



AMS 進階概念和程序

AMS 進階使用者指南



版本 October 3, 2025

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMS 進階使用者指南: AMS 進階概念和程序

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標或商業外觀不得用於 Amazon 產品或服務之外的任何產品或服務，不得以可能在客戶中造成混淆的任何方式使用，不得以可能貶低或損毀 Amazon 名譽的任何方式使用。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

Table of Contents

什麼是 AWS Managed Services ?	1
關於本指南	2
營運計劃	2
加速營運計畫	2
進階操作計劃	2
入門	3
重要用語	3
服務描述	8
AWS Managed Services (AMS) AMS 進階操作計劃功能	8
我們做什麼、我們不做什麼	12
AMS 責任矩陣 (RACI)	13
AMS 環境基本元件	30
AMS 帳戶限制	33
AMS 服務水準目標 SLOs)	35
支援 AWS 的服務	36
支援的組態	38
不支援的作業系統	41
AMS 進階介面	41
VPC 端點	42
AMS 受保護的命名空間	43
AMS 預留字首	44
AMS 維護時段	45
AMS 資訊資源	46
AMS 合規	46
AMS 支援的合規標準	47
共同的責任	49
AMS Amazon Machine Image AMIs)	49
安全性增強AMIs	52
AD FS 和 AMS 之間的整合如何運作	53
AMS 受管 Active Directory	54
應用程式部署	56
服務管理	58
帳戶控管	58
服務開始	58

客戶關係管理 (CRM)	59
CRM 程序	60
CRM 會議	60
CRM 會議安排	61
CRM 每月報告	62
成本最佳化	63
成本最佳化架構	63
成本最佳化責任矩陣	65
服務時數	66
取得說明	66
規劃的事件管理	68
AMS PEM 條件	68
PEM 的類型	68
AMS PEM 程序	68
PEM FAQs	69
網路架構	70
MALZ 網路架構	70
關於多帳戶登陸區域網路架構	70
選擇單一 MALZ 或多個 MALZs	72
多帳戶登陸區域帳戶	75
SALZ 網路架構	103
AMS 單一帳戶登陸區域共用服務	104
設定 AMS	105
AMS 預設設定	105
DNS 解析預設值 (MALZ)	106
EC2 IAM 執行個體描述檔	106
AMS 中基準監控的提醒	113
日誌保留和輪換預設值	127
使用 AMS 主控台	128
使用 AMS API 和 CLI	129
REST 呼叫的 AMS API HTTP 端點	129
安裝或升級 AMS CLI	130
在 CLI、Ruby、Python 和 Java 中使用 AMS API	131
AMS 自備 EPS	140
為您的帳戶開啟 BYOEPS	141
接收 AMS 通知	144

使用 SNS 的 AMS AMI 通知	145
服務通知	148
RFC 狀態變更通知	148
設定私有和公有 DNS	152
AMS 輸出流量管理	153
部署 IAM 資源	154
自動化 IAM 佈建	155
使用 IAM 角色和設定檔設定許可	171
請求新的 IAM 使用者角色或執行個體描述檔	171
使用 IAM 角色政策陳述式限制許可	171
使用 Amazon EC2 IAM 執行個體描述檔限制許可	173
AD FS 宣告規則和 SAML 設定	173
ADFS 宣告規則組態	173
Web 主控台	174
使用 SAML 存取 API 和 CLI	174
限制使用網路 ACL	178
Outpost 上的 AMS	178
AWS Outposts 安裝和操作管理	178
在 上佈建 AMS 受管資源 AWS Outposts	181
AMS 在 上的限制 AWS Outposts	181
AWS Outposts 合規的 AMS	182
AMS AWS Outposts FAQs	183
使用標籤	184
AMS 基礎設施自動標記	186
AMS 建議的標籤	187
標記大量更新備註	190
資源排程器	192
部署資源排程器	192
自訂資源排程器	193
使用資源排程器	194
AMS 資源排程器成本估算器	194
AMS Resource Scheduler 最佳實務	195
AWS Systems Manager 在 AMS Advanced 中	197
可用的 AMS Advanced SSM 文件	197
AMS Advanced SSM 文件版本	197
Systems Manager 定價	198

離線 AMS 帳戶	198
從單一帳戶登陸區域帳戶離線	199
從多帳戶登陸區域帳戶離職	202
變更管理模式	217
模式概觀	218
AMS 中模式和帳戶的類型	218
AMS 模式和應用程式或工作負載	221
AMS 模式的真實使用案例	225
RFC 模式	228
了解 RFCs	228
什麼是變更類型？	260
故障診斷 RFC 錯誤	271
直接變更模式	279
直接變更模式入門	279
安全與合規	282
直接變更模式中的變更管理	285
使用直接變更模式建立堆疊	287
直接變更模式使用案例	290
開發人員模式	291
開發人員模式入門	292
安全與合規	294
變更管理	295
佈建基礎設施	300
偵測性控制	300
記錄、監控和事件管理	300
事件管理	300
修補管理	301
持續性管理	301
安全性和存取管理	301
AMS 中的自助式佈建模式	301
AMS 中的 SSP 模式入門	302
Amazon API Gateway	303
企業版 Alexa	303
Amazon AppStream 2.0	305
Amazon Athena	307
Amazon Bedrock	307

Amazon CloudSearch	308
Amazon CloudWatch Synthetics	309
Amazon Cognito	310
Amazon Comprehend	312
Amazon Connect	312
Amazon Data Firehose	314
Amazon DevOps Guru	315
Amazon DocumentDB (with MongoDB compatibility)	315
Amazon DynamoDB	316
Amazon Elastic Container Registry	317
EC2 Image Builder	318
上的 Amazon ECS AWS Fargate	320
上的 Amazon EKS AWS Fargate	322
Amazon EMR	324
Amazon EventBridge	327
Amazon Forecast	329
Amazon FSx	331
Amazon FSx for OpenZFS	332
Amazon FSx for NetApp ONTAP	333
Amazon Inspector Classic	334
Amazon Kendra	335
Amazon Kinesis Data Streams	336
Amazon Kinesis Video Streams	337
Amazon Lex	337
Amazon MQ	338
Amazon Managed Service for Apache Flink	339
Amazon Managed Streaming for Apache Kafka	340
Amazon Managed Service for Prometheus	341
Amazon Personalize	342
Amazon QuickSight	344
Amazon Rekognition	346
Amazon SageMaker AI	347
Amazon Simple Email Service	349
Amazon Simple Workflow Service	350
Amazon Textract	351
Amazon Transcribe	352

Amazon WorkSpaces	353
AMS 程式碼服務	354
AWS Amplify	357
AWS AppSync	358
AWS App Mesh	358
AWS Audit Manager	359
AWS Batch	360
AWS Certificate Manager	361
AWS Private Certificate Authority	362
AWS CloudEndure	365
AWS CloudHSM	366
AWS CodeBuild	367
AWS CodeCommit	368
AWS CodeDeploy	370
AWS CodePipeline	370
AWS Compute Optimizer	372
AWS DataSync	373
AWS Device Farm	374
AWS Elastic Disaster Recovery	375
AWS Elemental MediaConvert	376
AWS Elemental MediaLive	377
AWS Elemental MediaPackage	377
AWS Elemental MediaStore	378
AWS Elemental MediaTailor	379
AWS Global Accelerator	380
AWS Glue	380
AWS Lake Formation	382
AWS Lambda	383
AWS License Manager	384
AWS Migration Hub	385
AWS Outposts	385
AWS Resilience Hub	386
AWS Secrets Manager	387
AWS Security Hub	390
AWS Service Catalog AppRegistry	390
AWS Shield	391

AWS Snowball Edge	392
AWS Step Functions	393
AWS Systems Manager 參數存放區	394
AWS Systems Manager 自動化	395
AWS Transfer Family	397
AWS Transit Gateway	399
AWS WAF	399
AWS Well-Architected Tool	400
AWS X-Ray	401
VM Import/Export	402
客戶受管模式	403
Customer Managed 模式入門	403
AMS 和 AWS Service Catalog	403
Service Catalog 入門	404
開始之前，AMS 中的 Service Catalog	404
尋找您需要的資料 (SKMS)	408
什麼是服務知識管理？	408
尋找 VPC IDs	409
尋找子網路 IDs	411
尋找 AMI IDs	413
尋找安全群組 (SG) IDs	414
尋找 IAM 實體	415
尋找堆疊 IDs	415
尋找執行個體 IDs或 IP 地址	417
尋找 ARNs	419
依 ARN 尋找資源	421
尋找帳戶設定	422
尋找 FQDNs	423
尋找可用區域 (AZs)	424
尋找 SNS 主題	424
尋找備份設定	425
存取管理	426
什麼是 Access Management？	426
為什麼和何時存取您的帳戶	427
如何使用和何時使用根目錄	431
AMS Advanced 主控台和 Amazon EC2 存取	432

存取 AWS Management 主控台和 AMS 主控台	432
暫時 AMS 主控台存取	432
使用堡壘存取執行個體	433
DNS 易記堡壘名稱	435
節省單一帳戶登陸區域 (SALZ) 堡壘的成本	436
使用堡壘 IP 地址	436
執行個體存取範例	437
AMS 帳戶中以團隊或角色為基礎的存取控制	446
自動化 EC2 執行個體組態	447
自動化執行個體組態的先決條件	447
SSM Agent 自動安裝	448
先決條件	448
請求自動安裝 SSM Agent	449
SSM Agent 自動安裝的運作方式	449
自動化變更	449
在 Linux 執行個體上自動更新程式碼	450
在 Linux 執行個體上自動更新 PBIS	450
自動更新 SSM 和 CloudWatch 代理程式的最低版本	451
CloudWatch 組態檔案、更新詳細資訊	452
自動設定的日誌	453
監控和事件管理	455
什麼是監控？	456
AMS 監控系統監控什麼？	457
Active Directory Trust 的單一帳戶登陸區域主動監控	457
監控的運作方式	457
EC2 執行個體分組通知	458
標籤型提醒通知	459
檢視帳戶的監控組態	460
變更 帳戶的監控組態	460
AMS 中的應用程式感知事件通知	461
在您的 AMS 帳戶中佈建 AppRegistry 並建立應用程式	461
建立標籤以啟用案例擴充	461
為您的應用程式自訂 AMS 支援案例嚴重性	462
檢閱必要的許可	462
使用 OpsCenter	463
提醒通知	464

接收提醒	464
標籤型提醒通知	464
AMS 自動修復提醒	465
建立其他 CloudWatch 警示	472
建立自訂 CloudWatch 指標和警示	473
使用適用於 .Net 和 SQL 伺服器的 CloudWatch Application Insights	474
AMS 事件路由器	475
AMS 部署的 Amazon EventBridge 受管規則	475
建立 AMS 的受管規則	476
編輯 AMS 的受管規則	476
刪除 AMS 的受管規則	476
信任的修復程式	476
主要優點	476
可信任修復程式的運作方式	477
重要用語	477
開始使用信任的修復程式	478
支援的 Compute Optimizer 建議	481
支援的 Trusted Advisor 檢查	484
設定檢查修復	523
執行模式決策工作流程	526
設定修復教學課程	526
使用修復	528
修復日誌	532
最佳實務	535
常見問答集	535
日誌管理	537
什麼是日誌管理？	537
AMS 記錄的運作方式	537
存取您的日誌	537
AMS 彙總服務日誌	538
AMS 共用服務日誌	550
Amazon Elastic Compute Cloud (Amazon EC2) - 系統層級日誌	552
與 Splunk 整合	554
自訂您的日誌組態	554
更改 CloudWatch 日誌保留	554
啟用支援服務的記錄	555

安全管理	556
AMS 中的資料保護	556
Amazon Macie	557
GuardDuty	558
Amazon Route 53 Resolver DNS 防火牆	560
AWS Certificate Manager (ACM) 憑證	561
AMS 中的資料加密	562
身分與存取管理	563
多帳戶登陸區域 (MALZ) IAM 防護措施	563
使用身分驗證	564
安全事件記錄和監控	584
端點安全 (EPS)	584
惡意軟體緩解程序	588
Amazon Inspector 安全性	589
AMS 事件回應	591
法規遵循驗證	591
檢視您 合規狀態的多帳戶登陸區域 AWS Config 規則	592
AMS 多帳戶登陸區域服務控制政策限制	593
恢復能力	593
基礎架構安全	593
安全最佳實務	623
AMS 多帳戶登陸區域 EPS 非預設設定	623
AMS 護欄	623
MALZ Service 控制政策	624
安全事件回應	624
運作方式	624
準備	625
偵測	625
分析	626
包含	627
根除	628
復原	629
事件後報告	629
安全事件回應 Runbook	630
在 AMS Advanced 中變更請求安全性審查	634
客戶安全風險管理程序	635

AMS Advanced 技術標準	635
AMS Advanced 中的標準控制項	636
在您的環境中帶來高或極高安全風險的變更	655
持續性管理	658
什麼是持續性管理？	658
持續性管理的運作方式	658
備份計劃	658
備份文件庫	662
備份變更類型	663
監控和報告備份	664
災難復原回應	664
災難復原規劃	665
多站台或高可用性 (HA)	665
暖待命	666
指示燈	667
備份和還原	668
修補管理	673
AMS Patch Orchestrator：標籤型修補模型	674
使用修補程式協調器	675
Patch Orchestrator 先決條件	678
修補程式視窗	679
修補程式通知	680
修補基準	683
Patch Orchestrator 預留標籤	683
隨需修補	683
AMS 標準修補	683
支援的作業系統	684
支援的修補程式	685
修補和基礎設施設計	687
AMS 標準修補的運作方式	688
AMS 標準修補失敗	692
您可以在 AMS 標準修補中採取的動作	692
AMS 標準修補FAQs	695
修補服務承諾	697
標準修補	697
關鍵修補	698

報告和選項	702
隨需報告	702
AMS 修補程式報告	702
AMS 備份報告	710
防止和監控熱門發言者報告的事件	712
帳單費用詳細資訊報告	714
信任的修復程式報告	715
自助式報告	717
內部 API 操作	719
修補程式報告（每日）	722
備份報告（每日）	730
事件報告（每週）	733
帳單報告（每月）	736
彙總報告	738
AMS 自助式報告儀表板	740
資料保留政策	745
從 SSR 離職	746
取得支援	747
事件管理	747
什麼是事件管理？	748
事件管理服務承諾	749
事件管理範例	751
服務請求管理	756
何時使用服務請求	757
服務請求管理的運作方式	757
測試服務請求	758
建立服務請求	758
監控和更新服務請求	761
回應 AMS 產生的服務請求	762
帳單問題	762
隨需操作	763
隨需請求 AMS 操作	767
變更隨需操作方案	768
文件歷史紀錄	770
舊版更新	782
.....	dccvvi

什麼是 AWS Managed Services ?

歡迎使用 AWS Managed Services (AMS) , Amazon Web Services () 的基礎設施操作管理AWS。AMS 是一種企業服務，可提供 AWS 基礎設施的持續管理。

此使用者指南適用於 IT 和應用程式開發人員專業人員。假設對 IT 功能、聯網和應用程式部署術語和實務有基本的了解。

AMS 實作最佳實務並維護您的基礎設施，以減少營運開銷和風險。AMS 提供全生命週期服務來佈建、執行和支援您的基礎設施，並自動化常見的活動，例如變更請求、監控、修補程式管理、安全和備份服務。AMS 會強制執行您的公司和安全基礎設施政策，並可讓您使用偏好的開發方法開發解決方案和應用程式。

若要進一步了解 AMS 架構，請參閱[這些圖表](#)。

主題

- [關於此 AMS 使用者指南](#)
- [AMS 操作計劃](#)
- [AWS Managed Services 入門](#)
- [AMS 金鑰術語](#)
- [服務描述](#)
- [AMS 資訊資源](#)
- [AMS 合規](#)
- [AMS Amazon Machine Image AMIs\)](#)
- [AD FS 和 AMS 之間的整合如何運作](#)
- [AMS 受管 Active Directory](#)
- [AMS 應用程式部署](#)

Note

新 AWS 區域 會經常新增。如需最新 AMS 支援的作業系統 AWS 區域，以及最新的 AMS 支援的作業系統，請參閱 [支援的組態](#)。

若要進一步了解 AWS 區域，請參閱[管理 AWS 區域](#)。

AMS 致力於根據您的意見回饋持續改善我們的服務。我們使用多種機制來啟用您的自助式服務、自動化重複性任務，以及實作新 AWS 服務 和 功能。您可以隨時提交 AMS 服務請求，以建議新功能或功能改進。

AMS 營業時間為 24 小時，全年無休。

AMS 遵循一組 IT 服務管理 (ITSM) 實務，專注於使 IT 服務符合您業務需求。

關於此 AMS 使用者指南

此使用者指南適用於具有多帳戶或單一帳戶登陸區域的 AMS Advanced 客戶。如需 AMS 登陸區域方案的詳細資訊，請參閱 [AMS 金鑰術語](#)；另請參閱[多帳戶登陸區域架構](#)和[單一帳戶登陸區域架構](#)。

AMS 操作計劃

AWS Managed Services (AMS) 提供兩種操作計劃：AMS Accelerate 和 AMS Advanced。營運計劃提供一組特定的功能，並具有不同層級的服務、技術功能、需求、價格和限制。我們的營運計劃可讓您靈活地為每個 AWS 工作負載選擇適當大小的操作功能。本節概述功能和差異，以及與每個計劃相關的責任、功能和好處，以便您了解哪些操作計劃最適合您的帳戶。

如需兩個操作計劃的詳細功能比較，請參閱 [AWS Managed Services 功能](#)。

AMS Accelerate 操作計劃

AMS Accelerate 是 AMS 操作計劃，可協助您操作新環境或現有 AWS 環境的 day-to-day 基礎設施管理。AMS Accelerate 提供營運服務，例如監控、事件管理和安全性。AMS Accelerate 也為需要定期修補的 Amazon EC2 型工作負載提供選用的修補程式附加元件。

使用 AMS Accelerate，您可以決定 AWS 帳戶 您希望 AMS Accelerate 操作哪些區域、您希望 AMS Accelerate 操作的 AWS 區域、您需要的附加元件，以及您需要的服務層級協議 (SLAs)。如需詳細資訊，請參閱[使用 AMS Accelerate 操作計劃和服務描述](#)。

AMS 進階操作計劃

AMS Advanced 提供完整生命週期服務來佈建、執行和支援您的基礎設施。除了 AMS Accelerate 提供的操作服務之外，AMS Advanced 還包含其他服務，例如登陸區域管理、基礎設施變更和佈建、存取管理和端點安全。

AMS Advanced 會部署登陸區域，讓您遷移 AWS 工作負載並接收 AMS 操作服務。我們的受管多帳戶登陸區域已預先設定基礎設施，以促進身分驗證、安全性、聯網和記錄。

AMS Advanced 也包含變更和存取管理系統，可透過防止未經授權的存取或對 AWS 基礎設施實作風險變更來保護工作負載。客戶需要使用我們的變更管理系統來建立變更請求 (RFC)，以在 AMS Advanced 帳戶中實作大多數變更。您可以從由我們的安全與營運團隊預先審核的自動化變更程式庫建立 RFCs，或在 AMS Advanced 認為安全且支援時，請求由營運團隊審核和實作的手動變更。

AMS Advanced 也提供不同的 SLAs。如需詳細資訊，請參閱 [AWS Managed Services AMS Advanced 服務描述](#)。

AWS Managed Services 入門

如需多帳戶登陸區域 AMS 服務入門的詳細資訊，請參閱 [AWS Managed Services 入門簡介](#)。兩個入門指南提供服務和問題的說明，供您考慮以協助您開始使用。檢閱功能集 [AWS Managed Services 功能](#)，以及 [AWS Managed Services 資源](#) 中的目前資源。

AMS 金鑰術語

- AMS 進階：AMS 進階文件的「服務描述」一節中所述的服務。請參閱[服務描述](#)。
- AMS 進階帳戶：始終符合 AMS 進階加入要求中所有需求的 AWS 帳戶。如需 AMS Advanced 優點、案例研究以及聯絡銷售人員的資訊，請參閱 [AWS Managed Services](#)。
- AMS Accelerate Accounts：AWS 一直符合 AMS Accelerate Onboarding Requirements 中所有需求的帳戶。請參閱 [AMS Accelerate 入門](#)。
- AWS Managed Services：AMS 和 或 AMS Accelerate。
- AWS Managed Services 帳戶：AMS 帳戶和 或 AMS Accelerate 帳戶。
- 關鍵建議：AWS 透過服務請求發出的建議，通知您需要採取動作，以防止資源或的潛在風險或中斷 AWS 服務。如果您決定在指定日期之前不遵循關鍵建議，則需自行負責您的決定所造成的任何傷害。
- 客戶請求的組態：任何軟體、服務或其他未識別的組態：
 - 加速：[支援的組態](#)或 [AMS 加速；服務描述](#)。
 - AMS 進階：[支援的組態](#)或 [AMS 進階；服務描述](#)。
- 事件通訊：AMS 會與您通訊事件，或者您透過在 AMS Accelerate 支援中心和 AMS 主控台中建立的事件向 AMS 請求事件。AMS 加速主控台提供儀表板上的事件和服務請求摘要，以及支援中心的連結以取得詳細資訊。
- 受管環境：AMS 進階帳戶和 或由 AMS 操作的 AMS Accelerate 帳戶。

對於 AMS Advanced，這些包括多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) 帳戶。

- 帳單開始日期：的下一個工作日 AWS 會收到您在 AWS Managed Services 加入電子郵件中請求的資訊。AWS Managed Services 加入電子郵件是指 傳送給 AWS 您的電子郵件，以收集在帳戶中啟用 AWS Managed Services 所需的資訊。

對於您後續註冊的帳戶，帳單開始日期是 AWS Managed Services 為註冊帳戶傳送 AWS Managed Services 啟用通知後的第二天。AWS Managed Services 啟用通知會在下列情況發生：

1. 您授予相容 AWS 帳戶的存取權，並將其交給 AWS Managed Services。
 2. AWS Managed Services 設計並建置 AWS Managed Services 帳戶。
- 服務終止：您可以透過服務請求 AWS 提供至少 AWS Managed Services 30 天的通知，以終止所有 AWS Managed Services 帳戶的 AWS Managed Services 或指定 AWS Managed Services 帳戶的 AWS Managed Services。在服務終止日期，：
 1. AWS 視適用情況，將所有 AWS Managed Services 帳戶或指定 AWS Managed Services 帳戶的控制項交給您，或
 2. 適用時，各方會移除授予所有 AWS Managed Services 帳戶或指定 AWS Managed Services 帳戶 AWS 存取權 AWS Identity and Access Management 的角色。
 - 服務終止日期：服務終止日期是 30 天必要終止通知期間結束後日曆月的最後一天。如果必要的終止通知期間結束在日曆月的第 20 天之後，則服務終止日期是下一個日曆月的最後一天。以下是終止日期的範例案例。
 - 如果終止通知是在 4 月 12 日提供，則 30 天的通知會在 5 月 12 日結束。服務終止日期為 5 月 31 日。
 - 如果在 4 月 29 日提供終止通知，則 30 天的通知將於 5 月 29 日結束。服務終止日期為 6 月 30 日。
 - 您可用 AWS Managed Services : makes 的佈建，您可以從服務開始日期開始，存取和使用每個 AWS Managed Services 帳戶的 AWS Managed Services。AWS
 - 指定 AWS Managed Services 帳戶的終止：您可以透過服務請求 (「AWS Managed Services 帳戶終止請求」) 提供 AWS 通知，以基於任何原因終止指定 AWS Managed Services 帳戶的 AWS Managed Services。

事件管理術語：

- 事件：您的 AMS 環境中的變更。
- 警示：每當支援的事件 AWS 服務 超過閾值並觸發警示時，就會建立警示並傳送通知到您的聯絡人清單。此外，事件會在您的事件清單中建立。

- 事件：您的 AMS 環境或 AWS Managed Services 意外中斷或效能降低，導致 AWS Managed Services 或您回報的影響。
- 問題：一或多個事件的共用基礎根本原因。
- 事件解決或事件解決：
 - AMS 已將與該事件相關的所有無法使用 AMS 服務或資源還原為可用狀態，或
 - AMS 已判斷無法使用的堆疊或資源無法還原至可用狀態，或
 - AMS 已啟動您授權的基礎設施還原。
- 事件回應時間：建立事件以及 AMS 透過主控台、電子郵件、服務中心或電話提供初始回應之間的時間差異。
- 事件解決時間：AMS 或您建立事件與事件解決之間的時間差異。
- 事件優先順序：AMS 或您如何將事件的優先順序設定為低、中或高。
 - 低：AMS 服務的非關鍵問題。
 - 中：您受管環境中的 AWS 服務可用，但未如預期般執行（根據適用的服務描述）。
 - 高：(1) AMS 主控台或受管環境中的一或多個 AMS APIs 無法使用；或 (2) 受管環境中的一或多個 AMS 堆疊或資源無法使用，且無法使用可防止應用程式執行其功能。

AMS 可能會根據上述準則重新分類事件。

- 基礎設施還原：根據受影響的堆疊範本重新部署現有堆疊，並根據最後一個已知還原點啟動資料還原，除非您另有指定，否則無法解決事件。

基礎設施術語：

- 受管生產環境：客戶生產應用程式所在的客戶帳戶。
- 受管非生產環境：僅包含非生產應用程式的客戶帳戶，例如用於開發和測試的應用程式。
- AMS 堆疊：由 AMS 以單一單位管理的一或多個 AWS 資源群組。
- 不可變基礎設施：Amazon EC2 Auto Scaling 群組 (ASGs) 典型的基礎設施維護模型，其中針對每個部署替換了更新的基礎設施元件（在 AMI AWS 中），而不是就地更新。不可變基礎設施的優點是所有元件都會保持同步狀態，因為它們一律從相同的基礎產生。抗擾性與建置 AMI 的任何工具或工作流程無關。
- 互斥基礎設施：典型的基礎設施維護模型，適用於非 Amazon EC2 Auto Scaling 群組且包含單一執行個體或僅包含少數執行個體的堆疊。此模型最緊密地代表傳統的硬體型系統部署，其中系統會在生命週期開始時部署，然後隨著時間的推移，更新會分層到該系統上。系統的任何更新都會個別套用到執行個體，並可能因應用程式或系統重新啟動而導致系統停機（取決於堆疊組態）。

- 安全群組：執行個體的虛擬防火牆，用於控制傳入和傳出流量。安全群組會在執行個體層級執行，而非子網路層級。因此，VPC 中子網路中的每個執行個體可以指派不同的安全群組集。
- 服務水準協議 (SLAs)：與您簽訂 AMS 合約的一部分，定義預期的服務水準。
- SLA 無法使用和無法使用：
 - 您提交的 API 請求會導致錯誤。
 - 您提交的主控台請求導致 5xx HTTP 回應（伺服器無法執行請求）。
 - 在 AMS 受管基礎設施中構成堆疊或資源的任何 AWS 服務方案都處於「服務中斷」狀態，如[服務運作狀態儀表板](#)所示。
 - 在判斷服務點數的資格時，不會考慮直接或間接由 AMS 排除造成的無法使用。除非符合無法使用的條件，否則服務會被視為可用。
- 服務水準目標 (SLOs)：與您簽訂的一部分 AMS 合約，可定義 AMS 服務的特定服務目標。

修補詞彙：

- 強制性修補程式：重大安全性更新，以解決可能危及環境或帳戶安全狀態的問題。「重大安全性更新」是 AMS 支援之作業系統廠商評定為「重大」的安全性更新。
- 發佈的修補程式與發佈的修補程式：修補程式通常安排程發佈和發佈。緊急修補程式會在發現需要修補程式時宣佈，通常在修補程式發佈後不久宣佈。
- 修補程式附加元件：針對利用 AWS Systems Manager (SSM) 功能的 AMS 執行個體進行標籤型修補，讓您可以標記執行個體，並使用您設定的基準和視窗修補這些執行個體。
- 修補程式方法：
 - 就地修補：透過變更現有執行個體來完成的修補。
 - AMI 取代修補：透過變更現有 EC2 Auto Scaling 群組啟動組態的 AMI 參考參數來完成的修補。
- 修補程式提供者 (OS 廠商、第三方)：修補程式是由廠商或應用程式管理內文提供。
- 修補程式類型：
 - Critical Security Update (CSU)：受支援作業系統廠商評定為「Critical」的安全性更新。
 - 重要更新 (IU)：由受支援作業系統的廠商評定為「重要」或非安全性更新評定為「關鍵」的安全性更新。
 - 其他更新 (OU)：廠商對非 CSU 或 IU 之受支援作業系統的更新。
- 支援的修補程式：AMS 支援作業系統層級修補程式。廠商會釋出升級，以修正安全漏洞或其他錯誤，或改善效能。如需目前支援的 OSs 清單，請參閱[支援組態](#)。

安全術語：

- **Detective Controls**：由 AMS 建立或啟用的監控程式庫，可針對不符合安全、操作或客戶控制的組態持續監督客戶受管環境和工作負載，並透過通知擁有者、主動修改或終止資源來採取行動。

服務請求條款：

- **服務請求**：您希望 AMS 代表您採取之動作的請求。
- **提醒通知**：觸發 AMS 提醒時，AMS 發佈到您的服務請求清單頁面的通知。為您的帳戶設定的聯絡人也會透過設定的方法（例如電子郵件）收到通知。如果您的執行個體/資源上有聯絡人標籤，並且已同意雲端服務交付管理員 (CSDM) 以標籤為基礎的通知，則標籤中的聯絡資訊（金鑰值）也會收到自動 AMS 提醒的通知。
- **服務通知**：AMS 發佈到服務請求清單頁面的通知。

其他詞彙：

- **AWS Managed Services 介面**：適用於 AMS：AWS Managed Services 進階主控台、AMS CM API 和支援 API。對於 AMS Accelerate：支援主控台和支援 API。
- **客戶滿意度 (CSAT)**：AMS CSAT 會收到深入分析的通知，包括提供每個案例或通訊的案例通訊評分、每季調查等。
- **DevOps**：DevOps 是一種開發方法，在所有步驟中都強烈倡導自動化和監控。DevOps 的目標在於縮短開發週期、提高部署頻率，以及更可靠的版本，透過自動化的基礎，結合傳統上分開的開發和操作功能。當開發人員可以管理操作，並且操作通知開發時，問題和問題會更快地被發現和解決，而業務目標也更容易實現。
- **ITIL**：Information Technology Infrastructure Library（稱為 ITIL）是一種 ITSM 架構，旨在標準化 IT 服務的生命週期。ITIL 分為五個階段，涵蓋 IT 服務生命週期：服務策略、服務設計、服務轉換、服務操作和服務改進。
- **IT 服務管理 (ITSM)**：一組符合 IT 服務需求的實務。
- **受管監控服務 (MMS)**：AMS 會操作自己的監控系統 Managed Monitoring Service (MMS)，其會取用 AWS 運作狀態事件，並彙總 Amazon CloudWatch 資料和其他資料 AWS 服務，通知 AMS 運算子（線上全年無休）透過 Amazon Simple Notification Service (Amazon SNS) 主題建立的任何警示。
- **命名空間**：當您建立 IAM 政策或使用 Amazon Resource Name (ARNs) 時，您可以使用命名空間 AWS 服務來識別。您會在識別動作和資源時使用命名空間。

服務描述

AMS Advanced (AMS) 是 AWS Managed Services 服務的操作計劃，用於管理 AWS 基礎設施的操作。AMS Advanced 提供例行基礎設施操作，例如修補程式、持續性管理、安全管理和 IT 管理程序，例如事件、變更和服務請求管理。如需支援服務的清單，請參閱 [支援 AWS 的服務](#)。

YouTube 影片：[AMS 如何協助我在雲端中實現卓越營運？](#)

主題

- [AWS Managed Services \(AMS\) AMS 進階操作計劃功能](#)
- [我們做什麼、我們不做什麼](#)
- [AMS 責任矩陣 \(RACI\)](#)
- [AMS 環境基本元件](#)
- [AMS 帳戶限制](#)
- [AMS 服務水準目標 SLOs\)](#)
- [支援 AWS 的服務](#)
- [支援的組態](#)
- [AMS 中不支援作業系統的功能](#)
- [AMS 進階介面](#)
- [AMS VPC 端點](#)
- [AMS 受保護的命名空間](#)
- [AMS 預留字首](#)
- [AMS 維護時段](#)

AWS Managed Services (AMS) AMS 進階操作計劃功能

AMS Advanced 為支援的 AWS 服務提供下列功能：

- 記錄、監控、護欄和事件管理：

AMS 會設定和監控受管環境的記錄活動，並根據各種運作狀態檢查定義提醒。AMS 會調查適用 AWS 服務的提醒，而對這些服務的使用產生負面影響的提醒會導致事件的建立。AMS 會彙總和儲存因 CloudWatch、CloudTrail 和 Amazon S3 中系統日誌中的所有操作所產生的所有日誌。您可以要求設定其他提醒。除了 AMS 的預防性控制之外，AMS 部署組態防護機制和偵測性控制，以持續保

護您免受可能降低受管帳戶操作和安全性完整性的錯誤組態，進而強制執行您的控制，例如標記和合規。當偵測到受監控的控制項時，會產生警示，根據您可以修改的預先定義 AMS 預設值，導致資源的通知、修改或終止。

- 持續性管理（備份和還原）：

AMS 會根據您決定的排程間隔，使用標準的現有 AWS Backup 功能提供資源備份。AMS 可以使用 RFC 從特定快照執行還原動作。快照間隔之間發生的資料變更是您備份的責任。您可以在排程間隔之外提交 RFC 以進行備份或快照請求。在 AWS 區域中無法使用可用區域 (AZ) 的情況下，AMS 會在您的許可下，根據受影響的堆疊的範本和可用的 EBS 快照重新建立新的堆疊，以還原受管環境。

- 安全性和存取管理：

AMS 提供端點安全性 (EPS)，例如設定防毒和反惡意軟體保護。您也可以使用自己的 EPS 工具和程序，不使用 AMS for EPS 使用稱為自有 EPS (BYOEPS) 的功能。AMS 也會設定您在加入期間核准的預設 AWS 安全功能，例如 AWS Identity and Access Management (IAM) 角色和 Amazon EC2 安全群組，並使用標準 AWS 工具（例如 AWS Security Hub Amazon Macie、Amazon GuardDuty）來監控和回應安全問題。您可以透過您提供的已核准目錄服務來管理您的使用者。如需核准的目錄服務清單，請參閱 [支援的組態](#)。

AMS 包含端點安全 (EPS)，其中包含防毒 (AV) 和反惡意軟體保護、惡意軟體和入侵偵測 (Trend Micro)。安全群組是根據堆疊範本定義，並在啟動時根據應用程式（公有/私有）安全群組的可見性進行修改。

透過變更管理變更請求 (RFCs) 請求存取系統。存取管理可讓您存取不同的資源，例如 Amazon EC2 執行個體 AWS Management Console、和 APIs。在加入和聯合至 AWS 期間與 AMS Microsoft Active Directory 部署建立單向信任之後，您可以使用現有的公司登入資料進行所有互動。

- 修補程式管理：

AMS 會針對支援的作業系統 (OSs) 和預先安裝支援的作業系統的軟體，套用並安裝 EC2 執行個體的更新。如需支援的作業系統清單，請參閱 [支援的組態](#)。

AMS 提供兩種用於修補的模型：

- 傳統帳戶型修補的 AMS 標準修補程式，以及
- AMS Patch Orchestrator，用於標籤型修補。

在 AMS 標準修補程式中，您可以選擇每月維護時段，讓 AMS 執行大多數修補活動。AMS 會在選取的維護時段之外（使用適當的通知）套用重要的安全性更新，並在選取的維護時段期間套用重要的更新。AMS 還會在選取的維護時段將更新套用至基礎設施管理工具。您可以視需要從修補程式管理中排除堆疊或拒絕更新。

使用 AMS Patch Orchestrator，每個帳戶的預設維護時段由您定義，以便 AMS 執行修補活動。您可以為 AMS 排程額外的自訂維護時段，以使用標籤修補您定義的一組特定執行個體。AMS 會套用所有可用的更新，但您可以透過建立自訂修補程式基準來篩選或拒絕更新。對於這兩種模型，如果您核准或拒絕修補程式管理下提供的更新，但之後改變主意，則需負責透過 RFC 啟動更新。AMS 會追蹤資源的修補程式狀態，並在每月業務審查中反白不是最新的系統。修補程式管理僅限於受管環境中的堆疊，包括所有 AMS 受管應用程式和支援具有修補功能的 AWS 服務（例如 RDS）。為了在更新發佈時支援所有類型的基礎設施組態，AMS a) 會更新 EC2 執行個體，b) 提供更新的 AMS AMI 供您使用。您有責任安裝、設定、修補和監控上述未特別涵蓋的任何其他應用程式。

- 變更管理：

AMS 變更管理是您控制受管環境中變更的機制。AMS 使用預防性和偵測性控制的組合來促進此程序，並根據選取的 AMS 模式提供不同層級的控制和相關聯的風險。

AMS 環境中的所有動作都會登入 AWS CloudTrail。

如需 AMS 變更管理和不同模式的詳細資訊，請參閱 [AMS 變更管理指南](#) 和 [AMS 模式](#)。

- 自動化和自助式佈建管理：

您可以在 AMS Advanced 上以多種方式佈建 AWS 資源：

- 提交佈建和組態變更請求 (RFCs)
- 透過 AWS Service Catalog 部署
- 透過[直接變更模式](#)部署
- 透過[開發人員模式](#)部署。請記住，透過開發人員模式建立的資源不是由 AMS 管理。
- 針對 select AWS 服務 使用自助式佈建直接設定 AWS 服務（請參閱 [支援 AWS 的服務](#)）。

- 事件管理：

AMS 會主動通知您 AMS 偵測到的事件。AMS 會回應客戶提交和 AMS 產生的事件，並根據事件優先順序解決事件。除非另有指示，否則 AMS 判斷對您受管環境的安全有風險的事件，以及與 AMS 和其他 AWS 服務可用性相關的事件，都會主動採取行動。一旦收到您的授權，AMS 就會對所有其他事件採取動作。問題管理程序會處理週期性事件。

- 問題管理：

AMS 執行趨勢分析以識別和調查問題，並識別根本原因。問題可透過解決方法或永久解決方案來修復，以防止未來再次發生類似的服務影響。解決後，可能會針對任何「高」事件請求事件後報告 (PIR)。PIR 會擷取根本原因和採取的預防性動作，包括實作預防性措施。

- 報告：

AMS 為您提供每月服務報告，摘要 AMS 的關鍵績效指標，包括執行摘要和洞察、營運指標、受管資源、AMS 服務水準協議 (SLA) 合規性，以及有關支出、節省和成本最佳化的財務指標。報告是由指派給您的 AMS 雲端服務交付管理員 (CSDM) 交付。

- 服務請求管理：

若要請求受管環境、AMS AWS 或服務產品的相關資訊，請使用 AMS 主控台提交服務請求。您可以提交「如何」服務與功能相關問題 AWS 的服務請求，或請求其他 AMS 服務。

- 服務台：

AMS 為全職 Amazon 員工提供工程操作，以滿足非自動化的請求，包括事件管理、服務請求管理和變更管理。服務台全年無休運作。

- 指定的資源：

每個客戶都會獲指派 Cloud Service Delivery Manager (CSDM) 和 Cloud Architect (CA)。

- 您可以直接聯絡 CSDMs。他們在實作、遷移和營運生命週期的所有階段執行服務審查，以及交付報告和洞察。CSDMs 會每月執行業務審查，並詳細說明財務支出、節省成本的建議、服務使用率和風險報告等項目。他們深入探討營運效能統計資料，並提供改善領域的建議。
- 您可以直接聯絡 CAs 並提供技術專業知識，協助您最佳化 AWS 雲端的使用。範例 CA 活動包括選取遷移的工作負載、協助加入其他帳戶和工作負載、擔任操作活動的技術主管，例如遊戲日、災難復原測試、問題管理和技術建議，以充分利用 AMS 和 AWS。CAs 會在組織的各個層級推動技術討論，並協助事件管理、進行權衡、建立最佳實務和技術風險緩解。
- 開發人員模式：

此功能可讓您除了存取 AMS 變更管理程序之外，還允許直接存取 AWS 服務 APIs 和 AWS 主控台，以快速迭代 AMS 設定帳戶【1】內的基礎設施設計和部署。在變更管理程序之外使用開發人員模式許可佈建或設定的資源是您管理的責任（請參閱「自動化和自助式佈建管理」）。透過 AMS 變更管理程序佈建的資源受到支援，就像 AMS 上其他變更管理佈建的工作負載一樣。

- AWS 支援：

AMS 客戶可以選擇其補充 AMS 營運計畫所需的 AWS Support 層級。在 AMS 中註冊的帳戶可以訂閱商業支援或企業支援。若要了解 Support Plans 的差異，請參閱 [AWS Support Plans](#)。

- 客戶受管帳戶：

此功能可讓您在相同的受管環境中請求 AWS 帳戶，但工作負載和這些帳戶中 AWS 資源的持續操作是您的責任。AMS 會佈建客戶受管帳戶，但一旦帳戶建立，就不會將其他 AMS 功能或服務提供

給這些帳戶。AWS 不會在企業級進階支援中註冊客戶受管帳戶。您有責任以您選擇的支援費率在 AWS 支援中註冊客戶受管帳戶。

- 防火牆管理：

AMS 為支援的防火牆服務提供選用的受管防火牆解決方案，可針對受管環境中的網路啟用網際網路繫結輸出流量篩選。這不包括未使用 AWS 網路基礎設施且其流量直接進入網際網路的公有服務。此解決方案結合了領先業界的防火牆技術與 AMS 基礎設施管理功能，以部署、監控、管理、擴展和還原防火牆基礎設施。

加入 AMS 時，您會收到 AMS 網路基礎設施的完整清單。若要隨時取得執行以支援 AMS 基礎設施的更新服務清單，請提交服務請求，其中包含您想要的資訊的詳細資訊。若要請求變更網路設計，請建立描述您要進行之變更的服務請求，例如新增 VPC 或請求安全群組規則變更。

我們做什麼、我們不做什麼

AMS 為您提供了部署 AWS 基礎設施的標準化方法，並提供必要的持續營運管理。如需角色、責任和支援服務的完整描述，請參閱[服務描述](#)。

Note

若要請求 AMS 提供額外的 AWS 服務，請提交服務請求。如需詳細資訊，請參閱[提出服務請求](#)。

- 我們做什麼：

完成加入後，AMS 環境即可接收變更 (RFCs)、事件和服務請求。您與 AMS 服務的互動圍繞應用程式堆疊的生命週期進行。新堆疊是從預先設定的範本清單排序，啟動到特定的虛擬私有雲端 (VPC) 子網路，在操作生命週期內透過請求變更 (RFCs) 進行修改，並全年無休監控事件和事件。

AMS 會監控和維護作用中的應用程式堆疊，包括修補，除非需要變更或停用堆疊，否則堆疊在堆疊生命週期內不需要進一步的動作。AMS 偵測到會影響堆疊運作狀態和功能的事件會產生通知，且可能需要或不需要您的動作來解決或驗證。方法問題和其他查詢可以透過提交服務請求提出。

此外，AMS 可讓您啟用非由 AMS 管理的相容 AWS 服務。如需 AWS-AMS 相容服務的資訊，請參閱[自助式佈建模式](#)。

- 我們不執行的動作：

雖然 AMS 透過提供許多手動和自動化選項來簡化應用程式部署，但您必須負責應用程式的開發、測試、更新和管理。AMS 為會影響應用程式的基礎設施問題提供故障診斷協助，但 AMS 無法存取或驗證您的應用程式組態。

AMS 責任矩陣 (RACI)

Note

為了及時履行其義務，AWS Managed Services (AMS) 可能需要您輸入以決定適當的行動方案。AMS 會聯絡指定的客戶聯絡人，以取得所有這類釐清和輸入。AMS 預期會在 24 個工作天內回應這類查詢。如果 24 個工作小時內沒有回覆，AMS 可能會代表您選擇動作。

AMS 負責、負責、諮詢和告知或 RACI，矩陣會將主要責任指派給客戶或 AMS 以進行各種活動。

AMS 會管理您的 AWS 基礎設施。下表提供客戶和 AMS 在 AMS 受管環境中執行之應用程式生命週期中活動的責任概觀。

AMS 不負責客戶受管帳戶或在其中執行的基礎設施的任何下列活動；因此，此 RACI 不適用。

- R 代表負責的一方，負責執行工作以達成任務。
- C 代表已諮詢的對象；尋求意見的對象，通常是主題專家；以及與之進行雙邊溝通的對象。
- 我代表知情的一方，通常是在任務完成或可交付項目時收到進度通知的一方。
- 自助式佈建是指客戶透過 AWS API 或主控台使用自助式佈建的資源，包括開發人員模式和自助式佈建服務。

Note

有些區段同時包含 AMS 和客戶的 'R'。這是因為在 AWS 共同責任模型中，AMS 和客戶都擁有共同所有權來回應基礎設施和應用程式問題。

為了提供自助式佈建功能，AMS 已建立具有許可界限的提升 IAM 角色，以限制來自直接 AWS 服務存取的意外變更。角色不會阻止所有變更，而且您有責任遵守內部控制、合規，並驗證使用的所有 AWS 服務是否符合必要的認證。我們將此稱為自助式佈建模式。如需 AWS 合規要求的詳細資訊，請參閱[AWS 合規](#)。

對於您透過自助服務佈建的資源，AMS 提供事件管理、偵測控制和防護機制、報告、指定資源 (Cloud Service Delivery Manager 和 Cloud Architect)、安全與存取，以及透過服務請求的技術支援。此外，在適用的情況下，您需為在 AMS 變更管理系統之外佈建或設定的資源承擔持續性管理、修補程式管理、基礎設施監控和變更管理的責任。

活動	客戶	AWS Managed Services (AMS)
應用程式生命週期		
應用程式開發	R	I
應用程式基礎設施需求分析和設計	R	C
非標準 AMS 堆疊的設計和最佳化	R	C
AMS 標準堆疊的設計和最佳化	I	R
應用程式部署	R	C
AWS 基礎設施部署	C	R
應用程式監控	R	I
應用程式測試/最佳化	R	I
AWS 基礎設施最佳化指引	I	R
AWS 基礎設施監控	I	R
疑難排解和解決應用程式問題	R	C
故障診斷和解決 AWS 網路問題	C	R
對作業系統和基礎設施問題進行故障診斷和解決	C	R
自助式佈建	R	C
應用程式和 ITSM 整合		

活動	客戶	AWS Managed Services (AMS)
應用程式與 AWS 服務方案整合	R	C
ITSM 與 AWS Managed Services Interface 整合	R	C
聯網		
受管環境 VPC 和 VPC 設定和組態	C	R
為 VPCs 配置私有地址空間 (例如 /16)	R	C
設定和操作非 AWS Managed Services、客戶受管 Firewalls/Proxy/Bastions/HOSTs	R	C
在受管環境中設定和操作 AWS 安全 Groups/NAT/Customer 堡壘/NACL	I	R
客戶網路內的聯網 (例如 DirectConnect) 組態和實作	R	C
受管環境中的網路組態和實作	C	R
受管環境組態		
定義基準堆疊範本的預設 Auto Scaling 設定	I	R
建議 RI 最佳化	C	R
購買 RI 和 PIOP 容量	R	C
當容量過度佈建時移除容量 (客戶應用程式支援時)	C	R
建立/更新 AWS Managed Services 的 AWS 客戶特定資訊	C	R

活動	客戶	AWS Managed Services (AMS)
S3 組態	C	R
自助式佈建	R	C
Glacier 組態	C	R
定義封存政策	R	C
封存政策組態	C	R
選取客戶維護時段	R	I
AWS RDS 管理		
監控source/replica/RO複寫運作狀態	I	R
識別來源容錯移轉的 RCA	I	R
自動化快照（ 備份 ） 組態	C	R
自助式佈建	R	C
協調和排程資料庫引擎修補程式管理	C	R
自助式佈建	R	C
建議資料庫儲存和 PIOP 容量	C	R
自助式佈建	R	C
建議執行中資料庫的執行個體大小	C	R
自助式佈建	R	C
建議受管環境的 RI 最佳化	C	R
自助式佈建	R	C

活動	客戶	AWS Managed Services (AMS)
RDS 效能監控 (CloudWatch)	C	R
自助式佈建	R	C
RDS 事件訂閱組態 (SNS)	C	R
自助式佈建	R	C
RDS 安全群組組態	C	R
自助式佈建	R	C
RDS 引擎參數/選項組態	R	C
資料庫資料表設計	R	I
資料庫索引	R	I
資料庫日誌分析	R	I
AMS 變更管理		
建立客戶 RFCs (例如，存取creating/updating/deleting受管堆疊的資源、部署/更新應用程式、變更 AWS 服務方案的組態)	R	I
核准客戶 RFCs	I	R
建立 AWS Managed Services RFCs (例如存取資源、代表客戶建立資源、將更新套用至作業系統，做為修補程式管理的一部分)	I	R
核准非自動化 RFCs	R	I
提交新變更類型的請求	R	C
建立新的變更類型	I	R

活動	客戶	AWS Managed Services (AMS)
應用程式變更行事曆的維護	R	C
即將到來的維護時段通知	I	R
AWS Service Catalog		
建立產品組合和產品	R	I
將產品分發給最終使用者	R	I
建立標籤和標籤選項程式庫	R	C
與最終使用者共用產品組合和產品	R	I
修訂/更新產品組合和產品	R	I
建立和指派限制給產品組合和產品	R	C
將服務動作與 產品建立關聯	R	C
使用新版產品更新佈建的資源	R	I
佈建		
AWS Managed Services 基準 AMI 的客戶特定新增項目	R	C
設定用於佈建堆疊範本的其他已核准變更類型	C	R
啟動透過 AMS 變更管理程序或 AWS Service Catalog 提交的受管 Stacks 和相關聯的 AWS 資源。	I	R
	R	I
自助式佈建		
在透過 AMS 變更管理程序或 AWS Service Catalog 佈建的執行個體上安裝/更新自訂和第三方應用程式。	R	I

活動	客戶	AWS Managed Services (AMS)
佈建 - 堆疊架構		
提供作業系統授權（包括適用 AWS 服務的使用費，例如 EC2 和 RDS）	I	R
	R	I
自助式佈建		
透過 AMS 變更管理系統定義應用程式部署的基準基礎設施範本（堆疊）。	I	R
	R	I
自助式佈建		
建立基準核准的 AMIs ⁸	I	R
評估客戶應用程式庫存，並判斷是否符合可用的基礎設施範本（堆疊）	R	C
定義除了基準範本產品之外的唯一 Stacks	R	C
記錄、監控和事件管理		
記錄 AWS 基礎設施變更日誌	I	R
記錄所有應用程式變更日誌	R	C
透過 AMS 變更管理程序佈建之 AWS 基礎設施的修補、安全性、監控等代理程式和指令碼的安裝和組態。	I	R
	R	C
自助式佈建		
定義客戶特定的監控和事件需求	R	C
設定受管環境的警示	I	R
監控所有 AMS 設定的提醒	I	R
自助式佈建	R	C

活動	客戶	AWS Managed Services (AMS)
調查事件通知的基礎設施提醒	I	R
自助式佈建	R	C
調查應用程式警示	R	C
事件管理		
根據監控主動通知 AWS 基礎設施上的事件	I	R
自助式佈建	R	C
處理應用程式效能問題和中斷	R	I
分類事件優先順序	I	R
提供事件回應	I	R
提供事件解決方案/基礎設施還原	C	R
 Note SLAs 不適用於在 AMS 變更管理之外佈建的執行個體型資源，包括使用自助式佈建和開發人員模式佈建的資源。		
問題管理		
識別受管環境中的問題	C	R
針對受管環境中的問題執行 RCA	C	R
修復受管環境中的問題	C	R
識別和修復應用程式問題	R	I
安全管理		

活動	客戶	AWS Managed Services (AMS)
客戶基礎設施安全性和/或在客戶加入期間確定和同意的安全合規程序基準。	C	R
	R	C
自助式佈建		
維護受管 EPS 的有效授權	R	C
設定受管 EPS	I	R
自助式佈建	R	C
更新受管 EPS	I	R
自助式佈建	R	C
在透過 AMS CM 程序佈建的執行個體上監控惡意軟體。	I	R
	R	C
自助式佈建		
維護和更新病毒簽章。	I	R
自助式佈建	R	C
修復受惡意軟體感染的執行個體。	C	R
自助式佈建	R	C
安全事件管理	C	R
安全性 - 存取管理		
管理使用者的生命週期及其本機目錄服務的許可，這些許可用於存取 AWS Managed Services	R	I
操作聯合身分驗證系統（為客戶存取 AWS 主控台/APIs）	R	C

活動	客戶	AWS Managed Services (AMS)
接受並維護從 AWS Managed Services AD 到客戶受管 AD 的 Active Directory (AD) 信任	R	C
在加入期間，在每個受管帳戶中建立跨帳戶 IAM 管理員角色	R	C
保護每個帳戶的 AWS 根登入資料	I	R
定義受管環境的 IAM 資源	C	R
管理 AMS 工程師作業系統存取的特權憑證	I	R
管理 AMS 提供給客戶的作業系統存取權限憑證	R	I
安全事件回應 - 準備		
通訊		
提供 AMS 在安全事件通知和安全呈報期間使用的客戶安全聯絡人詳細資訊	R	I
存放和管理提供的客戶安全聯絡人詳細資訊，以便在安全事件和安全呈報期間使用	CIS	R
訓練		
在事件回應程序期間為客戶提供支援 AMS 的文件	I	R
透過安全遊戲日在事件回應程序期間練習共同的責任	RI	RC
資源管理		
設定支援的 AWS 服務 警示、警示關聯性、降噪和其他規則的安全管理	I	R

活動	客戶	AWS Managed Services (AMS)
維護資產 (AWS 資源) 庫存，並了解資產的資產價值和重要性。此資訊在事件遏制策略期間很有幫助	R	CIS
使用 AWS 標籤來識別資源和工作負載	R	CIS
定義和設定日誌保留和封存	CIS	R
安全基準 AWS 帳戶、組態、政策和存取管理	CIS	RC
安全事件回應 - Detect		
記錄、指標和監控		
設定記錄和監控，以啟用執行個體和帳戶的事件管理	CIS	R
監控 AWS 服務 支援的安全提醒	I	R
部署和管理端點安全工具	CIS	R
使用 AMS 支援的端點安全工具監控執行個體上的惡意軟體	I	R
透過傳出訊息通知客戶偵測到的事件	I	R
針對特定帳戶和工作負載的決策者傳送通知和任何後續更新，以改善事件回應時間	R	CIS
定義、部署和維護 AMS 標準偵測服務 (例如 Amazon GuardDuty 和 AWS Config)	CIS	R
記錄 AWS 基礎設施變更日誌	I	RC
啟用和設定記錄、監控以啟用應用程式的事件管理	R	C

活動	客戶	AWS Managed Services (AMS)
在支援 AWS 的安全服務（例如 Amazon GuardDuty）上實作和維護允許清單、拒絕清單和自訂偵測	RCI	R
安全事件報告		
通知 AMS 可疑活動或作用中的安全調查	R	CIS
將偵測到的安全事件和事件通知客戶	I	R
通知可能觸發安全事件回應程序的計劃事件	R	CIS
安全事件回應 - 分析		
調查和分析		
對受支援偵測來源產生的受支援安全提醒執行初始回應	I	RC
使用可用資料評估 false/true 陽性	RI	RC
視需要產生要與客戶共用之受影響執行個體的快照	I	R
執行鑑識任務，例如監管鏈、檔案系統分析、記憶體鑑識和二進位分析	R	CIS
收集應用程式日誌以協助調查	R	I
收集資料和日誌，以協助調查安全提醒	RCI	RC
讓 中的SMEs AWS 服務 參與安全調查	CIS	R
在調查期間與第三方供應商互動（例如，針對 EPS 反惡意軟體調查和與 TrendMicro 支援團隊互動）	RCI	I

活動	客戶	AWS Managed Services (AMS)
在調查期間，將受支援的調查日誌分享 AWS 服務 給客戶	I	R
通訊		
從受管資源的 AMS 偵測來源傳送提醒和通知	I	R
管理應用程式安全事件的提醒和通知	R	I
在安全事件調查期間與客戶安全聯絡人互動	R	I
安全事件回應 - 包含		
遏制策略和執行		
決定執行商定的遏制策略，並同意可能會影響遏制時段內服務可用性的後果	R	CIS
備份受影響的系統以進行進一步分析	CIS	R
包含應用程式和工作負載（透過應用程式特定的組態或回應活動）	R	CIS
根據安全事件和受影響的資源定義遏制策略	CIS	R
啟用受影響系統時間點備份的加密和安全儲存	CIS	R
執行支援 AWS 的資源遏制動作，包括 EC2 執行個體、網路和 IAM	CIS	R
安全事件回應 - 根除		
根除策略和執行		
根據安全事件和客戶應用程式工作負載上受影響的資源來定義根除選項	R	CIS

活動	客戶	AWS Managed Services (AMS)
決定同意的根除策略、根除執行的時間，以及後果	R	CIS
根據 AMS 受管工作負載上的安全事件和受影響的資源定義根除步驟	CIS	R
根除和強化 AWS 資源，包括 EC2 執行個體、網路和 IAM 根除	CIS	R
消除和強化應用程式和工作負載（透過應用程式特定的組態或回應活動）	R	I
安全事件回應 - 復原		
復原準備和執行		
依客戶要求設定備份計劃和目標	R	I
檢閱備份計劃以還原 AMS 受管工作負載	CIS	R
針對支援的資源執行備份還原活動 AWS 服務	I	R
備份客戶應用程式、應用程式組態和部署設定，並檢閱備份計畫，以在事件發生後還原客戶應用程式和工作負載	R	I
還原應用程式和客戶工作負載（透過應用程式特定的還原步驟）	R	I
安全事件回應 – 事件後報告		
事件後報告		
視需要與客戶事後事件分享適當的經驗教訓和行動項目	I	R
修補程式管理 ⁹		

活動	客戶	AWS Managed Services (AMS)
監控 EC2 執行個體支援的作業系統和預先安裝之作業系統適用的更新。	I	R
	R	C
自助式佈建		
通知客戶即將進行的更新 (僅適用於 AMS 標準修補程式)	I	R
從修補活動排除特定更新和/或特定堆疊	R	I
定義預設和自訂維護時段排程和其他參數 (例如維護時段持續時間) 以套用修補程式 (適用於 AMS 修補程式 僅限協調器)	R	I
定義自訂修補程式基準以篩選和排除特定修補程式 (僅適用於 AMS Patch Orchestrator)	R	I
標記執行個體以將其與自訂維護時段和修補程式基準建立關聯 (僅適用於 AMS Patch Orchestrator)	R	I
追蹤資源的修補程式狀態，並在每月業務審核中反白非最新的系統。	C	R
修補 Windows 作業系統，以及安裝在受 Windows Update 管理之作業系統上的 Microsoft 套件	I	R
	R	-
自助式佈建		
修補程式安裝的應用程式、軟體或應用程式相依性不受 Windows Update 管理	R	I
	R	-
自助式佈建		

活動	客戶	AWS Managed Services (AMS)
修補 Linux 作業系統和作業系統原生套件管理員啟用管理的任何套件（例如 Yum、Apt、Zypper）	I	R
自助式佈建	R	-
修補程式安裝的應用程式、軟體或應用程式相依性，並非由 Linux 作業系統的原生套件管理員管理	R	I
自助式佈建	R	-
持續性管理		
指定備份排程	R	I
依排程執行備份。	I	R
自助式佈建	R	C
驗證備份	R	I
請求備份還原活動	R	I
執行備份還原活動。	I	R
自助式佈建	R	C
還原受影響的堆疊和 VPCs。	I	R
自助式佈建	R	C
還原受影響的自訂/第三方應用程式	R	C
報告		
準備和交付每月服務報告	I	R
上的 AMS AWS Outposts		

活動	客戶	AWS Managed Services (AMS)
	R	I
隨需設定和擷取 API 稽核歷史記錄 (CloudTrail)。	I	R
自助式佈建	R	I
透過 AWS Managed Services Interface 提供事件歷史記錄的存取權	I	R
透過 AWS Managed Services Interface 提供變更歷史記錄的存取權。	I	R
自助式佈建	N/A	N/A
服務請求管理		
使用服務請求請求資訊	R	I
回覆服務請求	I	R
受管防火牆		
請求部署 AMS 受管防火牆	R	I
AMS 受管防火牆架構的設計和最佳化	I	R
部署 AWS Infrastructure 和 AMS 受管防火牆設備	I	R
提供防火牆授權 (包括適用 AWS 服務的使用費 – 例如 EC2)	R	I
定義預設網域允許清單	I	R
請求新增、修改和刪除自訂允許清單和安全性政策	R	I

活動	客戶	AWS Managed Services (AMS)
設定 AMS 受管防火牆的警示	I	R
監控所有 AMS 受管防火牆設定的提醒	I	R
執行防火牆組態的備份	I	R
請求備份還原活動	R	I
使用新版產品更新佈建的資源	I	R
記錄 AMS 受管防火牆日誌	I	R
將日誌從 AMS 受管防火牆轉送至 CloudWatch	I	R
在 AMS 受管防火牆中請求組態變更	R	I
在 AMS 受管防火牆中核准組態變更	I	R
在 AMS 受管防火牆中執行組態變更	I	R

⁸AMS 僅提供 Amazon EC2 AMIs

⁹AMS 只有在客戶與 OSes 廠商簽署延長支援協議時，才會負責生命週期結束作業系統

AMS 環境基本元件

Multi-Account Landing Zone

這是核心帳戶中基礎設施元件和潛在成本的預估值。這不包括頻寬、CloudWatch 詳細監控、記錄、警示、Route53、Amazon S3、Simple Notification Service (Amazon SNS)、快照或預留 Amazon EC2 執行個體等其他成本。

您需為 AMS 受管 AWS 登陸區域基礎設施所需的元件付費。預估會將純 AMS 多帳戶登陸區域環境的成本設為每月 2,450 USD，而純應用程式帳戶則為 50 USD。

如需定價的資訊，請參閱 [AWS 定價](#)。

基本環境元件

元件	預估 費用	描述
管理帳戶	60 美元	AWS Organizations Management 帳戶； 會建立和財務管理成員帳戶。它包含 AWS 登陸區域 (ALZ) 架構、帳戶組態堆疊集和 AWS Organization 服務控制政策 SCPs)。 • Directory Service : 35 美元 • CloudTrail : 7 美元 • CloudWatch : 6 美元 • 其他 : \$12
共用服務帳戶	2000 美元	包含存取管理 (即 Active Directory)、端點安全管理 (Trend Micro) 和堡壘 (SSH/RDP) 所需的基礎設施和資源；估計每月 2400 美元。此預估不包含 Trend Micro 授權的成本。 • EC2 : 800 美元 (含最低堡壘數量) • RDS : 300 美元 (EPS) • VPC (端點) : 400 美元 • Directory Service : 300 美元 • CloudWatch : 100 美元 • GuardDuty : 15 美元 • Secrets Manager : 10 美元 • 資料傳輸 : 10 美元 • 組態 : 10 美元 • 其他 : 45 美元
網路帳戶	350 美元	AMS 帳戶、內部部署網路和輸出流量之間網路路由的中心中樞。此外， 包含公有 DMZ 堡壘 (AMS 工程師存取 AMS 環境中主機的進入點)。價格可能會根據周遊 Transit Gateway 和 Direct Connect 的流量而提高。 • EC2 : \$250 (基礎)

元件	預估 費用	描述
		• VPC : 80 美元 • 其他 : \$20
日誌封存帳戶	20 美元	包含來自每個 AMS 環境帳戶的 AWS CloudTrail 和 AWS Config 日誌檔案副本的 S3 儲存貯體。隨著收集更多日誌，成本會增加。 • S3 : 10 美元 • CloudWatch : 5 美元 • 其他 : \$5
安全帳戶	20 美元	安全相關操作的中心中樞，以及將通知和提醒漏接至 AMS 控制平面服務的主要點。此外，會存放 Amazon Guard Duty 管理帳戶。使用 Amazon GuardDuty 分析更多事件時，成本會增加。 • CloudWatch : 15 美元 • 其他 : \$5

Single-Account Landing Zone

下表列出範例 AMS 受管基礎設施的元件。

基本環境元件，上次更新日期：2020/07/09

名稱	執行個體類型	作業系統	元件數量	
mc-eps-dsm	m5.large	Linux	2	
mc-management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	

名稱	執行個體類型	作業系統	元件數量	
目錄服務	N/A	N/A		
其他元件	N/A	N/A		

如需定價的資訊，請參閱 [AWS 定價](#)。

AMS 帳戶限制

AMS 多帳戶登陸區域中有三種不同的限制類型：AMS API 限制、AMS 資源限制和 AWS 限制。

AMS 單一帳戶登陸區域中需要考慮兩種不同的限制類型：AMS API 限制和 AWS 限制。

AMS 帳戶 API 限制

本節說明帳戶層級限制，在此限制之後 AWS Managed Services (AMS) 會調節 AMS SKMS API 服務。這表示，如果您一秒呼叫任何列出的 APIs 超過 10 次，其中一個呼叫是「限流」（您會收到 `ThrottleException`）。在極少數情況下，外部或下游相依性可能會調節 AMS API，然後 AMS 可能會以可能較低的速率調節您的 API 呼叫。

Note

如需 AMS SKMS API 的資訊，請透過 AWS Artifact 主控台的報告索引標籤下載參考。

對於列出的每個 AMS SKMS API，操作會在 10 TPS 後調節（每秒交易數）：

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`
- `ListVpcSummaries`

AMS 多帳戶登陸區域帳戶資源限制

帳戶資源限制與 AMS 多帳戶登陸區域應用程式帳戶和 VPCs 和子網路相關。

應用程式帳戶資源限制

每個組織有 50 個應用程式帳戶的軟性限制。如果您有超過 50 個應用程式帳戶的使用案例，請聯絡您的雲端服務交付管理員 (CSDM) 來轉送您的需求。

VPCs 和子網路資源限制

在組織的預先定義 AWS 區域內，每個應用程式帳戶有 10 VPCs 的軟性限制。

每個 VPC 可能有 1 到 10 個私有子網路層，橫跨 2 到 3 個可用區域。此外，每個 VPC 可能有 0 到 5 個公有子網路層，橫跨 2 到 3 個可用區域。如果您有超出這些限制的要求，請通知您的 CSDM 或雲端架構師檢閱您的使用案例。

AMS 多帳戶登陸區域應用程式與帳戶比率

AMS 多帳戶登陸區域支援每個應用程式一個帳戶；不過，每個應用程式帳戶的成本都很低，而且您每小時需支付 Transit Gateway 的連線數，以及流經 AWS Transit Gateway 的流量。因此，隔離的應用程式越常進入帳戶或 VPCs，成本就越高。

為了降低成本並仍然確保適當的職責劃分，AMS 建議您 1) 依業務流程緊密耦合的團隊將應用程式分組，以及 2) 不混合處於不同階段（產品與非產品）或由不同團隊管理的應用程式。如此一來，您將擁有較少的帳戶、存取管理和職責分離會更輕鬆，並且可以降低流量成本。

例如：企業在生產中擁有交易應用程式和產品組合管理應用程式，這兩個應用程式都由投資 IT 團隊管理，並互相交換大量流量。在此案例中，公司可以從將相同帳戶和 VPC 中的兩個應用程式分組中受益，因為投資 IT 團隊不需要請求存取多個應用程式帳戶，而且公司將節省流量成本。在這種情況下，公司應該在開發階段為相同的應用程式建立另一個帳戶，並向開發團隊提供存取權。

在另一個案例中，企業在生產環境中有薪資應用程式和會計應用程式，分別由人力資源 IT 和會計 IT 團隊管理。雖然薪資應用程式必須與會計應用程式交換資訊，但我們建議您隔離不同帳戶中的兩個應用程式，每個團隊一個，並使用網路帳戶在兩個應用程式的 VPCs 之間建立連線。透過這種方式，公司將防止人力資源 IT 團隊請求變更影響會計應用程式基礎設施，而他們對此並不知情。

如何將帳戶分組為組織單位 (OUs) 秘訣。OU 是一種邏輯分組機制，可讓您分類（群組）帳戶，並根據這些群組將政策和組態套用至。建立 OUs 的建議方法是以需要套用至特定帳戶群組的政策為基礎，而不是以報告結構內團隊的內部階層為基礎。OU 不等同於 Active Directory 的 OU，因此 AWS Organizations 不鼓勵在中嘗試複寫 AD OU 結構，並導致難以維護和/或操作結構。

AWS 帳戶限制

AWS 帳戶限制適用於您的 AWS Managed Services (AMS) 帳戶。判斷 AWS 服務預設和目前限制的最簡單方法是利用 [AWS Service Quotas](#)。AMS 建議將個別服務限制的大小調整到適當的大小，以在帳戶中執行服務（些）。限制就像護欄一樣，可保護您的帳戶的安全和成本失控。如果您想要提高特定限制，請向 AMS 提交服務請求，AMS Operations 會代表您提高限制。例如，RDS 執行個體的預設限制（或配額）為 40；如果您的工作負載需要 50 個 RDS 執行個體，請提出 AMS Operations 的服務請求，將限制提高到所需的值。

AMS 服務水準目標 SLOs)

下表說明 AWS Managed Services (AMS) 服務的目標。當您訂閱 AMS 時，與您共用的 SLA 文件會涵蓋 AMS 服務其他層面的服務水準協議 (SLAs)，包括事件管理。如需詳細資訊，請洽詢您的 CSDM。

AMS 服務層級目標

功能	效能指標 (PI)	Plus (Business Days, M-F 8AM to 6PM local time)	高級 (Calendar Days, 24 x 7)
變更管理	排程或拒絕自動化 RFCs所需的時間	<=30 分鐘	<=30 分鐘
	排程 RFCs排程執行時間的啟動時間	<=1 分鐘	<=1 分鐘
	CT 目錄中提供核准/拒絕非自動化 RFCs 所需的時間	<=48 小時	<=24 小時
	CT 目錄中無法使用核准/拒絕非自動化 RFCs 所需的時間	<=5 天	<=5 天
問題管理	完成根本原因分析 (RCA) 所需的時間	<=10 天	<=10 天
服務請求管理	第一次和後續每次回覆的回應時間	<=8 小時	<=4 小時

支援 AWS 的服務

AWS Managed Services (AMS) 為下列服務提供操作管理支援服務 AWS。每個 AWS 服務都是不同的，因此 AMS 的操作管理層級，支援會根據基礎 AWS 服務的性質和特性而有所不同。特定 AWS 服務會根據 AMS 提供的操作管理支援服務的複雜性和範圍進行分組。

Note

這三個群組 A、B 和 C，根據 2021 年 3 月 16 日之前 AMS 客戶的支援計劃 (Plus 或 Premium)，以 AMS 服務每個帳戶每月總花費的百分比表示定價。2021 年 3 月 16 日之後加入的 AMS 客戶應提交服務請求，以取得其他定價資訊。群組 A 表示不收取額外費用。B 群組表示 12% (Plus) 或 18% (Premium) 的額外費用。C 群組表示額外收取 25% (Plus) 或 42% (Premium) 的費用。

星號 (*) 表示客戶使用 AWS 主控台和 APIs 在 AMS 受管環境中部署的服務。如需以這種方式佈建和設定服務時客戶責任的其他詳細資訊[AWS Managed Services \(AMS\) AMS 進階操作計劃功能](#)，請參閱 中的「自動化和自助式佈建管理」。

兩星 (**) 表示 上的 Amazon EC2 AWS Outposts 將以群組 B 服務計費；在 上託管的所有其他資源 AWS Outposts 都會以標準費率計費。

支援 AWS 的服務

群組 A	群組 B	群組 C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift

群組 A	群組 B	群組 C
AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces*	Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

群組 A	群組 B	群組 C
	AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

如果您請求 AWS Managed Services 為以下未明確識別為支援的任何軟體或服務提供服務，則根據服務條款，為此類客戶請求組態提供的任何 AWS Managed Services 都將被視為「Beta 服務」。

支援的組態

AWS Managed Services (AMS) 支援的組態如下：

- 語言：AMS 提供英文版本。

- 防火牆服務：
 - Amazon Route 53 Resolver DNS 防火牆
 - Palo Alto VM 系列新一代防火牆
- 安全軟體：Deep Security from Trend Micro (必要)。AWS Marketplace：[Trend Micro Deep Security](#)
- 核准的目錄服務：Microsoft Active Directory (AD)
- [支援 AWS 的服務](#)。
- 支援 AWS 的區域：

AMS 在所有 AWS 區域的子集中運作；不過，AMS API/CLI 只會在「美國東部 (維吉尼亞北部)」區域用盡。如果您執行 AMS 變更管理 API (amscm) 或 AMS 服務知識管理 API (amsskms) 在非美國東部區域，您必須將 `--region us-east-1` 新增至命令。

- 美國東部 (維吉尼亞)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 美國東部 (俄亥俄)
- 加拿大 (中部)
- 南美洲 (聖保羅)
- 歐洲 (愛爾蘭)
- 歐洲 (法蘭克福)
- 歐洲 (倫敦)
- 歐洲西部 (巴黎)
- 亞太區域 (孟買)
- 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)
- Amazon Machine Image AMIs)：AMS 針對 AMS 支援的作業系統子集，根據 CIS 第 1 級基準提供安全增強型映像 (AMIs)。若要尋找具有可用安全增強型映像的作業系統，請參閱 AMS 安全使用者指南。若要存取本指南，請在 中 AWS Artifact 篩選 AWS Managed Services 的報告索引標籤。若要存取 AWS Artifact，請聯絡您的 CSDM 或參閱 [AWS Artifact 入門](#)。

支援的作業系統 (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (預期的 AMS 支援結束日期為 2026 年 6 月 30 日)
- Oracle Linux 9.x、8.x
- Red Hat Enterprise Linux (RHEL) 9.x、8.x
- SUSE Linux Enterprise Server 15 SP6
- 適用於 SAP 15 SP3 和更新版本的 SUSE Linux Enterprise Server
- Microsoft Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

支援的作業系統 (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (預期的 AMS 支援結束日期為 2026 年 6 月 30 日)
- 支援的終止支援 (EOS) 作業系統：

Note

終止支援 (EOS) 作業系統在作業系統製造商的一般支援期間之外，且具有更高的安全風險。只有當 AMS 所需的代理程式支援作業系統和...時，EOS 作業系統才會被視為支援的組態。

1. 您已擴充對作業系統廠商的支援，允許您接收更新，或
2. 使用 EOS 作業系統的任何執行個體都遵循進階使用者指南中 AMS 指定的[安全控制](#)，或
3. 您遵守 AMS 要求的任何其他補償性安全控制。

如果 AMS 不再支援 EOS 作業系統，AMS 會發出[關鍵建議](#)來升級作業系統。

AMS 所需的代理程式可能包括但不限於：Amazon CloudWatch AWS Systems Manager、端點安全 (EPS) 代理程式和 Active Directory (AD) Bridge (僅限 Linux)。

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4 和 SP5
- SUSE Linux Enterprise Server for SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Service for SAP 12 SP5

- Red Hat Enterprise Linux (RHEL) : 7.x
- Oracle Linux 7.5-7.9

AMS 中不支援作業系統的功能

不支援的作業系統是 中未列出的任何作業系統[支援的組態](#)。AMS 會將具有不支援作業系統的執行個體視為「客戶請求組態」，其受到 [AWS Beta 版和預覽版服務條款](#)的約束。

下列有限的 AMS 功能集可供具有不支援作業系統的執行個體使用：

功能	備註
事件管理	AMS 提供事件回應。
服務請求管理	AMS 會回應服務請求。
變更請求 (RFCs)	AMS 會評估 RFCs以進行執行。不支援的作業系統可能會影響執行 RFCs的能力。
監控	AMS 會監控和回應 Amazon EC2 系統狀態檢查和執行個體狀態檢查。系統狀態檢查包括：網路連線中斷、系統電源中斷、實體主機上的軟體問題，以及實體主機上會影響網路連線能力的硬體問題。 執行個體狀態檢查包括：網路或啟動組態不正確、記憶體耗盡、檔案系統損毀，以及核心不相容。
安全管理	AMS 會監控和回應 Amazon EC2 GuardDuty 調查結果 。
備份管理	AMS 使用 AMS 自訂的計劃和保存庫，在 AMS Advanced for EC2 中提供持續性管理 。EC2 AWS Backup

AMS 進階介面

- AMS 進階主控台：您可以使用 AMS 進階主控台來建立 RFCs、報告和回應事件、提出服務請求，以及尋找現有 VPCs和堆疊的相關資訊。如果不確定該怎麼做，或當您需要 AMS 或受管資源的協助時，請使用此界面建立服務請求。

- AWS Management Console：許多 AWS 主控台對於檢視 AMS 資訊很有用，例如：
 - Amazon EC2 主控台：使用 來檢視執行個體資訊，包括堡壘 IP 地址、Amazon EC2 Auto Scaling 群組和負載平衡器。
 - 多帳戶登陸區域 AWS Config 規則合規：您可以檢視跨帳戶的合規狀態，並識別不合規的資源。
 - AWS CloudFormation 主控台：使用 來檢視堆疊資訊，包括堆疊 IDs (您可以在這裡找到 Amazon RDS 堆疊和 Amazon RDS IDs，以及事件資訊)。
 - Amazon RDS 主控台：使用 來檢視事件資訊，例如您帳戶中網站上的 WordPress 應用程式文章。請注意，您必須擁有 Amazon RDS 執行個體 ID。

視登入角色的模式而定，您擁有不同層級的 AWS 管理主控台存取權。如需模式的詳細資訊，請參閱 [AMS 模式](#)。

- AMS 進階變更管理 API – 讀取/寫入：使用變更管理 API (CM API) 請求對受管基礎設施的新增和特定變更，包括資源監控、日誌、備份和修補程式組態。此外，使用此 API 請求存取 資源、刪除資源、建立 AMIs 和建立 IAM 執行個體描述檔。您可以透過 AMS CLI 和 SDKs 存取 CM API。
- AMS SKMS API – 唯讀：使用此 API 列出受管資源，並取得報告或準備變更請求所需的資訊。
- 支援 API：使用標準 支援 API 以程式設計方式建立和回應事件和服務請求。若要進一步了解，請參閱 [入門 支援](#)。
- AWS APIs – 唯讀：您的主要 IT 管理員可以使用 AWS APIs 來查看管理的所有資源、檢視 CloudTrail 日誌、帳單資訊，以及許多其他讀取函數。

AMS VPC 端點

VPC 端點可讓您將 VPC 私下連線至 ，AWS 服務 而不需要網際網路閘道。VPC 中的執行個體不需要公有 IP 地址，即可與服務中的資源通訊。

端點是虛擬裝置。端點為一種可水平擴展、備援且高可用性的 VPC 元件，允許 VPC 中之執行個體與服務之間的通訊，而不會強加網路流量的可用性風險或頻寬限制。若要進一步了解，請參閱 [VPC 端點](#)。

有兩種 VPC 端點類型：介面端點和閘道端點。

- 閘道端點：帳戶中的 VPC 預設會啟用 Amazon S3 Gateway 端點。
- 介面端點：AMS 環境中的執行個體可以與支援的 服務通訊，而無需離開 Amazon 網路。這對於單一帳戶登陸區域是選用的，而且預設不會在帳戶中啟用；請向 AMS 操作提交服務請求以啟用此功能。不過，對於多帳戶登陸區域，介面端點預設會在共用服務帳戶中啟用。

AMS 支援的介面端點清單：

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- Amazon EC2 API
- AWS Key Management Service
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

AMS 受保護的命名空間

AWS Managed Services (AMS) 的受保護命名空間清單。當您使用 AWS 資源時，請勿使用這些命名空間來防止與 AMS 發生衝突。如需其他 AWS 服務命名空間的詳細資訊，請參閱 [Amazon Resource Name \(ARNs\)和服務 AWS 命名空間](#)。

- `ams-*` (這是新資源的偏好命名標準)
- `/ams/*` (這是路徑型資源的偏好命名標準)
- `AWSManagedServices*` (這是適用於 CamelCase 的資源的偏好命名標準)
- `ams*` 和 `AMS*` 和 `Ams*`
- `AWS_*` 和 `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` 和 `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` 和 `EPS`
- `EPSThirdPartyMarketplaceSubscriptionRole`

- EPSDB*
- IAMPolicy*
- INGEST*
- LandingZone*
- Managed_Services*
- managementhost
- mc* 和 MC* 和 Mc*
- MMS*
- ms-
- NewAMS*
- Root*
- sentinel* 和 Sentinel*
- sentinel.int.
- StateMachine*
- StackSet-ams*
- StackSet-AWS-Landing-Zone
- TemplateId*
- UnhealthyInServiceBastion
- VPC_*

