hub API 參考AwsNetworkFirewallFirewallPolicyDetails中的。

範例

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
```

```
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
         }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

AwsNetworkFirewallRuleGroup物件提供有關 AWS Network Firewall 規則群組的詳細資訊。規則群組用於檢查和控制網路流量。無狀態規則群組適用於個別封包。可設定狀態規則群組會套用至其流量環境中的封包。

防火牆策略中參照規則群組。

下列範例顯示AwsNetworkFirewallRuleGroup物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsNetworkFirewallRuleGroup屬性的說明，請參閱 AWS Security Hub API 參考AwsNetworkFirewallRuleGroupDetails中的。

範例 — 無狀態規則群組

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
```

```
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
```

```
}
```

範例 — 可設定狀態規則群組

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
                         "Direction": "ANY",
                         "Protocol": "TCP",
                         "Source": "Any",
                         "SourcePort": "Any"
                     },
                     "RuleOptions": [
                         {
                            "Keyword": "sid:1"
                         }
                     ]
                 }
             ]
         }
    }
}
```

以下是AwsNetworkFirewallRuleGroup屬性的有效值範例清單：

- Action

  有效值：PASS | DROP | ALERT

- Protocol

有效值：IPTCPUDPICMP| HTTP | FTP | TLS SMB | DNS | DCERPC | SSH SMTP | IMAP | MSN | KRB5 IKEV2 | TFTP | NTP | DHCP

- Flags

  有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

  有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService

以下是AwsOpenSearchService資源之「 AWS 安全性搜尋結果格式」的範例。

AwsOpenSearchServiceDomain

該AwsOpenSearchServiceDomain對象包含有關 Amazon OpenSearch 服務域的信息。

下列範例顯示AwsOpenSearchServiceDomain物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsOpenSearchServiceDomain屬性的說明，請參閱 AWS Security Hub API 參考AwsOpenSearchServiceDomainDetails中的。

範例

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
```

```
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
```

```
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

以下是AwsRds資源之「 AWS 安全性搜尋結果格式」的範例。

AwsRdsDbCluster

該AwsRdsDbCluster物件提供有關 Amazon RDS 資料庫叢集的詳細資訊。

下列範例顯示AwsRdsDbCluster物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsDbCluster屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsDbClusterDetails中的。

範例

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
```

```
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
```

```
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

AwsRdsDbClusterSnapshot物件包含 Amazon RDS 資料庫叢集快照的相關資訊。

下列範例顯示AwsRdsDbClusterSnapshot物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsDbClusterSnapshot屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsDbClusterSnapshotDetails中的。

範例

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
```

```
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

此AwsRdsDbInstance物件提供有關 Amazon RDS 資料庫執行個體的詳細資訊。

下列範例顯示AwsRdsDbInstance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsDbInstance屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsDbInstanceDetails中的。

範例

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
```

```
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
```

```
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
```

```
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

AwsRdsDbSecurityGroup物件包含 Amazon 關聯式資料庫服務的相關資訊

下列範例顯示AwsRdsDbSecurityGroup物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsDbSecurityGroup屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsDbSecurityGroupDetails中的。

範例

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
```

```
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

AwsRdsDbSnapshot物件包含有關 Amazon RDS 資料庫叢集快照的詳細資訊。

下列範例顯示AwsRdsDbSnapshot物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsDbSnapshot屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsDbSnapshotDetails中的。

範例

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
```

```
}
```

AwsRdsEventSubscription

AwsRdsEventSubscription包含 RDS 事件通知訂閱的詳細資料。訂閱允許 RDS 將事件發佈到 SNS 主題。

下列範例顯示AwsRdsEventSubscription物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRdsEventSubscription屬性的說明，請參閱 AWS Security Hub API 參考AwsRdsEventSubscriptionDetails中的。

範例

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

以下是AwsRedshift資源之「 AWS 安全性搜尋結果格式」的範例。

AwsRedshiftCluster

該AwsRedshiftCluster物件包含有關 Amazon Redshift 叢集的詳細資料。

下列範例顯示AwsRedshiftCluster物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRedshiftCluster屬性的說明，請參閱 AWS Security Hub API 參考AwsRedshiftClusterDetails中的。

範例

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
```

```
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
```

```
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
```

```
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53

以下是AwsRoute53資源之「 AWS 安全性搜尋結果格式」的範例。

AwsRoute53HostedZone

此AwsRoute53HostedZone物件提供 Amazon Route 53 託管區域的相關資訊，包括指派給託管區域的四個名稱伺服器。託管區域代表可以一起管理的記錄集合，屬於單一父系網域名稱。

下列範例顯示AwsRoute53HostedZone物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsRoute53HostedZone屬性的描述，請參閱 AWS Security Hub API 參考資料 HostedZoneDetails中的 AwsRoute53。

範例

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
```

```
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

以下是AwsS3資源之「 AWS 安全性搜尋結果格式」的範例。

AwsS3AccessPoint

AwsS3AccessPoint提供有關 Amazon S3 存取點的資訊。S3 存取點是連接到 S3 儲存貯體的命名網路端點，可用於執行 S3 物件操作。

下列範例顯示AwsS3AccessPoint物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsS3AccessPoint屬性的說明，請參閱 AWS Security Hub API 參考資料AccessPointDetails中的AWSS3。

範例

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
```

```
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock提供帳戶之 Amazon S3 公用存取區塊組態的相關資訊。

下列範例顯示AwsS3AccountPublicAccessBlock物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsS3AccountPublicAccessBlock屬性的說明，請參閱 AWS Security Hub API 參考資料AccountPublicAccessBlockDetails中的 AWSS3。

範例

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

該AwsS3Bucket物件提供有關 Amazon S3 儲存貯體的詳細資訊。

下列範例顯示AwsS3Bucket物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsS3Bucket屬性的說明，請參閱 AWS Security Hub API 參考資料BucketDetails中的 AWSS3。

範例

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
```

```
            },
            "ExpirationDate": "2021-11-10T00:00:00.000Z",
            "ExpirationInDays": 365,
            "ExpiredObjectDeleteMarker": false,
            "Filter": {
                "Predicate": {
                    "Operands": [
                        {
                            "Prefix": "tmp/",
                            "Type": "LifecyclePrefixPredicate"
                        },
                        {
                            "Tag": {
                                "Key": "ArchiveAge",
                                "Value": "9m"
                            },
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
```

```
      "LogFilePrefix": "buckettestreadwrite23435/"
     },
     "BucketName": "DOC-EXAMPLE-BUCKET1",
     "BucketNotificationConfiguration": {
      "Configurations": [{
       "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
       "Events": [
        "s3:ObjectCreated:Put"
       ],
       "Filter": {
        "S3KeyFilter": {
         "FilterRules": [
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
         },
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
          "Value": "suf"
         },
         ]
        }
       },
       "Type": "LambdaConfiguration"
      }]
     },
     "BucketVersioningConfiguration": {
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
```

```
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
       }
      }]
     },
     "CreatedAt": "2007-11-30T01:46:56.000Z",
     "ObjectLockConfiguration": {
      "ObjectLockEnabled": "Enabled",
      "Rule": {
       "DefaultRetention": {
        "Days": null,
        "Mode": "GOVERNANCE",
        "Years": 12
       },
      },
     },
     "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
     "OwnerName": "s3bucketowner",
     "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": true,
         "BlockPublicPolicy": true,
         "IgnorePublicAcls": true,
         "RestrictPublicBuckets": true,
     },
     "ServerSideEncryptionConfiguration": {
         "Rules": [
             {
                 "ApplyServerSideEncryptionByDefault": {
                     "SSEAlgorithm": "AES256",
                     "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                 }
             }
         ]
      }
}
```

AwsS3Object

該`AwsS3Object`物件提供有關 Amazon S3 物件的資訊。

下列範例顯示`AwsS3Object`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsS3Object`屬性的說明，請參閱 AWS Security Hub API 參考資料ObjectDetails中的 AWSS3。

範例

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

以下是AwsSageMaker資源之「 AWS 安全性搜尋結果格式」的範例。

AwsSageMakerNotebookInstance

此AwsSageMakerNotebookInstance物件提供 Amazon SageMaker 筆記本執行個體的相關資訊，該執行個體是執行 Jupyter 筆記本應用程式的機器學習運算執行個體。

下列範例顯示AwsSageMakerNotebookInstance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsSageMakerNotebookInstance屬性的說明，請參閱 AWS Security Hub API 參考AwsSageMakerNotebookInstanceDetails中的。

範例

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
```

```
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

以下是AwsSecretsManager資源之「 AWS 安全性搜尋結果格式」的範例。

AwsSecretsManagerSecret

AwsSecretsManagerSecret物件提供有關 Secrets Manager 碼的詳細資訊。

下列範例顯示AwsSecretsManagerSecret物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsSecretsManagerSecret屬性的說明，請參閱 AWS Security Hub API 參考AwsSecretsManagerSecretDetails中的。

範例

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

以下是AwsSns資源之「 AWS 安全性搜尋結果格式」的範例。

AwsSnsTopic

該AwsSnsTopic物件包含有關 Amazon 簡單通知服務主題的詳細資訊。

下列範例顯示AwsSnsTopic物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsSnsTopic屬性的說明，請參閱 AWS Security Hub API 參考AwsSnsTopicDetails中的。

範例

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs

以下是AwsSqs資源之「 AWS 安全性搜尋結果格式」的範例。

AwsSqsQueue

AwsSqsQueue物件包含 Amazon 簡單佇列服務佇列的相關資訊。

下列範例顯示AwsSqsQueue物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsSqsQueue屬性的說明，請參閱 AWS Security Hub API 參考AwsSqsQueueDetails中的。

範例

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm

以下是AwsSsm資源之「 AWS 安全性搜尋結果格式」的範例。

AwsSsmPatchCompliance

此AwsSsmPatchCompliance物件會根據用來修正執行處理的修正程式基準，提供執行處理上修正程式狀態的相關資訊。

下列範例顯示AwsSsmPatchCompliance物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsSsmPatchCompliance屬性的說明，請參閱 AWS Security Hub API 參考AwsSsmPatchComplianceDetails中的。

範例

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
```

```
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

以下是AwsStepFunctions資源之「 AWS 安全性搜尋結果格式」的範例。

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine物件提供狀態機器的相關資訊， AWS Step Functions 狀態機器是由一系列事件驅動步驟組成的工作流程。

下列範例顯示AwsStepFunctionStateMachine物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsStepFunctionStateMachine屬性的說明，請參閱 AWS Security Hub API 參考AwsStepFunctionStateMachine中的。

範例

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

以下是AwsWaf資源之「 AWS 安全性搜尋結果格式」的範例。

AwsWafRateBasedRule

AwsWafRateBasedRule物件包含有關全域資源 AWS WAF 以速率為基礎的規則的詳細資訊。 AWS WAF 以速率為基礎的規則會提供設定，以指出何時允許、封鎖或計數請求。以速率為基礎的規則包括指定期間內到達的要求數目。

下列範例顯示AwsWafRateBasedRule物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsWafRateBasedRule屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRateBasedRuleDetails中的。

範例

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

此AwsWafRegionalRateBasedRule物件包含有關區域資源以速率為基礎的規則的詳細資訊。以速率為基礎的規則會提供設定，以指出何時允許、封鎖或計數要求。以速率為基礎的規則包括指定期間內到達的要求數目。

下列範例顯示AwsWafRegionalRateBasedRule物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsWafRegionalRateBasedRule屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRegionalRateBasedRuleDetails中的。

範例

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
```

```
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

該AwsWafRegionalRule對象提供有關 AWS WAF 地區規則的詳細信息。此規則會識別您要允許、封鎖或計數的 Web 要求。

下列範例顯示AwsWafRegionalRule物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsWafRegionalRule屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRegionalRuleDetails中的。

範例

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

AwsWafRegionalRuleGroup物件提供有關 AWS WAF 地區規則群組的詳細資訊。規則群組是您新增至 Web 存取控制清單 (Web ACL) 的預先定義規則集合。

下列範例顯示AwsWafRegionalRuleGroup物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsWafRegionalRuleGroup屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRegionalRuleGroupDetails中的。

範例

```
"AwsWafRegionalRuleGroup": {
```

```
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`提供有關 AWS WAF 區域 Web 存取控制清單 (Web ACL) 的詳細資訊。Web ACL 包含可識別您要允許、封鎖或計數之請求的規則。

以下是「 AWS 安全性`AwsWafRegionalWebAcl`發現項目格式」(ASFF) 中的發現項目範例。若要檢視`AwsApiGatewayV2Stage`屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRegionalWebAclDetails中的。

範例

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
```

```
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`提供有關 AWS WAF 規則的資訊。 AWS WAF 規則可識別您要允許、封鎖或計數的 Web 要求。

以下是「 AWS 安全性`AwsWafRule`發現項目格式」(ASFF) 中的發現項目範例。若要檢視`AwsApiGatewayV2Stage`屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRuleDetails中的。

範例

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`提供有關 AWS WAF 規則群組的資訊。規 AWS WAF 則群組是您新增至 Web 存取控制清單 (Web ACL) 的預先定義規則集合。

以下是「 AWS 安全性`AwsWafRuleGroup`發現項目格式」(ASFF) 中的發現項目範例。若要檢視`AwsApiGatewayV2Stage`屬性的說明，請參閱 AWS Security Hub API 參考AwsWafRuleGroupDetails中的。

範例

```
"AwsWafRuleGroup": {
```

```
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

`AwsWafv2RuleGroup`物件提供有關 AWS WAF V2 規則群組的詳細資訊。

下列範例顯示`AwsWafv2RuleGroup`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsWafv2RuleGroup`屬性的描述，請參閱 AWS Security Hub API 參考RuleGroupDetails中的AwsWafv2。

範例

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
```

```
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

`AwsWafWebAcl`物件提供有關 AWS WAF 網路 ACL 的詳細資訊。

下列範例顯示`AwsWafWebAcl`物件的「 AWS 安全性發現格式」(ASFF)。若要檢視`AwsWafWebAcl`屬性的說明，請參閱 AWS Security Hub API 參考AwsWafWebAclDetails中的。

範例

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
```

```
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

此AwsWafv2WebAcl物件提供有關 AWS WAF V2 網頁 ACL 的詳細資訊。

下列範例顯示AwsWafv2WebAcl物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsWafv2WebAcl屬性的描述，請參閱 AWS Security Hub API 參考WebAclDetails中的AwsWafv2。

範例

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
```

```
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

以下是AwsXray資源之「 AWS 安全性搜尋結果格式」的範例。

AwsXrayEncryptionConfig

AwsXrayEncryptionConfig物件包含的加密組態的相關資訊 AWS X-Ray。

下列範例顯示AwsXrayEncryptionConfig物件的「 AWS 安全性發現格式」(ASFF)。若要檢視AwsXrayEncryptionConfig屬性的說明，請參閱 AWS Security Hub API 參考AwsXrayEncryptionConfigDetails中的。

範例

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

與問題清單有關的容器詳細資訊。

下列範例顯示Container物件的「 AWS 安全性發現格式」(ASFF)。若要檢視Container屬性的說明，請參閱 AWS Security Hub API 參考ContainerDetails中的。

範例

```
"Container": {
    "ContainerRuntime": "docker",
```

```
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other

該Other對象允許您提供自定義字段和值。您可以在下列情況下使用該Other物件。

- 資源類型沒有對應的Details物件。若要提供資源的詳細資訊，請使用Other物件。
- 資源類型的Details物件不包含您要填入的所有屬性。在此情況下，請使用資源類型的Details物件來填入可用屬性。使用Other物件填入不在類型專屬物件中的屬性。
- 資源類型不是提供的類型之一。在此情況下，您Resource.Type將設定為Other，並使用Other物件來填入詳細資訊。

類型：最多 50 個鍵值對的映射

每個鍵/值對必須符合下列需求。

- 金鑰必須包含少於 128 個字元。
- 此值必須包含少於 1,024 個字元。

AWS安全中心的洞察

安 AWS Security Hub 洞察是相關發現項目的集合。該洞見會識別需要注意和介入的安全區域。舉例來說，洞見可能會指出 EC2 執行個體是偵測到不良安全實務的問題清單主體。洞見結合了各問題清單提供者的問題清單。

每個洞見都會根據 group by 陳述式和選用篩選條件定義。group by 陳述式會指出如何將相符的問題清單分組，並識別套用洞見的項目類型。舉例來說，如果洞見根據資源識別符分組，則洞見會產生資源識別符的清單。選用的篩選器會識別洞察的相符發現項目。例如，您可能只想要查看來自特定提供者的發現項目或與特定資源類型相關聯的發現項目。

Security Hub 提供數個內建的受管理見解。您無法刪除或修改受管洞見。

如果要追蹤您 AWS 環境和使用量特有的安全問題，可以建立自訂洞見。

只有在您已啟用可產生相符發現項目的整合或標準時，洞察才會傳回結果。例如，受管洞察 29. 按失敗 CIS 檢查計數排列的最高資源僅在啟用 CIS AWS 基礎標準時傳回結果。

主題

- 檢視和篩選深入解析清單
- 檢視洞見結果和問題清單並採取動作
- 受管的洞見
- 自訂洞見

檢視和篩選深入解析清單

「深入解析」頁面會顯示可用見解的清單。

根據預設，清單會同時顯示受管理和自訂見解。若要根據深入解析類型篩選分析清單，請從篩選欄位旁的下拉式功能表中選擇深入解析類型。

- 若要顯示所有可用的見解，請選擇 [所有見解]。此為預設選項。
- 若只要顯示受管理的見解，請選擇 Security Hub 受管理的見解。
- 若只要顯示自訂見解，請選擇 [自訂見解]。

您也可以根據分析名稱中的文字篩選分析清單。

在篩選欄位中，輸入要用來篩選清單的文字。篩選器不區分大小寫。篩選器會尋找包含深入解析名稱中任何位置文字的深入解析。

檢視洞見結果和問題清單並採取動作

AWSSecurity Hub 會先判斷符合篩選準則的發現項目，然後使用群組屬性將相符的發現項目分組。

在 In sights 主控台頁面中，您可以檢視結果和發現項目並對其採取行動。

如果您啟用跨區域彙總，則在彙總區域中，受管理見解的結果包括來自彙總區域和連結區域的發現項目。對於自訂分析結果，如果洞察未依「區域」進行篩選，則結果會包含彙總區域和連結區域的發現項目。

在其他地區，洞察結果僅適用於該區域。

如需如何設定跨區域彙總的相關資訊，請參閱跨區域彙總。

檢視分析結果並對其採取處理行動 (主控台)

洞見結果由洞見結果的分組清單組成。例如，如果洞察是依資源識別碼分組的，則洞察結果就是資源識別碼清單。結果清單中的每個項目都會指出該項目符合的問題清單數。

請注意，如果發現項目是依資源識別碼或資源類型分組，則結果會包含相符發現項目中的所有資源。這包括與篩選條件中指定的資源類型不同的資源類型的資源。例如，深入分析可識別與 S3 儲存貯體相關聯的發現項目。如果相符的發現項目同時包含 S3 儲存貯體資源和 IAM 存取金鑰資源，則洞察結果會列出這兩個資源。

結果清單會以最多到最少的相符問題清單排序。

Security Hub 只能顯示 100 個結果。如果群組值超過 100，您只會看到前 100 個。

除了結果清單之外，洞見結果還會顯示一組圖表，摘要下列屬性的相符問題清單數。

- 嚴重性標籤 — 每個嚴重性標籤的發現項目數目
- AWS 帳戶ID — 相符發現項目的前五個帳號 ID
- 資源類型 — 相符發現項目的前五大資源類型
- 資源 ID — 相符發現項目的前五個資源 ID
- 產品名稱-相符搜尋結果的前五名尋找提供者

若您已設定自訂動作，即可將選取的結果傳送到自訂動作。動作必須與Security Hub Insight Results事件類型的 CloudWatch 規則相關聯。請參閱 the section called “自動化回應與補救”。

如果您尚未設定自訂動作，則會停用 [動作] 功能表。

顯示洞見結果的清單並採取動作

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇 Insights。
3. 若要顯示洞見結果的清單，請選擇洞見名稱。
4. 選取各個結果的核取方塊，並傳送到自訂動作。
5. 從 Actions (動作) 選單選擇自訂動作。

檢視見解結果 (Security Hub API、AWS CLI)

若要檢視洞察結果，您可以使用 API 呼叫或AWS Command Line Interface.

若要檢視見解結果 (Security Hub API，AWS CLI)

- Security Hub API — 使用GetInsightResults操作。要確定要返回結果的洞察力，您需要洞察 ARN。若要取得自訂見解的洞察 ARN，請使用此GetInsights作業。
- AWS CLI— 在命令列中，執行get-insight-results命令。

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

範例：

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

檢視見解結果的發現項目 (主控台)

您可以從洞見結果清單顯示各個結果的問題清單。

顯示洞見問題清單並採取動作

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。

2. 在導覽窗格中，選擇 Insights。
3. 若要顯示洞見結果的清單，請選擇洞見名稱。
4. 若要顯示洞見結果的問題清單，請從結果清單選擇項目。

問題清單會顯示工作流程狀態為 NEW 或 NOTIFIED 選取洞見結果的作用中問題清單。

從問題清單，您可以執行下列動作。

- 變更清單的篩選條件和群組
- 檢視個別問題清單的詳細資訊
- 更新問題清單的工作流程狀態
- 將問題清單傳送到自訂動作

受管的洞見

AWSSecurity Hub 提供數個受管理的見解。

您無法編輯或刪除 Security Hub 受管理的見解。您可以檢視並對洞見結果和問題清單採取動作。您也可以使用受管洞見做為新自訂洞見的基礎。

如同所有洞見，如果您有啟用的產品整合或可產生相符問題清單的安全標準，則受管洞見只會傳回結果。

對於依資源識別碼分組的見解，結果會包含相符發現項目中所有資源的識別碼。這包括與篩選條件中的資源類型不同的資源。例如，洞察力 2 可識別與 Amazon S3 儲存貯體相關聯的發現項目。如果比對的發現項目同時包含 S3 儲存貯體資源和 IAM 存取金鑰資源，則洞察結果會同時包含這兩種資源。

Security Hub 提供下列受管理的見解：

1. AWS發現數量最多的資源

   ARN：arn:aws:securityhub:::insight/securityhub/default/1

   分組方式：資源識別碼

   尋找篩選器：

   - 記錄狀態為 ACTIVE
   - 工作流程狀態為 NEW 或 NOTIFIED

2. 具有公有寫入或讀取許可的 S3 儲存貯體

   ARN：arn:aws:securityhub:::insight/securityhub/default/10

   分組方式：資源識別碼

   尋找篩選器：

   - 類型開頭為 Effects/Data Exposure
   - 資源類型為 AwsS3Bucket
   - 記錄狀態為 ACTIVE
   - 工作流程狀態為 NEW 或 NOTIFIED

3. 產生最多問題清單的 AMI

   ARN：arn:aws:securityhub:::insight/securityhub/default/3

   依據分組：EC2 執行個體映像檔 ID

   尋找篩選器：

   - 資源類型為 AwsEc2Instance
   - 記錄狀態為 ACTIVE
   - 工作流程狀態為 NEW 或 NOTIFIED

4. 有關已知戰術、技術和程序 (TTP) 的 EC2 執行個體

   ARN：arn:aws:securityhub:::insight/securityhub/default/14

   分組依據：資源 ID

   尋找篩選器：

   - 類型開頭為 TTPs
   - 資源類型為 AwsEc2Instance
   - 記錄狀態為 ACTIVE
   - 工作流程狀態為 NEW 或 NOTIFIED

5. AWS具有可疑存取金鑰活動的主體

   ARN：arn:aws:securityhub:::insight/securityhub/default/9

   分組方式：IAM 存取金鑰主要名稱

尋找篩選器：

- 資源類型為 AwsIamAccessKey
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

6. AWS不符合安全標準/最佳實務的資源執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/6

分組依據：資源 ID

尋找篩選器：

- 類型為 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

7. AWS與潛在資料外洩相關的資源

ARN：arn:aws:securityhub:::insight/securityhub/default/7

分組方式:: 資源 ID

尋找篩選器：

- 類型開頭為 Effects/Data Exfiltration/
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

8. AWS與未經授權的資源消耗相關聯

ARN：arn:aws:securityhub:::insight/securityhub/default/8

分組依據：資源 ID

尋找篩選器：

- 類型開頭為 Effects/Resource Consumption
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

9. 不符合安全標準/最佳實務的 S3 儲存貯體

   ARN：arn:aws:securityhub:::insight/securityhub/default/11

   分組依據：資源 ID

   尋找篩選器：

   - 資源類型為 AwsS3Bucket
   - 類型為 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
   - 記錄狀態為 ACTIVE
   - 工作流程狀態為 NEW 或 NOTIFIED

10. 具有敏感資料的 S3 儲存貯體

    ARN：arn:aws:securityhub:::insight/securityhub/default/12

    分組依據：資源 ID

    尋找篩選器：

    - 資源類型為 AwsS3Bucket
    - 類型開頭為 Sensitive Data Identifications/
    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

11. 登入資料可能已洩漏

    ARN：arn:aws:securityhub:::insight/securityhub/default/13

    分組依據：資源 ID

    尋找篩選器：

    - 類型開頭為 Sensitive Data Identifications/Passwords/
    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

12. 缺少重要漏洞安全性修補程式的 EC2 執行個體

    ARN：arn:aws:securityhub:::insight/securityhub/default/16

分組依據：資源 ID

尋找篩選器：

- 類型開頭為 Software and Configuration Checks/Vulnerabilities/CVE
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

13. 具有一般異常行為的 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/17

分組依據：資源 ID

尋找篩選器：

- 類型開頭為 Unusual Behaviors
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

14. 具有可從網際網路存取連接埠的 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/18

分組依據：資源 ID

尋找篩選器：

- 類型開頭為 Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

15. 不符合安全標準或最佳實務的 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/19

分組依據：資源 ID

尋找篩選器：

- 類型以下列其中一個項目開頭：
  - Software and Configuration Checks/Industry and Regulatory Standards/
  - Software and Configuration Checks/AWS Security Best Practices
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

16. 向網際網路開放的 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/21

分組依據：資源 ID

尋找篩選器：

- 類型開頭為 Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

17. 與對手偵察相關聯的 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/22

分組依據：資源 ID

尋找篩選器：

- 類型以 TTPs/Discovery/Recon 開頭
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

18. AWS與惡意程式碼相關聯的資源

ARN：arn:aws:securityhub:::insight/securityhub/default/23

分組依據：資源 ID

尋找篩選器：

- 類型以下列其中一個項目開頭：
  - Effects/Data Exfiltration/Trojan
  - TTPs/Initial Access/Trojan
  - TTPs/Command and Control/Backdoor
  - TTPs/Command and Control/Trojan
  - Software and Configuration Checks/Backdoor
  - Unusual Behaviors/VM/Backdoor
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

19. AWS與加密貨幣相關的資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/24

    分組依據：資源 ID

    尋找篩選器：

    - 類型以下列其中一個項目開頭：
      - Effects/Resource Consumption/Cryptocurrency
      - TTPs/Command and Control/CryptoCurrency
    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

20. AWS未經授權存取嘗試的資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/25

    分組依據：資源 ID

    尋找篩選器：

    - 類型以下列其中一個項目開頭：
      - TTPs/Command and Control/UnauthorizedAccess
      - TTPs/Initial Access/UnauthorizedAccess
      - Effects/Data Exfiltration/UnauthorizedAccess
      - Unusual Behaviors/User/UnauthorizedAccess
      - Effects/Resource Consumption/UnauthorizedAccess

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

21. 過去一週最多命中的威脅 intel 指標

    ARN：arn:aws:securityhub:::insight/securityhub/default/26

    尋找篩選器：

    - 最近 7 天內建立

22. 按問題清單計數排列的熱門帳戶

    ARN：arn:aws:securityhub:::insight/securityhub/default/27

    分組方式:AWS 帳戶ID

    尋找篩選器：

    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

23. 按問題清單計數排列的熱門產品

    ARN：arn:aws:securityhub:::insight/securityhub/default/28

    分組方式：產品名稱

    尋找篩選器：

    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

24. 按問題清單計數排列的嚴重性

    ARN：arn:aws:securityhub:::insight/securityhub/default/29

    分組依據：嚴重性標籤

    尋找篩選器：

    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

25. 按問題清單計數排列的熱門 S3 儲存貯體

    ARN：arn:aws:securityhub:::insight/securityhub/default/30

分組依據：資源 ID

尋找篩選器：

- 資源類型為 AwsS3Bucket
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

26. 按問題清單計數排列的熱門 EC2 執行個體

ARN：arn:aws:securityhub:::insight/securityhub/default/31

分組依據：資源 ID

尋找篩選器：

- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

27. 按問題清單計數排列的熱門 AMI

ARN：arn:aws:securityhub:::insight/securityhub/default/32

依據分組：EC2 執行個體映像檔 ID

尋找篩選器：

- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

28. 按問題清單計數排列的熱門 IAM 使用者

ARN：arn:aws:securityhub:::insight/securityhub/default/33

分組方式：IAM 存取金鑰 ID

尋找篩選器：

- 資源類型為 AwsIamAccessKey
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

29. 按失敗 CIS 檢查計數排列的熱門資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/34

    分組依據：資源 ID

    尋找篩選器：

    - 產生器 ID 開頭為 arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule
    - 最後一天更新
    - 合規狀態為 FAILED
    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

30. 按問題清單計數排列的熱門整合

    ARN：arn:aws:securityhub:::insight/securityhub/default/35

    分組方式：產品 ARN

    尋找篩選器：

    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

31. 安全檢查失敗次數最多的資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/36

    分組依據：資源 ID

    尋找篩選器：

    - 最後一天更新
    - 合規狀態為 FAILED
    - 記錄狀態為 ACTIVE
    - 工作流程狀態為 NEW 或 NOTIFIED

32. 存在可疑活動的 IAM 使用者

    ARN：arn:aws:securityhub:::insight/securityhub/default/37

    依據分組：IAM 使用者

尋找篩選器：

- 資源類型為 AwsIamUser
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

33. AWS Health發現數量最多的資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/38

    分組依據：資源 ID

    尋找篩選器：

    - ProductName等於 Health

34. AWS Config發現數量最多的資源

    ARN：arn:aws:securityhub:::insight/securityhub/default/39

    分組依據：資源 ID

    尋找篩選器：

    - ProductName等於 Config

35. 發現項目最多的應用程式

    ARN：arn:aws:securityhub:::insight/securityhub/default/40

    分組方式：ResourceApplicationArn

    尋找篩選器：

    - RecordState等於 ACTIVE
    - Workflow.Status等於NEW或 NOTIFIED

自訂洞見

除了AWSSecurity Hub 受管理的見解，您可以在 Security Hub 中建立自訂見解，以追蹤您環境特定的問題。自訂見解提供一種追蹤策劃問題子集的方法。

以下是一些有助於設定的自訂見解範例：

- 如果您擁有管理員帳戶，則可以設定自訂分析，以追蹤影響成員帳戶的重要和高嚴重性發現項目。

- 如果你依靠一個具體集成AWS服務，您可以設定自訂分析，以追蹤該服務的關鍵和高嚴重性發現項目。
- 如果你依靠第三方整合，您可以設定自訂分析，以追蹤該整合產品的關鍵和高嚴重性發現項目。

您可以建立全新的自訂洞見，或從現有的自訂或受管洞見開始。

每個洞見都設有以下選項。

- 群組屬性— 分組屬性決定了哪些項目會顯示在分析結果清單中。例如，如果分組屬性為產品名稱，則分析結果會顯示與每個尋找項目提供者相關聯的發現項目數目。
- 可選過濾器-過濾器縮小了洞察力的匹配發現範圍。

  查詢發現項目時，安全性中心會將布林值 AND 邏輯套用至篩選器集。換句話說，只有當問題清單符合所有提供的篩選條件時，才會相符。例如，如果篩選器為「產品名稱為GuardDuty「和」資源類型為AwsS3Bucket，」然後比對發現項目必須符合這兩個條件。

  不過，安全性中樞會將布林值 OR 邏輯套用至使用相同屬性但不同值的篩選器。例如，如果篩選器為「產品名稱為GuardDuty「和」產品名稱是亞馬遜 Inspector，」然後是查找匹配項，如果它是由任何一個生成的GuardDuty或亞馬遜督察。

請注意，如果您使用資源識別碼或資源類型作為群組屬性，則分析結果會包含相符發現項目中的所有資源。此清單不限於符合資源類型篩選器的資源。例如，深入解析可識別與 S3 儲存貯體相關聯的發現項目，並依資源識別碼將這些發現項目分組。相符的發現項目包含 S3 儲存貯體資源和 IAM 存取金鑰資源。洞察結果包括兩種資源。

建立自訂分析 (主控台)

您可以從主控台建立全新的洞見。

若要建立自訂分析

1. 打開AWS安全中心主控台位於https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇 Insights。
3. 選擇 Create insight (建立洞見)。
4. 選取洞見的分組屬性：
   a. 選擇搜尋方塊以顯示篩選選項。
   b. 選擇 Group by (分組依據)。

c. 選取要用來將與此鑑識相關聯的發現項目分組的屬性。

d. 選擇 Apply (套用)。

5. (選用) 選擇要為此洞見使用的任何其他篩選條件。針對每個篩選，定義篩選準則，然後選擇申請。
6. 選擇 Create insight (建立洞見)。
7. 輸入 Insight name (洞見名稱) 並選擇 Create insight (建立洞見)。

建立自訂分析 (程式設計)

選擇您偏好的方法，然後按照步驟在 Security Hub 中以程式設計方式建立自訂分析。您可以指定篩選器，將深入解析中發現項目的集合縮小為特定子集。

下列索引標籤包含幾種語言的指示，可用來建立自訂分析。如需其他語言的支援，請參閱建置基礎的工具AWS。

Security Hub API

1. 運行CreateInsight操作。
2. 填入Name具有自定義見解的名稱的參數。
3. 填入Filters用來指定要包含在洞察中的發現項目的參數。
4. 填入GroupByAttribute參數，指定要使用哪個屬性將包含在深入解析中的發現項目分組。
5. (選擇性) 填入SortCriteria依特定欄位排序發現項目的參數。

如果您已啟用跨區域彙總並從聚合區域調用此 API，洞察將適用於彙總和鏈接區域中的匹配發現項目。

AWS CLI

1. 在命令列中，執行create-insight指令。
2. 填入name具有自定義見解的名稱的參數。
3. 填入filters用來指定要包含在洞察中的發現項目的參數。
4. 填入group-by-attribute參數，指定要使用哪個屬性將包含在深入解析中的發現項目分組。

如果您已啟用跨區域彙總並從彙總區域執行此命令，洞察會套用至來自彙總和連結區域的相符發現項目。

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

範例

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. 使用New-SHUBInsight指令程式。
2. 填入Name具有自定義見解的名稱的參數。
3. 填入Filter用來指定要包含在洞察中的發現項目的參數。
4. 填入GroupByAttribute參數，指定要使用哪個屬性將包含在深入解析中的發現項目分組。

如果您已啟用跨區域彙總並使用彙總區域中的此指令程式，洞察會套用至彙總和連結區域中的相符發現項目。

範例

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

修改自訂分析 (主控台)

您可以修改現有的自訂洞見，來變更分組值和篩選條件。進行變更後，您可以將更新儲存到原始洞見，或另存更新的版本為新的洞見。

修改洞見

1. 打開AWS安全中心主控台位於https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇 Insights。
3. 選擇要修改的自訂洞見
4. 視需要編輯深入解析組態。
   - 變更在洞見中用於將問題清單分組的屬性：
     a. 若要移除現有的群組，請選擇X旁邊的分組依據設置。
     b. 選擇搜尋方塊。
     c. 選取要用於分組的屬性。
     d. 選擇 Apply (套用)。
   - 若要從深入解析中移除篩選器，請選擇圓圈選取X旁邊的過濾器。
   - 新增篩選條件到洞見：
     a. 選擇搜尋方塊。
     b. 選取要用做篩選條件的屬性和值。
     c. 選擇 Apply (套用)。
5. 完成更新時，請選擇 Save insight (儲存洞見)。
6. 出現提示時，請執行以下其中一項作業：
   - 若要更新現有分析以反映您的變更，請選擇更新*<Insight_Name>*然後選擇儲存洞察。
   - 如果要以更新建立新的洞見，請選擇 Save new insight (儲存新的洞見)。輸入 Insight name (洞見名稱)，然後選擇 Save insight (儲存洞見)。

修改自訂分析 (程式設計)

若要修改自訂分析，請選擇您偏好的方法，然後依照指示進行。

Security Hub API

1. 運行`UpdateInsight`操作。
2. 若要識別自訂分析，請提供洞察的 Amazon 資源名稱 (ARN)。若要取得自訂分析的 ARN，請執行`GetInsights`操作。
3. 更新`Name`,`Filters`，以及`GroupByAttribute`參數根據需要。

AWS CLI

1. 在命令列中，執行update-insight指令。
2. 若要識別自訂分析，請提供洞察的 Amazon 資源名稱 (ARN)。若要取得自訂分析的 ARN，請執行get-insights指令。
3. 更新name,filters，以及group-by-attribute參數根據需要。

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

範例

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. 使用Update-SHUBInsight指令程式。
2. 若要識別自訂分析，請提供洞察的 Amazon 資源名稱 (ARN)。若要取得自訂分析的 ARN，請使用Get-SHUBInsight指令程式。
3. 更新Name,Filter，以及GroupByAttribute參數根據需要。

範例

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}
```

```
Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

從受管理的分析 (主控台) 建立新的自訂分析

您無法對受管洞見儲存變更，或將其刪除。您可以使用受管洞見做為新自訂洞見的基礎。

從受管洞見建立新的自訂洞見

1. 打開AWS安全中心主控台位於https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇 Insights。
3. 選擇要使用的受管洞見。
4. 視需要編輯深入解析組態。
   - 變更在洞見中用於將問題清單分組的屬性：
     a. 若要移除現有的群組，請選擇X旁邊的分組依據設置。
     b. 選擇搜尋方塊。
     c. 選取要用於分組的屬性。
     d. 選擇 Apply (套用)。
   - 若要從深入解析中移除篩選器，請選擇圓圈選取X旁邊的過濾器。
   - 新增篩選條件到洞見：
     a. 選擇搜尋方塊。
     b. 選取要用做篩選條件的屬性和值。
     c. 選擇 Apply (套用)。
5. 更新完成時，請選擇 Create insight (建立洞見)。
6. 出現提示時，請輸入洞察力名稱，然後選擇建立洞察力。

刪除自訂分析 (主控台)

當您不再想要自訂洞見時，可以將其刪除。您無法刪除受管洞見。

刪除自訂的洞見

1. 打開AWS安全中心主控台位於https://console.aws.amazon.com/securityhub/。

2. 在導覽窗格中，選擇 Insights。
3. 找到要刪除的自訂洞見。
4. 對於這個見解，請選擇更多選項圖標（卡片右上角的三個點）。
5. 選擇 刪除 。

刪除自訂分析 (程式設計)

若要刪除自訂分析，請選擇您偏好的方法，然後依照指示操作。

Security Hub API

1. 運行DeleteInsight操作。
2. 若要識別要刪除的自訂分析，請提供分析的 ARN。若要取得自訂分析的 ARN，請執行GetInsights操作。

AWS CLI

1. 在命令列中，執行delete-insight指令。
2. 若要識別自訂分析，請提供洞察力的 ARN。若要取得自訂分析的 ARN，請執行get-insights指令。

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

範例

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. 使用Remove-SHUBInsight指令程式。
2. 若要識別自訂分析，請提供洞察力的 ARN。若要取得自訂分析的 ARN，請使用Get-SHUBInsight指令程式。

範例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

自動化

Security Hub 自動化可協助您根據您的規格快速修改及修復發現項目。

Security Hub 目前支援兩種類型的自動化：

- 自動化規則 — 根據您定義的條件，以近乎即時的方式自動更新和隱藏發現項目。
- 自動化回應和補救 — 建立自訂 EventBridge 規則，以定義要針對特定發現項目和見解採取的自動動作。

自動化規則適用於 EventBridge 規則之前。也就是說，自動化規則會觸發並在發現項目傳送到之前更新 EventBridge。 EventBridge 然後規則會套用至更新的發現項目。

為安全性控制設定自動化時，我們建議您根據控制項 ID 進行篩選，而非標題或說明。雖然 Security Hub 偶爾更新控制標題和描述，控制項 ID 保持不變。

主題

- 自動化規則
- 自動化回應與補救

自動化規則

自動化規則可用來自動更新 Security Hub 中的發現項目。擷取發現項目時，Security Hub 可以套用各種規則動作，例如隱藏發現項目、變更其嚴重性，以及將附註新增至發現項目。當發現項目符合您指定的準則 (例如與發現項目相關聯的資源或帳號 ID 或其標題) 時，此類規則動作便會生效。

自動化規則的使用案例包括：

- 將發現項目的嚴重性提高為發現項目的資源 ID 是`CRITICAL`否參考業務關鍵資源。
- 如果發現項目會影響特定生產帳戶中的資源，`CRITICAL`則`HIGH`將發現項目的嚴重性從提高到。
- 指派具有`SUPPRESSED`工作流程狀態嚴重性的`INFORMATIONAL`特定發現項目。

自動化規則可用來更新「AWS安全性搜尋結果格式」(ASFF) 中的選取搜尋結果欄位。規則適用於新發現和更新的發現。

您可以從頭開始建立自訂規則，或使用 Security Hub 提供的規則範本。如果您使用規則範本，您可以根據使用案例的需要對其進行修改。

自動化規則如何運作

Security Hub 管理員可以透過定義規則條件來建立自動化規則。當發現項目符合定義的準則時，Security Hub 會將規則動作套用至該項目。如需有關可用條件與動作的詳細資訊，請參閱可用的規則條件和規則動作。

只有 Security Hub 管理員帳戶可以建立、刪除、編輯和檢視自動化規則。系統管理員建立的規則會套用至管理員帳戶和所有成員帳戶中的發現項目。透過提供成員帳號 ID 做為規則條件，Security Hub 管理員也可以使用自動化規則來更新發現項目，或對特定成員帳戶中的發現項目採取動作。

> **Important**
>
> 自動化規則僅適用於其建立時所AWS 區域在的規則。若要在多個區域中套用規則，委派的管理員必須在每個區域中建立規則。這可以通過安全中心控制台，Security Hub API 或完成AWS CloudFormation。您也可以使用多區域部署指令碼。

若要取得自動化規則如何變更發現項目的歷史記錄，請參閱尋找歷史。

自動化規則會套用至 Security Hub 在您建立規則後產生或擷取的新發現項目和更新的發現項目。Security Hub 會每隔 12-24 小時或相關聯的資源變更狀態時，更新控制發現項目。如需詳細資訊，請參閱執行安全檢查的排程。

Security Hub 目前最多支援 100 個系統管理員帳戶的自動化規則。

規則順序

建立自動化規則時，您可以為每個規則指定一個順序。這會決定 Security Hub 套用自動化規則的順序，並且當多個規則與相同的發現項目或發現項目欄位相關時，會變得很重要。

當多個規則作業與相同的搜尋結果或搜尋結果欄位相關時，規則順序數值最高的規則會最後套用，並具有最終效果。

當您在 Security Hub 主控台中建立規則時，Security Hub 會根據規則建立的順序自動指派規則順序。最近建立的規則具有規則順序的最低數值，因此會先套用。安全中心會依遞增順序套用後續規則。

當您透過 Security Hub API 建立規則時AWS CLI，Security Hub 會套用數值最低的`RuleOrder`規則。然後，它會以遞增順序套用後續規則。如果多個發現項目具有相同的結果`RuleOrder`，Security Hub 會先針對`UpdatedAt`欄位套用具有較早值的規則 (也就是說，最近編輯的規則會套用最近編輯的規則)。

您可以隨時修改規則順序。

規則順序範例：

規則 A（規則命令是**1**）：

- 規則 A 條件
  - ProductName = Security Hub
  - Resources.Type 是 S3 Bucket
  - Compliance.Status = FAILED
  - RecordState 是 NEW
  - Workflow.Status = ACTIVE
- 規則 A 動作
  - 更新Confidence至 95
  - 更新Severity至 CRITICAL

規則 B（規則命令是**2**）：

- 規則 B 條件
  - AwsAccountId = 123456789012
- 規則 B 動作
  - 更新Severity至 INFORMATIONAL

規則動作會先套用至符合規則 A 條件的 Security Hub 發現項目。接下來，規則 B 動作會套用至具有指定帳號識別碼的 Security Hub 發現項目。在此範例中，由於規則 B 最後適用，因此指定帳號 ID Severity 中發現項目中的結束值為INFORMATIONAL。根據「規則 A」動作，相符發現項目Confidence中的結束值為95。

可用的規則條件和規則動作

目前支援下列 ASFF 欄位做為自動化規則的條件。

退還欄位	篩選條件	欄位類型
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS,	字串

退還欄位	篩選條件	欄位類型
	NOT_EQUALS, PREFIX_NOT_EQUALS	
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ComplianceStatus	Is, Is Not	選擇：[FAILEDNOT_AVAILABLE ,PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
CreatedAt	Start, End, DateRange	日期（格式化為 2022-12-01T21：37:39.269 Z）

退還欄位	篩選條件	欄位類型
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
FirstObservedAt	Start, End, DateRange	日期（格式化為 2022-12-01T21：37:39.269 Z）
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
LastObservedAt	Start, End, DateRange	日期（格式化為 2022-12-01T21：37:39.269 Z）
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
NoteUpdatedAt	Start, End, DateRange	日期（格式化為 2022-12-01T21：37:39.269 Z）

退還欄位	篩選條件	欄位類型
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串

退還欄位	篩選條件	欄位類型
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceType	Is, Is Not	選取 (請參閱 ASFF 支援的資源)
SeverityLabel	Is, Is Not	選取：[CRITICALHIGH、MEDIUM、LOW、INFONAL]

退還欄位	篩選條件	欄位類型
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
UpdatedAt	Start, End, DateRange	日期（格式化為 2022-12-01T21：37:39.269 Z）
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
WorkflowStatus	Is, Is Not	選擇：[NEWNOTIFIED,RESOLVED,SUPPRESSED]

目前支援下列 ASFF 欄位做為自動化規則的動作：

- Confidence
- Criticality

- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

如需有關特定 ASFF 欄位的詳細資訊，請參閱AWS安全性發現格式 (ASFF) 語法和 AS FF 範例。

> **Tip**
>
> 如果您希望 Security Hub 停止產生特定控制項的發現項目，建議您停用控制項，而不是使用自動化規則。停用控制項時，Security Hub 會停止對其執行安全性檢查，並停止產生該控制項的發現項目，因此您不會產生該控制項的費用。建議您使用自動化規則，針對符合已定義條件的發現項目變更特定 ASFF 欄位的值。如需停用控制項的詳細資訊，請參閱在所有標準中啟用和停用控制項。

建立自動化規則

您可以從頭開始建立自訂規則，或使用預先填入的 Security Hub 規則範本。

您一次只能建立一個自動化規則。若要建立多個自動化規則，請多次遵循主控台程序，或使用您想要的參數多次呼叫 API 或命令。

您必須在要將規則套用至發現項目的每個區域和帳戶中建立自動化規則。

當您在 Security Hub 主控台中建立自動化規則時，Security Hub 會顯示規則套用之發現項目的預覽。如果您的規則條件包含「包含」或「NOT_CONTECT」篩選器，則目前不支援預覽。您可以為地圖和字串欄位類型選擇這些篩選器。

> **Important**
>
> AWS建議您不要在規則名稱、說明或其他欄位中包含個人識別資訊、機密或敏感資訊。

從範本建立規則 (僅限主控台)

目前只有 Security Hub 主控台支援規則範本。這些範本反映了自動化規則的常見使用案例，可協助您開始使用此功能。完成下列步驟，即可從主控台中的範本建立自動化規則。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。
3. 選擇 Create rule (建立規則)。針對「規則類型」，選擇「從範本建立規則」。
4. 從下拉式功能表中選取規則範本。
5. (選擇性) 如果您的使用案例有必要，請修改「規則」、「條件」和「自動化」動作區段。您必須指定至少一個規則條件和一個規則動作。

   如果您選取的條件支援，主控台會顯示符合您條件的發現項目預覽。
6. 針對規則狀態，選擇規則在建立後要為「啟用」或「停用」。
7. (選擇性) 展開 [其他設定] 區段。如果您希望此規則成為最後套用至符合規則準則之發現項目的規則，請選取忽略符合這些條件之發現項目的後續規則。
8. (選擇性) 對於標籤，將標籤新增為鍵值配對，以協助您輕鬆識別規則。
9. 選擇 Create rule (建立規則)。

建立自訂規則

選擇您偏好的方法，然後完成下列步驟以建立自訂自訂自動化規則。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。
3. 選擇 Create rule (建立規則)。針對規則類型，選擇建立自訂規則。
4. 在「規則」區段中，為您的規則提供唯一的規則名稱和說明。
5. 對於「條件」，請使用「鍵」、「運算子」和「值」下拉式功能表來指定規則條件。您必須指定至少一個規則條件。

如果您選取的條件支援，主控台會顯示符合您條件的發現項目預覽。

6. 針對「自動」動作，請使用下拉式功能表，指定當發現項目符合您的規則條件時，要更新哪些尋找欄位。您必須指定至少一個規則動作。
7. 針對規則狀態，選擇規則在建立後要為「啟用」或「停用」。
8. (選擇性) 展開 [其他設定] 區段。如果您希望此規則成為最後套用至符合規則準則之發現項目的規則，請選取忽略符合這些條件之發現項目的後續規則。
9. (選擇性) 對於標籤，將標籤新增為鍵值配對，以協助您輕鬆識別規則。
10. 選擇 Create rule (建立規則)。

API

1. `CreateAutomationRule`從 Security Hub 系統管理員帳戶執行。此 API 會建立具有特定 Amazon 資源名稱 (ARN) 的規則。
2. 提供規則的名稱和說明。
3. `true`如果您希望此規則成為最後套用至符合規則準則之發現項目的規則，請將`IsTerminal`參數設定為。
4. 對於`RuleOrder`參數，請提供規則的順序。Security Hub 會先套用此參數具有較低數值的規則。
5. 對於`RuleStatus`參數，請指定是否要啟用 Security Hub，並在建立後開始將規則套用至發現項目。如未指定任何值，則預設值為 `ENABLED`。值`DISABLED`表示規則在建立後暫停。
6. 針對`Criteria`參數，提供您希望 Security Hub 用來篩選發現項目的條件。規則動作將套用至符合條件的發現項目。如需支援條件的清單，請參閱可用的規則條件和規則動作。
7. 針對`Actions`參數，提供您希望 Security Hub 在發現項目與您定義的準則之間相符時採取的動作。如需支援動作的清單，請參閱可用的規則條件和規則動作。

API 請求示例：

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
```

```
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. 從 Security Hub 系統管理員帳戶執行`create-automation-rule`命令。此命令會建立具有特定 Amazon 資源名稱 (ARN) 的規則。
2. 提供規則的名稱和說明。
3. 如果您希望此規則成為最後一個套用至符合規則準則之發現項目的規則，請包含`is-terminal`參數。否則，請包括`no-is-terminal`參數。

4. 對於rule-order參數，請提供規則的順序。Security Hub 會先套用此參數具有較低數值的規則。
5. 對於rule-status參數，請指定是否要啟用 Security Hub，並在建立後開始將規則套用至發現項目。如未指定任何值，則預設值為 ENABLED。值DISABLED表示規則在建立後暫停。
6. 針對criteria參數，提供您希望 Security Hub 用來篩選發現項目的條件。規則動作將套用至符合條件的發現項目。如需支援條件的清單，請參閱可用的規則條件和規則動作。
7. 針對actions參數，提供您希望 Security Hub 在發現項目與您定義的準則之間相符時採取的動作。如需支援動作的清單，請參閱可用的規則條件和規則動作。

範例命令：

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

檢視自動化規則

選擇您偏好的方法，然後按照步驟檢視您的自動化規則和每個規則的詳細資料。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。
3. 選擇規則名稱。或者，選取規則。
4. 選擇「動作和檢視」。

API

1. 若要檢視您帳戶的自動化規則，請`ListAutomationRules`從 Security Hub 系統管理員帳戶執行。此 API 會傳回規則 ARN 和規則的其他中繼資料。此 API 不需要輸入參數，但您可以選擇性地`MaxResults`提供以限制結果數量和`NextToken`分頁參數。的初始值`NextToken`應該是`NULL`。

   API 請求示例：

   ```
   {
    "MaxResults": 50,
    "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
   }
   ```
2. 如需其他規則詳細資訊，包括規則的準則和動作，請`BatchGetAutomationRules`從 Security Hub 管理員帳戶執行。

   API 請求示例：

   ```
   {
       "AutomationRulesArns": [
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   ```

```
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. 若要檢視您帳戶的自動化規則，請從 Security Hub 系統管理員帳戶執行[list-automation-rules](#)命令。此命令會傳回規則 ARN 和規則的其他中繼資料。此命令不需要輸入參數，但您可以選擇性地`max-results`提供以限制結果數量和`next-token`分頁參數。

   範例命令：

   ```
   aws securityhub list-automation-rules  \
   --max-results 5 \
   --next-token cVpdnSampleTokenYcXgTockBW44c \
   --region us-east-1
   ```

2. 如需其他規則詳細資訊，包括規則的準則和動作，請從 Security Hub 系統管理員帳戶執行[batch-get-automation-rules](#)命令。

   範例命令：

   ```
   aws securityhub batch-get-automation-rules \
   --automation-rules-arns '["arn:aws:securityhub:us-
   east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
   cdef-EXAMPLE22222"]' \
   --region us-east-1
   ```

編輯自動化規則

當您編輯自動化規則時，這些變更會套用至 Security Hub 在規則編輯後產生或擷取的新發現項目和更新的發現項目。

選擇您偏好的方法，然後依照步驟編輯自動化規則的內容。您可以使用單一請求編輯一或多個規則。如需編輯規則順序的指示，請參閱[編輯規則順序](#)。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。
3. 選取您要編輯的規則。選擇「動作」和「編輯」
4. 視需要變更規則，然後選擇 [儲存變更]。

API

1. BatchUpdateAutomationRules從 Security Hub 系統管理員帳戶執行。
2. 對於RuleArn參數，請提供您要編輯之規則的 ARN。
3. 為您要編輯的參數提供新值。您可以編輯除外的任何參數RuleArn。

API 請求示例：

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. 從 Security Hub 系統管理員帳戶執行batch-update-automation-rules命令。
2. 對於RuleArn參數，請提供您要編輯之規則的 ARN。
3. 為您要編輯的參數提供新值。您可以編輯除外的任何參數RuleArn。

範例命令：

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

編輯規則順序

在某些情況下，您可能想要保留原樣的規則準則和動作，但是變更 Security Hub 套用自動化規則的順序。選擇您偏好的方法，然後按照步驟編輯規則順序。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。

3. 選取您要變更其順序的規則。選擇編輯優先順序。
4. 選擇「上移」，將規則的優先順序提高一個單位。選擇「下移」，將規則優先順序減少一個單位。選擇「移至頂端」，將規則的順序指定為 1 (這會讓規則優先順序高於其他現有規則)。

> **Note**
>
> 當您在 Security Hub 主控台中建立規則時，Security Hub 會根據規則建立的順序自動指派規則順序。最近建立的規則具有規則順序的最低數值，因此會先套用。

API

1. `BatchUpdateAutomationRules`從 Security Hub 系統管理員帳戶執行。
2. 針對`RuleArn`參數，提供您要編輯其順序之規則的 ARN。
3. 修改`RuleOrder`欄位的值。

> **Note**
>
> 如果多個規則具有相同的規則`RuleOrder`，Security Hub 會先針對`UpdatedAt`欄位套用具有較早值的規則 (也就是說，最近編輯的規則適用於最近編輯的規則)。

AWS CLI

1. 從 Security Hub 系統管理員帳戶執行`batch-update-automation-rules`命令。
2. 針對`RuleArn`參數，提供您要編輯其順序之規則的 ARN。
3. 修改`RuleOrder`欄位的值。

> **Note**
>
> 如果多個規則具有相同的規則`RuleOrder`，Security Hub 會先針對`UpdatedAt`欄位套用具有較早值的規則 (也就是說，最近編輯的規則適用於最近編輯的規則)。

刪除自動化規則

當您刪除自動化規則時，Security Hub 會將其從您的帳戶中移除，並且不再將該規則套用至發現項目。

選擇您偏好的方式，然後依照步驟刪除自動化規則。您可以刪除單一請求中的一或多個規則。

> **Tip**
>
> 除了刪除之外，您還可以停用規則。這會保留規則以供 future 使用，但是 Security Hub 不會將規則套用至任何相符的發現項目，除非您啟用該規則。

Console

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

   登入安全中心系統管理員帳戶。
2. 在導覽窗格中，選擇 [自動化]。
3. 選取您要刪除的規則。選擇「動作與刪除」(若要保留規則，但暫時停用規則，請選擇「停用」)。
4. 確認您的選擇，然後選擇 Delete (刪除)。

API

1. `BatchDeleteAutomationRules`從 Security Hub 系統管理員帳戶執行。
2. 對於`AutomationRulesArns`參數，請提供您要刪除之規則的 ARN (保留規則，但暫時停用該規則，並提`DISABLED`供`RuleStatus`參數)。

   API 請求示例：

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
```

```
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. 從 Security Hub 系統管理員帳戶執行batch-delete-automation-rules命令。
2. 對於automation-rules-arns參數，請提供您要刪除之規則的 ARN (保留規則，但暫時停用該規則，並提DISABLED供RuleStatus參數)。

範例命令：

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

自動化規則範例

本節包含一些常見使用案例的自動化規則範例。這些範例對應於 Security Hub 主控台中的規則範本。

當特定資源 (例如 S3 儲存貯體) 有風險時，將嚴重性提升為「嚴重」

在此範例中，當發現項目ResourceId中的是特定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體時，就會符合規則條件。規則動作是將相符發現項目的嚴重性變更為CRITICAL。您可以修改此範本以套用至其他資源。

API 請求示例：

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
```

```
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 指令範例：

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \
```

```
--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

提升與生產帳戶資源相關之發現項目的嚴重性

在此範例中，當在特定生產帳戶中產生HIGH嚴重性發現項目時，會比對規則條件。規則動作是將相符發現項目的嚴重性變更為CRITICAL。

API 請求示例：

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
```

```
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 指令範例：

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
```

```
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

隱藏資訊發現

在此範例中，規則條件與從 Amazon 傳送至 Security Hub 的INFORMATIONAL嚴重性發現項目相符 GuardDuty。規則動作是將相符搜尋結果的工作流程狀態變更為SUPPRESSED。

API 請求示例：

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
```

```
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 指令範例：

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
```

```
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}]' \
--region us-east-1
```

自動化回應與補救

使用 Amazon EventBridge，您可以自動化AWS服務，以自動回應系統事件，例如應用程式可用性問題或資源變更。AWS服務中的事件會以近乎即時且保證的方式交付到 EventBridge 。您可以撰寫簡單的規則來指出您感興趣的事件，以及當事件符合規則時要採取的自動化動作。可以自動觸發的動作如下：

- 呼叫 AWS Lambda 函數
- 調用 Amazon EC2 運行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 啟動 AWS Step Functions 狀態機器
- 通知 Amazon SNS 主題或 Amazon SQS 佇列
- 將問題清單傳送至第三方票證系統、聊天、SIEM 或事件反應及管理工具

Security Hub 會自動將所有新的發現項目和所有更新傳送至現有的發現項目 EventBridge 作為 EventBridge 事件。您也可以建立自訂動作，讓您將選取的發現項目和深入分析結果傳送至 EventBridge。

然後，您可以設定 EventBridge 規則來回應每種類型的事件。

如需使用的詳細資訊 EventBridge，請參閱 Amazon 使用 EventBridge 者指南。

> **Note**
>
> 最佳做法是確保授與使用者存取的權限 EventBridge 使用僅授與所需權限的最低權限 IAM 政策。
> 如需詳細資訊，請參閱 Amazon 中的身分識別和存取管理 EventBridge。

AWS解決方案中還提供了一組用於跨帳戶自動回應和補救的範本。範本會利用 EventBridge 事件規則和 Lambda 函數。您可以使用AWS CloudFormation和部署解決方案AWS Systems Manager。該解決方案可以建立完全自動化的回應和補救動作。它也可以使用 Security Hub 自訂動作來建立使用者觸發的回應和補救動作。如需如何設定及使用解決方案的詳細資訊，請參閱解決方案上AWS的自動化安全回應頁面。

主題

- 與安全中心整合的類型 EventBridge
- EventBridge Security Hub 的事件格式
- 設定自動傳送發現項目的 EventBridge 規則
- 使用自訂動作將發現項目和洞察結果傳送至 EventBridge

與安全中心整合的類型 EventBridge

Security Hub 使用下列 EventBridge 事件類型來支援下列類型的整合 EventBridge。

在 Security Hub 的 EventBridge 儀表板上，「所有事件」包含所有這些事件類型。

所有問題清單 (Security Hub Findings - Imported)

Security Hub 會自動將所有新的發現項目和所有更新傳送至現有的發現項目 EventBridge 作為Security Hub Findings - Imported事件。每個Security Hub Findings - Imported事件都包含一個發現。

每個BatchImportFindings和BatchUpdateFindings請求都會觸發一個Security Hub Findings - Imported事件。

對於管理員帳戶，中的事件摘要 EventBridge 包括來自其帳戶和其成員帳戶的發現項目的事件。

在彙總區域中，事件摘要包含來自彙總「區域」與「連結區域」之發現項目的事件。跨區域搜尋結果會以近乎即時的方式包含在事件摘要中。如需如何設定尋找結果彙總的相關資訊，請參閱跨區域彙總。

您可以在 EventBridge 自動將發現結果路由到 Amazon S3 儲存貯體、修復工作流程或第三方工具中定義規則。這些規則可以包含只有在發現項目具有特定屬性值時才套用規則的篩選器。

您可以使用此方法，將所有發現項目或具有特定特性的所有發現項目自動傳送至回應或修正工作流程。

請參閱 the section called “設定自動傳送發現項目的規則”。

自訂動作問題清單 (Security Hub Findings - Custom Action)

Security Hub 也會將與自訂動作相關聯的發現項目 EventBridge 當做Security Hub Findings - Custom Action事件傳送至。

對於使用 Security Hub 主控台的分析師而言，這對於想要將特定發現項目或一小組發現項目傳送至回應或補救工作流程的分析師非常有用。您一次最多可以為 20 個問題清單選取自訂動作。每個發現項目都會 EventBridge 以個別 EventBridge 事件的形式傳送至。

建立自訂動作時，請為其指派自訂動作 ID。您可以使用此 ID 建立 EventBridge 規則，該規則會在收到與該自訂動作 ID 相關聯的發現項目後採取指定動作。

請參閱 the section called “配置和使用自訂動作”。

例如，您可以在安全中心中建立名為的自訂動作`send_to_ticketing`。然後在中建立規則 EventBridge，該規則會在 EventBridge 收到包含`send_to_ticketing`自訂動作 ID 的發現項目時觸發。規則包含了將問題清單傳送至您票證系統的邏輯。然後，您可以在 Security Hub 中選取發現項目，並使用 Security Hub 中的自訂動作，將發現項目手動傳送至您的票務系統。

如需如何將 Security Hub 發現項目傳送至以 EventBridge 供進一步處理的範例，請參閱如何將AWS Security Hub自訂動作與整合以 PagerDuty及如何在合作AWS夥伴網路 (APN) 部落格AWS Security Hub上啟用自訂動作。

自訂動作的洞見結果 (Security Hub Insight Results)

您也可以使用自訂動作，將深入解析結果集作 EventBridge 為Security Hub Insight Results事件傳送至。洞察結果是匹配見解的資源。請注意，當您將分析結果傳送至時 EventBridge，您不會將發現項目

傳送至 EventBridge。您只會傳送與見解結果相關聯的資源識別碼。您一次最多可以傳送 100 個資源識別符。

與發現項目的自訂動作類似，您先在 Security Hub 中建立自訂動作，然後在中建立規則 EventBridge。

請參閱 the section called “配置和使用自訂動作”。

例如，假設您看到您想要與同事分享的特定深入分析結果。在這種情況下，您可以使用自定義操作通過聊天或票務系統將該見解結果發送給同事。

EventBridge Security Hub 的事件格式

Security Hub Findings - ImportedSecurity Findings - Custom Action、和Security Hub Insight Results事件類型使用下列事件格式。

事件格式是 Security Hub 傳送事件時所使用的格式 EventBridge。

Security Hub Findings - Imported

Security Hub Findings - Imported從 Security Hub 傳送以 EventBridge 使用下列格式的事件。

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

*<finding content>*是事件所傳送之發現項目的內容 (JSON 格式)。每個事件都會傳送一個發現項目。

如需尋找屬性的完整清單，請參閱AWS 安全性搜尋結果格式 (ASFF)。

如需如何設定由這些事件觸發之 EventBridge 規則的相關資訊，請參閱the section called “設定自動傳送發現項目的規則”。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action從 Security Hub 傳送以 EventBridge 使用下列格式的事件。每個發現項目都會在單獨的事件中傳送。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*是事件所傳送之發現項目的內容 (JSON 格式)。每個事件都會傳送一個發現項目。

如需尋找屬性的完整清單，請參閱AWS 安全性搜尋結果格式 (ASFF)。

如需如何設定由這些事件觸發之 EventBridge 規則的相關資訊，請參閱the section called “配置和使用自訂動作”。

Security Hub Insight Results

Security Hub Insight Results從 Security Hub 傳送以 EventBridge 使用下列格式的事件。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

如需如何建立由這些事件觸發之 EventBridge 規則的詳細資訊，請參閱the section called “配置和使用自訂動作”。

設定自動傳送發現項目的 EventBridge 規則

您可以在中建立規則 EventBridge ，以定義收到Security Hub Findings - Imported事件時要採取的動作。 Security Hub Findings - Imported事件由和的更新觸發`BatchImportFindings``BatchUpdateFindings`。

每個規則都包含一個事件模式，用於識別觸發規則的事件。事件模式一律包含事件來源 (`aws.securityhub`) 和事件類型 (Security Hub 發現項目-已匯入)。事件模式也可以指定篩選器，以識別套用規則的發現項目。

然後規則會識別規則目標。目標是在 EventBridge 收到「Security Hub 發現項目-已匯入」事件時要採取的動作，且發現項目符合篩選器。

此處提供的說明使用 EventBridge 控制台。使用主控台時， EventBridge會自動建立必要的以資源為基礎的策略，以 EventBridge 便寫入 CloudWatch 記錄。

您也可以使用 PutRuleAPI 的 EventBridge API 操作。但是，如果您使用 EventBridge API，則必須建立以資源為基礎的政策。如需所需政策的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的CloudWatch 日誌許可。

事件模式的格式

Security Hub 發現項目-匯入事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`將 Security Hub 識別為產生事件的服務。
- `detail-type`識別事件的類型。
- `detail`是選擇性的，並提供事件模式的篩選器值。如果事件模式不包含`detail`欄位，則所有發現項目都會觸發規則。

您可以根據任何發現項目屬性來篩選發現項目。您可以針對每個屬性提供一或多個值的逗號分隔陣列。

```
"<attribute name>": [ "<value1>", "<value2>"]
```

如果您為一個屬性提供多個值，則這些值會以連接`OR`。如果發現項目具有任何列出的值，則尋找項目符合個別屬性的篩選條件。例如，如果您同時提供`INFORMATIONAL`和`LOW`作為的值`Severity.Label`，則如果發現項目的嚴重性標籤為`INFORMATIONAL`或，則相符項目`LOW`。

屬性由連接`AND`。如果搜尋結果符合所有提供屬性的篩選條件，就會相符。

當您提供屬性值時，它必須反映該屬性在「AWS安全性發現格式」(ASFF) 結構中的位置。

> **Tip**
>
> 篩選控制項發現項目時，建議使用`SecurityControlId`或 `SecurityControlArn` ASFF 欄位作為篩選器，而不是使用`Title`或`Description`。後一個字段可以偶爾更改，而控制 ID 和 ARN 是靜態標識符。

在下列範例中，事件模式會為`ProductArn`和提供篩選器值`Severity.Label`，因此，如果尋找項目是由 Amazon Inspector 產生，且嚴重性標籤為`INFORMATIONAL`或，則會發現相符項目`LOW`。

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

建立事件規則

您可以使用預先定義的事件模式或自訂事件模式在中建立規則 EventBridge。如果您選取預先定義的樣式， EventBridge 會自動填滿`source`和`detail-type`。 EventBridge 也提供欄位來指定下列發現項目屬性的篩選值：

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`

- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

若要建立 EventBridge 規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 使用下列值建立監視尋找事件的 EventBridge 規則：
   - 針對 Rule type (規則類型) 選擇 Rule with an event pattern (具有事件模式的規則)。
   - 選擇如何建立事件模式。

若要使用... 建立事件模式	執行此作業...
一個範本	在「事件模式」區段中，選擇下列選項： • 在 Event source (事件來源) 欄位中，選擇 AWS services (服務)。 • 對於AWS服務，請選擇 Security Hub。 • 針對「事件類型」，選擇「Security Hub 發現項目-匯入 • (選用) 若要使規則更具體，請新增篩選條件值。例如，若要將規則限制為具有作用中記錄狀態的發現項目，請針對「特定記錄」狀態選擇「作用中」。

若要使用... 建立事件模式	執行此作業...

自訂事件模式
 	
(如果您要根據未顯示在 EventBridge 主控台中的屬性篩選發現項目，請使用自訂模式)。
	• 在 [事件模式] 區段中，選擇 [自訂模式 (JSON 編輯器)]，然後將下列事件模式貼到文字區域中：
	
	`{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }`
	
	• 更新事件模式以包含要用作篩選器的屬性和屬性值。
	
	例如，若要將規則套用至驗證狀態為的發現項目TRUE_POSITIVE ，請使用下列模式範例：
	
	`{ "source": [ "aws.securityhub" ],`

若要使用... 建立事件模式	執行此作業...

	<pre>"detail-type": [
	"Security
	Hub Findings -
	Imported"
	],
	"detail": {
	"findings": {
	"Verifica
	tionState":
	["TRUE_POSITIVE"]
	}
	}
	}</pre>

- 在 Target types (目標類型) 中，選擇 AWS service (服務)，在 Select a target (選取目標) 中，選擇 Amazon SNS 主題或 AWS Lambda 函數等任一目標。當接收到符合規則中定義之事件模式的事件時，就會觸發目標。

如需有關建立規則的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的建立可對事件做出反應的 Amazon EventBridge 規則。

使用自訂動作將發現項目和洞察結果傳送至 EventBridge

若要使用 Security Hub 自訂動作將發現項目或見解結果傳送至 EventBridge，您必須先在 Security Hub 中建立自訂動作。然後，定義適用於 EventBridge 您自訂動作的規則。

您最多可以建立 50 個自訂動作。

如果您啟用了跨區域聚總，並從聚總區域管理搜尋結果，請在聚總區域中建立自訂作業。

中的規則 EventBridge 使用自訂動作中的 ARN。

建立自訂動作 (主控台)

當您建立自訂動作時，您可以指定名稱、描述和唯一識別碼。

若要在資訊安全中心 (主控台) 中建立自訂動作

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。

2. 在導覽窗格中，選擇 Settings (設定)，然後選擇 Custom actions (自訂動作)。
3. 選擇 Create custom action (建立自訂動作)。
4. 為動作提供 Name (名稱)、Description (描述) 和 Custom action ID (自訂動作 ID)。

   Name (名稱) 必須小於 20 個字元。

   每個AWS帳戶的自訂動作 ID 必須是唯一的。
5. 選擇 Create custom action (建立自訂動作)。
6. 記下 Custom action ARN (自訂動作 ARN)。在您於 EventBridge 中建立規則以和此動作建立關聯時，您必須使用 ARN。

建立自訂動作 (Security Hub API、AWS CLI)

若要建立自訂動作，您可以使用 API 呼叫或AWS Command Line Interface.

若要建立自訂動作 (Security Hub API，AWS CLI)

- Security Hub API — 使用CreateActionTarget操作。建立自訂動作時，您會提供名稱、說明和自訂動作識別元。
- AWS CLI— 在命令列中，執行create-action-target命令。

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

範例

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

定義規則 EventBridge

若要處理自訂動作，您必須在中建立對應的規則 EventBridge。規則定義包括自訂動作的 ARN。

Security Hub 發現項目-自訂動作事件的事件模式具有下列格式：

```
{
  "source": [
```

```
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub 智慧型掃描結果事件的事件模式具有下列格式：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

在這兩種模式中，都*<custom action ARN>*是自訂動作的 ARN。您可以設定套用至多個自訂動作的規則。

此處提供的說明適用於主 EventBridge 控台。使用主控台時， EventBridge 會自動建立必要的以資源為基礎的策略，以 EventBridge 便寫入 CloudWatch 記錄。

您也可以使用 PutRuleAPI 的 EventBridge API 操作。但是，如果您使用 EventBridge API，則必須建立以資源為基礎的政策。如需所需政策的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的CloudWatch 日誌許可。

若要在中定義規則 EventBridge

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇 Rules(規則)。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的名稱和描述。
5. 針對 Event bus (事件匯流排)，選擇要與此規則建立關聯的事件匯流排。如果您想要此規則匹配來自您的帳戶的事件，請選取 預設值。當您帳戶中的 AWS 服務發出事件時，一律會前往您帳戶的預設事件匯流排。

6. 針對 Rule type (規則類型) 選擇 Rule with an event pattern (具有事件模式的規則)。
7. 選擇下一步。
8. 在事件來源，選擇 AWS 事件。
9. 針對事件模式，選擇事件模式表單。
10. 在事件來源欄位中，選擇 AWS 服務。
11. 對於AWS服務，請選擇 Security Hub。
12. 針對 Event type (事件類型)，執行下列其中一項操作：
    - 若要在將發現項目傳送至自訂動作時建立要套用的規則，請選擇 Security Hub 發現項目-自訂動作。
    - 若要建立在傳送見解結果至自訂動作時套用的規則，請選擇 Security Hub 智慧型掃描結果。
13. 選擇特定的自定義操作 ARN，添加自定義操作 ARN。

    如果規則套用至多個自訂動作，請選擇「新增」以新增更多自訂動作 ARN。
14. 選擇下一步。
15. 在 「選取目標」 下，選擇並設定要在符合此規則時呼叫的目標。
16. 選擇 Next (下一步)。
17. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 標籤。
18. 選擇 Next (下一步)。
19. 檢閱規則的詳細資訊，然後選擇 Create rule (建立規則)。

    當您對帳戶中的發現項目或洞察結果執行自訂動作時，會在中產生事件 EventBridge。

選取發現項目和見解結果的自訂動作

建立 Security Hub 自訂動作和 EventBridge 規則之後，您可以將發現項目和深入分析結果傳送至 EventBridge 進一步管理和處理。

EventBridge 只有在檢視事件的帳戶中，才會將事件傳送至。如果您使用管理員帳戶檢視發現項目，則事件會以管理員帳戶傳送至 EventBridge 。

為了使 AWS API 調用生效，目標代碼的實現必須將角色切換到成員帳戶中。這也表示您切換到的角色必須部署到需要動作的每個成員。

若要傳送發現項目至 EventBridge

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 顯示發現項目清單：
   - 從「搜尋結果」中，您可以檢視所有已啟用產品整合與控制項的發現項目。
   - 在安全性標準中，您可以瀏覽至從所選控制項產生的發現項目清單。請參閱 the section called "檢視控制項的詳細資訊"。
   - 從「整合」中，您可以導覽至已啟用整合所產生的發現項目清單。請參閱 the section called "檢視整合傳送的問題清單"。
   - 從 In sights，您可以導覽至發現項目清單，以取得深入解析結果。請參閱 the section called "檢視洞見結果和問題清單"。
3. 選取要傳送至的發現項目 EventBridge。您一次最多可以選取 20 個問題清單。
4. 從動作中，選擇與要套用之 EventBridge 規則對齊的自訂動作。

   Security Hub 會針對每個發現項目傳送個別的 Security Hub 發現項目-自訂動作事件。

若要傳送見解結果至 EventBridge

1. 開啟位於 https://console.aws.amazon.com/securityhub/ 的 AWS Security Hub 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 在「見解」頁面上，選擇包含要傳送之結果的深入分析 EventBridge。
4. 選取要傳送的深入分析結果 EventBridge。您一次最多可以選取 20 個結果。
5. 從動作中，選擇與要套用之 EventBridge 規則對齊的自訂動作。

AWS安全中心中的產品整合

AWSSecurity Hub 可以彙總安全性從多個AWS服務和支援的AWS合作夥伴網路 (APN) 安全解決方案尋找資料。此彙總可提供您AWS環境中安全性與合規性的全方位檢視。

您也可以傳送專屬自訂安全產品所產生的問題清單。

> **Important**
>
> 透過支援AWS的合作夥伴產品整合，Security Hub 只會接收並合併您AWS 帳戶在中啟用 Security Hub 之後產生的發現項目。
> 此服務不會追溯接收和合併您啟用 Security Hub 之前產生的安全性發現項目。

如需有關 Security Hub 如何針對擷取發現項目收費的詳細資訊，請參閱 Security Hub 定價。

主題

- 管理產品整合
- AWS 服務與 AWS Security Hub 的整合
- 可用的第三方合作夥伴產品整合
- 使用自訂產品整合將發現項目傳送至 AWS Security Hub

管理產品整合

中的「整合」頁面可讓您存取所有可用AWS和第三方產品整合。AWS Management ConsoleAWS安全中心 API 還提供了可讓您管理整合的操作。

> **Note**
>
> 某些整合無法在所有區域中使用。如果目前區域不支援整合，則不會在「整合」頁面上列出該整合。
> 另請參閱 the section called “在中國（北京）和中國（寧夏）支持的集成” 和 the section called “AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 支援的整合”。

檢視和篩選整合清單 (主控台)

您可以從 Integrations (整合) 頁面檢視和篩選整合清單。

檢視整合清單

1. 開啟 Sec AWS urity Hub 主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在 [安全性中心] 功能窗格中，選擇 [整合]。

在 Integrations (整合) 頁面上，會先列出與其他 AWS 服務的整合，再列出與第三方產品的整合。

針對每個整合，Integrations (整合) 頁面均提供以下資訊。

- 公司名稱
- 產品名稱
- 整合描述
- 整合的適用類別
- 啟用整合的方式
- 整合目前的狀態

您可以從下列欄位中輸入文字來篩選清單。

- 公司名稱
- 產品名稱
- 整合描述
- 類別

檢視產品整合的相關資訊 (資訊 Security Hub API、AWS CLI)

若要檢視產品整合的相關資訊，您可以使用 API 呼叫或AWS Command Line Interface. 您可以顯示有關所有產品整合的資訊，或已啟用之產品整合的相關資訊。

若要檢視所有可用產品整合的相關資訊 (資訊 Security Hub API，AWS CLI)

- Security Hub API — 使用`DescribeProducts`操作。若要識別要傳回的特定產品整合，請使用`ProductArn`參數提供整合 ARN。

- AWS CLI— 在命令列中，執行describe-products命令。若要識別要退回的特定產品整合，請提供整合 ARN。

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

範例

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

若要檢視您已啟用之產品整合的相關資訊 (Security Hub API，AWS CLI)

- Security Hub API — 使用ListEnabledProductsForImport操作。
- AWS CLI— 在命令列中，執行list-enabled-products-for-import命令。

```
aws securityhub list-enabled-products-for-import
```

啟用整合

在 Integrations (整合) 頁面上，每個整合都會提供啟用整合所需進行的步驟。

針對大多數與其他 AWS 服務的整合，唯一要進行的步驟是啟用其他服務。整合資訊包含前往服務首頁的連結。當您啟用其他服務時，系統會自動建立並套用允許 Security Hub 從服務接收發現項目的資源層級權限。

針對第三方產品整合，您可能需要從 AWS Marketplace 購買整合，再加以設定。整合資訊會提供執行這些任務的連結。

如果 AWS Marketplace 提供多個產品版本，請選取要訂閱的版本，然後選擇 Continue to Subscribe (繼續訂閱)。例如，有些產品提供標準版本和 AWS GovCloud (US) 版本。

當您啟用產品整合時，資源政策會自動連接到該產品訂閱。此資源原則會定義 Security Hub 從該產品接收發現項目所需的權限。

停用和啟用從整合接收問題清單的流程 (主控台)

在「整合」頁面上，對於傳送發現項目的整合，「狀態」 資訊會指出您目前是否正在接受發現項目。

如果要停止接受問題清單，請選擇 Stop accepting findings (停止接受問題清單)。

如果要繼續接受問題清單，請選擇 Accept findings (接受問題清單)。

從整合停用發現項目的流程 (Security Hub API,AWS CLI)

若要停用整合中發現項目的流程，您可以使用 API 呼叫或AWS Command Line Interface.

若要停用整合中的發現項目流程 (Security Hub API，AWS CLI)

- Security Hub API — 使用DisableImportFindingsForProduct操作。若要識別要停用的整合，您需要訂閱的 ARN。若要取得已啟用整合的訂閱 ARN，請使用ListEnabledProductsForImport作業。
- AWS CLI— 在命令列中，執行disable-import-findings-for-product命令。

```
aws securityhub disable-import-findings-for-product --product-subscription-
arn <subscription ARN>
```

範例

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

啟用來自整合的發現項目流程 (Security Hub API、AWS CLI)

若要啟用整合中發現項目的流程，您可以使用 API 呼叫或AWS Command Line Interface.

若要啟用整合的發現項目流程 (Security Hub API，AWS CLI)

- Security Hub API — 使用EnableImportFindingsForProduct操作。若要讓 Security Hub 接收來自整合的發現項目，您需要產品 ARN。若要取得可用整合的 ARN，請使用此DescribeProducts作業。
- AWS CLI：在命令列中執行 enable-import-findings-for-product 命令。

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

範例

```
aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

檢視整合傳送的問題清單

對於您接受發現項目 (狀態為「接受發現項目」) 的整合，若要檢視發現項目清單，請選擇「查看發現項目」。

問題清單會顯示工作流程狀態為 NEW 或 NOTIFIED 選取整合的作用中問題清單。

如果您啟用「跨區域聚總」，則在聚總區域中，清單會包含來自聚總區域與已啟用整合之連結區域的搜尋結果。Security Hub 不會根據跨區域彙總組態自動啟用整合。

在其他區域中，整合的搜尋結果清單只會包含目前「區域」的搜尋結果。

如需如何設定跨區域彙總的相關資訊，請參閱跨區域彙總。

從問題清單，您可以執行下列動作。

- 變更清單的篩選條件和群組
- 檢視個別問題清單的詳細資訊
- 更新問題清單的工作流程狀態
- 將問題清單傳送到自訂動作

AWS 服務與 AWS Security Hub 的整合

AWSSecurity Hub 支持與其他幾個集成AWS 服務。

> **Note**
>
> 某些整合功能僅適用於選取項目AWS 區域。
> 如果特定區域不支援整合，則不會在 Security Hub 主控台的 [整合] 頁面上列出該整合。
> 如需詳細資訊，請參閱 在中國（北京）和中國（寧夏）支持的集成 及 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 支援的整合。

除非下方指出，否則會在您啟用 Security Hub 之後，自動啟用將發現項目傳送至 Security Hub 的AWS服務整合。接收 Security Hub 發現項目的整合可能需要其他步驟才能啟用。檢閱每個整合的相關資訊以進一步了解。

與 Security Hub 的AWS服務整合概觀

以下是將發現項目傳送至安全中心或從 Security Hub 全中心接收發現項目的AWS服務概觀。

綜合AWS服務	Direction
AWS Config	發送發現
AWS Firewall Manager	發送發現
亞馬遜 GuardDuty	發送發現
AWS Health	發送發現
AWS Identity and Access Management Access Analyzer	發送發現
Amazon Inspector	發送發現
AWS IoT Device Defender	發送發現
Amazon Macie	發送發現
AWS Systems Manager 修補程式管理員	發送發現
AWS Audit Manager	接收發現
AWS Chatbot	接收發現
Amazon Detective	接收發現
Amazon Security Lake	接收發現
AWS Systems Manager檔案總管和 OpsCenter	接收和更新發現

綜合AWS服務	Direction	
AWS Trusted Advisor	接收發現	

AWS將發現項目傳送至 Security Hub 的服務

下列AWS服務會將發現項目傳送至 Security Hub，以與 Security Hub 整合。Security Hub 將發現項目轉換為AWS安全性發現格式。

AWS Config（發送發現）

AWS Config是一項可讓您評估、稽核和評估AWS資源組態的服務。 AWS Config持續監控和記錄您的AWS資源配置，並允許您根據所需的配置自動評估記錄的配置。

透過使用與整合AWS Config，您可以在 Security Hub 中將AWS Config受管理和自訂規則評估的結果視為發現項目。這些發現項目可與其他 Security Hub 發現項目一起檢視，提供安全性狀態的全面概觀。

AWS Config使用亞馬遜 EventBridge 將AWS Config規則評估發送到 Security Hub。Security Hub 會將規則評估轉換為遵循「AWS安全性搜尋結果格式」的發現項目。然後，Security Hub 會取得有關受影響資源的詳細資訊，例如 Amazon 資源名稱 (ARN) 和建立日期，以最佳方式豐富發現項目。AWS Config規則評估中的資源標籤不會包含在 Security Hub 發現項目中。

如需有關此整合的詳細資訊，請參閱下列各節。

AWS Config 如何將問題清單傳送到 Security Hub

安全中心中的所有發現項目都使用 ASFF 的標準 JSON 格式。ASFF 包含有關發現項目來源、受影響資源以及發現項目目前狀態的詳細資訊。 AWS Config透 EventBridge過以下方式將受管理和自訂規則評估傳送至 Security Hub。Security Hub 會將規則評估轉換為遵循 ASFF 的發現項目，並以最佳方式豐富發現項目。

AWS Config傳送至 Security Hub 的發現項目類型

啟動整合後，AWS Config會將所有AWS Config受管規則和自訂規則的評估傳送至 Security Hub。只會排除來自服務連結AWS Config規則的評估，例如用來執行安全性控制檢查的評估。

將發AWS Config現項目傳送至 Security Hub

當整合啟動時，Security Hub 會自動指派接收發現項目所需的權限AWS Config。Security Hub 使用 service-to-service 層級許可，為您提供一種安全的方式來啟動此整合，並AWS Config透過 Amazon 匯入發現項目 EventBridge。

傳送問題清單延遲

AWS Config建立新發現項目時，您通常可以在五分鐘內檢視 Security Hub 中的發現項目。

無法使用 Security Hub 時重試

AWS Config透過將發現項目傳送至 Security Hub 以盡最大努力的 EventBridge基礎。當事件未成功傳遞至 Security Hub 時，最多可 EventBridge重試傳遞 24 小時或 185 次，以先到者為準。

更新安全中心中的AWS Config現有發現項

AWS Config將發現項目傳送至 Security Hub 之後，它可以將更新傳送至相同的發現項目至 Security Hub，以反映對尋找活動的其他觀察。只會針對`ComplianceChangeNotification`事件傳送更新。如果沒有發生任何符合性變更，則不會將更新傳送至 Security Hub。Security Hub 會在最近更新 90 天後刪除發現項目，如果未發生更新，則會在建立後刪除 90 天。

AWS Config發現項目存在的區域

AWS Config發現發生在區域基礎上。 AWS Config將發現項目傳送至發現項目發生的相同區域或區域中的安全中心。

檢視安全中樞的AWS Config發現項目

若要檢視AWS Config發現項目，請從 [安全中心] 瀏覽窗格中選擇 [發現項目 若要篩選發現項目以僅顯示AWS Config發現項目，請在搜尋列下拉式清單中選擇「產品名稱」。輸入 Config，然後選擇套用。

解譯資訊安全中心中的AWS Config尋找名稱

Security Hub 將AWS Config規則評估轉換為. AWS 安全性搜尋結果格式 (ASFF) AWS Config與 ASFF 相比，規則評估使用不同的事件模式。下表會將AWS Config規則評估欄位與其 ASFF 對應項目，如同它們顯示在「安全性中樞」中一樣。

Config 規則評估尋找項目型	ASFF 問題清單類型	硬編碼值
細節。 awsAccountId	AwsAccountId	

Config 規則評估尋找項目型	ASFF 問題清單類型	硬編碼值
細節。 newEvaluationResult。resultRecordedTime	CreatedAt	
細節。 newEvaluationResult。resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region>「arn:: 安全集線器:: 產品/AWS /配置」
	ProductName	「Config」
	CompanyName	"AWS"
	區域	「歐盟中央 -1 號」
configRuleArn	GeneratorId, ProductFields	
細節。 ConfigRuleARN /查找/哈希	Id	
細節。 configRuleName	標題 ， ProductFields	
細節。 configRuleName	描述	「此發現項目是針對配置規則的資源符合性變更而建立的：${detail.ConfigRuleName} 」
組態項目「ARN」或 Security Hub 計算 ARN	資源 [我] .id	
詳細資訊. 資源類型	資源 [i]. 類型	"AwsS3Bucket"
	資源 [i]. 分區	"aws"
	資源 [i]. 地區	「歐盟中央 -1 號」
組態項目「組態」	資源 [i]. 詳細資訊	
	SchemaVersion	「

Config 規則評估尋找項目型	ASFF 問題清單類型	硬編碼值
	嚴重性. 標籤	請參閱下面的「解釋嚴重性標籤」
	類型	["軟體和組態檢查"]
細節。 newEvaluationResult. 合規性類型	合規性. 狀態	「失敗」、「不可用」、「已通過」或「警告」
	工作流程. 狀態	如果AWS Config發現項目是以「符合性」產生，則為「已解決」。狀態為「已通過」，或者如果「符合性」。狀態從「失敗」變更為「已通過」。否則，「工作流程. 狀態」將為「新建」。您可以透過 BatchUpdateFindingsAPI 作業變更此值。

解譯嚴重性標籤

AWS Config規則評估中的所有發現項目在 ASFF 中都有預設嚴重性標籤 MEDIUM。您可以使用 BatchUpdateFindingsAPI 作業更新發現項目的嚴重性標籤。

來自 AWS Config 的一般問題清單

Security Hub 將AWS Config規則評估轉換為跟隨 ASFF 的發現項目。以下是 ASFF AWS Config 中的典型發現項目範例。

> **Note**
>
> 如果說明超過 1024 個字元，則會截斷為 1024 個字元，結尾會顯示「(截斷)」。

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
```

```
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
```

```
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

啟用與設定整合

啟用 Security Hub 之後，系統會自動啟動此整合。 AWS Config立即開始將發現發現發送到 Security Hub。

停止將發現項目發佈到 Security Hub

若要停止將發現項目傳送至 Security Hub，您可以使用 Security Hub 主控台、安全中心 API 或AWS CLI.

請參閱 停用和啟用從整合接收問題清單的流程 (主控台) 或 從整合停用發現項目的流程 (Security Hub API,AWS CLI)。

AWS Firewall Manager（發送發現）

當資源的 Web 應用程式防火牆 (WAF) 原則或 Web 存取控制清單 (Web ACL) 規則不符合時，Firewall Manager 員會將發現項目傳送至 Security Hub。當未保護資源或發現攻擊時AWS Shield Advanced，Firewall Manager 員也會傳送發現項目。

啟用 Security Hub 之後，此整合會自動啟動。Firewall Manager 員會立即開始將發現項目傳送至 Security Hub

若要進一步了解整合，請檢視 Security Hub 主控台中的 [整合] 頁面。

若要深入瞭解 Firewall Manager 員，請參閱AWS WAF開發人員指南。

亞馬遜 GuardDuty （發送發現）

GuardDuty 發送它生成的所有發現到 Security Hub。

來自的新發現項目 GuardDuty 會在五分鐘內傳送至 Security Hub。發現項目的更新會根據設定 EventBridge 中 Amazon 的「已更新的發現項目 GuardDuty 」設定傳送。

當您使用 GuardDuty [設定] 頁面產生 GuardDuty 範例發現項目時，Security Hub 會收到發現項目範例，並忽略發現項目類型`[Sample]`中的前置詞。例如，中的範例尋找項目類型會顯示 GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions`為 [安全性`Recon:IAMUser/ResourcePermissions`中心] 中。

啟用 Security Hub 之後，此整合會自動啟動。 GuardDuty 立即開始將發現發現發送到 Security Hub。

如需有關 GuardDuty 整合的詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的與AWS安全中心整合。

AWS Health（發送發現）

AWS Health讓您持續掌握資源效能，以及AWS服務和帳戶的可用性。您可以使用AWS Health事件來了解服務和資源變更如何影響執行的應用程式AWS。

與的整合AWS Health不會使用`BatchImportFindings`。而是AWS Health使用 service-to-service 事件訊息將發現項目傳送至 Security Hub。

如需有關整合的詳細資訊，請參閱下列各節。

AWS Health 如何將問題清單傳送到 Security Hub

在 Security Hub 中，將安全問題作為問題清單進行追蹤。有些問題清單是由其他 AWS 服務或第三方合作夥伴偵測所得。Security Hub 也有一組規則，用來偵測安全問題並產生問題清單。

Security Hub 提供用來跨所有這些來源管理問題清單的工具。您可以檢視並篩選問題清單列表，並檢視問題清單的詳細資訊。請參閱 檢視尋找項目清單與詳細資訊 AWS Security Hub。您也可以追蹤問題清單的調查狀態。請參閱 針對中的發現採取行動 AWS Security Hub。

安全中心中的所有發現項目都使用標準 JSON 格式，稱為AWS 安全性搜尋結果格式 (ASFF). ASFF 包含有關問題來源、受影響的資源以及發現項目目前狀態的詳細資訊。

AWS Health 是負責將問題清單傳送至 Security Hub 的 AWS 服務之一。

AWS Health傳送至 Security Hub 的發現項目類型

啟用整合後，會將其產生的所有安全性相關發現項目AWS Health傳送至 Security Hub。發現項目會使用傳送至 Security Hub AWS 安全性搜尋結果格式 (ASFF)。安全性相關發現項目的定義如下：

- 與AWS安全服務相關聯的任何發現
- 任何與單詞`security`，`abuse`或`certificate`在AWS Health類型代碼中的發現
- 任何發現AWS Health服務在哪裡`risk`或 `abuse`

將發AWS Health現項目傳送至 Security Hub

當您選擇接受來源的發現項目時AWS Health，Security Hub 會自動指派接收發現項目所需的權限AWS Health。Security Hub 使用 service-to-service 層級許可，為您提供安全、簡單的方法來啟用此整合，並代表您AWS Health透過 Amazon EventBridge 匯入發現項目。選擇接受發現項目會授與 Security Hub 使用發現項目的權限AWS Health。

傳送問題清單延遲

AWS Health建立新的發現項目時，通常會在五分鐘內傳送至 Security Hub。

無法使用 Security Hub 時重試

AWS Health透過將發現項目傳送至 Security Hub 以盡最大努力的 EventBridge基礎。當事件未成功傳遞至 Security Hub 時，請 EventBridge重試傳送事件 24 小時。

更新 Security Hub 中的現有問題清單

AWS Health將發現項目傳送至 Security Hub 之後，它可以將更新傳送至相同的發現項目，以反映對尋找活動的其他觀察結果至 Security Hub。

發現項目存在的區域

針對全域事件，AWS Health會將調查結果傳送至 us-east-1 (AWS磁碟分割)、cn-西北 -1 (中國分割區) 和 -1 (磁碟分割) 中的 Security Hub。 gov-us-west GovCloud AWS Health將區域特定事件傳送至事件發生的相同區域中的 Security Hub。

檢視安全中樞的AWS Health發現項目

若要在 Security Hub 中檢視您的AWS Health發現項目，請從導覽面板中選擇發現項目。若要篩選發現項目以僅顯示AWS Health發現項目，請從「產品名稱」欄位選擇「Health 全狀況」

解譯資訊安全中心中的AWS Health尋找名稱

AWS Health使用將發現項目傳送至 Security Hub AWS 安全性搜尋結果格式 (ASFF)。 AWS Health與 Security Hub ASFF 格式相比，發現使用不同的事件模式。下表詳細說明了所有AWS Health發現字段及其 ASFF 對應項目，因為它們出現在 Security Hub 中。

Health 發現類型	ASFF 問題清單類型	硬編碼值
帳戶	AwsAccountId	
詳情. 開始時間	CreatedAt	
詳情活動說明. 最新說明	描述	
細節。 eventTypeCode	GeneratorId	
詳細信息。事件（包括帳戶）+ 詳細哈希值。	Id	
<region>「ARN: aws: 安全中心::: 產品/AWS /健康」	ProductArn	
帳戶或 resourceId	資源 [我] .id	
	資源 [i]. 類型	「其他」
	SchemaVersion	「
	嚴重性. 標籤	請參閱下面的「解釋嚴重性標籤」
「AWS Health-」的細節。 eventTypeCode	標題	
-	類型	["軟體和組態檢查"]
事件. 時間	UpdatedAt	
Health 主控台上事件的 URL	SourceUrl	

解譯嚴重性標籤

ASFF 發現項目中的嚴重性標籤是使用下列邏輯來決定：

- 嚴重性嚴重性如果：
  - AWS Health搜尋結果中的`service`欄位具有值 `Risk`
  - AWS Health搜尋結果中的`typeCode`欄位具有值 `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health搜尋結果中的`typeCode`欄位具有值 `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health搜尋結果中的`typeCode`欄位具有值 `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  嚴重性高，如果：
  - AWS Health搜尋結果中的`service`欄位具有值 `Abuse`
  - AWS Health尋找項目中的`typeCode`欄位包含值 `SECURITY_NOTIFICATION`
  - AWS Health尋找項目中的`typeCode`欄位包含值 `ABUSE_DETECTION`

  嚴重性中等，如果：
  - 發現項目中的`service`欄位是下列任何一項：`ACMARTIFACTAUDITMANAGER`,`BACKUP`,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`,,`CLOUDWATCH`,`CO` 或 `WAF`
  - AWS Health尋找項目中的「類型代碼」欄位包含值 `CERTIFICATE`
  - AWS Health尋找項目中的「類型代碼」欄位包含值 `END_OF_SUPPORT`