AMS 預留字首

AMS 資源屬性必須符合特定模式；例如，IAM 執行個體設定檔名稱、BackupVault 名稱、標籤名稱等，不得以 AMS 預留字首開頭。這些預留字首為：

```
*/aws_reserved/*  
ams- *  
/ams/*  
ams*  
AMS*  
Ams*  
aws*
```

```
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

AMS 維護時段

AWS Managed Services 維護時段（或維護時段）會執行 AWS Managed Services (AMS) 的維護活動，並在每個月的第二個星期四太平洋時間下午 3 點至下午 4 點重複執行。AMS 可能會變更維護時段，但需提前 48 小時通知。這是供 AWS Managed Services (AMS) 使用；用於執行受管基礎設施的維護活動，例如部署新的 AMS AMIs。

您的維護時段是 AMS 套用修補的時間，而且您會在加入時判斷維護時段。您也可以同意修補服務通知中提供的建議修補時段，或建議不同的時段。

如需建立維護時段的指引，請參閱[維護時段](#)。

AMS 資訊資源

AMS 提供數種資訊資源來協助您成功。

- AMS Accelerate 使用者指南：協助您了解 AMS Accelerate 提供的元件和功能，以及如何使用這些元件和功能。在這裡查看 AMS Accelerate 背景資訊和預設設定、尋找資源和操作說明範例的詳細資訊。[HTML 索引](#)、[PDF](#)
- AMS 進階使用者指南：協助您了解 AMS Advanced 提供的元件和功能，以及如何使用這些元件和功能。在這裡查看 AMS Advanced 背景資訊和預設設定、尋找資源和操作說明範例的詳細資訊。[HTML 索引](#)、[PDF](#)
- AMS 進階應用程式指南：說明將應用程式部署至 AWS Managed Services 基礎設施的步驟。如需應用程式部署和維護方法和考量事項的相關資訊，請參閱此處。[HTML 索引](#)、[PDF](#)。
- AMS 進階加入指南：描述在 AMS 帳戶中建立基本 AWS Managed Services 多帳戶或單一帳戶登陸區域基礎設施的初始步驟。在這裡查看有關 AMS 帳戶基本概念、驗證和問題的資訊，以準備您加入 AMS。[HTML 索引](#)、[PDF](#)。
- AMS 進階變更類型參考：提供有關 AWS Managed Services 目前變更類型的參考資料，包括變更類型結構描述，以及每個變更類型和秘訣的範例演練。包含變更類型的一般資訊協助您了解變更請求 (RFCs) 和 AMS 變更類型 CTs) 的所有層面。在這裡查看有關變更類型的詳細資訊，包括相關資訊的連結。[HTML 索引](#)、[PDF](#)。
- AMS CM (變更管理) API 參考：描述 AWS Managed Services CM API，提供建立和監控變更請求的操作，並提供由 Managed Services 管理之資源的相關資訊。[HTML 索引](#)。
- AMS 安全指南：描述專屬 AMS 安全資訊。

私有；可在 AWS 成品主控台的 AMS 報告索引標籤上取得。

- AMS 開發人員的資源：同時存取 amscm 和 amsskms 的 AMS CLI 和 SDK。請參閱 <https://console.aws.amazon.com/managedservices/>。
- AMS YouTube 影片：影片中說明的主要客戶操作。請參閱 [AWS Managed Services YouTube 教學影片](#)。
- AMS 部落格文章：AWS Managed Services 的特殊資訊。請參閱 [AWS 部落格](#)。

AMS 合規

AMS 已針對下列標準進行稽核，並有資格做為您必須取得合規認證之解決方案的一部分使用。

AMS 支援的合規標準

AMS 支援 AWS 合規標準。若要進一步了解 AWS 合規計劃，請參閱[AWS 合規](#)。

這些是 AMS 目前支援的合規標準。

FedRAMP：美國聯邦政府致力於以最具創新性、安全且經濟實惠的方式，將其服務提供給美國公民。雲端運算在聯邦政府如何實現營運效率和隨需創新以推動其在全國的任務方面扮演重要角色。這就是為什麼許多聯邦機構現在使用 AWS 雲端服務來處理、存放和傳輸聯邦政府資料的原因。

如需詳細資訊，請參閱 [FedRAMP](#)。

HIPAA：AWS 已擴展其健康保險流通與責任法案 (HIPAA) 合規計劃，將 AMS 納入 [HIPAA 合格服務](#)。如果您與 AWS 簽訂商業夥伴協議 (BAA)，您可以使用 AMS 協助建置符合 HIPAA 規範的應用程式。

請參閱[以 HIPAA 為重心的白皮書](#)，了解如何利用 AMS 處理和儲存健康資訊。如需詳細資訊，請參閱 [HIPAA 合規](#)。

HITRUST：健康資訊信任聯盟通用安全架構 (HITRUST CSF) 利用國家和國際公認的標準和法規，例如 GDPR、ISO、NIST、PCI 和 HIPAA，來建立一組完整的基準安全和隱私權控制。

如需詳細資訊，請參閱 [HITRUST CSF](#)。

ISO 27001：ISO/IEC 27001：2013 是一項安全管理標準，根據 ISO/IEC 27002 最佳實務指引指定安全管理最佳實務和全面的安全控制。此認證的基礎是制定和實作嚴格的安全計劃，其中包括制定和實作資訊安全管理系統 (ISMS)，該系統定義了 AWS 如何以全面、全面的方式永久管理安全。

如需詳細資訊，請參閱 [ISO/IEC 27001：2013](#)。

ISO 27017：ISO/IEC 27017：2015 提供雲端運算資訊安全方面的指導，建議實作雲端特定的資訊安全控制，以補充 ISO/IEC

27002 和 ISO/IEC 27001 標準的指引。此實務準則提供雲端服務提供者特有的額外資訊安全控制實作指引。

如需詳細資訊，請參閱 [ISO/IEC 27017 : 2015 合規](#)。

ISO 27018 : ISO/IEC 27018 : 2019 是一種實務準則，著重於保護雲端中的個人資料。它以 ISO/IEC 資訊安全標準 27002 為基礎，並提供適用於公有雲端個人身分識別資訊 (PII) 的 ISO/IEC 27002 控制實作指引。它還提供一組額外的控制和相關指導，旨在解決現有 ISO/IEC 27002 控制集未解決的公有雲端 PII 保護要求。

如需詳細資訊，請參閱 [ISO/IEC 27018 : 2019 合規](#)。

ISO 9001 : ISO 9001 : 2015 概述了記錄和審查在組織內實現有效品質管理所需的結構、責任和程序的程序導向方法。標準的特定章節包含主題的相關資訊，例如：

- 品質管理系統的要求，包括品質手冊的文件、文件控制和確定程序互動
- 管理的責任
- 資源的管理，包括人力資源和組織的工作環境
- 服務開發，包括從設計到交付的步驟
- 客戶滿意度
- 透過內部稽核和修正和預防性動作等活動來衡量、分析和改善 QMS

如需詳細資訊，請參閱 [ISO 9001 : 2015 合規](#)。

PCI：AMS 在服務提供者層級 1 具有支付卡產業 (PCI) 資料安全標準 (DSS) 3.2 版的合規證明。使用 AWS 產品和服務來存放、處理或傳輸持卡人資料的客戶，可以在管理自己的 PCI DSS 合規認證時使用 AMS。

如需 PCI DSS 的詳細資訊，包括如何索取 AWS PCI 合規套裝服務的複本，請參閱 [PCI DSS 第 1 級](#)。重要的是，您必須在 AMS 中設定精細的密碼政策，以符合 PCI DSS 3.2 版標準。如需必須強制執行哪些政策的詳細資訊，請參閱 [為您的 AWS Microsoft AD 目錄啟用 PCI 合規](#)。

SOC：AMS 系統和組織控制 (SOC) 報告是獨立的第三方檢查報告，示範 AMS 如何實現關鍵合規控制和目標。這些報告的目的是協助您和稽核人員了解為了支援操作和合規而建立的 AMS 控制。AMS SOC 報告有三種類型：

- AWS SOC 1 報告 - [使用 AWS Artifact 下載](#)
- AWS SOC 2：安全性、可用性和機密性報告 - [使用 AWS Artifact 下載](#)
- [AWS SOC 3：安全性、可用性和機密性報告](#)

如需詳細資訊，請參閱 [SOC 合規](#)。

共同的責任

安全性，包括 PCI 合規，是 [共同的責任](#)。請務必了解，AMS 合規狀態不會自動套用到您在 AWS 雲端中執行的應用程式。您需要確保使用 AWS 服務符合標準。如需 AMS 如何與特定活動的客戶一起運作的詳細資訊，請參閱 AMS [AMS 責任矩陣 \(RACI\)](#)。

AMS Amazon Machine Image AMIs)

AMS 每個月都會為 AMS 支援的作業系統產生更新的 Amazon Machine Image (AMIs)。此外，AMS 也會根據 CIS 層級 1 基準，為 [AMS 支援的作業系統子集產生安全性增強映像 \(AMIs\)](#)。若要了解哪些作業系統有可用的安全性增強映像，請參閱 AMS 安全使用者指南，該指南可透過 AWS Artifact -> 報告頁面（在左側導覽窗格中尋找報告選項）篩選 AWS Managed Services。若要存取 AWS Artifact，可聯絡您的 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

若要在新 AMS AMIs 發行時接收提醒，您可以訂閱名為「AMS AMI」的 Amazon Simple Notification Service (Amazon SNS) 通知主題。如需詳細資訊，請參閱使用 [SNS 的 AMS AMI 通知](#)。

AMS AMI 命名慣例為：customer-ams-<operating system>-<release date> -<version>。（例如，customer-ams-rhel6-2018.11-3）

僅使用開頭為的 AMS AMIs customer。

AMS 建議一律使用最新的 AMI。您可以透過以下方式找到最新的 AMIs：

- 在 AMS 主控台的 AMIs 頁面上查看。
- 檢視可從 CSDM 或此 ZIP 檔案取得的最新 AMS AMI CSV 檔案：[AMS 11.2024 AMI 內容和 ZIP 中的 CSV 檔案](#)。

如需過去的 AMI ZIP 檔案，請參閱 [文件歷史記錄](#)。

- 執行此 AMS SKMS 命令（需要 AMS SKMS SDK）：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

依作業系統 (OS) 新增至 AWS AMIs 內容

- Linux AMIs：
 - [AWS CLI 工具](#)
 - [NTP](#)
 - [Trend Micro Endpoint Protection Service 代理程式](#)
 - [程式碼部署](#)
 - [PBIS/超越信任 AD 橋接器](#)
 - [SSM 代理程式](#)
 - 重要修補程式的百勝升級
 - AMS 自訂指令碼/管理軟體（控制開機、AD 聯結、監控、安全性和記錄）
- Windows Server AMIs：
 - [Microsoft .NET Framework 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS 適用於 Windows PowerShell 的工具](#)

- AMS PowerShell 模組控制開機、AD 聯結、監控、安全性和記錄
- [Trend Micro Endpoint Protection Service 代理程式](#)
- [SSM 代理程式](#)
- [CloudWatch 代理程式](#)
- EC2Config 服務 (透過 Windows Server 2012 R2)
- EC2Launch (Windows Server 2016 和 Windows Server 2019)
- EC2LaunchV2 (Windows Server 2022 及更新版本)

Linux 型 AMIs :

- Amazon Linux 2023 (最新次要版本) (不支援最小 AMI)
- Amazon Linux 2 (最新次要版本)
- Amazon Linux 2 (ARM64)
- Red Hat Enterprise 7 (最新次要版本)
- Red Hat Enterprise 8 (最新次要版本)
- Red Hat Enterprise 9 (最新次要版本)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux : 如需產品概觀、定價資訊、用量資訊和支援資訊，請參閱 [Amazon Linux AMI \(HVM / 64 位元\)](#) 和 [Amazon Linux 2](#)。

如需詳細資訊，請參閱 [Amazon Linux 2 常見問答集](#)。

- RedHat Enterprise Linux (RHEL) : 如需產品概觀、定價資訊、用量資訊和支援資訊，請參閱 [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#)。
- Ubuntu Linux 18.04 : 如需產品概觀、定價資訊、用量資訊和支援資訊，請參閱 [Ubuntu 18.04 LTS - Bionic](#)。
- SUSE Linux Enterprise Server for SAP 應用程式 15 SP6 :
 - 每個帳戶執行下列步驟一次：
 1. 導覽至 AWS Marketplace。

2. 搜尋 SUSE 15 SAP 產品。
 3. 選擇繼續以訂閱。
 4. 選擇接受詞彙。
- 每次您需要啟動新的 SUSE Linux Enterprise Server for SAP Applications 15 SP6 執行個體時，請完成下列步驟： SP6
 1. 請注意訂閱 SUSE Linux Enterprise Server for SAP Applications 15 AMI 的 AMI ID。
 2. 建立部署 | 進階堆疊元件 | EC2 堆疊 | 建立變更類型 ct-14027q0sjyt1h RFC。將 *InstanceAmiId* 取代為您訂閱的 AWS Marketplace AMI ID。

Windows 型 AMIs：

Microsoft Windows Server (2016、2019 和 2022)，以最新的 Windows AMIs 為基礎。

如需建立 AMIs 的範例，請參閱 [建立 AMI](#)。

離職 AMS AMIs：

AMS 不會在離職期間取消與您共用任何 AMIs，以避免對您的任何停用造成影響。如果您想要從您的帳戶中移除 AMS AMIs，您可以使用 `cancel-image-launch-permission` API 來隱藏特定 AMIs。例如，您可以使用以下指令碼來隱藏先前與您的帳戶共用的所有 AMS AMIs：

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

您必須安裝 AWS CLI v2，指令碼才能在沒有錯誤的情況下執行。如需 AWS CLI 安裝步驟，請參閱 [安裝或更新最新版本的 AWS CLI](#)。如需 `cancel-image-launch-permission` 命令的詳細資訊，請參閱 [cancel-image-launch-permission](#)。

安全性增強 AMIs

AMS 為 AMIs 支援的作業系統子集提供以 CIS 第 1 級基準為基礎的安全性增強映像 (AMI)。若要尋找哪些作業系統有可用的安全增強型映像，請參閱 AWS Managed Services (AMS) 客戶安全指南。若要存取本指南，請開啟 AWS Artifact，選取左側導覽窗格中的報告，然後篩選 AWS Managed Services。如需如何存取的指示 AWS Artifact，請聯絡您的 CSDM 或參閱 [入門 AWS Artifact](#) 以取得詳細資訊。

AD FS 和 AMS 之間的整合如何運作

內部部署網路與 AMS 網域之間的單向信任是存取堆疊和 VPCs 的預設方法。建立 VPC 和堆疊時，會透過預先設定的 Active Directory 安全群組授予存取權。此外，對於 AWS 管理主控台的單一登入 (SSO)，AWS Management Console 可以使用 Active Directory Federation Service (AD FS) 或任何支援 SAML 的聯合軟體來設定對 的存取。

Note

AMS 可以聯合到許多聯合服務、Ping、Okta 等。您不限於 AD FS；我們在此提供了一個可用的聯合技術範例。

此處的資訊會從此部落格文章複製：[使用 AWS Windows Active Directory、AD FS 和 SAML 2.0 啟用聯合至](#)。

1. 當使用者（讓我們呼叫他 Bob）瀏覽到其網域內的 AD FS 範例網站 (<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx://>) 時，就會啟動流程。安裝 AD FS 時，您會為預設網站取得名為 adfs 的新虛擬目錄，其中包含此頁面。
2. 登入頁面會針對 AD 驗證 Bob。根據 Bob 使用的瀏覽器，可能會提示他輸入 AD 使用者名稱和密碼。
3. Bob 的瀏覽器收到來自 AD FS 的身分驗證回應形式的 SAML 聲明。
4. Bob 的瀏覽器會將 SAML 聲明發佈到 SAML AWS 的登入端點 (<https://signin.aws.amazon.com/saml://>)。在幕後，登入會使用 [AssumeRoleWithSAML](#) API 來請求臨時安全登入資料，然後建構的登入 URL AWS Management Console。
5. Bob 的瀏覽器會收到登入 URL，並重新導向至主控台。

從 Bob 的角度來看，程序會以透明的方式進行。他從內部網站開始，最後在 AWS Management Console，而不需要提供任何 AWS 登入資料。

Note

有關設定 AMS 主控台聯合的詳細資訊，請參閱：

- 多帳戶登陸區域：[設定 AMS 主控台的聯合](#)
- 單一帳戶登陸區域：[設定 AMS 主控台的聯合](#)

此外，請參閱[附錄：AD FS 宣告規則和 SAML 設定](#)。如需使用 AWS Microsoft AD 支援 Active Directory 感知應用程式的相關資訊，請參閱 AWS [管理 Microsoft AD 合規](#)。

AMS 受管 Active Directory

AMS 現在提供稱為 Managed Active Directory (又稱為 Managed AD) 的新服務，可讓 AMS 處理 Active Directory (AD) 基礎設施操作，同時讓您控制 Active Directory 管理。

Managed AD 的 AMS 支援類似於 Amazon Relational Database Service (Amazon RDS) 的 AMS 支援。在這兩種情況下，AWS (包括 AMS) 都支援建立和管理執行服務的基礎設施，同時執行存取控制和所有管理功能。此模型具有下列優點：

- 限制安全風險：AWS 且 AMS 不需要網域的管理權限。
- 直接整合：您可以使用目前的授權模型並與 AD 整合，而不需要與 AMS 連接。

備註：

- AMS 和您都無法存取 Managed AD 網域控制站，因此網域控制站上無法安裝任何軟體。這很重要，因為不允許在網域控制站上安裝軟體的第三方解決方案。

存取的運作方式如下：

- AWS Directory Service 團隊：可存取網域控制站。
- AMS：可存取 Directory Service APIs 以在網域上執行特定動作。這些動作包括拍攝 AD 快照、變更 AD 結構描述和其他動作。
- 您：可存取網域 (AD) 以建立使用者、群組等。
- 我們建議您在遷移公司 AD 之前先在 Managed AD 上執行概念驗證，因為並非所有來自傳統 AD 環境的功能都可在 Managed AD 環境中使用。
- AMS 不會管理 AD 管理或提供有關 AD 管理的指導。例如，AMS 不會提供有關組織單位結構、群組政策結構、AD 使用者命名慣例等的指導。

它的運作方式如下：

1. 除了您的 AMS 帳戶之外，AMS 還會 AWS 帳戶 為您加入新的，並透過 AWS Directory Service 佈建 Active Directory (AD) 環境 (另請參閱[什麼是 AWS Directory Service ?](#))。

以下是系統整合商需要從您收集的資訊，以便 AMS 加入 Managed AD：

- 帳戶資訊

- 為 AMS 受管 AD：AWS 帳戶 number AWS 帳戶 建立之 的帳戶 ID
- 要加入 Managed AD 的區域：AWS 區域
- 受管 Active Directory 資訊：
 - Microsoft AD Edition：Standard/Enterprise。AWS Microsoft AD (Standard Edition) 包含 1 GB 的目錄物件儲存。此容量最多可支援 5,000 個使用者或 30,000 個目錄物件，包括使用者、群組和電腦。AWS Microsoft AD (Enterprise Edition) 包含 17 GB 的目錄物件儲存體，最多可支援 100,000 個使用者或 500,000 個物件。

如需詳細資訊，請參閱 [AWS Directory Service FAQs](#)。

- 網域 FQDN：AMS Managed AD 網域的 FQDN。
- 網域 NetBIOS 名稱：AMS Managed AD 網域的 NetBIOS 名稱。
- 您想要 Managed AD 整合的 AMS 標準帳戶帳號 (AMS 會設定從 AMS 標準帳戶的 AD 到 Managed AD 的單向信任)
- 是否需要修改 Active Directory 結構描述，如果需要，要修改什麼？
- 根據預設，會佈建兩個網域控制站。您需要更多嗎？如果是這樣，您需要多少？原因是什麼？
- 受管 Active Directory 資訊的聯網：
 - 網域控制站的 Managed AD VPC CIDR (Managed AD 網域控制站私有子網路範圍內的 CIDR)：
 - 網域控制站的子網路 CIDR 1：【您的 CIDR 需要屬於 AMS Managed AD VPC CIDR】
 - 網域控制站的子網路 CIDR 2：【您的 CIDR 需要屬於 AMS Managed AD VPC CIDR】

例如：

- Managed AD VPC CIDR：192.168.0.0/16
- 網域控制器的 CIDR 1：192.168.1.0/24
- 網域控制器的 CIDR 2：192.168.2.0/24

為了避免 IP 地址衝突，請確定您指定的 Managed AD VPC CIDR 不會與您公司網路中使用的任何其他私有子網路 CIDR 衝突。

- VPN 技術（選用）：【Direct Connect/Direct Connect 和 VPN】
 - 開道的 BGP 自治系統編號 (ASN)：【客戶提供的 ASN】

- 您的 VPN 連接是否需要靜態路由：【是/否】
- 2. AMS 為您提供 AD 環境的管理員帳戶密碼，並要求您重設密碼，以便 AMS 工程師無法再存取您的 AD 環境。
- 3. 若要重設管理員帳戶密碼，請使用 Active Directory 使用者和電腦 (ADUC) 連線至您的 Active Directory 環境。ADUC 和其他遠端伺服器管理工具 (RSAT) 應該安裝在您在非 AMS 基礎設施上佈建的管理主機上並執行。Microsoft 有保護此類管理主機的 best practices。如需詳細資訊，請參閱[實作安全管理主機](#)。您可以使用這些管理主機來管理 Active Directory 環境。
- 4. 在日常操作中，AMS 最多會管理物件的 AWS 帳戶 AWS Directory Service 端；例如，VPC 組態、AD 備份、AD 信任建立和刪除等。您可以使用並管理您的 AD 環境；例如，使用者建立、群組建立、群組政策建立等。

如需最新的 RACI 資料表，請參閱《請參閱[服務描述](#)》中的「角色與責任」一節。

AMS 應用程式部署

AMS 應用程式開發人員指南提供下列部署的詳細說明和演練：

- AMS 工作負載擷取 CT 可讓您和 AMS 雲端遷移合作夥伴輕鬆將現有工作負載移至 AMS 受管 VPC。使用 AMS 工作負載擷取，您可以透過使用部署 | 擷取 | 來自遷移合作夥伴遷移執行個體的堆疊 | 建立 CT (ct-257p9zjk14ija) 提交 RFC 來建立 AMS AMI。您必須讓遷移 AWS 合作夥伴將執行個體從現場部署遷移至，以及將擷取執行個體的目標 AMS VPC 和子網路。

如需詳細資訊，請參閱 [《工作負載擷取》](#) 中的 AMS 應用程式開發人員指南。

- AWS CloudFormation 擷取變更類型 (ct-36cn2avfrrj9v) 功能可讓您輕鬆地使用現有的 CloudFormation 範本，在 AMS 受管 VPC 中部署自訂堆疊。

如需詳細資訊，請參閱 [CloudFormation 範本擷取](#) 中的 AMS 應用程式開發人員指南。

- 您可以將內部部署資料庫匯入新的資料庫到 AMS 管理的 Amazon S3 儲存貯體或 Amazon RDS 執行個體。您可以使用部署 | 進階堆疊元件 | 資料庫遷移服務 (DMS) 變更類型來執行此操作，包括建立複寫執行個體 (ct-27aplkhqr0ol)、建立複寫子網路群組 (ct-2q5azjd8p1ag5)、建立複寫任務 (ct-1d2fml15b9eth)、建立來源端點 (ct-0attesnjy2cx) 或建立來源端點 (S3) (ct-2oxl37nphsrjz) 和建立目標端點 (ct-3gf8dolbo8x9p) 或建立目標端點 (S3) (ct-05muqzievnk5)。

如需詳細資訊，請參閱 [Database Migration Service](#) 中的 AMS 應用程式開發人員指南。

- 您可以將現場部署 MS SQL 資料庫匯入 AMS 受管 RDS SQL 執行個體上的新資料庫。您可以使用各種 AMS 變更類型、Amazon RDS API 和 AWS 主控台來執行此操作。

如需詳細資訊，請參閱 AMS Application Guide at [Database \(DB\) Import to MS SQL RDS](#)。

AWS Managed Services 中的服務管理

主題

- [AWS Managed Services 中的帳戶控管](#)
- [AWS Managed Services 中的服務開始](#)
- [客戶關係管理 \(CRM\)](#)
- [AWS Managed Services 中的成本最佳化](#)
- [AWS Managed Services 中的服務時數](#)
- [在 AWS Managed Services 中取得說明](#)

AMS 服務的運作方式。

AWS Managed Services 中的帳戶控管

本節涵蓋 AMS 帳戶控管。

您獲指派一名雲端服務交付經理 (CSDM)，其跨 AMS 提供諮詢協助，並詳細了解您的受管環境的使用案例和技術架構。CSDMs 會視情況與帳戶管理員、技術帳戶管理員、AWS Managed Services 雲端架構師 (CAs) 和 AWS 解決方案架構師 (SAs) 合作，協助啟動新專案，並在整個軟體開發和操作程序中提供最佳實務建議。CSDM 是 AMS 的主要聯絡人。CSDM 的主要責任為：

- 與客戶組織和主持每月服務審查會議。
- 提供有關安全性、環境軟體更新和最佳化機會的詳細資訊。
- 擁護您的需求，包括 AMS 的功能請求。
- 回應並解決帳單和服務報告請求。
- 提供財務和容量最佳化建議的洞見。

AWS Managed Services 中的服務開始

服務起始：AWS Managed Services 帳戶的服務起始日期是第一個日曆月的第一天，之後 AWS 會通知您該 AWS Managed Services 帳戶加入要求中列出的活動已完成；前提是如果 AWS 在某個日曆月的 20 天後發出此類通知，則服務起始日期是該通知日期之後第二個日曆月的第一天。

服務起始

- R 代表負責方執行工作以達成任務。
- 我代表知情的一方，通常是在任務完成或可交付項目時收到進度通知的一方。

服務開始

步驟 #	步驟標題	描述	客戶	AMS
1.	客戶 AWS 帳戶移交	客戶建立新的 AWS 帳戶，並將其交給 AWS Managed Services	R	I
2.	AWS Managed Services 帳戶 - 設計	完成 AWS Managed Services 帳戶的設計	I	R
3.	AWS Managed Services 帳戶 - 組建	AWS Managed Services 帳戶是根據步驟 2 中的設計建置	I	R

客戶關係管理 (CRM)

AWS Managed Services (AMS) 提供客戶關係管理 (CRM) 程序，以確保與您建立和維護明確定義的關係。此關係的基礎是根據 AMS 對您業務需求的洞察。CRM 程序有助於準確且全面地了解：

- 您的業務需求以及如何滿足這些需求
- 您的功能和限制條件
- AMS 和您的不同責任與義務

CRM 程序允許 AMS 使用一致的方法來為您提供服務，並對您與 AMS 的關係提供控管。CRM 程序包括：

- 識別您的關鍵利益相關者
- 建立控管團隊
- 與您舉行並記錄服務審查會議
- 使用呈報程序提供正式的服務投訴程序

- 實作和監控您的滿意度和意見回饋程序
- 管理您的合約

CRM 程序

CRM 程序包含下列活動：

- 識別和了解您的業務流程和需求。您與 AMS 的協議可識別您的利益相關者。
- 定義要提供的服務，以符合您的需求和要求。
- 在服務審查會議中與您開會，討論 AMS 服務範圍、SLA、合約和您的業務需求的任何變更。可能會與您舉行臨時會議，以討論績效、成就、問題和行動計劃。
- 使用客戶滿意度調查和會議上提供的意見回饋來監控您的滿意度。
- 報告每月內部測量效能報告的效能。
- 與您一起檢閱服務，以判斷改善的機會。這包括經常與您就所提供 AMS 服務的水準和品質進行通訊。

CRM 會議

AMS 雲端服務交付管理員 (CSDMs) 會定期與您進行會議，以討論服務追蹤（操作、安全性和產品創新）和執行追蹤 (SLA 報告、滿意度措施和業務需求的變更)。

會議	用途	Mode	參與者
每週狀態檢閱 (選用)	未解決的問題或事件、修補、安全事件、問題記錄 12 週營運趨勢 (+/- 6) 應用程式運算子問題 週末排程	現場客戶location/Telecom/ Chime	AMS：CSDM 和雲端架構師 (CA) 客戶指派的團隊成員（例如：雲端/基礎設施、應用程式支援、架構團隊等）
每月業務審查	檢閱服務水準效能（報告、分析和趨勢） 財務分析	現場客戶location/Telecom/ Chime	AMS：CSDM、雲端架構師 (CA)、AMS 客戶團隊、AMS 技術

會議	用途	Mode	參與者
	產品藍圖 CSAT		產品經理 (TPM) (選用)、AMS OPS 經理 (選用) 您：Application Operator 代表
每季業務審查	記分卡和服務水準協議 (SLA) 效能和趨勢 (6 個月) 即將到來的 3/6/9/12 個月計劃/遷移 風險與風險緩解措施 關鍵改進計劃 產品藍圖項目 符合未來方向的機會 財務 節省成本計畫 業務最佳化	現場客戶位置	AMS：CSDM、 雲端架構 師、AMS 客戶團 隊、AMS 服務主 管、AMS 操作管 理員 您：Applica tion Operator 代表、Service 代表、Service Director

CRM 會議安排

AMS CSDM 負責記錄會議，包括：

- 建立議程，包括動作項目、問題和出席者清單。
- 建立每次會議審查的動作項目清單，以確保項目按排程完成和解決。
- 在會議後的一個工作天內，透過電子郵件將會議記錄和動作項目清單分發給會議出席者。
- 將會議記錄存放在適當的文件儲存庫中。

如果沒有 CSDM，領導會議的 AMS 代表會建立和分發會議記錄。

Note

您的 CSDM 會與您一起建立您的帳戶控管。

CRM 每月報告

您的 AMS CSDM 會準備並傳送每月服務效能簡報。簡報包含下列資訊：

- 報告日期
- 摘要和洞見：
 - 關鍵標註：總和作用中堆疊計數、堆疊修補狀態、帳戶加入狀態（僅限加入期間）、客戶特定問題摘要
 - 效能：事件解決、警示、修補、變更請求 (RFCs)、服務請求，以及主控台和 API 可用性的統計資料
 - 問題、挑戰、疑慮和風險：客戶特定問題狀態
 - 近期項目：客戶特定的加入或事件解決計劃
- 受管資源：堆疊的圖形和圓餅圖
- AMS 指標：監控和事件指標、事件指標、AMS SLA 遵循指標、服務請求指標、變更管理指標、儲存指標、持續性指標、Trusted Advisor 指標和成本摘要（以多種方式呈現）。功能請求。聯絡資訊。

Note

除了所描述的資訊之外，您的 CSDM 也會通知您範圍或條款任何重大變更，包括由 AMS 使用承包商進行營運活動。

AMS 會產生有關 CSDM 包含在每月報告中的修補和備份的報告。在報告產生系統中，AMS 會將一些您無法存取的基礎設施新增至您的帳戶：

- 報告原始資料的 S3 儲存貯體
- Athena 執行個體，具有查詢定義來查詢資料
- 從 S3 儲存貯體讀取原始資料的 Glue 爬蟲程式

AWS Managed Services 中的成本最佳化

AWS Managed Services 會在每月業務審查 (MBRs) 期間，每月為您提供詳細的成本使用率和節省報告。

AMS 遵循一組標準程序和機制，以識別受管帳戶中節省成本的途徑，並協助您規劃和推展變更，以最佳化您的 AWS 支出。

Note

AMS 正在開發影片，以協助成本最佳化。第一步是為您提供 PDF 和 Excel 試算表，其中包含成本最佳化最佳實務。若要存取這些資源，請開啟[成本最佳化 ZIP 檔案的快速指南](#)。

成本最佳化架構

AMS 遵循三個階段的方法，以最佳化您的 AWS 成本：

1. 識別受管環境中的成本最佳化管道
2. 向您介紹成本最佳化計劃
3. 協助以可衡量的方式實現成本最佳化

識別受管環境中的成本最佳化管道

AMS AWS 利用成本總管和 Trusted Advisor 等原生工具，同時利用架構最佳化、EC2 執行個體和以 AWS 帳戶為中心的最佳化等超過 20 種節省成本模式，為您建立量身打造的成本節省建議。

部分最佳化建議包括下列項目。

架構最佳化建議：

- 最佳 S3 儲存類別使用：Amazon S3 提供各種儲存類別，以根據資料存取、彈性和成本滿足各種工作負載需求。根據工作負載需求的 S3 Intelligent-Tiering 和 S3 儲存類別分析可讓您有效率地管理 S3 成本。
- 使用快取架構：在適用的情況下，利用快取執行個體可協助您取代某些資料庫執行個體，同時滿足您的 IOPS 需求。
- EBS 升級節省：將您的 EBS 磁碟區從 gp2 遷移至 gp3 可節省高達 20% 的成本，無論磁碟區大小為何，您都可以利用可預測的 3,000 IOPS 基準效能和 125 MiB/s。

- 使用彈性：AWS 提供自動擴展功能，可實現有效的資源使用率和成本最佳化途徑。根據需求定期檢閱和更新執行個體擴展政策，進一步節省成本。

EC2 以執行個體為中心的建議

- 執行個體權利調整：專注於根據用量調整執行個體大小和最佳組態的建議。建議也包括使用 Amazon EC2 Auto Scaling 功能，並在適用於 Amazon S3 上的 AWS Lambda 或靜態 Web 內容時取代 EC2 執行個體。
- 執行個體排程：使用 AMS Resource Scheduler 根據時間排程自動啟動和停止執行個體有助於控制成本，尤其是在非營業時間內未使用的非生產執行個體。
- 訂閱 Savings Plans：Savings plan 是節省 AWS 用量最簡單的方式。相較於 Amazon EC2 Instance Savings Plans 最多可節省 72%。Amazon EC2 Amazon SageMaker AI Savings Plans 為您的 Amazon SageMaker AI 服務用量提供高達 64% 的折扣。AMS 會根據您的 AWS 資源使用量，提供有關 Savings Plans 的適當建議。
- 預留執行個體 (RI) 用量和耗用量指引：Amazon EC2 預留執行個體 (RI) 提供相較於隨需定價的大幅折扣（高達 75%），並在用於特定可用區域時提供容量保留。
- Spot 執行個體用量：容錯工作負載可以使用 Spot 執行個體，並將價格降低至 90%。
- 閒置執行個體終止：識別和報告閒置或可終止的低使用率執行個體。

以帳戶為中心的建議

- 帳戶清除：在帳戶層級，AMS 也會識別未使用的 EBS 磁碟區、重複的 CloudTrail 追蹤、具有未使用資源的空帳戶等，並提供清除建議。
- SLA 建議：此外，AMS 會定期檢閱您的 Plus 和 Premium 帳戶，並建議為帳戶選擇正確的 SLA 層級。
- AMS 自動化最佳化：AMS 會持續最佳化用於提供 AMS 服務的 AMS 自動化和基礎設施。

向客戶展示並協助規劃

AMS 會與主要客戶利益相關者進行每月業務審查 (MBRs)，並呈現可節省成本的途徑、機制和建議，以及潛在的節省成本。我們進一步與您合作，規劃所需的變更。

協助建議實作並衡量成本影響

AMS 可協助實現和衡量成本影響和最佳化變更。

您可以評估建議變更的應用程式影響、風險和成功條件，並透過 AMS 主控台提出適當的變更請求 (RFCs)。AMS 會與您合作，並在受管帳戶中實作與成本最佳化相關的變更。AMS 會測量成本影響，並在每月業務審查 (MBRs) 中包含實現的節省。

成本最佳化責任矩陣

AMS 成本最佳化中的責任。

成本最佳化 RACI

活動	客戶	AMS
編譯節省成本的建議並準備報告	I	R
呈現節省成本報告	C	R
與節省成本相關的規劃變更	R	C
評估變更的影響和風險	R	C
提高 RFCs 以實作變更	R	C
檢閱 RFCs 並實作變更	C	R
測試應用程式並驗證變更實作	R	C

活動	客戶	AMS
測量變更後的成本影響並向客戶展示	I	R

AWS Managed Services 中的服務時數

功能	AMS 進階
	高級方案
服務請求	全年無休
事件管理 (P2-P3)	全年無休
備份與復原	全年無休
修補管理	全年無休
監控和提醒	全年無休
自動化變更請求 (RFC)	全年無休
非自動化的變更請求 (RFC)	全年無休
雲端服務交付管理員 (CSDM)	週一至週五：08：00–17：00，當地上班時間

在 AWS Managed Services 中取得說明

AMS 一年 365 天、每週 7 天、每天 24 小時為您提供事件管理、服務請求管理和變更管理的支援（根據套用至帳戶的 AMS 服務水準協議）。

若要報告影響受管環境的 AWS 或 AMS 服務效能問題，請使用 AMS 主控台並提交事件報告。如需詳細資訊，請參閱[報告事件](#)。如需 AMS 事件管理的一般資訊，請參閱[事件回應](#)。

若要要求資訊或建議，或從 AMS 請求其他服務，請使用 AMS 主控台並提交服務請求。如需詳細資訊，[請建立服務請求](#)。如需 AMS 服務請求的一般資訊，請參閱[服務請求管理](#)。

AWS Managed Services 中的計劃事件管理

AWS Managed Services (AMS) 計劃事件管理 (PEM) 是一種 AMS 服務產品。PEM 使用 AMS 服務在客戶事件和專案期間進行互動、協調和協助。PEM 協助協調一組符合 PEM 事件或專案商定範圍和時間表的相關 RFCs。

AMS PEM 條件

規劃的事件是範圍限制和時間限制的專案。AMS 會使用您提供的詳細資訊（包括計劃和範圍、預期成果，以及預期 AMS 操作會執行的變更），以便在 PEM 活動期間有效支援您。然後，您的雲端架構師 (CAs) 會檢閱和評估 PEM 活動的完整性、技術實作和 AMS 操作參與。在 CA 審查之後，AMS 操作會審查計劃，並與您的雲端服務交付經理 (CSDM) 協調營運團隊參與度。

PEM 的類型

以下是可用的 PEM 類型：

- 遊戲日
 - 操作遊戲日：一種以案例為基礎的操作回應遊戲方法，旨在驗證程序、人員和系統的整合。
 - 安全遊戲日：安全事件回應策略，採用以案例為基礎的遊戲方法來評估系統、程序和人員的整合。
- BYOEPS：使用 AMS「自有端點安全」(BYOEPS) 功能，將預設 Trend Micro Deep Security 代理程式取代為您偏好的端點安全解決方案或自訂 Trend Micro 授權。如需詳細資訊，請參閱[AMS 自備 EPS](#)。
- 災難復原：災難復原事件涉及 AMS 協助您進行規劃的 DR 活動。如需詳細資訊，請參閱[災難復原規劃](#)。
- 客戶安全事件：規劃的安全事件。例如，根使用者活動和滲透測試。
- 遷移支援：支援計劃的加入和遷移活動。

此工作流程有助於與 AMS 協作，以協調與 AMS 支援相關的計劃事件和遷移活動。對於 RFCs 的優先順序執行，最佳實務是使用隨需操作 (OOD) 參與。如需詳細資訊，請參閱[隨需操作](#)。

AMS PEM 程序

PEM 程序包含下列階段：

- **PEM 啟動**：您可以使用 CSDM 來定義規劃事件的目標，並判斷 AMS 操作所需的內容。AMS CAs 會檢閱 PEM 計劃的技術層面。CAs 在合規、執行最佳化和自動化方面與 AMS Security and Operations 合作，並定義 PEM 前執行任務和交付項目。然後，您的 CSDM 會建立 PEM 票證，並向 AMS 提供專案資訊和技術詳細資訊。AMS 需要 14 個日曆天的前置時間，才能讓 AMS 營運團隊有時間規劃、提供技術審查，以及指派資源。
- **PEM 檢閱**：AMS 操作團隊會檢閱 PEM 請求，並與 CSDM 合作，確認 PEM 計畫中的資訊正確且完整。
- **PEM 接受**：AMS 會檢閱提供的資訊，並與 CSDM 溝通 PEM 活動期間的支援層級。如果 PEM 包含完整資訊，且您的 CSDM 同意工作範圍，則 PEM 會獲得核准。
- **準備和執行**：AMS 可確保 PEM 開始之前所需的任務已完成，並促進內部和客戶通訊。AMS 可確保 PEM 計劃正確執行，並提供狀態和進度報告。

PEM FAQs

在 PEM 事件期間，如何讓 AMS 與 RFC/服務請求 (SR) 互動？

- 使用 CSDM 在 RFC/SR 主旨行中以格式共用的 PEM ID **PEM-ID**。
- 您也可以建立服務請求 (SR) 來討論您的使用案例，或詢問有關計劃事件的問題。如果您使用 SR，則 PEM 不必有效。

提交 PEM 相關 RFC 時，會執行哪些驗證？

- 驗證帳戶 ID 已列在 PEM 上。
- 驗證提供的開始和結束日期之間的 PEM 狀態是否已核准且處於作用中狀態。

PEM 請求是否有 SLAs 或 SLOs？

- PEMs 不會與 SLAs 或 SLOs 建立關聯。
- PEM 相關工作項目 SLOs (RFC/服務請求) 的 SLAs 和 SLO 由 AMS SLOs 定義。

如需詳細資訊，請參閱 [AMS 服務層級目標 SLOs](#)。

我們是否可以透過服務請求 (SR) 建立 PEM？

- 否，PEM 建立必須由 Cloud Service Delivery Manager (CSDM) 管理。

網路架構

AWS Managed Services (AMS) 提供兩種網路架構：

- 多帳戶登陸區域 (MALZ)：針對部署在個別成員帳戶中的工作負載，從共用帳戶提供常見服務，例如存取、端點安全、聯網。
- 單一帳戶登陸區域 (SALZ)：提供自我包含的帳戶，其中常見的服務，例如存取、端點安全性、聯網部署在與工作負載相同的帳戶中。建議用於需要高度隔離的工作負載，因為它會產生較高的 AWS 成本。

MALZ 網路架構

關於多帳戶登陸區域網路架構

在您開始 AWS Managed Services (AMS) 多帳戶登陸區域 (MALZ) 的加入程序之前，請務必了解 AMS 代表您建立的基準架構或登陸區域、其元件和函數。

AMS 多帳戶登陸區域是多帳戶架構，預先設定基礎設施，以促進身分驗證、安全性、聯網和記錄。

Note

如需成本的預估，請參閱 [AMS 多帳戶登陸區域環境基本元件](#)。

主題

- [服務區域](#)
- [組織單位](#)
- [服務控制政策和 AWS Organization](#)

下圖以高層級概述帳戶結構，以及如何將基礎設施隔離到每個帳戶：

服務區域

由於 Active Directory 和 Transit Gateway 目前的跨區域限制，AMS 多帳戶登陸區域內的所有資源都會部署在您選擇的單一 AWS 區域內。

組織單位

典型的 AMS 多帳戶登陸區域由四個最上層組織單位 (OUs) 組成：

- 核心組織單位 (OU) (用來將帳戶分組，以單一單位管理)
- 應用程式 OU
- 客戶管理的 OU
- 加速 OU

AMS 受管多帳戶登陸區域也可讓您建立自訂 OUs 以分組和組織 AWS 帳戶，並將自訂 SCPs 與其建立關聯；如需執行此操作的範例，請參閱[管理帳戶 | 建立自訂 OUs 和管理帳戶 | 分別建立自訂 SCP \(需要檢閱 \)](#)。AMS 提供四個可請求新 OUs 和帳戶的現有 OUs：加速、應用程式 > 受管、應用程式 > 開發和客戶受管。

- 加速 OU：

這是 AMS 多帳戶登陸區域 (MALZ) 中最上層的 OU。此 OU 下的帳戶是由具有 RFC 的 AMS 佈建 (部署 | 受管登陸區域 | 管理帳戶 | 建立加速帳戶，變更類型 ID：ct-2p93tyd5angmi)。在這些加速應用程式帳戶中，您可以受益於加速營運服務，例如監控和提醒、事件管理、安全管理和備份管理。如需詳細資訊，請參閱 [AMS Accelerate 帳戶](#)。

- 應用程式 > 受管 OU：

在 Application OU 的這個子組織單位中，帳戶完全由 AMS 管理，包括所有操作任務。操作任務包括服務請求管理、事件管理、安全管理、持續性管理、修補程式管理、成本最佳化、監控和事件管理。這些任務會針對您基礎設施的管理執行。您可以視需要建立多個子 OUs，直到達到 AWS 組織的巢狀 OUs 上限為止。如需詳細資訊，請參閱 [AWS Organizations 的配額](#)。

- 應用程式 > 開發 OU：

在 AMS 受管登陸區域中應用程式 OU 的這個子 OU 下，帳戶是[開發人員模式](#)帳戶，可提供您在 AMS 變更管理程序之外佈建和更新 AWS 資源的更高許可。此 OU 也支援視需要建立新的子系 OU。

- 客戶受管 OU：

這是 AMS 多帳戶登陸區域中最上層的 OU。此 OU 下的帳戶是由 AMS 使用 RFC 佈建。在這些帳戶中，工作負載和 AWS 資源的操作是您的責任。此 OU 也支援視需要建立新的子系 OU。

根據最佳實務，我們建議這些 OUs 和自訂請求的子 OUs 下的帳戶根據其功能和政策進行分組。

服務控制政策和 AWS Organization

AWS 為 AWS Organization 中的許可管理提供服務控制政策 (SCPs)。SCPs用於為使用者可以在哪些 OUs 中執行的動作定義額外的護欄。根據預設，AMS 提供一組部署在管理帳戶中 SCPs，可在不同的預設 OU 層級提供保護。如需 SCP 限制，請聯絡您的 CSDM。

您也可以建立自訂 SCPs並將其連接至特定 OUs。您可以使用變更類型 `ct-33ste5yc7hprs` 從您的 管理帳戶請求它們。AMS 接著會檢閱請求SCPs，再將其套用至目標 OUs。如需範例，請參閱[管理帳戶 | 建立自訂 OUs](#)和管理[帳戶 | 建立自訂 SCP \(需要檢閱 \)](#)。

選擇單一 MALZ 或多個 MALZs

下表提供在單一多帳戶登陸區域 (MALZ) 與多個多帳戶登陸區域 (例如兩個多帳戶登陸區域 - Prod 和非 Prod) 之間決定的一些高層級考量。一般而言，選擇取決於個別需求、法律要求和操作實務。

單一多帳戶登陸區域與多個多帳戶登陸區域

實體	單一 AMS 登陸區域	多個 (兩個或更多) 登陸區域
基本成本	較低，最佳化程度約為每月 3,000 美元。	較高，每個環境的額外費用約為 3,000 美元。
計費	單一帳單，因為單一帳單/管理帳戶。	每個多帳戶登陸區域的單獨帳單。目前，AWS Org 不支援單一帳單的多管理帳戶。
現有預留執行個體 (RIs的可攜性	低。AWS RIs目前無法跨多個帳單帳戶轉換。您會將現有的 RIs 重新用於多帳戶登陸區域。	更低。您會將 RIs 重新利用並分配到所有多帳戶登陸區域。
產品分層折扣	高。請參閱 磁碟區折扣 。	低。請參閱 磁碟區折扣 。
初始設定額外負荷 (在專案/遷移時間表上)	低。Active Directory、聯網和單一登入 (SSO) 整合僅限一次。	高。您將為每個登陸區域執行 Active Directory、網路整合和 SSO 整合。這可能會導致任何遷移專案的延遲。
常見服務可設定性	工作量低。您可以設定常見/共用的服務，例如 DNS、備份、監控、記錄等。	大量努力。需要額外的規劃，以解決常見的基礎設施或服務將位於何處。通過

實體	單一 AMS 登陸區域	多個（兩個或更多）登陸區域
		每個登陸區域中多個傳輸閘道 (TGWs) 的流量周遊可能會導致額外費用。
可擴展性	中。AMS 目前的實際限制為每個多帳戶登陸區域 150 個帳戶。在同一帳戶中執行應用程式的多個團隊或供應商可以存取不同團隊擁有的堆疊。此限制可以透過控制對 ServiceNow 層的應用程式特定堆疊的存取來減輕（透過整合 AMS ServiceNow Connector 應用程式和使用標籤）。詢問 AMS 技術交付管理員 (TDMs) 或雲端架構師 (CAs) 如何實作。	高。能夠利用多個多帳戶登陸區域來分配帳戶，同時實現帳戶或應用程式層級的隔離。管理大量帳戶可能會導致營運或成本開銷。
營運風險	（相依）低。操作整合和整備僅限一次。降低程序偏離的機率。	（相依）低。多個整合和操作活動。在此期間多個登陸區域中的偏離可能會導致操作風險。
多 AWS 區域	單一 AWS 區域。AMS 多帳戶登陸區域僅限於單一 AWS 區域。若要跨越多個 AWS 區域，請使用多個多帳戶登陸區域。	多 AWS 區域。使用多個多帳戶登陸區域，您可以將每個 MALZ 部署在一個區域中，並使用傳輸閘道 (TGW) 對等互連。
帳戶遷移或可攜性	是。您可以在同一個 AWS Organization 中將帳戶從一個 OU 移至另一個 OU。	否。AMS 不支援跨登陸區域遷移帳戶，也就是跨 AWS Organizations。工作負載可以透過傳輸閘道 (TGW) 或 VPC 對等互連跨登陸區域進行連接。
變更管理	中。對 TGW、Active Directory (AD) 或傳出（輸出）等常見元件進行破壞性變更可能會影響多帳戶登陸區域中的所有工作負載。不過，對 AMS 受管元件的變更會在內部測試，並在滾動更新中推送。	低。對 TGW、AD 或傳出（輸出）等常見元件進行破壞性變更只會影響該特定多帳戶登陸區域中的工作負載。

實體	單一 AMS 登陸區域	多個（兩個或更多）登陸區域
資料和存取控制	（相依）如果您想要連線至適用於 Prod 和非 Prod 工作負載的不同內部部署 ADs 和網路，請使用低控制。SAML 聯合、TGW 網域和安全群組 (SGs) 也有助於實作必要的控制項。	（相依）如果您想要連線至適用於 Prod 和非 Prod 工作負載的不同內部部署 ADs 和網路，請進行高度控制。針對嚴格的合規要求，使用個別的登陸區域。
合規與安全	（相依）如果有嚴格的合規需要完全隔離材料與非材料工作負載，則為低。AMS 標準已備妥預防性和偵測性控制。	（相依）由於多個多帳戶登陸區域可以透過完全隔離材料與非材料工作負載，協助達成嚴格的合規要求。AMS 標準已備妥預防性和偵測性控制。

建議：如果沒有嚴格的合規或多區域需求，從單一 AMS 多帳戶登陸區域開始，將在成本、安全性、卓越營運和遷移複雜性之間取得良好的平衡。如果遇到任何帳戶或業務限制，您可以隨時設定其他登陸區域。

單一多帳戶登陸區域與多個多帳戶登陸區域FAQs

選擇設定單一多帳戶登陸區域或多個多帳戶登陸區域時的一些常見問題：

Q1：如果遇到任何帳戶限制或業務限制，是否可以從單一多帳戶登陸區域開始，並移至多個多帳戶登陸區域？

答：是。您可以選擇在任何指定時間設定另一個多帳戶登陸區域：

- 需要設定新的帳單付款人帳戶（目前，AWS 不支援單一 AWS 組織中的多付款人帳戶）。
- 一旦填寫多帳戶登陸區域問卷，多帳戶登陸區域基礎建置最多需要 2 週的前置時間。
- 每個多帳戶登陸區域代表增加 ~3,000 USD/每月執行成本。
- 需要 N/W、AD、DNS 和 SSO 整合才能建立新的 MALZ。
- 任何預留執行個體 (RIs)、成本節省計劃將需要為新的多帳戶登陸區域設定 (RIs不可轉移)。
- AMS 多帳戶登陸區域不支援跨多帳戶登陸區域帳戶遷移帳戶，例如跨 AWS Orgs。不過，若要將應用程式從一個帳戶移至另一個帳戶，可以使用標準遷移方法。

Q2：什麼是對基礎/共用基礎設施進行 MALZ 更新/變更，並量化客戶風險的 AMS 方法？提供在程序中包裝哪些保證的詳細資訊。客戶如何放心 MALZ 更新/變更不會影響客戶？客戶是否需要採取任何措施來防止中斷？

答：AMS 使用內部工具遵循嚴格的變更方法，讓我們能夠定義、檢閱、排程和執行客戶環境的變更。

發佈更新的程序會強制執行程式碼檢閱、整合測試、在 Gamma 和 Beta 環境中部署，以及在 Beta 和 Gamma 環境中額外的製作時間和測試，然後再發佈給客戶環境。所有版本都包含轉返程序，並由版本團隊和建立和請求變更的團隊密切監控。發行版本的範圍僅限於 AMS 擁有和佈建的堆疊。平均而言，我們每週至少執行一個版本。

除此之外：

- AMS SLA 適用。根據 AMS 服務描述，任何事件引發的共用基礎設施維護活動都會遵循具備解決權的 SLA 或點數。
- 客戶不需要採取特殊的預防措施，以防止對常見基礎設施的干擾。客戶在 AWS Org 或 Core OU 帳戶中具有唯讀許可，因此客戶無法對 MALZ 核心環境進行任何破壞性變更。所有客戶對核心基礎設施的請求都需要 AMS 檢閱和核准。
- 在 App OU 層級傳播變更之前，客戶可以在個別非產品帳戶層級測試特定組織層級變更，例如 SCPs/角色。它正在 AMS 藍圖上，以允許多個 APP OUs(2020 年第 2 季)，這將進一步緩解進行某些 ORG 層級變更的風險。MALZ 團隊已針對「建置模式」帳戶發行個別的 OU，以確保客戶所有權和個別控制項的明確區隔。
- 其中大多數都是允許 AMS 以有效和有效率的方式操作工作負載的變更，不一定會影響客戶的工作負載。當 AMS 認為共用的基礎設施變更可能會影響客戶的工作負載，然後與客戶的變更時段保持一致。

高階建議，如果符合下列條件，請從多個多帳戶登陸區域開始：

- 如果它可協助您達成任何特定的合規。
- 如果您需要使用多區域。
- 如果您有不同的現場部署 ADs和網路，用於生產/材料與非生產/非材料工作負載，請明確隔離 b/w 工作負載。

多帳戶登陸區域帳戶

主題

- [管理帳戶](#)
- [網路帳戶](#)
- [共用服務帳戶](#)

- [Log Archive 帳戶](#)
- [安全帳戶](#)
- [應用程式帳戶類型](#)
- [AMS 工具帳戶 \(遷移工作負載 \)](#)

管理帳戶

當您開始使用 AMS 時，管理帳戶是您初始的 AWS 帳戶。它利用 AWS Organizations 做為管理帳戶（也稱為支付所有成員帳戶費用的付款人帳戶），讓帳戶能夠建立和財務管理成員帳戶。它包含 AWS 登陸區域 (ALZ) 架構、帳戶組態堆疊集、AWS Organization 服務控制政策 (SCPs 等)。

如需使用管理帳戶的詳細資訊，請參閱[管理帳戶的最佳實務](#)。

下圖提供管理帳戶中所含資源的高階概觀。

管理帳戶中的資源

除了上述標準服務之外，在加入期間不會在管理帳戶中建立其他 AWS 資源。加入 AMS 期間需要下列輸入：

- 管理帳戶 ID：您最初建立的 AWS 帳戶 ID。
- 核心帳戶電子郵件：提供與每個核心帳戶相關聯的電子郵件：聯網、共享服務、記錄和安全帳戶。
- 服務區域：提供將部署您 AMS 登陸區域所有資源的 AWS 區域。

網路帳戶

網路帳戶是 AMS 多帳戶登陸區域帳戶、內部部署網路和輸出流量之間網路路由的中樞。此外，此帳戶包含公有 DMZ 堡壘，是 AMS 工程師存取 AMS 環境中主機的進入點。如需詳細資訊，請參閱下列網路帳戶的高階圖表。

網路帳戶架構

下圖說明 AMS 多帳戶登陸區域環境，顯示跨帳戶的網路流量，並且是高可用性設定的範例。

AMS 會根據我們的標準範本和您在加入期間提供的所選選項，為您設定聯網的所有層面。標準 AWS 網路設計會套用至您的 AWS 帳戶，並為您建立 VPC，並透過 VPN 或 Direct Connect 連線至 AMS。如需 Direct Connect 的詳細資訊，請參閱 [AWS Direct Connect](#)。標準 VPCs 包括 DMZ、共用服務和應用程式子網路。在加入過程中，可能會請求和建立額外的 VPCs，以符合您的需求（例如，客戶部門、合作夥伴）。加入後，您會收到網路圖表：說明網路設定方式的環境文件。

Note

如需所有作用中服務的預設服務限制和限制的相關資訊，請參閱 [AWS 服務限制](#) 文件。

我們的網路設計是以 Amazon [「最低權限原則」](#) 為基礎建置。為了達成此目的，我們透過 DMZ 路由所有流量、輸入和輸出，但來自信任網路的流量除外。唯一信任的網路是透過使用 VPN 和/或 AWS Direct Connect (DX) 在內部部署環境和 VPC 之間設定的網路。透過使用堡壘執行個體授予存取權，從而防止直接存取任何生產資源。您的所有應用程式和資源都位於可透過公有負載平衡器連線的私有子網路內。公有輸出流量會透過輸出 VPC 中的 NAT 閘道（在網路帳戶中）流向網際網路閘道，然後流向網際網路。或者，流量可以透過 VPN 或 Direct Connect 流向內部部署環境。

私有網路連線至 AMS 多帳戶登陸區域環境

AWS 透過虛擬私有網路 (VPN) 連線或專用線路與 AWS Direct Connect 提供私有連線。多帳戶環境中的私有連線，是使用下列其中一種方法設定：

- 使用 Transit Gateway 的集中式 Edge 連線
- 將 Direct Connect (DX) 和/或 VPN 連線至帳戶虛擬私有雲端 (VPCs)

使用傳輸閘道的集中式邊緣連線

AWS Transit Gateway 是一項服務，可讓您將 VPCs 和內部部署網路連線至單一閘道。傳輸閘道 (TGW) 可用來合併現有的邊緣連線，並透過單一輸入/輸出點路由。傳輸閘道會在您 AMS 多帳戶環境的網路帳戶中建立。如需傳輸閘道的詳細資訊，請參閱 [AWS Transit Gateway](#)。

AWS Direct Connect (DX) 閘道用於透過傳輸虛擬介面將 DX 連接連接到傳輸閘道 VPCs VPNs。您將 Direct Connect 閘道與傳輸閘道建立關聯。然後，為您的 AWS Direct Connect 連線至 Direct Connect 閘道建立傳輸虛擬介面。如需 DX 虛擬介面的資訊，請參閱 [AWS Direct Connect 虛擬介面](#)。

此組態具有以下好處。您可以：

- 管理相同 AWS 區域中多個 VPCs 或 VPNs 單一連線。
- 將字首從內部部署公告至 AWS，以及從 AWS 公告至內部部署。

Note

如需搭配 AWS 服務使用 DX 的詳細資訊，請參閱彈性工具組一節 [Classic](#)。如需詳細資訊，請參閱 [傳輸閘道關聯](#)。

若要提高連線能力，建議您從不同 AWS Direct Connect 位置將至少兩個傳輸虛擬介面連接至 Direct Connect 閘道。如需詳細資訊，請參閱 [AWS Direct Connect 彈性建議](#)。

將 DX 或 VPN 連線至帳戶 VPCs

使用此選項時，您 AMS 多帳戶登陸區域中 VPCs 會直接連線至 Direct Connect 或 VPN。流量會直接從 VPCs 流向 Direct Connect 或 VPN，而不會周遊傳輸閘道。

網路帳戶中的資源

如聯網帳戶圖表所示，下列元件會在帳戶中建立，並需要您的輸入。

網路帳戶包含兩個 VPCs：輸出 VPC 和 DMZ VPC，也稱為周邊 VPC。

AWS Network Manager

AWS Network Manager 是一項服務，可讓您將傳輸閘道 (TGW) 網路視覺化，而無須支付 AMS 額外費用。它提供 AWS 資源和內部部署網路的集中式網路監控、拓撲圖和地理地圖中私有網路的單一全域檢視，以及使用率指標，例如位元組輸入/輸出、封包輸入/輸出、捨棄的封包，以及拓撲、路由和上/下連線狀態的變更提醒。如需相關資訊，請參閱 [AWS Network Manager](#)。

使用下列其中一個角色來存取此資源：

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

輸出 VPC

輸出 VPC 主要用於輸出流量到網際網路，由最多三個可用區域 (AZs) 中的公有/私有子網路組成。網路位址轉譯 (NAT) 閘道佈建在公有子網路中，傳輸閘道 (TGW) VPC 連接則建立在私有子網路中。來自所有網路的輸出或傳出網際網路流量會透過 TGW 透過私有子網路進入，然後透過 VPC 路由表路由至 NAT。

對於在公有子網路中包含公開應用程式的 VPCs，來自網際網路的流量會包含在該 VPC 中。傳回流量不會路由至 TGW 或輸出 VPC，而是透過 VPC 中的網際網路閘道 (IGW) 傳回。

Note

網路 VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.16.0/24。這是您 VPC 的主要 CIDR 區塊。

AMS 多帳戶登陸區域團隊建議 24 的範圍（具有更多 IP 地址），以便在未來部署其他資源/設備時提供一些緩衝。

Managed Palo Alto 輸出防火牆

AMS 提供受管 Palo Alto 輸出防火牆解決方案，可為多帳戶登陸區域環境（不包括公有服務）中的所有網路啟用網際網路繫結傳出流量篩選。此解決方案結合了領先業界的防火牆技術 (Palo Alto VM-300) 與 AMS 的基礎設施管理功能，可在合規的操作環境中部署、監控、管理、擴展和還原基礎設施。包括 Palo Alto Networks 在內的第三方無法存取防火牆；它們僅由 AMS 工程師管理。

流量控制

受管傳出防火牆解決方案會管理網域允許清單，其中包含備份和修補程式等服務所需的 AMS 網域，以及您定義的網域。當傳出網際網路流量路由到防火牆時，會開啟工作階段、評估流量，如果符合允許的網域，流量會轉送到目的地。

架構

受管輸出防火牆解決方案遵循高可用性模型，其中會根據可用區域 (AZs) 的數量部署兩到三個防火牆。解決方案利用來自預設輸出 VPC 的部分 IP 空間，但也為管理防火牆所需的其他資源佈建 VPC 延伸 (/24)。

網路流程

在高階，公有輸出流量路由保持不變，但流量從輸出 VPC 路由到網際網路的方式除外：

1. 目的地為網際網路的輸出流量會透過 VPC 路由表傳送至傳輸閘道 (TGW)
2. TGW 會透過 TGW 路由表將流量路由至輸出 VPC
3. VPC 透過私有子網路路由表將流量路由至網際網路
 - a. 在預設的多帳戶登陸區域環境中，網際網路流量會直接傳送到網路位址轉譯 (NAT) 閘道。受管防火牆解決方案會重新設定私有子網路路由表，將預設路由 (0.0.0.0/0) 指向防火牆介面。

防火牆本身包含三個界面：

1. 信任的界面：用於接收要處理的流量的私有界面。
2. 不受信任的界面：將流量傳送至網際網路的公有界面。由於防火牆執行 NAT，外部伺服器接受來自這些公有 IP 地址的請求。
3. 管理界面：防火牆 API、更新、主控台等的私有界面。

在所有路由中，流量都會維持在相同的可用區域 (AZ) 內，以減少跨可用區域流量。流量只會在容錯移轉發生時跨越 AZs。

允許清單修改

加入後，ams-allowlist 會建立名為 的預設允許清單，其中包含 AMS 所需的公有端點，以及用於修補 Windows 和 Linux 主機的公有端點。操作完成後，您可以在管理 | 受管防火牆 | 傳出 (Palo Alto) 類別下的 AMS 主控台中建立 RFC 的，以建立或刪除允許清單，或修改網域。請注意，ams-allowlist 無法修改。RFC 的是以完全自動化處理（並非手動）。

自訂安全政策

安全政策會根據流量屬性來決定是否封鎖或允許工作階段，例如來源和目的地安全區域、來源和目的地 IP 地址，以及服務。全自動化 RFCs 支援自訂安全政策。您可以在 Management | Managed Firewall | Outbound (Palo Alto) 類別中找到建立或刪除安全政策 CTs，也可以在 Deployment | Managed Firewall | Outbound (Palo Alto) 類別中找到編輯現有安全政策的 CT。您將能夠建立新的安全政策、修改安全政策或刪除安全政策。

Note

ams-allowlist 無法修改預設安全政策

CloudWatch PA 輸出儀表板

您可以在 CloudWatch 中找到兩個儀表板，以提供 Palo Alto (PA) 的彙總檢視。AMS-MF-PA-Egress-Config-Dashboard 提供 PA 組態概觀、允許清單的連結，以及包含其屬性的所有安全政策清單。AMS-MF-PA-Egress-Dashboard 可以自訂來篩選流量日誌。例如，若要建立安全政策的儀表板，您可以使用下列篩選條件建立 RFC：

[illegible]

容錯移轉模型

防火牆解決方案包含兩到三個 Palo Alto (PA) 主機（每個可用區域一個）。運作狀態檢查 Canary 會以固定排程執行，以評估主機的運作狀態。如果主機識別為運作狀態不良，AMS 會收到通知，並透過路由表變更，自動將該 AZ 的流量轉移到不同 AZ 中運作狀態良好的主機。由於運作狀態檢查工作流程持續執行，如果主機因為暫時性問題或手動修復而再次運作狀態良好，則流量會使用運作狀態良好的主機切換回正確的可用區域。

擴展

AMS 會監控防火牆的輸送量和擴展限制。當輸送量限制超過較低的浮水印閾值 (CPU/網路) 時，AMS 會收到提醒。低浮水印閾值表示資源接近飽和，到達 AMS 將評估一段時間內指標的時間點，並尋求擴展解決方案的建議。

備份與恢復

備份會在初始啟動期間、任何組態變更後，以及定期間隔建立。初始啟動備份是以每個主機為基礎建立，但組態變更和定期間隔備份會在叫用備份工作流時跨所有防火牆主機執行。AMS 工程師可以在這些時段之外建立其他備份，或應要求提供備份詳細資訊。

如有需要，AMS 工程師可以執行組態備份的還原。如果需要還原，則會在所有主機之間進行，以保持主機之間的組態同步。

當主機需要完整回收執行個體時，也會發生還原。佈建新的 EC2 執行個體時，會自動還原最新的備份。一般而言，主機不會定期回收，並且會保留給嚴重故障或必要的 AMI 交換。主機資源回收會手動啟動，並在資源回收發生之前通知您。

除了防火牆組態備份之外，您的特定允許清單規則會分別備份。修改您定義的允許清單規則時，會自動建立備份。如有必要，AMS 工程師可以執行允許清單備份的還原。

更新

AMS Managed Firewall Solution 需要一段時間的各種更新，才能對系統、其他功能或防火牆作業系統 (OS) 或軟體進行更新。

大多數變更不會影響執行環境，例如更新自動化基礎設施，但防火牆執行個體輪換或作業系統更新等其他變更可能會導致中斷。評估因更新造成的潛在服務中斷時，AMS 會與您協調以適應維護時段。

運算子存取

AMS 運算子會使用其 ActiveDirectory 登入資料登入 Palo Alto 裝置來執行操作（例如修補、回應事件等）。解決方案會保留標準 AMS Operator 身分驗證和組態變更日誌，以追蹤在 Palo Alto 主機上執行的動作。

預設日誌

根據預設，防火牆產生的日誌位於每個防火牆的本機儲存體中。加班，本機日誌將根據儲存使用率刪除。AMS 解決方案可將日誌從機器即時傳送至 CloudWatch 日誌；如需詳細資訊，請參閱 [CloudWatch Logs 整合](#)。

AMS 工程師仍然能夠在需要時直接從機器查詢和匯出日誌。此外，日誌可以運送到客戶擁有的 Panorama；如需詳細資訊，請參閱 [全景整合](#)。

解決方案收集的日誌如下：

RFC 狀態碼

日誌類型	描述
流量	顯示每個工作階段開始和結束的項目。每個項目都包含日期和時間、來源和目的地區域、地址和連接埠、應用程式名稱、套用至流程的安全規則名稱、規則動作（允許、拒絕或捨棄）、輸入和輸出界面、位元組數，以及工作階段結束原因。 類型欄指出項目是用於工作階段的開始或結束，還是工作階段遭到拒絕或捨棄。"drop" 表示封鎖指定 "any" 應用程式之流量的安全規則，而 "deny" 表示規則已識別特定應用程式。 如果在識別應用程式之前捨棄流量，例如當規則捨棄特定服務的所有流量時，應用程式會顯示為「不適用」。
威脅	顯示防火牆產生之每個安全警示的項目。每個項目都包含日期和時間、威脅名稱或 URL、來源和目的地區域、地址和連接埠、應用程式名稱，以及警示動作（允許或封鎖）和嚴重性。 類型欄指出威脅類型，例如「病毒」或「間諜軟體」；名稱欄是威脅描述或 URL；類別欄是威脅類別（例如「鍵盤記錄器」）或 URL 類別。
URL 篩選	顯示 URL 篩選條件的日誌，可控制對網站的存取，以及使用者是否可以将登入資料提交至網站。
組態	顯示每個組態變更的項目。每個項目都包含日期和時間、管理員使用者名稱、進行變更的 IP 地址、用戶端類型 (Web 介面或 CLI)、命令執行類型、命令是否成功或失敗、組態路徑，以及變更前後的值。
系統	顯示每個系統事件的項目。每個項目都包含日期和時間、事件嚴重性和事件描述。
警報	警示日誌會記錄系統所產生警示的詳細資訊。此日誌中的資訊也會在警示中報告。請參閱「定義警示設定」。
身分驗證	顯示當最終使用者嘗試存取由身分驗證政策規則控制存取的網路資源時，所發生身分驗證事件的相關資訊。使用者可以使用此資訊來協助疑難排解存取問題，並視需要調整使用者身分驗證政策。搭配相互關聯物件，使用

日誌類型	描述
	者也可以使用身分驗證日誌來識別使用者網路上的可疑活動，例如暴力攻擊。 或者，使用者可以設定身分驗證規則來記錄身分驗證逾時。這些逾時與使用者只需要對資源進行身分驗證一次，但可以重複存取的時間有關。查看逾時的相關資訊，有助於使用者決定是否及如何調整逾時。
統一	在單一檢視中顯示最新的流量、威脅、URL 篩選、WildFire 提交和資料篩選日誌項目。集體日誌檢視可讓使用者一起調查和篩選這些不同類型的日誌（而不是分別搜尋每個日誌集）。或者，使用者可以選擇要顯示的日誌類型：按一下篩選欄位左側的箭頭，然後選取流量、威脅、url、資料和/或森林大火，以僅顯示選取的日誌類型。

事件管理

AMS 會持續監控防火牆的容量、運作狀態和可用性。從防火牆產生的指標，以及 AWS/AMS 產生的指標，可用來建立 AMS 操作工程師收到的警示，他們將調查並解決問題。目前的警示涵蓋下列案例：

事件警示：

- 防火牆資料平面 CPU 使用率
 - CPU 使用率 - 資料平面 CPU（處理流量）
- 防火牆資料平面封包使用率高於 80%
 - 封包使用率 - 資料平面（處理流量）
- 防火牆資料平面工作階段使用率
- 防火牆資料平面工作階段作用中
- 防火牆 CPU 使用率彙總
 - 所有 CPU CPUs 使用率
- 依可用區域進行容錯移轉
 - 在 AZ 中發生容錯移轉時的警示
- 運作狀態不佳的 Syslog 主機
 - Syslog 主機運作狀態檢查失敗

管理警示：

- 運作狀態檢查監控失敗警示
 - 當運作狀態檢查工作流程意外失敗時
 - 這是針對工作流程本身，而不是防火牆運作狀態檢查失敗時
- 密碼輪換失敗警示
 - 當密碼輪換失敗時
 - API/服務使用者密碼每 90 天輪換一次

指標

所有指標都會擷取並儲存在網路帳戶中的 CloudWatch 中。您可以透過取得網路帳戶的主控制台存取權，以及導覽至 CloudWatch 主控台來檢視這些內容。您可以在指標索引標籤下檢視個別指標，也可以透過導覽至儀表板索引標籤，然後選取 AMS-MF-PA-Egress-Dashboard 來檢視特定指標和彙總指標的單一窗格儀表板檢視。

自訂指標：

- 運作狀態檢查
 - 命名空間：AMS/MF/PA/輸出
 - PARouteTableConnectionsByAZ
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- 防火牆產生
 - 命名空間：AMS/MF/PA/Egress/<instance-id>
 - DataPlaneCPUUtilizationPct
 - DataPlanePacketBufferUtilization
 - panGPGatewayUtilizationPct
 - panSessionActive
 - panSessionUtilization

CloudWatch Logs 整合

CloudWatch Logs 整合會將日誌從防火牆轉送到 CloudWatch Logs，以降低由於本機儲存使用率而遺失日誌的風險。當防火牆產生日誌時，日誌會即時填入，並且可以透過主控台或 API 隨需檢視。

可以使用 CloudWatch Insights 建置複雜的查詢以進行日誌分析或匯出至 CSV。此外，自訂 AMS Managed Firewall CloudWatch 儀表板也會顯示特定流量日誌查詢的快速檢視，以及一段時間內流量和政策命中次數的圖形視覺化。使用 CloudWatch 日誌也可以原生整合其他 AWS 服務，例如 AWS Kinesis。

Note

PA 日誌無法直接轉送至現有的內部部署或第三方 Syslog 收集器。AMS Managed Firewall 解決方案可將 PA 機器的日誌即時運送到 AWS CloudWatch Logs。您可以使用 CloudWatch Logs Insight 功能來執行隨機操作查詢。此外，日誌可以運送到 Palo Alto 的 Panorama 管理解決方案。CloudWatch 日誌也可以使用 CloudWatch Subscription Filters 轉送到其他目的地。在下一節中進一步了解 Panorama。若要進一步了解 Splunk，請參閱[與 Splunk 整合](#)。

全景整合

AMS Managed Firewall 可以選擇性地與您現有的 Panorama 整合。這可讓您從 Panorama 檢視防火牆組態，或從防火牆將日誌轉送至 Panorama。與 AMS Managed Firewall 的 Panorama 整合是唯讀的，不允許從 Panorama 對防火牆進行組態變更。Panorama 由您完全管理和設定，AMS 僅負責設定防火牆以與其通訊。

授權

AMS Managed Firewall 的價格取決於所使用的授權類型、每小時或自備授權 (BYOL)，以及設備執行的執行個體大小。您必須透過 AWS Marketplace 訂購您偏好的執行個體大小和 Palo Alto 防火牆授權。

- Marketplace 授權：從 MALZ 中的網路帳戶接受 VM 系列新一代防火牆套件 1 的條款與條件。
- BYOL 授權：從 MALZ 的網路帳戶接受 VM 系列新一代防火牆 (BYOL) 的條款與條件，並共用購買授權給 AMS 後取得的「BYOL 驗證程式碼」。

限制

目前，AMS 支援 VM-300 系列或 VM-500 系列防火牆。您可以在此處找到組態：[AWS EC2 執行個體上的 VM 系列模型](#)、

Note

AMS 解決方案會在主動-主動模式下執行，因為其 AZ 中的每個 PA 執行個體都會處理其受尊重 AZ 的輸出流量。因此，使用兩個 AZs，每個 PA 執行個體處理高達 5 Gbps 的輸出流量，並有效地在兩個 AZs 中提供整體 10 Gbps 輸送量。對於每個 AZ 中的所有限制也是如此。如果 AMS 運作狀態檢查失敗，我們會將流量從具有錯誤 PA 的 AZ 轉移到另一個 AZ，並且在執行個體替換期間，容量會減少到剩餘的 AZs 限制。

AMS 目前不支援 AWS Marketplace 上可用的其他 Palo Alto 套件；例如，您無法要求「VM 系列新一代防火牆套件 2」。請注意，使用 Palo Alto 的 AMS Managed Firewall 解決方案目前僅提供輸出流量篩選產品，因此使用進階 VM 系列套件不會提供任何額外的功能或優點。

加入要求

- 您必須檢閱並接受 AWS Marketplace 中來自 Palo Alto 的 VM 系列新一代防火牆的條款與條件。
- 您必須根據預期的工作負載，確認要使用的執行個體大小。
- 您必須提供不會與多帳戶登陸區域環境或內部部署中的網路衝突的 /24 CIDR 區塊。它必須與輸出 VPC 的類別相同（解決方案為輸出 VPC 佈建 /24 VPC 延伸）。

定價

AMS Managed Firewall 基礎基礎設施成本分為三個主要驅動程式：託管 Palo Alto 防火牆的 EC2 執行個體、軟體授權 Palo Alto VM 系列授權，以及 CloudWatch Integrations。

下列定價是以 VM-300 系列防火牆為基礎。

- EC2 執行個體：Palo Alto 防火牆會以 2-3 個 EC2 執行個體的高可用性模型執行，其中執行個體是以預期的工作負載為基礎。執行個體的成本取決於 AZs 的區域和數量
 - 例如 us-east-1、m5.xlarge、3AZs
 - $\$0.192 * 24 * 30 * 3 = \$414.72$
 - <https://aws.amazon.com/ec2/pricing/on-demand/>
 - Palo Alto 授權：Palo Alto VM-300 新一代防火牆的軟體授權成本取決於 AZ 數量和執行個體類型。
 - 例如 us-east-1、m5.xlarge、3AZs
 - $\$0.87 * 24 * 30 * 3 = \$1879.20$
 - https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing

- CloudWatch Logs 整合：CloudWatch Logs 整合使用 SysLog 伺服器 (EC2 - t3.medium)、NLB 和 CloudWatch Logs。伺服器的成本是根據 AZs 的區域和數量而定，而 NLB/CloudWatch 日誌的成本會根據流量使用率而有所不同。
 - 例如 us-east-1、t3.medium、3AZ
 - $\$0.0416 * 24 * 30 * 3 = \$89.86$
 - <https://aws.amazon.com/ec2/pricing/on-demand/>
 - <https://aws.amazon.com/cloudwatch/pricing/>

周邊 (DMZ) VPC

周邊或 DMZ、VPC 包含 AMS Operations 工程師存取 AMS 網路所需的資源。它包含跨 2-3 個 AZs 公有子網路，並在 Auto Scaling 群組 (ASG) 中包含 SSH Bastions 主機，供 AMS Operations 工程師登入或通道。連接至 DMZ 堡壘的安全群組包含來自 Amazon Corp Networks 的連接埠 22 傳入規則。

DMZ VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.16.0/24。這是您 VPC 的主要 CIDR 區塊。

Note

AMS 團隊建議 24 的範圍（具有更多 IP 地址），以便在將來部署防火牆等其他資源時提供一些緩衝。

AWS Transit Gateway

AWS Transit Gateway (TGW) 是一項服務，可讓您將 Amazon Virtual Private Clouds (VPCs) 和內部部署網路連線至單一閘道。傳輸閘道是處理 AMS 帳戶網路與外部網路之間路由的網路骨幹。如需傳輸閘道的相關資訊，請參閱 [AWS Transit Gateway](#)。

提供下列輸入來建立此資源：

- 傳輸閘道 ASN 編號*：為您的傳輸閘道提供私有自治系統編號 (ASN)。此為邊界閘道協定 (BGP) 工作階段的 AWS 端 ASN。16 位元的 ASN 範圍應介於 64512 到 65534。

共用服務帳戶

共用服務帳戶可做為大多數 AMS 資料平面服務的中樞。帳戶包含存取管理 (AD)、端點安全管理 (Trend Micro) 所需的基礎設施和資源，並包含客戶堡壘 (SSH/RDP)。共享服務帳戶中包含的資源的高階概觀如下圖所示。

共用服務 VPC 由三個可用區域 (AZs) 中的 AD 子網路、EPS 子網路和客戶堡壘子網路組成。共享服務 VPC 中建立的資源列於下方，需要您的輸入。

- 共用服務 VPC CIDR 範圍：建立 VPC 時，您必須以無類別網域間路由 (CIDR) 區塊的形式指定 VPC 的 IPv4 地址範圍；例如 10.0.1.0/24。這是您 VPC 的主要 CIDR 區塊。

Note

AMS 團隊建議 /23 的範圍。

- Active Directory 詳細資訊：Microsoft Active Directory (AD) 用於所有 AMS 多帳戶登陸區域帳戶的使用者/資源管理、身分驗證/授權和 DNS。AMS AD 也會設定對 Active Directory 的單向信任，以進行信任型身分驗證。建立 AD 需要下列輸入：
 - 網域完整網域名稱 (FQDN)：AWS Managed Microsoft AD 目錄的完整網域名稱。網域不應是您網路中現有網域的現有網域或子網域。
 - 網域 NetBIOS 名稱：如果您未指定 NetBIOS 名稱，AMS 會將名稱預設為目錄 DNS 的第一部分。例如，DNS corp.example.com 目錄的 corp。
- Trend Micro – 端點保護安全 (EPS)：Trend Micro 端點保護 (EPS) 是 AMS 中用於作業系統安全的主要元件。系統包含 Deep Security Manager (DSM)、EC2 執行個體、轉送 EC2 執行個體，以及存在於所有資料平面和客戶 EC2 執行個體中的代理程式。

您必須在 `EPSTMarketplaceSubscriptionRole` 共用服務帳戶中擔任，並訂閱 Trend Micro Deep Security (BYOL) AMI 或 Trend Micro Deep Security (Marketplace)。

建立 EPS 需要下列預設輸入（如果您想要從預設值變更）：

- 轉送執行個體類型：預設值 - m5.large
- DSM 執行個體類型：預設值 - m5.xlarge
- 資料庫執行個體大小：預設值 - 200 GB
- RDS 執行個體類型：預設值 - db.m5.large

- 客戶堡壘：共用服務帳戶中會提供 SSH 或 RDP 堡壘（或兩者），供您存取 AMS 環境中的其他主機。若要以使用者身分存取 AMS 網路 (SSH/RDP)，您必須使用「客戶」堡壘做為進入點。網路路徑源自內部部署網路，經過 DX/VPN 到傳輸閘道 (TGW)，然後路由到共用服務 VPC。一旦您能夠存取堡壘，就可以跳到 AMS 環境中的其他主機，前提是已授予存取請求。
- SSH 堡壘需要下列輸入。
 - SSH 堡壘所需執行個體容量：預設值 - 2。
 - SSH 堡壘上限執行個體：預設值 - 4。
 - SSH 堡壘最小執行個體：預設值 -2。
 - SSH 堡壘執行個體類型：預設值 - m5.large（可以變更為節省成本，例如 t3.medium）。
 - SSH 堡壘傳入 CIDRs：您網路中的使用者存取 SSH 堡壘的 IP 地址範圍。
- Windows RDP 堡壘需要下列輸入。
 - RDP 堡壘執行個體類型：預設值 - t3.medium。
 - RDP 堡壘所需最短工作階段：預設值 - 2。
 - RDP 工作階段上限：預設值 -10。
 - RDP 堡壘組態類型：您可以選擇下列其中一個組態
 - SecureStandard = 使用者會收到一個堡壘，只有一個使用者可以連接到堡壘。
 - SecureHA = 使用者在兩個不同的可用區域中接收兩個堡壘以連接到，只有一個使用者可以連接到堡壘。
 - SharedStandard = 使用者會收到一個要連線的堡壘，兩個使用者可以一次連線到相同的堡壘。
 - SharedHA = 使用者可以在兩個不同的可用區域中接收兩個堡壘以連接到，而兩個使用者可以一次連接到相同的堡壘。
 - 客戶 RDP 傳入 CIDRs：IP 地址範圍，您網路中的使用者將從其中存取 RDP 堡壘。

共用服務的更新：多帳戶登陸區域

AMS 會每月將資料平面版本套用至受管帳戶，恕不另行通知。

AMS 使用核心 OU 來提供共用服務，例如存取、聯網、EPS、日誌儲存、多帳戶登陸區域中的提醒彙總。AMS 負責解決這些共用服務的漏洞、修補和部署。AMS 會定期更新用於提供這些共用服務的資源，讓使用者可存取最新功能和安全性更新。更新通常每月進行。屬於這些更新一部分的資源包括：

- 屬於核心 OU 的帳戶。

管理帳戶、共享服務帳戶、網路帳戶、安全帳戶和日誌封存帳戶具有 RDP 和 SSH 堡壘、代理、管理主機和端點安全 (EPS) 的資源，通常每月更新。AMS 使用不可變的 EC2 部署做為共用服務基礎設施的一部分。

- 整合最新更新的新 AMS AMIs。

Note

AMS 運算子會在執行資料平面變更時利用內部警示抑制變更類型 (CT)，且該 CT 的 RFC 會出現在您的 RFC 清單中。這是因為在部署資料平面版本時，各種基礎設施可能會關閉、重新啟動、離線，或者可能會有 CPU 峰值或其他觸發警示的部署效果，這些警示在資料平面部署期間是不必要的。部署完成後，所有基礎設施都會驗證為正確執行，且警示會重新啟用。

Log Archive 帳戶

Log Archive 帳戶做為在 AMS 多帳戶登陸區域環境中封存日誌的中心中樞。帳戶中有一個 S3 儲存貯體，其中包含來自每個 AMS 多帳戶登陸區域環境帳戶的 AWS CloudTrail 和 AWS Config 日誌檔案副本。您可以使用此帳戶搭配 AWS Firehose 或 Splunk 等集中式記錄解決方案。此帳戶的 AMS 存取僅限於少數使用者；僅限稽核人員和安全團隊進行與帳戶活動相關的合規和鑑識調查。

安全帳戶

安全帳戶是用於存放安全相關操作的中樞，也是將通知和提醒漏接至 AMS 控制平面服務的要點。此外，安全帳戶會存放 Amazon Guard Duty 管理帳戶和 AWS Config 彙總工具。

應用程式帳戶類型

應用程式帳戶是您用來託管工作負載的 AMS 受管登陸區域架構中的 AWS 帳戶。AMS 提供三種類型的應用程式帳戶：

- [AMS 受管應用程式帳戶](#)
- [AMS Accelerate 帳戶](#)
- [客戶受管應用程式帳戶](#)

根據應用程式帳戶類型，應用程式帳戶會在 AWS Organizations 中的不同 OUs 中分組：

- 根 OU :
 1. 應用程式 OU
 - 受管 OU : AMS 受管帳戶
 - 開發 OU : 啟用開發人員模式的 AMS 受管帳戶
 2. 加速 OU : AMS 加速應用程式帳戶
 3. 客戶受管 OU : 客戶受管應用程式帳戶

應用程式帳戶是透過從 管理帳戶提交的 RFC 佈建：

- 使用 VPC [ct-1zdasmc2ewzrs](#) 建立應用程式帳戶
- 建立加速帳戶 [ct-2p93tyd5angmi](#)
- 建立客戶受管應用程式帳戶 [ct-3pwbixz27n3tn](#)

AMS 受管應用程式帳戶

完全由 AMS 管理的應用程式帳戶稱為 AMS 受管應用程式帳戶，其中部分或所有操作任務，例如服務請求管理、事件管理、安全管理、持續性管理（備份）、修補程式管理、成本最佳化，或基礎設施的監控和事件管理，皆由 AMS 執行。

AMS 執行的任務數量取決於您選擇的變更管理模式。AMS 受管帳戶支援不同的變更管理模式：

- [RFC 模式](#)
- [AMS 中的直接變更模式](#)
- [AMS 和 AWS Service Catalog](#)
- [AMS 進階開發人員模式](#)
- [AMS 中的自助式佈建模式](#)

如需變更管理和不同模式的詳細資訊，請參閱 [變更管理模式](#)。

有些 AWS 服務可在 AMS 受管帳戶中使用，無需 AMS 管理。這些 AWS 服務的清單以及如何將其新增至您的 AMS 帳戶，如 [自助式佈建](#) 一節所述。

AMS Accelerate 帳戶

AMS Accelerate 是 AMS 操作計劃，可操作支援工作負載的 AWS 基礎設施。您可以受益於 AMS Accelerate 操作服務，例如監控和提醒、事件管理、安全管理和備份管理，而無需進行新的遷移、遇到

停機時間或變更您使用 AWS 的方式。AMS Accelerate 也為需要定期修補的 EC2 型工作負載提供選用的修補程式附加元件。

使用 AMS Accelerate，您可以自由地原生使用、設定和部署所有 AWS 服務，或使用您偏好的工具。您將使用您偏好的存取和變更機制，同時 AMS 會一致地套用經過驗證的實務，以協助擴展您的團隊、最佳化成本、提高安全性和效率，以及改善彈性。

Note

AMS Advanced 中的 AMS Accelerate 帳戶沒有 AMS 變更管理 (RFCs) 或 AMS Advanced 主控台。相反地，它們具有 AMS Accelerate 主控台和功能。

加速帳戶只能從您的 AMS 多帳戶登陸區域管理帳戶佈建。Accelerate 提供不同的操作功能。如需進一步了解，請參閱[加速服務描述](#)。

- 您將繼續享受多帳戶登陸區域 (MALZ) 核心帳戶的一些功能，例如集中式記錄、單一帳單、安全帳戶和 SCPs 中的組態彙總器。
- AMS Accelerate 不提供某些 AMS Advanced 服務，例如 EPS、存取管理、變更管理和佈建。我們建議您遵循後續步驟來存取和設定傳輸閘道 (TGW)。

如需 Accelerate 的詳細資訊，請參閱[什麼是 Accelerate](#)。

建立您的 Accelerate 帳戶

若要建立 Accelerate 帳戶，請依照此處概述的步驟[建立 Accelerate 帳戶](#)。

存取您的 Accelerate 帳戶

在多帳戶登陸區域 (MALZ) 帳戶中佈建 Accelerate 帳戶後，具有[管理存取](#)許可的角色 AccelerateDefaultAdminRole 會位於帳戶中供您擔任。

若要存取新的 Accelerate 帳戶：

1. 使用 CustomerDefaultAssumeRole 角色登入管理帳戶的 IAM 主控台。
2. 在 IAM 主控台的導覽列上，選擇您的使用者名稱。
3. 選擇 Switch Role (切換角色)。如果這是第一次選擇此選項，則頁面會顯示更多資訊。讀取後，選擇 Switch Role (切換角色)。如果清除瀏覽器 cookie，則此頁面可以再次顯示。

- 在切換角色頁面上，輸入加速帳戶 ID 和要擔任的角色名稱：`AccelerateDefaultAdminRole`。

現在您已擁有存取權，您可以建立新的 IAM 角色，以繼續存取您的環境。如果您想要為 Accelerate 帳戶利用 SAML 聯合，請參閱[啟用 SAML 2.0 聯合身分使用者以存取 AWS 管理主控台](#)。

將您的 Accelerate 帳戶與 Transit Gateway 連線

AMS 不會管理 Accelerate 帳戶的網路設定。您可以選擇使用 AWS APIs 管理自己的網路（請參閱[網路解決方案](#)），或使用 AMS MALZ 中部署的現有 Transit Gateway (TGW) 連線至 AMS 管理的 MALZ 網路。

 Note

如果 Accelerate 帳戶位於相同的 AWS 區域，您只能將 VPC 連接到 TGW。如需詳細資訊，請參閱[傳輸閘道](#)。

若要將 Accelerate 帳戶新增至 Transit Gateway，請使用 [部署 | 受管登陸區域 | 網路帳戶 | 新增靜態路由](#) (ct-3r2ckznmt0a59) 變更類型來請求新路由，請包含此資訊：

- **Blackhole**：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。
- **DestinationCidrBlock**：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：10.0.2.0/24。
- **TransitGatewayAttachmentId**：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：tgw-attach-04eb40d1e14ec7272。
- **TransitGatewayRouteTableId**：TGW 路由表的 ID。範例：tgw-rtb-06ddc751c0c0c881c。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與 MALZ 網路中的任何其他 VPCs 通訊。
2. 與您的解決方案架構師一起決定您希望此加速 VPCs 與哪些 VPC 通訊。
3. 提交 [部署 | 受管登陸區域 | 網路帳戶 | 新增靜態路由](#) (ct-3r2ckznmt0a59) 變更類型，包括此資訊：
 - **Blackhole**：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。

- DestinationCidrBlock：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：10.0.2.0/24。
- TransitGatewayAttachmentId：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：tgw-attach-04eb40d1e14ec7272。
- TransitGatewayRouteTableId：TGW 路由表的 ID。範例：tgw-rtb-06ddc751c0c0c881c。

將新的 Accelerate 帳戶 VPC 連線至 AMS 多帳戶登陸區域網路（建立 TGW VPC 連接）：

1. 在您的多帳戶登陸區域聯網帳戶中，開啟 [Amazon VPC 主控台](#)。
2. 在導覽窗格中，選擇 Transit Gateways (傳輸閘道)。記錄您看到的傳輸閘道的 TGW ID。
3. 在您的 Accelerate 帳戶中，開啟 [Amazon VPC 主控台](#)。
4. 在導覽窗格中，選擇傳輸閘道附件 > 建立傳輸閘道附件。做出這些選擇：
 - 針對傳輸閘道 ID，選擇您在步驟 2 中記錄的傳輸閘道 ID。
 - 在 Attachment type (連接類型) 中，選擇 VPC。
 - 在 VPC Attachment (VPC 連接) 中，您可選擇輸入 Attachment name tag (連接名稱標籤) 的名稱。
 - 選擇是否啟用 DNS support (DNS 支援) 和 IPv6 Support (IPv6 支援)。
 - 對於 VPC ID，請選擇要連接至傳輸閘道的 VPC。此 VPC 必須至少有一個子網路與之建立關聯。
 - 在子網路 ID 中，為每個可用區域選取傳輸閘道用來路由流量的一個子網路。您必須選擇至少一個子網路。一個可用區域只能選取一個子網路。
5. 選擇 Create attachment (建立連接)。記錄新建立的 TGW 附件 ID。

將 TGW 連接與路由表建立關聯：

1. 決定要與 VPC 建立關聯的 TGW 路由表。建議您使用部署 | 受管登陸區域 | 網路帳戶 | 建立傳輸閘道路由表 (ct-3dscwaeyi6cup) 變更類型，為加速帳戶 VPCs 建立新的應用程式路由表。
2. 在網路帳戶上提交 [管理 | 受管登陸區域 | 網路帳戶 | 關聯 TGW 連接](#) (ct-3nmhh0qr338q6) RFC，將 VPC 或 TGW 連接與您選取的路由表建立關聯。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與多帳戶登陸區域網路中的任何其他 VPCs 通訊。
2. 與您的解決方案架構師一起決定您希望此加速帳戶 VPCs 與哪些 VPC 通訊。

3. 提交[部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由](#) (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

將 VPC Route 資料表設定為指向 AMS 多帳戶登陸區域傳輸閘道：

1. 與您的解決方案架構師一起決定您要將哪些流量傳送至 AMS 多帳戶登陸區域傳輸閘道。
2. 提交[部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由](#) (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

客戶受管應用程式帳戶

您可以建立 AMS 未以標準方式管理的帳戶。這些帳戶稱為客戶受管帳戶，可讓您完全控制在帳戶中自行操作基礎設施，同時享受由 AMS 管理的集中式架構的優點。

客戶受管帳戶無法存取 AMS 主控台或我們提供的任何服務（修補程式、備份等）。

客戶受管帳戶只能從您的 AMS 多帳戶登陸區域管理帳戶佈建。

不同的 AMS 模式以不同的方式使用應用程式帳戶；若要進一步了解模式，請參閱 [AWS Managed Services 模式](#)。

若要建立您的客戶受管應用程式帳戶，請參閱[管理帳戶 | 建立客戶受管應用程式帳戶](#)。

若要刪除客戶受管應用程式帳戶，請使用[管理帳戶 | 離線應用程式帳戶](#)。（[確認離職](#) CT 不適用於客戶受管應用程式帳戶。）

存取您的客戶受管帳戶

在多帳戶登陸區域中佈建客戶受管帳戶 (CMA) 之後，管理員角色 (MALZ) `CustomerDefaultAdminRole` 會位於帳戶中，供您透過 SAML 聯合身分擔任以設定帳戶。

若要存取 CMA：

1. 使用 `CustomerDefaultAssumeRole` 角色登入管理帳戶的 IAM 主控台。
2. 在 IAM 主控台的導覽列上，選擇您的使用者名稱。
3. 選擇 Switch Role (切換角色)。如果這是第一次選擇此選項，則頁面會顯示更多資訊。讀取後，選擇 Switch Role (切換角色)。如果清除瀏覽器 cookie，則此頁面可以再次顯示
4. 在切換角色頁面上，輸入客戶受管帳戶 ID 和要擔任的角色名稱：`CustomerDefaultAdminRole`。

現在您已擁有存取權，您可以建立新的 IAM 角色，以繼續存取您的環境。如果您想要為 CMA 帳戶利用 SAML 聯合，請參閱[啟用 SAML 2.0 聯合身分使用者以存取 AWS 管理主控台](#)。

將您的 CMA 與 Transit Gateway 連線

AMS 不會管理客戶受管帳戶 (CMAs) 的網路設定。您可以選擇使用 AWS APIs 管理自己的網路（請參閱[網路解決方案](#)），或使用 AMS MALZ 中部署的現有 Transit Gateway (TGW) 連線至 AMS 管理的多帳戶登陸區域網路。

Note

如果 CMA 位於相同的 AWS 區域，您只能將 VPC 連接到 TGW。如需詳細資訊，請參閱[傳輸閘道](#)。

若要將 CMA 新增至 Transit Gateway，請使用[網路帳戶請求新路由 | 新增靜態路由 \(ct-3r2ckznmt0a59\)](#) 變更類型，並包含此資訊：

- Blackhole：True 表示路由的目標無法使用。當傳輸閘道要捨棄靜態路由的流量時，請執行此操作。將流量路由到指定 TGW 連接 ID 的 False。預設值為 false。
- DestinationCidrBlock：用於目的地比對的 IPV4 CIDR 範圍。路由決策是根據最明確的匹配。範例：10.0.2.0/24。
- TransitGatewayAttachmentId：做為路由表目標的 TGW 附件 ID。如果 Blackhole 為 false，則需要此參數，否則將此參數保留空白。範例：tgw-attach-04eb40d1e14ec7272。
- TransitGatewayRouteTableId：TGW 路由表的 ID。範例：tgw-rtb-06ddc751c0c0c881c。

將新的客戶受管 VPC 連線至 AMS 多帳戶登陸區域網路（建立 TGW VPC 連接）：

1. 在您的多帳戶登陸區域聯網帳戶中，開啟 [Amazon VPC 主控台](#)。
2. 在導覽窗格中，選擇傳輸閘道。記錄您看到的傳輸閘道的 TGW ID。
3. 在您的客戶受管帳戶中，開啟 [Amazon VPC 主控台](#)。
4. 在導覽窗格中，選擇傳輸閘道附件 > 建立傳輸閘道附件。做出這些選擇：
 - a. 針對傳輸閘道 ID，選擇您在步驟 2 中記錄的傳輸閘道 ID。
 - b. 在 Attachment type (連接類型) 中，選擇 VPC。
 - c. 在 VPC Attachment (VPC 連接) 中，您可選擇輸入 Attachment name tag (連接名稱標籤) 的名稱。

- d. 選擇是否啟用 DNS support (DNS 支援) 和 IPv6 Support (IPv6 支援)。
 - e. 對於 VPC ID，請選擇要連接至傳輸閘道的 VPC。此 VPC 必須至少有一個子網路與之建立關聯。
 - f. 在子網路 ID 中，為每個可用區域選取傳輸閘道用來路由流量的一個子網路。您必須選擇至少一個子網路。一個可用區域只能選取一個子網路。
5. 選擇 Create attachment (建立連接)。記錄新建立的 TGW 附件 ID。

將 TGW 連接與路由表建立關聯：

決定要與 VPC 建立關聯的 TGW 路由表。我們建議您提交部署 | 受管登陸區域 | 網路帳戶 | 建立傳輸閘道路由表 (ct-3dscwaeyi6cup) RFC，為客戶受管 VPCs 建立新的應用程式路由表。若要將 VPC 或 TGW 連接與您選取的路由表建立關聯，請在網路帳戶上提交部署 | 受管登陸區域 | 網路帳戶 | 關聯 TGW 連接 (ct-3nmhh0qr338q6) RFC。

在 TGW 路由表中建立路由以連線至此 VPC：

1. 根據預設，此 VPC 將無法與多帳戶登陸區域中的任何其他 VPCs 通訊。
2. 與您的解決方案架構師一起決定您希望此客戶受管 VPCs 與哪些 VPC 通訊。提交部署 | 受管登陸區域 | 網路帳戶 | 針對網路帳戶新增靜態路由 (ct-3r2ckznmt0a59) RFC，以建立您需要的 TGW 路由。

 Note

此 CT (ct-3r2ckznmt0a59) 不允許將靜態路由新增至核心路由表 EgressRouteDomain；如果您的 CMA 需要允許輸出流量，請使用 ct-0xdawir96cy7k 提交管理 | 其他 | 其他 (MOO) RFC。

將 VPC Route 資料表設定為指向 AMS 多帳戶登陸區域傳輸閘道：

與您的解決方案架構師一起決定您要將哪些流量傳送至 AMS 多帳戶登陸區域傳輸閘道。更新您的 VPC 路由表，將流量傳送至先前建立的 TGW 連接

取得客戶受管帳戶的操作說明

AMS 可以透過將帳戶加入 AMS Accelerate，協助您操作您在客戶受管帳戶中部署的工作負載。透過 AMS Accelerate，您可以受益於營運服務，例如監控和提醒、事件管理、安全管理和備份管理，而無需進行新的遷移、遇到停機時間或變更使用方式 AWS。AMS Accelerate 也為需要定期修補的 EC2-based 工作負載提供選用的修補程式附加元件。透過 AMS Accelerate，您可以繼續使用、設定和部署所有原生 AWS 服務，或使用您偏好的工具；就像使用 AMS Advanced Customer Managed 帳戶一樣。您會使用偏好的存取和變更機制，同時 AMS 會套用經過驗證的實務，以協助擴展您的團隊、最佳化成本、提高安全性和效率，以及改善彈性。如需進一步了解，請參閱[加速服務描述](#)。

若要將客戶受管帳戶加入 Accelerate，請聯絡您的 CSDM，並遵循 [AMS Accelerate 入門](#) 中的步驟。

Note

AMS Advanced 中的 AMS Accelerate 帳戶沒有 AMS 變更管理（變更請求或 RFCs）或 AMS Advanced 主控台。相反地，它們具有 AMS Accelerate 主控台和功能。

AMS 工具帳戶（遷移工作負載）

您的多帳戶登陸區域工具帳戶（使用 VPC）有助於加速遷移工作、提高安全位置、降低成本和複雜性，以及標準化您的使用模式。

工具帳戶提供下列項目：

- 明確定義的界限，可讓您在生產工作負載之外存取系統整合商的複寫執行個體。
- 可讓您建立隔離的培養室，在將工作負載放入具有其他工作負載的帳戶之前，檢查工作負載是否有惡意軟體或未知的網路路由。
- 作為定義的帳戶設定，它可以更快地加入和設定遷移工作負載。
- 隔離的網路路由可保護來自內部部署 -> CloudEndure -> 工具帳戶 -> AMS 擷取映像的流量。擷取映像後，您可以透過 AMS 管理 | 進階堆疊元件 | AMI | 共用 (ct-1eiczxw8ihc18) RFC 將映像分享至目的地帳戶。

高階架構圖：

使用部署 | 受管登陸區域 | 管理帳戶 | 建立工具帳戶（使用 VPC）變更類型 (ct-2j7q1hgf26x5c)，快速部署工具帳戶，並在多帳戶登陸區域環境中執行個體化工作負載擷取程序。請參閱[管理帳戶、工具帳戶：建立（使用 VPC）](#)。

Note

我們建議您有兩個可用區域 (AZs)，因為這是遷移中樞。根據預設，AMS 會在每個帳戶中建立下列兩個安全群組 (SGs)。確認這兩個 SGs 存在。如果它們不存在，請向 AMS 團隊開啟新的服務請求，以請求它們。

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

確保 CloudEndure 複寫執行個體是在有路由傳回內部部署的私有子網路中建立。您可以確認私有子網路的路由表具有傳回 TGW 的預設路由。不過，執行 CloudEndure 機器切換應該進入「隔離」私有子網路，其中沒有傳回內部部署的路由，僅允許網際網路傳出流量。請務必確保隔離子網路中發生切換，以避免內部部署資源的潛在問題。

事前準備：

1. Plus 或 Premium 支援層級。
2. 部署 AMIs 之 KMS 金鑰的應用程式帳戶 IDs。
3. 工具帳戶，如先前所述建立。

AWS Application Migration Service (AWS MGN)

[AWS Application Migration Service](#) (AWS MGN) 可透過工具帳戶佈建期間自動建立的 `AWSManagedServicesMigrationRole` IAM 角色，在您的 MALZ Tools 帳戶中使用。您可以使用 AWS MGN 遷移在支援的 Windows 和 Linux [作業系統](#) 版本上執行的應用程式和資料庫。

如需 AWS 區域 支援 up-to-date，請參閱 [AWS 區域服務清單](#)。

如果 AWS MGN AWS 區域 目前不支援您的偏好，或 AWS MGN 目前不支援應用程式執行所在的作業系統，請考慮改為在工具帳戶中使用 [CloudEndure 遷移](#)。

請求 AWS MGN 初始化

AWS MGN 必須在第一次使用前由 AMS [初始化](#)。若要為新的工具帳戶請求此項目，請從工具帳戶提交 [管理 | 其他 | 其他 RFC](#)，其中包含下列詳細資訊：

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:
```

```
https://console.aws.amazon.com/mgn/home?region=MALZ\_PRIMARY\_REGION#/welcome using  
all default values  
to 'Create template' and complete the initialization process.
```