來自 AWS Health 的一般問題清單

AWS Health使用將發現項目傳送至 Security Hub AWS 安全性搜尋結果格式 (ASFF)。以下是典型發現項目的範例AWS Health。

> **Note**
>
> 如果說明超過 1024 個字元，它會被截斷為 1024 個字元，結尾會顯示 (截斷)。

```
{
```

```
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
```

```
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

啟用與設定整合

啟用 Security Hub 之後，此整合會自動啟動。 AWS Health立即開始將發現發現發送到 Security Hub。

停止將發現項目發佈到 Security Hub

若要停止將發現項目傳送至 Security Hub，您可以使用 Security Hub 主控台、Security Hub API 或 AWS CLI.

請參閱 停用和啟用從整合接收問題清單的流程 (主控台) 或 從整合停用發現項目的流程 (Security Hub API,AWS CLI)。

AWS Identity and Access Management Access Analyzer（發送發現）

使用 IAM 存取分析器，所有發現項目都會傳送至 Security Hub。

IAM Access Analyzer 使用邏輯推理來分析資源型政策，這些政策套用至帳戶中支援的資源。IAM Access Analyzer 偵測到可讓外部主體存取您帳戶中的資源的政策陳述式時，就會產生一個發現項目。

在 IAM Access Analyzer 中，只有管理員帳戶可以查看適用於組織的分析器發現項目。對於組織分析器而言，`AwsAccountId`ASFF 欄位會反映管理員帳號 ID。在下方`ProductFields`，`ResourceOwnerAccount`欄位會指出發現項目所在的帳戶。如果您為每個帳戶個別啟用分析器，Security Hub 會產生多個發現項目，一個用來識別系統管理員帳號 ID，另一個用來識別資源帳號 ID。

如需詳細資訊，請參閱 IAM 使用者指南中的與AWS安全中樞整合。

Amazon Inspector（發送發現）

Amazon Inspector 是一項弱點管理服務，可持續掃描您的AWS工作負載是否有漏洞。Amazon Inspector 會自動探索和掃描位於亞馬遜彈性容器登錄中的 Amazon EC2 執行個體和容器映像。掃描會尋找軟體弱點和意外的網路暴露。

啟用 Security Hub 之後，此整合會自動啟動。Amazon Inspector 立即開始將它產生的所有發現發現發送到 Security Hub。

如需有關整合的詳細資訊，請參閱 Amazon Inspector 使用者指南中的與AWS安全中心整合。

Security Hub 也可以從 Amazon Inspector 經典接收發現。Amazon Inspector 經典版會將調查結果傳送到 Security Hub，這些發現是透過評估執行所有支援的規則套件

如需有關整合的詳細資訊，請參閱 Amazon Inspector 經典使用者指南中的與AWS安全中心整合。

Amazon Inspector 和亞 Amazon Inspector 經典調查結果使用相同的產品 ARN。Amazon Inspector 發現有以下條目`ProductFields`：

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender（發送發現）

AWS IoT Device Defender是一項安全服務，可稽核 IoT 裝置的組態、監控連線裝置以偵測異常行為，並協助降低安全風險。

同時啟用AWS IoT Device Defender和 Security Hub 之後，請造訪 Sec urity Hub 主控台的 [整合] 頁面，然後選擇 [接受稽核]、[偵測] 或 [兩者] 的發現項目。 AWS IoT Device Defender稽核和偵測會開始將所有發現項目傳送至 Security Hub。

AWS IoT Device Defender稽核會將檢查摘要傳送至 Security Hub，其中包含特定稽核檢查類型和稽核作業的一般資訊。 AWS IoT Device Defender偵測會將機器學習 (ML)、統計資料和靜態行為的違規發現項目傳送至 Security Hub。稽核也會將尋找更新傳送至 Security Hub。

如需有關此整合的詳細資訊，請參閱AWS IoT開發人員指南中的與 AWS Security Hub 整合。

Amazon Macie（發送調查結果）

來自 Macie 的發現可能表示存在潛在的政策違規或敏感資料 (例如個人識別資訊 (PII)) 存在於您的組織存放在 Amazon S3 中的資料中。

啟用 Security Hub 之後，Macie 會自動開始將原則發現項目傳送至 Security Hub。您可以將整合設定為也將敏感資料發現項目傳送至 Security Hub。

在 Security Hub 中，原則或機密資料尋找項目的尋找項目類型會變更為與 ASFF 相容的值。例如，Macie 中的`Policy:IAMUser/S3BucketPublic`尋找項目類型會顯示為「安全性`Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`中心」中。

Macie 也會將產生的範例發現傳送至 Security Hub。對於發現項目範例，受影響資源的名稱為，`Sample`欄位的值為`true`。`macie-sample-finding-bucket`

如需詳細資訊，請參閱 Amazon Macie 使用者指南中的 Amazon Macie 與AWS安全中心整合。

AWS Systems Manager修補程式管理員 (傳送發現項

AWS Systems Manager當客戶叢集中的執行個體不符合其修補程式合規標準時，修補程式管理員會將發現項目傳送至 Security Hub。

Patch Manager 會使用安全性相關和其他類型的更新，自動修補受管理執行個體的程序。

啟用 Security Hub 之後，此整合會自動啟動。Systems Manager 修補程式管理員會立即開始將發現項目傳送 Security Hub

若要取得有關使用修補程式管理員的更多資訊，請參閱AWS Systems Manager《使AWS Systems Manager用指南》中的〈

AWS從 Security Hub 接收發現項目的服務

下列AWS服務與安全中心整合，並從安全中心接收發現項目。如有所說明，綜合服務亦可能更新調查結果。在此情況下，尋找您在整合式服務中所做的更新也會反映在 Security Hub 中。

AWS Audit Manager（接收發現）

AWS Audit Manager從 Security Hub 接收發現項目。這些發現項目可協助 Audit Manager 使用者準備稽核。

若要進一步瞭解 Audit Manager，請參閱 AWSAudit Manager 使用指南。 AWSSecurity Hub 檢查支援AWS Audit Manager列出 Security Hub 將發現項目傳送給 Audit Manager 的控制項。

AWS Chatbot（接收發現）

AWS Chatbot是一種互動式代理程式，可協助您監控 Slack 頻道和 Amazon Chime 聊天室中的AWS資源並與之互動。

AWS Chatbot從 Security Hub 接收發現項目。

若要深入了解有關與 Security Hub AWS Chatbot 整合的資訊，請參閱《AWS Chatbot管理員指南》中的 Security Hub 整合概觀。

亞馬遜 Detective（收到結果）

Detective ess 會自動從您的AWS資源收集日誌資料，並使用機器學習、統計分析和圖論來協助您視覺化並進行更快、更有效率的安全性調查。

安全中心與 Detective 整合可讓您從安全中心的亞馬遜 GuardDuty 調查結果轉換為 Detective。然後，您可以使用 Detective 工具和視覺效果來調查它們。整合不需要安全中心或 Detective 中的任何額外設定。

針對從其他收到的發現項目AWS 服務，Security Hub 主控台上的發現項目詳細資料面板包含 [Detective 中調查] 子區段。該小節包含「Detective」的連結，您可以在其中進一步調查發現項目標記的安全性問題。您還可以根據 Security Hub 發現在 Detective 中構建行為圖，以進行更有效的調查。如需詳細資訊，請參閱 Amazon Detective 管理指南中的AWS安全發現。

如果啟用「跨區域聚總」，則當您從聚總區域進行樞紐分析時，「Detective」會在發現項目來源的「區域」中開啟。

如果連結無效，則針對故障診斷建議，請參閱針對樞紐進行故障診斷。

亞馬遜安全湖（接收發現）

安全湖是一項完全受管理的安全性資料湖服務。您可以使用 Security Lake，將來自雲端、內部部署和自訂來源的安全性資料自動集中到儲存在帳戶中的資料湖中。訂閱者可以使用來自 Security Lake 的資料，用於調查和分析使用案例。

若要啟用此整合，您必須同時啟用這兩項服務，並將 Security Hub 新增為 Security Lake 主控台、Security Lake API 或中的來源AWS CLI。一旦您完成這些步驟，Security Hub 就會開始將所有發現項目傳送至安全湖。

Security Lake 會自動標準化 Security Hub 發現項目，並將其轉換為標準化的開放原始碼結構描述，稱為開放網路安全結構描述架構 在安全湖中，您可以新增一或多個訂閱者來使用 Security Hub 發現項目。

如需有關此整合的詳細資訊，包括將 Security Hub 新增為來源和建立訂閱者的指示，請參閱 Amazon AWS Security Lake 使用者指南中的與安全中心整合。

AWS Systems Manager資源管理器和 OpsCenter （接收和更新發現項目）

AWS Systems Manager資源管理器並從 Security Hub OpsCenter 接收發現，並更新安 Security Hub 中的這些發現項目。

Explorer 為您提供可自訂的儀表板，針對AWS環境的作業健康狀態和效能提供關鍵見解和分析。

OpsCenter 提供您檢視、調查及解決作業工作項目的中央位置。

如需有關 Explorer 的詳細資訊 OpsCenter，請參閱《AWS Systems Manager使用指南》中的〈作業管理〉。

AWS Trusted Advisor（接收發現）

為成千上萬 AWS 客戶提供服務的過程中學習到的最佳實務，都體現在 Trusted Advisor 中。Trusted Advisor 可檢查您的 AWS 環境，並在有可能節省成本、提升系統可用性與效能或填補安全漏洞時向您提出建議。

當您同時啟用Trusted Advisor和 Security Hub 時，整合會自動更新。

Security Hub 會將其AWS基礎安全性最佳做法檢查的結果傳送至。Trusted Advisor

如需與之整合的 Security Hub 控制項的詳細資訊Trusted Advisor，請參閱 Sup AWSport 使用者指南 AWS Trusted Advisor中的檢視 AWS Security Hub 控制項。

可用的第三方合作夥伴產品整合

AWSSecurity Hub 與多個第三方合作夥伴產品整合。整合可以執行下列一或多個動作：

- 將其產生的發現傳送至 Security Hub。
- 從 Security Hub 接收發現項目。
- 更新安全中心中的發現項目。

將發現項目傳送到 Security Hub 的所有整合都具有 Amazon 資源名稱 (ARN)。

> **Note**
>
> 某些整合功能僅適用於選取項目AWS 區域。

Security Hub 主控台的 [整合] 頁面會列出目前區域的所有支援整合。
如需詳細資訊，請參閱 在中國（北京）和中國（寧夏）支持的集成 及 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 支援的整合。

如果您有安全性解決方案並有興趣成為安全中心合作夥伴，請寄電子郵件至 <securityhub-partners@amazon.com>。如需詳細資訊，請參閱 Sec AWSurity Hub 合作夥伴整合指南。

與 Security Hub 的第三方整合概觀

以下是第三方整合的概觀，可將發現項目傳送至 Security Hub，或從 Security Hub 接收發現項目。

整合	Direction	ARN（如適用）
3CORESec – 3CORESec NTA	發送發現	arn:aws:securityhub: *<REGION>*::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	發送發現	arn:aws:securityhub: *<REGION>*:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	發送發現	arn:aws:securityhub: *<REGION>*::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	發送發現	arn:aws:securityhub: *<REGION>*::product/aqua-security/kube-bench
Armor – Armor Anywhere	發送發現	arn:aws:securityhub: *<REGION>*:679703615338:product/armor

整合	Direction	ARN（如適用）
		defense/armoranywhere
AttackIQ – AttackIQ	發送發現	arn:aws:securityhub: *<REGION>*::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	發送發現	arn:aws:securityhub: *<REGION>*:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	發送發現	arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	發送發現	arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws
Capitis Solutions – C2VS	發送發現	arn:aws:securityhub: *<REGION>*::product/capitis/c2vs
Check Point – CloudGuard IaaS	發送發現	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas

整合	Direction	ARN（如適用）
Check Point – CloudGuard Posture Management	發送發現	arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	發送發現	arn:aws:securityhub: *<REGION>*::product/claroty/xdome
Cloud Storage Security—Antivirus for Amazon S3	發送發現	arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	發送發現	arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	發送發現	arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	發送發現	arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	發送發現	arn:aws:securityhub: *<REGION>*::product/data-theorem/api-cloud-web-secure

整合	Direction	ARN（如適用）
Drata	發送發現	arn:aws:securityhub: *<REGION>*::product/drata/drata-integration
Forcepoint – Forcepoint CASB	發送發現	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	發送發現	arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	發送發現	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	發送發現	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	發送發現	arn:aws:securityhub: *<REGION>*::product/fugue/fugue

整合	Direction	ARN（如適用）
Guardicore – Centra 4.0	發送發現	arn:aws:securityhub: <REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	發送發現	arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	發送發現	arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	發送發現	arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	發送發現	arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer
Lacework – Lacework	發送發現	arn:aws:securityhub: <REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	發送發現	arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws

整合	Direction	ARN（如適用）
NETSCOUT – NETSCOUT Cyber Investigator	發送發現	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	發送發現	arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	發送發現	arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	發送發現	arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform
Prowler – Prowler	發送發現	arn:aws:securityhub: *<REGION>*::product/prowler/prowler
Qualys – Vulnerability Management	發送發現	arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	發送發現	arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm

整合	Direction	ARN（如適用）
SecureCloudDB – SecureCloudDB	發送發現	arn:aws:securityhub: *<REGION>*::product/securecloudb/securecloudb
SentinelOne – SentinelOne	發送發現	arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection
Snyk	發送發現	arn:aws:securityhub: *<region>*::product/snyk/snyk
Sonrai Security – Sonrai Dig	發送發現	arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig
Sophos – Server Protection	發送發現	arn:aws:securityhub: *<REGION>*:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	發送發現	arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	發送發現	arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda

整合	Direction	ARN（如適用）
Symantec – Cloud Workload Protection	發送發現	arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	發送發現	arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	發送發現	arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one
Vectra – Cognito Detect	發送發現	arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect
Wiz	發送發現	arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security
Atlassian - Jira Service Management	接收和更新發現	不適用
Atlassian - Jira Service Management Cloud	接收和更新發現	不適用
Atlassian – Opsgenie	接收發現	不適用
Fortinet – FortiCNP	接收發現	不適用
IBM – QRadar	接收發現	不適用

整合	Direction	ARN（如適用）
Logz.io Cloud SIEM	接收發現	不適用
MetricStream	接收發現	不適用
MicroFocus – MicroFocus Arcsight	接收發現	不適用
New Relic Vulnerability Management	接收發現	不適用
PagerDuty – PagerDuty	接收發現	不適用
Palo Alto Networks – Cortex XSOAR	接收發現	不適用
Palo Alto Networks – VM-Series	接收發現	不適用
Rackspace Technology – Cloud Native Security	接收發現	不適用
Rapid7 – InsightConnect	接收發現	不適用
RSA – RSA Archer	接收發現	不適用
ServiceNow – ITSM	接收和更新發現	不適用
Slack – Slack	接收發現	不適用
Splunk – Splunk Enterprise	接收發現	不適用
Splunk – Splunk Phantom	接收發現	不適用
ThreatModeler	接收發現	不適用
Trellix – Trellix Helix	接收發現	不適用

整合	Direction	ARN（如適用）
Caveonix – Caveonix Cloud	傳送和接收發現項目	arn:aws:securityhub: *<REGION>*::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	傳送和接收發現項目	arn:aws:securityhub: *<REGION>*::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	傳送和接收發現項目	arn:aws:securityhub: *<REGION>*::product/disruptops-inc/disruptops
Kion	傳送和接收發現項目	arn:aws:securityhub: *<REGION>*::product/cloudtamerio/cloudtamerio
Turbot – Turbot	傳送和接收發現項目	arn:aws:securityhub: *<REGION>*:453761072151:product/turbot/turbot

將發現項目傳送至 Security Hub 的第三方整

下列第三方合作夥伴產品整合會將發現項目傳送至 Security Hub。Security Hub 將發現項目轉換為AWS安全性發現格式。

3CORESec – 3CORESec NTA

整合類型：傳送

產品 ARN: arn:aws:securityhub:*<REGION>*::product/3coresec/3coresec

3CORESec為內部部署和AWS系統提供受管理的偵測服務。它們與 Security Hub 的整合可讓您掌握惡意程式碼、權限提升、橫向移動和不當網路分段等威脅。

產品連結

合作夥伴文

Alert Logic – SIEMless Threat Management

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

取得適當層級的涵蓋範圍：弱點與資產能見度、威脅偵測與事件管理AWS WAF，以及指派的 SOC 分析師選項。

產品連結

合作夥伴文

Aqua Security – Aqua Cloud Native Security Platform

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)為基於容器和無伺服器的應用程式提供完整的生命週期安全性，從 CI/CD 管道到運行時生產環境。

產品連結

合作夥伴文

Aqua Security – Kube-bench

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench是一種開放原始碼工具，可針對您的環境執行網際網路安全中心 (CIS) Kubernetes 基準測試。

產品連結

合作夥伴文

Armor – Armor Anywhere

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere提供管理的安全性和合規性AWS。

產品連結

合作夥伴文

AttackIQ – AttackIQ

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform模擬與 MITRE ATT&CK 框架一致的真實對抗行為，以幫助驗證和改善您的整體安全狀態。

產品連結

合作夥伴文

Barracuda Networks – Cloud Security Guardian

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry協助組織在公有雲中建置應用程式，並將工作負載移至公有雲時保持安全。

AWSMarketplace 連結

產品連結

BigID – BigID Enterprise

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

這BigID Enterprise Privacy Management Platform可協助公司管理和保護所有系統中的敏感資料 (PII)。

產品連結

合作夥伴文

Blue Hexagon – Blue Hexagon forAWS

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon是一個實時威脅檢測平台。它使用深度學習原則來偵測已知和未知的威脅，包括惡意軟體和網路異常。

產品連結

合作夥伴文

Capitis Solutions – C2VS

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VS是可自訂的合規性解決方案，可自動識別應用程式特定的錯誤設定及其根本原因。

產品連結

合作夥伴文

Check Point – CloudGuard IaaS

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard輕鬆將全方位威脅防護安全性延伸至AWS保護雲端中的資產。

產品連結

合作夥伴文

Check Point – CloudGuard Posture Management

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

SaaS 平台可提供可驗證的雲端網路安全性、進階 IAM 保護，以及全方位的合規與控管。

產品連結

合作夥伴文

Claroty – xDome

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome協助組織透過工業 (OT)、醫療保健 (IOMT) 和企業 (IoT) 環境中的延伸物聯網 (XIOT)，保護其網路實體系統的安全。

產品連結

合作夥伴文

Cloud Storage Security— Antivirus for Amazon S3

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security為 Amazon S3 物件提供雲端原生防惡意軟體和防毒掃描。

Antivirus for Amazon S3 針對 Amazon S3 中的物件和檔案提供即時和排程掃描，以偵測惡意軟體和威脅。它提供了問題和受感染文件的可見性和補救措施。

產品連結

合作夥伴文

Contrast Security – Contrast Assess

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess是一種 IAST 工具，可在 Web 應用程序，API 和微服務中提供實時漏洞檢測。 Contrast Assess與 Security Hub 整合，有助於為您的所有工作負載提供集中的能見度和回應。

產品連結

合作夥伴文

CrowdStrike – CrowdStrike Falcon

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

這款CrowdStrike Falcon單一輕量型感測器可整合新一代防毒、端點偵測與回應，以及透過雲端全年無休的全天候管理狩獵。

產品連結

合作夥伴文

CyberArk – Privileged Threat Analytics

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics收集、偵測、警示及回應特權帳戶的高風險活動和行為，以遏止進行中的攻擊。

產品連結

合作夥伴文

Data Theorem – Data Theorem

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem持續掃描 Web 應用程式、API 和雲端資源，以尋找安全漏洞和資料隱私漏洞，以防止資 AppSec 料外洩。

產品連結

合作夥伴文

Drata

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata是一個合規性自動化平台，可幫助您實現並維持與各種框架（例如 SOC2，ISO 和 GDPR）的合規性。Drata與 Security Hub 之間的整合可協助您將安全發現項目集中在一個位置。

AWSMarketplace 連結

合作夥伴文

Forcepoint – Forcepoint CASB

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB可讓您探索雲端應用程式的使用情況、分析風險，並針對 SaaS 和自訂應用程式強制執行適當的控制。

產品連結

合作夥伴文

Forcepoint – Forcepoint Cloud Security Gateway

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway是一種融合式雲端安全服務，無論使用者和資料在何處，都能為使用者和資料提供能見度、控制和威脅防護。

產品連結

合作夥伴文

Forcepoint – Forcepoint DLP

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP透過可見度和控制您的人員在任何地方以及資料所在的任何地方解決以人為本的風險

產品連結

合作夥伴文

Forcepoint – Forcepoint NGFW

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW讓您透過管理網路和回應威脅所需的可擴充性、保護和深入解析，將您的AWS環境連線至企業網路。

產品連結

合作夥伴文

Fugue – Fugue

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue是無代理程式、可擴充的 infrastructure-as-code 雲端原生平台，可使用相同原則自動執行雲端執行階段環境的持續驗證。

產品連結

合作夥伴文

Guardicore – Centra 4.0

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra為現代資料中心和雲端中的工作負載提供流量視覺化、微分段和入侵偵測。

產品連結

合作夥伴文

HackerOne – Vulnerability Intelligence

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

該HackerOne平台與全球黑客社區合作，以發現最相關的安全問題。 Vulnerability Intelligence使您的組織能夠超越自動掃描。它共享了道HackerOne德黑客驗證並提供了重現步驟的漏洞。

AWS市場鏈接

合作夥伴文

JFrog – Xray

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray是一種通用的應用程式安全性軟體組成分析 (SCA) 工具，可持續掃描二進位檔案的授權合規性和安全性弱點，讓您可以執行安全的軟體供應鏈。

AWSMarketplace 連結

合作夥伴文

Juniper Networks – vSRX Next Generation Firewall

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'VSrx 虛擬次世代防火牆提供完整的雲端虛擬防火牆，具備進階安全性、安全的 SD-WAN、強大的網路功能和內建自動化功能。

AWSMarketplace 連結

合作夥伴文

產品連結

k9 Security – Access Analyzer

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security在您的AWS Identity and Access Management帳戶發生重大存取變更時通知您。透過k9 Security，您可以瞭解使用者和 IAM 角色對重要資料AWS 服務和資料的存取權限。

k9 Security專為持續交付而建置，可讓您透過和 Terraform 的可行存取稽核和簡單的政策自動化來操作 IAM。AWS CDK

產品連結

合作夥伴文

Lacework – Lacework

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework是雲端的資料驅動安全平台。Lacework 雲端安全平台可大規模自動化雲端安全，讓您快速且安全地進行創新。

產品連結

合作夥伴文

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)為您的環境提供雲端安全狀態管理 (CSPM) 和雲端工作負載保護平台 (CWPP)。AWS

產品連結

合作夥伴文

NETSCOUT – NETSCOUT Cyber Investigator

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator是一個全企業的網路威脅、風險調查和鑑識分析平台，有助於減少網路威脅對企業的影響。

產品連結

合作夥伴文

Palo Alto Networks – Prisma Cloud Compute

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute是一個雲端原生網路安全平台，可保護 VM、容器和無伺服器平台。

產品連結

合作夥伴文

Palo Alto Networks – Prisma Cloud Enterprise

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

使用雲端安全分析、進階威脅偵測和合規監控保護您的 AWS 部署。

產品連結

合作夥伴文

Plerion – Cloud Security Platform

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion是一個雲端安全平台，具有獨特的威脅導向、風險導向方法，可為您的工作負載提供預防性、偵測和糾正措施。Plerion與 Security Hub 之間的整合可讓客戶在一個地方集中管理安全發現項目並採取行動。

AWSMarketplace 連結

合作夥伴文

Prowler – Prowler

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler是一種開放原始碼安全工具，可AWS執行與安全性最佳做法、強化和持續監控相關的檢查。

產品連結

合作夥伴文

Qualys – Vulnerability Management

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)持續掃描並識別漏洞，保護您的資產。

產品連結

合作夥伴文

Rapid7 – InsightVM

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM 為現代環境提供弱點管理，讓您有效率地找出弱點、排定優先順序並修復弱點。

產品連結

合作夥伴文

SecureCloudDB – SecureCloudDB

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/securecloudd b/securecloudd b`

SecureCloudDB是一種雲端原生資料庫安全性工具，可提供內部和外部安全性姿勢和活動的全面可見性。它會標記安全性違規，並針對可利用的資料庫弱點提供補救。

產品連結

合作夥伴文

SentinelOne – SentinelOne

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne是自主延伸偵測與回應 (XDR) 平台，涵蓋端點、容器、雲端工作負載和 IoT 裝置的 AI 支援防護、偵測、回應和狩獵。

AWSMarketplace 連結

產品連結

Snyk

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk提供安全性平台，可掃描執行於上執行的工作負載中的應用程式元件是否AWS有 這些風險會作為調查結果傳送至 Security Hub，協助開發人員和安全團隊視覺化並排定其餘AWS安全發現結果的優先順序。

AWSMarketplace 連結

合作夥伴文

Sonrai Security – Sonrai Dig

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig監控並修復雲端錯誤設定和原則違規情況，以便您改善安全性和合規狀態。

產品連結

合作夥伴文

Sophos – Server Protection

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection使用全面的 defense-in-depth 技術，保護組織核心的關鍵應用程式和資料。

產品連結

合作夥伴文

StackRox – StackRox Kubernetes Security

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox透過在整個容器生命週期 (建置、部署和執行) 中強制執行合規性和安全性原則，協助企業大規模保護其容器和 Kubernetes 部署的安全性。

產品連結

合作夥伴文

Sumo Logic – Machine Data Analytics

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic是一個安全的機器資料分析平台，可讓開發和安全作業團隊建置、執行和保護其AWS應用程式。

產品連結

合作夥伴文

Symantec – Cloud Workload Protection

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection透過反惡意軟體、入侵防護和檔案完整性監控，為您的 Amazon EC2 執行個體提供完整的保護。

產品連結

合作夥伴文

Tenable – Tenable.io

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

準確識別、調查和排定漏洞的優先順序。在雲端管理。

產品連結

合作夥伴文

Trend Micro – Cloud One

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One在適當的時間和地點為團隊提供正確的安全資訊。這項整合會即時將安全發現項目傳送至 Security Hub，以增強 Security Hub 中的AWS資源和Trend Micro Cloud One事件詳細資料的可見性。

AWSMarketplace 連結

合作夥伴文

Vectra – Cognito Detect

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra正在通過應用高級 AI 來檢測隱藏的網絡攻擊者並響應隱藏的網絡攻擊者，從而改變了網絡安全性。

AWSMarketplace 連結

合作夥伴文

Wiz – Wiz Security

整合類型：傳送

產品 ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz持續分析您、使用者和工作負載中的組態、弱點、網路、IAM 設定AWS 帳戶、機密等，以發現代表實際風險的關鍵問題。將 Wiz 與 Security Hub 整合，以視覺化方式呈現並回應 Wiz 從 Security Hub 主控台偵測到的問題。

AWSMarketplace 連結

合作夥伴文

從 Security Hub 接收發現的第三方整合

下列第三方合作夥伴產品整合會收到來自 Security Hub 的發現項目。如有說明，產品也可能會更新發現結果。在此情況下，尋找您在合作夥伴產品中所做的更新也會反映在 Security Hub 中。

Atlassian - Jira Service Management

整合類型：接收和更新

AWS Service Management Connectorfor Jira 將發現項目從 Security Hub 傳送到Jira. Jira問題是根據發現項目建立的。更新Jira問題時，相應的發現項目會在安全性中心中更新。

整合僅支援 Jira 伺服器和 Jira 資料中心。

如需整合及其運作方式的概觀，請觀看 Sec AWSurity Hub — 雙向整合的Atlassian Jira Service Management影片。

產品連結

合作夥伴文

Atlassian - Jira Service Management Cloud

整合類型：接收和更新

Jira Service Management Cloud是 Jira 服務管理的雲端元件。

AWS Service Management Connectorfor Jira 將發現項目從 Security Hub 傳送到Jira. 發現項目會觸發在中建立問題Jira Service Management Cloud。當您更新中的這些問題時Jira Service Management Cloud，對應的發現項目也會在 Security Hub 中更新。

產品連結

合作夥伴文

Atlassian – Opsgenie

整合類型：接收

Opsgenie是一個現代化的事件管理解決方案，用於營運永遠在線的服務，使開發和運營團隊能夠規劃服務中斷，並在事件發生時保持控制。

與 Security Hub 整合可確保關鍵任務安全相關事件會轉送給適當的團隊，以便立即解決。

產品連結

合作夥伴文

Fortinet – FortiCNP

整合類型：接收

FortiCNP是一種雲端原生保護產品，可將安全發現結果彙總為可行的見解，並根據風險評分來排定安全洞見的優先順序，以減少警示疲勞並加速補救。

AWSMarketplace 連結

合作夥伴文

IBM – QRadar

整合類型：接收

IBM QRadarSIEM 讓安全團隊能夠快速準確地偵測、排定優先順序、調查及回應威脅。

產品連結

合作夥伴文

Logz.io Cloud SIEM

整合類型：接收

Logz.io是提供日誌和事件數據的高級關聯的提供商，以幫助安全團隊實時檢測，分析和響應安全威脅。Cloud SIEM

產品連結

合作夥伴文

MetricStream – CyberGRC

整合類型：接收

MetricStream CyberGRC協助您管理、衡量和減輕網路安全風險。透過收到 Security Hub 調查結果，CyberGRC讓您更清楚瞭解這些風險，因此您可以排定網路安全投資的優先順序，並遵守 IT 政策。

AWSMarketplace 連結

產品連結

MicroFocus – MicroFocus Arcsight

整合類型：接收

ArcSight即時加速有效的威脅偵測與回應，整合事件關聯性，以及受監督與無監督的分析與回應自動化與協調。

產品連結

合作夥伴文

New Relic Vulnerability Management

整合類型：接收

New Relic Vulnerability Management從 Security Hub 接收安全性發現項目，因此您可以集中檢視安全性以及跨堆疊內容中的效能遙測。

AWSMarketplace 連結

合作夥伴文

PagerDuty – PagerDuty

整合類型：接收

PagerDuty數位作業管理平台讓團隊能夠自動將任何訊號轉化為正確的洞察力和行動，主動緩解對客戶造成影響的問題。

AWS使用者可以使用這PagerDuty組AWS整合來自信地擴展其AWS和混合式環境。

搭配 Security Hub 彙總且有組織的安全警示，PagerDuty可讓團隊自動化其威脅回應程序，並快速設定自訂動作，以防止潛在問題發生。

PagerDuty進行雲端移轉專案的使用者可以快速移動，同時減少整個移轉生命週期中發生的問題所造成的影響。

產品連結

合作夥伴文

Palo Alto Networks – Cortex XSOAR

整合類型：接收

Cortex XSOAR是一個安全性協調、自動化和回應 (SOAR) 平台，可與整個安全產品堆疊整合，以加速事件回應和安全性作業。

產品連結

合作夥伴文

Palo Alto Networks – VM-Series

整合類型：接收

Palo Alto VM-Series與 Security Hub 整合可收集威脅情報，並將其做為自動安全性原則更新傳送至新一VM-Series代防火牆，以封鎖惡意 IP 位址活動。

產品連結

合作夥伴文

Rackspace Technology – Cloud Native Security

整合類型：接收

Rackspace Technology 透過 Rackspace SOC、進階分析和威脅修復，在原生AWS安全產品之上提供受管理的安全性服務，進行全年無休的全天候監控。

產品連結

Rapid7 – InsightConnect

整合類型：接收

Rapid7 InsightConnect是一種安全性協調和自動化解決方案，讓您的團隊能夠最佳化 SOC 作業，幾乎沒有程式碼。

產品連結

合作夥伴文

RSA – RSA Archer

整合類型：接收

RSA ArcherIT 和安全風險管理可讓您判斷哪些資產對您的業務至關重要、建立並傳達安全性原則和標準、偵測並回應攻擊、識別和補救安全缺陷，以及建立明確的 IT 風險管理最佳實務。

產品連結

合作夥伴文

ServiceNow – ITSM

整合類型：接收和更新

與 Security Hub 的ServiceNow整合可讓您在中檢視來自 Security Hub 的安全性發現項目ServiceNow ITSM。您也可以設定ServiceNow為在收到來自 Security Hub 的發現項目時，自動建立事件或問題。

這些事件和問題的任何更新都會導致 Security Hub 中的發現項目更新。

如需整合及其運作方式的概觀，請觀看「AWSSecurity Hub-雙向整合 ServiceNow ITSM」影片。

產品連結

合作夥伴文

Slack – Slack

整合類型：接收

Slack是將人員、資料和應用程式整合在一起的業務技術堆疊層。大家可在一個位置有效率地一起工作、尋找重要資訊，以及存取數十萬種關鍵應用程式和服務，將工作做到最好。

產品連結

合作夥伴文

Splunk – Splunk Enterprise

整合類型：接收

Splunk使用 Amazon CloudWatch 事件作為安全中心發現的消費者。將您的資料傳送至Splunk進階安全性分析和 SIEM。

產品連結

合作夥伴文

Splunk – Splunk Phantom

整合類型：接收

透過 AWS Security Hub 應Splunk Phantom用程式，系統會將發現項目傳送至，以利Phantom用其他威脅情報資訊進行自動化內容豐富，或執行自動回應動作。

產品連結

合作夥伴文

ThreatModeler

整合類型：接收

ThreatModeler是一種自動化威脅建模解決方案，可保護和擴展企業軟體和雲端開發生命週期。

產品連結

合作夥伴文

Trellix – Trellix Helix

整合類型：接收

Trellix Helix是一個雲託管的安全操作平台，允許組織控制從警報到修復的任何事件。

產品連結

合作夥伴文

第三方整合，可將發現項目傳送至 Security Hub 並從中接收發現

下列第三方合作夥伴產品整合會將發現項目傳送至 Security Hub 並從中接收發現項目。

Caveonix – Caveonix Cloud

整合類型：傳送和接收

產品 ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

這個 Caveonix AI 支援的平台可自動執行混合雲中的可見性、評估和緩解功能，涵蓋雲端原生服務、VM 和容器。與 AWS Security Hub 整合，可合Caveonix併AWS資料和進階分析，以深入瞭解安全性警示和合規性。

AWSMarketplace 連結

合作夥伴文

Cloud Custodian – Cloud Custodian

整合類型：傳送和接收

產品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian使用戶能夠在雲中得到良好的管理。簡單的 YAML DSL 允許輕鬆定義的規則，以實現管理良好的雲端基礎架構，既安全又具成本優化。

產品連結

合作夥伴文

DisruptOps, Inc. – DisruptOPS

整合類型：傳送和接收

產品 ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps安全性作業平台透過使用自動護欄，協助組織在您的雲端維護最佳安全實務。

產品連結

合作夥伴文

Kion

整合類型：傳送和接收

產品 ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(之前稱為雲端攝影機 .io) 是一個完整的雲端治理解決方案，適用於. AWS Kion讓利益相關者能夠掌握雲端作業，並協助雲端使用者管理帳戶、控制預算和成本，並確保持續合規。

產品連結

合作夥伴文

Turbot – Turbot

整合類型：傳送和接收

產品 ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot確保您的雲端基礎架構安全、合規、可擴充且成本最佳化。

產品連結

合作夥伴文

使用自訂產品整合將發現項目傳送至 AWS Security Hub

除了整合式 AWS 服務和協力廠商產品所產生的發現項目之外，Security Hub 還可以使用其他自訂安全性產品所產生的發現項目。

您可以使用 BatchImportFindingsAPI 作業，手動將這些發現項目傳送至 Security Hub。

設定自訂整合時，請使用 Security Hub 合作夥伴整合指南中提供的準則和檢查清單。

傳送自訂安全產品問題清單的需求與建議

您必須先啟用 Security Hub，才能成功叫用 BatchImportFindingsAPI 作業。

您必須使用 the section called “問題清單格式” 來提供問題清單詳細資訊。針對自訂整合的問題清單，請使用下列要求和建議。

設定產品 ARN

當您啟用安全中心時，會在您目前的帳戶中產生 Security Hub 的預設產品 Amazon 資源名稱 (ARN)。

此產品 ARN 的格式如下：`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`。例如 `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`。

呼叫 `BatchImportFindings` API 作業時，請使用此產品 ARN 作為`ProductArn`屬性的值。

定義公司和產品名稱

您可以使用`BatchImportFindings`為將發現項目傳送至 Security Hub 的自訂整合設定偏好的公司名稱和產品名稱。

您指定的名稱會取代預先設定的公司名稱和產品名稱 (分別稱為個人名稱和預設名稱)，並顯示在 Security Hub 主控台和每個發現項目的 JSON 中。請參閱使用 BatchImportFindings 建立和更新問題清單。

設定問題清單 ID

您必須使用 `Id` 屬性提供、管理和增加您自己的問題清單 ID。

每個新發現項目都應該有唯一的尋找 ID。如果自訂產品傳送具有相同尋找項目識別碼的多個發現項目，Security Hub 只會處理第一個發現項目。

設定帳戶 ID

您必須使用 `AwsAccountId` 屬性指定自己的帳戶 ID。

設定建立日期和更新日期

您必須針對 `CreatedAt` 和 `UpdatedAt` 屬性提供自己的時間戳記。

從自訂產品更新問題清單

除了從自訂產品傳送新的問題清單之外，您也可以使用 `BatchImportFindings` API 操作更新自訂產品的現有問題清單。

如要更新現有問題清單，請使用現有的問題清單 ID (透過 `Id` 屬性)。在請求中適當更新資訊來重新傳送完整的問題清單，包括修改後的 `UpdatedAt` 時間戳記。

自訂整合範例

您可以將下列自訂產品整合範例做為建立自己專屬解決方案的指南。

將發現項目從Chef InSpec掃描傳送到 Security Hub

您可以建立執行Chef InSpec符合性掃描的 AWS CloudFormation 範本，然後將發現項目傳送至 Security Hub。

如需詳細資訊，請參閱使用Chef InSpec和 AWS Security Hub 進行持續合規監控。

將偵測到的容器弱點傳送Trivy至 Security Hub

您可以建立用AquaSecurity Trivy來掃描容器中是否有弱點的 AWS CloudFormation 範本，然後將這些弱點發現項目傳送至 Security Hub。

如需詳細資訊，請參閱如何使用Trivy和AWS Security Hub 建立容器弱點掃描的 CI/CD 管線。

安全控制和安 AWS 全中心的標準

AWS Security Hub 會使用、彙總和分析來自各種支援 AWS 和協力廠商產品的安全性發現項目。

Security Hub 也會針對規則執行自動且持續的安全性檢查，藉此產生自己的發現項目。這些規則由安全控制表示。這些控制項可能會在一個或多個安全標準中啟用。這些控制項可協助您判斷是否符合標準中的需求。

針對控制項進行安全性檢查會產生發現項目，您可以使用這些發現項目來監控您的 AWS 帳戶 安全狀況，並識別需要注意的 每個控制項都與 AWS 服務和資源有關。例如，對 CloudTrail.4 控制項進行安全性檢查會判斷您是否已在記錄檔上設定 AWS CloudTrail 記錄檔驗證。如需控制項的詳細資訊，請參閱檢視和管理安全性控制。

您可以在一或多個已啟用的安全中心標準中啟用控制項。當您啟用標準時，Security Hub 會自動啟用適用於標準的控制項。安全標準可讓您專注於特定的合規性架構。Security Hub 定義適用於每個標準的控制項。如需有關安全標準的更多資訊，請參閱檢視和管理安全性標準。

Security Hub 會根據安全性檢查的結果，計算整體安全分數和標準特定的安全分數。這些分數可協助您瞭解自己的安全性狀態。如需分數的詳細資訊，請參閱安全分數的計算方式。

如需安全性檢查 Security Hub 定價的相關資訊，請參閱 Security Hub 定價。

主題

- 用於設定標準和控制的 IAM 許可
- 安全檢查和安全分數在安全中心
- Security Hub 標準參考
- 檢視和管理安全性標準
- Security Hub 控制項參考
- 檢視和管理安全性控制

用於設定標準和控制的 IAM 許可

若要檢視有關安全控制的資訊，以及在標準中啟用和停用安全控制，您用來存取的 AWS Identity and Access Management (IAM) 角色 AWS Security Hub 需要許可才能呼叫下列 API 動作。如果不新增這些動作的權限，您將無法呼叫這些 API。若要取得必要的權限，您可以使用 Security

Hub 受管理的原則。或者，您可以更新自訂 IAM 政策以包含這些動作的許可。自訂原則也應包含DescribeStandardsControls和 UpdateStandardsControlAPI 的權限。

- **BatchGetSecurityControls**— 傳回目前帳戶與之一批安全控制的相關資訊 AWS 區域。
- **ListSecurityControlDefinitions**— 傳回套用至指定標準之安全性控制的相關資訊。
- **ListStandardsControlAssociations**— 識別安全性控制目前是在帳戶中啟用或停用每個已啟用的標準。
- **BatchGetStandardsControlAssociations**— 針對一批安全控制項，識別目前在指定標準中啟用或停用每個控制項。
- **BatchUpdateStandardsControlAssociations**— 用於在包含控制項的標準中啟用安全控制，或停用標準中的控制項。如果系統管理員不想允許成員帳戶啟用或停用控制項，這是現有 UpdateStandardsControlAPI 的批次替代方案。

除了上述 API 之外，您還應新增呼叫 **BatchGetControlEvaluations**IAM 角色的權限。此權限對於檢視控制項的啟用和符合性狀態、控制項的發現項目計數，以及 Security Hub 主控台上控制項的整體安全分數是必要的。由於只有主控台呼叫 **BatchGetControlEvaluations**，因此此 IAM 權限不會直接對應於公開記錄的 Security Hub API 或 AWS CLI 命令。

如需控制項和標準相關 API 的詳細資訊，請參閱 AWS Security Hub API 參考。

安全檢查和安全分數在安全中心

對於您啟用的每個控制項，都會 AWS Security Hub 執行安全性檢查。安全性檢查會判斷您的 AWS 資源是否符合控制項所包含的規則。

有些檢查會定期執行。其他檢查僅在資源狀態發生變更時執行。如需詳細資訊，請參閱 the section called “執行安全檢查的排程”。

許多安全性檢查會使用 AWS Config 受管理或自訂規則來建立符合性需求。若要執行這些檢查，您必須設定 AWS Config。如需詳細資訊，請參閱 the section called “AWS Config 規則和安全檢查”。其他使用自訂 Lambda 函數，這些函數由 Security Hub 管理，客戶看不到這些函數。

當 Security Hub 執行安全性檢查時，會產生發現項目並為其指派符合性狀態。如需符合性狀態的詳細資訊，請參閱發現項目之符合性狀態的值。

Security Hub 使用控制項發現項目的符合性狀態來判斷整體控制項狀態。Security Hub 也會針對所有已啟用的控制項和特定標準，計算安全分數。如需詳細資訊，請參閱 the section called “法規遵循狀態和控制狀態” 及 the section called “決定安全分數”。

如果您已開啟合併控制項發現項目，即使控制項與多個標準相關聯，Security Hub 仍會產生單一發現項目。如需詳細資訊，請參閱 合併控制項結果。

主題

- Security Hub 如何使用 AWS Config 規則執行安全性檢查
- AWS Config 產生控制項發現項所需的資源
- 執行安全檢查的排程
- 產生及更新控制項發現項
- 法規遵循狀態和控制狀態
- 決定安全分數

Security Hub 如何使用 AWS Config 規則執行安全性檢查

若要對環境的資源執行安全性檢查，請 AWS Security Hub 使用標準指定的步驟，或使用特定 AWS Config 規則。有些規則是受管理的規則，由管理 AWS Config。其他規則是 Security Hub 開發的自訂規則。

AWS Config Security Hub 用於控制項的規則稱為服務連結規則，因為這些規則是由 Security Hub 服務啟用和控制。

若要對這些 AWS Config 規則啟用檢查，您必須先 AWS Config 為帳號啟用，並啟用所需資源的資源記錄。如需如何啟用的資訊 AWS Config，請參閱配置 AWS Config。如需必要資源記錄的相關資訊，請參閱 AWS Config 產生控制項發現項所需的資源

Security Hub 如何產生服務連結規則

對於使用 AWS Config 服務連結規則的每個控制項，Security Hub 會在您的 AWS 環境中建立必要規則的執行個體。

這些服務連結規則專屬於 Security Hub。即使已存在相同規則的其他執行個體，其仍會建立這些服務連結規則。服務連結規則會在原始規則名稱`securityhub`之前新增，並在規則名稱後新增一個唯一識別碼。例如，對於原始 AWS Config 受管規則`vpc-flow-logs-enabled`，服務連結規則名稱會類似`securityhub-vpc-flow-logs-enabled-12345`。

可用於評估控制項的 AWS Config 規則數目有限制。Security Hub 創建的自定義 AWS Config 規則不會計入該限制。即使您已經達到帳戶中受管規則的 AWS Config 限制，也可以啟用安全性標準。若要進一步了解 AWS Config 規則限制，請參閱AWS Config 開發人員指南中的服務限制。

檢視控制項 AWS Config 規則的詳細資訊

對於使用 AWS Config 受管規則的控制項，控制項描述會包含規 AWS Config 則詳細資料的連結。自訂規則不會從控制項說明連結。如需控制項描述，請參閱Security Hub 控制項參考。從清單中選取控制項以查看其描述。

針對從這些控制項產生的發現項目，搜尋結果明細會包含相關 AWS Config 規則的連結。請注意，若要從尋找詳細資料導覽至 AWS Config 規則，您還必須在所選帳戶中擁有 IAM 權限才能導覽至 AWS Config。

「發現項目」頁面、「見解」頁面和「整合」頁面上的尋找項目詳細資訊包含規則詳細資料的規 AWS Config 則連結。請參閱the section called “檢視發現項目詳細資料”。

在控制項詳細資訊頁面上，發現項目清單的「調查」欄包含 AWS Config 規則詳細資訊的連結。請參閱the section called “檢視尋找項目資源的 AWS Config 規則”。

AWS Config 產生控制項發現項所需的資源

AWS Security Hub 針對 Security Hub 控制項執行安全性檢查，產生控制項發現項目 某些控制項會使用評估特定資源之符合性的 AWS Config 規則。若要讓 Security Hub 為具有變更觸發的排程類型的控制項產生發現項目，您必須在中開啟所需資源的記錄 AWS Config。對於具有定期排程型態的大多數控制項，您不需要記錄資源。但是，某些週期性控制需要資源記錄才能偵測合規性的變更。

此頁面提供跨標準所需資源的清單，以及依標準劃分的必要資源清單。第一個表格也會列出哪些 Security Hub 控制項會使用每個資源。

如果發現項目是由以規則為基礎的安全性檢查所產生， AWS Config 則發現項目詳細資訊會包含相關規則的「規 AWS Config 則」連結。若要導覽至規 AWS Config 則，您的帳戶必須具有 IAM 許可才能檢視 AWS Config 規則。

> **Note**
>
> AWS 區域 在無法使用控制項的情況下，對應的資源在中不可用 AWS Config。如需 Security Hub 控制項的區域限制清單，請參閱各區域控制項的可用性。

AWS Config 所有控制項所需的資源

若要讓 Security Hub 產生使用 AWS Config 規則的已啟用 Security Hub 變更觸發控制項的發現項目，您必須將這些資源記錄在中 AWS Config。此表格也指出哪些控制項需要特定資源。控制項可能需要多個資源。

服務	所需資源	相關控制
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.5
Amazon Athena	`AWS::Athena::WorkGroup`	雅典娜 .1
AWS Backup (AWS Backup)	`AWS::Backup::RecoveryPoint`	Backup。1
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.1
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4

服務	所需資源	相關控制
		CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4 CodeBuild.5
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`	數位 .9
	`AWS::DMS::ReplicationInstance`	公升 .6
	`AWS::DMS::ReplicationTask`	毫升 .7 公升 .8

服務	所需資源	相關控制
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.2 DynamoB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::EIP`	EC2.12
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EMR.1 SSM.1
	`AWS::EC2::LaunchTemplate`	EC2.25
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21
	`AWS::EC2::NetworkInterface`	EC2.22

服務	所需資源	相關控制
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19
	AWS::EC2::Subnet	EC2.15 ElastiCache.7 Lambda.5
	AWS::EC2::TransitGateway	EC2.23
	AWS::EC2::VPNConnection	EC2.20
	AWS::EC2::Volume	EC2.3
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9
	AWS::AutoScaling::LaunchConfiguration	AutoScaling.3 AutoScaling.4 Autoscaling.5

服務	所需資源	相關控制
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`	ECR.2 ECR.3
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12
	`AWS::ECS::Service`	ECS.2 ECS.10
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 等 .9

服務	所需資源	相關控制
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14

服務	所需資源	相關控制
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 精靈 .16
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8
Amazon EventBridge	AWS::Events::EventBus	EventBridge.3
	AWS::Events::Endpoint	EventBridge.4
Amazon FSx	AWS::FSx::FileSystem	FSX.1
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.18 KMS.2

服務	所需資源	相關控制
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.18 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.18 KMS.2
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`	KMS.3
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5
Amazon MSK	`AWS::MSK::Cluster`	毫克 .1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	每米 5 米 每小米 6

服務	所需資源	相關控制
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.9
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
Amazon OpenSearch 服務	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 OpenSearch.10

服務	所需資源	相關控制
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB DocumentDB DocumentDB 4 DocumentDB 5 海王星 .1 海王星 2 海王星 .4 海王星 .5 海王星 .7 海王星 .8 海王星 .9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.34 RDS.35

服務	所需資源	相關控制
	AWS::RDS::DBClusterSnapshot	DocumentDB 海王星 .3 海王星 .6 RDS.1 RDS.4
	AWS::RDS::DBInstance	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25
	AWS::RDS::DBSnapshot	DocumentDB RDS.1 RDS.4

服務	所需資源	相關控制
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10
Amazon Route 53	`AWS::Route53::HostedZone`	香港路線
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19

服務	所需資源	相關控制
	AWS::S3::Bucket	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic	SNS.1 SNS.2
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1

服務	所需資源	相關控制
Amazon SageMaker	AWS::SageMaker::NotebookInstance	SageMaker.2 SageMaker.3
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager.1 SecretsManager.2
AWS Step Functions	AWS::StepFunctions::StateMachine	StepFunctions.1
AWS WAF	AWS::WAF::Rule	WAF.6
	AWS::WAF::RuleGroup	WAF.7
	AWS::WAF::WebACL	WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10

AWS Config FSBP 標準所需的資源

若要讓 Security Hub 準確報告使用 AWS Config 規則的已啟用 AWS 基礎安全性最佳作法 (FSBP) 變更觸發控制項的發現項目，您必須將這些資源記錄在中。 AWS Config若要取得有關此標準的更多資訊，請參閱AWS 基礎安全性最佳做法 (FSBP) 標準。

服務	必要的資源
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`

服務	必要的資源
	AWS::EC2::Instance AWS::EC2::LaunchTemplate AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::VPNConnection AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment

服務	必要的資源
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon FSx	`AWS::FSx::FileSystem`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

Amazon OpenSearch 服務	`AWS::OpenSearch::Domain`

服務	必要的資源

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

服務	必要的資源
AWS WAF	AWS::WAF::Rule AWS::WAF::RuleGroup AWS::WAF::WebACL AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::RuleGroup AWS::WAFv2::WebACL

AWS Config CIS AWS 基準基準所需的資源

若要針對適用於網際網路安全中心 (CIS) AWS 基準測試 v1.2.0 和 v1.4.0 的已啟用控制項執行安全檢查，Security Hub 會執行針對保護 Amazon Web Services 的檢查所指定的確切稽核步驟，或使用特定的受管規則。 AWS Config

若要取得有關此標準的更多資訊，請參閱互聯網安全中心（CIS） AWS 基準基準 v1.2.0 和 1.4.0 版。

獨聯體 v1.4.0 所需的 AWS Config 資源

若要讓 Security Hub 準確地報告使用 AWS Config 規則的已啟用 CIS v1.4.0 變更觸發控制項的發現項目，您必須在中記錄這些資源。 AWS Config

服務	必要的資源
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::NetworkAcl AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy AWS::IAM::User

服務	必要的資源
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

獨聯體 V1.2.0 所需的 AWS Config 資源

若要讓 Security Hub 準確地報告使用 AWS Config 規則的已啟用 CIS v1.2.0 變更觸發控制項的發現項目，您必須在中記錄這些資源。 AWS Config

服務	必要的資源
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

AWS Config NIST SP 第 5 版所需的資源

若要讓 Security Hub 準確報告啟用的國家標準與技術研究所 (NIST) SP 800-53 修訂版 5 變更觸發的控制項使用 AWS Config 規則，您必須將這些資源記錄在中。 AWS Config您只需記錄具有已觸發變更之排程型態之控制項的資源。若要取得有關此標準的更多資訊，請參閱美國國家標準與技術研究院 (NIST)。

服務	必要的資源
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::RecoveryPoint`

服務	必要的資源
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

服務	必要的資源
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`
Amazon FSx	`AWS::FSx::FileSystem`

服務	必要的資源

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

Amazon OpenSearch 服務	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

服務	必要的資源
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

AWS Config PCI DSS 所需的資源

若要讓 Security Hub 準確地報告使用 AWS Config 規則的已啟用支付卡產業資料安全標準 (PCI DSS) 控制項的調查結果，您必須在中 AWS Config記錄這些資源。若要取得有關此標準的更多資訊，請參閱支付卡產業資料安全標準 (PCI DSS)。

服務	必要的資源
AWS CodeBuild	`AWS::CodeBuild::Project`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
Amazon OpenSearch 服務	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` `AWS::SSM::ManagedInstanceInventory`

服務	必要的資源
	AWS::SSM::PatchCompliance

AWS Config 服務管理標準所需的資源： AWS Control Tower

若要讓 Security Hub 準確報告已啟用服務管理標準的發現項目： AWS Control Tower 變更使用 AWS Config 規則的觸發控制項，您必須在中 AWS Config記錄下列資源。若要取得有關此標準的更多資訊，請參閱服務管理標準： AWS Control Tower。

服務	必要的資源
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CodeBuild	AWS::CodeBuild::Project
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::Instance AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::VPNConnection AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup

服務	必要的資源
	AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function

服務	必要的資源
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch 服務	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

服務	必要的資源

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

執行安全檢查的排程

啟用安全性標準後，會在兩小時內 AWS Security Hub 開始執行所有檢查。大多數檢查會在 25 分鐘內開始執行。Security Hub 透過評估控制項基礎的規則來執行檢查。在控制項完成第一次執行檢查之前，其狀態為 [無資料]。

當您啟用新標準時，Security Hub 最多可能需要 24 小時才能針對使用與其他已啟用標準的控制項相同的基礎 AWS Config 服務連結規則的控制項產生發現項目。例如，如果您在 AWS 基礎安全性最佳做法 (FSBP) 標準中啟用 Lambda.1，Security Hub 會建立服務連結規則，通常在幾分鐘內產生發現項目。此後，如果您在支付卡產業資料安全標準 (PCI DSS) 中啟用 Lambda.1，Security Hub 可能需要長達 24 小時才能產生此控制項的發現項目，因為它使用與 Lambda.1 相同的服務連結規則。

初始檢查之後，每個控制項的排程可以是週期性的，也可以是觸發變更。

- 定期檢查 — 這些檢查會在最近一次執行後的 12 或 24 小時內自動執行。Security Hub 確定週期性，您無法更改它。定期控制會在執行檢查時反映評估。如果您更新定期控制搜尋結果的工作流程狀態，然後在接下來檢查搜尋結果的符合性狀態不變，則工作流程狀態會保持在其已修改狀態。例如，如果您找不到 KMS.4- AWS KMS key 輪替應該啟用，然後修復發現項目，Security Hub 會將工作流程狀態從變更為。`NEW RESOLVED`如果您在下次定期檢查之前停用 KMS 金鑰輪替，則發現項目的工作流程狀態仍會保留`RESOLVED`。
- 變更觸發的檢查 — 這些檢查會在關聯的資源變更狀態時執行。 AWS Config 可讓您在連續記錄資源狀態變更和每日記錄之間進行選擇。如果您選擇每日記錄，如果資源狀態發生變更，則會在每 24 小時期間結束時 AWS Config 傳送資源組態資料。如果沒有變更，則不會傳送任何資料。這可能會延遲 Security Hub 發現項目的產生，直到 24 小時的期間完成為止。無論您選擇的錄製時間為何，Security Hub 每 18 小時都會檢查一次，以確保沒有遺 AWS Config 漏任何資源更新。

一般而言，Security Hub 會盡可能地使用變更觸發規則。若要讓資源使用變更觸發的規則，它必須支援 AWS Config 組態項目。

對於以受管理 AWS Config 規則為基礎的控制項，控制項說明會包含AWS Config 開發人員指南中規則說明的連結。該描述包括規則是觸發變更還是定期變更。

使用 Security Hub 自訂 Lambda 函數的檢查是定期的。

產生及更新控制項發現項

AWS Security Hub 透過對安全控制執行檢查來產生發現項目。這些發現項目使用 AWS 安全性搜尋結果格式 (ASFF)。請注意，如果尋找項目大小超過 240 KB 的最大值，則會移除`Resource.Details`物件。對於由 AWS Config 資源支援的控制項，您可以在主控 AWS Config 台上檢視資源詳細資訊。

Security Hub 通常會針對控制項的每個安全性檢查收費用。但是，如果多個控制項使用相同的 AWS Config 規則，則 Security Hub 只會針對 AWS Config 規則的每次檢查收費用一次。如果您開啟合併控制項發現項目，Security Hub 會產生單一發現項目以進行安全性檢查，即使該控制項包含在多個已啟用的標準中也是如此。

例如，網際網路安全中心 (CIS) AWS 基準標準和基礎安全性最佳做法標準中的多個控制項會使用`iam-password-policy`此 AWS Config 規則。每次 Security Hub 針對該 AWS Config 規則執行檢查時，都會針對每個相關控制項產生個別的搜尋結果，但只會針對檢查收費用一次。

合併控制項結果

在帳戶中開啟合併控制項發現項目時，Security Hub 會針對控制項的每個安全性檢查產生單一新的發現項目或尋找更新，即使控制項套用至多個已啟用的標準也是如此。若要查看控制項清單及其套用的標準，請參閱Security Hub 控制項參考。您可以開啟或關閉合併的控制項發現項目。我們建議將其打開以減少發現噪音。

如果您在 2023 年 2 月 23 日 AWS 帳戶 之前啟用 Security Hub，則必須依照本節稍後的指示，開啟合併控制項發現項目。如果您在 2023 年 2 月 23 日或之後啟用 Security Hub，您帳戶中的合併控制項發現項目會自動開啟。不過，如果您透過手動邀請程序使用 Security Hub 整合 AWS Organizations或受邀的成員帳戶，則只有在管理員帳戶中開啟成員帳戶時，才會在成員帳戶中開啟合併控制項發現項目。如果管理員帳戶中的功能已關閉，則會在成員帳戶中關閉該功能。此行為適用於新的和現有的成員帳戶。

如果您關閉帳戶中的合併控制項發現項目，Security Hub 會針對每個包含控制項的已啟用標準產生個別的搜尋結果。例如，如果四個已啟用的標準與相同的基礎 AWS Config 規則共用一個控制項，則在對控制項進行安全性檢查之後，您會收到四個個別的發現項目。如果您開啟合併控制項搜尋結果，則只會收到一個搜尋結果。如需合併如何影響您發現項目的詳細資訊，請參閱樣本控制結果。

當您開啟整合的控制項發現項目時，Security Hub 會建立新的與標準無關的發現項目，並封存原始的標準式發現項目。某些控制項尋找欄位和值會變更，且可能會影響現有的工作流程。如需這些變更的詳細資訊，請參閱合併的控制項結果 — ASFF 變更。

開啟合併的控制項發現項目也可能會影響第三方整合從 Security Hub 收到的發現項目。AWS 2.0.0 版的自動化安全回應支援整合的控制項發現項目。

開啟合併的控制項結果

若要開啟合併控制項發現項目，您必須登入系統管理員帳戶或獨立帳戶。

> **Note**
>
> 開啟合併的控制項發現項目之後，Security Hub 最多可能需要 24 小時才能產生新的合併發現結果，並封存原始的標準式發現項目。在這段期間，您可能會在帳戶中看到混合的標準和基於標準的發現結果。

Security Hub console

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中，選擇設定。
3. 選擇 [一般] 索引標籤。
4. 針對控制項，開啟合併控制項發現項目。
5. 選擇儲存。

Security Hub API

1. 執行 `UpdateSecurityHubConfiguration`。
2. 設定`ControlFindingGenerator`等於`SECURITY_CONTROL`。

   請求示例：

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. 執行 update-security-hub-configuration 命令。
2. 設定control-finding-generator等於SECURITY_CONTROL。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

關閉合併控制項發現項目

若要關閉合併控制項發現項目，您必須登入系統管理員帳戶或獨立帳戶。

> **Note**
>
> 關閉合併的控制項發現項目之後，Security Hub 最多可能需要 24 小時才能產生新的標準型發現項目，並將合併的發現項目歸檔。在此期間，您可能會在帳戶中看到基於標準和合併的結果混合在一起。

Security Hub console

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中，選擇設定。
3. 選擇 [一般] 索引標籤。
4. 對於控制項，請選擇編輯並關閉合併控制項發現項目。
5. 選擇儲存。

Security Hub API

1. 執行 UpdateSecurityHubConfiguration。
2. 設定ControlFindingGenerator等於STANDARD_CONTROL。

   請求示例：

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
```

```
}
```

AWS CLI

1. 執行 update-security-hub-configuration 命令。
2. 設定control-finding-generator等於STANDARD_CONTROL。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Compliance控制項結果詳細資料

針對控制項安全性檢查所產生的發現項目， AWS 安全性搜尋結果格式 (ASFF) 中的Compliance欄位包含與控制項發現項目相關的詳細資訊。Compliance 欄位包含以下資訊。

AssociatedStandards

在中啟用控制項的啟用標準。

RelatedRequirements

所有啟用標準中控制項的相關需求清單。這些要求來自控制項的第三方安全性架構，例如支付卡產業資料安全標準 (PCI DSS)。

SecurityControlId

資訊安全 Security Hub 支援的各種安全性標準控制項的識別碼。

Status

最近一次檢查的結果，Security Hub 運行給定的控制。之前的檢查結果會保留在存檔狀態，為期 90 天。

StatusReasons

包含值的原因清單Compliance.Status。針對每個原因，StatusReasons 包括原因代碼和描述。

下表列出可用的狀態原因代碼與說明。修正步驟取決於使用原因代碼產生發現項目的控制項。從中選擇一個控制項Security Hub 控制項參考以查看該控制項的修正步驟。

原因代碼	Compliance.Status	描述
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	多區域 CloudTrail 追蹤沒有有效的量度篩選器。
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	多區域 CloudTrail 軌跡不存在量度篩選器。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	帳戶沒有具有必要組態的多區域 CloudTrail 追蹤。
CLOUDTRAIL_REGION_INVAILD	WARNING	多區域 CloudTrail 軌跡不在目前的區域中。
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	沒有有效的警示動作。
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch 帳戶中不存在警報。
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config 狀態為 ConfigError	AWS Config 訪問被拒絕。 確認 AWS Config 已啟用且已被授與足夠的權限。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config 根據規則評估您的資源。 規則不適用於其範圍內的 AWS 資源、刪除指定的資源或評估結果已刪除。
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	符合性狀態是NOT_AVAILABLE 因為 AWS Config 傳回的狀態為「不適用」。

原因代碼	Compliance.Status	描述
		AWS Config 不提供狀態的原因。以下是「不適用」狀態的一些可能原因： • 資源已從規則的範圍中移 AWS Config 除。 • 規 AWS Config 則已刪除。 • 資源已刪除。 • AWS Config 規則邏輯可產生「不適用」狀態。
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Config 狀態為 `ConfigError`	這個原因代碼用於數種不同類型的評估錯誤。 此描述會提供特定的原因資訊。 錯誤類型可以是下列其中一種： • 由於缺乏許可，因此無法執行評估。此描述提供遺失的特定許可。 • 缺少或無效的參數值。此描述提供參數和參數值的需求。 • 從 S3 儲存貯體讀取時發生錯誤。此描述可識別儲存貯體並提供特定的錯誤。 • 遺失的 AWS 訂閱。 • 評估的一般逾時。 • 遭停權的帳戶。

原因代碼	Compliance.Status	描述
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config 狀態為 ConfigError	規 AWS Config 則正在建立中。
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	發生未知的錯誤。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	失敗	Security Hub 無法針對自訂 Lambda 執行階段執行檢查。
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	發現項目處於WARNING狀態，因為與此規則相關聯的 S3 儲存貯體位於不同的區域或帳戶中。 此規則不支援跨區域或跨帳戶檢查。 建議您在此區域或帳戶中停用此控制項。只能在資源所在的區域或帳戶中執行。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch 日誌指標篩選器沒有有效的 Amazon SNS 訂閱。
SNS_TOPIC_CROSS_ACCOUNT	WARNING	發現項目處於某個WARNING狀態。 與此規則相關聯的 SNS 主題由不同帳戶所擁有。當前帳戶無法獲取訂閱信息。 擁有 SNS 主題的帳戶必須將 SNS 主題的sns:ListSubscriptionsByTopic 權限授與目前帳戶。

原因代碼	Compliance.Status	描述
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	發現項目處於WARNING狀態，因為與此規則相關聯的 SNS 主題位於不同的區域或帳戶中。 此規則不支援跨區域或跨帳戶檢查。 建議您在此區域或帳戶中停用此控制項。只能在資源所在的區域或帳戶中執行。
SNS_TOPIC_INVALID	FAILED	與此規則相關聯的 SNS 主題無效。
THROTTLING_ERROR	NOT_AVAILABLE	相關 API 操作超過允許的速率。

ProductFields控制項結果詳細資料

當 Security Hub 執行安全性檢查並產生控制項發現項目時，ASFF 中的ProductFields屬性包含下列欄位：

ArchivalReasons:0/Description

說明 Security Hub 為何封存現有的發現項目。

例如，當您停用控制項或標準，以及開啟或關閉合併控制項發現項目時，Security Hub 會封存現有的發現項目。

ArchivalReasons:0/ReasonCode

提供 Security Hub 封存現有發現項目的原因。

例如，當您停用控制項或標準，以及開啟或關閉合併控制項發現項目時，Security Hub 會封存現有的發現項目。

StandardsGuideArn 或 StandardsArn

與控制項相關聯之標準的 ARN。

對於 CIS AWS 基準基準標準，該領域是StandardsGuideArn。

對於 PCI DSS 和 AWS 基礎安全性最佳做法標準，欄位為。StandardsArn

如果您開啟合併的控制項發現項目，Compliance.AssociatedStandards則會移除這些欄位。

StandardsGuideSubscriptionArn 或 StandardsSubscriptionArn

該帳戶訂閱標準的 ARN。

對於 CIS AWS 基準基準標準，該領域是StandardsGuideSubscriptionArn。

針對 PCI DSS 和 AWS 基礎安全性最佳做法標準，欄位為。StandardsSubscriptionArn

如果您開啟合併控制項發現項目，則會移除這些欄位。

RuleId 或 ControlId

控制項的識別碼。

對於 CIS AWS 基準基準標準，該領域是RuleId。

對於其他標準，欄位為ControlId。

如果您開啟合併的控制項發現項目，Compliance.SecurityControlId則會移除這些欄位。

RecommendationUrl

控制項之修正資訊的 URL。如果您開啟合併的控制項發現項目，Remediation.Recommendation.Url則會移除此欄位。

RelatedAWSResources:0/name

與發現項目相關聯的資源名稱。

RelatedAWSResource:0/type

與控制項相關聯的資源類型。

StandardsControlArn

組態的 ARN。如果您開啟合併的控制項發現項目，則會移除此欄位。

aws/securityhub/ProductName

對於以控制項為基礎的發現項目，產品名稱為 Security Hub。

aws/securityhub/CompanyName

對於以控制項為基礎的發現項目，公司名稱為 AWS。

`aws/securityhub/annotation`

控制項所發現之問題的描述。

`aws/securityhub/FindingId`

發現項目的識別碼。如果您開啟合併的控制項發現項目，則此欄位不會參考標準。

指派嚴重性給控制項發現

指派給 Security Hub 控制項的嚴重性可識別控制項的重要性。控制項的嚴重性決定指派給控制項發現項目的嚴重性標籤。

嚴重性標準

控制項的嚴重性是根據下列準則的評估來決定：

- 威脅執行者利用與控制項相關的組態弱點有多困難？

  難度取決於使用弱點執行威脅案例所需的複雜程度或複雜性。
- 這些弱點會導致您的 AWS 帳戶 或資源妥協的可能性有多大？

  您 AWS 帳戶 或資源的損害意味著您的數據或 AWS 基礎設施的機密性，完整性或可用性以某種方式損壞。

  入侵的可能性表示威脅案例會導致 AWS 服務或資源中斷或違反的可能性。

例如，請考慮下列組態弱點：

- 使用者存取金鑰不會每 90 天輪換一次。
- IAM 根使用者金鑰存在。

對於對手來說，這兩個弱點同樣難以利用。在這兩種情況下，對手都可以使用憑證盜竊或其他方法來獲取用戶密鑰。然後，他們可以使用它以未經授權的方式訪問您的資源。

但是，如果威脅執行者取得 root 使用者存取金鑰，則遭到入侵的可能性會更高，因為這樣可以提供他們更多的存取權。因此，root 使用者金鑰弱點具有較高的嚴重性。

嚴重性不會考慮基礎資源的重要性。重要性是與發現項目相關聯之資源的重要性層級。例如，與任務關鍵應用程式相關聯的資源比與非生產測試相關聯的資源更為重要。若要擷取資源重要性資訊，請使用「 AWS 安全性搜尋結果格式 (ASFF)`Criticality`」欄位。

下表對應了要惡意利用的難度，以及危害到安全性標籤的可能性。

	妥協極有可能	妥協可能	妥協不可能	妥協極不可能
非常容易利用	嚴重	嚴重	高	中
有點容易利用	嚴重	高	中	中
有點難以利用	高	中	中	低
非常難被利用	中	中	低	低

嚴重性定義

嚴重性標籤的定義如下。

嚴重 — 應立即修正問題，以避免問題升級。

舉例來說，開啟的 S3 儲存貯體將視作重大嚴重性問題。由於有許多威脅參與者會掃描開放的 S3 儲存貯體，因此外露 S3 儲存貯體中的資料很可能會被其他人探索並存取。

一般而言，可公開存取的資源會被視為重要的安全性問題。您應該以最緊迫的方式對待關鍵發現。您還應該考慮資源的重要性。

高 — 必須將此問題視為短期優先順序來解決。

例如，如果預設 VPC 安全群組對輸入和輸出流量開放，則會將其視為高嚴重性。威脅參與者使用此方法破壞 VPC 有些容易。威脅參與者也有可能在資源進入 VPC 後中斷或洩漏資源。

Security Hub 建議您將高嚴重性發現視為近期優先順序。您應立即採取補救措施。您還應該考慮資源的重要性。

中 — 這個問題應作為中期優先處理。

例如，傳輸中的資料缺乏加密被視為中等嚴重性發現項目。它需要複雜的 man-in-the-middle 攻擊才能利用這個弱點。換句話說，這有點困難。如果威脅情況成功，則某些數據可能會受到損害。

Security Hub 建議您儘早調查隱含的資源。您還應該考慮資源的重要性。

低 — 問題本身不需要採取任何動作。

例如，無法收集鑑識資訊會被視為低嚴重性。這種控制可以幫助防止 future 的妥協，但是缺少鑑識並不會直接導致妥協。

您不需要立即對低嚴重性發現項目採取行動，但是當您將這些問題與其他問題產生關聯時，它們可以提供內容。

資訊 — 找不到組態弱點。

換句話說，狀態為PASSEDWARNING、或NOT AVAILABLE。

沒有任何建議的動作。參考性問題清單能協助客戶證明自己處於合規狀態。

更新控制項發現項的規則

對指定規則進行後續檢查可能會產生新結果。例如，「避免使用 root 使用者」的狀態可能會從變更FAILED為PASSED。在這種情況下，會產生包含最新結果的新發現項目。

如果指定規則後續檢查產生的結果與目前結果一模一樣，則更新現有的問題清單。不產生任何新的問題清單。

如果刪除關聯的資源、資源不存在或控制項已停用，Security Hub 會自動封存控制項中的發現項目。資源可能不再存在，因為目前未使用關聯的服務。系統會根據下列其中一個條件自動封存發現項目：

- 發現結果在三到五天內不會更新（請注意，這是最好的努力，並不能保證）。
- 傳回相關的 AWS Config 評估NOT_APPLICABLE。

法規遵循狀態和控制狀態

「 AWS 安全性發現項目格式Compliance.Status」欄位說明控制項搜尋結果的結果。Security Hub 使用控制項發現項目的符合性狀態來判斷整體控制項狀態。控制項狀態會顯示在 Security Hub 主控台上控制項的詳細資料頁面上。

對於管理員帳戶，控制狀態會反映管理員帳戶和成員帳戶中的控制狀態。具體而言，如果控制項在系統管理員帳戶或任何成員帳戶中有一或多個失敗的發現項目，則控制項的整體狀態會顯示為「失敗」。如果您已設定彙總「區域」，則聚總「區域」中的控制項狀態會反映聚總「區域」與「連結區域」中的控制項狀態。具體而言，如果控制項在聚總「區域」或任何連結的「區域」中有一或多個失敗的發現項目，則控制項的整體狀態會顯示為「失敗」。

Security Hub 通常會在您第一次造訪 Security Hub 主控台的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內產生初始控制項狀態。您必須配置AWS Config 資源記錄，才能顯示控制狀態。首次產生控制項狀態之後，Security Hub 會根據前 24 小時的發現項目，每 24 小時更新一次控制項狀態。控制項詳細資訊頁面上的時間戳記會指出上次更新控制項狀態的時間。

> **Note**
>
> 在啟用控制中國地區和中國地區產生首次控制狀態後，最多可能需要 24 小時的時間 AWS GovCloud (US) Region。

發現項目之符合性狀態的值

系統會為每個發現項目的符合性狀態指派下列其中一個值：

- PASSED— 自動將安全中心設定Workflow.Status為RESOLVED。

  如果Compliance.Status發現項目從、或; 變更PASSED為FAILEDWARNING、或NOT_AVAILABLE; 且Workflow.Status是NOTIFIED或RESOLVED;，則 Security Hub 會自動設定Workflow.Status為NEW。

  如果您沒有與控制項對應的資源，Security Hub 會在帳戶層級產生PASSED發現項目。如果您擁有與控制項對應的資源，但隨後刪除資源，Security Hub 會建立NOT_AVAILABLE尋找項目並立即將其封存。18 小時後，您會收到一個PASSED發現結果，因為您不再擁有與控制項對應的資源。
- FAILED— 指出控制項未通過此發現項目的安全性檢查。
- WARNING— 指出檢查已完成，但 Security Hub 無法判斷資源是否處於PASSED或FAILED狀態。
- NOT_AVAILABLE— 指出因伺服器失敗、資源已刪除或 AWS Config 評估結果而造成檢查無法完成NOT_APPLICABLE。

  如果 AWS Config 評估結果是NOT_APPLICABLE，Security Hub 會自動封存發現項目。

控制狀態的值

Security Hub 會從控制項發現項目的符合性狀態衍生出整體控制項狀態。決定控制項狀態時，Security Hub 會忽略具有RecordState共ARCHIVED和的發現項目SUPPRESSED。Workflow.Status

控制狀態被分配下列值之一：

- 已通過 — 表示所有發現項目的符合性狀態為PASSED。
- 失敗 — 表示至少有一個發現項目的符合性狀態為FAILED。
- 未知 — 表示至少有一個發現項目的符合性狀態為WARNING或NOT_AVAILABLE。沒有發現項目的符合性狀態為FAILED。

- 無資料 — 表示控制項沒有發現項目。例如，新啟用的控制項會有此狀態，直到 Security Hub 開始為其產生發現項目為止。如果所有發現項目都在SUPPRESSED或目前「區域」中無法使用，則控制項也會具有此狀態。
- 已停用 — 表示目前帳戶和區域中的控制項已停用。目前沒有針對目前帳戶和區域中的此控制項執行安全性檢查。不過，停用控制項的發現可能會在停用後最多 24 小時內具有符合性狀態的值。

決定安全分數

Security Hub 主控台的 [摘要] 頁面和 [控制項] 頁面會顯示所有已啟用標準的摘要安全分數。在 [安全性標準] 頁面上，Security Hub 也會針對每個已啟用的標準，顯示介於 0-100% 之間的安全分數。

當您第一次啟用 Security Hub 時，Security Hub 會在您第一次造訪 Security Hub 主控台的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內計算摘要安全分數和標準安全分數。只有在您造訪這些頁面時啟用的標準，才會產生分數。若要檢視目前已啟用的標準清單，請呼叫 `GetEnabledStandards`API 作業。此外，必須配置 AWS Config 資源記錄才能顯示分數。安全分數摘要是標準安全分數的平均值。

在第一次產生分數之後，Security Hub 會每 24 小時更新一次安全分數。Security Hub 會顯示時間戳記，以指出上次更新安全分數的時間。

> **Note**
>
> 在中國和地區產生首次安全分數可能需要長達 24 小時的時間 AWS GovCloud (US) Region。

如果您開啟合併控制項發現項目，最多可能需要 24 小時才能更新安全分數。此外，啟用新的彙總區域或更新連結的區域會重設現有的安全分數。Security Hub 最多可能需要 24 小時才能產生新的安全分數，其中包括來自更新區域的資料。

安全分數的計算方式

安全分數代表「通過」控制項與已啟用控制項的比例。分數會以四捨五入至最接近的整數的百分比顯示。

Security Hub 會計算所有已啟用標準的摘要安全分數。Security Hub 也會針對每個已啟用的標準計算安全分數。為了計算分數，啟用的控制項包括狀態為「通過」、「失敗」和「未知」的控制項。狀態為「無資料」的控制項會從評分計算中排除。

Security Hub 會在計算控制狀態時忽略封存和隱藏的發現項目。這可能會影響安全分數。例如，如果您針對某個控制項隱藏所有失敗的發現項目，其狀態會變成「已通過」，進而改善您的安全分數。如需控制項狀態的詳細資訊，請參閱法規遵循狀態和控制狀態。

評分示例：

標準	通過控制	失敗的控制	未知的控制	標準分數
AWS 基礎安全性最佳做法 v1.0.0	168	22	0	88%
獨聯體 AWS 基金會基準 v1.4.0	8	29	0	22%
獨聯體 AWS 基金會基準 v1.2.0	6	35	0	15%
NIST 特別刊物 800-53 修訂版第五期	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

計算摘要安全分數時，Security Hub 只會計算跨標準的每個控制項一次。例如，如果您已啟用適用於三個已啟用標準的控制項，則該控制項僅會計為一個已啟用的控制項，以供評分使用。

在此範例中，雖然已啟用標準中已啟用的控制項總數為 528 個，但是 Security Hub 只會計算每個唯一控制項一次，以便進行評分。唯一啟用的控制項數目可能會低於 528 個。如果我們假設唯一啟用的控制項數目為 515，而唯一傳遞的控制項數目為 357，則摘要分數為 69%。此分數的計算方式是將唯一傳遞的控制項數除以唯一啟用的控制項數目。

您的摘要分數可能與標準安全分數不同，即使您只在目前的區域中的帳戶中啟用了一個標準。如果您已登入系統管理員帳戶，且成員帳戶已啟用其他標準或不同的標準，則可能會發生這種情況。如果您正在檢視彙總區域的分數，並且在連結的區域中啟用了其他標準或不同標準，也可能會發生這種情況。

管理員帳戶的安全分數

如果您已登入系統管理員帳戶，則系統管理員帳戶和所有成員帳戶中的控制狀態的摘要安全性分數和標準分數會計入帳戶。

如果即使是一個成員帳戶中的控制項狀態為「失敗」，則其狀態會在系統管理員帳戶中為「失敗」，並會影響系統管理員帳戶分數。

如果您已登入管理員帳戶，並且正在檢視彙總區域中的分數，安全性分數會將所有成員帳戶和所有連結區域的控制狀態納入考量。

安全分數 (如果您已設定彙總區域)

如果您已設定彙總 AWS 區域，則彙總安全分數和標準分數會列入所有控制項狀態 連結的區域。

如果某個連結「區域」中的控制項狀態為「失敗」，則其在聚總「區域」中的狀態為「失敗」，並會影響聚總「區域」評分。

如果您已登入管理員帳戶，並且正在檢視彙總區域中的分數，安全性分數會將所有成員帳戶和所有連結區域的控制狀態納入考量。

Security Hub 標準參考

AWS Security Hub 目前支援本節中詳述的安全性標準。

選擇標準以檢視標準的更多詳細資訊，以及套用至該標準的控制項。

Security Hub 標準和控制並不保證符合任何法規架構或稽核。相反地，這些控制項提供了一種監視 AWS 帳戶 和資源目前狀態的方法。

支援的標準

- AWS 基礎安全性最佳做法 (FSBP) 標準
- 互聯網安全中心（CIS） AWS 基準基準 v1.2.0 和 1.4.0 版
- 美國國家標準與技術研究院 (NIST)
- 支付卡產業資料安全標準 (PCI DSS)
- 服務管理標準

AWS 基礎安全性最佳做法 (FSBP) 標準

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

該標準可讓您持續評估所有工作負載 AWS 帳戶 和工作負載，以快速識別偏離最佳實務的區域。它提供有關如何改善和維護組織安全性狀態的可行性和規範性指引。

這些控制項包括來自多個資源的安全性最佳做法 AWS 服務。每個控制項也會指派一個類別，以反映套用至的安全性功能。如需詳細資訊，請參閱 the section called “控制類別”。

套用至 FSBP 標準的控制項

[帳戶。1] 應提供安全聯繫信息 AWS 帳戶

[ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約

[ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度

應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄

應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證

API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray

[原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯

[介面 5] API Gateway REST API 快取資料應在靜態時加密

API Gateway 路由應該指定授權類型

應該為 API Gateway V2 階段配置訪問日誌記錄

[AppSync.2] AWS AppSync 應啟用欄位層級記錄

[AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證

[Athena.1] Athena 工作群組應在靜態時加密

[AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查

[AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域

[AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）

[AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1

[自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址

[AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型

[AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板

[Backup 1] AWS Backup 復原點應該在靜態時加密

[CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成

[CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

[CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

[CloudFront.4] CloudFront 發行版應該配置原始容錯移轉

[CloudFront.5] CloudFront 發行版應啟用日誌記錄

[CloudFront.6] CloudFront 發行版應啟用 WAF

[CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證

[CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求

[CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量

[CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議

[CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

[CloudFront.13] CloudFront 發行版應使用源訪問控制

[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

[CloudTrail.2] CloudTrail 應啟用靜態加密

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據

[CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據

[CodeBuild.3] CodeBuild S3 日誌應加密

[CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置

[CodeBuild.5] CodeBuild 項目環境不應啟用特權模式

[Config 1] AWS Config 應該被啟用

[DMS.1] Database Migration Service 複製執行個體不應該是公用的

[DMS.6] DMS 複製執行個體應啟用自動次要版本升級

[DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄

[DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄

[DMS.9] DMS 端點應使用 SSL

[文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密

[文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

[文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的

[文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch

[文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護

[DynamoDB 資料表應該會根據需求自動擴展容量

[動態 DynamoDB] 資料表應該已啟用復原 point-in-time

[動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密

[動態 DynamoDB] 資料表應該已啟用刪除保護

[EC2.1] Amazon EBS 快照不應公開還原

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

[EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密

[EC2.4] 停止的 EC2 執行個體應在指定時間段後移除

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

[EC2.7] 應啟用 EBS 預設加密

[EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)

[EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址

[EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點

[EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址

[EC2.16] 應移除未使用的網路存取控制清單

[EC2.17] Amazon EC2 執行個體不應使用多個 ENI

[EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量

[EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠

[EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動

[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389

[EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求

[EC2.24] 不應使用 Amazon EC2 半虛擬實例類型

[EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面

[EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄

[ECR.1] ECR 私有儲存庫應設定影像掃描

[ECR.2] ECR 私有儲存庫應配置標籤不變性

[ECR.3] ECR 儲存庫應該至少設定一個生命週期原則

[ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。

[ECS.2] ECS 服務不應該自動分配公共 IP 地址

[ECS.3] ECS 任務定義不應共享主機的進程名稱空間

[ECS.4] ECS 容器應以非特權的方式執行

[ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取

[ECS.8] 密碼不應作為容器環境變量傳遞

[ECS.9] ECS 任務定義應具有記錄組態

[ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行

[ECS.12] ECS 叢集應使用容器深入解析

[EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS

[EFS.2] Amazon EFS 磁碟區應該在備份計劃中

[EFS.3] EFS 存取點應強制執行根目錄

[EFS.4] EFS 存取點應強制執行使用者身分

[EKS.1] EKS 叢集端點不應可公開存取

[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行

[EKS.8] EKS 叢集應啟用稽核記錄

[ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份

[ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級

[ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移

[ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密

[ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密

[ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH

[ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組

[ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告

[ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新

[ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch

[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS

[ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager

[ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定

[ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭

[ELB.5] 應啟用應用程式和傳統負載平衡器記錄

[ELB.6] 應該啟用應用 Application Load Balancer 刪除保護

[ELB.7] 傳統負載平衡器應啟用連線排空

[ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config

[ELB.9] 傳統負載平衡器應啟用跨區域負載平衡

[ELB.10] Classic Load Balancer 應該跨越多個可用區域

[ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

[ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域

[ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

[EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址

[EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置

[ES.1] 彈性搜尋網域應啟用靜態加密

[ES.2] 彈性搜索域名不應公開訪問

[E.3] 彈性搜尋網域應加密節點之間傳送的資料

[ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌

[.5] 彈性搜尋網域應啟用稽核記錄

[ES.6] 彈性搜尋網域至少應該有三個資料節點

[ES.7] 彈性搜尋網域至少應設定三個專用主節點

[.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線

[EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略

[FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區

[GuardDuty.1] GuardDuty 應該啟用

[IAM.1] IAM 政策不應允許完整的「*」管理特權

[IAM.2] IAM 使用者不應附加 IAM 政策

[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

[IAM.4] IAM 根使用者存取金鑰不應存在

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

[IAM.6] 應為根使用者啟用硬體 MFA

[IAM.7] IAM 使用者的密碼政策應具有強大的組態

[IAM.8] 應移除未使用的 IAM 使用者登入資料

[IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作

[Kinesis.1] Kinesis 串流應該在靜態時加密

[KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作

[KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策

不應意外刪除 [KMS AWS KMS keys .3]

[Lambda 1] Lambda 函數政策應該禁止公共訪問

[Lambda 2] Lambda 函數應該使用受支援的執行階段

VPC Lambda 函數應在多個可用區域中運作

[Macie.1] Amazon Macie 應該啟用

[Macie.2] 應啟用 Macie 自動化敏感資料探索功能

[MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密

[Neptune .1] Neptune DB 叢集在靜態時應加密

[Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch

[Neptune .3] Neptune DB 叢集快照不應該是公開的

[Neptune .4] Neptune 資料庫叢集應啟用刪除保護

[Neptune .5] Neptune 資料庫叢集應啟用自動備份

[Neptune .6] Neptune 資料庫叢集快照在靜態時應加密

[Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證

[Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照

[NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄

[NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組

[NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送

[NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送

[NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空

[NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護

OpenSearch 網域應啟用靜態加密功能

[打開搜索 .2] OpenSearch 域名不應該是公開訪問

OpenSearch 網域應該加密節點之間傳送的資料

應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄

OpenSearch 網域應該已啟用稽核記錄

OpenSearch 網域應該至少有三個資料節點

OpenSearch 網域應該啟用精細的存取控制

應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接

OpenSearch 網域應該已安裝最新的軟體更新

[PCA.1] AWS Private CA 根憑證授權單位應停用

[路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢

[RDS.1] RDS 快照應該是私有的

[RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config

[RDS.3] RDS 資料庫執行個體應啟用靜態加密

[RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密

[RDS.5] RDS 資料庫執行個體應設定為多個可用區域

[RDS.6] 應為 RDS 資料庫執行個體設定增強型監控

[RDS.7] RDS 叢集應該已啟用刪除保護

[RDS.8] RDS 資料庫執行個體應啟用刪除保護

[RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch

[RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證

[RDS.11] RDS 執行個體應該已啟用自動備份

[RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證

應啟用 RDS 自動次要版本升級

[RDS.14] Amazon Aurora 叢集應啟用回溯

[RDS.15] 應為多個可用區域設定 RDS 資料庫叢集

[RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照

[RDS.17] RDS 資料庫執行個體應設定為將標籤複製到快照

虛擬私人雲端應部署 RDS 執行 VPC

[RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱

[RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱

[RDS.21] 應為重要資料庫參數群組事件設定 RDS 事件通知訂閱

[RDS.22] 應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱

[RDS.23] RDS 執行個體不應使用資料庫引擎預設連接埠

[RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱

[RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱

[RDS.27] RDS 資料庫叢集應在靜態時加密

[RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch

[RDS.35] RDS 資料庫叢集應啟用自動次要版本升級

[紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問

[紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密

[紅移 3] 亞馬遜 Redshift 集群應啟用自動快照

[紅移 4] 亞馬遜 Redshift 叢集應啟用稽核記錄

[紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本

[紅移 .7] Redshift 叢集應使用增強型 VPC 路由

[Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名

[紅移 .9] Redshift 叢集不應使用預設的資料庫名稱

[紅移 .10] Redshift 叢集在靜態時應加密

[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定

[S3.2] S3 通用存儲桶應該阻止公共讀取訪問

[S3.3] S3 通用存儲桶應該阻止公共寫入訪問

[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求

[S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶

[S3.8] S3 通用存儲桶應阻止公共訪問

[S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄

[S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態

[S3.11] S3 一般用途儲存貯體應啟用事件通知

[S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取

[S3.13] S3 一般用途儲存貯體應具有生命週期組態

[S3.19] S3 存取點應該已啟用封鎖公用存取設定

[SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網

[SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動

[SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限

[SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉

[SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉

[SecretsManager.3] 刪除未使用的 Secrets Manager 秘密

[SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替

[SNS.1] SNS 主題應該使用靜態加密 AWS KMS

[SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄

[SQS.1] Amazon SQS 佇列應該在靜態時加密

[SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager

[SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」

[SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態

[SSM.4] SSM 文件不應該是公開的

[StepFunctions.1] Step Functions 狀態機應該打開日誌記錄

[WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能

[WAF.2] AWS WAF 經典區域規則至少應具有一個條件

[WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則

[WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組

[WAF.6] AWS WAF 經典全域規則至少應該有一個條件

[WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則

[WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

[WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組

[WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

互聯網安全中心（CIS）AWS 基準基準 v1.2.0 和 1.4.0 版

CIS AWS 基準基準可作為一組安全配置最佳實踐 AWS。這些業界公認的最佳做法可為您提供清晰、step-by-step 實施和評估程序。從作業系統到雲端服務和網路裝置，此基準測試中的控制項可協助您保護組織使用的特定系統。

AWS Security Hub 支持獨聯體 AWS 基礎基準測試 v1.2.0 和 1.4.0 版。

此頁面列出安全控制 ID 和標題。在 AWS GovCloud (US) Region 和中國地區，使用標準特定的控制 ID 和標題。如需安全控制 ID 和標題與標準特定控制 ID 和標題的對應，請參閱。合併如何影響控制 ID 和標題

互聯網安全中心（CIS）AWS 基準基準 v1.2.0

Security Hub 已滿足 CIS 安全軟件認證的要求，並已通過以下 CIS 基準獲得 CIS 安全軟件認證：

- 獨聯體基準基準獨聯體 AWS 基準，v1.2.0，1 級
- 獨聯體基準基準獨聯體 AWS 基準，v1.2.0，2 級

適用於獨聯體 AWS 基準基準 v1.2.0 的控制

[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

[CloudTrail.2] CloudTrail 應啟用靜態加密

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

[CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取

[CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌

[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

[CloudWatch.2] 確保未經授權的 API 調用存在日誌指標過濾器和警報

[CloudWatch.3] 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報

[CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報

[CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報

[CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報

[CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰

[CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示

[CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報

[CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報

[CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示

[CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示

[CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報

[CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報

[Config 1] AWS Config 應該被啟用

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入

[EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389

[IAM.1] IAM 政策不應允許完整的「*」管理特權

[IAM.2] IAM 使用者不應附加 IAM 政策

[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

[IAM.4] IAM 根使用者存取金鑰不應存在

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

[IAM.6] 應為根使用者啟用硬體 MFA

[IAM.8] 應移除未使用的 IAM 使用者登入資料

[IAM.9] 應該為根用戶啟用 MFA

[IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母

[IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母

[IAM.13] 確保 IAM 密碼政策至少需要一個符號

[IAM.14] 確保 IAM 密碼政策至少需要一個數字

[IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高

[IAM.16] 確保 IAM 密碼政策防止密碼重複使用

[IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期

[IAM.18] 確保已建立支援角色來管理事件 AWS Support

[IAM.20] 避免使用根用戶

[KMS.4] AWS KMS 按鍵旋轉應該已啟用

互聯網安全中心（CIS）AWS 基準基準 v1.4.0

Security Hub 支持獨聯體 AWS 基準基準的 v1.4.0。

適用於獨聯體 AWS 基準基準 v1.4.0 的控制

[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

[CloudTrail.2] CloudTrail 應啟用靜態加密

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

[CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取

[CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌

[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

[CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報

[CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報

[CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報

[CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰

[CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示

[CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報

[CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報

[CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示

[CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示

[CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報

[CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報

[Config 1] AWS Config 應該被啟用

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

[EC2.7] 應啟用 EBS 預設加密

[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389

[IAM.1] IAM 政策不應允許完整的「*」管理特權

[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

[IAM.4] IAM 根使用者存取金鑰不應存在

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

[IAM.6] 應為根使用者啟用硬體 MFA

[IAM.9] 應該為根用戶啟用 MFA

[IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高

[IAM.16] 確保 IAM 密碼政策防止密碼重複使用

[IAM.18] 確保已建立支援角色來管理事件 AWS Support

[IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料

[KMS.4] AWS KMS 按鍵旋轉應該已啟用

[RDS.3] RDS 資料庫執行個體應啟用靜態加密

[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定

[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求

[S3.8] S3 通用存儲桶應阻止公共訪問

[S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能

獨聯體 AWS 基金會基準 v1.2.0 與 1.4.0 版相比

本節總結了互聯網安全中心（CIS）AWS 基準測試 v1.4.0 和 v1.2.0 之間的差異。Security Hub 支持這個標準的兩個版本。

> **Note**
>
> 我們建議您升級至 CIS AWS 基準測試 v1.4.0，以保持最新的安全性最佳實務，但您可能同時啟用 v1.4.0 和 v1.2.0。如需詳細資訊，請參閱 啟用和停用安全性標準。如果您想要升級至 1.4.0 版，最好在停用 v1.2.0 之前先啟用 v1.4.0。如果您使用 Security Hub 整合 AWS Organizations 來集中管理多個帳戶，並且想要在所有帳戶中批次啟用 v1.4.0 (並選擇性停用 v1.2.0)，您可以從系統管理員帳戶執行 Security Hub 多帳戶指令碼。

獨聯體 AWS 基準基準 v1.4.0 中存在但不存在於 v1.2.0 中的控件

在獨聯體 AWS 基準基準 v1.4.0 中添加了以下控件。這些控件不包括在獨聯體 AWS 基準基準 v1.2.0 中。

安全控制識別碼	思維 4.0 要求	控制項標題
EC2.7	2.2.1	確保已啟用 EBS 磁碟區加密
EC2.21	5.1	確保沒有網路 ACL 允許從 0.0.0.0/0 傳入至遠端伺服器管理連接埠的流量
家居安 .22	1.12	確保停用 45 天 (含) 以上未使用的憑證
RDS.3	2.3.1	確保已啟用 RDS 執行個體的加密
S3.1	2.1.5.1	應啟用 S3 區塊公用存取設定

安全控制識別碼	思維 4.0 要求	控制項標題
S3.5	2.1.2	確保 S3 儲存貯體政策設定為拒絕 HTTP 請求
S3.8	2.1.5.2	S3 區塊公開存取設定應在儲存貯體層級啟用
S3.20	2.1.3	S3 一般用途儲存貯體應啟用 MFA 刪除

獨聯體 AWS 基準基準 v1.2.0 中存在但不存在於 v1.4.0 中的控件

以下控件僅存在於獨聯體 AWS 基準基準 v1.2.0 中。這些控件不包含在獨聯體 AWS 基準測試 v1.4.0 中。

安全控制識別碼	思維 2.0 要求	控制項標題	第 1.4.0 版中未包含的原因
CloudWatch.2	3.1	確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示	自動檢查 Security Hub 不支援
CloudWatch.3	3.2	確保在沒有 MFA 的情況下 AWS Management Console 登錄存在日誌指標過濾器和警報	自動檢查 Security Hub 不支援
EC2.13	4.1	確保沒有安全群組允許從 0.0.0.0/0 輸入連接埠 22	相反，請參閱，[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
EC2.14	4.2	確定沒有安全性群組允許從 0.0.0/0 輸入至連接埠 3389	自動檢查 Security Hub 不支援

安全控制識別碼	思維 2.0 要求	控制項標題	第 1.4.0 版中未包含的原因
IAM.2	1.16	IAM 使用者不應附加 IAM 政策	自動檢查 Security Hub 不支援
IAM .8	1.3	確保已停用 90 天或更長時間未使用的認證	相反，請參閱，[IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
IAM.11	1.5	確保 IAM 密碼政策至少需要一個大寫字母	不是本條件 1.4.0 的要求
IAM.12	1.6	確保 IAM 密碼政策至少需要一個小寫字母	不是本條件 1.4.0 的要求
IAM.13	1.7	確保 IAM 密碼政策至少需要一個符號	不是本條件 1.4.0 的要求
IAM.14	1.8	確保 IAM 密碼政策至少需要一個數字	不是本條件 1.4.0 的要求
IAM.17	1.11	確保 IAM 密碼政策在 90 天或更短的時間內過期	不是本條件 1.4.0 的要求
亞姆 .20	1.1	避免根用戶的用戶	相反，請參閱，[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

獨聯體 AWS 基準基準 v1.2.0 和 v1.4.0 中存在的控制

獨聯體 AWS 基準基準 v1.2.0 和 v1.4.0 中都存在以下控件。但是，控制項 ID 和某些控制項標題在每個版本中都有所不同。

安全控制識別碼	思維 2.0 要求	在 Cisv1.2.0 中的控制項標題	思維 4.0 要求	在 Cisv1.4.0 中的控制項標題
CloudTrail.1	2.1	確定 CloudTrail 已在所有區域中啟用	3.1	確定 CloudTrail 已在所有區域中啟用
CloudTrail.2	2.7	確保 CloudTrail 記錄檔在靜態時使用 AWS KMS keys	3.7	確保 CloudTrail 記錄檔在靜態時使用 AWS KMS keys
CloudTrail.4	2.2	確定已啟用 CloudTrail 記錄檔驗證	3.2	確定已啟用 CloudTrail 記錄檔驗證
CloudTrail.5	2.4	確保跟 CloudTrail 踪與 CloudWatch 日誌集成	3.4	確保跟 CloudTrail 踪與 CloudWatch 日誌集成
CloudTrail.6	2.3	確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取	3.3	確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
CloudTrail.7	2.6	確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌	3.6	確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌
CloudWatch.1	1.1 3.3	1.1 — 避免使用根用戶 3.3 — 確保針對 root 用戶的使用存在日誌指標過濾器和警報	1.7	不再使用 root 使用者進行管理和日常工作

安全控制識別碼	思維 2.0 要求	在 Cisv1.2.0 中的控制項標題	思維 4.0 要求	在 Cisv1.4.0 中的控制項標題
CloudWatch.4	3.4	確保 IAM 政策變更存在日誌指標篩選條件和警示	4.4	確保 IAM 政策變更存在日誌指標篩選條件和警示
CloudWatch.5	3.5	確保存在 CloudTrail配置更改的日誌指標過濾器和警報	4.5	確保存在 CloudTrail配置更改的日誌指標過濾器和警報
CloudWatch.6	3.6	確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報	4.6	確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報
CloudWatch.7	3.7	確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰	4.7	確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰
CloudWatch.8	3.8	確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	4.8	確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示
CloudWatch.9	3.9	確保存在 AWS Config 配置更改的日誌指標過濾器和警報	4.9	確保存在 AWS Config 配置更改的日誌指標過濾器和警報
CloudWatch.10	3.10	確保安全群組變更存在日誌指標篩選條件和警示	4.10	確保安全群組變更存在日誌指標篩選條件和警示

安全控制識別碼	思維 2.0 要求	在 Cisv1.2.0 中的控制項標題	思維 4.0 要求	在 Cisv1.4.0 中的控制項標題
CloudWatch.11	3.11	確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示	4.11	確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示
CloudWatch.12	3.12	確保網路閘道變更存在日誌指標篩選條件和警示	4.12	確保網路閘道變更存在日誌指標篩選條件和警示
CloudWatch.13	3.13	確保路由表變更存在日誌指標篩選條件和警示	4.13	確保路由表變更存在日誌指標篩選條件和警示
CloudWatch.14	3.14	確保 VPC 變更存在日誌指標篩選條件和警示	4.14	確保 VPC 變更存在日誌指標篩選條件和警示
Config.1	2.5	確保 AWS Config 已啟用	3.5	確定 AWS Config 已在所有區域中啟用
EC2.2	4.3	確保每個 VPC 的預設安全群組都會限制所有流量	5.3	確保每個 VPC 的預設安全群組都會限制所有流量
EC2.6	2.9	確保所有 VPC 中皆已啟用 VPC 流程日誌記錄	3.9	確保所有 VPC 中皆已啟用 VPC 流程日誌記錄
IAM.1	1.22	確保未建立允許完整「*: *」管理權限的 IAM 政策	1.16	確保並未連接允許完整 "*:*" 管理權限的 IAM 政策

安全控制識別碼	思維 2.0 要求	在 Cisv1.2.0 中的控制項標題	思維 4.0 要求	在 Cisv1.4.0 中的控制項標題
IAM.3	1.4	確保在每 90 天或更短的期限內輪換存取金鑰	1.14	確保在每 90 天或更短的期限內輪換存取金鑰
IAM.4	1.12	確保沒有 root 用戶訪問密鑰存在	1.4	確保沒有 root 用戶帳戶訪問密鑰存在
IAM.5	1.2	確保為擁有主控台密碼的所有 IAM 使用者啟用多因素身份驗證 (MFA)	1.10	確保為擁有主控台密碼的所有 IAM 使用者啟用多因素身份驗證 (MFA)
IAM.6	1.14	確定已為根使用者啟用硬體 MFA	1.6	確定已為根使用者帳戶啟用硬體 MFA
IAM.9	1.13	確定已為根使用者啟用 MFA	1.5	確定已為根使用者帳戶啟用 MFA
IAM.15	1.9	確保 IAM 密碼政策的密碼長度下限為 14 或更高	1.8	確保 IAM 密碼政策的長度至少在 14 個字元以上
IAM.16	1.10	確保 IAM 密碼政策防止重複使用密碼	1.9	確保 IAM 密碼政策防止重複使用密碼
IAM.18	1.20	確保已建立支援角色來管理事件 AWS Support	1.17	確保已建立支援角色來管理事件 AWS Support
KMS.4	2.8	確保已啟用客戶建立的 KMS 金鑰輪替	3.8	確保已啟用客戶建立的 KMS 金鑰輪替

查找獨聯體 AWS 基準基準 v1.4.0 的字段格式

當您啟用 CIS AWS 基準測試 v1.4.0 時，您將開始收到 AWS 安全查找格式（ASFF）的調查結果。對於這些發現，特定於標準的字段將參考 v1.4.0。對於 CIS AWS 基準測試 v1.4.0，請注意以下格式以GeneratorID及參考標準 Amazon 資源名稱 (ARN) 的任何 ASFF 欄位。

- 標準 ARN — `arn:partition:securityhub:region:account-id:standards/cis-aws-foundations-benchmark/v/1.4.0`
- **GeneratorID** – `cis-aws-foundations-benchmark/v/1.4.0/control ID`

您可以呼叫 GetEnabledStandardsAPI 作業來找出標準的 ARN。

> **Note**
>
> 當您啟用 CIS AWS 基準測試 v1.4.0 時，Security Hub 最多可能需要 18 小時才能針對使用與其他已啟用標準中已啟用控制項相同的 AWS Config 服務連結規則的控制項產生發現結果。如需詳細資訊，請參閱 執行安全檢查的排程。

如果您已開啟合併控制項發現項目，尋找欄位會有所不同。如需這些差異的詳細資訊，請參閱 合併對 ASFF 欄位與值的影響。如需開啟和關閉合併的 CIS 控制項結果範例，請參閱樣本控制結果。

CIS AWS 基準基準安全檢查安全性中心不支援

本節摘要說明安全性中樞目前不支援的 CIS 需求。互聯網安全中心（CIS）是一個獨立的非營利組織，制定了這些要求。

CIS AWS 基準基準 v1.2.0 安全性檢查安全中心不支援

安全中心目前不支援下列 CIS AWS 基準測試 v1.2.0 要求。

不支援的手動檢查

Security Hub 著重於自動安全檢查。因此，Security Hub 不支持 CIS AWS 基準測試 v1.2.0 的以下要求，因為它們需要手動檢查您的資源：

- 1.15 — 確保安全問題已註冊 AWS 帳戶
- 1.17 — 維護當前的聯繫方式
- 1.18 — 確保已註冊安全聯絡資訊

- 1.19 — 確保 IAM 執行個體角色用於從執行個體存取 AWS 資源
- 1.21 — 在初始使用者設定期間，請勿為具有主控台密碼的所有 IAM 使用者設定存取金鑰
- 4.4 — 確保 VPC 對等互連的路由表是「最少存取」

Security Hub 支持 CIS AWS 基準測試 v1.2.0 的所有自動檢查。

安全中心不支持的 CIS AWS 基準測試 v1.4.0 安全檢查

安全中心目前不支援下列 CIS AWS 基準測試 v1.4.0 要求。

不支援的手動檢查

Security Hub 著重於自動安全檢查。因此，Security Hub 不支持 CIS AWS 基準測試 v1.4.0 的以下要求，因為它們需要手動檢查您的資源：

- 1.1 — 維護當前的聯繫方式
- 1.2 — 確保安全聯繫信息已註冊
- 1.3 — 確保安全問題已註冊 AWS 帳戶
- 1.11 — 在初始使用者設定期間，請勿為具有主控台密碼的所有 IAM 使用者設定存取金鑰
- 1.18 — 確保 IAM 執行個體角色用於從執行個體存取 AWS 資源
- 1.21 — 確保 IAM 使用者透過聯合身分或 AWS Organizations 多帳戶環境集中管理
- 2.1.4 — 確保 Amazon S3 中的所有資料在需要時都已探查、分類和保護
- 5.4 — 確保 VPC 對等互連的路由表是「最少存取」

不支援的自動檢查

Security Hub 不支持依賴於自動檢查的 CIS AWS 基準測試 v1.4.0 的以下要求：

- 1.13 — 確保任何單一 IAM 使用者只能使用一個作用中存取金鑰
- 1.15 — 確保 IAM 使用者只能透過群組接收許可
- 1.19 — 確保所有存儲在 IAM 中過期的 SSL/TLS 證書都被刪除
- 1.20 — 確保所有區域均啟用 IAM 存取分析器
- 3.10 — 確定已針對 S3 儲存貯體啟用寫入事件的物件層級記錄
- 3.11 — 確定已針對 S3 儲存貯體啟用讀取事件的物件層級記錄
- 4.1 — 確保未經授權的 API 調用存在日誌指標過濾器和警報

- 4.2 — 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報
- 4.3 — 確保針對 root 帳戶的使用存在日誌指標過濾器和警報（這類似於自動化要求，1.7-消除 root 用戶進行管理和日常任務，這在安全中心支持）
- 4.15 — 確保存在更 AWS Organizations 改的日誌指標過濾器和警報
- 5.2 — 確保沒有安全群組允許從 0.0.0/0 輸入到遠端伺服器管理連接埠

美國國家標準與技術研究院 (NIST)

NIST SP 800-53 Rev.5 是由美國國家標準技術研究所（NIST）開發的網絡安全和合規框架，該機構是美國商務部的一部分。此法規遵循架構可協助您保護資訊系統和關鍵資源的可用性、機密性和完整性。美國聯邦政府機構和承包商必須遵守 NIST SP 800-53 以保護其系統，但私人公司可能會自願使用它作為降低網絡安全風險的指導框架。

Security Hub 提供支援特定 NIST SP 800-53 需求的控制項。這些控制項會透過自動安全檢查進行評估。Security Hub 控制項不支援需要手動檢查的 NIST SP 800-53 需求。此外，安全中心控制項僅支援自動 NIST SP 800-53 需求，這些需求在每個控制項的詳細資料中列為「相關需求」。從下列清單中選擇控制項以查看其詳細資訊。Security Hub 目前不支援控制項詳細資料中未提及的相關需求。

與其他框架不同，NIST SP 800-53 沒有規定如何評估其要求。相反，該框架提供了指導方針，而 Security Hub NIST SP 800-53 控制項代表服務對它們的理解。

如果您使用資訊安全中心整合 AWS Organizations 來集中管理多個帳戶，並且想要在所有帳戶上批次啟用 NIST SP 800-53，您可以從系統管理員帳戶執行 Security Hub 多帳戶指令碼。

如需 NIST SP 800-53 版本 5 的詳細資訊，請參閱 NIST 電腦安全性資源中心。

適用於 NIST SP 800-53 版本 5 的控制項

[帳戶。1] 應提供安全聯繫信息 AWS 帳戶

[帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations

[ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約

應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄

應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證

API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray

[原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯

[介面 5] API Gateway REST API 快取資料應在靜態時加密

API Gateway 路由應該指定授權類型

應該為 API Gateway V2 階段配置訪問日誌記錄

[AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證

[Athena.1] Athena 工作群組應在靜態時加密

[AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查

[AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域

[AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）

[AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1

[自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址

[AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型

[AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板

[Backup 1] AWS Backup 復原點應該在靜態時加密

[CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成

[CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

[CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

[CloudFront.4] CloudFront 發行版應該配置原始容錯移轉

[CloudFront.5] CloudFront 發行版應啟用日誌記錄

[CloudFront.6] CloudFront 發行版應啟用 WAF

[CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證

[CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求

[CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量

[CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議

[CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

[CloudTrail.2] CloudTrail 應啟用靜態加密

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

[CloudWatch.15] CloudWatch 警報應設定指定的動作

[CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間

[CloudWatch.17] 應啟動 CloudWatch 警報動作

[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據

[CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據

[CodeBuild.3] CodeBuild S3 日誌應加密

[CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置

[CodeBuild.5] CodeBuild 項目環境不應啟用特權模式

[Config 1] AWS Config 應該被啟用

[DMS.1] Database Migration Service 複製執行個體不應該是公用的

[DMS.6] DMS 複製執行個體應啟用自動次要版本升級

[DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄

[DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄

[DMS.9] DMS 端點應使用 SSL

[文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密

[文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

[文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的

[文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch

[文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護

[DynamoDB 資料表應該會根據需求自動擴展容量

[動態 DynamoDB] 資料表應該已啟用復原 point-in-time

[動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密

備份計劃中應該有 DynamoDB 資料表

[動態 DynamoDB] 資料表應該已啟用刪除保護

[EC2.1] Amazon EBS 快照不應公開還原

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

[EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密

[EC2.4] 停止的 EC2 執行個體應在指定時間段後移除

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

[EC2.7] 應啟用 EBS 預設加密

[EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)

[EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址

[EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點

[EC2.12] 應移除未使用的 Amazon EC2 EIP

[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入

[EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址

[EC2.16] 應移除未使用的網路存取控制清單

[EC2.17] Amazon EC2 執行個體不應使用多個 ENI

[EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量

[EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠

[EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動

[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389

[EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求

[EC2.24] 不應使用 Amazon EC2 半虛擬實例類型

[EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面

[EC2.28] 備份計劃應涵蓋 EBS 磁碟區

[EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄

[ECR.1] ECR 私有儲存庫應設定影像掃描

[ECR.2] ECR 私有儲存庫應配置標籤不變性

[ECR.3] ECR 儲存庫應該至少設定一個生命週期原則

[ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。

[ECS.2] ECS 服務不應該自動分配公共 IP 地址

[ECS.3] ECS 任務定義不應共享主機的進程名稱空間

[ECS.4] ECS 容器應以非特權的方式執行

[ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取

[ECS.8] 密碼不應作為容器環境變量傳遞

[ECS.9] ECS 任務定義應具有記錄組態

[ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行

[ECS.12] ECS 叢集應使用容器深入解析

[EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS

[EFS.2] Amazon EFS 磁碟區應該在備份計劃中

[EFS.3] EFS 存取點應強制執行根目錄

[EFS.4] EFS 存取點應強制執行使用者身分

[EKS.1] EKS 叢集端點不應可公開存取

[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行

[EKS.8] EKS 叢集應啟用稽核記錄

[ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份

[ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級

[ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移

[ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密

[ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密

[ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH

[ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組

[ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告

[ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新

[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS

[ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager

[ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定

[ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭

[ELB.5] 應啟用應用程式和傳統負載平衡器記錄

[ELB.6] 應該啟用應用 Application Load Balancer 刪除保護

[ELB.7] 傳統負載平衡器應啟用連線排空

[ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config

[ELB.9] 傳統負載平衡器應啟用跨區域負載平衡

[ELB.10] Classic Load Balancer 應該跨越多個可用區域

[ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

[ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域

[ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

[ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF

[EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址

[EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置

[ES.1] 彈性搜尋網域應啟用靜態加密

[ES.2] 彈性搜索域名不應公開訪問

[E.3] 彈性搜尋網域應加密節點之間傳送的資料

[ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌

[.5] 彈性搜尋網域應啟用稽核記錄

[ES.6] 彈性搜尋網域至少應該有三個資料節點

[ES.7] 彈性搜尋網域至少應設定三個專用主節點

[.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線

[EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略

[EventBridge.4] EventBridge 全域端點應啟用事件複寫

[FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區

[GuardDuty.1] GuardDuty 應該啟用

[IAM.1] IAM 政策不應允許完整的「*」管理特權

[IAM.2] IAM 使用者不應附加 IAM 政策

[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

[IAM.4] IAM 根使用者存取金鑰不應存在

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

[IAM.6] 應為根使用者啟用硬體 MFA

[IAM.7] IAM 使用者的密碼政策應具有強大的組態

[IAM.8] 應移除未使用的 IAM 使用者登入資料

[IAM.9] 應該為根用戶啟用 MFA

[IAM.19] 應為所有 IAM 使用者啟用 MFA

[IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作

[Kinesis.1] Kinesis 串流應該在靜態時加密

[KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作

[KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策

不應意外刪除 [KMS AWS KMS keys .3]

[KMS.4] AWS KMS 按鍵旋轉應該已啟用

[Lambda 1] Lambda 函數政策應該禁止公共訪問

[Lambda 2] Lambda 函數應該使用受支援的執行階段

[Lambda 3] Lambda 函數應該在 VPC 中

VPC Lambda 函數應在多個可用區域中運作

[Macie.1] Amazon Macie 應該啟用

[Macie.2] 應啟用 Macie 自動化敏感資料探索功能

[MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密

[MSK.2] MSK 叢集應該已設定增強型監控功能

[MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式

[MQ.6] RabbitMQ 代理程式應該使用叢集部署模式

[Neptune .1] Neptune DB 叢集在靜態時應加密

[Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch

[Neptune .3] Neptune DB 叢集快照不應該是公開的

[Neptune .4] Neptune 資料庫叢集應啟用刪除保護

[Neptune .5] Neptune 資料庫叢集應啟用自動備份

[Neptune .6] Neptune 資料庫叢集快照在靜態時應加密

[Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證

[Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照

[Neptune .9] Neptune 資料庫叢集應部署在多個可用區域

[NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署

[NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄

[NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組

[NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送

[NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送

[NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空

[NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護

OpenSearch 網域應啟用靜態加密功能

[打開搜索 .2] OpenSearch 域名不應該是公開訪問

OpenSearch 網域應該加密節點之間傳送的資料

應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄

OpenSearch 網域應該已啟用稽核記錄

OpenSearch 網域應該至少有三個資料節點

OpenSearch 網域應該啟用精細的存取控制

應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接

OpenSearch 網域應該已安裝最新的軟體更新

[PCA.1] AWS Private CA 根憑證授權單位應停用

[RDS.1] RDS 快照應該是私有的

[RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config

[RDS.3] RDS 資料庫執行個體應啟用靜態加密

[RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密

[RDS.5] RDS 資料庫執行個體應設定為多個可用區域

[RDS.6] 應為 RDS 資料庫執行個體設定增強型監控

[RDS.7] RDS 叢集應該已啟用刪除保護

[RDS.8] RDS 資料庫執行個體應啟用刪除保護

[RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch

[RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證

[RDS.11] RDS 執行個體應該已啟用自動備份

[RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證

應啟用 RDS 自動次要版本升級

[RDS.14] Amazon Aurora 叢集應啟用回溯

[RDS.15] 應為多個可用區域設定 RDS 資料庫叢集

[RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照

[RDS.17] RDS 資料庫執行個體應設定為將標籤複製到快照

虛擬私人雲端應部署 RDS 執行 VPC

[RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱

[RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱

[RDS.21] 應為重要資料庫參數群組事件設定 RDS 事件通知訂閱

[RDS.22] 應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱

[RDS.23] RDS 執行個體不應使用資料庫引擎預設連接埠

[RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱

[RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱

[RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護

[RDS.27] RDS 資料庫叢集應在靜態時加密

[RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch

[RDS.35] RDS 資料庫叢集應啟用自動次要版本升級

[紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問

[紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密

[紅移 3] 亞馬遜 Redshift 集群應啟用自動快照

[紅移 4] 亞馬遜 Redshift 叢集應啟用稽核記錄

[紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本

[紅移 .7] Redshift 叢集應使用增強型 VPC 路由

[Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名

[紅移 .9] Redshift 叢集不應使用預設的資料庫名稱

[紅移 .10] Redshift 叢集在靜態時應加密

[路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢

[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定

[S3.2] S3 通用存儲桶應該阻止公共讀取訪問

[S3.3] S3 通用存儲桶應該阻止公共寫入訪問

[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求

[S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶

[S3.7] S3 一般用途儲存貯體應使用跨區域複寫

[S3.8] S3 通用存儲桶應阻止公共訪問

[S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄

[S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態

[S3.11] S3 一般用途儲存貯體應啟用事件通知

[S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取

[S3.13] S3 一般用途儲存貯體應具有生命週期組態

[S3.14] S3 一般用途儲存貯體應啟用版本控制

[S3.15] S3 一般用途儲存貯體應啟用物件鎖定

[S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys

[S3.19] S3 存取點應該已啟用封鎖公用存取設定

[S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能

[SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網

[SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動

[SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限

[SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉

[SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉

[SecretsManager.3] 刪除未使用的 Secrets Manager 秘密

[SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替

[SNS.1] SNS 主題應該使用靜態加密 AWS KMS

[SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄

[SQS.1] Amazon SQS 佇列應該在靜態時加密

[SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager

[SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」

[SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態

[SSM.4] SSM 文件不應該是公開的

[WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能

[WAF.2] AWS WAF 經典區域規則至少應具有一個條件

[WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則

[WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組

[WAF.6] AWS WAF 經典全域規則至少應該有一個條件

[WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則

[WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

[WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組

[WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

[WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

支付卡產業資料安全標準 (PCI DSS)

Security Hub 中的支付卡行業數據安全標準（PCI DSS）提供了一套處理持卡人數據的 AWS 安全性最佳實踐。您可以使用此標準來發現處理持卡人資料之資源中的安全性弱點。Security Hub 目前在帳戶層級設定控制項的範圍。我們建議您在擁有儲存、處理或傳輸持卡人資料的資源的所有帳戶中啟用這些控制項。

此標準已通過 AWS 安全保證服務 LLC (AWS SAS) 的驗證，該團隊是由 PCI DSS 安全標準委員會 (PCI SSC) 認證的合格安全評估員 (QSA)，可提供 PCI DSS 指導和評估。 AWS SAS 已確認自動化檢查可協助客戶準備 PCI DSS 評估。

此頁面列出安全控制 ID 和標題。在 AWS GovCloud (US) Region 和中國地區，使用標準特定的控制 ID 和標題。如需安全控制 ID 和標題與標準特定控制 ID 和標題的對應，請參閱。合併如何影響控制 ID 和標題

套用至 PCI DSS 的控制項

[AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查

[CloudTrail.2] CloudTrail 應啟用靜態加密

[CloudTrail.3] CloudTrail 應該被啟用

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據

[CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據

[Config 1] AWS Config 應該被啟用

[DMS.1] Database Migration Service 複製執行個體不應該是公用的

[EC2.1] Amazon EBS 快照不應公開還原

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

[EC2.12] 應移除未使用的 Amazon EC2 EIP

[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入

[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS

[ES.1] 彈性搜尋網域應啟用靜態加密

[ES.2] 彈性搜索域名不應公開訪問

[GuardDuty.1] GuardDuty 應該啟用

[IAM.1] IAM 政策不應允許完整的「*」管理特權

[IAM.2] IAM 使用者不應附加 IAM 政策

[IAM.4] IAM 根使用者存取金鑰不應存在

[IAM.6] 應為根使用者啟用硬體 MFA

[IAM.8] 應移除未使用的 IAM 使用者登入資料

[IAM.9] 應該為根用戶啟用 MFA

[IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config

[IAM.19] 應為所有 IAM 使用者啟用 MFA

[KMS.4] AWS KMS 按鍵旋轉應該已啟用

[Lambda 1] Lambda 函數政策應該禁止公共訪問

[Lambda 3] Lambda 函數應該在 VPC 中

OpenSearch 網域應啟用靜態加密功能

[打開搜索 .2] OpenSearch 域名不應該是公開訪問

[RDS.1] RDS 快照應該是私有的

[RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config

[紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問

[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定

[S3.2] S3 通用存儲桶應該阻止公共讀取訪問

[S3.3] S3 通用存儲桶應該阻止公共寫入訪問

[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求

[S3.7] S3 一般用途儲存貯體應使用跨區域複寫

[SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網

[SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager

[SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」

[SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態

服務管理標準

服務管理的標準是另一個人 AWS 服務 管理的安全標準。例如，服務管理標準： AWS Control Tower是一種管理的服務管理標準。 AWS Control Tower 服務管理的標準與 Security Hub 透過下列方式管理的 AWS 安全性標準不同：

- 標準建立和刪除 — 您可以使用管理服務的主控台或 API 建立和刪除服務管理的標準，或使用 AWS CLI. 除非您以上述其中一種方式在管理服務中建立標準之前，該標準不會顯示在 Security Hub 主控台中，而且無法由 Security Hub API 或 AWS CLI.
- 不會自動啟用控制項 — 當您建立服務管理的標準時，Security Hub 和管理服務不會自動啟用適用於標準的控制項。此外，當 Security Hub 發布標準的新控制項時，它們不會自動啟用。這是從 Security Hub 管理的標準的偏離。如需有關在 Security Hub 中設定控制項的一般方式的詳細資訊，請參閱檢視和管理安全性控制。
- 啟用和停用控制項 — 我們建議您在管理服務中啟用和停用控制項，以避免漂移。
- 控制項的可用性 — 管理服務會選擇哪些控制項可作為服務管理標準的一部分。可用的控制項可能包括現有 Security Hub 控制項的全部或子集。

管理服務建立服務管理的標準並為其提供控制項之後，您就可以在 Security Hub 主控台、Security Hub API 或 AWS CLI中存取控制項發現項目、控制狀態和標準安全分數。管理服務中也可能提供部分或全部資訊。

從下列清單中選取服務管理的標準，以檢視其詳細資訊。

服務管理標準

- 服務管理標準： AWS Control Tower

服務管理標準： AWS Control Tower

本節提供服務管理標準的相關資訊： AWS Control Tower。

什麼是服務管理標準： AWS Control Tower？

此標準是專為 AWS Security Hub 和 AWS Control Tower. 它可讓您設定 AWS Control Tower 服務中安全中心偵測控制項 AWS Control Tower 旁邊的主動控制項。

主動式控制有助於確保您 AWS 帳戶 維持合規性，因為它們標記了可能導致政策違規或設定錯誤的動作。Detective 測控制項會偵測您的. AWS 帳戶透過為您的 AWS 環境啟用主動式和偵測控制，您可以在不同開發階段加強安全狀態。

> **Tip**
>
> 服務管理的標準與 AWS Security Hub 管理的標準不同。例如，您必須在管理服務中建立和刪除服務管理的標準。如需詳細資訊，請參閱 服務管理標準。

在 Security Hub 主控台和 API 中，您可以檢視服務管理標準：以 AWS Control Tower 及其他資 Security Hub 標準。

建立標準

只有在中建立標準時，才能使用此標準 AWS Control Tower。 AWS Control Tower 當您第一次使用下列其中一種方法啟用適用的控制項時，會建立標準：

- AWS Control Tower 控制台
- AWS Control Tower 應用程式介面 (呼叫 `EnableControl`API)
- AWS CLI （運行命`enable-control`令）

Security Hub 控制項在主控 AWS Control Tower 台中識別為 SH。 **##**（例如，SH。 CodeBuild1）。

當您建立標準時，如果您尚未啟用 Security Hub， AWS Control Tower 也會為您啟用 Security Hub。

如果您尚未設定 AWS Control Tower，則無法在安全中心主控台、安全中心 API 或中檢視或存取此標準 AWS CLI。即使您已設定 AWS Control Tower，您也無法在 Security Hub 中檢視或存取此標準，而不必先 AWS Control Tower 使用上述方法之一建立標準。

此標準僅適用於可用的AWS 區域AWS Control Tower 位置，包括 AWS GovCloud (US)。

啟用和停用標準中的控制項

在主控 AWS Control Tower 台中建立標準之後，您可以在這兩個服務中檢視標準及其可用控制項。

在您第一次建立標準之後，它沒有任何自動啟用的控制項。此外，當 Security Hub 新增控制項時，系統不會自動啟用服務管理標準： AWS Control Tower。您應該使用下列其中一種方法 AWS Control Tower 來啟用和停用中標準的控制項：

- AWS Control Tower 控制台
- AWS Control Tower API (呼叫`EnableControl`和 `DisableControl`API)
- AWS CLI （運行`enable-control`和`disable-control`命令）

當您變更中控制項的啟用狀態時 AWS Control Tower，變更也會反映在 Security Hub 中。

但是，停用安全中心中啟用的控制項會 AWS Control Tower 導致控制偏移。中的控制項狀態 AWS Control Tower 顯示為`Drifted`。您可以選取 AWS Control Tower 主控台中的 [重新註冊 OU]，或停用並重新啟 AWS Control Tower 用上述方法之一中的控制項，以解決此偏移問題。

在中完成啟用和停用動作可 AWS Control Tower 協助您避免控制漂移。

當您在中啟用或停用控制項時 AWS Control Tower，此動作會套用至所有帳戶和區域。如果您在 Security Hub 中啟用和停用控制項 (此標準不建議使用)，則此動作僅適用於目前的帳戶和區域。

> **Note**
>
> 中央設定無法用於管理服務管理標準： AWS Control Tower。如果您使用中央設定，則只能使用 AWS Control Tower 服務來針對集中管理的帳戶啟用和停用此標準中的控制項。

檢視啟用狀態和控制狀態

您可以使用下列其中一種方法來檢視控制項的啟用狀態：

- Security Hub 主控台、Security Hub API 或 AWS CLI

- AWS Control Tower 控制台
- AWS Control Tower 用於查看已啟用控件列表的 API（調用 ListEnabledControlsAPI）
- AWS CLI 以查看已啟用控件的列表（運行list-enabled-controls命令）

除非您在 Security Hub 中 AWS Control Tower 明確啟用該控制項，否則您Disabled在中停用的控制項在 Security Hub 中的啟用狀態為。

Security Hub 會根據控制項發現項目的工作流程狀態和符合性狀態來計算控制項狀態。如需啟用狀態和控制狀態的詳細資訊，請參閱檢視控制項的詳細資訊。

Security Hub 會根據控制項狀態計算服務管理標準： AWS Control Tower的安全分數。此分數僅適用於資訊安全中心。此外，您只能檢視安全中心中的控制項發現項目。在中不提供標準安全分數和控制項發現項目 AWS Control Tower。

> **Note**
>
> 當您啟用服務管理標準的控制項時： AWS Control Tower，Security Hub 最多可能需要 18 小時才能針對使用現有 AWS Config 服務連結規則的控制項產生發現項目。如果您已在 Security Hub 中啟用其他標準和控制項，則可能會有現有的服務連結規則。如需詳細資訊，請參閱 執行安全檢查的排程。

刪除標準

您可以使用下列其中一種方法停用所有適用的控制項， AWS Control Tower 來刪除中的此標準：

- AWS Control Tower 控制台
- AWS Control Tower 應用程式介面 (呼叫 DisableControlAPI)
- AWS CLI （運行命disable-control令）

停用所有控制項會刪除中所有受管理帳戶和受控管區域中的標準 AWS Control Tower。刪 AWS Control Tower 除中的標準會將其從 Security Hub 主控台的 [標準] 頁面中移除，而且您無法再使用 Security Hub API 或進行存取 AWS CLI。

> **Note**
>
> 停用安全中心標準中的所有控制項並不會停用或刪除標準。

停用 Security Hub 服務會移除服務管理的標準：以 AWS Control Tower 及您已啟用的任何其他標準。

尋找服務管理標準的欄位格式： AWS Control Tower

當您建立服務管理標準： AWS Control Tower 並為其啟用控制項時，您將開始接收 Security Hub 中的控制項發現項目。安全中心報告控制AWS 安全性搜尋結果格式 (ASFF). 這些是此標準的 Amazon 資源名稱 (ARN) 的 ASFF 值，並且：`GeneratorId`

- 標準 ARN — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

如需服務管理標準的搜尋範例： AWS Control Tower，請參閱樣本控制結果。

適用於服務管理標準的控制項： AWS Control Tower

服務管理標準： AWS Control Tower 支援屬於 AWS 基礎安全性最佳作法 (FSBP) 標準一部分的控制項子集。從下表中選擇一個控制項以檢視控制項的相關資訊，包括失敗發現項目的修正步驟。

下列清單顯示服務管理標準的可用控制項： AWS Control Tower控制項的區域限制符合 FSBP 標準中的必要控制區域限制。此清單顯示與標準無關的安全控制 ID。在主控 AWS Control Tower 台中，控制項識別碼會格式化為 SH。 ***##*** (例如 SH。 CodeBuild1 ）。在 Security Hub 中，如果您的帳戶中已關閉合併控制項發現項目，則該`ProductFields.ControlId`欄位會使用標準型控制 ID。基於標準的控制 ID 格式化為 CT。 ***`ControlId`***(例如，CT. CodeBuild1 ）。

- [帳戶。1] 應提供安全聯繫信息 AWS 帳戶
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- [介面 5] API Gateway REST API 快取資料應在靜態時加密
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證

- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域
- [AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）
- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型
- [AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板
- [CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤
- [CloudTrail.2] CloudTrail 應啟用靜態加密
- [CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證
- [CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [DynamoDB 資料表應該會根據需求自動擴展容量
- [動態 DynamoDB] 資料表應該已啟用復原 point-in-time
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.1] Amazon EBS 快照不應公開還原
- [EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密

- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
- [EC2.7] 應啟用 EBS 預設加密
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.2] ECS 服務不應該自動分配公共 IP 地址
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄

- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.5] 應啟用應用程式和傳統負載平衡器記錄
- [ELB.6] 應該啟用應用 Application Load Balancer 刪除保護
- [ELB.7] 傳統負載平衡器應啟用連線排空
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.9] 傳統負載平衡器應啟用跨區域負載平衡
- [ELB.10] Classic Load Balancer 應該跨越多個可用區域
- [ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [.5] 彈性搜尋網域應啟用稽核記錄

- [ES.6] 彈性搜尋網域至少應該有三個資料節點
- [ES.7] 彈性搜尋網域至少應設定三個專用主節點
- [.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.7] IAM 使用者的密碼政策應具有強大的組態
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- 不應意外刪除 [KMS AWS KMS keys .3]
- [KMS.4] AWS KMS 按鍵旋轉應該已啟用
- [Lambda 1] Lambda 函數政策應該禁止公共訪問
- [Lambda 2] Lambda 函數應該使用受支援的執行階段
- [Lambda 3] Lambda 函數應該在 VPC 中
- VPC Lambda 函數應在多個可用區域中運作
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護

- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [RDS.1] RDS 快照應該是私有的
- [RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config
- [RDS.3] RDS 資料庫執行個體應啟用靜態加密
- [RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密
- [RDS.5] RDS 資料庫執行個體應設定為多個可用區域
- [RDS.6] 應為 RDS 資料庫執行個體設定增強型監控
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.11] RDS 執行個體應該已啟用自動備份
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級

- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.17] RDS 資料庫執行個體應設定為將標籤複製到快照
- 虛擬私人雲端應部署 RDS 執行 VPC
- [RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱
- [RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱
- [RDS.21] 應為重要資料庫參數群組事件設定 RDS 事件通知訂閱
- [RDS.22] 應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱
- [RDS.23] RDS 執行個體不應使用資料庫引擎預設連接埠
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 4] 亞馬遜 Redshift 叢集應啟用稽核記錄
- [紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [紅移 .10] Redshift 叢集在靜態時應加密
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.2] S3 通用存儲桶應該阻止公共讀取訪問
- [S3.3] S3 通用存儲桶應該阻止公共寫入訪問
- [S3.5] S3 通用存儲桶應該要求使用 SSL 的請求
- [S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄
- [S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態
- [S3.11] S3 一般用途儲存貯體應啟用事件通知
- [S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取
- [S3.13] S3 一般用途儲存貯體應具有生命週期組態

- [S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [SSM.4] SSM 文件不應該是公開的
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組

如需有關此標準的詳細資訊，請參閱AWS Control Tower 使用者指南中的 Security Hub 控制項。

檢視和管理安全性標準

安全標準包括一組要求，以確定是否符合法規框架、業界最佳實務或公司政策。 AWS Security Hub 將這些需求對應至控制項，並對控制項執行安全性檢查，以評估是否符合標準的需求。控制可以在一個或多個標準中啟用。如果您開啟合併的控制項發現項目，Security Hub 會針對每個安全性檢查產生單一發現項目，即使控制項屬於多個已啟用標準的一部分。如需詳細資訊，請參閱 合併控制項結果。

如需可用標準的清單以及套用至標準的控制項，請參閱〈〉標準參考。Security Hub 主控台上的 [安全性標準] 頁面也會顯示 Security Hub 中所有支援的安全性標準及其啟用狀態。針對您帳戶中已啟用的每

個安全性標準 (或如果您在組織中至少有 AWS Organizations一個帳戶中使用整合)，您可以檢視下列資訊：

- 如果您使用中央組態，則標準在不同 Security Hub 組態原則中的啟用狀態
- 任何禁用標準的描述
- 目前在標準中啟用的控制項清單，以及這些控制項的整體狀態 (根據發現項目的符合性狀態)
- 套用至標準但目前已停用的控制項清單
- 標準的安全分數

Security Hub 會為每個標準產生一個安全分數。管理員帳戶可查看整個成員帳戶的彙總安全分數和控制狀態。如果您已設定彙總區域，則安全分數會反映所有連結區域之控制項的合規狀態。如需詳細資訊，請參閱 安全分數的計算方式。

主題

- 啟用和停用安全性標準
- 檢視標準的詳細資訊
- 啟用和停用特定標準中的控制項

啟用和停用安全性標準

您可以啟用或停用資訊安全中心中提供的每個安全性標準。

啟用任何安全性標準之前，請確定您已啟用 AWS Config 並設定資源記錄。否則，Security Hub 可能無法針對套用至標準的控制項產生發現項目。如需詳細資訊，請參閱 配置 AWS Config。

> **Note**
>
> 啟用和停用標準的指示會根據您是否使用中央規劃而有所不同。本節說明差異。集中設定可供整合 Security Hub 和的使用者使用 AWS Organizations。我們建議您使用中央組態來簡化在多帳戶、多區域環境中啟用和停用標準的程序。

啟用安全性標準

當您啟用安全性標準時，所有套用至該標準的控制項都會在其中自動啟用。Security Hub 也會開始針對套用至標準的控制項產生發現項目。

您可以選擇在每個標準中啟用和停用哪些控制項。停用控制項會停止產生控制項的發現項目，而在計算安全分數時會忽略控制項。

當您啟用 Security Hub 時，Security Hub 會在您第一次造訪 Security Hub 主控台上的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內，計算標準的初始安全分數。在中國和地區產生首次安全分數可能需要長達 24 小時的時間 AWS GovCloud (US) Region。只有在您造訪這些頁面時啟用的標準，才會產生分數。此外，必須配置 AWS Config 資源記錄才能顯示分數。在第一次產生分數之後，Security Hub 會每 24 小時更新一次安全分數。Security Hub 會顯示時間戳記，以指出上次更新安全分數的時間。若要檢視您帳戶中目前已啟用的標準清單，請叫用 GetEnabledStandardsAPI。

跨多個帳戶和區域啟用標準

若要在多個帳戶中啟用安全性標準 AWS 區域，您必須使用中央設定。

當您使用中央組態時，委派的系統管理員可以建立啟用一或多個標準的 Security Hub 組態原則。然後，您可以將組態原則與特定帳戶和組織單位 (OU) 或根建立關聯。設定原則會在您的主區域 (也稱為彙總區域) 和所有連結的區域中生效。

組態原則提供自訂功能。例如，您可以選擇在一個 OU 中僅啟用基 AWS 礎安全性最佳作法 (FSBP)，也可以選擇在另一個 OU 中啟用 FSBP 和網際網路安全中心 (CIS) AWS 基準測試 V1.4.0。如需建立啟用指定標準之組態原則的指示，請參閱 建立和關聯安全性中樞組態原則

如果您使用中央設定，Security Hub 不會自動在新帳戶或現有帳戶中啟用任何標準。而是在建立組態原則時，委派的管理員會定義要在不同帳戶中啟用哪些標準。Security Hub 提供建議的組態原則，其中僅啟用 FSBP。如需詳細資訊，請參閱 組態原則的類型。

> **Note**
>
> 委派的系統管理員可以建立組態原則，以啟用服務管理標準以外的任何標準： AWS Control Tower。您只能在 AWS Control Tower 服務中啟用此標準。如果您使用中央設定，則只能在中針對集中管理的帳戶啟用和停用此標準中的控制項 AWS Control Tower。

如果您希望某些帳戶設定自己的標準，而不是委派管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中個別設定標準。

在單一帳戶和區域中啟用標準

如果您不使用中央設定，或者您是自我管理帳戶，則無法使用設定原則來集中啟用多個帳戶和區域的標準。但是，您可以使用下列步驟在單一帳戶和區域中啟用標準。

Security Hub console

在一個帳戶和區域中啟用標準

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 確認您在要啟用標準的區域中使用安全性中樞。
3. 在 [安全中心] 瀏覽窗格中，選擇 [安全性標準]。
4. 針對您要啟用的標準，選擇 Enable (啟用)。這也會啟用該標準內的所有控制項。
5. 在您要在其中啟用標準的每個區域中重複此步驟。

Security Hub API

在一個帳戶和區域中啟用標準

1. 調用該 BatchEnableStandardsAPI。
2. 提供您要啟用之標準的 Amazon 資源名稱 (ARN)。若要取得標準 ARN，請呼叫 DescribeStandardsAPI。
3. 在您要在其中啟用標準的每個區域中重複此步驟。

AWS CLI

在一個帳戶和區域中啟用標準

1. 執行 batch-enable-standards 命令。
2. 提供您要啟用之標準的 Amazon 資源名稱 (ARN)。若要取得標準 ARN，請執行指describe-standards令。

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

範例

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. 在您要在其中啟用標準的每個區域中重複此步驟。

自動啟用預設安全性標準

如果您不使用中央設定，Security Hub 會在新帳戶加入您的組織時，自動啟用預設安全性標準。屬於預設標準一部分的所有控制項也會自動啟用。目前，自動啟用的預設安全性標準為基 AWS 礎安全性最佳實務 (FSBP) 和網際網路安全中心 (CIS) AWS 基準測試 v1.2.0。如果您偏好在新帳戶中手動啟用標準，可以關閉自動啟用的標準。

如果您使用中央組態，您可以建立啟用預設標準的組態原則，並將此原則與根建立關聯。您的所有組織帳號和 OU 都會繼承此組態原則，除非它們與不同的策略相關聯或是自我管理。

關閉自動啟用的標準

下列步驟僅適用於與整合， AWS Organizations 但不使用中央設定時。如果您未使用 [Organizations] 整合，可以在第一次啟用 Security Hub 時關閉預設標準，或者您也可以遵循停用標準的步驟。

Security Hub console

關閉自動啟用的標準的步驟

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   使用管理員帳戶的憑據登錄。
2. 在 [Security Hub] 瀏覽窗格的 [設定] 下，選擇 [組態]。
3. 在「帳戶」區段中，關閉「自動啟用預設標準」。

Security Hub API

關閉自動啟用的標準的步驟

1. 從 Security Hub 系統管理員帳戶叫用 UpdateOrganizationConfigurationAPI。
2. 若要關閉新成員帳戶中自動啟用的標準，請將「`AutoEnableStandards`等於」設定為`NONE`。

AWS CLI

關閉自動啟用的標準的步驟

1. 執行 update-organization-configuration 命令。
2. 包括`auto-enable-standards`參數以關閉新成員帳戶中自動啟用的標準。

```
aws securityhub update-organization-configuration --auto-enable-standards
```

停用安全性標準

當您停用安全性中心中的安全性標準時，會發生下列情況：

- 套用至標準的所有控制項也會停用，除非它們與其他標準相關聯。
- 不再執行停用控制項的檢查，而且不會針對停用的控制項產生其他發現項目。
- 停用控制項的現有發現項目會在大約 3-5 天後自動封存。
- Security Hub 為停用的控制項建立的 AWS Config 規則會遭到移除。

  這通常會在停用標準後的幾分鐘內發生，但可能需要更長的時間。如果第一個刪除規則的要求失敗，AWS Config 則 Security Hub 會每 12 小時重試一次。不過，如果您停用 Security Hub 或您沒有啟用任何其他標準，則 Security Hub 無法重試要求，這表示它無法刪除 AWS Config 規則。如果發生這種情況，並且您需要刪除 AWS Config 規則，請聯繫 AWS Support。

停用跨多個帳戶和區域的標準

若要停用跨多個帳戶和區域的安全性標準，您必須使用中央設定。

當您使用中央組態時，委派的管理員可以建立停用一或多個標準的組態原則。您可以將組態原則與特定帳戶和 OU 或根建立關聯。設定原則會在您的主區域 (也稱為彙總區域) 和所有連結的區域中生效。

組態原則提供自訂功能。例如，您可以選擇在一個 OU 中停用支付卡產業資料安全標準 (PCI DSS)，也可以選擇在另一個 OU 中同時停用 PCI DSS 和國家標準與技術研究所 (NIST) SP 800-53 Rev. 5。如需建立停用指定標準之組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

> **Note**
>
> 委派的系統管理員可以建立組態原則，以停用服務管理標準以外的任何標準： AWS Control Tower。您只能在 AWS Control Tower 服務中停用此標準。如果您使用中央設定，則只能在中針對集中管理的帳戶啟用和停用此標準中的控制項 AWS Control Tower。

如果您希望某些帳戶設定自己的標準，而不是委派管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中個別設定標準。

在單一帳戶和區域中停用標準

如果您不使用中央設定或是自我管理帳戶，則無法使用設定原則集中停用多個帳戶和區域中的標準。但是，您可以使用下列步驟來停用單一帳戶和區域中的標準。

Security Hub console

若要在一個帳戶和區域中停用標準

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 確認您在要停用標準的區域中使用安全性中樞。
3. 在 [安全中心] 瀏覽窗格中，選擇 [安全性標準]。
4. 針對您要停用的標準，選擇 Disable (停用)。
5. 在要禁用標準的每個區域中重複此操作。

Security Hub API

若要在一個帳戶和區域中停用標準

1. 調用該 BatchDisableStandardsAPI。
2. 針對您要停用的每個標準，提供標準訂閱 ARN。若要取得已啟用標準的訂閱 ARN，請呼叫 GetEnabledStandardsAPI。
3. 在要禁用標準的每個區域中重複此操作。

AWS CLI

若要在一個帳戶和區域中停用標準

1. 執行 batch-disable-standards 命令。
2. 針對您要停用的每個標準，提供標準訂閱 ARN。若要取得已啟用標準的訂閱 ARN，請執行命get-enabled-standards令。

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 subscription ARN"
```

範例

```
aws securityhub batch-disable-standards --standards-subscription-arns
 "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0"
```

3. 在要禁用標準的每個區域中重複此操作。

檢視標準的詳細資訊

在 AWS Security Hub 主控台上，標準的詳細資訊頁面包含下列資訊：

- 標準安全性分數，以及標準中已啟用之控制項之安全性檢查的視覺化摘要。如果與整合 AWS Organizations，則至少在一個組織帳號中啟用的控制項會被視為已啟用。
- 啟用或停用套用至標準之控制項的設定。
- 套用至標準的控制項清單。控制項會根據啟用狀態分為不同的索引標籤。[全部已啟用] 資料行中的控制項數目是 [失敗]、[未知]、[無資料] 和 [已傳遞] 資料行中的控制項總和。

您也可以使用安全中心 API，並擷 AWS CLI 取標準的詳細資料。以下各節將說明如何取得標準的詳細資料。

顯示已啟用標準 (主控台) 的詳細資料頁面

在「安全性標準」頁面中，您可以顯示已啟用標準的詳細資料頁面。

如果您已登入管理員帳戶，則可以檢視至少在一個成員帳戶中啟用的任何標準的詳細資料。

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在 [安全中心] 瀏覽窗格中，選擇 [安全性標準]。
3. 針對您要顯示其明細的標準，請選擇檢視結果。

標準安全分數和安全檢查摘要

標準詳細資料頁面的頂端是標準的安全分數。分數是傳遞控制項相對於標準的已啟用控制項 (具有資料) 數目的百分比。

Security Hub 通常會在您第一次造訪 Security Hub 主控台上的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內計算初始安全分數。只有在您造訪這些頁面時啟用的標準，才會產生分數。若要檢視目前已啟用的標準清單，請使用 GetEnabledStandardsAPI 作業。此外，必須配置 AWS Config 資源記錄才能

顯示分數。在第一次產生分數之後，Security Hub 會每 24 小時更新一次安全分數。Security Hub 會顯示時間戳記，以指出上次更新安全分數的時間。如需詳細資訊，請參閱 the section called “決定安全分數”。

> **Note**
>
> 在中國和地區產生首次安全分數可能需要長達 24 小時的時間 AWS GovCloud (US) Region。

分數旁邊是一個圖表，其中摘要針對已啟用標準之控制項的安全性檢查。此圖表顯示失敗和通過安全檢查的百分比。當您在圖表上暫停時，彈出式視窗會顯示以下內容：

- 每個嚴重性控制項的安全性檢查失敗次數
- 狀態為「未知」之控制項的安全性檢查次數
- 通過的安全檢查次數

對於管理員帳戶，標準分數和圖表會跨管理員帳戶和所有成員帳戶進行彙總。

除非您已設定彙總「區域」，否則「安全性」標準詳細資料頁面上的所有資料都是目前「區域」特定的。如果您已設定彙總區域，則安全分數會套用於所有區域，並在所有連結的區域中包含發現項目。標準詳細資料頁面上控制項的符合性狀態也會反映連結區域的發現項目，而安全性檢查的數目包括來自連結區域的發現項目。

檢視啟用標準中的控制項

當您造訪標準的詳細資料頁面時，您可以檢視適用於標準的安全性控制項清單。此清單會根據控制項的符合性狀態以及指派給每個控制項的嚴重性來排序。Security Hub 每 24 小時更新一次控制狀態和安全性檢查計數。每個索引標籤上的時間戳記會指出最近更新控制項狀態和安全性檢查計數的時間。如需詳細資訊，請參閱 the section called “法規遵循狀態和控制狀態”。

對於管理員帳戶，控制符合性狀態和安全性檢查的次數會彙總跨管理員帳戶和所有成員帳戶。

[全部已啟用] 索引標籤會列出目前在標準中啟用的所有控制項。對於管理員帳戶，[全部已啟用] 索引標籤包含在其帳戶的標準或至少一個成員帳戶中啟用的控制項。

在 [失敗]、[未知]、[無資料] 和 [已通過] 索引標籤上，會篩選 [全部已啟用] 索引標籤中的控制項，以僅包含具有特定狀態的啟用控制項。

[已停用] 索引標籤包含標準中已停用的控制項清單。對於管理員帳戶，[已停用] 索引標籤包含在其帳戶和所有成員帳戶的標準中停用的控制項。

對於每個控制項，標籤會顯示下列資訊：

- 控制項的狀態 (請參閱the section called “法規遵循狀態和控制狀態”)
- 指派給控制項的嚴重性
- 控制項 ID 和標題
- 作用中發現項目總數中失敗的作用中發現項目數目。如果適用，「檢查失敗」欄也會列出狀態為「未知」的發現項目數目。

除了每個標籤上的搜索過濾器之外，您還可以根據以下字段對列表進行排序：

- 符合性狀態
- 嚴重性
- ID
- 標題
- 檢查失敗

您可以使用任何欄排序每個清單。依預設，會排序 [全部已啟用] 索引標籤，讓失敗的控制項位於清單的頂端。這可協助您立即專注於需要修正的問題。

在其餘的索引標籤上，控制項預設會依嚴重性遞減順序排序。換句話說，關鍵控制首先是，然後是高，然後是中，然後是低嚴重性控制。

選擇您偏好的存取方式，然後依照步驟顯示已啟用標準的可用控制項。您也可以使用 DescribeStandardsControlAPI 操作來代替這些說明。

Security Hub console

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中選擇 [安全性標準]。
3. 選擇檢視標準的結果。頁面底部會列出套用至標準的控制項 (除以索引標籤)。

Security Hub API

1. 執行ListSecurityControlDefinitions並提供標準 Amazon 資源名稱 (ARN)，以取得該標準的控制 ID 清單。若要取得標準 ARN，請執行DescribeStandards。如果您未提供標準

ARN，此 API 會傳回所有 Security Hub 控制項識別碼。此 API 會傳回與標準無關的安全控制 ID，而非標準特定的控制 ID。

請求示例：

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. 執行ListStandardsControlAssociations以瞭解是否已在您帳戶中啟用的每個標準中啟用控制項。
3. 透過提供SecurityControlId或來識別控制項SecurityControlArn。分頁參數是可選的。

請求示例：

```
{
    SecurityControlId: Config.1
    NextToken: lkeyusdlk-sdlflsnd-ladfterb
    MaxResults: 5
}
```

AWS CLI

1. 執行list-security-control-definitions命令，並提供一或多個標準 ARN 以取得控制 ID 清單。若要取得標準 ARN，請執行指describe-standards令。如果您未提供標準 ARN，此命令會傳回所有 Security Hub 控制項識別碼。此命令會傳回與標準無關的安全性控制 ID，而不是標準特定的控制 ID。

```
aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
```

2. 執行list-standards-control-associations命令以瞭解是否已在您帳戶中啟用的每個標準中啟用控制項。
3. 透過提供security-control-id或來識別控制項security-control-arn。

範例命令：

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id Config.1
```

下載控制項清單

您可以將控制項清單的目前頁面下載到.csv檔案中。

如果您篩選了控制項清單，則下載的檔案只會包含符合篩選器設定的控制項。

如果您從清單中選擇特定控制項，則下載的檔案只會包含該控制項。

若要下載控制項清單的目前頁面或目前選取的控制項，請選擇 [下載]。

啟用和停用特定標準中的控制項

當您在中啟用標準時 AWS Security Hub，所有適用於該標準的控制項都會在該標準中自動啟用 (此標準的例外是服務管理的標準)。然後，您可以停用並重新啟用標準中的特定控制項。不過，我們建議您在所有已啟用的標準中對齊控制項的啟用狀態。

> **Note**
>
> 如果您使用 Security Hub 中央組態，委派的系統管理員可以針對所有已啟用標準的組織帳戶啟用和停用控制項。我們建議使用這種方法，以便控制項的啟用狀態能夠跨標準保持一致。不過，委派的管理員可以將帳戶指定為自我管理，讓他們能夠在特定標準中啟用和停用控制項。如需詳細資訊，請參閱 安全中心中的集中配置。

標準的詳細資訊頁面包含標準的適用控制項清單，以及該標準中目前已啟用和停用哪些控制項的相關資訊。

在標準詳細資料頁面上，您也可以啟用和停用特定標準中的控制項。您必須在每個和中分別啟用 AWS 帳戶 和停用控制項 AWS 區域。當您啟用或停用控制項時，它只會影響目前帳戶和區域。

您可以使用安全中心主控台、Security Hub API 或，在每個區域 Security Hub 啟用和停用控制項 AWS CLI。如果您已設定彙總「區域」，則會看到來自所有連結區域的控制項。如果某個控制項在連結的「區域」中可用，但在彙總「區域」中無法使用，則無法從彙總「區域」啟用或停用該控制項。如需多帳戶和多區域控制停用指令碼，請參閱在多帳戶環境中停用 Security Hub 控制項。

在特定標準中啟用控制項

若要啟用標準中的控制項，您必須先啟用至少一個套用控制項的標準。若要取得有關啟用標準的更多資訊，請參閱啟用和停用安全性標準。當您在標準中啟用控制項時，會 AWS Security Hub 開始產生該控制項的發現項目。Security Hub 會在整體安全分數和標準安全分數的計算中包含控制項狀態。即使您在多個標準中啟用控制項，如果您開啟合併的控制項發現項目，您仍會收到跨標準的每個安全性檢查的單一發現。如需了解更多資訊，請參閱合併的控制調查結果。

若要在標準中啟用控制項，該控制項必須在您目前的 [區域] 中可用。如需詳細資訊，請參閱依區域的控制項可用性。

請依照下列步驟啟用特定標準中的安全性中樞控制項。您也可以使用 `UpdateStandardsControl`API 動作來啟用特定標準中的控制項，而不是下列步驟。如需在所有標準中啟用控制項的指示，請參閱在單一帳戶和區域中啟用所有標準的控制。

Security Hub console

在特定標準中啟用控制項的步驟

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 從導覽窗格中選擇「安全性標準」。
3. 選擇檢視相關標準的結果。
4. 選取控制項。
5. 選擇「啟用控制項」(此選項不會針對已啟用的控制項顯示)。選擇啟用以確認。

Security Hub API

在特定標準中啟用控制項的步驟

1. 執行並提供標準 ARN`ListSecurityControlDefinitions`，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行`DescribeStandards`。此 API 會傳回與標準無關的安全控制 ID，而非標準特定的控制 ID。

   請求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 執行ListStandardsControlAssociations，並提供特定的控制項 ID，以傳回每個標準中控制項目前的啟用狀態。

   請求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. 執行 BatchUpdateStandardsControlAssociations。提供您要在其中啟用控制項之標準的 ARN。
4. 將AssociationStatus參數設定為等於ENABLED。