一旦 AMS 成功完成 RFC 並初始化工具帳戶中的 AWS MGN，您可以使用 `AWSManagedServicesMigrationRole` 來編輯預設範本以符合您的需求。

啟用對新 AMS 工具帳戶的存取

工具帳戶建立後，AMS 會為您提供帳戶 ID。您的下一個步驟是設定新帳戶的存取權。請遵循下列步驟。

1. 將適當的 Active Directory 群組更新為適當的帳戶 IDs。

新 AMS 建立的帳戶會佈建 `ReadOnly` 角色政策，以及允許使用者提交 RFCs 的角色。

工具帳戶也有額外的 IAM 角色和可用的使用者：

- IAM 角色：`AWSManagedServicesMigrationRole`
- IAM 使用者：`customer_cloud_endure_user`

2. 請求政策和角色，以允許服務整合團隊成員設定下一個層級的工具。

導覽至 AMS 主控台並存檔下列 RFCs：

a. 建立 KMS 金鑰。使用 [建立 KMS 金鑰（自動）](#) 或 [建立 KMS 金鑰（需要檢閱）](#)。

當您使用 KMS 加密擷取的資源時，使用與其餘多帳戶登陸區域應用程式帳戶共用的單一 KMS 金鑰，可為可在目的地帳戶中解密的擷取影像提供安全性。

b. 共用 KMS 金鑰。

使用 [管理 | 進階堆疊元件 | KMS 金鑰 | 共用（需要檢閱）變更類型 \(ct-05yb337abq3x5\)](#)，請求將新的 KMS 金鑰分享給將存放擷取 AMIs 的應用程式帳戶。

最終帳戶設定的範例圖形：

範例 AMS 預先核准的 IAM CloudEndure 政策

若要查看 AMS 預先核准的 IAM CloudEndure 政策：解壓縮 [WIGS 雲端持久性登陸區域範例](#) 檔案，然後開啟 `customer_cloud_endure_policy.json`。

測試 AMS Tools 帳戶連線和end-to-end設定

1. 從設定 CloudEndure 開始，並在將複寫至 AMS 的伺服器上安裝 CloudEndure 代理程式。
2. 在 CloudEndure 中建立專案。
3. 透過 Secrets Manager，輸入執行先決條件時共用的 AWS 登入資料。
4. 在複寫設定中：
 - a. 針對選擇要套用至複寫伺服器的安全群組選項，選取兩個 AMS "Sentinel" 安全群組（僅限私有和 EgressAll）。
 - b. 定義機器的切換選項（執行個體）。如需詳細資訊，請參閱[步驟 5。剪下](#)
 - c. 子網路：私有子網路。
5. 安全群組：
 - a. 選取兩個 AMS "Sentinel" 安全群組（僅限私有和 EgressAll）。
 - b. 切換執行個體必須與 AMS 受管 Active Directory (MAD) 和 AWS 公有端點通訊：
 - i. 彈性 IP：無
 - ii. 公有 IP：否
 - iii. IAM 角色：Customer-mc-ec2-instance-profile
 - c. 根據您的內部標記慣例設定標籤。
6. 在機器上安裝 CloudEndure 代理程式，並在 EC2 主控台中尋找要在 AMS 帳戶中出現的複寫執行個體。

AMS 擷取程序：

AMS Tools 帳戶衛生

在帳戶中完成共用 AMI 且不再需要複寫的執行個體之後，您會想要清除：

- 執行個體後 WIGs擷取：
 - 切換執行個體：在工作完成後，至少透過 AWS 主控台停止或終止此執行個體
 - 擷取前 AMI 備份：擷取執行個體並終止現場部署執行個體後移除
 - AMS 擷取的執行個體：共用 AMI 後關閉堆疊或終止
 - AMS 擷取AMIs：與目的地帳戶共用完成後刪除
- 遷移清除結束：記錄透過開發人員模式部署的資源，以確保定期進行清除，例如：
 - 安全群組

- 透過 Cloud-formation 建立的資源
- 網路 ACK
- 子網路
- VPC
- 路由表
- 角色
- 使用者和帳戶

大規模遷移 - 遷移工廠

請參閱 [AWS CloudEndure 遷移工廠解決方案簡介](#)。

SALZ 網路架構

下圖說明 AWS Managed Services (AMS) 單一帳戶登陸區域 (SALZ) VPC 網路配置，是高可用性設定的範例。

AMS 會根據我們的標準範本和您在加入期間提供的所選選項，為您設定聯網的所有層面。標準 AWS 網路設計會套用至您的 AWS 帳戶，並為您建立虛擬私有雲端 (VPC)，並透過 VPN 或 Direct Connect 連線至 AMS。進一步了解 [AWS Direct Connect 的 Direct Connect](#)。標準 VPCs 包括 DMZ、共用服務和應用程式子網路。在加入過程中，可能會請求和建立額外的 VPCs，以符合您的需求（例如，客戶部門、合作夥伴）。加入後，您會收到網路圖表。環境文件，說明您的網路設定方式。

Note

若要了解所有作用中服務的預設服務限制和限制，請參閱 [AWS 服務限制](#) 文件。

我們的網路設計是以 Amazon「[最低權限原則](#)」為基礎建置。為了達成此目的，我們透過閘道路由所有傳入和傳出流量，但來自信任網路的流量除外。唯一信任的網路是透過使用 VPN 和/或 AWS Direct Connect (DX) 在內部部署環境和 VPC 之間設定的網路。透過使用堡壘執行個體授予存取權，從而防止直接存取任何生產資源。您的所有應用程式和資源都位於可透過公有負載平衡器連線的私有子網路內。公有輸出流量會透過我們的轉送代理流向網際網路閘道，然後流向網際網路。或者，流量可以透過 VPN 或 Direct Connect 流向內部部署環境。

AMS 單一帳戶登陸區域共用服務

共用服務子網路包含 AMS Directory Services、自動化佈建和常見任務的 Management Host、防毒 (TrendMicro) 管理伺服器，以及內部堡壘主機：

- AMS Directory Services = AD 網域控制站

在 AMS 帳戶中建立 Active Directory、建立 AMS 網域、在啟動時將受管堆疊加入網域。

- 管理主機 = AMS 管理主機（自動佈建和常見任務）

做為要修改的 API 端點 AWS Directory Service，並與 AWS Directory Service 網域控制站互動。

- 安全服務：防毒 (TrendMicro) 管理伺服器 = EPS DSM + EPS 轉送

利用 Trend Micro++ Deep Security 軟體 (DSM)，在用戶端伺服器模型中運作，並具有後端資料庫，包括 Deep Security 管理員、代理程式和轉送。

- 內部堡壘主機 = 客戶堡壘

特殊用途伺服器，設計為網際網路的主要存取點，並做為其他 Amazon EC2 執行個體的代理。

設定 AMS

主題

- [了解 AMS 預設設定](#)
- [使用 AMS 主控台](#)
- [使用 AMS API 和 CLI](#)
- [AMS 自備 EPS](#)
- [接收 AMS 通知](#)
- [設定私有和公有 DNS](#)
- [AMS 輸出流量管理](#)
- [在 AMS Advanced 中部署 IAM 資源](#)
- [使用 IAM 角色和設定檔在 AMS 中設定許可](#)
- [AD FS 宣告規則和 SAML 設定](#)
- [限制使用網路 ACL](#)
- [Outpost 上的 AMS](#)
- [在 AMS 中使用標籤](#)
- [AWS Managed Services 資源排程器](#)
- [AWS Systems Manager 在 AMS Advanced 中](#)
- [離線 AMS 帳戶](#)

某些 AMS 設定任務可能會在加入時完成。

如需角色和責任的完整描述，包括 AMS [支援 AWS 的服務](#)，請參閱 [AMS 責任矩陣 \(RACI\)](#)。

Note

若要請求 AMS 提供額外的 AWS 服務，請提交服務請求。如需如何提出此請求的資訊，請參閱 [服務請求管理](#)。

了解 AMS 預設設定

您的 AWS Managed Services (AMS) 網路具有標準化組態，大多數 服務都有預設值。

本節說明 AMS 用於存取、監控和記錄、管理的預設設定。

如需多帳戶登陸區域或單一帳戶登陸區域基礎設施成本的範例，請參閱 [AMS 環境基本元件](#)。

主題

- [DNS 解析預設值 \(MALZ\)](#)
- [EC2 IAM 執行個體描述檔](#)
- [AMS 中基準監控的提醒](#)
- [日誌保留和輪換預設值](#)

DNS 解析預設值 (MALZ)

AWS Managed Services (AMS) 多帳戶登陸區域：在 AWS 環境中，可以透過設定解析程式轉送規則來整合 VPC 中 Route 53 Resolver 和 DNS 解析程式之間的網域名稱系統 (DNS) 解析。在這些規則可用於轉送 DNS 查詢之前，需要設定傳入和傳出解析程式端點，以便將這些查詢轉送到這些端點。

根據預設，AMS 中多帳戶設定的應用程式帳戶 VPCs 內的 DNS 查詢會轉送至共用服務帳戶中存在的 AWS Directory Service for Microsoft Active Directory (也稱為 Managed AD) 網域的條件式轉寄站。AMS 選擇性可讓您使用 AmazonProvidedDNS；例如，AmazonProvidedDNS 轉送 DNS 查詢。這可協助您利用目前僅透過 Amazon Route 53 支援 Amazon 提供之 DNS 的 VPC 端點。相應地，解析程式規則也會針對共用服務帳戶中預設部署的常見 VPC 端點自動設定。如需這些常見 VPC 端點的詳細資訊，請參閱 [AMS VPC 端點](#)。

若要在所有應用程式帳戶 VPCs 中設定動態主機組態通訊協定 (DHCP) 選項集，以針對 VPC 端點使用 Amazon 提供的 DNS，和讓 Route53 Resolver 規則指向共用服務帳戶中的常見 VPC 端點（具有內部部署網域的選用解析程式規則），建立管理 | 其他 | 其他 | 建立變更請求 (RFC) 以指定共用服務帳戶，和請求啟用 VPC 端點的應用程式帳戶 VPC 本機 DNS 和 Route 53 Resolver 規則。

EC2 IAM 執行個體描述檔

執行個體描述檔是適用於 IAM 角色的容器，可讓您在執行個體啟動時將角色資訊傳遞至 EC2 執行個體。

MALZ

有兩個 AMS 預設執行個體描述檔 `customer-mc-ec2-instance-profile` 和 `customer-mc-ec2-instance-profile-s3`。這些執行個體描述檔提供下表所述的許可。

政策描述

設定檔	Policies
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : 允許 Ec2 執行個體使用 SSM 代理程式。
	AMSInstanceProfileLoggingPolicy : 允許 Ec2 執行個體將日誌推送至 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy : 允許 Ec2 執行個體執行開機動作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy : 允許 Ec2 執行個體向 AMS 監控服務報告問題清單。
	AMSInstanceProfilePatchPolicy : 允許 Ec2 執行個體接收修補程式。
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : 允許 Ec2 執行個體使用 AMS 帶來您自己的 EPS 。
	AMSInstanceProfileLoggingPolicy : 允許 Ec2 執行個體將日誌推送至 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy : 允許 Ec2 執行個體執行開機動作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy : 允許 Ec2 執行個體向 AMS 監控服務報告問題清單。
	AMSInstanceProfilePatchPolicy : 允許 Ec2 執行個體接收修補程式。
	AMSInstanceProfileS3WritePolicy : 允許 Ec2 執行個體讀取/寫入客戶 S3 儲存貯體。

SALZ

有一個 AMS 預設執行個體描述檔 `customer-mc-ec2-instance-profile`，授予 IAM 執行個體政策 的許可 `customer_ec2_instance_profile_policy`。此執行個體描述檔提供下表所述的許可。設定檔會將許可授予執行個體上執行的應用程式，而非登入執行個體的使用者。

政策通常包含多個陳述式，其中每個陳述式會將許可授予一組不同的資源，或在特定條件下授予許可。

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。

EC2 預設 IAM 執行個體描述檔許可

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。

政策聲明	Effect	動作	描述和資源 (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 訊息動作	允許	AcknowledgeMessage、 DeleteMessage、 FailMessage、 GetEndpoint、 GetMessages、 SendReply	允許帳戶中的 EC2 Systems Manager 訊息動作。
Ec2 描述	允許	* (全部)	允許主控台顯示您帳戶中 EC2 的組態詳細資訊。
Iam 取得角色 ID	允許	GetRole	允許 EC2 從 <code>aws:iam::*:role/customer-*</code> 和取得您的 IAM ID <code>aws:iam::*:role/customer_*</code> 。
上傳日誌事件的執行個體	允許	建立日誌群組	允許在以下位置建立日誌： <code>aws:logs:*:*:log-group:i-*</code>

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 (任何)。

政策聲明	Effect	動作	描述和資源 (ARN)
MMS 的 CW	允許	建立日誌串流	允許將日誌串流至： <code>aws:logs:*:*:log-group:i-*</code>
		DescribeAlarms、 PutMetricAlarm、 PutMetricData	允許 CloudWatch 擷取您帳戶中的警示。 允許 CW 建立或更新警示，並將其與指定的指標建立關聯。 允許 CW 將指標資料點發佈至您的帳戶。
Ec2 標籤	允許	CreateTags、 DescribeTags、	允許在您帳戶中的指定執行個體上新增、覆寫和描述標籤。
明確拒絕 CW 日誌	拒絕	DescribeLogStreams、 FilterLogEvents、 GetLogEvents	不允許列出、篩選或取得日誌串流： <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			
SSM 動作	允許	DescribeAssociation、 GetDocument、 ListAssociations、 UpdateAssociationStatus、 UpdateInstanceInformation	允許帳戶中的各種 SSM 函數。

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 (任何)。

政策聲明	Effect	動作	描述和資源 (ARN)
S3 中的 SSM 存取	允許	GetObject、 PutObject、 AbortMultipartUpload、 ListMultipartUploadParts、 ListBucketMultipartUploads	允許 EC2 上的 SSM 在 中取得和更新物件，並中止分段物件上傳至 ，以及列出可用於 分段上傳的連接埠和儲存貯體 <code>aws:s3:::mc-*-internal-*/aws/ssm*</code> 。

Amazon EC2 Simple Storage Service (S3)

在 S3 中取得物件	允許	取得清單	允許 EC2 應用程式擷取和列出您帳戶中 S3 儲存貯體中的物件。
客戶加密日誌 S3 存取	允許	PutObject	允許 EC2 應用程式更新 中的物件 <code>aws:s3:::mc-*-logs-*/encrypted/app/*</code>
修補程式資料放置物件 S3	允許	PutObject	允許 EC2 應用程式將修補資料上傳至 S3 儲存貯體 <code>aws:s3:::awsms-a*-patch-data-*</code>
將自有日誌上傳至 S3	允許	PutObject	允許 EC2 應用程式將自訂日誌上傳至： <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元 (任何)。

政策聲明	Effect	動作	描述和資源 (ARN)
明確拒絕 MC 命名空間 S3 日誌	拒絕	GetObject* Put*	不允許 EC2 應用程式從下列位置取得或放置任何物件： aws:s3:::mc-*--logs-*/encrypted/mc* , aws:s3:::mc-*--logs-*/mc/* , aws:s3:::mc-a*-logs-*--audit/*
明確拒絕 S3 刪除	拒絕	* (全部)	不允許 EC2 應用程式對下列物件採取任何動作： aws:s3:::mc-a*-logs-*/* , aws:s3:::mc-a*-internal-*/* ,
明確拒絕 S3 CFN 儲存貯體	拒絕	刪除*	不允許 EC2 應用程式從下列位置刪除任何物件：aws:s3:::cf-templates-*
明確拒絕清單儲存貯體 S3	拒絕	ListBucket	不允許您從下列位置列出任何加密、稽核日誌或預留 (mc) 物件： aws:s3:::mc-*--logs-*

AWS Secrets Manager 在 Amazon EC2 中

CW = CloudWatch。ARN = Amazon Resource Name。* = 萬用字元（任何）。

政策聲明	Effect	動作	描述和資源 (ARN)
Trend Cloud One 秘密存取	允許	GetSecretValue	允許 Amazon EC2 存取 Trend Cloud One 遷移的秘密： <pre>aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:~::~secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>

AWS Key Management Service 在 Amazon EC2 中

Trend Cloud One 解密金鑰	允許	解密	允許 Amazon EC2 以別名名稱 / ams/eps/cloudone-migration 解密 AWS KMS 金鑰 <pre>arn:aws:kms:~::~alias/ ams/eps/cloudone-migrat ion</pre>

如果您不熟悉 Amazon IAM 政策，請參閱 [IAM 政策概觀](#) 以取得重要資訊。

Note

政策通常包含多個陳述式，其中每個陳述式會將許可授予一組不同的資源，或在特定條件下授予許可。

AMS 中基準監控的提醒

了解 AMS 監控預設值。如需詳細資訊，請參閱[AMS 中的監控和事件管理](#)。

下表顯示監控的項目，以及預設提醒閾值。您可以在決定您想要的變更並訂閱相關 CloudWatch Amazon SNS 主題之後，使用管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 變更提醒閾值。如需建立和訂閱主題的詳細資訊，請參閱[訂閱主題](#)。如需一般資訊，請參閱 [Amazon SNS FAQs](#)。若要在警示超過閾值時直接收到通知，除了 AMS 的標準警示程序之外，請遵循有關如何覆寫警示組態的這些指示[接收 AMS 產生的提醒](#)。

Amazon CloudWatch 提供指標的延長保留。如需詳細資訊，請參閱 [CloudWatch 限制](#)。

Note

AMS 會定期校正其基準監控。新帳戶一律使用最新的基準監控加入，而表格說明新加入帳戶的基準監控。AMS 會定期更新現有帳戶中的基準監控，而且在進行更新之前，您可能會遇到時間延遲。如需詳細資訊，請參閱[檢視 AMS 帳戶的監控組態](#)。

Note

EC2 執行個體提醒預設為Non-root volume usage停用。如果您需要根據此警示產生提醒，則必須使用 RFC 變更類型 [ct-0erkoad6uyvg](#) 啟用它

基準監控的提醒

服務	安全性提醒	警示名稱和觸發條件	備註

對於星號 (*) 警示，AMS 會盡可能主動評估影響並修復；如果無法修復，則 AMS 會建立事件。當自動化無法修正問題時，AMS 會通知您事件案例並聘請 AMS 工程師。此外，這些提醒可以直接傳送到您的電子郵件（如果您已選擇加入 Direct-Customer-Alerts SNS 主題）。

Application Load Balancer (ALB) 執行個體	否	RejectedConnectionCount 總和 > 0，持續 1 分鐘，連續 5 次。	如果因負載平衡器達到其上限而遭到拒絕的連線數目，CloudWatch 會發出警示。
Application Load Balancer (ALB) 目標	否	TargetConnectionErrorCount 總和 > 0，持續 1 分鐘，連續 5 次。	如果負載平衡器和已註冊執行個體之間的連線數目未成功建立，則 CloudWatch 會發出警示。
Amazon EC2 執行個體 – Windows	否	SecureChannelFailure 過去 15 個資料點中的 10 個 > 0.0。	Windows 執行個體上的 CloudWatch 警示會在安全頻道連線失敗時發出警示。
Aurora 執行個體	否	CPUUtilization > 85% 持續 5 分鐘，連續 2 次。	CloudWatch 警示。
AWS Backup	是	DeleteRecoveryPoint 非預期的 IAM 角色主體或 IAM 使用者主體已刪除 AWS Backup 復原點。	CloudWatch 事件。刪除備份復原點時發出。
AWS Outposts	是	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability	資源之執行個體系列容量可用性的 CloudWatch AWS Outposts 警示。

服務	安全性提醒	警示名稱和觸發條件	備註
EC2 執行個體 - OSs	否	= 80%，持續 5 分鐘，連續 12 次。	
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability	資源之執行個體類型容量可用性的 CloudWatch AWS Outposts 警示。
		= 80%，持續 5 分鐘，連續 12 次。	
		AMSOupostsConnectedStatusC onnectedStatus	AWS Outposts 服務連結連線上的 CloudWatch 警示，少於 1 個會受損。
		< 1 表示 5 分鐘，連續 1 次。	
		AMSOupostsCapacityExceptio nCapacityExceptions	執行個體啟動 AWS Outposts 資源時容量不足錯誤的 CloudWatch 警示
		0 表示 5 分鐘，連續 1 次。	.
		CPUUtilization*	CloudWatch 警示。高 CPU 使用率是應用程式狀態變更的指標，例如死鎖、無限迴圈、惡意攻擊和其他異常。
		>= 95%，持續 5 分鐘，連續 6 次。	
		StatusCheckFailed	CloudWatch 警示。
		> 0 持續 5 分鐘，連續 3 次。	
		根磁碟區用量	
		>= 95%，持續 5 分鐘，連續 6 次。	

服務	安全性提醒	警示名稱和觸發條件	備註
		非根磁碟區用量 > 85% 持續 5 分鐘，連續 2 次。 預設停用；如需其他資訊，請參閱 https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info。	
		記憶體可用* MemoryFree < 5% 持續 5 分鐘，連續 6 次。	
	是	EPS 惡意軟體 執行個體上發現惡意軟體。	CloudWatch 事件。
Amazon EC2 執行個體 - Linux	否	根磁碟區 Inode 用量 平均 >= 95%，持續 5 分鐘，連續 6 次。 免費交換* 記憶體交換 < 5% 持續 5 分鐘，連續 6 次。	CloudWatch 警示。僅適用於 Linux 執行個體。

服務	安全性提醒	警示名稱和觸發條件	備註
ElastiCache 叢集	否	CurrConnections = 65000	此警示會通知 AMS ElastiCache 主機的最大連線限制。 CloudWatch 警示。如果您想要更新此閾值，請聯絡 AMS 支援。

服務	安全性提醒	警示名稱和觸發條件	備註
ElastiCache 節點	否	CPUUtilization 平均 > 15 分鐘的預先定義值，連續 2 次。	CloudWatch 警示。預設為 90。 如果是 Redis，請根據執行個體類型使用下列其中一個值： • cache.t1.micro : 90% • cache.m1.small : 90% • cache.m1.medium : 90% • cache.m1.large : 45% • cache.m1.xlarge : 22.5% • cache.m2.xlarge : 45% • cache.m2.4xlarge : 11.25% • cache.c1.xlarge : 11.25% • cache.t2.micro : 90% • cache.t2.small : 90% • cache.t2.medium : 45% • cache.m3.medium : 90% • cache.m3.large : 45% • cache.m3.xlarge : 22.5% • cache.m3.2xlarge : 11.25% • cache.r3.large : 45% • cache.r3.xlarge : 22.5% • cache.r3.2xlarge : 11.25% • cache.r3.4xlarge : 5.625% • cache.r3.8xlarge : 2.8125%
ElastiCache 節點 - memcached	否	SwapUsage 最大 > 50,000,000 位元組，持續 5 分鐘，連續 5 次。	CloudWatch 警示。僅適用於 memcached。

服務	安全性提醒	警示名稱和觸發條件	備註
OpenSearch 叢集	否	ClusterStatus.red 最大值為 ≥ 1，持續 1 分鐘，連續 1 次。 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	CloudWatch 警示。至少一個主要碎片及其複本不會分配到節點。若要進一步了解，請參閱 Red Cluster 狀態。
OpenSearch 網域	否	KMSKeyError ≥ 1 表示 1 分鐘，連續 1 次。	CloudWatch 警示。用於在您的網域中加密靜態資料的 KMS 加密金鑰停用。重新啟用它來恢復正常操作。若要進一步了解，請參閱 OpenSearch Service Service 的靜態資料加密。
		ClusterStatus.yellow 最大值為 ≥ 1，持續 1 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	至少一個複本碎片不會分配到節點。若要進一步了解，請參閱 黃色叢集狀態。
		FreeStorageSpace 最小值為 ≤ 20480，持續 1 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	您叢集內的節點縮減至 20 GiB 的可用儲存空間。若要進一步了解，請參閱 缺少可用的儲存空間。

服務	安全性提醒	警示名稱和觸發條件	備註
		ClusterIndexWritesBlocked ≥ 1 持續 5 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	叢集正在封鎖寫入請求。若要進一步了解，請參閱 ClusterBlockException。
		節點 最小值為 $< x$，持續 1 天，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	x 是您叢集中的節點數。此警示表示您叢集中至少有一個節點已無法連線達 1 天時間。若要進一步了解，請參閱失敗的叢集節點。
		CPUUtilization 平均 $\geq 80\%$，持續 15 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	100% 的 CPU 使用率很常見，但持續高平均值是有問題的。可考慮使用較大的執行個體類型或新增執行個體。
		JVMMemoryPressure 最大值 $\geq 80\%$，持續 5 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	如果使用量增加，叢集可能遇到記憶體不足錯誤。可考慮垂直擴展。Amazon ES 針對 Java 堆積使用執行個體 RAM 的一半，堆積大小上限為 32 GiB。您可以垂直擴展執行個體高達 64 GiB 的 RAM，屆時便能透過新增執行個體進行水平擴展。

服務	安全性提醒	警示名稱和觸發條件	備註
		MasterCPUUtilization 平均 $\geq 50\%$，持續 15 分鐘，連續 3 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	請考慮為您的 專用主節點 使用較大的執行個體類型。由於其在叢集穩定性和 藍/綠部署 中扮演的角色，專用主節點的平均 CPU 用量應該低於資料節點。
		MasterJVMMemoryPressure 最大值 $\geq 80\%$，持續 15 分鐘，連續 1 次 當觸發此提醒時，AMS 會採取主動動作來降低操作影響。	請考慮為您的 專用主節點 使用較大的執行個體類型。由於其在叢集穩定性和 藍/綠部署 中扮演的角色，專用主節點的平均 CPU 用量應該低於資料節點。
OpenSearch 執行個體	否	AutomatedSnapshotFailure 最大值為 ≥ 1，持續 1 分鐘，連續 1 次。	CloudWatch 警示。自動快照失敗。此故障通常是紅色叢集運作狀態的結果。請參閱 紅色叢集狀態 。
Elastic Load Balancing 執行個體	否	SurgeQueueLength > 100 持續 1 分鐘，連續 15 次。	如果待定路由的請求數量過多，CloudWatch 會發出警示。
		HTTPCode_ELB_5XX_Count 總和 > 0，持續 5 分鐘，連續 3 次。	來自負載平衡器之過多 HTTP 5XX 回應碼的 CloudWatch 警示。
		SpilloverCount > 1 持續 1 分鐘，連續 15 次。	如果因為突增佇列已滿而拒絕的請求數量過多，CloudWatch 會發出警示。

服務	安全性提醒	警示名稱和觸發條件	備註
GuardDuty 服務	是	不適用；所有調查結果（威脅目的）都會受到監控。每個問題清單對應至提醒。 GuardDuty 調查結果的變更。這些變更包括新產生的問題清單或後續出現的現有問題清單。	支援的 GuardDuty 調查結果類型清單位於 GuardDuty 作用中調查結果類型 上。
醫療保健	各有不同	AWS Health Dashboard	與 AMS 支援的基準服務相關的 AWS Health Dashboard (AWS Health) 事件狀態變更時，會傳送通知。如需詳細資訊，請參閱 支援的服務 。
AWS Managed Microsoft AD	否	Active Directory 狀態	服務事件。當目錄在事件後正常運作時發出。
		AWS Managed Microsoft AD 執行個體會傳送作用中狀態事件。	
		目錄狀態受損	服務事件。當目錄以降級狀態執行時發出。已偵測到一個或多個問題，且並非所有目錄操作都能以完整的操作容量運作；
		AWS Managed Microsoft AD 執行個體會傳送受損的目錄狀態事件。	
		無法運作的目錄狀態	服務事件。當目錄無法運作時發出。所有目錄端點均已回報問題。
		AWS Managed Microsoft AD 執行個體會傳送無法操作的狀態事件。	
		刪除目錄狀態	服務事件。當目錄目前正在刪除時發出。
		AWS Managed Microsoft AD 執行個體會傳送刪除目錄狀態事件。	

服務	安全性提醒	警示名稱和觸發條件	備註
		失敗的目錄狀態 AWS Managed Microsoft AD 執行個體會傳送失敗狀態事件。	服務事件。當無法建立目錄時發出。
		RestoreFailed Directory 狀態 AWS Managed Microsoft AD 執行個體會傳送還原失敗的目錄狀態事件。	服務事件。從快照還原目錄時發出失敗。
Amazon RDS 執行個體	否	低儲存提醒會在資料庫執行個體的配置儲存用盡時觸發。	RDS-EVENT-0007，請參閱 使用 Amazon RDS 事件通知 的詳細資訊。
		資料庫執行個體失敗 因為不相容的組態或基礎儲存問題，資料庫執行個體已失敗。開始資料庫執行個體的時間點還原。	服務事件。RDS-EVENT-003 1、 Amazon RDS 事件類別和事件訊息 。
		未嘗試容錯移轉 Amazon RDS 不會因為資料庫執行個體最近發生的容錯移轉，而嘗試請求的容錯移轉。	服務事件。RDS-EVENT-003 4、 Amazon RDS 事件類別和事件訊息 。
		資料庫執行個體的參數無效 例如，MySQL 無法啟動，因為此執行個體類別的記憶體相關參數設定過高，因此客戶動作會是修改記憶體參數並重新啟動資料庫執行個體。	服務事件。RDS-EVENT-003 5、 Amazon RDS 事件類別和事件訊息 。

服務	安全性提醒	警示名稱和觸發條件	備註
		無效的子網路 IDs 資料庫執行個體 資料庫執行個體位於不相容的網路中。部分指定的子網路 ID 無效或不 存在。	服務事件。RDS-EVENT-003 6、 Amazon RDS 事件類別和事件訊息 。
		資料庫執行個體僅供讀取複本錯誤 僅供讀取複寫程序發生錯誤。如需更多詳細資訊，請參閱事件訊息。如需有關對僅供讀取複本錯誤進行故障診斷的資訊，請參閱 對 MySQL 僅供讀取複本問題進行故障診斷 。	服務事件。RDS-EVENT-004 5、 Amazon RDS 事件類別和事件訊息 。
		資料庫執行個體讀取複寫已結束 僅供讀取複本上的複寫已結束。	服務事件。RDS-EVENT-005 7、 Amazon RDS 事件類別和事件訊息 。
		建立 statspack 使用者帳戶時發生錯誤 建立 Statspack 使用者帳戶 PERFSTAT 時發生錯誤。在新增 Statspack 選項之前捨棄帳戶。	服務事件。RDS-EVENT-005 8、 Amazon RDS 事件類別和事件訊息 。
		資料庫執行個體復原開始 SQL Server 資料庫執行個體正在重新建立其鏡像。將會降低效能，直到鏡像重新建立完成。找到含有非 FULL 還原模型的資料庫。復原模型已變更回 FULL，並開始鏡像復原。(<dbname> : <recovery model found> 【 , ...】)。	服務事件。RDS-EVENT-006 6、 Amazon RDS 事件類別和事件訊息 。

服務	安全性提醒	警示名稱和觸發條件	備註
		資料庫叢集的容錯移轉已失敗。	RDS-EVENT-0069，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		無效的許可復原 S3 儲存貯體 您用來為 SQL Server 原生備份與還原存取 Amazon S3 儲存貯體的 IAM 角色設定不正確。如需詳細資訊，請參閱 設定原生備份和還原 。	服務事件。RDS-EVENT-0081、 Amazon RDS 事件類別和事件訊息 。
		Aurora 無法從 Amazon S3 儲存貯體複製備份資料。	RDS-EVENT-0082，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		資料庫執行個體耗用其配置儲存體的 90% 以上時，會發出低儲存提醒	RDS-EVENT-0089，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		Aurora Serverless 資料庫叢集擴展失敗時的通知服務。	RDS-EVENT-0143，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		資料庫執行個體處於無效狀態。無需採取任何動作。稍後將重試自動擴展。	RDS-EVENT-0219，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		資料庫執行個體已達到儲存已滿閾值，且資料庫已關閉。	RDS-EVENT-0221，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		此事件表示 RDS 執行個體儲存體自動擴展無法擴展，可能有多個原因導致自動擴展失敗。	RDS-EVENT-0223，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。

服務	安全性提醒	警示名稱和觸發條件	備註
		儲存自動擴展已觸發將達到最大儲存閾值的擱置擴展儲存任務。	RDS-EVENT-0224，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		資料庫執行個體具有目前在可用區域中無法使用的儲存類型。稍後將重試自動擴展。	RDS-EVENT-0237，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		RDS 無法佈建代理的容量，因為子網路中沒有足夠的可用 IP 地址。	RDS-EVENT-0243，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		您 AWS 帳戶的儲存體已超過允許的儲存體配額。	RDS-EVENT-0254，請參閱 Amazon RDS 事件類別和事件訊息 的詳細資訊。
		CPUUtilization 平均 CPU 使用率 > 90%，持續 15 分鐘，連續 2 次。	CloudWatch 警示。
		DiskQueueDepth 總和 > 75 持續 1 分鐘，連續 15 次。	
		FreeStorageSpace 平均 < 1,073,741,824 位元組，持續 5 分鐘，連續 2 次。	
		SwapUsage 平均 >= 104,857,600 個位元組，持續 5 分鐘，連續 2 次。	

服務	安全性提醒	警示名稱和觸發條件	備註
Amazon Redshift 叢集	否	RedshiftClusterStatus 叢集在 5 分鐘內未處於維護模式 < 1 時的運作狀態。	1 代表運作狀態良好的叢集。
Amazon Macie	是	新產生的提醒和現有提醒的更新。 Macie 會在問題清單中找到任何變更。這些變更包括新產生的問題清單或後續出現的現有問題清單。	Amazon Macie 提醒。如需支援的 Macie 提醒類型清單，請參閱 分析 Amazon Macie 調查結果 。請注意，並非所有帳戶都啟用 Macie。

觸發此提醒時，AMS 會採取主動動作（擴展叢集）。

如需修補工作的資訊，請參閱 [AMS 自動修復提醒](#)。

[觀看 Andrew 的影片以進一步了解 \(7 : 03\)](#)

日誌保留和輪換預設值

本節說明 AMS 日誌管理預設值；如需詳細資訊，請參閱 [日誌管理](#)。

- 輪換 = 執行個體內的日誌周轉
- 保留 = 我們在 Amazon CloudWatch Logs 和 Amazon Simple Storage Service (S3) 中保留日誌的時間

日誌會視需要保留在 CloudWatch Logs 中（您可以設定此項目）和 S3 中。它們不會過期或遭到刪除，且會受限於服務耐久性。如需詳細的 S3 耐久性資訊，請參閱 [Amazon S3 中的資料保護](#)。

您可以請求變更所有日誌的日誌保留，但日誌為稽核和安全性原因無限期 AWS CloudTrail 保留。

日誌輪換是在執行個體內設定。根據預設，作業系統和安全性日誌會在超過 100MB 時每小時輪換，這樣做是為了確保您不會在執行個體中的磁碟上執行短時間。

執行個體內的日誌代理程式會將日誌線上上傳至 CloudWatch Logs，再從該處將日誌封存至 S3。

日誌會以產生的原始格式存放在 CloudWatch Logs 和 S3 中，不會進行預先處理。

使用 AMS 主控台

AWS 管理主控台中的 AMS 主控台可讓您與 AMS 互動，並操作您的 AMS 進階受管和 AMS Accelerate 資源。AMS 主控台的行為通常類似於任何 AWS 主控台；不過，由於 AMS 是私有組織，因此只有為 AMS 啟用的帳戶才能存取主控台。在您的帳戶中啟用 AMS 後，您可以在統一搜尋列中搜尋「受管服務」來存取主控台。

Note

視您的帳戶角色而定，您可以存取 AMS Advanced 主控台或 AMS Accelerate 主控台。

使用 AMS 主控台時，請注意下列注意事項：

- AMS 主控台是帳戶特定的。因此，如果您在組織的「測試」帳戶中，您將無法查看該組織的「產品」帳戶中的資源。同樣地，您必須擁有 AMS Advanced 角色才能存取 AMS Advanced 主控台。
- AMS 主控台會在您驗證時套用 IAM 政策，以決定您可以存取的主控台，以及您可以在其中執行的動作。您的管理員可能會將其他政策套用至預設 AMS 政策，以限制您可以在 主控台中看到和執行的操作。

AMS Advanced 主控台具有下列功能：

- 開啟頁面：開啟頁面包含資訊方塊和連結，可協助您存取現有的 RFCs、事件、服務請求和報告。
- 左側導覽窗格中的功能頁面、連結：
 - 儀表板：提供帳戶目前狀態的概觀，包括：
 - 變更請求：查看有多少 RFCs 正在等待您的回應，並在該篩選條件作用中時跳至 RFC 清單頁面。查看有多少 RFCs 正在等待您的核准，並在該篩選條件作用中時跳至 RFC 清單頁面。查看有多少 RFCs 為開啟，並在該篩選條件作用中時跳至 RFC 清單頁面。按一下檢視所有連結，開啟 RFCs 的清單頁面。
 - 事件：查看有多少事件案例正在等待您的回應，並使用該篩選條件跳至事件清單頁面。請參閱和開啟的數量，並跳至啟用該篩選條件的事件清單頁面。按一下檢視所有連結，開啟事件清單頁面。
 - 服務請求：查看有多少服務請求正在等待您的回應，並在啟用該篩選條件的情況下跳至服務請求清單頁面。請參閱和開啟的數量，並跳至啟用該篩選條件的服務請求清單頁面。按一下檢視所有連結，開啟服務請求清單頁面。
 - 最近更新的 RFCs：日期、RFC 詳細資訊的連結和狀態

- 最近建立的事件和服務請求：日期、連結至案例詳細資訊，以及類型（事件或服務請求）
- RFCs：開啟帳戶的現有 RFCs 清單
- 事件：開啟帳戶的開啟事件清單
- 服務請求：開啟帳戶開啟的服務請求清單
- 報告：開啟報告頁面和預設報告、每日備份和每日修補程式以及每月計費
- 資源：
 - VPCs：開啟帳戶的現有 VPCs 清單
 - 堆疊：開啟帳戶的現有堆疊清單
 - AMIs：開啟可用的 AMS AMIs 清單
- 功能焦點：主控台最新更新的相關資訊
- 開發人員資源：可下載檔案的頁面，包括 AMS 進階變更管理 SDK 等
- 文件：AWS Managed Services 文件登陸頁面

使用 AMS API 和 CLI

AWS Managed Services (AMS) API 與其他 APIs 類似。AWS 您可以在 AMS API [參考中閱讀 AMS API](#)。

REST 呼叫的 AMS API HTTP 端點

除了各種 SDKs，AMS 還提供 CLI；您也可以針對 AMS 端點叫用 REST API 呼叫。

有兩個 AMS APIs（兩者的端點都位於 us-east-1）：

- 變更管理：使用此 API 請求存取或變更您的基礎設施，包括建立和更新 RFCs、部署新執行個體、更新和刪除執行個體、取得 CTs 的相關資訊，以及建立 AMIs。HTTP 端點為：

`https://amscm.us-east-1.amazonaws.com`

- SKMS：使用此 API 取得基礎設施的相關資訊，包括 VPCs、堆疊、子網路和 AMIs。HTTP 端點為：

`https://amsskms.us-east-1.amazonaws.com`

安裝或升級 AMS CLI

AMS CLI 是與 AMS API 互動的簡單方法，用於本節的範例。如需 AWS CLI 和 AMS CLI 的使用慣例，請參閱[使用 AWS 命令列界面](#)。

如需安裝 SAML 的資訊，請參閱 [AD FS 宣告規則和 SAML 設定](#)。

若要安裝或升級 AMS CLI，請遵循下列指示：

Note

您必須擁有此程序的管理員登入資料。

AWS CLI 是使用 AWS Managed Services (AMS) CLIs (變更管理和 SKMS) 的先決條件。

1. 若要安裝 AWS CLI，請參閱[安裝 AWS 命令列界面](#)，並遵循適當的指示。請注意，在該頁面底部有使用不同安裝程式、[Linux](#)、[MS Windows](#)、[macOS](#)、[虛擬環境](#)、[Bundled Installer \(Linux、macOS 或 Unix\)](#) 的說明。

安裝之後，請執行 `aws help` 來驗證安裝。

2. 安裝 AWS CLI 後，若要安裝或升級 AMS CLI，請下載 AMS AMS CLI 或 AMS SDK 可分發 zip 檔案並解壓縮。您可以透過 AMS 主控台左側導覽中的[開發人員資源](#)連結來存取 AMS CLI 可分發項目。
3. README 檔案提供任何安裝的指示。

開啟：

- CLI zip：僅提供 AMS CLI。
- SDK zip：提供所有 AMS APIs 和 AMS CLI。

對於 Windows，請執行適當的安裝程式（僅限 32 或 64 位元系統）：

- 32 位元：ManagedCloudAPI_x86.msi
- 64 位元：ManagedCloudAPI_x64.msi

對於 Mac/Linux，執行此命令以執行名為 `AWSManagedServices_InstallCLI.sh` 的檔案：`sh AWSManagedServices_InstallCLI.sh`。請注意，`amscm` 和 `amsskms` 目錄及其內容必須與 `AWSManagedServices_InstallCLI.sh` 檔案位於相同的目錄中。

- 如果您的公司登入資料是透過 AWS (AMS 預設組態) 聯合使用，您必須安裝登入資料管理工具，以存取您的聯合服務。例如，您可以使用此 AWS 安全部落格 [如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取](#)，以協助設定憑證管理工具。
- 安裝之後，請執行 `aws amscm help` 和 `aws amsskms help` 以查看命令和選項。

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

在 CLI、Ruby、Python 和 Java 中使用 AMS API

以下是所有可用語言的 AMS API `ListChangeTypeClassificationSummaries` 操作程式碼片段清單。

如需 Python、Ruby 和 Java SDKs，請參閱[適用於 Amazon Web Services 的工具](#)並向下捲動至 SDKs 區段。每個 SDK 安裝程式都包含具有其他程式碼片段的 README。

AMS API 到 CLI 範例

安裝 AMS CLI (需要 AWS CLI；請參閱[安裝或升級 AMS CLI](#)) 之後，您可以重新調整呼叫來執行任何 AMS API 操作，首先指定 AMS API `aws amscm` 或 `aws amsskms`，然後使用連字號取代駝案例來給予動作。最後，提供登入資料，例如 SAML。

若要進一步了解，請參閱[使用 AWS 命令列界面](#)。

範例：

- API: `'ChangeTypeClassificationSummaries[]' [Category,Subcategory,Item,Operation,ChangeTypeId]'`

- CLI : `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*]. [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

如果您使用 SAML 驗證，請將 `aws --profile saml` 新增至命令的開頭。例如

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

AMS API 到 Python 範例

若要搭配 Python 使用 AMS API，請安裝 AMS CLI 並安裝 boto3。請遵循下列步驟：

1. 安裝 AMS CLI。請參閱 [安裝或升級 AMS CLI](#)。
2. 安裝 boto3，適用於 Python 的 AWS SDK。如需詳細資訊，請參閱此部落格文章 [現已推出 – AWS SDK for Python \(Boto3\)](#)。

```
import boto3
```

3. 取得 AMS 變更管理用戶端：

```
cm = boto3.client('amscm')
```

4. 取得 AMS CTs：

```
cts = cm.list_change_type_classification_summaries()  
  
print(cts)
```

Python 範例

以下是在 AMS 中使用 Python、建立 EC2 執行個體和/或使用 Lambda 的一些範例。

建立 EC2 的 Python 範例

此範例說明如何從 Python 程式碼中使用 amscm RESTful API 來存檔和執行 RFC 程序。

1. 將 AMS CLI 安裝到您可以存取的位置；您需要其提供的檔案。
2. 呼叫 Python 程式庫並建立 EC2 執行個體：

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
```

```
print(RFC_Status_Code)
time.sleep(30)
elif RFC_Status_Code == "InProgress":
    print(RFC_Status_Code)
    time.sleep(30)
elif RFC_Status_Code == "Failure":
    print(RFC_Status_Code)
    break
else:
    print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

搭配 Lambda 的 Python 範例

此範例示範如何將 AMS 模型與程式碼綁定，以便您可以將其與 Lambda 或 EC2 搭配使用；不會或無法安裝的位置 `awscli`。

Note

AMS 不提供可匯入的 AMS 特定 Python SDK。`awscli` 安裝指令碼會在 CLI 的正常路徑中安裝 AMS 服務資料模型。對於 CLI 用量和系統 Python 用量，沒問題，因為 `awscli` 和 從相同的預設位置 `boto3` 讀取其服務模型 (`~/.aws/models`)。不過，當您想要在 Lambda 中透過 `boto3`（或任何其他非本機執行時間）使用 AMS 服務時，它會中斷，因為您不再擁有資料模型。以下是使用 函數封裝資料模型來修正此問題的方法。

您可以採取一些簡單的步驟，在 Lambda 或 EC2、Fargate 等其他執行時間中執行 AMS 整合的 Python 程式碼。下列工作流程顯示 AMS 整合 Lambda 函數所需的步驟。

透過將資料模型新增至程式碼的部署套件並更新 SDK 搜尋路徑，您可以模擬 SDK 體驗。

Important

此範例和所有顯示的非 Python 命令已在 Mac 電腦上測試。

範例工作流程：

1. 安裝 `amsccli`。這會在您的電腦 (Mac) `~/.aws/models` 上於 建立資料夾。
2. 將模型複製到本機目錄：`cp ~/.aws/models ./models`。
3. 將模型包含在程式碼的部署套件中。
4. 更新您的函數程式碼，將新模型新增至 SDK 路徑。請注意，此程式碼必須在匯入 `boto3` 或 `botocore` 之前執行！

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

由於範例模型位於名為 `models` 的目錄中，我們會將 `./models` 新增至 `AWS_DATA_PATH`。如果目錄名為 `/ams/boto3models`，我們會新增下列程式碼：

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

您的程式碼應該會成功尋找 AMS 模型。做為更具體的 re：packaging 範例，以下是 Lambda 特定的工作流程。

AMS Lambda 工作流程範例：

這些步驟會套用上述一般範例來建立 AWS Lambda 函數。

1. 安裝 `amsccli`。這會在您的電腦 (Mac) `~/.aws/models` 上於 建立資料夾。
2. 將模型複製到本機目錄：

```
cp ~/.aws/models ./models
```

3. 將模型新增至函數的部署 zip 檔案：

```
zip -r9 function.zip ./models
```

Important

更新您的函數程式碼，將新模型新增至 SDK 路徑。請注意，此程式碼必須在匯入 boto3 或 botocore 之前執行！

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

由於範例模型位於名為 `models` 的目錄中，因此我們將 `./models` 新增至 `AWS_DATA_PATH`。如果目錄名為 `/ams/boto3models`，我們會新增下列程式碼：

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

現在，部署您的 函數：

1. 將函數程式碼新增至部署 zip 檔案（如果您尚未這麼做）：

```
zip -g function.zip lambda-amscm-test.py
```

2. 使用您建立的 zip 檔案（主控台或 CLI）建立或更新函數：

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://
function.zip --region us-east-1
```

您的 AMS 整合 Python Lambda 現在應該可以運作。

 Note

您的函數必須具有的 IAM 許可，amscm 否則您會收到許可錯誤。

測試 amscm 的 Lambda 函數程式碼範例 (lambda-amscm-test.py 的內容)：

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

測試輸出 (成功)：

函數回應：

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

```
Request ID:  
"1cea13c0-ed46-43b1-b102-a8ea28529c27"
```

函數日誌：

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST  
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',  
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-  
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':  
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',  
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}  
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

AMS API 到 Ruby 範例

若要搭配 Ruby 使用 AMS API，請安裝 AWS Ruby 開發套件和 AMS CLI。請遵循下列步驟：

1. 安裝 AMS CLI。請參閱 [安裝或升級 AMS CLI](#)。
2. 安裝 AWS Ruby 開發套件。請參閱[適用於 Amazon Web Services 的工具](#)。
3. 使用以下命令設定 Ruby：

```
require 'aws-sdk'  
  
config = {  
  region: 'us-east-1',  
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. 取得 AMS CTs：

```
ams_cm = Aws::amscm::Client.new(config)  
  
cts = ams_cm.list_change_type_classification_summaries  
  
print(cts)
```

AMS API 到 Java 範例

若要搭配 Java 使用 AMS API，請安裝 AWS Java 開發套件和 AMS CLI。請遵循下列步驟：

1. 安裝 AMS CLI。請參閱 [安裝或升級 AMS CLI](#)。

2. 安裝 AWS Java 開發套件。請參閱[適用於 Amazon Web Services 的工具](#)。
3. 使用以下命令設定 Java：

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;

public static void getChangeTypeClassificationSummaries() {
```

4. 設定登入資料。建議您不要硬式編碼。

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. 建立 AMS 變更管理用戶端：

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. 取得 AMS CTs：

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);
```

}

AMS 自備 EPS

使用 AMS「使用您自己的端點安全」(BYOEPS) 功能，將預設的 Trend Micro Deep Security 代理程式取代為您自己的端點安全解決方案或 Trend Micro 授權。如果您已經擁有 Trend Micro Deep Security 以外的產品具成本效益的授權，或是提供 EPS 的團隊，或是您想要使用特定的 EPS 工具，請在執行個體中使用 BYOEPS。

BYOEPS 在帳戶層級運作。您帳戶中的執行個體使用 BYOEPS 或預設的 AMS 受管 EPS：

- 多帳戶登陸區域 (MALZ)：您可以指定使用 BYOEPS 或受管 EPS 的應用程式帳戶。
- 單一帳戶登陸區域 (SALZ)：您的 AMS 帳戶使用 BYOEPS 或受管 EPS。

BYOEPS，將您的 AWS 帳單減少為 Trend Micro Deep Security 的成本。您繼續產生 EPS 的成本，因為 AMS 受管 EPS 仍然需要保護存取管理（基礎和管理主機）所需的 AMS 建立和維護 EC2 執行個體。若要計算總成本影響，您必須考慮新工具的授權成本，以及在您需要的服務層級管理 EPS 的成本。

使用 BYOEPS 會變更 AMS 角色和安全管理責任：

- R 代表負責方，其會執行工作以達成任務。
- C 代表已諮詢的對象；尋求意見的對象，通常是主題專家；以及與之進行雙邊溝通的對象。
- 我代表知情；在進度上收到通知的一方，通常只在完成任務或可交付項目時。

安全管理	客戶	AWS Managed Services
為 AMS Shared Services 的 EC2 執行個體維護有效的 Managed EPS 授權	R	C
為 AMS 共用服務的 EC2 執行個體設定受管 EPS	I	R
更新 AMS Shared Services EC2 執行個體的受管 EPS	I	R

安全管理	客戶	AWS Managed Services
在 AMS Shared Services 的 EC2 執行個體上監控惡意軟體	I	R
維護和更新 AMS Shared Services EC2 執行個體的病毒簽章	I	R
針對 AMS Shared Services 的 EC2 執行個體，修復受惡意軟體感染的執行個體	C	R

當您使用 BYOEPS 時，您會失去 AMS 提供的其中一個安全控制。您仍然可以透過 Amazon GuardDuty、Amazon Macie 和程序控制等工具提供安全管理，例如檢閱 IAM 組態。使用 BYOEPS 不會影響 AMS 合規認證和證明。不過，許多安全架構和認證都有保護惡意軟體和惡意程式碼的要求。為了協助確保您的帳戶安全且合規，請評估您規劃的控制項，以確保其符合您工作負載合規認證的安全要求。

為您的帳戶開啟 BYOEPS

開啟 BYOEPS 的程序包含三個階段，並使用數個 RFCs。檢閱以下資訊，以了解開啟 BYOEPS 所需的三個階段。然後，與您的 CSDM 協調，為您的帳戶開啟 BYOEPS。

主題

- [階段 1：先決條件](#)
- [階段 2：在您的帳戶中啟用 BYOEPS](#)
- [階段 3：執行個體遷移](#)

階段 1：先決條件

- 預設 Amazon EC2 執行個體描述檔為 `customer-mc-ec2-instance-profile`。如果您除了預設設定檔之外，還使用不同的 Amazon EC2 執行個體設定檔，則允許 `/ams/end-point-security` 對 EC2 執行個體設定檔的資源執行 `ssm:GetParameter` 動作。

如果您無法更新 EC2 執行個體描述檔，請提交 RFC，以指定您需要更新的執行個體描述檔。

- 了解此變更的範圍。

透過 AMS 自動化變更類型 (CT) 部署可讓您指定用於建立的 AMI。

若要搭配使用 AMS 受管 EPS 的帳戶使用 BYOEPS，您必須使用 AMS 從這些 EC2 執行個體解除安裝 Trend Micro 代理程式，並更新這些執行個體上的 AMS 程式碼（例如開機指令碼）。這些動作可能需要重新開機，因此最佳實務是執行這些動作，做為維護時段的一部分。請聯絡您的 CSDM 以識別執行此活動的維護時段，並建立遷移計劃。針對遷移計劃，請考慮下列問題：

1. 您需要遷移多少個執行個體？將執行個體總數分割為較小的增量批次。
 2. 您將如何分批分割執行個體？例如，您可以依資源群組分割，並建立清單與 AMS 操作團隊共用。
 3. 每個批次需要多少時間？總共需要多少時間？請考慮您可能想要在相同的維護時段安裝偏好的 EPS 工具。這需要多少時間？
- 您的 CSDM 會與 AMS 操作團隊共用遷移計劃。如果您的執行個體機群超過 50，則請使用您的 CSDM，使用規劃的事件管理 (PEM) 程序建立規劃的事件。如需詳細資訊，請參閱 [AWS Managed Services 中的計劃事件管理](#)

AMS Operations 會與您的 CSDM 協調，並根據您帳戶中的執行個體數量，建議如何根據您的維護時段提交 RFCs。

- 使用自訂或 AMS AMIs 更新 EC2 執行個體啟動自動化或程序，以使用 2020 年 12 月之後發行的 AMS AMIs。

階段 2：在您的帳戶中啟用 BYOEPS

當您在帳戶中使用 BYOEPS 時，AMS 對安全管理的責任會變更。啟用 BYOEPS 之前，請先諮詢您的安全和雲端平台團隊。

若要為您的帳戶請求 BYOEPS，請使用 ct-0xdawir96cy7k 提交「MOO」更新 RFC（管理 | 其他 | 更新），並附上下列詳細資訊：

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS 會將參數存放區更新部署到帳戶，並更新 [Amazon EC2 IAM 執行個體描述檔](#)。

 Note

- 具有使用最新 AMS AMIs 之新執行個體啟動的帳戶可以略過 Trend Micro 代理程式安裝。2020 年 12 月之前的 AMIs 不支援 BYOEPS 功能。更新使用舊 AMIs 的自動化，以搭配 BYOEPS 功能支援使用最新的 AMS AMIs。
- 如需現有的 EC2 執行個體處理方式，請參閱階段 3：執行個體遷移

階段 3：執行個體遷移

根據您的使用案例，使用下列其中一個選項來遷移執行個體。如果您不確定要選擇哪個選項，請聯絡您的 CA 或 CSDM。

具有使用 AMS 受管 EPS 之 EC2 執行個體的帳戶

在維護時段期間，為了符合第 1 階段的規劃，每個需要加入 BYOEPS 的執行個體都會執行下列動作：

- 由 AMS 執行：將 AMS 程式碼（開機指令碼、模組等）更新至最新版本。這是必要的，因為舊的 AMS 開機指令碼沒有 BYOEPS 功能支援，並在每次開機時重新安裝 Trend Micro 代理程式。此外，請解除安裝 Trend Micro 代理程式。
- 由您執行：安裝和設定您偏好的 EPS 工具。

 Important

Trend Micro Agent 提供惡意軟體防護。請務必安裝適當的替代來保護您的執行個體。

若要進行這些變更，請分批提交變更類型為 ct-2iz9nvw8zlhst 的 RFCs，[Trend Micro DSM | Remove Trend Micro EPS Agent \(Review Required\)](#)。

沒有使用 AMS 受管 EPS 之 EC2 執行個體的帳戶

具有使用最新 AMS AMIs 之新執行個體啟動的帳戶可以略過 Trend Micro 代理程式安裝。2020 年 12 月之前的 AMIs 不支援 BYOEPS 功能。更新使用舊 AMIs 的自動化，以搭配 BYOEPS 功能支援使用最新的 AMS AMIs。

在 EC2 執行個體上新增您的代理程式

您可以使用 AMS 模式來部署 CrowdStrike 或 Qualys 等工具的代理程式，提交服務請求以取得協助。

接收 AMS 通知

您與 AMS 之間的通訊有許多原因：

- AMS 建立的 RFC 需要您的核准
- 建立的 AMS 案例，用於調查您建立的失敗 RFC
- 透過監控提醒建立的事件
- 修補服務通知，通知您即將進行的修補
- 服務請求和事件報告
- 每月 CRM 報告
- 偶爾重要的 AWS 公告（如果需要您採取任何動作，您的 CSDM 會與您聯絡）

所有這些通知都會傳送至您在加入時提供 AMS 的預設聯絡資訊（根帳戶電子郵件）。由於難以保持個別電子郵件的更新，我們建議您使用可在結束時更新的群組電子郵件。AMS 操作也會收到傳送給您的所有通知，並在做出回應之前進行分析。

AMS 通知服務提供兩種額外方式來設定通知的聯絡人：

- 使用聯絡人標籤標記您的資源（標籤鍵值為聯絡資訊），並將標籤鍵名稱提供給 CSDM。除了加入時建立的帳戶聯絡人之外，這些資源的警示也會傳送至金鑰值中提供的聯絡人。這對應用程式擁有者特別有用。如需詳細資訊，請參閱[標籤型提醒通知](#)。
- （加入時需要）將非資源型通知的聯絡人清單傳送到 CSDM。例如，您可能有一個名為 "SecurityContacts" 的清單和另一個名為 "OperationsContacts" 的清單，以此類推。AMS 會將清單新增至通知服務，而適用於該清單內容的警示會傳送給這些聯絡人。這對於組織事宜特別有用。

此進階警示路由功能適用於大多數基本 CloudWatch 警示，例如 Amazon EC2 執行個體故障、Amazon Elastic Block Store (Amazon EBS) 磁碟區容量使用率 - 根用量、Amazon EBS NonRoot 用量、高記憶體使用率、高交換用量，以及 Amazon EC2 的高 CPU 使用率。

此外，當您提交服務請求或事件報告時，您可以選擇新增「CC 電子郵件」（強烈建議），這些電子郵件地址會收到有關服務請求或事件的通知。

Important

雖然在服務請求和事件報告中提供的 CC 電子郵件地址會收到通訊的電子郵件通知，但其他通知，例如修補通知，會出現在您的服務請求清單中（電子郵件也會傳送給預設聯絡人），而不

會明確通知您有正在等待您注意的通訊。因此，我們強烈建議您盡可能新增 CC 電子郵件，並將預設的聯絡人電子郵件設定為群組，讓使用 AMS 的每個人都是其中的成員。

此外，您可以請求新 AMIs、RFC 狀態變更以及 AMS 帳戶中組態變更的特殊通知。接下來會討論這些選用的通知服務。

使用 SNS 的 AMS AMI 通知

AMS 提供 AMI 通知服務。您可以使用它來訂閱 Amazon Simple Notification Service (SNS) 主題，在 AMS AMI 更新發佈時通知您。您可以選擇只接收您使用的 AMS AMIs 的通知，也可以註冊以接收所有 AMS AMIs 的更新通知。如需 SNS 主題的詳細資訊，請參閱[什麼是 Amazon Simple Notification Service ?](#)

每當 AMIs 發佈時，我們會傳送通知給對應主題的訂閱者；本節說明如何訂閱 AMS AMI 通知。

訊息範例

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has been released. You are now able to launch new EC2 stacks from these AMIs. Please use this time to update any dependencies such as CloudFormation or Autoscaling groups. Release Notes Windows - Contains latest Windows Patches: Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004, KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091, KB4507459) Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057, KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux patches - All AMIs now force domainjoin-cli leave before domainjoin-cli join for better stability in the domain join process.\"\", \"images\": {\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\": \"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\", \"Timestamp\" : \"2021-09-03T19:05:57.882Z\", \"SignatureVersion\" : \"1\",
```



```
"Signature" : "example sig",
"SigningCertURL" : "example url",
"UnsubscribeURL" : "example url"
}
```

可能訂閱的 AMS AMI 主題：

- ALL：使用 customer-ams-all-amis。本主題訂閱會在任何 AMS AMIs 更新時通知您。
- AMS AWS Linux AMIs：對於 Amazon Linux，請使用 customer-ams-amazon1 和 customer-ams-amazon1-security-enhanced。對於 Amazon Linux 2，請使用 customer-ams-amazon2 和 customer-ams-amazon2-security-enhanced。
- AMS SUSE Linux AMIs：使用 customer-ams-sles12 或 customer-ams-sles15。
- AMS AWS RedHat AMIs：使用 customer-ams-rhel8、customer-ams-rhel8-security-enhanced、customer-ams-rhel7、customer-ams-rhel7-security-enhanced。
- AMS AWS CentOS AMIs：使用 customer-ams-centos7、customer-ams-centos7-security-enhanced。
- AMS Ubuntu AMIs：使用 customer-ams-ubuntu18。
- AMS AWS Windows AMIs：使用 customer-ams-windows2019、customer-ams-windows2019-security-enhanced、customer-ams-windows2016、customer-ams-windows2016-security-enhanced、customer-ams-windows2012、customer-ams-windows2012r2、customer-ams-windows2012r2-security-enhanced、customer-ams-windows2022。

若要使用 Amazon SNS 主控台訂閱 AMS 新 AMI 通知：

1. 開啟儀表板的 Amazon SNS 主控台 <https://console.aws.amazon.com/sns/v2/home>。
2. 在右上角，將您訂閱的 AMIs 變更為 AWS 區域。
3. 在左側導覽窗格中，選擇訂閱，然後選擇建立訂閱。
4. 請提供下列資訊：
 - a. 主題 ARN：arn:aws:sns:{**REGION**}:287847593866:{**AMS_AMI_NAME**} 其中 REGION 是選取的 AWS 區域 (SNS 通知的建立位置)，而 AMS_AMI_NAME 是您想要通知的 AMI。
範例：
 - 若要訂閱 AWS 區域 us-east-1 中新 AMS Amazon Linux AMIs 的通知，請使用此主題 ARN = arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1。

- 若要訂閱 AWS 區域 us-west-2 中新 AMS Window Server 2016 AMIs通知，請使用此主題
ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. 對於 通訊協定，選擇 電子郵件。
 - c. 針對 Endpoint (端點)，請輸入可用於接收通知的電子郵件地址。我們建議分發清單，而不是個人的電子郵件。
5. 選擇建立訂閱。
 6. 當您收到主旨行為「AWS Notification - Subscription Confirmation」的確認電子郵件時，請開啟電子郵件，然後選擇確認訂閱以完成您的訂閱。

 Note

您不限於通訊協定的電子郵件。如需其他可接受通訊協定及其使用方式的資訊，請參閱[訂閱](#)。

若要使用 AWS SNS 主控台取消訂閱 AMS 新 AMI 通知：

1. 開啟儀表板的 Amazon SNS 主控台<https://console.aws.amazon.com/sns/v2/home>。
2. 在導覽列中，將變更為您選擇的 AWS 區域。您必須使用要接收對應 AMIs 區域。
3. 在導覽窗格中，選擇訂閱，選擇訂閱，然後選擇動作 -> 刪除訂閱。
4. 出現確認提示時，請選擇刪除。

若要使用部署 | 擷取 | CloudFormation 範本的堆疊 | 建立 (ct-36cn2avfrj9v) 訂閱 AMS 新 AMI 通知：

1. 若要訂閱 AmazonLinuxSubscription，請建立並儲存執行參數 JSON 檔案；此範例會將其命名為 `CreateSubscribeAmiParams.json`：

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type": "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

```
}  
}
```

2. 使用下列內容建立並儲存 RFC 參數 JSON 檔案；此範例會將其命名為 CreateSubscribeAmiRfc.json 檔案：

```
{  
  "ChangeTypeId": "ct-36cn2avfrrj9v",  
  "ChangeTypeVersion": "1.0",  
  "Title": "cfn-ingest-subscribe-ami"  
}
```

3. 建立 RFC，指定 CreateSubscribeAmiRfc 檔案和 CreateSubscribeAmiParams 檔案：

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --  
execution-parameters file://CreateSubscribeAmiParams.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

如需建立 AMIs 的範例，請參閱[建立 AMI](#)。

如需以程式設計方式使用 AMIs 的資訊，請參閱[EC2 堆疊：建立](#)。

服務通知

當您需要採取行動或注意到可能會影響您的帳戶或資源的項目時，AMS 會傳送傳出服務請求或服務通知，包括：

- 基礎設施影響：當基礎 AWS 服務影響您的基礎設施時，AMS 會傳送服務通知，而且您需要在特定日期之前採取行動，否則您可能會中斷。
- EC2 硬體問題：AMS 會針對需要您在特定日期之前重新啟動 EC2 執行個體的 EC2 硬體問題傳送服務通知，或讓您知道 AMS 會為您重新啟動執行個體。這是重要的通知，因為重新啟動可能會導致中斷，而且您必須以可接受的日期回應，或使用 ct-09qbhy7kvtxqw 建立 RFC，以自行重新啟動執行個體。如果您未回應，這類服務通知會在五天內自動關閉。

RFC 狀態變更通知

AMS 透過電子郵件和 CloudWatch Events 提供 RFC 狀態變更的通知：

- 透過 AMS 主控台傳送的電子郵件：建立 RFC 精靈的第二個頁面上有一個選項，您可以在其中新增最多五個電子郵件地址，以便在 RFC 狀態變更時收到通知。
- CloudWatch Events：您可以為 CloudWatch Events 設定不同的規則和目標，以接收每個 RFC 狀態變更的通知。

電子郵件通知

您可以新增電子郵件地址，以接收您在 AMS 主控台或使用 AMS API/CLI 建立之 RFC 的 RFC 狀態變更。

在 AMS 主控台中，使用建立 RFC 精靈第二頁的電子郵件通知選項：

在 AMS API/CLI 中，將類似這樣的行新增至 RFC 的 RFC 參數區段（請勿將行新增至執行參數區段）：

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

通知的行為會根據 RFC 排程類型而有所不同：

- 已排程 RFCs 上接收電子郵件通知：已提交、已排程、InProgress、已完成、已拒絕、已取消、已自動拒絕或已自動取消。
- ASAP RFCs 會收到電子郵件通知：已提交、InProgress、已完成、已拒絕、已取消、AutoRejected 或自動取消。

Note

- 電子郵件通知會從此地址傳送：no-reply@managedservices.amazonaws.com。
- RFC 標題中的特殊字元和 URLs 會在我們傳送的電子郵件中修訂。這是安全措施。

CloudWatch Events 通知

AMS 透過 CloudWatch Events 提供 RFC 狀態變更的推送通知。若要取得這些通知：

1. 建立將傳送通知的主題和訂閱。您可以指定您喜歡的主題；如需執行此作業的相關資訊，請參閱 [SNS 主題和訂閱：建立](#)。

2. 使用 管理 | 其他 | 其他 | 建立變更類型提交 RFC，並在 RFC 狀態變更通知的請求中包含 SNS 主題和訂閱。

當您提交此功能的管理 | 其他 | 其他 RFC 請求時，您可以指定您有興趣收到通知的 RFC 狀態變更，以及變更類型，並設定其他篩選條件。例如，您可能想要請求僅在管理員存取變更類型為 EventType = RfcSubmitted 和 EventType = RfcUpdated 時收到通知。

這是您可以接收的 CloudWatch 事件通知範本（包含所有可能的值）：

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected | RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted | RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
      "StartTime": "null | Expected_Start_Time",
      "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled | ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
  }
}
```

```
}
```

支援的 RFC 狀態變更 (EventType)，如實際 CloudWatch Events 通知所示：

- RfcActionStateUpdated (無 AMS 主控台選項)：其中一個狀態的 RFC，稍後說明已變更。
- RfcApproved (無 AMS 主控台選項)：RFC 通過系統和/或 AMS 運算子驗證，並已核准完成。
- RfcAutoRejected (自動拒絕)：RFC 失敗的系統驗證或 AMS 運算子已拒絕。
- RfcCanceled (已取消或自動取消)：RFC 已由提交者或 AMS 運算子取消。
- RfcCompleted (Completed)：RFC 執行參數已完成，包括 UserData。
- RfcCreated (無 AMS 主控台選項)：RFC 已成功建立 (JSON 和提交的參數有效)。
- RfcInProgress (InProgress)：RFC 執行仍在進行中。
- RfcRejected (拒絕)：已拒絕 RFC 失敗的系統或 AMS 運算子驗證。
- RfcSubmitted (Submitted)：RFC 已提交且正在進行系統驗證。
- RfcUpdated (無 AMS 主控台選項)：RFC 已由 AMS 運算子手動更新。

此外，您可以將 CloudWatch Events (CWE) 通知傳送至任何支援的目的地，並在這些自動通知的基礎上建置您自己的系統：

- Amazon EC2 執行個體
- AWS Lambda 函數
- Amazon Kinesis Data Streams 中的串流
- Amazon Data Firehose 中的交付串流
- Amazon CloudWatch Logs 中的記錄群組
- Amazon ECS 任務
- Systems Manager Run Command
- Systems Manager Automation
- AWS Batch 任務
- Step Functions 狀態機器
- CodePipeline 中的管道
- CodeBuild 專案
- Amazon Inspector 評定範本

- Amazon SNS 主題
- Amazon SQS 佇列
- 內建目標：EC2 CreateSnapshot API 呼叫、EC2 RebootInstances API 呼叫、EC2 StopInstances API 呼叫和 EC2 TerminateInstances API 呼叫。
- 另一個 AWS 帳戶的預設事件匯流排

Note

我們會盡力傳送 RFC 狀態變更的 CloudWatch Events 通知。

設定私有和公有 DNS

在加入期間，AMS 會為受管資源和 AMS 之間的通訊設定私有 DNS 服務。

您可以使用 AMS Route 53 來管理應用程式資源 (Web 伺服器、應用程式伺服器、資料庫等) 的內部 DNS 名稱，而不將此資訊公開至公有網際網路。這增加了額外的安全層，也可讓您將 DNS 名稱映射到不同的 IP 地址，從主要資源容錯移轉到次要資源 (通常稱為「翻轉」)。

使用 [部署 | 進階堆疊元件 | DNS \(私有\) | 建立 \(ct-0c38gftq56zj6\)](#) 或 [部署 | 進階堆疊元件 | DNS \(公有\) | 建立 \(ct-0vzsr2nyraedl\)](#) 建立私有 DNS 資源後，您可以使用 [管理 | 進階堆疊元件 | DNS \(私有\) | 更新 \(ct-1d55pi44ff21u\)](#) 和 [管理 | 進階堆疊元件 | DNS \(公有\) | 更新 \(ct-1hzofpphabs3i\)](#)、設定額外或更新現有記錄集 CNAMEs。對於多帳戶登陸區域 (MALZ) 帳戶，在應用程式帳戶 VPCs 中建立的 DNS 資源可以與共用服務帳戶 VPC 共用，以使用 AMS AD 維護集中式 DNS。

MALZ

下圖說明多帳戶登陸區域 AMS 的可能 DNS 組態。它說明了 AMS 與典型客戶網路之間的混合 DNS 設定。客戶網路 DNS 伺服器中的正式名稱記錄 (CNAME) 轉送至共用服務帳戶中的 AMS AD DNS，其條件式轉送具有轉送至 A 記錄的 AMS FQDN CNAME。

SALZ

下圖說明單一帳戶登陸區域 (SALZ) 的可能 DNS 組態。它顯示 AMS 和典型客戶網路之間的混合 DNS 設定。客戶網路 DNS 伺服器的 CNAME 會轉送至具有條件式轉送的 AMS AD DNS，其 AMS FQDN 的 CNAME 會轉送至 A 記錄。

SALZ Route53 DNS

下圖說明單一帳戶登陸區域 (SALZ) 的可能 DNS 組態。它顯示 AMS 和典型客戶網路之間的混合 DNS 設定。客戶網路 DNS 伺服器的 CNAME 會轉送至具有條件式轉送的 AMS AD DNS，其 AMS FQDN 的 CNAME 會轉送至 A 記錄。這也將 Route53 用於傳出網路流量，因此帳戶中的任何應用程式都可以在具有最高可用性的帳戶中擁有 DNS 解析。

Route53 啟用的解析路徑：

- 嘗試解析 AMS MAD 名稱的執行個體 --> VPC +2 (Route53/AmazonProvidedDNS) --> 評估的條件式轉送器 --> Route53 MAD 條件式轉送器規則相符 --> Route53 傳出解析器 --> Managed AD DNS
- 嘗試解析客戶內部部署名稱的執行個體 --> VPC +2 (Route53/AmazonProvidedDNS) --> 評估的條件式轉寄站 --> 符合的 Route53 內部部署條件轉寄站規則 --> Route53 Outbound 解析程式 --> 客戶內部部署 DNS
- 嘗試解析網際網路名稱的執行個體 --> VPC +2 (Route53/AmazonProvidedDNS) --> 評估的條件式轉寄站 --> 沒有相符的轉寄站 --> 網路 DNS 服務

如需詳細資訊，請參閱[搭配 VPC 使用 DNS](#) 和[使用私有託管區域](#)。

AMS 輸出流量管理

根據預設，AMS 私有和客戶應用程式子網路目的地 CIDR 為 0.0.0.0/0 的路由具有網路位址轉譯 (NAT) 閘道做為目標。AMS 服務、TrendMicro 和修補是必須具有網際網路輸出存取權的元件，以便 AMS 能夠提供其服務，而 TrendMicro 和作業系統可以取得更新。

AMS 支援透過客戶管理的輸出裝置將輸出流量轉移到網際網路，只要：

- 它充當隱含（例如透明）代理。

以及

- 它允許 AMS HTTP 和 HTTPS 相依性（列於本節），以允許 AMS 受管基礎設施的持續修補和維護。

部分範例如下：

- 傳輸閘道 (TGW) 具有預設路由，指向多帳戶登陸區域網路帳戶中透過 AWS Direct Connect 連線的客戶受管內部部署防火牆。
- TGW 有一個預設路由，指向多帳戶登陸區域輸出 VPC 中的 AWS 端點，利用 AWS PrivateLink，指向另一個 AWS 帳戶中的客戶受管代理。
- TGW 預設路由指向另一個 AWS 帳戶中的客戶受管防火牆，並以 site-to-site 連接做為多帳戶登陸區域 TGW 的連接。

AMS 已識別對應的 AMS HTTP 和 HTTPS 相依性，並持續開發和精簡這些相依性。請參閱 [egressMgmt.zip](#)。除了 JSON 檔案之外，ZIP 還包含 README。

Note

- 此資訊並不全面 - 此處未列出某些必要的外部網站。
- 請勿在拒絕清單或封鎖策略下使用此清單。
- 此清單旨在做為輸出篩選規則集的起點，預期報告工具將用於精確判斷實際流量與清單的差異。

若要詢問有關篩選輸出流量的資訊，請傳送電子郵件給您的 CSDM：ams-csdm@amazon.com。

在 AMS Advanced 中部署 IAM 資源

AMS 會以兩種方式在您的多帳戶登陸區域 (MALZ) 應用程式和單一帳戶登陸區域 (SALZ) 帳戶中部署 IAM 資源：

- 自動化 IAM 佈建：AMS 中的此功能可讓您為 IAM 角色或政策佈建提交建立、更新或刪除變更類型，無需操作員檢閱，且會自動執行 IAM 和 AMS 驗證檢查。

必須使用 管理 | 受管帳戶 | AMS 自動化 IAM 佈建與讀寫許可 | [啟用（需要檢閱）](#) 變更類型 (ct-1706xvk6j9hf) 明確啟用此功能。如需詳細資訊，請參閱 [自動化 IAM 佈建 AMS](#)。啟用 AMS 自動化 IAM 佈建後，您可以存取建立、更新和刪除變更類型來管理您的 IAM 資源。

- 檢閱必要的 IAM 變更類型：此變更類型、部署 | 進階堆疊元件 | Identity and Access Management (IAM) | [建立實體或政策（需要檢閱）](#) (ct-3dpd8mdd9jn1r)，需要 AMS 運算子檢閱，如果需要釐清，有時可能需要幾天才能完成。

 Note

無論使用哪種方法，IAM 角色都會佈建至相關帳戶，而且在佈建角色之後，您必須在聯合解決方案中加入該角色。

自動化 IAM 佈建 AMS

AWS Managed Services (AMS) 支援 IAM 資源的自動化驗證和佈建，包括使用 AMS Advanced 變更請求 (RFCs) 和新變更類型 CTs) 的角色和政策。先前，這些請求經過半自動化程序，有時會導致長時間等待。現在，您可以使用 AMS 自動化 IAM 佈建來佈建 IAM 資源，並更快地取得結果。

AMS 中的自動化 IAM 佈建如何運作

自動化 IAM 佈建依賴 IAM 的自動執行期檢查來驗證 IAM 資源的變更。這些自動檢查會在執行建立、更新或刪除變更類型時執行，防止過度允許或模式不安全的 IAM 資源部署到您的帳戶。這可讓您將 IAM 檢閱中的嚴格程度與團隊的專業知識進行比對。我們建議初次使用雲端服務且需要手動檢查所有 IAM 資源變更的團隊使用現有檢閱所需的變更類型：部署 | 進階堆疊元件 | Identity and Access Management (IAM) | [建立實體或政策（需要檢閱）](#)，(ct-3dpd8mdd9jn1r)。具備 AWS 專業知識並控制其環境的團隊可以使用自動化 IAM 佈建來加速部署。您可以使用此功能透過自動執行時間檢查執行驗證，或在驗證成功後執行 IAM 資源的驗證和佈建。

 Important

AWS Managed Services 已主動實作驗證[執行期檢查](#)清單，以防止建立具有特定許可和條件的 IAM 資源或政策。如需這些權限和條件的說明，請參閱在 [AMS Advanced 中部署 IAM 資源](#)。自動化變更類型 [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#) 和 [ct-17cj84y7632o6](#)，可讓熟練管理 IAM 資源的使用者佈建 IAM 角色和政策，允許超出唯讀權限的動作。

此外，您可以使用透過自動變更類型 [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#) 和 [ct-17cj84y7632o6](#) 建立的角色來建立新的資源。不過，資源無法遵循 AMS 命名標準，也不是標準 AMS 堆疊的一部分。AMS 會盡最大努力提供這些特定資源的操作和安全性支援。

雖然手動和自動化程序都旨在維護我們的安全標準，但請務必注意兩者之間的檢查存在差異。自動化佈建可讓您更靈活地建立和更新角色和政策；因此，它們並不相同。建議您的組織仔細檢閱 AMS 使用者指南中列出的驗證[執行期檢查](#)，以確保它們符合您組織的期望和要求。

驗證流程

驗證和佈建流程

Note

此功能適用於具有 AWS 和 IAM 資源經驗的團隊，我們不建議新加入的團隊使用此功能 AWS。自動化驗證程序旨在捕捉大多數錯誤，並有助於團隊在了解其所需的許可時快速檢閱 IAM 的變更。若要安全有效地使用新的變更類型，我們建議您充分了解 AWS IAM，以及變更類型提供的[執行期檢查](#)，以判斷它們是否適合您的團隊。

在 AMS 中加入 AMS 自動化 IAM 佈建

若要使用新的變更類型，請先使用下列變更類型提交 RFC 來啟用 AMS 自動化 IAM 佈建：管理 | 受管帳戶 | 具有讀寫許可的 AMS 自動化 IAM 佈建 | [啟用（需要檢閱）](#) (ct-1706xvk6j9hf)。AWS 需要您的組織通過客戶安全風險管理 (CSRM) 程序，以確保這些變更類型的使用符合您的組織政策。AWS 作為必要審核的一部分，營運團隊會與您合作，以風險接受的形式取得安全團隊聯絡人的明確核准。若要進一步了解，請參閱 [RFC 客戶風險管理 \(CSRM\) 程序](#)。

在啟用具有讀寫許可的 AMS 自動化 IAM 佈建功能的 RFC 成功之後，AMS 會在用來提交啟用 RFC 的帳戶中啟用 AMS 自動化 IAM 佈建變更類型。若要確認帳戶已開啟 AMS 自動化 IAM 佈建，請檢查 IAM 主控台是否有 `AWSManagedServicesIAMProvisionAdminRole` 角色。

在加入過程中，AMS 會在帳戶的相同 AWS 區域中佈建 IAM Access Analyzer，以利用其存取預覽功能。IAM Access Analyzer 可協助識別組織和帳戶中與外部實體共用的資源、根據政策文法和最佳實務驗證 IAM 政策，並根據 AWS CloudTrail 日誌中的存取活動產生 IAM 政策。若要進一步了解，請參閱 [使用 AWS Identity and Access Management Access Analyzer](#)。

加入後，`AWSManagedServicesIAMProvisionAdminRole` 會部署到已啟用的帳戶。如果您選擇透過 SAML 聯合使用此角色，則必須將該角色加入聯合解決方案。

在加入過程中，您可以請求更新 `AWSManagedServicesIAMProvisionAdminRole` 的信任政策，以授予另一個 IAM 角色 ARN 來擔任此角色 AWS Security Token Service。

在 AMS 中使用 AMS 自動化 IAM 佈建

您可以使用下列 AMS 自動化 IAM 佈建變更類型建立 RFCs。

 Note

- 僅支援對角色和政策進行佈建。

更新角色時，更新 CT 會使用提供的受管政策 ARNs 和「擔任角色」政策文件，取代現有的受管政策 Amazon 資源名稱 (ARNs) 和「擔任角色」政策文件清單。在部分更新中，例如，不允許在現有受管政策 ARN 清單中新增或移除 ARNs，也不允許新增或移除個別政策陳述式至「擔任角色」政策文件。同樣地，更新政策時，更新 CT 會取代現有的政策文件，不允許在現有的政策文件中新增或移除個別政策陳述式。

- 選取「僅驗證」選項時，執行時間檢查時不會佈建任何 IAM 實體或政策。無論問題清單為何，RFC 狀態都是「成功」。「成功」狀態表示成功驗證提供的 IAM 實體或政策。

- 部署 | 進階堆疊元件 | Identity and Access Management (IAM) | [建立實體或政策 \(讀寫許可\)](#) (ct-1n9gfnog5x7fl)：會自動驗證和佈建新的 IAM 實體或政策。
- 管理 | 進階堆疊元件 | Identity and Access Management (IAM) | [更新實體或政策 \(讀寫許可\)](#) (ct-1e0xmuy1diafq)：現有 IAM 實體或政策會自動更新和驗證。
- 管理 | 進階堆疊元件 | Identity and Access Management (IAM) | [刪除實體或政策 \(讀寫許可\)](#) (ct-17cj84y7632o6)：刪除使用自動建立實體或政策變更類型佈建的現有 IAM 實體或政策。

您只能使用專用 IAM 角色呼叫上述三個 CTs：AWSManagedServicesIAMProvisionAdminRole。此角色僅適用於已使用 管理 | 受管帳戶 | AMS 自動化 IAM 佈建讀寫許可 | [啟用 \(需要檢閱\)](#) (ct-1706xvk6j9hf) 加入此功能的帳戶。

 Important

建立、更新和刪除變更類型一律會顯示在您的帳戶中，但預設不會開啟。如果您嘗試使用這些變更類型之一提交 RFC，但未先啟用 AMS 自動化 IAM 佈建功能，則會顯示「未授權」錯誤。

限制：

- 建立 CT 可能允許您建立具有建立 AWS 資源許可的 IAM 角色或政策。不過，這些角色和政策建立 AWS 的資源並非由 AMS 管理。最佳實務是遵循您的組織控制，以限制此類角色或政策的建立。
- 更新 CT 無法修改使用 CFN 擷取、直接變更模式、開發人員模式建立的 IAM 角色和政策，在某些情況下，也無法透過現有的 AMS 進階手動或自動 CTs 修改。