   請求示例：

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "ENABLED"}]
   }
   ```

AWS CLI

在特定標準中啟用控制項的步驟

1. 執行命list-security-control-definitions令，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行describe-standards。此命令會傳回與標準無關的安全性控制 ID，而不是標準特定的控制 ID。

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. 執行命list-standards-control-associations令，並提供特定的控制項 ID，以傳回每個標準中控制項目前的啟用狀態。

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

3. 執行 batch-update-standards-control-associations 命令。提供您要在其中啟用控制項之標準的 ARN。
4. 將AssociationStatus參數設定為等於ENABLED。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

停用特定標準中的控制項

當您停用標準中的控制項時，Security Hub 會停止產生控制項的發現項目。控制狀態不再用於計算標準的安全分數。

停用控制項的一種方法是停用控制項套用的所有標準。停用標準時，會停用套用至標準的所有控制項 (不過，這些控制項仍可能在其他標準中保持啟用狀態)。若要取得有關停用標準的資訊，請參閱the section called “啟用和停用標準”。

當您停用套用的標準來停用控制項時，會發生下列情況：

- 不再針對該標準執行控制項的安全性檢查。這表示控制項狀態不會影響標準安全性分數 (如果在其他標準中啟用控制項，Security Hub 將繼續執行控制項的安全性檢查)。
- 不會再為該控制項產生其他問題清單。
- 現有發現項目會在 3-5 天後自動存檔 (請注意，這是最好的努力，不能保證)。
- Security Hub 建立的相關 AWS Config 規則會移除。

當您停用標準時，Security Hub 不會追蹤哪些控制項已停用。如果您隨後再次啟用該標準，則套用至該標準的所有控制項都會自動啟用。此外，停用控制項是一次性動作。假設您停用控制項，然後啟用先前已停用的標準。如果標準包含該控制項，則會在該標準中啟用該控制項。當您在 Security Hub 中啟用標準時，會自動啟用適用於該標準的所有控制項。

您可以只在一或多個特定標準中停用控制項，而不是停用其所套用的標準來停用控制項。

若要減少發現雜訊，停用與您的環境無關的控制項會很有用。如需要停用哪些控制項的建議，請參閱您可能想要停用的 Security Hub 控制項。

請依照下列步驟停用特定標準中的控制項。您也可以使用 UpdateStandardsControlAPI 動作來停用特定標準中的控制項，而不是下列步驟。如需在所有標準中停用控制項的指示，請參閱在所有標準中啟用和停用控制項。

Security Hub console

若要停用特定標準中的控制項

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 從導覽窗格中選擇「安全性標準」。選擇檢視相關標準的結果。
3. 選取控制項。
4. 選擇「停用控制項」（已停用的控制項目不會顯示此選項）。
5. 提供停用控制項的原因，並選擇停用來確認。

Security Hub API

若要停用特定標準中的控制項

1. 執行並提供標準 ARNListSecurityControlDefinitions，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行DescribeStandards。此 API 會傳回與標準無關的安全控制 ID，而非標準特定的控制 ID。

   請求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 執行ListStandardsControlAssociations，並提供特定的控制項 ID，以傳回每個標準中控制項目前的啟用狀態。

   請求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. 執行 BatchUpdateStandardsControlAssociations。提供您要停用控制項之標準的 ARN。
4. 將AssociationStatus參數設定為等於DISABLED。如果您依照下列步驟執行已停用的控制項，API 會傳回 HTTP 狀態碼 200 回應。

   請求示例：

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

若要停用特定標準中的控制項

1. 執行命list-security-control-definitions令，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行describe-standards。此命令會傳回與標準無關的安全性控制 ID，而不是標準特定的控制 ID。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. 執行命list-standards-control-associations令，並提供特定的控制項 ID，以傳回每個標準中控制項目前的啟用狀態。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 執行 batch-update-standards-control-associations 命令。提供您要停用控制項之標準的 ARN。
4. 將AssociationStatus參數設定為等於DISABLED。如果您遵循下列步驟來取得已啟用的控制項，命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
```

```
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Security Hub 控制項參考

此控制項參考提供可用控制 AWS Security Hub 項的清單，以及每個控制項詳細資訊的連結。概觀表格會依照控制項 ID 的字母順序顯示控制項。此表格提供每個控制項的下列資訊：

- 安全控制 ID — 此 ID 適用於跨標準， AWS 服務 並指示控制項相關的和資源。無論帳戶中的合併控制項發現項目是開啟還是關閉，Security Hub 主控台都會顯示安全控制 ID。不過，只有在帳戶中開啟合併控制項發現項目時，Security Hub 發現項目才會參考安全性控制 ID。如果帳戶中的合併控制項發現項已關閉，則某些控制 ID 會因控制項發現項目中的標準而有所不同。如需將標準特定控制 ID 與安全性控制 ID 的對應，請參閱。合併如何影響控制 ID 和標題

  如果您想要設定安全性控制項的自動化功能，建議您根據控制項 ID 進行篩選，而非標題或說明。雖然 Security Hub 有時可能會更新控制項標題或說明，但控制項識別碼會保持不變。

  控制 ID 可能會跳過數字。這些是 future 控件的佔位符。
- 適用標準 — 指示控制套用於哪些標準。選取控制項以查看協力廠商合規性架構的特定需求。
- 安全控制標題 — 此標題適用於各種標準。無論帳戶中的合併控制項發現項目是開啟還是關閉，Security Hub 主控台都會顯示安全控制項標題。不過，只有在帳戶中開啟合併控制項發現項目時，Security Hub 發現項目才會參考安全性控制標題。如果您的帳戶中已關閉合併的控制項發現項目，則某些控制項標題會因控制項發現項目中的標準而異。如需將標準特定控制 ID 與安全性控制 ID 的對應，請參閱。合併如何影響控制 ID 和標題
- 嚴重性 — 控制項的嚴重性從安全的角度來看，識別其重要性。如需有關 Security Hub 如何判斷控制項嚴重性的資訊，請參閱指派嚴重性給控制項發現。
- 排程類型 — 指出何時評估控制項。如需詳細資訊，請參閱 執行安全檢查的排程。
- 支援自訂參數 — 指出控制項是否支援一或多個參數的自訂值。選取控制項以查看參數詳細資訊。如需詳細資訊，請參閱 自訂控制參數。

選取控制項以檢視進一步的詳細資訊。控制項會依服務名稱的字母順序列出。

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Account.1	應提供安全聯繫信息 AWS 帳戶	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	定期
帳戶 .2	AWS 帳戶 應該是 AWS Organizations 組織的一部分	尼斯特 SP	HIGH (高)	否	定期
ACM.1	匯入和 ACM 核發的憑證應在指定的時間段後續約	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發和定期
ACM.2	ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度	AWS 基礎安全性最佳做法 v1.0.0	HIGH (高)	否	變更觸發
APIGateway.1	應啟用 API Gateway REST 和 WebSocket API 執行記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
APIGateway.2	API Gateway REST API 階段應設定為使用 SSL 憑證進行後端驗證	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
APIGateway.3	API Gateway REST API 階段應啟用 AWS X-Ray 追蹤	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
APIGateway.4	API Gateway 應該與 WAF 網頁 ACL 相關聯	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
APIGateway.5	API Gateway REST API 快取資料應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
APIGateway.8	API Gateway 路由應指定授權類型	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期
APIGateway.9	應針對 API Gateway V2 階段設定存取記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
AppSync.2	AWS AppSync 應啟用欄位層級記錄	AWS 基礎安全性最佳做法 v1.0.0	中等	是	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
AppSync.5	AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
雅典娜 .1	Athena 工作群組應在靜態時加密	AWS 基礎安全性最佳做法 v1.0.0，服務管理標準： AWS Control Tower	中等	否	變更觸發
AutoScaling.1	與 Classic Load Balancer 相關聯的自動調度資源調度群組應該使用負載平衡器	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	低	否	變更觸發
AutoScaling.2	Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
AutoScaling.3	Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務版本 2 (IMDSv2)	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
AutoScaling.4	Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Autoscaling.5	使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
AutoScaling.6	Auto Scaling 群組應在多個可用區域使用多個執行個體類型	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
AutoScaling.9	EC2 Auto Scaling 群組應使用 EC2 啟動範本	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Backup。1	AWS Backup 復原點應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFormation.1	CloudFormation 堆疊應與 Simple Notification Service (SNS) (SNS) 整合	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
CloudFront.1	CloudFront 發行版應該配置一個默認的根對象	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudFront.3	CloudFront 分發應在傳輸過程中需要加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFront.4	CloudFront 發行版應設定原始容錯移轉	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
CloudFront.5	CloudFront 分發應該啟用日誌記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFront.6	CloudFront 發行版應啟用 WAF	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFront.7	CloudFront 發行版應使用自訂 SSL/TLS 憑證	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFront.8	CloudFront 發行版應使用 SNI 來提供 HTTPS 請求	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
CloudFront.9	CloudFront 分發應加密到自定義來源的流量	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudFront.10	CloudFront 分發不應在邊緣位置和自定義來源之間使用已過時的 SSL 協議	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
CloudFront.12	CloudFront 發行版不應指向不存在的 S3 來源	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	定期
CloudFront.13	CloudFront 分佈應使用原始訪問控制	AWS 基礎安全性最佳做法 v1.0.0	中等	否	變更觸發
CloudTrail.1	CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤	獨聯體 AWS 基礎基準測試 v1.2.0，獨聯體 AWS 基礎基準測試 v1.4.0，基 AWS 礎安全最佳實踐 1.0.0 版，服務管理標準：，NIST SP 800-53 版本 5 AWS Control Tower	HIGH (高)	否	定期
CloudTrail.2	CloudTrail 應該啟用靜態加密	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	中等	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudTrail.3	CloudTrail 應該啟用	PCI DSS v3.2.1	HIGH (高)	否	定期
CloudTrail.4	CloudTrail 應啟用記錄檔驗證	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	低	否	定期
CloudTrail.5	CloudTrail 跟踪應與 Amazon CloudWatch 日誌集成	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	低	否	定期
CloudTrail.6	確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	關鍵	否	變更觸發和定期
CloudTrail.7	確保 S3 儲存貯體上已啟用 CloudTrail S3 儲存貯體存取日誌	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch.1	針對「root」使用者的使用，應該存在記錄指標篩選器和警示	獨聯體 AWS 基礎基準 V1.2.0，PCI DSS v3.2.1，獨聯體基準基準 v1.4.0 AWS	低	否	定期
CloudWatch.2	確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0	低	否	定期
CloudWatch.3	確保不使用 MFA 的管理主控台登入存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0	低	否	定期
CloudWatch.4	確保 IAM 政策變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.5	確保存在 CloudTrail 配置更改的日誌指標過濾器和警報	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.6	確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.7	確保停用或排定刪除客戶建立的 CMK 存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch.8	確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.9	確保存在 AWS Config 配置更改的日誌指標過濾器和警報	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.10	確保安全群組變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.11	確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.12	確保網路閘道變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.13	確保路由表變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
CloudWatch.14	確保 VPC 變更存在日誌指標篩選條件和警示	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch.15	CloudWatch 警示應該已設定指定的動作	尼斯特 SP	HIGH (高)	是	變更觸發
CloudWatch.16	CloudWatch 記錄群組應保留一段指定的時間	尼斯特 SP	中等	是	定期
CloudWatch.17	CloudWatch 應啟用警示動作	尼斯特 SP	HIGH (高)	否	變更觸發
CodeBuild.1	CodeBuild Bitbucket 來源儲存庫 URL 不應包含敏感憑證	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發
CodeBuild.2	CodeBuild 專案環境變數不應包含純文字認證	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發
CodeBuild.3	CodeBuild S3 日誌應加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CodeBuild.4	CodeBuild 項目環境應該有一個日誌記錄配置	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
CodeBuild.5	CodeBuild 專案環境不應啟用特權模式	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
Config.1	AWS Config 應該啟用	獨聯體 AWS 基礎基準測試版 1.2.0，基 AWS 礎安全最佳實踐版本 1.0.0，PCI DSS V3.2.1，獨聯體 AWS 基準基準 V1.4.0，NIST SP 800-53 版本 5	中等	否	定期
DMS.1	Database Migration Service 複製執行個體不應為公用	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	定期
公司 .6	DMS 複寫執行個體應啟用自動次要版本升級	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
公司 .7	目標資料庫的 DMS 複寫工作應該已啟用記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
公司 .8	來源資料庫的 DMS 複寫工作應該已啟用記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
公司 .9	DMS 端點應該使用 SSL	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
DocumentDB	Amazon DocumentDB 叢集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
DocumentDB	Amazon DocumentDB 叢集應該有足夠的備份保留期	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	是	變更觸發
DocumentDB 3	Amazon DocumentDB 手動叢集快照不應該是公開的	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	關鍵	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DocumentDB 4	Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
DocumentDB 5	Amazon DocumentDB 叢集應啟用刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
DynamoDB 1	DynamoDB 資料表應該會根據需求自動調整容量	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期
DynamoDB 2	表格應該已 point-in-time 啟用復原	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
DynamoDB 3	DynamoDB 加速器 (DAX) 叢集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
DynamoB.4	備份計劃中應該存在 DynamoDB 表	尼斯特 SP	中等	是	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DynamoB.6	DynamoDB 資料表應該已啟用刪除保護功能	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
EC2.1	EBS 快照不應可公開還原	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	定期
EC2.2	VPC 預設安全群組不應允許輸入或輸出流量	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	HIGH (高)	否	變更觸發
EC2.3	連接的 EBS 磁碟區應該以靜態方式加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EC2.4	停止的 EC2 執行個體應在指定時間段後移除	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.6	應在所有 VPC 中啟用 VPC 流程記錄	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	中等	否	定期
EC2.7	應啟用 EBS 預設加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，獨聯體 AWS 基礎基準測試版 1.4.0 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期
EC2.8	EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
EC2.9	EC2 執行個體不應該有公用 IPv4 位址	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.10	應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	定期
EC2.12	應移除未使用的 EC2 EIP	投資產能 DSS 3.2.1 版本，尼斯特 SP 800-53 版本 5	低	否	變更觸發
EC2.13	安全性群組不應允許從 0.0.0.0/0 或:: /0 輸入連接埠 22	獨聯體 AWS 基準基準 V1.2.0，PCI DSS V3.2.1，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
EC2.14	安全性群組不應允許從 0.0.0.0/0 或:: /0 輸入連接埠 3389	獨聯體 AWS 基金會基準 v1.2.0	HIGH (高)	否	變更觸發
EC2.15	EC2 子網路不應自動指派公用 IP 位址	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EC2.16	應移除未使用的網路存取控制清單	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.17	EC2 實例不應使用多個 ENI	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
EC2.18	安全群組只允許授權連接埠不受限制的傳入流量	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	是	變更觸發
EC2.19	安全群組不應允許不受限制地存取具有高風險的連接埠	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	關鍵	否	變更觸發
EC2.20	AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EC2.21	網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，獨聯體 AWS 基礎基準測試版 1.4.0 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.22	應移除未使用的 EC2 安全群組	服務管理標準： AWS Control Tower	中等	否	定期
EC2.23	EC2 傳輸閘道不應自動接受 VPC 附件請求	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
EC2.24	不應使用 EC2 半虛擬實例類型	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
EC2.25	EC2 啟動範本不應將公有 IP 指派給網路界面	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
EC2.28	EBS 磁碟區應該在備份計畫中	尼斯特 SP	低	是	定期
EC2.51	EC2 Client VPN 端點應啟用用戶端連線記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ECR.1	ECR 專用儲存庫應設定映像掃描	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	定期
ECR.2	ECR 私有存儲庫應配置標籤不變性	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ECR.3	ECR 儲存庫應至少設定一個生命週期原則	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ECS.1	Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.2	ECS 服務不應該有自動分配給他們的公共 IP 地址	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.3	ECS 任務定義不應共享主機的進程命名空間	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ECS.4	ECS 容器應以非特權的方式執行	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.5	ECS 容器應僅限於對 root 檔案系統的唯讀存取	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.8	秘密不應作為容器環境變量傳遞	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.9	ECS 任務定義應具有記錄組態	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
ECS.10	ECS Fargate 服務應在最新的 Fargate 平台版本上運行	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ECS.12	ECS 叢集應使用容器深入解析	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EFS.1	應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	定期
EFS.2	Amazon EFS 磁碟區應該在備份計劃中	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	定期
EFS.3	EFS 存取點應強制執行根目錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EFS.4	EFS 存取點應強制執行使用者身分	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EKS.1	EKS 叢集端點不應可公開存取	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	定期
EKS.2	EKS 叢集應該在支援的 Kubernetes 版本上執行	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EK.8	EKS 叢集應啟用稽核記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
ElastiCache.1	ElastiCache Redis 叢集應啟用自動備份	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	是	定期
ElastiCache.2	ElastiCache 對於 Redis 緩存集群應啟用 auto 次要版本升級	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	定期
ElastiCache.3	ElastiCache 複寫群組應啟用自動容錯移轉	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
ElastiCache.4	ElastiCache 複製群組應該已 encryption-at-rest 啟用	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
ElastiCache.5	ElastiCache 複製群組應該已 encryption-in-transit 啟用	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
ElastiCache.6	ElastiCache 舊版 Redis 的複寫群組應啟用 Redis AUTH	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ElastiCache.7	ElastiCache 叢集不應使用預設子網路群組	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	定期
ElasticBeanstalk.1	Elastic Beanstalk 環境應啟用增強健康報告	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
ElasticBeanstalk.2	應啟用 Elastic Beanstalk 管理平台更新	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	是	變更觸發
ElasticBeanstalk.3	Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch	AWS 基礎安全性最佳做法 v1.0.0	HIGH (高)	是	變更觸發
ELB.1	應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期
ELB.2	具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ELB.3	Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止來設定	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.4	Application Load Balancer 應設定為刪除 http 標頭	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.5	應啟用應用程式和傳統負載平衡器記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.6	應啟用應用 Application Load Balancer 刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.7	傳統負載平衡器應啟用連線排空	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.8	具有 SSL 接聽程式的傳統負載平衡器應使用具有強式組態的預先定義安全性原則	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ELB.9	傳統負載平衡器應啟用跨區域負載平衡	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.10	Classic Load Balancer 應跨越多個可用區域	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
ELB.12	應 Application Load Balancer 應設定為防禦性或最嚴格的不同步緩和模式	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ELB.13	應用程式、網路和閘道負載平衡器應跨越多個可用區域	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
ELB.14	Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩和模式	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
易北省 16	應用程式負載平衡器應與 AWS WAF Web ACL 相關聯	尼斯特 SP	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EMR.1	Amazon EMR 叢集主節點不應具有公有 IP 地址	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	定期
EMR.2	應啟用 Amazon EMR 塊公共存取設置	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	關鍵	否	定期
ES.1	彈性搜尋網域應啟用靜態加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期
ES.2	彈性搜尋網域不應可公開存取	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	定期
ES.3	彈性搜尋網域應加密節點之間傳送的資料	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ES.4	應該啟用記錄 CloudWatch 檔的網域錯誤記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ES.5	應啟用稽核記錄功能	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ES.6	彈性搜索域至少應具有三個數據節點	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ES.7	彈性搜尋網域應設定至少三個專用主節點	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
ES.8	應使用最新的 TLS 安全性原則加密至彈性搜尋網域的連線	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
EventBridge.3	EventBridge 自訂事件匯流排應附有以資源為基礎的原則	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EventBridge.4	EventBridge 全域端點應啟用事件複寫	尼斯特 SP	中等	否	變更觸發
FSX.1	OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
GuardDuty.1	GuardDuty 應該啟用	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	HIGH (高)	否	定期
IAM.1	IAM 政策不應允許完整的「*」管理權限	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.2	IAM 使用者不應附加 IAM 政策	獨聯體 AWS 基礎基準測試版 1.2.0，基 AWS 礎安全性最佳實務版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，NIST SP 800-53 版本 5	低	否	變更觸發
IAM.3	IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全最佳實踐 1.0.0 版，服務管理標準：獨聯體 AWS 基礎基準測試版 1.4.0 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期
IAM.4	IAM 根使用者存取金鑰不應存在	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	關鍵	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.5	所有擁有主控台密碼的 IAM 使用者都應啟用 MFA	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全最佳實踐 1.0.0 版，服務管理標準：獨聯體 AWS 基礎基準測試版 1.4.0 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期
IAM.6	應為根使用者啟用硬體 MFA	獨聯體 AWS 基礎基準測試 v1.2.0，基 AWS 礎安全性最佳實踐版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，獨聯體基準基準 V1.4.0，NIST SP 800-53 版本 5 AWS	關鍵	否	定期
IAM.7	IAM 使用者的密碼政策應具有強式組態	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期
IAM .8	應移除未使用的 IAM 使用者登入資料	獨聯體 AWS 基礎基準測試版 1.2.0，基 AWS 礎安全性最佳實務版本 1.0.0 版，服務管理標準：，PCI DSS v3.2.1 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.9	應為根使用者啟用 MFA	獨聯體 AWS 基礎基準測試版 1.2.0，PCI DSS v3.2.1，獨聯體 AWS 基準基準 V1.4.0，NIST SP 800-53 版本 5	關鍵	否	定期
亞姆 .10	IAM 使用者的密碼政策應具有強式組態	PCI DSS v3.2.1	中等	否	定期
IAM.11	確保 IAM 密碼政策至少需要一個大寫字母	獨聯體 AWS 基金會基準 v1.2.0	中等	否	定期
IAM.12	確保 IAM 密碼政策至少需要一個小寫字母	獨聯體 AWS 基金會基準 v1.2.0	中等	否	定期
IAM.13	確保 IAM 密碼政策至少需要一個符號	獨聯體 AWS 基金會基準 v1.2.0	中等	否	定期
IAM.14	確保 IAM 密碼政策至少需要一個數字	獨聯體 AWS 基金會基準 v1.2.0	中等	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.15	確保 IAM 密碼政策的密碼長度下限為 14 或更高	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	中等	否	定期
IAM.16	確保 IAM 密碼政策防止重複使用密碼	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
IAM.17	確保 IAM 密碼政策在 90 天或更短的時間內過期	獨聯體 AWS 基金會基準 v1.2.0	低	否	定期
IAM.18	確保已建立支援角色來管理事件 AWS Support	獨聯體 AWS 基金會基準 v1.2.0，獨聯體 AWS 基準基準 v1.4.0	低	否	定期
亞姆 .19	應為所有 IAM 使用者啟用 MFA	投資產能 DSS 3.2.1 版本，尼斯特 SP 800-53 版本 5	中等	否	定期
亞姆 .20	避免使用 root 用戶	獨聯體 AWS 基金會基準 v1.2.0	低	否	定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.21	您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
家居安 .22	應移除 45 天未使用的 IAM 使用者登入資料	獨聯體 AWS 基金會基準 v1.4.0	中等	否	定期
Kinesis.1	Kinesis 串流應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
KMS.1	IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
KMS.2	IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
KMS.3	AWS KMS keys 不應被無意中刪除	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	關鍵	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
KMS.4	AWS KMS key 應啟用旋轉	獨聯體 AWS 基礎基準測試版 1.2.0，PCI DSS v3.2.1，獨聯體 AWS 基準基準 V1.4.0，NIST SP 800-53 版本 5	中等	否	定期
Lambda.1	Lambda 函數政策應禁止公開存取	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發
Lambda.2	Lambda 函數應使用支援的執行階段	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Lambda.3	Lambda 函數應該位於 VPC 中	投資產能 DSS 3.2.1 版本，尼斯特 SP 800-53 版本 5	低	否	變更觸發
Lambda.5	VPC Lambda 函數應在多個可用區域中運作	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
馬賽 .1	Amazon Macie 應該啟用	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
馬賽 .2	應啟用 Macie 自動化敏感資料探索	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	HIGH (高)	否	定期
MSK.1	MSK 叢集應在代理程式節點之間的傳輸過程中加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
MSK.2	MSK 叢集應設定增強型監控功能	尼斯特 SP	低	否	變更觸發
每米 5 米	ActiveMQ 代理程式應該使用主動/待命部署模式	尼斯特 SP	低	否	變更觸發
每克里數	RabbitMQ 代理程式應該使用叢集部署模式	尼斯特 SP	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
海王星 1 號	Neptune 資料庫叢集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
海王星 .2	Neptune 資料庫叢集應將稽核記錄發佈至 CloudWatch 記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
海王星 .3	Neptune 資料庫叢集快照不應該是公用的	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	關鍵	否	變更觸發
海王星 .4	Neptune 資料庫叢集應啟用刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	低	否	變更觸發
海王星 .5	Neptune 資料庫叢集應啟用自動備份	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	是	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
海王星 .6	Neptune 資料庫叢集快照應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
海王星 .7	Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
海王星 .8	Neptune 資料庫叢集應設定為將標籤複製到快照	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	低	否	變更觸發
海王星 .9	Neptune 資料庫叢集應部署在多個可用區域	尼斯特 SP	中等	否	變更觸發
NetworkFirewall.1	Network Firewall 防火牆應跨多個可用區域部署	尼斯特 SP	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
NetworkFirewall.2	應啟用 Network Firewall 記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
NetworkFirewall.3	Network Firewall 策略應至少有一個關聯的規則群組	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
NetworkFirewall.4	對於完整封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
NetworkFirewall.5	Network Firewall 策略的預設無狀態處理行動對於片段式封包應該是捨棄或轉送	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
NetworkFirewall.6	無狀態網路防火牆規則群組不應為空	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
NetworkFirewall.9	Network Firewall 防火牆應啟用刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Opensearch.1	OpenSearch 網域應啟用靜態加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	變更觸發
Opensearch.2	OpenSearch 網域不應可公開存取	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發
Opensearch.3	OpenSearch 網域應加密節點之間傳送的資料	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Opensearch.4	OpenSearch 應啟用記 CloudWatch 錄的網域錯誤記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Opensearch.5	OpenSearch 網域應啟用稽核記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Opensearch.6	OpenSearch 網域至少應該有三個資料節點	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Opensearch.7	OpenSearch 網域應啟用精細的存取控制	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
Opensearch.8	與 OpenSearch 網域的連線應使用最新的 TLS 安全性原則加密	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
打開搜索 .10	OpenSearch 網域應該已安裝最新的軟體更新	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
PCA.1	AWS Private CA 應停用根憑證授權單位	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	定期
RDS.1	RDS 快照應該是私有的	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.2	RDS 資料庫執行個體應該根據 PubliclyAccessible 組態決定禁止公用存取	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發
RDS.3	RDS 資料庫執行個體應啟用靜態加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準：，獨聯體 AWS 基礎基準測試版 1.4.0 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.4	RDS 叢集快照集和資料庫快照集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.5	RDS 資料庫執行個體應設定多個可用區域	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.6	應為 RDS 資料庫執行個體設定增強型監控	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	是	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.7	RDS 叢集應啟用刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
RDS.8	RDS 資料庫執行個體應啟用刪除保護	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.9	RDS 資料庫執行個體應將記錄發佈至 CloudWatch 記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.10	應為 RDS 執行個體設定 IAM 身份驗證	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.11	RDS 執行個體應啟用自動備份	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
RDS.12	應為 RDS 叢集設定 IAM 身分驗證	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.13	應啟用 RDS 自動次要版本升級	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
RDS.14	Amazon Aurora 叢集應啟用回溯	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	是	變更觸發
RDS.15	應針對多個可用區域設定 RDS 資料庫叢集	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.16	RDS 資料庫叢集應設定為將標籤複製到快照	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	低	否	變更觸發
RDS.17	RDS 資料庫執行個體應設定為將標籤複製到快照	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.18	RDS 執行個體應部署在 VPC 中	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.19	應針對重要叢集事件設定現有 RDS 事件通知訂閱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.20	應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.21	應針對重要資料庫參數群組事件設定 RDS 事件通知訂閱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.22	應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.23	RDS 執行個體不應使用資料庫引擎預設連接埠	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	否	變更觸發
RDS.24	RDS 資料庫叢集應使用自訂管理員使用者名稱	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.25	RDS 資料庫執行個體應使用自訂管理員使用者	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.26	RDS 資料庫執行個體應該受到備份計劃的保護	尼斯特 SP	中等	是	定期
RDS.27	RDS 資料庫叢集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5，服務管理標準： AWS Control Tower	中等	否	變更觸發
RDS.34	Aurora MySQL 資料庫叢集應將稽核記錄發佈至 CloudWatch 記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
RDS.35	RDS 資料庫叢集應啟用自動次要版本升級	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.1	Amazon Redshift 集群應禁止公共訪問	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	關鍵	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Redshift.2	與 Amazon Redshift 叢集的連線應在傳輸過程中加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.3	Amazon Redshift 叢集應該已啟用自動快照	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	是	變更觸發
Redshift.4	Amazon Redshift 叢集應啟用稽核記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.6	Amazon Redshift 應該已啟用自動升級到主要版本	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.7	Redshift 叢集應使用增強型 VPC 路由	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.8	Amazon Redshift 叢集不應使用預設的管理員使用者名稱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Redshift.9	Redshift 叢集不應使用預設的資料庫名稱	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
Redshift.10	Redshift 叢集應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
香港路線	路由 53 公共託管區域應記錄 DNS 查詢	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
S3.1	S3 一般用途儲存貯體應啟用區塊公用存取設定	AWS 基礎安全性最佳做法、服務管理標準：、PCI DSS v3.2.1 AWS Control Tower、獨聯體 AWS 基準基準測試版本 1.4.0、NIST SP 800-53 版本 5	中等	否	定期
S3.2	S3 一般用途儲存貯體應封鎖公用讀取存取	AWS 基礎安全性最佳做法、服務管理標準： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 版本 5	關鍵	否	變更觸發和定期

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.3	S3 一般用途儲存貯體應封鎖公用寫入存取	AWS 基礎安全性最佳做法、服務管理標準： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 版本 5	關鍵	否	變更觸發和定期
S3.5	S3 一般用途儲存貯體應需要使用 SSL 的請求	AWS 基礎安全性最佳做法、服務管理標準：、PCI DSS v3.2.1 AWS Control Tower、獨聯體 AWS 基準基準測試版本 1.4.0、NIST SP 800-53 版本 5	中等	否	變更觸發
S3.6	S3 一般用途儲存貯體政策應限制存取其他 AWS 帳戶	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
S3.7	S3 一般用途儲存貯體應使用跨區域複寫	投資產能 DSS 3.2.1 版本，尼斯特 SP 800-53 版本 5	低	否	變更觸發
S3.8	S3 一般用途儲存貯體應封鎖公用存取	AWS 基礎安全性最佳做法、服務管理標準：、獨聯體 AWS 基礎基準測試 v1.4.0 AWS Control Tower、NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.9	S3 一般用途儲存貯體應啟用伺服器存取記錄	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
S3.10	啟用版本控制的 S3 一般用途貯體應具有生命週期組態	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
S3.11	S3 一般用途儲存貯體應啟用事件通知	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
S3.12	ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
S3.13	S3 一般用途儲存貯體應有生命週期組態	AWS 基礎安全性最佳做法，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	低	是	變更觸發
S3.14	S3 一般用途儲存貯體應啟用版本控制	尼斯特 SP	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.15	S3 一般用途儲存貯體應啟用物件鎖定	尼斯特 SP	中等	是	變更觸發
S3.17	S3 一般用途儲存貯體應以靜態方式加密 AWS KMS keys	服務管理標準： AWS Control Tower，NIST SP 800-53 版本 5	中等	否	變更觸發
S3.19	S3 存取點應啟用封鎖公用存取設定	AWS 基礎安全性最佳做法，NIST SP 800-53 版本 5	關鍵	否	變更觸發
S3.20	S3 一般用途儲存貯體應啟用 MFA 刪除	獨聯體 AWS 基礎基準 V1.4.0，尼斯特 SP 800-53 版 5	低	否	變更觸發
SageMaker.1	Amazon SageMaker 筆記本實例不應該直接訪問互聯網	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	HIGH (高)	否	定期
SageMaker.2	SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SageMaker.3	使用者不應擁有 SageMaker 筆記本執行個體的 root 存取權	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
SecretsManager.1	Secrets Manager 密碼應該啟用自動輪換	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	變更觸發
SecretsManager.2	配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
SecretsManager.3	移除未使用的 Secrets Manager	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期
SecretsManager.4	Secrets Manager 密碼應在指定的天數內輪替	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	是	定期
SNS.1	SNS 主題應使用靜態加密 AWS KMS	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SNS.2	傳送至主題的通知訊息應啟用傳送狀態的記錄	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
SQS.1	Amazon SQS 佇列應在靜態時加密	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
SSM.1	EC2 執行個體應由下列項目管理 AWS Systems Manager	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	中等	否	變更觸發
SSM.2	安裝修補程式後，由系統管理員管理的 EC2 執行個體應具有合規修補程式合規狀態	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	HIGH (高)	否	變更觸發
SSM.3	由系統管理員管理的 EC2 執行個體應具有合規性的關聯合規性狀態	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： ，PCI DSS 3.2.1 版 AWS Control Tower，NIST SP 800-53 版本 5	低	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SSM.4	SSM 文件不應該是公開的	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	關鍵	否	定期
StepFunctions.1	Step Functions 狀態機器應該已開啟日誌記錄	AWS 基礎安全性最佳做法	中等	是	變更觸發
WAF.1	AWS WAF 應啟用傳統全域 Web ACL 記錄	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	定期
WAF.2	AWS WAF 傳統區域規則應具有至少一個條件	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.3	AWS WAF 傳統區域規則群組至少應該有一個規則	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.4	AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發

安全控制識別碼	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
WAF.6	AWS WAF 傳統全域規則應至少有一個條件	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.7	AWS WAF 傳統全域規則群組至少應該有一個規則	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.8	AWS WAF 傳統全域 Web ACL 至少應該有一個規則或規則群組	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.10	AWS WAF Web ACL 至少應該有一個規則或規則群組	AWS 基礎安全性最佳做法第 1.0.0 版，服務管理標準： AWS Control Tower, NIST SP 800-53 版本 5	中等	否	變更觸發
WAF.11	AWS WAF 應啟用網頁 ACL 記錄功能	尼斯特 SP	低	否	定期
WAF.12	AWS WAF 規則應啟用 CloudWatch 量度	AWS 基礎安全性最佳做法第 1.0.0 版，NIST SP 800-53 版本 5	中等	否	變更觸發

主題

- AWS 帳戶 控制

- AWS Certificate Manager 控制
- Amazon API Gateway 控制
- AWS AppSync 控制
- Amazon Athena 控制
- AWS Backup 控制
- AWS CloudFormation 控制
- Amazon CloudFront 控制
- AWS CloudTrail 控制
- Amazon CloudWatch 控制
- AWS CodeBuild 控制
- AWS Config 控制
- AWS Database Migration Service 控制
- Amazon DocumentDB 控件
- Amazon DynamoDB 控制
- Amazon 彈性容器登錄控制
- Amazon ECS 控制
- Amazon 彈性運算雲控制
- Amazon EC2 Auto Scaling 控制
- Amazon EC2 Systems Manager 控制
- Amazon Elastic File System 控制
- Amazon Elastic Kubernetes Service 控制
- Amazon ElastiCache 控制
- AWS Elastic Beanstalk 控制
- Elastic Load Balancing 控制
- Amazon EMR 控制
- 彈性搜索控件
- Amazon EventBridge 控制
- Amazon FSx 控制
- Amazon GuardDuty 控制

- AWS Identity and Access Management 控制
- Amazon Kinesis 控制
- AWS Key Management Service 控制
- AWS Lambda 控制
- Amazon Macie 控制
- Amazon MSK 控制
- Amazon MQ 控制
- Amazon Neptune 控
- AWS Network Firewall 控制
- Amazon OpenSearch 服務控制
- AWS Private Certificate Authority 控制
- Amazon Relational Database Service 控制
- Amazon Redshift 控制
- Amazon 路線 53 控制
- Amazon 簡單存儲服務控制
- Amazon SageMaker 控制
- AWS Secrets Manager 控制
- Amazon 簡單通知服務控制
- Amazon 簡單隊列服務控制
- AWS Step Functions 控制
- AWS WAF 控制

AWS 帳戶 控制

這些控制項與 AWS 帳戶。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[帳戶。1] 應提供安全聯繫信息 AWS 帳戶

相關需求：第五代公分 (2)

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`security-account-information-provided`

排程類型：定期

參數：無

此控制項會檢查 Amazon Web Services (AWS) 帳戶是否有安全聯絡資訊。如果未提供帳戶的安全連絡人資訊，則控制項會失敗。

備用的安全性聯絡人可 AWS 以在您無法使用的情況下，就帳戶的問題與其他人聯絡。通知可以是來自 AWS Support或其他 AWS 服務 團隊有關與您的使用關聯的安全性相關主題的 AWS 帳戶 通知。

修補

若要將替代聯絡人新增為您的安全聯絡人 AWS 帳戶，請參閱 B AWS illing and Cost Management 使用者指南中的新增、變更或移除其他聯絡人。

[帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations

分類:保護 > 安全存取管理 > 存取控制

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

嚴重性：高

資源類型：`AWS::::Account`

AWS Config 規則：`account-part-of-organizations`

排程類型：定期

參數：無

此控制項會檢查 AWS 帳戶 是否為透過管理的組織的一部分 AWS Organizations。如果帳戶不是組織的一部分，則控制項會失敗。

Organizations 可協助您集中管理您的環境，同時擴展工作負載 AWS。您可以使用多個 AWS 帳戶 來隔離具有特定安全性需求的工作負載，或符合 HIPAA 或 PCI 等架構的工作負載。透過建立組織，您可以將多個帳戶當作單一單位來管理 AWS 服務，並集中管理其對資源和區域的存取權限。

修補

若要建立新組織並自動加入 AWS 帳戶 組織，請參閱《AWS Organizations 使用指南》中的〈建立組織〉。若要將帳戶新增至現有組織，請參閱AWS Organizations 使用者指南中的邀請加入您的組織。
AWS 帳戶

AWS Certificate Manager 控制

這些控制項與 ACM 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約

相關要求：七月五日 SC-28 (3)、日本電子郵件

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::ACM::Certificate`

AWS Config 規則：`acm-certificate-expiration-check`

排程型態：變更已觸發與週期性

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`daysToExpiration`	ACM 憑證必須續約的天數	Integer	`14` 設定為 `365`	`30`

此控制項會檢查 AWS Certificate Manager (ACM) 憑證是否在指定期間內更新。它會檢查匯入的憑證和 ACM 提供的憑證。如果憑證未在指定的時間段內更新，則控制項會失敗。除非您在續約期間提供自訂參數值，否則 Security Hub 會使用預設值 30 天。

ACM 可以自動更新使用 DNS 驗證的憑證。對於使用電子郵件驗證的憑證，您必須回應網域驗證電子郵件。ACM 不會自動更新您匯入的憑證。您必須手動更新匯入的憑證。

修補

ACM 為 Amazon 發行的 SSL/TLS 憑證提供受管續約。這表示 ACM 會自動更新您的憑證 (如果您使用 DNS 驗證)，或是在憑證到期即將到期時傳送電子郵件通知給您。這些服務可供公有和私有 ACM 憑證使用。

透過電子郵件驗證的網域

如果憑證是到期後 45 天，ACM 會針對每個網域名稱傳送電子郵件給網域擁有者。若要驗證網域並完成續約，您必須回應電子郵件通知。

如需詳細資訊，請參閱AWS Certificate Manager 使用者指南中的透過電子郵件驗證的網域續約。

適用於經 DNS 驗證的網域

ACM 會自動更新使用 DNS 驗證的憑證。ACM 會在到期前 60 天驗證憑證是否可以更新。

如果無法驗證網域名稱，ACM 會傳送需要手動驗證的通知。它會在到期前 45 天、30 天、7 天和 1 天傳送這些通知。

如需詳細資訊，請參閱「AWS Certificate Manager 使用者指南」中的「透過 DNS 驗證的網域續約」。

[ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度

分類:識別 > 庫存 > 庫存服務

嚴重性：高

資源類型：`AWS::ACM::Certificate`

AWS Config 規則：`acm-certificate-rsa-check`

排程類型：已觸發變更

參數：無

此控制項會檢查所管理的 RSA 憑證是否 AWS Certificate Manager 使用至少 2,048 位元的金鑰長度。如果金鑰長度小於 2,048 位元，則控制項會失敗。

加密的強度與金鑰大小直接相關。我們建議使用金鑰長度至少 2,048 位元，以保護您的 AWS 資源，因為運算能力變得更低，伺服器也變得更先進。

修補

ACM 所發行之 RSA 憑證的金鑰長度下限已經是 2,048 位元。如需使用 ACM 發行新 RSA 憑證的指示，請參閱AWS Certificate Manager 使用者指南中的發行和管理憑證。

雖然 ACM 允許您匯入金鑰長度較短的憑證，但您必須使用至少 2,048 位元的金鑰來傳遞此控制項。匯入憑證後，您無法變更金鑰長度。相反地，您必須刪除金鑰長度小於 2,048 位元的憑證。如需有關將憑證匯入 ACM 的詳細資訊，請參閱《AWS Certificate Manager 使用指南》中的匯入憑證的先決條件。

Amazon API Gateway 控制

這些控制項與 API Gateway 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六 (9), 日本第七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型:`AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config 規則：`api-gw-execution-logging-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`loggingLevel`	Logging level (記錄層級)	列舉	`ERROR`, `INFO`	`No default value`

此控制項會檢查 Amazon API 閘道 REST 或 WebSocket API 的所有階段是否已啟用記錄功能。如果`loggingLevel`不是`ERROR`或`INFO`適用於 API 的所有階段，則控制項會失敗。除非您提供自訂參數值來指出應該啟用特定的記錄檔類型，否則 Security Hub 會在記錄層級為`ERROR`或時產生傳遞的發現項目`INFO`。

API Gateway REST 或 WebSocket API 階段應啟用相關記錄。API Gateway REST 和 WebSocket API 執行記錄可提供對 API Gateway REST 和 WebSocket API 階段所做請求的詳細記錄。這些階段包括 API 整合後端回應、Lambda 授權者回應，以及`requestId`用於 AWS 整合端點的。

修補

若要啟用 REST 和 WebSocket API 作業的記錄功能，請參閱 CloudWatch API Gateway 開發人員指南中的使用 API Gateway 主控台設定 API 記錄。

應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證

相關要求：第 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

類別:保護 > 資料保護

嚴重性：中

資源類型：`AWS::ApiGateway::Stage`

AWS Config 規則：`api-gw-ssl-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon API Gateway REST API 階段是否已設定 SSL 憑證。後端系統會使用這些憑證來驗證傳入的要求來自 API Gateway。

API Gateway REST API 階段應使用 SSL 憑證設定，以允許後端系統驗證來自 API Gateway 的要求。

修補

如需有關如何產生和設定 API Gateway REST API SSL 憑證的詳細指示，請參閱 API Gateway 開發人員指南中的產生和設定用於後端驗證的 SSL 憑證。

API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray

相關要求：冰箱 -53. R5 CA-7

類別：偵測 > 偵測服務

嚴重性：低

資源類型：`AWS::ApiGateway::Stage`

AWS Config 規則：`api-gw-xray-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查您的 Amazon API 閘道 REST API 階段是否已啟用 AWS X-Ray 主動追蹤。

X-Ray 主動追蹤可讓您更快速地回應基礎架構中的效能變更。效能的變更可能會導致 API 的可用性不足。X-Ray 主動追蹤可提供透過 API Gateway REST API 作業和連線服務的使用者請求的即時指標。

修補

如需如何針對 API Gateway REST API 作業啟用 X-Ray 主動追蹤的詳細指示，請參閱AWS X-Ray 開發人員指南 AWS X-Ray中的 Amazon API Gateway 主動追蹤支援。

[原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯

相關要求：交流 -4 (21)

分類:保護 > 保護服務

嚴重性：中

資源類型：`AWS::ApiGateway::Stage`

AWS Config 規則：`api-gw-associated-with-waf`

排程類型：已觸發變更

參數：無

此控制項會檢查 API Gateway 階段是否使用 AWS WAF Web 存取控制清單 (ACL)。如果 AWS WAF Web ACL 未附加到 REST API Gateway 階段，則此控制項會失敗。

AWS WAF 是一種網絡應用程序防火牆，可幫助保護 Web 應用程序和 API 免受攻擊。它可讓您設定 ACL，這是一組規則，可根據您定義的可自訂 Web 安全規則和條件，允許、封鎖或計數 Web 要求。確保您的 API Gateway 階段與 AWS WAF Web ACL 相關聯，以協助保護其免受惡意攻擊。

修補

如需如何使用 API Gateway 主控台將 AWS WAF 地區 Web ACL 與現有 API Gateway API 階段建立關聯的詳細資訊，請參閱 API Gateway 開發人員指南中的使用 AWS WAF 來保護您的 API。

[介面 5] API Gateway REST API 快取資料應在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::ApiGateway::Stage`

AWS Config 規則:`api-gw-cache-encrypted`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 API Gateway REST API 階段中啟用快取的所有方法是否已加密。如果 API Gateway REST API 階段中的任何方法設定為快取，且快取未加密，則控制項會失敗。Security Hub 只會在啟用該方法的快取時，才會評估特定方法的加密。

靜態資料加密可降低未經驗證的使用者存取儲存在磁碟上的資料的風險。 AWS它增加了另一組訪問控制，以限制未經授權的用戶訪問數據的能力。例如，在讀取資料之前，需要 API 權限才能解密資料。

API Gateway REST API 快取應在靜態時加密，以增加一層安全性。

修補

若要設定階段的 API 快取，請參閱 API Gateway 開發人員指南中的啟用 Amazon API 閘道快取。在快取設定中，選擇加密快取資料。

API Gateway 路由應該指定授權類型

相關需求：電腦 -53.R5 交流電 -3、尼斯五公分 (2)

類別:保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::ApiGatewayV2::Route`

AWS Config 規則：`api-gwv2-authorization-type-configured`

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`authorizationType`	API 路由的授權類型	列舉	`AWS_IAM`, `CUSTOM`, `JWT`	無預設值

此控制項會檢查 Amazon API Gateway 路由是否具有授權類型。如果 API Gateway 路由沒有任何授權類型，則控制項會失敗。或者，如果您希望控制項僅在路由使用參數中指定的授權類型時傳遞，則可以提供自訂`authorizationType`參數值。

API Gateway 支援多種機制來控制和管理 API 的存取。透過指定授權類型，您可以將 API 的存取限制為僅授權使用者或程序。

修補

若要設定 HTTP API 的授權類型，請參閱 API Gateway 開發人員指南中的 API Gateway 中的控制和管理 HTTP API 的存取。若要設定 API 的授權類型，請參閱 WebSocket API Gateway 開發人員指南中的「控制和管理 API Gateway 存取」。 WebSocket

應該為 API Gateway V2 階段配置訪問日誌記錄

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六 (9), 日本第七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::ApiGatewayV2::Stage`

AWS Config 規則：`api-gwv2-access-logs-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon API Gateway V2 階段是否已設定存取記錄。如果未定義存取記錄設定，則此控制項會失敗。

API Gateway 存取記錄提供有關誰存取您的 API 以及呼叫者如何存取 API 的詳細資訊。這些日誌適用於安全與存取稽核及鑑識調查等應用程式。啟用這些存取記錄檔以分析流量模式並對問題進行疑難排解。

如需其他最佳做法，請參閱 API Gateway 開發人員指南中的監控 REST API。

修補

若要設定存取記錄，請參閱 CloudWatch API Gateway 開發人員指南中的使用 API Gateway 主控台設定 API 記錄。

AWS AppSync 控制

這些控制項與資 AWS AppSync 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[AppSync.2] AWS AppSync 應啟用欄位層級記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::AppSync::GraphQLApi`

AWS Config 規則：`appsync-logging-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`fieldLoggingLevel`	欄位記錄層級	列舉	`ERROR`, `ALL`	`No default value`	

此控制項會檢查 AWS AppSync API 是否已開啟欄位層級記錄功能。如果欄位解析程式記錄層級設定為「無」，則控制項會失敗。除非您提供自訂參數值來指出應啟用特定的記錄檔類型，否則如果欄位解析程式記錄層級為或`ERROR`，Security Hub 會產生傳遞的發現項目。`ALL`

您可以使用記錄和指標來識別、故障診斷和最佳化您的 GraphQL 查詢。啟用 AWS AppSync GraphQL 的記錄功能可協助您取得 API 要求和回應的詳細資訊、識別和回應問題，以及遵守法規要求。

修補

若要開啟記錄功能 AWS AppSync，請參閱AWS AppSync 開發人員指南中的設定和組態。

[AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證

相關要求：交流 -2 (1)、交流 3 (1)、尼斯特。800-53.R5 交流 -3、交流 -3 (15)、日本交流 -3 (7)、日本交流 -6

分類:安全防護 > 安全存取管理 > 無密碼認證

嚴重性：高

資源類型：`AWS::AppSync::GraphQLApi`

AWS Config 規則：`appsync-authorization-check`

排程類型：已觸發變更

參數：

- `AllowedAuthorizationTypes`： `AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS`（不可定制）

此控制項會檢查您的應用程式是否使用 API 金鑰與 AWS AppSync GraphQL API 互動。如果使用 API 金鑰驗證 AWS AppSync GraphQL API，則控制項會失敗。

API 金鑰是應用程式中的硬式編碼值，由 AWS AppSync 服務在您建立未經驗證的 GraphQL 端點時產生。如果此 API 金鑰遭到入侵，您的端點容易遭到意外存取。除非您支持可公開訪問的應用程序或網站，否則我們不建議使用 API 密鑰進行身份驗證。

修補

若要為 AWS AppSync GraphQL API 設定授權選項，請參閱AWS AppSync 開發人員指南中的授權和驗證。

Amazon Athena 控制

這些控制項與 Athena 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Athena.1] Athena 工作群組應在靜態時加密

類別：保護 – 資料保護 – 靜態資料加密

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

嚴重性：中

資源類型：`AWS::Athena::WorkGroup`

AWS Config 規則：`athena-workgroup-encrypted-at-rest`

排程類型：已觸發變更

參數：無

此控制項會檢查 Athena 工作群組是否已靜態加密。如果 Athena 工作群組在靜態時未加密，則控制項會失敗。

在 Athena 中，您可以建立工作群組，以針對團隊、應用程式或不同的工作負載執行查詢。每個工作群組都具有對所有查詢啟用加密的設定。您可以選擇使用伺服器端加密搭配 Amazon 簡單儲存服務 (Amazon S3) 受管金鑰、使用 AWS Key Management Service (AWS KMS) 金鑰進行伺服器端加密，

或使用客戶受管 KMS 金鑰進行用戶端加密。靜態數據是指任何持續時間存儲在持久性非易失性存儲中的任何數據。加密可協助您保護此類資料的機密性，降低未經授權的使用者存取資料的風險。

修補

若要為 Athena 工作群組啟用靜態加密，請參閱 Amazon Athena 使用者指南中的編輯工作群組。在 [查詢結果組態] 區段中，選取 [加密查詢結果]。

AWS Backup 控制

這些控制項與資 AWS Backup 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Backup 1] AWS Backup 復原點應該在靜態時加密

相關要求：第五台 CP-9 (8)、日本電子郵件 SI-12

分類:保護 > 資料保護 > 加密 data-at-rest

嚴重性：中

資源類型：`AWS::Backup::RecoveryPoint`

AWS Config 規則：`backup-recovery-point-encrypted`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Backup 復原點是否在靜態時加密。如果復原點未在靜態時加密，則控制項會失敗。

AWS Backup 復原點是指在備份程序中建立的特定副本或資料快照。它代表了備份數據的特定時刻，並在原始數據丟失，損壞或無法訪問的情況下作為還原點。加密備份復原點可增加額外的保護層，防止未經授權的存取。加密是保護備份資料機密性、完整性和安全性的最佳作法。

修補

若要加密 AWS Backup 復原點，請參閱AWS Backup 開發人員指南 AWS Backup中的備份加密。

AWS CloudFormation 控制

這些控制項與資 CloudFormation 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：七月五四四 (12)、日本電腦五四 (5)

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::CloudFormation::Stack`

AWS Config 規則：`cloudformation-stack-notification-check`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon 簡易通知服務通知是否與 AWS CloudFormation 堆疊整合。如果 CloudFormation 堆疊沒有任何 SNS 通知與堆疊相關聯，則控制項會失敗。

使用 CloudFormation 堆疊設定 SNS 通知，有助於立即通知利益相關者堆疊發生的任何事件或變更。

修補

若要整合 CloudFormation 堆疊和 SNS 主題，請參閱AWS CloudFormation 使用者指南中的直接更新堆疊。

Amazon CloudFront 控制

這些控制項與資 CloudFront 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

相關要求：日本七七 (11)、日本七星期五 (16)

分類:保護 > 安全存取管理 > 不可公開存取的資源

嚴重性：高

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-default-root-object-configured`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分發是否設定為傳回預設根物件的特定物件。如果 CloudFront 散佈沒有設定預設根物件，則控制項會失敗。

使用者有時可能會要求發佈的根 URL，而不是發佈中的物件。發生這種情況時，指定預設根物件可協助避免暴露 Web 分佈的內容。

修補

若要設定 CloudFront 分發的預設根物件，請參閱 Amazon CloudFront 開發人員指南中的如何指定預設根物件。

[CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

相關要求：第 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-viewer-policy-https`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分發是否要求檢視者直接使用 HTTPS，或是否使用重新導向。如果`ViewerProtocolPolicy`設定`allow-all`為 for `defaultCacheBehavior` 或，則控制項會失敗`cacheBehaviors`。

HTTPS (TLS) 可用來協助防止潛在攻擊者利用 person-in-the-middle或類似攻擊來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能來測試應用程式，以瞭解效能設定檔和 TLS 的影響。

修補

若要加密傳輸中的 CloudFront 分發，請參閱在檢視者之間需要 HTTPS 進行通訊和 Amazon CloudFront 開發人員指南 CloudFront中的。

[CloudFront.4] CloudFront 發行版應該配置原始容錯移轉

相關要求：CP-10, 尼斯 -53.R5 SC-36, 尼斯. 800-53.R5 SC-5 (2), 奈特 800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：低

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-origin-failover-enabled`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon CloudFront 分發是否設定為具有兩個或多個起源的原始群組。

CloudFront 原始容錯移轉可提高可用性。如果主要來源無法使用或傳回特定的 HTTP 回應狀態碼，原始容錯移轉會自動將流量重新導向至次要來源。

修補

若要設定 CloudFront 分發的原始容錯移轉，請參閱 Amazon CloudFront 開發人員指南中的建立原始群組。

[CloudFront.5] CloudFront 發行版應啟用日誌記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯．五月五日六星期六 (4), 日本七點八十七 (7), 尼斯 .800-53.R5 (9), 尼斯 .800-53.R5 系統 -4 (20), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-accesslogs-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查是否已在 CloudFront 分發上啟用伺服器存取記錄。如果未針對分佈啟用存取日誌記錄，則此控制會失敗。

CloudFront 訪問日誌提供有關 CloudFront 接收的每個用戶請求的詳細信息。每個日誌都包含收到請求的日期和時間、提出請求的檢視者 IP 地址、請求的來源，以及檢視者提出請求的連接埠號碼等資訊。

這些日誌適用於安全與存取稽核及鑑識調查等應用程式。如需有關如何分析存取日誌的其他指引，請參閱 Amazon Athena 使用者指南中的查詢 Amazon CloudFront 日誌。

修補

若要設定 CloudFront 分發的存取記錄，請參閱 Amazon CloudFront 開發人員指南中的設定和使用標準日誌 (存取日誌)。

[CloudFront.6] CloudFront 發行版應啟用 WAF

相關要求：交流 -4 (21)

分類:保護 > 保護服務

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-associated-with-waf`

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudFront 發行版是否與 AWS WAF 傳統或 AWS WAF Web ACL 相關聯。如果分配與 Web ACL 沒有關聯，則控制項會失敗。

AWS WAF 是一種網絡應用程序防火牆，可幫助保護 Web 應用程序和 API 免受攻擊。其可讓您設定一組稱為 Web 存取控制清單 (Web ACL) 的規則，該組規則可根據您定義的可自訂 Web 安全規則與條件

來允許、封鎖或計數 Web 請求。確保您的 CloudFront 發行版與 AWS WAF Web ACL 相關聯，以幫助保護其免受惡意攻擊。

修補

若要將 AWS WAF Web ACL 與 CloudFront 分發產生關聯，請參閱 Amazon CloudFront 開發人員指南中的使用 AWS WAF 控制內容存取。

[CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證

相關要求：第 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-custom-ssl-certificate`

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudFront 發行版是否使用預設 SSL/TLS 憑證 CloudFront 提供。如果 CloudFront 發行版使用自訂 SSL/TLS 憑證，則此控制項會通過。如果 CloudFront 散發使用預設 SSL/TLS 憑證，則此控制項會失敗。

自訂 SSL/TLS 可讓您的使用者使用替代網域名稱存取內容。您可以在 AWS Certificate Manager (建議使用) 或 IAM 中儲存自訂憑證。

修補

若要使用自訂 SSL/TLS 憑證為 CloudFront 分發新增替代網域名稱，請參閱 Amazon CloudFront 開發人員指南中的新增替代網域名稱。

[CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：低

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-sni-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分發是否使用自訂 SSL/TLS 憑證，並設定為使用 SNI 來提供 HTTPS 請求。如果自訂 SSL/TLS 憑證已關聯，但 SSL/TLS 支援方法是專用 IP 位址，則此控制項會失敗。

伺服器名稱指示 (SNI) 是 TLS 通訊協定的延伸，2010 年之後推出的瀏覽器和用戶端支援此選項。如果您設定 CloudFront 為使用 SNI 提供 HTTPS 要求，請 CloudFront 將您的替代網域名稱與每個節點的 IP 位址建立關聯。當檢視器提交內容的 HTTPS 請求時，DNS 會將請求路由到正確節點的 IP 地址。您網域名稱的 IP 地址在 SSL/TLS 交握溝通期間決定；IP 地址並非專用於您的分佈。

修補

若要設定 CloudFront 散發使用 SNI 來提供 HTTPS 要求，請參閱 CloudFront 開發人員指南中的使用 SNI 提供 HTTPS 要求 (適用於大多數用戶端)。

[CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量

相關要求：第 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-traffic-to-origin-encrypted`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon CloudFront 分發是否正在加密到自訂來源的流量。對於原始通訊協定原則允許「僅限 http-ly」的 CloudFront 發行版，此控制項會失敗。如果發行版的原始協議策略是「匹配查看器」，而查看器協議策略是「全部」，則此控制也會失敗。

HTTPS (TLS) 可用來協助防止竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。

修補

若要將原始通訊協定政策更新為要求 CloudFront 連線加密，請參閱 Amazon CloudFront 開發人員指南中的在 CloudFront 與您的自訂原始伺服器之間進行通訊時需要 HTTPS 進行通訊。

[CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議

相關要求：東西 800-53.R5 (2), 交流 4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, -53.R5 SC-8 (1), 日本八分之五 (2), 日本七七 (6) AC-17 SC-12 SC-23

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-no-deprecated-ssl-protocols`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分發是否使用已淘汰的 SSL 通訊協定，在 CloudFront 節點和您的自訂來源之間進行 HTTPS 通訊。如果 CloudFront 發行版具有`CustomOriginConfig`其中`OriginSslProtocols`包含，則此控制項會失敗`SSLv3`。

2015 年，互聯網工程任務小組（IETF）正式宣布，由於協議安全性不足，SSL 3.0 應該被棄用。建議您使用 TLSv1.2 或更新版本，進行 HTTPS 通訊至您的自訂來源。

修補

若要更新 CloudFront 分發的原始 SSL 通訊協定，請參閱 Amazon CloudFront 開發人員指南中的「在 CloudFront 與您的自訂來源之間進行通訊時需要 HTTPS 進行通訊」。

[CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

相關需求：第五代公分 (2)

類別:識別 > 資源配置

嚴重性：高

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-s3-origin-non-existent-bucket`

排程類型：定期

參數：無

此控制項可檢查 Amazon CloudFront 分發是否指向不存在的 Amazon S3 起源。如果原點設定為指向不存在的值區，則 CloudFront 分配控制項會失敗。此控制項僅適用於沒有靜態網站託管的 S3 儲存貯體是 S3 來源的 CloudFront 散佈。

當您帳戶中的 CloudFront 散佈設定為指向不存在的值區時，惡意的第三方可以建立參照的值區，並透過您的散佈提供自己的內容。我們建議您檢查所有原點，而不考慮佈線行為，以確保您的分佈指向適當的原點。

修補

若要修改 CloudFront 分發以指向新來源，請參閱 Amazon CloudFront 開發人員指南中的更新分發。

[CloudFront.13] CloudFront 發行版應使用源訪問控制

類別:保護 > 安全存取管理 > 資源原則設定

嚴重性：中

資源類型：`AWS::CloudFront::Distribution`

AWS Config 規則：`cloudfront-s3-origin-access-control-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 來源的 CloudFront 分發是否已設定原始存取控制 (OAC)。如果未針對 CloudFront 散佈設定 OAC，則控制項會失敗。

使用 S3 儲存貯體做為 CloudFront 分發的來源時，您可以啟用 OAC。這只允許通過指定的 CloudFront 分發訪問值區中的內容，並禁止直接從存儲桶或其他發行版訪問。雖然 CloudFront 支援原始存取身分識別 (OAI)，但 OAC 提供額外的功能，而且使用 OAI 的散佈可以移轉至 OAC。雖然 OAI 提供了一種安全的方式來存取 S3 來源，但它有一些限制，例如缺乏對精細政策組態的支援，以及使用 POST 方法的 HTTP/HTTPS 要求 (需 AWS 區域 要 AWS 簽名版本 4 (Sigv4)。OAI 也不支援使用 AWS Key Management Service. OAC 是以使用 IAM 服務主體透過 S3 來源驗證的 AWS 最佳作法為基礎。

修補

若要針對具有 S3 來源的 CloudFront 分發設定 OAC，請參閱 Amazon CloudFront 開發人員指南中的限制對 Amazon S3 來源的存取。

AWS CloudTrail 控制

這些控制項與資 CloudTrail 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

相關要求：獨聯體 AWS 基金會基準測試版 1.2.0/2.1，獨聯體 AWS 基礎基準測試版 1.4.0/3.1，Nist.800-53.R5 交流 -6（9），指定信號澳洲 -3, 日本五月五日六星期六 (3), 日本 6 月 5 日 (4), 尼斯. 800-53.R5 AU-14 (1), 尼斯. 800-53.R5 七, 尼斯 -53.5 SC-7 (9), 等等 R5 四七 (8), 日本第五章 AU-10 AU-12

類別：識別 > 記錄日誌

嚴重性：高

資源類型：`AWS::::Account`

AWS Config 規則：`multi-region-cloudtrail-enabled`

排程類型：定期

參數：

- `readWriteType`：`ALL`（不可定制）

此控制項會檢查至少有一個多區域 CloudTrail 追蹤。它還會檢查至少一個這些軌跡的`ExcludeManagementEventSources`參數是否為空。

AWS CloudTrail 記錄您帳戶的 AWS API 呼叫，並將記錄檔傳送給您。記錄的資訊包含以下資訊。

- API 發起人的身分
- API 呼叫的時間
- API 發起人的來源 IP 地址
- 請求參數

- 由傳回的回應元素 AWS 服務

CloudTrail 提供帳戶 AWS API 呼叫的歷史記錄，包括從 AWS SDK AWS Management Console、命令列工具進行的 API 呼叫。歷史記錄還包括來自更高級別的 API 調用， AWS 服務 例如 AWS CloudFormation.

透過 CloudTrail 啟用安全性分析、資源變更追蹤和法規遵循稽核所產生的 AWS API 呼叫歷史記錄。多區域線索也提供了下列優勢。

- 多區域線索可協助偵測在未使用區域中發生的未預期活動。
- 多區域線索可確保根據預設，為線索啟用全域服務記錄日誌。全域服務事件記錄會記錄 AWS 全域服務產生的事件。
- 對於多區域追蹤，所有讀取和寫入作業的 CloudTrail 管理事件可確保. AWS 帳戶

依預設，使用建立的 CloudTrail 系統線為 AWS Management Console 多區域系統線。

修補

若要在中建立新的多區域系統線 CloudTrail，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。使用下列的值：

欄位	Value
其他設定, 記錄檔驗證	已啟用
選擇記錄事件、管理事件、API 活動	讀取和寫入。清除排除項的核取方塊。

若要更新現有的追蹤，請參閱《使用指南》中的AWS CloudTrail 〈更新追蹤〉。在管理事件中，針對 API 活動，選擇讀取和寫入。

[CloudTrail.2] CloudTrail 應啟用靜態加密

相關要求：PCI DSS V3.2.1/3.4，獨聯體 AWS 基礎基準 V1.2.0/2.7，獨聯體 AWS 基礎基準測試版 1.4.0/3.7，Ni.800-53.R5 澳大利亞 -9，Ni.800-53.R5 CA-9（1），1), 日本七七 (10), 日本七星期五 (6) SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::CloudTrail::Trail`

AWS Config 規則：`cloud-trail-encryption-enabled`

排程類型：定期

參數：無

此控制項會檢查 CloudTrail 是否設定為使用伺服器端加密 (SSE) AWS KMS key 加密。如果未定義，`KmsKeyId`則控制項會失敗。

若要為敏感 CloudTrail 記錄檔提供額外的安全性，您應該使用伺服器端加密搭配 AWS KMS keys (SSE-KMS) 來進行靜態加密的 CloudTrail 記錄檔。請注意，根據預設，傳送 CloudTrail 到儲存貯體的日誌檔會使用 Amazon 伺服器端加密使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。

修補

若要為 CloudTrail 記錄檔啟用 SSE-KMS 加密，請參閱使用AWS CloudTrail 者指南中的更新追蹤以使用 KMS 金鑰。

[CloudTrail.3] CloudTrail 應該被啟用

相關要求：投資產管理系統 DSS v3.2.1/10.1, 投資產管理系統 DSS V3.2.1/10.2.2, 投資管理系統 DSS V3.2.1/10.2.3, 投資管理系統 DSS V3.2.1/10.2.4, 投資管理系統 DSS V3.2.1/10.2.5, PCI V3.2.1/10.3.2, 支援資料輸入資源管理系統 V3.2.1/10.3.4, 支援資料輸入資源管理系統 V3.2.1/10.3.5, 投資管理系統 DSS V3.2.1/10.3.6

類別：識別 > 記錄日誌

嚴重性：高

資源類型：`AWS::::Account`

AWS Config 規則：`cloudtrail-enabled`

排程類型：定期

參數：無

此控制項 CloudTrail 會檢查您的 AWS 帳戶. 如果您的帳戶至少沒有一個 CloudTrail 追蹤，則控制項會失敗。

但是，某些 AWS 服務並未啟用所有 API 和事件的記錄功能。除了CloudTrail 支援的服務與整合中每項服務，您應該實作任何其他稽核追蹤， CloudTrail 並檢閱其他各項服務的說明文件。

修補

若要開始使用 CloudTrail 並建立系統線，請參閱《使用指南》中的 AWS CloudTrail 〈入門AWS CloudTrail使用〉自學課程。

[CloudTrail.4] 應啟用 CloudTrail 記錄檔驗證

相關要求：PCI DSS V3.2.1/10.5.2，PCI DSS V3.2.1/10.5.5，獨聯體基礎基準測試版 1.2.0/2.2，獨聯體 AWS 基礎基準測試版 1.4.0/3.2，Nist.800-53.R5 澳洲 9，SI-7 (7) AWS

類別:資料安全防護 > 資料完整性

嚴重性：低

資源類型：`AWS::CloudTrail::Trail`

AWS Config 規則：`cloud-trail-log-file-validation-enabled`

排程類型：定期

參數：無

此控制項會檢查記錄檔完整性驗證是否已在 CloudTrail追蹤上啟用。

CloudTrail 日誌檔驗證會建立數位簽章的摘要檔案，其中包含 CloudTrail 寫入 Amazon S3 之每個日誌的雜湊。您可以使用這些摘要檔來判斷記錄檔在 CloudTrail 傳送記錄檔之後是否已變更、刪除或未變更。

Security Hub 建議您在所有追蹤上啟用檔案驗證。記錄檔驗證可提供記錄檔的其他完整性 CloudTrail 檢查。

修補

若要啟用 CloudTrail 記錄檔驗證，請參閱《使用指南》 CloudTrail中的〈啟AWS CloudTrail 用記錄檔完整性驗證〉。

[CloudTrail.5] CloudTrail 追蹤應與 Amazon CloudWatch 日誌整合

相關要求：PCI DSS V3.2.1/10.5.3，獨聯體 AWS 基礎基準測試版 1.2.0/2.4，獨聯體 AWS 基礎基準測試版 1.4.0/3.4，Nist.800-53.R5 交流 -2（4），NIS.800-53.R5 交流 -4（26），澳洲上午 2 號, 尼斯 .800-53.R5 澳大利亞 6 (1), 尼斯 .800-53.R5 澳大利亞 6 (3), 尼斯 .800-53.R5 澳洲 6 (4), 卡 -53.53.5 澳大利亞 6 (5), 尼斯 SC-7 (9), 尼斯. 800-53.R5 SI-20, 尼斯. AU-10 AU-125), 尼斯 .800-53.R5 四七 (8)

類別：識別 > 記錄日誌

嚴重性：低

資源類型：`AWS::CloudTrail::Trail`

AWS Config 規則：`cloud-trail-cloud-watch-logs-enabled`

排程類型：定期

參數：無

此控制項會檢查 CloudTrail 追蹤是否設定為將記錄檔傳送至 CloudWatch 記錄檔。如果追蹤的`CloudWatchLogsLogGroupArn`屬性為空，則控制項會失敗。

CloudTrail 記錄在指定帳戶中進行的 AWS API 呼叫。記錄的信息包括以下內容：

- API 呼叫者的身分
- API 呼叫的時間
- API 呼叫者的來源 IP 位址
- 請求參數
- 由返回的響應元素 AWS 服務

CloudTrail 使用 Amazon S3 進行日誌檔案儲存和交付。您可以擷取指定 S3 儲存貯體中的 CloudTrail 日誌以進行長期分析。若要執行即時分析，您可以設定 CloudTrail 將記錄檔傳送至 CloudWatch 記錄檔。

對於在帳戶中所有區域中啟用的追蹤，請將所有這些區域的記錄檔 CloudTrail 傳送至 CloudWatch 記錄日誌群組。

Security Hub 建議您將 CloudTrail 記錄檔傳送至記 CloudWatch 錄檔。請注意，此建議旨在確保帳戶活動被捕獲、監控並適當地警告。您可以使用 CloudWatch 日誌與您的 AWS 服務. 此建議並不排除使用不同的解決方案。

將記 CloudTrail 錄檔傳送至 CloudWatch 記錄可根據使用者、API、資源和 IP 位址，加速即時和歷史活動記錄。您可以使用此方法針對異常或敏感性帳戶活動建立警示和通知。

修補

若要 CloudTrail 與 CloudWatch 記錄檔整合，請參閱AWS CloudTrail 使用指南中的〈將事件傳送至 CloudWatch 記錄檔〉。

[CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取

相關要求：獨聯體 AWS 基金會基準 v1.2.0/2.3，獨聯體基金會基準 v1.4.0/3.3 AWS

類別：識別 > 記錄日誌

嚴重性：嚴重

資源類型：`AWS::CloudTrail::Trail`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程型態：定期與變更觸發

參數：無

CloudTrail 記錄您帳戶中發出的每個 API 調用的記錄。這些日誌檔案會存放在 S3 儲存貯體中。CIS 建議將 S3 儲存貯體政策或存取控制清單 (ACL) 套用至 CloudTrail 記錄檔的 S3 儲存貯體，以防止公開存取 CloudTrail 日誌。允許公開存取 CloudTrail 記錄內容，可能有助於對手識別受影響帳戶使用或設定中的弱點。

若要執行此檢查，Security Hub 首先使用自訂邏輯來尋找存放 CloudTrail 日誌的 S3 儲存貯體。然後，它會使用 AWS Config 受管規則來檢查儲存貯體是否可公開存取。

如果您將日誌彙總到單一集中式 S3 儲存貯體，則 Security Hub 只會針對集中式 S3 儲存貯體所在的帳戶和區域執行檢查。對於其他帳戶和區域，控制項狀態為 [無資料]。

如果值區可公開存取，則檢查會產生失敗的發現項目。

修補

若要封鎖 CloudTrail S3 儲存貯體的公開存取，請參閱 Amazon 簡單儲存服務使用者指南中的設定 S3 儲存貯體的區塊公共存取設定。選取所有四個 Amazon S3 區塊公開存取設定。

[CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌

相關要求：獨聯體 AWS 基金會基準 v1.2.0/2.6，獨聯體基準基準 v1.4.0/3.6 AWS

類別：識別 > 記錄日誌

嚴重性：低

資源類型：`AWS::CloudTrail::Trail`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

S3 儲存貯體存取日誌會產生一個日誌，其中包含對 S3 儲存貯體發出的每個請求的存取記錄。存取日誌記錄包含要求的詳細資訊，例如要求類型、要求工作負載中指定的資源，以及要求的處理時間與日期。

CIS 建議您在 CloudTrail S3 儲存貯體上啟用儲存貯體存取記錄。

透過在目標 S3 儲存貯體上啟用 S3 儲存貯體記錄，您可以擷取可能影響目標儲存貯體中物件的所有事件。設定日誌放在單獨的儲存貯體中，可存取日誌資訊，這對安全性和事件反應工作流程極有幫助。

若要執行此檢查，Security Hub 會先使用自訂邏輯來尋找儲存記錄 CloudTrail 檔的值區，然後使用 AWS Config 受管理規則來檢查是否已啟用記錄。

如果 AWS 帳戶 將多個日誌檔 CloudTrail 交付到單一目的地 Amazon S3 儲存貯體，Security Hub 只會針對該儲存貯體所在區域中的目標儲存貯體評估此控制。這簡化了您的發現。但是，您應該 CloudTrail 在將日誌傳遞到目的地值區的所有帳戶中開啟。對於保留目標值區的帳戶以外的所有帳戶，控制狀態為「無資料」。

如果值區可公開存取，則檢查會產生失敗的發現項目。

修補

若要為 CloudTrail S3 儲存貯體啟用伺服器存取日誌，請參閱 Amazon 簡單儲存服務使用者指南中的啟用 Amazon S3 伺服器存取日誌。

Amazon CloudWatch 控制

這些控制項與資 CloudWatch 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

相關要求：PCI DSS v3.2.1/7.2.1，獨聯體 AWS 基礎基準 v1.2.0/1.1，獨聯體基金會基準 v1.2.0/3.3，獨聯體基礎基準測試 v1.4.0/1.7，獨聯體 AWS 基礎基準測試 v1.4.0/4.3 AWS AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

root 使用者可以不受限制地存取. AWS 帳戶我們強烈建議您避免使用 root 使用者執行日常工作。盡量減少 root 使用者的使用，並採用最低權限原則進行存取管理，可降低意外變更和意外洩漏高度權限憑證的風險。

最佳做法是，只有在需要執行帳戶和服務管理工作時才使用 root 使用者認證。將 AWS Identity and Access Management (IAM) 政策直接套用至群組和角色，但不套用至使用者。如需如何設定管理員供日常使用的教學課程，請參閱《IAM 使用者指南》中的「建立您的第一個 IAM 管理員使用者和群組」。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 1.7 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。
>
> 我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會

針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
度量命名空	**`LogMetrics`**
指標值	**`1`**
預設值	**`0`**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.2] 確保未經授權的 API 調用存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.1

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您建立指標篩選器，並警示未經授權的 API 呼叫。監控未經授權的 API 呼叫有助於揭露應用程式錯誤，可能會降低偵測惡意活動的時間。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準基準 v1.2 中針對控制項 3.1 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。

在下列情況下，檢查會導致FAILED發現結果：

- 未設定任何追蹤。
- 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。

在下列情況下，檢查會導致控制狀態為：NO_DATA

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題ListSubscriptionsByTopic。否則，Security Hub 會產生控制WARNING項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.3] 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.2

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您建立不受 MFA 保護的指標篩選器和警示主控台登入。監控單一因素主控台登入會增加不受 MFA 保護的帳戶可見性。

要運行此檢查，Security Hub 使用自定義邏輯來執行 CIS AWS 基準基準 v1.2 中針對控制項 3.2 規定的確切審核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
在下列情況下，檢查會導致`FAILED`發現結果：

- 未設定任何追蹤。
- 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。

在下列情況下，檢查會導致控制狀態為：`NO_DATA`

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態

欄位	Value
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.4，獨聯體基金會基準 v1.4.0/4.4 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

此控制項會將記錄導向至 CloudTrail 記錄檔，並建立對應的指標篩選器和警示，以 CloudWatch 檢查您是否即時監控 API 呼叫。

CIS 建議您針對 IAM 政策所做的變更建立指標篩選器和警示。監控這些變更有助於確保身分驗證和授權控制保持不變。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

> **Note**
>
> 我們在這些修復步驟中建議的濾波器模式與 CIS 指南中的濾波器模式不同。我們建議的篩選器僅針對來自 IAM API 呼叫的事件。

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) || ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) || ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) || ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) || ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) || ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) || ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態

欄位	Value
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.5，獨聯體基金會基準 v1.4.0/4.5 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您針對 CloudTrail組態設定的變更建立度量篩選器和警示。監控這些變更有助於確保帳戶活動的持續可見性。

若要執行此檢查，Security Hub 使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 4.5 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。

- 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。

在下列情況下，檢查會導致控制狀態為：NO_DATA

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題ListSubscriptionsByTopic。否則，Security Hub 會產生控制WARNING項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) ||

欄位	Value
	`($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
度量命名空	**`LogMetrics`**
指標值	**`1`**
預設值	**`0`**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*`your-metric-name`* 是...	大於/等於
比...	**`1`**

[CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.6，獨聯體基準基準 v1.4.0/4.6 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您針對失敗的主控台驗證嘗試建立指標篩選器和警示。監控失敗的主控台登入可能會降低偵測嘗試暴力破解登入資料的前置時間，這可能會提供可用於其他事件相互關聯的指標，例如來源 IP。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 4.6 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
在下列情況下，檢查會導致`FAILED`發現結果：

- 未設定任何追蹤。
- 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。

在下列情況下，檢查會導致控制狀態為：`NO_DATA`

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
度量命名空	**`LogMetrics`**
指標值	**`1`**
預設值	**`0`**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*`your-metric-name`* 是...	大於/等於
比...	**`1`**

[CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.7，獨聯體基金會基準 v1.4.0/4.7 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您針對已將狀態變更為停用或排程刪除的客戶管理金鑰建立指標篩選器和警示。無法繼續存取使用已停用或已刪除金鑰加密的資料。

若要執行此檢查，Security Hub 使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 4.7 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。如果`ExcludeManagementEventSources`包含，控制項也會失敗`kms.amazonaws.com`。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能基於不同的區域。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。

- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
度量命名空	**`LogMetrics`**

欄位	Value
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.8，獨聯體基金會基準 v1.4.0/4.8 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您針對 S3 儲存貯體政策的變更建立指標篩選器和警示。監控這些變更可能會降低偵測和更正敏感 S3 儲存貯體寬鬆政策的時間。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 4.8 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。
>
> 我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。
>
> 對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。

3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.9，獨聯體基金會基準 v1.4.0/4.9 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。

CIS 建議您針對 AWS Config 組態設定的變更建立度量篩選器和警示。監控這些變更有助於確保帳戶組態項目的持續可見性。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v1. 4.0 中針對控制項 4.9 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請按照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`

欄位	Value
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準 v1.2.0/3.10，獨聯體基金會基準 v1.4.0/4.10 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。安全群組是控制 VPC 中輸入和輸出流量的狀態封包篩選條件。

CIS 建議您針對安全性群組的變更建立指標篩選器和警示。監控這些變更有助於確保不會意外公開 資源和服務。

若要執行此檢查，Security Hub 使用自訂邏輯來執行 CIS AWS 基準測試 v 1.4.0 中針對控制項 4.10 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。
>
>   我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。
>
> 對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請依照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
度量命名空	**`LogMetrics`**
指標值	**`1`**
預設值	**`0`**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*`your-metric-name`* 是...	大於/等於

欄位	Value
比...	**1**

[CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示

相關要求：獨聯體 AWS 基金會基準指標 v1.2.0/3.11，獨聯體基金基準指標 v1.4.0/4.11 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。NACL 做為無狀態封包篩選條件使用，可控制 VPC 中子網路的輸入和輸出流量。

CIS 建議您針對 NACL 的變更建立度量篩選器和警示。監控這些變更有助於確保 AWS 資源和服務不會意外暴露。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v 1.4.0 中針對控制項 4.11 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。

在下列情況下，檢查會導致控制狀態為：NO_DATA

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題ListSubscriptionsByTopic。否則，Security Hub 會產生控制WARNING項的發現項目。

修補

若要傳遞此控制項，請依照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	{($.eventName=CreateNetwork Acl) \|\| ($.eventName=Creat eNetworkAclEntry) || ($.eventN

欄位	Value
	ame=DeleteNetworkAcl) || ($.eventName=DeleteNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclEntry) || ($.eventName=ReplaceNetworkAclAssociation)}
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示

相關要求：獨聯體 AWS 基金會基準指標 v1.2.0/3.12，獨聯體基金基準指標 v1.4.0/4.12 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:AWS::Logs::MetricFilter,AWS::CloudWatch::Alarm,AWS::CloudTrail::Trail,AWS::SNS::Topic

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。需要有網路閘道才能在 VPC 外部的目標傳送和接收流量。

CIS 建議您針對網路閘道的變更建立指標篩選器和警示。監控這些變更有助於確保所有輸入和輸出流量透過控制路徑周遊 VPC 邊界。

若要執行此檢查，Security Hub 會使用自訂邏輯來執行 CIS AWS 基準測試 v 1.2 中針對控制項 4.12 規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。
>
> 我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。
>
> 對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請依照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
度量命名空	**`LogMetrics`**
指標值	**`1`**
預設值	**`0`**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態

欄位	Value
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報

相關要求：獨聯體 AWS 基金會基準指標 v1.2.0/3.13，獨聯體基金基準指標 v1.4.0/4.13 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

此控制項會將記錄導向至 CloudTrail 記錄檔，並建立對應的指標篩選器和警示，以 CloudWatch 檢查您是否即時監控 API 呼叫。路由表會在子網路間路由網路流量，並路由到網路閘道。

CIS 建議您針對路由表的變更建立度量篩選器和警示。監控這些變更有助於確保所有 VPC 流量流經預期的路徑。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

  我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之NO_DATA控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制WARNING項的發現項目。

修補

> **Note**
>
> 我們在這些修復步驟中建議的濾波器模式與 CIS 指南中的濾波器模式不同。我們建議的篩選器僅鎖定來自 Amazon Elastic Compute Cloud (EC2) API 呼叫的事件。

若要傳遞此控制項，請依照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*your-metric-name* 是...	大於/等於
比...	**1**

[CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報

相關要求：獨聯體 AWS 基金會基準指標 v1.2.0/3.14，獨聯體基金基準指標 v1.4.0/4.14 AWS

類別：偵測 > 偵測服務

嚴重性：低

資源類型:`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,`AWS::SNS::Topic`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

您可以通過將 CloudTrail 日誌導向到日 CloudWatch 誌並建立相應的指標過濾器和警報來實時監視 API 調用。一個帳戶可有多個 VPC，而您可在兩個 VPC 之間建立對等連線，在 VPC 之間路由網路流量。

CIS 建議您針對 VPC 的變更建立量度篩選器和警示。監控這些變更有助於確保身分驗證和授權控制保持不變。

若要執行此檢查，Security Hub 使用自訂邏輯來執行 CIS AWS 基準測試 v 1.4.0 中針對控制項 4.14 所規定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

> **Note**
>
> 當 Security Hub 執行此控制項的檢查時，會尋找目前帳戶使用的 CloudTrail 追蹤。這些追蹤可能是屬於其他帳戶的組織追蹤。多區域軌跡也可能以不同的區域為基礎。
> 在下列情況下，檢查會導致`FAILED`發現結果：
>
> - 未設定任何追蹤。
> - 目前區域中且目前帳戶擁有的可用追蹤不符合控制需求。
>
> 在下列情況下，檢查會導致控制狀態為：`NO_DATA`
>
> - 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
> - 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。
>
> 我們建議組織追蹤記錄組織中許多帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。使用組織軌跡會導致組織成員帳戶中評估之`NO_DATA`控制項的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或者必須透過呼叫存取 Amazon SNS 主題`ListSubscriptionsByTopic`。否則，Security Hub 會產生控制`WARNING`項的發現項目。

修補

若要傳遞此控制項，請依照下列步驟為指標篩選器建立 Amazon SNS 主題、 AWS CloudTrail 追蹤、指標篩選器和警示。

1. 建立 Amazon SNS 主題。如需指示，請參閱 Amazon 簡單通知服務開發人員指南中的開始使用 Amazon SNS。建立接收所有 CIS 警示的主題，並至少建立一個主題訂閱。
2. 建立套用至所有 CloudTrail 系統的軌跡 AWS 區域。如需指示，請參閱《AWS CloudTrail 使用指南》中的〈建立系統線〉。

   記下您與 CloudTrail 追蹤關聯的 CloudWatch 記錄日誌群組名稱。您可以在下一個步驟中建立該記錄群組的度量篩選器。
3. 建立指標篩選條件。如需指示，請參閱 Amazon CloudWatch 使用者指南中的為日誌群組建立指標篩選器。使用下列的值：

欄位	Value
定義模式，過濾器模式	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink)`

欄位	Value
	`|| ($.eventName=EnableVpcClassicLink)}`
度量命名空	**LogMetrics**
指標值	**1**
預設值	**0**

4. 根據篩選器建立警示。如需指示，請參閱 Amazon CloudWatch 使用者指南中的根據日誌群組指標篩選器建立 CloudWatch 警示。使用下列的值：

欄位	Value
條件，臨界值類型	靜態
每當*`your-metric-name`* 是...	大於/等於
比...	**1**

[CloudWatch.15] CloudWatch 警報應設定指定的動作

類別：偵測 > 偵測服務

相關要求：NIST-五點五澳大利亞六 (1)、日本五月五日六 (5)、尼斯 .800-53.R5 鈣 -7、鐵四 (1)、尼斯 .), 尼斯 .800-53.R5 四四 (5) SI-20

嚴重性：高

資源類型：`AWS::CloudWatch::Alarm`

AWS Config 規則：**`cloudwatch-alarm-action-check`**

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
alarmActionRequired	如果參數設定為，true且警示在警示狀態變更為時有動作，則控制項會產生PASSED尋找結果ALARM。	Boolean	不可定制	true
insufficientDataActionRequired	如果參數設定為，true且警示在警示狀態變更為時有動作，則控制項會產生PASSED尋找結果INSUFFICIENT_DATA 。	Boolean	true 或 false *	false
okActionRequired	如果參數設定為，true且警示在警示狀態變更為時有動作，則控制項會產生PASSED尋找結果OK。	Boolean	true 或 false *	false

此控制項會檢查 Amazon CloudWatch 警示是否已為該ALARM州設定至少一個動作。如果警示沒有針對ALARM狀態設定動作，則控制項會失敗。或者，您可以包括自訂參數值，以便也要求INSUFFICIENT_DATA或OK狀態的警示動作。

> **Note**
>
> Security Hub 會根據 CloudWatch 度量警示來評估此控制項。度量警示可能是已設定指定動作之複合警示的一部分。控制FAILED項會在下列情況下產生發現項目：
>
> - 未針對度量警示設定指定的動作。
> - 度量警示是已設定指定動作之複合警示的一部分。

此控制項著重於 CloudWatch 警示是否已設定警示動作，而 CloudWatch.17 則著重於 CloudWatch 警示動作的啟動狀態。

我們建議 CloudWatch 您採取警示動作，以便在受監控的指標超出定義的臨界值時自動警示您。監控警報可協助您識別異常活動，並在警示進入特定狀態時快速回應安全性和操作問題。最常見的警示動作類型是將訊息傳送至 Amazon 簡單通知服務 (Amazon SNS) 主題來通知一個或多個使用者。

修補

如需 CloudWatch 警示支援動作的相關資訊，請參閱 Amazon CloudWatch 使用者指南中的警示動作。

[CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間

類別：識別 > 記錄日誌

相關要求：第五十六澳大利亞 6 (3)、日本八月五日六號 (3)、日本八月五日六號 (4)、尼斯．AU-10 AU-11 SI-12

嚴重性：中

資源類型：`AWS::Logs::LogGroup`

AWS Config 規則：**`cw-loggroup-retention-period-check`**

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`minRetentionTime`	CloudWatch 記錄群組的最短保留期 (以天為單位)	列舉	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

此控制項會檢查 Amazon 日 CloudWatch 誌群組的保留期是否至少為指定天數。如果保留期間小於指定數目，則控制項會失敗。除非您為保留期提供自訂參數值，否則 Security Hub 會使用預設值 365 天。

CloudWatch 記錄集中來自所有系統、應用程式的日誌，並 AWS 服務 在單一、可高度擴展的服務中。您可以使用 CloudWatch 日誌從 Amazon 彈性運算雲端 (EC2) 執行個體、Amazon Route 53 和其他來源監控 AWS CloudTrail、存放和存取日誌檔。保留記錄至少 1 年可協助您符合記錄保留標準。

修補

若要設定日誌保留設定，請參閱 Amazon CloudWatch 使用者指南中的變更 CloudWatch 日誌資料保留。

[CloudWatch.17] 應啟動 CloudWatch 警報動作

類別：偵測 > 偵測服務

相關要求：日本八月五日 -53.R5 澳大利亞 6 (1)、日本五月六日 (5)、尼斯 .800-53.R5 二氧化鈣 -7、日本八月五日 -53.R5 SI-4 (12)

嚴重性：高

資源類型：`AWS::CloudWatch::Alarm`

AWS Config 規則：**`cloudwatch-alarm-action-enabled-check`**

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudWatch 警示動作是否已啟動 (`ActionEnabled`應設定為 true)。如果停用警示的警示動作，則控制項會失敗。 CloudWatch

> **Note**
>
> Security Hub 會根據 CloudWatch 度量警示來評估此控制項。公制警報可能是已激活警報動作的複合警報的一部分。控制`FAILED`項會在下列情況下產生發現項目：
>
> - 未針對度量警示設定指定的動作。
> - 公制警報是已激活警報動作的複合警報的一部分。

此控制項著重於 CloudWatch 警示動作的啟動狀態，而 CloudWatch.15 則著重於 CloudWatch 警示中是否已設定任何`ALARM`動作。

當受監控的測量結果超出定義的臨界值時，警示動作會自動發出警示。如果停用警示動作，警示變更狀態時不會執行任何動作，而且不會收到監控指標變更的警示。我們建議您啟用 CloudWatch 警示動作，以協助您快速回應安全性和操作問題。

修補

啟動 CloudWatch 警示動作 (主控台)

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在功能窗格的 [警報] 下，選擇 [所有鬧鐘]。
3. 選取您要啟動動作的鬧鐘。
4. 在 [動作] 中，選擇 [警示動作 — 新增]，然後選擇 [啟用]。

如需啟用 CloudWatch 警示動作的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的警示動作。

AWS CodeBuild 控制

這些控制項與資 CodeBuild 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據

> **Important**
>
> 在 2024 年 1 月 10 日，此控制項的標題變更為上一個標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS 版本 3.2.1/8.2.1、N.800-53.R5 S-3

類別：保護 > 安全開發

嚴重性：嚴重

資源類型：`AWS::CodeBuild::Project`

AWS Config 規則：`codebuild-project-source-repo-url-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案 Bitbucket 來源儲存庫 URL 是否包含個人存取權杖或使用者名稱和密碼。如果 Bitbucket 來源儲存庫 URL 包含個人存取權杖或使用者名稱和密碼，則控制項會失敗。

> **Note**
>
> 此控制項會評估 CodeBuild 組建專案的主要來源和次要來源。如需有關專案來源的詳細資訊，請參閱《AWS CodeBuild 使用指南》中的多個輸入來源和輸出成品範例。

登入認證不應以純文字格式儲存或傳輸，也不應出現在來源儲存庫 URL 中。您應該在中訪問源提供程序，而不是個人訪問令牌或登錄憑據 CodeBuild，並將源存儲庫 URL 更改為僅包含指向 Bitbucket 存儲庫位置的路徑。使用個人訪問令牌或登錄憑據可能會導致意外的數據暴露或未經授權的訪問。

修補

您可以更新您的 CodeBuild 專案以使用 OAuth。

從 CodeBuild 項目源中刪除基本身份驗證/（GitHub）個人訪問令牌

1. 開啟主 CodeBuild 控台，網址為 https://console.aws.amazon.com/codebuild/。
2. 選擇包含個人存取字符或使用者名稱及密碼的建置專案。
3. 從 Edit (編輯) 中，選擇 Source (來源)。
4. 選擇斷開與 GitHub /位桶的連接。
5. 選擇「使用 OAuth Connect」，然後選擇「Connect 至 GitHub/位元儲存桶」。
6. 出現提示時，選擇 authorize as appropriate (適當授權)。
7. 視需要重新設定您的儲存庫 URL 和其他組態設定。
8. 選擇 Update source (更新來源)。

如需詳細資訊，請參閱《CodeBuild 使用指南》中的「AWS CodeBuild 使用案例型範例」。

[CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據

相關要求：PCI DSS V3.2.1/8.2.1、等級 5 IA-5 (7)、NIS.800-53.R5

類別：保護 > 安全開發

嚴重性：嚴重

資源類型：`AWS::CodeBuild::Project`

AWS Config 規則：`codebuild-project-envvar-awscred-check`

排程類型：已觸發變更

參數：無

此控制項會檢查專案是否包含環境變數 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。

身分驗證登入資料 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY 永遠不應以純文字形式存放，應該這可能會意外公開資料或使其受到未經授權的存取。

修補

若要從 CodeBuild 專案移除環境變數，請參閱《使用指南》 AWS CodeBuild中的〈變更組建專案的設 AWS CodeBuild 定〉。確保沒有為環境變量選擇任何內容。

您可以將具有敏感值的環境變數儲存在「 AWS Systems Manager 參數存放區」中 AWS Secrets Manager ，或從組建規格中擷取這些變數。如需指示，請參閱《AWS CodeBuild 使用指南》中「環境」一節中標示為「重要」的方塊。

[CodeBuild.3] CodeBuild S3 日誌應加密

相關要求：第五卡 -53.R5 CA-9 (1)、電腦五公分三 (6)、尼斯八百五十三 (5) SC-13、電子信號 -53.R5 SC-28、電子信號 (5) SC-28 (1)、

分類:保護 > 資料保護 > 加密 data-at-rest

嚴重性：低

資源類型：AWS::CodeBuild::Project

AWS Config 規則：codebuild-project-s3-logs-encrypted

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案的 Amazon S3 日誌是否已加密。如果停用專案 S3 日誌的加密，則控制 CodeBuild 項會失敗。

靜態資料加密是建議的最佳作法，以便在資料周圍新增存取管理層。 AWS 將靜態記錄檔加密可降低未經驗證的使用者存取儲存在磁碟上之資料的風險。它增加了另一組訪問控制，以限制未經授權用戶訪問數據的能力。

修補

若要變更 CodeBuild 專案 S3 日誌的加密設定，請參閱AWS CodeBuild 使用者指南 AWS CodeBuild中的變更組建專案的設定。

[CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置

相關要求：交流 -53.R5 (12)、交流電 -2 (4)、奈特。800-53.R5 交流 -6 (9)、尼斯特。800-53.R5 交流 -6 (9)、黑色 -53.R5、AU-10、六月五日 (3), 尼斯 .800-53.R5 (4), 日本 6 星期六 (4), 尼斯 .800-53.R5 (7), 尼斯 .800-53.R5 SC-7 (9), 尼斯 .800-53.R5 (9),), 尼斯 .800-53.R5 四七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::CodeBuild::Project`

AWS Config 規則：`codebuild-project-logging-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 CodeBuild 專案環境是否至少有一個記錄選項，無論是 S3 還是啟用 CloudWatch 日誌。如果 CodeBuild 專案環境未啟用至少一個記錄選項，則此控制項會失敗。

從安全的角度來看，記錄是一項重要功能，可以在發生任何安全事件時實現 future 鑑識工作。將 CodeBuild 專案中的異常與威脅偵測相關聯，可增加對這些安全威脅偵測的準確性的信心。

修補

如需有關如何設定 CodeBuild 專案記錄設定的詳細資訊，請參閱 CodeBuild 使用指南中的建立組建專案 (主控台)。

[CodeBuild.5] CodeBuild 項目環境不應啟用特權模式

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：交流 -2 (1)、交流 3 (1)、NIST -53.R5 交流 -3、交流 -3 (15)、指定交流 -3 (7)、交流 -3 (7)、交流 5 (7)、交流 5、交流 5 (10) 2)

類別:保護 > 安全存取管理

嚴重性：高

資源類型：`AWS::CodeBuild::Project`

AWS Config 規則：`codebuild-project-environment-privileged-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案環境是否已啟用或停用特權模式。如果 CodeBuild 專案環境已啟用特權模式，則控制項會失敗。

根據預設，Docker 容器不允許存取任何裝置。「Privileged」(特殊權限) 模式會授予建置專案之 Docker 容器對所有裝置的存取權。`privilegedMode`使用值設置`true`允許 Docker 守護程序在 Docker 容器中運行。Docker 守護程序偵聽 Docker API 請求並管理 Docker 對象，例如圖像，容器，網絡和卷。只有在構建項目用於構建 Docker 映像時，才應將此參數設置為 true。否則，應停用此設定，以防止意外存取 Docker API 以及容器的基礎硬體。設定`false`可協`privilegedMode`助保護重要資源免於遭到竄改和刪除。

修補

若要配置 CodeBuild 專案環境設定，請參閱CodeBuild 使用指南中的建立組建專案 (主控台)。在「環境」區段中，請勿選取「授權」設定。

AWS Config 控制

這些控制項與資 AWS Config 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Config 1] AWS Config 應該被啟用

相關要求：PCI DSS V3.2.1/10.5.2，PCI DSS v3.2.1/11.5，獨聯體 AWS 基礎基準測試 v1.2.0/2.5，獨聯體基礎基準測試版 1.4.0/3.5，Ni.800-53.R5 厘米 -3， AWS

類別：識別 > 清查

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：無 (自訂 Security Hub 規則)

排程類型：定期

參數：無

此控制項會檢查目前區域中的帳戶是否 AWS Config 已啟用，並記錄所有資源。如果未啟用或 AWS Config 未記錄所有資源，則控制項會失敗。

此 AWS Config 服務會對帳戶中支援的 AWS 資源執行組態管理，並將記錄檔傳送給您。記錄的資訊包括組態項目 (AWS 資源)、組態料號之間的關係，以及資源之間的任何組態變更。

Security Hub 建議您 AWS Config 在所有區域中啟用。 AWS Config 擷取的 AWS 組態項目歷程記錄可啟用安全性分析、資源變更追蹤和規範遵循稽核。

> **Note**
>
> Config 1 需要在您使用資訊安全中心的所有區域中啟用此 AWS Config 功能。
> 由於 Security Hub 是區域服務，因此針對此控制項執行的檢查只會檢查帳戶目前的 [區域]。它不會檢查所有區域。
> 如要允許針對每個區域中的全域資源進行安全檢查，您也必須記錄全域資源。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。
> AWS Config 支援的全域記錄資源類型包括 IAM 使用者、群組、角色和客戶受管政策。您可以考慮停用 Security Hub 控制項，以便在關閉全域資源記錄的區域中檢查這些資源類型。由於 IAM 是全球服務，因此 IAM 資源只會在開啟全域資源記錄的區域中記錄。如需詳細資訊，請參閱 您可能想要停用的 Security Hub 控制項。

修補

若要啟用 AWS Config 並設定它以記錄所有資源，請參閱AWS Config 開發人員指南中的「手動設定」。若要記錄全域資源並確保未排除任何資源類型，請選取所有具有可自訂覆寫項目的資源。刪除任何覆蓋設置，並將錄製頻率設置為連續錄製。

您也可以使用 AWS CloudFormation 範本來自動化此程序。若要取得更多資訊，請參閱《AWS CloudFormation 使用指南》中的AWS CloudFormation StackSets 範例樣板。

AWS Database Migration Service 控制

這些控制項與資 AWS DMS 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[DMS.1] Database Migration Service 複製執行個體不應該是公用的

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.2.1、PCI 直接安裝資料管理系統 V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::DMS::ReplicationInstance`

AWS Config 規則：`dms-replication-not-public`

排程類型：定期

參數：無

此控制項會檢查 AWS DMS 複寫執行個體是否為公用。要做到這一點，它檢查`PubliclyAccessible`字段的值。

私人複寫執行個體具有私人 IP 位址，您無法在複寫網路外部存取該 IP 位址。當來源和目標資料庫位於相同網路中時，複製執行個體應該具有私有 IP 位址。網路也必須使用 VPN 或 VPC 對等 AWS Direct Connect連接至複寫執行個體的 VPC。若要深入了解公有和私有複寫執行個體，請參閱AWS Database Migration Service 使用指南中的公用和私有複寫執行個體。

您也應該確保只有獲得授權的使用者才能存取您的 AWS DMS 執行個體組態。若要這麼做，請限制使用者的 IAM 許可以修改 AWS DMS 設定和資源。

修補

您無法在建立 DMS 複寫執行個體之後變更其公用存取設定。若要變更公開存取設定，請刪除目前的執行個體，然後重新建立它。請勿選取「可公開存取」選項。

[DMS.6] DMS 複製執行個體應啟用自動次要版本升級

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五四 (4)、七月五四 (5)

類別:偵測 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：`AWS::DMS::ReplicationInstance`

AWS Config 規則：`dms-auto-minor-version-upgrade-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS DMS 複寫執行個體是否已啟用自動次要版本升級。如果 DMS 複寫執行個體未啟用自動次要版本升級，則控制項會失敗。

DMS 會為每個支援的複寫引擎提供次要版本的自動升級，讓您可以保留複寫執行 up-to-date個體。次要版本可以引入新的軟件功能，錯誤修復，安全補丁和性能改進。藉由在 DMS 複製執行個體上啟用自動次要版本升級，系統會在維護時段期間自動套用次要升級，或在選擇 [立即套用變更] 選項時立即套用。

修補

若要在 DMS 複製執行個體上啟用自動次要版本升級，請參閱AWS Database Migration Service 使用指南中的修改複製執行個體。

[DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、黑色 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十七 (7), 尼斯 .800-53.R5 (9), 尼斯特. 800-53.R5 系統 -4 (20), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::DMS::ReplicationTask`

AWS Config 規則：`dms-replication-task-targetdb-logging`

排程類型：已觸發變更

參數：無

此控制項會檢查 DMS 複寫工作TARGET_APPLY和TARGET_LOAD的最低嚴重性LOGGER_SEVERITY_DEFAULT層級是否已啟用記錄。如果未啟用這些工作的記錄，或者最低嚴重性層級小於，則控制項會失敗LOGGER_SEVERITY_DEFAULT。

DMS 在遷移過程中使用 Amazon CloudWatch 記錄資訊。使用記錄工作設定，您可以指定要記錄哪些元件活動以及記錄多少資訊。您應該為下列工作指定記錄：

- TARGET_APPLY – 將資料和資料定義語言 (DDL) 陳述式套用到目標資料庫。
- TARGET_LOAD – 將資料載入目標資料庫。

透過啟用監視、疑難排解、稽核、效能分析、錯誤偵測和復原，以及歷史分析和報告，記錄在 DMS 複寫工作中扮演重要的角色。它有助於確保成功複製資料庫之間的資料，同時保持資料完整性並符合法規要求。在疑難排解期間，這些元件很少需要 DEFAULT 以外的日誌記錄層級。我們建議您保持這些元件DEFAULT的記錄層級，除非特別要求變更它 AWS Support。的最低記錄層級DEFAULT可確保將資訊訊息、警告和錯誤訊息寫入記錄檔。此控制項會檢查前述複寫工作的記錄層級是否至少為下列其中一項：LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG、或LOGGER_SEVERITY_DETAILED_DEBUG。

修補

若要啟用目標資料庫 DMS 複寫工作的記錄功能，請參閱《AWS Database Migration Service 使用手冊》中的〈檢視和管理 AWS DMS 任務記錄〉。

[DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、黑色 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十七 (7), 尼斯 .800-53.R5 (9), 尼斯特. 800-53.R5 系統 -4 (20), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::DMS::ReplicationTask

AWS Config 規則：dms-replication-task-sourcedb-logging

排程類型：已觸發變更

參數：無

此控制項會檢查 DMS 複寫工作SOURCE_CAPTURE和SOURCE_UNLOAD的最低嚴重性LOGGER_SEVERITY_DEFAULT層級是否已啟用記錄。如果未啟用這些工作的記錄，或者最低嚴重性層級小於，則控制項會失敗LOGGER_SEVERITY_DEFAULT。

DMS 在遷移過程中使用 Amazon CloudWatch 記錄資訊。使用記錄工作設定，您可以指定要記錄哪些元件活動以及記錄多少資訊。您應該為下列工作指定記錄：

- SOURCE_CAPTURE— 從來源資料庫或服務擷取進行中的複寫或變更資料擷取 (CDC) 資料，並傳遞至SORTER服務元件。
- SOURCE_UNLOAD— 在滿載期間，資料會從來源資料庫或服務卸載。

透過啟用監視、疑難排解、稽核、效能分析、錯誤偵測和復原，以及歷史分析和報告，記錄在 DMS 複寫工作中扮演重要的角色。它有助於確保成功複製資料庫之間的資料，同時保持資料完整性並符合法規要求。在疑難排解期間，這些元件很少需要 DEFAULT 以外的日誌記錄層級。我們建議您保持這些元件DEFAULT的記錄層級，除非特別要求變更它 AWS Support。的最低記錄層級DEFAULT可確保將資訊訊息、警告和錯誤訊息寫入記錄檔。此控制項會檢查前述複寫工作的記錄層級是否至少為下列其中一項：LOGGER_SEVERITY_DEFAULTLOGGER_SEVERITY_DEBUG、或LOGGER_SEVERITY_DETAILED_DEBUG。

修補

若要啟用來源資料庫 DMS 複製作業的記錄功能，請參閱AWS Database Migration Service 使用指南中的檢視和管理 AWS DMS 作業記錄。

[DMS.9] DMS 端點應使用 SSL

相關要求：東西 800-53.R5 交流 4、SC-13、等級 800-53.R5 SC-23、等級 800-53.R5 SC-23 (3)、電子信號 -53.R5 (4)、等級 800-53.R5 (4)、等級 -53.R5 SC-8、

分類:保護 > 加密 data-in-transit

嚴重性：中

資源類型：AWS::DMS::Endpoint

AWS Config 規則：dms-endpoint-ssl-configured

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS DMS 端點是否使用 SSL 連線。如果端點不使用 SSL，則控制項會失敗。

SSL/TLS 連線會加密 DMS 複寫執行個體與資料庫之間的連線，藉此提供一層安全性。透過驗證是否正在與預期的資料庫建立連線，使用憑證可提供額外的安全性。它會檢查自動安裝在您佈建的所有資料庫執行個體上的伺服器憑證。透過在 DMS 端點上啟用 SSL 連線，即可在移轉期間保護資料的機密性。

修補

若要將 SSL 連線新增至新的或現有的 DMS 端點，請參閱使用指南 AWS Database Migration Service中的AWS Database Migration Service 搭配使用 SSL。

Amazon DocumentDB 控件

這些控制項與亞馬遜文件資料庫資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`docdb-cluster-encrypted`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon 文件資料庫叢集是否在靜態時加密。如果 Amazon 文件資料庫叢集未在靜態時加密，則控制項會失敗。

靜態數據是指任何持續時間存儲在持久性非易失性存儲中的任何數據。加密可協助您保護此類資料的機密性，降低未經授權使用者存取資料的風險。Amazon DocumentDB 叢集中的資料應該在靜態時加

密，以增加一層安全性。Amazon DocumentDB 使用 256 位元進階加密標準 (AES-256)，使用儲存在 () 中的加密金鑰來加密您的資料。 AWS Key Management Service AWS KMS

修補

您可以在建立 Amazon DocumentDB 叢集時啟用靜態加密。建立叢集後，您無法變更加密設定。如需詳細資訊，請參閱 Amazon DocumentDB 開發人員指南中的為 Amazon DocumentDB 叢集啟用靜態加密。

[文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

相關要求：SI-12

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`docdb-cluster-backup-retention-check`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`minimumBackupRetentionPeriod`	最短備份保留期 (天)	Integer	7 設定為 35	7	

此控制項會檢查 Amazon DocumentDB 叢集的備份保留期是否大於或等於指定的時間範圍。如果備份保留期間小於指定的時間範圍，則控制項會失敗。除非您為備份保留期提供自訂參數值，否則 Security Hub 會使用預設值 7 天。

備份可協助您更快速地從安全性事件中復原，並強化系統的復原能力。透過將 Amazon DocumentDB 叢集的備份自動化，您可以將系統還原到某個時間點，並將停機時間和資料遺失降到最低。在 Amazon

DocumentDB 中，叢集的預設備份保留期為 1 天。必須將其增加到 7 到 35 天之間的值，才能通過此控制。

修補

若要變更 Amazon DocumentDB 叢集的備份保留期，請參閱亞馬遜文件資料庫開發人員指南中的修改 Amazon DocumentDB 叢集。在「Backup」中，選擇備份保留期間。

[文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS:DBSnapshot`

AWS Config 規則：`docdb-cluster-snapshot-public-prohibited`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 手動叢集快照是否為公開狀態。如果手動叢集快照為公用，則控制項會失敗。

除非有意，否則 Amazon DocumentDB 手動叢集快照不應該是公開的。如果您將未加密的手動快照共用為公用，則所有 AWS 帳戶人都可以使用該快照。公開快照可能會導致非預期的資料暴露。

> **Note**
>
> 此控制項會評估手動叢集快照。您無法共用 Amazon DocumentDB 自動化叢集快照。不過，您可以透過複製自動快照，然後共用副本來建立手動快照。

修補

若要移除 Amazon DocumentDB 手動叢集快照的公開存取權，請參閱 Amazon Document DB 開發人員指南中的共用快照。以編程方式，您可以使用 Amazon DocumentDB 操作。`modify-db-snapshot-attribute`設定`attribute-name`為`values-to-remove`和`restore`。`all`

[文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`docdb-cluster-audit-logging-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 叢集是否將稽核日誌發佈到 Amazon CloudWatch 日誌。如果叢集未將稽核記錄發佈至 CloudWatch 記錄，則控制項會失敗。

Amazon DocumentDB (與 MongoDB 相容性) 可讓您稽核叢集中執行的事件。已記錄事件的範例包括成功和失敗的身分驗證嘗試、在資料庫中放入集合，或建立索引。根據預設，Amazon DocumentDB 中的稽核功能會停用，並要求您採取動作來啟用稽核功能。

修補

若要將 Amazon DocumentDB 稽核日誌發佈到日 CloudWatch 誌，請參閱 Amazon Document DB 開發人員指南中的啟用稽核功能。

[文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護

相關要求：鎳鋅 -53.R5 路卡 -9 (1)、指定 5 公分 (5 公分)、電子信號 -53.R5 公分 (2)、電子顯示器 -53.R5 公分 (3)、電子顯示器 -53.R5 SC-5 (2)

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`docdb-cluster-deletion-protection-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 叢集是否已啟用刪除保護。如果叢集未啟用刪除保護，則控制項會失敗。

啟用叢集刪除保護可提供額外的保護層，防止未經授權的使用者意外刪除資料庫或刪除。啟用刪除保護時，無法刪除 Amazon DocumentDB 叢集。您必須先停用刪除保護，刪除要求才能成功執行。當您在 Amazon DocumentDB 主控台中建立叢集時，依預設會啟用刪除保護。

修補

若要為現有 Amazon DocumentDB 叢集啟用刪除保護，請參閱亞馬遜文件資料庫開發人員指南中的修改 Amazon DocumentDB 叢集。在「修改叢集」段落中，選擇啟用刪除保護。

Amazon DynamoDB 控制

這些控制項與 DynamoDB 資源相關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[DynamoDB 資料表應該會根據需求自動擴展容量

相關要求：指定的 CP-10，電腦 -53.R5 CP-2 (2)，指定的指令介面卡 -6 (2)，指定項目：800-53.R5 SC-5 (2)，筆記型號 800-53.R5（2），指定型號 800-53.R5 SI-13 (5) SC-36

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::DynamoDB::Table`

AWS Config 規則：`dynamodb-autoscaling-enabled`

排程類型：定期

參數：

參數	Description (描述)	Type	有效的自訂值	Security Hub 預設值
`minProvisionedReadCapacity`	DynamoDB auto 擴展的佈建讀取容量單位數下限	Integer	1 設定為 `40000`	無預設值

參數	Description (描述)	Type	有效的自訂值	Security Hub 預設值
`targetReadUtilization`	讀取容量的目標使用率百分比	Integer	`20` 設定為 `90`	無預設值
`minProvisionedWriteCapacity`	DynamoDB auto 擴展的佈建寫入容量單位數下限	Integer	`1` 設定為 `40000`	無預設值
`targetWriteUtilization`	寫入容量的目標使用率百分比	Integer	`20` 設定為 `90`	無預設值

此控制項會檢查 Amazon DynamoDB 資料表是否可視需要擴展其讀取和寫入容量。如果表格未使用隨需容量模式或已配置 auto 擴展的佈建模式，則控制項會失敗。根據預設，此控制項只需要設定其中一種模式，而不考慮特定層級的讀取或寫入容量。或者，您可以提供自訂參數值，以要求特定層級的讀取和寫入容量或目標使用率。

隨需求調整容量可避免限制例外狀況，這有助於維持應用程式的可用性。隨需容量模式下的 DynamoDB 表僅受 DynamoDB 輸送量預設表格配額的限制。若要提高這些配額，您可以在佈建模式下使用 AWS Support.DynamoDB 表提交支援票證，並使用 auto 動擴展功能動態調整佈建的輸送量容量，以回應流量模式。如需 DynamoDB 請求節流的詳細資訊，請參閱 Amazon DynamoDB 開發人員指南中的請求節流和爆發容量。

修補

若要在容量模式下對現有表格啟用 DynamoDB 自動擴展，請參閱 Amazon DynamoDB 開發人員指南中的在現有表格上啟用 DynamoDB 自動擴展。

[動態 DynamoDB] 資料表應該已啟用復原 point-in-time

相關要求：指定電腦 -53.R5 CP-10、指定電源 6 (2)、指定點 (8) -53.R5 CP-9、NIST-53.R5 SC-5 (2)、日本電子郵件 (5) SI-12 SI-13

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::DynamoDB::Table`

AWS Config 規則：`dynamodb-pitr-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DynamoDB 表格是否已啟用 point-in-time 復原 (PITR)。

備份可協助您更快速地從安全性事件中復原。它們還可以增強系統的彈性。動 DynamoDB 料庫 point-in-time 復原會自動執行動 DynamoDB 資料表的備份。它減少了從意外刪除或寫入操作中恢復的時間。已啟用 PITR 的 DynamoDB 表格可以還原到過去 35 天內的任何時間點。

修補

若要將 DynamoDB 表格還原到某個時間點，請參閱 Amazon DynamoDB 開發人員指南中的將 DynamoDB 表還原到某個時間點。

[動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::DynamoDB::Cluster`

AWS Config 規則：`dax-encryption-enabled`

排程類型：定期

參數：無

此控制項會檢查 DAX 叢集是否已靜態加密。

靜態資料加密可降低未經驗證的使用者存取儲存在磁碟上的資料的風險。 AWS加密功能會新增另一組存取控制，以限制未經授權使用者存取資料的能力。例如，在讀取資料之前，需要 API 權限才能解密資料。

修補

建立叢集之後，您無法啟用或停用靜態加密。您必須重新建立叢集，才能啟用靜態加密。如需如何建立已啟用靜態加密的 DAX 叢集的詳細指示，請參閱 Amazon DynamoDB 開發人員指南AWS Management Console中的使用啟用靜態加密。

備份計劃中應該有 DynamoDB 資料表

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::DynamoDB::Table`

AWS Config 規則：**`dynamodb-resources-protected-by-backup-plan`**

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`backupVaultLockCheck`	如果參數設定為`true`且資源使用「文件 AWS Backup 庫鎖定」，則控制項會產生`PASSED`發現結果。	Boolean	`true` 或 `false` *	無預設值

此控制項會評估`ACTIVE`狀態中的 Amazon DynamoDB 資料表是否涵蓋在備份計劃中。如果備份計劃未涵蓋 DynamoDB 表格，則控制項會失敗。如果將`backupVaultLockCheck`參數設定為等於`true`，則僅當 DynamoDB 表格在 AWS Backup 鎖定的儲存庫中備份時，控制項才會通過。

AWS Backup 是一項全受管備份服務，可協助您集中並自動備份資 AWS 服務料。使用時 AWS Backup，您可以建立定義備份需求的備份計劃，例如備份資料的頻率，以及保留這些備份的時間長度。在備份計劃中包含 DynamoDB 表可協助您保護資料免於意外遺失或刪除。

修補

若要將 DynamoDB 表新增至 AWS Backup 備份計劃，請參閱AWS Backup 開發人員指南中的將資源指派給備份計劃。

[動態 DynamoDB] 資料表應該已啟用刪除保護

相關要求：鎳鋅 -53.R5 路卡 -9 (1)、指定 5 公分 (5 公分)、電子信號 -53.R5 公分 (2)、電子顯示器 -53.R5 公分 (3)、電子顯示器 -53.R5 SC-5 (2)

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：`AWS::DynamoDB::Table`

AWS Config 規則：**`dynamodb-table-deletion-protection-enabled`**

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DynamoDB 資料表是否已啟用刪除保護。如果 DynamoDB 表格未啟用刪除保護，則控制項會失敗。

您可以使用刪除保護屬性保護 DynamoDB 表格免於意外刪除。針對資料表啟用此屬性有助於確保系統管理員在一般資料表管理作業期間，不會意外刪除資料表。這有助於防止您的正常業務運營中斷。

修補

若要為 DynamoDB 表格啟用刪除保護，請參閱 Amazon Dynam oDB 開發人員指南中的使用刪除保護。

Amazon 彈性容器登錄控制

這些控制項與 Amazon ECR 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ECR.1] ECR 私有儲存庫應設定影像掃描

相關要求：5 RA-5

類別:識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::ECR::Repository

AWS Config 規則：ecr-private-image-scanning-enabled

排程類型：定期

參數：無

此控制項會檢查私有 Amazon ECR 儲存庫是否已設定映像掃描。如果私有 ECR 存放庫未設定為在推送或連續掃描時進行掃描，則控制項會失敗。

ECR 圖像掃描有助於識別容器映像中的軟件漏洞。ECR 會使用開放原始碼 Claire 專案中的常見弱點和入侵 (CVE) 資料庫，並提供掃描發現項目清單。在 ECR 儲存庫上設定影像掃描會增加一層驗證，以確保所儲存影像的完整性和安全性。

修補

若要設定 ECR 儲存庫的映像掃描，請參閱 Amazon 彈性容器登錄使用者指南中的映像掃描。

[ECR.2] ECR 私有儲存庫應配置標籤不變性

相關要求：鎳碳酸鈣 -9 (1)、日本五公分二、五點八公分 (1)

類別:識別 > 庫存 > 標籤

嚴重性：中

資源類型：AWS::ECR::Repository

AWS Config 規則：ecr-private-tag-immutability-enabled

排程類型：已觸發變更

參數：無

此控制項會檢查私有 ECR 儲存庫是否已啟用標籤不變性。如果私有 ECR 存放庫已停用標籤不變性，則此控制項會失敗。如果啟用標籤不變性且具有值，則此規則會通過。IMMUTABLE

Amazon ECR 標籤不變性可讓客戶依賴影像的描述性標籤，作為追蹤和唯一識別影像的可靠機制。不可變的標籤是靜態的，這意味著每個標籤都指向一個唯一的圖像。這提高了可靠性和可擴展性，因為使用靜態標籤將始終導致部署相同的映像。配置時，標籤不變性可防止標籤被覆蓋，從而減少了攻擊面。

修補

若要建立已設定不可變標籤的存放庫，或更新現有儲存庫的映像標籤可變性設定，請參閱 Amazon Elastic 容器登錄使用者指南中的映像標籤可變性。

[ECR.3] ECR 儲存庫應該至少設定一個生命週期原則

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別:識別 > 資源配置

嚴重性：中

資源類型：`AWS::ECR::Repository`

AWS Config 規則：`ecr-private-lifecycle-policy-configured`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECR 儲存庫是否已設定至少一個生命週期政策。如果 ECR 存放庫未設定任何生命週期原則，則此控制項會失敗。

Amazon ECR 生命週期政策可讓您指定儲存庫中映像的生命週期管理。透過設定生命週期政策，您可以根據存留時間或計數，自動清理未使用的影像和映像到期。將這些工作自動化可協助您避免無意中在儲存庫中使用過時的映像檔。

修補

若要設定生命週期政策，請參閱 Amazon 彈性容器登錄使用者指南中的建立生命週期政策預覽。

Amazon ECS 控制

這些控制項與 Amazon ECS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。

相關要求：交流 -2 (1)、交流 3 (1)、尼斯特。800-53.R5 交流 -3 (15)、指定交流 -3 (7)、指定交流 -3 (7)、指定交流 -6

類別：保護 > 安全存取管理

嚴重性：高

資源類型：`AWS::ECS::TaskDefinition`

AWS Config 規則：`ecs-task-definition-user-for-host-mode-check`

排程類型：已觸發變更

參數：

- `SkipInactiveTaskDefinitions`：`true`（不可定制）

此控制項會檢查具有主機網路模式的作用中 Amazon ECS 任務定義是否具有容器定義`privileged`或`user`容器定義。對於具有主機網路模式和容器定義為空白和或空白的`privileged=false`工作定義`user=root`，控制項會失敗。

此控制項只會評估 Amazon ECS 任務定義的最新使用中修訂版。

此控制項的目的在於確保在您執行使用主機網路模式的工作時刻意定義存取權。如果工作定義具有提升的權限，這是因為您已選擇該組態。當工作定義已啟用主機網路，而且您未選擇提升的權限時，此控制項會檢查是否有意外的權限提升。

修補

如需如何更新任務定義的相關資訊，請參閱 Amazon 彈性容器服務開發人員指南中的更新任務定義。

當您更新工作定義時，它不會更新從先前工作定義啟動的執行中工作。若要更新執行中的工作，您必須使用新的工作定義重新部署工作。

[ECS.2] ECS 服務不應該自動分配公共 IP 地址

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網路設定 > 無法公開存取的資源

嚴重性：高

資源類型：AWS::ECS::Service

AWS Config規則:ecs-service-assign-public-ip-disabled(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：

- exemptEcsServiceArns（不可定制）。Security Hub 不會填入此參數。此規則豁免之 Amazon ECS 服務的 ARN 清單 (逗號分隔)。

  此規COMPLIANT則是 Amazon ECS 服務已AssignPublicIP設定為ENABLED且已在此參數清單中指定時。

  此規則是NON_COMPLIANT如果 Amazon ECS 服務已AssignPublicIP設定為ENABLED且未在此參數清單中指定。

此控制項會檢查 Amazon ECS 服務是否設定為自動指派公有 IP 地址。如果AssignPublicIP是，則此控制項失敗ENABLED。如果是，則此控制項AssignPublicIP會傳遞DISABLED。

公用 IP 位址是可從網際網路存取的 IP 位址。如果您使用公有 IP 地址啟動 Amazon ECS 執行個體，則可以從網際網路存取您的 Amazon ECS 執行個體。Amazon ECS 服務不應可公開存取，因為這可能會允許意外存取您的容器應用程式伺服器。

修補

若要停用自動公有 IP 指派，請參閱 Amazon 彈性容器服務開發人員指南中的若要為您的服務設定 VPC 和安全群組設定。

[ECS.3] ECS 任務定義不應共享主機的進程名稱空間

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:識別 > 資源配置

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config規則：ecs-task-definition-pid- 模式檢查

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義是否設定為與其容器共用主機的程序命名空間。如果工作定義與主機上執行的容器共用主機的處理序命名空間，則控制項會失敗。此控制項只會評估 Amazon ECS 任務定義的最新使用中修訂版。

進程 ID（PID）命名空間提供進程之間的分離。它可以防止系統進程可見，並允許 PID 被重複使用，包括 PID 1。如果主機的 PID 命名空間與容器共享，它將允許容器查看主機系統上的所有進程。這減少了主機和容器之間流程層級隔離的好處。這些情況可能會導致未經授權存取主機本身的處理序，包括操控和終止處理序的能力。客戶不應與主機上運行的容器共享主機的進程命名空間。

修補

若要在任務定義`pidMode`上進行設定，請參閱 Amazon 彈性容器服務開發人員指南中的任務定義參數。

[ECS.4] ECS 容器應以非特權的方式執行

相關要求：交流 -2 (1)、交流 3 (1)、尼斯特。800-53.R5 交流 -3 (15)、指定交流 -3 (7)、指定交流 -3 (7)、指定交流 -6

類別:保護 > 安全存取管理 > 根使用者存取限制

嚴重性：高

資源類型：`AWS::ECS::TaskDefinition`

AWS Config規則：ecs-containers-nonprivileged

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義之容器定義中的`privileged`參數是否設定為`true`。如果此參數等於，則控制項會失敗`true`。此控制項只會評估 Amazon ECS 任務定義的最新使用中修訂版。

建議您從 ECS 工作定義中移除提升的權限。當權限參數為時 `true`，容器會在主機容器執行個體上提供更高的權限 (類似於 root 使用者)。

修補

若要在任務定義上設定參`privileged`數，請參閱 Amazon 彈性容器服務開發人員指南中的進階容器定義參數。

[ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取

相關要求：交流 -2 (1)、交流 3 (1)、尼斯特。800-53.R5 交流 -3 (15)、指定交流 -3 (7)、指定交流 -3 (7)、指定交流 -6

類別：保護 > 安全存取管理

嚴重性：高

資源類型：`AWS::ECS::TaskDefinition`

AWS Config規則：ecs-containers-readonly-access

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 容器是否僅限於掛載根檔案系統的唯讀存取權限。如果參數設定為`false`或`readonlyRootFilesystem`參數不存在於工作定義中的容器定義中，則控制項會失敗。此控制項只會評估 Amazon ECS 任務定義的最新使用中修訂版。

啟用此選項可減少安全性攻擊媒介，因為容器執行個體的檔案系統無法竄改或寫入，除非容器執行個體對其檔案系統資料夾和目錄具有明確的讀寫權限。此控制也遵循最低權限原則。

修補

將容器定義限制為 root 檔案系統的唯讀存取

1. 開啟 Amazon ECS 傳統主控台，網址為 https://console.aws.amazon.com/ecs/。
2. 在左側導覽窗格中，選擇 [工作定義]。
3. 選取具有需要更新之容器定義的作業定義。對於每個，請完成以下步驟：
   - 從下拉式清單中，選擇 [使用 JSON 建立新修訂版本]。
   - 新增`readonlyRootFilesystem`參數，並在任務定義內`true`的容器定義中將其設定為。
   - 選擇建立。

[ECS.8] 密碼不應作為容器環境變量傳遞

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

分類:保護 > 安全開發 > 未硬式編碼的憑證

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config規則：ecs-no-environment-secrets

排程類型：已觸發變更

參數：

- 秘密金鑰 =AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY, ECS_ENGINE_AUTH_DATA (不可自訂)

此控制項會檢查容器定義參數中任何變environment數的索引鍵值是否包含AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY、或ECS_ENGINE_AUTH_DATA。如果任何容器定義中的單一環境變數等於AWS_ACCESS_KEY_ID、或AWS_SECRET_ACCESS_KEY，則此控制項會失敗ECS_ENGINE_AUTH_DATA。此控制項不涵蓋從其他位置 (例如 Amazon S3) 傳入的環境變數。此控制項只會評估 Amazon ECS 任務定義的最新使用中修訂版。

AWS Systems Manager 參數存放區可協助您改善組織的安全性狀態。我們建議使用參數存放區來儲存機密和認證，而不是直接將它們傳遞到容器執行個體，或將它們硬式編碼到程式碼中。

修補

若要使用 SSM 建立參數，請參閱《使用指南》中的〈建立 Systems Manager 參數AWS Systems Manager 〉。如需建立指定密碼之任務定義的詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的使用 Secret Manager 指定敏感資料。

[ECS.9] ECS 任務定義應具有記錄組態

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六 (9), 日本第七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config規則：ecs-task-definition-log-配置

排程類型：已觸發變更

參數：無

此控制項會檢查最新的作用中 Amazon ECS 任務定義是否具有指定的記錄組態。如果工作定義未定義logConfiguration屬性，或者至少一個容器定義中的值logDriver為 null，則控制項會失敗。

記錄可協助您維護 Amazon ECS 的可靠性、可用性和效能。從工作定義收集資料可提供可見性，這可協助您偵錯程序並找出錯誤的根本原因。如果您使用的記錄解決方案不需要在 ECS 任務定義中定義 (例如協力廠商記錄解決方案)，您可以在確保正確擷取和傳遞記錄檔之後停用此控制項。

修補

若要為 Amazon ECS 任務定義定義日誌組態，請參閱 Amazon 彈性容器服務開發人員指南中的任務定義中的指定日誌組態。

[ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五四 (4)、七月五四 (5)

類別:識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::ECS::Service

AWS Config規則：ecs-fargate-latest-platform-version

排程類型：已觸發變更

參數：

- latestLinuxVersion: 1.4.0 (不可定制)
- latestWindowsVersion: 1.0.0 (不可定制)

此控制項可檢查 Amazon ECS Fargate 服務是否正在執行最新的 Fargate 平台版本。如果平台版本不是最新版本，則此控制項會失敗。

AWS Fargate 平台版本是指 Fargate 任務基礎結構的特定運行時環境，該基礎結構是內核和容器運行時版本的組合。隨著運行時環境的發展，新的平台版本會發布。例如，可能會針對核心或作業系統更新、新功能、錯誤修正或安全性更新發行新版本。系統會為 Fargate 任務自動部署安全性更新與修補程式。如果發現影響平台版本的安全性問題，請 AWS 修補平台版本。

修補

若要更新現有服務 (包括其平台版本)，請參閱 Amazon 彈性容器服務開發人員指南中的更新服務。

[ECS.12] ECS 叢集應使用容器深入解析

相關要求：日本八月五日 -53.R5 澳大利亞 6 (3)、日本五月六日 (4)、尼斯 .800-53.R5 硫酸鈣-7、日本 -53.R5 SI-2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::ECS::Cluster`

AWS Config規則：`ecs-container-insights-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 ECS 叢集是否使用容器深入解析。如果未針對叢集設定容器深入解析，則此控制項會失敗。

監控是維護 Amazon ECS 叢集的可靠性、可用性和效能的重要組成部分。使用 CloudWatch 容器深入解析，從容器化應用程式和微服務收集、彙總和摘要指標和記錄。 CloudWatch 自動收集許多資源的指標，例如 CPU、記憶體、磁碟和網路。Container Insights 還提供診斷資訊，例如容器重新啟動故障，協助您快速隔離和解決這些故障。您也可以針對容器深入解析收集的指標設定 CloudWatch 警示。

修補

若要使用容器洞見，請參閱 Amazon 使用 CloudWatch 者指南中的更新服務。

Amazon 彈性運算雲控制

這些控制項與 Amazon EC2 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[EC2.1] Amazon EBS 快照不應公開還原

相關要求：PCI DSS V3.2.1/1.2.1、PCI 資料管理系統 (DSS) 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/7.2.1、技術支援系統 DSS V3.2.1/7.2.1、AC-21、解密卡 -53.R5 交流 -3 (7)、21), 星期五交流 -6, 星期五, 星期五七, 星期五七 (11), 尼斯特. 800-53.R5 (16), 星期五七七 (20), 尼斯特. 800-53.R5 (20), SC-7 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::::Account`

AWS Config 規則：`ebs-snapshot-public-restorable-check`

排程類型：定期

參數：無

此控制項會檢查 Amazon 彈性區塊存放區快照是否不公開。如果任何人都可以還原 Amazon EBS 快照，則控制會失敗。

EBS 快照用於在特定時間點將 EBS 磁碟區上的資料備份到 Amazon S3。您可以使用快照來還原 EBS 磁碟區的先前狀態。公開共享快照很少會有人願意接受。通常公開共享快照的決定都是錯誤的，或者並未完全了解其中含義。這項檢查有助於確保所有這些共享都是完整的規劃並且有意的。

若要將公開 EBS 快照設為私有，請參閱 Amazon EC2 Linux 執行個體使用者指南中的共用快照。在「動作」的「修改權限」中，選擇「私人

[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量

相關要求：PCI DSS V3.2.1/1.2.1，PCI DSS V3.2.1/1.3.4，PCI DSS V3.2.1/2.1，獨聯體基礎基準測試版 1.2.0/4.3，獨聯體 AWS 基礎基準測試 V1.4.0/5.3，Ni.800-53.R5 交流 -4，，早上七點七 (16), 日本七點七 (21), 日本七星期七 (21), 尼斯 .800-53.R5 (5), 日本七星期七 (5) AWS

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::EC2::SecurityGroup`

AWS Config 規則：vpc-default-security-group-closed

排程類型：已觸發變更

參數：無

此控制項會檢查 VPC 的預設安全性群組是否允許輸入或輸出流量。如果安全性群組允許輸入或輸出流量，則控制項會失敗。

預設安全群組的規則允許所有來自指派至相同安全群組網路界面 (及其相關聯執行個體) 的傳出和傳入流量。建議您不要使用預設的安全性群組。由於您無法刪除預設安全群組，建議您變更預設安全群組的規則設定，限制傳入和傳出流量。這可以避免在意外地為資源 (例如 EC2 執行個體) 設定預設安全群組時產生意外的流量。

修補

若要修正此問題，請先建立新的最低權限安全性群組。如需指示，請參閱 Amazon VPC 使用者指南中的建立安全群組。然後，將新的安全群組指派給 EC2 執行個體。如需指示，請參閱 Amazon EC2 Linux 執行個體使用者指南中的變更執行個體的安全群組。

將新的安全性群組指派給資源後，請從預設安全性群組中移除所有輸入和輸出規則。如需指示，請參閱 Amazon VPC 使用者指南中的刪除安全群組規則。

[EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::EC2::Volume

AWS Config 規則：encrypted-volumes

排程類型：已觸發變更

參數：無

此控制項會檢查處於連接狀態的 EBS 磁碟區是否已進行加密。如要通過此檢查，EBS 磁碟區必須為使用中狀態且經過加密。如果沒有連接 EBS 磁碟區，則其便不在此檢查的範圍內。

為了為您 EBS 磁碟區上的敏感資料新增多一層的安全，建議您啟用靜態 EBS 加密。Amazon EBS 加密提供 EBS 資源的直接加密解決方案，使您無須建置、維護和保全您自己的金鑰管理基礎設施。它會在建立加密磁碟區和快照時使用 KMS 金鑰。

若要進一步了解 Amazon EBS 加密，請參閱 Amazon EC2 Linux 執行個體使用者指南中的亞馬遜 EBS 加密。

修補

沒有直接的方法可以加密現有的未加密磁碟區或快照。您只能在建立磁碟區或快照時進行加密。

如果您預設啟用加密，Amazon EBS 會使用 Amazon EBS 加密的預設金鑰加密產生的新磁碟區或快照。即使您沒有啟用預設加密，您可以在建立獨立的磁碟區或快照時啟用加密。在這兩種情況下，您都可以覆寫 Amazon EBS 加密的預設金鑰，並選擇對稱的客戶受管金鑰。

如需詳細資訊，請參閱 Amazon EC2 執行個體使用者指南中的建立 Amazon EBS 磁碟區和複製 Amazon EBS 快照。

[EC2.4] 停止的 EC2 執行個體應在指定時間段後移除

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別：識別 > 清查

嚴重性：中

資源類型：`AWS::EC2::Instance`

AWS Config 規則：`ec2-stopped-instance`

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`AllowedDays`	在產生失敗的發現之前，EC2 執行個體允許處於停止狀態的天數。	Integer	1 設定為 365	`30`

此控制項可檢查 Amazon EC2 執行個體停止的時間是否超過允許的天數。如果 EC2 執行個體停止的時間超過允許的最長時間，則控制會失敗。除非您針對允許的最大期間提供自訂參數值，否則 Security Hub 會使用 30 天的預設值。

如果 EC2 執行個體已經很長一段時間沒有執行，就會產生安全風險，因為執行個體沒有進行主動維護 (分析、修補、更新)。如果稍後啟動，缺乏適當的維護可能會導致您的 AWS 環境發生意外問題。若要在一段時間內安全地維護 EC2 執行個體處於非作用中狀態，請定期啟動以進行維護，然後在維護後停止執行個體。理想情況下，這應該是一個自動化的過程。

修補

若要終止非作用中 EC2 執行個體，請參閱 Amazon EC2 執行個體使用者指南中的終止執行個體。

[EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄

相關要求：獨聯體 AWS 基礎基準測試版 1.2.0/2.9，PCI DSS 3.2.1/10.3.3，PCI DSS V3.2.1/10.3.4，PCI DSS V3.2.1/10.3.5，PCI DSS V3.2.1/10.3.6，獨聯體 AWS 基礎基準測試 V1.4.0/3.9，日本 6 月 5 日 (3), 尼斯 .800-53.R5 澳大利亞六 (3), 日本六月五日六 (4), 尼斯 .800-53.R5 SI-7 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::EC2::VPC`

AWS Config 規則：`vpc-flow-logs-enabled`

排程類型：定期

參數：

- `trafficType`：`REJECT` (不可定制)

此控制項可檢查 VPC 是否找到並啟用 Amazon VPC 流程日誌。流量類型設定為`Reject`。

使用 VPC 流程記錄功能，您可以擷取有關進出 VPC 網路介面的 IP 位址流量資訊。建立流程記錄後，您可以在 CloudWatch 記錄中檢視和擷取其資料。為了降低成本，您也可以將流程日誌傳送到 Amazon S3。

Security Hub 建議您為 VPC 的封包拒絕啟用流程記錄。流程記錄可讓您了解周遊 VPC 的網路流量，並可偵測異常流量或在安全性工作流程期間提供洞察。

根據預設，記錄包括 IP 位址流程中不同元件的值，包括來源、目的地和通訊協定。如需日誌欄位的詳細資訊和說明，請參閱 Amazon VPC 使用者指南中的 VPC 流程日誌。

修補

若要建立 VPC 流程日誌，請參閱 Amazon VPC 使用者指南中的建立流程日誌。開啟 Amazon VPC 主控台後，請選擇您的虛擬私人雲端。在「篩選」中選擇「拒絕」或「全部」

[EC2.7] 應啟用 EBS 預設加密

相關要求：獨聯體 AWS 基礎基準測試 (1.4.0/2.2.1)、Nist.800-53.R5 鈣 -9 (1)、Ni.800-53.R5 (1)、電腦 -53.R5 (5)、NIS.800-53.R5 SC-28 (1)、SC-13 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`ec2-ebs-encryption-by-default`

排程類型：定期

參數：無

此控制項會檢查 Amazon 彈性區塊存放區 (Amazon EBS) 預設是否啟用帳戶層級加密。如果未啟用帳戶層級加密，則控制項會失敗。

當您的帳戶啟用加密時，Amazon EBS 磁碟區和快照複本會在靜態時加密。這為您的資料增加了一層額外的保護。如需詳細資訊，請參閱適用於《Amazon EC2 Linux 執行個體使用者指南》中的預設加密。

請注意，下列執行個體類型不支援加密：R1、C1 和 M1。

修補

若要設定 Amazon EBS 磁碟區的預設加密，請參閱 Amazon EC2 執行個體使用者指南中的預設加密。

[EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)

相關要求：交流 -3、尼什八達交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、交流 -6

分類:保護 > 網絡安全

嚴重性：高

資源類型：`AWS::EC2::Instance`

AWS Config 規則：`ec2-imdsv2-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 執行個體中繼資料版本是否設定為執行個體中繼資料服務版本 2 (IMDSv2)。如果`HttpTokens`設定為 IMDSv2 的必要項目，則會通過控制項。如果設定為，`HttpTokens`則控制項會失敗`optional`。

您可以使用執行個體中繼資料來設定或管理執行中的執行 IMDS 可讓您存取臨時且經常輪換的認證。這些認證不需要手動或以程式設計方式將機密認證散佈至執行個體。IMDS 會在本機連接至每個 EC2 執行個體。它運行在一個特殊的「本地鏈接」IP 地址 169.254.169.254。只有在執行個體上執行的軟體才能存取此 IP 位址。

IMDS 的第 2 版為以下類型的漏洞添加了新的保護。這些弱點可用來嘗試存取 IMDS。

- 開啟網站應用防火牆
- 开放式反向代理
- 伺服器端要求偽造 (SSRF) 漏洞
- 開放第 3 層防火牆和網路位址轉譯 (NAT)

Security Hub 建議您使用 ImDSv2 設定 EC2 執行個體。

修補

若要使用 IMDSv2 設定 EC2 執行個體，請參閱 Amazon EC2 執行個體使用者指南中的需要 IMDSv2 的建議路徑。

[EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網絡配置 > 公共 IP 地址

嚴重性：高

資源類型：`AWS::EC2::Instance`

AWS Config 規則：`ec2-instance-no-public-ip`

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 執行個體是否擁有公用 IP 位址。如果該`publicIp`字段存在於 EC2 實例配置項中，則控制失敗。此控制項僅適用於 IPv4 位址。

公用 IPv4 位址是可從網際網路存取的 IP 位址。如果您使用公有 IP 地址啟動執行個體，則可以從網際網路存取 EC2 執行個體。私人 IPv4 位址是無法從網際網路存取的 IP 位址。您可以使用私有 IPv4 地址在相同 VPC 或連接的私有網路中的 EC2 執行個體之間進行通訊。

IPv6 位址是全域唯一的，因此可從網際網路存取。不過，依預設，所有子網路的 IPv6 定址屬性都設定為 false。如需 IPv6 的詳細資訊，請參閱 Amazon VPC 擬私人雲端使用者指南中的 VPC 中的 IP 定址。

如果您有合法的使用案例來維護具有公有 IP 地址的 EC2 執行個體，則可以從此控制項中隱藏發現結果。如需前端架構選項的詳細資訊，請參閱AWS 架構部落格或這是我的架構系列。

修補

使用非預設 VPC，預設情況下不會為您的執行個體指派公用 IP 位址。

當您將 EC2 執行個體啟動至預設 VPC 時，系統會為其指派公用 IP 位址。將 EC2 執行個體啟動至非預設 VPC 時，子網路組態會決定其是否接收公有 IP 位址。子網路具有用於判斷子網路中的新 EC2 執行個體是否從公用 IPv4 位址集區接收公用 IP 位址的屬性。

您無法手動將自動指派的公用 IP 地址與 EC2 執行個體建立關聯或取消關聯。若要控制 EC2 執行個體是否接收公有 IP 位址，請執行下列其中一個動作：

- 修改子網路的公用 IP 位址屬性。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的修改子網的公有 IPv4 定址屬性。
- 在啟動期間啟用或停用公用 IP 定址功能。這會覆寫子網路的公用 IP 位址屬性。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的執行個體啟動期間指派公用 IPv4 地址。

如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon EC2 使用者指南》中的「公有 IPv4 地址和外部 DNS 主機名稱」。

如果您的 EC2 執行個體與彈性 IP 地址相關聯，則可以從網際網路存取您的 EC2 執行個體。您可以隨時解除彈性 IP 地址與執行個體或網路介面的關聯。若要取消彈性 IP 地址的關聯，請參閱 Amazon EC2 Linux 執行個體使用者指南中的取消彈性 IP 地址的關聯。

[EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、奈特 -800-53.R5 交流 4、NIST-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七星 (16), 日本七點七 (20), 日本七星期七 (21), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3)

分類:保護 > 安全網絡配置 > API 私有訪問

嚴重性：中

資源類型：`AWS::EC2::VPC`

AWS Config 規則：`service-vpc-endpoint-enabled`

排程類型：定期

參數：

- `serviceName`：`ec2`（不可定制）

此控制項可檢查是否為每個 VPC 建立 Amazon EC2 的服務端點。如果虛擬私人雲端沒有為 Amazon EC2 服務建立的 VPC 端點，則控制項會失敗。

此控制項會評估單一帳號中的資源。它無法描述帳號之外的資源。由 AWS Config 於 Security Hub 不會執行跨帳戶檢查，因此您會看到跨帳戶共用的 VPC `FAILED` 發現項目。Security Hub 建議您隱藏這些`FAILED`發現項目。

若要改善 VPC 的安全狀態，您可以將 Amazon EC2 設定為使用界面 VPC 端點。界面端點採用這種技術 AWS PrivateLink，可讓您私下存取 Amazon EC2 API 操作。它將 VPC 和 Amazon EC2 之間的所有網路流量限制到 Amazon 網路。由於僅在相同區域內支援端點，因此您無法在 VPC 和不同區域中的服務之間建立端點。這樣可以防止意外的 Amazon EC2 API 呼叫其他區域。

若要進一步了解如何為 Amazon EC2 建立 VPC 端點，請參閱 Amazon EC2 和 Linux 執行個體使用者指南中的 Amazon EC2 使用者指南中的介面 VPC 人雲端節點。

修補

若要從 Amazon VPC 主控台建立與 Amazon EC2 的界面端點，請參閱指南中的建立 VPC 端點。AWS PrivateLink 對於「服務名稱」，請選擇「喜好」。 ## .ec2。

您也可以建立端點政策並將其連接到 VPC 端點，以控制對 Amazon EC2 API 的存取。如需建立 VPC 端點政策的指示，請參閱 Amazon EC2 Linux 執行個體使用者指南中的建立端點政策。

[EC2.12] 應移除未使用的 Amazon EC2 EIP

相關需求：PCI 直接安全防護系統 V3.2.1/2.4、N.800-53.R5 CM-8 (1)

類別：保護 > 安全網路組態

嚴重性：低

資源類型：`AWS::EC2::EIP`

AWS Config 規則：`eip-attached`

排程類型：已觸發變更

參數：無

此控制項可檢查分配給 VPC 的彈性 IP (EIP) 地址是否連接至 EC2 執行個體或使用中的彈性網路界面 (ENI)。

發現失敗表示您可能有未使用的 EC2 EIP。

這將幫助您在持卡人數據環境（CDE）中維護 EIP 的準確資產庫存。

若要發行未使用的 EIP，請參閱 Amazon EC2 執行個體使用者指南中的釋放彈性 IP 地址。

[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入

相關要求：獨聯體 AWS 基礎基準測試 v1.2.0/4.1，PCI DSS V3.2.1/1.2.1，PCI DSS V3.2.1/1.3.1，PCI DSS V3.2.1/2.2.2，指示燈 -53.R5 交流 4，指標 -800-53.R5 交流 -4（21），(11), 早上七點七 (16), 日本七點七 (21), 西元七七 (21), 早上七點七 (4), 早上七點七 (5)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：restricted-ssh

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EC2 安全群組是否允許從 0.0.0/0 或:/0 到連接埠 22 的輸入。如果安全性群組允許從 0.0.0.0/0 或:: /0 輸入至連接埠 22，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。不建議安全群組允許連接埠 22 不受限制的輸入存取。移除與遠端主控台服務 (如 SSH) 的不受限連線能力可降低伺服器暴露在風險中的機會。

修補

若要禁止輸入連接埠 22，請移除允許與 VPC 相關聯之每個安全性群組進行此類存取的規則。如需指示，請參閱 Amazon VPC 使用者指南中的更新安全群組規則。在 Amazon VPC 主控台中選取安全群組後，選擇動作 > 編輯輸入規則。移除允許存取通訊埠 22 的規則。

[EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389

相關要求：獨聯體 AWS 基金會基準 v1.2.0/4.2

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則:**restricted-common-ports**(建立的規則為restricted-rdp)

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EC2 安全群組是否允許從 0.0.0/0 或:/0 到連接埠 3389 的輸入。如果安全性群組允許從 0.0.0/0 或:: /0 輸入至連接埠 3389，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。不建議安全群組允許連接埠 3389 不受限制的輸入存取。移除與遠端主控台服務 (如 RDP) 的不受限連線能力可降低伺服器暴露在風險中的機會。

修補

若要禁止輸入連接埠 3389，請移除允許與 VPC 相關聯之每個安全性群組進行此類存取的規則。如需指示，請參閱 Amazon VPC 使用者指南中的更新安全群組規則。在 Amazon VPC 主控台中選取安全群組後，選擇動作 > 編輯輸入規則。移除允許存取通訊埠 3389 的規則。

[EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 網絡安全

嚴重性：中

資源類型：`AWS::EC2::Subnet`

AWS Config 規則：`subnet-auto-assign-public-ip-disabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon 虛擬私有雲端 (Amazon VPC) 子網路中的公有 IP 指派是否已`MapPublicIpOnLaunch`設定為。`FALSE`如果旗標設定為，則控制項會通過`FALSE`。

所有子網路都有一個屬性，可決定在子網路中建立的網路介面是否自動接收公用 IPv4 位址。啟動至啟用此屬性之子網路的執行個體，會將公用 IP 位址指派給其主要網路介面。

修補

若要將子網路設定為不指派公有 IP 位址，請參閱 Amazon VPC 使用者指南中的修改子網路的公用 IPv4 定址屬性。清除 [啟用自動指派公用 IPv4 位址] 核取方塊。

[EC2.16] 應移除未使用的網路存取控制清單

相關需求：第八方厘米 8 (1)

分類:防範 > 網絡安全

嚴重性：低

資源類型：`AWS::EC2::NetworkAcl`

AWS Config 規則：vpc-network-acl-unused-check

排程類型：已觸發變更

參數：無

此控制項會檢查是否有任何未使用的網路存取控制清單 (ACL)。

控制項會檢查資源的項目組態，AWS::EC2::NetworkAcl並決定網路 ACL 的關係。

如果唯一的關係是網路 ACL 的 VPC，則控制項會失敗。

如果列出了其他關係，則會通過控制。

修補

如需有關刪除未使用網路 ACL 的指示，請參閱 Amazon VPC 使用者指南中的刪除網路 ACL。您無法刪除預設網路 ACL 或與子網路相關聯的 ACL。

[EC2.17] Amazon EC2 執行個體不應使用多個 ENI

相關要求：交流 -4 (21)

网络安全

嚴重性：低

資源類型：AWS::EC2::Instance

AWS Config 規則：ec2-instance-multiple-eni-check

排程類型：已觸發變更

參數：

- Adapterids— 連接到 EC2 執行個體的網路介面 ID 清單 (不可自訂)

此控制項會檢查 EC2 執行個體是否使用多個彈性網路介面 (ENI) 或彈性網狀架構介面卡 (EFA)。如果使用單一網路介面卡，則此控制項會通過。控制項包括可選參數清單，以識別允許的 ENI。如果屬於 Amazon EKS 叢集的 EC2 執行個體使用多個 ENI，則此控制也會失敗。如果 EC2 執行個體需要有多個 ENI 做為 Amazon EKS 叢集的一部分，您可以隱藏這些控制發現項目。

多個 ENI 可能會導致雙重主目錄執行個體，表示具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。

修補

若要從 EC2 執行個體分離網路界面，請參閱 Amazon EC2 Linux 執行個體使用者指南中的將網路界面與執行個體分離。

[EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量

相關要求：交流 4、交流電 -4、交流 -4 (21)、尼斯特。800-53.R5 的 SC-7、星期五、七、七、五、七、七、四、七 (4)、SC-7 (5)

分類:保護 > 安全網絡配置 > 安全組配置

嚴重性：高

資源類型：`AWS::EC2::SecurityGroup`

AWS Config 規則：`vpc-sg-open-only-to-authorized-ports`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`authorizedTcpPorts`	授權 TCP 連接埠列表	IntegerList（最多 32 個項目）	1 設定為 65535	`[80,443]`
`authorizedUdpPorts`	授權的 UDP 連接埠清單	IntegerList（最多 32 個項目）	1 設定為 65535	無預設值

此控制項可檢查 Amazon EC2 安全群組是否允許來自未授權連接埠的不受限制的傳入流量。控制狀態的確定方式如下：

- 如果您使用的預設值`authorizedTcpPorts`，如果安全群組允許來自通訊埠 80 和 443 以外的任何連接埠的未限制傳入流量，則控制項會失敗。
- 如果您為`authorizedTcpPorts`或提供自訂值`authorizedUdpPorts`，如果安全性群組允許來自任何未列出連接埠的不受限制的傳入流量，則控制項會失敗。

- 如果未使用任何參數，則任何具有不受限制輸入流量規則的安全性群組的控制項都會失敗。

安全群組提供輸入和輸出網路流量的狀態篩選。 AWS安全性群組規則應遵循最低權限存取的主體。不受限制的存取 (IP 位址加上 /0 尾碼) 可增加遭受惡意活動 (例如駭客入侵、 denial-of-service 攻擊和資料遺失) 的機會。除非特別允許連接埠，否則連接埠應拒絕不受限制的存取。

修補

若要修改安全群組，請參閱 Amazon VPC 使用者指南中的使用安全群組。

[EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠

相關要求：交流 4、尼斯 800-53.R5 交流電 -4 (21)、奈特．11), 早上七點七 (16), 日本七點七 (21), 日本七點七 (21), 日本七點七 (4), 日本七點七 (5)

類別:保護 > 受限制的網絡訪問

嚴重性：嚴重

資源類型：`AWS::EC2::SecurityGroup`

AWS Config 規則:**`restricted-common-ports`**(建立的規則為`vpc-sg-restricted-common-ports`)

排程類型：已觸發變更

參數：`"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560`可定制）

此控制項可檢查 Amazon EC2 安全群組的不受限制傳入流量是否可供視為高風險的指定連接埠存取。如果安全性群組中的任何規則允許從「0.0.0.0/0」或「:: /0」到這些連接埠的輸入流量，則此控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。不受限制的訪問（0.0.0.0/0）增加了惡意活動的機會，例如黑客 denial-of-service 攻擊，攻擊和數據丟失。任何安全性群組都不應允許不受限制的輸入存取下列連接埠：

- 20、21 (FTP 服務器)
- 22 (SSH)
- 23（遠程電話）

- 25 (SMTP)
- 流行三角
- RPC 135 (端子)
- 143 (地圖)
- 445 (西夫斯)
- 1433, 1434 (少女 SQL)
- 3000（圍棋，Node.js 和紅寶石網頁開發框架）
- 三 306 (MySQL)
- 3389 (RDP)
- 4333 (阿赫普)
- 网页 Python 发框架
- 5432 (后格雷斯利亚州)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch 控制面板)
- 代理伺服器
- 8088 (舊版 HTTP 連接埠)
- 8888 (替代連接埠)
- 九二百或九三百 OpenSearch

修補

若要從安全群組刪除規則，請參閱 Amazon EC2 Linux 執行個體使用者指南中的從安全群組刪除規則。

[EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原力 > 復原 > 高可用性

嚴重性：中

資源類型：`AWS::EC2::VPNConnection`

AWS Config 規則：`vpc-vpn-2-tunnels-up`

排程類型：已觸發變更

參數：無

VPN 通道是一種加密連結，其中資料可以從客戶網路傳送至站台對站台 VPN 連線，或從 AWS 網 AWS 站間傳送。每個 VPN 連接包含兩個 VPN 通道，您可以同時使用這些通道以獲得高可用性。確保兩個 VPN 通道都已啟動以進行 VPN 連線，對於確認 AWS VPC 與遠端網路之間的安全且高可用性連線非常重要。

此控制項會檢查 AWS Site-to-Site VPN 提供的兩個 VPN 通道是否處於「啟用」狀態。如果一個或兩個通道都處於「關閉」狀態，則控制會失敗。

修補

若要修改 VPN 通道選項，請參閱〈Site-to-Site VPN 使用者指南〉中的〈修改 AWS Site-to-Site VPN 通道選項〉。

[EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389

相關要求：獨聯體 AWS 基礎基準測試版 1.4.0/5.1，指定交流 -4（21），Nist.800-53.R5 CA-9（1），Nist.800-53.R5 厘米 -2，指定線 5 厘米 -2（2），), 早上五月七日 (5)

分類:保護 > 安全網絡配置

嚴重性：中

資源類型：`AWS::EC2::NetworkAcl`

AWS Config 規則：`nacl-no-unrestricted-ssh-rdp`

排程類型：已觸發變更

參數：無

此控制項會檢查網路存取控制清單 (NACL) 是否允許不受限制地存取 SSH/RDP 輸入流量的預設 TCP 連接埠。如果 NACL 輸入項目允許對 TCP 連接埠 22 或 3389 使用 '0.0.0.0/0' 或 ':: /0' 的來源 CIDR 區塊，則規則會失敗。

對遠端伺服器管理連接埠的存取，例如連接埠 22 (SSH) 和連接埠 3389 (RDP)，不應該可公開存取，因為這可能會允許非預期存取 VPC 中的資源。

修補

如需 NACL 的詳細資訊，請參閱《VPC 使用者指南》中的〈網路 ACL〉。

[EC2.22] 應移除未使用的 Amazon EC2 安全群組

> **Important**
>
> 從特定標準淘汰 — Security Hub 於 2023 年 9 月 20 日從 AWS 基礎安全性最佳做法標準和 NIST SP 800-53 版本 5 中移除了此控制項。此控制項仍然是服務管理標準的一部分： AWS Control Tower。如果安全群組連接至 EC2 執行個體或 elastic network interface，此控制項會產生傳遞的發現。但是，對於某些使用案例，未連接的安全性群組不會造成安全性風險。您可以使用其他 EC2 控制項 (例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19) 來監控您的安全群組。

類別：識別 > 清查

嚴重性：中

資源類型:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config 規則：`ec2-security-group-attached-to-eni-periodic`

排程類型：定期

參數：無

此 AWS 控制項可檢查安全群組是否連接至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 elastic network interface。如果安全群組與 Amazon EC2 執行個體或 elastic network interface 沒有關聯，則控制將失敗。

修補

若要建立、指派和刪除安全群組，請參閱 Amazon EC2 使用者指南中的安全群組。

[EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求

相關要求：交流 -4 (21)、鎳碳酸鈣 -9 (1)、奈特 .

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::EC2::TransitGateway`

AWS Config 規則：ec2-transit-gateway-auto-vpc-attach-disabled

排程類型：已觸發變更

參數：無

此控制項可檢查 EC2 傳輸閘道是否自動接受共用 VPC 附件。對於自動接受共用 VPC 附件要求的傳輸閘道，此控制項會失敗。

開啟可將傳輸閘道AutoAcceptSharedAttachments設定為自動接受任何跨帳戶 VPC 附件要求，而無需驗證要求或附件來源的帳戶。為了遵循授權和驗證的最佳做法，我們建議關閉此功能，以確保僅接受授權的 VPC 附件請求。

修補

若要修改傳輸閘道，請參閱 Amazon VPC 開發人員指南中的修改傳輸閘道。

[EC2.24] 不應使用 Amazon EC2 半虛擬實例類型

相關需求：第五代公分 (2)

類別:識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::EC2::Instance

AWS Config 規則：ec2-paravirtual-instance-check

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 執行個體的虛擬化類型是否為半虛擬化。如果 EC2 執行個體virtualizationType的設定為，則控制會失敗paravirtual。

Linux Amazon 機器映像 (AMI) 使用兩種虛擬化類型之一：半虛擬化 (PV) 或硬體虛擬機器 (HVM)。PV 和 HVM AMI 之間的主要區別在於開機的方式以及是否可以利用特殊的硬體延伸 (CPU、網路和儲存) 來獲得更好的效能。

歷史上，在許多情況下，PV 訪客比 HVM 訪客具有更好的效能，但由於 HVM 虛擬化中的增強以及 HVM AMI 之 PV 驅動程式的可用性，這已不再成立。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的 Linux AMI 虛擬化類型。

修補

若要將 EC2 執行個體更新為新的執行個體類型，請參閱 Amazon EC2 Linux 執行個體使用者指南中的變更執行個體類型。

[EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網路設定 > 無法公開存取的資源

嚴重性：高

資源類型：`AWS::EC2::LaunchTemplate`

AWS Config 規則：`ec2-launch-template-public-ip-disabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EC2 啟動範本是否設定為在啟動時將公用 IP 地址指派給網路界面。如果 EC2 啟動範本設定為將公用 IP 位址指派給網路介面，或者至少有一個網路介面具有公用 IP 位址，則控制項會失敗。

公共 IP 地址是可以從互聯網訪問的地址。如果您使用公用 IP 位址設定網路介面，則可以從網際網路存取與這些網路介面相關聯的資源。EC2 資源不應可公開存取，因為這可能允許非預期存取您的工作負載。

修補

若要更新 EC2 啟動範本，請參閱 Amazon EC2 Auto Scaling 使用者指南中的變更預設網路界面設定。

[EC2.28] 備份計劃應涵蓋 EBS 磁碟區

類別:復原 > 復原 > 啟用備份

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

嚴重性：低

資源類型：AWS::EC2::Volume

AWS Config 規則：**ebs-resources-protected-by-backup-plan**

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
backupVaultLockCheck	如果參數設定為true且資源使用「文件 AWS Backup 庫鎖定」，則控制項會產生PASSED發現結果。	Boolean	true 或 false *	無預設值

此控制項會評估in-use狀態中的 Amazon EBS 磁碟區是否涵蓋在備份計劃中。如果備份計劃未涵蓋 EBS 磁碟區，則控制項會失敗。如果您將backupVaultLockCheck參數設定為等於true，則僅當 EBS 磁碟區在 AWS Backup 鎖定的資料保險箱中備份時，控制項才會通過。

備份可協助您更快速地從安全性事件中復原。它們還可以增強系統的彈性。在備份計劃中包含 Amazon EBS 磁碟區，可協助您保護資料免於意外遺失或刪除。

修補

若要將 Amazon EBS 磁碟區新增至 AWS Backup 備份計劃，請參閱AWS Backup 開發人員指南中的將資源指派給備份計劃。

[EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄

相關要求：交流 -53.R5 (12)、交流電 -2 (4)、奈特。800-53.R5 交流 -6 (9)、尼斯特。800-53.R5 交流 -6 (9)、黑色 -53.R5、AU-10、六月五日 (3), 尼斯 .800-53.R5 (4), 日本 6 星期六 (4), 尼斯 .800-53.R5 (7), 尼斯 .800-53.R5 SC-7 (9), 尼斯 .800-53.R5 (9),), 尼斯 .800-53.R5 四七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::EC2::ClientVpnEndpoint

AWS Config 規則：**ec2-client-vpn-connection-log-enabled**

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Client VPN 端點是否已啟用用戶端連線記錄。如果端點未啟用用戶端連線記錄，則控制項會失敗。

客戶 Client VPN 端點允許遠程客戶端安全地連接到中的 Virtual Private Cloud (VPC)（VPC）中 AWS 的資源。連線記錄可讓您追蹤 VPN 端點上的使用者活動，並提供可見度。啟用連線日誌記錄時，您可以在日誌群組中指定日誌串流的名稱。如果您未指定記錄串流，Client VPN 服務會為您建立一個記錄串流。

修補

若要啟用連線記錄，請參閱《AWS Client VPN 管理手冊》中的「啟用現有 Client VPN 端點的連線記錄」。

Amazon EC2 Auto Scaling 控制

這些控制項與 Amazon EC2 Auto Scaling 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查

相關要求：PCI DSS V3.2.1/2.2、Ni.800-53.R5 CA-7、NIT.800-53.R5 CP-2 (2)、日期：800-53.R5 SI-2

類別：識別 > 清查

嚴重性：低

資源類型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 規則：`autoscaling-group-elb-healthcheck-required`

排程類型：已觸發變更

參數：無

此控制項會檢查與 Classic Load Balancer 相關聯的 Auto Scaling 群組是否正在使用 Elastic Load Balancing 健康狀態檢查。

這可確保群組可根據負載平衡器提供的其他測試，藉此確定執行個體的運作狀態。使用 Elastic Load Balancing 運作狀態檢查可協助支援使用 EC2 Auto Scaling 群組之應用程式的可用性。

修補

若要新增 Elastic Load Balancing 運作狀態檢查，請參閱 Amazon EC2 Auto Scaling 使用者指南中的新增 Elastic Load Balancing 運作狀態檢查。

[AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域

相關要求：指定的 CP-10，電腦 -53.R5 CP-2 (2)，指定的指令介面卡 -6 (2)，指定項目：800-53.R5 SC-5 (2)，筆記型號 800-53.R5（2），指定型號 800-53.R5 SI-13 (5) SC-36

分類:復原 > 復原力 > 高可用性

嚴重性：中

資源類型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 規則：`autoscaling-multiple-az`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`minAvailabilityZones`	可用區域的最小數目	列舉	`2, 3, 4, 5, 6`	`2`	

此控制項可檢查 Amazon EC2 Auto Scaling 群組是否至少跨越指定數量的可用區域 (AZ)。如果「Auto Scaling」群組至少沒有跨越指定數目的 AZ，則控制項會失敗。除非您為最小 AZ 數目提供自訂參數值，否則 Security Hub 會使用兩個 AZ 的預設值。

不跨越多個 AZ 的 Auto Scaling 群組無法在另一個 AZ 中啟動執行個體，以便在設定的單一 AZ 無法使用時進行補償。不過，在某些使用案例 (例如批次作業) 或需要將 AZ 間傳輸成本維持在最低的情況下，可能會偏好使用具有單一可用區域的 Auto Scaling 群組。在這種情況下，您可以停用此控制項或隱藏其發現項目。

修補

若要將 AZ 新增至現有的 Auto Scaling 群組，請參閱 Amazon EC2 Auto Scaling 展使用者指南中的新增和移除可用區域。

[AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）

相關要求：交流 -3、交流 -3、交流 -3 (15)、奈特 .

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 規則：`autoscaling-launchconfig-requires-imdsv2`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EC2 自動擴展群組啟動的所有執行個體是否已啟用 IMDSv2。如果執行個體中繼資料服務 (IMDS) 版本未包含在啟動組態中，或者同時啟用了 IMDSv1 和 IMDSv2，則控制項會失敗。

IMDS 提供執行個體的相關資料，讓您用來設定或管理執行中的執行個體。

IMDS 的第 2 版新增了 IMDSv1 中沒有的新保護，以進一步保護您的 EC2 執行個體。

修補

「Auto Scaling」群組一次與一個啟動組態相關聯。您無法在建立啟動組態之後修改啟動組態。若要變更 Auto Scaling 群組的啟動組態，請使用現有的啟動組態做為啟用 IMDSv2 的新啟動組態的基礎。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的設定新執行個體的執行個體中繼資料選項。

[AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 規則：`autoscaling-launch-config-hop-limit`

排程類型：已觸發變更

參數：無

此控制項會檢查中繼資料 Token 可以移動的網路躍點數目。如果中繼資料回應躍點限制大於，則控制項會失敗1。

執行個體中繼資料服務 (IMDS) 提供 Amazon EC2 執行個體的中繼資料資訊，對於應用程式組態非常有用。將中繼資料服務的 HTTP PUT 回應限制為僅 EC2 執行個體，可保護 IMDS 免於未經授權的使用。

IP 封包中的存留時間 (TTL) 欄位會在每個躍點上減少一個。此減少可用於確保封包不會在 EC2 之外傳輸。IMDSv2 可保護可能錯誤設定為開放路由器、第 3 層防火牆、VPN、通道或 NAT 裝置的 EC2 執行個體，防止未經授權的使用者擷取中繼資料。使用 IMDSv2 時，包含秘密權杖的PUT回應無法在執行個體之外傳輸，因為預設中繼資料回應躍點限制已設定為。1但是，如果此值大於1，則令牌可以離開 EC2 實例。

修補

若要修改現有啟動組態的中繼資料回應躍點限制，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的修改現有執行個體的執行個體中繼資料選項。

[自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::AutoScaling::LaunchConfiguration`

AWS Config 規則：`autoscaling-launch-config-public-ip-disabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Auto Scaling 群組關聯的啟動設定是否會將公用 IP 位址指派給群組的執行個體。如果關聯的啟動組態指派公用 IP 位址，則控制項會失敗。

Auto Scaling 群組啟動組態中的 Amazon EC2 執行個體不應具有關聯的公有 IP 地址，但在有限的節點情況下除外。Amazon EC2 執行個體應該只能從負載平衡器後方存取，而不是直接暴露在網際網路上。

修補

「Auto Scaling」群組一次與一個啟動組態相關聯。您無法在建立啟動組態之後修改啟動組態。若要變更 Auto Scaling 群組的啟動組態，請使用現有啟動組態作為新啟動組態的基礎。然後更新 Auto Scaling 群組，以便使用新啟動組態。如需 step-by-step 指示，請參閱 Amazon EC2 Auto Scaling 使用者指南中的變更自動擴展群組的啟動組態。建立新的啟動設定時，在 [其他設定] 下，對於 [進階詳細資料] 的 [IP 位址類型]，請選擇 [不要將公用 IP 位址指派給任何執行個體]。

變更啟動組態後，Auto Scaling 會以新的組態選項啟動新執行個體。現有的執行個體不受影響。若要更新現有的執行個體，建議您重新整理執行個體，或允許自動調度資源，依據終止政策，逐漸將較舊的執行個體取代為較新的執行個體。如需更新 Auto Scaling 執行個體的詳細資訊，請參閱 Amazon EC2 Auto Scaling 使用者指南中的更新 Auto Scaling 執行個體。

[AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型

相關要求：指定的 CP-10，電腦 -53.R5 CP-2 (2)，指定的指令介面卡 -6 (2)，指定項目：800-53.R5 SC-5 (2)，筆記型號 800-53.R5（2），指定型號 800-53.R5 SI-13 (5) SC-36

分類:復原 > 復原力 > 高可用性

嚴重性：中

資源類型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 規則：`autoscaling-multiple-instance-types`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EC2 Auto Scaling 群組是否使用多種執行個體類型。如果「Auto Scaling 例」群組只定義了一個例證類型，則控制項會失敗。

您可以將應用程式部署於在多個可用區域執行的多種執行個體類型之間，以增強可用性。Security Hub 建議您使用多個執行個體類型，以便在選擇的可用區域中執行個體容量不足時，Auto Scaling 群組可以啟動其他執行個體類型。

修補

若要建立具有多個執行個體類型的 Auto Scal ing 群組，請參閱 Amazon EC2 Auto Scaling 使用者指南中的具有多個執行個體類型的 Auto Scaling 群組和購買選項。

[AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::AutoScaling::AutoScalingGroup`

AWS Config 規則：`autoscaling-launch-template`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EC2 Auto Scaling 群組是否從 EC2 啟動範本建立。如果未使用啟動範本建立 Amazon EC2 Auto Scaling 群組，或者未在混合執行個體政策中指定啟動範本，則此控制會失敗。

您可以從 EC2 啟動範本或啟動組態建立 EC2 Auto Scaling 群組。不過，使用啟動範本建立 Auto Scaling 群組可確保您可以存取最新的功能和改進項目。

修補

若要使用 EC2 啟動範本建立自動擴展群組，請參閱 Amazon EC2 Auto Scaling 使用者指南中的使用啟動範本建立 Auto Scaling 群組。如需有關如何以啟動範本取代啟動組態的詳細資訊，請參閱 Amazon EC2 Windows 執行個體使用者指南中的以啟動範本取代啟動組態。

Amazon EC2 Systems Manager 控制

這些控制項與由管理的 Amazon EC2 執行個體相關 AWS Systems Manager。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager

相關要求：PCI DSS V3.2.1/2.4、電子顯示卡 -9 (1)、介面卡 -9 (1)、NIT.800-53.R5 厘米 -2 (2)、指定訊號 -53.R5 公分 (8)、Ni.800-53.R5 公分 (8)、5 厘米至 8 (3), 日本電腦 -800-53.R5 SA-15 (2), 尼斯. 800-53.R5 (8), 奈特. 800-53.R5 SI-2 (3) SA-15

類別：識別 > 清查

嚴重性：中

評估的資源：`AWS::EC2::Instance`

所需的 AWS Config 錄製資
源：`AWS::EC2::Instance`，`AWS::SSM::ManagedInstanceInventory`

AWS Config 規則：`ec2-instance-managed-by-systems-manager`

排程類型：已觸發變更

參數：無

此控制項會檢查帳戶中已停止和執行中的 EC2 執行個體是否由管理 AWS Systems Manager。Systems Manager 是 AWS 服務 您可以用來檢視和控制您的 AWS 基礎結構。

為了協助您維護安全性與合規性，Systems Manager 會掃描已停止和執行中的代管執行個體。代管執行個體是設定為搭配 Systems Manager 使用的機器。然後，Systems Manager 會針對偵測到的任何原則違規，報告或採取更正動作。Systems Manager 也可協助您設定和維護您的代管執行個體。

若要深入瞭解，請參閱AWS Systems Manager 使用者指南。

修補

若要使用系統管理員管理 EC2 執行個體，請參閱AWS Systems Manager 使用者指南中的 Amazon EC2 主機管理。在「組態選項」區段中，您可以保留預設選擇，或視需要變更偏好的組態。

[SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」

相關要求：PCI DSS v3.2.1/6.2、電子信息系統 (800) -53.R5 (3)、介質管理系統 (3)、介質管理系統 (2)、等級 800-53.R5 系統 -2 (3)、等級

類別：偵測 > 偵測服務

嚴重性：高

資源類型：`AWS::SSM::PatchCompliance`

AWS Config 規則：`ec2-managedinstance-patch-compliance-status-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Systems Manager 修補程式符合性的符合性狀態，`COMPLIANT`或是在執行個體上安裝修補程式`NON_COMPLIANT`之後。如果符合性狀態為，則控制項會失敗`NON_COMPLIANT`。控制項只會檢查由系統管理員修補程式管理員所管理的執行個體。

根據組織的要求修補 EC2 執行個體，可減少 AWS 帳戶.

修補

Systems Manager 建議您使用修補程式原則來設定受管理執行個體的修補 您也可以使用 Systems Manager 文件 (如下列程序所述) 來修補執行個體。

修補不相容的修補程式

1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/
2. 在 [節點管理] 中，選擇 [執行命令]，然後選擇 [執行命令]。
3. 選擇 AWS- 的選項RunPatchBaseline。
4. 將 Operation (操作) 變更為 Install (安裝)。
5. 選擇「手動選擇執行個體」，然後選擇不相容的執行個體。
6. 選擇執行。
7. 命令完成後，若要監視已修補執行個體的新符合性狀態，請在導覽窗格中選擇 [規範遵循]。

[SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態

相關要求：PCI DSS V3.2.1/2.4、介面卡 -9 (1)、介面卡 -9 (1)、介面卡 -8 (2)、Ni.800-53.R5 厘米 -2 (2)、指定訊號 -53.R5 公分 (8)、鎳 5 四二 (3)

類別：偵測 > 偵測服務

嚴重性：低

資源類型：`AWS::SSM::AssociationCompliance`

AWS Config 規則：ec2-managedinstance-association-compliance-status-check

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Systems Manager 關聯符合性的狀態，`COMPLIANT`或是在執行個體上執行關聯`NON_COMPLIANT`之後。如果關聯符合性狀態為，則控制項會失敗`NON_COMPLIANT`。

狀態管理器關聯是指派給您的代管執行個體的組態。該組態會定義您想在執行個體上維持的狀態。例如，關聯可以指定必須在執行個體上安裝並執行防毒軟體，或者必須關閉特定連接埠。

建立一或多個 State Manager 關聯之後，規範遵循狀態資訊即可供您使用。您可以在主控台中檢視符合性狀態，或是回應 AWS CLI 指令或對應的 Systems Manager API 動作。對於關聯，「組態符合性」會顯示符合性狀態 (`Compliant`或`Non-compliant`)。它也會顯示指派給關聯的嚴重性層級，例如`Critical`或`Medium`。

若要進一步瞭解州政府管理員關聯規範遵循，請參閱AWS Systems Manager 使用者指南中的關於 State Manager 關聯規範遵循

修補

失敗的關聯可能與不同的項目有關，包括目標和 SSM 文件名稱。若要修正此問題，您必須先透過檢視關聯歷史記錄來識別並調查關聯。如需檢視關聯歷史記錄的指示，請參閱《AWS Systems Manager 使用指南》中的檢視關聯歷史記錄。

調查之後，您可以編輯關聯以更正識別的問題。您可以編輯關聯來指定新的名稱、排程、嚴重性層級或目標。編輯關聯後，會 AWS Systems Manager 建立新版本。若要取得有關編輯關聯的指示，請參閱《使用指南》中的〈編輯和建立新版本的關聯AWS Systems Manager〉。

[SSM.4] SSM 文件不應該是公開的

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網路設定 > 無法公開存取的資源

嚴重性：嚴重

資源類型：`AWS::SSM::Document`

AWS Config 規則：`ssm-document-not-public`

排程類型：定期

參數：無

此控制項會檢查帳戶所擁有的 AWS Systems Manager 文件是否為公開。如果具有擁有者的 SSM 文件`Self`是公開的，則此控制項會失敗。

公開的 SSM 文件可能會允許意外存取您的文件。公用 SSM 文件可能會公開有關您的帳戶、資源和內部程序的重要資訊。

除非您的使用案例需要公開共用，否則我們建議您針對擁有的 Systems Manager 文件封鎖公開共用設定`Self`。

修補

若要封鎖 SSM 文件的公開共用，請參閱《使用者指南》中的「封鎖 SSM 文件的公開共AWS Systems Manager 用」。

Amazon Elastic File System 控制

這些控制項與 Amazon EFS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：efs-encrypted-check

排程類型：定期

參數：無

此控制項會檢查 Amazon Elastic File System 是否設定為使用來加密檔案資料 AWS KMS。檢查會在下列情況下失敗。

- Encrypted在DescribeFileSystems回應false中設定為。
- DescribeFileSystems回應中的KmsKeyId索引鍵與的KmsKeyId參數不符efs-encrypted-check。

請注意，此控制項不會使用的KmsKeyId參數efs-encrypted-check。其只會檢查 Encrypted 的值。

若要為 Amazon EFS 中的敏感資料增加一層安全性，您應該建立加密的檔案系統。Amazon EFS 支援靜態檔案系統的加密。您可以在建立 Amazon EFS 檔案系統時啟用靜態資料加密。若要進一步了解 Amazon EFS 加密，請參閱 Amazon 彈性檔案系統使用者指南中的 Amazon EFS 中的資料加密。

修補

如需如何加密新 Amazon EFS 檔案系統的詳細資訊，請參閱 Amazon Elastic File System 使用者指南中的加密靜態資料。

[EFS.2] Amazon EFS 磁碟區應該在備份計劃中

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

分類:復原 > 復原能力 > Backup

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：efs-in-backup-plan

排程類型：定期

參數：無

此控制項可檢查 Amazon Elastic File System (Amazon EFS) 檔案系統是否已新增至中的備份計劃 AWS Backup。如果備份計劃中未包含 Amazon EFS 檔案系統，則控制會失敗。

在備份計畫中包含 EFS 檔案系統可協助您保護資料免於遭到刪除和資料遺失。

修補

若要為現有 Amazon EFS 檔案系統啟用自動備份功能，請參閱開AWS Backup 發人員指南中的入門 4：建立 Amazon EFS 自動備份。

[EFS.3] EFS 存取點應強制執行根目錄

相關要求：交流 -6 (10)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::EFS::AccessPoint

AWS Config 規則：efs-access-point-enforce-root-directory

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EFS 存取點是否設定為強制執行根目錄。如果的值設定Path為 / (檔案系統的預設根目錄)，則控制項會失敗。

強制執行根目錄時，使用存取點的 NFS 用戶端會使用存取點上設定的根目錄，而不是檔案系統的根目錄。針對存取點強制執行根目錄，藉由確保存取點的使用者只能存取指定子目錄的檔案，有助於限制資料存取。

修補

如需有關如何強制執行 Amazon EFS 存取點根目錄的指示，請參閱 Amazon Elastic File System 使用者指南中的使用存取點強制執行根目錄。

[EFS.4] EFS 存取點應強制執行使用者身分

相關要求：交流 -6 (2)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::EFS::AccessPoint`

AWS Config 規則：`efs-access-point-enforce-user-identity`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EFS 存取點是否設定為強制執行使用者身分。如果在建立 EFS 存取點時未定義 POSIX 使用者身分，則此控制會失敗。

Amazon EFS 存取點是應用程式特定的 EFS 檔案系統進入點，此進入點可讓您更輕鬆地管理共用資料集的應用程式存取。存取點可以針對透過存取點提出的所有檔案系統要求，強制執行使用者身分 (包括使用者的 POSIX 群組)。存取點也可以針對檔案系統強制執行不同的根目錄，讓用戶端只能存取指定目錄或其子目錄中的資料。

修補

若要強制執行 Amazon EFS 存取點的使用者身分，請參閱 Amazon Elastic File System 使用者指南中的使用存取點強制使用者身分。

Amazon Elastic Kubernetes Service 控制

這些控制項與 Amazon EKS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[EKS.1] EKS 叢集端點不應可公開存取

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全存取管理 > 無法公開存取的資源

嚴重性：高

資源類型：`AWS::EKS::Cluster`

AWS Config 規則：`eks-endpoint-no-public-access`

排程類型：定期

參數：無

此控制項會檢查 Amazon EKS 叢集端點是否可公開存取。如果 EKS 叢集具有可公開存取的端點，則控制項會失敗。

當您建立新叢集時，Amazon EKS 會為您用來與叢集通訊的受管 Kubernetes API 伺服器建立端點。默認情況下，此 API 服務器端點是公開提供給互聯網。API 伺服器的存取權是使用 AWS Identity and Access Management (IAM) 和原生 Kubernetes 角色型存取控制 (RBAC) 的組合來保護。透過移除端點的公開存取權，您可以避免無意暴露和存取叢集。

修補

若要修改現有 EKS 叢集的端點存取，請參閱 Amazon EKS 使用者指南中的修改叢集端點存取。您可以在建立新 EKS 叢集時為其設定端點存取。如需建立新 Amazon EKS 叢集的相關指示，請參閱 Amazon EKS 使用者指南中的建立 Amazon EKS 叢集。

[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行

相關要求：第七八十三條路卡 -9 (1)、等級 5 公分 (2)、指定信號：800-53.R5 SI-2 (2)、指定信號 -53.R5 系統 -2 (4)、等級

類別:識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：`AWS::EKS::Cluster`

AWS Config 規則：`eks-cluster-supported-version`

排程類型：已觸發變更

參數：

- `oldestVersionSupported`：`1.25`（不可定制）

此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS 叢集是否在受支援的 Kubernetes 版本上執行)。如果 EKS 叢集在不支援的版本上執行，則控制項會失敗。

如果您的應用程式不需要特定版本的 Kubernetes，建議您針對叢集使用 EKS 支援的最新可用 Kubernetes 版本。如需詳細資訊，請參閱 Amazon EKS Kubernetes 發行日曆和 Amazon EKS 版本支援和 Amazon EKS 使用者指南中的常見問題集。

修補

若要更新 EKS 叢集，請在 Amazon EKS 使用者指南中更新 Amazon EKS 叢集 Kubernetes 版本。

[EKS.8] EKS 叢集應啟用稽核記錄

相關要求：交流 -53.R5 (12)、交流電 -2 (4)、奈特。800-53.R5 交流 -6 (9)、尼斯特。800-53.R5 交流 -6 (9)、黑色 -53.R5、AU-10、六月五日 (3), 尼斯 .800-53.R5 (4), 日本 6 星期六 (4), 尼斯 .800-53.R5 (7), 尼斯 .800-53.R5 SC-7 (9), 尼斯 .800-53.R5 (9),), 尼斯 .800-53.R5 四七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::EKS::Cluster`

AWS Config 規則：`eks-cluster-logging-enabled`

排程類型：定期

參數：無

此控制項會檢查 Amazon EKS 叢集是否已啟用稽核記錄。如果未為叢集啟用稽核記錄，則控制項會失敗。

EKS 控制平面記錄可將稽核和診斷日誌直接從 EKS 控制平面提供到您帳戶中的 Amazon CloudWatch 日誌。您可以選取所需的記錄類型，記錄會以記錄串流的形式傳送至中每個 EKS 叢集的 CloudWatch 群組。記錄可讓您掌握 EKS 叢集的存取和效能。透過將 EKS 叢集的 EKS 控制平面記錄傳送至記 CloudWatch 錄檔，您可以在中央位置記錄作業以供稽核和診斷之用。

修補

若要啟用 EKS 叢集的稽核日誌，請參閱 Amazon EKS 使用者指南中的啟用和停用控制平面日誌。

Amazon ElastiCache 控制

這些控制項與資 ElastiCache 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

類別:復原 > 復原 > 啟用備份

嚴重性：高

資源類型：`AWS::ElastiCache::CacheCluster`

AWS Config 規則：**`elasticache-redis-cluster-automatic-backup-check`**

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`snapshotRetentionPeriod`	快照保留期間下限 (天)	Integer	1 設定為 35	1

此控制項會評估 Amazon ElastiCache for Redis 叢集是否已排程自動備份。如果 Redis 叢集的控制項小`SnapshotRetentionLimit`於指定的時間段，則會失敗。除非您為快照保留期間提供自訂參數值，否則 Security Hub 會使用預設值 1 天。

Amazon ElastiCache 的 Redis 集群可以備份他們的數據。您可以使用備份來還原叢集或植入新叢集。備份包含叢集的中繼資料，以及叢集中的所有資料。所有備份都會寫入 Amazon Simple Storage Service (Amazon S3)，該服務提供耐久性儲存空間。您可以建立新的 Redis 叢集，並使用備份中的資料填入資料來還原資料。您可以使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 和 ElastiCache API 來管理備份。

修補

若要在 Redis 叢集上排定 ElastiCache 自動備份，請參閱 Amazon ElastiCache 使用者指南中的排程自動備份。

[ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五四 (4)、七月五四 (5)

類別:識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：`AWS::ElastiCache::CacheCluster`

AWS Config 規則：`elasticache-auto-minor-version-upgrade-check`

排程類型：定期

參數：無

此控制項會評估 Redis 是否 ElastiCache 會自動將次要版本升級套用至快取叢集。如果 ElastiCache Redis 快取叢集沒有自動套用次要版本升級，則此控制項會失敗。

`AutoMinorVersionUpgrade`這是一項功能，您可以在 ElastiCache Redis 開啟，以便在新的次要快取引擎版本可用時自動升級快取叢集。這些升級可能包括安全性修補程式和錯誤修正。保持安 up-to-date 裝修補程式是保護系統的重要步驟。

修補

若要將自動次要版本升級套用至 Redis 快取叢集的現有 ElastiCache 版本，請參閱 Amazon ElastiCache 使用者指南中的升級引擎版本。

[ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移

相關要求：CP-10, 尼斯 -53.R5 SC-36, 尼斯. 800-53.R5 SC-5 (2), 奈特 800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 規則：elasticache-repl-grp-auto-failover-enabled

排程類型：定期

參數：無

此控制項會檢查 Redis 複寫群組是否 ElastiCache 已啟用自動容錯移轉。如果沒有為 Redis 複寫群組啟用自動容錯移轉，則此控制項會失敗。

啟用複寫群組的自動容錯移轉時，主要節點的角色會自動容錯移轉至其中一個僅供讀取複本。此容錯移轉和複本升級可確保您可以在升級完成後繼續寫入新的主要項目，以減少發生故障時的整體停機時間。

修補

若要針對 Redis 複寫群組啟 ElastiCache 用現有的自動容錯移轉，請參閱 Amazon ElastiCache 使用者指南中的修改 ElastiCache 叢集。如果使用 ElastiCache 主控台，請將 [自動容錯移轉] 設為 [啟用]。

[ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

分類:保護 > 資料保護 > 加密 data-at-rest

嚴重性：中

資源類型：AWS::ElastiCache::ReplicationGroup

AWS Config 規則：elasticache-repl-grp-encrypted-at-rest

排程類型：定期

參數：無

此控制項會檢 ElastiCache 查 Redis 複寫群組是否在靜態時加密。如果 Redis 複寫群組未在靜態時加密，則此控制項會失敗。 ElastiCache

靜態資料加密可降低未經驗證的使用者存取儲存在磁碟上之資料的風險。 ElastiCache 針對 Redis 複寫群組，應在靜態時加密，以增加安全性層。

修補

若要在 Redis 複寫群組上設定靜態加密，請參閱 Amazon ElastiCache 使用者指南 ElastiCache 中的啟用靜態加密。

[ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密

相關要求：東西 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 規則：`elasticache-repl-grp-encrypted-in-transit`

排程類型：定期

參數：無

此控制項會檢查 Redis 複寫群組是否 ElastiCache 在傳輸過程中加密。如果 Redis 複寫群組在傳輸中未加密，則此控制項會失敗。 ElastiCache

加密傳輸中的資料可降低未經授權的使用者竊聽網路流量的風險。在 Redis 複寫群組上啟用傳輸中加密，每當資料從一個位置移動到另一個位置時，例如叢集中的節點之間或叢集與應用程式之間，都會加密資料。 ElastiCache

修補

若要在 Redis 複寫群組上設定傳輸中加密，請參閱 Amazon ElastiCache 使用者指南 ElastiCache 中的啟用傳輸中加密。

[ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH

相關要求：交流 -2 (1)、交流 3 (1)、尼什八達 -53.R5 交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、日本交流 -6

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::ElastiCache::ReplicationGroup`

AWS Config 規則：`elasticache-repl-grp-redis-auth-enabled`

排程類型：定期

參數：無

此控制項會檢查 Redis 複寫群組是否已啟 ElastiCache 用 Redis AUTH。如果 Redis 複寫群組的節點版本低 ElastiCache 於 6.0 且`AuthToken`未使用，則控制項會失敗。

當您使用 Redis 驗證權杖或密碼時，Redis 需要密碼才能允許用戶端執行命令，以提升資料安全性。對於 Redis 6.0 及更新版本，我們建議使用以角色為基礎的存取控制 (RBAC)。由於 RBAC 不支援 6.0 之前的 Redis 版本，因此此控制項只會評估無法使用 RBAC 功能的版本。

修補

若要在 Redis 複寫群組上使 ElastiCache 用 Redis AUTH，請參閱 Amazon ElastiCache 使用者指南中的修改 Redis 叢集上現有 ElastiCache 的 AUTH 權杖。

[ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組

相關要求：交流 4、交流電 -4、交流 -4 (21)、尼斯特。800-53.R5 的 SC-7、星期五、七、七、五、七、七、四、七 (4)、SC-7 (5)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::ElastiCache::CacheCluster`

AWS Config 規則：`elasticache-subnet-group-check`

排程類型：定期

參數：無

此控制項會檢查 ElastiCache 叢集是否設定了自訂子網路群組。如果`CacheSubnetGroupName`具有值，則控制項會失敗 ElastiCache 叢集`default`。

啟動 ElastiCache 叢集時，如果沒有預設子網路群組，則會建立預設子網路群組。預設群組會使用預設 Virtual Private Cloud (VPC) 中的子網路。我們建議您使用自訂子網路群組，這些群組對叢集所在的子網路有更嚴格的限制，以及叢集從子網路繼承的網路。

修補

若要為 ElastiCache 叢集建立新的子網路群組，請參閱 Amazon ElastiCache 使用者指南中的建立子網路群組。

AWS Elastic Beanstalk 控制

這些控制項與 Elastic Beanstalk 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告

相關要求：NIS.800-53.R5 CA-7、尼斯

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::ElasticBeanstalk::Environment`

AWS Config 規則：`beanstalk-enhanced-health-reporting-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查您的 AWS Elastic Beanstalk 環境是否已啟用增強型健全狀況報告。

Elastic Beanstalk 增強型健全狀況報告可讓您更快速地回應基礎架構的健康狀態變更。這些變更可能會導致應用程式缺乏可用性。

Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。Elastic Beanstalk 健康代理程式 (包含在支援的 Amazon 機器映像 (AMI) 中，可評估環境 EC2 執行個體的日誌和指標。

如需詳細資訊，請參閱AWS Elastic Beanstalk 開發人員指南中的增強型健全狀況報告和監控。

修補

如需如何啟用增強型健全狀況報告的指示，請參閱AWS Elastic Beanstalk 開發人員指南中的使用 Elastic Beanstalk 主控台啟用增強型健全狀況報告。

[ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五四 (4)、七月五四 (5)

類別:偵測 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::ElasticBeanstalk::Environment

AWS Config 規則：elastic-beanstalk-managed-updates-enabled

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
UpdateLevel	版本更新層級	列舉	minor, patch	無預設值

此控制項會檢查是否已針對 Elastic Beanstalk 環境啟用受管平台更新。如果未啟用受管平台更新，則控制項會失敗。根據預設，如果啟用任何類型的平台更新，則控制項會通過。或者，您可以提供自訂參數值，以需要特定的更新層級。

啟用受管理平台更新可確保安裝環境適用的最新可用平台修正、更新和功能。保持最新的修補程式安裝是保護系統的重要步驟。

修補

若要啟用受管理平台更新，請參閱開AWS Elastic Beanstalk 發人員指南中的「受管理平台更新」下的「設定受管理平台更

[ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS::ElasticBeanstalk::Environment

AWS Config 規則：elastic-beanstalk-logs-to-cloudwatch

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`RetentionInDays`	在到期前保留記錄事件的天數	列舉	`1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653`	無預設值

此控制項會檢查 Elastic Beanstalk 環境是否設定為將記錄檔傳送至 CloudWatch 記錄檔。如果 Elastic Beanstalk 環境未設定為將記錄檔傳送至記錄，則控制項會失敗。 CloudWatch 或者，如果您希望控制項僅在到期前的指定天`RetentionInDays`數保留記錄檔時才傳遞，則可以為參數提供自訂值。

CloudWatch 協助您收集並監控應用程式和基礎結構資源的各種指標。您也可以使用根據特定指標 CloudWatch 來設定警示動作。我們建議將 Elastic Beanstalk 整合在一起， CloudWatch 以提高 Elastic Beanstalk 環境的可見度。Elastic Beanstalk 日誌包括 eb-activity.log，從環境 nginx 或 Apache 代理服務器訪問日誌，以及特定於環境的日誌。

修補

若要整合 Elastic Beanstalk 與 CloudWatch 記錄，請參閱AWS Elastic Beanstalk 開發人員指南中的將執行個體 CloudWatch 記錄串流至記錄。

Elastic Load Balancing 控制

這些控制項與 Elastic Load Balancing 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS

相關要求：PCI DSS V3.2.1/2.3, 投資管理系統 DSS v3.2.1/4.1, NIT.800-53.R5 AC-17 (2), 奈特. 800-53.R5 IA-5 (1), 尼斯. 800-53.R5 SC-12 (3), 等等 (3), 早上八點五分之七 (4), 日本七點七 (4), 日本八月八日 -53.R5 (6), 日本八月八日 -53.R5 (2) SC-13 SC-23 SC-23

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`alb-http-to-https-redirection-check`

排程類型：定期

參數：無

此控制項會檢查是否已在應用程式負載平衡器的所有 HTTP 接聽程式上設定 HTTP 至 HTTPS 重新導向。如果應用程式負載平衡器的任何 HTTP 接聽程式未設定 HTTP 至 HTTPS 重新導向，則控制項會失敗。

開始使用應用程式負載平衡器之前，您必須新增一或多個接聽程式。接聽程式是使用已設定通訊協定和連接埠檢查連線請求的一種程序。接聽程式同時支援 HTTP 和 HTTPS 通訊協定。您可以使用 HTTPS 接聽程式，將加密和解密的工作卸載到負載平衡器。若要在傳輸中強制執行加密，您應該使用應用程式負載平衡器的重新導向動作，將用戶端 HTTP 要求重新導向至連接埠 443 上的 HTTPS 要求。

若要深入了解，請參閱應用程式負載平衡器使用者指南中的應用程式負載平衡器的接聽程式。

修補

若要將 HTTP 要求重新導向至 HTTPS，您必須新增應用程式負載平衡器接聽程式規則或編輯現有規則。

如需有關新增規則的指示，請參閱應用程式負載平衡器使用者指南中的新增規則。針對「通訊協定：連接埠」，選擇「HTTP」，然後輸入**80**。針對 [新增動作]，[重新導向至]，選擇 [HTTPS]，然後輸入**443**。

如需有關編輯現有規則的指示，請參閱應用程式負載平衡器使用者指南中的編輯規則。針對「通訊協定：連接埠」，選擇「HTTP」，然後輸入**80**。針對 [新增動作]，[重新導向至]，選擇 [HTTPS]，然後輸入**443**。

[ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager

相關要求：第 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 加密傳輸中的資料

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 規則：`elb-acm-certificate-required`

排程類型：已觸發變更

參數：無

此控制項會檢查 Classic Load Balancer 是否使用 AWS Certificate Manager (ACM) 提供的 HTTPS/SSL 憑證。如果使用 HTTPS/SSL 接聽程式設定的 Classic Load Balancer 未使用 ACM 提供的憑證，則控制項會失敗。

若要建立憑證，您可以使用 ACM 或支援 SSL 和 TLS 通訊協定的工具，例如 OpenSSL。Security Hub 建議您使用 ACM 為負載平衡器建立或匯入憑證。

ACM 與傳統負載平衡器整合，因此您可以在負載平衡器上部署憑證。您也應該自動續訂這些憑證。

修補

如需如何將 ACM SSL/TLS 憑證與 Classic Load Balancer 產生關聯的詳細資訊，請參閱 AWS 知識中心文章如何將 ACM SSL/TLS 憑證與傳統、應用程式或 Network Load Balancer 產生關聯？

[ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定

相關要求：東西 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 規則：`elb-tls-https-listeners-only`

排程類型：已觸發變更

參數：無

此控制項會檢查您的 Classic Load Balancer 接聽程式是否已設定 HTTPS 或 TLS 通訊協定，以供前端 (用戶端至負載平衡器) 連線使用。如果 Classic Load Balancer 具有接聽程式，則此控制項適用。如果您的 Classic Load Balancer 未設定接聽程式，則控制項不會報告任何發現項目。

如果 Classic Load Balancer 接聽程式針對前端連線設定 TLS 或 HTTPS，則控制項會通過。

如果監聽器未針對前端連線設定 TLS 或 HTTPS，則控制項會失敗。

開始使用負載平衡器之前，您必須新增一或多個接聽程式。接聽程式是使用已設定通訊協定和連接埠檢查連線請求的一種程序。偵聽程式可以同時支援 HTTP 和 HTTPS/TLS 通訊協定。您應該始終使用 HTTPS 或 TLS 接聽程式，以便負載平衡器在傳輸過程中執行加密和解密的工作。

修補

若要修正此問題，請更新您的接聽程式以使用 TLS 或 HTTPS 通訊協定。

將所有不相容的接收器變更為TLS/HTTPS 接聽程式

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 Load Balancing (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取您的 Classic Load Balancer。
4. 在 Listeners (接聽程式) 標籤上，選擇 Edit (編輯)。
5. 對於「Load Balancer 通訊協定」未設定為 HTTPS 或 SSL 的所有監聽器，請將設定變更為 HTTPS 或 SSL。
6. 對於所有修改的監聽器，請在憑證索引標籤上選擇變更預設值。
7. 對於 ACM 和 IAM 憑證，請選取憑證。
8. 選擇儲存為預設。
9. 更新所有監聽程式之後，請選擇 [儲存]。

[ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭

相關要求：七七 (4)、日本第五站

分類:保護 > 網絡安全

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`alb-http-drop-invalid-header-enabled`

排程類型：已觸發變更

參數：無

此控制項會評估 AWS 應用程式負載平衡器，以確保它們設定為刪除無效的 HTTP 標頭。如果的`routing.http.drop_invalid_header_fields.enabled`值設定為，則控制項會失敗`false`。

根據預設，應用程式負載平衡器未設定為卸除無效的 HTTP 標頭值。移除這些標頭值可防止 HTTP 不同步攻擊。

請注意，如果 ELB.12 已啟用，您可以停用此控制項。

修補

若要修正此問題，請將負載平衡器設定為卸除無效的標頭欄位。

設定負載平衡器刪除無效標頭欄位

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格上，選擇 Load balancers (負載平衡器)。
3. 選擇應用程式負載平衡器。
4. 從「動作」 中選擇 「編輯屬性」。
5. 在 [刪除無效標頭欄位] 下，選擇 [啟用]
6. 選擇儲存。

[ELB.5] 應啟用應用程式和傳統負載平衡器記錄

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六 (9), 日本第七 (8) AU-12

日誌記錄

嚴重性：中

資源類型:`AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`elb-logging-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查「應用程式負載平衡器」和「傳統負載平衡器」記錄是否已啟用。如果`access_logs.s3.enabled`是，則控制項失敗`false`。

Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。您可以使用這些存取日誌來分析流量模式和排除問題。

若要深入了解，請參閱 Classic Load Balancer 使用者指南中的傳統負載平衡器的存取記錄。

修補

若要啟用存取記錄，請參閱《應用程式負載平衡器使用者指南》中的步驟 3：設定存取記錄。

[ELB.6] 應該啟用應用 Application Load Balancer 刪除保護

相關要求：鎳鋅 -53.R5 路卡 -9 (1)、指定 5 公分 (5 公分)、電子信號 -53.R5 公分 (2)、電子顯示器 -53.R5 公分 (3)、電子顯示器 -53.R5 SC-5 (2)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`elb-deletion-protection-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查應用 Application Load Balancer 是否已啟用刪除保護。如果未設定刪除保護，則控制項會失敗。

啟用刪除保護以保護您的 Application Load Balancer 不被刪除。

修補

為避免您的負載平衡器上遭意外刪除，您可以啟用刪除保護。您的負載平衡器的刪除保護預設為停用。

如果您為負載平衡器啟用刪除保護，則必須先停用刪除保護，然後才能刪除負載平衡器。

若要啟用刪除保護，請參閱應用程式負載平衡器使用者指南中的刪除保護。

[ELB.7] 傳統負載平衡器應啟用連線排空

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

分類:復原 > 復原力

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config規則:`elb-connection-draining-enabled`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查傳統負載平衡器是否已啟用連線排空。

在傳統負載平衡器上啟用連線排除功能，可確保負載平衡器停止向解除註冊或運作狀態不佳的執行個體傳送要求。它使現有連接保持打開狀態。這對 Auto Scaling 群組中的執行個體特別有用，可確保連線不會突然切斷。

修補

若要在 Classic Load Balancer 上啟用連線排空，請參閱傳統負載平衡器使用者指南中的設定傳統負載平衡器的連線排空。

[ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config

相關要求：東西 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 加密傳輸中的資料

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 規則：`elb-predefined-security-policy-ssl-check`

排程類型：已觸發變更

參數：

- predefinedPolicyName：ELBSecurityPolicy-TLS-1-2-2017-01（不可定制）

此控制項會檢查 Classic Load Balancer HTTPS/SSL 接聽程式是否使用預先定義的原則。ELBSecurityPolicy-TLS-1-2-2017-01如果 Classic Load Balancer HTTPS/SSL 接聽程式未使用，則控制項會失敗。ELBSecurityPolicy-TLS-1-2-2017-01

安全性原則是 SSL 通訊協定、密碼和伺服器順序喜好設定選項的組合。預先定義的原則會控制用戶端與負載平衡器之間 SSL 交涉期間所支援的加密、通訊協定和偏好設定順序。

使用ELBSecurityPolicy-TLS-1-2-2017-01可協助您符合要求您停用特定版本的 SSL 和 TLS 的合規性和安全性標準。如需詳細資訊，請參閱傳統負載平衡器使用者指南中的傳統負載平衡器預先定義的 SSL 安全性原則。

修補

如需如何ELBSecurityPolicy-TLS-1-2-2017-01搭配 Classic Load Balancer 使用預先定義的安全性原則的詳細資訊，請參閱傳統負載平衡器使用者指南中的設定安全性設定。

[ELB.9] 傳統負載平衡器應啟用跨區域負載平衡

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原力 > 高可用性

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：elb-cross-zone-load-balancing-enabled

排程類型：已觸發變更

參數：無

此控制項會檢查傳統負載平衡器 (CLB) 是否已啟用跨區域負載平衡。如果 CLB 未啟用跨區域負載平衡，則控制項會失敗。

負載平衡器節點只會將流量分配到其可用區域中已註冊的目標。停用跨區域負載平衡時，每個負載平衡器節點只會將流量分發到其可用區域內已註冊的目標。如果可用區域中的已註冊目標數目不一樣，流量將不會平均分配，而且與另一個區域中的執行個體相比，一個區域中的執行個體最終可能會過度使

用。啟用跨區域負載平衡後，Classic Load Balancer 的每個負載平衡器節點將請求平均分配到所有已啟用的可用區域中已註冊的執行個體。如需詳細資訊，請參閱 Elastic Load Balancing 使用指南中的跨區域負載平衡。

修補

若要在 Classic Load Balancer 中啟用跨區域負載平衡，請參閱傳統負載平衡器使用者指南中的啟用跨區域負載平衡。

[ELB.10] Classic Load Balancer 應該跨越多個可用區域

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原力 > 高可用性

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 規則：`clb-multiple-az`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`minAvailabilityZones`	可用區域的最小數目	列舉	`2, 3, 4, 5, 6`	`2`

此控制項會檢查 Classic Load Balancer 是否已設定為至少跨越指定數目的可用區域 (AZ)。如果 Classic Load Balancer 未跨越至少指定數目的 AZ，則控制項會失敗。除非您為最小 AZ 數目提供自訂參數值，否則 Security Hub 會使用兩個 AZ 的預設值。

您可以設定 Classic Load Balancer，在單一可用區域或多個可用區域的 Amazon EC2 執行個體之間分發傳入的請求。如果唯一設定的可用區域無法使用，則不跨越多個可用區域的 Classic Load Balancer 將流量重新導向至另一個可用區域中的目標。

修補

若要將可用區域新增至 Classic Load Balancer，請參閱 Classic Load Balancer 使用者指南中的為傳統負載平衡器新增或移除子網路。

[ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

相關要求：交流 -4 (21)、鎳碳酸鈣 -9 (1)、奈特 .

產品分類:資料保護 > 資料完整性

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`alb-desync-mode-check`

排程類型：已觸發變更

參數：

- `desyncMode`：`defensive, strictest`（不可定制）

此控制項會檢查應用程式負載平衡器是否設定為防禦性或最嚴格的不同步緩和模式。如果 Application Load Balancer 未設定防禦性或最嚴格的不同步緩和模式，則控制項會失敗。

HTTP 不同步問題可能會導致要求走私，並使應用程式容易遭受要求佇列或快取中毒。反過來，這些弱點可能導致憑證填滿或執行未經授權的命令。應用程式負載平衡器設定為防禦性或最嚴格的不同步緩和模式，可保護您的應用程式免受 HTTP 不同步可能造成的安全性問題影響。

修補

若要更新應用程式負載平衡器的不同步緩和模式，請參閱《應用程式負載平衡器使用者指南》中的「不同步緩和模式」。

[ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`elbv2-multiple-az`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`minAvailabilityZones`	可用區域的最小數目	列舉	`2, 3, 4, 5, 6`	2

此控制項會檢查 Elastic Load Balancer V2 (應用程式、網路或閘道 Load Balancer) 是否已註冊至少指定數目的可用區域 (AZ) 的執行個體。如果 Elastic Load Balancer V2 沒有在指定數量的 AZ 中註冊執行個體，則控制項會失敗。除非您為最小 AZ 數目提供自訂參數值，否則 Security Hub 會使用兩個 AZ 的預設值。

Elastic Load Balancing 會自動將傳入流量分配到一或多個可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。當傳入流量隨著時間發生變化，Elastic Load Balancing 會擴展您的負載平衡器。建議至少設定兩個可用區域，以確保服務的可用性，因為如果 Elastic Load Balancer 無法使用，將流量導向另一個可用區域。設定多個可用區域將有助於避免應用程式發生單一故障點。

修補

若要將可用區域新增至 Application Load Balancer，請參閱 Application Load Balancer 使用者指南中的應用程式負載平衡器的可用區域。若要將可用區域新增至 Network Load Balancer，請參閱網路負載平衡器使用者指南中的網路負載平衡器。若要將可用區域新增至閘道 Load Balancer，請參閱閘道 Load Balancer 使用者指南中的建立閘道負載平衡器。

[ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式

相關要求：交流 -4 (21)、鎳碳酸鈣 -9 (1)、奈特 .

類別:資料保護 > 資料完整性

嚴重性：中

資源類型：`AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 規則：`clb-desync-mode-check`

排程類型：已觸發變更

參數：

- `desyncMode`：`defensive, strictest`（不可定制）

此控制項會檢查 Classic Load Balancer 是否設定為防禦性或最嚴格的不同步緩和模式。如果 Classic Load Balancer 未設定為防禦性或最嚴格的不同步緩和模式，則控制項會失敗。

HTTP 不同步問題可能會導致要求走私，並使應用程式容易遭受要求佇列或快取中毒。反過來，這些漏洞可能導致憑證劫持或執行未經授權的命令。經典負載平衡器設定為防禦性或最嚴格的不同步緩和模式，可保護您的應用程式免受 HTTP 不同步可能造成的安全性問題影響。

修補

若要更新 Classic Load Balancer 上的不同步緩和模式，請參閱傳統負載平衡器使用者指南中的修改不同步緩和模式。

[ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF

相關要求：交流 -4 (21)

分類:保護 > 保護服務

嚴重性：中

資源類型：`AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 規則：`alb-waf-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查應用程式負載平衡器是否與 AWS WAF 典型或 AWS WAF Web 存取控制清單 (Web ACL) 相關聯。如果 AWS WAF 組態的`Enabled`欄位設定為，則控制項會失敗`false`。

AWS WAF 是一種網絡應用程序防火牆，可幫助保護 Web 應用程序和 API 免受攻擊。使用時 AWS WAF，您可以設定 Web ACL，這是一組規則，可根據您定義的可自訂 Web 安全規則和條件，允許、封鎖或計數 Web 要求。建議您將 Application Load Balancer 與 AWS WAF Web ACL 建立關聯，以協助保護其免於遭受惡意攻擊。

修補

若要將應用程式負載平衡器與 Web ACL 建立關聯，請參閱開發人員指南中的建立 Web ACL 與 AWS 資源的關聯或取消關聯。AWS WAF

Amazon EMR 控制

這些控制項與 Amazon EMR 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::EMR::Cluster`

AWS Config 規則：`emr-master-no-public-ip`

排程類型：定期

參數：無

此控制項會檢查 Amazon EMR 叢集上的主節點是否具有公用 IP 地址。如果公用 IP 位址與任何主節點執行個體相關聯，則控制項會失敗。

公用 IP 位址會在執行個體的`NetworkInterfaces`組態`PublicIp`欄位中指定。此控制項只會檢查處於`RUNNING`或`WAITING`狀態的 Amazon EMR 叢集。

修補

在啟動期間，您可以控制是否將預設或非預設子網路中的執行個體指派公用 IPv4 位址。依預設，預設子網路會將此屬性設定為`true`。非預設子網路的 IPv4 公開尋址屬性設定為`false`，除非該屬性是由 Amazon EC2 啟動執行個體精靈建立的。在此情況下，屬性會設定為`true`。

啟動後，您無法手動取消公用 IPv4 位址與執行個體的關聯。

若要修復發現失敗的項目，您必須在私有子網路 (IPv4 公用位址屬性設定為) 的 VPC 中啟動新叢集。`false`如需指示，請參閱 Amazon EMR 管理指南中的將叢集啟動到 VPC。

[EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全存取管理 > 無法公開存取的資源

嚴重性：嚴重

資源類型：`AWS::::Account`

AWS Config 規則：`emr-block-public-access`

排程類型：定期

參數：無

此控制項會檢查您的帳戶是否設定了 Amazon EMR 區塊公開存取。如果未啟用封鎖公用存取設定，或允許連接埠 22 以外的任何連接埠，則控制項會失敗。

如果叢集具有允許來自連接埠上公有 IP 地址輸入流量的安全組態，Amazon EMR 區塊公用存取可防止您在公有子網路中啟動叢集。在您的 AWS 帳戶 中的使用者啟動叢集時，Amazon EMR 會檢查叢集安全群組中的連接埠規則，並將其與您的傳入流量規則進行比較。如果安全群組具有開啟公有 IP 地址 IPv4 0.0.0.0/0 或 IPv6 ::/0 連接埠的傳入規則，且這些連接埠未指定為您帳戶的例外狀況，則 Amazon EMR 不會允許使用者建立叢集。

> **Note**
>
> 預設為啟用封鎖公開存取。為了增強帳戶保護，建議您保持啟用狀態。

修補

若要為 Amazon EMR 設定區塊公開存取，請參閱 Amazon EMR 管理指南中的使用 Amazon EMR 區塊公開存取。

彈性搜索控件

這些控制項與彈性搜尋資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[ES.1] 彈性搜尋網域應啟用靜態加密

相關要求：PCI DSS V3.2.1/3.4、介面卡 -9 (1)、介面卡 -9 (1)、介面卡 5 (1)、電子顯示器 (6)、電子顯示器 (5)、介面卡 5 (10)、等級 800-53.R5 SC-28 (1)、SC-13 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則：`elasticsearch-encrypted-at-rest`

排程類型：定期

參數：無

此控制項會檢查 Elasticsearch 網域是否已啟用靜態加密組態。如果未啟用靜態加密，則檢查會失敗。

為了為您的敏感數據增加一層安全性 OpenSearch，您應該將您 OpenSearch 的配置為靜態加密。彈性搜尋網域提供靜態資料的加密功能。此功能用 AWS KMS 來儲存和管理您的加密金鑰。為了執行加密，其會使用 256 位元金鑰的進階加密標準演算法 (AES-256)。

若要進一步了解靜 OpenSearch 態加密，請參閱 Amazon 服務開發人員指南中的 Amazon OpenSearch 服 OpenSearch 務靜態資料加密。

某些執行個體類型 (例如`t.small`和`t.medium`) 不支援靜態資料加密。如需詳細資訊，請參閱 Amazon OpenSearch 服務開發人員指南中支援的執行個體類型

修補

若要為新的和現有的 Elasticsearch 網域啟用靜態加密，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用靜態資料加密。

[ES.2] 彈性搜索域名不應公開訪問

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

分類:保護 > 安全網絡配置 > VPC 內的資源

嚴重性：嚴重

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則：`elasticsearch-in-vpc-only`

排程類型：定期

參數：無

此控制項會檢查彈性搜尋網域是否位於 VPC 中。它不會評估 VPC 子網路路由組態來決定公用存取權。您應該確保 Elasticsearch 域未附加到公共子網絡。請參閱 Amazon OpenSearch 服務開發人員指南中以資源為基礎的政策。您也應該確保您的 VPC 已根據建議的最佳實務進行設定。請參閱 Amazon VPC 使用者指南中適用於 VPC 的安全性最佳實務。

VPC 中部署的 Elasticsearch 網域可透過私人網路與 VPC 私人雲端資源進行通訊，而不需要周遊公用 AWS 網際網路。此組態會限制對傳輸中資料的存取，以提高安全性狀態。VPC 提供許多網路控制，以確保對 Elasticsearch 網域的存取安全，包括網路 ACL 和安全性群組。Security Hub 建議您將公用 Elasticsearch 網域移轉至 VPC，以利用這些控制項。

修補

如果您建立了具備公有端點的網域，您稍後便無法將其置放於 VPC 內。反之，您必須建立新網域並遷移您的資料。反之亦然。如果您在 VPC 中建立了網域，該網域便無法擁有公有端點。您必須改為建立另一個網域或停用此控制項。

請參閱 Amazon OpenSearch 服務開發人員指南中的 VPC 中啟動您的 Amazon OpenSearch 服務域。

[E.3] 彈性搜尋網域應加密節點之間傳送的資料

相關要求：東西 800-53.R5 交流 4、SC-13、等級 800-53.R5 SC-23、等級 800-53.R5 SC-23 (3)、電子信號 -53.R5 (4)、等級 800-53.R5 (4)、等級 -53.R5 SC-8、

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則：`elasticsearch-node-to-node-encryption-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已啟用 node-to-node 加密功能。

HTTPS (TLS) 可用來協助防止潛在攻擊者透過或類似攻擊竊取網路流量或操控網路流量 person-in-the-middle 。只能允許透過 HTTPS (TLS) 進行加密連線。啟用 Elasticsearch 網域的 node-to-node 加密功能可確保叢集內部通訊在傳輸過程中加密。

可能會有與此配置相關的性能損失。在啟用此選項之前，您應該注意並測試效能權衡。

修補

如需在新網域和現有網域上啟用 node-to-node 加密的相關資訊，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用 node-to-node加密。

[ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 – 記錄日誌

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則：`elasticsearch-logs-to-cloudwatch`

排程類型：已觸發變更

參數：

- `logtype = 'error'` (不可定制)

此控制項會檢查 Elasticsearch 網域是否設定為將錯誤記錄檔傳送至 CloudWatch 記錄檔。

您應該啟用 Elasticsearch 網域的錯誤記錄檔，並將這些記錄檔傳送至記錄 CloudWatch 檔以供保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。

修補

如需如何啟用日誌發佈的相關資訊，請參閱 Amazon Ser OpenSearch vice 開發人員指南中的啟用日誌發佈 (主控台)。

[.5] 彈性搜尋網域應啟用稽核記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則:`elasticsearch-audit-logging-enabled`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：

- `cloudWatchLogsLogGroupArnList`（不可定制）。Security Hub 不會填入此參數。應針對稽核 CloudWatch 記錄設定的記錄檔記錄群組清單 (逗號分隔)。

  此規則是`NON_COMPLIANT`如果未在此參數清單中指定 Elasticsearch 網域的 CloudWatch 記錄檔群組。

此控制項會檢查 Elasticsearch 網域是否已啟用稽核記錄。如果 Elasticsearch 網域未啟用稽核記錄，則此控制項會失敗。

審核日誌是高度可定制的。它們可讓您追蹤 Elasticsearch 叢集上的使用者活動，包括驗證成功與失敗、要求、索引變更以 OpenSearch及傳入的搜尋查詢。

修補

如需啟用稽核日誌的詳細指示，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用稽核日誌。

[ES.6] 彈性搜尋網域至少應該有三個資料節點

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則:`elasticsearch-data-node-fault-tolerance`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已設定至少三個資料節點，而且`zoneAwarenessEnabled`是。`true`

Elasticsearch 網域至少需要三個資料節點，才能達到高可用性和容錯能力。部署具有至少三個資料節點的 Elasticsearch 網域可確保在節點失敗時進行叢集作業。

修補

若要修改彈性搜尋網域中的資料節點數目

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/。
2. 在「網域」下方，選擇您要編輯的網域名稱。
3. 選擇 Edit domain (編輯網域)。
4. 在 [資料節點] 下，將 [節點數目] 設定為大於或等於的數字`3`。

   對於三個可用區域部署，請設定為三個的倍數，以確保跨可用區域的平均分配。
5. 選擇提交。

[ES.7] 彈性搜尋網域至少應設定三個專用主節點

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config規則:`elasticsearch-primary-node-fault-tolerance`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已設定至少三個專用主要節點。如果網域未使用專用主節點，則此控制項會失敗。如果 Elasticsearch 網域有五個專用主節點，則此控制項會通過。但是，可能不必使用三個以上的主要節點來降低可用性風險，並且會產生額外的成本。

Elasticsearch 網域至少需要三個專用的主節點，才能達到高可用性和容錯能力。由於還有其他節點需要管理，因此可能會在資料節點藍/綠部署期間過濾專用主節點資源。部署具有至少三個專用主節點的 Elasticsearch 網域，可確保節點故障時有足夠的主節點資源容量和叢集作業。

修補

若要修改 OpenSearch 網域中專用主要節點的數目

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/。
2. 在「網域」下方，選擇您要編輯的網域名稱。
3. 選擇 Edit domain (編輯網域)。
4. 在專用主節點下，將執行個體類型設定為所需的執行個體類型。
5. 設定主節點數目等於三個或更大。
6. 選擇提交。

[.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線

相關要求：東西 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::Elasticsearch::Domain`

AWS Config 規則:`elasticsearch-https-required`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查與 Elasticsearch 網域的連線是否使用最新的 TLS 安全性原則。如果 Elasticsearch 網域未使用最新的支援政策，或者如果未啟用 HTTPS，則控制項會失敗。目前支援的最新 TLS 安全性原則為`Policy-Min-TLS-1-2-PFS-2023-10`。

HTTPS (TLS) 可用來協助防止潛在攻擊者利用 person-in-the-middle或類似攻擊來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能來測試應用程式，以瞭解效能設定檔和 TLS 的影響。相較於舊版 TLS，TLS 1.2 提供了多項安全性增強功能。

修補

若要啟用 TLS 加密，請使用 UpdateDomainConfigAPI 作業來設定DomainEndpointOptions物件。這會設定`TLSSecurityPolicy`.

Amazon EventBridge 控制

這些控制項與資 EventBridge 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略

相關要求：交流 -2、交流 -2、交流 -2 (1)、指定交流 -3、指定交流 -3、指定交流 -5 (15)、交流 -3 (15)、交流 -3 (7)、指定交流 -3 (7)、指令碼

類別:保護 > 安全存取管理 > 資源原則設定

嚴重性：低

資源類型：`AWS::Events::EventBus`

AWS Config 規則：`custom-schema-registry-policy-attached`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon EventBridge 自訂事件匯流排是否附加了以資源為基礎的政策。如果自訂事件匯流排沒有以資源為基礎的政策，則此控制項會失敗。

根據預設， EventBridge 自訂事件匯流排沒有附加以資源為基礎的政策。這可讓帳戶中的主參與者存取事件匯流排。藉由將以資源為基礎的政策附加至事件匯流排，您可以將事件匯流排的存取限制為指定帳戶，也可以刻意將存取權授與其他帳戶中的實體。

修補

若要將以資源為基礎的政策附加到 EventBridge 自訂事件匯流排，請參閱 Amazon EventBridge 使用者指南中的管理事件匯流排許可。

[EventBridge.4] EventBridge 全域端點應啟用事件複寫

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::Events::Endpoint`

AWS Config 規則：`global-endpoint-event-replication-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EventBridge 全球端點是否啟用事件複寫。如果未為全域端點啟用事件複寫，則控制項會失敗。

全球端點有助於讓您的應用程式具備區域容錯能力。若要開始，請將 Amazon Route 53 運作狀態檢查指派給端點。啟動容錯移轉時，健全狀況檢查會報告「狀況不良」狀態。在容錯移轉初始化的幾分鐘內，所有自訂事件都會路由至次要區域中的事件匯流排，並由該事件匯流排處理。當您使用全域端點時，您可以啟用事件複寫。事件複寫會使用受管規則，將所有自訂事件傳送至主要和次要區域中的事件匯流排。建議您在設定全域端點時啟用事件複寫。事件複寫可協助您確認已正確設定全域端點。需要事件複寫，才能從容錯移轉事件自動復原。如果您沒有啟用事件複寫，則必須手動將 Route 53 健康狀態檢查重設為「狀況良好」，然後再將事件重新路由回主要區域。

> **Note**
>
> 如果您使用的是自訂事件匯流排，則需要在每個區域中使用相同名稱且使用相同帳戶的自訂偶數匯流排，以便容錯移轉正常運作。啟用事件複寫可能會增加您的每月成本。如需有關定價的資訊，請參閱 Amazon EventBridge 定價。

修補

若要啟用 EventBridge 全球端點的事件複寫，請參閱 Amazon EventBridge 使用者指南中的建立全域端點。對於事件複製，選取已啟用事件複製。

Amazon FSx 控制

這些控制項與 Amazon FSx 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別:識別 > 庫存 > 標籤

嚴重性：低

資源類型：`AWS::FSx::FileSystem`

AWS Config 規則：`fsx-openzfs-copy-tags-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenZFS 檔案系統的 Amazon FSx 是否設定為將標籤複製到備份和磁碟區。如果 OpenZFS 檔案系統未設定為將標記複製到備份和磁碟區，則控制項會失敗。

識別和清查您的 IT 資產是治理和安全性的重要方面。標籤可協助您以不同的方式對 AWS 資源進行分類，例如依用途、擁有者或環境。當您有許多相同類型的資源時，這很有用，因為您可以根據指定給資源的標籤快速識別特定資源。

修補

若要設定 OpenZFS 檔案系統的 FSx 以將標籤複製到備份和磁碟區，請參閱 Amazon FSx OpenZFS 使用者指南中的更新檔案系統。

Amazon GuardDuty 控制

這些控制項與資 GuardDuty 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[GuardDuty.1] GuardDuty 應該啟用

相關要求：PCI DSS V3.2.1/11.4、等級交流 -2 (12)、NIS.800-53.R5 交流 -2 (12)、NIS.800-53.R5 (5)、NIS.800-53.R5 卡路由 7、Ni.800-53.R5 C.7、Ni.800-53.5 (3)、SA-11 (1), 東西 800-53.R5 SA-11 (6), 尼什 (5) SA-15 (2), 奈特. 800-53.R5 (8), 等等. R5 SC-5 (1), 尼斯 .800-53.R5 (3), 尼斯特. 800-53.R5 (1), 尼斯特. 800-53.R5 (3), 尼斯. 800-53.R5 四 (1), 尼斯. SA-15 SI-20.r5 四四 (2), 尼斯特. 800-53.R5 四 (22), 奈特.

類別：偵測 > 偵測服務

嚴重性：高

資源類型：`AWS::::Account`

AWS Config 規則：`guardduty-enabled-centralized`

排程類型：定期

參數：無

此控制項會檢查您的 GuardDuty 帳戶和區域 GuardDuty 是否已啟用 Amazon。

強烈建議您 GuardDuty 在所有支援的 AWS 區域中啟用。這樣做可 GuardDuty 以產生有關未經授權或不尋常活動的發現，即使在您未主動使用的區域也是如此。這也允 GuardDuty 許監視全球 CloudTrail 事件， AWS 服務 例如 IAM。

修補

若要修正此問題，請啟 GuardDuty用。

有關如何啟 GuardDuty用的詳細資訊 (包括如 AWS Organizations 何使用管理多個帳戶)，請參閱 Amazon 使用 GuardDuty 者指南 GuardDuty中的入門。

AWS Identity and Access Management 控制

這些控制與 IAM 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[IAM.1] IAM 政策不應允許完整的「*」管理特權

相關要求：PCI DSS V3.2.1/7.2.1，獨聯體基礎基準測試版 1.2.0/1.22，獨聯體 AWS 基礎基準測試版 1.4.0/1.16，Nist.800-53.R5 交流 -2（1），Nist.800-53.R5 交流 3，-53.R5 交流電 -5、交流 -6、交流 -6 (10)、奈特 800-53.R5 交流 -6 (2)、指定交流 -6 (2)、交流 -6 (3) AWS

類別：保護 > 安全存取管理

嚴重性：高

資源類型：`AWS::IAM::Policy`

AWS Config 規則：`iam-policy-no-statements-with-admin-access`

排程類型：已觸發變更

參數：

- `excludePermissionBoundaryPolicy: true`（不可定制）

此控制項會透`"Action": "*"`過包含超過的陳述式，來檢查 IAM 政策的預設版本 (也稱為客戶受管政策) 是否具有管理員存取權限`"Resource": "*"`。`"Effect": "Allow"`如果您使用具有此類陳述式的 IAM 政策，則控制項會失敗。

控制項只會檢查您建立的客戶受管政策。它不會檢查內嵌和 AWS 受管理的政策。

IAM 政策會定義授與使用者、群組或角色的一組權限。遵循標準安全性 AWS 建議，建議您授與最低權限，這表示只授與執行工作所需的權限。在您提供完整管理權限而非使用者需要的最低許可組時，您便會向潛在的不需要動作公開資源。

相較於允許完整的管理權限，建議您決定使用者需要做什麼，然後打造政策，讓使用者只執行這些任務。以最小的一組許可開始，然後依需要授予額外的許可更加安全。不要從太寬鬆的許可開始，稍後才嘗試限縮這些許可。

您應該移除具有`"Action": "*"`結束聲明`"Effect": "Allow"` 的 IAM 政策`"Resource": "*"`。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修改您的 IAM 政策，使其不允許完整的「*」管理權限，請參閱 IAM 使用者指南中的編輯 IAM 政策。

[IAM.2] IAM 使用者不應附加 IAM 政策

相關要求：PCI DSS V3.2.1/7.2.1、獨聯體 AWS 基礎基準測試版 1.2.0/1.16、NIS.800-53.R5 交流 -2、NIS.800-53.R5 交流 3、指定交流 3、-53.R5 交流 -6 (3)

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::IAM::User`

AWS Config 規則：`iam-user-no-policies-check`

排程類型：已觸發變更

參數：無

此控制項可檢查您的 IAM 使用者是否已附加政策。如果您的 IAM 使用者已附加政策，則控制項會失敗。相反地，IAM 使用者必須繼承 IAM 群組的許可或擔任角色。

根據預設，IAM 使用者、群組和角色無法存取 AWS 資源。IAM 政策將權限授與使用者、群組或角色。建議您將 IAM 政策直接套用至群組和角色，但不要套用至使用者。在群組或角色層級指派權限，會減少隨使用者數量成長而增加的存取管理複雜性。降低存取管理複雜性，可能會降低無意中讓委託人接收或保留過多權限的機會。

> **Note**
>
> Amazon 簡易電子郵件服務建立的 IAM 使用者是使用內嵌政策自動建立的。Security Hub 會自動從此控制項豁免這些使用者。

AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要解決此問題，請建立 IAM 群組，然後將政策附加到該群組。然後，將使用者新增至群組。政策即會套用到群組中的每個使用者。若要移除直接附加至使用者的政策，請參閱 IAM 使用者指南中的新增和移除 IAM 身分許可。

[IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

相關要求：獨聯體 AWS 基礎基準指標 v1.2.0/1.4，獨聯體 AWS 基礎基準測試版 1.4.0/1.14，尼斯。

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::IAM::User`

AWS Config 規則：`access-keys-rotated`

排程類型：定期

參數：

- `maxAccessKeyAge`：`90`（不可定制）

此控制項會檢查作用中的存取金鑰是否會在 90 天內輪換。

我們強烈建議您不要產生和移除帳戶中的所有存取金鑰。相反地，建議的最佳做法是建立一或多個 IAM 角色，或透過使用聯合 AWS IAM Identity Center。您可以使用這些方法來允許使用者存取 AWS Management Console 和 AWS CLI。

每種方法都有其使用案例。對於擁有現有中央目錄或計劃需要超過目前 IAM 使用者限制的企業，同盟通常比較好。在 AWS 環境外執行的應用程式需要存取金鑰，才能以程式設計方式存取 AWS 資源。

但是，如果需要程式設計存取的資源在內部執行 AWS，最佳做法是使用 IAM 角色。角色可讓您授予資源存取，而無須在組態中硬式編碼存取金鑰 ID 和私密存取金鑰。

若要進一步了解如何保護您的存取金鑰和帳戶，請參閱中管理 AWS 存取金鑰的最佳做法AWS 一般參考。另請參閱博客文章在使用程序化訪問 AWS 帳戶 時保護您的指南。

如果您已有存取金鑰，Security Hub 建議您每 90 天輪換一次存取金鑰。輪換存取金鑰可降低使用與被盜用或已終止帳戶相關聯存取金鑰的機會。這也能確保無法使用可能遺失、毀損或遭竊的舊金鑰存取資料。請在您輪換存取金鑰後一律更新應用程式。

存取金鑰由存取金鑰 ID 和私密存取金鑰組成。它們是用來簽署您向其發出的程式設計要求。 AWS使用者需要自己的存取金鑰，才能 AWS 從、Windows PowerShell 工具 AWS CLI、 AWS SDK 或使用個人 API 作業直接 HTTP 呼叫進行程式設計呼叫。 AWS 服務

如果您的組織使用 AWS IAM Identity Center (IAM 身分中心)，您的使用者可以登入 Active Directory、內建的身分與存取權管理身分中心目錄，或是連線至 IAM 身分中心的其他身分識別提供者 (IdP)。然後，他們可以映射到 IAM 角色，使他們能夠運行 AWS CLI 命令或調用 AWS API 操作，而無需訪問密鑰。若要深入了解，請參閱《使用AWS Command Line Interface 者指南》 AWS IAM Identity Center 中的〈設定 AWS CLI 要使用的〉。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要輪替超過 90 天的存取金鑰，請參閱《IAM 使用者指南》中的輪替存取金鑰。對於存取金鑰年齡超過 90 天的任何使用者，請遵循指示操作。

[IAM.4] IAM 根使用者存取金鑰不應存在

相關要求：PCI DSS V3.2.1/2.1，PCI DSS 3.2.1/2.2，PCI DSS V3.2.1/7.2.1，獨聯體基礎基準測試版 1.2.0/1.12，獨聯體 AWS 基礎基準測試版 1.4.0/1.4，Ni.800-53.R5 交流 -2 (1) ，交流 -6 交流 -6, 交流 -6 (10), 交流 -6 (2) AWS

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：`AWS::::Account`

AWS Config 規則：iam-root-access-key-check

排程類型：定期

參數：無

此控制項會檢查 root 使用者存取金鑰是否存在。

root 使用者是中最具權限的使用者 AWS 帳戶。 AWS 存取金鑰可讓您以程式設計方式存取特定帳戶。

Security Hub 建議您移除與根使用者相關聯的所有存取金鑰。這限制了可用於破壞您帳戶的向量。這也會鼓勵建立和使用擁有最低權限的角色類型帳戶。

修補

若要刪除根使用者存取金鑰，請參閱《IAM 使用者指南》中的〈刪除根使用者的存取金鑰〉。若要從 AWS 帳戶 in 刪除 root 使用者存取金鑰 AWS GovCloud (US)，請參閱《使用指南》中的刪除我的 AWS GovCloud (US) 帳戶根AWS GovCloud (US) 使用者存取金鑰。

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

相關要求：獨聯體 AWS 基礎基準測試 V1.2.0/1.2，獨聯體 AWS 基礎基準測試版 1.4.0/1.10，Nia-53.R5 交流 2（1），NIS.800-53.R5 IA-2（1），NIS.800-53.R5（1），IA-2 (8)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：mfa-enabled-for-iam-console-access

排程類型：定期

參數：無

此控制項可檢查是否為使用主控台密碼的所有 IAM 使用者啟用 AWS 多因素身份驗證 (MFA)。

Multi-Factor authentication (MFA) 在使用者名稱和密碼之外，多增加一層保護。啟用 MFA 後，當使用者登入 AWS 網站時，系統會提示他們輸入使用者名稱和密碼。此外，系統會提示他們從其 AWS MFA 裝置輸入驗證碼。

我們建議您為擁有主控台密碼的所有帳戶啟用 MFA。MFA 的設計旨在為主控台存取提供更高的安全。身分驗證委託人必須擁有發出時效性金鑰的裝置，並且必須擁有登入資料的知識。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要為 IAM 使用者新增 MFA，請參閱 IAM 使用者指南中 AWS的使用多因素身份驗證 (MFA)。

我們為符合條件的客戶提供免費的 MFA 安全密鑰。查看您是否符合資格，並訂購免費密鑰。

[IAM.6] 應為根使用者啟用硬體 MFA

相關要求：PCI DSS V3.2.1/8.3.1，獨聯體 AWS 基礎基準 V1.2.0/1.14，獨聯體基礎基準測試版 1.4.0/1.6，Nist.800-53.R5 交流 -2（1），NIS.800-53.R5 交流 -3（15），2 (6), 奈特. 800-53.R5 IA-2 (8) AWS

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：`AWS::::Account`

AWS Config 規則：`root-account-hardware-mfa-enabled`

排程類型：定期

參數：無

此控制項會檢查您 AWS 帳戶 是否已啟用使用硬體多重要素驗證 (MFA) 裝置以 root 使用者認證登入。如果未啟用 MFA，或允許任何虛擬 MFA 裝置使用根使用者認證登入，則控制項會失敗。

虛擬 MFA 可能無法提供與硬體 MFA 裝置相同層級的安全。我們強烈建議您只在等待硬體的購買核准或等待硬體就定位時，使用虛擬 MFA 裝置。若要深入了解，請參閱 IAM 使用者指南中的啟用虛擬多重要素驗證 (MFA) 裝置 (主控台)。

基於時間的一次性密碼（TOTP）和通用第二因素（U2F）令牌都可作為硬件 MFA 選項。

修補

若要為根使用者新增硬體 MFA 裝置，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用硬體 MFA 裝置 (主控台)。

我們為符合條件的客戶提供免費的 MFA 安全密鑰。查看您是否符合資格，並訂購免費密鑰。

[IAM.7] IAM 使用者的密碼政策應具有強大的組態

相關要求：交流 -2 (1)、日本交流 -2 (1)、日本交流 -2 (3)、NIS.800-53.R5 交流 -3 (15)、IA-5 (1)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`RequireUppercaseCharacters`	密碼中至少需要一個大寫字元	Boolean	`true` 或 `false` *	`true`
`RequireLowercaseCharacters`	密碼中至少需要一個小寫字元	Boolean	`true` 或 `false` *	`true`
`RequireSymbols`	密碼中至少需要一個符號	Boolean	`true` 或 `false` *	`true`
`RequireNumbers`	密碼至少需要一個數字	Boolean	`true` 或 `false` *	`true`

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
MinimumPasswordLength	密碼中的字元數目下限	Integer	8 設定為 128	8
PasswordReusePrevention	舊密碼可重複使用前的密碼輪換次數	Integer	12 設定為 24	無預設值
MaxPasswordAge	密碼到期前的天數	Integer	1 設定為 90	無預設值

此控制項會檢查 IAM 使用者的帳戶密碼政策是否使用強式組態。如果密碼原則不使用強式設定，則控制項會失敗。除非您提供自訂參數值，否則 Security Hub 會使用前表中提到的預設值。PasswordReusePrevention和MaxPasswordAge參數沒有預設值，因此，如果您排除這些參數，Security Hub 會在評估此控制項時忽略密碼輪換次數和密碼保留時間的次數。

若要存取 AWS Management Console，IAM 使用者需要密碼。最佳做法是，Security Hub 強烈建議您不要建立 IAM 使用者，而是使用聯合。同盟可讓使用者使用其現有的公司認證來登入 AWS Management Console。使用 AWS IAM Identity Center (IAM 身分中心) 建立或聯合使用者，然後在帳戶中扮演 IAM 角色。

若要進一步了解身分識別提供者和同盟，請參閱 IAM 使用者指南中的身分識別提供者和聯合。若要進一步了解 IAM 身分中心，請參閱使AWS IAM Identity Center 用者指南。

如果您需要使用 IAM 使用者，Security Hub 建議您強制建立強式使用者密碼。您可以在上設定密碼原則，以指 AWS 帳戶 定密碼的複雜性需求和強制循環期間。當您建立或變更密碼原則時，大部分的密碼原則設定會在使用者下次變更其密碼時強制執行。某些設定會立即強制執行。

修補

若要更新您的密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。

[IAM.8] 應移除未使用的 IAM 使用者登入資料

相關要求：PCI DSS V3.2.1/8.1.4，獨聯體 AWS 基礎基準測試版 1.2.0/1.3，NIST -53.R5 交流 -2，指針交流 -2，指針 -800-53.R5 交流 -2 (3)，NIS.800-53.R5 交流 -3，交流 -6 号交流电

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::IAM::User`

AWS Config 規則：`iam-user-unused-credentials-check`

排程類型：定期

參數：

- `maxCredentialUsageAge`：`90`（不可定制）

此控制項會檢查 IAM 使用者是否擁有 90 天未使用的密碼或使用中存取金鑰。

IAM 使用者可以使用不同類型的登入 AWS 資料 (例如密碼或存取金鑰) 存取資源。

Security Hub 建議您移除或停用 90 天以上未使用的所有認證。停用或移除不必要的登入資料，可以減少使用與被盜用或放棄帳戶相關聯登入資料的機會。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

當您在 IAM 主控台中檢視使用者資訊時，存取金鑰有效期、密碼存留時間和上次活動等欄位。如果上述任一欄的值大於 90 天，請將這些使用者的登入資料設定為非作用中。

您也可以使用認證報告來監控使用者，並識別 90 天以上沒有活動的使用者。您可以從 IAM 主控台下載`.csv`格式的認證報告。

識別非作用中的帳戶或未使用的認證後，請停用它們。如需指示，請參閱 IAM 使用者指南中的建立、變更或刪除 IAM 使用者密碼 (主控台)。

[IAM.9] 應該為根用戶啟用 MFA

相關要求：PCI DSS V3.2.1/8.3.1，獨聯體 AWS 基礎基準 V1.2.0/1.13，獨聯體基礎基準測試版 1.4.0/1.5，Nist.800-53.R5 交流 -2（1），尼斯 -800-53.R5 交流 -3（15），2 (6), 奈特. 800-53.R5 IA-2 (8) AWS

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：`AWS::::Account`

AWS Config 規則：`root-account-mfa-enabled`

排程類型：定期

參數：無

root 使用者可以完整存取 AWS 帳戶. MFA 在使用者名稱和密碼之外，多增加一層保護。啟用 MFA 後，當使用者登入時 AWS Management Console，系統會提示他們輸入使用者名稱和密碼，以及從其 AWS MFA 裝置輸入驗證碼。

當您為 root 使用者使用虛擬 MFA 時，CIS 建議使用的裝置不是個人裝置。使用保持充飽電及安全的專用行動裝置 (平板電腦或手機)，不要與任何個別的個人裝置混用。這會降低因裝置遺失、裝置以舊換新造成的 MFA 存取遺失風險，或擁有該裝置的個人不再任職於公司。

修補

若要為 root 使用者啟用 MFA，請參閱《AWS 帳號管理參考指南》中的針對 AWS 帳戶 root 使用者啟用 MFA。

[IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config

相關要求：投資產管理系統 DSS v3.2.1/8.1.4，投資產管理系統 DSS V3.2.1/8.2.3，PCI DSS V3.2.1/8.2.5

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：iam-password-policy

排程類型：定期

參數：無

此控制項會檢查 IAM 使用者的帳戶密碼政策是否使用下列最低 PCI DSS 設定。

- RequireUppercaseCharacters— 密碼中至少需要一個大寫字元。(預設 = true)
- RequireLowercaseCharacters— 密碼中至少需要一個小寫字元。(預設 = true)
- RequireNumbers— 密碼至少需要一個數字。(預設 = true)
- MinimumPasswordLength— 密碼最小長度。(預設值 = 7 或更長)
- PasswordReusePrevention— 允許重複使用之前的密碼數量。(預設值 = 4)
- MaxPasswordAge — 密碼到期前的天數。(預設值 = 90)

修補

若要更新您的密碼政策以使用建議的組態，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。

[IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.5

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：iam-password-policy

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策確保密碼使用不同的字元集。

CIS 建議密碼原則至少需要一個大寫字母。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。對於密碼強度，請選取至少需要一個拉丁字母 (A—Z) 的大寫字母。

[IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.6

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策確保密碼使用不同的字元集。CIS 建議密碼原則至少需要一個小寫字母。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。對於密碼強度，請選取至少需要一個拉丁字母 (A—Z) 的小寫字母。

[IAM.13] 確保 IAM 密碼政策至少需要一個符號

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.7

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策確保密碼使用不同的字元集。

CIS 建議密碼原則至少需要一個符號。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。對於密碼強度，請選取至少需要一個非英數字元。

[IAM.14] 確保 IAM 密碼政策至少需要一個數字

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.8

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策確保密碼使用不同的字元集。

CIS 建議密碼原則至少需要一個數字。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。對於密碼強度，請選取至少需要一個數字。

[IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.9，獨聯體基金會基準 v1.4.0/1.8 AWS

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策確保密碼至少達到指定長度。

CIS 建議密碼原則需要 14 個字元的密碼長度下限。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。對於「密碼最小長度」，請輸入**14**或更大的數字。

[IAM.16] 確保 IAM 密碼政策防止密碼重複使用

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.10，獨聯體基金會基準 v1.4.0/1.9 AWS

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

此控制項會檢查要記住的密碼數目是否設定為 24。如果值不是 24，則控制項會失敗。

IAM 密碼政策可防止同一使用者重複使用指定密碼。

CIS 建議密碼策略防止重複使用密碼。防止重複使用密碼以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。在「防止密碼重複使用」中，輸入 **24**

[IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期

相關要求：獨聯體 AWS 基金會基準指標 v1.2.0/1.11

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::::Account`

AWS Config 規則：`iam-password-policy`

排程類型：定期

參數：無

IAM 密碼政策可能會要求密碼在指定天數後輪換或過期。

CIS 建議密碼政策在 90 天或更短時間後過期密碼。縮短密碼生命週期以提高帳戶彈性，因應暴力登入嘗試。要求定期密碼變更，也有助於下列案例：

- 在您不知情時，密碼遭竊或被盜用。這會透過系統入侵、軟體漏洞或內部威脅而發生。
- 某些企業和政府的 web 篩選條件或代理伺服器可以攔截並記錄流量，即使流量加密。
- 許多人在很多系統 (如工作、電子郵件和個人) 都使用相同的密碼。
- 遭入侵的最終使用者工作站可能有按鍵記錄器。

修補

若要變更密碼政策，請參閱《IAM 使用者指南》中的〈設定 IAM 使用者的帳戶密碼政策〉。在 [開啟密碼到期時間] 中，輸入**90**或較小的數字。

[IAM.18] 確保已建立支援角色來管理事件 AWS Support

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.20，獨聯體基金會基準 v1.4.0/1.17 AWS

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::::Account`

AWS Config 規則：`iam-policy-in-use`

排程類型：定期

參數：

- `policyARN`：`arn:partition:iam::aws:policy/AWSSupportAccess`（不可定制）
- `policyUsageType`：`ANY`（不可定制）

AWS 提供支援中心，可用於事件通知和回應，以及技術支援和客戶服務。

建立 IAM 角色，讓授權使用者透過 Sup AWS port 管理事件。透過對存取控制實施最低權限，IAM 角色將需要適當的 IAM 政策來允許支援中心存取，以便管理事件 AWS Support。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修正此問題，請建立角色以允許授權的使用者管理 AWS Support 事件。

若要建立用於 AWS Support 存取的角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在 IAM 導覽窗格中，選擇「角色」，然後選擇「建立角色」。
3. 對於 [角色類型]，選擇 [其他] AWS 帳戶。
4. 在「帳戶 AWS 帳戶 ID」中，輸入您 AWS 帳戶 要授與資源存取權的 ID。

   如果將擔任此角色的使用者或群組位在相同帳戶，則請輸入本機帳戶號碼。

> **Note**
>
> 指定帳戶的管理員可以授予許可給該帳戶中的任何 使用者來擔任此角色。若要執行此操作，管理員要將政策連接到授予 `sts:AssumeRole` 動作之許可的使用者或群組。在該政策中，資源必須是角色 ARN。

5. 選擇下一步：許可。
6. 搜尋受管政策 `AWSSupportAccess`。
7. 選取 `AWSSupportAccess` 受管政策的核取方塊。
8. 選擇下一步：標籤。
9. (選擇性) 若要將中繼資料新增至角色，請將標籤附加為索引鍵值配對。

   如需在 IAM 中使用標籤的詳細資訊，請參閱 IAM 使用者指南中的標記 IAM 使用者和角色。
10. 選擇下一步：檢閱。
11. 針對 Role name (角色名稱)，輸入您的角色名稱。

    角色名稱在您的 AWS 帳戶. 不區分大小寫。
12. (選用) 在 Role description (角色說明) 中，輸入新角色的說明。
13. 檢閱角色，然後選擇 Create role (建立角色)。

[IAM.19] 應為所有 IAM 使用者啟用 MFA

相關要求：PCI DSS V3.2.1/8.3.1、指定交流 -2 (1)、指定信號交流 -3 (15)、介質管理系統交流 -3 (15)、iA-2 (1)、日本 iA-2 (6)、iS.800-53.IA-2 (2)、

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::IAM::User`

AWS Config 規則：`iam-user-mfa-enabled`

排程類型：定期

參數：無

此控制項會檢查 IAM 使用者是否已啟用多重要素驗證 (MFA)。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要為 IAM 使用者新增 MFA，請參閱《IAM 使用者指南》中 AWS的〈為使用者啟用 MFA 裝置〉。

[IAM.20] 避免使用根用戶

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：獨聯體 AWS 基金會基準 v1.2.0/1.1

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::IAM::User`

AWS Config 規則:`use-of-root-account-test`(自訂 Security Hub 規則)

排程類型：定期

參數：無

此控制項會檢查是否 AWS 帳戶 有 root 使用者的使用限制。控制項會評估下列資源：

- Amazon Simple Notification Service (Amazon SNS) 主題
- AWS CloudTrail 小徑
- 與 CloudTrail 軌跡相關聯的度量過濾器
- 基於過濾器 Amazon CloudWatch 警報

如果下列一或多個陳述式成立，則此檢查會導致FAILED發現：

- 帳戶中不存在 CloudTrail 追蹤。
- CloudTrail 追蹤已啟用，但未設定至少一個包含讀取和寫入管理事件的多區域追蹤。
- 系 CloudTrail 統已啟用追蹤，但未與 CloudWatch 記錄記錄群組相關聯。
- 不使用網際網路安全中心 (CIS) 規定的確切度量篩選器。規定的度量過濾器是`'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`。
- 帳戶中不存在以量度篩選器為基礎的 CloudWatch 警示。
- CloudWatch 設定為傳送通知至相關 SNS 主題的警示不會根據警示條件觸發。
- SNS 主題不符合傳送訊息至 SNS 主題的限制條件。
- SNS 主題至少沒有一個訂閱者。

NO_DATA如果下列一或多個陳述式為 true，則此檢查會導致控制狀態：

- 多區域追蹤是以不同區域為基礎。Security Hub 只能在追蹤所在的區域中產生發現項目。
- 多區域追蹤屬於不同的帳戶。Security Hub 只能針對擁有追蹤的帳戶產生發現項目。

WARNING如果下列一或多個陳述式為 true，則此檢查會導致控制狀態：

- 當前帳戶不擁有 CloudWatch 警報中引用的 SNS 主題。
- 當前帳戶在調用 SNS API 時無法訪問 `ListSubscriptionsByTopic` SNS 主題。

> **Note**
>
> 我們建議您使用組織追蹤記錄組織中多個帳戶的事件。組織追蹤預設為多區域追蹤，且只能由管 AWS Organizations 理帳戶或 CloudTrail 委派的系統管理員帳戶管理。針對組織成員帳戶中評估的控制項，使用組織軌跡會導致 NO_DATA 的控制項狀態。在成員帳戶中，Security Hub 只會針對成員擁有的資源產生發現項目。與組織軌跡相關的發現項目會在資源擁有者的帳號中產生。您可以使用跨區域彙總，在 Security Hub 委派的系統管理員帳戶中查看這些發現項目。

最佳做法是，只有在需要執行帳戶和服務管理工作時才使用 root 使用者認證。將 IAM 政策直接套用至群組和角色，但不套用至使用者。如需設定管理員供日常使用的指示，請參閱 IAM 使用者指南中的建立您的第一個 IAM 管理員使用者和群組。

修補

解決此問題的步驟包括設定 Amazon SNS 主題、 CloudTrail追蹤、指標篩選器以及指標篩選器的警示。

建立 Amazon SNS 主題

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 建立接收所有獨聯體警示的 Amazon SNS 主題。

   至少建立一個主題訂閱者。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

接下來，設置一個適用 CloudTrail 於所有區域的活動。若要執行此作業，請遵循 the section called "[CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤" 中的修補步驟。

記下您與 CloudTrail 追蹤相關聯的 CloudWatch 記錄日誌群組名稱。您可以建立該記錄群組的度量篩選器。

最後，創建度量過濾器和警報。

建立指標篩選條件和警示

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 Log groups (日誌群組)。
3. 選取與您建立 CloudTrail 之追蹤相關聯之「 CloudWatch 記錄」記錄群組的核取方塊。
4. 從「動作」 中選擇「建立量度篩選」。
5. 在定義陣列之下，執行下列操作：

   a. 複製以下模式，然後將它貼入 Filter Pattern (篩選條件模式) 欄位。

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. 選擇下一步。
6. 在「指派量度」下，執行下列操作：

   a. 在 [篩選器名稱] 中，輸入量度篩選器的名稱。

b. 針對測量結果命名空間，輸入 **LogMetrics**

如果您對所有 CIS 日誌指標過濾器使用相同的命名空間，則所有 CIS Benchmark 指標都會分組在一起。

c. 在「測量結果名稱」中，輸入測量結果的名稱。記住指標的名稱。建立警示時，您將需要選取指標。

d. 針對 Metric value (指標值)，輸入 **1**。

e. 選擇下一步。

7. 在「檢閱並建立」下，確認您為新量度篩選器提供的資訊。然後，選擇「建立量度篩選器」。
8. 在功能窗格中，選擇 [記錄群組]，然後選擇您在 [指標篩選器] 下建立的篩選器。
9. 選取篩選器的核取方塊。選擇 Create alarm (建立警示)。
10. 在「指定量度和條件」下，執行下列操作：

a. 在「條件」下，選擇「靜態」做為臨界值。

b. 針對「定義警示條件」，選擇「大於/等於」。

c. 對於 「定義臨界值」，輸入**1**。

d. 選擇下一步。

11. 在「設定動作」 下，執行下列動作：

a. 在 [警報狀態觸發] 下，選擇 [在警報中]

b. 在 Select an SNS topic (選取 SNS 主題) 下，選擇 Select an existing SNS topic (選取現有的 SNS 主題)。

c. 在「傳送通知至」中，輸入您在上一個程序中建立的 SNS 主題的名稱。

d. 選擇下一步。

12. 在 [新增名稱和說明] 下，輸入警示的 [名稱] 和 [說明]，例如**CIS-1.1-RootAccountUsage**。然後選擇下一步。
13. 在 [預覽並建立] 下，檢閱警示組態。然後選擇 Create Alarm (建立警示)。

[IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作

相關要求：交流 -2、交流 -2、交流 -2 (1)、指定交流 -3、指定交流 -3、指定交流 -5 (15)、交流 -3 (15)、交流 -3 (7)、指定交流 -3 (7)、交流 5 (10)、交流 -6 (2), 日本交流 -6 (2), 交流 -6 (3)

類別:偵測裝置 > 安全存取管理

嚴重性：低

資源類型：AWS::IAM::Policy

AWS Config 規則：iam-policy-no-statements-with-full-access

排程類型：已觸發變更

參數：

- excludePermissionBoundaryPolicy：True（不可定制）

此控制項會檢查您建立的 IAM 身分型政策是否具有使用 * 萬用字元的 Allow 陳述式，針對任何服務上的所有動作授與許可。如果任何原則陳述式包含"Effect": "Allow"與，則控制項會失敗"Action": "Service:*"。

例如，策略中的下列陳述式會導致發現失敗。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

如果與一"Effect": "Allow"起使用，控制項也會失敗"NotAction": "*service*:*"。在這種情況下，NotAction元素可讓您存取中所有動作 AWS 服務，但中指定的動作除外NotAction。

此控制僅適用於客戶受管 IAM 政策。它不適用於由管理的 IAM 政策 AWS。

將許可指派給時 AWS 服務，請務必在 IAM 政策中設定允許的 IAM 動作範圍。您應該將 IAM 動作限制為只有需要的動作。這可協助您佈建最低權限權限。如果政策附加到可能不需要許可的 IAM 主體，則過於寬鬆的政策可能會導致權限提升。

在某些情況下，您可能想要允許具有類似前置詞的 IAM 動作，例如DescribeFlowLogs和DescribeAvailabilityZones。在這些授權的情況下，您可以在通用前綴中添加一個後綴的萬用字符。例如 ec2:Describe*。

如果您使用帶有尾碼萬用字元的前置 IAM 動作，則此控制項會通過。例如，原則中的下列陳述式會導致傳遞的發現項目。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

以這種方式將相關 IAM 動作分組時，也可以避免超過 IAM 政策大小限制。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。但是，可以在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修正此問題，請更新您的 IAM 政策，使其不允許完整的「*」管理權限。如需如何編輯 IAM 政策的詳細資訊，請參閱 IAM 使用者指南中的編輯 IAM 政策。

[IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料

相關要求：獨聯體 AWS 基金會基準指標 v1.4.0/1.12

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::IAM::User`

AWS Config 規則：**`iam-user-unused-credentials-check`**

排程類型：定期

參數：無

此控制項可檢查 IAM 使用者是否擁有 45 天以上未使用的密碼或作用中存取金鑰。若要這樣做，它會檢查 AWS Config 規則的`maxCredentialUsageAge`參數是否等於 45 或更多。

使用者可以使用不同類型的認證來存取 AWS 資源，例如密碼或存取金鑰。

CIS 建議您移除或停用 45 天以上未使用的所有憑證。停用或移除不必要的登入資料，可以減少使用與被盜用或放棄帳戶相關聯登入資料的機會。

此控制 AWS Config 項的規則使用`GetCredentialReport`和 `GenerateCredentialReport`API 作業，這些作業只會每四小時更新一次。IAM 使用者的變更最多可能需要四個小時才能看到此控制項。

> **Note**
>
> AWS Config 應該在您使用安全中心的所有區域中啟用。不過，您可以在單一區域中啟用全域資源的記錄功能。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

當您在 IAM 主控台中檢視使用者資訊時，存取金鑰有效期、密碼存留時間和上次活動等欄位。如果這些資料行中的值大於 45 天，請讓這些使用者的認證處於非作用中狀態。

您也可以使用認證報告來監控使用者，並識別 45 天以上沒有活動的使用者。您可以從 IAM 主控台下載`.csv`格式的認證報告。

識別非作用中的帳戶或未使用的認證後，請停用它們。如需指示，請參閱 IAM 使用者指南中的建立、變更或刪除 IAM 使用者密碼 (主控台)。

Amazon Kinesis 控制

這些控制項與 Kinesis 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Kinesis.1] Kinesis 串流應該在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::Kinesis::Stream`

AWS Config 規則：`kinesis-stream-encrypted`

排程類型：已觸發變更

參數：無

此控制項可檢查 Kinesis Data Streams 是否已使用伺服器端加密進行靜態加密。如果 Kinesis 串流未使用伺服器端加密進行靜態加密，則此控制項會失敗。

伺服器端加密是 Amazon Kinesis Data Streams 中的一項功能，可在資料處於靜態狀態之前自動加密。 AWS KMS key資料會在寫入 Kinesis 串流儲存層之前加密，並在從儲存體擷取資料後解密。因此，您的資料會在 Amazon Kinesis Data Streams 服務中進行靜態加密。

修補

如需為 Kinesis 串流啟用伺服器端加密的相關資訊，請參閱如何開始使用伺服器端加密？ 在 Amazon Kinesis 開發人員指南中。

AWS Key Management Service 控制

這些控制項與資 AWS KMS 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作

相關要求：交流 -2、交流 -2、交流 -2 (1)、指定交流 -3、指定交流 -3、指定交流 -5 (15)、交流 -3 (15)、交流 -3 (7)、指定交流 -3 (7)、指令碼

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::IAM::Policy`

AWS Config 規則：`iam-customer-policy-blocked-kms-actions`

排程類型：已觸發變更

參數：

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`（不可定制）
- `excludePermissionBoundaryPolicy`：`True`（不可定制）

檢查 IAM 客戶受管政策的預設版本是否允許主體對所有資源使用 AWS KMS 解密動作。如果政策足夠開放以允許kms:Decrypt或對所有 KMS 金鑰kms:ReEncryptFrom執行動作，則控制項會失敗。

控制項只會檢查資源項目中的 KMS 金鑰，而且不會考慮原則的「條件」元素中的任何條件。此外，控制項還會評估附加和未連接的客戶管理政策。它不會檢查內嵌政策或 AWS 受管理的政策。

您可以透過控制哪些人可以使用 KMS 金鑰 AWS KMS，並存取加密資料。IAM 政策定義身分識別 (使用者、群組或角色) 可對哪些資源執行的動作。遵循安全性最佳作法， AWS 建議您允許最低權限。換句話說，您應該僅授與kms:Decrypt或kms:ReEncryptFrom權限，並僅授與執行工作所需的金鑰。否則，使用者可能會使用不適合您資料的金鑰。

決定使用者存取加密資料所需的最小金鑰集，而不是授與所有金鑰的權限。然後設計原則，讓使用者只能使用這些金鑰。例如，不允kms:Decrypt許所有 KMS 金鑰的權限。相反，kms:Decrypt只允許您帳戶的特定區域中的密鑰。通過採用最低權限原則，您可以降低數據意外披露的風險。

修補

若要修改 IAM 客戶受管政策，請參閱《IAM 使用者指南》中的編輯客戶受管政策。編輯政策時，請為Resource欄位提供您要允許解密動作之特定金鑰的 Amazon 資源名稱 (ARN)。

[KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策

相關要求：交流 -2、交流 -2、交流 -2 (1)、指定交流 -3、指定交流 -3、指定交流 -5 (15)、交流 -3 (15)、交流 -3 (7)、指定交流 -3 (7)、指令碼

類別：保護 > 安全存取管理

嚴重性：中

資源類型：

- AWS::IAM::Group
- AWS::IAM::Role
- AWS::IAM::User

AWS Config 規則：iam-inline-policy-blocked-kms-actions

排程類型：已觸發變更

參數：

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`（不可定制）

此控制項會檢查 IAM 身分 (角色、使用者或群組) 中內嵌的內嵌政策是否允許對所有 KMS 金鑰執行 AWS KMS 解密和重新加密動作。如果政策足夠開放以允許`kms:Decrypt`或對所有 KMS 金鑰`kms:ReEncryptFrom`執行動作，則控制項會失敗。

控制項只會檢查資源項目中的 KMS 金鑰，而且不會考慮原則的「條件」元素中的任何條件。

您可以透過控制哪些人可以使用 KMS 金鑰 AWS KMS，並存取加密資料。IAM 政策定義身分識別 (使用者、群組或角色) 可對哪些資源執行的動作。遵循安全性最佳作法， AWS 建議您允許最低權限。換句話說，您應該僅授與身分識別所需的權限，並僅授與執行工作所需的金鑰。否則，使用者可能會使用不適合您資料的金鑰。

決定使用者存取加密資料所需的最小金鑰集，而不是授與所有金鑰的權限。然後設計原則，讓使用者只能使用這些金鑰。例如，不允`kms:Decrypt`許所有 KMS 金鑰的權限。而是僅允許您帳戶的特定區域中特定密鑰的權限。通過採用最低權限原則，您可以降低數據意外披露的風險。

修補

若要修改 IAM 內嵌政策，請參閱《IAM 使用者指南》中的編輯內嵌政策。編輯政策時，請為`Resource`欄位提供您要允許解密動作之特定金鑰的 Amazon 資源名稱 (ARN)。

不應意外刪除 [KMS AWS KMS keys .3]

相關要求：SC-12, 日本電腦 -53.5 SC-12 (2)

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：嚴重

資源類型：`AWS::KMS::Key`

AWS Config 規則:`kms-cmk-not-scheduled-for-deletion-2`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已排程刪除 KMS 金鑰。如果已排程刪除 KMS 金鑰，則控制項會失敗。

KMS 金鑰一旦刪除，就無法復原。如果刪除 KMS 金鑰，則使用 KMS 金鑰加密的資料也會永久無法復原。如果已使用排定要刪除的 KMS 金鑰加密有意義的資料，請考慮將資料解密或以新 KMS 金鑰重新加密資料，除非您有意執行加密刪除。

排定刪除 KMS 金鑰時，如果排程發生錯誤，則會強制執行強制等待期，以允許有時間還原刪除作業。預設等待期為 30 天，但在排定刪除 KMS 金鑰時，可縮短至最短 7 天。在等待期間，可以取消排定的刪除，並且不會刪除 KMS 金鑰。

如需有關刪除 KMS 金鑰的其他資訊，請參閱AWS Key Management Service 開發人員指南中的刪除 KMS 金鑰。

修補

若要取消已排程的 KMS 金鑰刪除，請參閱開AWS Key Management Service 發人員指南中的排程和取消金鑰刪除 (主控台) 下的若要取消金鑰刪除。

[KMS.4] AWS KMS 按鍵旋轉應該已啟用

相關要求：PCI DSS V3.2.1/3.6.4，獨聯體 AWS 基礎基準測試 v1.2.0/2.8，獨聯體基礎 AWS 基準測試 V1.4.0/3.8，NIS.800-53.R5 SC-12，尼斯 SC-12 SC-28

嚴重性：中

資源類型：`AWS::KMS::Key`

AWS Config 規則：`cmk-backing-key-rotation-enabled`

排程類型：定期

參數：無

AWS KMS 可讓客戶輪換備份金鑰，這是儲存在 AWS KMS KMS 金鑰的金鑰 ID 中的金鑰材料。它是用來執行加密操作的備份金鑰，例如加密和解密。自動化輪換金鑰目前會保留之前所有的備份金鑰，以便透明解密加密的資料。

CIS 建議您啟用 KMS 金鑰輪替。輪換加密金鑰有助於降低被盜用金鑰造成的可能影響，因為可能公開的舊金鑰無法存取使用新金鑰加密的資料。

修補

若要啟用 KMS 金鑰輪換，請參閱AWS Key Management Service 開發人員指南中的如何啟用和停用自動金鑰輪換。

AWS Lambda 控制

這些控制項與 Lambda 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Lambda 1] Lambda 函數政策應該禁止公共訪問

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.2、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/7.2.1、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::Lambda::Function`

AWS Config 規則：`lambda-function-public-access-prohibited`

排程類型：已觸發變更

參數：無

此控制項會檢查 Lambda 函數資源型政策是否禁止在帳戶外進行公開存取。如果允許公開存取，則控制項會失敗。如果從 Amazon S3 叫用 Lambda 函數，且該政策不包含限制公用存取的條件，則控制項也會失敗，例如`AWS:SourceAccount`。我們建議您在儲存貯體政策`AWS:SourceAccount`中使用其他 S3 條件，以獲得更完善的存取。

Lambda 函數不應該可公開存取，因為這可能會允許非預期地存取您的函數程式碼。

修補

若要修正此問題，您必須更新函數的以資源為基礎的政策，以移除權限或新增條件`AWS:SourceAccount`。您只能從 Lambda API 或 AWS CLI更新以資源為基礎的政策。

若要開始，請在 Lambda 主控台上檢閱以資源為基礎的政策。識別具有可公開原則之`Principal`欄位值的原則陳述式，例如`"*"`或`{ "AWS": "*" }`。

您無法從控制台編輯策略。若要移除函數的權限，請從中執行`remove-permission`命令 AWS CLI。

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

取代*<function-name>*為 Lambda 函數的名稱，*<statement-id>*以及您要移除之陳述式的陳述式 ID (Sid)。

[Lambda 2] Lambda 函數應該使用受支援的執行階段

相關要求：第七八十三條路卡 -9 (1)、等級 5 公分 (2)、指定信號：800-53.R5 SI-2 (2)、指定信號 -53.R5 系統 -2 (4)、等級

類別：保護 > 安全開發

嚴重性：中

資源類型：AWS::Lambda::Function

AWS Config 規則：lambda-function-settings-check

排程類型：已觸發變更

參數：

- runtime：dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2（不可定制）

此控制項會檢查執行階段的 Lambda 函數設定是否符合針對每種語言支援執行階段設定的預期值。如果 Lambda 函數不使用受支援的執行階段，則控制項會失敗。

控制項會檢查先前在參數下註明的執行階段的功能設定。Security Hub 會忽略套件類型為的函式Image。

Lambda 執行階段是以作業系統、程式設計語言和軟體程式庫的組合為基礎，這些程式庫會受到維護和安全性更新的影響。當安全性更新不再支援執行階段元件時，Lambda 會棄用執行階段。即使您無法建立使用已停用執行階段的函數，該函數仍可用於處理叫用事件。我們建議確保您的 Lambda 函數是最新的，並且不要使用已過時的執行階段環境。如需支援的執行階段清單，請參閱AWS Lambda 開發人員指南中的 Lambda 執行階段。

修補

有關支持的運行時間和棄用計劃的更多信息，請參閱開發人員指AWS Lambda 南中的運行時棄用策略。當將執行時間遷移至最新版本時，請遵循語言發佈者提供的語法和指導。我們也建議您套用執行階段更新，以協助減少在執行階段版本不相容的罕見情況下對工作負載造成影響的風險。

[Lambda 3] Lambda 函數應該在 VPC 中

相關要求：PCI DSS v3.2.1/1.2.1、PCI 資料管理系統 V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.2、PCI DSS V3.2.1/1.3.4、技術支援 DSS V3.2.1/1.3.4、指令介面 (AC-21)、解密技術 -53.R5 交流 -3 (7)、21)，星期五交流 -6, 星期五, 星期五七, 星期五七 (11), 尼斯特. 800-53.R5 (16), 星期五七七 (20), 尼斯特. 800-53.R5 (20), SC-7 (4), 日本七星期五 (9)

嚴重性：低

資源類型：`AWS::Lambda::Function`

AWS Config 規則：**`lambda-inside-vpc`**

排程類型：已觸發變更

參數：無

此控制項可檢查 Lambda 函數是否部署在虛擬私有雲 (VPC) 中。如果 Lambda 函數未部署在 VPC 中，則控制項會失敗。Security Hub 不會評估 VPC 子網路路由組態來判斷公用連線能力。您可能會看到 Lambda @Edge 資源的失敗發現項目。

在 VPC 中部署資源可增強網路組態的安全性和控制能力。此類部署也提供跨多個可用區域的延展性和高容錯能力。您可以自訂 VPC 部署以滿足各種應用程式需求。

修補

若要將現有功能設定為連線至 VPC 中的私有子網路，請參閱開發人員指南中的設定 VPC 存取。AWS Lambda 我們建議至少選擇兩個私有子網路以獲得高可用性，並至少選擇一個符合功能連線需求的安全性群組。

VPC Lambda 函數應在多個可用區域中運作

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::Lambda::Function`

AWS Config 規則：`lambda-vpc-multi-az-check`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
availabilityZones	可用區域的最小數目	列舉	2, 3, 4, 5, 6	2

此控制項會檢查連線至虛擬私有雲端 (VPC) 的 AWS Lambda 函數是否至少在指定數目的可用區域 (AZ) 中運作。如果函數至少在指定的 AZ 數目中運作，則控制項會失敗。除非您為最小 AZ 數目提供自訂參數值，否則 Security Hub 會使用兩個 AZ 的預設值。

在多個 AZ 之間部署資源是確保架構內具有高可用性的 AWS 最佳實務。可用性是機密性、完整性和可用性三合會安全性模型的核心支柱。連接到 VPC 的所有 Lambda 函數都應具有異地同步備份部署，以確保單一故障區域不會導致作業中斷。

修補

如果您將功能設定為連線到帳戶中的 VPC，請在多個 AZ 中指定子網路以確保高可用性。如需指示，請參閱AWS Lambda 開發人員指南中的設定 VPC 存取權。

Lambda 會在多個 AZ 中自動執行其他函數，以確保在單一區域發生服務中斷時，可以處理事件。

Amazon Macie 控制

這些控制項與 Macie 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Macie.1] Amazon Macie 應該啟用

相關要求：NIS.800-53.R5 CA-7、鎳鋅 -53.R5 鈣 -9 (1)、日本電腦 -53.R5 R5、NIS.800-53.R5 S-8 (19)、日本

類別：偵測 > 偵測服務

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`macie-status-check`

排程類型：定期

此控制項會檢查帳戶是否已啟用 Amazon Macie。如果未為帳戶啟用 Macie，則控制項會失敗。

Amazon Macie 會使用機器學習和模式比對來探索敏感資料、提供資料安全風險的可見性，並提供自動化保護以防範這些風險。Macie 會自動持續評估 Amazon Simple Storage Service (Amazon S3) 儲存貯體的安全性和存取控制，並產生發現結果以通知您 Amazon S3 資料的安全性或隱私權存在潛在問題。Macie 也會自動化敏感資料 (例如個人識別資訊 (PII)) 的探索和報告，讓您更好地瞭解存放在 Amazon S3 中的資料。若要進一步了解，請參閱 Amazon Macie 使用者指南。

修補

若要啟用 Macie，請參閱 Amazon Macie 使用者指南中的啟用 Macie。

[Macie.2] 應啟用 Macie 自動化敏感資料探索功能

相關要求：NIS.800-53.R5 CA-7、鎳鋅 -53.R5 鈣 -9 (1)、日本電腦 -53.R5 R5、NIS.800-53.R5 S-8 (19)、日本

類別：偵測 > 偵測服務

嚴重性：高

資源類型：`AWS::::Account`

AWS Config 規則：`macie-auto-sensitive-data-discovery-check`

排程類型：定期

此控制項可檢查 Amazon Macie 管理員帳戶是否啟用自動化敏感資料探索功能。如果沒有為 Macie 管理員帳戶啟用自動敏感資料探索，則控制項會失敗。此控制項僅適用於管理員帳戶。

Macie 會在亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體中自動探索和報告敏感資料，例如個人識別資訊 (PII)。透過自動化的敏感資料探索功能，Macie 會持續評估儲存貯體庫存，並使用取樣技術，從儲存貯體中識別和選取具代表性的 S3 物件。然後 Macie 會分析選取的物件，檢查它們是否有敏感資料。隨著分析的進展，Macie 會更新其提供有關 S3 資料的統計資料、庫存資料和其他資訊。Macie 也會產生發現項目，以報告找到的敏感資料。

修補

若要建立和設定自動化敏感資料探索任務以分析 S3 儲存貯體中的物件，請參閱 Amazon Macie 使用者指南中的為您的帳戶設定自動化敏感資料探索。

Amazon MSK 控制

這些控制項與 Apache 卡夫卡 (Amazon MSK) 資源的 Amazon 受管串流有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密

相關要求：東西 800-53.R5 交流 4、SC-13、等級 800-53.R5 SC-23、等級 800-53.R5 SC-23 (3)、電子信號 -53.R5 (4)、等級 800-53.R5 (4)、等級 -53.R5 SC-8、

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：`AWS::MSK::Cluster`

AWS Config 規則：`msk-in-cluster-node-require-tls`

排程類型：已觸發變更

參數：無

此控制項可檢查傳輸中 Amazon MSK 叢集是否在叢集的代理程式節點之間使用 HTTPS (TLS) 加密。如果叢集代理程式節點連線啟用純文字通訊，則控制項會失敗。

HTTPS 使用 TLS 移動資料，因此提供了額外的安全層，並可用來協助防止潛在攻擊者利用 person-in-the-middle 或類似攻擊來竊聽或操控網路流量。依預設，Amazon MSK 會使用 TLS 加密傳輸中的資料。但是，您可以在建立叢集時覆寫此預設值。我們建議使用透過 HTTPS (TLS) 代理節點連線的加密連線。

修補

若要更新 MSK 叢集的加密設定，請參閱 Amazon Apache Kafka 受管串流開發人員指南中的更新叢集的安全設定。

[MSK.2] MSK 叢集應該已設定增強型監控功能

相關要求：NIS.800-53.R5 CA-7、尼斯

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::MSK::Cluster

AWS Config 規則：msk-enhanced-monitoring-enabled

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon MSK 叢集是否已設定增強型監控，這些監控層級至少PER_TOPIC_PER_BROKER指定為。如果叢集的監視層級設為DEFAULT或，則控制項會失敗PER_BROKER。

PER_TOPIC_PER_BROKER監控層級可提供更精細的 MSK 叢集效能洞察，並提供與資源使用率相關的指標，例如 CPU 和記憶體使用率。這可協助您識別個別主題和代理程式的效能瓶頸和資源使用模式。反過來，這種可見性可以優化您的卡夫卡經紀人的性能。

修補

若要設定 MSK 叢集的增強型監控，請完成以下步驟：

1. 開啟 Amazon MSK 主控台，網址為 https://console.aws.amazon.com/msk/home?region=us-east-1#/home/。
2. 在導覽窗格中，選擇叢集。然後，選擇叢集。
3. 對於動作，選取編輯監視。
4. 選取 [增強型主題層級監視] 選項。
5. 選擇儲存變更。

如需監控層級的詳細資訊，請參閱 Amazon Apache Kafka 受管串流開發人員指南中的更新叢集的安全設定。

Amazon MQ 控制

這些控制項與 Amazon MQ 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：低

資源類型：`AWS::AmazonMQ::Broker`

AWS Config 規則：`mq-active-deployment-mode`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ ActiveMQ 代理程式的部署模式是否設定為作用中/待命。如果將單一執行個體代理程式 (預設為啟用) 設定為部署模式，則控制項會失敗。

主動/待命部署為您的 Amazon MQ ActiveMQ 代理程式提供高可用性。 AWS 區域主動/待命部署模式包括兩個不同可用區域中的兩個代理程式執行個體 (以備援配對設定)。這些代理程式會與您的應用程式同步通訊，以減少故障時間的停機時間和資料遺失。

修補

若要使用主動/待命部署模式建立新的 ActiveMQ 代理程式，請參閱 Amazon MQ 開發人員指南中的建立和設定 ActiveMQ 代理程式。對於部署模式，請選擇作用中/待命代理程式。您無法變更現有代理程式的部署模式。相反，您必須創建一個新的代理並從舊代理複製設置。

[MQ.6] RabbitMQ 代理程式應該使用叢集部署模式

相關要求：CP-10、NIS.800-53.R5 CP-6 (2)、日本電腦 800-53.R5 SC-36、NIST-53.R5 SC-5 (2)、等級 800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：低

資源類型：`AWS::AmazonMQ::Broker`

AWS Config 規則：`mq-rabbit-deployment-mode`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ RabbitMQ 代理程式的部署模式是否設定為叢集部署。如果將單一執行個體代理程式 (預設為啟用) 設定為部署模式，則控制項會失敗。

叢集部署為您的 Amazon MQ RabbitMQ 代理程式提供高可用性。 AWS 區域叢集部署是由三個 RabbitMQ 代理程式節點組成的邏輯分組，每個節點都有自己的 Amazon Elastic Block Store (Amazon EBS) 磁碟區和一個共用狀態。叢集部署可確保將資料複製到叢集中的所有節點，如此可在發生故障時減少停機時間和資料遺失。

修補

若要使用叢集部署模式建立新的 RabbitMQ 代理程式，請參閱 Amazon MQ 開發人員指南中的建立和連接 RabbitMQ 代理程式。對於部署模式，請選擇叢集部署。您無法變更現有代理程式的部署模式。相反，您必須創建一個新的代理並從舊代理複製設置。

Amazon Neptune 控

這些控制項與 Neptune 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[Neptune .1] Neptune DB 叢集在靜態時應加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-encrypted`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否在靜態時加密。如果 Neptune 資料庫叢集未在靜態時加密，則控制項會失敗。

靜態數據是指任何持續時間存儲在持久性非易失性存儲中的任何數據。加密可協助您保護此類資料的機密性，降低未經授權使用者存取資料的風險。加密 Neptune DB 叢集可保護您的資料和中繼資料，防止未經授權的存取。它還滿足了生產文件系統 data-at-rest 加密的合規要求。

修補

您可以在建立 Neptune 資料庫叢集時啟用靜態加密。建立叢集後，您無法變更加密設定。如需詳細資訊，請參閱 Neptune 使用者指南中的靜態加密 Neptune 資源。

[Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.R5、尼斯 -53.R5、八月五日至五月六日 (3), 日本六月六日 (4), 尼斯 .800-53.R5 澳洲 6 (5), 尼斯. 800-53.R5 (7), 尼斯. 800-53.R5 (7), Nist.800-53.5 (7), 尼斯, 尼斯 .800-53.R5 四 (8), 尼斯特. AU-12 SI-20

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-cloudwatch-log-export-enabled`

排程類型：已觸發變更

參數：無

此控制項可檢查 Neptune 資料庫叢集是否將稽核日誌發佈到 Amazon CloudWatch 日誌。
如果 Neptune 資料庫叢集未將稽核記錄發佈至 CloudWatch 記錄，則控制項會失敗。
`EnableCloudWatchLogsExport`應該設定為`Audit`。

整合了 Amazon Neptune 和 Amazon CloudWatch ，因此您可以收集和分析效能指標。Neptune 會自動將指標傳送至 CloudWatch 警報，也支援 CloudWatch 警示。審核日誌是高度可定制的。當您稽核資料庫時，可以監督資料上的每項作業，並將其記錄到稽核歷程檔中，包括存取哪個資料庫叢集以及存取方式的相關資訊。我們建議您傳送這些記錄檔， CloudWatch 以協助您監視 Neptune 資料庫叢集。

修補

若要將 Neptune 稽核日誌發佈到 CloudWatch 日誌，請參閱 Neptune 使用者指南中的將 Neptune CloudWatch 日誌發佈到 Amazon 日誌。在 [記錄匯出] 區段中，選擇 [稽核]。

[Neptune .3] Neptune DB 叢集快照不應該是公開的

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網路設定 > 無法公開存取的資源

嚴重性：嚴重

資源類型：`AWS::RDS::DBClusterSnapshot`

AWS Config 規則：`neptune-cluster-snapshot-public-prohibited`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 手動資料庫叢集快照集是否為公用。如果 Neptune 手動資料庫叢集快照集為公用，則控制項會失敗。

除非有意，否則 Neptune 資料庫叢集手動快照不應為公用。如果您將未加密的手動快照共用為公用，則所有 AWS 帳戶人都可以使用該快照。公開快照可能會導致非預期的資料暴露。

修補

若要移除 Neptune 手動資料庫叢集快照的公開存取權，請參閱 Neptune 使用者指南中的共用資料庫叢集快照。

[Neptune .4] Neptune 資料庫叢集應啟用刪除保護

相關要求：鎳鋅 -53.R5 路卡 -9 (1)、指定 5 公分 (5 公分)、電子信號 -53.R5 公分 (2)、電子顯示器 -53.R5 公分 (3)、電子顯示器 -53.R5 SC-5 (2)

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-deletion-protection-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否已啟用刪除保護。如果 Neptune 資料庫叢集未啟用刪除保護，則控制項會失敗。

啟用叢集刪除保護可提供額外的保護層，防止未經授權的使用者意外刪除資料庫或刪除。啟用刪除保護時，無法刪除 Neptune 資料庫叢集。您必須先停用刪除保護，刪除要求才能成功執行。

修補

若要為現有 Neptune 資料庫叢集啟用刪除保護，請參閱 Amazon Aurora 使用者指南中的使用主控台、CLI 和 API 修改資料庫叢集。

[Neptune .5] Neptune 資料庫叢集應啟用自動備份

相關要求：SI-12

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-backup-retention-check`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`minimumBackupRetentionPeriod`	最短備份保留期 (天)	Integer	7 設定為 35	7	

此控制項會檢查 Neptune DB 叢集是否已啟用自動備份，以及備份保留期間是否大於或等於指定的時間範圍。如果 Neptune DB 叢集未啟用備份，或保留期間小於指定的時間範圍，則控制項會失敗。除非您為備份保留期提供自訂參數值，否則 Security Hub 會使用預設值 7 天。

備份可協助您更快速地從安全性事件中復原，並強化系統的復原能力。透過自動化 Neptune DB 叢集的備份，您將能夠將系統還原到某個時間點，並將停機時間和資料遺失降到最低。

修補

若要啟用自動備份並為 Neptune 資料庫叢集設定備份保留期，請參閱 Amazon RDS 使用者指南中的啟用自動備份。對於 Backup 保留期，請選擇大於或等於 7 的值。

[Neptune .6] Neptune 資料庫叢集快照在靜態時應加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::RDS::DBClusterSnapshot`

AWS Config 規則：`neptune-cluster-snapshot-encrypted`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集快照集是否在靜態時加密。如果 Neptune 資料庫叢集未在靜態時加密，則控制項會失敗。

靜態數據是指任何持續時間存儲在持久性非易失性存儲中的任何數據。加密可協助您保護此類資料的機密性，降低未經授權使用者存取資料的風險。Neptune DB 叢集快照中的資料應該在靜態時加密，以增加一層安全性。

修補

您無法加密現有的 Neptune 資料庫叢集快照集。相反地，您必須將快照還原到新的資料庫叢集，並在叢集上啟用加密。您可以從加密的叢集建立加密快照。如需指示，請參閱 Neptune 使用指南中的從資料庫叢集快照還原和在 Neptune 中建立資料庫叢集快照。

[Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證

相關要求：交流 -2 (1)、交流 3 (1)、尼什八達 -53.R5 交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、日本交流 -6

分類:安全防護 > 安全存取管理 > 無密碼認證

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-iam-database-authentication`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否已啟用 IAM 資料庫驗證。如果未為 Neptune 資料庫叢集啟用 IAM 資料庫驗證，則控制項會失敗。

適用於 Amazon Neptune 資料庫叢集的 IAM 資料庫身份驗證無需在資料庫組態中存放使用者登入資料，因為身份驗證是使用 IAM 從外部管理 啟用 IAM 資料庫身份驗證後，每個請求都必須使用簽 AWS 名版本 4 進行簽署。

修補

根據預設，當您建立 Neptune 資料庫叢集時，會停用 IAM 資料庫驗證。若要啟用它，請參閱 Neptune 使用者指南中的啟用 Neptune 中的 IAM 資料庫身份驗證。

[Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別:識別 > 庫存 > 標籤

嚴重性：低

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-copy-tags-to-snapshot-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune DB 叢集是否設定為在建立快照時將所有標記複製到快照。如果 Neptune 資料庫叢集未設定為將標籤複製到快照，則控制項會失敗。

識別和清查您的 IT 資產是治理和安全性的關鍵方面。您應該使用與其父系 Amazon RDS 資料庫叢集相同的方式標記快照。複製標籤可確保資料庫快照的中繼資料與父資料庫叢集的中繼資料相符，而資料庫快照的存取原則也符合父資料庫執行個體的存取原則。

修補

若要將標籤複製到 Neptune 資料庫叢集的快照，請參閱 Neptune 使用者指南中的複製 Neptune 中的標籤。

[Neptune .9] Neptune 資料庫叢集應部署在多個可用區域

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`neptune-cluster-multi-az-enabled`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon Neptune 資料庫叢集是否在多個可用區域 (AZ) 中具有僅供讀取複本執行個體。如果叢集僅部署在一個 AZ 中，則控制項會失敗。

如果 AZ 無法使用，且在定期維護事件期間，僅供讀取複本會做為主要執行個體的容錯移轉目標。亦即，如果主要執行個體失敗，則 Neptune 會提升僅供讀取複本以成為主要執行個體。相反地，如果您的資料庫叢集不包含任何僅供讀取複本執行個體，則當主要執行個體失敗時，資料庫叢集仍無法使用，直到重新建立為止。重新建立主要執行個體所花費的時間比提升僅供讀取複本要長得多。為確保高可用性，建議您建立一或多個僅供讀取複本執行個體，這些執行個體與主執行個體具有相同的資料庫執行個體類別，且位於與主執行個體不同的 AZ 中。

修補

若要在多個 AZ 中部署 Neptune 資料庫叢集，請參閱 Neptune 使用者指南中的 Neptune 資料庫叢集中的僅供讀取複本資料庫執行個體。

AWS Network Firewall 控制

這些控制項與 Network Firewall 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::NetworkFirewall::Firewall`

AWS Config 規則：`netfw-multi-az-enabled`

排程類型：已觸發變更

參數：無

此控制項會評估透過管理的防火牆 AWS Network Firewall 是否跨多個可用區域 (AZ) 部署。如果防火牆僅部署在一個 AZ 中，則控制項會失敗。

AWS 全球基礎設施包括多個 AWS 區域。AZ 是每個區域內實體分離且隔離的位置，透過低延遲、高輸送量和高度備援的網路連線。透過在多個 AZ 上部署 Network Firewall 防火牆，您可以平衡和轉移 AZ 之間的流量，進而協助您設計高可用性解決方案。

修補

跨多個 AZ 部署 Network Firewall 防火牆

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 [Network Firewall] 下，選擇 [防火牆]。
3. 在「防火牆」頁面上，選取您要編輯的防火牆。
4. 在防火牆詳細資料頁面上，選擇防火牆詳細資料標籤。
5. 在 [關聯的原則和 VPC] 區段中，選擇 [編輯]
6. 若要新增 AZ，請選擇 [新增子網路]。選取您要使用的 AZ 和子網路。請確定您至少選取兩個 AZ。

7. 選擇儲存。

[NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄

相關要求：交流 -53.R5 (12)、交流電 -2 (4)、奈特。800-53.R5 交流 -6 (9)、尼斯特。800-53.R5 交流 -6 (9)、黑色 -53.R5、AU-10、六月五日 (3), 尼斯 .800-53.R5 (4), 日本 6 星期六 (4), 尼斯 .800-53.R5 (7), 尼斯 .800-53.R5 SC-7 (9), 尼斯 .800-53.R5 (9),), 尼斯 .800-53.R5 四七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::NetworkFirewall::LoggingConfiguration`

AWS Config 規則：`netfw-logging-enabled`

排程類型：定期

參數：無

此控制項會檢查 AWS Network Firewall 防火牆是否已啟用記錄。如果未啟用至少一種記錄類型的記錄，或記錄目的地不存在，則控制項會失敗。

記錄可協助您維護防火牆的可靠性、可用性和效能。在 Network Firewall 中，記錄會提供有關網路流量的詳細資訊，包括狀態引擎接收封包流程的時間、封包流程的詳細資訊，以及針對封包流程採取的任何可設定狀態規則動作。

修補

若要啟用防火牆的記錄功能，請參閱AWS Network Firewall 開發人員指南中的更新防火牆的記錄設定。

[NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

分類:保護 > 安全網絡配置

嚴重性：中

資源類型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 規則：netfw-policy-rule-group-associated

排程類型：已觸發變更

參數：無

此控制項會檢查 Network Firewall 策略是否有任何關聯的可設定狀態或無狀態規則群組。如果未指派無狀態或可設定狀態的規則群組，則控制項會失敗。

防火牆政策定義防火牆如何監控和處理 Amazon Virtual Private Cloud (Amazon VPC) 中的流量。無狀態和可設定狀態規則群組的組態有助於篩選封包和流量流程，並定義預設流量處理。

修補

若要將規則群組新增至 Network Firewall 政策，請參閱AWS Network Firewall 開發人員指南中的更新防火牆政策。如需有關建立和管理規則群組的資訊，請參閱中的規則群組 AWS Network Firewall。

[NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

分類:保護 > 安全網絡配置

嚴重性：中

資源類型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 規則：netfw-policy-default-action-full-packets

排程類型：已觸發變更

參數：

- statelessDefaultActions: aws:drop,aws:forward_to_sfe（不可定制）

此控制項會檢查 Network Firewall 原則完整封包的預設無狀態處理行動是捨棄還是轉送。如果選取Drop或Forward，則會通過控制項，如果選取，Pass則會失敗。

防火牆政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為Pass可允許非預期的流量。

修補

若要變更您的防火牆政策，請參閱AWS Network Firewall 開發人員指南中的更新防火牆政策。針對「無狀態」預設動作，選擇 「編輯」。然後，選擇 [移除] 或 [轉寄至可設定狀態規則群組] 做為 [動作]。

[NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

分類:保護 > 安全網絡配置

嚴重性：中

資源類型：`AWS::NetworkFirewall::FirewallPolicy`

AWS Config 規則：`netfw-policy-default-action-fragment-packets`

排程類型：已觸發變更

參數：

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe` (不可定制)

此控制項會檢查「Network Firewall」原則之片段封包的預設無狀態動作是捨棄還是轉送。如果選取`Drop`或`Forward`，則會通過控制項，如果選取，`Pass`則會失敗。

防火牆政策定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為`Pass`可允許非預期的流量。

修補

若要變更您的防火牆政策，請參閱AWS Network Firewall 開發人員指南中的更新防火牆政策。針對「無狀態」預設動作，選擇 「編輯」。然後，選擇 [移除] 或 [轉寄至可設定狀態規則群組] 做為 [動作]。

[NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空

相關要求：七點五交流四 (21)、日本七點七、七點七 (11)、日本七點七 (11)、七點五、七七 (16)、日本顯示 .800-53.R5 (21)、

分類:保護 > 安全網絡配置

嚴重性：中

資源類型：AWS::NetworkFirewall::RuleGroup

AWS Config 規則：netfw-stateless-rule-group-not-empty

排程類型：已觸發變更

參數：無

此控制項會檢查中的無狀態規則群組是否 AWS Network Firewall 包含規則。如果規則群組中沒有規則，控制項就會失敗。

規則群組包含定義防火牆如何處理 VPC 中流量的規則。如果防火牆策略中存在空的無狀態規則群組，可能會給人以為規則群組會處理流量的印象。但是，當無狀態規則群組為空時，不會處理流量。

修補

若要將規則新增至 Network Firewall 規則群組，請參閱AWS Network Firewall 開發人員指南中的更新可設定狀態規則群組。在防火牆詳細資料頁面上，對於無狀態規則群組，選擇編輯以新增規則。

[NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護

相關要求：鎳鋅 -53.R5 路卡 -9 (1)、指定 5 公分 (5 公分)、電子信號 -53.R5 公分 (2)、電子顯示器 -53.R5 公分 (3)、電子顯示器 -53.R5 SC-5 (2)

分類:保護 > 網絡安全 > 高可用性

嚴重性：中

資源類型：AWS::NetworkFirewall::Firewall

AWS Config 規則：netfw-deletion-protection-enabled

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Network Firewall 防火牆是否已啟用刪除保護。如果未啟用防火牆的刪除保護，則控制項會失敗。

AWS Network Firewall 是可設定狀態的受管網路防火牆和入侵偵測服務，可讓您檢查和篩選進出虛擬私人雲端 (VPC) 或之間的流量。刪除保護設定可防止意外刪除防火牆。

修補

若要在現有的 Network Firewall 防火牆上啟用刪除防護，請參閱AWS Network Firewall 開發人員指南中的更新防火牆。對於 [變更保護]，選取 [啟用]。您也可以透過呼叫 UpdateFirewallDeleteProtectionAPI 並將`DeleteProtection``true`欄位設定為來啟用刪除保護。

Amazon OpenSearch 服務控制

這些控制項與 OpenSearch 服務資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

OpenSearch 網域應啟用靜態加密功能

相關要求：PCI DSS V3.2.1/1.2.1、PCI 資料管理系統 (DSS) 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/7.2.1、信號卡 -9 (1)、電子信息管理系統 SC-28 (1), 尼斯·五七七 (6) SC-13 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::OpenSearch::Domain`

AWS Config 規則：`opensearch-encrypted-at-rest`

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用 encryption-at-rest 組態。如果未啟用靜態加密，則檢查會失敗。

若要為敏感資料提供額外的安全性，您應該將 OpenSearch Service 網域設定為靜態加密。當您設定靜態資料的加密時，會 AWS KMS 儲存和管理您的加密金鑰。若要執行加密，請 AWS KMS 使用 256 位元金鑰的進階加密標準演算法 (AES-256)。

若要進一步了解靜態 OpenSearch 服務加密，請參閱 Amazon 服務開發人員指南中的 Amazon OpenSearch 服 OpenSearch 務靜態資料加密。

修補

若要為新網域和現有 OpenSearch 網域啟用靜態加密，請參閱 Amazon Ser OpenSearch vice 開發人員指南中的啟用靜態資料加密。

[打開搜索 .2] OpenSearch 域名不應該是公開訪問

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

分類:保護 > 安全網絡配置 > VPC 內的資源

嚴重性：嚴重

資源類型：`AWS::OpenSearch::Domain`

AWS Config 規則：`opensearch-in-vpc-only`

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否位於 VPC 中。它不會評估 VPC 子網路路由組態來決定公用存取權。

您應該確定網 OpenSearch 域未附加至公用子網路。請參閱 Amazon OpenSearch 服務開發人員指南中以資源為基礎的政策。您也應該確保您的 VPC 已根據建議的最佳實務進行設定。請參閱 Amazon VPC 使用者指南中適用於 VPC 的安全性最佳實務。

OpenSearch VPC 內部署的網域可透過私人 AWS 網路與 VPC 資源通訊，而不需要周遊公用網際網路。此組態會限制對傳輸中資料的存取，以提高安全性狀態。VPC 提供許多網路控制來保護網 OpenSearch 域存取安全，包括網路 ACL 和安全性群組。Security Hub 建議您將公用 OpenSearch 網域移轉至 VPC，以利用這些控制項。

修補

如果您建立了具備公有端點的網域，您稍後便無法將其置放於 VPC 內。反之，您必須建立新網域並遷移您的資料。反之亦然。如果您在 VPC 中建立了網域，該網域便無法擁有公有端點。您必須改為建立另一個網域或停用此控制項。

如需指示，請參閱 Amazon OpenSearch 服務開發人員指南中的在 VPC 中啟動 Amazon OpenSearch 服務網域。

OpenSearch 網域應該加密節點之間傳送的資料

相關要求：東西 800-53.R5 交流 4、SC-13、等級 800-53.R5 SC-23、等級 800-53.R5 SC-23 (3)、電子信號 -53.R5 (4)、等級 800-53.R5 (4)、等級 -53.R5 SC-8、

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::OpenSearch::Domain`

AWS Config 規則：`opensearch-node-to-node-encryption-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用 node-to-node 加密。如果在網域上停用 node-to-node 加密，則此控制項會失敗。

HTTPS (TLS) 可用來協助防止潛在攻擊者透過或類似攻擊竊取網路流量或操控網路流量 person-in-the-middle 。只能允許透過 HTTPS (TLS) 進行加密連線。啟用 OpenSearch 網域 node-to-node 加密可確保叢集內部通訊在傳輸過程中加密。

可能會有與此配置相關的性能損失。在啟用此選項之前，您應該注意並測試效能權衡。

修補

若要在 OpenSearch 網域上啟用 node-to-node 加密，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用 node-to-node 加密。

應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：opensearch-logs-to-cloudwatch

排程類型：已觸發變更

參數：

- logtype = 'error'（不可定制）

此控制項會檢查 OpenSearch 網域是否設定為將錯誤記錄檔傳送至 CloudWatch 記錄檔。如果網域未啟用錯誤記錄， CloudWatch 則此控制項會失敗。

您應該啟用 OpenSearch 網域的錯誤記錄檔，並將這些記錄檔傳送至 CloudWatch 記錄檔以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。

修補

若要啟用日誌發佈，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用日誌發佈 (主控台)。

OpenSearch 網域應該已啟用稽核記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：opensearch-audit-logging-enabled

排程類型：已觸發變更

參數：

- cloudWatchLogsLogGroupArnList(無法自訂) — Security Hub 不會填入此參數。應針對稽核 CloudWatch 記錄設定的記錄檔記錄群組清單 (逗號分隔)。

此規則是NON_COMPLIANT如果未在此參數清單中指定 OpenSearch網域的 CloudWatch 記錄檔群組。

此控制項會檢查 OpenSearch 網域是否已啟用稽核記錄。如果 OpenSearch 網域未啟用稽核記錄，則此控制項會失敗。

審核日誌是高度可定制的。它們可讓您追蹤OpenSearch 叢集上的使用者活動，包括驗證成功與失敗、要OpenSearch求、索引變更以及傳入的搜尋查詢。

修補

如需啟用稽核日誌的指示，請參閱 Amazon OpenSearch 服務開發人員指南中的啟用稽核日誌。

OpenSearch 網域應該至少有三個資料節點

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：opensearch-data-node-fault-tolerance

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否設定至少有三個資料節點，而且zoneAwarenessEnabled是true。如果 OpenSearch 網域小於 3 或instanceCountzoneAwarenessEnabled是，則此控制項會失敗false。

OpenSearch 網域至少需要三個資料節點才能達到高可用性和容錯能力。部署具有至少三個資料節點的 OpenSearch 網域可確保在節點失敗時進行叢集作業。

修補

若要修改 OpenSearch 網域中的資料節點數目

1. 登錄到 AWS 控制台並打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/。

2. 在「我的網域」下，選擇要編輯的網域名稱，然後選擇「編輯」。
3. 在 [資料節點] 下，將節點數目設定為大於的數字3。如果您要部署到三個可用區域，請將數字設定為三個的倍數，以確保跨可用區域的平均分配。
4. 選擇提交。

OpenSearch 網域應該啟用精細的存取控制

相關要求：交流 -2 (1)、交流 3 (1)、尼斯特。800-53.R5 交流 -3 (15)、指定交流 -3 (7)、指定交流 -3 (7)、指定交流 -6

類別:保護 > 安全存取管理 > 受限制的敏感 API 動作

嚴重性：高

資源類型：`AWS::OpenSearch::Domain`

AWS Config 規則：`opensearch-access-control-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用精細的存取控制。如果未啟用精細的存取控制，則控制項會失敗。精細的存取控制需要`advanced-security-options`在 OpenSearch 參數`update-domain-config`中啟用。

精細的存取控制提供了控制 Amazon OpenSearch 服務上資料存取的其他方式。

修補

若要啟用精細的存取控制，請參閱 Amazon 服務開發人員指南中的 Amazon OpenSearch 服務中的精細存取控制。 OpenSearch

應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接

相關要求：東西 800-53.R5 AC-17 (2), 交流 -4, 奈特. 800-53.R5 IA-5 (1), 奈特. 800-53.R5 (3), 尼斯. 800-53.R5 SC-13, 奈特. 七月八日 (5), 日本八分之五 (1), 星期六 (5), 七月八日 (6) SC-12 SC-23 SC-23

分類:保護 > 資料保護 > 加密 data-in-transit

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：opensearch-https-required

排程類型：已觸發變更

參數：

- tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10（不可定制）

此控制項會檢查 Amazon OpenSearch 服務網域的連線是否使用最新的 TLS 安全政策。如果 OpenSearch 網域未使用最新的支援原則或未啟用 HTTPS，則控制項會失敗。

HTTPS (TLS) 可用來協助防止潛在攻擊者利用 person-in-the-middle 或類似攻擊來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能來測試應用程式，以瞭解效能設定檔和 TLS 的影響。相較於舊版 TLS，TLS 1.2 提供了多項安全性增強功能。

修補

若要啟用 TLS 加密，請使用 UpdateDomainConfigAPI 作業。設定要設定的DomainEndpointOptions欄位TLSSecurityPolicy。如需詳細資訊，請參閱 Amazon OpenSearch 服務開發人員指南中的 Node-to-node 加密。

OpenSearch 網域應該已安裝最新的軟體更新

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五、五四 (4)、七月五四 (5)

類別:偵測 > 漏洞、修補程式和版本管理

嚴重性：低

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：opensearch-update-check

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon OpenSearch 服務網域是否已安裝最新的軟體更新。如果有軟體更新可用，但網域尚未安裝，則控制項會失敗。

OpenSearch 服務軟體更新提供適用於環境的最新平台修正、更新和功能。保持安 up-to-date 裝修補程式有助於維護網域安全性和可用性。如果未對所需的更新採取任何動作，服務軟體會自動更新 (通常在 2 週後)。我們建議您在網域的低流量期間排程更新，以將服務中斷的情況降到最低。

修補

若要安裝 OpenSearch 網域的軟體更新，請參閱 Amazon OpenSearch 服務開發人員指南中的開始更新。

AWS Private Certificate Authority 控制

這些控制項與資 AWS Private CA 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[PCA.1] AWS Private CA 根憑證授權單位應停用

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：低

資源類型：`AWS::ACMPCA::CertificateAuthority`

AWS Config 規則：`acm-pca-root-ca-disabled`

排程類型：定期

參數：無

此控制項會檢查是否 AWS Private CA 有已停用的根憑證授權單位 (CA)。如果啟用根 CA，則控制項會失敗。

使用時 AWS Private CA，您可以建立包含根 CA 和從屬 CA 的 CA 階層。對於日常工作，尤其是在生產環境中，您應該盡量減少根 CA 的使用。根 CA 應該只用於發行中繼 CA 的憑證。這可以讓您透過不會造成損害的方式存放根 CA，並讓中繼 CA 執行發行終端實體憑證的日常任務。

修補

若要停用根 CA，請參閱AWS Private Certificate Authority 使用指南中的更新 CA 狀態。

Amazon Relational Database Service 控制

這些控制項與 Amazon RDS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[RDS.1] RDS 快照應該是私有的

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.6、PCI 資料管理系統 V3.2.1/7.2.1、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 規則：`rds-snapshots-public-prohibited`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 快照是否為公開狀態。如果 RDS 快照集是公用的，則控制項會失敗。此控制項可評估 RDS 執行個體、Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集。

RDS 快照會用來備份特定時間點您 RDS 執行個體上的資料。快照可以用來還原 RDS 執行個體先前的狀態。

除非預期，否則 RDS 快照不應處於公有狀態。如果您以公開方式共用未加密的手動快照，這會讓所有 AWS 帳戶人都可以使用快照。這可能會導致意外公開您 RDS 執行個體的資料。

請注意，如果將組態變更為允許公開存取， AWS Config 則規則最多可能會在 12 小時內無法偵測到變更。在 AWS Config 規則偵測到變更之前，即使組態違反規則，檢查仍會通過。

若要進一步了解共用資料庫快照，請參閱 Amazon RDS 使用者指南中的共用資料庫快照。

修補

若要從 RDS 快照移除公開存取，請參閱 Amazon RDS 使用者指南中的共用快照。對於資料庫快照的可見性，我們選擇私人。

[RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config

相關要求：PCI DSS V3.2.1/1.2.1、PCI DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.2、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、PCI DSS V3.2.1/7.2.1、插入式資料管理系統 V3.2.1/7.2.1、，日本七月七日 (11), 日本七點七 (16), 日本七星期七 (16), 尼斯 .800-53.R5 SC-7 (4), 日本七星期七 (4), 日本七點七 (4)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：`rds-instance-public-access-check`

排程類型：已觸發變更

參數：無

此控制項會透過評估執行個體組態項目中的`PubliclyAccessible`欄位來檢查 Amazon RDS 執行個體是否可公開存取。

Neptune 資料庫執行個體和 Amazon DocumentDB 叢集沒有`PubliclyAccessible`旗標，因此無法進行評估。不過，這個控制項仍然可以產生這些資源的發現項目。您可以隱藏這些發現項目。

RDS 執行個體組態中的 `PubliclyAccessible` 值會指出資料庫執行個體是否可以公開存取。將資料庫執行個體設為 `PubliclyAccessible` 時，其為具有可公開解析 DNS 名稱的面向網際網路執行個體，且此名稱可解析為公有 IP 地址。當無法公開存取資料庫執行個體時，其為具備解析為私有 IP 地址 DNS 名稱的內部執行個體。

除非您打算讓 RDS 執行個體可公開存取，否則 RDS 執行個體不應設定`PubliclyAccessible`值。這樣做可能會允許不必要的資料庫執行個體流量。

修補

若要移除 RDS 資料庫執行個體的公開存取權，請參閱 Amazon RDS 使用者指南中的修改 Amazon RDS 資料庫執行個體。對於「公共訪問」，請選擇否。

[RDS.3] RDS 資料庫執行個體應啟用靜態加密

相關要求：獨聯體 AWS 基礎基礎基準測試 V1.4.0/2.3.1，電腦 -53.R5 鈣 -9（1），等等。SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：`rds-storage-encrypted`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon RDS 資料庫執行個體是否已啟用儲存加密。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以針對 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集產生發現項目。如果這些發現是沒有用的，那麼你可以抑制它們。

如需為您在 RDS 資料庫執行個體中的敏感資料新增多一層安全，建議您設定 RDS 資料庫執行個體進行靜態加密。如要加密您的 RDS 資料庫執行個體和靜態快照，請為您的 RDS 資料庫執行個體啟用加密選項。靜態加密的資料包括資料庫執行個體的基礎儲存體、其自動化備份、僅供讀取複本，以及快照。

RDS 加密資料庫執行個體會使用開放標準 AES-256 加密演算法，來加密託管 RDS 資料庫執行個體伺服器上的資料。加密資料後，Amazon RDS 會透明地處理資料的存取和解密身份驗證，對效能的影響降到最低。您不需要修改資料庫用戶端應用程式即可使用加密。

Amazon RDS 加密目前適用於所有資料庫引擎和儲存類型。大多數資料庫執行個體類別可以使用 Amazon RDS 加密。若要了解不支援 Amazon RDS 加密的資料庫執行個體類別，請參閱 Amazon RDS 使用者指南中的加密 Amazon RDS 資源。

修補

如需在 Amazon RDS 中加密資料庫執行個體的相關資訊，請參閱 Amazon RDS 使用者指南中的加密 Amazon RDS 資源。

[RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型:`AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 規則：`rds-snapshot-encrypted`

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫快照是否已加密。如果 RDS 資料庫快照未加密，則控制項會失敗。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以針對 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集的快照產生發現結果。如果這些發現是沒有用的，那麼你可以抑制它們。

靜態資料加密可降低未經驗證的使用者存取儲存在磁碟上之資料的風險。RDS 快照中的資料應在靜態時加密，以增加一層安全性。

修補

若要加密 RDS 快照，請參閱 Amazon RDS 使用者指南中的加密 Amazon RDS 資源。加密 RDS 資料庫執行個體時，加密的資料會包含執行個體的基礎儲存體、其自動備份、僅供讀取複本和快照。

您只能在建立 RDS 資料庫執行個體時加密，而不能在建立資料庫執行個體之後加密。不過，因為您可以加密未加密快照的副本，所以可以有效地將加密新增至未加密的資料庫執行個體。亦即，您可以建立資料庫執行個體的快照，然後建立該快照的加密副本。接著，從加密快照中還原資料庫執行個體，因此您有原始資料庫執行個體的加密副本。

[RDS.5] RDS 資料庫執行個體應設定為多個可用區域

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：rds-multi-az-support

排程類型：已觸發變更

參數：無

此控制項可檢查 RDS 資料庫執行個體是否已啟用高可用性。

RDS 資料庫執行個體應針對多個可用區域 (AZ) 設定。這樣可以確保存儲的數據的可用性。異地同步備份部署允許自動容錯移轉，如果 AZ 可用性發生問題，以及在定期 RDS 維護期間。

修補

若要在多個 AZ 中部署資料庫執行個體，請參閱 Amazon RDS 使用者指南，將資料庫執行個體修改為異地同步備份資料庫執行個體部署。

[RDS.6] 應為 RDS 資料庫執行個體設定增強型監控

相關要求：NIS.800-53.R5 CA-7、尼斯

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config 規則：rds-enhanced-monitoring-enabled

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
monitoringInterval	監督測量結果收集間隔之間的秒數	列舉	1, 5, 10, 15, 30, 60	無預設值	

此控制項可檢查 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫執行個體是否啟用增強型監控功能。如果未針對執行個體啟用增強型監控，則控制項會失敗。如果您提供`monitoringInterval`參數的自訂值，則只有在指定間隔收集執行處理的增強型監督測量結果時，控制項才會傳遞。

在 Amazon RDS 中，增強型監控可以更快速地回應基礎設施中的效能變更。這些效能變更可能會導致資料的可用性不足。增強型監控提供 RDS 資料庫執行個體所在作業系統的即時指標。代理程式已安裝在執行個體上。代理程式可以比 Hypervisor 層更準確地取得指標。

如果您想查看資料庫執行個體上不同的程序或執行緒如何使用 CPU，增強型監控指標可以派上用場。如需詳細資訊，請參閱 Amazon RDS User Guide (《Amazon RDS 使用者指南》) 中的 Enhanced Monitoring (增強型監控)。

修補

如需為資料庫執行個體啟用增強型監控的詳細指示，請參閱 Amazon RDS 使用者指南中的設定和啟用增強型監控。

[RDS.7] RDS 叢集應該已啟用刪除保護

相關要求：電腦 -53.R5 公分 -3、電子信箱

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`rds-cluster-deletion-protection-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫叢集是否已啟用刪除保護。如果 RDS 資料庫叢集未啟用刪除保護，則控制項會失敗。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以針對 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集產生發現項目。如果這些發現是沒有用的，那麼你可以抑制它們。

啟用叢集刪除保護是一個額外的保護層，防止未經授權的實體意外刪除資料庫或刪除。

啟用刪除保護時，無法刪除 RDS 叢集。刪除要求成功之前，必須先停用刪除保護。

修補

若要啟用 RDS 資料庫叢集的刪除保護，請參閱 Amazon RDS 使用者指南中的使用主控台、CLI 和 API 修改資料庫叢集。對於刪除保護，請選擇啟用刪除保護。

[RDS.8] RDS 資料庫執行個體應啟用刪除保護

相關要求：NIS.800-53.R5 公分-三、電腦五、六、五、五、五、五、五、SI-13 (5)

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：`rds-instance-deletion-protection-enabled`

排程類型：已觸發變更

參數：

- `databaseEngines`：`mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web`（不可定制）

此控制項會檢查使用其中一個所列資料庫引擎的 RDS 資料庫執行個體是否已啟用刪除保護。如果 RDS 資料庫執行個體未啟用刪除保護，則控制項會失敗。

啟用執行個體刪除保護是一個額外的保護層，防止未經授權的實體意外刪除資料庫或刪除。

啟用刪除保護時，無法刪除 RDS 資料庫執行個體。刪除要求成功之前，必須先停用刪除保護。

修補

若要啟用 RDS 資料庫執行個體的刪除保護，請參閱 Amazon RDS 使用者指南中的修改 Amazon RDS 資料庫執行個體。對於刪除保護，請選擇啟用刪除保護。

[RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 尼斯 .800-53.R5 介質-七, 日本七點七 (10), 尼斯 .800-53.R5 四 (8), 尼斯 .800-53.R5 系統 -3 (8), 星期五四 (20), AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：rds-logging-enabled

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon RDS 資料庫執行個體是否設定為將下列日誌發佈到 Amazon CloudWatch 日誌。如果執行個體未設定為將下列記錄檔發佈到記錄檔，則控制項會失敗： CloudWatch

- Oracle：(警示、稽核、追蹤、監聽器)
- PostgreSQL: (後期, 升級)
- MySQL：（審核，錯誤，一般， SlowQuery ）
- MariaDB：（審計，錯誤，一般， ） SlowQuery
- SQL 伺服器：（錯誤，代理程式）
- Aurora：（審核，錯誤，一般， SlowQuery ）
- 極光-MySQL 的：（審計，錯誤，一般， ） SlowQuery
- 極光後：（PostgreSQL 級）。

RDS 資料庫應該已啟用相關記錄。數據庫日誌記錄提供對 RDS 發出的請求的詳細記錄。資料庫記錄可協助進行安全性和存取稽核，並協助診斷可用性問題。

修補

若要將 RDS 資料庫日誌發佈到 CloudWatch 日誌，請參閱 Amazon RDS 使用者指南中的指定要發佈到 CloudWatch 日誌的日誌。

[RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證

相關要求：交流 -2 (1)、交流 3 (1)、尼什八達 -53.R5 交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、日本交流 -6

分類:安全防護 > 安全存取管理 > 無密碼認證

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：rds-instance-iam-authentication-enabled

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫執行個體是否已啟用 IAM 資料庫驗證。如果未針對 RDS 資料庫執行個體設定 IAM 身分驗證，則控制項會失敗。此控制項只會評估具有下列引擎類型的 RDS 執行個體：mysqlpostgresauroraaurora-mysql、、aurora-postgresql、、和mariadb。RDS 執行個體也必須處於下列其中一種狀態，才能產生發現項目：availablebacking-upstorage-optimization、、或storage-full。

IAM 資料庫身份驗證允許使用身份驗證令牌而不是密碼對數據庫實例進行身份驗證 進出資料庫的網路流量使用 SSL 加密。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 IAM 資料庫身分驗證。

修補

若要在 RDS 資料庫執行個體上啟用 IAM 資料庫身份驗證，請參閱 Amazon RDS 使用者指南中的啟用和停用 IAM 資料庫身份驗證。

[RDS.11] RDS 執行個體應該已啟用自動備份

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：db-instance-backup-enabled

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`backupRetentionMinimum`	最短備份保留期 (天)	Integer	7 設定為 35	7	
`checkReadReplicas`	檢查 RDS 資料庫執行個體是否已啟用僅供讀取複本的備份	Boolean	不可定制	`false`	

此控制項可檢查 Amazon Relational Database Service 執行個體是否已啟用自動備份，以及備份保留期間是否大於或等於指定的時間範圍。僅供讀取複本會從評估中排除。如果未啟用執行個體的備份，或保留期間小於指定的時間範圍，則控制項會失敗。除非您為備份保留期提供自訂參數值，否則 Security Hub 會使用預設值 7 天。

備份可協助您更快速地從安全性事件中復原，並加強系統的彈性。Amazon RDS 可讓您設定每日完整執行個體磁碟區快照。如需 Amazon RDS 自動備份的詳細資訊，請參閱 Amazon RDS 使用者指南中的使用備份。

修補

若要在 RDS 資料庫執行個體上啟用自動備份，請參閱 Amazon RDS 使用者指南中的啟用自動備份。

[RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證

相關要求：交流 -2 (1)、交流 3 (1)、尼什八達 -53.R5 交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、日本交流 -6

分類:安全防護 > 安全存取管理 > 無密碼認證

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`rds-cluster-iam-authentication-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 資料庫叢集是否已啟用 IAM 資料庫身份驗證。

IAM 資料庫身份驗證允許對資料庫執行個體進行無密碼驗證。驗證使用驗證令牌。進出資料庫的網路流量使用 SSL 加密。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 IAM 資料庫身分驗證。

修補

若要為資料庫叢集啟用 IAM 身份驗證，請參閱 Amazon Aurora 使用者指南中的啟用和停用 IAM 資料庫身份驗證。

應啟用 RDS 自動次要版本升級

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五、五四 (4)、七月五四 (5)

類別:檢測 > 漏洞和補丁管理

嚴重性：高

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：`rds-automatic-minor-version-upgrade-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫執行個體是否啟用自動次要版本升級。

啟用自動次要版本升級可確保已安裝關聯式資料庫管理系統 (RDBMS) 的最新次要版本更新。這些升級可能包括安全性修補程式和錯誤修正。保持最新的修補程式安裝是保護系統的重要步驟。

修補

若要啟用現有資料庫執行個體的自動次要版本升級，請參閱 Amazon RDS 使用者指南中的修改 Amazon RDS 資料庫執行個體。對於自動次要版本升級，請選取是。

[RDS.14] Amazon Aurora 叢集應啟用回溯

相關要求：指定信息 CP-10，指定信息處理器 6，指定點 -53.R5 CP-6（1），指定信息：800-53.R5 CP-6（2），指定信息：800-53.R5 CP-9，指定信號 SI-13

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`aurora-mysql-backtracking-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`BacktrackWindowInHours`	回溯 Aurora MySQL 叢集的小時數	Double	`0.1` 設定為 `72`	無預設值	

此控制項會檢查 Amazon Aurora 叢集是否已啟用回溯功能。如果叢集沒有啟用回溯，則控制項會失敗。如果您為`BacktrackWindowInHours`參數提供自訂值，則只有在回溯至指定的時間長度內，控制項才會通過。

備份可協助您更快速地從安全性事件中復原。它們還可以增強系統的彈性。Aurora 回溯可減少將資料庫復原到某個時間點的時間。它不需要數據庫還原即可執行此操作。

修補

若要啟用 Aurora 回溯，請參閱 Amazon Aurora 使用者指南中的設定回溯。

請注意，您無法在現有叢集上啟用回溯。相反地，您可以建立已啟用回溯的翻製。如需 Aurora 回溯限制的詳細資訊，請參閱回溯概觀中的限制清單。

[RDS.15] 應為多個可用區域設定 RDS 資料庫叢集

相關要求：指定的 CP-10，電腦 -53.R5 CP-6 (2)，日本電腦 800-53.R5 SC-36，日本電腦 -53.R5 SC-5 (2)，日期：800-53.R5 SI-13 (5)

分類:復原 > 復原能力 > 高可用性

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`rds-cluster-multi-az-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫叢集是否已啟用高可用性。如果 RDS 資料庫叢集未部署在多個可用區域 (AZ) 中，則控制項會失敗。

RDS 資料庫叢集應設定為多個 AZ，以確保已儲存資料的可用性。部署到多個 AZ 允許在 AZ 可用性問題和定期 RDS 維護事件期間進行自動容錯移轉。

修補

若要在多個 AZ 中部署資料庫叢集，請參閱 Amazon RDS 使用者指南，將資料庫執行個體修改為異地同步備份資料庫執行個體部署。

Aurora 全域資料庫的補救步驟不同。若要為 Aurora 全域資料庫設定多個可用區域，請選取您的資料庫叢集。然後，選擇「動作」 和「新增閱讀器」，然後指定多個 AZ。如需詳細資訊，請參閱 Amazon Aurora 使用者指南中的將 Aurora 複本新增至資料庫叢集。

[RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別：識別 > 清查

嚴重性：低

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則:`rds-cluster-copy-tags-to-snapshots-enabled`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫叢集是否設定為在建立快照時將所有標籤複製到快照。

識別和清查您的 IT 資產是治理和安全性的關鍵方面。您必須掌握所有 RDS 資料庫叢集，才能評估其安全狀態，並針對潛在的弱點區域採取行動。快照的標記方式應與其父項 RDS 資料庫叢集相同。啟用此設定可確保快照集會繼承其父項資料庫叢集的標記。

修補

若要自動將標籤複製到 RDS 資料庫叢集的快照，請參閱 Amazon Aurora 使用者指南中的使用主控台、CLI 和 API 修改資料庫叢集。選取「複製標籤到快照」。

[RDS.17] RDS 資料庫執行個體應設定為將標籤複製到快照

相關要求：鎳碳酸鈣 -9 (1)、微信五公分二 (2)

類別：識別 > 清查

嚴重性：低

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則:`rds-instance-copy-tags-to-snapshots-enabled`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫執行個體是否設定為在建立快照時將所有標籤複製到快照。

識別和清查您的 IT 資產是治理和安全性的關鍵方面。您必須掌握所有 RDS 資料庫執行個體的能見度，以便評估其安全狀態並針對潛在弱點區域採取行動。快照的標記方式應與其父項 RDS 資料庫執行個體相同。啟用此設定可確保快照集會繼承其父項資料庫執行處理的標記。

修補

若要自動將標籤複製到 RDS 資料庫執行個體的快照，請參閱 Amazon RDS 使用者指南中的修改 Amazon RDS 資料庫執行個體。選取「複製標籤到快照」。

虛擬私人雲端應部署 RDS 執行 VPC

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網絡配置 > VPC 內的資源

嚴重性：高

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則:`rds-deployed-in-vpc`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 執行個體是否已部署在 EC2-VPC 上。

VPC 提供許多網路控制，以確保 RDS 資源的存取安全。這些控制項包括 VPC 端點、網路 ACL 和安全群組。若要利用這些控制項，建議您在 EC2-VPC 上建立 RDS 執行個體。

修補

如需將 RDS 執行個體移至 VPC 的指示，請參閱 Amazon RDS 使用者指南中的更新資料庫執行個體的 VPC。

[RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱

相關要求：NIS.800-53.R5 CA-7、尼斯

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::RDS::EventSubscription`

AWS Config 規則:`rds-cluster-event-notifications-configured`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項可檢查資料庫叢集的現有 Amazon RDS 事件訂閱是否已啟用下列來源類型和事件類別索引鍵值配對的通知：