- 刪除 CT 無法刪除未使用 AMS Automated IAM Provisioning Create CT 建立的現有角色或政策。
- 直接變更模式角色不支援具有讀寫許可的 AMS 自動化 IAM 佈建功能。這表示您無法使用這些角色佈建或更新具有讀寫許可的 IAM 角色和政策。
- 具有讀寫許可的 AMS 自動化 IAM 佈建建立、更新和刪除變更類型與 ServiceNow 連接器不相容。

AMS 自動化 IAM 佈建的執行期檢查

自動化 IAM 佈建會利用的檢查 AWS Identity and Access Management Access Analyzer，並根據 AMS 界限政策執行額外的檢查和驗證。AMS 根據 IAM 最佳實務定義了額外的檢查和驗證、體驗在雲端中操作客戶工作負載，以及集體 AMS IAM 手動評估體驗。

您可以在變更請求 (RFC) 輸出中檢視政策執行期檢查問題清單。調查結果包括資源識別符、產生調查結果的角色和/或政策內的位置，以及概述 IAM 實體或資源無法通過檢查的訊息。這些調查結果可協助您撰寫功能正常且符合安全最佳實務的政策。

Note

自動化 IAM 佈建會嘗試特定實體或政策定義中無法通過檢查的位置。根據類型，位置可能包含資源名稱或 ARN，或陣列中的索引。例如，協助您調整實體或政策以取得成功結果的陳述式。

為了獲得順暢的 AMS 自動化 IAM 佈建體驗，最佳實務是使用「僅限驗證」選項來執行驗證檢查，直到 RFC 輸出中報告的驗證檢查中沒有問題清單為止。當驗證檢查回報沒有問題清單時，請選擇從 AMS 主控台建立複本，以快速建立現有 RFC 的副本。當您準備好佈建時，請在參數區段中，將僅驗證值從是切換為否，然後繼續。

以下是 AMS Automated IAM Provisioning 執行以確保 IAM 資源安全的執行期檢查：

Note

若要佈建包含這些自動變更類型拒絕之動作的 IAM 政策，您必須遵循 RFC 客戶安全風險管理 (CSRM) 程序。使用下列變更類型：部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策（需要檢閱）(ct-3dpd8mdd9jn1r)。

- IAM Access Analyzer 政策檢查和驗證：另請參閱 [Access Analyzer 政策檢查參考](#) 和 [IAM Access Analyzer 政策驗證](#)。

- AMS 許可界限政策檢查：預設拒絕的一組服務上的動作。如需詳細資訊，請參閱[自動 IAM 佈建許可界限檢查](#)。
- 客戶定義的許可界限政策檢查：一組遭拒服務的其他限制動作。如需詳細資訊，請參閱[自動 IAM 佈建許可界限檢查](#)。
- AMS 定義的自訂檢查：在請求的 IAM 實體或政策中識別各種不安全和過度寬鬆政策或存取模式的檢查，並在找到請求時拒絕請求。如需詳細資訊，請參閱[AWS JSON 政策元素：主體](#)。

問題清單	描述
您可以從信任區域以外的外部帳戶存取角色。	此調查結果是指在您信任區域以外的角色信任政策中列出的委託人。信任區域定義為建立角色的帳戶，或帳戶所屬 AWS 的組織。不屬於帳戶或相同 AWS Organization 的實體是外部實體。若要解決調查結果，請檢閱委託人 ARNs 中的帳戶 ID，並確保他們屬於您，並且是 AMS 加入的帳戶。
角色可由帳戶 <i>External_Account_ID</i> 所擁有的外部實體存取，而該外部實體並非 AMS 客戶擁有的帳戶 <i>Account_ID</i> 所擁有。	如果角色信任政策包含的主體 ARN 具有您未擁有的帳戶 ID 和 AMS 加入帳戶，則會產生此調查結果。若要解決此問題清單，請從角色信任政策中移除任何這類委託人。
正式使用者 ID 不是 IAM 信任政策中支援的主體。	IAM 信任政策不支援正式主體 IDs。若要解決問題清單，請從角色信任政策中移除任何這類委託人。
角色可由信任區域以外的外部 Web 身分存取。	如果角色信任政策允許 SAML IdP 以外的外部 Web 身分提供者 (IdP)，則會產生此調查結果。若要解決此問題清單，請檢閱角色信任政策，並移除允許 <code>sts:AssumeRoleWithWebIdentity</code> 操作的陳述式。
角色可透過 SAML 聯合存取；不過，提供的 SAML 身分提供者 (IdP) 不存在。	如果角色信任政策包含您帳戶中不存在的 SAML IdP，就會產生此調查結果。若要解決此問題，請確定您的帳戶中存在所有列出的 SAML IdP。

問題清單	描述
政策包含相當於管理員或進階使用者存取的特權動作。考慮將許可範圍縮減為特定服務、動作或資源。如果使用 NotAction 或 NotResource 等進階政策元素，請確保它們不會授予比您預期更多的存取權，尤其是在允許陳述式中。	在 中，最佳安全實務是在使用 IAM 政策設定許可時，僅 AWS Identity and Access Management 授予執行任務所需的許可。透過定義可在特定條件下對特定資源採取的動作來執行此操作，也稱為最低權限許可。當自動化偵測到政策授予廣泛的許可，且不遵循最低權限原則時，就會產生此調查結果。若要解決問題清單，請檢閱並減少許可。
陳述式包含 <i>Service_Name</i> 的特權動作。考慮使用拒絕陳述式排除這些動作。如需特殊權限動作清單，請參閱 AMS 文件中的邊界政策參考。	AMS 將特定服務的特權動作識別為具有風險，並需要客戶安全團隊進一步的風險審查和接受。當自動化偵測到授予此類許可的指定政策時，就會產生此調查結果。若要解決此問題清單，請在政策中拒絕這些動作。如需動作清單，請參閱 AMS 界限政策。如需 AMS 界限政策的詳細資訊，請參閱 AMS 自動化 IAM 佈建許可界限檢查。
陳述式會授予對 <i>Service_Name</i> 的特權 RFC 變更類型的存取權：ct-1n9gfnog5x7fl、ct-1e0xmu y1diafq 和 ct-17cj84y7632o6。考慮將許可範圍限定為特定變更類型，或使用拒絕陳述式排除這些變更類型。	如果政策授予使用自動 IAM 佈建變更類型 (CTs 許可，則會產生此調查結果。CTs 必須接受風險，且只能透過加入的角色使用。因此，您無法授予這些 CTs 許可。若要解決此問題清單，請使用這些 CTs 拒絕 RFC 動作。
陳述式包含不在 <i>Service_Name</i> 資源範圍內的特權動作。考慮將動作範圍限定為特定資源，或使用 AMS 命名空間字首排除資源。如果使用萬用字元，請確保它們將範圍限制為您的資源。	如果政策授予不在指定服務資源範圍內的特權動作，則會產生此調查結果。萬用字元通常會建立過於寬鬆的政策，將廣泛的資源或動作帶入許可的範圍。若要解決問題清單，請減少您擁有之資源的許可範圍，或排除 AMS 命名空間中的資源。如需 AMS 命名空間字首的清單，請參閱 AMS 文件中的邊界政策。請注意，並非所有字首都適用於所有服務。如需 AMS 界限政策的詳細資訊，請參閱 AMS 自動化 IAM 佈建許可界限檢查。

問題清單	描述
無效的帳戶 ID 或 Amazon Resource Name (ARN)。	如果政策或角色信任政策中指定的任何 ARN 或帳戶 ID 無效，就會產生此調查結果。若要檢閱服務的有效資源 ARN 的資源，請參閱 服務授權參考 。請確定帳戶 ID 是 12 位數的號碼，且帳戶處於作用中狀態 AWS。
在 ARN 中對帳戶 ID 使用萬用字元 (*) 受到限制。	如果在 ARN 的帳戶 ID 欄位中指定萬用字元 (*)，則會產生此調查結果。帳戶 ID 欄位中的萬用字元符合任何帳戶，並可能授予資源意外的許可。若要解決此問題，請以特定帳戶 ID 取代萬用字元。
指定的資源帳戶不是由擁有 <i>Account_ID</i> 的相同 AMS 客戶擁有。	如果資源 ARN 中指定的帳戶 ID 不屬於您，且不是由 AMS 管理，則會產生此調查結果。若要解決此問題，請確定所有資源（如政策中的 ARN 所指定）都屬於由 AMS 管理的帳戶。
角色名稱位於 AMS 限制的命名空間中。	如果您嘗試建立名稱開頭為 AMS 預留字首的角色，就會產生此調查結果。若要解決此問題，請針對您的使用案例特有的角色使用名稱。如需 AMS 預留字首清單，請參閱 AMS 預留字首 。
政策名稱位於 AMS 限制的命名空間中。	如果您嘗試建立名稱開頭為 AMS 預留字首的政策，就會產生此調查結果。若要解決此問題，請針對您的使用案例特定的政策使用名稱。如需 AMS 預留字首清單，請參閱 AMS 預留字首 。
ARN 中的資源 ID 位於 AMS 限制的命名空間中。	如果您嘗試建立將許可授予 AMS 命名空間中具名資源的政策，就會產生此調查結果。若要解決此問題，請務必將許可範圍限定為資源，或拒絕許可範圍限定為 AMS 命名空間中的資源。如需 AMS 命名空間的詳細資訊，請參閱 AMS 限制命名空間 。

問題清單	描述
無效的政策變數案例。將變數更新為 <i>Variable_Names</i> 。	如果嘗試在不正確的情況下建立包含 IAM 全域政策變數的政策，則會產生此調查結果。若要解決此問題，請針對政策中的全域變數使用正確的大小寫。如需全域變數的清單，請參閱AWS 全域條件內容索引鍵。如需政策變數的詳細資訊，請參閱 IAM 政策元素：變數和標籤
陳述式包含不在 KMS 金鑰範圍內的特權動作。請考慮將這些許可範圍限定為特定金鑰，或排除 AMS 擁有的金鑰。	如果政策包含的許可範圍不限於您擁有的特定 KMS 金鑰，則會產生此調查結果。若要解決此問題，請將許可範圍限定為特定金鑰，或排除 AMS 擁有的金鑰。AMS 擁有的金鑰具有特定的別名集。如需 AMS 擁有的金鑰別名清單，請參閱 AMS 自動化 IAM 佈建許可界限檢查。
陳述式包含不在 KMS 金鑰別名範圍內的特權動作。請考慮將這些許可限定為您的金鑰或別名，或排除 AMS 擁有的金鑰別名。	如果政策包含的許可範圍不限於您擁有的特定 KMS 金鑰別名，則會產生此調查結果。若要解決此問題，請將許可範圍限定為特定金鑰，或排除 AMS 擁有的金鑰。AMS 擁有的金鑰具有特定的別名集。如需 AMS 擁有的金鑰別名清單，請參閱 AMS 自動化 IAM 佈建許可界限檢查。
陳述式包含權限動作，這些動作並未使用 充分限定 KMS 金鑰的範圍 <code>kms:ResourceAliases condition</code> 。請考慮使用特定別名名稱，以及條件索引鍵的適當集合運算子。如果在別名名稱中使用萬用字元，請確保它們將範圍限制為一組有限的 KMS 金鑰。	如果您使用 條件來限定 KMS 金鑰的許可範圍，而不是使用 來縮小 KMS 金鑰的別名範圍 <code>kms:ResourceAliases</code> ，則會產生此調查結果。或者，如果 <code>kms:ResourceAliases</code> 條件金鑰的值也包含 AMS 擁有的 KMS 金鑰別名。若要解決此問題，請將 條件更新為僅縮小 KMS 金鑰別名的許可範圍，或排除 AMS 擁有 KMS 金鑰的別名。如需 AMS 擁有的金鑰別名清單，請參閱 AMS 自動化 IAM 佈建許可界限檢查。

問題清單	描述
角色必須連接 <code>customer_deny_policy</code> 。在受管政策 ARN 清單中包含政策 ARNs。	如果您建立的角色未連接 <code>customer_deny_policy</code> ，則會產生此調查結果。若要解決此問題，請在受管政策 ARNs 清單中包含 <code>customer_deny_policy</code> 。
AWS 受管政策過於寬鬆，或授予受 AMS 界限政策限制的許可。	如果角色的 <code>ManagedPolicyArns</code> 值包含任何可提供相關服務完整或管理員層級存取權的 AMS 受管政策，就會產生此調查結果。若要解決此問題，請檢閱 AWS 受管政策的使用，並使用提供縮小範圍許可的政策，或定義遵循最低權限原則的自有政策。
客戶受管政策位於受限的 AMS 命名空間中。	如果命名空間中名稱字首為 <code>aws_iam_</code> 的任何客戶受管政策連接到角色，則會產生此調查結果。若要解決此問題，請從角色的 <code>ManagedPolicyArns</code> 清單中移除政策。
<code>customer_deny_policy</code> 無法從角色分離。在受管政策 ARN 清單中包含政策 ARNs。	如果在更新期間從角色分離 <code>customer_deny_policy</code> ，則會產生此調查結果。若要解決此問題，請將 <code>customer_deny_policy</code> 新增至角色的 <code>ManagedPolicyArns</code> 欄位，然後再試一次。
客戶受管政策是在 AMS 變更管理服務之外佈建，或未經事先驗證。	如果一個或多個現有的客戶受管政策 ARNs 連接到角色，且政策不是透過 AMS 變更管理服務（透過 RFC）佈建，則會產生此調查結果。例如，開發人員模式或直接變更模式可讓客戶在沒有 RFC 的情況下佈建 IAM 政策。若要解決此問題，請從角色的 <code>ManagedPolicyArns</code> 清單中移除客戶受管政策 ARNs。
提供的受管政策 ARNs 計數超過每個角色配額連接的政策。	如果連接到角色的受管政策總數超過每個角色配額的政策，就會產生此調查結果。如需 IAM 配額的詳細資訊，請參閱 IAM 和 AWS STS 配額、名稱要求和字元限制 。使用此資訊來減少您連接到角色的政策數量。

問題清單	描述
信任政策大小 ({trust_policy}) 超過擔任角色政策大小的 {size} 配額。	如果擔任角色政策文件的大小超過政策大小配額，就會產生此調查結果。如需 IAM 配額的詳細資訊，請參閱 IAM 和 AWS STS 配額、名稱要求和字元限制 。
陳述式包含 Amazon S3 的所有變動動作。考慮僅將這些許可範圍限定為必要的動作。如果使用萬用字元，請確保它們限制一組可變動動作。	如果指定的政策授予所有 Amazon Simple Storage Service 變動許可，無論一或多個資源為何，都會產生此調查結果。若要解決此問題，請僅針對儲存貯體包含必要的 Amazon S3 變動動作。
陳述式包含 Amazon S3 中任何儲存貯體不允許的特權動作。考慮新增拒絕這些動作的陳述式。	如果政策授予任何儲存貯體的特權動作，就會產生此調查結果。如需特殊權限動作的清單，請參閱 AMS 自動化 IAM 佈建許可界限檢查 在政策中解析此調查結果、移除或拒絕這些動作。
陳述式包含不在 Amazon S3 中儲存貯體範圍內的特權動作。請考慮包含您的儲存貯體，或使用 AMS 命名空間字首排除儲存貯體。如果使用萬用字元，請確定它們符合您命名空間中的儲存貯體。	如果政策僅授予 Amazon S3 動作，且該動作範圍不限於您的儲存貯體，則會產生此調查結果。如果指定儲存貯體資源時使用萬用字元，通常會發生這種情況。若要解決此問題，請指定您擁有的儲存貯體名稱或 ARNs，或排除具有 AMS 命名空間字首的儲存貯體。
陳述式包含不在 Amazon S3 中儲存貯體範圍內的特權動作。考慮避免使用範圍限制帳戶中所有儲存貯體的萬用字元 (*)。	如果政策授予 Amazon S3 動作，且該動作範圍不限於您的儲存貯體，則會產生此調查結果。如果指定儲存貯體資源時使用萬用字元，通常會發生這種情況。若要解決此問題，請指定您擁有的儲存貯體名稱或 ARNs，或排除具有 AMS 命名空間字首的儲存貯體。

問題清單	描述
陳述式包含的資源萬用字元範圍適用於所有 Amazon S3 儲存貯體，包括不存在的儲存貯體和您未擁有的儲存貯體。考慮使用條件和 <code>s3:ResourceAccount</code> 條件索引鍵來限定許可範圍。	如果政策將許可授予使用萬用字元指定的儲存貯體，則會產生此調查結果。使用萬用字元通常會導致範圍內的不存在或非擁有者儲存貯體。若要解決此問題，請使用條件和 <code>aws:ResourceAccount</code> 條件索引鍵，將許可範圍限定為目前帳戶中的儲存貯體。如需詳細資訊，請參閱限制存取特定 AWS 帳戶擁有的 Amazon S3 儲存貯體。
陳述式包含 <code>NotResource</code> 政策元素，範圍可能涵蓋大量儲存貯體，包括不存在的儲存貯體和您未擁有的儲存貯體。考慮使用條件和 <code>s3:ResourceAccount</code> 條件索引鍵來限定許可範圍。	如果政策使用 <code>NotResources</code> 政策元素來指定儲存貯體資源，就會產生此調查結果。元素的使用範圍 <code>NotResource</code> 可能很大，包括不存在或非擁有者儲存貯體。若要解決此問題，請使用條件和 <code>aws:ResourceAccount</code> 條件索引鍵，將許可範圍限定為目前帳戶中的儲存貯體。
陳述式包含儲存貯體 <i>Bucket_Name</i> 的 Amazon S3 動作，這些儲存貯體不存在、帳戶 <i>Account_ID</i> 不擁有，或名稱包含範圍可能涵蓋大量儲存貯體的萬用字元，包括不存在的儲存貯體和您未擁有的儲存貯體。考慮使用條件和 <code>s3:ResourceAccount</code> 條件索引鍵來限定許可範圍	如果政策將許可授予不存在、不屬於您擁有的儲存貯體，或儲存貯體名稱中有涵蓋大量儲存貯體的萬用字元，且存取範圍不限於目前帳戶，則會產生此調查結果。若要解決此問題，請使用條件和 <code>aws:ResourceAccount</code> 條件索引鍵，將許可範圍限定為目前帳戶中的儲存貯體。
陳述式包含儲存貯體 <i>Bucket_Name</i> 的 Amazon S3 動作，這些儲存貯體不存在、帳戶 <i>Account_ID</i> 未擁有，或名稱包含的萬用字元範圍可能涵蓋大量儲存貯體，包括不存在的儲存貯體和您未擁有的儲存貯體。在條件中使用 <code>s3:ResourceAccount</code> 或指定的資源帳戶不會限制存取。	如果政策將許可授予不存在、非您擁有的儲存貯體，或儲存貯體名稱中有涵蓋大量儲存貯體的萬用字元，且存取範圍僅限於特定帳戶，則會產生此調查結果。不過，<code>aws:ResourceAccount</code> 條件索引鍵中指定的帳戶不屬於您，並由 AMS 管理。若要解決此問題，請更新 <code>aws:ResourceAccount</code> 條件金鑰，並設定您擁有並由 AMS 管理的適當帳戶 ID。

問題清單	描述
陳述式包含不在 Amazon EC2 執行個體範圍內的特權動作。請考慮將動作範圍限定為特定執行個體 ARNs，或排除具有 AMS 命名空間字首中值之名稱標籤索引鍵的執行個體。如果使用萬用字元，請確保它們符合您擁有的命名空間。	如果政策針對 AMS 擁有的 Amazon EC2 執行個體授予特權動作，則會產生此調查結果。AMS 執行個體會使用 AMS 命名空間中值的名稱標籤索引鍵進行標記。若要解決此問題，請使用 StringNotLike 運算子指定您的資源或排除具有 aws:ResourceTag/Name 索引鍵的 AMS 執行個體，該索引鍵會排除 AMS 命名空間中的值
陳述式包含不在 AWS Systems Manager 參數存放區資源範圍內的特權動作。請考慮指定參數 ARNs，或使用 AMS 命名空間字首排除參數。如果使用萬用字元，請確保它們僅限定您的參數範圍。	如果政策將許可授予您未擁有的參數，則會產生此調查結果。這通常是在使用萬用字元時，或者具有 AMS 命名空間字首的參數會列在政策陳述式中的資源下。若要解決此問題，請指定命名空間內的參數，或使用拒絕陳述式排除 AMS 參數。
陳述式包含對資源的特權動作 AWS Systems Manager。考慮限定許可範圍，以僅針對您的資源讀取動作或動作。	如果政策針對 Systems Manager 資源授予參數存放區或唯讀動作以外的許可，則會產生此調查結果。若要解決此問題清單，請將許可降低為僅唯讀動作或參數存放區。
陳述式包含的權限動作範圍不在您所擁有 <i>Service_Name</i> 的 {message} 範圍內。考慮將這些許可限定為適當的特定資源類型，或排除 AMS 擁有的資源。如果使用萬用字元，請確保它們符合##。	如果政策允許未針對您的資源授予的特權動作，特別是針對具名資源，則會產生此調查結果。若要解決此問題清單，請檢閱您的資源清單，並查看它們是否僅範圍位於您的命名空間中的資源。或者，排除 AMS 命名空間中的資源。

問題清單	描述
陳述式包含 {<i>Service_Name</i>} 的標記動作，其範圍不限於名稱標籤索引鍵的特定值。請考慮使用命名空間中的值設定 <code>aws:RequestTag/Name</code> 條件索引鍵來定義這些動作的範圍，或使用 AMS 命名空間字首中的值來設定 <code>StringNotLike</code> 條件 <code>aws:RequestTag/Name</code> 索引鍵來限制這些動作。	如果政策授予指定服務的標記許可，且許可範圍不限於規格標籤索引鍵/值，則會產生此調查結果。若要縮小標籤動作中可使用的索引鍵或值的範圍，例如，在請求執行動作時，請使用 <code>aws:RequestTag/tag key</code> 條件。因此，若要解決此問題，請使用此條件索引鍵來限制名稱空間中的索引鍵或值。或者，使用 AMS 命名空間中的值拒絕 <code>Name</code> 標籤索引鍵 (<code>aws:RequestTag/Name</code>)。
驗證 IAM 角色信任政策時發生內部錯誤。	當 CT 自動化透過 IAM Access Analyzer 服務對 IAM 角色信任政策執行驗證時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證客戶受管政策時發生內部錯誤。	當 CT 自動化透過 IAM Access Analyzer 服務對客戶受管政策執行驗證時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
在 中找不到存取分析器 AWS ##。無法執行角色信任政策的存取預覽檢查。	在 中找不到 IAM Access Analyzer 資源時，會產生此調查結果 AWS 區域。請聯絡 AMS Operations，在 AWS 區域中疑難排解和建立 IAM Access Analyzer 資源。
角色 <i>Role_Name</i> 的無效信任政策	當提供的 IAM 角色包含無效的信任政策時，會產生此調查結果。若要解決此問題，請檢閱信任政策以確認其有效。
IAM Access Analyzer 遇到內部錯誤。無法建立角色 <i>Role_Name</i> 的存取預覽	當自動化透過 IAM Access Analyzer 建立角色的存取預覽時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。

問題清單	描述
無法為角色 <i>Role_Name</i> 的信任政策建立存取預覽	當自動化透過 IAM Access Analyzer 建立角色的存取預覽時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證列出的 SAML IdP 時發生內部錯誤。	當自動化在驗證角色信任政策中列出的所提供 SAML IdPs 時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證許可時發生內部錯誤 AWS Key Management Service。	當自動化在驗證所提供政策中的 AWS KMS 金鑰許可時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證列出的受管政策 ARNs 內部錯誤。	當自動化在驗證列出的受管政策 ARNs 時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證預設 <i>customer_deny_policy</i> 附件時發生內部錯誤。	當自動化在驗證 <i>customer_deny_policy</i> 是否連接到角色時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
驗證角色 <i>Role_Name</i> 的受管政策出現的內部錯誤	當自動化在驗證角色的受管政策 ARNs 時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。

問題清單	描述
針對客戶定義的界限政策驗證 <i>Policy_name</i> 時發生內部錯誤 AWSManagedServicesIAMProvisionCustomerBoundaryPolicy	當自動化在驗證包含自訂拒絕清單的政策時發生錯誤時，就會產生此調查結果。若要解決此問題，請重新提交 RFC。如果錯誤仍然存在，請聯絡 AMS Operations 對錯誤進行故障診斷。
帳戶中AWSManagedServicesIAMProvisionCustomerBoundaryPolicy 存在客戶定義的界限政策。不過，政策包含允許授予許可的陳述式。政策只能包含拒絕陳述式。	當包含自訂拒絕清單的政策包含授予許可的陳述式時，就會產生此調查結果。雖然自訂拒絕清單存在於您的帳戶中做為 IAM 受管政策，但無法用於許可管理。政策只能包含拒絕陳述式，指出您希望 AMS Automated IAM Provisioning 在 AMS Automated IAM Provisioning 建立的 IAM 政策中驗證和拒絕這些動作。
陳述式包含您的組織為 <i>Service_Name</i> 定義的特權動作。考慮使用拒絕陳述式排除這些動作。請參閱您帳戶中名為 的政策，以參考限制的動作清單。	當自動化偵測到您在自訂拒絕清單中定義的政策中的任何動作時，就會產生此調查結果。若要解決調查結果，請檢閱您的政策陳述式，並移除自訂拒絕清單中定義的任何動作，或新增拒絕這些動作的拒絕陳述式。
角色必須連接 <i>POLICY_ARN</i> 。在受管政策 ARN 清單中包含政策 ARNs。	如果您建立的角色未連接 <i>POLICY_ARN</i> ，就會產生此調查結果。若要解決此問題，請在角色的 ManagedPolicyArns 欄位中包含 <i>POLICY_ARN</i> ，然後再試一次。
<i>POLICY_ARN</i> 無法從角色分離。在受管政策 ARN 清單中包含政策 ARNs。	如果在更新期間將 <i>POLICY_ARN</i> 從角色分離，則會產生此調查結果。若要解決此問題，請將 <i>POLICY_ARN</i> 新增至角色的 ManagedPolicyArns 欄位，然後再試一次。

AMS 自動化 IAM 佈建許可界限檢查

AMS 許可界限檢查可協助您遵守 AMS 提供的預設許可界限政策。此政策是 AMS Automated IAM Provisioning 拒絕的動作清單。佈建包含這些限制動作的政策需要額外明確的風險接受。在此處下載政策：[finitv-policy.zip](#)。

使用客戶定義的許可界限政策檢查，自訂 AMS 許可界限政策預設值以外的拒絕動作。當您使用下列變更類型加入 AMS 自動 IAM 佈建時：管理 | 受管帳戶 | AMS 具有讀寫許可的自動 IAM 佈建 | [啟用（需要檢閱）](#) (ct-1706xvk6j9hf)，您可以包含自訂拒絕動作清單，以指定其他限制動作。

您可以使用變更類型更新拒絕動作清單：管理 | 受管帳戶 | 具有讀寫許可的自動化 IAM 佈建 | [更新自訂拒絕清單](#) (ct-2r9xvd3sdsic0)。您必須使用專用 IAM 角色 `AWSTechnicalAccountAdministrator` 來執行此變更類型。

Note

- 您必須為每個更新提供拒絕動作的完整清單。新清單會取代上一個清單。
- 拒絕動作清單只能包含要拒絕的動作。不支援允許動作。
- 拒絕動作清單位於帳戶內，做為名為 `AWSTechnicalAccountAdministrator` 的 IAM 受管政策 `AWSTechnicalAccountAdministratorCustomerBoundaryPolicy`。政策不得連接到任何角色。
- 用於表示 AMS Automated IAM Provisioning 中拒絕動作的許可界限一詞與 IAM 許可界限具有不同的內容意義。IAM 許可界限會設定政策在執行時間可授予 IAM 實體的最大許可。如需 IAM 許可界限的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [政策類型](#)。AMS Automated IAM Provisioning 中的許可界限可防止您佈建包含特定許可集的 IAM 政策，例如拒絕動作清單。

故障診斷 AMS 自動化 IAM 佈建代理和錯誤

使用 AMS 自動化 IAM 佈建時，您可能會遇到三種問題：

- RFC 錯誤：這些原因可能有多種；例如輸入不正確。如需詳細資訊，請參閱 [針對 AMS 中的 RFC 錯誤進行故障診斷](#)。
- SSM 錯誤：這些情況可能因各種原因而發生，例如格式不良。如需詳細資訊，請參閱 [疑難排解 Systems Manager 自動化](#)。
- 驗證檢查問題清單：當自動化 IAM 佈建執行的許多驗證檢查之一發現問題時，就會發生這種情況。如需驗證檢查的清單，以及要修正的建議動作，請參閱 [AMS 自動化 IAM 佈建的執行期檢查](#)。

使用 IAM 角色和設定檔在 AMS 中設定許可

AMS 使用 AWS Identity and Access Management (IAM) 來管理使用者、存取金鑰等安全登入資料，以及控制使用者和應用程式可存取之 AWS 資源的許可。AMS 提供預設 IAM 使用者角色和預設 Amazon EC2 執行個體描述檔（包括允許資源存取預設 IAM 使用者角色的陳述式）。

請求新的 IAM 使用者角色或執行個體描述檔

AMS 使用 IAM 角色透過聯合服務設定使用者許可，並將 IAM 執行個體描述檔設定為該 IAM 角色的容器。

您可以使用部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策（需要檢閱）變更類型 (ct-3dpd8mdd9jn1r) 請求自訂 IAM 角色，或使用管理 | 應用程式 | IAM 執行個體描述檔 | 建立管理 | 應用程式 | IAM 執行個體描述檔 | 建立（需要檢閱）變更類型 (ct-0ixp4ch2tiu04) 請求 IAM 執行個體描述檔。請參閱本節中每個的說明。

Note

AMS 具有 IAM 政策，`customer_deny_policy`可封鎖危險的命名空間和動作。此政策預設會連接到所有 AMS 客戶角色，對使用者來說很少是問題。您的 IAM 使用者和角色請求不包含此政策，但自動將包含在 IAM 角色的請求`customer_deny_policy`中，可協助 AMS 更快地部署新的 IAM 執行個體設定檔。您可以請求排除`customer_deny_policy`政策。不過，此請求會經過繁重的安全審查，而且可能會因為安全原因而遭到拒絕。

使用 IAM 角色政策陳述式限制許可

AMS 使用 IAM 角色，透過聯合服務設定使用者許可。

單一帳戶登陸區域 AMS：請參閱 [SALZ：預設 IAM 使用者角色](#)。

多帳戶登陸區域 AMS：請參閱 [MALZ：預設 IAM 使用者角色](#)。

IAM 角色是 IAM 實體，定義一組提出 AWS 服務請求的許可。IAM 角色不會與特定使用者或群組建立關聯。相反地，信任的實體會擔任角色，例如 IAM 使用者、應用程式 AWS 或服務，例如 Amazon EC2。如需詳細資訊，請參閱 [IAM 角色](#)。

您可以使用 AWS Security Token Service (STS) API 操作 [AssumeRole](#)，在 Policy 請求欄位下傳遞更嚴格的 IAM 政策，來縮小擔任 AMS IAM 使用者角色的使用者所需的政策範圍。

接下來會提供可用來限制 CT 存取的政策陳述式範例。

您可以使用您設定的 Active Directory (AD) 群組和 AWS Security Token Service (STS) API 操作 [AssumeRole](#)，為特定使用者或群組設定許可，包括限制對特定變更類型 (CTs) 存取。您可以使用下列政策陳述式，以各種方式限制 CT 存取。

預設 IAM 執行個體描述檔中的 AMS 變更類型陳述式，允許存取所有 AMS API 呼叫 (amscm 和 amsskms) 和所有變更類型：

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. 僅允許兩個指定 CTs 的存取和所有動作的陳述式，其中「動作」是 AMS API 操作 (amscm 或 amsskms)，而「資源」代表現有的變更類型 IDs 和版本編號：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. 僅允許對兩個指定 CT 存取 CreateRfc、UpdateRfc 和 SubmitRfc 的陳述式：CTs

3. 允許在所有可用的 CT 上存取 CreateRfc、UpdateRfc 和 SubmitRfc 的陳述式：CTs
4. 拒絕限制 CT 上所有動作存取並允許其他 CTs 的陳述式：

使用 Amazon EC2 IAM 執行個體描述檔限制許可

IAM 執行個體描述檔是 IAM 角色的容器，您可以在執行個體啟動時用來將角色資訊傳遞至 Amazon EC2 執行個體。

目前有一個 AWS Managed Services (AMS) 預設執行個體描述檔 `customer-mc-ec2-instance-profile` 授予許可給在執行個體上執行的應用程式，而不是登入執行個體的使用者。如果您想要授予執行個體對某個物件的存取權，您可能想要修改預設執行個體描述檔，或建立新的設定檔，也不要授予其他執行個體的存取權。您可以使用 [管理 | 應用程式 | IAM 執行個體描述檔 | 建立變更類型 \(ct-0ixp4ch2tiu04\)](#) 來請求新的 IAM 執行個體描述檔。提交 RFC 時，您可以建立自己的執行個體描述檔，並將其納入為 `InstanceProfileDescription`，也可以直接通知 AMS（使用相同的欄位）您想要的變更。由於這是手動 CT，AMS 必須核准變更，並將與您聯絡。

如果您不熟悉 Amazon IAM 政策，請參閱 [IAM 政策概觀](#) 以取得重要資訊。還有一個很好的部落格文章：[Demystifying Amazon EC2 Resource-Level Permissions](#)。請注意，AMS 目前不支援以資源為基礎的存取控制，但支援使用 IAM 角色政策的資源層級控制（如需差異的說明，請參閱 [AWS 使用 IAM 的服務](#)）。

單一帳戶登陸區域 AMS：

若要查看預設 AMS IAM 執行個體描述檔授予的許可表，請前往 [EC2 IAM 執行個體描述檔](#)。

AD FS 宣告規則和 SAML 設定

AWS Managed Services (AMS) 的 ActiveDirectory Federation Services (AD FS) 宣告規則和 SAML 設定 AWS Managed Services

如需如何安裝和設定 AD FS step-by-step 說明，請參閱 [使用 Windows Active Directory、ADFS 和 SAML 2.0 啟用與 AWS 的聯合](#)。

ADFS 宣告規則組態

如果您已有 ADFS 實作，請設定以下內容：

- 依賴方信任
- 宣告規則

依賴方信任和宣告規則步驟是從[使用 Windows Active Directory、AD FS 和 SAML 2.0 部落格啟用聯合到 AWS](#)

- 宣告規則：
 - Nameid：每個部落格文章的組態
 - RoleSessionName：如下所示設定
 - 宣告規則名稱：**RoleSessionName**
 - 屬性存放區：**Active Directory**
 - LDAP 屬性：**SAM-Account-Name**
 - 傳出宣告類型：**https://aws.amazon.com/SAML/Attributes/RoleSessionName**
 - 取得 AD 群組：每個[部落格文章](#)的組態
 - 角色宣告：如下所示設定

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam::$1:saml-provider/  
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web 主控台

您可以使用以下連結，將 **#ADFS-FQDN#** 取代為 ADFS 實作的 FQDN，來存取 AWS Web 主控台。

<https://#ADFS-FQDN#/adfs/ls/IdpInitiatedSignOn.aspx>

您的 IT 部門可以透過群組政策，將上述連結部署至使用者人口。

使用 SAML 存取 API 和 CLI

如何使用 SAML 設定 API 和 CLI 存取。

python 套件來源於以下部落格文章：

- NTLM：[如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取](#)
- 表單：[如何使用 SAML 2.0 實作聯合 API/CLI 存取的一般解決方案](#)

- PowerShell : [如何使用 Windows PowerShell 設定對 AWS 的聯合 API 存取](#)

指令碼組態

1. 使用記事本++，將預設區域變更為正確的區域
2. 使用記事本++，停用測試和開發環境的 SSL 驗證
3. 使用記事本++，設定 idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Windows 組態

以下說明適用於 python 套件。產生的登入資料有效期為 1 小時。

1. [下載並安裝 python \(2.7.11\)](#)
2. [下載並安裝 AWS CLI 工具](#)
3. 安裝 AMS CLI :
 - a. 下載雲端服務交付管理員 (CSDM) 提供的 AMS 可分發 zip 檔案並解壓縮。

有數個目錄和檔案可供使用。
 - b. 根據您的作業系統開啟 Managed Cloud Distributables -> CLI -> Windows 或 Managed Cloud Distributables -> CLI -> Linux / MacOS 目錄，以及：

對於 Windows，請執行適當的安裝程式（此方法僅適用於 Windows 32 或 64 位元系統）：

- 32 位元：ManagedCloudAPI_x86.msi
- 64 位元：ManagedCloudAPI_x64.msi

對於 Mac/Linux，請執行名為的檔案：MC_CLI.sh。您可以執行此命令來執行此操作：sh MC_CLI.sh。請注意，amscm 和 amsskms 目錄及其內容必須與 MC_CLI.sh 檔案位於相同的目錄中。

- c. 如果您的公司登入資料是透過與 AWS (AMS 預設組態) 聯合使用，您必須安裝登入資料管理工具，以存取您的聯合服務。例如，您可以使用此 AWS 安全部落格 [如何使用 SAML 2.0 和 AD FS 實作聯合 API 和 CLI 存取](#)，以協助設定憑證管理工具。

d. 安裝之後，請執行 `aws amscm help` 和 `aws amsskms help` 以查看命令和選項。

4. 下載必要的 SAML 指令碼

下載至 `c:\aws\scripts`

5. [下載 PIP](#)

下載至 `c:\aws\downloads`

6. 使用 PowerShell 安裝 PIP

`<pythondir>.\python.exe c:\aws\downloads\get-pip.py`

7. 使用 PowerShell 安裝 boto 模組

`<pythondir\scripts>pip 安裝 boto`

8. 使用 PowerShell 安裝請求模組

`<pythondir\scripts>pip 安裝請求`

9. 使用 PowerShell 安裝請求安全模組

`<pythondir\scripts>pip 安裝請求【安全性】`

10. 使用 PowerShell 安裝 beautifulsoup 模組

`<pythondir\scripts>pip 安裝 beautifulsoup4`

11. 使用 PowerShell，在使用者設定檔中建立名為 `.aws` 的資料夾 (`%userprofile%\aws`)

`mkdir .aws`

12. 使用 PowerShell，在 `.aws` 資料夾中建立登入資料檔案

新項目登入資料 - 類型檔案 `-force`

登入資料檔案不得有副檔名

檔案名稱必須全部小寫，且具有名稱登入資料

13. 使用記事本開啟登入資料檔案並貼上下列資料，指定正確的區域

```
[default]
output = json
region = us-east-1
aws_access_key_id =
```

```
aws_secret_access_key =
```

14. 使用 PowerShell、SAML 指令碼和登入

<pythondir>.\python.exe c : \aws\scripts\samlapi.py

使用者名稱：【USERNAME】@upn

選擇您要擔任的角色

Linux 組態

產生的登入資料有效期為 1 小時。

1. 使用 WinSCP 傳輸 SAML 指令碼
2. 使用 WinSCP 傳輸根 CA 憑證（忽略用於測試和開發）
3. 將 ROOT CA 新增至信任的根憑證（忽略用於測試和開發）

\$ openssl x509 -inform der -in 【certname】.cer -out certificate.pem（忽略用於測試和開發）

將 certificate.pem 的內容新增至 /etc/ssl/certs/ca-bundle.crt 檔案結尾（忽略用於測試開發）

4. 在 home/ec2-user 5 中建立 .aws 資料夾

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. 使用 WinSCP，將登入資料檔案傳輸至 .aws 資料夾
6. 安裝 boto 模組

\$ sudo pip 安裝 boto

7. 安裝請求模組

\$ sudo pip 安裝請求

8. 安裝 beautifulsoup 模組

\$ sudo pip 安裝 beautifulsoup4

9. 將指令碼複製到 home/ec2-user

設定必要的許可

執行指令碼：`https://samlapi.py`

限制使用網路 ACL

網路存取控制清單 (NACL) 是 VPC 的選用安全層，可做為防火牆來控制傳入和傳出一或多個子網路的流量。您可以使用與您的安全群組相似的規則來設定網路 ACL，以為您的 VPC 新增額外的安全 layer。如需安全群組和網路 ACLs 之間差異的詳細資訊，請參閱[安全群組和網路 ACLs 的比較](#)。

不過，在 AMS 受管多帳戶登陸區域中，為了讓 AMS 有效管理和監控基礎設施，NACLs 的使用僅限於下列範圍：

- 多帳戶登陸區域核心帳戶不支援 NACLs，例如管理帳戶、聯網、共享服務、記錄和安全性。
- 多帳戶登陸區域應用程式帳戶支援 NACLs，只要它們僅用作「拒絕」清單，並具有「允許全部」以允許 AMS 監控和管理操作。

在大規模的多帳戶環境中，您也可以利用集中式輸出防火牆等功能來控制 AMS 多帳戶登陸區域中的傳出流量和/或 AWS 傳輸閘道路由表，以隔離 VPCs 之間的網路流量。

Outpost 上的 AMS

[AWS Outposts](#) 是一種受管硬體解決方案，可將 AMS 受管登陸區域延伸至客戶資料中心。使用 AMS 支援 AWS Outposts，尋求 AMS 提供的雲端專業知識、節省成本和標準化平台的客戶不再受限於內部託管資源 AWS 區域。開啟 AMS 後 AWS Outposts，具有內部部署需求的客戶現在可以進行現代化 AWS，同時享受 AMS 提供的修補、備份、佈建、事件管理、業務持續性和成本最佳化服務。

在 AMS 多帳戶登陸區域或單一帳戶登陸區域帳戶中 AWS Outposts 啟用後，您可以遵循現有的 AMS 變更管理程序來佈建和管理 AWS 資源。您可以透過指定您的 AWS Outposts 特定子網路來管理 AMS 託管基礎設施。可以使用 AWS Outposts 自助佈建服務角色直接在 AWS Outposts 主控台中管理 AWS Outposts 生命週期。

如需角色的資訊，請參閱 [AWS Outposts](#)。

AWS Outposts 安裝和操作管理

AMS on AWS Outposts 程序的加入包含：

1. Outposts 規劃
2. 訂單驗證
3. Outpost 加入 AMS
4. 生命週期管理

AWS Outposts 規劃

在 AWS Outposts 規劃期間，您可以識別 AWS Outposts 使用案例的 AMS，並與主要利益相關者互動，包括您的 AMS 客戶團隊和 AWS Outposts 代表，以調整容量策略。

1. 一旦識別 AWS Outposts 在上需要 AMS 的使用案例，請讓您的 AMS 客戶團隊討論容量規劃。
2. 確定 AWS Outposts 容量需求後，您的 AMS 客戶團隊會與服務 AWS Outposts 團隊一起討論 AWS Outposts 加入計劃、角色和責任。在此期間，會將 AWS Outposts 單一聯絡點 (SPOC) 指派給您。AWS Outposts SPOC 可協助完成 AWS Outposts 調整大小需求。

AWS Outposts 訂單驗證

在訂單驗證期間，您可以建立 AWS Outposts 網站，並直接在 AWS Outposts 主控台或透過 AWS Outposts 帳戶代表訂購所需的容量。

一旦 AMS 客戶團隊與 AWS Outposts 團隊保持一致，您就可以使用變更類型 ID `ct-3qe6io8t6jtny` 請求 AWS Outposts 自行佈建的服務角色，以建立您的網站並 AWS Outposts 直接在 AWS Outposts 主控台中訂購。

或者，您也可以透過 AWS Outposts SPOC 建立 Outpost 站點和訂單。在網站和訂單驗證和 AWS Outposts 安裝期間，您的 AWS Outposts SPOC 仍會繼續提供狀態更新給您和 AMS 客戶團隊。

AWS Outposts 加入 AMS

在 AMS 受管 VPC 中啟用 AWS Outposts 裝置後，您可以請求建立監視器，以追蹤 Outposts 硬體的可用量、容量、例外狀況和網路連線能力。遵循接下來所述的監控部署步驟，您的 AWS Outposts 硬體會由 AMS 主動監控。

1. 安裝並啟用您的 AWS Outposts 後，您可以使用 Management | Other | Other | Create (`ct-1e1xtak34nx76`) 變更類型，向 RFC 提交下列範本，以請求 AWS Outposts 特定的監控。AMS 操作可確保在 AMS 內部工具中追蹤 AWS Outposts 子網路。
 - AWS Outposts ID
 - 子網 CIDR

- 建議的 AWS Outposts 警示：
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direct Connect ConnectionAlert
- 針對上述每個提醒，指定下列參數：
 - 統計資料（建議使用「平均」。其他選項包括總和、最大值、最小值、樣本計數和 p90）
 - 期間（建議使用「5 分鐘」。其他選項包括 10 和 30 秒、1、5 和 15 分鐘、1 和 6 小時，以及 1 天）
 - 閾值類型（建議使用「靜態」。「異常」也是選項。）
 - 條件（「每當呼叫計數大於」，「等於」、「小於」也是選項。）
 - 條件值（預設為「25%」。另一個正整數是允許的。）
 - 通知主題（自動指派 AMS 操作主題。不過，也可以新增任何其他或自訂主題。）

2. 監控和操作支援

- AMS 操作會監控 AWS Outposts 指標是否有網路連線中斷或元件故障。AMS 操作會針對 AWS Outposts 問題提供第一個回應服務，並視需要升級至 Premium 支援或 EC2 支援。
 - AMS 操作可用於解決與 AWS Outposts 單元相關的問題。
3. 當 EC2 執行個體狀態或系統狀態檢查失敗時，AMS 操作會遵循現有程序，讓執行個體重新上線。如果重新啟動失敗或 AWS Outposts 容量不足，則 AMS 操作團隊成員會直接通知您，以決定後續步驟。

AWS Outposts 生命週期管理

一旦 AWS Outposts 加入您的 AMS 帳戶，如果發生任何可用性、容量或網路例外狀況，您會收到通知。您可以透過主控台或 AWS Outposts SPOC AWS Outposts 直接 AWS Outposts 停用。

您可以使用 AWS Outposts 自助式佈建服務角色或開發人員模式，AWS Outposts 直接在 AWS Outposts 主控台中管理。您也可以 AWS Outposts 透過 CSDM 或 AWS Outposts 單一聯絡點 (SPOC) 提出請求。

上的高可用性 AWS Outposts 可以透過部署兩個或多個來實現 AWS Outposts。設定兩個或多個會為您的 Amazon Relational Database Service 執行個體 AWS Outposts 啟用多可用區域選項。

在 上佈建 AMS 受管資源 AWS Outposts

在 AMS 帳戶 AWS Outposts（單一帳戶登陸區域、多帳戶登陸區域和加速帳戶）中佈建託管於（例如，Amazon EC2、Amazon EMR、Amazon EKS、Amazon ECS、Amazon EBS 和 Amazon S3）AWS 的資源，會受到與其中資源相同的 AMS 支援層級 AWS 區域。您可以使用 AMS 變更管理、自助式佈建服務或開發人員模式來建立和修改 上建立的資源 AWS Outposts。

目前，所有執行個體類型 (M5/M5d、C5/C5d、R5/R5d、I3en, G4dn)、Amazon Elastic Block Store、Amazon Elastic Container Service、Amazon Elastic Kubernetes Service、Amazon EMR、Amazon Relational Database Service DBs、Application Load Balancer 和 App Mesh Envoy 代理都可直接使用 AWS Outposts。這些資源符合與現有區域中資源相同的 AMS 操作支援資格。

AMS 在 上的限制 AWS Outposts

- AWS Outposts託管資源的操作支援取決於一致的網路連線能力。AWS Outposts 網路連線中斷可防止 AMS 操作對中斷連線 AWS Outposts 單元上發生的任何事件或問題進行故障診斷。如需 AMS on AWS Outposts 服務層級意外，請參閱更新的[AWS 服務層級協議 \(SLAs\)](#)。
- Amazon Relational Database Service :
 - 根據預設，建立 RDS 變更類型 (ct-2z60dyvto9g6c) 會啟用異地同步備份，且需要資料庫子網路群組。資料庫子網路群組在兩個不同的可用區域 (AZ) 中需要兩個子網路。如果您只有一個 AWS Outposts，則建立資料庫子網路群組是一個問題，因為 AWS Outposts 只會指派給單一可用區域。若要規避此限制，請遵循下列指示：
 1. 使用管理 | 其他 | 其他 CT 透過 RFC 請求資料庫子網路群組，並在 上指定子網路 AWS Outposts。
 2. 建立自訂 CFN 範本以部署 RDS AWS Outposts，並指定在上一個步驟中建立的子網路群組。若要進一步了解如何執行此作業，請參閱[自訂資源](#)。
 3. 請求 AMS 透過 AMS CFN 擷取 CT (ct-36cn2avfrj9v) 部署包含目標 RDS 執行個體的 CFN 範本。
 4. 請注意，由於 RDS Service 的限制，的 RDS 目前 AWS Outposts 不提供指標和日誌。
 - 工作負載擷取 (WIGs)：只有在 WIGs 前 EC2 執行個體位於非AWS Outposts 子網路上時，Linux WIGs才能運作。原因是 Linux WIGs 預設會使用 m4.large 在第一個 EC2 執行個體子網路中建立 WIGs 節點。由於 AWS Outposts 沒有該執行個體類型，WIGs無法啟動其工作者節點。解決方法是在非AWS Outposts 子網路中建立初始 EC2 執行個體，然後在其中建立目標執行個體 AWS Outposts。此外，目前僅支援 Nitro 型 EC2 執行個體類型，包括 C5, C5d, M5, M5d, R5, R5d, G4 和 I3en AWS Outposts。

- Amazon Elastic Block Store (EBS)：建立 EBS 磁碟區 CT (ct-16xg8qguovg2w) 無法運作，因為磁碟區會在 中建立 AWS，而不是 AWS Outposts 因為我們不提供 AWS Outposts Amazon 資源編號 (ARN) 作為 CT 的輸入參數。
- 網路連線：網路連線是您團隊的責任 AWS Outposts。
- 由於 AWS Outposts 帳單性質和企業支援需求，非 AMS 帳戶中 AWS Outposts 啟用的布朗菲爾德和帳戶接管：無法轉移至 AMS。

AWS Outposts 合規的 AMS

AWS Outposts 合規證明的 AMS

AWS Outposts 控制平面已證明符合 HIPAA 資格、PCI 和 ISO 合規。不過，尚未證明 AWS Outposts 控制平面上的 AMS AWS Outposts。因此，我們鼓勵客戶追求環境的 AWS Outposts 合規認證 AMS。

為了控制 Outpost 單位的資源建立，建議客戶隔離開發人員對 Outpost 的存取權，以防止開發人員在標準 AMS 受管帳戶中存取過多。

需要 FedRAMP 合規的 AMS 受管工作負載

最重要的是，必須先評估 AMS 管理帳戶是否符合法規，因為控制平面資料會從 流出 AWS Outposts 至 AMS 管理帳戶。

如果需要 FedRAMP 認證，且 AMS 帳戶結構合規，建議您使用已具備必要認證的資料中心廠商，並擁有所有服務連結設備（或已加密輸出資料）。

最後，您可以與您的客戶團隊合作部署 SCP，將資料限制為 AWS Outposts，並防止在託管 Outpost 的帳戶中建立任何區域內資源，藉此實施額外的資料保護。

對 AMS 帳戶現有合規的影響

使用的帳戶 AWS Outposts 不需要重新測試合規性，只要沒有消耗受管制的資料，而且帳戶在邏輯上是分開的。只要跨帳戶身分驗證/授權和傳入/傳出資料流程在 VPCs 之間隔離，AMS 管理帳戶就可以管理非受管制和受管制的帳戶。因此，即使不合規的 Outpost 帳戶和現有的合規應用程式帳戶都在同一組織（包括共用服務、聯網、記錄、主要、安全 AMS 服務）中，合規應用程式帳戶仍會保留合規，因為資料在邏輯上是分開的。

AMS AWS Outposts FAQs

哪些使用案例符合 上的 AMS 支援資格 AWS Outposts ？

需要成熟雲端操作模型的企業 AWS Outposts 可以利用 上的 AMS，其工作負載需要低延遲（例如，工廠機器人管理和大型主機遷移）、邊緣運算（例如，遠端工作站和邊緣資料簡化）和大型資料傳輸負載。

這個功能有什麼用？

AMS 可監控 AWS Outposts 硬體，並首次回應任何 AWS Outposts 硬體問題。此外，下列支援 上託管的所有受管資源的功能 AWS Outposts：

- 記錄、監控、護欄和事件管理
- 持續性管理
- 安全與存取管理
- 修補管理
- 變更管理
- 自動化和自助式佈建管理
- 事件和問題管理
- 報告 (AMS on 一開始不支援 AWS Outposts 硬體的報告 AWS Outposts)
- 服務請求管理
- 開發人員模式
- 企業支援

如何使用此功能？

AWS Outposts 規劃：在 AWS Outposts 規劃期間，您已識別 AWS Outposts 使用案例的 AMS，並將與主要利益相關者互動，包括 AMS 客戶團隊和 AWS Outposts 代表，以協調容量策略。

訂單驗證：在訂單驗證期間，您可以建立 AWS Outposts 網站，並直接在 AWS Outposts 主控台或透過您的 AWS Outposts 帳戶代表訂購所需的容量。

AWS Outposts 加入 AMS：在您的 AMS 受管 VPC 中啟用 AWS Outposts 單位後，您可以使用 AMS 使用者指南 () 中的 範本提交變更請求 (RFC)，以請求您的 AWS Outposts 加入您的 AMS 帳戶 [AWS Outposts](#)。然後，AMS 操作會使用 RFC 上提供的輸入，為您的 Outpost 建立子網路和監控。

生命週期管理：AWS Outposts 加入 AMS 帳戶後，您會收到任何可用性、容量或網路例外狀況的通知。您可以透過 AWS Outposts 主控台或 AWS Outposts 單一聯絡點 (SPOC) 直接停用 AWS Outposts。

AMS 的限制是什麼 AWS Outposts？

資料駐留（例如，國家特定資料當地語系化法等）使用案例尚未經過 AMS 的驗證。AWS Outposts

AWS Outposts 由於 AWS Outposts 帳單性質和企業支援需求，非 AMS 帳戶中啟用的 無法轉換為 AMS。

AWS Outposts 控制平面已證明符合 HIPAA 資格、PCI 和 ISO 合規。不過，尚未證明 AWS Outposts 控制平面上的 AMS AWS Outposts。因此，我們鼓勵客戶追求環境的 AWS Outposts 合規認證 AMS。

我可以選擇退出此功能嗎？

在 AWS Outposts AMS 環境中佈建是選用的。一旦部署到您的 AMS 帳戶，AWS Outposts 即可隨時透過 AWS Outposts 主控台取消佈建，如果不再需要的話。

如何 AWS Outposts 向 AMS 收費？

AMS 調高 AWS Outposts 費用將套用至群組 B 層。

AMS 服務水準協議將如何變更以容納 AWS Outposts？

事件管理取決於 AWS Outposts 可用性。AWS Outposts 可用性取決於客戶網路可用性，這是客戶的責任。AWS Outposts 可用性也取決於 AWS Outposts 硬體運作時間，這取決於 AWS Outposts 服務水準協議。

另請參閱[AWS Outposts FAQs](#)。

在 AMS 中使用標籤

主題

- [AMS 基礎設施自動標記](#)
- [AMS 建議的標籤](#)
- [標記大量更新備註](#)

提供標籤可能很有價值。如需深入資訊，請參閱[標記您的 Amazon EC2 資源](#)。

建立執行個體的 RFCs，例如 Amazon S3 儲存貯體或 AWS Elastic Load Balancer (ELB)，通常提供結構描述，可讓您新增最多七個標籤（金鑰/值對）；您可以透過提交管理 | 進階堆疊元件 | Amazon S3 儲存 | 更新 CT，將更多標籤新增至 S3 儲存貯體。Amazon EC2、Amazon EFS、Amazon RDS 和多層 (HA 雙層和 HA 單層) 結構描述最多允許 50 個標籤。標籤會在結構描述的 ExecutionParameters 部分中指定。

使用 AMS 主控台時，您必須啟用其他組態檢視，才能新增標籤。

Tip

許多 CT 結構描述都有靠近結構描述頂端的 Description 和 Name 欄位。這些欄位用於命名堆疊或堆疊元件，而不會命名您要建立的資源。有些結構描述提供參數來命名您正在建立的資源，有些則不會。例如，建立 Amazon EC2 堆疊的 CT 結構描述不提供參數來命名 Amazon EC2 執行個體。若要這樣做，您必須建立索引鍵為 "Name" 的標籤，以及您想要名稱的值。如果您未建立此類標籤，Amazon EC2 執行個體會顯示在 Amazon EC2 主控台中，但沒有名稱屬性。

是否有標籤限制？是：

- 標籤會區分大小寫。
- 鍵長度上限為 128 個 Unicode 字元。
- 值長度上限為 256 個 Unicode 字元。
- 每一資源標籤數最多為 50。
- 保留的字首為 aws:。
- AWS 產生的標籤名稱和值會自動指派 aws: 字首，您無法指派此值。使用者定義的標籤名稱在成本配置報告中有字首 user:。
- 每個資源只能使用每個鍵一次。如果您嘗試在相同資源上使用相同的金鑰兩次，您的請求會遭到拒絕。
- 允許的字元包括 Unicode 字母、空格、數字和下列特殊字元：+ - = . _ : /

哪些 AWS 資源類型支援標籤？請參閱[現在使用每個 AWS 資源最多 50 個標籤來組織您的資源。](#)

AMS 基礎設施自動標記

AMS 可以使用 [部署 | 進階堆疊元件 | 標籤 | 建立 \(需要檢閱\) 變更類型 \(ct-0176f0n99vcps\)](#)，在多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) 帳戶中標記 AMS 建立的所有資源以進行管理。這可協助您識別 AMS 為管理目的而建立的資源。

AMS 可以根據命名標準自動識別 AMS 建立的資源，並檢查資源是否具有下列標籤索引鍵和值 - "AppName"、"AppId"、"AMSResource" 和 "EnvironmentType"。如果標籤索引鍵不存在或值為空，則 AMS 可以使用標籤值 "AMSIInfrastructure" 自動建立這些標籤索引鍵。

您可以根據組織的標記標準，在 AMS 建立的資源上自訂所需的標籤。當您向 AMS 提交請求時，可以包含自己的標籤索引鍵和標籤值。遵循這些 AWS 標籤命名標準：[標記最佳實務](#)

Note

對於 MALZ 帳戶，僅應用程式帳戶支援 AMS 基礎設施的自訂標記。核心帳戶目前不支援自訂標記。

如果您在 RFC 中提供的標籤索引鍵名稱已存在於資源上，則標籤值會替換為您在 RFC 中提供的新標籤值。

標籤鍵：值對的總長度不得超過 256 個字元。

使用 [部署 | 進階堆疊元件 | 標籤 | 建立 \(需要檢閱\) 變更類型 \(ct-0176f0n99vcps\)](#) 在 RFC 中包含以下資訊，以標記 AMS 建立的資源。

1. 多帳戶登陸區域或單一帳戶登陸區域帳戶的清單，其中您想要標記 AMS 建立的資源以進行管理。
2. 必要的 tag-key 名稱和 tag-value (如有需要)。根據預設，AMS 可以使用標籤鍵名稱標記為 "EnvironmentType"，並使用標籤值標記為 "AMSIInfrastructure"。如果您需要自訂標籤索引鍵名稱和標籤值，請遵循 AWS 標籤命名標準：[標記最佳實務](#)

AMS 基礎設施標記目前支援這些資源：

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
```



```

Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing

```

* "arn : aws : s3 : : awsms-a*-patch-data-*"、"arn : aws : s3 : : ams-a*-log-management-*"、"arn : aws : s3 : : cf-templates-*"、"arn : aws : s3 : : mc-a*"、"arn : aws : s3 : : : ams-a*-backup-reports-*"、"arn : aws : s3 : : : amsams-a*-patch-data-customer-reports-*"、"arn : aws : s : : amsams-a*-patch-data-raw-*"、"、"arn : s : s : : patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

AMS 建議的標籤

AMS 會在支援的資源上建議下列標籤。強烈建議使用星號 (*) 標籤。

Note

您可以使用標籤來排程修補。如需詳細資訊，請參閱 [AMS Advanced Patch Orchestrator：標籤型修補模型](#)。

AMS 預留字首

AMS 資源屬性必須符合特定模式；例如，IAM 執行個體設定檔名稱、BackupVault 名稱、標籤名稱等，不得以 AMS 預留字首開頭。這些預留字首為：

```

*/aws_reserved/*
ams- *
/ams/*
ams *
AMS *
Ams *
aws *
AWS *
AWS_ *

```

```
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

AMS 建議的標籤

標籤鍵	支援的值	備註
AppName*	不受限制。	識別將駐留在資源上或需要存取資源的應用程式。這有助於 AMS 與您之間的追蹤和通訊。
AppId*		
EnvironmentType *		將開發、測試和生產基礎設施區分為資源的環境。
OwnerTeamEmail *	分發清單電子郵件地址	識別負責資源之團隊的分發清單電子郵件地址。電子郵件不應是個人電子郵件

標籤鍵	支援的值	備註
		件；它必須是匿名電子郵件，例如分發清單。
ComplianceFramework	無限制	識別應套用至資源的控制項和政策。
CostCenter		識別與資源相關聯的成本中心或業務單位（通常用於成本分配和追蹤）。
Customer		供擁有來自多個客戶 (AMS 子客戶) 資源的 AMS 客戶使用。將受管環境中的資源分組到他們服務的特定客戶。識別特定資源或服務群組上的特定用戶端。
DataClassification		識別資源支援的特定資料機密性層級。識別應套用至資源的控制項和政策。
HoursOfOperation		識別應該啟動、停止、刪除或輪換資源的日期或時間。
OwnerTeam		識別負責資源的團隊。促進與負責資源的團隊進行溝通。

標籤鍵	支援的值	備註
Patch Group	您有兩種選擇： - 您可以使用 AMS Advanced Patch Orchestrator 中概述的資訊提交服務請求：標籤型修補模型，AMS 會在您指定的資源上建立，並使用您提供的資訊為您建立Patch Group標籤。 - 如果您已在資源上建立Patch Group標籤，則支援的值不受限制。	要在自動修補維護時段中包含哪些資源。
ProjectId	無限制	識別資源支援的專案。
SupportPriority	機密性、完整性或可用性的六個可能縮寫之一；縮寫的順序是優先順序。例如，I.C.A. 表示順序為完整性、機密性、可用性。其他可接受的值為 C.I.A.、C.A.I.、I.A.C.、A.C.I. 和 A.I.C.。	識別哪些類型的支援應該是優先順序：機密性、完整性或可用性。

標記大量更新備註

這些備註適用於[標籤 | 大量更新](#)和[標籤 | 大量更新（需要檢閱）](#)變更類型範例演練。

大量更新標籤的注意事項：

- 支援的 服務：
 - 對於[標籤 | 大量更新（需要檢閱）](#)：全部。

- 對於[標籤 | 大量更新](#)：
 - Auto Scaling
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Amazon S3 儲存貯體
- 若要產生逗號分隔值 (CSV) 檔案，請在 AWS 主控台中登入資源群組 > 標籤編輯器，尋找您要標記的資源，然後將它們匯出至 CSV 檔案。如需詳細資訊，請參閱將[結果匯出至 CSV](#)。

注意：建議使用 S3 預先簽章的 URL 來提供 CSV 物件位置。

- 必須有具有 服務、類型和識別符標頭的資料欄。這些資料欄是強制性的。
- 將資料欄識別符重新命名為 ID。
- 資料欄服務、類型和識別符 (變更為 ID) 的值由資源群組下的標籤編輯器提供。
- 如果標籤編輯器下沒有要標記的資源，請使用資料欄識別符 (變更為 ID) 的資源的 Amazon Resource Name (ARN)，並將服務和類型保留空白。
- 要新增或修改之標籤的資料欄標頭的格式必須為 Tag : **TagKey**。
- 要刪除之標籤的資料欄標頭的格式必須為 Untag : **TagKey**。
- 每一列都是要標記或取消標記的資源。
- 如果要將標籤新增至資源，請在適當的標籤 : **TagKey** 欄下指定標籤的值。
- 如果要從資源刪除標籤，請在適當的 Untag : **TagKey** 欄下指定 True。
- 如果標籤 : **TagKey** 或 Untag : **TagKey** 不適用於資源，請將破折號 (-) 新增至個別資料欄或保留空白。

注意：取消標籤覆寫標籤 - 這是因為與標籤不同，需要手動將取消標籤新增至 CSV 檔案，因此我們假設的目的是移除標籤，而不是修改標籤。

- 不符合條件的任何其他資料欄都會遭到忽略。

Important

標籤編輯器匯出會針對所有資源填入所有標籤的矩陣，缺少的標籤會填入「未標記」的值。重複使用此匯出 CSV 做為 RFC 的輸入，會導致建立先前遺失的所有標籤，常值為「未標記」。

Note

如需將標籤匯出至 CSV 檔案的資訊，請參閱[尋找資源以標記 -> 將結果匯出至 CSV](#)。

AWS Managed Services 資源排程器

使用 AWS Managed Services (AMS) Resource Scheduler 來排程自動啟動和停止您帳戶中的 AutoScaling 群組、Amazon EC2 執行個體和 RDS 執行個體。這有助於降低資源不應全年無休執行的基礎設施成本。解決方案建置在 [上的執行個體排程器 AWS](#) 之上，但包含 AMS 需求特有的其他功能和自訂。

Note

根據預設，AMS Resource Scheduler 不會與不屬於 AWS CloudFormation 堆疊的資源互動。資源必須是以「stack-」、「sc-」或「SC-」開頭的堆疊的一部分。若要排程不屬於 CloudFormation 堆疊的資源，您可以將 Resource Scheduler 堆疊參數更新 `ScheduleNonStackResources` 為 Yes。

AMS Resource Scheduler 使用期間和排程：

- 期間定義資源排程器執行的時間，例如開始時間、結束時間和當月天數。
- 排程包含您定義的期間，以及其他組態，例如 SSM 維護時段、時區、休眠設定等；並指定資源應在何時執行，並指定設定的期間規則。

您可以使用 AMS Resource Scheduler 的自動化變更類型 (CTs) 來設定這些期間和排程。

如需 AMS Resource Scheduler 可用設定的完整詳細資訊，請參閱 [解決方案元件](#) 中對應的 AWS 執行個體排程器文件。如需解決方案的架構檢視，請參閱 [Architecture overview.html](#) 中對應的 AWS 執行個體排程器文件。

部署 AMS 資源排程器

若要部署 AMS 資源排程器，請使用自動化變更類型 (CT)：部署 | AMS 資源排程器 | 解決方案 | 部署 (ct-0ywnhc8e5k9z5) 來引發 RFC，然後部署帳戶中的解決方案。執行 RFC 後，包含具有預設組態

之 AMS Resource Scheduler 資源的 CloudFormation 堆疊會自動佈建至您的帳戶。如需 Resource Scheduler 變更類型的詳細資訊，請參閱 [AMS Resource Scheduler](#)。

Note

若要了解您的帳戶中是否已部署 AMS Resource Scheduler，請檢查該帳戶的 AWS Lambda 主控台，並尋找 AMSResourceScheduler 函數。

在您的帳戶中佈建 AMS Resource Scheduler 之後，建議您檢閱預設組態，並視需要根據您的偏好設定自訂組態，例如標籤索引鍵、時區、排程服務等。如需建議自訂的詳細資訊，請參閱 [自訂 AMS 資源排程器](#)，下一步。

若要進行自訂組態，或僅確認資源排程器組態，

自訂 AMS 資源排程器

我們建議您使用更新 AMS Resource Scheduler 變更類型來自訂 AMS Resource Scheduler 的下列屬性，請參閱 [AMS Resource Scheduler](#)。

- 標籤名稱：Resource Scheduler 用來將執行個體排程與 資源建立關聯的標籤名稱。預設值為排程。
- 排程服務：以逗號分隔的清單，列出資源排程器可以管理的服務。預設值為 "ec2, rds, autoscaling"。有效值為 "ec2"、"rds" 和 "autoscaling"。
- 預設時區：指定資源排程器要使用的預設時區。預設值為 UTC。
- 使用 CMK：以逗號分隔的 Amazon KMS 客戶受管金鑰 (CMK) ARNs 清單，可將許可授予資源排程器。
- 使用 LicenseManager：可以授予許可給該資源排程器以逗號分隔的 AWS Licence Manager ARNs 清單。

Note

AMS 可能會隨時釋出功能和修正，讓 AMS Resource Scheduler 在您的帳戶中保持最新狀態。發生這種情況時，您對 AMS 資源排程器進行的任何自訂都會保留。

使用 AMS 資源排程器

若要在部署解決方案後設定 AMS Resource Scheduler，請使用自動化 Resource Scheduler CTs 來建立、刪除、更新和描述（取得詳細資訊）AMS Resource Scheduler 期間（資源排程器執行的時間）和排程（設定的期間和其他選項）。如需使用 AMS Resource Scheduler 變更類型的範例，請參閱 [AMS Resource Scheduler](#)。

若要選取要由 AMS Resource Scheduler 管理的資源，請在部署和排程建立之後，使用 AMS 標籤建立 CTs，以您在部署期間提供的標籤索引鍵標記 Auto Scaling 群組、Amazon RDS 堆疊和 Amazon EC2 資源，並將定義的排程作為標籤值。標記資源後，資源會根據您定義的資源排程器排程排程為啟動或停止。

使用 AMS Resource Scheduler 無需額外費用。不過，解決方案會使用數個 AWS 服務，而且您在使用這些資源時需要支付費用。如需詳細資訊，請參閱[架構概觀](#)。

若要選擇退出 AMS 資源排程器：

- 對於暫時選擇退出或停用：使用自動化管理 | AMS 資源排程器 | 狀態 | 停用變更類型 (ct-14v49adibs4db) 提交 RFC
- 對於永久移除：提交管理 | 其他 | 其他 | 更新（需要檢閱）(ct-0xdawir96cy7k) RFC 請求從資源排程器版本自動化系統移除

AMS 資源排程器成本估算器

為了追蹤成本節省，AMS Resource Scheduler 具有每小時計算排程器管理之 Amazon EC2 和 RDS 資源預估成本節省的元件。然後，此節省成本的資料會發佈為 CloudWatch 指標 (AMS/ResourceScheduler)，以協助您追蹤資料。成本節省估算器只會預估執行個體執行時數的節省。它不會考慮任何其他成本，例如與資源相關聯的資料傳輸成本。

使用 Resource Scheduler 啟用成本節省估算器。它會每小時執行一次，並從中擷取成本和用量資料 AWS Cost Explorer。從該資料中，它會計算每個執行個體類型的每小時平均成本，然後在未排定的情況下執行整天的預估成本。節省成本是預測成本與 Cost Explorer 在特定日期實際報告成本之間的差異。

例如，如果執行個體 A 使用 Resource Scheduler 設定為從上午 9 點到下午 5 點執行，即指定日期的 8 小時。Cost Explorer 會將成本報告為 \$1，用量報告為 8。因此，每小時的平均成本為 0.125 美元。如果未使用 Resource Scheduler 排程執行個體，則執行個體會在當天執行 24 小時。在這種情況下，成本會是 $24 \times 0.125 = \$3$ 。資源排程器可協助您節省 2 美元的成本。

為了節省成本估算器僅從 Cost Explorer 擷取由 Resource Scheduler 管理的資源的成本和用量，Resource Scheduler 用於目標資源的標籤索引鍵需要啟用為帳單儀表板中的成本分配標籤。如果帳戶屬於組織，則需要在組織的管理帳戶中啟用標籤金鑰。如需執行此操作的資訊，請參閱[啟用使用者定義的成本分配標籤](#)和[使用者定義的成本分配標籤](#)

在標籤金鑰啟用為成本分配標籤之後，AWS 帳單會開始追蹤資源排程器所管理資源的成本和用量，並在該資料可用之後，成本節省估算器會開始計算成本節省，並在 CloudWatch 中的 AMS/ResourceScheduler 指標命名空間下發佈資料。

成本估算器秘訣

成本節省估算器不接受折扣，例如預留執行個體、節省計劃等，並將其計算納入考量。估算器會從 Cost Explorer 取得使用成本，並計算資源每小時的平均成本。如需詳細資訊，請參閱[了解您的 AWS 成本資料集：備忘單](#)

為了節省成本估算器僅從 Cost Explorer 擷取由 Resource Scheduler 管理的資源的成本和用量，Resource Scheduler 用於目標資源的標籤索引鍵需要啟用為帳單儀表板中的成本分配標籤。如果帳戶屬於組織，則需要在組織的管理帳戶中啟用標籤金鑰。如需執行此作業的資訊，請參閱[使用者定義的成本分配標籤](#)。如果未啟用成本分配標籤，估算器就無法計算節省成本並發佈指標，即使已啟用也一樣。

AMS Resource Scheduler 最佳實務

排程 Amazon EC2 執行個體

- 執行個體關閉行為必須設定為 stop，而不是設定為 terminate。對於使用 AMS Amazon EC2 建立自動變更類型 (ct-14027q0sjyt1h) 建立的 stop 執行個體，這是預先設定為，並且可以透過將 InstanceInitiatedShutdownBehavior 屬性設定為，為使用 AWS CloudFormation 擷取建立的 Amazon EC2 執行個體設定 stop。如果執行個體已將關閉行為設為 terminate，則當 Resource Scheduler 停止執行個體時，執行個體將會結束，且排程器將無法備份執行個體。
- AMS Resource Scheduler 不會個別處理屬於 Auto Scaling 群組的 Amazon EC2 執行個體，即使它們已加上標籤。
- 如果目標執行個體根磁碟區使用 KMS 客戶主金鑰 (CMK) 加密，則需要將額外的 kms:CreateGrant 許可新增至您的 Resource Scheduler IAM 角色，排程器才能啟動此類執行個體。根據預設，此許可不會新增至角色，以改善安全性。如果您需要此許可，請使用 Management | AMS Resource Scheduler | Solution | Update change type 提交 RFC，並指定 KMS CMKs 的 ARNs 逗號分隔清單。

排程 Auto Scaling 群組

- AMS Resource Scheduler 會啟動或停止 Auto Scaling 群組的自動擴展，而不是群組中的個別執行個體。也就是說，排程器會還原 Auto Scaling 群組的大小（開始）或將大小設定為 0（停止）。
- 使用指定的標籤標記 AutoScaling 群組，而不是群組中的執行個體。
- 在停止期間，AMS Resource Scheduler 會存放 Auto Scaling 群組的最小、預期和最大容量值，並將最小和預期容量設定為 0。在啟動期間，排程器會還原停止期間的 Auto Scaling 群組大小。因此，Auto Scaling 群組執行個體必須使用適當的容量組態，以便執行個體的終止和重新啟動不會影響 Auto Scaling 群組中執行的任何應用程式。
- 如果在執行期間修改 Auto Scaling 群組（最小或最大容量），排程器會存放新的 Auto Scaling 群組大小，並在停止排程結束時還原群組時使用。

排程 Amazon RDS 執行個體

- 排程器可以在停止 RDS 執行個體之前擷取快照（不適用於 Aurora 資料庫叢集）。此功能預設為開啟，且建立 RDS 執行個體快照 AWS CloudFormation 範本參數設為 true。快照會保留到下次停止 Amazon RDS 執行個體並建立新的快照為止。

排程器可以啟動/停止屬於叢集或 Amazon RDS Aurora 資料庫或多可用區域 (Multi-AZ) 組態的 Amazon RDS 執行個體。不過，當排程器無法停止 Amazon RDS 執行個體時，請檢查 Amazon RDS 限制，尤其是多可用區域執行個體。若要排程 Aurora 叢集啟動或停止，請使用排程 Aurora 叢集範本參數（預設為 true）。Aurora 叢集（而非叢集內的個別執行個體）必須使用初始組態期間定義的標籤索引鍵和排程名稱做為標籤值來標記，以排程該叢集。

每個 Amazon RDS 執行個體都有每週維護時段，在此期間會套用任何系統變更。在維護時段期間，Amazon RDS 會自動啟動已停止超過七天的執行個體，以套用維護。請注意，維護事件完成後，Amazon RDS 不會停止執行個體。

排程器允許指定是否要將 Amazon RDS 執行個體的偏好維護時段新增為其排程的執行期間。如果沒有其他執行期間指定執行個體應執行，且維護事件已完成，解決方案將在維護時段開始時啟動執行個體，並在維護時段結束時停止執行個體。

如果維護事件未在維護時段結束時完成，執行個體將在維護事件完成後的排程間隔之前執行。

 Note

排程器不會驗證資源是否已啟動或停止。它會發出 API 呼叫並繼續。如果 API 呼叫失敗，它會記錄錯誤以進行調查。

AWS Systems Manager 在 AMS Advanced 中

AWS Systems Manager 文件 (SSM 文件) 定義 Systems Manager 對 AWS 資源執行的動作。Systems Manager 包含十幾個預先設定的文件，您可以在執行時間指定參數。文件使用 JavaScript 物件標記法 (JSON) 或 YAML，其中包括您指定的步驟和參數。

AWS Managed Services (AMS) 是 SSM 文件的受信任發佈者。AMS 擁有的 SSM 文件只會與加入的 AMS 帳戶共用，一律以預留字首 (AWSManagedServices-*) 開頭，並在 Systems Manager 主控台中顯示，如 所擁有 AWS。SSM 文件開發和發佈的 AMS 程序遵循 AWS 最佳實務，並在整個文件生命週期中需要多個對等審核。如需共用 SSM 文件 AWS 的最佳實務的詳細資訊，請參閱[共用 SSM 文件的最佳實務](#)。

可用的 AMS Advanced SSM 文件

AMS Advanced SSM 文件僅供 AMS Advanced 客戶使用，用於自動化操作工作流程以操作您的帳戶。

若要從 查看可用的 AMS Advanced SSM 文件 AWS Management Console：

1. 在[AWS Systems Manager 主控台](#)開啟 Systems Manager 主控台。
2. 選擇與我共用。
3. 在搜尋列中，依文件名稱字首篩選，然後等於，並將值設定為 AWSManagedServices-。

如需 AWS CLI 指示，請參閱[使用共用的 SSM 文件](#)。

AMS Advanced SSM 文件版本

SSM 文件支援版本控制。AMS Advanced SSM 文件無法從客戶的帳戶修改，也無法重新共用。它們由 AMS Advanced 集中管理和維護，以便操作帳戶。

版本編號會隨著特定 中的每個文件更新而遞增 AWS 區域。當新區域可用時，兩個區域中的相同文件內容可以有不同的版本編號；這是典型的，並不表示其行為會有所不同。如果您想要比較兩個 AMS Advanced SSM 文件，建議您將其雜湊與 CLI AWS 進行比較：

```
aws ssm describe-document \  
--name AWSManagedServices-DOCUMENTNAME \  
--output text --query "Document.Hash"
```

如果兩個 SSM 文件的雜湊相符，則它們是相同的。

AMS 中的 Systems Manager 定價

AMS Advanced SSM 文件存取沒有相關成本。執行期成本會根據 SSM 文件的類型、其步驟和執行期持續時間而有所不同。如需詳細資訊，請參閱 [AWS Systems Manager 定價](#)。

離線 AMS 帳戶

AMS 為單一帳戶登陸區域和多帳戶登陸區域帳戶提供離職協助。

AMS 不會在離職期間取消與您共用任何 AMIs，以避免對您的任何停用情況造成影響。如果您想要從您的帳戶中移除 AMS AMIs，您可以使用 `cancel-image-launch-permission` API 來隱藏特定 AMIs。例如，您可以使用以下指令碼來隱藏先前與您的帳戶共用的所有 AMS AMIs：