```
DBCluster: ["maintenance","failure"]
```

如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

RDS 事件通知使用 Amazon SNS 來讓您了解 RDS 資源的可用性或組態的變更。這些通知允許快速響應。如需有關 RDS 事件通知的其他資訊，請參閱 Amazon RDS 使用者指南中的使用 Amazon RDS 事件通知。

修補

若要訂閱 RDS 叢集事件通知，請參閱 Amazon RDS 使用者指南中的訂閱 Amazon RDS 事件通知。使用下列的值：

欄位	Value
來源類型	叢集
要包含的叢集	所有叢集
要包含的活動類別	選擇特定活動類別或所有活動類別

[RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱

相關要求：NIS.800-53.R5 CA-7、尼斯

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::RDS::EventSubscription`

AWS Config 規則:`rds-instance-event-notifications-configured`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項可檢查資料庫執行個體的現有 Amazon RDS 事件訂閱是否已啟用下列來源類型和事件類別索引鍵值配對的通知：

```
DBInstance: ["maintenance","configuration change","failure"]
```

如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

RDS 事件通知使用 Amazon SNS 來讓您了解 RDS 資源的可用性或組態的變更。這些通知允許快速響應。如需有關 RDS 事件通知的其他資訊，請參閱 Amazon RDS 使用者指南中的使用 Amazon RDS 事件通知。

修補

若要訂閱 RDS 執行個體事件通知，請參閱 Amazon RDS 使用者指南中的訂閱 Amazon RDS 事件通知。使用下列的值：

欄位	Value
來源類型	執行個體
要包含的實例	所有實例
要包含的活動類別	選擇特定活動類別或所有活動類別

[RDS.21] 應為重要資料庫參數群組事件設定 RDS 事件通知訂閱

相關要求：NIS.800-53.R5 CA-7、尼斯

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::RDS::EventSubscription`

AWS Config 規則:`rds-pg-event-notifications-configured`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon RDS 事件訂閱是否存在且啟用下列來源類型 (事件類別鍵值配對) 的通知。

```
DBParameterGroup: ["configuration change"]
```

RDS 事件通知使用 Amazon SNS 來讓您了解 RDS 資源的可用性或組態的變更。這些通知允許快速響應。如需有關 RDS 事件通知的其他資訊，請參閱 Amazon RDS 使用者指南中的使用 Amazon RDS 事件通知。

修補

若要訂閱 RDS 資料庫參數群組事件通知，請參閱 Amazon RDS 使用者指南中的訂閱 Amazon RDS 事件通知。使用下列的值：

欄位	Value
來源類型	參數群組
要包括的參數群組	所有參數群組
要包含的活動類別	選擇特定活動類別或所有活動類別

[RDS.22] 應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱

相關要求：NIS.800-53.R5 CA-7、尼斯

分類:偵測設備 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：`AWS::RDS::EventSubscription`

AWS Config 規則:`rds-sg-event-notifications-configured`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon RDS 事件訂閱是否存在且啟用下列來源類型 (事件類別鍵值配對) 的通知。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS 來讓您了解 RDS 資源的可用性或組態的變更。這些通知允許快速響應。如需有關 RDS 事件通知的其他資訊，請參閱 Amazon RDS 使用者指南中的使用 Amazon RDS 事件通知。

修補

若要訂閱 RDS 執行個體事件通知，請參閱 Amazon RDS 使用者指南中的訂閱 Amazon RDS 事件通知。使用下列的值：

欄位	Value
來源類型	安全群組
要包含的安全性群組	所有安全性群組
要包含的活動類別	選擇特定活動類別或所有活動類別

[RDS.23] RDS 執行個體不應使用資料庫引擎預設連接埠

相關要求：交流 4、交流電 -4、交流 -4 (21)、尼斯特。800-53.R5 的 SC-7、星期五、七、七、五、七、七、四、七 (4)、SC-7 (5)

類別：保護 > 安全網路組態

嚴重性：低

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則:`rds-no-default-ports`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 叢集或執行個體是否使用資料庫引擎預設連接埠以外的連接埠。如果 RDS 叢集或執行個體使用預設連接埠，則控制項會失敗。

如果您使用已知連接埠部署 RDS 叢集或執行個體，攻擊者可能會猜測叢集或執行個體的相關資訊。攻擊者可將此資訊與其他資訊搭配使用，連線至 RDS 叢集或執行個體，或取得應用程式的其他相關資訊。

當您變更連接埠時，您也必須更新用來連線至舊連接埠的現有連接字串。您也應該檢查資料庫執行個體的安全群組，以確保其包含允許在新連接埠上進行連線的輸入規則。

修補

若要修改現有 RDS 資料庫執行個體的預設連接埠，請參閱 Amazon RDS 使用者指南中的修改 Amazon RDS 資料庫執行個體。若要修改現有 RDS 資料庫叢集的預設連接埠，請參閱 Amazon

Aurora 使用者指南中的使用主控台、CLI 和 API 修改資料庫叢集。對於資料庫連接埠，請將連接埠值變更為非預設值。

[RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：`rds-cluster-default-admin-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 資料庫叢集是否已變更其預設值的管理員使用者名稱。控制項不適用於類型 Neptune (海王星資料庫) 或文件資料庫 (DocumentDB) 的引擎。如果將管理員使用者名稱設定為預設值，則此規則將失敗。

建立 Amazon RDS 資料庫時，您應該將預設管理員使用者名稱變更為唯一值。默認用戶名是公共知識，應在 RDS 數據庫創建期間進行更改。變更預設使用者名稱可降低意外存取的風險。

修補

若要變更與 Amazon RDS 資料庫叢集關聯的管理員使用者名稱，請建立新的 RDS 資料庫叢集，並在建立資料庫時變更預設管理員使用者名稱。

[RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：`rds-instance-default-admin-check`

排程類型：已觸發變更

參數：無

此控制項會檢查您是否已將 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫執行個體的管理使用者名稱變更為預設值。控制項不適用於類型 Neptune (海王星資料庫) 或文件資料庫 (DocumentDB) 的引擎。如果管理使用者名稱設定為預設值，則控制項會失敗。

Amazon RDS 資料庫上的預設管理使用者名稱是公開知識。建立 Amazon RDS 資料庫時，您應該將預設管理使用者名稱變更為唯一值，以降低意外存取的風險。

修補

若要變更與 RDS 資料庫執行個體相關聯的管理使用者名稱，請先建立新的 RDS 資料庫執行個體。建立資料庫時變更預設的管理使用者名稱。

[RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護

類別:復原 > 復原 > 啟用備份

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、指定點：800-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、NiST SI-12 SI-13

嚴重性：中

資源類型：`AWS::RDS::DBInstance`

AWS Config 規則：**`rds-resources-protected-by-backup-plan`**

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`backupVaultLockCheck`	如果參數設定為 true 且資源使用文件 AWS Backup 庫鎖定，則控制項會產生PASSED發現結果。	Boolean	`true` 或 `false` *	無預設值	

此控制項可評估備份計劃是否涵蓋 Amazon RDS 資料庫執行個體。如果 RDS 資料庫執行個體不在備份計劃的涵蓋範圍內，則此控制會失敗。如果您將`backupVaultLockCheck`參數設定為等於`true`，則只有在例證在 AWS Backup 鎖定的資料保險箱中備份時，控制才會通過。

AWS Backup 是一項全受管備份服務，可集中並自動備份資料。 AWS 服務您可以使 AWS Backup用建立稱為備份計畫的備份原則。您可以使用這些計劃來定義備份需求，例如備份資料的頻率，以及這些備份的保留時間。在備份計劃中包含 RDS 資料庫執行個體，可協助您保護資料免於意外遺失或刪除。

修補

若要將 RDS 資料庫執行個體新增至 AWS Backup 備份計劃，請參閱AWS Backup 開發人員指南中的指派資源給備份計劃。

[RDS.27] RDS 資料庫叢集應在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：**`rds-cluster-encrypted-at-rest`**

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫叢集是否已靜態加密。如果 RDS 資料庫叢集未在靜態時加密，則控制項會失敗。

靜態數據是指任何持續時間存儲在持久性非易失性存儲中的任何數據。加密可協助您保護此類資料的機密性，降低未經授權使用者存取資料的風險。加密 RDS 資料庫叢集可保護您的資料和中繼資料，防止未經授權的存取。它還滿足了生產文件系統 data-at-rest 加密的合規要求。

修補

您可以在建立 RDS 資料庫叢集時啟用靜態加密。建立叢集後，您無法變更加密設定。如需詳細資訊，請參閱 Amazon Aurora 使用者指南中的加密 Amazon Aurora 資料庫叢集。

[RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：**`rds-aurora-mysql-audit-logging-enabled`**

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon Aurora MySQL 資料庫叢集是否設定為將稽核日誌發佈到 Amazon CloudWatch 日誌。如果叢集未設定為將稽核記錄發佈至記錄，則控制項會失敗。 CloudWatch

稽核記錄會擷取資料庫活動的記錄，包括登入嘗試、資料修改、結構描述變更，以及其他基於安全性和符合性目的而稽核的事件。當您設定 Aurora MySQL 資料庫叢集以將稽核日誌發佈到 Amazon 日誌中的 CloudWatch 日誌群組時，您可以對日誌資料執行即時分析。 CloudWatch 日誌將日誌保留在高度耐用的存儲中。您也可以在中建立警示和檢視指標 CloudWatch。

> **Note**
>
> 另一種將稽核記錄發佈至記錄 CloudWatch 檔的方式是啟用進階稽核，並將叢集層級 DB 參數`server_audit_logs_upload`設定為。`1`的預設值`server_audit_logs_upload parameter`為`0`。不過，我們建議您改用下列修正指示來傳遞此控制項。

修補

若要將 Aurora MySQL 資料庫叢集稽核日誌發佈到 CloudWatch 日誌，請參閱 Amazon Aurora 使用者指南中的將 Amazon 極光 MySQL CloudWatch 日誌發佈到亞馬遜日誌。

[RDS.35] RDS 資料庫叢集應啟用自動次要版本升級

相關要求：七月八日 -53.R5 系統二、七月五四 (2)、七月五四 (4)、七八、五、五四 (4)、七月五四 (5)

類別:偵測 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：`AWS::RDS::DBCluster`

AWS Config 規則：**`rds-cluster-auto-minor-version-upgrade-enable`**

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 異地同步備份資料庫叢集是否已啟用自動次要版本升級。如果異地同步備份資料庫叢集未啟用自動次要版本升級，則控制項會失敗。

RDS 提供自動次要版本升級，讓您可以讓 RDS 資料庫叢集保持最新狀態。次要版本可以引入新的軟件功能，錯誤修復，安全補丁和性能改進。透過在 RDS 資料庫叢集上啟用自動次要版本升級，叢集及叢集中的執行個體會在有新版本可用時接收到次要版本的自動更新。更新會在維護時段期間自動套用。

修補

若要在異地同步備份資料庫叢集上啟用自動次要版本升級，請參閱 Amazon RDS 使用者指南中的修改異地同步備份資料庫叢集。

Amazon Redshift 控制

這些控制項與 Amazon Redshift 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

分類:保護 > 安全網路設定 > 無法公開存取的資源

嚴重性：嚴重

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-cluster-public-access-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否可公開存取。它會評估叢集配置項目中的`PubliclyAccessible`欄位。

Amazon Redshift 叢集組態的`PubliclyAccessible`屬性會指出叢集是否可公開存取。當叢集`PubliclyAccessible`設定為時`true`，它是一個面向網際網路的執行個體，具有可公開解析的 DNS 名稱，可解析為公用 IP 位址。

當叢集無法公開存取時，它是具有 DNS 名稱的內部執行個體，可解析為私有 IP 位址。除非您打算讓叢集可公開存取，否則不應將叢集`PubliclyAccessible`設定為`true`。

修補

若要更新 Amazon Redshift 叢集以停用公用存取權，請參閱《Amazon Redshift 管理指南》中的修改叢集。將「公開存取」設定為「否」

[紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密

相關要求：東西 800-53.R5 交流 4、SC-13、等級 800-53.R5 SC-23、等級 800-53.R5 SC-23 (3)、電子信號 -53.R5 (4)、等級 800-53.R5 (4)、等級 -53.R5 SC-8、

類別：保護 > 資料保護 > 傳輸中資料加密

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-require-tls-ssl`

排程類型：已觸發變更

參數：無

此控制項可檢查是否需要與 Amazon Redshift 叢集的連線，才能在傳輸過程中使用加密。如果 Amazon Redshift 叢集參數`require_SSL`未設定為`True`，則檢查會失敗。

TLS 可用來協助防止潛在攻擊者利用 person-in-the-middle 或類似攻擊來竊聽或操控網路流量。只應允許透過 TLS 加密的連線。加密傳輸中的資料可能會影響效能。您應該使用此功能來測試應用程式，以瞭解效能設定檔和 TLS 的影響。

修補

若要將 Amazon Redshift 參數群組更新為需要加密，請參閱 Amazon Redshift 管理指南中的修改參數群組。設置`require_ssl`為真。

[紅移 3] 亞馬遜 Redshift 集群應啟用自動快照

相關要求：CP-10、NIST-53.R5 CP-6、NIST-53.R5 CP-6 (1)、NIST-53.R5 CP-6 (2)、指令碼：800-53.R5 CP-9、指定點 -53.5 SC-5 (2)、指令碼 -53.5 SC-5 (2)、SI-13 (5)

類別:復原 > 復原 > 啟用備份

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-backup-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值	
`MinRetentionPeriod`	快照保留期間下限 (天)	Integer	7 設定為 35	7	

此控制項可檢查 Amazon Redshift 叢集是否已啟用自動快照，以及保留期間大於或等於指定時間範圍。如果叢集未啟用自動快照，或保留期間小於指定的時間範圍，則控制項會失敗。除非您為快照保留期間提供自訂參數值，否則 Security Hub 會使用預設值 7 天。

備份可協助您更快速地從安全性事件中復原。它們可以加強您系統的韌性。根據預設，Amazon Redshift 會定期拍攝快照。此控制項會檢查自動快照是否已啟用並保留至少七天。如需 Amazon Redshift 自動化快照的詳細資訊，請參閱 Amazon Redshift 管理指南中的自動化快照。

修補

若要更新 Amazon Redshift 叢集的快照保留期，請參閱亞 Amazon Redshift 管理指南中的修改叢集。對於 Backup，請將快照保留設定為 7 或更大的值。

[紅移 4] 亞馬遜 Redshift 叢集應啟用稽核記錄

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則:`redshift-cluster-audit-logging-enabled`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：

- `loggingEnabled = true`（不可定制）

此控制項會檢查 Amazon Redshift 叢集是否已啟用稽核記錄。

Amazon Redshift 稽核記錄可提供叢集中連線和使用者活動的其他相關資訊。此資料可以存放在 Amazon S3 中並加以保護，對安全稽核和調查很有幫助。如需詳細資訊，請參閱 Amazon Redshift 管理指南中的資料庫稽核記錄。

修補

若要設定 Amazon Redshift 叢集的稽核記錄，請參閱 Amazon Redshift 管理指南中的使用主控台設定稽核。

[紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本

相關要求：第 800-53.R5 CA-9 (1)、電子信號 -53.R5 厘米 -2、指定信號：800-53.R5 CP-9、顯示卡 -5 (2)、指定線 (4)、等級 -2 (5)

類別:檢測 > 漏洞和補丁管理

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-cluster-maintenancesettings-check`

排程類型：已觸發變更

參數：

- `allowVersionUpgrade = true`（不可定制）

此控制項可檢查 Amazon Redshift 叢集是否已啟用自動主要版本升級功能。

啟用自動主要版本升級，可確保在維護時段期間安裝 Amazon Redshift 叢集的最新主要版本更新。這些更新可能包括安全性修補程式和錯誤修正。保持最新的修補程式安裝是保護系統的重要步驟。

修補

若要解決此問題 AWS CLI，請使用 Amazon Redshift `modify-cluster` 命令來設定屬`--allow-version-upgrade`性。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

哪裡*`clustername`*是您的 Amazon Redshift 集群的名稱。

[紅移 .7] Redshift 叢集應使用增強型 VPC 路由

相關要求：交流 4、交流電 -4、交流 -4 (21)、尼斯特。800-53.R5 的 SC-7、星期五、七、七、七、七 (4)、尼斯 -53.R5 (20)、SC-7 (9)

分類:保護 > 安全網絡配置 > API 私有訪問

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-enhanced-vpc-routing-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否已`EnhancedVpcRouting`啟用。

增強型 VPC 路由會強制叢集`COPY`和資料存放庫之間的所有`UNLOAD`流量通過您的 VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流量記錄來監控網路流量。

修補

如需詳細的修復指示，請參閱 Amazon Redshift 管理指南中的啟用增強型 VPC 路由。

[Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-default-admin-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否已將管理員使用者名稱變更為預設值。如果 Redshift 叢集的管理員使用者名稱設定為，則此控制項將失敗。`awsuser`

建立 Redshift 叢集時，您應該將預設的管理員使用者名稱變更為唯一值。默認用戶名是公共知識，應在配置時更改。變更預設使用者名稱可降低意外存取的風險。

修補

您無法在建立 Amazon Redshift 叢集之後變更其管理員使用者名稱。若要建立新叢集，請依照此處的指示進行。

[紅移 .9] Redshift 叢集不應使用預設的資料庫名稱

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:識別 > 資源組態

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-default-db-name-check`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否已將資料庫名稱變更為預設值。如果 Redshift 叢集的資料庫名稱設定為，控制項將會失敗。`dev`

建立 Redshift 叢集時，您應該將預設資料庫名稱變更為唯一值。預設名稱是公開知識，應在設定時進行變更。舉例來說，如果在 IAM 政策條件中使用已知名名稱，可能會導致無意中存取。

修補

您無法在建立 Amazon Redshift 叢集之後變更其資料庫名稱。如需有關建立新叢集的指示，請參閱 Amazon Redshift 入門指南中的開始使用 Amazon Redshift。

[紅移 .10] Redshift 叢集在靜態時應加密

相關要求：第五卡 -53.R5 CA-9 (1)、電腦五公分三 (6)、尼斯八百五十三 (5) SC-13、電子信號 -53.R5 SC-28、電子信號 (5) SC-28 (1)、

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::Redshift::Cluster`

AWS Config 規則：`redshift-cluster-kms-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否在靜態時加密。如果 Redshift 叢集未在靜態時加密，或者加密金鑰與規則參數中提供的金鑰不同，則控制項會失敗。

在 Amazon Redshift 中，您可以為您的叢集開啟資料庫加密，以協助保護靜態資料。開啟叢集的加密時，叢集和其快照的資料區塊和系統中繼資料會加密。靜態資料加密是建議的最佳作法，因為它會為您的資料增加一層存取管理。靜態加密 Redshift 叢集可降低未經授權的使用者存取儲存在磁碟上資料的風險。

修補

若要修改 Redshift 叢集以使用 KMS 加密，請參閱 Amazon Redshift 管理指南中的變更叢集加密。

Amazon 路線 53 控制

這些控制項與路線 53 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::Route53::HostedZone`

AWS Config 規則：`route53-query-logging-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Route 53 公用託管區域是否已啟用 DNS 查詢記錄功能。如果 Route 53 公用託管區域未啟用 DNS 查詢記錄，則控制項會失敗。

記錄 Route 53 託管區域的 DNS 查詢可解決 DNS 安全性和合規性需求，並授予可見性。記錄檔包括查詢的網域或子網域、查詢的日期和時間、DNS 記錄類型 (例如 A 或 AAAA)，以及 DNS 回應碼 (例如，或) 等資訊。`NoError` `ServFail`啟用 DNS 查詢記錄時，Route 53 會將日誌檔發佈到 Amazon CloudWatch 日誌。

修補

若要記錄 Route 53 公有託管區域的 DNS 查詢，請參閱 Amazon Route 53 開發人員指南中的設定 DNS 查詢記錄。

Amazon 簡單存儲服務控制

這些控制項與 Amazon S3 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS、投資管理系統 DSS V3.2.1/1.3.6、獨聯體 AWS 基礎基準測試 V1.4.0/2.1.5、交流電 -4, 交流電 -4, 交流 -4 (21), 尼斯特. 800-53.R5 交流 6, 奈特. 800-53.R5 的交流 -6, 尼斯 .800-53.R5 (十一), 日本七星期七 (3), 日本七星期七 (4), 尼斯 .800-53.R5 (9) AC-21

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::::Account`

AWS Config 規則：`s3-account-level-public-access-blocks-periodic`

排程類型：定期

參數：

- `ignorePublicAcls`：`true` (不可定制)
- `blockPublicPolicy`：`true` (不可定制)
- `blockPublicAcls`：`true` (不可定制)
- `restrictPublicBuckets`：`true` (不可定制)

此控制項會檢查先前的 Amazon S3 區塊公開存取設定是否在帳戶層級為 S3 一般用途儲存貯體設定。如果將一或多個區塊公用存取設定設定設定設定設定為，則控制項會失敗`false`。

如果將任何設定設定為`false`，或未設定任何設定，則控制項會失敗。

Amazon S3 公共存取區塊的設計目的是在整個 AWS 帳戶 或個別 S3 儲存貯體層級提供控制，以確保物件永遠不會擁有公開存取權。透過存取控制清單 (ACL)、儲存貯體政策或兩者來授予對儲存貯體和物件的公開存取許可。

除非您打算公開存取 S3 儲存貯體，否則您應該設定帳戶層級 Amazon S3 區塊公開存取功能。

若要進一步了解，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 區塊公開存取。

修補

若要為您啟用 Amazon S3 區塊公開存取 AWS 帳戶，請參閱 Amazon 簡單儲存服務使用者指南中的為您的帳戶設定區塊公共存取設定。

[S3.2] S3 通用存儲桶應該阻止公共讀取訪問

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.2、PCI DSS V3.2.1/1.3.6、PCI 資料管理系統 V3.2.1/7.2.1、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-public-read-prohibited`

排程型態：定期與變更觸發

參數：無

此控制項可檢查 Amazon S3 一般用途儲存貯體是否允許公開讀取存取。系統會評估封鎖公開存取的設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。如果值區允許公開讀取存取，則控制項會失敗。

某些使用案例可能要求網際網路上的每個人都能夠從 S3 儲存貯體讀取。然而，這類情況很少見。為了確保資料的完整性和安全，您的 S3 儲存貯體不應允許公開讀取。

修補

若要封鎖 Amazon S3 儲存貯體上的公開讀取存取，請參閱 Amazon 簡單儲存服務使用者指南中的設定 S3 儲存貯體的區塊公共存取設定。

[S3.3] S3 通用存儲桶應該阻止公共寫入訪問

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS 3.2.1/1.3.1、PCI DSS V3.2.1/1.3.2、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、PCI DSS V3.2.1/7.2.1、交流電 -4, 交流電 -4, 交流 -4 (21), 尼斯特. 800-53.R5 交流 6, 奈特. 800-53.R5 的交流 -6, 尼斯 .800-53.R5 (十一), 日本七星期七 (3), 日本七星期七 (4), 尼斯 .800-53.R5 (9) AC-21

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-public-write-prohibited`

排程型態：定期與變更觸發

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否允許公用寫入存取。系統會評估封鎖公開存取的設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。如果值區允許公用寫入存取權，則控制項會失敗。

某些使用案例需要網際網路上的每個人都能夠寫入您的 S3 儲存貯體。然而，這類情況很少見。為了確保資料的完整性和安全，您的 S3 儲存貯體不應允許公開寫入。

修補

若要封鎖 Amazon S3 儲存貯體上的公開寫入存取權，請參閱 Amazon 簡單儲存服務使用者指南中的設定 S3 儲存貯體的區塊公共存取設定。

[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS V3.2.1/4.1，獨聯體 AWS 基礎基準測試版 1.4.0/2.1.2，NIST 800-53.R5 AC-17（2），NIST-53.R5，iA-5（1），NIS.800-53.R5（1），SC-23 (3), 日本七星-五月七日 (4), 尼什 (5), 尼什 (8), 西洋 -53.R5 SC-8 (2), 日本的. SC-12 SC-13 SC-23

類別：保護 > 安全存取管理

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-ssl-requests-only`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否具有需要使用 SSL 請求的政策。如果值區政策不需要使用 SSL 的要求，則控制項會失敗。

S3 儲存貯體應具有政策，要求所有請求 (`Action: S3:*`) 僅接受 S3 資源政策中透過 HTTPS 傳輸的資料 (由條件金鑰表示) `aws:SecureTransport`。

修補

若要更新 Amazon S3 儲存貯體政策以拒絕非安全傳輸，請參閱。 使用 Amazon 簡單儲存服務使用者指南中的 Amazon S3 主控台新增儲存貯體政策。

新增類似下列原則中的原則陳述式。以您要修改的值區名稱取`awsexamplebucket`代。

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::awsexamplebucket",
                "arn:aws:s3:::awsexamplebucket/*"
            ],
            "Condition": {
                "Bool": {
```

```
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

如需詳細資訊，請參閱知識中心文章我應該使用哪些 S3 儲存貯體政策來遵守 s3- AWS Config 規則 bucket-ssl-requests-only？ 。

[S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別:保護 > 安全存取管理 > 受限制的敏感 API 作業動作

嚴重性：高

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-blacklisted-actions-prohibited`

排程類型：已觸發變更

參數：

- `blacklistedactionpatterns`：`s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl`（不可定制）

此控制項會檢查 Amazon S3 一般用途儲存貯體政策是否防止其他 AWS 帳戶 主體對 S3 儲存貯體中的資源執行拒絕動作。如果值區政策允許另一個主參與者執行一或多個先前動作，則控制項會失敗 AWS 帳戶。

實施最低權限存取對於降低安全風險以及錯誤或惡意的影響至關重要。如果 S3 儲存貯體政策允許從外部帳戶存取，可能會導致內部威脅或攻擊者洩漏資料。

此`blacklistedactionpatterns`參數允許成功評估 S3 儲存貯體的規則。對於未包含在`blacklistedactionpatterns`清單中的動作模式，此參數會授與外部帳戶的存取權。

修補

若要更新 Amazon S3 儲存貯體政策以移除許可，請參閱。 使用 Amazon 簡單儲存服務使用者指南中的 Amazon S3 主控台新增儲存貯體政策。

在 [編輯值區原則] 頁面的 [原則編輯] 文字方塊中，執行下列其中一個動作：

- 移除授與其他拒絕動作 AWS 帳戶 存取權的陳述式。
- 從陳述式中移除允許的拒絕動作。

[S3.7] S3 一般用途儲存貯體應使用跨區域複寫

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：PCI DSS V3.2.1/2.2、等級 5 澳大利亞管理系統 (2)、技術指令介面卡 (2)、電子信息技術指標 (800) -53.R5 CP-6 (1)、定義伺服器 -53.5 (1)、Ni.800-53.5 (2)、), 早上五點五 (2), 尼斯卡 (5) CP-10 SC-36 SI-13

類別：保護 > 安全存取管理

嚴重性：低

資源類型：`AWS::S3::Bucket`

AWS Config 規則：**`s3-bucket-replication-enabled`**

排程類型：已觸發變更

參數：

- `ReplicationType: CROSS-REGION`（不可定制）

此控制項可檢查 Amazon S3 一般用途儲存貯體是否已啟用跨區域複寫。如果值區未啟用跨區域複寫，則控制項會失敗。

複製是在相同或不同值區之間對物件進行自動、非同步複製 AWS 區域。複寫會將新建立的物件和物件更新從來源儲存貯體複製到目的地值區或值區。 AWS 最佳作法建議您針對相同擁有的來源和目的地值區進行複寫 AWS 帳戶。除了可用性之外，建議您考慮其他系統強化設定。

修補

若要在 S3 儲存貯體上啟用跨區域複寫，請參閱 Amazon 簡單儲存服務使用者指南中針對同一帳戶擁有的來源和目的地儲存貯體設定複寫。針對「來源值區」，選擇「套用至值區中的所有物件」。

[S3.8] S3 通用存儲桶應阻止公共訪問

相關要求：獨聯體 AWS 基礎基準測試版 1.4.0/2.1.5，NIST 800-53.R5 交流 -3，NIST-53.R5 交流 -3（7），NIST 800-53.R5 交流 4，尼斯 -53.R5 交流 -4（21），星期六七 (11), 星期五七 (16), 星期六七 (20), 星期六七 (20), 星期五七七 (21), 尼斯 .800-53.R5 (3), 西洋 -53.R5 (4), 七 (9) AC-21

分類:保護 > 安全存取管理 > 存取控制

嚴重性：高

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-level-public-access-prohibited`

排程類型：已觸發變更

參數：

- `excludedPublicBuckets`(不可自訂) — 以逗號分隔的已知允許公用 S3 儲存貯體名稱清單

此控制項可檢查 Amazon S3 一般用途儲存貯體是否在儲存貯體層級封鎖公用存取。如果將下列任何設定設定為，則控制項會失敗`false`：

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`

- `restrictPublicBuckets`

S3 儲存貯體層級的封鎖公用存取提供控制項，以確保物件永遠不會擁有公開存取權。透過存取控制清單 (ACL)、儲存貯體政策或兩者來授予對儲存貯體和物件的公開存取許可。

除非您打算公開存取 S3 儲存貯體，否則您應該設定儲存貯體層級 Amazon S3 區塊公共存取功能。

修補

如需有關如何在儲存貯體層級移除公開存取權的資訊，請參閱 Amazon S3 使用者指南中的封鎖對 Amazon S3 儲存的公開存取。

[S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：交流電 -2 (4)、交流電四 (26)、奈特 .800-53.R5 交流 -6 (9)、指定交流 -6 (9)、AU-10、尼斯 -53.5、三、三、三、三五月五日六星期六 (4), 日本七點八十五 (7), 尼斯 .800-53.R5 (9), 尼斯. AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-logging-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否啟用伺服器存取記錄。如果未啟用伺服器存取記錄，則控制項會失敗。啟用記錄功能後，Amazon S3 會將來源儲存貯體的存取日誌交付到所選目標儲存貯體。目標值區必須與來源值區位於 AWS 區域 同一個值區，且不得設定預設保留期間。目標記錄值區不需要啟用伺服器存取記錄，您應該隱藏此值區的發現項目。

伺服器存取記錄可提供對值區發出要求的詳細記錄。伺服器存取記錄可協助安全性和存取稽核。如需詳細資訊，請參閱 Amazon S3 的安全最佳實務：啟用 Amazon S3 伺服器存取記錄。

修補

若要啟用 Amazon S3 伺服器存取日誌，請參閱 Amazon S3 使用者指南中的啟用 Amazon S3 伺服器存取日誌。

[S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。Security Hub 也會在 2024 年 3 月從 AWS 基礎安全性最佳做法標準中移除此控制項，但它仍會包含在 NIST SP 800-53 版本 5 版標準中。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：指定電腦 -53.R5、指定電源 6 (2)、NIST-53.R5 CP-9、Ni.800-53.R5 SC-5 (2)、日本電腦 -53.R5 SI-13 (5) CP-10

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-version-lifecycle-policy-check`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon S3 一般用途版本化儲存貯體是否具有生命週期組態。如果值區沒有生命週期設定，則控制項會失敗。

我們建議您為 S3 儲存貯體建立生命週期組態，以協助您定義 Amazon S3 在物件生命週期內採取的動作。

修補

如需在 Amazon S3 儲存貯體上設定生命週期的詳細資訊，請參閱在儲存貯體上設定生命週期組態和管理儲存生命週期。

[S3.11] S3 一般用途儲存貯體應啟用事件通知

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。Security Hub 也會在 2024 年 3 月從 AWS 基礎安全性最佳做法標準中移除此控制項，但它仍將包含在 NIST SP 800-53 版本 5 版標準中：。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：NIS.800-53.R5 CA-七、七、三、三三 (8)、尼斯。

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-event-notifications-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`eventTypes`	偏好的 S3 事件類型清單	EnumList（最多 28 個項目）	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:Dele`	無預設值

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
			teMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMark	

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
			erCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplic	

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
			ation, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

此控制項會檢查 Amazon S3 一般用途儲存貯體是否啟用 S3 事件通知。如果儲存貯體上未啟用 S3 事件通知，則控制項會失敗。如果您為`eventTypes`參數提供自訂值，則只有在針對指定類型的事件啟用事件通知時，控制項才會傳遞。

啟用 S3 事件通知時，您會在發生影響 S3 儲存貯體的特定事件時收到警示。例如，您可以收到有關物件建立、移除物件和物件還原的通知。這些通知可以提醒相關團隊意外或故意修改，這些修改可能導致未經授權的數據訪問。

修補

如需偵測 S3 儲存貯體和物件變更的相關資訊，請參閱 Amazon S3 使用者指南中的 Amazon S3 事件通知。

[S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：交流 -2 (1)、交流 3 (1)、尼什八達 -53.R5 交流 -3、交流 -3 (15)、尼什八達 -53.R5 交流 -3 (7)、日本交流 -6

分類:保護 > 安全存取管理 > 存取控制

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-acl-prohibited`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon S3 一般用途儲存貯體是否透過存取控制清單 (ACL) 提供使用者許可。如果設定 ACL 來管理值區的使用者存取權，則控制項會失敗。

ACL 是早於 IAM 的舊版存取控制機制。我們建議您使用 S3 儲存貯體政策或 AWS Identity and Access Management (IAM) 政策來管理 S3 儲存貯體的存取權，而不是 ACL。

修補

若要傳遞此控制項，您應該停用 S3 儲存貯體的 ACL。如需指示，請參閱 Amazon 簡單儲存服務使用者指南中的控制物件擁有權和停用儲存貯體的 ACL。

若要建立 S3 儲存貯體政策，請參閱使用 Amazon S3 主控台新增儲存貯體政策。若要在 S3 儲存貯體上建立 IAM 使用者政策，請參閱使用使用者政策控制儲存貯體的存取。

[S3.13] S3 一般用途儲存貯體應具有生命週期組態

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：指定電腦 -53.R5、指定電源 6 (2)、NIST-53.R5 CP-9、Ni.800-53.R5 SC-5 (2)、日本電腦 -53.R5 SI-13 (5) CP-10

類別:保護 > 資料保護

嚴重性：低

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-lifecycle-policy-check`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`targetTransitionDays`	物件轉移至指定的儲存類別時，物件建立後的天數	Integer	`1` 設定為 `36500`	無預設值
`targetExpirationDays`	刪除物件後建立物件的天數	Integer	`1` 設定為 `36500`	無預設值
`targetTransitionStorageClass`	目的地 S3 儲存類別類型	列舉	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_I`	無預設值

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
			`A, GLACIER, GLACIER_IR, DEEP_ARCHIVE`	

此控制項會檢查 Amazon S3 一般用途儲存貯體是否具有生命週期組態。如果值區沒有生命週期設定，則控制項會失敗。如果您為上述一或多個參數提供自訂值，則只有在原則包含指定的儲存區類別、刪除時間或轉換時間時，控制項才會傳遞。

為 S3 儲存貯體建立生命週期組態，可定義您希望 Amazon S3 在物件生命週期內採取的動作。例如，您可以將物件轉移到另一個儲存類別、將它們封存或在指定的時間段後刪除它們。

修補

如需在 Amazon S3 儲存貯體上設定生命週期政策的相關資訊，請參閱在儲存貯體上設定生命週期組態，並參閱 Amazon S3 使用者指南中的管理儲存生命週期。

[S3.14] S3 一般用途儲存貯體應啟用版本控制

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

分類:保護 > 資料保護 > 資料刪除保護

相關要求：八月五日九星期五 (2)、日本電腦 (CP-10)、NIST-53.R5 CP-6、指定點 5 CP-6 (1)、指令碼：800-53.R5 CP-6 (2)、Nist.800-53.R5 (2)、Nist.800-53.5 5 SI-12, 奈特. 800-53.5 SI-13 (5)

嚴重性：低

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-versioning-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否已啟用版本控制。如果值區的版本控制項已暫停，則控制項會失敗。

版本控制可將物件的多個變體保留在同一個 S3 儲存貯體中。您可以使用版本控制來保留、擷取和還原 S3 儲存貯體中存放的物件的早期版本。版本控制可協助您從非預期的使用者動作和應用程式失敗中復原。

> **Tip**
>
> 隨著值區中的物件數量因版本而增加，您可以設定生命週期組態，根據規則自動封存或刪除已建立版本化的物件。如需詳細資訊，請參閱適用於版本化物件的 Amazon S3 生命週期管理。

修補

若要在 S3 儲存貯體上使用版本控制，請參閱 Amazon S3 使用者指南中的在儲存貯體上啟用版本控制。

[S3.15] S3 一般用途儲存貯體應啟用物件鎖定

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

分類:保護 > 資料保護 > 資料刪除保護

相關要求：第五台 CP-6 (2)

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：`s3-bucket-default-lock-enabled`

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
`mode`	S3 物件鎖定保留模式	列舉	`GOVERNANCE`，`COMPLIANCE`	無預設值

此控制項會檢查 Amazon S3 一般用途儲存貯體是否已啟用物件鎖定。如果值區未啟用物件鎖定，則控制項會失敗。如果您為`mode`參數提供自訂值，則只有在 S3 Object Lock 使用指定的保留模式時，控制項才會通過。

您可以使用 S3 物件鎖定使用 write-once-read-many (WORM) 模型來存放物件。物件鎖定可協助防止 S3 儲存貯體中的物件在固定時間或無限期內遭到刪除或覆寫。您可以使用 S3 物件鎖定，以滿足必須使用 WORM 儲存體的法規要求，或多加一道保護以免物件遭到變更和刪除。

修補

若要為新的和現有的 S3 儲存貯體設定物件鎖定，請參閱 Amazon S3 使用者指南中的設定 S3 物件鎖定。

[S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys

> **Important**
>
> 2024 年 3 月 12 日，此控制項的標題變更為顯示的標題。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

類別：保護 – 資料保護 – 靜態資料加密

相關要求：第五代 SC-12 (2)、電腦五點五公分 -3 (6)、鼻子 800-53.R5 SC-13、鎳 53.R5 SC-28、薄膜 -53.R5 SC-28 (1)、尼斯卡 -53.5 (1)、尼斯卡 -53.5 (1)、6), 尼斯 .800-53.5 澳大利亞

嚴重性：中

資源類型：`AWS::S3::Bucket`

AWS Config 規則：**`s3-default-encryption-kms`**

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否使用 AWS KMS key (SSE-KMS 或 DSSE-KMS) 加密。如果儲存貯體使用預設加密 (SSE-S3) 加密，則控制項會失敗。

伺服器端加密 (SSE) 是由接收資料的應用程式或服務在其目的地加密資料。除非另有指定，否則 S3 儲存貯體預設會使用 Amazon S3 受管金鑰 (SSE-S3) 進行伺服器端加密。不過，若要增加控制權，您可以選擇將儲存貯體設定為改為使用伺服器端加密 AWS KMS keys (SSE-KMS 或 DSSE-KMS)。Amazon S3 會在物件層級將資料寫入資料中心的磁碟時加密，並在您存取 AWS 資料時為您解密。

修補

若要使用 SSE-KMS 加密 S3 儲存貯體，請參閱 Amazon S3 使用者指南中的指定伺服器端加密 AWS KMS (SSE-KMS)。若要使用 DSSE-KMS 加密 S3 儲存貯體，請參閱 Amazon S3 使用者指南中的使用 AWS KMS keys (DSSE-KMS) 指定雙層伺服器端加密。

[S3.19] S3 存取點應該已啟用封鎖公用存取設定

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全存取管理 > 無法公開存取的資源

嚴重性：嚴重

資源類型：`AWS::S3::AccessPoint`

AWS Config 規則：**`s3-access-point-public-access-blocks`**

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon S3 存取點是否已啟用區塊公用存取設定。如果存取點未啟用封鎖公用存取設定，則控制項會失敗。

Amazon S3 區塊公開存取功能可協助您在三個層級管理 S3 資源的存取：帳戶、儲存貯體和存取點層級。每個層級的設定都可以獨立設定，讓您對資料擁有不同層級的公開存取限制。存取點設定無法個別覆寫較高層級 (帳戶層級或指派給存取點的值區) 上限制較嚴格的設定。相反地，存取點層級的設定是相加的，這表示它們會在其他層級的設定進行補充，並與其他層級的設定一起運作。除非您打算公開存取 S3 存取點，否則應啟用封鎖公用存取設定。

修補

Amazon S3 目前不支援在建立存取點後變更存取點的封鎖公開存取權限設定。當您建立新的存取點時，預設會啟用所有封鎖公用存取設定。建議您啟用所有設定，除非您知道您有特別需要停用任一設定。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的管理公用存取點。

[S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能

相關要求：獨聯體 AWS 基礎基準測試 V1.4.0，鎳氫 -53.R5 CA-9（1），NIST-53.R5 厘米 -2，微信 -53.R5 厘米 -2（2），日本電腦 -53.R5 厘米 -3，

分類:保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：`AWS::S3::Bucket`

AWS Config 規則：**`s3-bucket-mfa-delete-enabled`**

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon S3 一般用途儲存貯體上是否啟用多因素身份驗證 (MFA) 刪除。如果值區未啟用 MFA 刪除，則控制項會失敗。

在 Amazon S3 儲存貯體中使用 S3 版本控制時，您可以選擇性地設定儲存貯體以啟用 MFA 刪除，以新增另一層安全性。當您這樣做時，儲存貯體擁有者必須在任一要求中包含兩種身分驗證形式，才能刪除版本或變更儲存貯體的版本控制狀態。如果您的安全憑證遭到入侵，MFA 刪除可提供額外的安全

性。MFA 刪除還可以協助防止意外刪除值區刪除，方法是要求啟動刪除動作的使用者以 MFA 代碼證明 MFA 裝置的實體擁有，並在刪除動作中增加額外的摩擦和安全性。

> **Note**
>
> MFA 刪除功能需要值區版本控制作為相依性。儲存貯體版本控制是一種將 S3 物件的多種變體保留在同一個儲存貯體中的方法。此外，只有以 root 使用者身分登入的儲存貯體擁有者可以啟用 MFA 刪除並在 S3 儲存貯體上執行刪除動作。

修補

若要在儲存貯體上啟用 S3 版本控制和設定 MFA 刪除，請參閱 Amazon 簡單儲存服務使用者指南中的設定 MFA 刪除。

Amazon SageMaker 控制

這些控制項與資 SageMaker 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網

相關要求：PCI DSS V3.2.1/1.2.1、投資管理系統 DSS V3.2.1/1.3.1、PCI DSS V3.2.1/1.3.4、PCI DSS V3.2.1/1.3.4、投資管理系統 DSS V3.2.1/1.3.6、Ni.800-53.R5 AC-21、交流電 -4 (21), 交流 6, 尼斯 .800-53.R5 交流 -6, 尼斯 .800-53.R5, 星期五 (20), 尼斯 .800-53.R5 (16), 尼斯 .800-53.R5 (16), 尼斯特 -53.R5 (20), 3), 早上七點七 (4), 日本七星期五 (9)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：`AWS::SageMaker::NotebookInstance`

AWS Config 規則：`sagemaker-notebook-no-direct-internet-access`

排程類型：定期

參數：無

此控制項會檢查 SageMaker 筆記本執行個體是否已停用直接網際網路存取。如果已針對筆記本執行個體啟用`DirectInternetAccess`欄位，則控制項會失敗。

如果您在不使用 VPC 的情況下設定 SageMaker 執行個體，則執行個體預設會啟用直接網際網路存取。您應該使用 VPC 設定執行個體，並將預設設定變更為 [停用] — 透過 VPC 存取網際網路。若要從筆記型電腦訓練或託管模型，您需要存取網際網路。若要啟用網際網路存取，您的 VPC 必須具有介面端點 (AWS PrivateLink) 或 NAT 閘道，以及允許輸出連線的安全群組。若要進一步了解如何將筆記本執行個體 Connect 到 VPC 中的資源，請參閱 Amazon SageMaker 開發人員指南中的將筆記本執行個體連接到 VPC 中的資源。您也應該確保只有授權使用者才能存取您的 SageMaker 組態。限制允許使用者變更 SageMaker 設定和資源的 IAM 許可。

修補

建立筆記本執行個體之後，您無法變更網際網路存取設定。相反地，您可以停止、刪除和重新建立具有封鎖網際網路存取權的執行個體。若要刪除允許直接存取網際網路的筆記本執行個體，請參閱 Amazon SageMaker 開發人員指南中的使用筆記本執行個體建立模型：清理。若要重建拒絕網際網路存取的筆記本執行個體，請參閱建立筆記本執行個體。對於 [網路]、[直接網際網路存取]，選擇 [停用]-透過 VPC 存取網際網路。

[SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動

相關要求：指定的要求：AC-21、交流 -3、NIST -53.R5 交流 -3、交流 -3 (7)、尼斯特 800-53.R5 交流 4、NIS.800-53.R5 交流 4 (21)、指定線 -53.R5 交流 -6、五月五日七 (16), 日本七點七 (20), 日本七點七 (20), 日本七點七 (21), 日本七點七 (3), 日本七點七 (3), 日本七七 (4), 日本七星期七 (4)

分類:保護 > 安全網絡配置 > VPC 內的資源

嚴重性：高

資源類型：`AWS::SageMaker::NotebookInstance`

AWS Config 規則：`sagemaker-notebook-instance-inside-vpc`

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker 筆記型電腦執行個體是否在自訂虛擬私有雲 (VPC) 內啟動。如果 SageMaker 筆記本執行個體未在自訂 VPC 中啟動，或在 SageMaker 服務 VPC 中啟動筆記本執行個體，則此控制項會失敗。

子網路是 VPC 內的一系列 IP 位址。我們建議盡可能將資源保存在自訂 VPC 內，以確保基礎架構的安全網路保護。Amazon VPC 是一個虛擬網路，專用於您 AWS 帳戶的. 使用 Amazon VPC，您可以控制 SageMaker Studio 和筆記型電腦執行個體的網路存取和網際網路連線。

修補

建立筆記本執行個體之後，您無法變更 VPC 設定。相反地，您可以停止、刪除和重新建立執行個體。如需指示，請參閱 Amazon SageMaker 開發人員指南中的使用筆記本執行個體建立模型：清理。

[SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限

相關要求：交流 -2 (1)、交流 -6 (15)、指定交流 -6 (10)、指定交流 -6 (5)、指定交流 -6、交流 -6 (2)

類別:保護 > 安全存取管理 > 根使用者存取限制

嚴重性：高

資源類型：`AWS::SageMaker::NotebookInstance`

AWS Config 規則：`sagemaker-notebook-instance-root-access-check`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon SageMaker 筆記型電腦執行個體的根存取是否開啟。如果針對 SageMaker 筆記本執行個體開啟 root 存取權，則控制項會失敗。

為了遵守最低權限的主體，建議您將 root 存取權限限制為執行個體資源，以避免意外過度佈建權限。

修補

若要限制 SageMaker 筆記本執行個體的根存取權限，請參閱 Amazon SageMaker 開發人員指南中的控制 SageMaker 筆記本執行個體的根存取權。

AWS Secrets Manager 控制

這些控制項與 Secrets Manager 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉

相關要求：交流 -2 (1)、交流電 -3 (15)

類別：保護 > 安全開發

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：secretsmanager-rotation-enabled-check

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
maximumAllowedRotationFrequency	秘密旋轉頻率允許的最大天數	Integer	1 設定為 365	無預設值

此控制項會檢查儲存在中的密碼 AWS Secrets Manager 是否設定為自動旋轉。如果未使用自動旋轉設定密碼，則控制項會失敗。如果您為maximumAllowedRotationFrequency參數提供自訂值，則只有在指定的時間範圍內自動旋轉密碼時，控制項才會通過。

Secrets Manager 可協助您改善組織的安全性狀態。密碼包括資料庫認證、密碼和協力廠商 API 金鑰。您可以使用 Secrets Manager 集中儲存密碼、自動加密密碼、控制密碼的存取，以及安全且自動地輪換密碼。

Secrets Manager 可以旋轉密碼。您可以使用輪替代短期密碼的長期密碼。輪換您的密碼會限制未經授權的使用者可以使用遭入侵密碼的時間長度 出於這個原因，你應該經常輪換你的秘密。若要進一步瞭解輪換，請參閱AWS Secrets Manager 使用者指南中的旋轉 AWS Secrets Manager 密碼。

修補

若要開啟 Secrets Manager 密碼的自動輪替功能，請參閱使用AWS Secrets Manager 者指南中的使用主控台設定 AWS Secrets Manager 密碼的自動輪換。您必須選擇並配置旋轉 AWS Lambda 功能。

[SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉

相關要求：交流 -2 (1)、交流電 -3 (15)

類別：保護 > 安全開發

嚴重性：中

資源類型：`AWS::SecretsManager::Secret`

AWS Config 規則：`secretsmanager-scheduled-rotation-success-check`

排程類型：已觸發變更

參數：無

此控制項會根據輪換排程檢查 AWS Secrets Manager 密碼是否成功旋轉。如果`RotationOccurringAsScheduled`是，則控制項失敗`false`。控制項只會評估已開啟旋轉的密碼。

Secrets Manager 可協助您改善組織的安全性狀態。密碼包括資料庫認證、密碼和協力廠商 API 金鑰。您可以使用 Secrets Manager 集中儲存密碼、自動加密密碼、控制密碼的存取，以及安全且自動地輪換密碼。

Secrets Manager 可以旋轉密碼。您可以使用輪替代短期密碼的長期密碼。輪換您的密碼會限制未經授權的使用者可以使用遭入侵密碼的時間長度 出於這個原因，你應該經常輪換你的秘密。

除了將密碼設定為自動輪換之外，您還應確保這些密碼根據輪換排程成功輪換。

若要進一步瞭解輪換，請參閱AWS Secrets Manager 使用者指南中的旋轉 AWS Secrets Manager 密碼。

修補

如果自動輪換失敗，則 Secrets Manager 可能會遇到組態錯誤。若要輪換秘密管理員中的密碼，您可以使用 Lambda 函數來定義如何與擁有密碼的資料庫或服務互動。

如需診斷和修正與密碼輪替相關的常見錯誤的說明，請參閱《AWS Secrets Manager 使用指南》中的「疑難排解密碼 AWS Secrets Manager 輪換」。

[SecretsManager.3] 刪除未使用的 Secrets Manager 秘密

相關要求：交流 -2 (1)、交流電 -3 (15)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：secretsmanager-secret-unused

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
unusedForDays	密碼可保持未使用的最大天數	Integer	1 設定為 365	90

此控制項會檢查 AWS Secrets Manager 密碼是否已在指定的時間範圍內存取。如果密碼未使用超過指定的時間範圍，則控制項會失敗。除非您為存取期間提供自訂參數值，否則 Security Hub 會使用預設值 90 天。

刪除未使用的密碼與輪換密碼一樣重要。未使用的密碼可能會被其以前的用戶濫用，他們不再需要訪問這些密碼。此外，隨著越來越多的用戶可以訪問某個秘密，有人可能處理不當並將其洩露給未經授權的實體，從而增加了濫用的風險。刪除未使用的密碼有助於撤銷不再需要密碼的使用者的密碼存取權。它也有助於降低使用 Secrets Manager 的成本。因此，定期刪除未使用的秘密至關重要。

修補

若要刪除非使用中的 Sec AWS Secrets Manager ret 管理員密碼，請參閱AWS Secrets Manager 使用者指南中的刪除密碼。

[SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替

相關要求：交流 -2 (1)、交流電 -3 (15)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：secretsmanager-secret-periodic-rotation

排程類型：定期

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
maxDaysSinceRotation	密碼可以保持不變的最大天數	Integer	1 設定為 180	90

此控制項會檢查 AWS Secrets Manager 秘密是否在指定的時間範圍內至少旋轉一次。如果秘密至少不經常旋轉，則控制項會失敗。除非您為輪換期間提供自訂參數值，否則 Security Hub 會使用預設值 90 天。

輪換秘密可以幫助您降低未經授權使用您的秘密的風險 AWS 帳戶。範例包括資料庫認證、密碼、協力廠商 API 金鑰，甚至是任意文字。如果您很長一段時間沒有更改密碼，那麼秘密的可能性就更有可能被洩露。

隨著越來越多的用戶可以訪問某個秘密，很可能是有人處理不當並將其洩露給未經授權的實體。秘密可以透過日誌和快取資料洩漏。它們可以針對除錯目的共用，而在除錯完成之後未變更或撤銷。由於上述所有原因，秘密應該經常輪換。

您可以在中設定密碼的自動輪替 AWS Secrets Manager。透過自動輪換功能，您可以用短期密碼取代長期機密，大幅降低遭到入侵的風險。我們建議您為 Secrets Manager 設定自動輪換。如需更多詳細資訊，請參閱 AWS Secrets Manager 使用者指南中的輪換 AWS Secrets Manager 密碼。

修補

若要開啟 Secrets Manager 密碼的自動輪替功能，請參閱使用AWS Secrets Manager 者指南中的使用主控台設定 AWS Secrets Manager 密碼的自動輪換。您必須選擇並配置旋轉 AWS Lambda 功能。

Amazon 簡單通知服務控制

這些控制項與 Amazon SNS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[SNS.1] SNS 主題應該使用靜態加密 AWS KMS

> **Important**
>
> 安全中心將於 2024 年 3 月從 AWS 基礎安全性最佳做法標準中移除此控制項，但仍將包含在 NIST SP 800-53 版本 5 版標準中。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::SNS::Topic`

AWS Config 規則：`sns-encrypted-kms`

排程類型：已觸發變更

參數：無

此控制項可檢查 Amazon SNS 主題是否使用 AWS Key Management Service (AWS KMS) 中管理的金鑰進行靜態加密。如果 SNS 主題不使用 KMS 金鑰進行伺服器端加密 (SSE)，則控制項會失敗。根據預設，SNS 會使用磁碟加密來儲存訊息和檔案。若要傳遞此控制項，您必須改為選擇使用 KMS 金鑰進行加密。這增加了一層額外的安全性，並提供了更多的存取控制靈活性。

靜態資料加密可降低未經驗證的使用者存取儲存在磁碟上的資料的風險。 AWS在讀取數據之前，需要 API 權限才能解密數據。建議您使用 KMS 金鑰加密 SNS 主題，以增加一層安全性。

修補

若要為 SNS 主題啟用 SSE，請參閱 Amazon 簡單通知服務開發人員指南中的啟用 Amazon SNS 的伺服器端加密 (SSE) 主題。在您可以使用 SSE 之前，您還必須設定 AWS KMS key 原則以允許主題的加密和解密郵件。如需詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的設定 AWS KMS 許可。

[SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄

> **Important**
>
> 安全中心將在 2024 年 3 月移除此控制項。如需詳細資訊，請參閱 Security Hub 控制項的變更記錄。

相關要求：AU-12，日本電子郵件 -53.R5 澳大利亞

類別：識別 > 記錄日誌

嚴重性：中

資源類型：`AWS::SNS::Topic`

AWS Config 規則：`sns-topic-message-delivery-notification-enabled`

排程類型：已觸發變更

參數：無

此控制項會檢查傳送至 Amazon SNS 主題的端點通知訊息的傳遞狀態是否啟用記錄功能。如果未啟用郵件的傳遞狀態通知，則此控制項會失敗。

記錄是維護服務可靠性、可用性和效能的重要組成部分。記錄郵件傳遞狀態有助於提供操作見解，如下所示：

- 得知訊息是否已傳遞至 Amazon SNS 端點。
- 識別從 Amazon SNS 端點傳送至 Amazon SNS 的回應。
- 決定訊息停留時間 (發佈時間戳記與傳送至 Amazon SNS 端點之間的時間)。

修補

若要設定主題的交付狀態記錄，請參閱 Amazon SNS 訊息交付狀態，請參閱 Amazon 簡單通知服務開發人員指南。

Amazon 簡單隊列服務控制

這些控制項與 Amazon SQS 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[SQS.1] Amazon SQS 佇列應該在靜態時加密

相關要求：電腦 -53.R5 CA-9 (1)、等級 5 厘米 -3 (6)、奈特．SC-13 SC-28 SC-28

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：`AWS::SQS::Queue`

AWS Config 規則:`sqs-queue-encrypted`(自訂 Security Hub 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SQS 佇列是否在靜態時加密。如果佇列未使用 SQL 管理的金鑰 (SSE-SQS) 或 () 金鑰 (SSE-KMS) 加密，則控制項 AWS Key Management Service 會失敗。AWS KMS

靜態資料加密可降低未經授權使用者存取儲存在磁碟上資料的風險。伺服器端加密 (SSE) 會使用 SQL 管理的加密金鑰 (SSE-SQS) 或金鑰 (SSE-KMS) 來保護 SQS 佇列中訊息的內容。 AWS KMS

修補

若要為 SQS 佇列設定 SSE，請參閱 Amazon 簡單佇列服務開發人員指南中的設定佇列的伺服器端加密 (SSE) (主控台)。

AWS Step Functions 控制

這些控制項與 Step Functions 資源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[StepFunctions.1] Step Functions 狀態機應該打開日誌記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::StepFunctions::StateMachine

AWS Config 規則：step-functions-state-machine-logging-enabled

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許的自訂值	Security Hub 預設值
logLevel	最低記錄等級	列舉	ALL, ERROR, FATAL	無預設值

此控制項會檢查狀 AWS Step Functions 態機器是否已開啟記錄。如果狀態機器沒有開啟記錄，則控制項會失敗。如果您為logLevel參數提供自訂值，則只有在狀態機器已開啟指定的記錄層級時，控制項才會通過。

監控可協助您維持 Step Functions 的可靠性、可用性和效能。您應該從使用的中收集盡可能多的 AWS 服務 監視資料，以便更輕鬆地偵錯多點失敗。為您的 Step Functions 狀態機器定義記錄組態可讓您追蹤 Amazon Lo CloudWatch gs 中的執行歷史記錄和結果。或者，您可以只追蹤錯誤或嚴重事件。

修補

若要開啟 Step Functions 狀態機器的記錄，請參閱AWS Step Functions 開發人員指南中的設定記錄。

AWS WAF 控制

這些控制項與資 AWS WAF 源有關。

這些控制項可能並非全部可用 AWS 區域。如需詳細資訊，請參閱 各區域控制項的可用性。

[WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六 (9), 日本第七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::WAF::WebACL

AWS Config 規則：waf-classic-logging-enabled

排程類型：定期

參數：無

此控制項會檢查 AWS WAF 全域 Web ACL 是否已啟用記錄。如果未啟用 Web ACL 的記錄，則此控制項會失敗。

記錄是維護 AWS WAF 全球可靠性、可用性和效能的重要組成部分。這是許多組織中的業務和合規性要求，可讓您對應用程式行為進行疑難排解。它還提供有關由附加到的 Web ACL 分析的流量的詳細資訊 AWS WAF。

修補

若要啟用 AWS WAF Web ACL 的記錄功能，請參閱AWS WAF 開發人員指南中的記錄 Web ACL 流量資訊。

[WAF.2] AWS WAF 經典區域規則至少應具有一個條件

相關要求：交流 -4 (21)、日本七點七、七點七、七、七七 (21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAFRegional::Rule

AWS Config 規則：waf-regional-rule-not-empty

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 地區規則是否具有至少一個條件。如果規則中沒有條件，則控制項會失敗。

WAF 區域規則可以包含多個條件。規則的條件允許流量檢查並採取定義的處理行動 (允許、封鎖或計數)。沒有任何條件，交通通過沒有檢查。WAF 區域規則沒有條件，但名稱或標籤建議允許、封鎖或計數，可能會導致錯誤的假設是發生這些動作之一。

修補

若要將條件新增至空白規則，請參閱AWS WAF 開發人員指南中的新增和移除規則中的條件。

[WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則

相關要求：交流 -4 (21)、日本七點七、七點七、七、七七 (21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAFRegional::RuleGroup`

AWS Config 規則：`waf-regional-rulegroup-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 地區規則群組是否具有至少一個規則。如果規則群組中沒有規則，控制項就會失敗。

WAF 區域規則群組可以包含多個規則。規則的條件允許流量檢查並採取定義的處理行動 (允許、封鎖或計數)。沒有任何規則，交通通過沒有檢查。WAF 區域規則群組沒有規則，但名稱或標籤建議允許、封鎖或計數，可能會導致錯誤的假設是其中一個動作正在發生。

修補

若要將規則和規則條件新增至空白規則群組，請參閱《開發人員指南》中的〈從 AWS WAF 傳統規則群組新增和刪除規則〉和〈新增和移除規則中的條AWS WAF 件〉。

[WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAFRegional::WebACL`

AWS Config 規則：`waf-regional-webacl-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF Classic 區域性 網頁 ACL 是否包含任何 WAF 規則或 WAF 規則群組。如果 Web ACL 不包含任何 WAF 規則或規則群組，則此控制項會失敗。

WAF 地區 Web ACL 可以包含檢查和控制 Web 請求的規則和規則群組集合。如果 Web ACL 是空的，則網路流量可以通過而不會被 WAF 偵測到或採取行動，具體取決於預設動作。

修補

若要將規則或規則群組新增至空白的 AWS WAF 傳統區域性 Web ACL，請參閱AWS WAF 開發人員指南中的編輯 Web ACL。

[WAF.6] AWS WAF 經典全域規則至少應該有一個條件

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAF::Rule`

AWS Config 規則：`waf-global-rule-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域規則是否包含任何條件。如果規則中沒有條件，則控制項會失敗。

WAF 全域規則可以包含多個條件。規則的條件允許流量檢查並採取定義的處理行動 (允許、封鎖或計數)。沒有任何條件，交通通過沒有檢查。WAF 全域規則沒有條件，但具有建議允許、封鎖或計數的名稱或標籤，可能會導致錯誤的假設是其中一個動作正在發生。

修補

如需建立規則和新增條件的指示，請參閱AWS WAF 開發人員指南中的建立規則和新增條件。

[WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAF::RuleGroup`

AWS Config 規則：`waf-global-rulegroup-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域規則群組是否具有至少一個規則。如果規則群組中沒有規則，控制項就會失敗。

WAF 全域規則群組可以包含多個規則。規則的條件允許流量檢查並採取定義的處理行動 (允許、封鎖或計數)。沒有任何規則，交通通過沒有檢查。WAF 全域規則群組沒有規則，但具有建議允許、封鎖或計數的名稱或標記，可能會導致錯誤的假設是其中一個動作正在發生。

修補

如需將規則新增至規則群組的指示，請參閱AWS WAF 開發人員指南中的建立 AWS WAF 傳統規則群組。

[WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

相關要求：交流 -4 (21)、日本七點七、七點七、七、七七 (21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAF::WebACL`

AWS Config 規則：`waf-global-webacl-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域 Web ACL 是否包含至少一個 WAF 規則或 WAF 規則群組。如果 Web ACL 不包含任何 WAF 規則或規則群組，則控制項會失敗。

WAF 全域 Web ACL 可以包含檢查和控制 Web 要求的規則和規則群組集合。如果 Web ACL 是空的，則網路流量可以通過而不會被 WAF 偵測到或採取行動，具體取決於預設動作。

修補

若要將規則或規則群組新增至空的 AWS WAF 全域 Web ACL，請參閱AWS WAF 開發人員指南中的編輯 Web ACL。針對「篩選」，選擇「全域」(CloudFront)。

[WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組

相關需求：鎳碳酸鈣 -9 (1)、五分之五公分

類別：保護 > 安全網路組態

嚴重性：中

資源類型：`AWS::WAFv2::WebACL`

AWS Config 規則：`wafv2-webacl-not-empty`

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF V2 Web 存取控制清單 (Web ACL) 是否包含至少一個規則或規則群組。如果 Web ACL 不包含任何規則或規則群組，則控制項會失敗。

Web ACL 可讓您對受保護的資源回應的所有 HTTP (S) Web 要求進行精細控制。Web ACL 應包含檢查和控制 Web 請求的規則和規則群組集合。如果 Web ACL 為空，則 Web 流量可以通過而不會被偵測到或採取行動， AWS WAF 具體取決於預設動作。

修補

若要將規則或規則群組新增至空的 WAFV2 Web ACL，請參閱AWS WAF 開發人員指南中的編輯 Web ACL。

[WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六七 (10), 日本七星期七 (9), 日本七星期七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::WAFv2::WebACL

AWS Config 規則：**wafv2-logging-enabled**

排程類型：定期

參數：無

此控制項會檢查 AWS WAF V2 Web 存取控制清單 (Web ACL) 是否已啟動記錄。如果停用 Web ACL 的記錄，則此控制項會失敗。

記錄會維護的可靠性、可用性和效能 AWS WAF。此外，記錄是許多組織中的業務和合規性要求。藉由記錄 Web ACL 分析的流量，您可以疑難排解應用程式行為。

修補

若要啟用 AWS WAF Web ACL 的記錄，請參閱AWS WAF 開發人員指南中的管理 Web ACL 的記錄。

[WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

相關要求：尼斯 -800-53.R5 交流 4 (26)、AU-10、尼斯 (800-53.R5)、尼斯．800-53.R5、歐洲交流 4、銀幣 -800-53.R5 澳洲 6 (3)、尼斯卡 -800-53.5 (3)、鎳 R5 星期六七 (10), 日本七星期七 (9), 日本七星期七 (8) AU-12

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::WAFv2::RuleGroup

AWS Config 規則：**wafv2-rulegroup-logging-enabled**

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 規則或規則群組是否已啟用 Amazon CloudWatch 指標。如果規則或規則群組未啟用 CloudWatch 量度，控制項就會失敗。

在 AWS WAF 規則和規則群組上設定 CloudWatch 量度可提供流量流量的可見度。您可以查看觸發哪些 ACL 規則，以及接受和封鎖哪些要求。此可見性可協助您識別相關資源上的惡意活動。

修補

若要在 AWS WAF 規則群組上啟用 CloudWatch 量度，請呼叫 UpdateRuleGroupAPI。
若要在 AWS WAF 規則上啟用 CloudWatch 量度，請呼叫 UpdateWebACL API。
將`CloudWatchMetricsEnabled`欄位設定為`true`。當您使用 AWS WAF 主控台建立規則或規則群組時，會自動啟用 CloudWatch 量度。

檢視和管理安全性控制

控制項是安全性標準中的一項保護，可協助組織保護其資訊的機密性、完整性和可用性。在安全中心，控制項與特定 AWS 資源有關。

合併控制項檢視

Security Hub 主控台的 [控制項] 頁面會顯示目前所有可用的控制項 AWS 區域 (您可以造訪 [安全性標準] 頁面並選擇啟用的標準，以檢視標準內容中的控制項)。Security Hub 會為控制項指派一致的安全性控制 ID、標題和說明跨標準。控制項 ID 包括相關 AWS 服務 和唯一的編號 (例如 CodeBuild .3)。

您可以在 Security Hub 主控台的 [控制項] 頁面上取得下列資訊：

- 根據通過的控制項比例與含資料的已啟用控制項總數進行比較的整體安全分數
- 所有已啟用控制項的安全性檢查失敗百分比
- 針對不同嚴重性的控制項，通過和失敗的安全性檢查次數
- 根據啟用狀態劃分為不同索引標籤的控制項清單。不適用於任何已啟用標準的可用控制項會顯示在「已停用」欄中。未處理的控制項 (例如目前「區域」中無法使用的控制項) 會顯示在「無資料」欄中。[全部] 資料行中的控制項數目等於 [失敗]、[未知]、[通過]、[停用] 和 [無資料] 資料行中的控制項總和。

您可以從「控制項」頁面選擇控制項來檢視其明細，並對控制項產生的發現項目採取動作。在此頁面中，您也可以啟用或停用目前 AWS 帳戶 和中的安全性控制 AWS 區域。[控制項] 頁面中的啟用和停用動作適用於各種標準。如需詳細資訊，請參閱 在所有標準中啟用和停用控制項。

對於管理員帳戶，[控制項] 頁面會反映整個成員帳戶的控制項狀態。如果至少一個成員帳戶中的控制項檢查失敗，控制項會顯示在 [控制項] 頁面的 [失敗] 索引標籤中。如果您已設定聚總區域，「控制

項」頁面會反映所有連結區域的控制項狀態。如果至少一個連結的「區域」中的控制項檢查失敗，控制項會顯示在「控制項」頁面的「失敗」頁籤中。

合併控制項檢視會變更控制「 AWS 安全性搜尋結果格式」(ASFF) 中的搜尋欄位，這些欄位可能會影響工作流程 如需詳細資訊，請參閱 合併的控制項檢視 — ASFF 變更。

控制項的整體安全分數

「控制項」頁面會顯示介於 0—100% 之間的整體安全分數。整體安全分數是根據傳遞的控制項與含資料的已啟用控制項總數比較的比例來計算。

> **Note**
>
> 若要檢視控制項的整體安全分數，您必須新增權限，才能呼叫**`BatchGetControlEvaluations`**您用來存取 Security Hub 的 IAM 角色。檢視特定標準的安全分數不需要此權限。

當您啟用 Security Hub 時，Security Hub 會在您第一次造訪 Security Hub 主控台的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內計算初始安全分數。在中國和地區產生首次安全分數可能需要長達 24 小時的時間 AWS GovCloud (US) Region。只有在您造訪這些頁面時啟用的標準，才會產生分數。若要檢視目前已啟用的標準清單，請使用 `GetEnabledStandards`API 作業。此外，必須配置 AWS Config 資源記錄才能顯示分數。整體安全分數是標準安全分數的平均值。

在第一次產生分數之後，Security Hub 會每 24 小時更新一次安全分數。Security Hub 會顯示時間戳記，以指出上次更新安全分數的時間。

如果您已設定彙總區域，整體安全分數會反映跨連結區域的控制項發現項目。

主題

- 控制類別
- 在所有標準中啟用和停用控制項
- 在啟用的標準中自動啟用新控制項
- 自訂控制參數
- 您可能想要停用的 Security Hub 控制項
- 檢視控制項的詳細資訊
- 篩選和排序控制項清單
- 檢視控制項發現項目並採取動作

控制類別

每個控制項都會指定一個品類。控制項的類別會反映控制項套用的安全性功能。

類別值包含品類、類別中的子類別，以及子類別中的分類器 (選擇性)。例如：

- 識別 > 庫存
- 保護 > 資料保護 > 加密傳輸中的資料

以下是可用類別、子類別和分類器的描述。

識別

發展組織理解，以管理系統、資產、資料和能力的網路安全風險。

庫存

該服務是否實施了正確的資源標記策略？ 此標記策略是否包括資源擁有者？

服務使用哪些資源？ 這些資源是此服務已核准的資源嗎？

您是否可以查看已核准的庫存？ 例如，您是否使用 Amazon EC2 Systems Manager 和 Service Catalog 等服務？

日誌

您是否安全地啟用了該服務的所有相關日誌記錄？ 記錄檔的範例包括：

- Amazon VPC 流程日誌
- Elastic Load Balancing 存取日誌
- Amazon CloudFront 日誌
- Amazon CloudWatch 日誌
- Amazon Relational Database Service 記錄
- Amazon OpenSearch 服務慢速索引日誌
- X 射線追蹤
- AWS Directory Service 日誌
- AWS Config 項目
- 快照

保護

制定和實施適當的保護措施，以確保提供關鍵基礎設施服務和安全編碼實務。

安全存取管理

服務是否在其 IAM 或資源政策中使用最低特權做法？

密碼和私密的複雜性是否足夠？ 它們是否適當輪換？

此服務是否使用多重因素認證 (MFA)？

服務是否避免 root 使用者？

以資源為基礎的政策是否允許公開存取？

安全網路組態

此服務是否避免公有和不安全的遠端網路存取？

此服務是否正確使用 VPC？ 例如，是否需要在 VPC 中執行任務？

此服務是否正確地分割並隔離敏感資源？

資料保護

靜態資料加密 — 服務是否會加密靜態資料？

傳輸中的資料加密 — 服務是否會加密傳輸中的資料？

資料完整性 — 服務是否驗證資料的完整性？

資料刪除保護 — 服務是否保護資料免於意外刪除？

資料管理/使用 — 您是否使用 Amazon Macie 之類的服務來追蹤敏感資料的位置？

API 保護

服務是否會用 AWS PrivateLink 來保護服務 API 作業？

保護服務

正確的保護服務是否已就緒？ 他們是否提供正確的涵蓋範圍？

保護服務可協助您擺脫針對服務的攻擊和入侵。保護服務的範例 AWS 包括 AWS Control Tower、AWS WAF、 AWS Shield Advanced、Vanta、機 Secrets Manager、IAM 存取分析器和 AWS Resource Access Manager.

安全開發

您使用安全的編碼實務嗎？

您是否避免了諸如開放式 Web 應用程式安全專案 (OWASP) 前十個等漏洞？

偵測

制定和實施適當的活動，以識別網路安全事件的發生。

偵測服務

正確的偵測服務是否已就緒？

他們是否提供正確的涵蓋範圍？

檢 AWS 測服務的例子包括 Amazon GuardDuty AWS Security Hub，Amazon Inspector，Amazon Detective，Amazon CloudWatch 警報 AWS IoT Device Defender，和 AWS Trusted Advisor.

回應

制定並實施適當的活動，以針對偵測到的網路安全事件採取行動。

回應動作

您是否迅速回應安全性事件？

您是否有任何作用中的嚴重或高嚴重性問題清單？

鑑識

您可以安全地取得服務的鑑識資料嗎？ 例如，您是否取得與真正正面發現相關聯的 Amazon EBS 快照？

您是否設立一個鑑識帳戶？

復原

制定和實施適當的活動，以維持恢復計劃，並恢復因網路安全事件而受損的任何功能或服務。

恢復能力

服務組態是否支援正常容錯移轉、彈性擴展和高可用性？

您是否已建立備份？

在所有標準中啟用和停用控制項

AWS Security Hub 產生已啟用控制項的搜尋結果，並在計算安全性分數時考慮所有啟用的控制 您可以選擇在所有安全標準中啟用和停用控制項，或在不同標準中以不同的方式設定啟用狀態。我們建議您使用前一個選項，在此選項中，控制項的啟用狀態會與所有已啟用的標準保持一致。本節說明如何跨標準啟用和停用控制項。若要啟用或停用一個或多個特定標準中的控制項，請參閱啟用和停用特定標準中的控制項。

如果您已設定彙總區域，Security Hub 主控台會顯示來自所有連結區域的控制項。如果控制項可在連結的區域中使用，但在彙總區域中無法使用，則無法從彙總區域啟用或停用該控制項。

> **Note**
>
> 啟用和停用控制項的指示會根據您是否使用中央規劃而有所不同。本節說明差異。集中設定可供整合 Security Hub 和的使用者使用 AWS Organizations。我們建議您使用中央組態來簡化在多帳戶、多區域環境中啟用和停用控制項的程序。

啟用控制項

當您在標準中啟用控制項時，Security Hub 會開始執行控制項的安全性檢查，並產生控制項發現項目。

Security Hub 會在整體安全分數和標準安全分數的計算中包含控制項狀態。如果您開啟合併的控制項發現項目，即使您已在多個標準中啟用控制項，也會收到用於安全性檢查的單一發現項目。如需了解更多資訊，請參閱合併的控制調查結果。

在多個帳戶和區域中實現所有標準的控制

若要在多個帳戶之間啟用安全性控制 AWS 區域，您必須使用中央設定。

當您使用中央組態時，委派的系統管理員可以建立 Security Hub 組態原則，以在啟用的標準中啟用指定的控制項。然後，您可以將組態原則與特定帳戶和組織單位 (OU) 或根建立關聯。設定原則會在您的主區域 (也稱為彙總區域) 和所有連結的區域中生效。

組態原則提供自訂功能。例如，您可以選擇在一個 OU 中啟用所有控制項，也可以選擇在另一個 OU 中僅啟用 Amazon Elastic Compute Cloud (EC2) 控制項。資料粒度等級取決於您組織中安全性涵蓋範

圍的預期目標。如需建立可跨標準啟用指定控制項之組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

> **Note**
>
> 委派的管理員可以建立組態原則，以管理除服務管理標準以外的所有標準中的控制項： AWS Control Tower。此標準的控制項應在 AWS Control Tower 服務中設定。

如果您希望某些帳戶設定自己的控制項，而不是委派的系統管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中個別設定控制項。

在單一帳戶和區域中啟用所有標準的控制

如果您不使用中央設定或是自我管理帳戶，則無法使用設定原則在多個帳戶和區域中集中啟用控制項。但是，您可以使用下列步驟在單一帳戶和區域中啟用控制項。

Security Hub console

在一個帳戶和區域中啟用跨標準的控制

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 從導覽窗格中選擇 [控制項]。
3. 選擇「已停用」頁標。
4. 選擇控制項旁邊的選項。
5. 選擇「啟用控制項」(此選項不會針對已啟用的控制項顯示)。
6. 在要啟用控制項的每個「區域」中重複此動作。

Security Hub API

在一個帳戶和區域中啟用跨標準的控制

1. 調用該 ListStandardsControlAssociationsAPI。提供安全控制 ID。

   請求示例：

```
{
    "SecurityControlId": "IAM.1"
```

```
}
```

2. 調用該 BatchUpdateStandardsControlAssociationsAPI。針對未在中啟用控制項的任何標準，提供 Amazon 資源名稱 (ARN)。若要取得標準 ARN，請執行DescribeStandards。
3. 將AssociationStatus參數設定為等於ENABLED。如果您遵循這些步驟來取得已啟用的控制項，API 會傳回 HTTP 狀態碼 200 回應。

   請求示例：

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. 在要啟用控制項的每個「區域」中重複此動作。

AWS CLI

在一個帳戶和區域中啟用跨標準的控制

1. 執行 list-standards-control-associations 命令。提供安全控制 ID。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. 執行 batch-update-standards-control-associations 命令。針對未在中啟用控制項的任何標準，提供 Amazon 資源名稱 (ARN)。若要取得標準 ARN，請執行指describe-standards令。
3. 將AssociationStatus參數設定為等於ENABLED。如果您遵循下列步驟來取得已啟用的控制項，命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. 在要啟用控制項的每個區域中重複執行。

在啟用的標準中自動啟用新控制項

Security Hub 會定期發布新的安全控制，並將其添加到一個或多個標準。您可以選擇是否在啟用的標準中自動啟用新控制項。

> **Note**
>
> 我們建議使用中央配置來自動啟用新的控制項。如果您的組態原則包含要停用的控制項清單 (以程式設計方式反映`DisabledSecurityControlIdentifiers`參數)，Security Hub 會自動啟用跨標準的所有其他控制項，包括新發行的控制項。如果您的原則包含要啟用的控制項清單 (這反映`EnabledSecurityControlIdentifiers`參數)，Security Hub 會自動停用跨標準的所有其他控制項，包括新發行的控制項。如需詳細資訊，請參閱 Security Hub 組態原則的運作方式。

選擇您偏好的存取方式，並依照步驟在已啟用的標準中自動啟用新的控制項。下列指示只適用於未使用中央設定。

Security Hub console

自動啟用新控制項

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在功能窗格中，選擇 [設定]，然後選擇 [一般] 索引標籤。
3. 在 [控制項] 下選擇 [編輯]
4. 在啟用的標準中開啟自動啟用新控制項。
5. 選擇儲存。

Security Hub API

自動啟用新控制項

1. 調用該 UpdateSecurityHubConfigurationAPI。
2. 若要自動啟用已啟用標準的新控制項，請`AutoEnableControls`將設定為`true`。如果您不想自動啟用新的控制項，請設定`AutoEnableControls`為 false。

AWS CLI

自動啟用新控制項

1. 執行 update-security-hub-configuration 命令。
2. 若要自動啟用已啟用標準的新控制項，請指定`--auto-enable-controls`。如果您不想自動啟用新的控制項，請指定`--no-auto-enable-controls`。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

範例命令

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

停用控制項

當您停用所有標準中的控制項時，會發生下列情況：

- 控制項的安全性檢查已不再執行。
- 不會再為該控制項產生其他問題清單。
- 現有發現項目會在 3-5 天後自動封存 (請注意，這是最好的工作)。
- Security Hub 建立的任何相關 AWS Config 規則都會遭到移除。

您可以在一個或多個特定標準中禁用它，而不是禁用所有標準中的控制項。如果您這麼做，Security Hub 不會針對您停用控制項的標準執行安全性檢查，因此不會影響這些標準的安全性分數。但是，如果在其他標準中啟用控制項，Security Hub 會保留 AWS Config 規則並繼續執行安全性檢查以進行控制項。這可能會影響您的摘要安全分數。如需在特定標準中規劃控制項的指示，請參閱啟用和停用特定標準中的控制項。

若要減少發現雜訊，停用與您的環境無關的控制項會很有用。如需要停用哪些控制項的建議，請參閱您可能要停用的 Security Hub 控制項。

停用標準時，會停用套用至標準的所有控制項 (不過，這些控制項可能會在其他標準中保持啟用狀態)。若要取得有關停用標準的資訊，請參閱the section called “啟用和停用標準”。

當您停用標準時，Security Hub 不會追蹤哪些控制項已停用。如果您隨後再次啟用該標準，則套用至該標準的所有控制項都會自動啟用。此外，停用控制項是一次性的動作。假設您停用控制項，然後啟用先

前已停用的標準。如果標準包含該控制項，則會在該標準中啟用該控制項。當您在 Security Hub 中啟用標準時，會自動啟用適用於該標準的所有控制項。

在多個帳戶和區域中停用所有標準的控制

若要停用跨多個帳戶的安全性控制 AWS 區域，您必須使用中央設定。

當您使用中央組態時，委派的系統管理員可以建立 Security Hub 組態原則，在已啟用的標準中停用指定的控制項。然後，您可以將組態原則與特定帳戶、OU 或根建立關聯。設定原則會在您的主區域 (也稱為彙總區域) 和所有連結的區域中生效。

組態原則提供自訂功能。例如，您可以選擇停用一個 OU 中的所有 AWS CloudTrail 控制項，也可以選擇停用另一個 OU 中的所有 IAM 控制。資料粒度等級取決於您組織中安全性涵蓋範圍的預期目標。如需建立可跨標準停用指定控制項之組態原則的指示，請參閱建立和關聯安全性中樞組態原則。

> **Note**
>
> 委派的管理員可以建立組態原則，以管理除服務管理標準以外的所有標準中的控制項： AWS Control Tower。此標準的控制項應在 AWS Control Tower 服務中設定。

如果您希望某些帳戶設定自己的控制項，而不是委派的系統管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中個別設定控制項。

在單一帳戶和區域中停用所有標準中的控制項

如果您不使用中央設定或是自我管理帳戶，則無法使用設定原則集中停用多個帳戶和區域中的控制項。但是，您可以使用下列步驟來停用單一帳戶和區域中的控制項。

Security Hub console

在一個帳戶和區域中停用跨標準的控制

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 從導覽窗格中選擇 [控制項]。
3. 選擇控制項旁邊的選項。
4. 選擇「停用控制項」（已停用的控制項目不會顯示此選項）。
5. 選取停用控制項的原因，然後選擇停用來確認。
6. 在要禁用控件的每個區域中重複此操作。

Security Hub API

在一個帳戶和區域中停用跨標準的控制

1. 調用該 ListStandardsControlAssociationsAPI。提供安全控制 ID。

   請求示例：

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. 調用該 BatchUpdateStandardsControlAssociationsAPI。提供在中啟用控制項之任何標準的 ARN。若要取得標準 ARN，請執行DescribeStandards。
3. 將AssociationStatus參數設定為等於DISABLED。如果您依照下列步驟執行已停用的控制項，API 會傳回 HTTP 狀態碼 200 回應。

   請求示例：

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
   v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}}]
   }
   ```

4. 在要禁用控件的每個區域中重複此操作。

AWS CLI

在一個帳戶和區域中停用跨標準的控制

1. 執行 list-standards-control-associations 命令。提供安全控制 ID。

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

2. 執行 batch-update-standards-control-associations 命令。提供在中啟用控制項之任何標準的 ARN。若要取得標準 ARN，請執行指describe-standards令。
3. 將AssociationStatus參數設定為等於DISABLED。如果您依照下列步驟執行已停用的控制項，則命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. 在要禁用控件的每個區域中重複此操作。

在啟用的標準中自動啟用新控制項

AWS Security Hub 定期釋放新控制項，並將它們新增至一個或多個標準。您可以選擇是否在啟用的標準中自動啟用新控制項。

> **Note**
>
> 如果您使用中央組態，並在組態原則中包含要停用的特定控制項清單 (以程式設計方式反映DisabledSecurityControlIdentifiers參數，Security Hub 會自動啟用跨標準的所有其他控制項，包括新發行的控制項。如需詳細資訊，請參閱 Security Hub 組態原則的運作方式。

我們建議您使用安全中心中央組態來自動啟用新的安全性控制項。您可以建立組態原則，其中包含要跨標準停用的控制項清單。預設會啟用所有其他控制項，包括新發行的控制項。或者，您可以建立包含要跨標準啟用的控制項清單的策略。預設情況下，所有其他控制項 (包括新發行的控制項) 都會停用。如需詳細資訊，請參閱 安全中心中的集中配置。

當新的控制項新增至您尚未啟用的標準時，Security Hub 不會啟用這些控制項。

下列指示只適用於未使用中央設定。

選擇您偏好的存取方式，並依照步驟在已啟用的標準中自動啟用新的控制項。

Security Hub console

自動啟用新控制項

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在功能窗格中，選擇 [設定]，然後選擇 [一般] 索引標籤。
3. 在 [控制項] 下選擇 [編輯]
4. 在啟用的標準中開啟自動啟用新控制項。
5. 選擇儲存。

Security Hub API

自動啟用新控制項

1. 執行 UpdateSecurityHubConfiguration。
2. 若要自動啟用已啟用標準的新控制項，請AutoEnableControls將設定為true。如果您不想自動啟用新的控制項，請設定AutoEnableControls為 false。

AWS CLI

自動啟用新控制項

1. 執行 update-security-hub-configuration 命令。
2. 若要自動啟用已啟用標準的新控制項，請指定--auto-enable-controls。如果您不想自動啟用新的控制項，請指定--no-auto-enable-controls。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

範例命令

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

如果您沒有自動啟用新的控制項，則必須手動啟用它們。如需說明，請參閱the section called “在所有標準中啟用和停用控制項”。

自訂控制參數

某些 Security Hub 控制項會使用會影響控制項評估方式的參數。一般而言，這類控制項會根據 Security Hub 定義的預設參數值來評估。但是，對於這些控制項的子集，您可以自訂參數值。當您自訂控制項的參數值時，Security Hub 會開始針對您指定的值評估控制項。如果控制項基礎的資源滿足自訂值，Security Hub 會產生一個PASSED發現項目。如果資源不符合自訂值，Security Hub 會產生一個FAILED發現項目。

透過自訂控制參數，您可以調整 Security Hub 所建議和監控的安全性最佳作法，以符合您的業務需求和安全性預期。您可以自訂一或多個參數，以取得符合您安全性需求的發現項目，而不是隱藏控制項的發現項目。

以下是一些自定義控件參數的示例用例：

- [CloudWatch.16] — CloudWatch 記錄群組應保留指定的時間段

  您可以指定保留期間。
- [IAM.7] — IAM 使用者的密碼政策應具有強大的組態

  您可以指定與密碼強度相關的參數。
- [EC2.18] — 安全群組只允許授權連接埠不受限制的傳入流量

  您可以指定授權哪些連接埠允許不受限制的傳入流量。
- [Lambda .5] — VPC Lambda 函數應在多個可用區域中運作

  您可以指定產生傳遞之發現項目的可用區域數目下限。

本節說明如何自訂和管理控制項參數。

自訂控制項參數如何運作

控制項可以有一個或多個可自訂的參數。個別控制項參數的可能資料類型包括：

- Boolean
- Double
- 列舉
- EnumList
- Integer

- IntegerList
- 字串
- StringList

對於某些控制項，可接受的參數值也必須落入指定的範圍內才能有效。在這些情況下，Security Hub 會提供可接受的範圍。

Security Hub 選擇默認參數值，並可能偶爾更新它們。自訂控制參數後，除非您變更它，否則其值會繼續為您為參數指定的值。也就是說，即使參數的自訂值與 Security Hub 定義的目前預設值相符，參數也會停止追蹤預設 Security Hub 值的更新。以下是控制項的範例 [ACM.1] — 匯入和 ACM 核發的憑證應在指定的時間段後續約：

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

在上述範例中，daysToExpiration參數的自訂值為30。此參數的目前預設值也是30。如果安全性中心將預設值變更為14，則此範例中的參數將不會追蹤該變更。它將保留的值30。

如果您想要追蹤參數之預設 Security Hub 值的更新，請將ValueType欄位設定為DEFAULT而非CUSTOM。如需詳細資訊，請參閱 回復為單一科目與區域中的預設參數值。

當您變更參數值時，也會觸發新的安全性檢查，以根據新值評估控制項。然後，Security Hub 會根據新值產生新的控制項發現項目。在定期更新以控制發現項目時，Security Hub 也會使用新的參數值。如果您變更控制項的參數值，但尚未啟用任何包含控制項的標準，Security Hub 不會使用新值執行任何安全性檢查。您必須為 Security Hub 啟用至少一個相關標準，才能根據新的參數值評估控制項。