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --  
query 'Images[].ImageId' --output text) ;  
do  
aws ec2 cancel-image-launch-permission --image-id $ami ;  
done
```

您必須安裝 AWS CLI v2，指令碼才能在沒有錯誤的情況下執行。如需 AWS CLI 安裝步驟，請參閱[安裝或更新最新版本的 AWS CLI](#)。如需 `cancel-image-launch-permission` 命令的詳細資訊，請參閱 [cancel-image-launch-permission](#)。

Note

服務終止日期是 30 天必要終止通知期間結束後日曆月的最後一天。如果必要的終止通知期間結束在日曆月的第 20 天之後，則服務終止日期是下一個日曆月的最後一天。以下是終止日期的範例案例。

- 如果終止通知是在 4 月 12 日提供，則 30 天的通知會在 5 月 12 日結束。服務終止日期為 5 月 31 日。

- 如果在 4 月 29 日提供終止通知，則 30 天的通知將於 5 月 29 日結束。服務終止日期為 6 月 30 日。

主題

- [從 AMS 單一帳戶登陸區域帳戶離職](#)
- [從 AMS 多帳戶登陸區域帳戶離職](#)

從 AMS 單一帳戶登陸區域帳戶離職

AMS 會在 AMS 終止前 30 天內提供離職協助。

您必須請求離職協助至少 7 天，才能提供此類協助。離職協助有兩種形式：

- 控制交接：AMS 會將帳戶控制與所有 AMS 受管應用程式的存取憑證一起轉返給您，或
- 帳戶關閉的資源終止：AMS 會刪除 AMS 受管環境中的所有資料，並取消佈建帳戶中的任何作用中資源。提交離職請求時，客戶可以請求該 AMS：
 - 刪除或保留存放在 Amazon S3 儲存貯體上的資料物件（包括日誌）
 - 移除或保留 Amazon S3 儲存貯體
 - 移除或保留 AWS Backup 還原點

Important

任何其他特定請求（視合理性而定）都必須在初始化離職之前傳達給 AMS。

選用先決條件（如果需要）：

Note

在離職請求之前，客戶可以使用 AWS Snowball Edge 或與之 AWS 互動的任何其他媒體，請求 AMS 協助以現有格式傳輸您的資料。

除了資料備份之外，以下客戶資料也可以作為離職協助的一部分提供：

- 儲存在儲存服務中的資料，包括 日誌

- 客戶特定的變更類型結構描述
- 變更類型結構描述的 CloudFormation 範本

如果在 AMS 終止時未完成離職活動，我們會移交（帳戶）的控制項，讓您完成任何待定活動。

函式	已移除的項目	影響	所需的動作
監控、記錄、提醒	已移除 AMS 監控 MMS（受管監控系統）已取消訂閱 已移除資源交錯和警示管理員 基準 CloudWatch 警示會保留在現有資源上 GuardDuty 和 Macie：所有權會還原給您	AMS 不再能夠存取或檢視您的資源和環境。	您擁有已移除和已取消訂閱服務的意外情況。
備份管理	雖然 AWS Backup 服務仍可使用，但 AMS Backup 自動化會移除。除非請求刪除，否則會保留備份保存庫和資料。	AMS 不再監控備份任務或在事件期間執行還原動作。警示和提醒已停用。刪除 IAM 備份角色和 KMS 金鑰會使 AMS 備份無法操作。	必須重新設定 AMS Backup Plans。所有監控和修復擁有權都會傳回給您。
服務管理的 AMS 自動化	AMS 策劃的 AWS SSM 自動化 Runbook、Amazon Simple Notification Service (SNS) 和	您的帳戶沒有 AMS 存取權。所有自動化已停用。	需要時，需要重新建立所有自動化，包括 SSM、SNS 和 Lambda 函數。

函式	已移除的項目	影響	所需的動作
	AWS Lambda 函數不再可用。		
合規	AMS 對所有 GuardDuty 和 AWS Config 規則的可見性和監控已移除，但這些規則仍保留在帳戶中。	Amazon GuardDuty 和 規則的所有監控、報告和修復不再由 AMS 管理。AWS Config	監控和修復您要擔任的所有安全與合規工具。
執行個體上的代理程式	移除對 Resource Scheduler、Resource Tagger 或自動化執行個體組態的存取權，以在 EC2 執行個體中安裝所需的代理程式。	執行個體上的 CloudWatch 和 SSM 代理程式會保留在現有的組態中，但 AMS 不再協助這些組態。	您可以管理標記和執行個體上的 CloudWatch 和 SSM 代理程式組態。
修補程式和報告基礎設施	AMS 不再管理修補前和修補後活動，並移除對這些服務的存取和可見性。	AMS 不會再於修補之前建立執行個體的快照、不會再安裝和監控修補安裝，也不會再通知您結果。報告和「稽核」S3 儲存貯體會依您的請求保留在您的帳戶中。AMS 不再產生服務指標報告。	您可以保留過去建立的修補程式基準和快照。此外，修補程式維護時段的組態仍會保留，但 AMS 不再安裝或修復修補程式。所有基礎設施操作指標的報告現在都是您的責任。
程序管理	所有帳戶都會從針對事件提供的服務管理中離職，包括服務請求、問題和變更、管理。	AMS 先前透過事件和服務請求修復的所有服務中斷，以及環境的變更，以及根本原因調查，都會由 AMS 進行更長的管理。	您可以重新取得所有程序管理的完整所有權。

從 AMS 多帳戶登陸區域帳戶離職

有兩種 AWS 帳戶類型可以從 AMS 進階多帳戶登陸區域下架：

- 應用程式帳戶
- 核心帳戶

若要從 AMS 多帳戶登陸區域移出所有帳戶，您必須先移出所有應用程式帳戶，才能移出核心帳戶。

若要接管和繼續在離職的應用程式或核心帳戶中操作工作負載，請務必與您的 AMS 帳戶團隊一起檢閱本文件。本文件概述 AMS 在離職程序期間執行的變更。

要完成的任務，以便繼續操作離職帳戶

您從 AMS 多帳戶登陸區域移出之帳戶的持續操作需要下列任務：

- 開啟開發人員模式：若要取得更多帳戶的許可，請先開啟開發人員模式，再從 AMS 關閉應用程式帳戶。當您開啟開發人員模式時，您可以更輕鬆地進行必要的變更，以準備離職。請勿嘗試移除或修改 AMS 基礎設施資源。如果您刪除 AMS 基礎設施資源，則 AMS 可能無法成功脫離您的帳戶。如需如何啟用開發人員模式的詳細資訊，請參閱 [AMS 進階開發人員模式入門](#)。

如果您在開啟開發人員模式後無法完成準備離職的必要變更，請聯絡您的 AMS 客戶團隊以討論您的需求。

- 選擇 EC2 堆疊存取的替代方法：從 AMS 離職應用程式帳戶後，您無法使用 RFCs 存取堆疊資源。檢閱 [離職變更](#)，然後選擇替代存取方法，以保留堆疊的存取權。如需詳細資訊，請參閱 [存取替代方案](#)。

離線 AMS 應用程式帳戶

若要從多帳戶登陸區域環境移出應用程式帳戶，請為每個帳戶完成以下步驟：

1. 確認帳戶中沒有開啟 RFCs。如需詳細資訊，請參閱 [建立、複製、更新、尋找和取消 RFCs](#)。
2. 確認您可以存取帳戶的主要或根使用者電子郵件地址。
3. 從應用程式帳戶提交 RFC 與 [應用程式帳戶 | 確認離職](#) (ct-2wlfo2jxj2rkj) 變更類型。在 RFC 中，指定要離職的應用程式帳戶。
4. 從管理帳戶，使用 [管理帳戶 | 離線應用程式帳戶](#) (ct-0vdiy51oyrhbm) 變更類型提交 RFC。在 RFC 中，指定要離職的應用程式帳戶。此外，指出您是否要刪除或保留與登陸區域的傳輸閘道連接。

5. 若要確保 AMS 帳單已停止，請通知 CSDM 您離職帳戶。

應用程式帳戶離職後會發生下列情況：

- 所有元件都會與 AMS 服務取消關聯，但您建立的資源會保留在帳戶中。您可以選擇保留或關閉 AMS 離職帳戶。
- 應用程式帳戶離職後，核心帳戶和其他剩餘的應用程式帳戶可正常運作。
- AMS 帳單會停止，但在您關閉帳戶之前，不會停止 AWS 帳單。如需詳細資訊，請參閱[關閉帳戶前的須知](#)。
- 如果帳戶已關閉，則該帳戶在處於 suspended 狀態的組織中可見 90 天。在 90 天後，已關閉的帳戶會永久移除，而且不會再出現在您的組織中。
- 帳戶關閉後，您仍然可以登入並提交支援案例或聯絡人 支援 90 天。
- 90 天後，任何保留在帳戶中的內容都會永久刪除，剩餘的 AWS 服務也會終止。

應用程式帳戶離職常見問答集

問：是否可以使用聯合 IAM 角色繼續存取我從 AMS 多帳戶登陸區域離職的應用程式帳戶？

是。AMS 建立的[預設 AWS Identity and Access Management \(IAM\) 角色](#)在 AMS 離職後仍可在帳戶中使用。不過，這些角色和政策旨在與 AMS 存取管理搭配使用。若要為使用者提供必要的存取權，您可能需要部署自己的 IAM 資源。

問：如何完整存取我從 AMS 多帳戶登陸區域離職的應用程式帳戶？

離職應用程式帳戶會移至 AWS Organizations 帳戶結構中的已棄用組織單位 (OU)。此移動會取消先前封鎖根使用者存取的 SCP 存取限制。如需如何重設根使用者憑證的資訊，請參閱[重設遺失或忘記的根使用者密碼](#)。

問：應用程式帳戶離職期間會進行哪些變更？

如需 AMS 在服務離線帳戶時所採取動作的資訊，請參閱 [離職變更](#)。

問：我可以在沒有將其從傳輸閘道分離的情況下讓應用程式帳戶離職嗎？

是。使用 [管理帳戶 | 離線應用程式帳戶](#) (ct-0vdiy51oyrhbm) 變更類型來提交 RFC，並將 DeleteTransitGatewayAttachment 參數指定為 False。

問：退出應用程式帳戶需要多長時間？

當您使用 [管理帳戶 | 離線應用程式帳戶](#) (ct-0vdiy51oyrhbm) 變更類型時，RFCs 會在 1 小時內完成。

問：我是否必須關閉離職帳戶？

否。不需要在 AMS 離職後關閉帳戶。在離職程序期間，AMS 會移除 AWS 帳戶的存取和管理，但您的帳戶和帳戶中的資源仍會保留。請務必注意，在 AMS 離職後，您完全負責管理和維護 AWS 您的帳戶和資源。在離職程序完成後，AMS 不會對您的帳戶中可能發生的任何問題、事件或服務中斷負責。如需詳細資訊，請參閱[如何關閉 AWS 帳戶？](#)。

問：如果我提交帳戶關閉請求，是否立即刪除所有現有的資源？

否。帳戶關閉不會終止您的資源。帳戶中的資源會在關閉請求後 90 天自動終止。AMS 帳單會停止，但在您關閉帳戶之前，AWS 資源帳單不會停止。如需詳細資訊，請參閱[關閉帳戶前的須知](#)。

問：我可以排程應用程式帳戶的離職嗎？

是。您可以排程在特定時間執行 RFCs。不過，[應用程式帳戶 | 確認離職](#) RFC 必須先完成，才能排程[管理帳戶 | 離職應用程式帳戶](#) RFC。如需詳細資訊，請參閱[RFC 排程](#)。

應用程式帳戶離職 RACI

- R：責任方。負責完成所列任務的一方。
- 答：當責方。核准已完成任務的一方。
- C：諮詢方。尋求意見的一方，通常作為主題專家，並與之進行雙邊溝通。
- I：知情方。通知進度的一方，通常只在完成任務或交付項目時。

活動	客戶	AWS Managed Services (AMS)
先決條件		
驗證將離職之每個 AWS 帳戶 ID 的根電子郵件地址存取權	R	C
檢閱有關建議客戶動作的 AMS 文件，並為 AMS 離職準備帳戶	R	C
如有需要，請提交 RFC 以啟用開發人員模式，為 AMS 離職準備帳戶	R	I
如有需要，請選擇 EC2 堆疊存取的替代方法。	R	I

活動	客戶	AWS Managed Services (AMS)
離職		
提交 RFCs 以確認和請求退出應用程式帳戶	R	I
來自應用程式帳戶的離線 AMS 元件	I	R
通知已離職帳戶的 AMS CSDM 以停止 AMS 帳單	R	I
離職後		
重設根使用者帳戶密碼，並驗證離職帳戶中的根存取權	R	C
關閉帳戶或遵循 AMS 離職文件中建議客戶動作的 AMS 指引，以繼續操作帳戶	R	C

Offboard Core 帳戶

若要移出多帳戶登陸區域核心帳戶，請完成下列步驟：

1. 確認登陸區域中的所有應用程式帳戶已從 AMS 離職。
2. 確認您帳戶中沒有開啟 RFCs。如需詳細資訊，請參閱[建立、複製、更新、尋找和取消 RFCs](#)。
3. 確認您可以存取所有 Core 帳戶的主要或根使用者電子郵件地址。如需詳細資訊，請參閱[多帳戶登陸區域帳戶](#)。
4. 確認您可以存取管理帳戶的主要或根使用者電話號碼。使用 AWSManagedServicesBillingRole IAM 角色更新電話號碼。如需詳細資訊，請參閱[如何更新與帳戶相關聯的 AWS 電話號碼？](#)。
5. 登入您的 AMS 登陸區域管理帳戶並提交 AMS 服務請求。在服務請求中，指定 將整個登陸區域移出。

核心帳戶離職後會發生下列情況：

- 所有元件都會與 AMS 服務取消關聯，但某些 AWS 資源會保留在帳戶中。您可以選擇保留或關閉 AMS 離職核心帳戶。
- AMS 帳單會停止，但在您關閉帳戶之前，不會停止 AWS 帳單。如需詳細資訊，請參閱[關閉帳戶前須知事項](#)。
- 如果帳戶已關閉，則該帳戶在處於 suspended 狀態的組織中可見 90 天。在 90 天後，已關閉的成員帳戶會永久移除，而且不會再出現在您的組織中。
- 帳戶關閉後，您仍然可以登入並提交支援案例或聯絡人 支援 90 天。
- 帳戶關閉 90 天後，帳戶內保留的任何內容都會永久刪除，剩餘的 AWS 服務也會終止。

核心帳戶離職常見問答集

問：我可以使用聯合 IAM 角色來繼續存取離職的核心帳戶嗎？

是。AMS 建立的[預設 AWS Identity and Access Management \(IAM\) 角色](#)在離職帳戶中仍然可用。不過，這些角色和政策旨在與 AMS 存取管理搭配使用。若要為使用者提供必要的存取權，您可能需要部署自己的 IAM 資源。

問：從 AMS 多帳戶登陸區域離職後，如何取得 Management、Shared Services、Networking 或其他非應用程式 [MALZ](#) 帳戶的完整存取權？

離職後，請遵循[重設遺失或忘記的根使用者密碼](#)中的指示，使用主要（根）使用者登入資料來存取管理帳戶以外的核心帳戶。與其他帳戶類型不同，管理帳戶會保留與根使用者相關聯的無法存取多重要素驗證 (MFA) 裝置，以防止使用。若要重新取得根存取權，您必須遵循[遺失的 MFA 裝置復原程序](#)。

問：核心帳戶離職期間會進行哪些變更？

如需 AMS 在服務離線帳戶時所採取動作的資訊，請參閱 [離職變更](#)。

問：核心帳戶離職需要多長時間才能完成？

核心帳戶離職程序通常需要 30 天才能完成。不過，為了確保所有必要步驟都正確完成，您必須在離職開始前至少 7 天啟動離職請求。為了方便轉換，請事先規劃並提交您的離職請求。

問：如何在 AMS 離職後管理共用元件？

AMS Managed Active Directory 和其他共用服務基礎設施元件專為 AMS 操作員存取而設計。您可能需要更新 Amazon Elastic Compute Cloud (Amazon EC2) 安全群組、AWS Organizations 服務控制政策 (SCP) 或進行其他變更，以保留這些元件的完整存取權。

問：我可以關閉離職的核心帳戶嗎？

根據預設，應用程式帳戶在 MALZ Core 帳戶上具有多個相依性，例如 AWS Organizations 成員資格、傳輸閘道網路連線，以及透過 AMS Managed Active Directory 的 DNS 解析。解決這些相依性之後，您可以解除委任並關閉離職的核心帳戶。如需詳細資訊，請參閱[多帳戶登陸區域帳戶](#)。

核心帳戶離職 RACI

- R：責任方。負責完成所列任務的一方。
- 答：當責方。核准已完成任務的一方。
- C：諮詢方。尋求意見的一方，通常是主題專家，並與之進行雙邊溝通。
- I：通知方。通知進度的一方，通常只在完成任務或可交付項目時。

活動	客戶	AWS Managed Services (AMS)
先決條件		
驗證將離職之每個 AWS 帳戶 ID 的根電子郵件地址存取權	R	C
驗證對 的存取，並更新管理帳戶的根使用者電話號碼	R	C
檢閱有關建議客戶動作的 AMS 文件，並為 AMS 離職準備帳戶	R	C
離職		
提交服務請求以請求離職登陸區域	R	I
來自核心帳戶的離線 AMS 元件	I	R
離職後		
重設根使用者帳戶密碼，並驗證離職帳戶中的根存取權	R	C
關閉帳戶或遵循 AMS 離職文件中建議客戶動作的 AMS 指引，以繼續操作帳戶	R	C

離職變更

下表說明 AMS 針對多帳戶登陸區域離職、潛在影響和建議動作所採取的動作。

元件	Account type (帳戶類型)	對離職採取的動作	潛在影響	建議的客戶動作
存取管理	應用程式帳戶	離職後，無法再提交just-in-time、有時間限制的存取的堆疊存取 RFCs，以透過 AMS 堡壘主機存取 EC2 堆疊 AMS 不再管理任何現有 EC2 資源堆疊上的存取相關元件 (PBIS Open 代理程式、網域聯結指令碼)	無法透過 RFS 使用 AMS 堡壘來存取 EC2 執行個體 從非 AMS 啟動的 EC2 執行個體，前提是 AMIs 未加入 Managed Active Directory 網域 如果未移除，現有資源堆疊中的 AMS 啟動指令碼可能會因為缺少 AMS 相依性而產生錯誤，並防止重新加入不同的網域	使用替代方法來存取 EC2 執行個體 (請參閱 存取替代方案) 從現有的 EC2 資源堆疊移除 AMS 啟動指令碼 (請參閱 停用 AMS EC2 啟動指令碼)
存取管理 (續)	核心帳戶	如果您從 PBIS Open 遷移到 PBIS Enterprise (AD Bridge)，則 AMS 不會在核心帳戶離職後續約授權	如果允許 PBIS Enterprise 授權過期，Active Directory 登入資料不適用於現有的 Linux EC2 執行個體堆疊	如果您遷移至 PBIS Enterprise (AD Bridge)，則決定是否要維持授權或取消委任 (請參閱 PBIS Open/Enterprise (AD Bridge))
記錄、監控、事件/事件管理	應用程式和核心帳戶	要部署的 AMS 元件 AMS 中基準監控的提醒 已移除 現有的已部署 Amazon CloudWatch 警示會保留，但不會再建立 AMS 事件	新建立的資源未套用 AMS 基準監控和警示	定義、擷取和分析操作指標，以檢視工作負載事件並採取適當的動作。

元件	Account type (帳戶類型)	對離職採取的動作	潛在影響	建議的客戶動作
		AWS Config 已從 AMS 和 MALZ Core 安全帳戶移除彙總授權 AWS Config 規則保持部署，Amazon GuardDuty 保持啟用，但不再建立 AMS 事件	基礎設施指標警示和安全性事件不會再產生 AMS 事件 AWS Config 不再彙總至中央帳戶	實作任何必要的提醒工作流程，以繼續對新資源套用必要的操作監控和警示，以及從 AWS Config 和 Amazon GuardDuty 接收安全提醒。
持續性管理（備份和還原）	應用程式帳戶	AMS 不再監控備份任務或執行備份和還原請求 AMS 預設備份保存庫、備份加密金鑰和備份角色仍會保留	可能不會注意到備份操作失敗	監控和檢閱備份計劃組態
修補管理	應用程式和核心帳戶	AMS 不再監控修補操作是否成功執行或執行手動修補 AMS 不再更新 AMS 基礎設施元件 AMS 提供的修補程式基準會保留 AMS 提供的 AWS Systems Manager 修補程式自動化 Runbook 未共用，不再可供使用	可能不會注意到修補操作失敗 依賴 AMS 提供的 Systems Manager Automation Runbook 的現有修補程式組態必須重新設定，才能繼續不間斷	視需要檢閱並重新設定修補組態

元件	Account type (帳戶類型)	對離職採取的動作	潛在影響	建議的客戶動作
網路管理	應用程式帳戶	如果指定，則會移除離職應用程式帳戶中的傳輸閘道連接	離職應用程式帳戶無法再使用傳輸閘道存取共用服務，例如 Managed Active Directory 或其他應用程式帳戶	將指定DeleteTransitGatewayAttachment 為 False以保留傳輸閘道連線
安全管理	應用程式帳戶	帳戶已從中央 Trend Micro DSM 主控台分離。此外，端點代理程式不會再透過 AMS 事件程序轉送警示 Trend Micro 代理程式會保持安裝狀態，但不再由 AMS 管理或更新 AMS 提供的部署 Trend Micro 代理程式的 AMI 自訂不再由 AMS 維護或更新	可能不會注意到 EC2 執行個體端點惡意軟體偵測 Trend Micro 代理程式不會部署在從非 AMS 提供的 AMIs 啟動的 EC2 執行個體上	考慮繼續或終止 Trend Micro 的選項（請參閱 Trend Micro Deep Security ）
安全管理（續）	核心帳戶	Trend Micro DSM 基礎設施保留在共用服務帳戶中，但不再由 AMS 維護或更新 Trend Micro DSM 不再透過 AMS 事件程序轉送提醒	EC2 執行個體端點惡意軟體偵測可能會被忽略 如果基礎設施未維護（定義更新、授權等），EC2 執行個體端點保護可能會受到影響	決定是否要繼續或終止 Trend Micro（請參閱（請參閱 Trend Micro Deep Security ）

元件	Account type (帳戶類型)	對離職採取的動作	潛在影響	建議的客戶動作
變更管理	應用程式和核心帳戶	AMS RFC 主控台和 API 已移除 包含帳戶層級存取限制的 AMS 自訂服務控制政策 (SCPs) 會在應用程式帳戶離職期間分離，並在核心帳戶離職期間刪除	您必須使用原生 AWS API 來建立新資源、變更現有資源或更新現有 AWS CloudFormation 堆疊 不再透過 AMS 提供的 SCPs 在帳戶層級強制執行存取限制	確定使用者角色提供足夠的存取權以使用 AWS 服務 建立 SCPs 以提供帳戶層級許可限制
服務管理的 AMS 作業系統映像和自動化	應用程式和核心帳戶	AMS 不再支援 AMS 提供的 EC2 AMIs 中包含的自訂和啟動指令碼 AMS 提供的 EC2 AMIs 仍可在您的離職帳戶中使用 AMS 提供的 Systems Manager Automation Runbook 未共用，不再可供使用	離職後，AMS 提供 AMIs，FAILURE 因為 AMS 元件缺少相依性 AWS CloudFormation 依賴 AMS 提供的 Systems Manager Automation Runbook 的操作程序可能會失敗	檢閱和更新依賴 AMS 提供的 AMIs 或 Systems Manager Automation Runbook 的任何建置或操作程序
共享服務基礎設施	核心帳戶	AMS 存取已移除，且 AMS 不再管理共用元件，包括 AMS Managed Active Directory AWS Transit Gateway，以及 AWS Organizations	共用基礎設施失去管理	重設 AMS Managed Active Directory 的管理員存取權，並擔任共用服務元件的管理
報告	應用程式和核心帳戶	AMS 不再收集彙總報告的帳戶或資源層級詳細資訊	無法深入了解營運和業務指標（備份和修補涵蓋範圍、變更管理和事件活動）	使用自己的解決方案取代跨帳戶所需的任何彙總資料報告

元件	Account type (帳戶類型)	對離職採取的動作	潛在影響	建議的客戶動作
AMS 客戶團隊和服務台	應用程式和核心帳戶	AMS 帳戶團隊 (CSDM、CA) 和 AMS 操作服務台不再支援離職帳戶	在 AMS 設計的多帳戶登陸區域架構和相關元件方面擁有專業知識，失去營運支援	確保有足夠的人員並熟悉帳戶結構和資源，以支援環境中的操作

存取替代方案

以下是在離開 AMS 帳戶後保留 EC2 堆疊存取權的替代方法：

- 使用 Session Manager 存取具有更高許可的 EC2 執行個體，而不需要堡壘或傳入網路存取。如需詳細資訊，請參閱[AWS Systems Manager Session Manager](#)。
- 使用新的網域登入資料將 EC2 執行個體重新加入不同的 Active Directory 網域。如果您使用 AWS Directory Service，請參閱[將 EC2 執行個體加入您的 AWS Managed Microsoft AD 目錄](#)。
- 使用您透過其他其中一種存取方法或透過 Run Command 建立的本機使用者帳戶。[AWS Systems Manager](#)

停用 AMS EC2 啟動指令碼

Linux 作業系統

使用分發的套件管理員解除安裝ams-modules套件。例如，對於 Amazon Linux 2，請使用 `yum remove ams-modules`。

Windows 作業系統

若要在 Windows 中停用 EC2 啟動指令碼，請完成下列步驟：

1. Windows Server 2008/2012/2012r2/2016/2019：

從任務排程器停用或移除 Managed Services Startup 排程任務。若要列出排程任務，請執行 `Get-ScheduledTask -TaskName '*Ec2*'` 命令。

Windows Server 2022：

移除 [EC2Launch v2 任務](#)。此任務Initialize-AMSBoot會在執行個體postReady上的 C : \ProgramData\Amazon\EC2Launch\config\agent-config.yml 階段中執行。以下是範例 的程式碼片段agent-config.yml :

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (選用) 移除下列檔案內容 :

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*
C:\Windows\System32\WindowsPowerShell\v1.0\Modules
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (AD Bridge)

若要判斷您使用的是 PBIS Open 或 PBIS Enterprise (AD Bridge) 版本，請在 Linux EC2 受管執行個體中執行下列命令：

```
yum info | grep pbis
```

以下是顯示 PBIS Enterprise (AD Bridge) 的範例輸出：

```
Name       : pbis-enterprise
From repo   : pbise
Name       : pbis-enterprise-devel
Repo       : pbise
Description : The pbis-enterprise-devel package includes the development
```

PBIS 開啟

PBIS Open 是 BeyondTrust 不再支援的已棄用產品。如需詳細資訊，請參閱 [BeyondTrust pbis-open 文件](#)。

AD Bridge (PBIS Enterprise)

您可以執行下列任一作業：

- 續約授權並繼續操作 AD Bridge。請聯絡 BeyondTrust 以討論授權和支援。
- 停止使用 AD Bridge。執行下列 Shell 命令，從 Linux 受管執行個體中移除 PBIS-Enterprise 套件。如需詳細資訊，請參閱 BeyondTrust 文件 [離開網域並解除安裝 AD Bridge Agent](#)。

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

離開 AMS 受管 Active Directory 網域而不移除 PBIS 代理程式

您可以選擇離開 AMS 受管 Active Directory，而不移除 PBIS 代理程式。根據您的作業系統，使用下列其中一個解決方案：

Linux operating systems

使用 AMS 受管 AD 的 PBIS 執行下列 shell 命令，以退出 Linux EC2 執行個體。如需詳細資訊，請參閱 [BeyondTrust pbis-open](#) 或 [BeyondTrust AD Bridge](#) 文件，具體取決於您使用的版本。

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

您可能會看到類似以下的錯誤訊息：

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]  
Cannot resolve network address for KDC in requested realm
```

如果發生此錯誤，請執行下列命令來刪除 AD 提供者登錄檔並重新啟動 lwsmd 服務：

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory\DomainJoin]'
```

使用您從上一個命令（例如 **A123EXAMPLE.AMAZONAWS.COM**）收到的目錄 ID 輸出來執行下列命令：

```
$ /opt/pbis/bin/regshell delete_tree \  
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\  
\DIRECTORYID]'  
  
$ /etc/pbis/redhat/lwsmd restart  
  
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:  
  
Test-ComputerSecureChannel -verbose  
  
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

Note

請務必停用或移除 Managed Services Startup 排程任務，如 中所述[停用 AMS EC2 啟動指令碼](#)。

Trend Micro Deep Security

使用下列其中一個選項來繼續或停止使用 Trend Micro Deep Security：

繼續使用

- (如果要卸任整個 MALZ) 核心帳戶卸任後，請將卸任的應用程式帳戶重新連線至現有的 Trend Micro Deep Security Manager (DSM)，並在共用服務帳戶中維護授權。如需詳細資訊，請參閱[新增 AWS 雲端帳戶](#)和[檢查您的授權資訊](#)。
 1. 登入共用服務帳戶並導覽至 Secrets Manager 主控台。
 2. 擷取存放在 /ams/eps/ 路徑中的 DSM 主控台管理員登入資料。
 3. 登入 DSM 主控台，網址為 <https://dsm.sentinel.int>。
 4. 選擇使用跨帳戶角色，然後輸入 **arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role**。將 ACCOUNTID 取代為離職的應用程式帳戶 ID。

5. 選擇下一步。
 6. 等待幾分鐘讓 DSM 處理帳戶探索，並顯示同步成功。
- 將已離職的應用程式帳戶重新連線至新的 Trend Micro DSM 安裝。如需詳細資訊，請參閱[啟用和保護代理](#)程式和[啟用代理](#)程式。
 - 將離職應用程式帳戶重新連線至 Trend Micro Cloud One。如需詳細資訊，請參閱[從 Deep Security 遷移至 Workload Security](#)，以及[從內部部署 DSM 遷移](#)。

停用用量

- 從離職的應用程式帳戶解除安裝 Trend Micro Deep Security Agents。如需詳細資訊，請參閱[解除安裝 Deep Security](#)。

變更管理模式

AWS Managed Services (AMS) 使用變更管理模式來保護 AMS Advanced 中的變更。變更管理模式可協助您維持環境的高操作標準，並控制風險並防止負面影響。AMS Advanced 有不同的模式，可提供不同層級的控制和風險。除了客戶受管模式之外，所有模式都由 AMS 管理。以下是可用的變更管理模式：

- RFC 模式（先前為標準 CM 模式）：提供「變更請求」(RFC) 系統和 AMS 自訂變更類型 (CTs)
- 直接變更模式：與 RFC 模式相同，加上使用 AWS APIs 和主控台來建立 AMS 受管資源
- AMS 上的 AWS Service Catalog：類似於直接變更模式，但不是使用 AMS 變更管理系統 (RFCs)，而是使用 AWS Service Catalog 來建立 AMS 接著管理的資源。
- 開發人員模式：與直接變更模式相同，只有您使用 AWS APIs 和主控台建立的資源不受 AMS 管理 - 您要負責其管理
- 自助服務佈建 (SSP) 模式：與開發人員模式相同，但無法存取 AMS 變更管理系統（無 RFCs）
- 客戶受管模式：AMS 為您提供多帳戶登陸區域登陸區域，但所有資源管理都是您的責任

AWS Managed Services (AMS) 變更管理系統使用變更管理 (CM) API，為多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) 帳戶提供建立和管理變更請求 (RFCs) 的操作。

變更請求 (RFC) 是您或 AMS 透過 AMS 界面建立的請求，用於對受管環境進行變更，並包含特定操作的變更類型 (CT) ID。

AMS 變更管理 (CM) API 提供建立和管理變更請求 (RFCs) 的操作。您可以建立、更新、提交、核准、拒絕和取消 RFCs。AMS 運算子可以建立、更新、提交、核准、拒絕、取消並將 RFCs 標記為關閉。

如需不在標籤或其他名稱中使用的 AMS 預留字首清單，請參閱[預留字首](#)。

如需每個變更類型的資訊，包括結構描述和範例，請參閱[AMS 變更類型參考](#)。

Note

所有變更管理 API 呼叫都會記錄在 AWS CloudTrail 中。如需詳細資訊，請參閱[存取您的日誌](#)。

模式概觀

使用此資訊來協助您選擇適當的 AWS Managed Services (AMS) 模式來託管您的應用程式，這取決於您實現業務成果所需的彈性和規範控管組合。

此資訊的目標對象為：

- 客戶團隊負責其登陸區域的策略和管理。此資訊將協助團隊規劃 AMS 受管登陸區域的基礎，以及他們想要提供給其內部和外部客戶的 AMS 模式。
- 負責將應用程式遷移至 AMS 的業務和應用程式擁有者。此資訊將有助於規劃應用程式遷移，並使用適當的 AMS 模式來遷移/託管其應用程式。請注意，相同的應用程式可以在其軟體開發生命週期 (SDLC) 生命週期的不同階段，以多個 AMS 模式託管。
- AMS 合作夥伴的任務是引導客戶了解建置和遷移至 AMS 的不同選項。

在設定 AMS 受管平台的基礎階段，以及當您從基礎轉換到雲端採用之旅的遷移階段時，這些資訊最有用，就在加入 AMS 完成後，而且您專注於應用程式控管和操作。

AMS 中模式和帳戶的類型

AWS Managed Services (AMS) 模式可以定義為在每種模式的特定控管架構下與 AMS 服務互動的方式。會記下登陸區域差異、多帳戶登陸區域或 MALZ，以及單一帳戶登陸區域或 SALZ。

 Note

如需應用程式部署和選擇正確 AMS 模式的詳細資訊，請參閱 [AMS 模式和應用程式或工作負載](#)。
如需不同模式的實際使用案例，請參閱 [AMS 模式的實際使用案例](#)

下表提供每個 AMS 服務模式的說明。

AMS 功能	RFC 模式 (先前為標準 CM 模式) /OOD*	直接變更模式	AWS Service Catalog	自助式佈建/開發人員模式	客戶受管
登陸區域組態	MALZ 和 SALZ	MALZ 和 SALZ		MALZ 和 SALZ	

AMS 功能	RFC 模式 (先前為標準 CM 模式) /OOD*	直接變更模式	AWS Service Catalog	自助式佈建/開發人員模式	客戶受管
變更管理	變更排程、檢閱手動變更和變更記錄	與 RFC 模式相同，適用於高風險變更，例如 IAM 或安全群組	無		
記錄、監控、護欄和事件管理	是 (支援的資源)			否	
持續性管理	是 (支援的資源)			不適用/否	否
安全管理	執行個體層級安全控制和帳戶層級控制			帳戶層級控制	AWS Org 層級控制
修補管理	是			不適用/否	否
事件和問題管理	AMS 支援資源的回應和解析 SLA			所產生資源的回應 SLA	否
報告	是			否	
服務請求管理	是			僅支援 請求	否

*隨需操作 (OOD) 提供客戶使用 RFC 模式透過專用資源管理其變更的服務。如需詳細資訊，請參閱 [隨需操作方案目錄](#)，並與您的雲端服務交付管理員 (CSDM) 交談。

Note

[AMS 中的自助式佈建模式](#) 和 [AMS 進階開發人員模式](#) 似乎都適合根植於原生 AWS Services 的複雜架構的應用程式。架構工作負載時，您會根據您的業務環境，在卓越營運和敏捷性之間做

出取捨。這是考慮為您的應用程式選取 SSP 模式或開發人員模式的好方法。選擇項目也可能根據應用程式的 SDLC 階段而變更。例如：當應用程式為生產就緒時，SSP 模式可能會因為在此模式下的 AMS 護欄更嚴格，而成為更適當的選項。護欄是以預防性控制的形式強制執行，例如應用程式 OU 層級的 IAM 更新和 SCPs RFC 型變更控制。這些業務決策可以讓您了解工程設計的優先順序。您可以最佳化，以增加應用程式擁有者在「生產前」階段的彈性，而犧牲控管和營運支援。

MALZ 架構和相關聯的 AMS 模式

AMS 多帳戶登陸區域 (MALZ) 可讓您選擇自動佈建預設組織單位 (OU) 下的應用程式帳戶（或資源帳戶）：客戶受管 OU、受管 OU 或開發 OU。在每個 OUs 下建立的應用程式帳戶中佈建的基礎設施，受限於這些基礎 OUs 提供的特定 AMS 模式。在同一個應用程式帳戶中尋找兩種或多種模式的混合是很常見的。例如：RFC 模式和 SSP 模式可以共存於託管由 API Gateway 和 Lambda 組成之管道架構的 AMS 受管帳戶中，用於觸發函數，以及用於擷取和協同運作的 EC2, S3 和 SQS。在此情況下，SSP 模式會套用至 Lambda 和 API Gateway。

圖 1 顯示如何在 AMS 中透過基礎 OUs 提供不同的模式。在 AMS 中請求新的應用程式帳戶時，您必須選取帳戶的 OU。

MALZ 架構和相關聯的 AMS 模式

AMS 利用以 AWS 最佳實務為基礎的基礎 OUs，做為使用服務控制政策 (SCPs) 邏輯管理帳戶的方法。這可做為對每個 AMS 模式強制執行控管架構的方法。套用至基礎 OUs 的任何控管和安全護欄（以 SCPs 的形式）也會自動套用至自訂/子 OUs。您可以為子 OUs 請求其他 SCPs。請務必了解應用程式帳戶與模式不同。模式會套用至帳戶內佈建的基礎設施，並定義 AMS 與客戶之間的操作責任。

圖 1：MALZ 架構和相關聯的 AMS 模式

Note

「限制性」表示您可以為這些 OUs 請求自訂政策，這些政策由 AMS case-by-case 核准，以確保它們不會干擾 AMS 提供卓越營運的能力。如需 AMS 護欄的詳細清單，請參閱《使用者指南》中的 [AMS 護欄](#)。

AMS 模式和應用程式或工作負載

選擇正確的模式時，請考慮應用程式的營運和管理需求，方法是請求新的應用程式帳戶或在現有的應用程式帳戶中託管應用程式。為每個應用程式或工作負載選擇適當的 AMS 模式取決於下列因素：

- 環境將提供的 SDLC 生命週期函數類型（例如，具有未修改變更的沙盒、具有一些頻繁變更的 UAT、具有最少變更且受到高度管制的生產）
- 所需的控管政策（透過 OU 層級 SCPs 強制執行）
- 操作模型（如果您想要承擔操作責任，或想要將其委外至 AMS）
- 所需的業務成果，例如在雲端中操作的時間，以及操作成本。

Note

如需每個 AMS 服務的模式類型說明，請參閱 [AMS 中的模式和帳戶的類型](#)。
如需不同模式的實際使用案例，請參閱 [AMS 模式的實際使用案例](#)

下表概述應用程式擁有者的關鍵考量事項，以協助決定最適合的 AMS 模式。應用程式擁有者應在應用程式遷移之前包含評估階段，以完全了解適用於其特定應用程式的模式。範例：對於以雲端原生服務或無伺服器架構為基礎的應用程式，最佳選項可能是開始在開發人員模式下建置和反覆運算，並使用 AMS Managed – SSP 模式將最終基礎設施部署為程式碼。在這種情況下，可能需要進行光線重構，以確保為自動化部署建立的任何 CloudFormation 範本都符合 AMS 制定的擷取準則。此外，任何 IAM 許可都需要 AMS Security 核准，以確保它們遵循最低權限模型。

選取來託管應用程式的 AMS 模式，可協助您建置所需的雲端操作模型。

Note

根據為託管應用程式選取的不同 AMS 模式，單一 AMS 受管登陸區域中可以存在多個雲端操作模型。

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管

操作準備

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
記錄、監控和事件管理	負責所有受管基礎設施的 AMS			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	客戶負責
持續性管理	AMS 負責執行客戶選取的備份計劃			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
執行個體層級存取管理	使用內部部署網域透過單向 AD 信任管理的 AMS。需要受管基礎設施才能加入 AMS 網域			不適用	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
安全管理和帳戶層級存取管理	所有受管帳戶的 AMS 責任			負責所有受管帳戶的 AMS	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
修補管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
變更管理	所有受管帳戶的 AMS 責任			負責自助服務佈建服務 (SSP) 的客戶	客戶負責在 AMS CM 系統外使用開發人員 IAM 角色佈建的資源	
佈建管理	AMS 中提供的佈建選項的規範和標準化	依照 AMS 規範標準直接使用 AWS Service Catalog 的 AWS 服務 API 的彈性	依照 AMS 規範標準直接使用 AWS 服務 API 的彈性	為 SSP 服務直接使用 AWS 服務 APIs 彈性	直接使用 AWS 服務 API 進行佈建的彈性	
事件管理和稽核	所有受管帳戶的 AMS 回應				客戶負責在 AMS 變更管理系統外使用開發人員 IAM 角色佈建的資源	

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
GuardRails 和共用基礎設施（網路）和安全架構	使用 AMS 核心帳戶的規範和標準化					彈性和自訂運用 AMS 核心帳戶
應用程式整備						
應用程式重構	需要光線重構				需要光線重構（如果使用 AMS 標準 CM 佈建）	不需要重構
支援 AWS 服務	僅限於 AMS 支援的內容					不受限制
業務考量事項						
操作就緒時間	三到六個月			6 個月以上取決於客戶應用程式操作能力		6-18 個月取決於客戶基礎設施和應用程式操作能力
成本	\$\$\$\$			\$\$\$	\$\$	\$

決策問題	標準 CM 模式/OOD*	AWS Service Catalog	直接變更模式	自助式佈建	開發人員模式	客戶受管
應用程式範例	具有 3 層堆疊的 Web 伺服器，具有合規和法規要求的應用程式			使用 API Gateway 的 Web 伺服器，利用 ECS/EKS 的容器化應用程式	在使用 Lambda、Glue、Athena 等的 Data Lake 應用程式上反覆/最佳化	分散式帳戶/應用程式，例如沙盒、第三方受管應用程式

*隨需操作 (OOD) 提供客戶使用標準 CM 模式，透過專用資源管理其變更。如需詳細資訊，請參閱 [方案的隨需操作目錄](#)，並與您的雲端服務交付管理員 (CSDM) 交談。

 Note

SSP 模式和開發人員模式之間的價格比較假設已佈建相同的 AWS 服務。

比較 AMS 模式與業務和 IT 目標

如所示，如果您要為應用程式尋找高度受控和標準化的控管模型，則 AMS 受管的標準變更、AWS Service Catalog 或直接變更模式是最適合的。如果您需要專注於應用程式創新的自訂控管模型，而不需要操作準備，請選取客戶受管模式。使用客戶受管模式，當您負責建立人員、程序和工具以支援操作功能時，可能需要更長的時間來操作應用程式，例如事件管理、組態管理、佈建管理、安全管理、修補程式管理等。

AMS 模式的真實使用案例

檢查這些項目，以協助判斷如何使用 AMS 模式。

- 使用案例 1，透過時間敏感的資料中心退出來降低成本的必要業務：具有吸引人業務事件的企業，例如資料中心退出，有興趣在雲端上重新託管其內部部署應用程式。大多數現場部署庫存都由 Windows 和 Linux 伺服器組成，並混合作業系統版本。如此一來，客戶還希望利用遷移到雲端提供的成本節省，並改善其應用程式的技術和安全狀態。客戶想要快速移動，但尚未建置內部雲端操作專業知識。客戶必須找到重構的平衡，太多重構可能會對緊迫的時間軸造成風險。不過，透過一些重

構，例如更新作業系統版本和最佳化資料庫，應用程式可以實現更高水準的效能。在此範例中，客戶可以選擇 AMS 受管 RFC 模式來重新託管大部分的應用程式。AMS 提供基礎設施操作，同時引導客戶操作團隊在雲端中安全操作的最佳實務。

AMS 受管 AWS Service Catalog 和 AMS 受管直接變更模式可為客戶提供額外的靈活性，同時實現相同的業務成果和目標。此外，客戶可以使用 AMS Operations On Demand (OOD) 產品，讓專用 AMS 操作工程師優先執行變更請求 (RFCs)。

將未差異化的基礎設施操作任務（修補、備份、帳戶管理等）卸載至 AMS 時，客戶可以繼續專注於最佳化其應用程式，並在雲端操作上提升其內部團隊。AMS 會每月向客戶提供節省成本的報告，並針對資源最佳化提出建議。在此使用案例中，如果在 Windows 2003 和 2008 等舊版作業系統上託管 end-of-life 應用程式，而客戶決定不重構，則這些應用程式也可以遷移到 AMS，並託管在利用客戶受管模式的帳戶中。

- 使用案例 2，在安全的 AMS 界限內使用 Lambda、Glue、Athena 建置資料湖：企業希望設定 Data Lake，以滿足 AMS 中多個應用程式的報告需求。客戶想要使用 S3 儲存貯體來儲存資料集，而 AWS Athena 會針對每個報告的資料集進行查詢。S3 和 AWS Athena 將部署在不同的 AMS 受管帳戶中。使用 S3 的帳戶也有其他服務，例如 Glue、Lambda 和 Step Functions，以建置資料擷取管道。在這種情況下，Glue、Lambda、Athena 和 Step Functions 被視為自助式佈建 (SSP) 服務。客戶也在帳戶中部署 EC2 執行個體，做為臨機操作工具/指令碼伺服器。客戶從請求 AMS 在其 AMS 受管帳戶中啟用 SSP 服務開始。AMS 會為客戶可擔任的每個服務佈建 IAM 角色，一旦該角色加入到客戶的聯合解決方案。為了方便管理，客戶也可以將個別 IAM 角色的政策合併為一個自訂角色，減輕在 AWS 服務之間工作時切換角色的需求。在帳戶中啟用角色後，客戶就可以根據其需求設定服務。不過，客戶必須使用 AMS 變更管理系統來請求其他許可，視其使用案例而定。

例如，若要存取 Glue 爬蟲程式，Glue 需要額外的許可。還需要其他許可才能建立 Lambda 的事件來源。客戶將使用 AMS 更新 IAM 角色，以允許 Athena 跨帳戶存取查詢 S3 儲存貯體。還需要透過 Lambda 的 AMS 變更管理更新服務角色或服務連結角色，以呼叫 Step Functions 服務，以及透過 Glue 讀取和寫入所有 S3 儲存貯體。AMS 與客戶合作，確保遵循最低權限的存取模型，並且請求的 IAM 變更不會過度寬鬆，並使環境面臨不必要的風險。客戶的資料湖團隊會花費時間規劃客戶架構特定服務所需的所有 IAM 許可，並請求 AMS 啟用這些許可。這是因為所有 IAM 變更都會手動處理，並經過 AMS 安全團隊的審核。應用程式部署排程中應考量處理這些請求的時間。

由於 SSP 服務在帳戶中運作，客戶可以透過 AMS 事件管理和服務請求請求支援和報告問題。不過，AMS 不會主動監控 Lambda 的效能和並行指標，或 Glue 的工作指標。客戶有責任確保為 SSP 服務啟用適當的記錄和監控。帳戶中的 EC2 執行個體和 S3 儲存貯體完全由 AMS 管理。

- 使用案例 3，在 AMS 中快速且靈活地設定 CICD 部署管道：客戶希望設定以 Jenkins 為基礎的 CICD 管道，將程式碼管道部署到 AMS 中的所有應用程式帳戶。客戶可能會發現它最適合在 AMS

受管直接變更模式 (DCM) 或 AMS 受管開發人員模式下託管此 CICD 管道，因為它可靈活地在 EC2 上設定具有所需自訂組態的 Jenkins 伺服器，並具有所需的 IAM 許可來存取 CloudFormation 和託管成品儲存庫的 S3 儲存貯體。雖然這也可以在 AMS 受管 RFC 模式中完成，但客戶團隊需要為 IAM 角色建立多個手動 RFCs，以針對 AMS 手動檢閱的最低許可集進行反覆運算。DCM 可讓客戶在 AWS 上實現其營運目標，同時避免在使用 AMS 受管 RFCs 模式時為 IAM 角色建立多個手動 RFC 的需求，以針對 AMS 手動檢閱的最低寬鬆許可集進行反覆運算。這需要時間和客戶方面的教育，才能提升 AMS 程序和工具。使用開發人員模式，客戶可以從「開發人員角色」開始，使用原生 AWS APIs 佈建基礎設施。設定此管道最快速且最靈活的方法是使用 AMS Managed-Developer 模式。開發人員模式提供最快速且最簡單的方式，同時犧牲操作整合，而 DCM 的靈活性較低，但確實提供與 RFC 模式相同的操作支援層級。

- 使用案例 4，AMS 基礎中的自訂操作模型：客戶正在查看截止日期驅動的資料中心退出，且其其中一個企業應用程式完全由第三方 MSP 管理，包括應用程式操作和基礎設施操作。假設客戶沒有時間重新考慮此應用程式，因此可以由 AMS 操作，則客戶受管模式是適合的選項。客戶可以利用 AMS 受管登陸區域的自動化和快速設定。他們可以利用集中式帳戶管理，透過集中式聯網帳戶控制帳戶販賣和連線。它還透過 AMS Payer 帳戶合併所有客戶受管帳戶的費用，以簡化其帳單。客戶可以靈活地設定其自訂存取管理模型，其 MSP 與用於 AMS 受管帳戶的標準存取管理不同。如此一來，使用客戶受管模式，他們可以設定 AMS 受管環境，同時滿足清空內部部署環境的業務需求。在此情況下，如果客戶也有要遷移至雲端的 Windows 應用程式，並選擇將他們移至客戶受管帳戶，則客戶必須負責建立雲端操作模型。視客戶轉換傳統 IT 程序及訓練人員的能力而定，這可能會複雜、昂貴且耗時。客戶可以透過將此類工作負載「抬高和轉移」到 AMS 受管帳戶，並將基礎設施操作卸載到 AMS 來節省時間和成本。

Note

客戶有時可能會覺得需要在 RFC 或 SSP 模式的控管架構與開發人員模式之間移動應用程式帳戶。例如，客戶可以在 AMS 受管模式下託管應用程式，做為初始提升和轉移遷移的一部分，但加班想要重新寫入應用程式，以針對雲端原生 AWS 服務將其最佳化。他們可以將生產前帳戶的模式從 AMS 受管 RFC 變更為 AMS 受管開發人員模式，為他們提供佈建基礎設施的靈活性和敏捷性。不過，一旦使用「開發人員角色」進行基礎設施佈建變更，相同的基礎設施就無法移回 AMS 受管 RFC 模式。這是因為 AMS 無法保證在 AMS 變更管理系統之外佈建的基礎設施操作。客戶可能需要建立新的應用程式帳戶，以提供 AMS 受管 RFC 模式，然後透過 CloudFormation 範本或擷取至 AMS 受管帳戶的自訂 AMIs 重新部署「最佳化」基礎設施組態。這是部署生產就緒組態的乾淨方法。部署後，應用程式將受到規範的 AMS 控管和操作。這同樣適用於客戶受管模式和 AMS 受管模式之間的切換模式。

RFC 模式

RFC 模式是 AMS Advanced 操作計劃客戶的預設模式。其中包括變更管理系統，其中包含變更或 RFCs 的請求，以及變更類型的目錄，可用來請求對帳戶新增或變更所需的變更。此變更管理系統提供安全層級，以限制誰可以變更您的帳戶。

如需 AMS 進階變更類型的詳細資訊，請參閱[什麼是 AMS 變更類型？](#)。

如需加入 AMS Advanced 的詳細資訊，請參閱[AWS Managed Services 加入簡介](#)。

如需變更類型範例演練，請參閱 AMS 進階變更類型參考依分類[變更](#)類型一節中相關變更類型的「其他資訊」一節。

Note

RFC 模式先前稱為「變更管理模式」或「標準 CM 模式」。

主題

- [了解 RFCs](#)
- [什麼是變更類型？](#)
- [針對 AMS 中的 RFC 錯誤進行故障診斷](#)

了解 RFCs

變更請求或 RFCs 會以兩倍的方式運作。首先，RFC 本身需要參數。這些是 CreateRfc API 中的選項。其次，RFC 的動作需要參數（執行參數）。若要了解 CreateRfc 選項，請參閱 AMS API 參考的[CreateRfc](#) 一節。這些選項通常會出現在建立 RFC 頁面的其他組態區域中。

您可以使用 CreateRfc API、CLI 或使用 AMS `aws amscm create-rfc` 主控台建立 RFC 頁面來建立和提交 RFC。如需建立 RFC 的教學課程，請參閱[建立 RFC](#)。

主題

- [什麼是 RFCs？](#)
- [使用 AMS API/CLI 進行身分驗證](#)
- [了解 RFC 安全性審查](#)
- [了解 RFC 變更類型分類](#)

- [了解 RFC 動作和活動狀態](#)
- [了解 RFC 狀態碼](#)
- [了解 RFC 更新 CTs 和 CloudFormation 範本偏離偵測](#)
- [排程 RFCs](#)
- [核准或拒絕 RFCs](#)
- [請求 RFC 限制執行期間](#)
- [建立、複製、更新、尋找和取消 RFCs](#)
- [搭配 RFCs 使用 AMS 主控台](#)
- [了解常見的 RFC 參數](#)
- [註冊 RFC 每日電子郵件](#)

什麼是 RFCs？

變更請求或 RFC 是您在 AMS 受管環境中進行變更的方式，或要求 AMS 代表您進行變更的方式。若要建立 RFC，您可以選擇 AMS 變更類型、選擇 RFC 參數（例如排程），然後使用 AMS 主控台或 API 命令 [CreateRfc](#) 和 [SubmitRfc](#) 提交請求。

RFC 包含兩個規格，一個用於 RFC 本身，另一個用於變更類型 (CT) 參數。在命令列，您可以使用內嵌 RFC 命令或 JSON 格式的標準 [CreateRfc](#) 範本，該範本是您填寫並提交的，以及您建立的 CT JSON 結構描述檔案（根據 CT 參數）。CT 名稱是 CT 的非正式描述。CSIO（類別、子類別、項目、操作）是 CT 的更正式描述。建立 RFC 時，只能指定 CT ID。

當變更成功完成（成功）或失敗（失敗）時，AMS 會通知您。

Note

如需 RFC 失敗疑難排解的資訊，請參閱 [針對 AMS 中的 RFC 錯誤進行故障診斷](#)。

下圖說明您提交的 RFC 工作流程。

使用 AMS API/CLI 進行身分驗證

使用 AMS API/CLI 時，您必須使用臨時憑證進行身分驗證。若要請求聯合身分使用者的臨時安全登入資料，請使用 [GetFederationToken](#)、[AssumeRole](#)、[AssumeRoleWithSAML](#) 或 [AssumeRoleWithWebIdentity](#) AWS 安全字串服務 (STS) APIs。

常見的選擇是 SAML。設定之後，您會將引數新增至您呼叫的每個操作。例如：`aws --profile saml amscm list-change-type-categories`。

SAML 2.0 設定檔的捷徑是在每個 API/CLI 開始時使用設定設定檔變數 `set AWS_DEFAULT_PROFILE=saml`（對於 Windows；對於 Linux，則為 `export AWS_DEFAULT_PROFILE=saml`）。如需設定 CLI 環境變數的詳細資訊，請參閱[設定 AWS 命令列界面、環境變數](#)。

了解 RFC 安全性審查

AWS Managed Services (AMS) 變更管理核准程序可確保我們對您帳戶中所做的變更執行安全審查。

AMS 會根據 AMS 技術標準評估所有變更請求 (RFCs)。任何可能因為偏離技術標準而降低您帳戶安全性狀態的變更，都會經過安全性審查。在安全性審查期間，AMS 會強調相關風險，並且在高或極高安全性風險的情況下，您的授權安全人員會接受或拒絕 RFC。也會評估所有變更，以評估對 AMS 操作能力的負面影響。如果發現潛在的負面影響，則需要在 AMS 內進行額外的審核和核准。

AMS 技術標準

AMS 技術標準定義最低安全標準、組態和程序，以建立帳戶的基準安全性。AMS 和您都必須遵循這些標準。

任何可能因為偏離技術標準而降低您帳戶安全狀態的變更，都會經過風險接受程序，其中 AMS 會反白顯示相關風險，並由授權安全人員從您端接受或拒絕。也會評估所有此類變更，以評估是否對 AMS 操作帳戶的能力有任何負面影響，如果是，則需要在 AMS 內進行額外的審核和核准。

RFC 客戶安全風險管理 (CSRM) 程序

當您的組織某人請求變更您的受管環境時，AMS 會檢閱變更，以判斷請求是否會因超出技術標準而使帳戶的安全狀態惡化。如果請求確實降低了帳戶的安全狀態，AMS 會向您的安全團隊聯絡人通知相關風險，並執行變更；或者，如果變更在環境中帶來高或非常高的安全風險，則 AMS 會以風險接受的形式向您的安全團隊聯絡人尋求明確核准（接下來說明）。AMS 客戶風險接受程序旨在：

- 確保明確識別風險並傳達給正確的擁有者
- 將已識別的環境風險降至最低
- 從了解組織風險設定檔的指定安全聯絡人取得並記錄核准
- 降低已識別風險的持續營運開銷

如何存取技術標準和高風險或極高風險

我們已提供 AMS 技術標準文件供您在 <https://console.aws.amazon.com/artifact/> 中做為報告參考。使用 AMS 技術標準文件，了解在提交變更請求 (RFC) 之前，變更是否需要您的授權安全聯絡人接受風險。

使用預設 AWS Managed Services (AMS) 技術標準」，以尋找技術標準報告。AWS Artifact
AWSManagedServicesChangeManagementRole

Note

單一帳戶登陸區域中的 Customer_ReadOnly_Role 可存取 AMS 技術標準文件。在多帳戶登陸區域中，安全管理員使用的 AWSManagedServicesAdminRole 和應用程式團隊使用的 AWSManagedServicesChangeManagementRole 可用來存取文件。如果您的團隊使用自訂角色，請建立其他 | 其他 RFC 來請求存取權，我們將更新指定的自訂角色。

了解 RFC 變更類型分類

您在提交 RFC 時使用的變更類型分為兩個廣泛的類別：

- 部署：此分類用於建立資源。
- 管理：此分類用於更新或刪除資源。Management 類別也包含存取執行個體、加密或共用 AMIs，以及啟動、停止、重新啟動或刪除堆疊的變更類型。

了解 RFC 動作和活動狀態

RfcActionState (API) / 活動狀態（主控台）可協助您了解 RFC 上人工介入或動作的狀態。主要用於手動 RFCs，RfcActionState 可協助您了解您或 AMS 操作何時需要採取動作，並協助您了解 AMS 操作何時正在積極處理 RFC。這可提高 RFC 在其生命週期內所採取動作的透明度。

RfcActionState (API)/活動狀態（主控台）定義：

- AwsOperatorAssigned：AWS 運算子正在積極處理您的 RFC。
- AwsActionPending：預期來自 AWS 的回應或動作。
- CustomerActionPending：預期來自客戶的回應或動作。
- NoActionPending：AWS 或客戶不需要採取任何動作。
- NotApplicable：此狀態無法由 AWS 運算子或客戶設定，且僅用於在釋出此功能之前建立 RFCs。

RFC 動作狀態會根據提交的變更類型是否需要手動檢閱，且排程是否設定為 ASAP 而有所不同。

- RFC `ActionState` 在檢閱、核准和啟動具有延遲排程的手動變更類型期間變更：
 - 在您提交手動、排程的 RFC 之後，`ActionState` 會自動變更為 `AwsActionPending`，以指出操作員需要檢閱和核准 RFC。
 - 當運算子開始主動檢閱 RFC 時，`ActionState` 會變更為 `AwsOperatorAssigned`。
 - 當運算子核准您的 RFC 時，RFC 狀態會變更為已排程，而 `ActionState` 會自動變更為 `NoActionPending`。
 - 達到 RFC 的排程開始時間時，RFC 狀態會變更為 `InProgress`，而 `ActionState` 會自動變更為 `AwsActionPending`，表示需要指派運算子來檢閱 RFC。
 - 當運算子開始主動執行 RFC 時，他們會將 `ActionState` 變更為 `AwsOperatorAssigned`。
 - 完成後，運算子會關閉 RFC。這會自動將 `ActionState` 變更為 `NoActionPending`。

Important

- 您無法設定動作狀態。它們會根據 RFC 中的變更自動設定，或由 AMS 運算子手動設定。
- 如果您將通訊新增至 RFC，`ActionState` 會自動設定為 `AwsActionPending`。
- 建立 RFC 時，`ActionState` 會自動設定為 `NoActionPending`。
- 提交 RFC 時，`ActionState` 會自動設定為 `AwsActionPending`。
- 當 RFC 遭到拒絕、取消或完成且狀態為成功或失敗時，`ActionState` 會自動重設為 `NoActionPending`。
- 動作狀態會同時針對自動和手動 RFCs 啟用，但對於手動 RFCs 來說主要很重要，因為這類 RFCs 通常需要通訊。

檢閱 RFC 動作狀態使用案例範例

使用案例：手動 RFC 程序的可見性

- 提交手動 RFC 後，RFC 動作狀態會自動變更為 `AwsActionPending`，表示操作員需要檢閱和核准 RFC。當運算子開始主動檢閱 RFC 時，RFC 動作狀態會變更為 `AwsOperatorAssigned`。
- 請考慮已獲核准並排定且已準備好開始執行的手動 RFC。一旦 RFC 狀態變更為 `InProgress`，RFC 動作狀態會自動變更為 `AwsActionPending`。當運算子開始主動執行 RFC `AwsOperatorAssigned` 時，它會再次變更為。

- 手動 RFC 完成時（關閉為「成功」或「失敗」），RFC 動作狀態會變更為 NoActionPending，表示客戶或運算子不需要進一步的動作。

使用案例：RFC 通訊

- 當手動 RFC 為 時Pending Approval，AMS Operator 可能需要您提供進一步的資訊。運算子會將通訊發佈至 RFC，並將 RFC 動作狀態變更為 CustomerActionPending。當您透過新增 RFC 通訊來回應時，RFC 動作狀態會自動變更為 AwsActionPending。
- 當自動或手動 RFC 失敗時，您可以將通訊新增至 RFC 詳細資訊，向 AMS Operator 詢問 RFC 失敗的原因。新增通訊時，RFC 動作狀態會自動設定為 AwsActionPending。當 AMS 運算子挑選 RFC 以檢視您的通訊時，RFC 動作狀態會變更為 AwsOperatorAssigned。當運算子透過新增 RFC 通訊來回應時，RFC 動作狀態可能會設定為 CustomerActionPending，表示客戶預期有另一個回應，或 NoActionPending，表示不需要或預期客戶的任何回應。

了解 RFC 狀態碼

RFC 狀態碼可協助您追蹤請求。您可以在 CLI 輸出中的 RFC 執行期間觀察這些狀態碼，或在主控台中重新整理 RFC 清單頁面。

您也可以在此 RFC 的詳細資訊頁面上看到 RFC 的代碼，如下所示：

您可能會在清單中看到您未提交的 RFC。當 AMS 運算子使用僅限內部的 CT 時，他們會在 RFC 中提交它，並顯示在 RFC 清單中。如需詳細資訊，請參閱[僅限內部的變更類型](#)。

 Important

您可以請求 RFC 狀態變更的通知。如需詳細資訊，請參閱 [RFC 狀態變更通知](#)。

RFC 狀態碼

成功	失敗
編輯：RFC 已建立但未提交	拒絕：RFCs通常會因為驗證失敗而遭到拒絕；例如，指定了無法使用的資源，即子網路
PendingApproval / Submitted：已提交 RFC，且系統正在判斷是否需要核准，並視需要取得該核准	已取消：RFCs通常會取消，因為在設定的開始時間之前不會通過驗證

成功	失敗
AWS 核准/客戶核准：RFC 已核准。自動化 RFCs 由 AWS 核准，手動 RFCs 由 Operators 核准，有時由客戶核准	失敗：RFC 失敗；如需失敗原因，請參閱輸出中的 StatusReason，AMS 操作會自動建立故障票證並視需要與您通訊
已排程：RFC 已通過語法和需求檢查，並排定執行	
InProgress：RFC 正在執行中，請注意，佈建多個資源或具有長時間執行 UserData RFCs 需要更長的時間才能執行	
已執行：已執行 RFC	
成功/成功：RFC 已成功完成	

 Note

已取消或拒絕 RFCs 可以使用 [UpdateRfc](#) 重新提交；另請參閱 [更新 RFCs](#)。

如果 RFC 通過所有必要條件（例如，指定所有必要參數），狀態會變更為 PendingApproval（即使自動化 CTs 需要核准，如果語法和參數檢查通過，也會自動發生）。如果未通過，狀態會變更為 Rejected。StatusReason 提供有關拒絕的資訊；ExecutionOutput 欄位提供有關核准和完成的資訊。錯誤代碼包括：

- InvalidRfcStateException：RFC 處於不允許呼叫操作的狀態。例如，如果 RFC 已移至提交狀態，就無法再修改。
- InvalidRfcScheduleException：已違反 StartTime、EndTime 或 TimeoutInMinutes 參數。
- InternalServerError：系統發生問題。
- InvalidArgumentException：未正確指定參數；例如，使用無法接受的值。
- ResourceNotFoundException：找不到堆疊 ID 等值。

如果排定的請求開始和結束時間（也稱為變更執行時段）在核准變更之前發生，RFC 狀態會變更為 Canceled。如果變更獲得核准，RFC 狀態會變更為 Scheduled。ASAP RFCs 的變更執行時段是提交的時間加上 CT ExpectedExecutionDuration 的值。

在變更執行時段到達之前的任何時間，都可以修改或取消排定的變更（在 CLI RequestedStartTime 中使用 提交）。如果已修改排程變更，則必須重新提交。

當變更開始時間到達（排程或 ASAP）且核准完成後，狀態會變更為 InProgress 且無法進行任何修改。如果在指定的變更執行時段內完成變更，狀態會變更為 Success。如果變更的任何部分失敗，或變更在變更執行時段結束時仍在進行中，狀態會變更為 Failure。

Note

在 InProgress、Success 或 Failure 變更狀態期間，無法修改或取消 RFC。

下圖說明從 CreateRFC 呼叫到解析的 RFC 狀態。

了解 RFC 更新 CTs 和 CloudFormation 範本偏離偵測

在 AMS 中佈建的資源使用修改過的 AWS CloudFormation 範本。如果資源直接透過服務的 AWS 管理主控台變更參數，則該資源的 CloudFormation 建立記錄會變得不同步。如果發生這種情況，且您嘗試使用 AMS 更新變更類型來更新 AMS 中的資源，則 AMS 會參考原始資源組態，並可能重設變更的參數。此重設可能會損壞，因此如果偵測到任何額外的 AMS 組態變更，AMS 會不允許具有更新變更類型的 RFCs。

如需更新變更類型的清單，請使用 主控台篩選條件。

漂移修復FAQs

AMS 漂移修復的問題和答案。您可以使用兩種變更類型來啟動偏離修復，一種是執行模式=手動或「需要檢閱」，另一種是執行模式=自動。

漂移修復支援的資源 (ct-3kinq0u4l33zf)

這些是漂移修復變更類型 (ct-3kinq0u4l33zf) 支援的資源。若要修復任何資源，請改用「需要檢閱」(ct-34sxfo53yuzah) 變更類型。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
```

```
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

偏離修復變更類型

有關使用 AMS 偏離修復變更類型的問答。

如需偏離修補功能的支援資源清單，請參閱 [漂移修復支援的資源 \(ct-3kinq0u4l33zf\)](#)。

Important

漂移修復會修改堆疊範本和/或參數，而且必須更新本機範本儲存庫或更新這些堆疊的任何自動化，才能使用最新的堆疊範本和參數。使用舊範本和/或參數而不同步可能會導致基礎資源的變更受損。

不需要的檢閱、自動化、CT (ct-3kinq0u4l33zf) 支援每個 RFC 僅修復 10 個資源。若要以 10 個批次修復剩餘的資源，請建立新的 RFCs，直到所有資源都修復為止。

我應該使用哪種偏離修復變更類型？

在以下情況下，我們建議您使用不需要檢閱的自動化 CT (ct-3kinq0u4l33zf)：

- 您嘗試使用自動化 CT 執行現有堆疊資源的更新，而 RFC 會被拒絕，因為堆疊是 DRIFTED。
- 您過去曾使用更新 CT，但因為堆疊已 DRIFTED 而失敗。您不需要再次嘗試更新，可以改用檢閱所需的手動 CT。

我們建議只在漂移修復不支援漂移資源類型時，才使用所需的檢閱手動 CT (ct-34sxfo53yuzah)，不需要檢閱、自動化、CT (ct-3kinq0u4l33zf)，或漂移修復不需要檢閱、自動化、CT 失敗。

修補期間對堆疊執行哪些變更？

修復需要更新堆疊範本和/或參數，具體取決於漂移的屬性。修補也會在修補期間更新堆疊的堆疊政策，並在修補完成後將堆疊政策還原至先前的值。

如何查看對堆疊範本和/或參數執行的變更？

在 RFC 的回應中，會提供變更摘要，其中包含下列資訊：

- `ChangeSummaryJson`：包含堆疊範本和/或參數的變更摘要，做為偏離修復的一部分。修補會以多個階段執行。此變更摘要包含個別階段的變更。如果修復成功，請檢查最後一個階段的變更。如需依順序執行的階段，請參閱 JSON 中的 `ExecutionPlan`。例如，存在時的 `RestoreReferences` 區段一律在結尾執行，並包含修正後變更的 JSON。如果修復是在 `DryRun` 模式下執行，則這些變更都不會套用至堆疊。
- `PreRemediationStackTemplateAndConfigurationJson`：在堆疊上觸發修復之前，包含 `CloudFormation Stack` 的組態快照，包括範本、參數、輸出、`StackPolicyBody`。

執行修復之後，我需要做什麼？

Important

您需要使用 RFC 摘要中提供的最新範本和參數，更新本機範本儲存庫或任何會更新修復堆疊的自動化。請務必這麼做，因為使用舊範本和/或參數可能會對堆疊資源造成進一步的破壞性變更。

在此修復期間，我的應用程式是否會生效？

修復是一種離線程序，僅在 `CloudFormation` 堆疊組態上執行。不會對基礎資源執行更新。

在修復之後，我可以繼續使用管理 | 其他 | 其他 RFCs 對資源執行更新嗎？

我們建議您一律使用可用的自動更新 CTs 執行堆疊資源的更新。當可用的更新 CTs 不支援您的使用案例時，請使用管理 | 其他 | 其他請求。

修補是否在堆疊中建立新的資源？

修復不會在堆疊中建立新的資源。不過，修補會建立新的輸出並更新堆疊範本 [中繼資料](#) 區段，以存放修補摘要供您參考。

修復永遠成功嗎？

修復需要仔細分析和驗證範本組態，以判斷是否可以執行。在這些驗證失敗的情況下，修復程序會停止，且堆疊範本或參數不會進行任何變更。此外，只能對支援的資源類型執行修復。

如果修復不成功，如何執行堆疊資源的更新？

您可以使用 管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k) 來請求變更。AMS 會監控這類案例，並致力於改善修補解決方案。

我可以修復同時具有支援和不支援資源類型的堆疊嗎？

是。不過，只有在堆疊中找到支援的資源類型時，才會執行修復。如果任何不支援的資源類型為 DRIFTED，則不會繼續修復。

對於透過非 CFN 擷取 CTs 建立的堆疊，是否可以請求修復？

是。無論用於建立堆疊的變更類型為何，都可以在堆疊上執行修補。

我是否可以知道在修復之前將對堆疊執行的變更？

是。這兩種變更類型都提供 DryRun 選項，您可以用來請求在堆疊修復時執行的變更。不過，最終修復變更可能會因修復時堆疊上存在的偏離而有所不同。

排程 RFCs

排程功能可讓您選擇 RFCs 的開始時間。下列選項可在 排程功能中使用：

- 盡快執行此變更：一旦核准，AMS 就會執行 RFC。大多數 CTs 都會自動核准。如果不希望 RFC 在特定時間啟動，請使用此選項。
- 排程此變更：設定要執行 RFC 的日期、時間和時區。對於自動變更類型，最佳實務是在您計劃提交 RFC 至少 10 分鐘後請求開始時間。若要檢閱必要的變更類型，您必須在計劃提交 RFC 至少 24 小時後請求開始時間。如果設定的開始時間未核准 RFC，則會拒絕 RFC。

設定 RFC 排程

若要排程 RFC，請使用下列其中一種方法：

盡快執行此變更：

- 主控台：不執行任何動作。這會使用預設 RFC 排程。
- API 或 CLI：移除建立 RFC 操作中的 RequestedStartTime 和 RequestedEndTime 選項。

如果 RFCs 提交後的三十天內未獲得核准，即會自動拒絕。

排程此變更：

- 主控台：選取排程此變更選項按鈕。開始時間區域隨即開啟。手動輸入一天，或使用行事曆小工具來挑選一天。以 UTC 輸入以 ISO 8601 格式表示的時間，並使用下拉式清單來挑選位置。根據預設，AMS 使用 ISO 8601 格式 YYYYMMDDThhmmssZ 或 YYYY-MM-DDThh:mm:ssZ，接受任一格式。

Note

預設結束時間是從您輸入的開始時間起算 4 小時。若要將排程變更的結束時間設定為超過 4 小時，請使用 API 或 CLI 來執行變更。

- API 或 CLI：在建立 RFC 操作中提交 RequestedStartTime 和 RequestedEndTime 參數的值。傳遞已設定的 RequestedEndTime 不會停止已啟動的自動變更類型的執行。對於「需要檢閱」變更類型，如果 RequestedEndTime 在 AMS Operations 研究仍在進行中時達到，而且您正在與 AMS 通訊，則可以請求 延伸，或者您可能需要重新提交 RFC。

Tip

如需 UTC 時間讀取的範例，請參閱 Time-is 網站上的 [UTC](#)。日期/時間值為 2016-12-05 的 ISO 8601 格式範例，時間為下午 2:20:2016-12-05T14:20:00Z 或 20161205T142000Z。

如果您提供...

- 只有 RequestedStartTime，RFC 會被視為已排程，並使用 RequestedEndTime ExecutionDurationInMinutes 值填入。
- 只有 RequestedEndTime，我們擲回 InvalidArgumentException。
- RequestedStartTime 和 RequestedEndTime 我們 RequestedEndTime 都會以指定的開始時間加上 ExecutionDurationInMinutes 值來覆寫。
- 無論是 RequestedStartTime 還是 RequestedEndTime，我們都會將這些值保留為 null，並將 RFC 視為 ASAP RFC。

Note

對於所有排程 RFCs，未指定的結束時間會寫入為指定的時間 RequestedStartTime 加上所提交變更類型的 ExpectedExecutionDurationInMinutes 屬性。例如，如果 ExpectedExecutionDurationInMinutes 是 "60"（分鐘），且指定

的 RequestedStartTime 是 2016-12-05T14:20:00Z(2016 年 12 月 5 日上午 4:20)，則實際結束時間將設定為 2016 年 12 月 5 日上午 5:20。若要尋找 ExpectedExecutionDurationInMinutes 特定變更類型的，請執行此命令：

```
aws amscm --profile saml get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

使用 RFC Priority 選項

在 execution mode = manual 變更類型中使用 Priority 選項，提醒 AMS Operations 請求的緊急程度。

中的優先順序選項 execution mode = manual：

將手動 RFC 的優先順序指定為高、中或低。分類為高 RFCs 會在分類為中 RFCs 之前經過審核和核准，但需受 RFC 服務水準目標 SLOs) 及其提交時間的約束。具有低優先順序或未指定優先順序 RFCs 會依提交順序進行處理。

核准或拒絕 RFCs

使用核准必要（手動）CTs RFCs 必須經過您或 AMS 的核准。會自動處理預先核准的 CTs。如需詳細資訊，請參閱 [CT 核准要求](#)。

Note

使用「需要檢閱」CTs 時，AMS 建議您使用 ASAP 排程選項（在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准，則會自動拒絕 RFC。

如果 AMS 成功提交核准所需的 RFC，則必須獲得您的明確核准。或者，如果您提交核准所需的 RFC，則必須由 AMS 核准。如果您需要核准 AMS 提交的 RFC，則會傳送電子郵件或其他預先決定的通訊給您請求核准。通訊包含 RFC ID。傳送通訊後，請執行下列其中一項操作：

- 主控台核准或拒絕：使用相關 RFC 的 RFC 詳細資訊頁面：

- API/CLI 核准：[ApproveRfc](#) 會將變更標記為已核准。如果需要兩者，擁有者和運算子都必須採取動作。以下是 CLI 核准命令的範例。在下列範例中，將 RFC_ID 取代為適當的 RFC ID。

```
aws amscm approve-rtc --rtc-id RFC_ID
```

- API/CLI 拒絕：[RejectRfc](#) 會將變更標記為已拒絕。以下是 CLI 拒絕命令的範例。在下列範例中，將 RFC_ID 取代為適當的 RFC ID。

```
aws amscm reject-rtc --rtc-id RFC_ID --reason "no longer relevant"
```

請求 RFC 限制執行期間

先前稱為中斷日，您可以請求限制特定時段。在此期間無法執行任何變更。

若要設定限制的執行期間，請使用 [UpdateRestrictedExecutionTimes](#) API 操作，並以 UTC 設定特定期間。您指定的期間會覆寫先前指定的任何期間。如果您在指定的限制執行時間提交 RFC，提交會失敗，並顯示無效的 RFC 排程錯誤。您最多可以指定 200 個限制時段。根據預設，不會設定限制期間。以下是範例 請求命令（已設定 SAML 身分驗證）：

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

您也可以執行 [RestrictedExecutionTimes](#) API 操作來檢視目前的 [RestrictedExecutionTimes](#) 設定。
[ListRestrictedExecutionTimes](#) 範例：

```
aws amscm --profile saml list-restricted-execution-times
```

如果您想要在指定的限制執行時間提交 RFC，請使用 [OverrideRestrictedTimeRanges](#) 值新增 [RestrictedExecutionTimesOverrideId](#)，然後像平常一樣提交 RFC。最佳實務是僅將此方法用於關鍵或緊急 RFC。如需詳細資訊，請參閱 [SubmitRfc](#) 的 API 參考。

建立、複製、更新、尋找和取消 RFCs

下列範例會逐步解說各種 RFC 操作。

主題

- [建立 RFC](#)

- [使用 AMS 主控台複製 RFCs \(重新建立 \)](#)
- [更新 RFCs](#)
- [尋找 RFCs](#)
- [取消 RFCs](#)

建立 RFC

使用主控台建立 RFC

以下是 AMS 主控台中 RFC 建立程序的第一頁，其中開啟快速卡並啟用瀏覽變更類型：

以下是 AMS 主控台中 RFC 建立程序的第一頁，並啟用依類別選取：

運作方式：

1. 導覽至建立 RFC 頁面：在 AMS 主控台的左側導覽窗格中，按一下 RFCs 以開啟 RFCs 清單頁面，然後按一下建立 RFC。
2. 在預設瀏覽變更類型檢視中選擇熱門的變更類型 (CT)，或在依類別選擇檢視中選擇 CT。
 - 依變更類型瀏覽：您可以在快速建立區域中按一下熱門的 CT，以立即開啟執行 RFC 頁面。請注意，您無法透過快速建立選擇較舊的 CT 版本。

若要排序 CTs，請使用卡片或資料表檢視中的所有變更類型區域。在任一檢視中，選取 CT，然後按一下建立 RFC 以開啟執行 RFC 頁面。如果適用，建立較舊版本選項會顯示在建立 RFC 按鈕旁。

 - 依類別選擇：選取類別、子類別、項目和操作，如果適用，CT 詳細資訊方塊會開啟，其中包含使用較舊版本建立的選項。按一下建立 RFC 以開啟執行 RFC 頁面。
3. 在執行 RFC 頁面上，開啟 CT 名稱區域以查看 CT 詳細資訊方塊。需要主旨（如果您在瀏覽變更類型檢視中選擇 CT，則會為您填入）。開啟其他組態區域以新增 RFC 的相關資訊。

在執行組態區域中，使用可用的下拉式清單或輸入必要參數的值。若要設定選用的執行參數，請開啟其他組態區域。

4. 完成後，請按一下執行。如果沒有錯誤，RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
5. 開啟執行參數區域以查看您提交的組態。重新整理頁面以更新 RFC 執行狀態。或者，取消 RFC 或使用頁面頂端的選項建立 RFC 的副本。

使用 CLI 建立 RFC

運作方式：

1. 使用內嵌建立（您發出包含所有 RFC 和執行參數的 `create-rfc` 命令）或範本建立（您建立兩個 JSON 檔案，一個用於 RFC 參數，另一個用於執行參數），並使用兩個檔案作為輸入發出 `create-rfc` 命令。此處說明這兩種方法。
2. 使用傳回的 RFC ID 提交 RFC：`aws amscm submit-rfc --rfc-id ID` 命令。

監控 RFC：`aws amscm get-rfc --rfc-id ID` 命令。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

您可以將任何 `CreateRfc` 參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 `--notification` `{"Email\": {\"EmailRecipients\": [\"email@example.com\"]}}"` RFC 參數部分（而非執行參數）。如需所有 `CreateRfc` 參數的清單，請參閱 [AMS 變更管理 API 參考](#)。

內嵌建立：

使用內嵌提供的執行參數發出建立 RFC 命令（在內嵌提供執行參數時逸出引號），然後提交傳回的 RFC ID。例如，您可以將內容取代為如下內容：

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
"TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

範本建立：

Note

此建立 RFC 的範例使用 Load Balancer (ELB) 堆疊變更類型。

1. 尋找相關的 CT。下列命令會搜尋項目名稱中包含「ELB」的 CT 分類摘要，並以資料表形式建立類別、項目、操作和 ChangeTypeId 的輸出（兩者的子類別都是 Advanced stack components）。

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
  [Category,Item,Operation,ChangeTypeId]" --output table
```

```
-----
|                               CtSummaries                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rsebx9 |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

2. 尋找最新版本的 CT：

ChangeTypeId 和 ChangeTypeVersion：此演練的變更類型 ID 為 ct-123h45t6uz7jl（建立 ELB），若要了解最新版本，請執行此命令：

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. 了解選項和要求。下列命令會將結構描述輸出至名為 CreateElbParams.json。

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
  "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 修改並儲存執行參數 JSON 檔案。此範例會命名檔案 CreateElbParams.json。

對於佈建 CT，StackTemplateId 包含在結構描述中，並且必須在執行參數中提交。

對於 TimeoutInMinutes，允許在 RFC 失敗之前建立堆疊的分鐘數，此設定不會延遲 RFC 執行，但您必須提供足夠的時間（例如，不要指定 "5"）。對於具有長時間執行 UserData CTs，有效值為「60」到「360」：建立 EC2 和建立 ASG。對於所有其他佈建 CTs，我們建議使用允許的「60」上限。

提供您要建立堆疊的 VPC ID；您可以使用 CLI 命令取得 VPC IDaws amsskms list-vpc-summaries。

```
{
```

```

"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv000000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters": {
  "ELBSubnetIds":      ["SUBNET_ID"],
  "ELBHealthCheckHealthyThreshold": 4,
  "ELBHealthCheckInterval": 5,
  "ELBHealthCheckTarget": "HTTP:80/",
  "ELBHealthCheckTimeout": 60,
  "ELBHealthCheckUnhealthyThreshold": 5,
  "ELBScheme":         false
}
}

```

5. 將 RFC JSON 範本輸出到目前資料夾中名為 CreateElbRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. 修改並儲存 CreateElbRfc.json 檔案。由於您在不同的檔案中建立執行參數，請移除該 ExecutionParameters 行。例如，您可以將內容取代為如下內容：

```

{
  "ChangeTypeVersion": "2.0",
  "ChangeTypeId":      "ct-123h45t6uz7jl",
  "Title":              "Create ELB"
}

```

7. 建立 RFC。下列命令會指定執行參數檔案和 RFC 範本檔案：

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-parameters file://CreateElbParams.json
```

您會在回應中收到新 RFC 的 ID，並且可以使用它來提交和監控 RFC。在您提交之前，RFC 會保持在編輯狀態，不會啟動。

提示

Note

您可以使用 AMS API/CLI 來建立 RFC，而無需建立 RFC JSON 檔案或 CT 執行參數 JSON 檔案。若要這樣做，您可以使用 `create-rfc` 命令並將所需的 RFC 和執行參數新增至命令，這稱為「內嵌建立」。請注意，所有佈建 CTs 都包含在 `execution-parameters` 具有資源參數的 `Parameters` 陣列區塊中。參數必須具有以反斜線 (\) 逸出的引號。

另一個建立 RFC 的記錄方法稱為「範本建立」。您可以在此處為 RFC 參數建立 JSON 檔案，並為執行參數建立另一個 JSON 檔案，並使用 `create-rfc` 命令提交這兩個檔案。這些檔案可以做為範本，並再次用於未來的 RFCs。

使用 範本建立 RFCs 時，您可以使用 命令，透過發出命令來建立具有所需內容的 JSON 檔案，如下所示。這些命令會使用顯示的內容建立名為 "parameters.json" 的檔案；您也可以使用這些命令來建立 RFC JSON 檔案。

使用 AMS 主控台複製 RFCs（重新建立）

您可以使用 AMS 主控台來複製現有的 RFC。

若要使用 AMS 主控台複製或重新建立 RFC，請遵循下列步驟：

1. 尋找相關的 RFC。在左側導覽中，按一下 RFCs。

RFCs 儀表板隨即開啟。

2. 捲動頁面，直到您找到要複製的 RFC。使用篩選選項縮小清單範圍。選擇您要複製的 RFC。

RFC 詳細資訊頁面隨即開啟。

3. 按一下建立複本。

建立變更請求頁面隨即開啟，並將所有選項設定為原始 RFC 中的。

4. 進行您想要的變更。若要設定其他選項，請將基本選項變更為進階。設定所有選項後，請選擇提交。

作用中 RFC 詳細資訊頁面會開啟，其中包含複製 RFC 的新 RFC ID，而複製的 RFC 會出現在 RFC 儀表板中。

更新 RFCs

您可以更新 RFC 然後提交或重新提交，以重新提交已被拒絕或尚未提交的 RFC。請注意，大多數 RFCs 都會遭到拒絕，因為在提交之前 `RequestedStartTime` 已通過指定的，或指定的 `TimeoutInMinutes` 不足以執行 RFC（由於 `TimeoutInMinutes` 不會延長成功的 RFC，我們建議針對 Amazon EC2 或具有長時間執行 `UserData` 的 Amazon EC2 Auto Scaling 群組，一律將此設定為至少 "60" 且最多 "360"）。本節說明如何使用 `UpdateRfc` 命令的 CLI 版本，使用新的 RFC 參數更新 RFC，或使用字串化 JSON 或更新的參數檔案更新新參數。

此範例說明使用 AMS `UpdateRfc` API 的 CLI 版本（請參閱[更新 RFC](#)）。雖然更新某些資源 (DNS 私有和公有、負載平衡器堆疊和堆疊修補組態) 有變更類型，但沒有 CT 可更新 RFC。

我們建議您一次提交一個 `UpdateRfc` 操作。如果您提交多個更新，例如在 DNS 堆疊上，更新可能無法同時嘗試更新 DNS。

必要資料：`RfcId`：您正在更新的 RFC。

選擇性資料：`ExecutionParameters`：除非您更新非必要欄位，例如 `Description`，否則您可以提交修改後的執行參數，以解決導致 RFC 被拒絕或取消的問題。所有提交的非空值都會覆寫原始 RFC 中的這些值。

1. 尋找相關的已拒絕或取消的 RFC，您可以使用此命令（您可以使用 取代值 `Canceled`）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 您可以修改下列任何 RFC 參數：

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

更新描述欄位的範例命令：

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"  
--region us-east-1
```

更新 ExecutionParameters VpcId 欄位的範例命令：

```
aws amscm update-rfc --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id  
"RFC_ID" --region us-east-1
```

使用包含更新的執行參數檔案更新 RFC 的範例命令；請參閱步驟 2 中的範例執行參數檔案：[EC2 堆疊 | 建立](#)：

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --  
rfc-id "RFC_ID" --region us-east-1
```

3. 使用 submit-rfc 和您在第一次建立 RFC 時擁有的相同 RFC ID 重新提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，您在命令列不會收到確認或錯誤訊息。

4. 若要監控請求的狀態和檢視執行輸出，請執行下列命令。

```
aws amscm get-rfc --rfc-id RFC_ID
```

尋找 RFCs

使用主控台尋找變更請求 (RFC)

若要使用 AMS 主控台尋找 RFC，請遵循下列步驟。

Note

此程序僅適用於排程 RFCs，也就是未使用 ASAP 選項的 RFCs。

1. 在左側導覽中，按一下 RFCs。

RFCs 儀表板隨即開啟。

2. 捲動清單或使用篩選選項來精簡清單。

RFC 清單會依篩選條件而變更。

3. 選擇您想要之 RFC 的主旨連結。

RFC 詳細資訊頁面會開啟該 RFC，其中包含 RFC ID 等資訊。

4. 如果儀表板中有許多 RFCs，您可以使用篩選條件選項依 RFC 搜尋：

- 主旨：建立 RFC 時提供給 RFC 的主旨行或標題（在 API/CLI 中）。
- RFC ID：RFC 的識別符。
- 活動狀態：如果您知道 RFC 狀態，您可以在 `AwsOperatorAssigned` 之間進行選擇，表示運算子目前正在查看 RFC，`AwsActionPending` 表示 AMS 運算子必須執行某些動作，然後 RFC 執行才能繼續，或者 `CustomerActionPending` 表示您需要採取一些動作，才能繼續執行 RFC。
- 狀態：如果您知道 RFC 狀態，您可以選擇：
 - 已排程：已排程 RFCs。
 - 已取消：已取消 RFCs。
 - 進行中：RFCs 進行中。
 - 成功：成功執行 RFCs。
 - 已拒絕：已拒絕 RFCs。
 - 編輯：正在編輯 RFCs。
 - 失敗：失敗 RFCs。
 - 待核准：在 AMS 或您核准之前無法繼續進行 RFCs。一般而言，這表示您需要核准 RFC。您會在服務請求清單中收到此服務通知。
- 變更類型：挑選類別、子類別、項目和操作，然後為您擷取變更類型 ID。
- 請求的開始時間或請求的結束時間：此篩選條件選項可讓您選擇之前或之後，然後輸入日期和選擇性的時間 (hh:mm 和時區)。此篩選條件只會在排程 RFCs（非 ASAP RFCs 上成功運作）。
- 狀態：已排程、已取消、進行中、成功、已拒絕、編輯或失敗。
- 主旨：您使用給定 RFC 的 API/CLI 建立 RFC 的主旨（或標題）。
- 變更類型 ID：使用與 RFC 一起提交的變更類型識別符。

搜尋可讓您新增篩選條件，如下列螢幕擷取畫面所示。

5. 按一下您想要之 RFC 的主旨連結。

RFC 詳細資訊頁面會開啟該 RFC，其中包含 RFC ID 等資訊。

使用 CLI 尋找變更請求 (RFC)

您可以使用多個篩選條件來尋找 RFC。

若要檢查變更類型版本，請使用下列命令：

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

 Note

您可以將任何CreateRfc參數與任何 RFC 搭配使用，無論它們是否為變更類型結構描述的一部分。例如，若要在 RFC 狀態變更時取得通知，請將此行新增至請求的 --notification "{\\"Email\\": {\\"EmailRecipients\\" : [\\"email@example.com\\"]}}\" RFC 參數部分（而非執行參數）。如需所有 CreateRfc 參數的清單，請參閱 [AMS 變更管理 API 參考](#)。

如果您不記下 RFC ID，且稍後需要找到它，您可以使用 AMS 變更管理 (CM) 系統來搜尋它，並使用篩選條件或查詢縮小結果範圍。

1. CM API [ListRfcSummaries](#) 操作具有篩選條件。您可以根據邏輯 AND 操作中的 Attribute和 Value組合，或根據 Attribute、Condition和 [篩選](#)結果Values。

RFC 篩選

屬性	有效值	有效條件	預設條件	備註
ActualEndTime	任何代表 ISO8601 日期時間的字串（例如，「2017 0101T000000Z」）	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值，其中第一個值應代表在第二個值之前發生的日期

屬性	有效值	有效條件	預設條件	備註
ActualStartTime	任何代表 ISO8601 日期時間的字串 (例如, 「2017 0101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期
AutomationStatusId	手動、自動化	等於	等於	只有兩個自動化狀態
ChangeTypeId	任何有效的變更類型 ID ; 例如 ct-123h45t6uz7jl	等於	等於	尋找變更類型或 CSIO
ChangeTypeVersion	任何有效的變更類型 ID ; 例如 1.0	等於	等於	尋找變更類型或 CSIO
CreatedBy	任何字串 (長度上限為 2048 個字元)	包含	包含	RFC 的 CreatedBy 欄位包含建立它的使用者的 ARN
CreatedTime	任何代表 ISO8601 日期時間的字串 (例如, 「2017 0101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期
LastModifiedTime	任何代表 ISO8601 日期時間的字串 (例如, 「2017 0101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期

屬性	有效值	有效條件	預設條件	備註
LastSubmittedTime	任何代表 ISO8601 日期時間的字串 (例如, 「20170101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期
RequestedEndTime	任何代表 ISO8601 日期時間的字串 (例如, 「20170101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期
RequestedStartTime	任何代表 ISO8601 日期時間的字串 (例如, 「20170101T000000Z」)	之前、之後、之間	無	Before 或 After 條件只接受值欄位中的一個值。介於條件在值欄位中必須剛好有兩個值, 其中第一個值應代表在第二個值之前發生的日期
RfcStatusId	已取消、編輯、失敗、InProgress、PendingApproval、已拒絕、已排程、成功	等於	等於	在 AMS 主控台重新整理 RFC 清單或執行 GetRfc
標題	任何有效的 RFC 標題	包含	包含	不支援每個個別欄位中的規則表達式。不區分大小寫的搜尋

範例：

若要尋找與 SQS 相關的所有 RFCs IDs (其中 SQS 包含在 CT 的項目部分) , 您可以使用此命令 :

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

這會傳回如下內容 :

```
-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components      |SQS   |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notification    |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

另一個適用於 的篩選條件list-rfc-summaries是 AutomationStatusId , 用於尋找自動化或手動RFCs :

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

另一個適用於 的篩選條件list-rfc-summaries是 Title (主控台的主旨) :

```
Attribute=Title,Value=RFC-TITLE
```

JSON 中傳回 RFCs的新請求結構範例 , 其中 :

- (標題包含「Windows 2012」或「Amazon Linux」) 和
- (RfcStatusId EQUALS "Success" 或 "InProgress") 和
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    }
  ]
}
```

```
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

Note

使用更進階的 `Filters`，AMS 打算在即將發行的版本中棄用下列欄位：

- 值：值欄位是篩選條件欄位的一部分。使用支援更進階功能的值欄位。
- `RequestedEndTimeRange`：在支援更進階功能的篩選條件欄位中使用 `RequestedEndTime`
- `RequestedStartTimeRange`：在支援更進階功能的篩選條件欄位中使用 `RequestedStartTime`。

如需有關使用 CLI 查詢的資訊，請參閱[如何使用 --query Option 篩選輸出](#)和查詢語言參考[JMESPath Specification](#)。

2. 如果您使用的是 AMS 主控台：

前往 RFCs 清單頁面。如有需要，您可以篩選 RFC 主體，這是您在建立 RFC Title 時輸入的內容。

提示

Note

此程序僅適用於排定的 RFCs，也就是未使用 ASAP 選項的 RFCs。

取消 RFCs

您可以使用 主控台或 AMS API/CLI 來取消 RFC。

若要使用主控台取消 RFC，請在 RFC 清單中尋找 RFC，開啟它，然後按一下取消。

必要資料：

- Reason：取消 RFC 的原因。
 - RfcId：您要取消的 RFC。
1. 一般而言，您會在提交 RFC 後立即取消 RFC（因此 RFC ID 應該很方便）；否則，除非您已排定，且早於指定的開始時間，否則您將無法取消 RFC。如果您需要尋找 RFC ID，您可以使用此命令（您可以將 Value 取代 PendingApproval 為手動核准的 RFC）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. 取消 RFC 的範例命令：

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --region us-east-1
```

搭配 RFCs 使用 AMS 主控台

AMS 主控台提供的功能可協助您成功建立和提交 RFCs。

使用 RFC 清單頁面（主控台）

AMS 主控台 RFCs 清單頁面為您提供下列選項：

- 透過篩選條件進行進階 RFC 搜尋。如需相關資訊，請參閱[尋找 RFCs](#)。
- 尋找上次修改 RFC 的時間。此值代表上次變更 RFC 狀態的時間。

- 使用 RFC 主體檢視 RFC 詳細資訊。選擇此連結會開啟該 RFC 的詳細資訊頁面。
- 檢視 RFC 狀態。如需相關資訊，請參閱[了解 RFC 狀態碼](#)。

使用 RFC 快速建立（主控台）

使用 RFC 快速建立卡或清單資料表，或依分類選擇 RFCs 的變更類型。

如需詳細資訊，請參閱[建立 RFC](#)。

新增 RFC 通訊和附件（主控台）

您可以在 RFC 提交之後並在核准之前新增通訊；例如，當 RFC 處於「PendingApproval」狀態時。核准 RFC 之後（處於「排程」或「InProgress」的狀態），便無法新增通訊，因為它可以解釋為請求的變更。RFC 完成後（狀態為「已取消」、「已拒絕」、「成功」或「失敗」），雖然 RFC 關閉超過 30 天後，會再次啟用通訊。

Note

每個通訊限制為 5,000 個字元。

附件的限制：

- 每個通訊僅三個附件。
- 每個 RFC 限制 50 個附件。
- 每個附件的大小必須小於 5 MB。
- 只接受文字檔案，例如純文字 (.txt)、逗號分隔值 (.csv)、JSON (.json) 或 YAML (.yaml)。如果是 YAML 格式，則必須使用副檔名 連接檔案.yaml。

Note

禁止包含 XML 內容的文字檔案。如果您有要與 AMS 共用的 XML 內容，請使用服務請求。

- 檔案名稱限制為 255 個字元，只有數字、字母、空格、破折號 (-)、底線 (_) 和點 (.)。
- 目前不支援更新和刪除 RFC 上的附件。

若要將通訊和附件新增至 RFC，請遵循下列步驟：

1. 在 AMS 主控台的 RFC 詳細資訊頁面上，找到頁面底部的對應區段。

在任何通訊之前：

在一些通訊之後：

2. 若要新增通訊，請在回覆文字方塊中輸入訊息。若要連接與通訊相關的檔案，請選擇新增附件，然後選擇您想要的檔案。
3. 完成後，請選擇提交。

新的通訊以及附加檔案的連結會出現在 RFC 詳細資訊頁面上的通訊清單中。

設定 RFC 電子郵件通知（主控台）

AMS 主控台變更請求建立頁面可讓您選擇新增電子郵件地址，以接收 RFC 狀態變更的通知：

此外，您可以將通知的電子郵件地址新增至任何變更類型，例如：

```
aws amscm create-rfc --change-type-id <Change type ID>
                        --change-type-version 1.0 --title "TITLE"
                        --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}\""
```

在請求的 RFC 參數部分中，將類似的行 (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"`) 新增至任何變更類型內嵌或範本請求，而非參數部分。

了解常見的 RFC 參數

以下是您必須提交的 RFC 參數，以及 RFCs 中常用的參數：

- 變更類型資訊：ChangeTypeId 和 ChangeTypeVersion。錯誤變更類型 IDs 和版本編號的清單，請參閱[變更類型參考](#)。

使用 `query` 引數在 `CLI list-change-type-classification-summaries` 中執行，以縮小結果範圍。例如，縮小結果以變更 `Item` 名稱中包含「存取」的類型。

```
aws amscm list-change-type-classification-summaries --query
"ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

執行 `get-change-type-version` 並指定變更類型 ID。下列命令會取得 `ct-2tylseo8rxpsc` 的 CT 版本。

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxpsc
```

- 標題：RFC 的名稱；這會成為 AMS 主控台 RFC 清單中 RFC 的主體，您可以使用 `GetRfc` 命令和上的篩選條件進行搜尋 `Title`
- 排程：如果您想要排程 RFC，您必須包含 `RequestedStartTime` 和 `RequestedEndTime` 參數，或使用排程此變更主控台選項。對於 ASAP RFC（在核准後立即執行），使用 CLI 時，請保留 `RequestedStartTime` 和 `RequestedEndTime` null。使用主控台時，請接受 ASAP 選項。

如果遺漏 `RequestedStartTime`，RFC 會遭到拒絕。

- 佈建 CTs：執行參數或 `Parameters` 是佈建資源所需的特定設定。它們因 CT 而異。
- 非佈建 CTs：未佈建資源的 CTs，例如存取 CTs 或其他 | 其他，或刪除堆疊，具有最少的執行參數且沒有 `Parameters` 區塊。
- 有些 RFCs 還需要您指定 `TimeoutInMinutes`，或在 RFC 失敗之前，允許多少分鐘建立堆疊。對於長時間執行的 `UserData`，有效值為 60（分鐘）到 360。如果無法在超過 `TimeoutInMinutes` 之前完成執行，RFC 會失敗。不過，此設定不會延遲 RFC 的執行。
- 建立執行個體的 RFCs，例如 S3 儲存貯體或 ELB，通常提供結構描述，可讓您新增最多七個標籤（索引鍵/值對）。您可以使用部署 | 進階堆疊元件 | 標籤 | 建立變更類型 (`ct-3cx7we852p3af`) 提交 RFC，將更多標籤新增至 S3 儲存貯體。EC2、EFS、RDS 和多層 (HA 雙層和 HA 單層) 結構描述最多允許 50 個標籤。標籤是在結構描述 `ExecutionParameters` 的一部分中指定。提供標籤可能很有價值。如需詳細資訊，請參閱 [標記您的 Amazon EC2 資源](#)。

使用 AMS 主控台時，您必須開啟其他組態區域，才能新增標籤。

Tip

許多 CT 結構描述都有靠近結構描述頂端的 `Description` 和 `Name` 欄位。這些欄位用於命名堆疊或堆疊元件，而不會命名您正在建立的資源。有些結構描述提供參數來命名您正在建

立的資源，有些則不會。例如，建立 EC2 堆疊的 CT 結構描述不提供參數來命名 EC2 執行個體。若要這樣做，您必須建立索引鍵為 "Name" 的標籤，以及您想要名稱的值。如果您未建立此類標籤，您的 EC2 執行個體會顯示在 EC2 主控台中，但沒有名稱屬性。

使用 RFC AWS 區域選項

AMS API 和 CLI (amscm 和 amsskms) 端點位於 `us-east-1`。如果您與安全性聲明標記語言 (SAML) 聯合，則在加入時會為您提供指令碼，將您的 AWS 區域設定為 `us-east-1`。如果您使用 SAML，則不需要在發出命令時指定 `--region` 選項。如果您的 SAML 設定為使用 `us-east-1`，但您的帳戶不在該 AWS 區域中，則您必須在發出其他 AWS 命令時指定您的登入帳戶區域（例如 `aws s3`）。

Note

本指南中提供的大多數命令範例不包含 `--region` 選項。

註冊 RFC 每日電子郵件

您可以使用 RFC 摘要功能，註冊每日電子郵件，總結您帳戶在過去 24 小時內的 RFC 活動。RFC 摘要功能是一個簡化的程序，可減少您收到有關帳戶 RFCs 的電子郵件通知數量。RFC 摘要可能會降低您錯過待回應動作的可能性。

若要開啟 RFC 摘要功能，請聯絡您的 AMS Cloud Service Delivery Manager (CSDM)。CSDM 會訂閱您。您最多可以請求將 20 個電子郵件地址（或別名）包含在 RFC 摘要電子郵件清單中。目前的電子郵件排程固定為 09:00 UTC-8。

若要關閉 RFC 摘要功能，請聯絡您的 CSDM 並提出您的請求。

如果您未設定 RFC 摘要並希望收到有關 RFCs 通知，或者如果您想要 RFCs 摘要提供比 RFC 摘要更詳細的資訊，請使用變更管理系統來設定 CloudWatch Events 通知或每個個別 RFC 的電子郵件通知。如需設定 RFC 通知的資訊，請參閱 [RFC 狀態變更通知](#)。

RFC 摘要中包含的主題包括下列項目：

- 待客戶核准：列出處於 PendingApproval 狀態的 RFCs，等待您的核准
- 待客戶回覆：列出正在等待 RFCs 通訊回覆的 RFC
- 等待 AWS 核准或回覆：列出等待 AMS 回覆或核准的 RFCs

- 已完成：列出成功、失敗、已取消和已拒絕狀態RFCs

以下是 RFC 摘要範例：

什麼是變更類型？

變更類型是指 AWS Managed Services (AMS) 變更請求 (RFC) 執行並包含變更動作本身的動作，以及變更類型 – 手動與自動。AMS 有大量變更類型，其他 Amazon Web 服務不會使用。您可以在提交變更請求 (RFC) 以部署、管理或存取 資源時使用這些變更類型。

主題

- [自動化和手動 CTs](#)
- [CT 核准要求](#)
- [變更類型版本](#)
- [建立變更類型](#)
- [更新變更類型](#)
- [僅限內部的變更類型](#)
- [變更類型結構描述](#)
- [管理變更類型的許可](#)
- [從變更類型編輯敏感資訊](#)
- [使用查詢選項尋找變更類型](#)

自動化和手動 CTs

變更類型的限制條件是它們是自動還是手動，這是變更類型AutomationStatusId屬性，在 AMS 主控台中稱為執行模式。

自動化變更類型具有預期的結果和執行時間，並且通常在一小時內透過 AMS 自動化系統執行（這主要取決於 CT 正在佈建的資源）。手動變更類型並不常見，但會受到不同的處理，因為它們需要 AMS 運算子先對 RFC 採取行動，才能執行。有時這表示與 RFC 提交者通訊，因此手動變更類型需要不同的時間長度才能完成。

對於所有排程RFCs，未指定的結束時間會寫入為指定的時間RequestedStartTime加上所提交變更類型的ExpectedExecutionDurationInMinutes屬性。例如，如果

ExpectedExecutionDurationInMinutes 是 "60" (分鐘) , 且指定的 RequestedStartTime 是 2016-12-05T14:20:00Z(2016 年 12 月 5 日上午 4 : 20) , 則實際結束時間將設定為 2016 年 12 月 5 日上午 5 : 20。若要尋找ExpectedExecutionDurationInMinutes特定變更類型的 , 請執行此命令 :

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

執行模式 = 手動RFCs 必須在主控台中設定為在未來至少 24 小時執行。此警告不適用於 AMS API/CLI , 但請務必提前至少 8 小時排程手動 RFCs。

Note

使用「需要檢閱」CTs時 , AMS 建議您使用 ASAP 排程選項 (在主控台中選擇 ASAP , 在 API/CLI 中保留開始和結束時間空白) , 因為這些 CTs 需要 AMS 運算子來檢查 RFC , 並在核准和執行之前與您通訊。如果您排程這些 RFCs , 請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准 , 則會自動拒絕 RFC。

AMS 旨在四小時內回應手動 CT , 並會盡快對應 , 但實際執行 RFC 可能需要更長的時間。

如需手動且需要 AMS 檢閱CTs 清單 , 請參閱 主控台開發人員資源頁面上的變更類型 CSV 檔案。

YouTube 影片 : [如何尋找 AMS RFCs的自動變更類型 ?](#)

若要在 AMS 主控台中尋找 CT 的執行模式 , 您必須使用瀏覽變更類型搜尋選項。結果會顯示相符變更類型或變更類型的執行模式。

若要使用 AMS CLI 尋找AutomationStatus特定變更類型的 , 請執行此命令 :

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

您也可以在此 [AMS 變更類型參考中查詢變更類型](#) , 該參考提供有關所有 AMS 變更類型的資訊。

 Note

AMS API/CLI 目前不是 AWS API/CLI 的一部分。若要存取 AMS API/CLI，您可以透過 AMS 主控台下載 AMS 開發套件。

CT 核准要求

AMS CTs一律有兩個核准條件：AwsApprovalId 和 CustomerApprovalId，指出 RFC 是否需要 AMS 或您或任何人核准執行。

核准條件與執行模式有些相關；如需詳細資訊，請參閱 [自動化和手動 CTs](#)。

若要了解 CT 的核准條件，您可以查看 [AMS 變更類型參考](#)，或執行 [GetChangeTypeVersion](#)。兩者也會為您提供 CT AutomationStatusId或執行模式。

您可以使用 AMS 主控台或下列命令來核准 RFCs：

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 核准條件

如果 CT 核准條件為	它需要來自 的核准	及
AwsApprovalId: Required	AMS 變更類型系統、	無需採取任何動作。此條件是自動化 CTs 的典型條件。
AwsApprovalId: NotRequiredIfSubmitter	如果提交的 RFC 是針對其所提交的帳戶，則 AMS 變更類型系統不會有其他人，	無需採取任何動作。此條件適用於手動 CTs因為 AMS 運算子一律會檢閱它們。
CustomerApprovalId: NotRequired	AMS 變更類型系統、	如果 RFC 通過語法和參數檢查，則會自動核准。

如果 CT 核准條件為	它需要來自 的核准	及
CustomerApprovalId: Required	AMS 變更類型系統與您，	系統會傳送通知給您，您必須透過回應通知或執行 ApproveRfc 操作來明確核准 RFC。
CustomerApprovalId: NotRequiredIfSubmitter	如果您提交 RFC，則 AMS 變更類型系統不會有其他人。	如果 RFC 通過語法和參數檢查，則會自動核准。
緊急安全事件或修補程式	AMS	已自動核准並實作。

變更類型版本

變更類型會進行版本控制，並在對變更類型進行主要更新時變更版本。

使用 AMS 主控台選取變更類型之後，您可以選擇開啟其他組態區域並選取變更類型版本。您也可以 API/CLI 命令列指定變更類型版本。您可能會因為各種原因而想要這樣做，包括：

- 您知道您想要的更新變更類型版本必須符合您用來建立現在要更新之資源的建立變更類型版本。例如，您可能有一個使用 ELB 建立變更類型版本 1 建立的 Elastic Load Balancer (ELB) 執行個體。若要更新它，請選擇 ELB 更新第 1 版。
- 您想要使用的變更類型版本，其中包含與最新變更類型不同的選項。我們不建議這麼做，因為 AMS 更新變更類型主要基於安全考量，建議您一律選擇最新版本。

建立變更類型

建立變更類型會比對version-to-version與更新變更類型。也就是說，您用來佈建資源的變更類型版本必須符合稍後用來修改該資源的更新變更類型版本。例如，如果您使用建立 S3 儲存貯體變更類型 2.0 版建立 S3 儲存貯體，且稍後想要提交 RFC 來修改該 S3 儲存貯體，則您也必須使用更新 S3 儲存貯體變更類型 2.0 版，即使更新 S3 儲存貯體變更類型具有 3.0 版。

我們建議您保留在佈建具有建立變更類型的資源時所使用的變更類型 ID 和版本記錄，以防您稍後想要使用更新變更類型進行修改。

更新變更類型

AMS 提供更新變更類型，以更新使用建立變更類型建立的資源。更新變更類型必須與最初用於佈建資源 version-to-version 的建立變更類型相符。

建議您保留您在佈建資源時所使用的變更類型 ID 和版本記錄，以便輕鬆更新。

YouTube 影片：[如何使用更新 CTs來變更 AWS Managed Services \(AMS\) 帳戶中的資源？](#)

僅限內部的變更類型

您可以查看僅供內部使用的變更類型。這是為了讓您知道 AMS 可以或會採取哪些動作。如果您想要有僅供內部使用的變更類型，請提交服務請求。

例如，有一個管理 | 監控和通知 | CloudWatch 警示抑制 | 更新僅限內部的 CT。AMS 會使用它來部署基礎設施更新（例如修補），以關閉更新可能錯誤觸發的警示通知。提交此 CT 時，您會在 RFC 清單中注意到 CT 的 RFC。在 RFC 中部署的任何僅限內部 CT 都會顯示在 RFC 清單中。

變更類型結構描述

所有變更類型都會為資源的建立、修改或存取中的輸入提供 JSON 結構描述。結構描述提供參數及其描述，供您建立變更請求 (RFC)。

成功執行 RFC 會產生執行輸出。對於佈建 RFCs，執行輸出包含代表 CloudFormation 中堆疊的 "stack_id"，並且可以在 CloudFormation 主控台中搜尋。執行輸出有時包含所建立執行個體 ID 的輸出，該 ID 可用於在對應的 AWS 主控台中搜尋執行個體。例如，建立 ELB CT 執行輸出包含可在 CloudFormation 中搜尋的 "stack_id"，並輸出可在 Elastic Load Balancing Amazon EC2 主控台中搜尋的 key=ELB value=<stack-xxxx>。

讓我們檢查 CT 結構描述。這是 CodeDeploy Application Create 的結構描述，這是一個相當小的結構描述。有些結構描述的區域非常大Parameter。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy application
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
```

結構描述的第一部分提供 AMS 所請求變更類型的相關資訊。

```

        "description": "The reason for the request.",
        "type": "string",
        "minLength": 1,
        "maxLength": 500
    },
    "VpcId": {
        "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
        "type": "string",
        "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
        "description": "Must be stm-sft6rv000000000000",
        "type": "string",
        "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
        "description": "A name for the stack or stack component
;
        this becomes the Stack Name.",
        "type": "string",
        "minLength": 1,
        "maxLength": 255
    },
    "Tags": {
        "description": "Up to seven tags (key/value pairs) to
categorize the resource.",
        "type": "array",
        "items": {
            "type": "object",
            "properties": {
                "Key": {
                    "type": "string",
                    "minLength": 1,
                    "maxLength": 127
                },
                "Value": {
                    "type": "string",
                    "minLength": 1,
                    "maxLength": 255
                }
            }
        },
        "additionalProperties": false,
        "required": [

```

TimeoutInMinutes 參數可讓您指出執行變更類型的界限時間。對於長時間執行的 **UserData**，有效值為 60 到 360。

```

        "Key",
        "Value"
    ]
},
"minItems": 1,
"maxItems": 7
},
"TimeoutInMinutes": {
    "description": "The maximum amount of time, in minutes,
to
    allow for execution of the change. This will not prolong
execution,
    but the RFC fails if the change is not completed in the
specified time.
    Valid values are 60 up to 360, for long-running
UserData.",
    "type": "number",
    "minimum": 0,
    "maximum": 60
},
"Parameters": {
    "description": "Specifications for the stack.",
    "type": "object",
    "properties": {
        "CodeDeployApplicationName": {
            "description": "The name of an AWS CodeDeploy
application.",
            "type": "string",
            "minLength": 1,
            "maxLength": 100,
            "pattern": "^[a-zA-Z0-9._+=, @-]{1,100}$"
        }
    },
    "additionalProperties": false,
    "required": [
        "CodeDeployApplicationName"
    ]
}
},
"additionalProperties": false,

```

參數區段可讓您為要建立的資源或您要請求的動作指定設定。

「其他屬性」區段可讓您知道需要哪些參數，以及哪些參數是選用的。


```
"required": [
  "Description",
  "VpcId",
  "StackTemplateId",
  "Name",
  "TimeoutInMinutes",
  "Parameters"
]
```

Note

此結構描述最多允許七個標籤；不過，EC2、EFS、RDS 和多層建立結構描述最多允許 50 個標籤。

管理變更類型的許可

您可以使用自訂政策來限制哪些變更類型 (CTs) 可供不同的群組或使用者使用。

若要進一步了解如何執行此作業，請參閱 AMS 使用者指南一節[設定許可](#)。

從變更類型編輯敏感資訊

AMS 變更類型結構描述提供參數屬性，"metadata":"ams:sensitive":"true"用於包含敏感資訊的參數，例如密碼。設定此屬性時，提供的輸入會隱藏。請注意，您無法設定此參數屬性；不過，如果您使用 AMS 來建立變更類型，並具有您想要在輸入時隱藏的參數，您可以請求此參數。

使用查詢選項尋找變更類型

此範例示範如何使用 AMS 主控台來尋找您要提交之 RFC 的適當變更類型。

您可以使用 主控台或 API/CLI 來尋找變更類型 ID (CT) 或版本。有兩種方法：搜尋或選擇分類。對於這兩種選擇類型，您可以選擇最常使用、最近使用或按字母順序排序搜尋。

YouTube 影片：[如何使用 AWS Managed Services CLI 建立 RFC，以及在哪裡可以找到 CT 結構描述？](#)

在 AMS 主控台的 RFCs -> 建立 RFC 頁面上：

- 選取依變更類型瀏覽（預設值）時：

- 使用快速建立區域從 AMS 最熱門CTs 中選取。按一下標籤，隨即開啟執行 RFC 頁面，並自動為您填入主旨選項。視需要完成其餘選項，然後按一下執行以提交 RFC。
- 或者，向下捲動至所有變更類型區域，並開始在選項方塊中輸入 CT 名稱，您不需要具有確切或完整的變更類型名稱。您也可以輸入相關字詞，依變更類型 ID、分類或執行模式（自動或手動）搜尋 CT。

選取預設卡檢視後，相符的 CT 卡會在您輸入時顯示，選取卡片並按一下建立 RFC。選取資料表檢視後，選擇相關的 CT，然後按一下建立 RFC。這兩種方法都會開啟執行 RFC 頁面。

- 或者，若要探索變更類型選擇，請按一下頁面頂端的依類別選擇，以開啟一系列的下拉式選項方塊。
- 選擇類別、子類別、項目和操作。該變更類型的資訊方塊會顯示頁面底部的面板。
- 當您準備好時，請按 Enter，並顯示相符的變更類型清單。
- 從清單中選擇變更類型。該變更類型的資訊方塊會出現在頁面底部。
- 在您擁有正確的變更類型之後，請選擇建立 RFC。

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

Note

AMS API/CLI (`amscm` 和 `amsskms`) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

若要使用 AMS CM API 搜尋變更類型（請參閱 [ListChangeTypeClassificationSummaries](#)）或 CLI：

您可以使用篩選條件或查詢來搜尋。`ListChangeTypeClassificationSummaries` 操作具有 `Category`、`Item`、`Subcategory` 和的 [篩選條件](#) 選項 `Operation`，但值必須完全符合現有的值。若要在使用 CLI 時獲得更靈活的結果，您可以使用 `--query` 選項。

使用 AMS CM API/CLI 變更類型篩選

屬性	有效值	有效/預設條件	備註
ChangeTypeId	代表 ChangeTypeId 的任何字串（例如：ct-abc123xyz7890）	等於	如需變更類型 IDs，請參閱 變更類型參考 。 如需變更類型 IDs，請參閱尋找變更類型或 CSIO。
類別	任何自由格式文字	包含	不支援每個個別欄位中的規則運算式。不區分大小寫的搜尋
Subcategory			
項目			
作業			

1. 以下是列出變更類型分類的一些範例：

下列命令會列出所有變更類型類別。

```
aws amscm list-change-type-categories
```

下列命令會列出屬於指定類別的子類別。

```
aws amscm list-change-type-subcategories --category CATEGORY
```

下列命令會列出屬於指定類別和子類別的項目。

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. 以下是使用 CLI 查詢搜尋變更類型的一些範例：

下列命令會搜尋項目名稱中包含 "S3" 的 CT 分類摘要，並以資料表形式建立類別、子類別、項目、操作和變更類型 ID 的輸出。

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+
|               ListChangeTypeClassificationSummaries               |
+-----+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+-----+-----+
```

3. 然後，您可以使用變更類型 ID 來取得 CT 結構描述並檢查參數。下列命令會將結構描述輸出至名為 CreateS3Params.schema.json。

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

如需有關使用 CLI 查詢的資訊，請參閱[如何使用 --query Option 篩選輸出](#)和查詢語言參考[JMESPath Specification](#)。

4. 在您擁有變更類型 ID 之後，建議您驗證變更類型的版本，以確保它是最新版本。使用此命令來尋找指定變更類型的版本：

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

若要尋找AutomationStatus特定變更類型的，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
  query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

若要尋找ExpectedExecutionDurationInMinutes特定變更類型的，請執行此命令：

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
  --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

針對 AMS 中的 RFC 錯誤進行故障診斷

許多 AMS 佈建 RFC 失敗可以透過 CloudFormation 文件進行調查。請參閱[對 AWS CloudFormation 進行故障診斷：對錯誤進行故障診斷](#)

以下各節提供其他疑難排解建議。

AMS 中的「管理」RFC 錯誤

AMS「管理」類別變更類型 (CTs) 可讓您請求存取資源，以及管理現有的資源。本節說明一些常見問題。

RFC 存取錯誤

- 請確定您在 RFC 中指定的使用者名稱和 FQDN 正確且存在於網域中。如需尋找 FQDN 的說明，請參閱[尋找 FQDN](#)。
- 請確定您為存取指定的堆疊 ID 是 EC2-related 堆疊。ELB 和 Amazon Simple Storage Service (S3) 等堆疊不是存取 RFCs 的候選項目，而是使用您的唯讀存取角色來存取這些堆疊資源。如需尋找堆疊 ID 的說明，請參閱[尋找堆疊 IDs](#)
- 請確定您提供的堆疊 ID 正確且屬於相關帳戶。

如需其他存取 RFC 失敗的說明，請參閱[存取管理](#)。

YouTube 影片：[如何正確提出變更請求 \(RFC\)，以避免拒絕和失敗？](#)

RFC（手動）CT 排程錯誤

大多數變更類型是 ExecutionMode=Automated，但有些是 ExecutionMode=Manual，這會影響您應該如何排程它們以避免 RFC 失敗。

如果您使用 AMS 主控台建立 RFCs 則使用 ExecutionMode=Manual 的排程 RFC 必須設定為未來至少 24 小時執行。此警告不適用於 AMS API/CLI，但請務必提前至少 8 小時排程手動 RFCs。

AMS 旨在四小時內回應手動 CT，並會盡快對應，但實際執行 RFC 可能需要更長的時間。

搭配手動更新 CTs 使用 RFCs

當您要更新的堆疊類型有更新變更類型時，AMS Operations 會拒絕管理 | 其他 | 其他 RFCs 更新堆疊。

RFC 刪除堆疊錯誤

RFC 刪除堆疊失敗：如果您使用管理 | 標準堆疊 | 堆疊 | 刪除 CT，您會在 AWS CloudFormation 主控台中看到具有 AMS 堆疊名稱之堆疊的詳細事件。您可以對照 AMS 主控台內的堆疊名稱來檢查堆疊。AWS CloudFormation 主控台提供有關失敗原因的更多詳細資訊。

在刪除堆疊之前，您應該考慮堆疊的建立方式。如果您使用 AMS CT 建立堆疊，但未新增或編輯堆疊資源，則可以預期刪除堆疊，而不會發生問題。不過，建議您先從堆疊移除任何手動新增的資源，再提交刪除堆疊 RFC。例如，如果您使用完整堆疊 CT (HA Two Tier) 建立堆疊，它會包含安全群組 - SG1。如果您接著使用 AMS 建立另一個安全群組 - SG2SG2，並在建立為完整堆疊一部分的 SG1 中參考新的 SG2，然後使用刪除堆疊 CT 刪除堆疊，則 SG1 不會刪除，因為它由 SG2 參考。

Important

刪除堆疊可能會產生不想要和非預期的後果。基於此原因，AMS 偏好 **not** 代表客戶刪除堆疊或堆疊資源。請注意，AMS 只會代表您刪除無法使用適當的自動變更類型刪除的資源（透過提交的管理 | 其他 | 其他 | 更新變更類型）。其他考量

- 如果資源已啟用「刪除保護」，則如果您提交管理 | 其他 | 其他 | 更新變更類型，且刪除保護移除後，您可以使用自動 CT 來刪除該資源，則 AMS 可協助解除封鎖。
- 如果堆疊中有多個資源，而且您只想要刪除一部分的堆疊資源，請使用 CloudFormation 更新變更類型（請參閱 [CloudFormation 擷取堆疊：更新](#)）。您也可以提交管理 | 其他 | 其他 | 更新變更類型，如有需要，AMS 工程師可協助您製作變更集。
- 如果您提交管理 | 其他 | 其他 | 更新以解決偏離（在 AWS CloudFormation CloudFormation Service 支援的範圍內），並提供 ChangeSet，然後您可以使用自動化 CT、管理/自訂堆疊/堆疊從 CloudFormation 範本/核准變更集和更新來驗證和執行，則 AMS 可以提供協助。

AMS 會維護上述限制，以協助確保沒有非預期或非預期的資源刪除。

如需詳細資訊，請參閱 [AWS CloudFormation 故障診斷：刪除堆疊失敗](#)。

RFC 更新 DNS 錯誤

更新 DNS 託管區域的多個 RFCs 可能會失敗，有些可能沒有原因。同時建立多個 RFCs 以更新 DNS 託管區域（私有或公有）可能會導致某些 RFCs 因為它們同時嘗試更新相同的堆疊。AMS 變更管理拒絕或失敗無法更新堆疊的 RFCs，因為堆疊已由另一個 RFC 更新。AMS 建議您一次建立一個 RFC，並等待 RFC 成功，然後再為相同的堆疊提出新的 RFC。

RFC IAM 實體錯誤

AMS 會將多個預設 IAM 角色和設定檔佈建至專為滿足您的需求而設計的 AMS 帳戶。不過，您可能需要偶爾請求額外的 IAM 資源。

提交請求自訂 IAM 資源 RFCs 程序遵循手動 RFCs 的標準工作流程，但核准程序也包含安全審查，以確保採取適當的安全控制。因此，程序通常需要比其他手動 RFCs 更長的時間。若要縮短這些 RFCs 的週期時間，請遵循下列準則。

如需 IAM 審核的含義及其如何映射至技術標準和風險接受程序的詳細資訊，請參閱 [了解 RFC 安全性審查](#)。

常見的 IAM 資源請求：

- 如果您要求與主要雲端相容應用程式相關的政策，例如 CloudEndure，請參閱 AMS 預先核准的 IAM CloudEndure 政策：解壓縮 [WIGs 雲端持久性登陸區域範例](#) 檔案並開啟 `customer_cloud_endure_policy.json`

Note

如果您想要更寬鬆的政策，請與您的 CloudArchitect/CSDM 討論您的需求，並視需要在提交實作政策的 RFC 之前取得 AMS 安全審查和簽署。

- 如果您想要修改 AMS 預設在帳戶中部署的資源，建議您要求修改後的資源複本，而不是變更現有的資源複本。
- 如果您要請求人類使用者的許可（而不是將許可連接到使用者），請將許可連接到角色，然後授予使用者擔任該角色的許可。如需執行此操作的詳細資訊，請參閱 [暫時 AMS Advanced 主控台存取](#)。
- 如果您需要臨時遷移或工作流程的特殊許可，請在請求中提供這些許可的結束日期。
- 如果您已與安全團隊討論請求的主旨，請盡可能向 CSDM 提供其核准的證據，並提供詳細資訊。

如果 AMS 拒絕 IAM RFC，我們會提供拒絕的明確原因。例如，我們可能會拒絕 IAM 政策建立請求，並解釋政策的不適當之處。在這種情況下，您可以進行已識別的變更並重新提交請求。如果需要進一步釐清請求的狀態，請提交服務請求，或聯絡您的 CSDM。

下列清單說明 AMS 檢閱 IAM RFCs 時嘗試緩解的典型風險。如果您的 IAM RFC 有任何這些風險，可能會導致 RFC 遭到拒絕。如果您需要例外狀況，AMS 會向您的安全團隊請求核准。若要尋求此類例外狀況，請與 CSDM 協調。

 Note

AMS 可能會基於任何原因拒絕對帳戶內部 IAM 資源的任何變更。如需有關 RFC 拒絕的疑慮，請透過服務請求聯絡 AMS Operations，或聯絡您的 CSDM。

- 權限提升，例如允許您修改自己的許可，或修改帳戶中其他資源許可的許可。範例：
 - 使用 `iam:PassRole` 搭配另一個更特殊權限的角色。
 - 從角色或使用者連接/提取 IAM 政策的許可。
 - 帳戶中 IAM 政策的修改。
 - 在管理基礎設施環境中進行 API 呼叫的能力。
- 修改為您提供 AMS 服務所需的資源或應用程式的許可。範例：
 - 修改 AMS 基礎設施，例如堡壘、管理主機或 EPS 基礎設施。
 - 刪除日誌管理 AWS Lambda 函數或日誌串流。
 - 預設 CloudTrail 監控應用程式的刪除或修改。
 - Directory Services Active Directory (AD) 的修改。
 - 停用 CloudWatch (CW) 警示。
 - 修改帳戶中部署做為登陸區域一部分的主體、政策和命名空間。
- 在最佳實務之外部署基礎設施，例如允許在危及資訊安全的狀態下建立基礎設施的許可。範例：
 - 建立公有或未加密的 S3 儲存貯體或公開共用 EBS 磁碟區。
 - 公有 IP 地址的佈建。
 - 修改安全群組以允許廣泛存取。
- 過於廣泛的許可，可能導致應用程式影響，例如可能導致基礎設施和帳戶中應用程式的資料遺失、完整性遺失、不當組態或服務中斷的許可。範例：
 - 透過 `ModifyNetworkInterfaceAttribute` 或等 APIs 停用或重新導向網路流量 `UpdateRouteTable`。
 - 透過從受管主機分離磁碟區來停用受管基礎設施。
- 不屬於 AMS 服務描述且 AMS 不支援的服務許可。

AMS 服務描述中未列出的服務無法在 AMS 帳戶中使用。若要請求支援某項功能或服務，請聯絡您的 CSDM。

- ~~不符合您所述目標的許可，因為這些許可太慷慨或過於保守，或是套用至錯誤的資源。範例：~~

- 請求對具有強制 KMS 加密的 S3 儲存貯體 `s3:PutObject` 的許可，而沒有相關金鑰的 `KMS:Encrypt` 許可。
- 與帳戶中不存在的資源相關的許可。
- IAM RFCs，其中 RFC 的描述似乎不符合請求。

「部署」RFC 錯誤

AMS「部署」類別變更類型 CTs) 可讓您請求將各種 AMS 支援的資源新增至您的帳戶。

大多數建立資源的 AMS CTs 都是以 AWS CloudFormation 範本為基礎。身為客戶，您可以唯讀存取所有 AWS 服務 AWS CloudFormation，包括，您可以使用 AWS CloudFormation 主控台，根據堆疊描述快速識別 AWS CloudFormation 代表您堆疊的堆疊。失敗的堆疊可能處於 `DELETE_COMPLETE` 狀態。識別 AWS CloudFormation 堆疊後，事件會顯示無法建立的特定資源，以及原因。

使用 CloudFormation 文件進行疑難排解

大多數 AMS 佈建 RFCs 使用 CloudFormation 範本，該文件有助於進行故障診斷。請參閱該 AWS CloudFormation 範本的文件：

- 建立應用程式負載平衡器失敗：[AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- 建立 Auto Scaling 群組：[AWS::AutoScaling::AutoScalingGroup \(Auto Scaling 群組\)](#)
- 建立 memcached 快取：[AWS::ElastiCache::CacheCluster \(快取叢集\)](#)
- 建立 Redis 快取：[AWS::ElastiCache::CacheCluster \(快取叢集\)](#)
- 建立 DNS 託管區域（與建立 DNS 私有/公有搭配使用）：[AWS::Route53::HostedZone \(R53 託管區域\)](#)
- 建立 DNS 紀錄集（與建立 DNS 私有/公有搭配使用）：[AWS::Route53::RecordSet \(資源紀錄集\)](#)
- 建立 EC2 堆疊：[AWS::EC2::Instance \(彈性運算雲端\)](#)
- 建立彈性檔案系統 (EFS)：[AWS::EFS::FileSystem \(彈性檔案系統\)](#)
- Create Load Balancer：[AWS::ElasticLoadBalancing::LoadBalancer \(Elastic Load Balancer\)](#)
- 建立 RDS 資料庫：[AWS::RDS::DBInstance \(關聯式資料庫\)](#)
- 建立 Amazon S3：[AWS::S3::Bucket \(簡易儲存服務\)](#)
- 建立佇列：[AWS::SQS::Queue \(簡易佇列服務\)](#)

RFC 建立 AMIs 錯誤

Amazon Machine Image (AMI) 是一種範本，其中包含軟體組態 (例如作業系統、應用程式伺服器 and 應用程式)。您可從 AMI 啟動執行個體，執行個體是 AMI 的複本，在雲端中以虛擬伺服器的形式執行。AMIs 非常有用，而且需要建立 EC2 執行個體或 Auto Scaling 群組；不過，您必須遵守一些需求：

- 您為指定的執行個體 `Ec2InstanceId` 必須處於停止狀態，RFC 才能成功。請勿將 Auto Scaling 群組 (ASG) 執行個體用於此參數，因為 ASG 會終止已停止的執行個體。
- 若要建立 AMS Amazon Machine Image (AMI)，您必須從 AMS 執行個體開始。在您可以使用執行個體來建立 AMI 之前，您必須先確保其已停止並從其網域中退出，以做好準備。如需詳細資訊，請參閱 [使用 Sysprep 建立標準 Amazon Machine Image](#)
- 您為新 AMI 指定的名稱在帳戶中必須是唯一的，否則 RFC 失敗。如何執行此作業，請參閱 [AMI | Create](#)，如需詳細資訊，請參閱 [AWS AMI Design](#)。

Note

如需準備建立 AMI 的詳細資訊，請參閱 [AMI | Create](#)。

建立 EC2s 或 ASGs 錯誤的 RFCs

對於具有逾時的 EC2 或 ASG 失敗，AMS 建議您確認使用的 AMI 是否已自訂。如果是，請參閱本指南中包含的 AMI 建立步驟（請參閱 [AMI | Create](#)），以確保正確建立 AMI。建立自訂 AMI 時的常見錯誤未遵循指南中的步驟來重新命名或叫用 Sysprep。

建立 RDS RFCs

Amazon Relational Database Service (RDS) 失敗可能有許多不同的原因，因為您可以在建立 RDS 時使用許多不同的引擎，而且每個引擎都有自己的需求和限制。嘗試建立 AMS RDS 堆疊之前，請仔細檢閱 AWS RDS 參數值，請參閱 [CreateDBInstance](#)。

若要進一步了解 Amazon RDS，包括大小建議，請參閱 [Amazon Relational Database Service 文件](#)。

建立 Amazon S3s 錯誤的 RFCs

建立 S3 儲存貯體時，一個常見的錯誤不是使用儲存貯體的唯一名稱。如果您提交的名稱與先前提交的名稱相同的 S3 儲存貯體建立 CT，將會失敗，因為 S3 儲存貯體已存在於該 `BucketName`。這將在 AWS CloudFormation 主控台中詳細說明，您將在其中看到堆疊事件顯示儲存貯體名稱已在使用中。

RFC 驗證與執行錯誤

RFC 失敗和相關訊息在所選 RFC 的 AMS 主控台 RFC 詳細資訊頁面上的輸出訊息中不同：

- 驗證失敗原因僅適用於狀態欄位
- 執行失敗原因可在執行輸出和狀態欄位中取得。

RFC 錯誤訊息

當您遇到下列所列變更類型 (CTs) 的錯誤時，您可以使用這些解決方案來協助您尋找問題來源並加以修正。

```
{"errorMessage": "An error has occurred during RFC execution. We are investigating the issue.", "errorType": "InternalError"}
```

如果您在參考下列疑難排解選項後需要進一步協助，請透過 RFC 通訊聯絡 AMS 或建立服務請求。如需詳細資訊，請參閱 [RFC 通訊和連接（主控台）](#) 和 [在 AMS 中建立服務請求](#)。

工作負載擷取 (WIGS) 錯誤

Note

您可以下載適用於 Windows 和 Linux 的驗證工具，並直接在內部部署伺服器以及 AWS 中的 EC2 執行個體上執行。這些可透過 AMS 進階應用程式開發人員指南的 [遷移工作負載：Linux 擷取前驗證](#) 和 [遷移工作負載：Windows 擷取前驗證](#) 找到。

- 確定 EC2 執行個體存在於目標 AMS 帳戶中。例如，如果您已將 AMI 從非 AMS 帳戶共用到 AMS 帳戶，您必須先使用共用 AMI 在 AMS 帳戶中建立 EC2 執行個體，才能提交工作負載擷取 RFC。
- 檢查連接至執行個體的安全群組是否允許輸出流量。SSM 代理程式需要能夠連線到其公有端點。
- 檢查執行個體是否具有與 SSM 代理程式連線的正確許可。這些許可隨附於 customer-mc-ec2-instance-profile，您可以在 EC2 主控台中檢查此項目：

EC2 執行個體堆疊停止錯誤

- 檢查執行個體是否已處於已停止或終止狀態。

- 如果 EC2 執行個體在線上且您看到 `InternalError` 錯誤，請提交服務請求讓 AMS 進行調查。
- 請注意，您無法使用變更類型管理 | 進階堆疊元件 | EC2 執行個體堆疊 | 停止 `ct-3mvvt2zkyvej` 來停止 Auto Scaling 群組 (ASG) 執行個體。如果您需要停止 ASG 執行個體，請提交服務請求。

EC2 執行個體堆疊建立錯誤

`InternalError` 訊息來自 CloudFormation；`CREATION_FAILED` 狀態原因。您可以依照下列步驟，在 CloudWatch 堆疊事件中找到堆疊失敗的詳細資訊：

- 在 AWS 管理主控台中，您可以在建立、更新或刪除堆疊時檢視堆疊事件的清單。從這個清單中找到故障的事件，然後檢視該事件的狀態原因。

狀態原因可能包含來自 AWS CloudFormation 或特定服務的錯誤訊息，可協助您了解問題。

- 如需檢視堆疊事件的詳細資訊，請參閱 [AWS 管理主控台上的檢視 AWS CloudFormation 堆疊資料和資源](#)。

EC2 執行個體磁碟區還原錯誤

當 EC2 執行個體磁碟區還原失敗時，AMS 會建立內部故障診斷 RFC。這是因為 EC2 執行個體磁碟區還原是災難復原 (DR) 的重要部分，而 AMS 會自動為您建立此內部故障診斷 RFC。

建立內部故障診斷 RFC 時，會顯示橫幅，為您提供 RFC 的連結。此內部故障診斷 RFC 可讓您更清楚了解 RFC 失敗，而不是提交導致相同錯誤的重試 RFCs，或讓您針對此失敗手動聯絡 AMS，您可以追蹤變更並知道 AMS 正在處理失敗。這也減少了其變更 `time-to-recovery` (TTR) 指標，因為 AMS Operators 會主動處理 RFC 失敗，而不是等待您的請求。

如何取得 RFC 的協助

您可以聯絡 AMS 來識別失敗的根本原因。AMS 營業時間為 24 小時，全年無休。

AMS 提供多種管道，供您尋求協助或提出服務請求。

- 若要要求資訊或建議，或存取 AMS 受管 IT 服務，或從 AMS 請求其他服務，請使用 AMS 主控台並提交服務請求。如需詳細資訊，請參閱 [建立服務請求](#)。如需 AMS 服務請求的一般資訊，請參閱 [服務請求管理](#)。
- 若要報告影響受管環境的 AWS 或 AMS 服務效能問題，請使用 AMS 主控台並提交事件報告。如需詳細資訊，請參閱 [報告事件](#)。如需 AMS 事件管理的一般資訊，請參閱 [事件回應](#)。
- 有關您或您的資源或應用程式如何使用 AMS 的特定問題，或要呈報事件，請傳送電子郵件至下列一個或多個：

1. 首先，如果您不滿意服務請求或事件報告回應，請傳送電子郵件給 CSDM：ams-csdm@amazon.com
2. 接下來，如果需要呈報，您可以傳送電子郵件給 AMS Operations Manager（但您的 CSDM 可能會這樣做）：ams-opsmanager@amazon.com
3. 進一步呈報將向 AMS Director 呈報：ams-director@amazon.com
4. 最後，您可以隨時聯絡 AMS VP：ams-vp@amazon.com

AMS 中的直接變更模式

主題

- [直接變更模式入門](#)
- [安全與合規](#)
- [直接變更模式中的變更管理](#)
- [使用直接變更模式建立堆疊](#)
- [直接變更模式使用案例](#)

AWS Managed Services (AMS) 直接變更模式 (DCM) 透過提供 AMS Advanced Plus 和 Premium 帳戶的原生 AWS 存取權來佈建和更新 AWS 資源，以延伸 AMS 進階變更管理。使用 DCM 時，您可以選擇使用原生 AWS API（主控台或 CLI/SDK）或 AMS 進階變更管理變更請求 (RFCs)，而且在任何一種情況下，AMS 都完全支援資源和變更，包括監控、修補程式、備份、事件回應管理。透過 DCM 佈建的資源會在 AMS 服務知識管理系統 (SKMS) 中註冊、加入 AMS 受管 Active Directory 網域（如適用），並執行 AMS 管理代理程式。使用現有的工具（例如 CloudFormation、AWS SDK 和 CDK）來開發和部署 AMS 受管 CloudFormation 堆疊。

Note

直接變更模式不會移除 AMS 變更管理 RFCs。您可以使用 DCM 完整存取 AMS RFCs。

[觀看 Akash 的影片以進一步了解 \(6 : 30\)](#)

直接變更模式入門

首先檢查先決條件，然後在符合資格的 AMS Advanced 帳戶中提交變更請求 (RFC)。

1. 確認您要與 DCM 搭配使用的帳戶符合需求：

- 帳戶為 AMS Advanced Plus 或 Premium。
- 帳戶未啟用 Service Catalog。我們目前不支援同時將帳戶加入 DCM 和服務目錄。如果您已加入 Service Catalog，但對 DCM 感興趣，請與您的雲端服務交付管理員 (CSDM) 討論您的需求。如果您決定從 Service Catalog 切換到 DCM、離機 Service Catalog，若要這樣做，請在下面的變更請求中加入 ask。如需 AMS 中 Service Catalog 的詳細資訊，請參閱 [AMS 和服務目錄](#)。

2. 使用 管理 | 受管帳戶 | 直接變更模式 | 啟用變更類型 (ct-3rd4781c2nnhp) 提交變更請求 (RFC)。如需逐步解說範例，請參閱[直接變更模式 | 啟用](#)。

處理 CT 之後，預先定義的 IAM 角色 `AWSManagedServicesCloudFormationAdminRole` 和 `AWSManagedServicesUpdateRole` 會在指定的帳戶中佈建。

3. 使用內部聯合程序，將適當的角色指派給需要 DCM 存取的使用者。

Note

您可以指定任意數量的 `SAMLIdentityProviders`、AWS Services 和 IAM 實體（角色、使用者等）來擔任角色。您必須提供至少一個：`SAMLIdentityProviderARNs`、`IAMEntityARNs` 或 `AWSServicePrincipals`。如需詳細資訊，請洽詢您公司的 IAM 部門或 AMS 雲端架構師 (CA)。

直接變更模式 IAM 角色和政策

在帳戶中啟用直接變更模式時，會部署這些新的 IAM 實體：

`AWSManagedServicesCloudFormationAdminRole`：此角色會授予 CloudFormation 主控台的存取權、建立和更新 CloudFormation 堆疊、檢視偏離報告，以及建立和執行 CloudFormation ChangeSets。存取此角色是透過 SAML 供應商管理。

部署並連接到角色 `AWSManagedServicesCloudFormationAdminRole` 的受管政策如下：

- AMS 進階多帳戶登陸區域 (MALZ) 應用程式帳戶
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`

- 此政策代表授予的許可AWSManagedServicesCloudFormationAdminRole。您和合作夥伴使用此政策來授予帳戶中現有角色的存取權，並允許該角色啟動和更新帳戶中的 CloudFormation 堆疊。這可能需要額外的 AMS 服務控制政策 (SCP) 更新，以允許其他 IAM 實體啟動 CloudFormation 堆疊。
- AMS 進階單一帳戶登陸區域 (SALZ) 帳戶
 - AWSManagedServices_CloudFormationAdminPolicy1
 - AWSManagedServices_CloudFormationAdminPolicy2
 - cdk-legacy-mode-s3-access 【內嵌政策】
 - AWS ReadOnlyAccess 政策

AWSManagedServicesUpdateRole：此角色會授予下游 AWS 服務 APIs 的限制存取權。該角色部署的受管政策提供變動和非變動 API 操作，但通常限制變動操作（例如 Create/Delete/PUT）對某些服務，例如 IAM、KMS、GuardDuty、VPC、AMS 基礎設施資源和組態等。此角色的存取是透過 SAML 供應商管理。

部署並連接到角色AWSManagedServicesUpdateRole的受管政策包括：

- AMS 進階多帳戶登陸區域應用程式帳戶
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyPolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2AndRDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS 進階單一帳戶登陸區域帳戶
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2AndRDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
 - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

除此之外，受管政策AWSManagedServicesUpdateRole角色還ViewOnlyAccess連接了 AWS 受管政策。

安全與合規

安全與合規是 AMS Advanced 與身為客戶的您共同的責任。AMS Advanced Direct Change 模式不會變更此共同責任。

直接變更模式中的安全性

AMS Advanced 提供具有規範登陸區域、變更管理系統和存取管理的額外值。使用直接變更模式時，此責任模型不會變更。不過，您應該知道其他風險。

直接變更模式「更新」角色（請參閱[直接變更模式 IAM 角色和政策](#)）提供提升的許可，允許可存取該角色的實體變更帳戶中 AMS 支援服務的基礎設施資源。隨著許可提高，根據資源、服務和動作，存在各種風險，尤其是在由於監督、錯誤或未能遵守內部程序和控制架構而導致不正確的變更的情況下。

根據 AMS 技術標準，已識別下列風險並提出建議，如下所示。有關 AMS 技術標準的詳細資訊可透過取得 AWS Artifact。若要存取 AWS Artifact，請聯絡您的 CSDM 以取得指示，或前往 [入門 AWS Artifact](#)。

AMS-STD-001：標記

標準	是否會中斷	風險	建議
所有 AMS 擁有的資源都必須具有下列鍵值對 除了上述標籤之外，所有 AMS 擁有的標籤都必須具有字首，例如 AMS*或MC*upper/lower/mix大小寫。	是。CloudFormation、CloudTrail、EFS、OpenSearch、CloudWatch Logs、SQS、SSM、標記 api 的中斷 - 因為這些服務不支援限制 AMS 命名空間標記aws:TagsKey 的條件。 下表 AMS-STD-003 中提供的標準說明您可以變更 AppId、Environment 和 AppName，但不能變更 AMS 擁有的資	AMS 資源的不正確標記可能會對 AMS 端的資源的報告、提醒和修補操作產生不利影響。	必須重新分配存取權，才能對 AMS 團隊以外的任何人對 AMS 預設標記要求進行任何變更。

標準	是否會中斷	風險	建議
	源。無法透過 IAM 許可達成。		
不得根據您的變更請求刪除 AMS 擁有的堆疊上的任何標籤。	是。CloudFormation 不支援限制 AMS 命名空間標籤aws:TagsKey 的條件。		
不允許您在基礎設施中使用 AMS 標籤命名慣例，如下表 AMS-STD-002 所述。	是。中斷 CloudFormation、CloudTrail、Amazon Elastic File System (EFS)、OpenSearch、CloudWatch Logs、Amazon Simple Queue Service (SQS)、Amazon EC2 Systems Manager (SSM)、標記 API；這些服務不支援限制 AMS 命名空間標記aws:TagsKey 的條件。		

AMS-STD-002：身分與存取管理 (IAM)

標準	是否會中斷	風險	建議
4.7 不允許繞過變更管理程序 (RFC) 的動作，例如啟動或停止執行個體、建立 S3 儲存貯體或 RDS 執行個體等。只要在指派角色的邊界內執行動作。	是。自助服務動作的目的可讓您執行繞過 AMS RFC 系統的動作。	安全存取模型是 AMS 的核心技術面向，而主控台或程式設計存取的 IAM 使用者會規避此存取控制。AMS 變更管理不會監控 IAM 使用者存	IAM 使用者應該有時限限制，並根據最低權限和need-to-know 授予許可。

標準	是否會中斷	風險	建議
作，開發人員模式帳戶和自助式佈建模式服務 (SSPS) 就會豁免。		取權。存取只會記錄在 CloudTrail 中。	

AMS-STD-003：網路安全

標準	是否會中斷	風險	建議
S2. EC2 執行個體上的彈性 IP 只能與正式的風險接受協議或內部團隊的有效使用案例搭配使用。	是。自助服務動作可讓您關聯和取消關聯彈性 IP 地址 (EIP)。	將彈性 IP 新增至執行個體會公開至網際網路。這會增加資訊公開和未經授權的活動的風險。	透過安全群組封鎖對該執行個體的任何不必要的流量，並確認您的安全群組已與執行個體連接，以確保只允許基於業務原因而需要的流量。
S14. 您可以允許屬於相同客戶的帳戶之間的 VPC 對等互連和端點連線。	是。無法透過 IAM 政策進行。	離開帳戶界限後，不會監控離開您 AMS 帳戶的流量。	我們建議僅與您擁有的 AMS 帳戶進行對等互連。如果您的使用案例需要，請使用安全群組和路由表來限制哪些流量範圍、資源和類型可以透過相關連線輸出。
AMS 基礎 AMIs 可以在 AMS 受管和未受管帳戶之間共用，只要我們可以驗證它們是否屬於同一個 AWS 組織即可。		AMIs 可能包含敏感資料，而且可能會公開給非預期的帳戶。	僅與組織擁有的帳戶共用 AMIs，或在組織外部共用之前驗證使用案例和帳戶資訊。

AMS-STD-007：記錄

標準	是否會中斷	風險	建議
19. 任何日誌都可以從一個 AMS 帳戶轉送到相同客戶的另一個 AMS 帳戶。			
20. 只有在非 AMS 帳戶由相同 AMS 客戶擁有（透過確認他們位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱和 PAYER 連結帳戶相符）時，才能使用內部工具，從 AMS 轉送任何日誌到非 AMS 帳戶。	是。無法透過 IAM 政策實現客戶日誌的潛在不安全，因為無法驗證同一組織中的客戶帳戶。	日誌可能包含敏感資料，而且可能會公開給非預期的帳戶。	僅與 AWS 組織管理的帳戶共用日誌，或在組織外部共用之前驗證使用案例和帳戶資訊。我們可以透過多種方式驗證，請洽詢您的雲端服務交付管理員 (CSDM)。

與您的內部授權和身分驗證團隊合作，相應地控制直接變更模式角色的許可。

直接變更模式下的合規

直接變更模式與生產和非生產工作負載相容。您有責任確保遵守任何合規標準（例如 PHI、HIPAA、PCI），並確保使用直接變更模式符合您的內部控制架構和標準。

直接變更模式中的變更管理

變更管理是 AMS Advanced 用來實作變更請求的程序。變更請求 (RFC) 是由您或 AMS Advanced 透過 AMS Advanced 界面建立的請求，用於對您的受管環境進行變更，並包含特定操作的 AMS Advanced 變更類型 (CT) ID。如需詳細資訊，請參閱[變更管理](#)。

Note

直接變更模式不會移除 AMS 變更管理 RFCs，您仍然可以使用 DCM 完整存取 AMS RFCs。

AMS 直接變更模式 (DCM) 透過提供 AMS Advanced Plus 和 Premium 帳戶的原生 AWS 存取權來佈建和更新 AWS 資源，以擴展 AMS 進階變更管理。已透過 IAM 角色授予直接變更模式許可的使用者，可以使用原生 AWS API 存取來佈建和變更其 AMS Advanced 帳戶中的資源。使用者仍然可以使用相同的 IAM 角色來使用 AMS 進階變更管理 RFCs。在這兩種情況下，AMS 都完全支援資源和變更，包括監控、修補、備份、事件回應管理。在這些帳戶中沒有適當角色的使用者，必須使用 AMS 進階變更管理 RFC 程序進行變更。

變更管理使用案例

基於安全考量，AMS Advanced 中的某些變更只能透過變更管理請求 (RFC) 程序來完成。AWSManagedServicesCloudFormationAdminRole 僅限於透過 CloudFormation (CFN) 採取的動作。如需如何透過 DCM 建立堆疊的詳細資訊，請參閱[使用直接變更模式建立堆疊](#)。AWSManagedServicesUpdateRole 受限於下列動作。

如需每個變更類型的範例逐步解說，包括管理 | 受管帳戶 | 直接變更模式 | 啟用 (ct-3rd4781c2nnhp) 變更類型，請參閱 AMS 進階變更類型參考[依分類變更](#)類型一節中相關變更類型的「其他資訊」一節。

服務	動作
AWS Key Management Service (AWS KMS)	更新
AWS Certificate Manager	建立
AWS Identity and Access Management (IAM)	任何
AWS VPN	任何
AMS 資源排程器	
AWS Backup	建立備份計畫
AMS 工作負載擷取 (WIGs)	任何
AMS 輸出篩選 (受管 Palo Alto)	
AMS Advanced MALZ 帳戶變更	
Amazon GuardDuty	任何
AMS 進階堆疊存取	

服務	動作
Amazon Elastic Block Store (EBS) 磁碟區	刪除
Amazon Elastic Block Store (EBS) 預設加密	啟用預設加密
Amazon Elastic Compute Cloud (Amazon EC2)	變更主機名稱
Amazon Machine Image (AMI)	刪除、共用
Amazon EC2 安全群組	任何
AMS 進階 SSPS	
AWS Managed Microsoft AD	
AMS Advanced 開發人員模式	
Amazon Simple Storage Service (Amazon S3)	建立 S3 儲存貯體政策
AWS Systems Manager	建立

使用直接變更模式建立堆疊

使用 在 CloudFormation 中啟動堆疊時，有兩個需求AWSManagedServicesCloudFormationAdminRole，以便 AMS 管理堆疊：

- 範本必須包含 AmsStackTransform。
- 堆疊名稱必須以字首開頭，stack-後面接著 17 個字元的英數字串。

 Note

若要成功使用 AmsStackTransform，您必須確認堆疊範本包含 CAPABILITY_AUTO_EXPAND功能，以便 AWS CloudFormation (CFN) 建立或更新堆疊。您可以透過CAPABILITY_AUTO_EXPAND在 create-stack 請求中傳遞 來執行此操作。如果在範本中AmsStackTransform包含 時未確認此功能，CFN 會拒絕請求。如果您的範本中有轉換，CFN 主控台會確保您傳遞此功能，但當您透過其 APIs 與 CFN 互動時，可能會錯過此功能。

每當您使用下列 CFN API 呼叫時，都必須傳遞此功能：

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

使用 DCM 建立或更新堆疊時，會在堆疊上執行 CFN 擷取和堆疊更新 CTs 的相同驗證和增強，如需詳細資訊[AWS CloudFormation](#)，請參閱[擷取指導方針、最佳實務和限制](#)。例外情況是，AMS 預設安全群組 (SGs) 不會連接到 Auto Scaling 群組 (ASGs) 中的任何獨立 EC2 執行個體或 EC2 執行個體。當您使用獨立 EC2 執行個體或 ASGs 建立 CloudFormation 範本時，您可以連接預設 SGs。

Note

IAM 角色現在可以使用 建立和管理AWSManagedServicesCloudFormationAdminRole。

AMS 預設 SGs 具有輸入和輸出規則，允許執行個體成功啟動，並在稍後透過 SSH 或 RDP 由 AMS 操作與您存取。如果您發現 AMS 預設安全群組過於寬鬆，您可以使用更嚴格的規則建立自己的 SGs，並將其連接到執行個體，只要它仍然允許您和 AMS 操作在事件期間存取執行個體。

AMS 預設安全群組如下：

- SentinelDefaultSecurityGroupPrivateOnly：可透過此 SSM 參數在 CFN 範本中存取 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll：可透過此 SSM 參數在 CFN 範本中存取 `ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 轉換

將Transform陳述式新增至 CloudFormation 範本。這會新增 CloudFormation 巨集，以在啟動時向 AMS 驗證和註冊堆疊。

JSON 範例

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
```

```
}  
}
```

YAML 範例

```
Transform:  
  Name: AmsStackTransform  
  Parameters:  
    StackId: !Ref 'AWS::StackId'
```

更新現有堆疊的範本時，也請新增 Transform 陳述式。

JSON 範例

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Description" : "Create an SNS Topic",  
  "Transform": {  
    "Name": "AmsStackTransform",  
    "Parameters": {  
      "StackId": {"Ref" : "AWS::StackId"}  
    }  
  },  
  "Parameters": {  
    "TopicName": {  
      "Type": "String",  
      "Default": "HelloWorldTopic"  
    }  
  },  
  "Resources": {  
    "SnsTopic": {  
      "Type": "AWS::SNS::Topic",  
      "Properties": {  
        "TopicName": {"Ref": "TopicName"}  
      }  
    }  
  }  
}
```

YAML 範例

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

堆疊名稱

堆疊名稱必須以字首開頭，stack-後面接著 17 個字元的英數字串。這是為了維持與在 AMS 堆疊 IDs 上操作之其他 AMS 系統的相容性。

以下是產生相容堆疊 IDs 的方法範例：

Bash：

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python：

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell：

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_}))
```

直接變更模式使用案例

以下是直接變更模式的使用案例：

透過 進行資源佈建和管理 AWS CloudFormation

- 整合現有的 CloudFormation 型工具和程序。

持續的資源管理和更新

- 低風險的小型原子變化。
- 否則會透過手動或自動 RFC 執行的變更。
- 需要原生 AWS API 存取的工具。
- 如果您處於遷移階段，則可以使用 DCM 角色。遷移團隊會利用 DCM 上的許可來建立或修改堆疊。
- DCM 角色可用於 CI/CD 管道，以建立新的 AMIs、建立 Amazon ECS 任務等。

AMS 進階開發人員模式

主題

- [AMS 進階開發人員模式入門](#)
- [開發人員模式中的安全性和合規性](#)
- [在開發人員模式下變更管理](#)
- [在 AMS 開發人員模式下佈建基礎設施](#)
- [AMS 開發人員模式下的偵測控制](#)
- [在 AMS 開發人員模式下記錄、監控和事件管理](#)
- [AMS 開發人員模式下的事件管理](#)
- [AMS 開發人員模式下的修補程式管理](#)
- [AMS 開發人員模式下的持續性管理](#)
- [AMS 開發人員模式下的安全性和存取管理](#)

AWS Managed Services (AMS) 開發人員模式使用 AMS Advanced Plus 和 Premium 帳戶中的更高許可，在 AMS Advanced 變更管理程序之外佈建和更新 AWS 資源。AMS Advanced Developer 模式透過在 AMS Advanced Virtual Private Cloud (VPC) 中利用原生 AWS API 呼叫來執行此操作，讓您能夠在受管環境中設計和實作基礎設施和應用程式。

使用已啟用開發人員模式的帳戶時，系統會為透過 AMS 進階變更管理程序或使用 AMS Amazon Machine Image (AMI) 佈建的資源提供持續性管理、修補程式管理和變更管理。不過，這些 AMS 管理功能不適用於透過 AWS APIs 佈建的資源。

您有責任監控在 AMS 進階變更管理程序之外佈建的基礎設施資源。開發人員模式與生產和非生產工作負載相容。透過提高的許可，您更有責任確保遵守內部控制。

Important

您使用開發人員模式建立的資源只有在使用 AMS 進階變更管理程序建立時，才能由 AMS Advanced 管理。

開發人員模式是您可以採用的 AMS 進階模式之一。如需詳細資訊，請參閱[模式概觀](#)。

AMS 進階開發人員模式入門

了解具有 AMS 進階開發人員模式的各種 AMS 進階帳戶，以及如何成功實作開發人員模式。

主題

- [開始使用 AMS 開發人員模式之前](#)
- [AMS 開發人員模式的先決條件](#)
- [如何實作 AMS 進階開發人員模式](#)
- [AMS 進階開發人員模式許可](#)

開始使用 AMS 開發人員模式之前

在實作開發人員模式之前，您應該知道幾件事。

AMS Advanced 無法管理 DevMode 帳戶中透過變更請求 (RFCs) 在 AMS Advanced 變更管理程序之外建立的現有堆疊或資源。不過，當帳戶位於 DevMode 時，AMS Advanced 會繼續使用 RFCs 管理透過 AMS Advanced 變更管理程序佈建的資源。

您無法從 DevMode 帳戶開始，之後再將其隱藏到 AMS 進階受管應用程式帳戶。

AMS 開發人員模式的先決條件

以下是實作開發人員模式的先決條件：

- 您必須是至少擁有一個已加入 AMS Advanced Plus 或 Premium 帳戶的 AMS Advanced 客戶。
- 您使用的任何帳戶都必須是 AMS Advanced Plus 或 Premium 帳戶。

- 多帳戶登陸區域 (MALZ)：您必須使用AWSManagedServicesDevelopmentRole預先定義的 AWS Identity and Access Management (IAM) 角色。您請求此角色。下一節說明如何取得開發人員模式許可。
- 單一帳戶登陸區域 (SALZ)：您必須使用customer_developer_role預先定義的 AWS Identity and Access Management (IAM) 角色。您請求此角色。下一節說明如何取得開發人員模式許可。

如何實作 AMS 進階開發人員模式

您可以請求使用預先定義的 IAM 角色佈建符合資格的 AMS Advanced 帳戶，以實作開發人員模式：

- MALZ：AWSManagedServicesDevelopmentRole
- SALZ：customer_developer_role

然後，您將角色指派給聯合網路中的相關使用者。

AMS Advanced 建議您確保使用開發人員模式符合您的內部控制架構和標準，因為開發人員模式會建立兩種變更向量：適用於 AMS 進階受管資源的 AMS 進階變更管理，以及適用於您身為客戶管理之資源的客戶受管角色聯合。雖然 AMS Advanced 程序仍符合我們的宣告，但客戶程序和控制架構可能需要更新。

在 AMS Advanced 帳戶中實作開發人員模式

1. 確認您想要與開發人員模式搭配使用的帳戶符合 中列出的要求[AMS 開發人員模式的先決條件](#)。
2. 使用變更類型 (CT) 管理 | 受管帳戶 | 開發人員模式 | 啟用 (需要檢閱) 提交變更請求 (RFC)。如需如何使用此 CT 的範例，請參閱[開發人員模式 | 啟用 \(需要檢閱 \)](#)。

處理 CT 之後，預先定義的 IAM 角色 (AWSManagedServicesDevelopmentRoleMALZ 為 , SALZ customer_developer_role為) 會在請求的帳戶中佈建。

3. 使用內部聯合程序，將適當的角色指派給需要開發人員模式存取的使用者。

AMS Advanced 建議您限制存取，以防止不需要或未核准的資源佈建或變更。

AMS 進階開發人員模式許可

預先定義的角色 (AWSManagedServicesDevelopmentRole適用於 MALZ、customer_developer_role適用於 SALZ) 會授予許可，以在 AMS Advanced VPC 內建立應用程式基礎設施資源，包括 IAM 角色，同時限制存取由 AMS Advanced 操作的共用服務元件 (例

如，管理主機、網域控制站、Trend Micro EPS、堡壘和不支援的 AWS 服務)。此角色也會限制對下列項目的存取 AWS 服務：Amazon GuardDuty AWS Organizations、AWS Directory Service APIs 和 AMS Advanced 日誌。

雖然角色可讓您建立其他 IAM 角色，但開發人員模式存取中包含的相同許可界限會在 建立的任何 IAM 角色上強制執行AWSManagedServicesDevelopmentRole。

開發人員模式中的安全性和合規性

安全與合規是 AMS Advanced 與身為客戶的您共同的責任。AMS Advanced Developer 模式會將變更管理程序之外佈建或透過變更管理佈建，但使用開發人員模式許可更新之資源的共同責任轉移給您。如需共同責任的詳細資訊，請參閱 [AWS Managed Services](#)。

注意：

- DevMode 可讓您和您的授權團隊略過 AMS 安全性核心的deny-by-default原則。優點、自助服務、較少等待 AMS 的時間必須權衡缺點，任何人都可以在不了解其安全團隊的情況下執行非預期且破壞性的動作。用於啟用開發模式和直接變更模式的自動變更類型會公開，且組織中任何獲授權的人員都可以執行這些 CTs 並啟用這些模式。
- 您負責從使用者基礎管理 CT 執行的許可。
- AMS 不會管理 CT 執行許可

建議：

- 保護
 - 客戶可以透過許可防止存取此 CT，請參閱[使用 IAM 角色政策陳述式限制許可](#)
 - 透過實作 ITSM 系統等代理來防止存取此 CT
 - 利用可視需要防止政策和行為的服務控制政策 (SCPs)，請參閱 [AMS Preventative and Detective Controls Library](#)
- 偵測
 - 監控 RFC 的這些 CTs (啟用開發人員模式 ct-1opjmhuddw194 和直接變更模式，啟用 ct-3rd4781c2nnhp) 正在執行並相應地回應
 - 檢閱和/或稽核您的帳戶是否存在 IAM 資源，以識別已部署開發人員模式或直接變更模式的帳戶
- 回應
 - 視需要在開發人員模式中移除帳戶

開發人員模式中的安全性

AMS Advanced 提供具有規範登陸區域、變更管理系統和存取管理的額外值。使用開發人員模式時，AMS Advanced 的安全值會使用建立基準 AMS Advanced 安全性強化網路的標準 AMS Advanced 帳戶相同的帳戶組態來保留。網路受到角色中強制執行的許可界限 (AWSManagedServicesDevelopmentRole適用於 MALZ，customer_developer_role適用於 SALZ) 的保護，這會限制使用者分解帳戶設定時建立的參數保護。

例如，具有角色的使用者可以存取 Amazon Route 53，但 AMS Advanced 內部託管區域受到限制。相同的許可界限會在建立的 IAM 角色上強制執行AWSManagedServicesDevelopmentRole，在上強制執行許可界限AWSManagedServicesDevelopmentRole，以限制使用者細分帳戶加入 AMS Advanced 時建立的參數保護。

開發人員模式中的合規

開發人員模式與生產和非生產工作負載相容。您有責任確保遵守任何合規標準（例如 PHI、HIPAA、PCI），並確保使用開發人員模式符合您的內部控制架構和標準。

在開發人員模式下變更管理

變更管理是 AMS Advanced 服務用來實作變更請求的程序。變更請求 (RFC) 是由您或 AMS Advanced 透過 AMS Advanced 界面建立的請求，用於對受管環境進行變更，並包含特定操作的變更類型 (CT) ID。如需詳細資訊，請參閱[變更管理模式](#)。

在授予開發人員模式許可的 AMS Advanced 帳戶中，不會強制執行變更管理。已使用 IAM 角色 (AWSManagedServicesDevelopmentRole適用於 MALZ、customer_developer_role適用於 SALZ) 授予開發人員模式許可的使用者，可以使用原生 AWS API 存取來佈建和變更其 AMS Advanced 帳戶中的資源。在這些帳戶中沒有適當角色的使用者，必須使用 AMS 進階變更管理程序進行變更。

Important

您使用開發人員模式建立的資源，只有在使用 AMS 進階變更管理程序建立時，才能由 AMS Advanced 管理。AMS Advanced 會拒絕針對在 AMS Advanced 變更管理程序之外建立的資源提交至 AMS Advanced 的變更請求，因為這些變更必須由您處理。

自助式佈建服務 API 限制

開發人員模式支援所有 AMS Advanced 自行佈建服務。對自行佈建服務的存取受個別使用者指南章節中概述的限制約束。如果您的開發人員模式角色無法使用自助佈建服務，您可以透過開發人員模式變更類型請求更新的角色。

下列服務不提供服務 APIs 的完整存取權：

開發人員模式中限制的自助佈建服務

服務	備註
Amazon API Gateway	允許所有閘道 APIs 呼叫，但 除外 SetWebACL。
Application Auto Scaling	只能註冊或取消註冊可擴展的目標，並放置或刪除擴展政策。
AWS CloudFormation	無法存取或修改名稱字首為 的 CloudFormation 堆疊 mc-。
AWS CloudTrail	無法存取或修改名稱字首為 ams- 和/或 的 CloudTrail 資源 mc-。
Amazon Cognito（使用者集區）	無法關聯軟體字符。 無法建立使用者集區、使用者匯入任務、資源伺服器或身分提供者。
AWS Directory Service	Connect 和 WorkSpaces 服務只需要下列 AWS Directory Service 動作。開發人員模式許可界限政策會拒絕所有其他 Directory Service 動作： - ds:AuthorizeApplication - ds:CreateAlias - ds:CreateIdentityPoolDirectory - ds>DeleteDirectory - ds:DescribeDirectories

服務	備註
	• ds:GetAuthorizedApplicationDetails • ds:ListAuthorizedApplications • ds:UnauthorizeApplication 在單一帳戶登陸區域帳戶中，邊界政策明確拒絕存取 AMS Advanced 使用的 AMS Advanced 受管目錄，以維護對已啟用開發模式之帳戶的存取。
Amazon Elastic Compute Cloud	無法存取包含字串的 Amazon EC2 APIs：DhcpOptions、Gateway、Subnet、VPC和VPN。 無法存取或修改標籤字首為 AMS、ManagementHostASG、mc和/或的 Amazon EC2 資源sentinel。
Amazon EC2（報告）	僅授予檢視存取權（無法修改）。注意：Amazon EC2 報告正在移動。報告選單項目將從 Amazon EC2 主控台導覽選單中移除。若要在移除之後檢視 Amazon EC2 用量報告，請使用 AWS Billing 和 Cost Management 主控台。

服務	備註
AWS Identity and Access Management (IAM)	無法刪除現有的許可界限，或修改 IAM 使用者密碼政策。 除非您使用正確的 IAM 角色 (AWSManagedServicesDevelopmentRole 適用於 MALZ、customer_developer_role 適用於 SALZ))，否則無法建立或修改 IAM 資源。 無法修改字首為 :ams、customer_deny_policy 、mc和/或的 IAM 資源sentinel。 建立新的 IAM 資源（角色、使用者或群組）時，必須連接許可界限 (MALZ : AWSManagedServicesDevelopmentRolePermissionsBoundary 、SALZ : ams-app-infra-permissions-boundary)。
AWS Key Management Service (AWS KMS)	無法存取或修改 AMS 進階受管 KMS 金鑰。
AWS Lambda	無法存取或修改字首為 的 AWS Lambda 函數AMS。
CloudWatch Logs	無法存取名稱字首為 mc、awslambda和/或的 CloudWatch 日誌串流AMS。
Amazon Relational Database Service (Amazon RDS)	無法存取或修改名稱字首為 的 Amazon Relational Database Service (Amazon RDS) 資料庫 (DBs) : mc-。
AWS Resource Groups	只能存取 Get、List和 Search 資源群組 API 動作。
Amazon Route 53	無法存取或修改 Route53 AMS 進階維護的資源。

服務	備註
Amazon S3	無法存取名稱字首為：ams-*、ms-a、ams或的 Amazon S3 儲存貯體mc-a。
AWS Security Token Service	唯一允許的安全性字符服務 API 是 DecodeAuthorizationMessage 。
Amazon SNS	無法存取名稱字首為：AMS-、Energon-Topic 或的 SNS 主題MMS-Topic 。
AWS Systems Manager 管理員 (SSM)	無法修改字首為 ams、mc或的 SSM 參數svc。 無法SendCommand 針對標籤字首為 ams或的 Amazon EC2 執行個體使用 SSM APImc。
AWS 標記	您只能存取字首為的 AWS 標記 API 動作Get。
AWS Lake Formation	下列 AWS Lake Formation API 動作遭拒： - lakeformation:DescribeResource - lakeformation:GetDataLakeSettings - lakeformation:DeregisterResource - lakeformation:RegisterResource - lakeformation:UpdateResource - lakeformation:PutDataLakeSettings
Amazon Elastic Inference	您只能呼叫 Elastic Inference API 動作elastic-inference:Connect 。此許可包含在連接到 customer_sagemaker_admin_policy 的中customer_sagemaker_admin_role 。此動作可讓您存取 Elastic Inference 加速器。

服務	備註
AWS Shield	無法存取任何此服務 APIs 或主控台。
Amazon Simple Workflow Service	無法存取任何此服務 APIs 或主控台。

在 AMS 開發人員模式下佈建基礎設施

沒有開發人員模式 IAM 角色的使用者 `AWSTransientServicesDevelopmentRole`，在已啟用開發人員模式的帳戶中，必須遵循利用 AMS 進階 AMIs 的 AMS 進階變更管理程序。具有正確角色 (MALZ : `AWSTransientServicesDevelopmentRole`、SALZ : `customer_developer_role`) 的使用者可以使用 AMS 進階變更管理系統和 AMS 進階 AMIs 但不需要。

Note

尚未透過 AMS 進階工作負載擷取處理，或在 AWS AMS 進階帳戶中建立的 AMI，將不會包含 AMS 進階所需組態。

AMS 開發人員模式下的偵測控制

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

在 AMS 開發人員模式下記錄、監控和事件管理

記錄、監控和事件管理不適用於在 AMS 進階變更管理程序之外佈建的資源，也不適用於透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源。

AMS 開發人員模式下的事件管理

事件回應時間沒有變更。對於在變更管理程序之外佈建的資源，或是透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，事件解決是最大的努力。

 Note

AMS 服務水準協議 (SLA) 不適用於在 AMS 變更管理系統 (變更請求或 RFCs) 之外建立或更新的資源，包含開發人員模式；因此，在開發人員模式中更新或建立的資源會自動降級為 P3，AMS 支援會盡最大努力。

AMS 開發人員模式下的修補程式管理

修補程式管理不適用於在 AMS 進階變更管理程序之外佈建的資源，或透過變更管理佈建的資源，然後使用開發人員模式許可由帳戶修改。修補時間：

- 對於重大安全性更新：在廠商發佈後 10 個工作天內，透過變更管理佈建的資源，然後由使用開發人員模式許可的帳戶進行變更。
- 重要更新：在廠商發佈後 2 個月內，透過變更管理佈建的資源，然後由使用開發人員模式許可的帳戶更改。

AMS 開發人員模式下的持續性管理

持續性管理不適用於在 AMS 進階變更管理程序之外佈建的資源，或透過變更管理佈建的資源，然後使用開發人員模式許可由帳戶修改。

針對在 AMS 進階變更管理程序之外佈建的資源，或是透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，環境復原啟動時間最多可能需要 12 小時。

AMS 開發人員模式下的安全性和存取管理

對於在 AMS 進階變更管理程序之外佈建的資源，或是透過變更管理佈建，然後使用開發人員模式許可由帳戶修改的資源，反惡意軟體保護是您的責任。未透過 AMS Advanced 變更管理佈建的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的存取權可能由金鑰對控制，而不是提供聯合存取。

AMS 中的自助式佈建模式

AWS Managed Services (AMS) 自助式佈建 (SSP) 模式可讓您完整存取 AMS 受管帳戶中的原生 AWS 服務和 API 功能。您可以透過標準化、縮小範圍、AWS Identity and Access Management 角色來存取服務。AMS 提供服務請求和事件管理。警示、監控、記錄、修補、備份和變更管理是您的責任。在許多情況下，自助式佈建服務 (SSPs) 是自我管理或無伺服器，不需要管理特定操作任務，例如修補。您可以在 AMS 防護機制定義的環境界限內使用這些服務，而任何 IAM 變更 (包括服務連結角色、服

務角色、跨帳戶角色或政策更新) 都需要經過 AMS Operations 核准，才能維護平台的基準安全性。您可以利用 AWS CloudFormation 範本來自動化這些服務的部署，但並非所有 SSP 服務都支援此功能。

Important

在 AWS Managed Services (AMS) 帳戶中使用 SSP 模式來存取和使用 AWS 服務，但有上述限制。

您可以在沒有 AMS 管理的情況下，在您的 AMS 帳戶中 AWS 服務使用一些。「自助式佈建模式」服務，或簡稱為「SSPS」，說明如何將它們新增至您的 AMS 帳戶和每個帳戶的FAQs」，如一節所述。

自助式佈建服務會照原樣提供，而且您需負責管理這些服務。AMS 不會對與這些服務相關聯的資源提供提醒、監控、記錄或修補。AMS 提供 IAM 角色，可讓您安全地在 AMS 帳戶中使用服務。AMS SLAs 不適用。

對於您透過自助服務佈建的資源，AMS 提供事件管理、偵測控制和防護機制、報告、指定資源 (Cloud Service Delivery Manager 和 Cloud Architect)、安全性和存取，以及透過服務請求提供的技術支援。此外，在適用的情況下，您需為在 AMS 變更管理系統之外佈建或設定的資源承擔持續性管理、修補程式管理、基礎設施監控和變更管理的責任。

AMS 中的 SSP 模式入門

自助式佈建是您可以用於多帳戶登陸區域 (MALZ) 的 AMS 模式之一。如需詳細資訊，請參閱[模式概觀](#)。

為了提供自助式佈建功能，AMS 已建立具有許可界限的提升 IAM 角色，以限制直接 AWS 服務存取的意外變更。這些角色不會阻止所有變更，而且您必須遵守內部控制和合規政策，並驗證所有 AWS 服務正在使用的都符合必要的認證。這是自助式佈建模式。如需 AWS 合規要求的詳細資訊，請參閱[AWS 合規](#)。

若要將自助式佈建服務新增至多帳戶登陸區域應用程式帳戶，請依照服務的指示，使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (CT)，包括檢閱所需的 CT 或自動 CT。

Note

若要請求 AMS 提供額外的自助式佈建服務，請提交服務請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon API Gateway

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon API Gateway 功能。[Amazon API Gateway](#) 是一項全受管服務，可讓開發人員輕鬆建立、發佈、維護、監控和保護任何規模 APIs。您可以使用 AWS Management Console 建立 REST 和 WebSocket APIs，做為應用程式從後端服務存取資料、商業邏輯或功能的大門，例如在 Amazon Elastic Compute Cloud ([Amazon EC2](#)) 上執行的工作負載、在 上執行的程式碼[AWS Lambda](#)、任何 Web 應用程式或即時通訊應用程式。

API Gateway 會處理所有涉及接受和處理多達數十萬個並行 API 呼叫的任務，包括流量管理、授權和存取控制、監控和 API 版本管理。API Gateway 沒有最低費用或啟動成本。您只需為收到的 API 呼叫和傳出的資料量付費，並且使用 API Gateway 分層定價模型，您可以隨著 API 用量的擴展而降低成本。若要進一步了解，請參閱 [Amazon API Gateway](#)。

常見問答集：AMS 中的 API Gateway

問：如何請求存取 AMS 帳戶中的 Amazon API Gateway？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 API Gateway。此 RFC 會將下列 IAM 角色佈建至您的帳戶：
`customer_apigateway_author_role`和 `customer_apigateway_cloudwatch_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon API Gateway 有哪些限制？

- API Gateway 組態僅限於沒有 AMS-或 字MC-首的資源，以防止對 AMS 基礎設施進行任何修改。
- CREATE VPCLink 的 權限會停用，以防止 Elastic Load Balancer 不受管制的建立。如果需要 VPCLinks，請參閱 [Application Load Balancer | Create](#)。

問：在我的 AMS 帳戶中使用 Amazon API Gateway 的先決條件或相依性是什麼？

這取決於您要部署的 API Gateway 類型。它可以是獨立服務，但也可以請求存取現有的服務（例如網路負載平衡器）。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Alexa for Business

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Alexa for Business 功能。Alexa for Business 是一項服務，可讓您的組織和員工使用 Alexa 來完成更多工作。透過 Alexa for Business，您可以使用 Alexa 作為智慧助理，在會議室、桌上，甚至在家裡或外出時使用的 Alexa 裝置中提高生產力。IT 和設施管理員可以使用 Alexa for Business 來衡量和提高其工作場所中現有會議室的使用率。

若要進一步了解，請參閱 [Alexa for Business](#)。

AWS Managed Services 中的 Alexa for Business 常見問答集

問：如何在我的 AMS 帳戶中請求存取 Alexa for Business？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny)

變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳

戶：customer_alex_console_role。customer_alex_device_setup_user 也會為 Alexa for Business 提供的裝置設定工具建立；然後，可以使用此裝置設定工具來設定您的裝置。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

Alexa for Business 閘道可讓您將 Alexa for Business 連線至 Cisco Webex 和 Poly Group 系列端點，以使用語音控制會議。閘道軟體會在您的現場部署硬體上執行，並將 Alexa for Business 的會議指令安全地代理到 Cisco 端點。閘道需要兩對 AWS 登入資料才能與 Alexa for Business 通訊。我們為 Alexa for Business 閘道提供兩個有限存取customer_alex_gateway_installer_usercustomer_alex_gateway_execution_user的 IAM 使用者：一個用於安裝閘道，另一個用於操作閘道；您可以透過提交 RFC 與部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策（需要檢閱）變更類型(ct-3dpd8mdd9jn1r) 來請求這些使用者。

Note

若要產生用量報告並將其傳送至 Amazon S3，請在自行佈建的服務 RFC 中指定 Amazon S3 儲存貯體名稱。

問：在我的 AMS 帳戶中使用 Alexa for Business 有哪些限制？

沒有限制。Alexa for Business 的完整功能可供 Alexa for Business 自助佈建服務角色使用。

問：在我的 AMS 帳戶中使用 Alexa for Business 的先決條件或相依性是什麼？

- 如果您想要使用 WPA2 Enterprise Wi-Fi 來設定共用裝置，請在裝置設定工具中指定此網路安全類型，其中 AWS Private Certificate Authority 需要。
- AMS 只會建立以命名空間 "A4B" 開頭的私密金鑰。這僅限於此命名空間。

問：什麼 Alexa for Business 功能需要單獨的 RFCs？

若要向 Alexa for Business 註冊 Alexa Voice Service (AVS) 裝置，請提供 Alexa 內建裝置製造商的存取權。若要這樣做，需要在 Alexa for Business 主控台中建立 IAM 角色，該角色可以使用 **管理 | 其他 | 其他變更類型** 進行部署。這可讓 AVS 裝置製造商代表您向 Alexa for Business 註冊和管理裝置。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon AppStream 2.0

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon AppStream 2.0 (AppStream 2.0) 功能。AppStream 2.0 可讓您將桌面應用程式移至 AWS，而無需重寫。您可以在 AppStream 2.0 上安裝應用程式、設定啟動組態，並將應用程式提供給使用者。AppStream 2.0 提供多種虛擬機器選項，讓您可以選取最符合您應用程式需求的執行個體類型，並設定自動調整規模參數，以便輕鬆滿足最終使用者的需求。AppStream 2.0 可讓您在自己的網路中啟動應用程式，這表示您的應用程式可以與您現有的 AWS 資源互動。

Amazon AppStream 2.0 可讓您使用映像建置器快速輕鬆地安裝、測試和更新應用程式。支援在 Microsoft Windows Server 2012 R2、Windows Server 2016 或 Windows Server 2019 上執行的任何應用程式，您不需要進行任何修改。測試完成後，您可以設定應用程式啟動組態、預設使用者設定，並發佈映像以供使用者存取。

若要進一步了解，請參閱 [AppStream 2.0](#)。

AWS Managed Services 常見問答集中的 AppStream 2.0

問：如何請求存取 AMS 帳戶中的 AppStream 2.0？

透過使用 **管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-3qe6io8t6jtny)** 變更類型提交 RFC，請求存取 AppStream 2.0。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_appstream_console_role`。

`customer_appstream_stream_role` 也會部署以串流應用程式，要求使用者使用其 Active Directory 登入憑證進行身分驗證。

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AppStream 2.0 有哪些限制？

- 下列功能必須由 AMS 支援團隊設定，且需要特定的 RFCs。有關請求其他功能的說明，請參閱第 4 節。
 - 從介面 VPC 端點建立和串流。
 - 支援 Amazon S3 端點的主資料夾和私有網路上的應用程式設定持續性。
 - 建立並選擇可在所有機群串流執行個體上使用的 IAM 角色。

- 加入 AppStream 2.0 機群和映像建置器 Microsoft Active Directory 網域。
- 建立 AppStream 2.0 自訂用量報告。
- 目前不支援自訂品牌。

問：在我的 AMS 帳戶中使用 AppStream 2.0 有哪些先決條件或相依性？

提交 RFC 以加入 AppStream 2.0 時，請包含要用於 AppStream 2.0 用量報告的 Amazon S3 儲存貯體名稱。儲存貯體名稱會新增至 AppStream 2.0 加入時 `customer-appstream-usagereports-policy` 建立的。

問：哪些 AppStream 2.0 功能需要單獨的 RFCs？

- 若要選擇 AppStream 2.0 的介面 VPC 端點，請提交管理 | 其他 | 其他 | 更新變更類型 RFC，以在您的帳戶中建立 VPC 端點。如需為 AppStream 2.0 建立自訂端點的步驟，請參閱 AppStream 2.0 使用者指南中的 [從介面 VPC 端點建立和串流](#)。
- 透過使用管理 | 其他 | 其他 | 建立變更類型 RFC 請求 Amazon S3 VPC 端點，即可設定對私有網路上主資料夾和應用程式設定持續性的 Amazon S3 端點支援。RFC 必須分別包含託管主資料夾內容的目標 Amazon S3 儲存貯體，或應用程式設定 Amazon S3 儲存貯體。此 RFC 將為 AppStream 2.0 提供存取 Amazon S3 VPC 端點所需的許可。如需為串流建立自訂端點的步驟，請參閱 AppStream 2.0 使用者指南中的 [將 Amazon S3 VPC 端點用於主資料夾和應用程式設定持續性](#)。
- 若要建立和選擇可在所有機群串流執行個體上使用的 IAM 角色，請提交部署 | 進階堆疊元件 | 身分與存取管理 (IAM) | 建立實體或政策 (需要檢閱) 變更類型 (ct-3dpd8mdd9jn1r) RFC，以要求具有必要政策的 IAM 角色。IAM 角色名稱應一律以字首："customer_appstream" 開頭。
- Amazon AppStream 2.0 機群和映像建置器可以透過在 Active Directory (AD) 中提交管理 | 其他 | 其他 | 更新服務帳戶建立的變更類型 RFC 來加入 Microsoft Active Directory 中的網域。在授予建立和管理 Active Directory 電腦物件的許可的 AppStream 2.0 文件中，定義了加入 Microsoft Active Directory 所需的最低許可。 <https://docs.aws.amazon.com/appstream2/latest/developerguide/active-directory-admin.html#active-directory-permissions>
- 若要建立自訂 AppStream 2.0 用量報告，請提交管理 | 其他 | 其他 | 建立變更類型 RFC 請求如下：
 - 建立「AppStreamUsageReports」CFN 堆疊
 - 帳戶中佈建「customer_appstream_usagereports_role」
 - 此外，請提供下列詳細資訊：
 - 提供 CRON 表達式來排程爬蟲程式執行。根據預設，每天為 23:00 UTC。
 - 用於 Athena 查詢結果的 Amazon S3 儲存貯體 ARN。此儲存貯體應有字首：aws-athena-query-results

- AppStream 2.0 用量報告日誌的 Amazon S3 儲存貯體 ARN。

佈建角色後，將角色加入您的聯合解決方案並登入，然後存取 AWS GlueAWS Glue 和 Athena 以使用用量報告角色產生自訂報告。如需使用 AppStream 2.0 用量報告的詳細資訊，請參閱 [AppStream 2.0 文件中的建立自訂報告和分析 AppStream 2.0 用量資料](#)。AppStream

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Athena

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Athena (Athena) 功能。Athena 是一種互動式查詢服務，可協助您使用標準 SQL 分析 Amazon S3 中的資料。Athena 無伺服器，所以不需管理基礎設施，而且您只需支付所執行查詢的費用。您可以指向 Amazon S3 中的資料、定義結構描述，並使用標準 SQL 開始查詢。大多數結果會在幾秒鐘內交付。使用 Athena，您不需要複雜的 extract-transform-load (ETL) 任務來準備資料以供分析。這可讓具備 SQL 技能的任何人直接分析大規模資料集。若要進一步了解，請參閱 [Amazon Athena](#)。

常見問答集：AMS 中的 Athena

問：如何請求存取 AMS 帳戶中的 Amazon Athena？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 Athena。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_athena_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Athena 有哪些限制？

沒有限制。Amazon Athena 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Athena 的先決條件或相依性是什麼？

Athena 使用以建立的資料目錄/中繼存放區，因此對 AWS Glue 服務具有主要相依性 AWS Glue。因此，AWS Glue 許可會包含在成功的 Athena RFC 中。

角色customer_athena_console_role具有 Amazon S3 儲存貯體的先決條件。若要建立新的儲存貯體，請使用自動化 CT ct-1a68ck03fn98r (部署 | 進階堆疊元件 | S3 儲存 | 建立)。當您使用此自動化 CT 為 Athena 建立 S3 儲存貯體時，儲存貯體名稱必須以字首 開頭athena-query-results-*。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Bedrock

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Bedrock 功能。Amazon Bedrock 是一項全受管服務，可讓領先業界的 AI 新創公司提供高效能的基礎模型 (FMs)，並透過統一

的 API AWS 供您使用。您可以從各種基礎模型中做選擇，找出最適合您使用案例的模型。Amazon Bedrock 還提供了一系列廣泛的功能，以建置具有安全性、隱私性和負責任之 AI 的生成式 AI 應用程式。使用 Amazon Bedrock 時，您可以輕鬆地為您的使用案例進行試驗，並評估最佳基礎模型，利用微調和檢索增強生成 (RAG) 等技術私下自訂資料，以及建置使用企業系統和資料來源執行任務的代理程式。

藉助 Amazon Bedrock 的無伺服器體驗，您可以快速入門，使用您自己的資料私下自訂基礎模型，並使用 AWS 工具輕鬆安全地整合和部署到您的應用程式中，而無需管理任何基礎設施。如需詳細資訊，請參閱 [Amazon Bedrock](#)。

常見問答集：AMS 中的 Amazon Bedrock

問：如何請求存取 AMS 帳戶中的 Amazon Bedrock？

若要請求存取 Amazon Bedrock，請使用 Management | AWS service | Self-visited service | Add (需要檢閱) (ct-3qe6io8t6jtny) 變更類型提交 RFC。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_bedrock_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Bedrock 有哪些限制？

- 預設不支援 Amazon Bedrock 知識庫做為 SSPS 角色的一部分，因為其相依於 AMS 上目前不支援的 Amazon OpenSearch Service Serverless。
- 由於 Bedrock Studio 依賴於 Amazon DataZone 等不支援的服務，因此不支援 Bedrock Studio。

問：在我的 AMS 帳戶中使用 Amazon Bedrock 的先決條件或相依性是什麼？

- 需要 AWS Marketplace 許可的第三方模型訂閱必須由預設角色完成 (AWSManagedServicesAdminRole 在 MALZ 上和 SALZ Customer_ReadOnly_Role 上)。這是因為預設角色包含 AWS Marketplace 許可。
- 如果使用資料加密，則您必須在請求建立主控台角色時提供 AWS KMS 金鑰 ARN。此外，使用中的 Amazon S3 儲存貯體名稱中必須有「bedrock」。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon CloudSearch

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon CloudSearch 功能。Amazon CloudSearch 是 AWS 雲端中的受管服務，可讓您以經濟實惠的方式設定、管理和擴展網站或應用程式

的搜尋解決方案。Amazon CloudSearch 支援 34 種語言和熱門搜尋功能，例如反白、自動完成和地理空間搜尋。若要進一步了解，請參閱 [Amazon CloudSearch](#)。

Note

AWS 自 2024 年 7 月 25 日起，已關閉新客戶對 Amazon CloudSearch 的存取權。Amazon CloudSearch 現有客戶可以繼續正常使用服務。AWS 會繼續投資 Amazon CloudSearch 的安全性、可用性和效能改善，但我們不打算推出新功能。

若要了解 Amazon CloudSearch 和 Amazon OpenSearch Service 之間的差異，以及如何轉換至 OpenSearch Service，請聯絡您的雲端架構師 (CA) 以取得指引。如需轉換至 OpenSearch Service 的詳細資訊，請參閱[從 Amazon CloudSearch 轉換至 Amazon OpenSearch Service 服務](#)。

AWS Managed Services 常見問答集中的 Amazon CloudSearch

問：如何請求存取 AMS 帳戶中的 Amazon CloudSearch？

透過使用 Management | AWS service | Self-visited Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon CloudSearch。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_csearch_admin_role`和 `customer_csearch_dev_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon CloudSearch 有哪些限制？

Amazon CloudSearch 的完整功能可在您的 AMS 帳戶中使用。Amazon CloudSearch 目前支援所有 AMS 支援的資料庫解決方案。請注意，DynamoDB 目前是唯一無法編製索引的受管 AWS 資料庫解決方案。

問：在我的 AMS 帳戶中使用 Amazon CloudSearch 的先決條件或相依性是什麼？

Amazon CloudSearch 依賴 Amazon S3 與身分提供者合作，以自動分析輸入資料並判斷資料表欄位。此 RFC 未提供對 Amazon S3 的存取，必須在服務請求中另外請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon CloudWatch Synthetics

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon CloudWatch Synthetics 功能。您可以使用 Amazon CloudWatch Synthetics 建立 'canary' 來監控您的端點和 APIs。

Canary 是可設定的指令碼，以 Node.js 或 Python 撰寫，按排程執行。Canary 會使用 Node.js 或 Python 作為架構，在您的帳戶中建立 Lambda 函數。Canary 透過 HTTP 和 HTTPS 通訊協定運

作。Canary 會檢查端點的可用性和延遲，並可儲存載入時間資料和 UI 螢幕擷取畫面。它們會監控您的 REST API、URL 和網站內容，並且可以檢查來自網路釣魚、程式碼插入和跨網站指令碼的未經授權變更。

Canary 遵循與客戶相同的路由並執行相同的動作，讓您可以持續驗證客戶體驗，即使您的應用程式上沒有任何客戶流量。透過使用 Canary，您可以在客戶之前發現問題。若要進一步了解，請參閱 [Amazon CloudWatch：使用合成監控](#)。

AWS Managed Services 中的 Amazon CloudWatch Synthetics 常見問答集

問：如何請求存取 AMS 帳戶中的 Amazon CloudWatch Synthetics？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon CloudWatch Synthetics。此 RFC 會將下列 IAM 角色佈建至您的帳戶：'customer_cw_synthetics_console_role' 和 'customer_cw_synthetics_canary_lambda_role'。在帳戶中佈建後，您必須在聯合解決方案中加入 'customer_cw_synthetics_console_role' 角色。

問：在我的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 有哪些限制？

在您的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 沒有限制。禁止為 AMS 提供服務角色 'customer_cw_synthetics_canary_lambda_role' 以外的 Canary 建立角色。

問：在我的 AMS 帳戶中使用 Amazon CloudWatch Synthetics 有哪些先決條件或相依性？

Canary 建立並使用預設的 Amazon CloudWatch Synthetics S3 儲存貯體：`"cw-syn-results-accountnumber-default-region"`

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Cognito 使用者集區

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Cognito 使用者集區功能。Amazon Cognito 使用者集區提供安全的使用者目錄，可擴展到數億使用者。Amazon Cognito 使用者集區是全受管服務，無需擔心伺服器基礎設施的啟動。此服務可讓您管理最終使用者的集區，可用來與內部應用程式整合。此服務為您提供自訂資料庫或 Web 或行動應用程式最終使用者目錄的替代方案。同時，Amazon Cognito 使用者集區提供目錄服務的完整功能，例如密碼政策、多重要素驗證、密碼復原和自我註冊服務。它還允許應用程式聯合其他熱門公有服務的存取，例如 OpenID、Facebook、Amazon 或 Google。

Amazon Cognito 分為兩個主要產品。Amazon Cognito 使用者集區和 Amazon Cognito 身分提供者。本節著重於 Amazon Cognito 使用者集區，提供 Amazon S3 或 DynamoDB 等 AWS 其他服務的存取權。此服務可讓您使用 Amazon Cognito 使用者集區或第三方身分提供者來提供 AWS 服務的存取權。它也提供使用匿名訪客存取 AWS 的服務存取權。由於 Amazon Cognito 使用者集區的強大性質，它將

以操作手動服務的形式逐case-by-case手動管理，以避免潛在的安全中斷到帳戶中。若要進一步了解，請參閱 [Amazon Cognito 使用者集區](#)。

AWS Managed Services 常見問答集中的 Amazon Cognito 使用者集區

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Cognito 使用者集區？

在 AMS 中實作 Amazon Cognito 使用者集區是 2 個步驟：

1. 提交管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型，並請求在您的 AMS 帳戶中建立 Amazon Cognito 使用者集區。加入下列資訊：
 - AWS 區域。
 - Cognito 使用者集區的名稱。
 - 如果您想要使用 Amazon Simple Email Service (Amazon SES) 來傳送訊息和通知，而不是預設的內部 Cognito 郵件服務，則客戶應該為帳戶中的 Amazon SES Service 提供已驗證的電子郵件地址。此地址將用於訊息的「寄件人」和「REPLY-TO」欄位。他們還必須指出啟用 Amazon SES 的區域 (us-east-1、eu-west-1 或 us-west-2)。
 - 如果您想要使用簡訊進行一次性密碼和驗證，則客戶應該指出這一點。
2. 透過提交管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求使用者存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_cognito_admin_role`和 `customer_cognito_importjob_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。這些角色可讓您管理 Amazon Cognito 使用者集區、管理集區中的使用者和群組、為使用者建立 Importjobs、修改通知和訂閱訊息、將應用程式與使用者集區建立關聯、將聯合服務自我管理新增至集區，以及刪除已建立的集區。

問：在我的 AMS 帳戶中使用 Amazon Cognito 使用者集區有哪些限制？

您將無法建立 Amazon Cognito 使用者集區。該動作需要建立 IAM 角色，才能利用 Amazon Cognito 使用的服務，例如 Amazon SES 和 Amazon Simple Notification Service (Amazon SNS)。

問：在我的 AMS 帳戶中使用 Amazon Cognito 使用者集區的先決條件或相依性是什麼？

如果您想要使用 Amazon SES 透過電子郵件將訊息和通知傳送到使用者集區，他們應該已在帳戶中啟用 Amazon SES 服務，並已驗證應該在已傳送電子郵件的「FROM」和「REPLY-TO」欄位中使用的電子郵件地址。如需使用 Amazon SES 驗證電子郵件地址的詳細資訊，請參閱 [在 Amazon SES 中驗證電子郵件地址](#)。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Comprehend

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Comprehend 功能。Amazon Comprehend 是一種自然語言處理 (NLP) 服務，使用機器學習在文字中尋找洞見和關係，不需要機器學習體驗。Amazon Comprehend 使用機器學習來協助您探索非結構化資料中的洞見和關係。服務可識別文字的語言；擷取關鍵片語、位置、人物、品牌或事件；了解文字的正面或負面程度；使用字符化和部分語音分析文字；並自動依主題組織文字檔案的集合。您也可以使用 Amazon Comprehend 中使用 AutoML 功能來建置一組自訂的實體或文字分類模型，這些模型專為您的組織需求量身打造。若要進一步了解，請參閱 [Amazon Comprehend](#)。

AWS Managed Services 常見問答集中的 Amazon Comprehend

問：如何請求存取 AMS 帳戶中的 Amazon Comprehend？

您可以透過提交兩個 AMS Service RFCs 來請求 Amazon Comprehend 主控台和資料存取角色：

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_comprehend_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Comprehend 有哪些限制？

透過 Amazon Comprehend 主控台建立新的 IAM 角色功能受到限制。否則，Amazon Comprehend 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Comprehend 的先決條件或相依性是什麼？

如果 Amazon S3 儲存貯體使用 AWS KMS 金鑰加密，則需要 Amazon S3 和 AWS Key Management Service (AWS KMS) 才能使用 Amazon Comprehend。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Connect

Note

在仔細考慮之後，我們決定終止對 Amazon Connect Voice ID 的支援，自 2026 年 5 月 20 日起生效。自 2025 年 5 月 20 日起，Amazon Connect Voice ID 將不再接受新客戶。身為在 2025 年 5 月 20 日之前註冊服務的現有客戶，您可以繼續使用 Amazon Connect Voice ID 功能。2026 年 5 月 20 日之後，您將無法再使用 Amazon Connect Voice ID。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Connect 功能。Amazon Connect 是全通道雲端聯絡中心，可協助公司以較低的成本提供卓越的客戶服務。Amazon Connect 可為客戶和客服人員提供順暢的語音和聊天體驗。這包括一組用於技能型路由的工具、功能強大的即時和歷史分析，以及easy-to-use管理工具 - 全部都具有pay-as-you-go定價。

您可以在 AMS 多帳戶登陸區域或單一帳戶登陸區域帳戶中建立一或多個虛擬聯絡中心執行個體。您可以使用現有的 SAML 2.0 身分提供者進行代理程式存取，或使用 Amazon Connect 原生支援進行使用者生命週期管理。

此外，您可以從 Amazon Connect 主控台為每個 Amazon Connect 執行個體申請免付費電話/直撥電話號碼。您可以使用easy-to-use圖形使用者介面建立豐富的聯絡流程，以實現所需的客戶體驗和轉接。聯絡流程可以利用 AWS Lambda 函數與現場部署資料存放區和 API 整合。您也可以使用 Kinesis Streams 和 Firehose 啟用資料串流。

通話錄音、聊天文字記錄和報告存放在使用 AWS KMS 金鑰加密的 Amazon S3 儲存貯體中。聯絡流程日誌可以儲存到 CloudWatch 日誌群組。

若要進一步了解，請參閱 [Amazon Connect](#)。

AWS Managed Services 常見問答集中的 Amazon Connect

問：如何請求存取 AMS 帳戶中的 Amazon Connect？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_connect_console_role和customer_connect_user_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Connect 有哪些限制？

沒有限制。Amazon Connect 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Connect 的先決條件或相依性是什麼？

- 您必須使用標準 AMS RFCs 建立 AWS KMS 金鑰和 Amazon S3 儲存貯體；儲存通話錄音和聊天文字記錄時需要 Amazon S3 儲存貯體。
- 如果您想要與 Active Directory (AD) 整合，則需要 AD Connector 才能整合 AMS 託管的 Amazon Connect 執行個體和您的內部部署目錄服務。AD Connector 可以在您的帳戶中設定，方法是請求 'Management | Other | Other' RFC。
- 您可以根據您的聯絡流程需求，啟用下列選用的自行佈建服務。
 - AWS Lambda：您可以使用 Lambda 函數來擴展聯絡流程，以利用現有的內部部署資料存放區或 APIs。您可以使用 Lambda 自行佈建服務來建立 Lambda 函數。

- Amazon Kinesis Data Streams：您可以建立資料串流，以啟用資料串流至外部應用程式。您可以串流聯絡追蹤記錄或客服人員事件。
- Amazon Kinesis Data Firehose：您可以建立 Data Firehose，將大量聯絡追蹤記錄串流至外部應用程式。
- Amazon Lex：您可以利用 Amazon Lex Chatbots，利用 Amazon Alexa 服務建立智慧聯絡流程，以獲得豐富的客戶體驗和自動化。
- 問：如何請求新增撥出或撥入通話的國家/地區清單？

若要新增撥出或撥入通話的國家/地區清單，請向 AMS 提交服務請求。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Data Firehose

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Data Firehose 功能。Firehose 是可靠地將串流資料載入資料湖、資料存放區和分析工具的最簡單方法。它可以擷取、轉換串流資料，並將資料載入 Amazon S3、Amazon Redshift、Amazon OpenSearch Service 和 [Splunk](#)，以便使用您目前已使用的現有商業智慧工具和儀表板進行近乎即時的分析。這是一種全受管服務，可自動擴展以符合資料的輸送量，而且不需要持續管理。它也可以在載入資料之前批次處理、壓縮、轉換和加密資料，將目的地使用的儲存量降至最低，並提高安全性。若要進一步了解，請參閱[什麼是 Amazon Data Firehose？](#)

AWS Managed Services 常見問答集中的 Firehose

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Data Firehose？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_kinesis_firehose_user_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Firehose 有哪些限制？

沒有限制。Amazon Data Firehose 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Firehose 的先決條件或相依性是什麼？

必須為每個交付串流請求新的服務連結 IAM 角色。您也可以使用所需的資源許可（包括 S3 儲存貯體/KMS 金鑰/Lambda 函數/Kinesis 串流）更新角色政策，為所有串流重複使用單一服務連結角色。

在您提交 RFC 以新增 Firehose 之後，AMS Operations 工程師將透過服務請求與您聯絡，以取得您想要與 Data Firehose 連線的資源 ARNs（例如 AWS KMS S3、Lambda 和 Kinesis Streams）。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DevOpsGuru

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DevOpsGuru 功能。Amazon DevOpsGuru 是一項全受管操作服務，可讓開發人員和操作員輕鬆改善其應用程式的效能和可用性。DevOpsGuru 可讓您卸載與識別操作問題相關的管理任務，以便快速實作建議以改善應用程式。DevOpsGuru 會建立反應式洞見，您現在可以用來改善應用程式。它也會建立主動洞見，協助您避免未來可能會影響應用程式的操作問題。DevOpsGuru 會套用機器學習來分析您的操作資料和應用程式指標和事件，以識別偏離正常操作模式的行為。當 DevOpsGuru 偵測到操作問題或風險時，您會收到通知。對於每個問題，DevOps 都會提供智慧型建議，以解決目前和預測的未來營運問題。

若要進一步了解，請參閱[什麼是 Amazon DevOpsGuru](#)。

AWS Managed Services 常見問答集中的 Amazon DevOpsGuru

問：如何在我的 AMS 帳戶中請求存取 Amazon DevOpsGuru？

若要請求存取，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_devopsguru_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon DevOpsGuru 有哪些限制？

沒有限制。Amazon DevOpsGuru 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon DevOpsGuru 的先決條件或相依性是什麼？

沒有先決條件。DevOpsGuru 會利用下列 AWS 服務：Amazon CloudWatch Logs、RDS Insights AWS X-Ray AWS Lambda 和 AWS CloudTrail。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DocumentDB（與 MongoDB 相容）

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DocumentDB（具有 MongoDB 相容性）功能。Amazon DocumentDB（與 MongoDB 相容）是一種快速、可擴展、高可用性且全受管的文件資料庫服務，可支援 MongoDB 工作負載。Amazon DocumentDB 為您提供大規模操作關鍵任務 MongoDB 工作負載時所需的效能、可擴展性和可用性。Amazon DocumentDB 會透過模擬 MongoDB 用戶端從 MongoDB 伺服器預期的回應來實作 Apache 2.0 開放原始碼 MongoDB

3.6 API，讓您將現有的 MongoDB 驅動程式和工具與 Amazon DocumentDB 搭配使用。在 Amazon DocumentDB 中，儲存和運算會分離，允許每個獨立擴展，而且無論您的資料大小為何，您都可以新增最多 15 個低延遲僅供讀取複本，將讀取容量增加到每秒數百萬個請求。Amazon DocumentDB 旨在提供 99.99% 的可用性，並跨三個 AWS 可用區域 (AZs) 複寫資料的六個副本。您可以使用 AWS Database Migration Service (DMS) 免費（六個月）將內部部署或 Amazon Elastic Compute Cloud (Amazon EC2) MongoDB 資料庫遷移至 Amazon DocumentDB，幾乎沒有停機時間。若要進一步了解，請參閱 [Amazon DocumentDB（與 MongoDB 相容）](#)。

AWS Managed Services 常見問答集中的 Amazon DocumentDB

問：如何請求存取 AMS 帳戶中的 Amazon DocumentDB？

您可以透過提交兩個 AMS RFCs 來請求 Amazon DocumentDB 主控台和資料存取角色：主控台存取和資料存取：

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon DocumentDB。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_documentdb_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon DocumentDB 有哪些限制？

Amazon DocumentDB 需要 Amazon RDS 特定的許可。由於 AMS 完全管理 Amazon RDS，Amazon DocumentDB 的 IAM 角色包含對 Amazon RDS 上動作的一些限制。將適用以下限制：

- 對 DeleteDBInstance 和 DeleteDBCluster APIs 存取已受到限制。若要使用這些刪除 APIs，請提交 RFC 與 管理 | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策（需要檢閱）變更類型 (ct-27tuth19k52b4)。
- 您無法從 Amazon RDS 執行個體新增或移除標籤。
- 您無法將 Amazon DocumentDB 執行個體設為公有。

問：在我的 AMS 帳戶中使用 Amazon DocumentDB 的先決條件或相依性是什麼？

如果 Amazon S3 儲存貯體使用 AWS KMS 金鑰加密，AWS KMS 則需要 Amazon S3 和 才能使用 Amazon DocumentDB。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DynamoDB

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon DynamoDB (DynamoDB) 功能。Amazon DynamoDB 是金鑰值和文件資料庫，可在任何規模提供單一位數毫秒的效能。它是一個

全受管、多區域、多活動資料庫，具有內建安全性、備份和還原，以及適用於網際網路擴展應用程式的記憶體內快取。如需詳細資訊，請參閱 [Amazon DynamoDB](#)。

Amazon DynamoDB Accelerator (DAX) 是全部寫入快取服務，設計目的是要簡化將快取新增至 DynamoDB 資料表的程序。DAX 適用於需要高效能讀取的應用程式。

AWS Managed Services 常見問答集中的 DynamoDB

問：如何在我的 AMS 帳戶中請求存取 DynamoDB 和 DAX？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 DynamoDB 和 DAX。此 RFC 會將下列 IAM 角色和政策佈建至您的帳戶：

- DynamoDB 角色名稱：customer_dynamodb_role
- DAX 服務角色名稱：customer_dax_service_role
- DynamoDB 政策名稱：customer_dynamodb_policy
- DAX 服務政策：customer_dax_service_policy

在帳戶中佈建後，您必須在聯合解決方案customer_dynamodb_role中加入。

問：在我的 AMS 帳戶中使用 DynamoDB 有哪些限制？

支援所有 DynamoDB 功能，包括 DynamoDB Accelerator (DAX)。

為任何指定資料表建立警示時，警示名稱必須以「客戶*」字首；例如 customer-employee-table-high-put-latency。

為 DynamoDB 建立 Amazon SNS 主題時，必須命名為：dynamodb。

若要刪除 DynamoDB 建立的 Amazon SNS 主題，請提交管理 | 其他 | 其他 | 更新變更類型 RFC。

問：在我的 AMS 帳戶中使用 DynamoDB 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 DynamoDB 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Elastic Container Registry

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Elastic Container Registry (Amazon ECR) 功能。Amazon Elastic Container Registry 是全受管的 [Docker](#) 容器登錄檔，可讓開發人員輕鬆儲存、管理和部署 Docker 容器映像。Amazon ECR 與 [Amazon Elastic Container](#)

[Service \(Amazon ECS\)](#) 整合，可簡化生產工作流程的開發。Amazon ECR 無需操作您自己的容器儲存庫，也無需擔心擴展基礎基礎設施。Amazon ECS 會將您的映像託管在高可用性和可擴展的架構中，讓您可以可靠地部署應用程式的容器。與 AWS Identity and Access Management (IAM) 整合可提供每個儲存庫的資源層級控制。使用 Amazon ECR，無需預付費用或承諾。您只需為存放在儲存庫中的資料量和傳輸至網際網路的資料付費。

若要進一步了解，請參閱 [Amazon Elastic Container Registry](#)。

AWS Managed Services 常見問答集中的 Amazon Elastic Container Registry

問：如何請求存取 AMS 帳戶中的 Amazon ECR？

透過使用 [管理 | AWS 服務 | 自助佈建服務 | 新增 \(ct-1w8z66n899dct\)](#) 變更類型提交 RFC，請求存取 Amazon ECR。此 RFC 會將下列 IAM 角色佈建至您的帳戶：
`customer_ecr_console_role`和 `customer_ecr_poweruser_instance_profile_policy`分別`customer_ecr_poweruser_instance_profile`搭配相關聯的 IAM 政策
`customer_ecr_console_policy`和 `customer_ecr_poweruser_instance_profile_policy`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon ECR 有哪些限制？

AMS 命名空間有在您的 AMS 帳戶中使用 Amazon ECR 的限制。容器映像的字首不得為 "AMS-" 或 "Sentinel-"。

問：在我的 AMS 帳戶中使用 Amazon ECR 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon ECR 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 EC2 Image Builder

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 EC2 Image Builder 功能。EC2 Image Builder 是一項全受管 AWS 服務，可讓您更輕鬆地自動化建立、管理和部署自訂、安全且 up-to-date 「黃金」伺服器映像，這些映像已預先安裝並預先設定軟體和設定，以符合特定 IT 標準。

您可以使用 AWS Management Console、AWS CLI 或 APIs 在 AWS 帳戶中建立自訂映像。當您使用時 AWS Management Console，Amazon EC2 Image Builder 精靈會引導您完成以下步驟：

- 提供起始成品
- 新增和移除軟體
- 自訂設定和指令碼
- 執行選取的測試

- 將映像分發至 AWS 區域

您建置的映像會在您的帳戶中建立，並且可以持續針對作業系統修補程式進行設定。若要進一步了解，請參閱 [EC2 Image Builder](#)。

AWS Managed Services 常見問答集中的 EC2 Image Builder

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 EC2 Image Builder？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色：`customer_ec2_imagebuilder_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：EC2 Image Builder 有哪些限制？

AMS 不支援使用基礎設施組態的服務預設值。您可以建立新的基礎設施組態或使用現有的基礎設施組態。

AMS 目前不支援建立容器配方。

問：啟用 EC2 Image Builder 的先決條件或相依性有哪些？

- EC2 Image Builder 服務連結角色：您不需要手動建立服務連結角色。當您在 AWS Management Console、CLI 或 AWS API AWS 中建立第一個 Image Builder 資源時，Image Builder 會為您建立服務連結角色。
- 用於使用 Image Builder 建置映像和執行測試的執行個體必須能夠存取 Systems Manager 服務。如果來源映像尚未存在，則 SSM 代理程式會安裝在來源映像上，並在建立映像之前將其移除。
- AWS IAM：與執行個體描述檔建立關聯的 IAM 角色必須具有許可，才能執行映像中包含的建置和測試元件。下列 IAM 角色政策必須連接到與執行個體描述檔相關聯的 IAM 角色：`EC2InstanceProfileForImageBuilder`和 `AmazonSSMManagedInstanceCore`。IAM 角色名稱應該包含 `*imagebuilder*`關鍵字。
- 如果您設定記錄，則基礎設施組態中指定的執行個體描述檔必須具有目標儲存貯體 (S3) 的 `s3:PutObject`許可 `arn:aws:s3:::{bucket-name}/*`。例如：

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::{bucket-name}/*"
  }
]
```