自訂參數值適用於已啟用的標準。您無法自訂目前區域不支援的控制項參數。如需個別控制項的區域限制清單，請參閱控制區域限制。

自訂控制參數

自訂控制參數的指示會根據您是否使用中央規劃而有所不同。中央組態是委派的 Security Hub 系統管理員可用來管理其組織中帳戶和組織單位 (OU) 之間 AWS 區域的 Security Hub 功能的一項功能。

如果您的組織使用中央組態，委派的管理員可以建立包含自訂控制項參數的組態原則。這些政策可以與集中管理的成員帳戶和 OU 產生關聯，並在您的本地區域和所有連結的區域中生效。委派的系統管理員也可以將一或多個帳戶指定為自我管理帳戶，讓帳戶擁有者在每個區域中分別設定自己的參數。如果您的組織不使用中央設定，您必須在每個帳戶和區域中個別自訂控制參數。

跨多個帳戶和區域自訂控制參數

使用中央設定時，您可以針對跨多個帳戶和區域的集中管理帳戶和 OU 自訂控制參數。我們建議您使用中央組態，因為它可讓您在組織的不同部分對齊控制參數值。例如，您的所有測試帳戶可能使用某些參數值，並且所有生產帳戶可能使用不同的值。

如果您是使用中央設定之組織的委派 Security Hub 系統管理員，請選擇偏好的方法，然後依照步驟自訂多個帳戶和區域的控制參數。

Security Hub console

若要在多個帳戶和區域中自訂控制參數

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   確定您已登入本地區域。
2. 在功能窗格中，選擇 [設定和組態]。
3. 選擇 Policies (政策) 標籤。
4. 若要建立包含自訂參數的新組態原則，請選擇 [建立原則]。若要在現有組態原則中指定自訂參數，請選取原則，然後選擇 [編輯]。

   使用自訂參數建立新的組態原則

   1. 在 [自訂原則] 區段中，選擇您要啟用的安全性標準和控制項。
   2. 選取 [自訂控制參數]。
   3. 選取控制項，然後指定一個或多個參數的自訂值。
   4. 若要自訂更多控制項的參數，請選擇 [自訂其他控制項]
   5. 在 [帳戶] 區段中，選取您要套用原則的帳戶或 OU。

6. 選擇下一步。
7. 選擇 [建立原則並套用]。在您的首頁區域和所有連結的區域中，此動作會覆寫與此組態原則相關聯之帳戶和 OU 的現有組態設定。帳戶和 OU 可透過直接應用或從父項繼承，與組態原則產生關聯。

在現有組態原則中新增或編輯自訂參數

1. 在 [控制項] 區段的 [自訂原則] 底下，指定您想要的新自訂參數值。
2. 如果這是您第一次在此原則中自訂控制項參數，請選取 [自訂控制項參數]，然後選取要自訂的控制項。若要自訂更多控制項的參數，請選擇 [自訂其他控制項]
3. 在 [帳戶] 區段中，確認您要套用原則的帳戶或 OU。
4. 選擇下一步。
5. 檢閱您的變更，並確認變更正確無誤。完成後，選擇 [儲存原則並套用]。在您的首頁區域和所有連結的區域中，此動作會覆寫與此組態原則相關聯之帳戶和 OU 的現有組態設定。帳戶和 OU 可透過直接應用或從父項繼承，與組態原則產生關聯。

Security Hub API

若要在多個帳戶和區域中自訂控制參數

使用自訂參數建立新的組態原則

1. 從首頁區域中委派的系統管理員帳戶叫用 CreateConfigurationPolicyAPI。
2. 針對`SecurityControlCustomParameters`物件，提供您要自訂之每個控制項的識別元。
3. 針對`Parameters`物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提`CUSTOM`供`ValueType`。對於`Value`，提供參數的資料類型和自訂值。該`Value`字段不能為空`ValueType`時`CUSTOM`。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以叫用 GetSecurityControlDefinitionAPI 來尋找控制項的支援參數、資料類型和有效值。

在現有組態原則中新增或編輯自訂參數

1. 從首頁區域中委派的系統管理員帳戶叫用 UpdateConfigurationPolicyAPI。
2. 對於`Identifier`欄位，請提供您要更新之組態政策的 Amazon 資源名稱 (ARN) 或識別碼。
3. 針對`SecurityControlCustomParameters`物件，提供您要自訂之每個控制項的識別元。

4. 針對Parameters物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提CUSTOM供ValueType。對於Value，提供參數的資料類型和自訂值。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以叫用 GetSecurityControlDefinitionAPI 來尋找控制項的支援參數、資料類型和有效值。

建立新設定原則的 API 要求範例：

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

若要在多個帳戶和區域中自訂控制參數

使用自訂參數建立新的組態原則

1. 從首頁區域中委派的系統管理員帳戶執行create-configuration-policy命令。
2. 針對SecurityControlCustomParameters物件，提供您要自訂之每個控制項的識別元。
3. 針對Parameters物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提CUSTOM供ValueType。對於Value，提供參數的資料類型和自訂值。該Value字段不能為空ValueType時CUSTOM。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以透過執行get-security-control-definition指令尋找控制項的支援參數、資料類型和有效值。

新增或編輯現有組態原則中的參數

1. 若要在現有組態原則中新增或更新自訂輸入參數，請從主區域中的委派管理員帳戶執行update-configuration-policy命令。
2. 在identifier欄位中，提供您要更新之政策的 Amazon 資源名稱 (ARN) 或識別碼。
3. 針對SecurityControlCustomParameters物件，提供您要自訂之每個控制項的識別元。
4. 針對Parameters物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提CUSTOM供ValueType。對於Value，提供參數的資料類型和自訂值。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以透過執行get-security-control-definition指令尋找控制項的支援參數、資料類型和有效值。

建立新組態原則的範例命令：

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

在單一帳戶與區域中自訂控制參數

如果您不使用中央設定或擁有自我管理帳戶，您可以一次在一個區域中為帳戶自訂控制參數

選擇您喜歡的方法，然後按照步驟自定義控制參數。您的變更僅適用於您目前所在地區的帳戶。若要自訂其他區域中的控制參數，請在您要自訂參數的每個額外帳戶和區域中重複下列步驟。相同的控制項可以在不同的區域中使用不同的參數值。

Security Hub console

在一個帳戶和區域中自訂控制參數

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中，選擇 [控制項]。在表格中，選擇支援自訂參數的控制項，並且您想要變更的參數。「自訂參數」欄會指出哪些控制項支援自訂參數。
3. 在控制項的詳細資訊頁面上，選擇 [參數] 索引標籤，然後選擇 [編輯]。
4. 指定所需的參數值。
5. 選擇性地在「變更原因」區段中，選取自訂參數的原因。
6. 選擇儲存。

Security Hub API

在一個帳戶和區域中自訂控制參數

1. 調用該 UpdateSecurityControlAPI。
2. 針對`SecurityControlId`，提供您要自訂之控制項的 ID。
3. 針對`Parameters`物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提`CUSTOM`供`ValueType`。對於`Value`，提供參數的資料類型和自訂值。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以叫用 GetSecurityControlDefinitionAPI 來尋找控制項的支援參數、資料類型和有效值。
4. (選擇性) 提供自訂控制參數的原因。`LastUpdateReason`

API 請求示例：

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

在一個帳戶和區域中自訂控制參數

1. 執行 update-security-control 命令。
2. 針對`security-control-id`，提供您要自訂之控制項的 ID。
3. 針對`parameters`物件，提供您要自訂之每個參數的名稱。針對您自訂的每個參數，提`CUSTOM`供`ValueType`。對於`Value`，提供參數的資料類型和自訂值。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。您可以透過執行get-security-control-definition指令尋找控制項的支援參數、資料類型和有效值。
4. (選擇性) 提供自訂控制參數的原因。`last-update-reason`

範例命令：

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

檢查控制參數的狀態

驗證和檢查控制參數的變更狀態很重要。這有助於確保控制項能如您預期般運作，並提供預期的安全性值。若要確認參數更新是否成功，您可以在 Security Hub 主控台上檢閱控制項的詳細資料。在主控台上，選擇要顯示其詳細資料的控制項。「參數」標籤會顯示參數變更的狀態。

以程式設計方式，如果您更新參數的請求是有效的，則該`UpdateStatus`字段的值是`UPDATING`對BatchGetSecurityControls操作的響應。這表示更新有效，但您的發現項目可能尚未包含更新的參數值。當值`UpdateState`變更為時`READY`，您的發現項目會開始包含更新的參數值。

此作`UpdateSecurityControl`業會傳回無效參數值的回`InvalidInputException`應。回應會提供有關失敗原因的其他詳細資訊。例如，您可能指定的值超出參數的有效範圍。或者，您指定的值不使用正確的資料類型。使用有效的輸入再次提交您的請求。如果參數更新不成功，Security Hub 會保留該參數的目前值。

如果您嘗試更新參數值時發生內部失敗，Security Hub 會自動重試 (如果您已 AWS Config 啟用)。如需詳細資訊，請參閱 配置 AWS Config。

檢閱控制項參數

您可以複查帳戶中個別控制參數的目前值。如果您使用中央組態，委派的 Security Hub 系統管理員也可以檢閱組態原則中指定的參數值。

選擇您偏好的方法，並依照步驟檢閱目前的控制參數值。

Security Hub console

檢閱目前參數值的步驟

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中，選擇 [控制項]。選擇一個控制項。
3. 選擇參數索引標籤。此頁籤顯示控制項目前的參數值。

Security Hub API

檢閱目前參數值的步驟

呼叫 BatchGetSecurityControlsAPI，並提供一或多個安全控制 ID 或 ARN。回應中的`Parameters`物件會顯示指定控制項的目前參數值。

API 請求示例：

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

檢閱目前參數值的步驟

執行命batch-get-security-controls令，並提供一或多個安全控制 ID 或 ARN。回應中的Parameters物件會顯示指定控制項的目前參數值。

範例命令：

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

選擇您偏好的方法，以便在中央組態原則中檢視目前的參數值。

Security Hub console

檢閱組態原則中目前的參數值

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   使用主區域中委派安全中心系統管理員帳戶的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 在 [原則] 索引標籤上，選取組態原則，然後選擇 [檢視詳細資料]。然後會顯示策略詳細資訊，包括目前的參數值。

Security Hub API

檢閱組態原則中目前的參數值

1. 從首頁區域中委派的系統管理員帳戶叫用 GetConfigurationPolicyAPI。
2. 提供您要查看其詳細資料之組態原則的 ARN 或識別碼。回應包括目前的參數值。

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

檢閱組態原則中目前的參數值

1. 從首頁區域中委派的系統管理員帳戶執行get-configuration-policy命令。
2. 提供您要查看其詳細資料之組態原則的 ARN 或識別碼。回應包括目前的參數值。

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

您的控制項結果也會顯示目前的參數值。在中AWS 安全性發現格式 (ASFF) 語法，這些值會顯示在Compliance物件的Parameters欄位中。若要檢閱 Security Hub 主控台上的發現項目，請在導覽窗格中選擇 [發現項目]。若要以程式設計方式檢閱發現項目，請使用 GetFindings

> **Note**
>
> 發行自訂控制項參數功能之後，Security Hub 會更新現有的控制項發現項目，以包含 Parameters ASFF 欄位。這可能需要長達 24 小時。

還原為預設控制參數值

控制參數可以具有 Security Hub 定義的預設值。我們可能會更新參數的預設值，以反映不斷發展的安全性最佳做法。如果您尚未指定控制項參數的自訂值，控制項會自動追蹤這些更新並使用新的預設值。

您可以還原為使用控制項的預設參數值。執行此操作的方式取決於您是否使用中央規劃。

> **Note**
>
> 並非所有控制項參數都有預設的 Security Hub 值。在這種情況下，當`ValueType`設定為時`DEFAULT`，沒有 Security Hub 使用的特定預設值。而是，在沒有自訂值的情況下，Security Hub 會忽略參數。

在多個科目與區域回復為預設參數值

如果您使用中央設定，您可以針對跨多個帳戶和區域還原集中管理帳戶和 OU 的控制參數。

選擇您偏好的方法，然後按照步驟使用中央配置在多個帳戶和區域中還原為預設參數值。

Security Hub console

在多個帳戶和區域中還原為預設參數值

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/

   使用安全中心委派系統管理員帳戶在主區域中的認證登入。
2. 在功能窗格中，選擇 [設定和組態]。
3. 選擇 Policies (政策) 標籤。
4. 選取策略，然後選擇 [編輯]。
5. 在 [自訂原則] 底下，[控制項] 區段會顯示您為其指定自訂參數的控制項清單。
6. 尋找具有要還原之一或多個參數值的控制項。然後，選擇「移除」以恢復為預設值。
7. 在 [帳戶] 區段中，確認您要套用原則的帳戶或 OU。
8. 選擇下一步。
9. 檢閱您的變更，並確認變更正確無誤。完成後，選擇 [儲存原則並套用]。在您的首頁區域和所有連結的區域中，此動作會覆寫與此組態原則相關聯之帳戶和 OU 的現有組態設定。帳戶和 OU 可透過直接應用或從父項繼承，與組態原則產生關聯。

Security Hub API

在多個帳戶和區域中還原為預設參數值

1. 從首頁區域中委派的系統管理員帳戶叫用 UpdateConfigurationPolicyAPI。
2. 在`Identifier`欄位中，提供您要更新之政策的 Amazon 資源名稱 (ARN) 或識別碼。

3. 針對SecurityControlCustomParameters物件，提供您要還原一或多個參數之每個控制項的識別元。
4. 在Parameters物件中，針對您要還原的每個參數，提DEFAULT供ValueType欄位。設定ValueType為時DEFAULT，您不需要為Value欄位提供值。如果您的要求中包含一個值，Security Hub 會忽略它。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。

> **Warning**
>
> 如果您省略SecurityControlCustomParameters欄位中的控制項物件，Security Hub 會將控制項的所有自訂參數還原為其預設值。完全空白的清單SecurityControlCustomParameters會將所有控制項的自訂參數還原為其預設值。

API 請求示例：

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
```

```
                            "ValueType": "DEFAULT"
                        }
                    }
                }
            ]
        }
    }
}
```

AWS CLI

在多個帳戶和區域中還原為預設參數值

1. 從首頁區域中委派的系統管理員帳戶執行update-configuration-policy命令。
2. 在identifier欄位中，提供您要更新之政策的 Amazon 資源名稱 (ARN) 或識別碼。
3. 針對SecurityControlCustomParameters物件，提供您要還原一或多個參數之每個控制項的識別元。
4. 在Parameters物件中，針對您要還原的每個參數，提DEFAULT供ValueType欄位。設定ValueType為時DEFAULT，您不需要為Value欄位提供值。如果您的要求中包含一個值，Security Hub 會忽略它。如果您的請求省略控制項支援的參數，則該參數會保留其目前的值。

> **Warning**
>
> 如果您省略SecurityControlCustomParameters欄位中的控制項物件，Security Hub 會將控制項的所有自訂參數還原為其預設值。完全空白的清單SecurityControlCustomParameters會將所有控制項的自訂參數還原為其預設值。

範例命令：

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
```

```
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}'
```

回復為單一科目與區域中的預設參數值

如果您不使用中央設定或擁有自我管理帳戶，您可以一次在一個區域中回復為使用帳戶的預設參數值。

選擇您偏好的方法，然後依照步驟將帳戶在單一區域中還原為預設參數值。若要恢復到其他區域中的預設參數值，請在每個額外的「區域」中重複這些步驟。

> **Note**
>
> 如果您停用 Security Hub，則會重設您的自訂控制項參數。如果您 future 再次啟用 Security Hub，所有控制項都會使用預設參數值來啟動。

Security Hub console

在一個帳戶和區域中還原為預設參數值

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中，選擇 [控制項]。選擇要還原為預設參數值的控制項。
3. 在`Parameters`標籤上，選擇控制參數旁邊的「自訂」。然後，選擇刪除自定義。此參數現在會使用預設的 Security Hub 值，並追蹤預設值的 future 更新。
4. 針對要還原的每個參數值重複上述步驟。

Security Hub API

在一個帳戶和區域中還原為預設參數值

1. 調用該 UpdateSecurityControlAPI。
2. 針對`SecurityControlId`，提供您要還原其參數之控制項的 ARN 或 ID。

3. 在Parameters物件中，針對您要還原的每個參數，提DEFAULT供ValueType欄位。設定ValueType為時DEFAULT，您不需要為Value欄位提供值。如果您的要求中包含一個值，Security Hub 會忽略它。
4. (選擇性) 提供回復為預設參數值的原因。LastUpdateReason

API 請求示例：

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

在一個帳戶和區域中還原為預設參數值

1. 執行 update-security-control 命令。
2. 針對security-control-id，提供您要還原其參數之控制項的 ARN 或 ID。
3. 在parameters物件中，針對您要還原的每個參數，提DEFAULT供ValueType欄位。設定ValueType為時DEFAULT，您不需要為Value欄位提供值。如果您的要求中包含一個值，Security Hub 會忽略它。
4. (選擇性) 提供回復為預設參數值的原因。last-update-reason

範例命令：

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

支援自訂參數的控制項

如需支援自訂參數的安全控制項清單，您可以參閱 Security Hub 主控台上的 [控制項] 頁面或Security Hub 控制項參考. 若要以程式設計方式擷取此清單，您可以使用此ListSecurityControlDefinitions作業。在回應中，`CustomizableProperties`物件會指出哪些控制項支援可自訂參數。

您可能想要停用的 Security Hub 控制項

我們建議停用某些 AWS Security Hub 控制項，以減少發現噪音並限制成本。

處理全球資源的控制項

某些資源 AWS 服務 支援全域資源，這表示您可以從任何 AWS 區域. 為了節省成本 AWS Config，您可以在除一個區域以外的所有區域中禁用全局資源的記錄。不過，Security Hub 靜止影像會在啟用控制項的所有區域執行安全性檢查，並根據每個區域每個帳戶的檢查次數向您收費。因此，為了減少發現噪音並節省 Security Hub 的成本，您還應該在除記錄全球資源的區域以外的所有區域中停用涉及全域資源的控制項。

> **Note**
>
> 如果您使用中央組態，Security Hub 會自動停用與所有區域 (主區域除外) 中涉及全域資源的控制項。其他控制項會在所有可用的區域中啟用。若要將這些控制項的發現項目限制為只有一個「區域」，您可以更新記 AWS Config 錄器設定，並關閉所有區域中的全域資源記錄，但本地區域除外。如需中央規劃的更多資訊，請參閱安全中心中的集中配置。

對於具有定期排程類型的控制項，必須在 Security Hub 中停用這些控制項，以防止計費。`includeGlobalResourceTypes`將 AWS Config 參數設定為`false`不會影響定期 Security Hub 控制項。

如果您停用記錄一或多個區域中的全域資源，則 AWS Config 應啟用 [Config.1] 控制項會在這些區域中產生失敗的發現。這是因為 Config.1 需要記錄全局資源才能通過。您可以手動或透過自動化規則隱藏此控制項的發現項目。

以下是涉及全域資源的安全中樞控制項清單：

- [帳戶。1] 應提供安全聯繫信息 AWS 帳戶
- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.7] IAM 使用者的密碼政策應具有強大的組態
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config
- [IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母
- [IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母
- [IAM.13] 確保 IAM 密碼政策至少需要一個符號
- [IAM.14] 確保 IAM 密碼政策至少需要一個數字
- [IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高
- [IAM.16] 確保 IAM 密碼政策防止密碼重複使用
- [IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support

- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.20] 避免使用根用戶
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

處理 CloudTrail 日誌記錄的控制

此控制項處理使用 AWS Key Management Service (AWS KMS) 加密 AWS CloudTrail 追蹤記錄。如果您在集中式記錄帳戶中記錄這些追蹤，則只需在帳戶和發生集中記錄的區域中啟用此控制項。

> **Note**
>
> 如果您使用中央設定，則控制項的啟用狀態會在主「區域」和「連結的區域」之間保持一致。您無法在某些地區停用控制項，並在其他地區啟用該控制項。在此情況下，請抑制下列控制項的發現項目，以減少尋找雜訊。

- [CloudTrail.2] CloudTrail 應啟用靜態加密

處理 CloudWatch 警報的控制項

如果您偏好使用 Amazon GuardDuty 進行異常偵測，而不是 Amazon CloudWatch 警示，您可以停用這些控制項，這些控制將重點放在 CloudWatch 警示上。

- [CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報

- [CloudWatch.2] 確保未經授權的 API 調用存在日誌指標過濾器和警報
- [CloudWatch.3] 確保沒有 MFA 的管理控制台登錄存在日誌指標過濾器和警報
- [CloudWatch.4] 確保 IAM 政策更改存在日誌指標過濾器和警報
- [CloudWatch.5] 確保存在配 CloudTrail AWS Config置更改的日誌指標過濾器和警報
- [CloudWatch.6] 確保 AWS Management Console 驗證失敗存在日誌指標過濾器和警報
- [CloudWatch.7] 確保存在日誌指標過濾器和警報，以停用或排程刪除客戶管理的金鑰
- [CloudWatch.8] 確保 S3 儲存貯體政策變更存在日誌指標篩選器和警示
- [CloudWatch.9] 確保存在 AWS Config 配置更改的日誌指標過濾器和警報
- [CloudWatch.10] 確保安全組更改存在日誌指標過濾器和警報
- [CloudWatch.11] 確定網路存取控制清單 (NACL) 的變更存在記錄指標篩選器和警示
- [CloudWatch.12] 確定網路閘道變更存在記錄指標篩選器和警示
- [CloudWatch.13] 確保路由表更改存在日誌度量過濾器和警報
- [CloudWatch.14] 確保 VPC 更改存在日誌指標過濾器和警報

檢視控制項的詳細資訊

對於每個 AWS Security Hub 控件，您可以顯示有用的詳細信息的頁面。

控制項詳細資訊頁面的頂端提供控制項的簡介，包括：

- 啟用狀態 — 頁面頂端會告訴您是否已針對至少一個成員帳戶中的一個標準啟用控制項。如果您已設定彙總區域，則至少在一個「區域」中針對至少一個標準啟用該控制項，則會啟用該控制項。如果控制項已停用，您可以從此頁面啟用控制項。如果已啟用控制項，您可以從此頁面停用它。如需詳細資訊，請參閱 the section called “在所有標準中啟用和停用控制項”。
- 控制項狀態 — 此狀態會根據控制項發現項目的符合性狀態彙總控制項的效能。Security Hub 通常會在您第一次造訪 Security Hub 主控台上的 [摘要] 頁面或 [安全性標準] 頁面後的 30 分鐘內產生初始控制狀態。狀態僅適用於您造訪這些頁面時啟用的控制項。使用 `UpdateStandardsControl`API 作業可啟用或停用控制項。此外，必須配置 AWS Config 資源記錄才能顯示控制狀態。第一次產生控制項狀態之後，Security Hub 會根據前 24 小時的發現項目，每 24 小時更新一次控制項狀態。在標準詳細資料頁面和控制項詳細資料頁面上，Security Hub 會顯示時間戳記，以指出上次更新狀態的時間。

  管理員帳戶可查看整個管理員帳戶和成員帳戶的彙總控制狀態。如果您已設定聚總區域，則控制項狀態會包含所有連結區域的搜尋結果。如需控制項狀態的詳細資訊，請參閱the section called “法規遵循狀態和控制狀態”。

> **Note**
>
> 在啟用控制中國地區和中國地區產生首次控制狀態後，最多可能需要 24 小時的時間 AWS GovCloud (US) Region。

[標準和需求] 索引標籤會列出控制項可啟用的標準，以及與不同合規性架構控制項相關的需求。

詳細資訊頁面的底部包含控制項之作用中發現項目的相關資訊。控制項發現項目是由針對控制項的安全檢查所產生。控制項搜尋結果清單不包含已封存的發現項目。

尋找項目清單使用顯示清單不同子集的標籤。在大多數索引標簽中，搜尋結果清單會顯示工作流程狀態為NEWNOTIFIED、或的發現項目RESOLVED。另一個標籤會顯示SUPPRESSED發現項目。

對於每個發現項目，此清單可讓您存取尋找詳細資訊，例如符合性狀態和相關資源。您也可以設定每個搜尋結果的工作流程狀態，並將搜尋結果傳送至自訂動作。如需詳細資訊，請參閱 the section called “檢視控制項發現項目並採取動作”。

檢視控制項的詳細資訊

選擇您偏好的存取方式，然後依照下列步驟檢視控制項的詳細資訊。詳細資訊適用於目前帳戶和區域，包括下列項目：

- 控制項的標題和說明
- 失敗控制項發現項的補救指示連結
- 控制項的嚴重性
- 控制項的啟用狀態
- (在主控台上) 控制項的最近發現項目清單。使用安全中心 API 時 AWS CLI，或用於擷`GetFindings`取控制項發現項目。

Security Hub console

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 在導覽窗格中選擇 [控制項]。
3. 選取控制項。

Security Hub API

1. 執行並提供一或多個標準 ARN[ListSecurityControlDefinitions](#)，以取得該標準的控制 ID 清單。若要取得標準 ARN，請執行[DescribeStandards](#)。如果您未提供標準 ARN，此 API 會傳回所有 Security Hub 控制項識別碼。此 API 會傳回與標準無關的安全控制 ID，而不是在這些功能發行之前存在的標準型控制 ID。

   請求示例：

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 執行[BatchGetSecurityControls](#)以取得目前 AWS 帳戶 和中一或多個控制項的詳細資訊 AWS 區域。

   請求示例：

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. 執行[list-security-control-definitions](#)命令，並提供一或多個標準 ARN 以取得控制 ID 清單。若要取得標準 ARN，請執行指describe-standards令。如果您未提供標準 ARN，此命令會傳回所有 Security Hub 控制項識別碼。此命令會傳回與標準無關的安全性控制 ID，而不是在這些功能發行之前存在的標準型控制 ID。

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
   ```

2. 執行命[batch-get-security-controls](#)令以取得目前 AWS 帳戶 和中一或多個控制項的詳細資訊 AWS 區域。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

篩選和排序控制項清單

在 [控制項] 頁面上，您可以看到控制項清單。您可以篩選和排序清單，以便著重於控制項的特定子集。

- 全部已啟用 (至少在一個已啟用的標準中啟用的控制項)
- 失敗 (具有`Failed`狀態的控制項)
- 未知 (具有`Unknown`狀態的控制項)
- 通過 (具有`Passed`狀態的控制項)
- 已停用 (在所有標準中停用的控制項)
- 沒有資料 (沒有發現項目的控制項)
- 全部 (所有控制項，已啟用與停用，且不考慮控制項狀態或搜尋結果計數)

如需控制項狀態的詳細資訊，請參閱法規遵循狀態和控制狀態。

如果您正在使用整合， AWS Organizations 且已登入 AWS Security Hub 管理員帳戶，則 [全部已啟用] 索引標籤會包含至少在一個成員帳戶中啟用的控制項。如果您已設定聚總區域，則「全部已啟用」頁標會包含至少在一個連結「區域」中啟用的控制項。

依預設，會顯示 [失敗] 索引標籤。在每個索引標籤上，控制項預設會依嚴重性排序，從「嚴重」到「低」。您也可以依照控制項 ID、符合性狀態、嚴重性或失敗檢查次數來排序控制項。搜尋列可讓您搜尋特定控制項。

> **Tip**
>
> 如果您有根據控制項發現項目的自動化工作流程，建議您使用`SecurityControlId`或`SecurityControlArn` ASFF 欄位作為篩選器，而不是`Title`或`Description`。後一個字段可以偶爾更改，而控制 ID 和 ARN 是靜態標識符。

選擇控制項旁邊的選項會顯示一個側面板，其中顯示目前啟用控制項的標準。您也可以查看目前停用控制項的標準。在此面板中，您可以透過在所有標準中停用控制項來停用控制項。若要取得有關跨標準啟

用和停用控制項的更多資訊，請參閱在所有標準中啟用和停用控制項。對於管理員帳戶，側邊面板中顯示的資訊會反映所有成員帳戶。

在 Security Hub API 上，執行ListSecurityControlDefinitions以取回控制 ID 清單。一旦你有興趣的控制 ID，運行BatchGetSecurityControls以獲取有關當前 AWS 帳戶 和控件的子集的數據 AWS 區域。

檢視控制項發現項目並採取動作

控制項詳細資訊頁面會顯示控制項的作用中發現項目清單。此清單不包含已封存的發現項目。

控制項詳細資訊頁面支援尋找彙總。如果您已設定聚總區域，則控制項詳細資訊頁面上的控制項狀態和安全性檢查清單會包含來自所有連結的檢查 AWS 區域。

此清單提供了篩選和排序發現項目的工具，以便您可以先專注於更緊急的發現項目。發現項目可能包含相關服務主控台中資源詳細資料的連結。對於以 AWS Config 規則為基礎的控制項，您可以檢視有關規則和組態時間表的詳細資訊。

您也可以使用 AWS Security Hub API 擷取發現項目清單。如需詳細資訊，請參閱 the section called “擷取尋找項目詳細資訊 (程式化)”。

主題

- 檢視控制項搜尋與尋找資源的相關明細
- 樣本控制結果
- 篩選、排序和下載控制項發現項目
- 對控制發現採取行動

檢視控制項搜尋與尋找資源的相關明細

AWS Security Hub 提供每個控制項發現項目的下列詳細資訊，以協助您進行調查：

- 使用者對發現項目所做的變更歷史記錄
- 用於發現的.json文件
- 與發現項目相關之資源的相關資訊
- 與發現項目相關的組態規則
- 使用者已新增至尋找項目的注意事項

下一節將說明如何存取這些詳細資料。

尋找歷史

尋找歷程記錄是一項 Security Hub 功能，可讓您追蹤過去 90 天內對發現項目所做的變更。

尋找歷史記錄可用於控制項發現項目和其他 Security Hub 發現項目。如需詳細資訊，請參閱 尋找歷史。

檢視完整的 .json 以尋找發現項目

您可以顯示並下載完整.json的發現項目。

若要顯示.json，請在尋找 .json 欄中，選擇圖示。

在「尋找 JSON」面板上，若要下載.json，請選擇「下載」。

檢視尋找項目資源的相關資訊

[資源] 欄包含資源類型和資源識別碼。

若要顯示有關資源的資訊，請選擇資源識別碼。對於 AWS 帳戶，如果帳戶是組織成員帳戶，則資訊會同時包含帳戶 ID 和帳戶名稱。對於手動邀請的帳戶，資訊僅包含帳戶 ID。

如果您有權檢視其原始服務中的資源，則資源識別碼會顯示服務的連結。例如，對於 AWS 使用者，資源詳細資料會提供檢視 IAM 中使用者詳細資料的連結。

如果資源位於不同的帳戶中，Security Hub 會顯示訊息通知您。

檢視搜尋結果資源的組態時間表

調查的其中一個途徑是中資源的配置時間表 AWS Config。

如果您有檢視發現項目資源之組態時間表的權限，則尋找項目清單會提供時間表的連結。

如果資源位於不同的帳戶中，Security Hub 會顯示訊息通知您。

若要導覽至中的組態時間表 AWS Config

1. 在「調查」欄中，選擇圖示。
2. 在功能表上，選擇 [設定時間軸]。如果您沒有組態時間表的存取權，則不會顯示連結。

檢視尋找項目資源的 AWS Config 規則

如果控制項以 AWS Config 規則為基礎，則您可能也想要檢視 AWS Config 規則的詳細資料。 AWS Config 規則資訊可協助您更好地瞭解檢查為何通過或失敗。

如果您有檢視控制 AWS Config 項規則的權限，則發現項目清單會提供中 AWS Config 規則的連結 AWS Config。

如果資源位於不同的帳戶中，Security Hub 會顯示訊息通知您。

若要導覽至規 AWS Config 則

1. 在「調查」欄中，選擇圖示。
2. 在功能表上，選擇 [Config 規則]。如果您沒有規則的存取權， AWS Config 則不會連結 Config 規則。

檢視發現項目的備註

如果發現項目具有相關聯的註記，則「已更新」欄會顯示附註圖示。

若要顯示與發現項目相關聯的備註，請執行下列

在「已更新」欄中，選擇附註圖示。

樣本控制結果

控制項發現項目的格式會根據您是否已開啟合併的控制項發現項目而有所不同。當您開啟此功能時，Security Hub 會產生控制項檢查的單一尋找項目，即使該控制項套用至多個已啟用的標準也是如此。如需詳細資訊，請參閱 合併控制項結果。

下一節顯示範例控制項發現項目。其中包括帳戶中關閉合併控制項發現項目時，來自每個 Security Hub 標準的發現項目，以及在開啟時跨標準尋找控制項範例。

> **Note**
>
> 發現結果將參考「中國地 AWS GovCloud (US) 區」和「區域」中的不同欄位和值。如需詳細資訊，請參閱 合併對 ASFF 欄位與值的影響。

已關閉合併的控制項發現項目

- AWS 基礎安全性最佳作法 (FSBP) 標準的搜尋範例
- 互聯網安全中心（CIS） AWS 基準基準 v1.2.0 的樣本發現
- 互聯網安全中心（CIS） AWS 基準基準 v1.4.0 的樣本發現
- 美國國家標準與技術研究所 (NIST) SP 800-53 版本 5 的樣本搜尋結果

- 支付卡產業資料安全標準 (PCI DSS) 的搜尋範例
- 服務管理標準的搜尋範例： AWS Control Tower

已開啟合併的控制項發現

- 跨標準尋找範例

關於 FSBP 的樣本發現


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
```

```
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
```

```
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

獨聯體 AWS 基準基準 v1.2.0 的樣本發現

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
```

```
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

獨聯體 AWS 基準基準 v1.4.0 的樣本發現

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
```

```
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
```

```
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

搜尋結果樣本

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
```

```
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
```

```
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

PCI DSS 的搜尋範例

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
```

```
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
```

```
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

服務管理標準的搜尋範例： AWS Control Tower

> **Note**
>
> 只有當您是在中建立標準的 AWS Control Tower 使用者時，才能使用此標準 AWS Control Tower。如需詳細資訊，請參閱 服務管理標準： AWS Control Tower。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
```

```
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "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/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
```

```
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

跨標準搜尋範例 (開啟合併控制項結果時)

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
```

```
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
```

```
        { "StandardsId": "standards/pci-dss/v/3.2.1"},
        { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
        { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
        { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

篩選、排序和下載控制項發現項目

您可以使用篩選索引標籤，根據符合性狀態來篩選控制項發現項目清單。您也可以根據其他發現項目欄位值來篩選清單，並從清單中下載發現項目。

篩選和排序控制項尋找清單

[全部檢查] 索引標籤會列出工作流程狀態為NEW、NOTIFIED或的所有使用中發現項目RESOLVED。依預設，會排序清單，使失敗的發現項目位於清單的頂端。此排序順序可協助您排定需要解決的發現項目的優先順序。

[失敗]、[未知] 和 [通過] 索引標籤上的清單會根據的值進行篩選Compliance.Status。這些清單也只包含工作流程狀態為NEW、NOTIFIED或的使用中發現項目RESOLVED。

[隱藏] 索引標籤包含工作流程狀態為的作用中發現項目清單SUPPRESSED。

除了每個索引標籤上的內建篩選器之外，您還可以使用下列欄位中的值來篩選清單：

- 帳戶 ID
- 工作流程狀態

- 合規狀態
- 資源 ID
- 資源類型

您可以使用任何欄排序每個清單。

下載控制項發現清單

如果您導覽至「安全性標準」並選擇標準，您會看到該標準的控制項清單。從清單中選擇控制項會帶您前往控制項詳細資訊頁面，其中包含控制項的發現項目清單。從這裡，您可以將控制項發現項目下載至 .csv 檔案。

如果您篩選尋找項目清單，則下載項目只會包含符合篩選條件的控制項。

如果您從清單中選取特定的發現項目，則下載只會包含選取的發現項目。

若要下載發現項目，請選擇 [下載]。即會下載發現項目的目前頁面。

對控制發現採取行動

若要反映調查的目前狀態，您可以設定工作流程狀態。如需詳細資訊，請參閱 the section called “設定發現項目的工作流程狀態”。

在中 AWS Security Hub，您也可以將選定的發現項目傳送至 Amazon 中的自訂動作 EventBridge。如需更多詳細資訊，請參閱 the section called “將問題清單傳送至自訂動作”。

使用「摘要」控制面板

在 AWS Security Hub 主控台上，[摘要] 頁面上的儀表板可協助您識別AWS環境中存在安全性問題的區域，而不需要額外的分析工具或複雜的查詢。您可以自訂儀表板配置、新增或移除 Widget，以及篩選資料以將重點放在特定感興趣的區域。您也可以將篩選條件儲存為篩選器集，以便日後快速擷取特定類型 future 資料。

如果您自訂儀表板或篩選資料，Security Hub 會自動儲存您的設定以供後續使用。此外，您的 Security Hub 帳戶的每個使用者都會獨立儲存這些設定。這表示不同的使用者可以為儀表板設定不同的配置、Widget 和篩選器集。

每次開啟 [摘要] 儀表板時，Security Hub 都會自動重新整理大多數儀表板資料。但是，某些數據的更新頻率較低。例如，安全分數和控制狀態每 24 小時更新一次。

如果您為 Security Hub 設定了跨區域彙總區域，則儀表板資料會包含彙總區域與所有連結區域的發現項目。如果您是組織委派的 Security Hub 系統管理員，資料會包含系統管理員帳戶和成員帳戶的發現項目。您可以選擇按帳戶過濾數據。如果您擁有成員帳戶或獨立帳戶，則資料僅包含您帳戶的發現項目。

摘要儀表板的可用小器具

摘要儀表板包含反映現代雲端安全威脅狀況的 Widget，並以AWS客戶的安全性作業和體驗為指導。某些小部件默認顯示，而其他小部件則不顯示。您可以透過新增或移除 Widget 來自訂儀表板檢視。

要添加它們，請選擇「摘要」頁面右上角的「添加小工具」。在搜尋列中，輸入小工具的標題。將小器具拖放到儀表板上。

窗口小部件默認顯示

依預設，「摘要」控制面板包含下列 Widget：

安全標準

顯示您最近的摘要安全分數，以及每個 Security Hub 標準的安全分數。安全分數 (介於 0—100% 之間) 代表傳遞控制項相對於所有已啟用控制項的比例。如需這些分數的詳細資訊，請參閱安全分數的計算方式。此 Widget 可協助您瞭解整體安全性狀態。

發現數量最多的資產

提供發現項目最多的資源、帳戶和應用程式的概觀。清單會依發現項目的數目遞減順序排序。在 Widget 中，每個索引標籤都會顯示該類別中的前六個項目，並依嚴重性和資源類型分組。如果您在

「發現項目總數」欄中選擇數字，Security Hub 會開啟顯示資產發現項目的頁面。此 Widget 可協助您快速識別哪些核心資產具有潛在安全威脅。

依區域搜尋結果

顯示每AWS 區域個已啟用 Security Hub 的發現項目總數 (依嚴重性分組)。此 Widget 可協助您識別可能影響特定區域的安全性問題。如果您在彙總區域中開啟儀表板，此 Widget 可協助您監控每個連結區域中潛在的安全性問題。

最常見的威脅類型

提供您AWS環境中 10 種最常見威脅類型的明細資訊。這包括諸如權限提升、使用公開認證或與惡意 IP 位址通訊等威脅。

若要檢視此資料， GuardDuty必須啟用 Amazon。如果是，請在此 Widget 中選擇安全威脅類型，以開啟 GuardDuty 主控台並檢閱與此安全威脅相關的發現項目。此 Widget 可協助您評估其他安全性問題的潛在威脅。

具有漏洞利用的軟件漏洞

提供您AWS環境中存在且已知漏洞的軟體弱點摘要。您也可以檢閱有修正程式和沒有可用修正程式的弱點明細。

若要檢視此資料，必須啟用 Amazon Inspector 查器。如果是，請在此 Widget 中選擇一個統計資料以開啟 Amazon Inspector 主控台，並查看有關該弱點的更多詳細資訊。此 Widget 可協助您根據其他安全性問題評估軟體弱點。

隨時間推移的新發現

顯示過去 90 天內每日新發現項目數量的趨勢。您可以依嚴重性或提供者劃分資料，以取得其他內容。此小部件可幫助您了解在過去 90 天內發現數量是否在特定時間激增或下降。

發現數量最多的資源

提供產生最多發現項目的資源摘要，並依下列資源類型劃分：Amazon Simple Storage Service (Amazon S3) 儲存貯體、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和AWS Lambda 函數。

在 Widget 中，每個索引標籤都會著重於先前的其中一個資源類型，列出產生最多發現項目的 10 個資源執行個體。若要複查特定資源的發現項目，請選擇資源執行環境。此 Widget 可協助您分類與一般AWS資源相關聯的安全性發現項目。

窗口小部件默認隱藏

下列小器具也可用於「摘要」儀表板，但依預設會隱藏它們：

具有最多發現結果的 AMI

提供產生最多發現項目的 10 個 Amazon 機器映像 (AMI) 清單。只有在您的帳戶啟用 Amazon EC2 時，才能使用此資料。它可協助您識別哪些 AMI 構成潛在安全性風險。

調查結果最多的 IAM 主體

提供產生最多發現項目的 10 AWS Identity and Access Management (IAM) 使用者清單。此小工具可幫助您執行管理和計費任務。它會顯示哪些使用者對 Security Hub 使用的貢獻最多。

發現項目最多的帳戶 (依嚴重性)

顯示產生最多發現項目的 10 個帳戶的圖表，並依嚴重性分組。此 Widget 可協助您決定要將分析和修正工作集中在哪些帳戶上。

發現項目最多的帳號 (依資源類型)

顯示產生最多發現項目的 10 個帳號圖表，並依資源類型分組。此 Widget 可協助您判斷哪些帳號和資源類型要排定優先順序，以便進行分析和修正。

洞察

列出五個 Security Hub 受管理的見解，以及它們產生的發現項目數目。深入分析可識別需要注意的特定安全性區域。

來自AWS整合的最新發現

顯示您從整合式安全中心收到的發現項目數目AWS 服務。它也會顯示您最近收到每個整合服務發現的時間。此 Widget 會提供來自多個合併的發現項目資料AWS 服務。若要深入研究，請選擇整合式服務。Security Hub 接著會開啟該服務的主控台。

篩選「摘要」儀表板

若要組織「摘要」控制面板上的資料，並僅包含與您最相關的安全性資料，您可以篩選儀表板。例如，如果您是應用程式團隊的成員，您可以在生產環境中為關鍵應用程式建立專用檢視。如果您是安全團隊的成員，則可以建立專用檢視，協助您專注於高嚴重性的發現項目。若要篩選「摘要」控制面板上的資料，請在儀表板上方的篩選方塊中輸入篩選條件。如果您套用篩選準則，則條件會套用至儀表板上的所有資料，但「見解」和「安全性」標準 Widget 中的資料除外。

您可以使用下列欄位來篩選資料：

- 帳戶名稱
- 帳戶 ID
- 應用程式 Amazon 資源名稱 (ARN)
- 應用程式名稱
- 產品名稱 (適用於將發現項目傳送至 Security Hub 的AWS 服務或協力廠商產品)
- 記錄狀態
- 區域
- 資源標籤
- 嚴重性
- 工作流程狀態

依預設，儀表板資料會使用下列條件篩選：`Workflow status`is `NOTIFIED` 或`NEW`、AND `Record state` 為`ACTIVE`。這些準則顯示在儀表板上方，篩選器方塊下方。若要移除這些條件，請在篩選器 Token 中為您要移除的條件選擇 X。

如果您套用要再次使用的篩選條件，您可以將其儲存為篩選器集。篩選器集是您建立並儲存的一組篩選條件，以便在您在「摘要」控制面板上檢閱資料時重新套用。

> **Note**
>
> 下列欄位無法儲存為篩選器集的一部分：應用程式 ARN、應用程式名稱和資源標籤。

建立和儲存篩選器集

請依照下列步驟建立並儲存篩選集。

建立和儲存篩選集的步驟

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇摘要。
3. 在「摘要」控制面板上方的篩選器方塊中，輸入篩選器集的篩選條件。
4. 在 [清除篩選器] 功能表上，選擇 [儲存新篩選器集]。

5. 在「儲存篩選集」對話方塊中，輸入篩選集的名稱。
6. (選擇性) 若要在每次開啟「摘要」頁面時使用預設的篩選器集，請選取該選項以將其設定為預設檢視。
7. 選擇儲存。

若要在您已建立和儲存的篩選器集之間切換，請使用「摘要」控制面板上方的 「選擇篩選器集」選單。當您選取篩選器集時，Security Hub 會將篩選器集的準則套用至儀表板上的資料。

更新或刪除過濾器集

請遵循下列步驟來更新或刪除現有的篩選器集。如果您刪除目前設定為 [摘要] 儀表板預設檢視的篩選器集，則預設檢視會重設為預設的 Security Hub 檢視。

更新或刪除篩選器集

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇摘要。
3. 在「摘要」頁面上方的 「選擇過濾器集」選單中，選擇過濾器集。
4. 在 [清除篩選器] 功能表上，執行下列其中一個動作：
   - 若要更新過濾器集，請選擇「更新目前的過濾器集」。然後，在出現的對話方塊中輸入您的變更。
   - 若要刪除過濾器集，請選擇刪除目前的過濾器集。然後，在出現的對話方塊中選擇「刪除」。

自訂摘要控制面板

您可以透過多種方式自訂「摘要」控制面板。您可以從儀表板中新增和移除 Widget。您也可以重新排列儀表板上的 Widget 並調整其大小。

如果您自訂儀表板，Security Hub 會立即套用您的變更，並儲存新的儀表板設定。您的變更會套用至您在所有瀏覽器AWS 區域和瀏覽器中的儀表板檢視。

若要自訂摘要控制面板

1. 開啟AWS安全中心主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格中，選擇摘要。
3. 執行下列任何一項：

- 若要新增小工具，請選擇頁面右上角的「新增小工具」。在搜尋列中，輸入要新增的小工具標題。然後，將小工具拖曳至您想要的位置。
- 若要移除小工具，請選擇 Widget 右上角的三個點。
- 若要移動 Widget，請選擇 Widget 左上角的控點，然後將 Widget 拖曳至您想要的位置。
- 若要變更 Widget 的大小，請選擇 Widget 右下角的調整大小控點。拖移小工具的邊緣，直到小工具成為您偏好的大小。

若要隨後還原原始設定，請選擇頁面頂端的 [重設為預設版面配置]。

建立 Security Hub 資源 AWS CloudFormation

AWS Security Hub 與整合 AWS CloudFormation，這項服務可協助您建立資源模型並設定資 AWS 源，以減少建立和管理資源和基礎架構的時間。您可以建立描述所需的所有 AWS 資源 (例如自動化規則) 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 Security Hub 資源。描述您的資源一次，然後在多個區域中一遍又一遍地佈建相同 AWS 帳戶 的資源。

Security Hub 和 AWS CloudFormation 範本

若要佈建和設定 Security Hub 及相關服務的資源，您必須瞭解AWS CloudFormation 範本的運作方式。範本是 JSON 或 YAML 格式的文字檔案。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 設計師協助您開始 AWS CloudFormation 使用範本。如需詳細資訊，請參閱什麼是 AWS CloudFormation 設計師？ 在《AWS CloudFormation 使用者指南》中。

您可以為下列 Security Hub 資源類型建立 AWS CloudFormation 範本：

- 啟用 Security Hub
- 指定組織的委派 Security Hub 管理員
- 啟用安全標準
- 建立自訂分析
- 建立自動化規則
- 訂閱第三方產品整合

如需詳細資訊，包括資源的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation 使用者指南中的AWS Security Hub 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

使用 Amazon 簡易通知服務訂閱 Security Hub 公告

本節提供使用 Amazon Simple Notification Service (Amazon SNS) 訂閱 AWS Security Hub 公告的相關資訊，以接收有關 Security Hub 的通知。

訂閱後，您將收到有關以下事件的通知（請注意每個事件`AnnouncementType`的相應事件）：

- `GENERAL`— 有關 Security Hub 服務的一般通知。
- `UPCOMING_STANDARDS_CONTROLS`— 指定的 Security Hub 控制項或標準即將推出。這種類型的公告可協助您在發行版本之前準備回應和補救工作流程。
- `NEW_REGIONS`— 對 Security Hub 的 Support 是在一個新的AWS 區域.
- `NEW_STANDARDS_CONTROLS`— 新增 Security Hub 控制項或標準。
- `UPDATED_STANDARDS_CONTROLS`— 現有的 Security Hub 控制項或標準已更新。
- `RETIRED_STANDARDS_CONTROLS`— 現有的 Security Hub 控制項或標準已淘汰。
- `UPDATED_ASFF`— 已更新AWS安全性發現格式 (ASFF) 語法、欄位或值。
- `NEW_INTEGRATION`— 提供與其他AWS服務或第三方產品的新集成。
- `NEW_FEATURE`— 提供新的 Security Hub 功能。
- `UPDATED_FEATURE`— 現有的 Security Hub 功能已更新。

所有 Amazon SNS 所支援格式的通知。您可以在所有 Security Hub 提供的資訊安全AWS 區域中心中訂閱安全性中樞通告。

使用者必須擁有訂閱 Amazon SNS 主題的`Subscribe`權限。您可以使用 Amazon SNS 政策、IAM 政策或兩者兼而有之。如需詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的 IAM 和 Amazon SNS 政策。

> **Note**
>
> Security Hub 會將有關 Security Hub 服務更新的 Amazon SNS 公告傳送給任何訂閱AWS帳戶。若要接收有關 Security Hub 發現的通知，請參閱檢視尋找項目清單與詳細資訊 AWS Security Hub。

您可以訂閱 Amazon SNS 主題的亞馬遜簡單佇列服務 (Amazon SQS) 佇列，但必須使用位於同一區域的 Amazon SNS 主題亞馬遜資源名稱 (ARN)。如需詳細資訊，請參閱 Amazon 簡單佇列服務開發人員指南中的教學：訂閱 Amazon SQS 佇列至 Amazon SNS 主題。

您也可以使用AWS Lambda函數在收到通知時叫用事件。如需詳細資訊，包括函數程式碼範例，請參閱AWS Lambda開發人員指南中的教學課程：AWS Lambda搭配 Amazon 簡單通知服務使用。

每個區域的 Amazon SNS 主題 ARN 如下。

AWS 區域	Amazon SNS 主題 ARN
美國東部 (俄亥俄)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
美國東部 (維吉尼亞北部)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
美國西部 (加利佛尼亞北部)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
美國西部 (奧勒岡)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
非洲 (開普敦)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
亞太區域 (香港)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
亞太區域 (海德拉巴)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`

AWS 區域	Amazon SNS 主題 ARN
亞太區域 (雅加達)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
亞太區域 (孟買)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
亞太區域 (大阪)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
亞太區域 (首爾)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
亞太區域 (新加坡)	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
亞太區域 (雪梨)	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
亞太區域 (東京)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
加拿大 (中部)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中國 (北京)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements

AWS 區域	Amazon SNS 主題 ARN
中國 (寧夏)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
歐洲 (法蘭克福)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
歐洲 (愛爾蘭)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
歐洲 (倫敦)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
歐洲 (米蘭)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
Europe (Paris)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
歐洲 (西班牙)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
歐洲 (斯德哥爾摩)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
歐洲 (蘇黎世)	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements

AWS 區域	Amazon SNS 主題 ARN
以色列 (特拉維夫)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Middle East (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
中東 (阿拉伯聯合大公國)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
南美洲 (聖保羅)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (美國東部)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (美國西部)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

分割區內各個區域的訊息通常相同，因此您可以訂閱每個分割區中的一個區域，以接收影響該分割區中所有區域的通告。與成員帳戶相關聯的通告不會在管理員帳戶中複製。因此，每個帳戶（包括管理員帳戶）只會有每個公告的一份副本。您可以決定要使用哪個帳戶來訂閱 Security Hub 通告。

如需訂閱 Security Hub 公告成本的相關資訊，請參閱 Amazon SNS 定價。

訂閱 Security Hub 通告 (主控台)

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在 [地區] 清單中，選擇您要訂閱 Security Hub 通告的 [區域]。此範例使用 `us-west-2` 區域。
3. 在導覽窗格中選擇 Subscriptions (訂閱)，然後選擇 Create subscription (建立訂閱)。

4. 在主題 ARN 框中輸入主題 ARN。例如 `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`。
5. 在 [通訊協定] 中，選擇您要接收 Security Hub 通告的方式。如果您選擇「電子郵件」，請在 Endpoint 中輸入您要用來接收通知的電子郵件地址。
6. 選擇建立訂閱。
7. 確認訂閱。例如，如果您選擇電子郵件通訊協定，Amazon SNS 會傳送訂閱確認訊息到您提供的電子郵件。

訂閱 Security Hub 通告 () AWS CLI

1. 執行以下命令：

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. 確認訂閱。例如，如果您選擇電子郵件通訊協定，Amazon SNS 會傳送訂閱確認訊息到您提供的電子郵件。

Amazon SNS 訊息格式

下列範例顯示 Amazon SNS 發出有關引入新安全控制的安全 Security Hub 公告。訊息內容會根據公告類型而有所不同，但所有公告類型的格式都相同。您也可以選擇包含提供有關公告詳細資訊的`Link`欄位。

範例：新控制項的 Security Hub 公告 (電子郵件通訊協定)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
```

```
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

範例：新控制項的 Security Hub 公告 (電子郵件 JSON 通訊協定)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
```

```
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

AWS Security Hub 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端內部的安全：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要進一步瞭解適用於 AWS Security Hub 的合規計劃，請參閱 合規計劃範圍內的 AWS 服務。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的請求和適用法律和法規。

本文件可協助您瞭解如何在使用 Security Hub 時套用共同的責任模型。下列主題說明如何設定 Security Hub 以符合您的安全性和合規性目標。您也會學到如何使用其他可AWS協助您監控和保護 Security Hub 資源的服務。

主題

- AWS Security Hub 中的資料保護
- AWS的 Identity and Access Management AWS Security Hub
- AWS Security Hub 的合規驗證
- AWS安全中心的彈性
- AWS Security Hub 中的基礎設施安全
- AWS Security Hub 和介面 VPC 端點 (AWS PrivateLink)

AWS Security Hub 中的資料保護

AWS 共同的責任模型適用於 AWS Security Hub 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。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 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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 AWS 時，需要 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 Name (名稱) 欄位。這包括當您使用 Security Hub 或其他AWS 服務使用主控台AWS CLI、API 或 AWS SDK 時。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。

Security Hub 是多租戶服務供應項目。為了確保資料保護，Security Hub 會加密元件服務之間的靜態資料和傳輸中的資料。

AWS的 Identity and Access Management AWS Security Hub

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權。IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Security Hub 資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- AWS Security Hub 搭配 IAM 的運作方式
- Security Hub 的身分識別型原則範例
- Security Hub 的服務連結角色

- AWSAWS Security Hub 的受管理原則
- 對 AWS Security Hub 身分與存取進行疑難排解

物件

您使用 AWS Identity and Access Management (IAM) 的方式會因您在安全中心中執行的工作而有所不同。

服務使用者 — 如果您使用 Security Hub 服務執行工作，則系統管理員會為您提供所需的認證和權限。當您使用更多 Security Hub 功能來完成工作時，您可能需要額外的權限。瞭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。如果您無法存取資訊安全中心中的功能，請參閱對 AWS Security Hub 身分與存取進行疑難排解。

服務管理員 — 如果您負責公司的安全中心資源，您可能擁有 Security Hub 的完整存取權。決定您的服務使用者應該存取哪些 Security Hub 功能和資源是您的工作。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。若要進一步了解貴公司如何搭配 Security Hub 使用 IAM，請參閱AWS Security Hub 搭配 IAM 的運作方式。

IAM 管理員 — 如果您是 IAM 管理員，可能需要瞭解如何撰寫政策以管理 Security Hub 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Security Hub 身分型政策範例，請參閱。Security Hub 的身分識別型原則範例

使用身分驗證

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證 (登入至 AWS)。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證都是聯合身分的範例。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。您 AWS 藉由使用聯合進行存取時，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。如需有關登入至 AWS 的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。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) 以提高帳戶的安全。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

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。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

最佳實務是要求人類使用者 (包括需要管理員存取權的使用者)搭配身分提供者使用聯合功能，使用暫時憑證來存取 AWS 服務。

聯合身分是來自您企業使用者目錄的使用者、Web 身分供應商、AWS Directory Service、Identity Center 目錄或透過身分來源提供的憑證來存取 AWS 服務 的任何使用者。聯合身分存取 AWS 帳戶時，會擔任角色，並由角色提供暫時憑證。

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來源中的一組使用者和群組，以便在您的所有 AWS 帳戶和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 AWS 帳戶 中的一種身分，具備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。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials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。您無法以群組身分登入。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過程變得更為容易。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 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。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，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。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。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人)存取您帳戶中的資源。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色作為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。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。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。只有在服務收到需要與其他 AWS 服務 或資源互動才能完成的請求之後，才會提出 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》。
  - 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 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 帳戶 中，並由該服務所擁有。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 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到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

您可以透過建立政策並將其附加到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體 (使用者、根使用者或角色工作階段)發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式儲存在 AWS 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。若要授與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。具備該政策的使用者便可以從 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。受管政策則是獨立的政策，您可以將這些政策附加到 AWS 帳戶 中的多個使用者、群組和角色。受管政

策包含 AWS 管理政策和客戶管理政策。如需瞭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。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。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 Simple Storage Service (Amazon S3)、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。若要進一步了解 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 支援其他較少見的政策類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可範圍。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 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 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需組織和 SCP 的更多相關資訊，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。如需更多資訊，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。若要了解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS Security Hub 搭配 IAM 的運作方式

在您用AWS Identity and Access Management來管理 Security Hub 的存取權限之前，請先了解哪些 IAM 功能可與 Security Hub 搭配使用。

您可以與 Amazon Macie 一起使用的 IAM 功能

IAM 功能	馬西支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	是
存取控制清單 (ACL)	否
以屬性為基礎的存取控制 (ABAC) — 策略中的標籤	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

有關 Security Hub 和其他如何使AWS 服務用大多數 IAM 功能的高級視圖 AWS 服務，請參閱 IAM 使用者指南中的 IAM。

Security Hub 的身分識別型原則

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。若要瞭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，因為這會套用至附加的使用者或角色。如要瞭解您在 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。

Security Hub 支援身分識別型原則。如需詳細資訊，請參閱 Security Hub 的身分識別型原則範例。

以資源 = 為基礎的安全性中樞原則

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。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。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

若要啟用跨帳戶存取權，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。當主體和資源在不同的 AWS 帳戶 中時，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) 存取資源的許可。其透過將身分型政策附加到實體來授予許可。不過，如果資源型政策會為相同帳戶中的主體授與存取，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 角色與資源型政策有何差異。

Security Hub 不支援以資源為基礎的原則。您無法將 IAM 政策直接附加到 Security Hub 資源。

Security Hub 的原則動作

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。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

Security Hub 中的原則動作會在動作之前使用下列前置詞：

```
securityhub:
```

例如，若要授與使用者啟用 Security Hub 的權限，這是與 Security Hub API `EnableSecurityHub` 作業相對應的動作，請在其原則中包含`securityhub:EnableSecurityHub`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Security Hub 會定義它自己的一組動作，說明您可以使用此服務執行的工作。

```
"Action": "securityhub:EnableSecurityHub"
```

如需在單一陳述式中指定多個動作，請用逗號分隔。例如：

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

您也可以使用萬用字元 (*) 指定多個動作。例如，若要指定開頭是 `Get` 文字的所有動作，請包含以下動作：

```
"Action": "securityhub:Get*"
```

但是，根據最佳實務，您應該定義遵循「最低權限」原則的政策。換句話說，您應建立其中只包含執行特定任務所需許可的政策。

使用者必須具有DescribeStandardsControl作業的存取權BatchGetSecurityControls，才能存取BatchGetStandardsControlAssociations、和ListStandardsControlAssociations。

使用者必須具有UpdateStandardsControls作業的存取權，才能存取BatchUpdateStandardsControlAssociations、和UpdateSecurityControl。

如需 Security Hub 動作的清單，請參閱服務授權參考AWS Security Hub中所定義的動作。如需指定 Security Hub 動作的原則範例，請參閱Security Hub 的身分識別型原則範例。

資源

支援政策資源	否

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 (例如列出作業)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

Security Hub 定義以下資源類型：

- Hub (樞紐)
- 產品
- 尋找聚合器，也稱為跨區域彙總器
- 自動化規則
- 配置策略

您可以使用 ARN 在策略中指定這些類型的資源。

如需 Security Hub 資源類型和每個資源類型的 ARN 語法清單，請參閱服務授權參考AWS Security Hub中所定義的資源類型。若要瞭解您可以針對每種資源類型指定哪些動作，請參閱服務授權參考

AWS Security Hub中所定義的動作。如需指定資源的策略範例，請參閱Security Hub 的身分識別型原則範例。

Security Hub 的原則條件金鑰

支援服務特定政策條件索引鍵	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。

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。若您為單一條件索引鍵指定多個值，AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才會授與陳述式的許可。

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 IAM 使用者名稱標記時，將存取資源的許可授與該 IAM 使用者。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定的條件索引鍵。若要查看 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 AWS 全域條件內容索引鍵。

如需 Security Hub 條件金鑰的清單，請參閱服務授權參考AWS Security Hub中的條件金鑰。若要瞭解可將條件索引鍵與哪些動作和資源搭配使用，請參閱由定義的動作AWS Security Hub。如需使用條件索引鍵的原則範例，請參閱Security Hub 的身分識別型原則範例。

安全中心中的存取控制清單 (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。

Security Hub 不支援 ACL，這表示您無法將 ACL 附加至 Security Hub 資源。

以屬性為基礎的存取控制 (ABAC) 搭配 Security Hub

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 AWS 中，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)，以及許多 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。

若要根據標籤控制存取，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索引鍵，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索引鍵，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)。

您可以將標籤附加到 Security Hub 資源。您也可以透過在策略的`Condition`元素中提供標籤資訊來控制對資源的存取。

如需標記 Security Hub 資源的相關資訊，請參閱標記 AWS Security Hub 資源。如需根據標籤控制資源存取的身分型原則範例，請參閱。Security Hub 的身分識別型原則範例

使用 Security Hub 的臨時登入資料

支援臨時憑證	是

您使用臨時憑證進行登入時，某些 AWS 服務 無法運作。如需詳細資訊，包括那些 AWS 服務 搭配臨時憑證運作，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

如果您使用使用者名稱和密碼之外的任何方法登入 AWS Management Console，則您正在使用臨時憑證。例如，當您使用公司的單一登入(SSO)連結存取 AWS 時，該程序會自動建立臨時憑證。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)。

您可使用 AWS CLI 或 AWS API，手動建立臨時憑證。接著，您可以使用這些臨時憑證來存取 AWS。AWS 建議您動態產生臨時憑證，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或等 AWS STS API 作業來取得臨時安全登入資料GetFederationToken。

Security Hub 支援使用臨時登入資料。

Security Hub 的轉寄存取工作階段

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在 AWS 中執行動作時，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 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。只有在服務收到需要與其他 AWS 服務 或資源互動才能完成的請求之後，才會提出 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》。

例如，AWS 服務當您整合安全中心，Organizations AWS Organizations 及當您指定組織中組織的委派 Security Hub 系統管理員帳戶時，Security Hub 會向下游發出 FAS 要求。

對於其他工作，Security Hub 會使用服務連結角色代表您執行動作。如需有關此角色的詳細資訊，請參閱

AWS Security Hub使用名`AWSServiceRoleForSecurityHub`為的 AWS Identity and Access Management (IAM) 服務連結角色。此服務連結角色是直接連結至 Security Hub 的 IAM 角色。它是由 Security Hub 預先定義的，它包括 Security Hub 呼叫其他AWS 服務並代表您監視AWS資源所需的所有權限。Security Hub 會在所有可用的安全中心使用此服務連結的角色。AWS 區域

服務連結角色可讓您輕鬆設定 Security Hub，因為您不需要手動新增必要的權限。資訊安全中心定義其服務連結角色的權限，除非權限另有定義，否則只有 Security Hub 可以擔任該角色。定義的許可包括信任政策和許可政策，而且您無法將該許可政策附加到任何其他 IAM 實體。

若要檢視服務連結角色的詳細資料，請在 Security Hub 主控台的 [設定] 頁面上，選擇 [一般]，然後選擇 [檢視服務權限]。

您只能刪除 Security Hub 服務連結的角色，只有在已啟用資訊安全中心的所有區域中第一次停用資訊安全中心後。這樣可以保護您的 Security Hub 資源，因為您無法不小心移除存取這些資源的權限。

如需其他支援服務連結角色之服AWS務的相關資訊，請參閱 IAM 使用者指南中的與 IAM 搭配使用的服務，並在服務連結角色欄中找出具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

主題

- Security Hub 的服務連結角色權限
- 建立 Security Hub 的服務連結角色
- 編輯 Security Hub 的服務連結角色
- 刪除 Security Hub 的服務連結角色

Security Hub 的服務連結角色權限

Security Hub 使用名為AWSServiceRoleForSecurityHub的服務連結角色。這是存取資源所需的AWS Security Hub服務連結角色。服務連結角色可讓 Security Hub 接收來自其他人的發現項目，AWS服務並設定必要的AWS Config基礎結構以執行控制項的安全性檢查。

AWSServiceRoleForSecurityHub 服務連結角色信任下列服務以擔任角色：

- securityhub.amazonaws.com

AWSServiceRoleForSecurityHub 服務連結角色使用受管政策AWSSecurityHubServiceRolePolicy。

您必須授與權限，才能允許 IAM 身分 (例如角色、群組或使用者) 建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForSecurityHub服務連結角色，您用來存取 Security Hub 的 IAM 身分必須具有必要的權限。若要授與必要權限，請將下列原則附加至角色、群組或使用者。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

建立 Security Hub 的服務連結角色

當您第一次啟用 Security Hub，或在先前未啟用的支援區域中啟用 Security Hub 時，會自動建立AWSServiceRoleForSecurityHub服務連結角色。您也可以使用 IAM 主控台、IAM CLI 或 IAM API 來手動建立 AWSServiceRoleForSecurityHub 服務連結角色。

> **Important**
>
> 針對 Security Hub 系統管理員帳戶建立的服務連結角色不適用於 Security Hub 成員帳戶。

如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的建立服務連結角色。

編輯 Security Hub 的服務連結角色

Security Hub 不允許您編輯AWSServiceRoleForSecurityHub服務連結的角色。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。

刪除 Security Hub 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。這樣就不會有未積極監控或維護的未使用實體。

> **Important**
>
> 若要刪除AWSServiceRoleForSecurityHub服務連結角色，您必須先停用所有已啟用資訊安全中心的區域中的資訊安全中心。

當您停用 Security Hub 時，不會自動刪除AWSServiceRoleForSecurityHub服務連結的角色。如果您再次啟用 Security Hub，它會開始使用現有的AWSServiceRoleForSecurityHub服務連結角色。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForSecurityHub 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

。

Security Hub 的服務角色

Security Hub 不會假設或使用服務角色。若要代表您執行動作，Security Hub 會使用服務連結的角色。如需有關此角色的詳細資訊，請參閱Security Hub 的服務連結角色。

> **Warning**
>
> 變更服務角色的權限可能會在您使用 Security Hub 時造成作業上的問題。只有當 Security Hub 提供指引時，才編輯服務角色。

Security Hub 的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 帳戶 中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Security Hub 使用服務連結的角色代表您執行動作。如需有關此角色的詳細資訊，請參閱Security Hub 的服務連結角色。

Security Hub 的身分識別型原則範例

根據預設，使用者和角色沒有建立或修改 Security Hub 資源的權限。他們也無法使用 AWS Management Console、AWS CLI 或 AWS API 執行任務。管理員必須建立 IAM 政策，授與使用者和角色在指定資源上執行特定 API 操作所需的許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要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》中的在 JSON 索引標籤上建立政策。

主題

- 政策最佳實務
- 使用安全中心主控台
- 範例：允許使用者檢視他們自己的許可
- 範例：允許使用者建立和管理組態原則
- 範例：允許使用者檢視發現項目
- 範例：允許使用者建立和管理自動化規則

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以建立、存取或刪除您帳戶中的 Security Hub 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 受管政策並朝向最低權限許可的目標邁進：如需開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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予對服務動作的存取權，前提是透過特定 AWS 服務 (例如 AWS CloudFormation)使用條件。如需更多資訊，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。
- 需要多重要素驗證 (MFA)：如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。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。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

使用安全中心主控台

若要存取 AWS Security Hub 主控台，您必須擁有最低的一組許可。這些權限必須允許您列出和檢視有關AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許其最基本主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保這些使用者和角色可以使用 Security Hub 主控台，請同時將下列AWS受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

範例：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。此政策包含在主控台上，或是使用 AWS CLI 或 AWS API 透過編寫程式的方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "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": "*"
        }
    ]
}
```

範例：允許使用者建立和管理組態原則

此範例顯示如何建立 IAM 政策，以允許使用者建立、檢視、更新和刪除組態政策。此範例原則也可讓使用者啟動、停止及檢視原則關聯。若要讓此 IAM 政策運作，使用者必須是組織的委派 Security Hub 管理員。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

範例：允許使用者檢視發現項目

此範例顯示如何建立可讓使用者檢視 Security Hub 發現項目的 IAM 政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

範例：允許使用者建立和管理自動化規則

此範例顯示如何建立 IAM 政策，以允許使用者建立、檢視、更新和刪除 Security Hub 自動化規則。若要讓此 IAM 政策運作，使用者必須是 Security Hub 管理員。若要限制權限 (例如，允許使用者僅檢視自動化規則)，您可以移除建立、更新和刪除權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Security Hub 的服務連結角色

AWS Security Hub使用名`AWSServiceRoleForSecurityHub`為的 AWS Identity and Access Management (IAM) 服務連結角色。此服務連結角色是直接連結至 Security Hub 的 IAM 角色。它是由 Security Hub 預先定義的，它包括 Security Hub 呼叫其他AWS 服務並代表您監視AWS資源所需的所有權限。Security Hub 會在所有可用的安全中心使用此服務連結的角色。AWS 區域

服務連結角色可讓您輕鬆設定 Security Hub，因為您不需要手動新增必要的權限。資訊安全中心定義其服務連結角色的權限，除非權限另有定義，否則只有 Security Hub 可以擔任該角色。定義的許可包括信任政策和許可政策，而且您無法將該許可政策附加到任何其他 IAM 實體。

若要檢視服務連結角色的詳細資料，請在 Security Hub 主控台的 [設定] 頁面上，選擇 [一般]，然後選擇 [檢視服務權限]。

您只能刪除 Security Hub 服務連結的角色，只有在已啟用資訊安全中心的所有區域中第一次停用資訊安全中心後。這樣可以保護您的 Security Hub 資源，因為您無法不小心移除存取這些資源的權限。

如需其他支援服務連結角色之服AWS務的相關資訊，請參閱 IAM 使用者指南中的與 IAM 搭配使用的服務，並在服務連結角色欄中找出具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

主題

- Security Hub 的服務連結角色權限
- 建立 Security Hub 的服務連結角色
- 編輯 Security Hub 的服務連結角色

- 刪除 Security Hub 的服務連結角色

Security Hub 的服務連結角色權限

Security Hub 使用名為AWSServiceRoleForSecurityHub的服務連結角色。這是存取資源所需的AWS Security Hub服務連結角色。服務連結角色可讓 Security Hub 接收來自其他人的發現項目，AWS 服務並設定必要的AWS Config基礎結構以執行控制項的安全性檢查。

AWSServiceRoleForSecurityHub 服務連結角色信任下列服務以擔任角色：

- securityhub.amazonaws.com

AWSServiceRoleForSecurityHub 服務連結角色使用受管政策 AWSSecurityHubServiceRolePolicy。

您必須授與權限，才能允許 IAM 身分 (例如角色、群組或使用者) 建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForSecurityHub服務連結角色，您用來存取 Security Hub 的 IAM 身分必須具有必要的權限。若要授與必要權限，請將下列原則附加至角色、群組或使用者。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

建立 Security Hub 的服務連結角色

當您第一次啟用 Security Hub，或在先前未啟用的支援區域中啟用 Security Hub 時，會自動建立AWSServiceRoleForSecurityHub服務連結角色。您也可以使用 IAM 主控台、IAM CLI 或 IAM API 來手動建立 AWSServiceRoleForSecurityHub 服務連結角色。

> **Important**
>
> 針對 Security Hub 系統管理員帳戶建立的服務連結角色不適用於 Security Hub 成員帳戶。

如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的建立服務連結角色。

編輯 Security Hub 的服務連結角色

Security Hub 不允許您編輯AWSServiceRoleForSecurityHub服務連結的角色。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。

刪除 Security Hub 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。這樣就不會有未積極監控或維護的未使用實體。

> **Important**
>
> 若要刪除AWSServiceRoleForSecurityHub服務連結角色，您必須先停用所有已啟用資訊安全中心的區域中的資訊安全中心。
> 如果在嘗試刪除服務連結角色時未停用 Security Hub，則刪除會失敗。如需詳細資訊，請參閱停用 Security Hub。

當您停用 Security Hub 時，不會自動刪除AWSServiceRoleForSecurityHub服務連結的角色。如果您再次啟用 Security Hub，它會開始使用現有的AWSServiceRoleForSecurityHub服務連結角色。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForSecurityHub 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWSAWS Security Hub 的受管理原則

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。

AWS 受管理的策略：AWSSecurityHubFullAccess

您可將 `AWSSecurityHubFullAccess` 政策連接到 IAM 身分。

此原則會授與允許主體完整存取所有 Security Hub 動作的系統管理權限。必須先將此原則附加至主體，才能為其帳戶手動啟用 Security Hub。例如，具有這些權限的主參與者可以檢視及更新發現項目的狀態。他們可以配置自定義見解並啟用集成。它們可以啟用和停用標準和控制項。管理員帳戶的主參與者也可以管理成員帳戶。

許可詳細資訊

此政策包含以下許可。

- `securityhub`— 允許主參與者完整存取所有 Security Hub 動作。
- `guardduty`— 允許校長獲取有關 Amazon GuardDuty 帳戶狀態的信息。
- `iam`— 允許主參與者建立服務連結角色。
- `inspector`— 允許校長在 Amazon Inspector 中獲取有關帳戶狀態的信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
```

```
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus"
            ],
            "Resource": "*",
        }
    ]
}
```

Security Hub 受管理的策略：AWSSecurityHubReadOnlyAccess

您可將 AWSSecurityHubReadOnlyAccess 政策連接到 IAM 身分。

此原則會授與唯讀權限，讓使用者檢視 Security Hub 中的資訊。附加此原則的主參與者無法在安全性中心中進行任何更新。例如，具有這些權限的主參與者可以檢視與其帳戶相關聯的發現項目清單，但無法變更發現項目的狀態。他們可以檢視見解的結果，但無法建立或設定自訂見解。他們無法設定控制項或產品整合。

許可詳細資訊

此政策包含以下許可。

- securityhub— 允許使用者執行傳回項目清單或項目詳細資訊的動作。這包括以Get、List或開頭的 API 作業Describe。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSecurityHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "securityhub:Get*",
                "securityhub:List*",
                "securityhub:BatchGet*",
                "securityhub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略：AWSSecurityHubOrganizationsAccess

您可將 AWSSecurityHubOrganizationsAccess 政策連接到 IAM 身分。

此原則會授與中 AWS Organizations 支援 Security Hub 與 Organizations 整合所需的系統管理權限。

這些權限可讓組織管理帳戶指定 Security Hub 的委派系統管理員帳戶。它們也允許委派的 Security Hub 系統管理員帳戶啟用組織帳戶做為成員帳戶。

此原則僅提供組 Organizations 的權限。組織管理帳戶和委派的 Security Hub 系統管理員帳戶也需要安全性中心中相關動作的權限。您可以使用AWSSecurityHubFullAccess受管理的策略來授與這些權限。

許可詳細資訊

此政策包含以下許可。

- organizations:ListAccounts— 允許主參與者擷取屬於組織一部份的帳戶清單。
- organizations:DescribeOrganization— 允許主參與者擷取有關組織的資訊。
- organizations:ListRoots— 允許主參與者列出組織的根目錄。
- organizations:ListDelegatedAdministrators— 可讓主參與者列出組織的委派管理員。
- organizations:ListAWSServiceAccessForOrganization— 允許主參與者列出組織使用的 AWS 服務 項目。

- organizations:ListOrganizationalUnitsForParent— 允許主參與者列出父 OU 的子系組織單位 (OU)。
- organizations:ListAccountsForParent— 允許主參與者列出父 OU 的子項帳戶。
- organizations:DescribeAccount— 允許主參與者擷取組織中帳號的相關資訊。
- organizations:DescribeOrganizationalUnit— 允許主參與者擷取組織中 OU 的相關資訊。
- organizations:DescribeOrganization— 允許主參與者擷取有關組織組態的資訊。
- organizations:EnableAWSServiceAccess— 允許主參與者啟用與 Organizations 的 Security Hub 整合。
- organizations:RegisterDelegatedAdministrator— 允許主參與者指定 Security Hub 的委派系統管理員帳戶。
- organizations:DeregisterDelegatedAdministrator— 允許主參與者移除 Security Hub 的委派系統管理員帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS 受管理的策略：AWSSecurityHubServiceRolePolicy

您不得將 AWSSecurityHubServiceRolePolicy 連接到 IAM 實體。此原則會附加至服務連結角色，可讓 Security Hub 代表您執行動作。如需詳細資訊，請參閱 the section called “服務連結角色”。

此原則會授與允許服務連結角色對 Security Hub 控制項執行安全性檢查的系統管理權限。

許可詳細資訊

此政策包含執行以下動作的許可：

- cloudtrail— 檢索有關 CloudTrail 軌跡的信息。
- cloudwatch— 檢索當前 CloudWatch 警報。
- logs-檢索 CloudWatch 日誌的指標過濾器。
- sns— 擷取 SNS 主題的訂閱清單。
- config-檢索有關配置記錄器，資源和 AWS Config 規則的信息。也允許服務連結角色建立和刪除 AWS Config 規則，以及針對規則執行評估。
- iam— 獲取並生成帳戶的憑據報告。

- organizations— 擷取組織的帳戶和組織單位 (OU) 資訊。
- securityhub— 擷取有關如何設定 Security Hub 服務、標準和控制項的資訊。
- tag— 擷取有關資源標籤的資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
```

```
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
            }
        }
    ]
```

```
}
```

Security Hub 更新 AWS 受管理的策略

檢視有關 Security Hub AWS 受管理原則更新的詳細資料，因為這項服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Security Hub 文件歷程記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSSecurityHubReadOnlyAccess— 更新到現有策略	Security Hub 透過新增`Sid`欄位來更新此受管理的原則。	2024年2月22 日
AWSSecurityHubFullAccess— 更新到現有策略	Security Hub 更新了政策，因此它可以確定是否在帳戶中啟用 Amazon GuardDuty 和亞馬遜檢查器。這有助於客戶將來自多個安全性相關的資訊匯集在一起。 AWS 服務	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess— 更新到現有策略	Security Hub 更新了策略以授予其他權限，以允許對 AWS Organizations 委派的管理員功能進行只讀訪問。這包括根、組織單位 (OU)、帳戶、組織結構和服務存取等詳細資料。	2023 年 11 月 16 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 新增`BatchGetSecurityControls` `DisassociateFromAdministratorAccount` 、和`UpdateSecurityControl` 權限來讀取和更新可自訂的安全性控制內容。	2023 年 11 月 26 日

變更	描述	日期
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 新增了讀取與發現項目相關之資源標籤的 `tag:GetResources` 權限。	2023 年 11 月 7 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 已新增`BatchGetStandardsControlAssociations` 權限，以取得標準中控制項啟用狀態的相關資訊。	2023 年 9 月 27 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	安全中心添加了新的權限來獲取 AWS Organizations 數據以及讀取和更新 Security Hub 配置，包括標準和控制。	2023 年 9 月 20 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 將現有`config:DescribeConfigRuleEvaluationStatus` 權限移至原則中的不同陳述式。`config:DescribeConfigRuleEvaluationStatus` 權限現在已套用至所有資源。	2023 年 3 月 17 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 將現有`config:PutEvaluations` 權限移至原則中的不同陳述式。`config:PutEvaluations` 權限現在已套用至所有資源。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy – 更新現有政策	Security Hub 新增了新的權限，以允許服務連結角色將評估結果傳遞給。 AWS Config	2021 年 6 月 29 日

變更	描述	日期
AWSSecurityHubServiceRolePolicy— 已新增至受管理策略清單	已新增受管理原則的相關資訊 AWSSecurityHubServiceRolePolicy，此原則由 Security Hub 服務連結角色所使用。	2021 年 6 月 11 日
AWSSecurityHubOrganizationsAccess— 新政策	Security Hub 新增了一個新的原則，授與與 Organizations 整合 Security Hub 所需的權限。	2021 年 3 月 15 日
Security Hub 開始跟踪更改	Security Hub 開始跟踪其 AWS 託管策略的更改。	2021 年 3 月 15 日

對 AWS Security Hub 身分與存取進行疑難排解

使用下列資訊可協助您診斷和修正使用 Security Hub 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在安全中心執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想要以程式設計方式存取 Security Hub
- 我是系統管理員，想要允許其他人存取 Security Hub
- 我想允許我以外的人員存AWS 帳戶取我的 Security Hub 資源

我沒有在安全中心執行動作的授權

若 AWS Management Console 告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是為您提供登入憑證的人員。

當使用者`mateojackson`嘗試使用主控台來檢視 *`Widget`* 的詳細資料，但沒有`securityhub:`*`GetWidget`*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 securityhub:*GetWidget* 資源。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞至 Security Hub。

有些 AWS 服務 允許您傳遞現有的角色至該服務，而無須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。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Security Hub 中執行動作時，就會發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。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。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想要以程式設計方式存取 Security Hub

若使用者想要與 AWS Management Console 之外的 AWS 互動，則需要程式設計存取權。授予程式設計存取權的方式取決於存取 AWS 的使用者類型。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請依照您要使用的介面所提供的指示操作。

哪個使用者需要程式設計存取權？	到	By
		• 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 設定 AWS CLI 來使用 AWS IAM Identity Center。 • 關於 AWS SDKs、工具和 AWS APIs，請參閱 AWSSDKs 和工具參考指南 中的 IAM Identity Center 驗證。
IAM	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請遵循 IAM 使用者指南 中 使用臨時憑證搭配 AWS 資源 中的指示。
IAM	(不建議使用) 使用長期憑證簽署 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 使用 IAM 使用者憑證進行驗證。 • 關於 AWS SDKs 和工具，請參閱 AWSSDKs 和工具參考指南 中的 使用長期憑證進行驗證。 • 關於 AWS API，請參閱 IAM 使用者指南 中的 管理 IAM 使用者的存取金鑰。

我是系統管理員，想要允許其他人存取 Security Hub

若要提供存取權，請新增權限至您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立權限合集。請遵循 AWS IAM Identity Center 使用者指南 的 建立權限合集 中的指示。
- 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。請遵循 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。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示。
  - (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 新增權限至使用者 (主控台) 中的指示。

我想允許我以外的人員存AWS 帳戶取我的 Security Hub 資源

您可以建立一個角色，讓其他帳戶中的使用者或您的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：

- 若要瞭解 Security Hub 是否支援這些功能，請參閱AWS Security Hub 搭配 IAM 的運作方式。
- 如需了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 如需了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有的 AWS 帳戶。
- 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)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

AWS Security Hub 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 AWS Security Hub 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱合規計劃內的 AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱在 AWS Artifact 中下載報告。

使用 Security Hub 時，您的合規責任取決於資料的敏感度、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：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心基準環境的架構考量和步驟。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- AWS Config – 此 AWS 服務可評定資源組態與內部實務、業界準則和法規的合規狀態。
- AWS Security Hub：此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

AWS安全中心的彈性

AWS 全球基礎設施是以 AWS 區域 與可用區域為中心而建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。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、容錯能力和可擴展性能力，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 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

AWS Security Hub 中的基礎設施安全

作為一種受管服務，AWS Security Hub 受 AWS 全域網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS 架構良好的框架中的基礎設施保護。

您可以使用AWS已發佈的 API 呼叫，透過網路存取 Security Hub。用戶端必須支援下列項目：

- 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，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS Security Hub 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，以在您的 VPC 與 AWS Security Hub 間建立私有連線。介面端點採用這項技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或AWS直接連線的情況下，私密存取 Security Hub API。VPC 中的執行個體不需要公用 IP 位址即可與安全中心 API 通訊。您的 VPC 和安全中心之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個彈性網絡介面表示。

如需詳細資訊，請參閱AWS PrivateLink指南中的介面 VPC 端點 (AWS PrivateLink)。

安全中心 VPC 端點的考量

在為 Security Hub 設定介面虛擬私人雲端端點之前，請務必先檢閱AWS PrivateLink指南中的介面端點內容和限制。

安全中心支援從您的 VPC 呼叫其所有 API 動作。

> **Note**
>
> 安全中心不支援亞太區域 (大阪) 區域的 VPC 端點。

建立安全中心的介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為安全中樞服務建立 VPC 端點。如需詳細資訊，請參閱 《AWS PrivateLink 指南》中的建立介面端點。

使用下列服務名稱建立安全中心的 VPC 端點：

- com.amazonaws.*region*.securityhub

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 Security Hub 發出 API 要求，例如`securityhub.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱AWS PrivateLink南中的透過介面端點存取服務。

建立安全性中樞的 VPC 端點原則

您可以將端點策略附加到控制對 Security Hub 的存取權的 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AWS PrivateLink指南中的使用 VPC 端點控制對服務的存取。

範例：安全中樞動作的 VPC 端點原則

以下是安全性中樞端點原則的範例。連接至端點時，此原則會授與所有資源上所有主體列出之 Security Hub 動作的存取權。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。如需 VPC 共用的相關資訊，請參閱 Amazon VPC 使用者指南中的與其他帳戶共用您的 VPC。

記錄 AWS Security Hub API 呼叫 AWS CloudTrail

AWSSecurity Hub 與服務整合AWS CloudTrail，可提供安全中心中的使用者、角色或服務所採取的動作記錄的AWS服務。 CloudTrail 將 Security Hub 的 API 呼叫擷取為事件。擷取的呼叫包括來自 Security Hub 主控台的呼叫，以及對 Security Hub API 作業的程式碼呼叫。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 Security Hub 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 主控台上的最新事件。使用 CloudTrail 收集的資訊，您可以判斷向 Security Hub 發出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資料。

若要進一步了解 CloudTrail，包括如何設定和啟用它，請參閱AWS CloudTrail使用者指南。

安全中心資訊 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。當支援的事件活動發生在 Security Hub 中時，該活動會與 CloudTrail 事件歷史記錄中的其他AWS服務事件一起記錄在事件中。您可以檢視、搜尋和下載 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需帳戶中持續的事件記錄 (包括 Security Hub 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。根據預設，在主控台建立線索時，該線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他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 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

Security Hub 支援將所有安全中心 API 動作記錄為記 CloudTrail 錄檔中的事件。若要檢視 Security Hub 作業的清單，請參閱 Security Hub API 參考。

將下列動作的活動記錄到時 CloudTrail，的值會設定`responseElements`為`null`。這樣可確保敏感資訊不會包含在 CloudTrail 記錄中。

- `BatchImportFindings`

- GetFindings
- GetInsights
- GetMembers
- UpdateFindings

每一筆事件或日誌項目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：

- 該請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 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登入資料
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

範例：Security Hub 記錄檔項目

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CreateInsight動作的 CloudTrail 記錄項目。在本範例中，建立了名為 Test Insight 的洞見。此 ResourceId 屬性指定為 Group by (分組依據) 彙整工具，而且此洞見不指定任何選用篩選條件。如需洞見的詳細資訊，請參閱AWS安全中心的洞察。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

標記 AWS Security Hub 資源

標籤是可選的標籤，您可以定義並指派給AWS資源，包括特定類型的 AWS Security Hub 資源。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。例如，您可以使用標籤來區分資源、識別支援特定合規性需求或工作流程的資源，或分配成本。

您可以將標籤指派給下列類型的 Security Hub 資源：自動化規則、組態原則和Hub資源。

主題

- 標記基本面
- 在 IAM 政策中使用標籤
- 將標籤新增至 AWS Security Hub 資源
- 檢閱 AWS Security Hub 資源的標籤
- 編輯 AWS Security Hub 資源的標籤
- 從 AWS Security Hub 資源移除標籤

標記基本面

資源最多可以擁有 50 個標籤。每個標籤皆包含由您定義的必要「標籤金鑰」與選用「標籤值」。標籤關鍵字是一般標示，可做為更特定標籤值的品類。標籤值是標籤金鑰的描述項。

例如，如果您為不同的環境建立不同的自動化規則 (測試帳戶的一組自動化規則，另一組用於生產帳戶)，則可以為這些規則指派`Environment`標籤金鑰。關聯的標籤值可能`Test`適用於與測試帳戶相關聯的規則，以及`Prod`與生產帳戶和 OU 相關聯的規則。

當您定義和指派標籤給 AWS Security Hub 資源時，請記住下列事項：

- 每個資源的上限為 50 個標籤。
- 對於每個資源，每個標籤鍵必須是唯一的，並且只能有一個標籤值。
- 標籤鍵與值皆區分大小寫。最佳做法是，我們建議您定義策略，以便將標籤資本化，並在資源中一致地實作該策略。
- 一個標籤鍵最多可包含 128 個 UTF-8 字元。一個標籤值最多可包含 256 個 UTF-8 字元。字符可以是字母，數字，空格或以下符號：_。：/= +-@
- 前`aws:`綴保留供使用AWS。您不能在您定義的任何標籤鍵或值中使用它。此外，您無法變更或移除使用此前置詞的標籤鍵或值。使用此字首的標籤不會計入每個資源 50 個標籤的配額。

- 您指派的任何標籤僅適用於您的標籤，AWS 帳戶且僅適用於您指派標籤的標籤。AWS 區域
- 如果您使用 Security Hub 將標籤指派給資源，標籤只會套用至直接儲存在適用 Security Hub 中的資源AWS 區域。這些資源不會套用到 Security Hub 為您建立、使用或維護在其他方面的任何相關聯、支援資源AWS 服務。例如，如果您將標籤指派給自動化規則，該規則會更新與 Amazon Simple Storage Service (Amazon S3) 相關的發現項目，則標籤只會套用至指定區域的 Security Hub 中的自動化規則。它們不適用於您的 S3 存儲桶。若要將標籤指派給關聯的資源，您可以使用AWS Resource Groups或存放資源AWS 服務的標籤，例如 Amazon S3 用於 S3 儲存貯體。將標籤指派給相關聯的資源可協助您識別 Security Hub 資源的支援資源。
- 如果刪除資源，也會刪除指定給資源的任何標籤。

> **Important**
>
> 請勿在標籤中儲存機密或其他類型的敏感資料。標籤可以從許多人訪問AWS 服務，包括AWS Billing and Cost Management。它們不打算用於敏感數據。

若要新增和管理 Security Hub 資源的標籤，您可以使用 Security Hub 主控台、Security Hub API 或標 AWS Resource Groups記 API。使用 Security Hub，您可以在建立資源時將標籤新增至資源。您也可以新增和管理個別現有資源的標籤。使用 Resource Groups，您可以為跨越多AWS 服務個現有資源 (包括 Security Hub) 的大量新增和管理標籤。

有關其他標記提示和最佳做法，請參閱標記資AWS源使用指南中的標記AWS資源。

在 IAM 政策中使用標籤

開始標記資源後，您可以在 AWS Identity and Access Management (IAM) 政策中定義以標籤為基礎的資源層級許可。透過這種方式使用標籤，您可以對您中的哪些使用者和角色AWS 帳戶有權建立和標記資源，以及哪些使用者和角色有權更一般地新增、編輯和移除標籤。若要根據標籤控制存取，您可以在 IAM 政策的「條件」元素中使用與標籤相關的條件金鑰。

例如，如果資源的`Owner`標籤指定了使用者名稱，您可以建立 IAM 政策，讓使用者能夠完整存取所有 AWS Security Hub 資源：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
```

```
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

如果您定義標籤型、資源層級許可，則許可會立即生效。這表示您的資源一旦建立就會更安全，而且您可以快速開始強制使用新資源的標籤。您也可以使用資源層級許可，以控制哪些標籤金鑰和值可以與新的和現有的資源相關聯。如需詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制對 AWS 資源的存取。

將標籤新增至 AWS Security Hub 資源

若要將標籤新增至個別 AWS Security Hub 資源，您可以使用 Security Hub 主控台或 Security Hub API。控制台不支持向Hub資源添加標籤。

若要同時將標籤新增至多個 Security Hub 資源，請使用標記 API 的AWS Resource Groups標記作業。

> **Important**
>
> 將標籤新增至資源可能會影響資源的存取。在將標籤新增至資源之前，請先檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

Console

將標籤加入資源

當您建立自動化規則或組態原則時，Security Hub 主控台會提供新增標籤的選項。您可以在「標籤」區段中提供標籤鍵和標籤值。

Security Hub API & AWS CLI

將標籤加入資源

若要建立資源並以程式設計方式為其新增一或多個標籤，請針對您要建立的資源類型使用適當的作業：

- 若要建立設定原則並在其中新增一或多個標籤，請叫用 CreateConfigurationPolicyAPI，或者，如果您使用的是AWS CLI，請執行create-configuration-policy命令。
- 若要建立自動化規則並在其中新增一或多個標籤，請叫用 CreateAutomationRuleAPI，或者，如果您使用的是AWS CLI，請執行create-automation-rule命令。
- 若要啟用 Security Hub 並將一或多個標籤新增至您的Hub資源，請叫用 EnableSecurityHubAPI，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行enable-security-hub命令。

在您的請求中，使用tags參數為每個要新增至資源的標籤指定標籤鍵和可選標籤值。該tags參數指定對象的數組。每個物件都會指定一個標籤鍵及其相關聯的標籤值。

若要將一或多個標籤新增至現有的資源，請使用 Security Hub API 的TagResource作業，或者，如果您使用的是AWS CLI，請執行標籤資源命令。在您的請求中，指定要新增標籤的資源的 Amazon 資源名稱 (ARN)。使用tags參數可為要加入的每個標籤指定標籤鍵 (keyvalue) 和可選標籤值 ()。該tags參數指定對象的數組，每個標籤鍵及其相關聯的標籤值一個對象。

例如，下列AWS CLI命令會將含有Environment標籤值的標Prod籤金鑰新增至指定的組態原則。此範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

CLI 指令範例：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

其中：

- resource-arn指定要新增標籤之組態原則的 ARN。
- *Environment*是要新增至規則之標籤的標籤鍵。
- *Prod*是指定標籤鍵的標籤值 (*Environment*)。

在下列範例中，命令會將數個標籤新增至組態原則。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

對於tags陣列中的每個物件，key和引value數都是必需的。不過，value引數的值可以是空字串。如果您不想將標籤值與標籤鍵建立關聯，請不要指定value引數的值。例如，下列命令會加入沒有關聯Owner標籤值的標籤鍵：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

如果標記作業成功，Security Hub 會傳回空的 HTTP 200 回應。否則，Security Hub 會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

檢閱 AWS Security Hub 資源的標籤

您可以使用 Security Hub 主控台或 Security Hub API 來檢閱 Security Hub 自動化規則或組態原則的標籤 (標籤金鑰和標記值)。控制台不支持查看Hub資源的標籤。

若要同時檢閱多個 Security Hub 資源的標籤，請使用標記 API 的AWS Resource Groups標記作業。

Console

若要檢閱資源的標籤

1. 使用 Security Hub 系統管理員的認證，開啟 AWS Security Hub 主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 根據您要新增標籤的資源類型，執行下列其中一個動作：
   - 若要檢閱自動化規則的標籤，請在導覽窗格中選擇「自動化」。然後，選擇自動化規則。
   - 若要檢閱組態原則的標籤，請在瀏覽窗格中選擇 [組態]。然後，在 [原則] 索引標籤上，選取設定原則旁邊的選項。側邊面板隨即開啟，顯示指派給策略的標籤數目。您可以展開「標籤」標頭以查看標籤鍵和標籤值。

「標籤」區段會列出目前指定給資源的所有標籤。

Security Hub API & AWS CLI

若要檢閱資源的標籤

若要擷取和檢閱現有資源的標籤，請呼叫 ListTagsForResourceAPI。在您的請求中，使用`resourceArn`參數來指定資源的 Amazon 資源名稱 (ARN)。

如果您使用的是AWS CLI，請執行list-tags-for-resource命令並使用`resource-arn`參數來指定資源的 ARN。例如：

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如果操作成功，Security Hub 返回一個`tags`數組。陣列中的每個物件都會指定目前指派給資源的標籤 (標籤鍵和標籤值)。例如：

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

其中`Environment`、`CostCenter`和`Owner`是指派給資源的標籤鍵。 `Prod`是與標籤鍵相關聯的標籤值。 `12345`是與標籤鍵相關聯的標籤值。`Owner`標籤鍵沒有關聯的標籤值。

若要擷取具有標籤的所有 Security Hub 資源清單，以及指派給這些資源的所有標籤，請使用AWS Resource Groups標記 API 的GetResources作業。在您的請求中，將`ResourceTypeFilters`參數的值設定為`securityhub`。若要使用執行此操作AWS CLI，請執行 get-resources 命令，並將`resource-type-filters`參數的值設定為。`securityhub`例如：

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

如果作業成功，Resource Groups 會傳回`ResourceTagMappingList`陣列。陣列會針對每個具有標籤的 Security Hub 資源包含一個物件。每個物件都會指定 Security Hub 資源的 ARN，以及指派給資源的標籤索引鍵和值。

編輯 AWS Security Hub 資源的標籤

若要編輯 AWS Security Hub 資源的標籤 (標籤金鑰或標籤值)，您可以使用 Security Hub API。安全中心主控台目前不支援標籤編輯。

若要同時編輯多個 Security Hub 資源的標籤，請使用標記 API 的AWS Resource Groups標記作業。

> **Important**
>
> 編輯資源的標籤可能會影響資源的存取。在編輯資源的標籤金鑰或值之前，請先檢閱任何可能使用標籤來控制資源存取權的 AWS Identity and Access Management (IAM) 政策。

Security Hub API & AWS CLI

若要編輯資源的標籤

當您以程式設計方式編輯資源的標籤時，會以新值覆寫現有標籤。因此，編輯標籤的最佳方式取決於您要編輯標籤鍵、標籤值還是兩者。若要編輯標籤關鍵字，請移除目前的標籤並新增標籤。

若只要編輯或移除與標籤金鑰相關聯的標籤值，請使用 Security Hub API 的TagResource作業覆寫現有值。如果您使用的是AWS CLI，請執行標籤資源命令。在您的請求中，指定要編輯或移除其標籤值的資源的 Amazon 資源名稱 (ARN)。

若要編輯標籤值，請使用`tags`參數指定要變更其標籤值的標籤鍵。您也應該指定金鑰的新標籤值。例如，下列AWS CLI命令會`Prod`將指派給指定自動化規則之`Environment`標籤金鑰的標籤值從變更`Test`為。此範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

其中：

- `resource-arn`指定組態原則的 ARN。
- *`Environment`*是與要變更的標籤值相關聯的標籤鍵。
- *`Test`*是指定標籤鍵的新標籤值 (*`Environment`*)。

若要從標籤鍵移除標籤值，請勿為參數中索`value`引鍵的引`tags`數指定值。例如：

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

如果作業成功，Security Hub 會傳回空的 HTTP 200 回應。否則，Security Hub 會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

從 AWS Security Hub 資源移除標籤

若要從安 AWS Security Hub 資源移除標籤，您可以使用 Security Hub API。安全中心主控台目前不支援標籤移除。

若要同時從多個 Security Hub 資源中移除標籤，請使用標記 API 的AWS Resource Groups標記作業。

> **Important**
>
> 從資源中移除標籤可能會影響對資源的存取。移除標籤之前，請先檢閱任何可能使用標籤控制資源存取權的 AWS Identity and Access Management (IAM) 政策。

Security Hub API & AWS CLI

若要從資源中移除標籤

若要以程式設計方式從資源中移除一或多個標籤，請使用 Security Hub API 的UntagResource作業。在您的請求中，使用`resourceArn`參數指定要從中移除標籤的資源的 Amazon 資源名稱 (ARN)。使用`tagKeys`參數指定要移除之標籤的標籤鍵。若要移除多個標籤，請為每個要移除的標籤附加`tagKeys`參數和引數，並以 & 符號分隔，例如。`tagKeys=`*`key1`*`&tagKeys=`*`key2`*若只要從資源中移除特定標籤值 (而非標籤鍵)，請編輯標籤，而不要移除標籤。

如果您使用的是AWS CLI，請執行 untag-resource 命令，從資源中移除一或多個標籤。對於`resource-arn`參數，請指定要從中移除標籤的資源 ARN。使用`tag-keys`參數指定要移除之

標籤的標籤鍵。例如，下列命令會從指定的組態原則移除標Environment籤 (標籤索引鍵和標籤值)：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

其中resource-arn指定要從中移除標籤的組態原則的 ARN，而且*Environment*是要移除之標籤的標籤索引鍵。

要從資源中刪除多個標籤，請添加每個額外的標籤鍵作為tag-keys參數的引數。例如：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

如果作業成功，Security Hub 會傳回空的 HTTP 200 回應。否則，Security Hub 會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

Security Hub 配額

您的每個配額都AWS 帳戶有特定的預設配額 (先前稱為限制) AWS 服務。這些配額是您帳戶的服務資源或作業數目上限。本主題連結至您帳戶適用於 AWS Security Hub 資源和作業的配額。除非另有說明，否則每個配額都適用於您的帳戶AWS 區域。

有些配額可以增加，有些則無法增加。若要要求增加配額，請使用 Service Quotas 主控台。若要瞭解如何要求提高配額，請參閱 Service Quotas 使用者指南中的要求增加配額。如果 Service Quotas 主控台上無法使用配額，請使用上的服務限制增加表單AWS Support Center Console來要求提高配額。

最大配額

如需適用於 Security Hub 資源的配額清單，請參閱 AWS AWS 一般參考.

費率配額

如需適用於 Security Hub API 作業的配額清單，請參閱 AWSSecurity Hub API 參考。

如果您已設定跨區域彙總，只要呼叫連結的區域`BatchImportFindings`和彙總區域，就會造成`BatchUpdateFindings`影響。此`GetFindings`作業會從連結的區域和彙總區域擷取發現項目。不過，`BatchEnableStandards`和作`UpdateStandardsControl`業是區域特有的。

Security Hub 區域限制

某些 AWS Security Hub 功能僅在某些情況下提供AWS 區域。以下各節將指定這些區域限制。

如需安全中樞可使用的區域清單，請參閱 AWS AWS 一般參考.