- 建立名為 'imagebuilder' 的 SNS 主題，以接收來自 EC2 Image Builder 的任何提醒和通知。

使用 AMS SSP 在 AMS 帳戶中的 AWS Fargate 上佈建 Amazon ECS

使用 AMS 自助式佈建 (SSP) 模式直接在 AMS 受管帳戶中存取 Amazon ECS on AWS Fargate 功能。AWS Fargate 是一項技術，您可以與 Amazon ECS 搭配使用來執行容器（請參閱 [上的容器 AWS](#)），而無需管理 Amazon EC2 執行個體的伺服器或叢集。使用 AWS Fargate，您不再需要佈建、設定或擴展虛擬機器叢集來執行容器。這樣一來即無須選擇伺服器類型、決定何時擴展叢集，或最佳化叢集壓縮。

若要進一步了解，請參閱 [上的 Amazon ECS AWS Fargate](#)。

AWS Managed Services 常見問答集中的 Fargate 上的 Amazon ECS

問：如何在 AMS 帳戶中請求存取 Fargate 上的 Amazon ECS？

透過使用 Management | AWS service | Self-visioned service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Fargate 上的 Amazon ECS。此 RFC 會將下列 IAM 角色佈建至您的帳戶：
customer_ecs_fargate_console_role (如果沒有提供現有 IAM 角色將 ECS 政策與 建立關聯) customer_ecs_fargate_events_service_role、customer_ecs_task_execution_service_role 和 customer_ecs_codedeploy_service_role 和
AWSServiceRoleForApplicationAutoScaling_ECSService。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Fargate 上的 Amazon ECS 有哪些限制？

- Amazon ECS 任務監控和記錄會被視為您的責任，因為容器層級活動發生在 Hypervisor 上方，而記錄功能受到 Fargate 上的 Amazon ECS 限制。身為 Fargate 上的 Amazon ECS 使用者，我們建議

您採取必要步驟來啟用 Amazon ECS 任務的記錄。如需詳細資訊，請參閱[為您的容器啟用 awslogs 日誌驅動程式](#)。

- 容器層級的安全和惡意軟體保護也被視為您的責任。Fargate 上的 Amazon ECS 不包含 Trend Micro 或預先設定的網路安全元件。
- 此服務適用於多帳戶登陸區域和單一帳戶登陸區域 AMS 帳戶。
- 根據預設，自我佈建角色中的 Amazon ECS [Service Discovery](#) 會受到限制，因為建立 Route 53 私有託管區域需要更高的許可。若要在服務上啟用服務探索，請提交[管理 | 其他 | 其他 | 更新變更類型](#)。若要提供為 Amazon ECS Service 啟用 Service Discovery 所需的資訊，請參閱 [Service Discovery 手冊](#)。
- AMS 目前不會管理或限制用於在 Amazon ECS Fargate 上部署至容器的映像。您將能夠從 Amazon ECR、Docker Hub 或任何其他私有映像儲存庫部署映像。因此，我們建議不要部署公有或任何不安全的影像，因為它們可能會導致帳戶發生惡意活動。

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon ECS 的先決條件或相依性是什麼？

- 以下是 Fargate 上 Amazon ECS 的相依性；不過，使用自行佈建的角色啟用這些服務不需要其他動作：
 - CloudWatch Logs
 - CloudWatch 活動
 - CloudWatch 警示
 - CodeDeploy
 - App Mesh
 - 雲端地圖
 - Route 53
- 根據您的使用案例，以下是 Amazon ECS 所依賴的資源，在您的帳戶中使用 Fargate 上的 Amazon ECS 之前可能需要的資源：
 - 要與 Amazon ECS 服務搭配使用的安全群組。您可以使用[部署 | 進階堆疊元件 | 安全群組 | 建立 \(自動\) \(ct-3pc215bnwb6p7\)](#)，或者，如果您的安全群組需要特殊規則，請使用[部署 | 進階堆疊元件 | 安全群組 | 建立 \(需要檢閱\) \(ct-1oxx2g2d7hc90\)](#)。注意：您使用 Amazon ECS 選取的安全群組必須專門為 Amazon ECS 服務或叢集所在的 Amazon ECS 建立。您可以在 [Amazon Elastic Container Service 中的設定 Amazon ECS](#) 和[安全性一節](#)中進一步了解。<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/security.html>
 - 應用程式負載平衡器 (ALB)、網路負載平衡器 (NLB)、傳統負載平衡器 (ELB)，用於任務之間的負載平衡。

- ALBs 的目標群組。
- 要與您的 Amazon ECS 叢集整合的應用程式網格資源（例如 Virtual Router、Virtual Services、Virtual Nodes）。
- 目前，在標準 AMS 變更類型之外建立時，AMS 無法自動降低與支援安全群組許可相關的風險。我們建議您請求特定安全群組以搭配 Fargate 叢集使用，以限制使用非指定用於 Amazon ECS 的安全群組的可能性。

使用 AMS SSP 在您的 AMS 帳戶中 AWS Fargate 佈建 Amazon EKS

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 Amazon EKS on AWS Fargate 功能。AWS Fargate 是一種技術，可為容器提供隨需、大小正確的運算容量（若要了解容器，請參閱[什麼是容器？](#)）。使用 AWS Fargate，您不再需要佈建、設定或擴展虛擬機器群組來執行容器。這樣一來即無須選擇伺服器類型、決定何時擴展節點群組，或最佳化叢集壓縮。

Amazon Elastic Kubernetes Service (Amazon EKS) 透過 AWS Fargate 使用 Kubernetes 提供的 AWS 上游可擴展模型建置的控制器，將 Kubernetes 與整合。這些控制器作為 Amazon EKS 受管 Kubernetes 控制平面的一部分執行，並負責將原生 Kubernetes Pod 排程到 Fargate。Fargate 控制器包括新的排程器，除了數個變換與驗證許可控制器之外，也會隨著預設 Kubernetes 排程器執行。當您啟動符合在 Fargate 上執行之條件的 Pod 時，在叢集中執行的 Fargate 控制器便會辨識、更新及將 Pod 排程至 Fargate。

若要進一步了解，請參閱 [Amazon EKS on AWS Fargate Now Generally Available](#) 和 [Amazon EKS 安全最佳實務指南](#)（包括「建議」，例如「檢閱和撤銷不必要的匿名存取」等）。

Tip

AMS 具有變更類型：部署 | 進階堆疊元件 | 身分與存取管理 (IAM) | 建立 OpenID Connect 提供者 (ct-30ecvfi3tq4k3)，可與 Amazon EKS 搭配使用。如需範例，請參閱 [Identity and Access Management \(IAM\) | Create OpenID Connect Provider](#)。

AWS Managed Services 常見問答集 AWS Fargate 中的 Amazon EKS

問：如何在我的 AMS 帳戶中請求存取 Fargate 上的 Amazon EKS？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶。

- `customer_eks_fargate_console_role`.

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

- 這些服務角色授予 Amazon EKS on Fargate 代表您呼叫其他 AWS 服務的許可：
 - `customer_eks_pod_execution_role`
 - `customer_eks_cluster_service_role`

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon EKS 有哪些限制？

- AMS 不支援建立 [受管](#)或[自我管理](#)的 EC2 節點群組。如果您需要使用 EC2 工作者節點，請聯絡您的 AMS Cloud Service Delivery Manager (CSDM) 或 Cloud Architect (CA)。
- AMS 不包含 Trend Micro 或預先設定的容器映像網路安全元件。您需要管理自己的映像掃描服務，以在部署之前偵測惡意容器映像。
- 由於 CloudFormation 相互依存性，不支援 EKSCtl。
- 在叢集建立期間，您有停用叢集控制平面記錄的許可。如需詳細資訊，請參閱 [Amazon EKS 控制平面記錄](#)。我們建議您在建立叢集時啟用所有重要的 API、身分驗證和稽核記錄。
- 在叢集建立期間，Amazon EKS 叢集的叢集端點存取預設為公有；如需詳細資訊，請參閱 [Amazon EKS 叢集端點存取控制](#)。建議您將 Amazon EKS 端點設定為私有。如果公有存取需要端點，則最佳實務是僅針對特定 CIDR 範圍將其設定為公有。
- AMS 沒有強制和限制用於部署到 Amazon EKS Fargate 容器之映像的方法。您可以從 Amazon ECR、Docker Hub 或任何其他私有映像儲存庫部署映像。因此，部署可能在該帳戶上執行惡意活動的公有映像會有風險。
- AMS 不支援透過雲端開發套件 (CDK) 或 CloudFormation Ingest 部署 EKS 叢集。
- 您必須使用 [ct-3pc215bnwb6p7 部署 | 進階堆疊元件 | 安全群組 | 在資訊清單檔案中建立](#)和參考，以建立輸入。這是因為角色`customer-eks-alb-ingress-controller-role`未獲授權建立安全群組。

問：在我的 AMS 帳戶中在 Fargate 上使用 Amazon EKS 的先決條件或相依性是什麼？

若要使用 服務，必須設定下列相依性：

- 如需驗證服務，必須安裝 KUBECTL 和 `aws-iam-authenticator`；如需詳細資訊，請參閱[管理叢集身分驗證](#)。
- Kubernetes 倚賴稱為「服務帳戶」的概念。為了在 EKS 上利用 kubernetes 叢集內的服務帳戶功能，必須使用下列輸入進行管理 | 其他 | 更新 RFC：

- **【必要】** Amazon EKS 叢集名稱
- **【必要】** 將部署服務帳戶 (SA) 的 Amazon EKS 叢集命名空間。
- **【必要】** Amazon EKS 叢集 SA 名稱。
- **【必要】** 要關聯的 IAM 政策名稱和許可/文件。
- **【必要】** 正在請求的 IAM 角色名稱。
- **【選用】** OpenID Connect 提供者 URL。如需詳細資訊，請參閱
 - [在叢集上啟用服務帳戶的 IAM 角色](#)
 - [為服務帳戶介紹精細的 IAM 角色](#)
- 建議您設定和監控 Config 規則
 - 公有叢集端點
 - 停用 API 記錄

您有責任監控和修復這些 Config 規則。

如果您想要部署 [ALB 傳入控制器](#)，請提交管理 | 其他 | 其他更新 RFC，以佈建要與 ALB 傳入控制器 Pod 搭配使用的必要 IAM 角色。建立要與 ALB 傳入控制器建立關聯的 IAM 資源（請在 RFC 中包含這些資源）需要下列輸入：

- **【必要】** Amazon EKS 叢集名稱
- **【選用】** OpenID Connect 提供者 URL
- **【選用】** Amazon EKS 叢集命名空間，其中將部署應用程式負載平衡器 (ALB) 輸入控制器服務。
【預設：kube-system】
- **【選用】** Amazon EKS 叢集服務帳戶 (SA) 名稱。**【預設：aws-load-balancer-controller】**

如果您想要在叢集中啟用信封秘密加密（我們建議），請在 RFC 的描述欄位中提供您要使用的 KMS 金鑰 IDs，以新增服務 (Management | AWS service | Self-visited service | Add (ct-1w8z66n899dct)。若要進一步了解信封加密，請參閱 [Amazon EKS 使用 AWS KMS 新增秘密的信封加密](#)。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon EMR

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon EMR 功能。Amazon EMR 是領先業界的雲端大數據平台，可使用 Apache Spark、Apache Hive、Apache HBase、Apache Flink、Apache Hudi 和 Presto 等開放原始碼工具來處理大量資料。使用 Amazon EMR，您可以執行

PB 級分析，成本不到傳統內部部署解決方案的一半，比標準 Apache Spark 快 3 倍以上。對於短期執行的任務，您可以向上和向下旋轉叢集，並為使用的執行個體每秒付費。對於長時間執行的工作負載，您可以建立高度可用的叢集，以自動擴展以滿足需求。

您可以在 AMS 多帳戶登陸區域或單一帳戶登陸區域帳戶中建立一或多個 Amazon EMR 叢集執行個體，以支援暫時性和持久性 Amazon EMR 叢集。您也可以啟用 Kerberos 身分驗證，以啟用來自內部部署 Active Directory 網域的身分驗證使用者。

您可以使用 Amazon EMR 叢集利用多個資料存放區，以支援使用案例特定的 Hadoop 工具和程式庫。您可以使用 OnDemand 或 Spot 執行個體建立 Amazon EMR 叢集，並設定自動擴展以管理容量並降低成本。

叢集日誌檔案可以封存到 Amazon S3 儲存貯體以進行記錄和偵錯。您也可以存取 Amazon EMR 叢集中託管的 Web 介面，以支援雜湊管理要求或為客戶記錄書籍體驗。

若要進一步了解，請參閱 [Amazon EMR](#)。

AWS Managed Services 常見問答集中的 Amazon EMR

問：如何請求存取 AMS 帳戶中的 Amazon EMR？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

在帳戶中佈建後，您必須在聯合解決方案中加入 `customer_emr_console_role`。

問：在我的 AMS 帳戶中使用 Amazon EMR 有哪些限制？

從 AWS 主控台在 EC2 叢集上建立 Amazon EMR 時，我們建議您使用建立叢集 – 進階選項。Amazon EMR 叢集必須透過新增索引鍵為「for-use-with-amazon-emr-managed-policies」且值為「true」的標籤來建立。在安全選項中選取下列組態：

- 選取叢集的自訂角色：
 - EMR 角色：`Customer_emr_cluster_service_role`

- EC2 執行個體設定檔：Customer_emr_cluster_instance_profile
- Auto Scaling 角色：Customer_emr_cluster_autoscaling_role
- EC2 安全群組：
 - 主要：ams-emr-master-security-group
 - 核心與任務：ams-emr-worker-security-group
 - 服務存取：ams-emr-serviceaccess-security-group

問：在我的 AMS 帳戶中使用 Amazon EMR 的先決條件或相依性是什麼？

AMS 會為 Amazon EMR 主節點、工作者節點和服務節點建立預設安全群組。

要與 Amazon EMR 叢集搭配使用的啟動範本和安全群組必須具有值為 "true" 的標籤索引鍵 "for-use-with-amazon-emr-managed-policies"。

預設 Amazon EMR 叢集執行個體描述檔可讓您存取資源，例如 s3 儲存貯體和 dynamodb 資料表，其名稱包含 "emr"。您可以請求其他 IAM 政策，以使用與 Amazon EMR 搭配使用的任何其他資源。下列資源 ARN 可與使用 customer_emr_cluster_instance_profile 的 Amazon EMR 任務搭配使用：

- arn : aws : dynamodb : * : * : table/*emr*
- arn : aws : kinesis : * : * : stream/*emr*
- arn : aws : sns : * : * : *emr*arn : aws : sqs : * : * : *emr*
- arn : aws : sqs : * : * : *emr*
- arn : aws : sqs : * : * : AWS-ElasticMapReduce-*
- arn : aws : sdb : * : * : domain : *emr*
- arn : aws : s3 : : *emr*

如果 Amazon EMR 叢集需要 kerberos 身分驗證：

- 提供要用於每個角化 Amazon EMR 叢集的領域名稱和內部部署 Active Directory IP 地址。
- 基礎設施需求：

多帳戶登陸區域 (MALZ)：提交 RFC 以在現有應用程式帳戶中建立新的受管應用程式帳戶或新的 VPC。

單一帳戶登陸區域 (SALZ)：提交 RFC 以在 VPC 中建立新的子網路。

- 在內部部署 Active Directory 上設定叢集領域傳入的信任。
- 在 Managed AD 中提交 RFC 來設定領域 DNS 區域。
- 領域組態：

MALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以更新 VPC DHCP 選項集，以使用網域名稱尾碼的領域名稱。

SALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC，以產生新的 Amazon EMR AMI，以使用網域名稱尾碼的特定領域。

若要部署 Amazon EMR Studio，角色 `customer_emr_cluster_service_role` 具有 Amazon Simple Storage Service 儲存貯體的先決條件。若要建立儲存貯體，請使用自動化 CT `ct-1a68ck03fn98r`（部署 | 進階堆疊元件 | S3 儲存 | 建立）。當您使用此自動化 CT 為 Amazon EMR 建立 Amazon S3 儲存貯體時，儲存貯體名稱必須以字首開頭 `customer-emr-*`。此外，您必須在與 Amazon EMR 叢集相同的 AWS 區域中建立儲存貯體。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon EventBridge

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon EventBridge 功能。Amazon EventBridge 為無伺服器事件匯流排服務，可讓您輕鬆將應用程式與來自各種來源的資料互相連線。EventBridge 可從您自己的應用程式、Software-as-a-Service(SaaS) 應用程式 AWS 和服務提供即時資料串流，並將該資料路由至等目標 AWS Lambda。您可設定路由規則來決定要將資料送往何處，以便建立即時對您所有資料來源做出反應的應用程式架構。EventBridge 可讓您建置鬆耦合和分散式的事件驅動架構。

若要進一步了解，請參閱 [Amazon EventBridge](#)。

AWS Managed Services 常見問答集中的 EventBridge

問：如何請求存取 AMS 帳戶中的 EventBridge？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 EventBridge。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_eventbridge_role` 和 `customer_eventbridge_scheduler_execution_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

執行角色，`customer_eventbridge_scheduler_execution_role` 是 EventBridge 排程器擔任代表您與其他互動的 IAM 角色 AWS 服務。連接到此角色的許可政策會授予 EventBridge 排程器調用目標的存取權。

 Note

根據預設，EventBridge 排程器會使用 EventBridge 的 AWS 擁有金鑰來加密資料。若要使用 EventBridge 的客戶受管金鑰來加密資料，請使用 [Management | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）變更類型 \(ct-3qe6io8t6jtny\)](#) 提交 RFC 以進行服務佈建。

問：在我的 AMS 帳戶中使用 EventBridge 有哪些限制？

您必須提交 AMS RFCs 並建立下列資源：觸發批次任務的服務角色、SQS 佇列、CodeBuild、CodePipeline 和 SSM 命令。

問：在我的 AMS 帳戶中使用 EventBridge 的先決條件或相依性是什麼？

您必須使用 [部署 | EventBridge 進階堆疊元件 | Identity and Access Management \(IAM\) | 建立實體或政策（需要檢閱）變更類型 \(ct-3dpd8mdd9jn1r\)](#) 請求具有 RFC 的 EventBridge 服務角色，才能使用 EventBridge 觸發其他 AWS 資源 AWS Batch，例如 Lambda、Amazon SNS、Amazon SQS 或 Amazon CloudWatch Logs 資源。指定請求您的服務角色時要叫用的服務。若要了解叫用目標所需的許可，請參閱[使用 EventBridge 的資源型政策](#)。

EventBridge 已與整合 AWS CloudTrail，此服務提供由使用者、角色或 EventBridge AWS 服務中所採取動作的記錄。必須啟用並允許 CloudTrail 將日誌檔案存放到 S3 儲存貯體。注意：所有 AMS 帳戶都已啟用 CloudTrail，因此不需要採取任何動作。

問：角色 `customer_eventbridge_scheduler_execution_role` 具有 AWS Key Management Service 金鑰的先決條件（選用，如果用於加密）。如何在靜態/傳輸資料加密中採用 AWS KMS CMKs？

根據預設，EventBridge 排程器會加密儲存在 AWS 擁有金鑰（靜態加密）下的事件中繼資料和訊息資料。EventBridge 排程器也會使用 Transport Layer Security (TLS)（傳輸中加密）加密 EventBridge 排程器與其他服務之間傳遞的資料。

如果您的特定使用案例要求您控制和稽核可在 EventBridge 排程器上保護資料的加密金鑰，您可以使用客戶受管金鑰。

在使用 Amazon EventBridge 加入 AWS KMS 許可之前，您必須使用 [管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）變更類型](#) 來請求 RFC。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Forecast

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Forecast (預測) 功能。Amazon Forecast 是一種全受管服務，使用機器學習來提供高度準確的預測。

Note

AWS 自 2024 年 7 月 29 日起，已關閉新客戶對 Amazon Forecast 的存取權。Amazon Forecast 現有客戶可以繼續照常使用服務。AWS 會繼續投資 Amazon Forecast 的安全性、可用性和效能改善，但不 AWS 打算推出新功能。

如果您想要使用 Amazon Forecast，請聯絡您的 CSDM，以便他們可以進一步指導您如何將 [Amazon Forecast 用量轉移至 Amazon SageMaker Canvas](#)。

根據 Amazon.com 使用的相同技術，Forecast 使用機器學習來結合時間序列資料和其他變數來建置預測。預測不需要機器學習經驗即可開始。您只需要提供歷史資料，以及您認為可能會影響預測的任何其他資料。例如，對襯衫特定顏色的需求可能會隨季節和存放位置而改變。這種複雜的關係很難自行判斷，但機器學習非常適合識別它。提供資料後，預測會自動檢查資料、識別有意義的內容，並產生預測模型，能夠進行比僅查看時間序列資料高出 50% 的預測。

若要進一步了解，請參閱 [Amazon Forecast](#)。

AWS Managed Services 常見問答集中的 Amazon Forecast

問：如何請求存取 AMS 帳戶中的預測？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS Firewall Manager 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_forecast_admin_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用預測有哪些限制？

預設 S3 儲存貯體存取僅允許您存取命名模式為 'customer-forecast-*' 的儲存貯體。如果您有自己的資料儲存貯體命名慣例，請與您的 Cloud Architect (CA) 討論儲存貯體命名和相關存取設定。例如：

- 您可以使用 'AmazonForecast-ExecutionRole-*' 等命名和相關聯的適當 S3 儲存貯體存取來定義特定 AmazonForecast 服務角色。請參閱 IAM 主控台下的服務角色 - AmazonForecast-ExecutionRole-Admin 和 IAM 政策 - customer_forecast_default_s3_access_policy。
- 您可能需要將相關的 S3 儲存貯體存取與 IAM 聯合角色建立關聯。請參閱 IAM 主控台下的 IAM 政策 - customer_forecast_default_s3_access_policy。

問：在我的 AMS 帳戶中使用 Forecast 有哪些先決條件或相依性？

- 使用 Forecast 之前，必須先建立適當的 Amazon S3 儲存貯體 (Amazon S3)。特別是，預設 S3 儲存貯體存取是使用命名模式「customer-forecast-*」
- 如果您想要在 'customer-forecast-*' 以外的 S3 儲存貯體上使用命名模式，則必須在儲存貯體上建立具有 S3 存取許可的新服務角色：
 1. 使用命名 'AmazonForecast-ExecutionRole-{suffix}' 來建立新的服務角色。
 2. 要建立的新 IAM 政策類似於 customer_forecast_default_s3_access_policy，並與新服務角色和相關聯合管理員角色相關聯（例如 'customer_forecast_admin_role'）

問：如何使用 Amazon Forecast 增強資料安全性？

- 對於靜態資料加密，您可以使用 AWS KMS 來佈建客戶管理的 CMK，以保護 Amazon S3 服務上的資料儲存：
 - 使用佈建金鑰在儲存貯體上啟用預設加密，並設定儲存貯體政策以接受 AWS KMS 資料加密，同時放置資料。
 - 以 AWS KMS 金鑰使用者身分啟用 Amazon Forecast 服務角色 'AmazonForecast-ExecutionRole-*' 和聯合管理角色（例如 'customer_forecast_admin_role'）。
- 對於傳輸中的資料加密，您可以設定 HTTPS 通訊協定，這是在 Amazon S3 儲存貯體政策上傳物件時的必要通訊協定。
- 存取控制的進一步限制，為 Amazon Forecast 服務角色 'AmazonForecast-ExecutionRole-*' 和管理員角色（例如 'customer_forecast_admin_role'）的核准存取啟用儲存貯體政策。

問：使用 Amazon Forecast 時的最佳實務為何？

- 您應該充分了解資料分類實務，並在搭配 Amazon Forecast 使用 S3 儲存貯體時，找出相關的資料安全需求。
- 對於 Amazon S3 儲存貯體組態，強烈建議您在 S3 儲存貯體政策中啟用 HTTPS 強制執行。
- 您必須知道 Amazon S3 儲存貯體上的管理員角色 'customer_forecast_admin_role' 支援許可存取 (Get/Delete/Put S3 物件)，其命名為 'customer-forecast-*'。Amazon S3 注意：如果您需要多個團隊的精細存取控制，請遵循下列實務：
 - 定義以團隊為基礎的存取 IAM 身分（角色/使用者），具有對相關 Amazon S3 儲存貯體的最低權限存取權。
 - 建立以團隊/專案為基礎的 AWS KMS CMKs 會授予對對應 IAM 身分的適當存取權。（使用者存取權和 'AmazonForecast-ExecutionRole-{team/project}'）。

- 使用已建立 AWS KMS CMKs 設定 S3 儲存貯體預設加密。
- 在 S3 儲存貯體政策上使用 HTTPS 通訊協定強制執行 S3 API 流量。
- 強制執行 S3 儲存貯體組態，以針對相關 IAM 身分（使用者存取和儲存貯體的 'AmazonForecast-ExecutionRole-{team/project}'）。
- 如果您想要將 'customer_forecast_admin_role' 用於一般用途，請考慮先前列出的點以保護 S3 儲存貯體。

問：Amazon Forecast 的合規資訊在哪裡？

請參閱 [AWS 服務合規計劃](#)。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon FSx 功能。Amazon FSx 提供全受管第三方檔案系統。Amazon FSx 為您提供第三方檔案系統的原生相容性，其功能集適用於 Windows 型儲存、高效能運算 (HPC)、機器學習和電子設計自動化 (EDA) 等工作負載。Amazon FSx 會自動執行耗時的管理任務，例如硬體佈建、軟體組態、修補和備份。Amazon FSx 將檔案系統與雲端原生 AWS 服務整合，讓它們更適用於更廣泛的工作負載集。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 [Amazon FSx](#)。

AWS Managed Services 常見問答集中的 Amazon FSx

問：如何請求存取 AMS 帳戶中的 Amazon FSx？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_fsx_admin_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon FSx 有哪些限制？

沒有限制。服務的完整功能可供使用。

問：在我的 AMS 帳戶中使用 Amazon FSx 有哪些先決條件或相依性？

沒有先決條件。不過，對於多可用區等進階組態，您必須安裝和管理 DFS 複寫和 DFS 命名空間服務。如需詳細資訊，請參閱[部署多可用區域檔案系統](#)。

問：如何將 Amazon FSx 檔案系統與多帳戶登陸區域 Managed AD 整合？

建立 Amazon FSx 檔案系統時，您可以將 MALZ Managed AD 指定為 'AWS Managed Microsoft Active Directory' for Windows Authentication。如需詳細資訊，請參閱[搭配 AWS Directory Service for Microsoft Active Directory 使用 Amazon FSx](#)

您也必須先將 Managed AD 分享給應用程式帳戶。透過使用 Management | Directory Service | Directory | Share Directory 變更類型 (ct-369odosk0pd9w) 提交 RFC 來執行此操作。

問：哪些使用者屬於 AWS 委派 FSx 管理員群組？

只有 IT 檔案伺服器管理員。此群組具有所有檔案共享的完整存取權限。

問：我應該使用佈建 FSx 系統時建立的預設檔案共享、共享嗎？

否，不建議依佈建使用預設檔案共享、共享。它將完整存取權授予每個人，這違反最低權限原則。相反地，請建立符合您業務需求的較小自訂檔案共享。

問：如何為業務中的特定組織建立自訂檔案共享？

如需建立自訂[檔案共享](#)的說明，請參閱檔案共享。使用最低權限原則限制每個檔案共享的存取。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx for OpenZFS

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon FSx for OpenZFS 功能。FSx for OpenZFS 是一種全受管檔案儲存服務，可讓您輕鬆地將內部部署 ZFS 或其他 Linux 型檔案伺服器中的資料移至 AWS，而無需變更應用程式程式碼或管理資料的方式。它提供以開放原始碼 OpenZFS 檔案系統建置的高度可靠、可擴展性、高效能和功能豐富的檔案儲存，提供 OpenZFS 檔案系統的熟悉功能和功能，以及全受管 AWS 服務的敏捷性、可擴展性和簡易性。對於建置雲端原生應用程式的開發人員，它提供簡單、高效能的儲存體，具有豐富的資料使用功能。

FSx for OpenZFS 檔案系統可使用業界標準的 NFS 通訊協定 (v3、v4.0、v4.1、v4.2)，從 Linux、Windows 和 macOS 運算執行個體和容器廣泛存取。FSx for OpenZFS 採用 AWS Graviton 處理器和最新的 AWS 磁碟和聯網技術（包括 AWS 可擴展可靠資料包聯網和 AWS Nitro 系統），可提供高達 100 萬個 IOPS，延遲數百微秒。透過對即時point-in-time快照和資料複製等 OpenZFS 功能的完整支援，FSx for OpenZFS 可讓您輕鬆地將內部部署檔案伺服器取代為提供熟悉檔案系統功能的 AWS 儲存體，並消除執行冗長資格和變更或重新建構現有應用程式或工具的需求。此外，透過結合 OpenZFS 資料管理功能的強大功能與最新 AWS 技術的高效能和成本效益，FSx for OpenZFS 可讓您建置和執行高效能的資料密集型應用程式。

做為全受管服務，FSx for OpenZFS 可讓您在 上輕鬆啟動、執行和擴展全受管檔案系統 AWS，以取代您在內部部署中執行的檔案伺服器，同時協助提供更好的敏捷性和降低成本。使用 FSx for OpenZFS，您不再需要擔心設定和佈建檔案伺服器和儲存磁碟區、複寫資料、安裝和修補檔案伺服器軟體、偵測和解決硬體故障，以及手動執行備份。它還提供與其他 AWS 服務的豐富整合，例如 AWS Identity and Access Management (IAM)、AWS Key Management Service (AWS KMS)、Amazon CloudWatch 和 AWS CloudTrail。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 [Amazon FSx](#)。

AWS Managed Services 常見問答集中的 Amazon FSx for OpenZFS

問：如何請求在我的 AMS 帳戶中使用 FSx for OpenZFS 的存取權？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx OpenZFS。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_fsx_ontap_admin_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 FSx for OpenZFS 有哪些限制？

取代 Amazon FSx 彈性網路介面 (ENIs) 上的安全群組需要您提交管理 | 其他 | 其他 | 更新 RFCs 因為安全群組是 AMS 環境的關鍵周邊。這是唯一的限制。

問：在我的 AMS 帳戶中使用 FSx for OpenZFS 的先決條件或相依性是什麼？

沒有先決條件。不過，您必須[使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx](#) 已安裝。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx for NetApp ONTAP

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon FSx for NetApp ONTAP 功能。Amazon FSx for NetApp ONTAP 是一項全受管服務，可在 NetApp 的熱門 ONTAP 檔案系統上提供高度可靠、可擴展、高效能且功能豐富的檔案儲存。它提供 NetApp 檔案系統的熟悉功能、效能、功能和 APIs，具有完全受管的靈活性、可擴展性和簡易性 AWS 服務。

Amazon FSx for NetApp ONTAP 提供功能豐富、快速且靈活的共用檔案儲存，可從 Linux、Windows 和在內部部署中執行 AWS 的 macOS 運算執行個體廣泛存取。FSx for ONTAP 提供低於毫秒延遲的高效能 SSD 儲存體，讓您只要按一下按鈕，即可快速且輕鬆地管理您的資料。它也會自動將資料分層為成本較低的彈性儲存，無需佈建或管理容量，並可讓您為工作負載達到 SSD 效能層級，同時只需

為一小部分的資料支付 SSD 儲存費用。它提供高可用性和耐用的儲存，具有全受管備份，並支援跨區域災難復原，並支援熱門的資料安全和防毒應用程式，讓您更輕鬆地保護和保護您的資料。對於使用 NetApp ONTAP 內部部署的客戶，FSx for ONTAP 是將檔案型應用程式從內部部署遷移、備份或爆量到的理想解決方案，AWS 而無需變更應用程式程式碼或管理資料的方式。

Amazon FSx for NetApp ONTAP 是全受管服務，可讓您在雲端輕鬆啟動和擴展可靠、高效能且安全的共用檔案儲存。使用 Amazon FSx for NetApp ONTAP，您不再需要擔心設定和佈建檔案伺服器 and 儲存磁碟區、複寫資料、安裝和修補檔案伺服器軟體、偵測和解決硬體故障、管理容錯移轉和容錯回復，以及手動執行備份。它也提供與其他的豐富整合 AWS 服務，例如 AWS Identity and Access Management Amazon WorkSpaces AWS Key Management Service 和 AWS CloudTrail。

Amazon FSx 為您提供兩種檔案系統供您選擇：適用於 Windows 應用程式的 Amazon FSx for Windows File Server 和適用於運算密集型工作負載的 Amazon FSx for Lustre。若要進一步了解，請參閱 [Amazon FSx](#)。

AWS Managed Services 常見問答集中的 Amazon FSx for NetApp ONTAP

問：如何在我的 AMS 帳戶中請求存取 Amazon FSx for NetApp ONTAP？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon FSx for NetApp ONTAP。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_fsx_ontap_admin_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon FSx for NetApp ONTAP 有哪些限制？

取代 Amazon FSx for NetApp ONTAP 彈性網路介面 (ENIs) 上的安全群組需要您提交管理 | 其他 | 其他 | 更新 RFCs 因為安全群組是 AMS 環境的關鍵周邊。這是唯一的限制。

問：在我的 AMS 帳戶中使用 Amazon FSx for NetApp ONTAP 的先決條件或相依性是什麼？

沒有先決條件。不過，您必須[使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx](#) 已安裝。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Inspector Classic

Note

支援結束通知：2026 年 5 月 20 日，AWS 將結束對 Amazon Inspector Classic 的支援。2026 年 5 月 20 日之後，您將無法再存取 Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。Amazon Inspector Classic 將不再提供給新帳戶，以及過去六個月內尚未完成評估的帳戶。對於所有其他帳戶，存取將持續有效至 2026 年 5 月 20 日，之後您將無法再存取

Amazon Inspector Classic 主控台或 Amazon Inspector Classic 資源。如需詳細資訊，請參閱 [Amazon Inspector Classic 終止支援](#)。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Inspector Classic 功能。Amazon Inspector Classic 是一種自動化安全評估服務，可協助改善部署在 AWS 上的應用程式的安全性和合規性。Amazon Inspector Classic 會自動評估應用程式是否有暴露、漏洞和與最佳實務的偏差。執行評估後，Amazon Inspector Classic 會產生依嚴重性層級排定優先順序的安全調查結果詳細清單。這些調查結果可以直接檢閱，也可以作為詳細評估報告的一部分，這些報告可透過 Amazon Inspector Classic 主控台或 API 取得。若要進一步了解，請參閱 [Amazon Inspector Classic](#)。

AWS Managed Services 常見問答集中的 Amazon Inspector

問：如何在我的 AMS 帳戶中請求存取 Amazon Inspector Classic？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Amazon Inspector Classic。此 RFC 會將 `customer_inspector_admin_role` IAM 角色佈建至您的帳戶。此角色包含受 AWS 管 AmazonInspectorFullAccess 政策。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Inspector Classic 有哪些限制？

沒有限制。Amazon Inspector Classic 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Inspector Classic 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Inspector Classic 沒有先決條件或相依性。

在 AMS 中使用新的 Amazon Inspector

您現在可以在 AMS 帳戶中使用新的 Amazon Inspector。

對於 Amazon Inspector Classic，`AmazonInspectorFullAccess` 需要 `customer-inspector-admin-role-ssm-inspector-agent-policy` 和 `customer-inspector-admin-role`。不過，SSPS 角色已更新 `customer-inspector-admin-role`，現在包含額外的 `policyAmazonInspector2FullAccess`。此新政策允許新版本 Amazon Inspector 的 API 許可。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kendra

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Kendra 功能。Amazon Kendra 是一種智慧型搜尋服務，使用自然語言處理和進階機器學習演算法傳回從資料搜尋問題的

特定答案。與傳統的關鍵字式搜尋不同，Amazon Kendra 會使用其語意和內容理解功能來判斷文件是否與搜尋查詢相關。Amazon Kendra 會傳回問題的特定答案，因此您的體驗即將與人類專家互動。Amazon Kendra 具有高度可擴展性，能夠滿足效能需求，與 Amazon S3 和 Amazon Lex 等 AWS 其他服務緊密整合，並提供企業級安全性。若要進一步了解，請參閱 [Amazon Kendra](#) 。

AWS Managed Services 常見問答集中的 Amazon Kendra

問：如何請求存取 AMS 帳戶中的 Amazon Kendra ？

若要請求存取 Amazon Inspector Classic，請使用 Management | AWS service | Self-visited Service | Add (ct-3qe6io8t6jtny) 變更類型提交 RFC。此 RFC 會將 `customer_kendra_console_role` IAM 角色佈建至您的帳戶。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kendra 有哪些限制？

沒有限制。Amazon Kendra 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kendra 的先決條件或相依性是什麼？

Amazon Kendra 入門沒有先決條件或相依性。不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kinesis Data Streams

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Kinesis Data Streams (KDS) 功能。Amazon Kinesis Data Streams 是一種高度可擴展且耐用的即時資料串流服務。KDS 可以持續從數十萬個來源擷取每秒 GB 的資料，例如網站點擊串流、資料庫事件串流、金融交易、社交媒體摘要、IT 日誌和位置追蹤事件。收集的資料以毫秒為單位提供，以啟用即時分析使用案例，例如即時儀表板、即時異常偵測、動態定價等。若要進一步了解，請參閱 [Amazon Kinesis Data Streams](#)。

AWS Managed Services 中的 Kinesis Data Streams 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Kinesis Data Streams ？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC，請求存取 Amazon Kinesis Data Streams。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_kinesis_data_streaming_user_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 有哪些限制？

沒有限制。Amazon Kinesis Data Streams 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Kinesis Data Streams 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Kinesis Video Streams

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Kinesis Video Streams (KVS) 功能。Amazon Kinesis Video Streams 可協助您安全地將視訊從連線裝置串流到 AWS 以進行分析、機器學習 (ML)、播放和其他處理。Kinesis Video Streams 會自動佈建並彈性擴展從數百萬個裝置擷取串流影片資料所需的所有基礎設施。它也會長期儲存、加密和索引串流中的影片資料，並可讓您透過 easy-to-use 存取資料。APIs Kinesis Video Streams 可讓您播放影片以進行即時和隨需檢視，並透過與 Amazon Rekognition Video 整合，以及適用於 Apache MxNet、TensorFlow 和 OpenCV 等 ML 架構的程式庫，快速建置利用電腦視覺和影片分析的應用程式。若要進一步了解，請參閱 [Amazon Kinesis Video Streams](#)。

AWS Managed Services 中的 Amazon Kinesis Video Streams 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Kinesis Video Streams？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC，請求存取 Amazon Kinesis Video Streams。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_kinesis_video_streaming_user_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Video Streams 有哪些限制？

沒有限制。Amazon Kinesis Video Streams 的完整功能可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Video Streams 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Kinesis Video Streams 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Lex

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Lex 功能。Amazon Lex 是一種使用語音和文字在任何應用程式中建置對話界面的服務。Amazon Lex 提供自動語音辨識 (ASR) 的

進階深度學習功能，可將語音轉換為文字，以及自然語言理解 (NLU) 來辨識文字的意圖，讓您能夠建置具有高度吸引力使用者體驗和逼真的對話互動的應用程式。透過 Amazon Lex，任何開發人員現在都可以使用與支援 Amazon Alexa 相同的深度學習技術，讓您能夠快速輕鬆地建置複雜的自然語言、對話式機器人或聊天機器人。若要進一步了解，請參閱 [Amazon Lex](#)。

AWS Managed Services 中的 Amazon Lex 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Lex？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_lex_author_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Lex 有哪些限制？

Amazon Lex 與 Lambda 的整合僅限於沒有「AMS-」字首的 Lambda 函數，以防止對 AMS 基礎設施進行任何修改。

問：在我的 AMS 帳戶中使用 Amazon Lex 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon Lex 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon MQ

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon MQ 功能。Amazon MQ 是 Apache ActiveMQ 的受管訊息代理程式服務，可協助您在雲端中設定和操作訊息代理程式。訊息代理程式允許不同的軟體系統，通常使用不同的程式設計語言，並在不同的平台上進行通訊和交換資訊。Amazon MQ 透過管理 ActiveMQ 的 ActiveMQ 是熱門的開放原始碼訊息代理程式。將您目前的應用程式連線至 Amazon MQ 會使用業界標準 APIs 和通訊協定進行傳訊，包括 JMS、NMS、AMQP、STOMP、MQTT 和 WebSocket。使用標準表示在大多數情況下，遷移到時不需要重寫任何訊息程式碼 AWS。若要進一步了解，請參閱 [什麼是 Amazon MQ？](#)

AWS Managed Services 常見問答集中的 Amazon MQ

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon MQ？

在您的 AMS 帳戶中使用 Amazon MQ 是一個兩步驟的程序：

1. 佈建 Amazon MQ 中介裝置。若要這樣做，請透過 RFC 提交包含 Amazon MQ 代理程式的 CFN 範本，並使用 `部署 | 擷取 | 從 CloudFormation 範本堆疊 | 建立變更類型 (ct-36cn2avfrj9v)`，或使用 `管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76)` 變更類型，請求在您的帳戶中佈建 Amazon MQ 代理程式。
2. 存取 Amazon MQ 主控台。佈建 Amazon MQ 中介裝置之後，透過使用 `Management | AWS service | Self-visited service | Add change type (ct-1w8z66n899dct)` 提交 RFC 來取得 Amazon MQ 主控台的存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_mq_console_role`。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入該角色。

問：在我的 AMS 帳戶中使用 Amazon MQ 有哪些限制？

Amazon MQ 的完整功能可在您的 AMS 帳戶中使用；不過，由於需要更高的許可，因此無法透過政策佈建 Amazon MQ 代理程式。如需如何在帳戶中佈建 Amazon MQ 代理程式的詳細資訊，請參閱上述內容。

問：在我的 AMS 帳戶中使用 Amazon MQ 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Amazon MQ 沒有先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Service for Apache Flink

使用 AMS 自助式服務佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Managed Service for Apache Flink 功能。Managed Service for Apache Flink 是分析串流資料、取得可行洞見以及即時回應業務和客戶需求的最簡單方法。Amazon Managed Service for Apache Flink 可降低建置、管理和整合串流應用程式與其他 AWS 服務的複雜性。SQL 使用者可以輕鬆查詢串流資料，或使用範本和互動式 SQL 編輯器建置整個串流應用程式。Java 開發人員可以使用開放原始碼 Java 程式庫和 AWS 整合快速建置複雜的串流應用程式，以即時轉換和分析資料。Amazon Managed Service for Apache Flink 會處理持續執行即時應用程式所需的一切，並自動擴展以符合傳入資料的磁碟區和輸送量。使用 Amazon Managed Service for Apache Flink，您只需為串流應用程式使用的資源付費。沒有最低費用或設定成本。若要進一步了解，請參閱 [Amazon Managed Service for Apache Flink](#)。

AWS Managed Services 常見問答集中的 Managed Service for Apache Flink

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Managed Service for Apache Flink？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny)

變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

customer_kinesis_analytics_application_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Apache Flink 有哪些限制？

- 組態僅限於沒有「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。
- 刪除或建立新的 Kinesis Data Streams 或 Firehose 的許可已從政策中移除。我們有另一個允許此動作的政策。

問：在我的 AMS 帳戶中使用 Amazon Kinesis Data Streams 的先決條件或相依性是什麼？

有幾個相依性：

- Amazon Managed Service for Apache Flink 要求在使用 Managed Service for Apache Flink 設定應用程式之前，必須先建立 Kinesis Data Streams 或 Firehose。
- 資源型政策許可應指出特定的輸入資料來源。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Streaming for Apache Kafka

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 功能。Amazon Managed Streaming for Apache Kafka 是一種全受管 AWS 串流資料服務，可讓您輕鬆地建置和執行使用 Apache Kafka 處理串流資料的應用程式，而無需成為操作 Apache Kafka 叢集的專家。Amazon MSK 會為您管理 Apache Kafka 叢集和 Apache ZooKeeper 節點的佈建、組態和維護。Amazon MSK 也會在 AWS 主控台中顯示關鍵 Apache Kafka 效能指標。

Amazon MSK 為您的 Apache Kafka 叢集提供多層安全性，包括 VPC 網路隔離、控制平面 API 授權的 AWS IAM、靜態加密、傳輸中的 TLS 加密、TLS 型憑證身分驗證、安全 SASL/SCRAM 身分驗證 AWS Secrets Manager。若要進一步了解，請參閱 [Amazon MSK](#)。

AWS Managed Services 常見問答集中的 Amazon MSK

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon MSK？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 政策和角色佈建至您的帳戶：

- customer-msk-admin-policy.json
- AmazonMSKFullAccess
- customer-msk-admin-role.json

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：使用 Amazon MSK 有哪些限制？

若要讓 Amazon MSK 將代理程式日誌交付至您設定的目的地，請確定 AmazonMSKFullAccess 政策已連接至您的 IAM 角色。因此，完整存取許可已就緒。

問：使用 Amazon MSK 有哪些先決條件或相依性？

在建立 MSK 叢集之前，您必須在該 VPC 內擁有 VPC 和子網路。根據預設，AMS 在預設 [建立 AMS VPC](#) 時會涵蓋此項目。

若要了解 Amazon MSK 的限制，請參閱 [Amazon MSK 限制](#)。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Service for Prometheus

使用 AMS 自助式服務佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 Amazon Managed Service for Prometheus (AMP) 功能。Amazon Managed Service for Prometheus 是無伺服器、且與 Prometheus 相容的監控服務，適用於容器指標，可讓您更輕鬆地大規模監控容器環境。透過 Amazon Managed Service for Prometheus，您可以使用目前用來監控容器化工作負載效能的相同開放原始碼 Prometheus 資料模型和查詢語言，並享有改良的可擴展性、可用性和安全性，而無需管理基礎設施。

隨著工作負載的擴展和縮減，Amazon Managed Service for Prometheus 會自動擴展操作指標的擷取、儲存和查詢。它與 AWS 安全服務整合，以快速且安全地存取資料。如需詳細資訊，請參閱 [什麼是 Amazon Managed Service for Prometheus？](#)

AWS Managed Services 常見問答集中的 Amazon Managed Service for Prometheus

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Managed Service for Prometheus？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer-prometheus-console-role`。在帳戶中佈建之後，您必須在聯合解決方案中加入`customer-prometheus-console-role`角色。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Prometheus 有哪些限制？

支援所有功能。

問：在我的 AMS 帳戶中使用 Amazon Managed Service for Prometheus 的先決條件或相依性是什麼？

Amazon Managed Service for Prometheus 沒有先決條件或相依性。不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Personalize

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Personalize 功能。Amazon Personalize 是一種機器學習服務，可讓開發人員輕鬆地使用其應用程式為客戶建立個人化建議。

機器學習越來越常用於透過提供個人化產品和內容建議、量身訂做的搜尋結果和有針對性的行銷活動來提高客戶參與度。不過，由於複雜性，開發產生這些複雜建議系統所需的機器學習功能，現在已超過大多數組織觸手可及的範圍。Amazon Personalize 可讓沒有先前機器學習經驗的開發人員，使用從 Amazon.com：// 上多年使用的機器學習技術，輕鬆地在其應用程式中建置複雜的個人化功能。

使用 Amazon Personalize，您可以從應用程式提供活動串流 – 按一下、頁面檢視、註冊、購買等 – 以及您想要建議的項目庫存，例如文章、產品、影片或音樂。您也可以選擇向 Amazon Personalize 提供使用者的其他人口統計資訊，例如年齡或地理位置。Amazon Personalize 將處理和檢查資料、識別有意義的內容、選取正確的演算法，以及訓練和最佳化針對您的資料自訂的個人化模型。Amazon Personalize 分析的所有資料都會保持私有和安全，僅用於您的自訂建議。您可以透過簡單的 API 呼叫開始提供個人化建議。您只需支付使用量的費用，而且沒有最低費用，也沒有預付承諾。

若要進一步了解，請參閱 [Amazon Personalize](#)。

AWS Managed Services 中的 Amazon Personalize 常見問答集

問：如何請求存取 AMS 帳戶中的 Amazon Personalize？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權，而且您需要指定要由 AWS 個人化用來產生建議的資料的 S3 儲存貯體。此

RFC 會將下列 IAM 角色佈建至您的帳戶：customer_personalize_console_role和customer_personalize_service_role。

- 在帳戶中佈建 customer_personalize_console_role 後，您必須在聯合解決方案中加入角色。您也可以customer_personalize_console_policy將 連接到 以外的其他現有角色Customer_ReadOnly_Role。
- 將 customer_personalize_service_role 提供給您的帳戶後，您可以在建立新的資料集群組時參考其 ARN。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：aws_code_pipeline_service_role_policy。

問：在我的 AMS 帳戶中使用 Amazon Personalize 有哪些限制？

Amazon Personalize 組態僅限於沒有 'ams-' 或 'mc-' 字首的資源，以防止對 AMS 基礎設施進行任何修改。

問：在我的 AMS 帳戶中使用 Amazon Personalize 有哪些先決條件或相依性？

- 如果存放資料的 S3 儲存貯體已加密，則必須提供 KMS 金鑰 ID，以便我們允許 Amazon Personalize 使用的角色解密儲存貯體。

Amazon Personalize 不支援預設 KMS S3 金鑰。如果需要使用 KMS，請建立自訂金鑰，並透過開啟變更類型 KMS 金鑰 | Create（需要檢閱）的 RFC 來新增下列政策：

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```



```
}
```

- 必須使用下列儲存貯體政策建立 S3 儲存貯體。透過提交變更類型為 S3 儲存 | 建立政策的 RFC 來執行此操作。此政策允許 Amazon Personalize 存取資料；該儲存貯體將包含 Amazon Personalize 要使用的資料。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon QuickSight

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 QuickSight 功能。QuickSight 是一種快速、雲端驅動的商業智慧服務，可為您組織中的每個人提供洞見。作為全受管服務，QuickSight 可讓您輕鬆建立和發佈互動式儀表板，其中包含機器學習 (ML) 洞見。若要進一步了解，請參閱 [Amazon QuickSight](#)。

AWS Managed Services 中的 QuickSight 常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 QuickSight？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_quicksight_console_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 QuickSight 有哪些限制？

- AWS 由於 IAM 政策相依性，您將無法存取 QuickSight 上的資源設定。不過，AMS 團隊會為您啟用每個資源，以回應啟用服務的請求。
- 此模型不支援個別使用者和群組的資源存取，因為此功能可讓使用者修改可能影響 AMS 基礎設施的 IAM 許可。
- 由於變更 IAM 物件涉及風險，因此不支援從 QuickSight 中邀請 IAM 身分的功能。
- QuickSight 服務提供兩種版本：Enterprise 和 Standard。兩者都提供 AMS 上支援的單一登入 (SSO) 選項。不過，Enterprise Edition 可以選擇將 QuickSight 與 Active Directory (AD) 整合。AMS 上的 QuickSight 不支援與 AD 整合，因為 AMS 帳戶結構與 QuickSight 信任要求之間不相容。

問：在我的 AMS 帳戶中使用 QuickSight 的先決條件或相依性是什麼？

- 當 AMS 收到此 RFC 以新增 QuickSight 時，系統會傳送服務請求給您以取得其他資訊；請提供下列項目：
 - QuickSight 帳戶名稱（例如，*CustomerName*-quicksight）
 - QuickSight 版本 (Standard 與 Enterprise)
 - 要啟用 QuickSight 服務 AWS 的區域（預設為您的 AMS AWS 區域）。
 - QuickSight 帳戶的通知電子郵件地址。
 - （選用）要分析的資料檔案所在的 S3 儲存貯體。
 - 連線至 QuickSight 的 VPC 和子網路 IDs 支援新增 VPC 連線的功能，可啟用 QuickSight 與帳戶內部資源之間的私有連線。

AMS 運算子會代表您執行註冊程序，並設定兩個 QuickSight 功能：

- [自動探索](#)資料來源。
- [VPC 連線](#)。

 Note

這些動作必須由 AMS 運算子執行，因為在登入過程中需要更高的 IAM 和 VPC 許可。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Rekognition

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Rekognition 功能。Amazon Rekognition 可讓您使用經過驗證、可擴展性高的深度學習技術，輕鬆地將映像和影片分析新增至應用程式，無需機器學習專業知識。透過 Amazon Rekognition，您可以識別影像和影片中的物件、人物、文字、場景和活動，以及偵測任何不適當的內容。Amazon Rekognition 還提供高度準確的臉部分分析和臉部搜尋功能，可用於偵測、分析和比較各種使用者驗證、人員計數和公共安全使用案例的臉部。

使用 Amazon Rekognition 自訂標籤，您可以在影像中識別特定於您業務需求的物件和場景。例如，您可以建置模型來分類組裝線上的特定機器組件，或偵測運作狀態不佳的植物。Amazon Rekognition 自訂標籤會為您處理模型開發繁重的工作，因此不需要機器學習體驗。您只需要提供您要識別的物件或場景的影像，而服務會處理其餘項目。

若要進一步了解，請參閱 [Amazon Rekognition](#)。

AWS Managed Services 常見問答集中的 Amazon Rekognition

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon Rekognition？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_rekognition_console_role & customer_rekognition_service_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Rekognition 有哪些限制？

Amazon Rekognition 的完整功能可供 Amazon Rekognition 自行佈建的服務角色使用。

問：在我的 AMS 帳戶中使用 Amazon Rekognition 有哪些先決條件或相依性？

如果您使用 Kinesis Video Streams 為 Amazon Rekognition Video 串流處理器或資料串流提供來源串流影片，做為將資料寫入 Kinesis Data Streams 的目的地，請在建立 RFC kinesisStreamName 時為 AMS 提供。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon SageMaker AI

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon SageMaker AI 功能。SageMaker AI 可讓每位開發人員和資料科學家快速建置、訓練和部署機器學習模型。Amazon SageMaker AI 是一項全受管服務，涵蓋整個機器學習工作流程，以標記和準備您的資料、選擇演算法、訓練模型、調校和最佳化部署、進行預測，以及採取動作。您的模型可以更快地進入生產環境，減少許多工作量並降低成本。若要進一步了解，請參閱 [Amazon SageMaker AI](#)。

AWS Managed Services 常見問答集中的 SageMaker AI

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 SageMaker AI？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_sagemaker_admin_role 和服務角色 AmazonSageMaker-ExecutionRole-Admin。在您的帳戶中佈建 SageMaker AI 之後，您必須在聯合解決方案中加入該customer_sagemaker_admin_role角色。您無法直接存取服務角色；SageMaker AI 服務會在執行各種動作時使用它，如下所述：[傳遞角色](#)。

問：在我的 AMS 帳戶中使用 SageMaker AI 有哪些限制？

- AMS Amazon SageMaker AI IAM 角色不支援下列使用案例：
 - 目前不支援 SageMaker AI Studio。
 - 不支援 SageMaker AI Ground Truth 來管理私有人力資源，因為此功能需要對 Amazon Cognito 資源的過度允許存取。如果需要管理私有人力資源，您可以請求具有合併 SageMaker AI 和 Amazon Cognito 許可的自訂 IAM 角色。否則，我們建議您使用公有人力資源（由 Amazon Mechanical Turk 提供支援）或 AWS Marketplace 服務供應商進行資料標記。
- 建立 VPC 端點以支援對 SageMaker AI 服務的 API 呼叫 (aws.sagemaker.{region}.notebook、com.amazonaws.{region}.sagemaker.api & com.amazonaws.{region}.sagemaker.runtime)，因為許可範圍不能縮小為僅限 SageMaker AI 相關服務。若要支援此使用案例，請提交管理 | 其他 | 其他 RFC 以建立相關的 VPC 端點。
- 不支援 SageMaker AI 端點自動擴展，因為 SageMaker AI 需要任何 ("*") 資源的DeleteAlarm許可。若要支援端點自動擴展，請提交管理 | 其他 | 其他 RFC 來設定 SageMaker AI 端點的自動擴展。

問：在我的 AMS 帳戶中使用 SageMaker AI 的先決條件或相依性是什麼？

- 下列使用案例在使用前需要特殊組態：
 - 如果 S3 儲存貯體將用於存放模型成品和資料，則必須使用部署 | 進階堆疊元件 | S3 儲存 | 建立 RFC，請求名為 且具有必要關鍵字 ("SageMaker"、"Sagemaker"、"sagemaker" 或 "aws-glue") 的 S3 儲存貯體。
 - 如果將使用彈性檔案存放區 (EFS)，則必須在相同的子網路中設定 EFS 儲存，並由安全群組允許。
 - 如果其他資源需要直接存取 SageMaker AI 服務（筆記本、API、執行時間等），則必須由下列人員請求組態：
 - 提交 RFC 以建立端點的安全群組（部署 | 進階堆疊元件 | 安全群組 | 建立（自動））。
 - 提交管理 | 其他 | 其他 | 建立 RFC 以設定相關的 VPC 端點。

問：**customer_sagemaker_admin_role**可以直接存取的資源支援哪些命名慣例？（以下用於更新和刪除許可；如果您需要資源的其他支援命名慣例，請聯絡 AMS 雲端架構師進行諮詢。）

- 資源：傳遞AmazonSageMaker-ExecutionRole-*角色
 - 許可：SageMaker AI 自助佈建服務角色支援您使用 SageMaker AI 服務角色 (AmazonSageMaker-ExecutionRole-*) 搭配 AWS Glue AWS RoboMaker和 AWS Step Functions。
- 資源：Secrets Manager 上的 AWS 秘密
 - 許可：使用AmazonSageMaker-*字首描述、建立、取得、更新秘密。
 - 許可：描述，當SageMaker資源標籤設定為 時取得秘密true。
- 資源：上的儲存庫 AWS CodeCommit
 - 許可：使用AmazonSageMaker-*字首建立/刪除儲存庫。
 - 許可：在具有下列字首、 *sagemaker**SageMaker*和 的儲存庫上提取/推送 Git*Sagemaker*。
- 資源：Amazon ECR (Amazon Elastic Container Registry) 儲存庫
 - 許可：許可：使用下列資源命名慣例 時，設定、刪除儲存庫政策並上傳容器映像*sagemaker*。
- 資源：Amazon S3 儲存貯體
 - 許可：當資源具有下列字首時，取得、放置*Sagemaker*、刪除物件、中止分段上傳 S3 物件：*SageMaker*、 *sagemaker*和 aws-glue。
 - 許可：當SageMaker標籤設定為 時取得 S3 物件true。
- 資源：Amazon CloudWatch Log Group

- 許可：建立日誌群組或串流、放置日誌事件、列出、更新、建立、刪除具有下列字首的日誌交付：`/aws/sagemaker/*`。
- 資源：Amazon CloudWatch 指標
 - 許可：使用下列字首時放置指標資料：`AWS/SageMaker`、`AWS/SageMaker/`、`aws/SageMaker`、`aws/SageMaker/`、`aws/sagemaker`、`aws/sagemaker/`和 `/aws/sagemaker/`。
- 資源：Amazon CloudWatch Dashboard
 - 許可：使用下列字首時建立/刪除儀表板：`customer_*`。
- 資源：Amazon SNS（簡易通知服務）主題
 - 許可：使用下列字首時訂閱/建立主題：`*SageMaker*`、`*sagemaker*`和 `*Sagemaker*`。

問：**AmazonSageMakerFullAccess**和 **customer_sagemaker_admin_role** 之間的差異是什麼？

`customer_sagemaker_admin_role` 搭配的 `customer_sagemaker_admin_policy`提供與 **AmazonSageMakerFullAccess** 幾乎相同的許可，除了：

- 與 AWS RoboMaker、Amazon Cognito 和資源連線的許可 AWS Glue。
- SageMaker AI 端點自動擴展。您必須提交 RFC 與管理 | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策（需要檢閱）變更類型 (ct-27tuth19k52b4)，以暫時或永久提升自動擴展許可，因為自動擴展需要在 CloudWatch 服務上進行寬鬆存取。

問：如何在靜態資料加密中採用 AWS KMS 客戶受管金鑰？

您必須確保金鑰政策已在客戶受管金鑰上正確設定，以便相關的 IAM 使用者或角色可以使用金鑰。如需詳細資訊，請參閱[AWS KMS 金鑰政策文件](#)。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Simple Email Service

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Simple Email Service (Amazon SES) 功能。Amazon Simple Email Service 是一種雲端電子郵件傳送服務，旨在協助數位行銷人員和應用程式開發人員、傳送行銷、通知和交易電子郵件。

您可以使用 SMTP 界面或其中一個 AWS SDKs，直接將 Amazon SES 整合到現有的應用程式。您也可以將 Amazon SES 的電子郵件傳送功能整合至您已使用的軟體，例如票證系統和電子郵件用戶端。

若要進一步了解，請參閱 [Amazon Simple Email Service](#)。

AWS Managed Services 常見問答集中的 Amazon SES

問：如何請求存取 AMS 帳戶中的 Amazon SES？

透過使用 [管理 | AWS 服務 | 自助佈建服務 | 新增 \(ct-1w8z66n899dct\)](#) 變更類型提交 RFC，請求存取 Amazon SES。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_ses_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon SES 的先決條件或相依性是什麼？

- 您必須設定 S3 儲存貯體政策，以允許 Amazon SES 將事件發佈至儲存貯體。
- 您必須使用預設 (AWS SES) 或設定 CMK 金鑰，以允許 Amazon SES 加密電子郵件，並將事件推送至屬於帳戶的其他服務資源，例如 Amazon S3、Amazon SNS、Lambda 和 Firehose。

問：在我的 AMS 帳戶中使用 Amazon SES 有哪些限制？

您必須提出 RFCs 才能建立下列資源：

- 具有 PutEvents 許可的 SMTP 使用者和 IAM 服務角色，傳送至 Kinesis Firehose 串流。
- 您必須使用 AMS 變更類型建立新的 AWS 資源，例如 S3 儲存貯體、Firehose 串流、SNS 主題，Amazon SES 規則和組態集的目的地才能使用這些資源。
- SMTP 登入資料。若要請求新的 SMTP 登入資料，請使用變更類型（[管理 | 其他 | 其他 | 建立](#)）。AMS 會建立登入資料，並將其新增至 Secrets Manager。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Simple Workflow Service

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Simple Workflow Service (Amazon SWF) 功能。Amazon Simple Workflow Service 可協助開發人員建置、執行和擴展具有平行或循序步驟的背景任務。您可以在雲端中將 Amazon SWF 視為全受管狀態追蹤器和任務協調器。如果您應用程式的步驟需要超過 500 毫秒才能完成，您需要追蹤處理狀態，或者如果任務失敗，則需要復原或重試，Amazon SWF 可以為您提供協助。若要進一步了解，請參閱 [Amazon Simple Workflow Service](#)。

AWS Managed Services 常見問答集中的 Amazon SWF

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Amazon SWF？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_swf_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon SWF 有哪些限制？

Lambda InvokeFunction 許可已包含在此服務中，但新增至所有 AMS 客戶角色 customer_deny_policy 的 AMS 明確拒絕存取 AMS Lambda 函數和 AMS 擁有的資源。若要在 Amazon SWF 中標記或取消標記資源，請提交管理 | 其他 | 其他變更類型。

問：在我的 AMS 帳戶中使用 Amazon SWF 的先決條件或相依性是什麼？

Amazon SWF 取決於 AWS Lambda 服務，因此，已提供叫用 Lambda 的許可做為此角色的一部分，而且從 Amazon SWF 叫用 Lambda 不需要額外的許可。否則，使用 Amazon SWF 沒有先決條件。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Textract

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Textract 功能。Amazon Textract 是一項全受管的機器學習服務，可自動從掃描文件中擷取列印的文字、手寫和其他資料，這些文件超出簡易光學字元辨識 (OCR)，以識別、了解並從表單和資料表擷取資料。若要進一步了解，請參閱 [Amazon Textract](#)。

AWS Managed Services 常見問答集中的 Amazon Textract

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Amazon Textract？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_textract_human_review_execution_role、customer_textract_console_role 和 customer_ec2_textract_instance_profile。在帳戶中佈建後，您必須在聯合解決方案 customer_textract_console_role 中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Textract 有哪些限制？

在您的 AMS 帳戶中使用 Amazon Textract 沒有限制。

問：在我的 AMS 帳戶中使用 Amazon Textract 有哪些先決條件或相依性？

您必須提交 RFC 部署 | 進階堆疊元件 | S3 儲存 | 建立 (ct-1a68ck03fn98r) 來請求建立 S3 儲存貯體。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Transcribe

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Amazon Transcribe 功能。Amazon Transcribe 是一種全受管且持續訓練的自動語音辨識服務，可從音訊檔案自動產生時間戳記的文字文字記錄。Amazon Transcribe 可讓開發人員輕鬆地將 speech-to-text 功能新增至其應用程式。音訊資料幾乎無法讓電腦搜尋和分析。因此，錄製的語音需要轉換為文字，才能用於應用程式。從歷史上來看，客戶必須與轉錄供應商合作，這些供應商需要他們簽署昂貴的合約，並且很難整合到他們的技術堆疊中來完成此任務。其中許多供應商使用過時的技術無法很好地適應不同的案例，例如聯絡中心中常見的低傳真電話音訊，這會導致準確性不佳。

Amazon Transcribe 使用稱為自動語音辨識 (ASR) 的深度學習程序，快速準確地將語音轉換為文字。Amazon Transcribe 可用來轉錄客戶服務呼叫、自動化隱藏式字幕和字幕，以及為媒體資產產生中繼資料，以建立可完全搜尋的封存。您可以使用 Amazon Transcribe Medical 將醫療 speech-to-text 功能新增至臨床文件應用程式。若要進一步了解，請參閱 [Amazon Transcribe](#)。

AWS Managed Services 常見問答集中的 Amazon Transcribe

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Amazon Transcribe？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_transcribe_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Amazon Transcribe 有哪些限制？

除非 RA 和 另有指定，否則在使用轉錄時，您必須使用 'customer-transcribe*' 做為儲存貯體的字首。

您無法在 Amazon 轉錄中建立 IAM 角色。

您無法針對預設 SSPS 中的輸出資料使用服務受管 S3 儲存貯體 (如有需要，請聯絡您的帳戶 CA)。

如果您想要使用不屬於 AMS 命名空間的客戶受管 KMS 金鑰，則必須提交風險接受。

問：在我的 AMS 帳戶中使用 Amazon Transcribe 的先決條件或相依性是什麼？

S3 必須能夠存取名為 'customer-transcribe*' 的儲存貯體。如果您的 S3 儲存貯體使用 KMS 金鑰加密，則需要 KMS 才能使用 Amazon Transcribe。如果儲存貯體不需要加密，則可以移除「KMStranscribeAllow」。