跨區域彙總限制

在中AWS GovCloud (US)，跨區域彙總僅適用於發現項目、尋找更新和深入分AWS GovCloud (US)析。具體而言，您只能彙總 AWS GovCloud (美國東部) 和 (美國西部) 之間的發現項目、尋找更新和 AWS GovCloud 深入解析。

在中國地區，跨區域彙總僅適用於中國區域的發現結果、尋找更新和見解。具體而言，您只能彙總中國（北京）和中國（寧夏）之間的調查結果，發現更新和見解。

您不能使用默認情況下禁用的區域作為您的彙總區域。如需預設為停用的區域清單，請參閱在中啟用區域AWS 一般參考。

各區域整合的可用性

某些整合無法在所有區域中使用。如果特定區域無法使用整合，則當您選擇該區域時，該整合不會列在 Security Hub 主控台的 [整合] 頁面上。

在中國（北京）和中國（寧夏）支持的集成

中國（北京）和中國（寧夏）地區僅支持以下與AWS服務的整合：

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager 修補程式管理員

中國 (北京) 和中國 (寧夏) 區域僅支援下列第三方整合：

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 支援的整合

AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域僅支援下列與服務的整合 AWS：

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域僅支援下列第三方整合：

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie

- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series（僅適用於 AWS GovCloud （美國西部））
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

各區域標準的可用性

服務管理標準：AWS Control Tower僅適用於AWS Control Tower支援的區域，包括AWS GovCloud (US). 若要取得AWS Control Tower支援的區域清單，請參閱《使AWS 區域用指南》AWS Control Tower中的〈AWS Control Tower使用方式〉。

其他安全性標準可在 Security Hub 提供的所有區域中使用。

各區域控制項的可用性

Security Hub 控制項可能不適用於所有區域。若要查看每個區域中無法使用的控制項清單，請參閱控制區域限制。如果控制項在您登入的區域中無法使用，控制項就不會出現在 Security Hub 主控台中的控制項清單上。例外情況是，如果您已登入彙總區域。在這種情況下，您可以看到彙總區域或一個或多個連結區域中可用的控制項。

控制區域限制

AWS Security Hub 控制項可能無法在所有使用 AWS 區域。此頁面顯示特定區域無法使用的控制項。如果控制項在您登入的區域中無法使用，控制項就不會出現在 Security Hub 主控台中的控制項清單上。例外情況是，如果您已登入彙總區域。在這種情況下，您可以看到彙總區域或一個或多個連結區域中可用的控制項。

內容

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 非洲 (開普敦)
- 亞太區域 (香港)
- 亞太區域 (海德拉巴)
- 亞太區域 (雅加達)
- 亞太區域 (墨爾本)
- 亞太區域 (孟買)
- 亞太區域 (大阪)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (雪梨)
- 亞太區域 (東京)
- 加拿大 (中部)

- 加拿大西部 (卡加利)
- 中國 (北京)
- 中國 (寧夏)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (米蘭)
- Europe (Paris)
- 歐洲 (西班牙)
- 歐洲 (斯德哥爾摩)
- 歐洲 (蘇黎世)
- 以色列 (特拉維夫)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)
- 南美洲 (聖保羅)
- AWS GovCloud (美國東部)
- AWS GovCloud (美國西部)

美國東部 (俄亥俄)

美國東部 (俄亥俄) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

美國東部 (維吉尼亞北部)

美國東部 (維吉尼亞北部) 不支援下列控制項。

- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組

美國西部 (加利佛尼亞北部)

美國西部 (加利佛尼亞北部) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制

- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [EKS.1] EKS 叢集端點不應可公開存取
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

美國西部 (奧勒岡)

美國西部 (奧勒岡) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件

- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

非洲 (開普敦)

非洲 (開普敦) 不支援以下控制項。

- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密

- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.12] 應移除未使用的 Amazon EC2 EIP
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EKS.1] EKS 叢集端點不應可公開存取
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制

- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [RDS.1] RDS 快照應該是私有的
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

亞太區域 (香港)

亞太區域 (香港) 不支援下列控制項。

- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

亞太區域 (海德拉巴)

亞太區域 (海德拉巴) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄

- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密

- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告

- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.5] 應啟用應用程式和傳統負載平衡器記錄
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式

- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch

- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶
- [S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則

- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

亞太區域 (雅加達)

亞太區域 (雅加達) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）
- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型
- [AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄

- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.17] 應啟動 CloudWatch 警報動作
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求

- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.2] ECS 服務不應該自動分配公共 IP 地址
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.9] ECS 任務定義應具有記錄組態
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密

- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄

- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.11] S3 一般用途儲存貯體應啟用事件通知
- [S3.13] S3 一般用途儲存貯體應具有生命週期組態
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件

- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

亞太區域 (墨爾本)

亞太區域 (墨爾本) 不支援下列控制項。

- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制

- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.1] Amazon EBS 快照不應公開還原
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄

- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [EKS.8] EKS 叢集應啟用稽核記錄
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區

- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.7] IAM 使用者的密碼政策應具有強大的組態
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config
- [IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母
- [IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母
- [IAM.13] 確保 IAM 密碼政策至少需要一個符號
- [IAM.14] 確保 IAM 密碼政策至少需要一個數字
- [IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高
- [IAM.16] 確保 IAM 密碼政策防止密碼重複使用
- [IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密

- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [RDS.1] RDS 快照應該是私有的
- [RDS.3] RDS 資料庫執行個體應啟用靜態加密
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集

- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [S3.15] S3 一般用途儲存貯體應啟用物件鎖定
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [SSM.4] SSM 文件不應該是公開的
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

亞太區域 (孟買)

亞太區域 (孟買) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

亞太區域 (大阪)

亞太區域 (大阪) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 DynamoDB] 資料表應該已啟用復原 point-in-time
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.1] Amazon EBS 快照不應公開還原
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除

- [EC2.7] 應啟用 EBS 預設加密
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.2] ECS 服務不應該自動分配公共 IP 地址
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.9] ECS 任務定義應具有記錄組態
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行

- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.6] 應該啟用應用 Application Load Balancer 刪除保護
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.9] 傳統負載平衡器應啟用跨區域負載平衡
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- 不應意外刪除 [KMS AWS KMS keys .3]
- [Lambda 1] Lambda 函數政策應該禁止公共訪問
- [Lambda 2] Lambda 函數應該使用受支援的執行階段
- [Lambda 3] Lambda 函數應該在 VPC 中

- VPC Lambda 函數應在多個可用區域中運作
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [RDS.1] RDS 快照應該是私有的
- [RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密
- [RDS.6] 應為 RDS 資料庫執行個體設定增強型監控
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護

- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.15] S3 一般用途儲存貯體應啟用物件鎖定
- [S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

亞太區域 (首爾)

亞太區域 (首爾) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

亞太區域 (新加坡)

亞太區域 (新加坡) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

亞太區域 (雪梨)

亞太區域 (雪梨) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

亞太區域 (東京)

亞太區域 (東京) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

加拿大 (中部)

加拿大 (中部) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制

- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

加拿大西部 (卡加利)

加拿大西部 (卡加利) 不支援下列控制項。

- [帳戶。1] 應提供安全聯繫信息 AWS 帳戶
- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- [介面 5] API Gateway REST API 快取資料應在靜態時加密
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域
- [AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）
- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址

- [AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型
- [AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌
- [CloudWatch.17] 應啟動 CloudWatch 警報動作
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [動態 DynamoDB] 資料表應該已啟用刪除保護
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠
- [EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.2] ECS 服務不應該自動分配公共 IP 地址
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.9] ECS 任務定義應具有記錄組態
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中

- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [EKS.8] EKS 叢集應啟用稽核記錄
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.7] 傳統負載平衡器應啟用連線排空
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.10] Classic Load Balancer 應該跨越多個可用區域
- [ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料

- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [.5] 彈性搜尋網域應啟用稽核記錄
- [ES.6] 彈性搜尋網域至少應該有三個資料節點
- [ES.7] 彈性搜尋網域至少應設定三個專用主節點
- [.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.7] IAM 使用者的密碼政策應具有強大的組態
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config
- [IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母
- [IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母
- [IAM.13] 確保 IAM 密碼政策至少需要一個符號
- [IAM.14] 確保 IAM 密碼政策至少需要一個數字
- [IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高
- [IAM.16] 確保 IAM 密碼政策防止密碼重複使用
- [IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料

- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- 不應意外刪除 [KMS AWS KMS keys .3]
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄

- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.17] RDS 資料庫執行個體應設定為將標籤複製到快照
- 虛擬私人雲端應部署 RDS 執行 VPC
- [RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱
- [RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱
- [RDS.21] 應為重要資料庫參數群組事件設定 RDS 事件通知訂閱
- [RDS.22] 應針對重要資料庫安全性群組事件設定 RDS 事件通知訂閱
- [RDS.23] RDS 執行個體不應使用資料庫引擎預設連接埠
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 4] 亞馬遜 Redshift 叢集應啟用稽核記錄
- [紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [紅移 .10] Redshift 叢集在靜態時應加密

- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態
- [S3.11] S3 一般用途儲存貯體應啟用事件通知
- [S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取
- [S3.13] S3 一般用途儲存貯體應具有生命週期組態
- [S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys
- [S3.19] S3 存取點應該已啟用封鎖公用存取設定
- [S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [SSM.4] SSM 文件不應該是公開的
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組

- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能
- [WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

中國 (北京)

中國 (北京) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護

- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch

- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照

- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

中國 (寧夏)

中國 (寧夏) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯

- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分

- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Lambda 1] Lambda 函數政策應該禁止公共訪問
- [Lambda 2] Lambda 函數應該使用受支援的執行階段
- [Lambda 3] Lambda 函數應該在 VPC 中
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空

- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密

- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

歐洲 (法蘭克福)

歐洲 (法蘭克福) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

歐洲 (愛爾蘭)

歐洲 (愛爾蘭) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

歐洲 (倫敦)

歐洲 (倫敦) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制

- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

歐洲 (米蘭)

歐洲 (米蘭) 不支援下列控制項。

- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)

- [EC2.12] 應移除未使用的 Amazon EC2 EIP
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EKS.1] EKS 叢集端點不應可公開存取
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- 不應意外刪除 [KMS AWS KMS keys .3]
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照

- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [RDS.1] RDS 快照應該是私有的
- [RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

Europe (Paris)

歐洲 (巴黎) 不支援下列控制項。

- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象

- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

歐洲 (西班牙)

歐洲 (西班牙) 不支援下列控制項。

- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄

- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL

- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [DynamoDB 資料表應該會根據需求自動擴展容量
- [動態 DynamoDB] 資料表應該已啟用復原 point-in-time
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.1] Amazon EBS 快照不應公開還原
- [EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
- [EC2.7] 應啟用 EBS 預設加密
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區

- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.5] 應啟用應用程式和傳統負載平衡器記錄
- [ELB.6] 應該啟用應用 Application Load Balancer 刪除保護
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.9] 傳統負載平衡器應啟用跨區域負載平衡
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址

- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- [KMS.4] AWS KMS 按鍵旋轉應該已啟用
- [Lambda 1] Lambda 函數政策應該禁止公共訪問
- [Lambda 2] Lambda 函數應該使用受支援的執行階段
- [Lambda 3] Lambda 函數應該在 VPC 中
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式

- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [RDS.1] RDS 快照應該是私有的
- [RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config
- [RDS.3] RDS 資料庫執行個體應啟用靜態加密

- [RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密
- [RDS.5] RDS 資料庫執行個體應設定為多個可用區域
- [RDS.6] 應為 RDS 資料庫執行個體設定增強型監控
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch
- [RDS.10] 應為 RDS 執行個體設定身分與存取權管理身分驗證
- [RDS.11] RDS 執行個體應該已啟用自動備份
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 1] 亞馬遜 Redshift 集群應禁止公共訪問
- [紅移 2] 與亞馬遜 Redshift 叢集的連接應在傳輸過程中進行加密
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.5] S3 通用存儲桶應該要求使用 SSL 的請求
- [S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶
- [S3.7] S3 一般用途儲存貯體應使用跨區域複寫
- [S3.8] S3 通用存儲桶應阻止公共訪問

- [S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄
- [S3.15] S3 一般用途儲存貯體應啟用物件鎖定
- [S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

歐洲 (斯德哥爾摩)

歐洲 (斯德哥爾摩) 不支援下列控制項。

- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密

- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

歐洲 (蘇黎世)

歐洲 (蘇黎世) 不支援下列控制項。

- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API Gateway 路由應該指定授權類型

- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CloudTrail.7] 確保 S3 儲存貯體上已啟用 S3 儲存 CloudTrail 貯體存取日誌
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄

- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [DynamoDB 資料表應該會根據需求自動擴展容量
- [動態 DynamoDB] 資料表應該已啟用復原 point-in-time
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.9] Amazon EC2 執行個體不應該有公有 IPv4 地址
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄

- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.9] 傳統負載平衡器應啟用跨區域負載平衡
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料

- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份

- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [RDS.1] RDS 快照應該是私有的
- [RDS.3] RDS 資料庫執行個體應啟用靜態加密
- [RDS.5] RDS 資料庫執行個體應設定為多個可用區域
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢

- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

以色列 (特拉維夫)

以色列 (特拉維夫) 不支援下列控制項。

- [ACM.1] 匯入和 ACM 核發的憑證應在指定時間後續約
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄

- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch

- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
- [EC2.10] 應將 Amazon EC2 設定為使用針對 Amazon EC2 服務建立的 VPC 端點
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [EKS.8] EKS 叢集應啟用稽核記錄
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級

- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.4] 應將應 Application Load Balancer 設定為刪除 http 標頭
- [ELB.6] 應該啟用應用 Application Load Balancer 刪除保護
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [ES.1] 彈性搜尋網域應啟用靜態加密
- [ES.2] 彈性搜索域名不應公開訪問
- [E.3] 彈性搜尋網域應加密節點之間傳送的資料
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在

- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.7] IAM 使用者的密碼政策應具有強大的組態
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.10] IAM 使用者的密碼政策應該有強烈的排序 AWS Config
- [IAM.11] 確保 IAM 密碼政策至少需要一個大寫字母
- [IAM.12] 確保 IAM 密碼政策至少需要一個小寫字母
- [IAM.13] 確保 IAM 密碼政策至少需要一個符號
- [IAM.14] 確保 IAM 密碼政策至少需要一個數字
- [IAM.15] 確保 IAM 密碼政策的密碼長度下限為 14 或更高
- [IAM.16] 確保 IAM 密碼政策防止密碼重複使用
- [IAM.17] 確保 IAM 密碼政策在 90 天或更短的時間內過期
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護

- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.1] RDS 快照應該是私有的
- [RDS.4] RDS 叢集快照和資料庫快照在靜態時應加密
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照

- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 3] 亞馬遜 Redshift 集群應啟用自動快照
- [Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.2] S3 通用存儲桶應該阻止公共讀取訪問
- [S3.3] S3 通用存儲桶應該阻止公共寫入訪問
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉
- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [SSM.3] 由系統管理員管理的 Amazon EC2 執行個體應具有「合規」的關聯合規性狀態
- [SSM.4] SSM 文件不應該是公開的
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能

- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能
- [WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

Middle East (Bahrain)

中東 (巴林) 不支援下列控制項。

- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- [EC2.20] AWS 網站對站點 VPN 連線的兩個 VPN 通道都應啟動

- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [紅移 6] 亞馬遜 Redshift 應該啟用自動升級到主要版本
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [SSM.2] 安裝修補程式後，由系統管理員管理的 Amazon EC2 執行個體修補程式合規狀態應為「合規」
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

中東 (阿拉伯聯合大公國)

中東 (阿拉伯聯合大公國) 不支援下列控制項。

- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應該啟用 API Gateway REST 和 WebSocket API 執行日誌記錄
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密

- [AutoScaling.1] 與 Classic Load Balancer 關聯的 Auto Scaling 組應使用負載平衡器健康狀態檢查
- [Backup 1] AWS Backup 復原點應該在靜態時加密
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudTrail.1] CloudTrail 應啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤
- [CloudTrail.6] 確保用於存放 CloudTrail 日誌的 S3 儲存貯體無法公開存取
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [CloudWatch.17] 應啟動 CloudWatch 警報動作
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.1] Database Migration Service 複製執行個體不應該是公用的
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密

- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期
- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.3] 附加的 Amazon EBS 磁碟區應靜態加密
- [EC2.4] 停止的 EC2 執行個體應在指定時間段後移除
- [EC2.6] 應在所有 VPC 中啟用虛擬私人雲端流程記錄
- [EC2.8] EC2 執行個體應該使用執行個體中繼資料服務版本 2 (IMDSv2)
- [EC2.12] 應移除未使用的 Amazon EC2 EIP
- [EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入
- [EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.9] ECS 任務定義應具有記錄組態
- [EFS.1] 應將彈性檔案系統設定為使用的靜態檔案資料加密 AWS KMS
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取
- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行

- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS
- [ELB.3] Classic Load Balancer 接聽程式應該使用 HTTPS 或 TLS 終止來設定
- [ELB.9] 傳統負載平衡器應啟用跨區域負載平衡
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.1] IAM 政策不應允許完整的「*」管理特權
- [IAM.2] IAM 使用者不應附加 IAM 政策
- [IAM.3] IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
- [IAM.4] IAM 根使用者存取金鑰不應存在
- [IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.8] 應移除未使用的 IAM 使用者登入資料
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.18] 確保已建立支援角色來管理事件 AWS Support
- [IAM.19] 應為所有 IAM 使用者啟用 MFA

- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [IAM.22] 應移除 45 天未使用的 IAM 使用者登入資料
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- [KMS.1] IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作
- [KMS.2] IAM 主體不應具有允許對所有 KMS 金鑰進行解密動作的 IAM 內嵌政策
- [KMS.4] AWS KMS 按鍵旋轉應該已啟用
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料

- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- OpenSearch 網域應該已安裝最新的軟體更新
- [RDS.1] RDS 快照應該是私有的
- [RDS.2] RDS 資料庫執行個體應該禁止公開存取，視設定而定 PubliclyAccessible AWS Config
- [RDS.3] RDS 資料庫執行個體應啟用靜態加密
- [RDS.5] RDS 資料庫執行個體應設定為多個可用區域
- [RDS.6] 應為 RDS 資料庫執行個體設定增強型監控
- [RDS.8] RDS 資料庫執行個體應啟用刪除保護
- [RDS.11] RDS 執行個體應該已啟用自動備份
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.2] S3 通用存儲桶應該阻止公共讀取訪問
- [S3.3] S3 通用存儲桶應該阻止公共寫入訪問
- [S3.5] S3 通用存儲桶應該要求使用 SSL 的請求
- [S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶
- [S3.7] S3 一般用途儲存貯體應使用跨區域複寫
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.1] Secrets Manager 秘密應該啟用自動旋轉

- [SecretsManager.2] 配置了自動旋轉的秘密 Secrets Manager 密鑰應該成功旋轉
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SQS.1] Amazon SQS 佇列應該在靜態時加密
- [SSM.1] Amazon EC2 執行個體應由以下公司管理 AWS Systems Manager
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能

南美洲 (聖保羅)

南美洲 (聖保羅) 不支援下列控制項。

- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源

- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [RDS.7] RDS 叢集應該已啟用刪除保護
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.16] RDS 資料庫叢集應設定為將標籤複製到快照
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組

AWS GovCloud (美國東部)

AWS GovCloud (美國東部) 不支援下列控制項。

- [帳戶。1] 應提供安全聯繫信息 AWS 帳戶
- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域
- [AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）

- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型
- [AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [CloudWatch.17] 應啟動 CloudWatch 警報動作
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [DynamoDB 資料表應該會根據需求自動擴展容量
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.9] ECS 任務定義應具有記錄組態
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取

- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [EKS.8] EKS 叢集應啟用稽核記錄
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.2] 具有 SSL/HTTPS 接聽程式的傳統負載平衡器應該使用由提供的憑證 AWS Certificate Manager
- [ELB.8] 具有 SSL 接聽程式的傳統負載平衡器應使用具有強式設定的預先定義安全性原則 AWS Config
- [ELB.10] Classic Load Balancer 應該跨越多個可用區域
- [ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [GuardDuty.1] GuardDuty 應該啟用
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Kinesis.1] Kinesis 串流應該在靜態時加密

- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式
- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制

- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級
- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態
- [S3.11] S3 一般用途儲存貯體應啟用事件通知
- [S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取
- [S3.13] S3 一般用途儲存貯體應具有生命週期組態
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能
- [SageMaker.1] Amazon SageMaker 筆記本實例不應該直接訪問互聯網
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替

- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SSM.4] SSM 文件不應該是公開的
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件
- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能
- [WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

AWS GovCloud (美國西部)

AWS GovCloud (美國西部) 不支援下列控制項。

- [帳戶。1] 應提供安全聯繫信息 AWS 帳戶
- [帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations
- [ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度
- 應將 API Gateway REST API 階段設定為使用 SSL 憑證進行後端驗證
- API 網關 REST API 階段應該已啟用跟踪 AWS X-Ray
- [原則 4] API Gateway 器應該與 WAF 網頁 ACL 相關聯
- API Gateway 路由應該指定授權類型
- 應該為 API Gateway V2 階段配置訪問日誌記錄
- [AppSync.2] AWS AppSync 應啟用欄位層級記錄
- [AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證
- [Athena.1] Athena 工作群組應在靜態時加密
- [AutoScaling.2] Amazon EC2 Auto Scaling 組應涵蓋多個可用區域
- [AutoScaling.3] Auto Scaling 組啟動配置應將 EC2 實例配置為需要實例元數據服務版本 2（IMDSv2）

- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1
- [自動擴展 .5] 使用自動擴展群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址
- [AutoScaling.6] Auto Scaling 群組應在多個可用區域中使用多個執行個體類型
- [AutoScaling.9] Amazon EC2 Auto Scaling 組應該使用 Amazon EC2 啟動模板
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成
- [CloudFront.1] CloudFront 發行版應該配置一個默認的根對象
- [CloudFront.3] CloudFront 發行版在傳輸過程中應該需要加密
- [CloudFront.4] CloudFront 發行版應該配置原始容錯移轉
- [CloudFront.5] CloudFront 發行版應啟用日誌記錄
- [CloudFront.6] CloudFront 發行版應啟用 WAF
- [CloudFront.7] CloudFront 發行版本應使用自訂 SSL/TLS 憑證
- [CloudFront.8] CloudFront 發行版應該使用 SNI 來提供 HTTPS 請求
- [CloudFront.9] CloudFront 發行版應該加密到自定義來源的流量
- [CloudFront.10] CloudFront 發行版不應在邊緣位置和自定義來源之間使用已棄用的 SSL 協議
- [CloudFront.12] CloudFront 發行版不應指向不存在的 S3 來源
- [CloudFront.13] CloudFront 發行版應使用源訪問控制
- [CloudWatch.15] CloudWatch 警報應設定指定的動作
- [CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間
- [CloudWatch.17] 應啟動 CloudWatch 警報動作
- [CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據
- [CodeBuild.2] CodeBuild 項目環境變量不應包含純文本憑據
- [CodeBuild.3] CodeBuild S3 日誌應加密
- [CodeBuild.4] CodeBuild 項目環境應該具有日誌記錄 AWS Config配置
- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式
- [DMS.6] DMS 複製執行個體應啟用自動次要版本升級
- [DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄
- [DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄
- [DMS.9] DMS 端點應使用 SSL
- [文件 DB.1] Amazon DocumentDB 叢集應在靜態時加密
- [文件 DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期

- [文件 DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的
- [文件 DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch
- [文件 DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護
- [DynamoDB 資料表應該會根據需求自動擴展容量
- [動態 B. 3] DynamoDB 加速器 (DAX) 叢集應在靜態時加密
- 備份計劃中應該有 DynamoDB 資料表
- [EC2.15] Amazon EC2 子網路不應該自動指派公有 IP 地址
- [EC2.16] 應移除未使用的網路存取控制清單
- [EC2.17] Amazon EC2 執行個體不應使用多個 ENI
- [EC2.21] 網路 ACL 不應允許從 0.0.0/0 輸入連接埠 22 或連接埠 3389
- [EC2.22] 應移除未使用的 Amazon EC2 安全群組
- [EC2.23] Amazon EC2 傳輸閘道不應自動接受 VPC 附件請求
- [EC2.24] 不應使用 Amazon EC2 半虛擬實例類型
- [EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面
- [EC2.28] 備份計劃應涵蓋 EBS 磁碟區
- [ECR.1] ECR 私有儲存庫應設定影像掃描
- [ECR.2] ECR 私有儲存庫應配置標籤不變性
- [ECR.3] ECR 儲存庫應該至少設定一個生命週期原則
- [ECS.1] Amazon ECS 任務定義應具有安全的聯網模式和使用者定義。
- [ECS.3] ECS 任務定義不應共享主機的進程名稱空間
- [ECS.4] ECS 容器應以非特權的方式執行
- [ECS.5] ECS 容器應僅限於對根檔案系統的唯讀存取
- [ECS.8] 密碼不應作為容器環境變量傳遞
- [ECS.9] ECS 任務定義應具有記錄組態
- [ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行
- [ECS.12] ECS 叢集應使用容器深入解析
- [EFS.2] Amazon EFS 磁碟區應該在備份計劃中
- [EFS.3] EFS 存取點應強制執行根目錄
- [EFS.4] EFS 存取點應強制執行使用者身分
- [EKS.1] EKS 叢集端點不應可公開存取

- [EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行
- [EKS.8] EKS 叢集應啟用稽核記錄
- [ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份
- [ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級
- [ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移
- [ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密
- [ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密
- [ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH
- [ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組
- [ElasticBeanstalk.1] Elastic Beanstalk 環境應啟用增強的健康報告
- [ElasticBeanstalk2] 應啟用 Elastic Beanstalk 管理平台更新
- [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch
- [ELB.10] Classic Load Balancer 應該跨越多個可用區域
- [ELB.12] Application Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.13] 應用程式、網路和閘道負載平衡器應跨越多個可用區域
- [ELB.14] Classic Load Balancer 應設定為防禦性或最嚴格的不同步緩解模式
- [ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF
- [EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置
- [ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌
- [EventBridge.3] EventBridge 自定義事件總線應該附加基於資源的策略
- [EventBridge.4] EventBridge 全域端點應啟用事件複寫
- [FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區
- [IAM.6] 應為根使用者啟用硬體 MFA
- [IAM.9] 應該為根用戶啟用 MFA
- [IAM.21] 您建立的 IAM 客戶受管政策不應允許針對服務執行萬用字元動作
- [Kinesis.1] Kinesis 串流應該在靜態時加密
- VPC Lambda 函數應在多個可用區域中運作
- [Macie.1] Amazon Macie 應該啟用
- [Macie.2] 應啟用 Macie 自動化敏感資料探索功能
- [MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式

- [MQ.6] RabbitMQ 代理程式應該使用叢集部署模式
- [MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密
- [MSK.2] MSK 叢集應該已設定增強型監控功能
- [Neptune .1] Neptune DB 叢集在靜態時應加密
- [Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch
- [Neptune .3] Neptune DB 叢集快照不應該是公開的
- [Neptune .4] Neptune 資料庫叢集應啟用刪除保護
- [Neptune .5] Neptune 資料庫叢集應啟用自動備份
- [Neptune .6] Neptune 資料庫叢集快照在靜態時應加密
- [Neptune .7] Neptune 資料庫叢集應啟用 IAM 資料庫身份驗證
- [Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照
- [Neptune .9] Neptune 資料庫叢集應部署在多個可用區域
- [NetworkFirewall.1] Network Firewall 防火牆應跨多個可用區域部署
- [NetworkFirewall.2] 應啟用 Network Firewall 日誌記錄
- [NetworkFirewall.3] Network Firewall 策略應至少有一個關聯的規則組
- [NetworkFirewall.4] 對於完整封包，Network Firewall 策略的預設無狀態處理行動應為捨棄或轉送
- [NetworkFirewall.5] 對於分散式封包，Network Firewall 策略的預設無狀態處理行動應該是捨棄或轉送
- [NetworkFirewall.6] 無狀態 Network Firewall 規則群組不應為空
- [NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護
- OpenSearch 網域應啟用靜態加密功能
- [打開搜索 .2] OpenSearch 域名不應該是公開訪問
- OpenSearch 網域應該加密節點之間傳送的資料
- 應該啟用 OpenSearch 網域錯誤記錄到 CloudWatch 記錄
- OpenSearch 網域應該已啟用稽核記錄
- OpenSearch 網域應該至少有三個資料節點
- OpenSearch 網域應該啟用精細的存取控制
- 應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接
- [PCA.1] AWS Private CA 根憑證授權單位應停用
- [RDS.12] 應為 RDS 叢集設定身分與存取權管理身分驗證
- 應啟用 RDS 自動次要版本升級

- [RDS.14] Amazon Aurora 叢集應啟用回溯
- [RDS.15] 應為多個可用區域設定 RDS 資料庫叢集
- [RDS.24] RDS 資料庫叢集應使用自訂管理員使用者名稱
- [RDS.25] RDS 資料庫執行個體應使用自訂管理員使用者名稱
- [RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護
- [RDS.27] RDS 資料庫叢集應在靜態時加密
- [RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch
- [RDS.35] RDS 資料庫叢集應啟用自動次要版本升級
- [紅移 .7] Redshift 叢集應使用增強型 VPC 路由
- [Redshift.8] 亞馬遜 Redshift 群集不應使用默認的管理員用戶名
- [紅移 .9] Redshift 叢集不應使用預設的資料庫名稱
- [紅移 .10] Redshift 叢集在靜態時應加密
- [路線 53.2] 路線 53 公共託管區域應記錄 DNS 查詢
- [S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定
- [S3.8] S3 通用存儲桶應阻止公共訪問
- [S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態
- [S3.11] S3 一般用途儲存貯體應啟用事件通知
- [S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取
- [S3.13] S3 一般用途儲存貯體應具有生命週期組態
- [S3.14] S3 一般用途儲存貯體應啟用版本控制
- [S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能
- [SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動
- [SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限
- [SecretsManager.3] 刪除未使用的 Secrets Manager 秘密
- [SecretsManager.4] Secrets Manager 密鑰應在指定的天數內輪替
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄
- [SSM.4] SSM 文件不應該是公開的
- [StepFunctions.1] Step Functions 狀態機應該打開日誌記錄
- [WAF.1] 應啟用 AWS WAF 傳統的全域網頁 ACL 記錄功能
- [WAF.2] AWS WAF 經典區域規則至少應具有一個條件

- [WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則
- [WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組
- [WAF.6] AWS WAF 經典全域規則至少應該有一個條件
- [WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則
- [WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組
- [WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組
- [WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能
- [WAF.12] AWS WAF 規則應該啟用量度 CloudWatch

停用 Security Hub

> **Note**
>
> 如果您使用中央組態，AWSSecurity Hub 委派的系統管理員可以建立組態原則，停用特定帳戶和組織單位 (OU) 中的 Security Hub，並在其他人中保持啟用。設定原則會在您的家用區域和所有連結的區域中生效。如需詳細資訊，請參閱安全中心中的集中配置。

您可以使用 Security Hub 主控台、Security Hub API，或停AWS CLI用 Security Hub。

當您停用帳戶的 Security Hub 時，會發生下列情況：

- 沒有新的發現項目會針對帳戶進行處理。
- 90 天之後，您現有的發現項目和深入解析，以及任何 Security Hub 組態設定都會遭到刪除，且無法復原。

  如果您想要儲存現有的發現項目，必須先匯出它們，然後才能停用 Security Hub。如需詳細資訊，請參閱the section called “帳戶動作對 Security Hub 資料的影響”。
- 任何啟用的標準和控制項都會停用。

在下列情況下，您無法停用安全中心：

- 您的帳戶是組織指定的 Security Hub 系統管理員帳戶。如果您使用中央設定，則無法將停用 Security Hub 的組態原則與委派的系統管理員帳戶建立關聯。其他帳戶的關聯可以成功，但 Security Hub 不會將此類原則套用至委派的系統管理員帳戶。
- 您的帳戶是 Security Hub 系統管理員帳戶的邀請，而且您擁有已啟用的成員帳戶。您必須先解除所有成員帳戶的關聯，才能停用 Security Hub。請參閱 the section called “取消關聯成員帳戶”。

您必須先取消與其系統管理員帳戶的關聯，才能停用成員帳戶的 Security Hub。對於組織帳戶，只有管理員帳戶可以取消成員帳戶的關聯。如需詳細資訊，請參閱the section called “取消組織成員帳戶的關聯”。對於手動邀請的帳戶，管理員帳戶或成員帳戶都可以取消與成員帳戶的關聯。如需詳細資訊，請參閱 the section called “取消關聯成員帳戶” 或 the section called “取消與管理員帳戶的關聯” 。如果您使用中央設定，則不需要解除關聯，因為您可以建立停用特定成員帳戶中 Security Hub 的原則。

當您停用帳戶中的安全中心時，它只會在目前的區域中停用。不過，如果您使用中央組態來停用特定帳戶中的 Security Hub，則會在主 [區域] 和所有連結的區域中停用此功能。

選擇您偏好的方法，然後按照步驟停用 Security Hub。

Security Hub console

若要停用 Security Hub

1. 開啟 Sec AWS urity Hub 主控台，網址為 https://console.aws.amazon.com/securityhub/。
2. 在導覽窗格選擇設定。
3. 在 [設定] 頁面上，選擇 [一般]。
4. 在 [停用 AWS Security Hub] 下方，選擇 [停用 AWS Security Hub 然後再次選擇禁用 AWS Security Hub。

Security Hub API

若要停用 Security Hub

調用該 DisableSecurityHubAPI。

AWS CLI

若要停用 Security Hub

執行 disable-security-hub 命令。

範例命令：

```
aws securityhub disable-security-hub
```

Security Hub 控制項的變更記錄

下列變更記錄會追蹤 AWS Security Hub 安全性控制項的重大變更，這可能會導致控制項的整體狀態及其發現項目的符合性狀態變更。如需有關 Security Hub 如何評估控制項狀態的資訊，請參閱法規遵循狀態和控制狀態。變更可能需要在這個記錄檔中輸入幾天後，才會影響所有 AWS 區域 可用控制項的內容。

此記錄檔會追蹤自 2023 年 4 月以來發生的變更。

選取控制項以檢視其詳細資訊。標題變更會在每個控制項的詳細說明中記錄 90 天。

Important

作為對控制項進行定期審查的一部分，Security Hub 將於 2024 年 3 月從所有安全標準中移除以下控制項。刪除所有 AWS 帳戶 ， AWS 區域 可能需要長達一個月。從帳戶移除控制項後，Security Hub 會在五天內封存相關的發現項目，並在 90 天後刪除它們。如果您希望在 Security Hub 移除這些控制項發現項目之前停止接收這些發現項目，您可以使用 Security Hub 主控台、API 或停用它們 AWS CLI。

- [CodeBuild.5] CodeBuild 項目環境不應啟用特權模式。 在 Codebuild 專案中啟用特殊權限模式不會對客戶環境造成額外風險。
- [Athena.1] Athena 工作群組應在靜態時加密。 Athena 工作群組會將日誌傳送到 Amazon S3 儲存貯體，Amazon S3 現在可在新的和現有的 S3 儲存貯體上使用 S3 受管金鑰 (SS3-S3) 提供預設加密。
- [CloudFormation.1] CloudFormation 堆棧應與 Simple Notification Service (SNS) 集成。將 AWS CloudFormation 堆疊與 SNS 主題整合不再是安全性最佳做法。雖然將重要 AWS CloudFormation 堆疊與 SNS 主題整合可能很有用，但並非所有堆疊都需要這麼做。
- [SNS.2] 傳送至主題的通知訊息應啟用傳送狀態的記錄。 記錄 SNS 主題的傳遞狀態已不再是安全性最佳作法。雖然記錄重要 SNS 主題的傳遞狀態可能很有用，但並非所有主題都需要這樣做。
- [IAM.20] 避免使用根用戶。 此控制項的功能已納入現有控制項中[CloudWatch.1] 對於「root」用戶的使用，應存在日誌指標過濾器和警報。
- [AutoScaling.4] Auto Scaling 群組啟動設定的中繼資料回應躍點限制不應超過 1。 EC2 中繼資料服務的躍點限制取決於工作負載。

此外，下列控制項只會從「 AWS 基礎安全性最佳作法」(FSBP) 標準中移除，但仍會包含在 NIST SP 800-53 r5 標準中：

- [S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態由[S3.13] S3 一般用途儲存貯體應具有生命週期組態和取代[S3.14] S3 一般用途儲存貯體應啟用版本控制，這兩者都屬於 FSBP 標準。
- [S3.11] S3 一般用途儲存貯體應啟用事件通知。 雖然在某些情況下，S3 儲存貯體的事件通知可能很有用，但這並不是一般的安全最佳做法。
- [SNS.1] SNS 主題應該使用靜態加密 AWS KMS。 由於 SNS 已預設加密所有主題，因此不再建議使用 AWS KMS 加密主題作為安全性最佳實務。

變更日期	控制項 ID 和標題	變更說明
2024年3月22日	應使用最新的 TLS 安全策略加密與 OpenSearch 域的連接	從連線到 OpenSearch 網域變更的控制項標題應使用 TLS 1.2 加密至 OpenSearch 網域的連線應使用最新的 TLS 安全性原則加密。先前，控制項只檢查 OpenSearch 網域的連線是否使用 TLS 1.2。控制項現在會產生一個PASSED發現是否使用最新的 TLS 安全性原則加密 OpenSearch 網域。控制項標題和描述已更新，以反映目前的行為。
2024年3月22日	[.8] 應使用最新的 TLS 安全策略加密至彈性搜尋網域的連線	從連線至 Elasticsearch 網域變更的控制項標題應使用 TLS

變更日期	控制項 ID 和標題	變更說明
		1.2 加密，而連線至 Elasticsearch 網域應使用最新的 TLS 安全性原則加密。先前，控制項只會檢查與彈性搜尋網域的連線是否使用 TLS 1.2。如果使用最新的 TLS 安全策略加密 Elasticsearch 域，控制項現在會產生一個PASSED發現。控制項標題和描述已更新，以反映目前的行為。
2024年3月12日	[S3.1] S3 一般用途儲存貯體應啟用區塊公開存取設定	從 S3 封鎖公用存取設定變更的標題應啟用至 S3 一般用途儲存貯體，應啟用封鎖公用存取設定。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.2] S3 通用存儲桶應該阻止公共讀取訪問	S3 儲存貯體的變更標題應禁止公開讀取 S3 一般用途儲存貯體的存取權限，應該會封鎖公用讀取存取 Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。

變更日期	控制項 ID 和標題	變更說明
2024年3月12日	[S3.3] S3 通用存儲桶應該阻止公共寫入訪問	從 S3 儲存貯體變更標題應禁止對 S3 一般用途儲存貯體的公開寫入存取權限，應封鎖公用寫入存取權 Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.5] S3 通用存儲桶應該要求使用 SSL 的請求	從 S3 儲存貯體變更標題應該要求使用安全通訊端層至 S3 一般用途儲存貯體的請求，應該要求才能使用 SSL。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶	從授予儲存貯體政策的 S3 許可變更標題應限制 AWS 帳戶 在 S3 一般用途儲存貯體政策應限制對其他儲存貯體政策的存取 AWS 帳戶。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.7] S3 一般用途儲存貯體應使用跨區域複寫	從 S3 儲存貯體變更的標題應啟用跨區域複寫至 S3 一般用途儲存貯體，應使用跨區域複寫。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。

變更日期	控制項 ID 和標題	變更說明
2024年3月12日	[S3.7] S3 一般用途儲存貯體應使用跨區域複寫	從 S3 儲存貯體變更的標題應啟用跨區域複寫至 S3 一般用途儲存貯體，應使用跨區域複寫。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.8] S3 通用存儲桶應阻止公共訪問	從 S3 區塊公開存取設定變更的標題應該在儲存貯體層級啟用至 S3 一般用途儲存貯體，應該會封鎖公用存取。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.9] S3 一般用途儲存貯體應啟用伺服器存取記錄	應為 S3 一般用途儲存貯體啟用伺服器存取記錄的變更標題，才能啟用伺服器存取記錄。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.10] 啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態	已啟用版本控制的 S3 儲存貯體變更標題應將生命週期政策設定為啟用版本控制的 S3 一般用途儲存貯體應具有生命週期組態 Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。

變更日期	控制項 ID 和標題	變更說明
2024年3月12日	[S3.11] S3 一般用途儲存貯體應啟用事件通知	S3 儲存貯體中變更的標題應啟用 S3 一般用途儲存貯體的事件通知應啟用事件通知。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.12] ACL 不應用於管理使用者對 S3 一般用途儲存貯體的存取	S3 存取控制清單 (ACL) 中變更的標題不應用於管理使用者對 ACL 的儲存貯體存取，不應該用於管理使用者對 S3 一般用途儲存貯體的存取。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.13] S3 一般用途儲存貯體應具有生命週期組態	從 S3 儲存貯體變更的標題應該將生命週期政策設定為 S3 一般用途儲存貯體應具有生命週期組態 Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.14] S3 一般用途儲存貯體應啟用版本控制	從 S3 儲存貯體變更的標題應該使用版本控制到 S3 一般用途儲存貯體應啟用版本控制。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。

變更日期	控制項 ID 和標題	變更說明
2024年3月12日	[S3.15] S3 一般用途儲存貯體應啟用物件鎖定	從 S3 儲存貯體變更的標題應設定為使用物件鎖定至 S3 一般用途儲存貯體，應啟用物件鎖定。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月12日	[S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys	S3 儲存貯體中變更的標題應在靜態時加密 AWS KMS keys至 S3 一般用途儲存貯體，應使用靜態加密 AWS KMS keys。Security Hub 將標題變更為新 S3 儲存貯體類型的帳戶。
2024年3月7日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`nodejs20.x` 和`ruby3.3`作為參數。

變更日期	控制項 ID 和標題	變更說明
2024年2月22 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`dotnet8`作為參數。
2024年2月5 日	[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行	Security Hub 更新了 Amazon EKS 叢集可以在其上執行的最舊受支援 Kubernetes 版本，以產生通過的發現項目。目前支援的最舊版本為 Kubernetes `1.25`。
2024 年 1 月 10 日	[CodeBuild.1] CodeBuild 比特桶源存儲庫 URL 不應包含敏感憑據	從CodeBuild GitHub 或比特桶源存儲庫 URL 更改的標題應該使用 OAuth 來CodeBuild 源存儲庫 URL 不應包含敏感憑據。Security Hub 刪除了 OAuth 的提及，因為其他連接方法也可以是安全的。Security Hub 刪除了提及， GitHub 因為它不再可能在 GitHub 源存儲庫 URL 中具有個人訪問令牌或用戶名和密碼。

變更日期	控制項 ID 和標題	變更說明
2024 年 1 月 8 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 不再支援`go1.x`和`java8`作為參數，因為這些都是淘汰的執行階段。
2023 年 12 月 29 日	[RDS.8] RDS 資料庫執行個體應啟用刪除保護	RDS.8 會檢查使用其中一個受支援資料庫引擎的 Amazon RDS 資料庫執行個體是否已啟用刪除保護。Security Hub 現在支援`custom-oracle-ee` `oracle-ee-cdb` 、和`oracle-se2-cdb`作為資料庫引擎。
2023 年 12 月 22 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`java21`和`python3.12` 作為參數。Security Hub 不再支持`ruby2.7`作為參數。

變更日期	控制項 ID 和標題	變更說明
2023 年 12 月 15 日	[CloudFront.1] CloudFront 發行版應該配置一個默認的根對象	CloudFront.1 檢查 Amazon CloudFront 分發是否已設定預設根物件。Security Hub 將此控制項的嚴重性從「嚴重」降低到「高」，因為新增預設根物件是建議，取決於使用者的應用程式和特定需求。
2023 年 12 月 5 日	[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入	從安全性群組變更控制標題不應允許從 0.0.0.0/0 輸入連接埠 22 到安全性群組，不應允許從 0.0.0.0/0 或::/0 到連接埠 22 的輸入。
2023 年 12 月 5 日	[EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389	將控制標題從 [確保沒有安全性群組允許從 0.0.0.0/0 輸入連接埠 3389 到安全性群組不應允許從 0.0.0.0/0 或:: /0 到連接埠 3389 的輸入。

變更日期	控制項 ID 和標題	變更說明
2023 年 12 月 5 日	[RDS.9] RDS 資料庫執行個體應該將記錄檔發佈到記錄 CloudWatch	RDS 資料庫執行個體應啟用資料庫記錄中變更的控制項標題，應將記錄發佈至記 CloudWatch 錄。Security Hub 識別此控制項只會檢查是否將日誌發佈到 Amazon CloudWatch 日誌，而不會檢查 RDS 日誌是否已啟用。如果 RDS 資料庫執行個體設定為將記錄發佈到記錄，則控制項會產生發PASSED CloudWatch 現項目。控制項標題已更新，以反映目前的行為。
2023 年 11 月 17 日	[EC2.19] 安全性群組不應允許不受限制地存取高風險連接埠	EC2.19 會檢查被視為高風險的指定連接埠是否可存取安全性群組的不受限制傳入流量。Security Hub 已更新此控制項，以在將受管理的前置詞清單作為安全性群組規則的來源提供這些清單。如果前綴列表包含字符串 '0.0.0.0/0' 或 ':: /0'，則控制項生成一個FAILED發現。

變更日期	控制項 ID 和標題	變更說明
2023 年 11 月 16 日	[CloudWatch.15] CloudWatch 警報應設定指定的動作	從CloudWatch 警報變更的控制項標題應該具有針對警 CloudWatch 示狀態設定的動作，應該已設定指定的動作。
2023 年 11 月 16 日	[CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間	CloudWatch 記錄群組中變更的控制項標題應保留至少 1 年，以便 CloudWatch 記錄群組應保留指定的時間段。
2023 年 11 月 16 日	VPC Lambda 函數應在多個可用區域中運作	從 VPC Lambda 函數變更控制標題應該在多個可用區域中運作，而 VPC Lambda 函數應該在多個可用區域中運作。
2023 年 11 月 16 日	[AppSync.2] AWS AppSync 應啟用欄位層級記錄	從變更的控制項標題 AWS AppSync 應該開啟要求層級和欄位層級記錄，以便啟AWS AppSync 用欄位層級記錄。
2023 年 11 月 16 日	[EMR.1] Amazon EMR 叢集主節點不應具有公有 IP 地址	從 Amazon 彈性 MapReduce叢集主節點變更的控制標題不應具有連至 Amazon EMR 叢集主節點的公有 IP 地址不應具有公用 IP 地址。

變更日期	控制項 ID 和標題	變更說明
2023 年 11 月 16 日	[打開搜索 .2] OpenSearch 域名不應該是公開訪問	從OpenSearch 網域變更的控制項標題應該位於 VPC 中變更為OpenSearch網域，不應可公開存取。
2023 年 11 月 16 日	[ES.2] 彈性搜索域名不應公開訪問	從 Elasticsearch 網域變更的控制項標題應該位於 VPC 到彈性搜尋網域不應該可公開存取。
2023 年 10 月 31 日	[ES.4] 應該啟用彈性搜索域錯誤日誌記錄到 CloudWatch 日誌	ES.4 會檢查彈性搜尋網域是否設定為將錯誤日誌傳送到 Amazon 日誌。 CloudWatch 控制項先前針對 Elasticsearch 網域產生了一個發PASSED現項目，該網域的任何記錄已設定為傳送至 CloudWatch 記錄檔。Security Hub 已更新控制項，以僅針對設定為將錯誤記錄檔傳送至記錄的 Elasticsearch 網域產生尋PASSED找項目。 CloudWatch 控制項也已更新，排除不支援錯誤記錄檔的 Elasticsearch 版本進行評估。

變更日期	控制項 ID 和標題	變更說明
2023 年 10 月 16 日	[EC2.13] 安全性群組不應允許從 0.0.0.0/0 輸入或:/0 到連接埠 22 的輸入	EC2.13 會檢查安全群組是否允許不受限制的輸入存取連接埠 22。Security Hub 已更新此控制項，以在將受管理的前置詞清單作為安全性群組規則的來源提供這些清單。如果前綴列表包含字符串 '0.0.0.0/0' 或 ':: /0'，則控制項生成一個FAILED發現。
2023 年 10 月 16 日	[EC2.14] 安全性群組不應允許從 0.0.0.0/0 或:/0 輸入至連接埠 3389	EC2.14 會檢查安全群組是否允許不受限制的輸入存取連接埠 3389。Security Hub 已更新此控制項，以在將受管理的前置詞清單作為安全性群組規則的來源提供這些清單。如果前綴列表包含字符串 '0.0.0.0/0' 或 ':: /0'，則控制項生成一個FAILED發現。

變更日期	控制項 ID 和標題	變更說明
2023 年 10 月 16 日	[EC2.18] 安全群組只允許授權連接埠不受限制的傳入流量	EC2.18 會檢查使用中的安全性群組是否允許不受限制的傳入流量。Security Hub 已更新此控制項，以在將受管理的前置詞清單作為安全性群組規則的來源提供這些清單。如果前綴列表包含字符串 '0.0.0.0/0' 或 ':: /0'，則控制項生成一個FAILED發現。
2023 年 10 月 16 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持python3.11 作為參數。
2023 年 10 月 4 日	[S3.7] S3 一般用途儲存貯體應使用跨區域複寫	Security Hub 新增的參數ReplicationType 值為，CROSS-REGION 以確保 S3 儲存貯體已啟用跨區域複寫，而不是啟用相同區域複寫。

變更日期	控制項 ID 和標題	變更說明
2023 年 9 月 27 日	[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行	Security Hub 更新了 Amazon EKS 叢集可以在其上執行的最舊受支援 Kubernetes 版本，以產生通過的發現項目。目前支援的最舊版本為 Kubernetes 1.24。
2023 年 9 月 20 日	CloudFront.2 — CloudFront 發行版應啟用原始訪問身份	Security Hub 淘汰此控制項，並將其從所有標準中移除。反之，請參閱 [CloudFront.13] CloudFront 發行版應使用源訪問控制。Origin 存取控制是目前的安全性最佳做法。此控制項將在 90 天內從文件中移除。

變更日期	控制項 ID 和標題	變更說明
2023 年 9 月 20 日	[EC2.22] 應移除未使用的 Amazon EC2 安全群組	Security Hub 從 AWS 基礎安全性最佳實踐（FSBP）和美國國家標準與技術研究所（NIST）SP 800-53 版 5 中刪除了此控制。它仍然是服務管理標準的一部分： AWS Control Tower。如果安全群組連接至 EC2 執行個體或 elastic network interface，此控制項會產生傳遞的發現。但是，對於某些使用案例，未連接的安全性群組不會造成安全性風險。您可以使用其他 EC2 控制項 (例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19) 來監控您的安全群組。
2023 年 9 月 20 日	EC2.29 — EC2 執行個體應該在虛擬私人 VPC 中啟動	Security Hub 淘汰此控制項，並將其從所有標準中移除。Amazon EC2 已將 EC2-經典實例遷移到 VPC。此控制項將在 90 天內從文件中移除。

變更日期	控制項 ID 和標題	變更說明
2023 年 9 月 20 日	S3.4 — S3 儲存貯體應啟用伺服器端加密	Security Hub 淘汰此控制項，並將其從所有標準中移除。Amazon S3 現在可在新的和現有的 S3 儲存貯體上使用 S3 受管金鑰 (SS3-S3) 提供預設加密。對於使用 SS3-S3 或 SS3-KMS 伺服器端加密加密的現有儲存貯體，加密設定不會變更。此控制項將在 90 天內從文件中移除。
2023 年 9 月 14 日	[EC2.2] VPC 預設安全性群組不應允許輸入或輸出流量	已變更的控制項標題 VPC 預設安全性群組不應允許對 VPC 預設安全性群組的輸入和出站流量不應允許輸入或輸出流量。
2023 年 9 月 14 日	[IAM.9] 應該為根用戶啟用 MFA	根使用者應啟用從 Virtual MFA 變更的控制項標題，才能讓 root 使用者啟用至 MFA。
2023 年 9 月 14 日	[RDS.19] 應針對重要叢集事件設定現有 RDS 事件通知訂閱	從 RDS 事件通知訂閱變更控制項標題應針對重要叢集事件設定為現有 RDS 事件通知訂閱應針對重要叢集事件設定。

變更日期	控制項 ID 和標題	變更說明
2023 年 9 月 14 日	[RDS.20] 應針對重要資料庫執行個體事件設定現有 RDS 事件通知訂閱	從 RDS 事件通知訂閱變更控制項標題應針對重要資料庫執行個體事件設定為現有 RDS 事件通知訂閱，應針對重要資料庫執行個體事件設定。
2023 年 9 月 14 日	[WAF.2] AWS WAF 經典區域規則至少應具有一個條件	從 WAF 區域規則變更的控制項標題應具有至少一個條件，以AWS WAF 傳統區域規則應具有至少一個條件。
2023 年 9 月 14 日	[WAF.3] AWS WAF 傳統區域規則群組至少應該有一個規則	從 WAF 區域規則群組變更的控制項標題至少應具有一個規則，AWS WAF 傳統區域規則群組應至少有一個規則。
2023 年 9 月 14 日	[WAF.4] AWS WAF 傳統區域網路 ACL 至少應該有一個規則或規則群組	從 WAF 地區 Web ACL 變更的控制項標題應該至少有一個規則或規則群組，以AWS WAF 傳統區域 Web ACL 應該至少有一個規則或規則群組。

變更日期	控制項 ID 和標題	變更說明
2023 年 9 月 14 日	[WAF.6] AWS WAF 經典全域規則至少應該有一個條件	從 WAF 全域規則變更控制項標題應具有至少一個條件，AWS WAF 傳統全域規則應該至少有一個條件。
2023 年 9 月 14 日	[WAF.7] AWS WAF 傳統全域規則群組至少應該有一個規則	從 WAF 全域規則群組變更的控制項標題應該至少有一個規則，AWS WAF 傳統全域規則群組應該至少有一個規則。
2023 年 9 月 14 日	[WAF.8] AWS WAF 傳統的全域網路 ACL 至少應該有一個規則或規則群組	從 WAF 全域 Web ACL 變更的控制項標題應該至少有一個規則或規則群組，以AWS WAF 傳統全域 Web ACL 應該至少有一個規則或規則群組。
2023 年 9 月 14 日	[WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組	從 WAFv2 Web ACL 變更控制項標題至少應該有一個規則或規則群組到 AWS WAF Web ACL，至少應該有一個規則或規則群組。
2023 年 9 月 14 日	[WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能	應啟用從AWS WAF v2 Web ACL 記錄中變更的控制項標題，以啟用AWS WAF 網頁 ACL 記錄。

變更日期	控制項 ID 和標題	變更說明
2023 年 7 月 20 日	S3.4 — S3 儲存貯體應啟用伺服器端加密	S3.4 會檢查 Amazon S3 儲存貯體是否已啟用伺服器端加密，或 S3 儲存貯體政策明確拒絕沒有伺服器端加密的`PutObject`請求。Security Hub 已更新此控制項，以包含使用 KMS 金鑰 (DSSE-KMS) 的雙層伺服器端加密。當 S3 儲存貯體使用 SSE-S3、SSE-KMS 或 DSSE-KMS 加密時，控制項會產生傳遞的發現項目。
2023 年 7 月 17 日	[S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys	S3.17 會檢查 Amazon S3 儲存貯體是否使用. AWS KMS key Security Hub 已更新此控制項，以包含使用 KMS 金鑰 (DSSE-KMS) 的雙層伺服器端加密。當 S3 儲存貯體使用 SSE-KMS 或 DSSE-KMS 加密時，控制項會產生傳遞的發現項目。

變更日期	控制項 ID 和標題	變更說明
2023 年 6 月 9 日	[EKS.2] EKS 叢集應該在受支援的 Kubernetes 版本上執行	EKS.2 會檢查 Amazon EKS 叢集是否在受支援的 Kubernetes 版本上執行。目前支援的最舊版本為。`1.23`
2023 年 6 月 9 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`ruby3.2`作為參數。
2023 年 6 月 5 日	[介面 5] API Gateway REST API 快取資料應在靜態時加密	Apigateway 5. 檢查 Amazon API Gateway REST API 階段中的所有方法是否在靜態時加密。Security Hub 更新控制項，只有在啟用該方法的快取時，才評估特定方法的加密。
2023 年 5 月 18 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`java17`作為參數。

變更日期	控制項 ID 和標題	變更說明
2023 年 5 月 18 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 不再支持`nodejs12.x` 作為參數。
2023年4月23 日	[ECS.10] ECS Fargate 服務應在最新的 Fargate 平台版本上運行	ECS.10 檢查 Amazon ECS Fargate 服務是否正在運行最新的 Fargate 平台版本。客戶可以直接透過 ECS 部署 Amazon ECS，也可以使用. CodeDeploy Security Hub 已更新此控制項，以便在您使用 CodeDeploy 部署 ECS Fargate 服務時產生「通過」的發現項目。
2023 年 4 月 20 日	[S3.6] S3 一般用途儲存貯體政策應限制對其他儲存貯體的存取 AWS 帳戶	S3.6 會檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策是否防止其他 AWS 帳戶 主體對 S3 儲存貯體中的資源執行拒絕動作。Security Hub 更新了控制項，以說明值區策略中的條件。

變更日期	控制項 ID 和標題	變更說明
2023 年 4 月 18 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 現在支持`python3.10` 作為參數。
2023 年 4 月 18 日	[Lambda 2] Lambda 函數應該使用受支援的執行階段	Lambda.2 會檢查執行階段的 AWS Lambda 函數設定是否符合針對每種語言支援執行階段所設定的預期值。Security Hub 不再支持`dotnetcore3.1` 作為參數。
2023 年 4 月 17 日	[RDS.11] RDS 執行個體應該已啟用自動備份	RDS.11 會檢查 Amazon RDS 執行個體是否已啟用自動備份，且備份保留期大於或等於 7 天。Security Hub 已更新此控制項以將僅供讀取複本排除在評估之外，因為並非所有引擎都支援僅供讀取複本上的自動備份。此外，RDS 不提供在建立僅供讀取複本時指定備份保留期的選項。僅供讀取複本建立的備份保留期預`0`設為。

AWS Security Hub 使用者指南的文件記錄

下表說明 Sec AWS urity Hub 文件的更新。

> **Note**
>
> 對於安全控制版本，指定的日期是所有帳戶和區域中可用控制項的日期。控制項可能需要 1-2 週才能到達所有帳戶和區域。

變更	描述	日期
控制參數的上下文配置	如果您使用中央組態，您現在可以從 Security Hub 主控台上控制項的詳細資料頁面，在內容中設定控制項參數。	2024年3月29 日
更新至現有的受管理策略	Security Hub 更新了`AmazonSecurityHubReadOnlyAccess` 通過添加`Sid`字段命名的AWS 受管理策略。	2024年2月22 日
新的安全控制	現在應該啟用控制項 [Macie.2] Macie 自動化敏感資料探索功能。如需此控制項的區域限制，請參閱依區域提供控制項。	2024年2月19 日
Security Hub 可在加拿大西部 (卡加利) 使用	Security Hub 現已在加拿大西部（卡爾加里）提供。所有 Security Hub 功能現在都可在此區域中使用，但某些安全性控制項除外。如需詳細資訊，請參閱依區域的控制項可用性。	2023 年 12 月 20 日

新的安全控制	下列新的 Security Hub 控制項可用： • the section called “[Backup 1] AWS Backup 復原點應該在靜態時加密” • the section called “[動態 DynamoDB] 資料表應該已啟用刪除保護” • the section called “[EC2.51] EC2 Client VPN 端點應啟用用戶端連線記錄” • the section called “[EKS.8] EKS 叢集應啟用稽核記錄” • the section called “[EMR.2] 應該啟用 Amazon EMR 塊公共訪問設置” • the section called “[FSx.1] OpenZFS 檔案系統的 FSx 應設定為將標籤複製到備份和磁碟區” • the section called “[Macie.1] Amazon Macie 應該啟用” • the section called “[MSK.2] MSK 叢集應該已設定增強型監控功能” • the section called “[Neptune .9] Neptune 資料庫叢集應部署在多個可用區域” • the section called “[Network Firewall.1] Network Firewall 防火牆應跨多個可用區域部署”	2023 年 12 月 14 日

	• the section called “[Network Firewall.2] 應啟用 Network Firewall 日誌記錄” • the section called “ OpenSearch 網域應該已安裝最新的軟體更新” • the section called “[PCA.1] AWS Private CA 根憑證授權單位應停用” • the section called “[S3.19] S3 存取點應該已啟用封鎖公用存取設定” • the section called “[S3.20] S3 一般用途儲存貯體應啟用 MFA 刪除功能”	
尋找豐富	Security Hub 添加了新的發現字段 `AwsAccountName` `ApplicationArn` ，和`ApplicationName` AWS 安全發現格式（ASFF）。	2023 年 11 月 27 日
摘要儀表板增強功能	您現在可以在 Security Hub 主控台的 [摘要] 頁面上存取更多儀表板 Widget、儲存儀表板篩選器集以快速關注特定安全性問題，以及自訂儀表板配置。	2023 年 11 月 27 日
中央配置	中央配置現在可用。透過中央設定，Security Hub 委派的系統管理員可以跨多個組織帳戶、組織單位 (OU) 和區域設定 Security Hub、標準和控制項。	2023 年 11 月 27 日

受管理策略的更新	Security Hub 為AWSSecurityHubServiceRolePolicy 受管理的原則新增了新的權限，讓 Security Hub 讀取和更新可自訂的安全性控制內容。	2023 年 11 月 26 日
自訂控制參數	您現在可以為選取的 Security Hub 控制項自訂參數值。這可以使特定控制項的發現與您的業務需求和安全性期望更加相關。	2023 年 11 月 26 日
受管理策略的更新	Security Hub 更新了AWSSecurityHubFullAccess 允許您分別使用 Security Hub 功能和與集成的AWSSecurityHubOrganizationsAccess 管理策略 AWS Organizations。	2023 年 11 月 16 日

已新增至服務管理標準的現有安全性控制： AWS Control Tower	下列現有的 Security Hub 控制項已新增至服務管理標準： AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • 公司 .9 • DocumentDB • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • 每米 5 米 • 每克里數 • 莫斯科 • RDS.12 • RDS.15 • S3.17	2023 年 11 月 14 日
受管理策略的更新	Security Hub 將新的標記權限新增至`AWSSecurityHubServiceRolePolicy` 受管理的原則，可讓 Security Hub 讀取與發現項目相關的資源標記。	2023 年 11 月 7 日

新的安全控制	下列新的 Security Hub 控制項可用： • the section called “[AppSync.5] AWS AppSync GraphQL API 不應該使用 API 密鑰進行身份驗證” • the section called “[DMS.6] DMS 複製執行個體應啟用自動次要版本升級” • the section called “[DMS.7] 目標資料庫的 DMS 複寫任務應該已啟用記錄” • the section called “[DMS.8] 來源資料庫的 DMS 複製任務應該已啟用記錄” • the section called “[DMS.9] DMS 端點應使用 SSL” • the section called “[文件DB.3] 亞馬遜 DocumentDB 手動叢集快照不應該是公開的” • the section called “[文件DB.4] Amazon DocumentDB 叢集應將稽核日誌發佈到日誌 CloudWatch ” • the section called “[文件DB.5] 亞馬遜 DocumentDB 叢集應啟用刪除保護” • the section called “[ECS.9] ECS 任務定義應具有記錄組態” • the section called “[EventBridge.3] EventBridge 自定義	2023 年 10 月 10 日

事件總線應該附加基於資源的策略”

- the section called “[EventBridge.4] EventBridge 全域端點應啟用事件複寫”
- the section called “[MSK.1] MSK 叢集在代理程式節點之間的傳輸過程中應加密”
- the section called “[MQ.5] ActiveMQ 代理程式應該使用主動/待命部署模式”
- the section called “[MQ.6] RabbitMQ 代理程式應該使用叢集部署模式”
- the section called “[NetworkFirewall.9] Network Firewall 防火牆應啟用刪除保護”
- the section called “[RDS.34] Aurora MySQL 資料庫叢集應將稽核記錄發佈至記錄檔 CloudWatch ”
- the section called “[RDS.35] RDS 資料庫叢集應啟用自動次要版本升級”
- the section called “[路線53.2] 路線 53 公共託管區域應記錄 DNS 查詢”
- the section called “[WAF.12] AWS WAF 規則應該啟用量度 CloudWatch ”

受管理策略的更新	Security Hub 已將新的組 Organizations 動作新增至`AWSSecurityHubServiceRolePolicy` 受管理的原則，讓 Security Hub 擷取帳戶和組織單位 (OU) 資訊。我們也新增了新的 Security Hub 動作，可讓 Security Hub 讀取和更新服務組態，包括標準和控制項。	2023 年 9 月 27 日

已新增至服務管理標準的現有安全性控制： AWS Control Tower	下列現有的 Security Hub 控制項已新增至服務管理標準： AWS Control Tower • the section called “[Athena.1] Athena 工作群組應在靜態時加密” • the section called “[文件DB.1] Amazon DocumentDB 叢集應在靜態時加密” • the section called “[文件DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期” • the section called “[Neptune .1] Neptune DB 叢集在靜態時應加密” • the section called “[Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch ” • the section called “[Neptune .3] Neptune DB 叢集快照不應該是公開的” • the section called “[Neptune .4] Neptune 資料庫叢集應啟用刪除保護” • the section called “[Neptune .5] Neptune 資料庫叢集應啟用自動備份” • the section called “[Neptune .6] Neptune 資料庫叢集快照在靜態時應加密” • the section called “[Neptune .7] Neptune 資料	2023 年 9 月 26 日

	庫叢集應啟用 IAM 資料庫身份驗證” • the section called “[Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照” • the section called “[RDS.27] RDS 資料庫叢集應在靜態時加密”	
合併控制項檢視與合併控制項搜尋結果 AWS GovCloud (US)	合併的控制項檢視與合併控制項發現項目現在可在中使用 AWS GovCloud (US) Region。Security Hub 主控台的 [控制項] 頁面會顯示跨標準的所有控制項。每個控制項在標準中都有相同的控制項 ID。當您開啟合併的控制項發現項目時，即使控制項套用至多個已啟用的標準，您也會收到每個安全性檢查的單一搜尋結果。	2023 年 9 月 6 日
中國區域提供的合併控制項檢視與合併控制項結果	中國區域現已提供合併控制項檢視與合併控制項搜尋結果。Security Hub 主控台的 [控制項] 頁面會顯示跨標準的所有控制項。每個控制項在標準中都有相同的控制項 ID。當您開啟合併的控制項發現項目時，即使控制項套用至多個已啟用的標準，您也會收到每個安全性檢查的單一搜尋結果。	2023 年 8 月 28 日

以色列 (特拉維夫) 地區提供安全中心	Security Hub 現已在以色列（特拉維夫）上市。所有 Security Hub 功能現在都可在此區域中使用，但某些安全性控制項除外。如需詳細資訊，請參閱依區域的控制項可用性。	2023 年 8 月 8 日

新的安全控制	下列新的 Security Hub 控制項可用： • the section called “[Athena.1] Athena 工作群組應在靜態時加密” • the section called “[文件DB.1] Amazon DocumentDB 叢集應在靜態時加密” • the section called “[文件DB.2] Amazon DocumentDB 叢集應該有足夠的備份保留期” • the section called “[Neptune .1] Neptune DB 叢集在靜態時應加密” • the section called “[Neptune .2] Neptune 資料庫叢集應將稽核記錄發佈至記錄 CloudWatch ” • the section called “[Neptune .3] Neptune DB 叢集快照不應該是公開的” • the section called “[Neptune .4] Neptune 資料庫叢集應啟用刪除保護” • the section called “[Neptune .5] Neptune 資料庫叢集應啟用自動備份” • the section called “[Neptune .6] Neptune 資料庫叢集快照在靜態時應加密” • the section called “[Neptune .7] Neptune 資料	2023 年 7 月 28 日

	庫叢集應啟用 IAM 資料庫身份驗證” • the section called “[Neptune .8] 應將 Neptune 資料庫叢集設定為將標籤複製到快照” • the section called “[RDS.27] RDS 資料庫叢集應在靜態時加密”	
自動化規則條件的新運算子	您現在可以針對自動化規則對應和字串準則使用「包含」和「NOT_CONTECT」比較運算子。	2023 年 7 月 25 日
自動化規則	Security Hub 現在提供自動化規則，可根據您指定的準則自動更新發現項目。	2023 年 6 月 13 日
新的第三方整合	Snyk是新的協力廠商整合，會將發現項目傳送至 Security Hub。	2023 年 6 月 12 日

已新增至服務管理標準的現有安全性控制： AWS Control Tower	下列現有的 Security Hub 控制項已新增至服務管理標準： AWS Control Tower • the section called “[帳戶。1] 應提供安全聯繫信息 AWS 帳戶” • the section called “API Gateway 路由應該指定授權類型” • the section called “應該為 API Gateway V2 階段配置訪問日誌記錄” • the section called “[CodeBuild.3] CodeBuild S3 日誌應加密” • the section called “[EC2.25] Amazon EC2 啟動範本不應將公有 IP 指派給網路界面” • the section called “[ELB.1] 應將應 Application Load Balancer 設定為將所有 HTTP 要求重新導向至 HTTPS” • the section called “[紅移 .10] Redshift 叢集在靜態時應加密” • the section called “[SageMaker.2] SageMaker 筆記型電腦執行個體應在自訂 VPC 中啟動” • the section called “[SageMaker.3] 用戶不應該擁有對 SageMaker 筆記本實例的 root 訪問權限”	2023 年 6 月 12 日

	• the section called “[WAF.10] AWS WAF 網路 ACL 至少應該有一個規則或規則群組”	
新的安全控制	下列新的 Security Hub 控制項可用： • the section called “[ACM.2] ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度” • the section called “[AppSync.2] AWS AppSync 應啟用欄位層級記錄” • the section called “[CloudFront.13] CloudFront 發行版應使用源訪問控制” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk 應該將日誌流式傳輸到 CloudWatch” • the section called “[S3.17] S3 一般用途儲存貯體在靜態時應使用 AWS KMS keys” • the section called “[StepFunctions.1] Step Functions 狀態機應該打開日誌記錄”	2023 年 6 月 6 日
亞太區域 (墨爾本) 提供安全中心	Security Hub 現已在亞太區域 (墨爾本) 推出。所有 Security Hub 功能現在都可在此區域中使用，但某些安全性控制項除外。如需詳細資訊，請參閱依區域的控制項可用性。	2023 年 5 月 25 日

尋找歷史	Security Hub 現在可以追蹤過去 90 天內發現項目的歷史記錄。	2023 年 5 月 4 日
新的安全控制	下列新的 Security Hub 控制項可用： • the section called “[EKS.1] EKS 叢集端點不應可公開存取” • the section called “[ELB.16] 應用程式負載平衡器應該與網路 ACL 相關聯 AWS WAF” • the section called “[紅移 .10] Redshift 叢集在靜態時應加密” • the section called “[S3.15] S3 一般用途儲存貯體應啟用物件鎖定”	2023 年 3 月 29 日
擴大對整合控制發現的支援	AWS v2.0.0 版的自動化安全回應現在支援整合的控制項發現項目。	2023 年 3 月 24 日
Security Hub 在新推出 AWS 區域	Security Hub 現已在亞太區域 (海德拉巴)、歐洲 (西班牙) 和歐洲 (蘇黎世) 推出。這些區域中可用的控制項存在限制。	2023 年 3 月 21 日
更新到受管理的策略	Security Hub 已更新`AWSSecurityHubServiceRolePolicy` 受管理策略中的現有權限。	2023 年 3 月 17 日

適用於 NIST 800-53 標準的全新安全性控制	Security Hub 已新增下列安全性控制項，適用於 NIST 800-53 標準： • the section called “[帳戶 .2] AWS 帳戶 應該是組織的一部分 AWS Organizations” • the section called “[CloudWatch.15] CloudWatch 警報應設定指定的動作” • the section called “[CloudWatch.16] CloudWatch 記錄群組應保留一段指定的時間” • the section called “[CloudWatch.17] 應啟動 CloudWatch 警報動作” • the section called “備份計劃中應該有 DynamoDB 資料表” • the section called “[EC2.28] 備份計劃應涵蓋 EBS 磁碟區” • EC2.29 — EC2 執行個體應該在 VPC 中啟動 (已停用) • the section called “[RDS.26] RDS 資料庫執行個體應該受到備份計劃的保護” • the section called “[S3.14] S3 一般用途儲存貯體應啟用版本控制” • the section called “[WAF.11] 應該啟用 AWS WAF 網頁 ACL 記錄功能”	2023 年 3 月 3 日

美國國家標準與技術研究院	資訊 Security Hub 現在支援 NIST 800-53 第 5 版標準，並提供超過 200 種適用的安全性控制項。	2023 年 2 月 28 日
合併控制項檢視與控制項發現	隨著整合控制項檢視的發行，Security Hub 主控台的 [控制項] 頁面會顯示您跨標準的所有控制項。每個控制項在標準中都有相同的控制項 ID。當您開啟合併的控制項發現項目時，即使控制項套用至多個已啟用的標準，您也會收到每個安全性檢查的單一搜尋結果。	2023 年 2 月 23 日

新的安全控制	下列新的 Security Hub 控制項可用。某些控制項具有地區限制。 • the section called “[ElastiCache.1] ElastiCache Redis 叢集應啟用自動備份” • the section called “[ElastiCache.2] Redis 緩存集群應啟 ElastiCache 用自 auto 次要版本升級” • the section called “[ElastiCache.3] ElastiCache 對於 Redis 複製組應啟用自動故障轉移” • the section called “[ElastiCache.4] ElastiCache 對於 Redis 的複製組，應在靜態時加密” • the section called “[ElastiCache.5] ElastiCache 對於 Redis 的複製組應在傳輸過程中進行加密” • the section called “[ElastiCache.6] ElastiCache 對於 6.0 版之前的 Redis 複製組應使用 Redis 的 AUTH” • the section called “[ElastiCache.7] ElastiCache 叢集不應使用預設子網路群組”	2023 年 2 月 16 日

新增 ASFF 欄位	Security Hub 已添加 ProductFields。 ArchivalReasons：0 /說明和。 ProductFields ArchivalReasons:0/ ReasonCode 轉換為 AWS 安全性發現格式 (ASFF)。	2023 年 2 月 8 日
新增 ASFF 欄位	Security Hub 已新增合規性。 AssociatedStandards 和合規性。 SecurityControlId 到「 AWS 安全性發現格式」(ASFF)。	2023 年 1 月 31 日
漏洞詳細信息現已可	您現在可以在 Security Hub 主控台中查看弱點詳細資訊，瞭解 Amazon Inspector 傳送至 Security Hub 的發現項目。	2023年1月14日
Security Hub 在中東（阿拉伯聯合大公國）可用	Security Hub 現已在中東 (阿拉伯聯合大公國) 推出。某些控制項具有地區限制。	2023 年 1 月 12 日
添加了第三方集成 MetricStream	Security Hub 現在支援與中國和 AWS GovCloud (US). 以外 MetricStream的所有區域進行第三方整合。	2023 年 1 月 11 日
增加組織帳戶限制	Security Hub 現在支援每個區域的每個 Security Hub 系統管理員帳戶最多 11,000 個成員帳戶。	2022 年 12 月 27 日
ElasticBeanstalk.3 回滾	安全中心回滾控制 [ElasticBeanstalk.3] Elastic Beanstalk 應該將日誌 CloudWatch從所有區域的 FSBP 標準流式傳輸到。	2022 年 12 月 21 日

Security Hub 添加了新的安全控制	新的 Security Hub 控制項可供已啟用 FSBP 標準的客戶使用。某些控制項具有地區限制。	2022 年 12 月 15 日
即將推出的功能指引	Security Hub 計劃發行兩項新功能：合併控制項檢視與合併控制項發現項目。這些即將推出的功能可能會影響依賴控制項尋找欄位和值的現有工作流程。	2022 年 12 月 9 日
Amazon 安全湖集成現已推出	安全湖現在通過接收 Security Hub 發現與 Security Hub 集成。	2022 年 11 月 29 日
Support 服務管理標準： AWS Control Tower	Security Hub 支援稱為服務管理標準的新安全性標準： AWS Control Tower。 AWS Control Tower 管理此標準。	2022 年 11 月 28 日
獨聯體 AWS 基金會基準 v1.4.0 現已在中國地區推出	Security Hub 現在支持中國地區的 CIS AWS 基準測試 v1.4.0。	2022 年 11 月 18 日
Jira 服務管理雲端整合現已推出	Jira 服務管理雲端現在會在所有可用區域 (中國區域除外) 收到安全中心的發現項目。	2022 年 11 月 17 日
AWS IoT Device Defender 現已提供整合	AWS IoT Device Defender 現在會將發現項目傳送至所有可用區域的安全中心。	2022 年 11 月 17 日
Support 獨聯體 AWS 基準基準 v1.4.0	Security Hub 現在提供支持 CIS AWS 基準測試 v1.4.0 的安全控制。此標準適用於所有可用區域，中國地區除外。	2022 年 11 月 9 日

Support 安全中心公告 AWS GovCloud (US)	您現在可以使用 (美國東部) 和 AWS GovCloud (美國西部) 中的 Amazon 簡單通知服務 AWS GovCloud (Amazon SNS) 訂閱 Security Hub 公告，以接收有關安全中心的通知。	2022 年 10 月 3 日
AWS Security Hub 增加了一個新的安全控制	新的 Security Hub 控制項 AutoScaling.9 可供已啟用 FSBP 標準的客戶使用。控制項可能有地區限制。	2022 年 9 月 1 日
訂閱安 Security Hub 公告	您現在可以使用 Amazon Simple Notification Service (Amazon SNS) 訂閱 Security Hub 公告，以接收有關 Security Hub 的通知。	2022 年 8 月 29 日
跨區域彙總的區域擴充	跨區域彙總現在可用於發現項目、尋找更新和深入分 AWS GovCloud (US)析。	2022 年 8 月 2 日
新的第三方產品整合	Fortinet-FortiCnP 是接收 Security Hub 發現項目的協力廠商整合，而 JFrog 是將發現項目傳送至 Security Hub 的協力廠商整合。	2022 年 7 月 26 日
已退休	安全中心已淘汰 EC2.27-執行 EC2 執行個體不應使用金鑰配對，這是 AWS 基礎安全最佳做法 (FSBP) 標準中的先前控制項。	2022 年 7 月 20 日

Lambda .2 不再支持 python3.6	安全中心不再支援 python3.6 作為 Lamb da.2 的參數。2-Lambda 函數應該使用支援的執行階段，這是 AWS 基礎安全性最佳實務 (FSBP) 標準中的控制項。	2022 年 7 月 19 日
AWS Security Hub 添加了新的安全控制	新的 Security Hub 控制項可供已啟用 FSBP 標準的客戶使用。某些控制項具有地區限制。	2022 年 6 月 22 日
AWS Security Hub 支援新的區域	Security Hub 現已在亞太區域 (雅加達) 推出。此區域中無法使用某些控制項。	2022 年 6 月 7 日
改進了 AWS Security Hub 和之間的集成 AWS Config	Security Hub 使用者可以將 AWS Config 規則評估的結果視為安全中心中的發現項目。	2022 年 6 月 6 日
新增選擇退出自動啟用標準的功能	對於與之整合的使用者 AWS Organizations，此功能可讓您登入 Security Hub 系統管理員帳戶，並選擇不符合自動啟用標準的新成員帳戶。	2022 年 4 月 25 日
擴充的跨區域彙總	新增跨區域彙總以控制狀態和安全分數。	2022 年 4 月 20 日
CompanyName 並且現在 ProductName 是最上層屬性	增加了新的頂級屬性，用於設置與自定義集成相關的公司和產品名稱	2022 年 4 月 1 日
在 AWS 基礎安全性最佳做法標準中新增控制項	在「 AWS 基礎安全性最佳做法」標準中新增了 5 個新控制項。	2022 年 3 月 31 日

增加了新的資源詳細信息對象到 ASFF	已將AwsRdsDbSecurityGroup 資源類型新增至 ASFF。	2022 年 3 月 25 日
在 ASFF 中新增其他資源詳細資訊	新增了AwsAutoScalingScalingGroup 、、AwsElbLoadBalancer 和的其他詳細資訊AwsCodeBuildProject 。AwsRedshiftCluster	2022 年 3 月 25 日
在 AWS 基礎安全性最佳做法標準中新增控制項	在 AWS 基礎安全性最佳做法標準中新增 15 個新控制項。	2022 年 3 月 16 日
為 AWS 基礎安全性最佳做法標準和支付卡產業資料安全標準 (PCI DSS) 新增控制項	為 Amazon OpenSearch 服務，Amazon RDS，亞馬 Amazon EC2，Elastic Load Balancing 和 CloudFront AWS 基礎安全最佳實踐標準添加了新的控件。此外，PCI DSS 也新增了兩個新的 OpenSearch 服務控制項。	2022 年 2 月 15 日
為 ASFF 增加了新的欄位	增加了新的領域：樣品。	2022 年 1 月 26 日
增加了集成 AWS Health	AWS Health 使用 service-to-service 事件訊息將發現項目傳送至 Security Hub。	2022年1月19日
增加了集成 AWS Trusted Advisor	Trusted Advisor 將其檢查結果作為 Security Hub 的發現發現發現發現發送到 Security Hub。Security Hub 會將其 AWS 基礎安全性最佳做法檢查的結果傳送至。 Trusted Advisor	2022 年 1 月 18 日

更新 ASFF 中的資源詳細資訊物件	新增了 `MixedInstancesPolicy` 和 `AvailabilityZones` 至 `AwsAutoScalingAutoScalingGroup` 。已新增 `MetadataOptions` 到 `AwsAutoScalingLaunchConfiguration` 。已新增 `BucketVersioningConfiguration` 到 `AwsS3Bucket` 。	2021 年 12 月 20 日
對於 ASFF 文檔更新輸出	ASFF 屬性的描述先前在單一主題中。每個頂層物件和每個資源詳細資料物件現在都位於其自己的主題中。ASFF 語法主題包含這些主題的連結。	2021 年 12 月 20 日
已將新的資源詳細資訊物件新增至 ASFF AWS Network Firewall	針對 AWS Network Firewall，已新增下列資源詳細資訊物件：`AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` 、和`AwsNetworkFirewallRuleGroup` 。	2021 年 12 月 20 日
增加了對 Amazon Inspector 的新版本的支持	Security Hub 與 Amazon Inspector 查器的新版本以及與亞 Amazon Inspector 經典集成。Amazon Inspector 將發現發送到 Security Hub。	2021 年 11 月 29 日
改變了 EC2.19 的嚴重性	EC2.19 (安全群組不應允許不受限制地存取高風險連接埠) 的嚴重性從「高」變更為「重大」。	2021 年 11 月 17 日

新的整合 Sonrai Dig	Security Hub 現在提供與Sonrai Dig. Sonrai Dig監控雲端環境以識別安全風險。 Sonrai Dig將發現項目傳送至 Security Hub。	2021 年 11 月 12 日
更新了 CIS 2.1 和 CloudTrail .1 控件的檢查	除了檢查至少有一個多區域 CloudTrail 軌跡之外，CIS 2.1 和 CloudTrail .1 現在還要檢查至少一個多區域 CloudTrail 軌跡中的`ExcludeManagementEventSources` 參數是否為空。	2021 年 11 月 9 日
增加了對 VPC 端點的支持	Security Hub 現已整合 AWS PrivateLink 並支援 VPC 端點。	2021 年 11 月 3 日
將控制項新增至 AWS 基礎安全性最佳做法標準	增加了 Elastic Load Balancing（ELB.2 和 ELB.8）和（SSM.4）的新控制項。 AWS Systems Manager	2021 年 11 月 2 日
為 EC2.19 控制項的檢查新增連接埠	EC2.19 現在也會檢查安全性群組是否不允許不受限制的輸入存取下列連接埠：3000 (Go、Node.js 和 Ruby 網頁開發架構)、5000 (Python 網頁開發架構)、8088 (舊版 HTTP 連接埠) 和 8888 (替代 HTTP 連接埠)	2021 年 10 月 27 日

添加了與 LOGZ.IO 雲 SIEM 的集成	Logz.io 是 Cloud SIEM 的供應商，提供日誌和事件數據的高級關聯性，以幫助安全團隊實時檢測，分析和響應安全威脅。Logz.io 從 Security Hub 接收發現項目。	2021 年 10 月 25 日
增加了對發現項目跨區域彙總的支援	跨區域彙總可讓您檢視所有發現項目，而不必變更「區域」。管理員帳戶選擇彙總區域和連結的區域。管理員帳戶及其成員帳戶的搜尋結果會從連結的區域彙總至彙總區域。	2021 年 10 月 20 日
更新 ASFF 中的資源詳細資訊物件	將檢視器憑證詳細資料新增至 AwsCloudFrontDistribution 已新增其他詳細資訊至AwsCodeBuildProject 。已將負載平衡器屬性新增至AwsElbV2LoadBalancer 。已將 S3 儲存貯體擁有者帳戶識別碼新增至AwsS3Bucket 。	2021 年 10 月 8 日
新增資源詳細資訊物件至 ASFF	已將下列新資源詳細資訊物件新增至 ASFF：AwsEc2VpcEndpointService ,AwsEcrRepository ,AwsEksCluster ,,AwsOpenSearchServiceDomain ,,AwsWafRateBasedRule , AwsWafRegionalRateBasedRule AwsXrayEncryptionConfig	2021 年 10 月 8 日

從 Lambda.2 控件中刪除不推薦使用的運行時	在 AWS 基礎安全性最佳實務標準中，從 [Lambda.2] Lambda 函數中移除**dotnetcore2.1** 執行階段應該使用支援的執行階段。	2021 年 10 月 6 日
檢查點集成的新名稱	與檢查點圓頂 9 弧的集成現在是檢查點 CloudGuard 姿勢管理。整合 ARN 沒有變更。	2021 年 10 月 1 日
刪除了與阿爾西德的集成	與艾爾西德 K審計的集成已停止。	2021 年 9 月 30 日
改變了 EC2.19 的嚴重性	[EC2.19] 安全性群組的嚴重性不應允許不受限制地存取具有高風險的連接埠，從「中」變更為「高」。	2021 年 9 月 30 日
中國地區 AWS Organizations 目前支援與整合	現在，中國（北京）和中國（寧夏）支持與 Organizations 的安全中心集成。	2021 年 9 月 20 日
S3.1 和 PCI.S3.6 控制項的新 AWS Config 規則	S3.1 和 PCI.S3.6 都會確認已啟用 Amazon S3 區塊公開存取設定。這些控制項的 AWS Config 規則會從變更`s3-account-level-public-access-blocks` 為`s3-account-level-public-access-blocks-periodic` 。	2021 年 9 月 14 日
從 Lambda.2 控件中刪除了不推薦使用的運行時	在 AWS 基礎安全性最佳實務標準中，從 [Lambda.2] Lambda 函數移除`nodejs10.x` 和`ruby2.5`執行階段應該使用支援的執行階段。	2021 年 9 月 13 日

改變了 CIS 2.2 控制的嚴重性	在 CIS AWS 基準基準標準中，2.2 的嚴重性。— 確定已啟用 CloudTrail 記錄檔驗證已從 [低] 變更為 [中]。	2021 年 9 月 13 日
更新了基礎安全性最佳做法標準中的 ECS.1、Lambda 達 2 和 SSM.1 AWS	在「 AWS 基礎安全性最佳作法」標準中，ECS.1 現在具有設定為的`SkipInactiveTaskDefinitions` 參數。`true`這可確保控制項僅檢查作用中的工作定義。對於 Lambda 2，將 Python 3.9 添加到運行時列表中。SSM.1 現在會檢查已停止和執行中的執行個體。	2021 年 9 月 7 日
控制項現在會排除 Lambda @Edge 資源	在支付卡產業資料安全標準 (PCI DSS) 標準中，PCI.Lambda.2 控制項現在不包括 Lambda @Edge 資源。	2021 年 9 月 7 日
添加了集成 HackerOne Vulnerability Intelligence	Security Hub 現在提供與HackerOne Vulnerability Intelligence. 整合會將發現項目傳送至 Security Hub。	2021 年 9 月 7 日
更新 ASFF 中的資源詳細資訊物件	對於`AwsKmsKey` ，已新增`KeyRotationStatus` 。針對`AwsS3Bucket` 、已新增`AccessControlList` `BucketLoggingConfiguration` `BucketNotificationConfiguration` 、、和`BucketWebsiteConfiguration` 。	2021 年 9 月 2 日

新增資源詳細資訊物件至 ASFF	已將下列新資源詳細資訊物件新增至 ASFF: `AwsAutoScalingLaunchConfiguration` `AwsEc2VpnConnection` 、和`AwsEcrContainerImage` 。	2021 年 9 月 2 日
在 ASFF 中新增`Vulnerabilities` 物件的詳細資訊	中`Cvss`、已新增`Adjustments` 和`Source`。在中`VulnerablePackages` ，新增了檔案路徑和套件管理員。	2021 年 9 月 2 日
中國地區現已支援系統管理員總管和 OpsCenter 整合	安全中心與 SSM Explorer 整合，現 OpsCenter 已在中國（北京）和中國（寧夏）提供支援。	2021 年 8 月 31 日
退休 Lambda .4 控制項	Security Hub 正在淘汰控制項 [Lambda.4] Lambda 函數應該已設定無效字母佇列。當控制項停用時，該控制項將不再顯示在主控台上，而且 Security Hub 不會對該控制項執行檢查。	2021 年 8 月 31 日
淘汰 PCI 控制項	Security Hub 正在淘汰控制項 [PCI.EC2.3] 應移除未使用的 EC2 安全群組。當控制項停用時，該控制項將不再顯示在主控台上，而且 Security Hub 不會對該控制項執行檢查。	2021 年 8 月 27 日

變更 Security Hub 將發現項目傳送至自訂動作的方式	當您將發現項目傳送至自訂動作時，Security Hub 現在會在個別Security Hub Findings - Custom Action事件中傳送每個發現項目。	2021 年 8 月 20 日
為自訂 Lambda 執行階段新增了新的合規狀態原因代碼	新增新的LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE 合規性狀態原因代碼。此原因代碼表示 Security Hub 無法針對自訂 Lambda 執行階段執行檢查。	2021 年 8 月 20 日
AWS Firewall Manager 中國地區現已支援整合	現在，中國（北京）和中國（寧夏）支持與 Firewall Manager 器集成的安全中心。	2021 年 8 月 19 日
與和的新整Caveonix Cloud合 Forcepoint Cloud Security Gateway	Security Hub 現在提供與Caveonix Cloud和的整合Forcepoint Cloud Security Gateway。這兩種整合都會將發現項目傳送 Security Hub	2021 年 8 月 10 日
在 ASFF 中加入了新CompanyName 的ProductName 、和Region屬性	在 ASFF 的最上層新增CompanyName ProductName 、和Region欄位。這些欄位會自動填入，除了自訂產品整合外，無法使用BatchImportFindings 或更新BatchUpdateFindings 。在主控台上，尋找篩選器會使用這些新欄位。在 API 中，CompanyName 和ProductName 篩選器會使用下的屬性ProductFields 。	2021 年 7 月 23 日

在 ASFF 中新增和更新資源詳細資訊物件	添加了新的AwsRdsEventSubscription 資源類型和資源詳細信息。已新增資源類型的資AwsEcsService 源詳細資料。已將屬性新增至資AwsElasticsearchDomain 源詳細資訊物件。	2021 年 7 月 23 日
將控制項新增至 AWS 基礎安全性最佳做法標準	為 Amazon API Gateway（Apigateway .5），Amazon EC2（EC2.19），Amazon ECS（ECS2），Elastic Load Balancing（ELB.7），Amazon OpenSearch 服務（.5 到 .8），Amazon RDS（RDS.16 到 RDS.23），亞馬遜 Redshift（紅移）和 Amazon SQS .1。	2021 年 7 月 20 日
在服務連結角色受管理原則中移動權限	移動受管理策略內的 config:PutEvaluations 權限AWSSecurityHubServiceRolePolicy ，以便將其套用至所有資源。	2021 年 7 月 14 日
將控制項新增至 AWS 基礎安全性最佳做法標準	為 Amazon API Gateway（4），Amazon（. CloudFront 5 和 CloudFront .6），Amazon EC2 CloudFront （EC2.17 和 EC2.18），Amazon ECS（ECS1），Amazon OpenSearch 服務（4），（IAM.21），亞馬遜 RDS（RDS.15）和 Amazon S3（S3.8）添加了新的控制。 AWS Identity and Access Management	2021 年 7 月 8 日

新增控制項發現項目的合規狀態原因代碼	INTERNAL_SERVICE_ERROR 表示發生未知的錯誤。 SNS_TOPIC_CROSS_ACCOUNT 表示 SNS 主題由不同帳戶擁有。 SNS_TOPIC_INVALID 表示相關聯的 SNS 主題無效。	2021 年 7 月 6 日
添加了集成 AWS Chatbot	添加了集成 AWS Chatbot. Security Hub 將發現項目傳送至 AWS Chatbot.	2021 年 6 月 30 日
新增服務連結角色受管理原則的權限	已新增受管理原則的新權限，AWSSecurityHubServiceRolePolicy 以允許服務連結角色傳遞評估結果給 AWS Config。	2021 年 6 月 29 日
ASFF 中新增與更新的資源詳細資訊物件	新增 ECS 叢集和 ECS 任務定義的新資源詳細資料物件。更新 EC2 執行個體物件以列出相關聯的網路界面。已新增 API Gateway V2 階段的用戶端憑證識別碼。已新增 S3 儲存貯體的生命週期組態。	2021 年 6 月 24 日
更新彙總控制狀態和標準安全分數的計算	Security Hub 現在每 24 小時計算一次整體控制狀態和標準安全分數。對於管理員帳戶，分數現在會反映每個帳戶是否啟用或停用每個控制項。	2021 年 6 月 23 日
更新有關 Security Hub 處理暫停帳戶的資訊	已新增有關安 Security Hub 如何處理中暫停之帳戶的資訊 AWS。	2021 年 6 月 23 日

添加了選項卡以顯示單個管理員帳戶的已啟用和禁用的控件	對於管理員帳戶，標準詳細資料頁面上的主要索引標籤包含跨帳號的彙總資訊。新的 [為此帳號啟用] 和 [為此帳號停用] 索引標籤會列出針對個別管理員帳號啟用或停用的帳號。	2021 年 6 月 23 日
已新增java8.al2 至的參數Lambda.2	在 AWS 基礎安全性最佳做法標準中，已新增java8.al2 至控制項支援的執行階段。Lambda.2	2021 年 6 月 8 日
與 MicroFocus ArcSight 網童軍網絡調查員的新集成	添加了 MicroFocus ArcSight 與網童軍網絡調查員的集成。 MicroFocus ArcSight 從 Security Hub 接收發現項目。NETSCOUT 網絡調查員發送調查結果到 Security Hub。	2021 年 6 月 7 日
已新增詳細資訊 AWSSecurityHubServiceRolePolicy	已更新受管理策略區段AWSSecurityHubServiceRolePolicy ，以新增由 Security Hub 服務連結角色使用的現有受管理策略的詳細資料。	2021 年 6 月 4 日
與 Jira 服務管理的新整合	Jira 的 AWS 服務管理連接器會將發現項目傳送給 Jira，並使用它們來建立 Jira 問題。當 Jira 問題更新時，資訊安全中心中的對應發現項目也會更新。	2021 年 5 月 26 日

更新了亞太區域 (大阪) 地區支援的控制清單	更新了 CIS AWS 基金會標準和支付卡產業資料安全標準 (PCI DSS)，以指出亞太區域 (大阪) 不支援的控制項。	2021 年 5 月 21 日
與雲端安全系統整合的新功能	為雲添加了與 Sysdig 安全的集成。整合會將發現項目傳送至 Security Hub。	2021 年 5 月 14 日
將控制項新增至 AWS 基礎安全性最佳做法標準	添加了新的控制 Amazon API Gateway（阿比蓋特 2 和 3），AWS CloudTrail（CloudTrail.4 和 CloudTrail .5），Amazon EC2（EC2.15 和 EC2.16），（ElasticBeanstalk1 和 ElasticBeanstalk .2），AWS Elastic Beanstalk（Lambda .4），Amazon RDS AWS Lambda（RDS.12-RDS.14），亞馬遜 Redshift（紅移。 AWS Secrets Manager SecretsManager SecretsManager AWS WAF	2021 年 5 月 10 日
更新 GuardDuty 和 Amazon RDS 控制	將嚴重性PCI.GuardDuty.1 從「中」變更為「高」。GuardDuty.1 已將databaseEngines 參數新增至RDS.8。	2021 年 5 月 4 日
新增資源詳細資訊至 ASFF	在中Resources.Details ，為亞馬遜 EC2 網絡 ACL，亞馬遜 EC2 子網絡和 AWS Elastic Beanstalk 環境添加了新的資源詳細信息對象。	2021 年 5 月 3 日

新增主控台欄位以提供 Amazon EventBridge 規則的篩選器值	Security Hub EventBridge 規則的新預先定義篩選器模式提供可用來指定篩選器值的主控台欄位。	2021 年 4 月 30 日
添加了與 AWS Systems Manager 資源管理器和集成 OpsCenter	Security Hub 現在支持與系統管理器資源管理器和 OpsCenter. 整合會從 Security Hub 接收發現項目，並更新安全中心中的發現項目。	2021 年 4 月 26 日
產品整合的新類型	新的整合類型表示產品整合會更新從 Security Hub 接收到的發現項目。`UPDATE_FINDINGS_IN_SECURITY_HUB`	2021 年 4 月 22 日
已將「主帳戶」一詞變更為「管理員帳戶」。	「主帳戶」一詞變更為「管理員帳戶」。Security Hub 主控台和 API 中的術語也會變更。	2021 年 4 月 22 日
更新了網絡套接字。1 替換 HTTP	更新了 Apigateway 的標題、說明和補救措施。控制項現在會檢查 Websocket API 執行記錄，而非 HTTP API 執行記錄。	2021 年 4 月 9 日
現已在北京和寧夏支援 Amazon GuardDuty 整合	中國 (北京) 和中國 (寧夏) 區域現已支援與 GuardDuty 安全中心整合。	2021 年 4 月 5 日
已新增`nodejs14.x` 至 Lambda.2 控制項支援的執行階段	基礎安全性最佳做法標準中的 Lambda.2 控制項現在支援執行階段。`nodejs14.x`	2021 年 3 月 30 日
在亞太地區（大阪）啟動 Security Hub	亞太區域 (大阪) 區域現已推出 Security Hub。	2021 年 3 月 29 日

已新增尋找提供者欄位以尋找詳細	在發現項目詳細資料面板上，新的「尋找提供者欄位」區段包含尋找可信度、重要性、相關發現項目、嚴重性和類型的提供者值。	2021 年 3 月 24 日
增加了從 Amazon Macie 接收敏感發現的選項	與 Macie 的整合現在可以設定為將敏感發現項目傳送至 Security Hub。	2021 年 3 月 23 日
轉換 AWS Organizations 為帳戶管理	對於擁有成員帳戶的現有管理員帳戶的客戶，請新增有關如何透過邀請管理帳戶變更為使用 Organizations 管理帳戶的新資訊。	2021 年 3 月 22 日
ASFF 中的新物件，瞭解 Amazon S3 公用存取區塊組態的相關資訊	在中`Resources` ，新的`AwsS3AccountPublicAccessBlock` 資源類型和詳細資料物件提供有關帳戶 Amazon S3 公用存取區塊組態的資訊。在`AwsS3Bucket` 資源詳細資料物件中，`PublicAccessBlockConfiguration` 物件提供 S3 儲存貯體的公用存取區塊組態。	2021 年 3 月 18 日

ASFF 中的新物件，可讓尋找提供者更新特定欄位	在中使用 ASFF 中的新FindingProviderFields 物件BatchImportFindings 來提供Confidence 、、Criticality RelatedFindings Severity、和Types的值。原始欄位只能使用更新BatchUpdateFindings 。	2021 年 3 月 18 日
ASFF DataClassification 中資源的新物件	ASFF 中的新Resources.DataClassification 物件可用來提供資源上偵測到之機密資料的相關資訊。	2021 年 3 月 18 日
為可用的合規狀態代碼增加CONFIG_RETURNS_NOT_APPLICABLE 價值	對於NOT_AVAILABLE 符合性狀態，請移除原因代碼RESOURCE_NO_LONGER_EXISTS 並新增原因代碼CONFIG_RETURNS_NOT_APPLICABLE 。	2021 年 3 月 16 日
用於與之整合的新受管政策 AWS Organizations	新的受管理原則AWSSecurityHubOrganizations Access 會提供組織管理帳戶和委派 Security Hub 系統管理員帳戶所需的組織權限。	2021 年 3 月 15 日
受管理策略和服務連結的角色資訊已移至「安全性」章節	有關受管理策略的資訊會進行修訂和擴充。受管理策略資訊和服務連結角色的資訊都已移至「安全性」一章。	2021 年 3 月 15 日

與 SecureCloud數據庫的新集成	將 SecureCloud DB 添加到第三方集成列表中。 SecureCloudDB 是一種雲端原生資料庫安全性工具，可提供內部和外部安全性姿勢和活動的全面可見性。 SecureCloudDB 將發現發送到 Security Hub。	2021 年 3 月 4 日
獨聯體 1.1 和獨聯體 3.1 的嚴重性修訂-獨聯體 3.14 控制	獨聯體 1.1 和獨聯體 3.1-獨聯體 3.14 控制的嚴重性更改為低。	2021 年 3 月 3 日
移除了 RDS.11 控制項	從基礎安全性最佳做法標準中移除 RDS.11 控制項。	2021 年 3 月 3 日
更新了多寶集成	Turbot 整合已更新，以傳送和接收發現結果。	2021 年 2 月 26 日
在基礎安全性最佳做法標準中新增控制項	添加了 Amazon API Gateway（Apigateway 1），Amazon EC2（EC2.9 和 EC2.10），Amazon Elastic File System（EFS.2），Amazon OpenSearch 服務（ES.2 和 ES.3），Elastic Load Balancing（ELB.6）和（ ）（KMS.3）的新控件。 AWS Key Management Service AWS KMS	2021 年 2 月 11 日
在 DescribeProducts API 中添加了可選的ProductArn 過濾器	DescribeProducts API 作業現在包含選用ProductArn 參數。此ProductArn 參數可用來識別要傳回詳細資訊的特定產品整合。	2021 年 2 月 3 日

透過雲端儲存安全與 Amazon S3 防毒軟體的全新整合	與 Amazon S3 防毒軟體的整合會將病毒掃描結果傳送到 Security Hub，做為發現結果。	2021 年 1 月 27 日
更新管理員帳戶的安全分數計算程序	對於系統管理員帳戶，Security Hub 會使用不同的程序來計算安全分數。新程序可確保分數包含針對成員帳戶啟用但針對管理員帳戶停用的控制項。	2021 年 1 月 21 日
ASFF 中的新字段和對象	已新增`Action`物件，以追蹤針對資源發生的動作。新增欄位至`AwsEc2NetworkInterface` 物件以追蹤 DNS 名稱和 IP 位址。已將新`AwsSsmPatchCompliance` 物件新增至資源詳細資訊。	2021 年 1 月 21 日
在基礎安全性最佳做法標準中新增控制項	為 Amazon CloudFront （1 到 CloudFront .4），Amazon DynamoDB（動態 B CloudFront .1 通過動態 B.1），Elastic Load Balancing （ELB.3 到 ELB.5），Amazon RDS（RDS.9 到 RDS.11），Amazon Redshift（紅移 1 通過紅移 3 和紅傳 6）和亞馬遜（SNS）添加了新的控制。	2021 年 1 月 15 日

工作流程狀態會根據記錄狀態或規範遵循狀態重設	如果已存檔的搜尋結NEW果啟動，NOTIFIED或RESOLVED尋找項目的符合性狀態從、或變更為、或，Security Hub 會自動將工作流程狀態從PASSED或重設為NOT_AVAILABLE 。FAILED WARNING這些變更表示需要進行額外的調查。	2021 年 1 月 7 日
新增控制項型發現項目的ProductFields 資訊	針對從控制項產生的發現項目，以 AWS 安全性發現項目格式 (ASFF) 新增有關ProductFields 物件內容的資訊。	2020 年 12 月 29 日
受管理見解的更新	更改了洞察力 5 的標題。新增 32 個新洞察，可檢查存在可疑活動的 IAM 使用者。	2020 年 12 月 22 日
IAM.7 和 Lambda 圖 1 控制項的更新	在「 AWS 基礎安全性最佳做法」標準中，更新了 IAM.7 的參數。更新了 Lambda 1 的標題和說明。	2020 年 12 月 22 日
擴大與 ServiceNow ITSM 的整合	ServiceNow ITSM 整合可讓使用者在收到資 Security Hub 發現項目時自動建立事件或問題。這些事件或問題的更新會導致 Security Hub 中的發現項目更新。	2020 年 12 月 11 日
與 AWS Audit Manager 的新整合	Security Hub 現在提供與 AWS Audit Manager 的整合。此整合可讓 Audit Manager 從資訊 Security Hub 接收控制項型發現項目。	2020 年 12 月 8 日

與 Aqua 安全 Kube-bench 的新集成	Security Hub 添加了與 Aqua 安全 Kube-bench 的集成。整合會將發現項目傳送至 Security Hub。	2020 年 11 月 24 日
雲端託管服務現已在中國地區推出	與雲託管的整合現已在中國（北京）和中國（寧夏）地區推出。	2020 年 11 月 24 日
BatchImportFindings 現在可以用來更新其他欄位	之前，您無法使用BatchImportFindings 來更新Confidence Criticality 、RelatedFindings 、Severity、和Types欄位。現在，如果這些欄位尚未由更新BatchUpdateFindings ，則可以透過更新它們BatchImportFindings 。一旦更新它們BatchUpdateFindings ，就無法由更新BatchImportFindings 。	2020 年 11 月 24 日
Security Hub 現已與 AWS Organizations	客戶現在可以使用其組 Organizations 帳戶設定來管理成員帳戶。組織管理帳戶會指定 Security Hub 系統管理員帳戶，該帳戶會決定要在 Security Hub 中啟用哪些組織帳戶。手動邀請程序仍可用於不屬於組織的帳戶。	2020 年 11 月 23 日
刪除了高音量控件的單獨查找列表格式	當有大量發現項目時，控制項的發現項目清單不再使用「發現項目」頁面格式。	2020 年 11 月 19 日

新的和更新的第三方集成	Security Hub 現在支持與雲計算機的集成, 3 核安全, 探險者, 和庫伯尼特安全. StackRox IBM QRadar 不再傳送發現項目。它只接收發現。	2020 年 10 月 30 日
添加了從控件詳細信息頁面下載發現結果列表的選項。	在控制項詳細資料頁面上，新的 [下載] 選項可讓您將尋找清單下載至 .csv 檔案。下載的清單會遵守清單上的任何篩選條件。如果您選取特定發現項目，則下載的清單只會包含這些發現項目。	2020 年 10 月 26 日
增加了從標準詳細信息頁面下載控件列表的選項。	在標準詳細資料頁面上，新的 [下載] 選項可讓您將控制清單下載至 .csv 檔案。下載的清單會遵守清單上的任何篩選條件。如果您選取特定控制項，則下載的清單只會包含該控制項。	2020 年 10 月 26 日
全新和更新的合作夥伴整	Security Hub 現已與 ThreatModeler. 已更新下列合作夥伴整合，以反映其新產品名稱。扭鎖企業版現在是帕洛阿爾托網絡-Prisma 雲計算。同樣來自帕洛阿爾托網絡，Demisto 現在是皮質 XSOAR 和紅鎖現在是 Prisma 雲企業。	2020 年 10 月 23 日
Security Hub 在中國（北京）和中國（寧夏）成立	Security Hub 現已在中國 (北京) 和中國 (寧夏) 區域推出。	2020 年 10 月 21 日

修訂 ASFF 屬性和第三方整合的格式	ASFF 屬性和合作夥伴整合清單現在使用以清單為基礎的格式而非表格。ASFF 語法、屬性和類型分類現在位於不同的主題中。	2020 年 10 月 15 日
重新設計標準細節頁	已啟用標準的標準的標準明細頁面現在會顯示控制項的索引標籤式清單。標籤會根據控制項狀態篩選控制項清單。	2020 年 10 月 7 日
。替換 CloudWatch 事件。EventBridge	用 Amazon 替換了對 Amazon CloudWatch 活動的引用 EventBridge。	2020 年 10 月 1 日
與藍六角的新集成, 最佳 KAudit AWS, 和帕洛阿爾托網絡虛擬機系列.	Security Hub 現在集成了藍色六角形 AWS，Alcide KAudit 和帕洛阿爾托網絡虛擬機系列。藍色六角形 AWS 和 KAudit 將發現發現發送到 Security Hub。VM 系列會從安全中心接收發現項目。	2020 年 9 月 30 日

ASFF 中新增和更新的資源詳細資訊物件	已新增AwsApiGatewayRestApi 、、、AwsApiGatewayStage 、、AwsApiGatewayV2Api 、AwsApiGatewayV2Stage AwsCertificateManagerCertificate AwsElbLoadBalancer AwsIamGroup 、和的新Resources.Details 物件AwsRedshiftCluster 。 已新增AwsIamRole 和AwsIamAccessKey 物件的AwsCloudFrontDistribution 詳細資訊。	2020 年 9 月 30 日
ASFF 中資源的新ResourceRole 屬性，可追蹤資源是實行者還是目標。	資源的ResourceRole 屬性會指出資源是尋找活動的目標還是發現項目活動的執行者。有效值為 ACTOR 和 TARGET。	2020 年 9 月 30 日
新增 AWS Systems Manager 修補程式管理員至可用的 AWS 服務	AWS Systems Manager 修補程式管理員現在已與 Security Hub 整合。當客戶叢集中的執行個體不符合其修補程式合規標準時，修補程式管理員會將發現項目傳送至 Security Hub。	2020 年 9 月 22 日

在 AWS 基礎安全性最佳做法標準中新增控制項	為以下服務添加了新的控制：Amazon EC2（EC2.7 和 EC2.8），Amazon EMR（EMR），IAM（IAM.8），Amazon RDS（RDS.4 到 RDS.8），Amazon S3（S3.6）和（.1 和 .2）。AWS Secrets Manager SecretsManager SecretsManager	2020 年 9 月 15 日
IAM 政策用於控制BatchUpdateFindings 欄位存取權的新內容金鑰	現在可以將 IAM 政策設定為在使用時限制對欄位和欄位值的存取BatchUpdateFindings 。	2020 年 9 月 10 日
擴展BatchUpdateFindings 對成員帳戶的訪問	根據預設，成員帳戶現在擁有與管理員帳戶相同的存取權限。BatchUpdateFindings	2020 年 9 月 10 日
基礎安全性最佳做法標準 AWS KMS 中的新控制項	在基礎安全性最佳做法標準中新增兩個控制項 (KMS.1 和 KMS.2)。新的控制項可檢查 IAM 政策是否限制對解 AWS KMS 密動作的存取。	2020 年 9 月 9 日
已移除控制項的帳戶層級發現項目	Security Hub 不再產生控制項的帳戶層級發現項目。只會產生資源層級的發現項目。	2020 年 9 月 1 日
ASFF 中的新PatchSummary物件	已將PatchSummary 物件新增至 ASFF。此PatchSummary 物件會提供資源的修補程式符合性相關資訊 (相對於選取的相容性標準)。	2020 年 9 月 1 日

重新設計控制項詳情	控制項的詳細資料頁面已重新設計。控制項發現清單提供標籤，可讓您根據符合性狀態快速篩選清單。您也可以快速查看隱藏的發現項目。每個項目都可讓您存取有關搜尋結果資源、 AWS Config 規則及搜尋結果備註的其他詳細資訊。	2020 年 8 月 28 日
發現項目的新篩選選項	若要尋找篩選器，您可以使用 is not 篩選器來尋找欄位值不等於篩選器值的發現項目。您可以使用不 start in 來尋找欄位值不是以指定篩選器值開頭的發現項目。	2020 年 8 月 28 日
ASFF 中的新資源詳細資訊物件	已新增下列資源類型的新`Resources.Details` 物件：`AwsDynamoDbTable` `AwsEc2Eip` 、`AwsIamPolicy` 、`AwsIamUser` 、`AwsRdsDbCluster` 、、`AwsRdsDbClusterSnapshot` 、`AwsRdsDbSnapshot` 、`AwsSecretsManagerSecret`	2020 年 8 月 18 日
與 RSA 射手的新整合	Security Hub 現在與 RSA 射手集成。RSA 阿徹從 Security Hub 收到調查結果。	2020 年 8 月 18 日
「新描述」欄位 AwsKmsKey	已將`Description` 欄位新增至下的`AwsKmsKey` 物件`Resources.Details` 。	2020 年 8 月 18 日

已新增欄位至 AwsRdsDbInstance	已將數個屬性新增至下的`AwsRdsDbInstance` 物件`Resources.Details` 。	2020 年 8 月 18 日
更新 Security Hub 如何判斷控制項的整體狀態	對於沒有發現項目的控制項，狀態為 [無資料] 而非 [未知]。控制狀態包含科目層次與資源層次的搜尋結果。控制項狀態不會使用發現項目的工作流程狀態，除了忽略隱藏的發現項目。	2020 年 8 月 13 日
更新安 Security Hub 計算標準安全分數的方式	計算標準的安全分數時，Security Hub 現在會忽略狀態為「無資料」的控制項。安全分數是傳遞給已啟用控制項的控制項的比例，不包括沒有資料的控制項。	2020 年 8 月 13 日
在啟用的標準中自動啟用新控制項的新選項	添加了 「設置」 選項，以在已啟用的標準中自動啟用新控件。您也可以使用 `UpdateSecurityHubConfiguration` API 作業來設定此選項。	2020 年 7 月 31 日
支付卡產業資料安全標準 (PCI DSS) 標準的新控制	在 PCI DSS 標準中增加了新的控制項。新控制項的識別碼是 PCI.DM.1、PCI-2.5、PCI.EC2.6、PCI.ELBV2.1、PCI。 GuardDuty.1, PCI.IAM. 7, PCI.IAM. 8, PCI.S3.5, PCI. SageMaker 1、PCI.SSM.2 和 PCI.SSM.3 。	2020 年 7 月 29 日

基礎安全性最佳做法標準的全新和更新控制項	新增基礎安全性最佳作法標準的控制項。新控制項的識別碼為 AutoScaling .1、小型電腦 1、EC2.4、EC2.6、S3.5 和 SSM.3。更新 ACM.1 的標題，並將daysToExpiration 參數值變更為 30。	2020 年 7 月 29 日
ASFF 中的新Vulnerabilities 物件	已新增Vulnerabilities 物件，此物件提供與發現項目相關聯之弱點的相關資訊。	2020 年 7 月 1 日
適用於 Auto Scaling 群組、EC2 磁碟區和 EC2 VPC 的 ASFF 中的新Resource.Details 物件	已將AwsAutoScalingAutoScalingGroup AWSEc2Volume 、和AwsEc2Vpc 物件新增至Resource.Details 。	2020 年 7 月 1 日
ASFF 中的新NetworkPath 物件	已新增NetworkPath 物件，此物件提供與發現項目相關之網路路徑的相關資訊。	2020 年 7 月 1 日
自動解決發現Compliance.Status 項目 PASSED	對於來自控制項的發現項目PASSED，如果Compliance.Status 是，則 Security Hub 會自動設定Workflow.Status 為RESOLVED。	2020 年 6 月 24 日
AWS Command Line Interface 例子	已新增數個 Security Hub 工作的 AWS CLI 語法和範例。包括啟用 Security Hub、管理深入解析、管理標準和控制、管理產品整合，以及停用 Security Hub。	2020 年 6 月 24 日

ASFF 中的新Severity.Original 屬性	已新增 Severity.Original 屬性，這是尋找提供者的原始嚴重性。這會取代已取代的 Severity.Product 屬性。	2020 年 5 月 20 日
ASFF 中的新Compliance.StatusReasons 物件，以取得控制項狀態的詳細資訊	已新增 Compliance.StatusReasons 物件，可為控制項目前狀態提供其他內容。	2020 年 5 月 20 日
新的 AWS 基礎安全性最佳做法標準	新增新的 AWS 基礎安全性最佳做法標準，這是一組控制項，可偵測您部署的帳戶和資源何時偏離安全性最佳作法。	2020 年 4 月 22 日
用於更新發現項目的工作流程狀態的新主控台選項	新增使用 Security Hub 主控台或 API 來設定問題清單工作流程狀態的相關資訊。	2020 年 4 月 16 日
用於客戶更新發現的新 BatchUpdateFindings API	新增使用 BatchUpdateFindings 來更新與調查問題清單程序相關資訊的資訊。BatchUpdateFindings 已取代 UpdateFindings，後者已遭到取代。	2020 年 4 月 16 日
AWS 安全性發現格式 (ASFF) 的更新	新增了數個新的資源類型。新增了 Label 屬性到 Severity 物件。Label 的用途是取代 Normalized 欄位。新增了 Workflow 物件來追蹤調查問題清單的程序。Workflow 包含 Status 屬性，該屬性會取代現有的 Workflowstate 屬性。	2020 年 3 月 12 日

整合頁面的更新	更新以反映 Integrations (整合) 頁面的更新 針對每個整合，頁面現在會顯示整合類別，以及每個整合是否將發現項目傳送至 Security Hub 或從 Security Hub 接收發現項目。此頁面也會提供啟用各個整合所需進行的特定步驟。	2020 年 2 月 26 日
新的第三方產品整合	新增下列新產品整合：雲端託管人、 FireEye 螺旋、強制點 CASB、強制點 DLP、強制點 NGFW、機架空間雲端原生安全性和 Vectra.ai Cognito 偵測。	二零二零年二月21日
支付卡產業資料安全標準 (PCI DSS) 的新安全標準	新增支付卡產業資料安全標準 (PCI DSS) 的安全 Security Hub 安全標準。啟用此標準時，Security Hub 會針對與 PCI DSS 需求相關的控制項執行自動化檢查。	2020 年 2 月 13 日
AWS 安全性發現格式 (ASFF) 的更新	新增標準控制項相關需求的欄位。新增新的資源類型和新的資源詳細資訊。ASFF 現在也允許你提供最多 32 個資源。	2020 年 2 月 5 日
停用個別安全性標準控制項的新選項	新增如何控制是否啟用每個個別安全標準控制項的資訊。	2020 年 1 月 15 日
術語和概念的更新	更新一些描述並將新的詞彙新增至術語和概念。	二零一九年九月二十
AWS Security Hub 一般可用性發行	內容更新，以反映在預覽期間對 Security Hub 所做的改進。	2019 年 6 月 25 日

添加了 CIS AWS 基金會檢查的補救步驟	新增安全性中 Security Hub 支援的安全 AWS 性標準的補救步驟。	二○一九年四月十五
AWS Security Hub 的預覽版本	已發佈 AWS Security Hub 使用者指南的預覽版本。	二○一八年十一月十

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。