使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon WorkSpaces

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 WorkSpaces 功能。WorkSpaces 可讓您為使用者佈建以雲端為基礎的虛擬 Microsoft Windows 或 Amazon Linux 桌面，稱為 WorkSpaces。WorkSpaces 無需採購和部署硬體或安裝複雜軟體。您可以在需求變更時快速新增或移除使用者。使用者從支援的裝置使用用戶端應用程式存取其 WorkSpaces，或針對 Windows WorkSpaces 使用 Web 瀏覽器，並使用其現有的內部部署 Active Directory (AD) 登入資料登入。

若要進一步了解，請參閱 [Amazon WorkSpaces](#)。

AWS Managed Services 常見問答集中的 WorkSpaces

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 WorkSpaces？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_workspaces_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 WorkSpaces 有哪些限制？

Amazon WorkSpaces 自行佈建服務角色提供工作區的完整功能。

問：在我的 AMS 帳戶中使用 WorkSpaces 的先決條件或相依性是什麼？

- WorkSpaces 受限於 AWS 區域；因此，AD Connector 必須在託管 WorkSpaces 執行個體 AWS 的相同區域中設定。

客戶可以使用下列兩種方法之一，將 WorkSpaces 連線至客戶 AD：

1. 使用 AD 連接器將身分驗證代理到內部部署 Active Directory 服務（偏好）：

在整合 WorkSpaces 執行個體與內部部署目錄服務之前，在您的 AMS 帳戶中設定 Active Directory (AD) Connector。AD Connector 可做為現有 AD 使用者（來自您的網域）的代理，以使用現有的內部部署 AD 登入資料連線至 WorkSpaces。這是偏好的做法，因為 WorkSpaces 會直接加入客戶的內部部署網域，同時做為資源和使用者樹系，進而在客戶端產生更多控制權。

如需詳細資訊，請參閱[部署 Amazon WorkSpaces 的最佳實務（案例 1）](#)。

2. 使用 AD Connector 搭配 AWS Microsoft AD、共用服務 VPC，以及對內部部署的單向信任：

您也可以先建立從 AMS 受管 AD 到內部部署 AD 的單向傳出信任，以使用內部部署目錄驗證使用者。WorkSpaces 將使用 AD Connector 加入 AMS 受管 AD。然後，WorkSpaces 存取許可將透過 AMS 受管 AD 委派給 WorkSpaces 執行個體，而無需與您的內部部署環境建立雙向信任。在此案例中，使用者樹系將位於客戶 AD 中，而資源樹系將位於 AMS 受管 AD 中（可透過 RFC 請求對 AMS 受管 AD 的變更）。請注意，WorkSpaces VPC 與執行 AMS 受管 AD 的 MALZ 共用服務 VPC 之間的連線是透過 Transit Gateway 建立。

如需詳細資訊，請參閱[部署 Amazon WorkSpaces 的最佳實務（案例 6）](#)。

Note

AD Connector 可以透過提交具有必要 AD 組態詳細資訊的管理 | 其他 | 其他 | 建立變更類型 RFC 來進行設定；如需詳細資訊，請參閱[建立 AD Connector](#)。如果方法 2 用於在 AMS 受管 AD 中建立資源樹系，請執行 AMS 受管 AD，在 AMS 共用服務帳戶中提交另一個管理 | 其他 | 建立變更類型 RFC。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AMS Code 服務

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AMS Code 服務功能。AMS Code 服務是 AWS 程式碼管理服務的專屬綁定，如下所示。您可以選擇使用 AMS Code 服務在 AMS 中部署所有服務，也可以在 AMS 中個別部署。

AMS Code 服務包括下列服務：

- AWS CodeCommit：全受管[來源控制](#)服務，可託管安全的 Git 型儲存庫。它讓團隊可以在安全且高度可擴展的生態系統中協作程式碼。CodeCommit 不需要操作您自己的來源控制系統或擔心擴展其基礎設施。您可以使用 CodeCommit 安全地存放從原始程式碼到二進位檔的任何內容，並與您現有的 Git 工具無縫搭配使用。如需進一步了解，請參閱 [AWS CodeCommit](#)

若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 [使用 AMS SSP AWS CodeCommit 在您的 AMS 帳戶中佈建](#)。

- AWS CodeBuild：全受管持續整合服務，可編譯原始程式碼、執行測試，並產生準備好部署的軟體套件。使用 CodeBuild，您便不必佈建、管理、擴展自己的組建伺服器。CodeBuild 會持續擴展並同時處理多個組建，所以您的組建不必排入佇列中等候。您可以利用預先封裝好的組建環境立即開始使用，或是建立自訂的組建環境來使用您自己的組建工具。使用 CodeBuild 時，將依據您使用運算資源的分鐘數計費。如需進一步了解，請參閱 [AWS CodeBuild](#)

若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 [使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建](#)。

- AWS CodeDeploy：全受管部署服務，可將軟體部署自動化至各種運算服務，例如 Amazon EC2 和您的內部部署伺服器。AWS CodeDeploy 可協助您快速發行新功能，協助您避免在應用程式部署期間停機，並處理更新應用程式的複雜性。您可以使用 AWS CodeDeploy 來自動化軟體部署，無需進行容易出錯的手動操作。服務會擴展以符合您的部署需求。如需進一步了解，請參閱 [AWS CodeDeploy](#)

若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 [使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建](#)。

- AWS CodePipeline：全受管[持續交付](#)服務，可協助您自動化發行管道，以實現快速可靠的應用程式和基礎設施更新。根據您定義的發行模型，CodePipeline 可以自動在每次程式碼變更時建置、測試和部署程式碼。這可讓您快速且可靠地交付功能和更新。您可以輕鬆地 AWS CodePipeline 與第三方服務整合，例如 GitHub 或您自己的自訂外掛程式。使用時 AWS CodePipeline，您只需支付使用量的費用。沒有預付費用，也無需長期承諾。如需進一步了解，請參閱 [AWS CodePipeline](#)

若要在獨立於 AMS Code 服務的 AMS 帳戶中部署此項目，請參閱 [使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建](#)。

AWS Managed Services 常見問答集中的 AMS 程式碼服務

問：如何請求存取 AMS 帳戶中的 AMS Code 服務？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_code_suite_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。此時，AMS Operations 也會在您的帳戶中部署 CodeBuildcustomer_codebuild_service_role、CodeDeploy 和 CodePipeline customer_codedeploy_service_roleaws_code_pipeline_service_role服務的、服務角色。如果需要的其他 IAM 許可customer_codebuild_service_role，請提交 AMS 服務請求。

Note

您也可以個別新增這些服務；如需資訊，請分別參閱 [使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建](#)、[使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建](#)、[使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建](#)和。

問：在我的 AMS 帳戶中使用 AMS Code 服務有哪些限制？

- AWS CodeCommit：CodeCommit 上的觸發功能會因為建立 SNS 主題的相關權限而停用。針對 CodeCommit 的直接驗證受到限制；使用者應該使用登入資料協助程式進行驗證。有些 KMS 命令也會受到限制：kms:Encrypt、kms:Decrypt、kms:ReEncrypt、kms:GenerateDataKey、kms:GenerateDataKeyWithoutPlaintext 和 kms:DescribeKey。
- CodeBuild：對於 AWS CodeBuild 主控台管理員存取，許可在資源層級受到限制；例如，CloudWatch 動作在特定資源上受到限制，且 iam:PassRole 許可受到控制。
- CodeDeploy：目前 CodeDeploy 僅支援 Amazon EC2/內部部署上的部署。不支援透過 CodeDeploy 在 ECS 和 Lambda 上部署。
- CodePipeline：CodePipeline 功能、階段和提供者僅限於下列項目：
 - 部署階段：Amazon S3 和 AWS CodeDeploy
 - 來源階段：Amazon S3 AWS CodeCommit、Bit 儲存貯體和 GitHub
 - 組建階段：AWS CodeBuild 和 Jenkins
 - 核准階段：Amazon SNS
 - 測試階段：AWS CodeBuild、Jenkins、BlazeMeter、Ghost Inspector UI 測試、Micro Focus StormRunner Load、Runscope API 監控
 - 調用階段：Step Functions 和 Lambda

 Note

AMS Operations 會在您的帳戶 `customer_code_pipeline_lambda_policy` 中部署；它必須與 Lambda 叫用階段的 Lambda 執行角色連接。提供您要新增此政策的 Lambda 服務/執行角色名稱。如果沒有自訂 Lambda 服務/執行角色，則 AMS 會建立名為 `customer_code_pipeline_lambda_execution_role`，這是 `customer_lambda_basic_execution_role` 與的複本 `customer_code_pipeline_lambda_policy`。

問：在我的 AMS 帳戶中使用 AMS Code 服務的先決條件或相依性是什麼？

- CodeCommit：如果 S3 儲存貯體使用 AWS KMS 金鑰加密，AWS KMS 則需要 S3 和 才能使用 AWS CodeCommit。
- CodeBuild：如果定義的 AWS CodeBuild 服務角色需要額外的 IAM 許可，請透過 AMS 服務請求請求它們。

- CodeDeploy：無。
- CodePipeline：None. AWS supported 服務—AWS CodeCommit、AWS CodeBuild、AWS CodeDeploy—必須在啟動 CodePipeline 之前啟動，或與 CodePipeline 一起啟動。不過，這由 AMS 工程師完成。

使用 AMS SSP AWS Amplify 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Amplify 的功能。AWS Amplify 是一個完整的解決方案，可讓前端 Web 和行動開發人員輕鬆建置、連線和託管完整堆疊應用程式。Amplify 提供彈性，可隨著使用案例的演進而利用 AWS 服務的廣度。Amplify 提供建置完整堆疊 iOS、Android、Flutter、Web 和 React Native 應用程式的產品。如需詳細資訊，請參閱 [AWS Amplify](#)。

AWS Amplify 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Amplify 請求在我的 AMS 帳戶中設定？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_amplify_console_role。佈建至您的帳戶後，您必須在聯合解決方案中加入該角色。

此外，您必須提供風險接受，因為 AWS Amplify 具有基礎設施變更許可。若要這樣做，請使用您的 Cloud Service Delivery Manager (CSDM)。

問：AWS Amplify 在我的 AMS 帳戶中使用 有哪些限制？

除非 RA 和 另有指定，否則在使用 Amplify 時，您必須使用 'amplify*' 做為儲存貯體的字首。

問：AWS Amplify 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Amplify 在您的 AMS 帳戶中使用 沒有先決條件。

僅限 Malz 環境：Amplify 的預設加入角色為「customer_amplify_console_role」。若要使用自訂角色，請先部署 IAM 實體。然後，建立額外的 RFC，將您的自訂角色新增至應用程式帳戶允許清單的服務控制政策。

使用 AMS SSP 佈建 AWS AppSync

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS AppSync 的功能。可讓您建立彈性 API 來安全地存取、操作和合併來自一或多個資料來源的資料，以 AWS AppSync 簡化應用程式開發。AWS AppSync 是一種受管服務，可使用 GraphQL 讓應用程式輕鬆取得他們所需的資料。

透過 AWS AppSync，您可以在 NoSQL 資料存放區、關聯式資料庫、HTTP APIs 和自訂資料來源等各種資料來源上建置可擴展的應用程式，包括需要即時更新的應用程式 AWS Lambda。對於行動和 Web 應用程式，AWS AppSync 還會在裝置離線時提供本機資料存取，並在恢復上線時提供與可自訂衝突解決方案的資料同步。如需詳細資訊，請參閱 [AWS AppSync](#)。

AWS AppSync 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何在我的 AMS AWS AppSync 帳戶中請求存取權？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_appsync_service_role 和 customer_appsync_author_role。在帳戶中佈建後，您必須在聯合解決方案 customer_appsync_author_role 中加入。

問：使用 有哪些限制 AWS AppSync？

- 在 AppSync 上建立資料來源時，客戶需要指定先前建立的服務角色，不允許建立新角色，因此將傳回拒絕存取
- AppSync 角色設定為將許可限制為包含「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。

問：要使用哪些先決條件或相依性 AWS AppSync？

此服務允許將多個其他服務用作資料來源，使用它們的基本許可包含在服務角色 (customer_appsync_service_role) 中，但您必須在使用服務時手動選取服務角色。

使用 AMS SSP AWS App Mesh 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS App Mesh 的功能。AWS App Mesh 提供應用程式層級聯網，讓您的服務可以輕鬆地跨多種類型的運算基礎設施彼此通訊。App Mesh 會標準化您的服務通訊方式，為您提供 end-to-end 可見性，並確保應用程式的高可用性。

AWS App Mesh 透過為跨多種運算基礎設施建置的服務提供一致的可見性和網路流量控制，讓您輕鬆執行服務。App Mesh 不需要更新應用程式程式碼，即可變更監控資料的收集方式或在服務之間路由流量的方式。App Mesh 會設定每個服務以匯出監控資料，並跨應用程式實作一致的通訊控制邏輯。這可讓您輕鬆地快速找出錯誤的確切位置，並在發生故障或需要部署程式碼變更時自動重新路由網路流量。如需詳細資訊，請參閱 [AWS App Mesh](#)。

AWS App Mesh AWS Managed Services 常見問答集中的

常見問題和解答：

問：如何在我的 AMS AWS App Mesh 帳戶中請求存取權？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_app_mesh_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS App Mesh？

完整功能 AWS App Mesh 可在您的 AMS 帳戶中使用。

問：要使用哪些先決條件或相依性 AWS App Mesh？

AWS App Mesh 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Audit Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Audit Manager 功能。Audit Manager 可協助您持續稽核 AWS 用量，以簡化您評估風險的方式，以及是否符合法規和業界標準。Audit Manager 會自動化證據收集，讓您更容易評定您的政策、程序和活動是否有效運作。進行稽核時，Audit Manager 可協助您管理控制項的利益相關者審查，並協助您以大幅減少手動作業的方式建立稽核就緒的報告。若要進一步了解，請參閱 [Audit Manager](#)。

AWS Audit Manager 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Audit Manager 的？

您可以透過提交 AWS 服務 RFC 管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 來請求存取權。此 RFC 會在您的帳戶中佈建下列 IAM 角色：customer-audit-manager-admin-Role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS Audit Manager？

AWS Audit Manager 在您的 AMS 帳戶中使用 沒有限制。AWS Audit Manager 提供 的完整功能。

問：要使用哪些先決條件或相依性 AWS Audit Manager？

1. 您需要將您希望報告/評估所在的 s3 儲存貯體提供給 AMS。
2. 如果您想要使用 服務進行加密，您需要向 AMS 提供要使用的 KMS CMK ARN。
3. 如果您想要將 SNS 通知傳送至主題，您必須提供主題的名稱或 arn。
4. (選用) 如果您想要在 Audit Manager 中啟用 Organizations 做為多帳戶登陸區域的一部分，並且想要委派管理員帳戶，則需要額外的先決條件：在 RFC (管理 | AWS 服務 | 相容服務 | 新增) 的描述欄位中，提及您想要在 Audit Manager 設定中使用委派管理員帳戶，並提供下列詳細資訊：
 - KMS CMK ARN (最初用於設定 Audit Manager)
 - 做為此多帳戶登陸區域一部分的 Audit Manager 委派管理員帳戶 ID (可以是 MALZ 應用程式帳戶)

使用 AMS SSP AWS Batch 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Batch 的功能。AWS Batch 可讓開發人員、科學家和工程師輕鬆有效地執行數十萬個批次運算任務 AWS。會根據所提交批次任務的磁碟區和特定資源需求，AWS Batch 動態佈建最佳數量和類型的運算資源 (例如 CPU 或記憶體最佳化執行個體)。使用 AWS Batch，您不需要安裝和管理用於執行任務的批次運算軟體或伺服器叢集，讓您專注於分析結果和解決問題。如需詳細資訊，請參閱 [AWS Batch](#)。

AWS Batch 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Batch 的？

1. 若要請求存取 AWS Batch，請提交 RFC 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct)。此 RFC 會在您的帳戶中佈建下列 IAM 角色和政策：

IAM 角色：

- customer_batch_console_role
- customer_batch_ecs_instance_role
- customer_batch_events_service_role
- customer_batch_service_role
- customer_batch_ecs_task_role

政策：

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. 在帳戶中佈建之後，您必須在聯合解決方案`customer_batch_console_role`中加入角色。

問：使用 有哪些限制 AWS Batch？

建立運算環境時，應將 EC2 執行個體標記為「`customer_batch`」或「`customer-batch`」。如果執行個體未加上標籤，則當任務完成時，執行個體將不會以批次方式終止。

問：要使用哪些先決條件或相依性 AWS Batch？

AWS Batch 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Certificate Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Certificate Manager (ACM) 功能。AWS Certificate Manager 是一種服務，可讓您佈建、管理和部署公有和私有 Secure Sockets Layer/Transport Layer Security (SSL/TLS) 憑證，以搭配 AWS 服務和您的內部連線資源使用。SSL/TLS 憑證用於保護網路通訊，並透過網際網路以及私有網路上的資源建立網站身分。AWS Certificate Manager 移除購買、上傳和續約 SSL/TLS 憑證的耗時手動程序。

使用 AWS Certificate Manager，您可以請求憑證，將其部署在 ACM 整合 AWS 的資源上，例如 Elastic Load Balancer、Amazon CloudFront 分佈和 APIs 上的 API，並讓 AWS Certificate Manager 處理憑證續約。它還可讓您為內部資源建立私有憑證，並集中管理憑證生命週期。透過 佈建 AWS Certificate Manager 以搭配 ACM 整合服務使用的公有和私有憑證是免費的。您只需為執行應用程式所建立 AWS 的資源付費。使用 [AWS Private Certificate Authority](#)，您每月為 的操作和您發行的 AWS 私有 CA 私有憑證付費。若要進一步了解，請參閱 [AWS Certificate Manager - AWS Documentation](#)。

AWS Managed Services 常見問答集中的 ACM

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Certificate Manager 的？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_acm_create_role`。您可以使用此角色來建立和管理 ACM 憑證。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

即使您尚未新增 IAM 角色，也可以使用下列變更類型建立 ACM `customer_acm_create_role` 憑證：

- [ACM | 建立公有憑證](#)
- [ACM | 建立私有憑證](#)
- [具有其他 SANs ACM 憑證 | 建立](#)

問：使用 有哪些限制 AWS Certificate Manager？

您必須向 AMS 提交變更請求 (RFC) 來刪除或修改現有的憑證，因為這些動作需要完整的管理員存取權（使用管理 | 其他 | 更新變更類型 (ct-0xdawir96cy7k)。請注意，IAM 政策無法根據標籤名稱 (mc*、ams* 等) 排除權利。憑證不會產生成本，因此刪除未使用的憑證不限時。

問：使用 Certificate Manager 有哪些先決條件或相依性？

現有的公有 DNS 名稱，以及建立 DNS CNAME 記錄的存取權，但這些記錄不需要託管在受管帳戶中。

使用 AMS SSP AWS Private Certificate Authority 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Private Certificate Authority 的功能。私有憑證用於識別和保護私有網路上連線資源之間的通訊，例如伺服器、行動、和 IoT 裝置和應用程式。AWS 私有 CA 是一項受管私有 CA 服務，可協助您輕鬆安全地管理私有憑證的生命週期。AWS 私有 CA 為您提供高可用性的私有 CA 服務，無需預付投資和持續的維護成本來操作您自己的私有 CA。將 ACM 的憑證管理功能 AWS 私有 CA 延伸至私有憑證。可讓您集中建立和管理公有和私有憑證。您可以使用 AWS 管理主控台或 ACM API，輕鬆建立和部署 AWS 資源的私有憑證。對於 EC2 執行個體、容器、IoT 裝置和內部部署資源，您可以輕鬆建立和追蹤私有憑證，並使用您自己的用戶端自動化程式碼進行部署。您也可以靈活地建立私有憑證，並針對需要自訂憑證生命週期、金鑰演算法或資源名稱的應用程式自行管理它們。如需進一步了解，請參閱 [AWS 私有 CA](#)。

AWS 私有 CA AWS Managed Services 常見問答集中的

常見問題和解答：

問：如何在我的 AMS AWS 私有 CA 帳戶中請求存取權？

透過提交 AWS 服務 RFC 請求存取權（管理 | AWS 服務 | 相容服務）。透過此 RFC，將在您的帳戶中佈建下列 IAM 角色：`customer_acm_pca_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：使用 有哪些限制 AWS 私有 CA？

目前，AWS Resource Access Manager (AWS RAM) 無法用來共用您的 AWS 私有 CA 跨帳戶。

問：要使用哪些先決條件或相依性 AWS 私有 CA？

1. 如果您打算建立 CRL，則需要 S3 儲存貯體來存放。AWS 私有 CA 會自動將 CRL 存放在您指定的 Amazon S3 儲存貯體中，並定期更新。設定 CRL 之前，S3 儲存貯體必須具有下列儲存貯體政策。為了繼續此請求，請使用 `ct-0fpj1xa808sh2`（[管理 | 進階堆疊元件 | S3 儲存 | 更新政策](#)）建立 RFC，如下所示：

- 提供 S3 儲存貯體名稱或 ARN。
- 將下列政策複製到 RFC，並以您想要 `bucket-name` 的 S3 儲存貯體名稱取代。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
      ]
    }
  ]
}
```


2. 如果上述 S3 儲存貯體已加密，則 Service Principal `acm-pca.amazonaws.com` 需要解密許可。為了繼續此請求，請使用 `ct-3ovo7px2vsa6n`（[管理](#) | [進階堆疊元件](#) | [KMS 金鑰](#) | [更新](#)）建立 RFC，如下所示：

- 提供必須更新政策的 KMS 金鑰 ARN。
- 將下列政策複製到 RFC，並以您想要 `bucket-name` 的 S3 儲存貯體名稱取代。

```
{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}
```

3. AWS 私有 CA CRLs 不支援 S3 設定「封鎖透過新存取控制清單 (ACLs 公開存取)」。您必須使用 S3 帳戶和儲存貯體停用此設定，以允許 AWS 私有 CA 寫入 CRLs，如[如何安全地建立和存放 ACM Private CA 的 CRL](#)。如果您想要停用，請使用 `ct-0xdawir96cy7k` 建立新的 RFC（[管理](#) | [其他](#) | [其他](#) | [更新](#)）並連接風險接受。如果您對風險接受有任何疑問，請聯絡您的 Cloud Architect。

使用 AMS SSP 在您的 AMS 帳戶中 provision AWS CloudEndure

Note

成功啟動後 AWS Application Migration Service，CloudEndure Migration 服務會在所有 AWS 區域中終止生命週期。我們建議客戶使用 AWS Application Migration Service 來提升和轉移遷移至 GovCloud 區域和商業區域。如需詳細資訊，請參閱[什麼是 AWS Application Migration Service ?](#)。

如果您想要使用 AWS Application Migration Service，請聯絡您的 CA，讓他們可以引導您。

使用 AMS 自助式佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 AWS CloudEndure 功能。AWS CloudEndure 遷移可簡化、加速和自動化從實體、虛擬和雲端基礎設施到的大規模遷移 AWS。CloudEndure 災難復原 (DR) 可防止停機時間和資料因任何威脅而遺失，包括勒索軟體和伺服器損毀。

AWS Managed Services 常見問答集中的AWS CloudEndure

問：如何請求存取 AMS 帳戶中的 CloudEndure？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 使用者佈建至您的帳戶：customer_cloud_endure_user。在帳戶中佈建後，使用者存取金鑰和私密金鑰會在 AWS Secrets Manager 中共用。

這些政策也會佈建至帳戶：customer_cloud_endure_policy和 customer_cloud_endure_deny_policy。

此外，您必須提供風險接受，因為用於應用程式整合的 CloudEndure DR 解決方案具有基礎設施變更許可。若要這樣做，請與您的雲端服務交付管理員 (CSDM) 合作。

問：在我的 AMS 帳戶中使用 CloudEndure 有哪些限制？

雲端持久性複寫和轉換執行個體只能在您指定的子網路中啟動。

問：在我的 AMS 帳戶中使用 CloudEndure 的先決條件或相依性是什麼？透過 RFC 雙向通訊共用下列項目：

- 要啟動的複寫和轉換執行個體的 VPC 子網路詳細資訊。
- 如果 EBS 磁碟區已加密，則為 KMS Key Amazon Resource Name (ARN)。

使用 AMS SSP AWS CloudHSM 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CloudHSM 的功能。AWS CloudHSM 可協助您符合公司、合約、在 AWS 雲端中使用專用硬體安全模組 (HSM) 執行個體，確保資料安全的和法規合規要求。AWS 和 AWS Marketplace 合作夥伴提供各種解決方案來保護 AWS 平台內的敏感資料，但對於某些受合約或法規要求管理密碼編譯金鑰的應用程式和資料，可能需要額外的保護。AWS CloudHSM 會補足現有的資料保護解決方案，並允許您保護 HSMs 內的加密金鑰，這些加密金鑰是根據政府標準設計和驗證的安全金鑰管理。AWS CloudHSM 可讓您安全地產生、存放區、和管理用於資料加密的密碼編譯金鑰，只有您才能存取金鑰。如需詳細資訊，請參閱 [AWS CloudHSM](#)。

AWS CloudHSM 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS CloudHSM 的？

在您的 AMS 帳戶中使用是兩個步驟：

1. 請求 AWS CloudHSM 叢集。透過使用 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型提交 RFC 來執行此操作。包含下列詳細資訊：
 - AWS 區域。
 - VPC ID/ARN。提供與您提交的 RFC 位於相同帳戶中的 VPC ID/VPC ARN。
 - 為叢集指定至少兩個可用區域。
 - 將連線至 HSM 叢集的 Amazon EC2 執行個體 ID。
2. 存取 AWS CloudHSM 主控台。透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來執行此操作。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_cloudhsm_console_role`。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入該角色。

問：AWS CloudHSM 在我的 AMS 帳戶中使用有哪些限制？

存取 AWS CloudHSM 主控台無法讓您建立、終止或還原叢集。若要執行這些動作，請提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76) 變更類型。

問：AWS CloudHSM 在我的 AMS 帳戶中使用的先決條件或相依性是什麼？

您必須允許透過 VPC 中的用戶端 Amazon EC2 執行個體使用連接埠 2225 的 TCP 流量，或針對想要存取 HSM 叢集的內部部署伺服器使用 Direct Connect VPN。AWS CloudHSM 取決於 Amazon EC2 的安全群組和網路介面。對於日誌監控或稽核，HSM 依賴 CloudTrail (AWS API 操作) 和 CloudWatch Logs 進行所有本機 HSM 裝置活動。

問：誰會將更新套用至 AWS CloudHSM 用戶端和相關的軟體程式庫？

您負責套用程式庫和用戶端更新。您會想要監控 [CloudHSM 版本歷史記錄](#) 頁面的版本，然後使用 [CloudHSM 用戶端升級](#) 套用更新。

 Note

服務一律會自動套用 HSM AWS CloudHSM 設備的軟體修補程式。

使用 AMS SSP AWS CodeBuild 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeBuild 的功能。AWS CodeBuild 是一種全受管持續整合服務，可編譯原始程式碼、執行測試，並產生準備好部署的軟體套件。使用 CodeBuild，您便不必佈建、管理、擴展自己的組建伺服器。CodeBuild 會持續擴展並同時處理多個組建，所以您的組建不必排入佇列中等候。您可以利用預先封裝好的組建環境立即開始使用，或是建立自訂的組建環境來使用您自己的組建工具。使用 CodeBuild 時，將依據您使用運算資源的分鐘數計費。如需詳細資訊，請參閱 [AWS CodeBuild](#)。

 Note

若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中 `aws_code_pipeline_service_role` 佈建所有三個角色 `customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 `customer_codepipeline_service_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeBuild

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS CodeBuild 的？

AWS CodeBuild 在您的 AMS 帳戶中使用 是兩個步驟：

1. 佈建CodeBuild Service Role用於建置程序的，以與 AWS S3 儲存貯體、Amazon CloudWatch 和日誌群組協調
2. 請求存取 CodeBuild 主控台

您可以向 Management | AWS service | Self-visioned service | Add change type (ct-1w8z66n899dct) 提交 RFC，請求在您的 AMS 帳戶中設定兩者。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS CodeBuild 在我的 AMS 帳戶中使用 有哪些限制？

對於 AWS CodeBuild 主控台管理員存取，許可在資源層級受到限制；例如，CloudWatch 動作在特定資源上受到限制，且iam:PassRole許可受到控制。

問：在我的 AMS 帳戶中使用 CodeBuild 的先決條件或相依性是什麼？

如果定義的 AWS CodeBuild 服務角色需要額外的 IAM 許可，請透過 AMS 服務請求請求它們。

使用 AMS SSP AWS CodeCommit 在您的 AMS 帳戶中佈建

Note

AWS 已於 2024 年 7 月 25 日關閉新客戶對 AWS CodeCommit 的存取權。AWS CodeCommit 現有客戶可以繼續如常使用服務。AWS 會繼續投資的安全性、可用性和效能改善 AWS CodeCommit，但我們不打算推出新功能。

若要將 AWS CodeCommit Git 儲存庫遷移至其他 Git 供應商，請聯絡您的雲端架構師 (CA) 以取得指引。如需遷移 Git 儲存庫的詳細資訊，請參閱[如何將 AWS CodeCommit 儲存庫遷移至另一個 Git 供應商](#)。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeCommit 的功能。AWS CodeCommit 是一種全受管[來源控制](#)服務，可託管安全的 Git 型儲存庫。它可協助團隊在安全且高度可擴展的生態系統中協作程式碼。CodeCommit 不需要操作您自己的來源控制系統或擔心擴展其基礎設施。您可以使用 CodeCommit 安全地存放從原始程式碼到二進位檔的任何內容，並與您現有的 Git 工具無縫搭配使用。如需詳細資訊，請參閱[AWS CodeCommit](#)。

 Note

若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中aws_code_pipeline_service_role佈建所有三個角色customer_codebuild_service_rolecustomer_codedeploy_service_role、和。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeCommit

問：如何請求存取 AMS 帳戶中的 CodeCommit？

AWS CodeCommit 主控台和資料存取角色可以透過提交兩個 AWS 服務 RFCs、主控台存取和資料存取來請求：

- 透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS CodeCommit 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_codecommit_console_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

資料存取（例如訓練和實體清單）需要每個指定 S3 資料來源（必要）、輸出儲存貯體（必要）和 KMS（選用）之資料來源的個別 CTs。只要所有資料來源都已授予存取角色，AWS CodeCommit 工作建立就沒有限制。若要請求資料存取，請使用 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 提交 RFC。

問：AWS CodeCommit 在我的 AMS 帳戶中使用 有哪些限制？

CodeCommit 上的觸發功能會因為建立 SNS 主題的相關權限而停用。針對 CodeCommit 的直接驗證受到限制，使用者應該使用登入資料協助程式進行驗證。有些 KMS 命令也會受到限制：kms:Encrypt、kms:Decrypt、kms:ReEncrypt、kms:GenerateDataKeyWithoutPlaintext、kms:GenerateDataKey和 kms:DescribeKey。

問：AWS CodeCommit 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

如果 S3 儲存貯體使用 KMS 金鑰加密，則需要 S3 和 KMS 才能使用 AWS CodeCommit。

使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodeDeploy 的功能。AWS CodeDeploy 是一項全受管部署服務，可將軟體部署自動化至各種運算服務，例如 Amazon EC2 AWS Fargate AWS Lambda 和您的內部部署伺服器。AWS CodeDeploy 可協助您快速發行新功能，協助您避免在應用程式部署期間停機，並處理更新應用程式的複雜性。您可以使用 AWS CodeDeploy 來自動化軟體部署，無需進行容易出錯的手動操作。服務會擴展以符合您的部署需求。如需詳細資訊，請參閱 [AWS CodeDeploy](#)。

Note

若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中 `aws_code_pipeline_service_role` 佈建所有三個角色 `customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 `customer_codepipeline_service_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

AWS Managed Services 常見問答集中的 CodeDeploy

問：如何請求存取 AMS 帳戶中的 CodeDeploy？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 CodeDeploy。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_codedeploy_console_role` 和 `customer_codedeploy_service_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入 `customer_codedeploy_console_role` 角色。

問：在我的 AMS 帳戶中使用 CodeDeploy 有哪些限制？

目前我們僅支援運算平台做為 — Amazon EC2/內部部署。不支援藍/綠部署。

問：在我的 AMS 帳戶中使用 CodeDeploy 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 CodeDeploy 沒有先決條件或相依性。

使用 AMS SSP AWS CodePipeline 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS CodePipeline 的功能。AWS CodePipeline 是一種全受管 [持續交付](#) 服務，可協助您自動化發行管道，以快速且可靠的應用程式和基

礎設施更新。根據您定義的發行模型，CodePipeline 可以自動在每次程式碼變更時建置、測試和部署程式碼。這可讓您快速且可靠地交付功能和更新。您可以輕鬆地 AWS CodePipeline 與第三方服務整合，例如 GitHub 或您自己的自訂外掛程式。使用時 AWS CodePipeline，您只需支付使用量的費用。沒有預付費用，也無需長期承諾。如需詳細資訊，請參閱 [AWS CodePipeline](#)。

Note

若要使用單一 RFC 加入 CodeCommit、CodeBuild、CodeDeploy 和 CodePipeline，請提交 [管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）\(ct-3qe6io8t6jtny\)](#) 變更類型，並請求三種服務：CodeBuild、CodeDeploy 和 CodePipeline。然後，在您的帳戶中 `aws_code_pipeline_service_role` 佈建所有三個角色 `customer_codebuild_service_role`、`customer_codedeploy_service_role` 和 `customer_codepipeline_service_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。AMS 中的 CodePipeline 不支援來源階段的「Amazon CloudWatch Events」，因為它需要更高的許可才能建立服務角色和政策，這會略過最低權限模型和 AMS 變更管理程序。

AWS Managed Services 常見問答集中的 CodePipeline

問：如何請求存取 AMS 帳戶中的 CodePipeline？

透過為 `customer_code_pipeline_console_role` 相關帳戶中的 提交服務請求，請求存取 CodePipeline。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：`aws_code_pipeline_service_role_policy`。

問：在我的 AMS 帳戶中使用 CodePipeline 有哪些限制？

是。CodePipeline 功能、階段和提供者僅限於下列項目：

1. 部署階段：僅限 Amazon S3，以及 AWS CodeDeploy
2. 來源階段：僅限 Amazon S3 AWS CodeCommit、BitBucket 和 GitHub
3. 組建階段：僅限 AWS CodeBuild 和 Jenkins
4. 核准階段：僅限 Amazon SNS
5. 測試階段：僅限 Jenkins AWS CodeBuild、BlazeMeter、Ghost Inspector UI 測試、Micro Focus StormRunner Load 和 Runscope API 監控
6. 調用階段：僅限 Step Functions 和 Lambda

 Note

AMS Operations 將在您的帳戶 `customer_code_pipeline_lambda_policy` 中部署；它必須與 Lambda 執行角色連接，以用於 Lambda 調用階段。請提供您要新增此政策的 Lambda 服務/執行角色名稱。如果沒有自訂 Lambda 服務/執行角色，AMS 將建立一個名為 `customer_code_pipeline_lambda_execution_role` 的新角色，這會是 `customer_lambda_basic_execution_role` 與 `customer_code_pipeline_lambda_policy` 的複本。

問：在我的 AMS 帳戶中使用 CodePipeline 的先決條件或相依性是什麼？

AWS 支援的服務，AWS CodeCommit AWS CodeBuild AWS CodeDeploy 必須在啟動 CodePipeline 之前或同時啟動。

使用 AMS SSP AWS Compute Optimizer 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Compute Optimizer 的功能。AWS Compute Optimizer 建議工作負載的最佳 AWS 運算資源，以使用機器學習分析歷史使用率指標來降低成本並改善效能。過度佈建運算 (Amazon EC2 和 ASGs) 可能會導致不必要的基礎設施成本，而佈建不足的運算可能會導致應用程式效能不佳。Compute Optimizer 可協助您根據您的使用率資料，選擇最佳的 Amazon EC2 執行個體類型，包括屬於 Amazon EC2 Auto Scaling 群組的執行個體類型。如需詳細資訊，請參閱 [AWS Compute Optimizer](#)。

AWS Managed Services 常見問答集中的 Compute Optimizer

問：如何請求存取 AMS 帳戶中的 Compute Optimizer？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny)

變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

`customer_compute_optimizer_readonly_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Compute Optimizer 有哪些限制？

沒有限制。完整功能 AWS Compute Optimizer 可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 Compute Optimizer 的先決條件或相依性是什麼？

- 您必須提交 RFC（管理 | 其他 | 其他 | 更新），授權 AMS Ops 在帳戶中啟用服務。在部署期間，會建立服務連結角色 (SLR)，以允許收集指標和產生報告。SLR 標記為「AWSServiceRoleForComputeOptimizer」。如需詳細資訊，請參閱[使用的服務連結角色 AWS Compute Optimizer](#)
- 必須為下列指標啟用 CloudWatch 指標：
 - CPU 使用率：執行個體上使用的已配置 Amazon EC2 運算單位百分比。此指標可識別在所選執行個體上執行應用程式所需的處理能力。
 - 記憶體使用率：在取樣期間以某種方式使用的記憶體量。此指標識別在所選執行個體上執行應用程式所需的記憶體。記憶體使用率只會針對已安裝統一 CloudWatch 代理程式的資源進行分析。如需詳細資訊，請參閱使用 CloudWatch Agent 啟用記憶體使用率（第 10 頁）。
 - 網路傳入：執行個體在所有網路界面上接收的位元組數。此指標可識別傳入至單一執行個體的網路流量。
 - 網路輸出：執行個體在所有網路界面上傳送的位元組數。此指標可識別來自單一執行個體的傳出網路流量。
 - 本機磁碟輸入/輸出 (I/O)：本機磁碟的輸入/輸出操作數目。此指標可識別執行個體根磁碟區的效能

使用 AMS SSP AWS DataSync 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS DataSync 的功能。會在內部部署儲存體與 Amazon S3、Amazon Elastic File System (Amazon Elastic File System) 或 Amazon FSx 之間線上 AWS DataSync 移動大量資料。與資料傳輸相關的手動任務可能會降低遷移速度和 IT 操作的負擔。DataSync 消除或自動處理許多這些任務，包括編寫複製任務指令碼、排程和監控傳輸、驗證資料，以及最佳化網路使用率。DataSync 軟體代理程式會連線至您的網路檔案系統 (NFS) 和伺服器訊息區塊 (SMB) 儲存體，因此您不需要修改應用程式。DataSync 可以透過網際網路或 AWS Direct Connect 連結，以高達開放原始碼工具 10 倍的速度傳輸數百 TB 和數百萬個檔案。您可以使用 DataSync 將作用中資料集或封存遷移至 AWS、將資料傳輸至雲端以進行及時分析和處理，或將資料複寫至 AWS 以進行業務連續性。

如需詳細資訊，請參閱 [AWS DataSync](#)。

AWS Managed Services 常見問答集中的 DataSync

問：如何請求存取 AMS 帳戶中的 DataSync？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_datasync_console_role。

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

要用來串流任務日誌的 CloudWatch 日誌群組是 `"/aws/datasync"`。

問：在我的 AMS 帳戶中使用 DataSync 有哪些限制？

完整功能 AWS DataSync 可在您的 AMS 帳戶中使用。

問：在我的 AMS 帳戶中使用 DataSync 的先決條件或相依性是什麼？

- 與將使用 DataSync 服務角色 執行的 DataSync 任務相關聯的所有 S3 儲存貯體都需要 Amazon S3 ARNs (Amazon Resource Name) `customer_datasync_service_role`。DataSync
- DataSync 代理程式的 VPC 端點和安全群組必須在使用 VPC 端點之前，使用 RFC 搭配 管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型來請求。
- AWS DataSync 代理程式會以設備身分在 AMS 中執行。AWS DataSync 代理程式由 服務修補和更新；如需詳細資訊，請參閱 [AWS DataSync 常見問答集](#)。
- 若要啟動 AWS DataSync 代理程式，請使用 Management | Other | Other | Create (ct-1e1xtak34nx76) 變更類型提交 RFC，請求部署代理程式。提供 AWS DataSync Amazon EC2 AMI ID、執行個體類型、子網路、安全群組；並參考現有的 Amazon EC2 金鑰對或請求建立新的金鑰對。

Note

AMS 代表客戶手動佈建 AWS DataSync 代理程式，不需要在 AWS DataSync Amazon EC2 AMI 上進行 WIGS 擷取程序。

使用 AMS SSP AWS Device Farm 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Device Farm 的功能。AWS Device Farm 是一種應用程式測試服務，可讓您透過廣泛的桌面瀏覽器和真實行動裝置測試 Web 和行動應用程式，藉此改善其品質；無需佈建和管理任何測試基礎設施。此服務可讓您在多個桌面瀏覽器或真實裝置上同時執行測試，以加速測試套件的執行，並產生影片和日誌，協助您快速識別應用程式的問題。

如需詳細資訊，請參閱 [AWS Device Farm](#)。

AWS Device Farm 在 AWS Managed Services 常見問答集中

問：如何請求存取 AMS 帳戶中 AWS Device Farm 的？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_devicefarm_role。

在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：AWS Device Farm 在我的 AMS 帳戶中使用 有哪些限制？

除了在 'Name' 標籤中使用 AMS 命名空間之外，還提供 AWS Device Farm 服務的完整存取權。

問：AWS Device Farm 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

無。

使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elastic Disaster Recovery 的功能。使用經濟實惠的儲存、最少的運算和point-in-time復原，透過快速、可靠的內部部署和雲端應用程式復原，將停機時間和資料遺失 AWS Elastic Disaster Recovery 降至最低。當您使用 AWS Elastic Disaster Recovery 複寫在支援的作業系統上執行的內部部署或雲端型應用程式時，可以提高 IT 彈性。使用 AWS Management Console 來設定複寫和啟動設定、監控資料複寫，以及啟動執行個體以進行演練或復原。

如需詳細資訊，請參閱 [AWS Elastic Disaster Recovery](#)。

AWS Elastic Disaster Recovery AWS Managed Services 常見問答集中的

問：如何請求存取 AMS 帳戶中 AWS Elastic Disaster Recovery 的 ？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_drs_console_role。

在您的帳戶中佈建之後，您必須在聯合解決方案中加入該角色。

問：AWS Elastic Disaster Recovery 在我的 AMS 帳戶中使用 有哪些限制？

AWS Elastic Disaster Recovery 在您的 AMS 帳戶中沒有使用 的限制。

問：AWS Elastic Disaster Recovery 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

- 存取主控台角色之後，您必須初始化 Elastic Disaster Recovery 服務，以在帳戶中建立所需的 IAM 角色。

- 您必須提交變更類型 管理 | 應用程式 | IAM 執行個體描述檔 | 建立 (需要檢閱) 變更類型 ct-0ixp4ch2tiu04 RFC，以建立customer-mc-ec2-instance-profile執行個體描述檔的複製並連接AWSElasticDisasterRecoveryEc2InstancePolicy政策。您必須指定要連接新政策的機器。
- 如果執行個體未使用預設執行個體描述檔，則 AMS 可以透過自動化AWSElasticDisasterRecoveryEc2InstancePolicy連接。
- 您必須使用客戶擁有的 KMS 金鑰進行跨帳戶復原。來源帳戶的 KMS 金鑰必須遵循政策更新，以允許目標帳戶存取。如需詳細資訊，請參閱[與目標帳戶共用 EBS 加密金鑰](#)。
- 必須更新 KMS 金鑰政策，以便在您不想切換角色以檢視時允許 customer_drs_console_role 檢視政策。
- 對於跨帳戶、跨區域災難復原，AMS 必須將來源和目標帳戶設定為信任帳戶，並透過此帳戶部署容錯回復和AWS 適當大小的角色 AWS CloudFormation。

使用 AMS SSP AWS Elemental MediaConvert 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaConvert 的功能。AWS Elemental MediaConvert 是一種具有廣播級功能的檔案型視訊轉碼服務。它可讓您建立 video-on-demand(VOD) 內容，以進行大規模廣播和多螢幕交付。此服務結合了進階視訊和音訊功能，以及簡單的 Web 服務界面和pay-as-you-go定價。透過 AWS Elemental MediaConvert，您可以專注於提供令人信服的媒體體驗，而不必擔心建置和操作您自己的影片處理基礎設施的複雜性。

如需詳細資訊，請參閱 [AWS Elemental MediaConvert](#)。

AWS Managed Services 常見問答集中的 MediaConvert

問：如何請求存取 AMS 帳戶中的 MediaConvert？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_mediaconvert_author_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

customer_MediaConvert_Default_RoleMediaConvert 將使用第二個角色 來讀取來源 S3 儲存貯體並將輸出寫入目的地 S3 儲存貯體，並在您需要數位版權管理 (DRM) 時叫用 API 閘道。

問：在我的 AMS 帳戶中使用 MediaConvert 有哪些限制？

在 AMS 中使用 MediaConvert 沒有限制。

問：在我的 AMS 帳戶中使用 MediaConvert 有哪些先決條件或相依性？

在您的 AMS 帳戶中使用 MediaConvert 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaLive 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaLive 的功能。AWS Elemental MediaLive 是一種廣播級即時視訊處理服務。它可讓您建立高品質的影片串流，以交付至廣播電視和網際網路連線的多螢幕裝置，例如連接的TVs、平板電腦、智慧型手機和機上盒。此服務的運作方式是即時編碼您的即時視訊串流、取得較大的即時視訊來源，並將其壓縮為較小的版本，以分發給您的檢視器。使用 AWS Elemental MediaLive，您可以輕鬆地為即時事件和全年無休頻道設定串流，具有進階廣播功能、高可用性和pay-as-you-go定價。AWS Elemental MediaLive 可讓您專注於為觀眾建立令人信服的即時視訊體驗，而不需要建置和操作廣播級視訊處理基礎設施的複雜性。

如需詳細資訊，請參閱 [AWS Elemental MediaLive](#)。

AWS Managed Services 常見問答集中的 MediaLive

問：如何請求存取 AMS 帳戶中的 MediaLive？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_medialive_author_role。

作為此 RFC 的一部分，第二個角色會部署到您的帳戶；customer_medialive_service_role此角色可指派給您的 Media Live 頻道和輸入，以與其他服務互動，例如 Amazon S3、MediaStore 和 CloudWatch Logs。

在帳戶中佈建角色之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 MediaLive 有哪些限制？

在 AMS 中使用 MediaLive 沒有限制。

問：在我的 AMS 帳戶中使用 MediaLive 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaLive 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaPackage 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaPackage 的功能。AWS Elemental MediaPackage 可靠地準備和保護您的視訊，以便透過網際網路交付。從單一

視訊輸入，AWS Elemental MediaPackage 會建立格式化的視訊串流，以便在連接的 TVs、行動電話、電腦、平板電腦和遊戲主控台上播放。它可以輕鬆為瀏覽者實作熱門的影片功能（開始、暫停、倒轉等），就像 DVRs 上常見的功能一樣。AWS Elemental MediaPackage 也可以使用數位版權管理 (DRM) 自動保護您的內容。會自動 AWS Elemental MediaPackage 擴展以回應載入，因此您的瀏覽者將永遠獲得絕佳的體驗，而無需事先準確預測您需要的容量。

如需詳細資訊，請參閱 [AWS Elemental MediaPackage](#)。

AWS Managed Services 常見問答集中的 MediaPackage

問：如何請求存取 AMS 帳戶中 AWS Elemental MediaPackage 的？

透過提交管理 | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_mediapackage_author_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

系統會提供第二個角色 customer_mediapackage_service_role，該角色可指派給您的 Media Live 頻道和輸入，以便與其他服務互動，例如 S3 和 Secrets Manager。

問：在我的 AMS 帳戶中使用 MediaPackage 有哪些限制？

在 AMS 中使用 MediaPackage 沒有限制。

問：在我的 AMS 帳戶中使用 MediaPackage 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaPackage 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaStore 在您的 AMS 帳戶中佈建

Note

在仔細考慮之後，AWS 決定停止 MediaStore，自 2025 年 11 月 13 日起生效。如果您是 MediaStore 的作用中客戶，您可以正常使用 MediaStore，直到 2025 年 11 月 13 日服務支援結束為止。在此日期之後，您將無法再使用 MediaStore 或此服務提供的任何功能。

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaStore 的功能。AWS Elemental MediaStore 是一種針對媒體最佳化的 AWS 儲存服務。它為您提供交付即時串流影片內容所需的效能、一致性和低延遲。AWS Elemental MediaStore 會做為影片工作流程中的原始儲存

體。其高效能功能可滿足最嚴苛媒體交付工作負載的需求，並結合長期、經濟實惠的儲存體。如需詳細資訊，請參閱 [AWS Elemental MediaStore](#)。

AWS Managed Services 中的 MediaStore 常見問答集

問：如何請求存取 AMS 帳戶中的 MediaStore？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 MediaStore。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_mediastore_author_role。作為此 RFC 的一部分，第二個角色會部署到您的帳戶；如果您選擇啟用該功能，則 MediaStore 服務會使用該MediaStoreAccessLogs角色來記錄 CloudWatch 中的活動。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

目前，AMS Operations 也會在您的帳戶中部署此服務角色：aws_code_pipeline_service_role_policy。

問：在我的 AMS 帳戶中使用 MediaStore 有哪些限制？

在 AMS 中使用 MediaStore 沒有限制。

問：在我的 AMS 帳戶中使用 MediaStore 有哪些先決條件或相依性？

在您的 AMS 帳戶中使用 MediaStore 沒有先決條件或相依性。

使用 AMS SSP AWS Elemental MediaTailor 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Elemental MediaTailor 的功能。AWS Elemental MediaTailor 影片提供者會將個別目標式廣告插入其影片串流，而不會犧牲廣播層級quality-of-service。使用 AWS Elemental MediaTailor時，即時或隨需影片的瀏覽者都會收到串流，將您的內容與個人化的廣告結合在一起。但與其他個人化廣告解決方案不同，AWS Elemental MediaTailor 您的整個串流 - 影片和廣告 - 都會提供廣播級影片品質，以改善觀眾的體驗。會根據用戶端和伺服器端廣告交付指標 AWS Elemental MediaTailor 提供自動化報告，以準確測量廣告曝光和觀眾行為。您可以使用 輕鬆獲利非預期的高需求檢視事件，無需預付成本 AWS Elemental MediaTailor。它還可以提高廣告交付率，協助您從每個影片中獲利更多，並適用於更廣泛的內容交付網路、廣告決策伺服器和用戶端裝置。

如需詳細資訊，請參閱 [AWS Elemental MediaTailor](#)。

AWS Managed Services 常見問答集中的 MediaTailor

問：如何請求存取 AMS 帳戶中的 MediaTailor？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 MediaTailor。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer-mediatailor-role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 MediaTailor 有哪些限制？

在 AMS 中使用 MediaTailor 沒有限制。

問：在我的 AMS 帳戶中使用 MediaTailor 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 MediaTailor 沒有先決條件或相依性。

使用 AMS SSP AWS Global Accelerator 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Global Accelerator 功能。Global Accelerator 是一種網路層服務，您可以在其中建立加速器，以改善全球受眾使用的網際網路應用程式的可用性和效能。若要進一步了解，請參閱 [Global Accelerator](#)。

AWS Managed Services 中的 Global Accelerator 常見問答集

常見問題和解答：

問：如何請求在我的 AMS 帳戶中設定 Global Accelerator？

透過提交 AWS 服務 RFC 請求存取權（管理 | AWS 服務 | 自助佈建服務）。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色：customer_global_accelerator_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入主控台角色。

問：在我的 AMS 帳戶中使用 Global Accelerator 有哪些限制？

Global Accelerator 是一種全域服務，支援多個 AWS 區域中的端點，列於[AWS 區域資料表](#)中。

問：在我的 AMS 帳戶中使用 Global Accelerator 的先決條件或相依性是什麼？

當您設定加速器與 Global Accelerator 時，您可以將靜態 IP 地址與一或多個區域中的區域端點建立關聯 AWS。對於標準加速器，端點為 Network Load Balancer、Application Load Balancer、Amazon EC2 執行個體或彈性 IP 地址。對於自訂路由加速器，端點是具有一或多個 EC2 執行個體的虛擬私有雲端 (VPC) 子網路。

使用 AMS SSP AWS Glue 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Glue 的功能。AWS Glue 是一種全受管擷取、轉換和載入 (ETL) 服務，可協助您準備和載入資料以供分析。您可以在 [中按幾下滑鼠來](#)

建立和執行 ETL 任務 AWS Management Console。您可以指向存放在 AWS Glue 上的資料 AWS，並 AWS Glue 探索您的資料，並將相關聯的中繼資料（例如資料表定義和結構描述）存放在 AWS Glue Data Catalog。編製目錄後，您的資料即可立即搜尋、查詢，並可用於 ETL 動作。如需詳細資訊，請參閱 [AWS Glue](#)。

AWS Glue 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Glue 請求在我的 AMS 帳戶中設定？

透過使用 [管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 \(ct-1w8z66n899dct\)](#) 提交 RFC AWS Glue 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

- `customer_glue_console_role`
- `customer_glue_service_role`

上述角色包括下列連接的政策：

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

在帳戶中佈建角色之後，您必須在聯合解決方案中加入這些角色。

若要存取爬蟲程式、任務和開發端點（特定使用案例所需的角色），請使用 [部署 | 進階堆疊元件 | Identity and Access Management \(IAM\) | 建立實體或政策 \(ct-3dpd8mdd9jn1r\)](#) 提交 RFC。

問：AWS Glue 在我的 AMS 帳戶中使用 有哪些限制？

沒有限制。完整功能 AWS Glue 可在您的 AMS 帳戶中使用。對於您可以在其中撰寫和測試 ETL 指令碼的互動式環境，請在 AWS Glue Studio 上使用筆記本。AWS Glue 互動式工作階段和任務筆記本是無伺服器功能 AWS Glue，您可以在其中使用 AWS Glue 並使用 AWS Glue 服務角色。

AWS Glue 2.0 之前：AWS Glue 筆記本是非受管資源，可在帳戶中啟動 Amazon EC2 執行個體。最佳實務是啟動您自己的 Amazon EC2 執行個體，並安裝支援筆記本環境和開發所需的軟體。如需詳細資訊，請參閱[教學課程：設定本機 Apache Zeppelin 筆記本來測試和偵錯 ETL 指令碼](#)，以及[使用開發端點來開發指令碼](#)。

問：AWS Glue 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Glue 具有 Amazon S3、CloudWatch 和 CloudWatch Logs 的相依性。暫時性相依性會根據資料來源而有所不同，而且其他服務 AWS Glue 功能可能會與 互動（例如：Amazon Redshift、Amazon RDS、Athena）。

使用 AMS SSP AWS Lake Formation 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Lake Formation 的功能。AWS Lake Formation 是一種可在幾天內輕鬆設定安全資料湖的服務。資料湖是一個集中式、經策管且安全的儲存庫，可用原始格式存放您的所有資料並準備進行分析。資料湖可讓您細分資料孤島，再結合不同類型的分析來取得洞察並指導得出最佳的商業決策。

使用 Lake Formation 建立資料湖，就跟定義資料來源、您想要套用哪些資料存取和安全政策一樣簡單。Lake Formation 之後有助於您從資料庫和物件儲存中收集和編製資料目錄、將資料移至新的 Amazon S3 資料湖、使用機器學習演算法清理和分類資料，以及安全存取敏感資料。您的使用者可以存取集中式資料目錄（如需詳細資訊，請參閱[AWS Glue 常見問答集](#)），說明可用的資料集及其適當的使用方式。然後，您的使用者會利用這些資料集搭配其選擇的分析和機器學習服務，例如 [Amazon Redshift](#)、[Amazon Athena](#) 和（測試版）[Amazon EMR](#) for Apache Spark。Lake Formation 以中可用的功能為基礎[AWS Glue](#)。

如需詳細資訊，請參閱 [AWS Lake Formation](#)。

AWS Managed Services 中的 Lake Formation 常見問答集

問：如何請求存取 AMS 帳戶中 AWS Lake Formation 的？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny)

變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：

customer_lakeformation_data_analyst_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

此外，以下兩個角色是選用的：

- customer_lakeformation_admin_role
- customer_lakeformation_workflow_role

對於管理員許可，您可以選擇將角色加入customer_lakeformation_admin_role為相同 SSPS 變更類型 (ct-3qe6io8t6jtny) 的一部分。

如果您想要在 AWS Lake Formation 主控台中建立藍圖，您需要提交管理 | 其他 | 其他 RFC (ct-1e1xtak34nx76) 以部署 customer_lakeformation_workflow_role。在 RFC 中，如果建立

藍圖時儲存貯體是來源，您必須提供 S3 儲存貯體名稱。如果藍圖類型為 Classic Load Balancer Logs 或 Application Load Balancer Logs AWS CloudTrail，則 S3 儲存貯體適用。

問：AWS Lake Formation 在我的 AMS 帳戶中使用 有哪些限制？

Lake Formation 的完整功能可在 AMS 中使用。

問：AWS Lake Formation 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

Lake Formation 與 AWS Glue 服務整合，因此 AWS Glue 使用者只能存取具有 Lake Formation 許可的資料庫和資料表。此外，AWS Athena 和 Amazon Redshift 使用者只能查詢具有 Lake Formation 許可的 AWS Glue 資料庫和資料表。

使用 AMS SSP AWS Lambda 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Lambda 的功能。AWS Lambda 無需佈建或管理伺服器即可執行程式碼。您只需為使用的運算時間付費，程式碼未執行時無需付費。使用 Lambda，您可以為幾乎任何類型的應用程式或後端服務執行程式碼，完全無需管理。上傳您的程式碼，Lambda 會處理執行和擴展程式碼所需的一切，並提供高可用性。您可以設定程式碼以自動從其他 AWS 服務觸發，或直接從任何 Web 或行動應用程式呼叫它。如需詳細資訊，請參閱 [AWS Lambda](#)。

AWS Managed Services 常見問答集中的 Lambda

問：如何請求存取 AMS 帳戶中 AWS Lambda 的？

透過提交管理 | AWS 服務 | 自行佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_lambda_admin_role 和 customer_lambda_basic_execution_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS Lambda 在我的 AMS 帳戶中使用 有哪些限制？

- Lambda 函數旨在由事件來源調用。如需可做為 Lambda 事件來源的服務清單，請參閱[搭配使用 AWS Lambda 與其他 服務](#)。AMS 帳戶目前並未提供所有這些服務。如果您需要無法使用的服務，請使用您的 AMS CSDM 來提交例外狀況。
- 根據預設，AMS 會為您提供基本的 Lambda 啟動角色，其中包含 AWSLambdaBasicExecutionRole 和 AWSXrayWriteOnlyAccess 許可；如需相關資訊，請參閱[AWS Lambda 啟動角色](#)。如果您需要其他許可，例如能夠在 AMS VPC 中佈建 Lambda 函數，請使用 Management | AWS 服務 | 自助佈建服務 | 新增（需要檢閱）(ct-3qe6io8t6jtny) 變更類型提交 RFC。

問：AWS Lambda 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

沒有先決條件或相依性可開始使用 AWS Lambda；不過，根據您的特定使用案例，您可能需要存取其他 AWS 服務來建立事件來源，或您的函數執行各種動作的額外許可。如果需要其他許可，請使用 [Management | AWS 服務 | 自助佈建服務 | 新增 \(需要檢閱\) 變更類型 \(ct-3qe6io8t6jtny\)](#) 提交 RFC。

問：我需要做什麼才能在任何帳戶中執行 Lambda 函數？

若要在核心帳戶中部署 Lambda 函數，請使用下列準則：

- 確定的 SSPS AWS Lambda 已加入。
- 只要 AMS 資源受到保護且合規，AMS 責任就沒有禁止此部署的特定限制。
- 如果您希望 AMS 建立 Lambda 函數，則必須先使用 提供的 SSPS 角色 AWS Lambda。然後，如果您仍希望 AMS 協助部署或支援 函數，請聯絡您的 CA 並開始超出範圍 (OOS) 程序。

使用 AMS SSP AWS License Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS License Manager 的功能。與 AWS 服務 AWS License Manager 整合，透過單一 AWS 帳戶簡化跨多個 AWS 帳戶、IT 目錄和內部部署的授權管理。AWS License Manager 可讓管理員建立模擬其授權協議條款的自訂授權規則，然後在 Amazon EC2 執行個體啟動時強制執行這些規則。中的規則 AWS License Manager 可讓您透過實際停止執行個體啟動，或通知管理員有關違規的情況，來限制授權違規。如需詳細資訊，請參閱 [AWS License Manager](#)。

AWS Managed Services 常見問答集中的 License Manager

常見問題和解答：

問：如何 AWS License Manager 請求在我的 AMS 帳戶中設定？

透過使用 [管理 | AWS 服務 | 自助佈建服務 | 新增 \(ct-1w8z66n899dct\)](#) 變更類型提交 RFC AWS License Manager 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_license_manager_role`。在您的帳戶中佈建 License Manager IAM 角色後，您必須在聯合解決方案中加入該角色。

問：AWS License Manager 在我的 AMS 帳戶中使用 有哪些限制？

您可以將 AWS License Manager 規則與您擁有 AMIs 建立關聯（依「由我擁有」進行篩選）。如果您選擇強制執行與 AMI 的限制關聯（例如：只能支援此 AMI 的 100 個 vCPU）並耗盡限制，則未來使用該 AMI 啟動會遭到封鎖，並傳回錯誤，指出「沒有可用的授權」。這是此服務的預期行為（不允

許授權耗盡)。如果您用盡限制，但需要再次啟動 AMI，則必須修改在 中設定的規則 AWS License Manager。

問：AWS License Manager 在我的 AMS 帳戶中使用的先決條件或相依性是什麼？

AWS License Manager 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Migration Hub 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Migration Hub 的功能。AWS Migration Hub 提供單一位置，可讓您追蹤跨多個 AWS 和合作夥伴解決方案的應用程式遷移進度。使用 Migration Hub 可讓您選擇最符合您需求的 AWS 和合作夥伴遷移工具，同時提供跨應用程式產品組合遷移狀態的可見性。Migration Hub 也為個別應用程式提供關鍵指標和進度，無論使用哪些工具來進行遷移。這可讓您快速取得所有遷移的進度更新、輕鬆識別和疑難排解任何問題，並減少遷移專案所花費的整體時間和精力。如需詳細資訊，請參閱 [AWS Migration Hub](#)。

AWS Managed Services 常見問答集中的遷移中樞

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Migration Hub？

透過使用 Management | AWS service | Self-visioned service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Migration Hub。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_migrationhub_author_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：Migration Hub 有哪些限制？

無。

問：啟用 Migration Hub 的先決條件有哪些？

在您的 AMS 帳戶中開始使用 Migration Hub 沒有先決條件。不過，在管理服務期間，可能需要 Migration Hub 以外的許可，例如將許可寫入 Amazon S3 以上傳伺服器資訊。

使用 AMS SSP AWS Outposts 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Outposts 的功能。AWS Outposts 是一項全受管服務，可將 AWS 基礎設施、AWS 服務、APIs 和工具延伸至幾乎所有資料中心、主機代管空間或內部部署設施，以獲得一致的混合體驗。AWS Outposts 非常適合需要低延遲存取內部部署系統、本機資料處理或本機資料儲存的工作負載。如需詳細資訊，請參閱 [AWS Outposts](#)。

AWS Outposts 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS Outposts 請求在我的 AMS 帳戶中設定？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC AWS Outposts 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_outposts_role。在帳戶中佈建角色後，您必須在聯合解決方案中加入該角色。

問：AWS Outposts 在我的 AMS 帳戶中使用 有哪些限制？

AWS Outposts 在您的 AMS 帳戶中使用 沒有限制。

問：AWS Outposts 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Outposts 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Resilience Hub 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Resilience Hub 的功能。AWS Resilience Hub 可協助您主動準備和保護您的 AWS 應用程式免受中斷。Resilience Hub 提供彈性評估和驗證，整合到您的軟體開發生命週期中，以發現彈性弱點。Resilience Hub 可協助您預估應用程式是否可以符合復原時間目標 (RTO) 和復原點目標 (RPO) 目標，並協助在問題發佈到生產環境之前解決問題。在生產環境中部署 AWS 應用程式之後，您可以使用 Resilience Hub 繼續追蹤應用程式的彈性狀態。如果發生中斷，Resilience Hub 會傳送通知給操作員，以啟動相關聯的復原程序。

AWS Resilience Hub 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Resilience Hub 的？

透過使用 Management | AWS service | Self-visioned Service | Add (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Resilience Hub。此 RFC 會將下列 IAM 角色和政策佈建至您的帳戶：

IAM 角色

- customer_resiliencehub_console_role
- customer_resiliencehub_service_role

Policies

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

在帳戶中佈建角色之後，您必須在聯合解決方案 `customer_resiliencehub_console_role` 中加入角色。

問：AWS Resilience Hub 在我的 AMS 帳戶中使用 有哪些限制？

沒有限制。您的 AMS 帳戶中提供 Resilience Hub 的完整功能。

問：AWS Resilience Hub 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Resilience Hub 沒有先決條件或相依性。

使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Secrets Manager 的功能。AWS Secrets Manager 可協助您保護存取應用程式、服務和 IT 資源所需的秘密。此服務可讓您在整個生命週期中輕鬆輪換、管理和擷取資料庫登入資料、API 金鑰和其他秘密。使用者和應用程式透過呼叫 Secrets Manager APIs 來擷取秘密，無需以純文字硬式編碼敏感資訊。Secrets Manager 提供秘密輪換與 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的內建整合。此外，此服務可延伸至其他類型的秘密，包括 API 金鑰和 OAuth 權杖。如需詳細資訊，請參閱 [AWS Secrets Manager](#)。

Note

根據預設，AMS 運算子可以在 中存取使用帳戶預設 AWS KMS 金鑰 AWS Secrets Manager (CMK) 加密的秘密。如果您希望 AMS Operations 無法存取您的秘密，請使用自訂 CMK，並搭配 AWS Key Management Service (AWS KMS) 金鑰政策來定義適用於存放在秘密中資料的許可。

AWS Managed Services 常見問答集中的 Secrets Manager

問：如何請求存取 AMS 帳戶中 AWS Secrets Manager 的 ？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-3qe6io8t6jtny) 變更類型提交 RFC 來請求 Secrets Manager 的存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：
`customer_secrets_manager_console_role`和 `customer-rotate-secrets-`

lambda-role。customer_secrets_manager_console_role 用作佈建和管理秘密的管理員角色，並customer-rotate-secrets-lambda-role用作輪換秘密的 Lambda 函數的 Lambda 執行角色。在帳戶中佈建之後，您必須在聯合解決方案中加入customer_secrets_manager_console_role角色。

問：AWS Secrets Manager 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Secrets Manager 可在您的 AMS 帳戶中使用，以及秘密的自動輪換功能。不過，請注意，不支援使用「建立新的 Lambda 函數以執行輪換」來設定輪換，因為它需要更高的許可才能建立 AWS CloudFormation 堆疊 (IAM 角色和 Lambda 函數建立)，這會略過變更管理程序。AMS Advanced 僅支援「使用現有的 Lambda 函數來執行輪換」，您可以在其中管理 Lambda 函數，以使用 AWS Lambda SSPS Admin 角色輪換秘密。AMS Advanced 不會建立或管理 Lambda 來輪換秘密。

問：AWS Secrets Manager 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

下列命名空間保留供 AMS 使用，無法做為直接存取的一部分使用 AWS Secrets Manager：

- arn : aws : secretsmanager : * : * : secret : ams-shared/*
- arn : aws : secretsmanager : * : * : secret : customer-shared/*
- arn : aws : secretsmanager : * : * : secret : ams/*

使用 Secrets Manager (AMS SSPS) 共用金鑰

在 RFC、服務請求或事件報告的純文字中與 AMS 共用秘密會導致資訊公開事件，而 AMS 會修訂您重新產生金鑰的案例和請求中的資訊。

您可以在此命名空間 下使用 [AWS Secrets Manager](#)(Secrets Manager)customer-shared。

使用 Secrets Manager 共用金鑰常見問答集

問：必須使用 Secrets Manager 共用哪種類型的秘密？

幾個範例是用於建立 VPN 的預先共用金鑰、身分驗證金鑰 (IAM、SSH)、授權金鑰和密碼等機密金鑰。

問：如何使用 Secrets Manager 與 AMS 共用金鑰？

1. 使用您的聯合存取和適當的角色登入 AWS 管理主控台：

對於 SALZ , Customer_ReadOnly_Role

對於 MALZ , AWSManagedServicesChangeManagementRole。

2. 導覽至 [AWS Secrets Manager 主控台](#) , 然後按一下存放新的秘密。
3. 選取 Other type of secrets (其他機密類型)。
4. 以純文字形式輸入秘密值 , 並使用預設 KMS 加密。按一下 Next (下一步)。
5. 輸入秘密名稱和描述 , 名稱一律以客戶共用/ 開頭。例如 , Customer-shared/mykey2022。按一下 Next (下一步)。
6. 保持停用自動輪換 , 按一下下一步。
7. 檢閱並按一下儲存以儲存秘密。
8. 透過服務請求、RFC 或事件報告以秘密名稱回覆我們 , 以便我們識別和擷取秘密。

問：使用 Secrets Manager 共用金鑰需要哪些許可？

SALZ：尋找customer_secrets_manager_shared_policy受管 IAM 政策，並確認政策文件與以下建立步驟中附加的政策文件相同。確認政策已連接至下列 IAM 角色：Customer_ReadOnly_Role。

MALZ：驗證 AMSSecretsManagerSharedPolicy已連接至角色，該AWSManagedServicesChangeManagementRole角色可讓您在ams-shared命名空間中執行GetSecretValue動作。

範例：

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
  "Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

當您新增 AWS Secrets Manager 做為自助式佈建服務時，會授予必要的許可。

使用 AMS SSP AWS Security Hub 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Security Hub 的功能。AWS Security Hub 為您提供安全狀態的全方位檢視，AWS 以及安全產業標準和最佳實務的合規性。Security Hub 會集中並優先處理來自 AWS 帳戶、服務和支援的第三方合作夥伴的安全和合規調查結果，以協助您分析安全趨勢並識別最高優先順序的安全問題。如需詳細資訊，請參閱 [AWS Security Hub](#)。

AWS Managed Services 常見問答集中的 Security Hub

問：如何請求存取 AMS 帳戶中 AWS Security Hub 的？

透過使用 Management | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC，請求存取 Security Hub。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_securityhub_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 Security Hub 有哪些限制？

封存功能已被記錄為潛在的安全和操作風險，並已被限制為自我佈建服務安全角色的一部分。

問：AWS Security Hub 在我的 AMS 帳戶中使用的先決條件或相依性是什麼？

AWS Security Hub 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AppRegistry 功能。AppRegistry 可從中央位置啟用應用程式搜尋、報告和管理動作。建置器很少在單一 AWS 帳戶中建立應用程式。它們通常會依生命週期階段區隔應用程式資源，例如開發、測試和生產。AppRegistry 可讓您將 AWS 定義帳戶中的所有資源集合分組和檢視。

使用 AppRegistry，您可以存放 AWS 應用程式、與應用程式相關聯的資源集合，以及應用程式屬性群組。若要進一步了解，請參閱 [什麼是 AppRegistry](#)。

常見問答集：在 AMS AWS Service Catalog AppRegistry 中

問：如何請求存取 AMS 帳戶中 AWS Service Catalog AppRegistry 的？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型提交 RFC，請求存取 AppRegistry。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer-appregistry-console-role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS Service Catalog AppRegistry 在我的 AMS 帳戶中使用 有哪些限制？

除了在 'Name' 標籤中使用 AMS 命名空間之外，還提供 AppRegistry 服務的完整存取權。

問：AWS Service Catalog AppRegistry 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 AppRegistry 沒有先決條件或相依性。

使用 AMS SSP AWS Shield Advanced 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Shield Advanced 的功能。AWS Shield Advanced 是一種受管分散式拒絕服務 (DDoS) 保護服務，可保護在 上執行的應用程式 AWS。Shield Advanced 提供全年無休的偵測和自動內嵌緩解措施，可將應用程式停機時間和延遲降至最低，因此不需要讓 AWS Support 參與，即可受益於 DDoS 保護。有兩種方案 AWS Shield：標準和進階；AMS 提供 Shield Advanced。若要進一步了解，請參閱 [Shield Advanced](#)。

所有 AWS 客戶都能從自動保護中受益 AWS Shield Standard，無需額外付費。可 AWS Shield Standard 防禦以您的網站或應用程式為目標的最常見、經常發生的網路和傳輸層 DDoS 攻擊。當您 AWS Shield Standard 搭配 Amazon CloudFront 和 Amazon Route 53 使用時，您可以獲得針對所有已知基礎設施（第 3 層和第 4 層）攻擊的全方位可用性保護。

如需針對在 Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB) AWS Global Accelerator、Amazon CloudFront 和 Amazon Route 53 資源上執行的應用程式進行攻擊的更高層級保護，您可以訂閱 AWS Shield Advanced。

除了 隨附的網路和傳輸層保護之外 AWS Shield Standard，AWS Shield Advanced 還提供額外偵測和防禦，以防範大型和複雜的 DDoS 攻擊、近乎即時的攻擊可見性，以及與 AWS WAF Web 應用程式防火牆整合。AWS Shield Advanced 也可讓您全年無休地存取 AWS Shield 回應團隊 (SRT)，並保護 Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (Elastic Load Balancing) AWS Global Accelerator、Amazon CloudFront 和 Amazon Route 53 費用中的 DDoS 相關峰值。

AWS Managed Services 常見問答集中的 Shield Advanced

問：如何請求存取 AMS 帳戶中的 Shield Advanced？

透過使用 管理 | AWS 服務 | 自行佈建服務 | 新增 (ct-1w8z66n899dct) 變更類型提交 RFC 來請求存取 Shield Advanced。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_shield_role和 aws_drt_shield_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

在角色部署到您的帳戶後，您可以使用 customer_shield_role 來確認 AWS Shield Advanced 帳戶中的訂閱。

 Note

請注意，使用 會產生月費和一年的承諾 AWS Shield Advanced。此外，在 AMS AWS Shield Advanced 中使用 可授權 AMS 升級至 AWS Shield (SRT)，其可能會在升級分散式拒絕服務 (DDoS AWS WAF) 事件期間變更您的 Web 應用程式防火牆 () 規則。這些變更將與 AMS 協調進行。

問：在我的 AMS 帳戶中使用 Shield Advanced 有哪些限制？

雖然不是限制，但您應該了解使用 Shield Advanced 部署 `aws_drt_shield_role`，這可讓 AWS Shield 團隊 (SRT) 在升級的 DDoS 事件期間對 AMS 帳戶內的 AWS WAF 規則進行緊急變更。AMS 建議這樣做，以最快的速度修復 DDoS 攻擊，並在 AMS 升級至 SRT 之後發生。

問：在我的 AMS 帳戶中使用 Shield Advanced 的先決條件或相依性是什麼？

在您的 AMS 帳戶中使用 Shield Advanced 沒有先決條件或相依性。

使用 AMS SSP AWS Snowball Edge 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 Snowball Edge 功能。Snowball Edge 是一種 PB 級資料傳輸解決方案，使用專為安全而設計的裝置，將大量資料傳入和傳出 AWS 雲端。Snowball Edge 透過大規模資料傳輸解決常見的挑戰，包括高網路成本、長傳輸時間和安全問題。您可以使用 Snowball Edge 遷移分析資料、基因體資料、影片庫、映像儲存庫、備份，以及封存部分資料中心關機、磁帶取代或應用程式遷移專案。使用 Snowball Edge 傳輸資料簡單、快速、更安全，而且透過高速網際網路傳輸資料的成本可能低至五分之一。

使用 Snowball Edge，您不需要撰寫任何程式碼或購買任何硬體來傳輸資料。從使用 AWS 管理主控台為 Snowball [建立匯入任務](#) 開始，Snowball 裝置會自動運送給您。一旦裝置送達，請將裝置連接至您的本機網路，下載並執行 Snowball 用戶端 (「用戶端」) 以建立連線，然後使用用戶端選取您要傳輸至裝置的檔案目錄。然後，用戶端會高速加密檔案並將其傳輸至裝置。傳輸完成且裝置準備好要送回後，E Ink 運送標籤會自動更新，而且您可以使用 Amazon Simple Notification Service (Amazon SNS)、文字訊息或直接在主控台中追蹤任務狀態。如需詳細資訊，請參閱 [AWS Snowball Edge](#)。

AWS Managed Services 常見問答集中的 Snowball Edge

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Snowball Edge 的？

在 AMS 中實作 Snowball Edge 是一個兩步驟的程序：

1. 提交管理 | 其他 | 其他 | 建立 (ct-1e1xtak34nx76) 變更類型，並為您的 AMS 帳戶請求 Snowball Edge 的服務角色。
2. 透過提交管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 來請求使用者存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_snowball_export_role`、`customer_snowball_console_role`和 `customer_snowball_import_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS Snowball Edge 在我的 AMS 帳戶中使用 有哪些限制？

的完整功能 AWS Snowball Edge 可在您的 AMS 帳戶中使用。

問：AWS Snowball Edge 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

您必須擁有上述的服務角色帳戶。

使用 AMS SSP AWS Step Functions 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Step Functions 的功能。AWS Step Functions 是一種 Web 服務，可讓您使用視覺化工作流程來協調分散式應用程式和微服務的元件。您可以從個別元件建立應用程式，這些元件會各自執行不同的功能或任務，讓您快速擴展及變更應用程式。Step Functions 提供可靠的方法來協調元件，並逐步完成應用程式的函數。Step Functions 提供圖形主控台，將應用程式的元件視覺化為一系列步驟。它會自動觸發和追蹤每個步驟，並在發生錯誤時重試，因此您的應用程式每次都會按順序和預期執行。Step Functions 會記錄每個步驟的狀態，因此當發生問題時，您可以快速診斷和偵錯問題。如需詳細資訊，請參閱 [AWS Step Functions](#)。

AWS Managed Services 常見問答集中的步驟函數

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Step Functions 的？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Step Functions 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_step_functions_role`。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：AWS Step Functions 在我的 AMS 帳戶中使用 有哪些限制？

的完整功能 AWS Step Functions 可在您的 AMS 帳戶中使用。

問：AWS Step Functions 在我的 AMS 帳戶中使用的先決條件或相依性是什麼？

在執行時間，Step Functions 使用的角色必須能夠存取步驟函數使用的服務。例如，步驟函數可以依賴 Lambda 函數。撰寫步驟函數的人可能同時建立 Lambda 函數，也需要請求存取該服務。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS Systems Manager 參數存放區

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Systems Manager 參數存放區功能。AWS Systems Manager 參數存放區為組態資料管理和秘密管理提供安全的階層式儲存。您可以存放密碼、資料庫字串和授權碼之類的資料做為參數值。您存放的值可以是純文字或加密資料。然後您可以使用建立參數時指定的唯一名稱來參考它的值。參數存放區具有高度可擴展性、可用性和耐用性，由 AWS 雲端提供支援。若要進一步了解，請參閱[AWS Systems Manager 參數存放區](#)。

Note

如果您想要具有生命週期管理的專用秘密存放區，請使用 [使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建](#) 而非 參數存放區。Secrets Manager 可讓您自動輪換秘密，協助您滿足安全和合規要求。Secrets Manager 為 Amazon RDS 上的 MySQL、PostgreSQL 和 Amazon Aurora 提供內建整合，可透過自訂 Lambda 函數擴充到其他類型的秘密。

AWS Systems Manager AWS Managed Services 常見問答集中的參數存放區

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Systems Manager 參數存放區？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC 來請求存取 AWS Systems Manager 參數存放區。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_systemsmanager_parameterstore_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 參數存放區有哪些限制？

您必須使用 AWS 受管金鑰；存取會受到限制，無法建立自訂 KMS 金鑰。不過，如果需要自訂金鑰，請提交 RFC 以使用此 IAM 角色建立客戶受管金鑰 (CMK) | 進階堆疊元件 | KMS 金鑰 | 建立變更類型 (ct-1d84keiri1jhg)，customer_systemsmanager_parameterstore_console_role 做為

IAMPrincipalsRequiringDecryptPermissions和

IAMPrincipalsRequiringEncryptPermissionsPrincipal 參數的值。建立 KMS 金鑰之後，您可以使用它建立安全字串。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 參數存放區的先決條件或相依性為何？

沒有先決條件；不過，SSM 參數存放區依賴 KMS 來建立安全字串，因此您可以加密和解密儲存在參數存放區中的值。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS Systems Manager 自動化

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Systems Manager 自動化功能。AWS Systems Manager 自動化使用 Runbook、動作和服務配額，簡化 Amazon Elastic Compute Cloud 執行個體和其他 AWS 資源的常見維護和部署任務。它可讓您大規模建置、執行和監控自動化。Systems Manager Automation 是一種 Systems Manager 文件，可定義 Systems Manager 在受管執行個體上執行的動作。您用來執行常見維護和部署任務的 Runbook，例如在受管執行個體中執行命令或自動化指令碼。Systems Manager 包含可協助您使用 Amazon Elastic Compute Cloud 標籤以大型執行個體群組為目標的功能，以及協助您根據定義限制推展變更的速度控制。Runbook 是使用 JavaScript 物件標記法 (JSON) 或 YAML 撰寫。使用 Systems Manager Automation 主控台內的 Document Builder (文件建置器)，不過，您可以建立 Runbook，而無需以原生 JSON 或 YAML 撰寫。或者，您可以使用 Systems Manager 提供的 Runbook 搭配符合您需求的預先定義步驟。若要進一步了解，請參閱 AWS Systems Manager 文件中的[使用 Runbook](#)。

Note

雖然 Systems Manager Automation 支援 20 種可在 Runbook 中使用的動作類型，但是在編寫要在 AMS Advanced 帳戶中使用的 Runbook 時，您可以使用有限數量的動作。同樣地，Systems Manager 提供的 Runbook 數量有限，可以直接使用，也可以從您自己的 Runbook 中使用。如需詳細資訊，請參閱下列常見問答集中的限制。

AWS Systems Manager AWS Managed Services 中的自動化常見問答集

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 Systems Manager Automation？

透過使用 [管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 \(ct-1w8z66n899dct\)](#) 提交 RFC 來請求存取 AWS Systems Manager 自動化。此 RFC 會將下列 IAM 角色佈建至您的帳戶。

戶：customer_systemsmanager_automation_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 自動化有哪些限制？

您必須使用有限的一組 Systems Manager 支援動作來撰寫 Runbook，才能在受管執行個體內執行命令和/或指令碼。您可以搭配任何限制使用的動作概述如下。

AWS Systems Manager 自動化限制

動作	描述	限制
aws : assertAwsResourceProperty –	宣告 AWS 資源狀態或事件狀態	僅限 EC2 執行個體
aws : aws : branch –	執行條件式自動化步驟	無限制
aws : createTags –	建立 AWS 資源的標籤	僅適用於您撰寫的 SSM 自動化 Runbook
aws : executeAutomation –	執行另一個自動化	只有您撰寫的自動化 Runbook
aws : executeScript –	執行指令碼	僅限不對任何服務進行任何 API 呼叫的指令碼
aws : 暫停 –	暫停自動化	無限制
aws : runCommand –	在受管執行個體上執行命令	僅使用 System Manager 提供的文件 - AWS-RunShellScript 和 AWS-RunPowerShellScript
aws : sleep –	延遲自動化	無限制
aws : waitForAwsResourceProperty –	等待 AWS 資源屬性	僅限 EC2 執行個體

您也可以選擇使用 Systems Manager 提供的 Runbook AWS-RunShellScript 和 AWS-RunPowerShellScript，從 Systems Manager 主控台使用「執行命令」功能直接執行命令或指令碼。您也可以將這些 Runbook 巢狀化為 Runbook，以因應額外的驗證前和/或驗證後或任何複雜的自動化邏輯。

該角色遵循最低權限原則，並且只提供在受管執行個體中撰寫、執行和擷取 Runbook 執行命令和/或指令碼所需的許可。它不會為 AWS Systems Manager 服務提供的任何其他功能提供許可。雖然此功能可讓您撰寫自動化 Runbook，但執行 Runbook 無法以 AMS 擁有的資源為目標。

問：在我的 AMS 帳戶中使用 AWS Systems Manager 自動化的先決條件或相依性是什麼？

沒有先決條件；不過，您必須確保在撰寫 Runbook 時遵循內部程序和/或合規控制。我們也建議在針對生產資源執行 Runbook 之前，先徹底測試 Runbook。

問：Systems Manager 政策是否可以 `customer_systemsmanager_automation_policy` 連接到其他 IAM 角色？

否，與其他已啟用自行佈建的服務不同，此政策只能指派給佈建的預設角色 `customer_systemsmanager_automation_console_role`。

與其他 SSPS 角色的政策不同，此 SSM SSPS 政策無法與其他自訂 IAM 角色共用，因為此 AMS 服務僅適用於在受管執行個體內執行命令或自動化指令碼。如果這些許可被允許連接到其他自訂 IAM 角色，可能具有其他服務的許可，則允許的動作範圍可以擴展到受管服務，並可能降低您帳戶的安全狀態。

若要根據我們的 AMS 技術標準評估任何變更請求 (RFCs)，請使用各自的 Cloud Architect 或服務交付管理員，請參閱 [RFC 安全性審查](#)。

Note

AWS Systems Manager 可讓您使用與帳戶共用的 Runbook。我們建議您在使用共用 Runbook 時小心謹慎，並執行盡職調查檢查，並確保在執行 Runbook 之前檢閱內容以了解其執行的命令/指令碼。如需詳細資訊，請參閱 [共用 SSM 文件的最佳實務](#)。

使用 AMS SSP AWS Transfer Family 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接存取 AMS 受管帳戶中的 AWS Transfer Family (Transfer 系列) 功能。AWS Transfer Family 是一種全受管 AWS 服務，可讓您透過安全檔案傳輸通訊協定 (SFTP) 傳輸檔案，進出 Amazon Simple Storage Service (Amazon S3) 儲存體。SFTP 也稱為 Secure Shell (SSH) 檔案傳輸通訊協定。SFTP 已應用在不同業界間的資料交換工作流程，例如金融服務、健保、廣告、零售等。

透過 AWS SFTP，您可以在中存取 SFTP 伺服器，AWS 而不需要執行任何伺服器基礎設施。您可以使用此服務將以 SFTP 為基礎的工作流程遷移至，AWS 同時維持最終使用者的用戶端和組態。您

必須先將主機名稱與 SFTP 伺服器端點建立關聯，然後新增您的使用者，並以適當的存取層級佈建他們。完成後，使用者的傳輸請求會直接從 AWS SFTP 伺服器端點服務。若要進一步了解，請參閱[AWS Transfer for SFTP](#)，也請參閱[建立啟用 SFTP 的伺服器](#)。

AWS Transfer for SFTP 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Transfer for SFTP 的？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Transfer for SFTP 來請求存取。透過此 RFC，會在您的帳戶中佈建下列 IAM 角色和政策：

- `customer_transfer_author_role`。此角色旨在讓您透過主控台管理 SFTP 服務。
- `customer_transfer_sftp_server_logging_role`。此角色旨在連接到 SFTP 伺服器。它允許 SFTP 伺服器將日誌提取到 CloudWatch。
- `customer_transfer_sftp_user_role`。此角色旨在連接到 SFTP 使用者。它允許 SFTP 使用者與 S3 儲存貯體互動。
- `policy_customer_transfer_scope_down_policy`。此政策是縮小範圍的政策，可套用至 SFTP 使用者，以將 S3 儲存貯體的存取權限制在其主資料夾。
- `customer_transfer_sftp_efs_user_role`。此角色旨在連接到 SFTP 使用者。它允許 SFTP 使用者與 EFS 檔案系統互動。

在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS Transfer for SFTP 在我的 AMS 帳戶中使用 有哪些限制？

AWS SFTP 組態的傳輸僅限於沒有「AMS-」或「MC-」字首的資源，以防止對 AMS 基礎設施進行任何修改。

問：AWS Transfer for SFTP 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

- 在建立 AWS Transfer for SFTP 伺服器和使用之前，您必須擁有名稱包含關鍵字「傳輸」的 Amazon S3 儲存貯體。
- 若要使用「客戶識別提供者」，您必須部署 API Gateway、Lambda 函數和使用儲存庫 (AD、Secrets Manager 等)。如需詳細資訊，請參閱[啟用 AWS Transfer for SFTP 使用 和使用身分提供者的密碼身分驗證 AWS Secrets Manager](#)。<https://docs.aws.amazon.com/transfer/latest/userguide/authenticating-users.html>

使用 AMS SSP AWS Transit Gateway 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Transit Gateway 的功能。AWS Transit Gateway 是一種服務，可讓您將 Amazon Virtual Private Cloud (VPCs) 和內部部署網路連線至單一閘道。隨著執行中的工作負載數量增加 AWS，您需要能夠跨多個帳戶和 Amazon VPCs 擴展網路，以跟上成長速度。今天，您可以使用對等互連來連接對 Amazon VPCs。不過，在沒有集中管理連線政策的能力的情況下，管理多個 Amazon VPC point-to-point 連線，可能成本高昂且繁瑣。若要進行內部部署連線，您需要將 AWS VPN 連接到每個個別的 Amazon VPC。此解決方案在 VPCs 增加到數百個時，建置和難以管理可能會很耗時。如需詳細資訊，請參閱 [AWS Transit Gateway](#)。

AWS Transit Gateway 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Transit Gateway 的？

透過使用 管理 | AWS 服務 | 自助佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS Transit Gateway 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_tgw_console_role。在帳戶中佈建後，您必須在聯合解決方案中加入角色。

問：AWS Transit Gateway 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Transit Gateway 可在您的 AMS 單一帳戶登陸區域帳戶中使用，但 Transit Gateway 路由的路由表修改除外。透過提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76) 來請求路由表變更。

Note

此服務僅支援單一帳戶登陸區域 (SALZ)，不支援多帳戶登陸區域 (MALZ)。

問：AWS Transit Gateway 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Transit Gateway 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP 在您的 AMS 帳戶中佈建 AWS WAF Web 應用程式防火牆

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS WAF 的功能。AWS WAF 是一種 Web 應用程式防火牆 (AWS WAF)，可協助保護您的 Web 應用程式免受可能影響應用程式可用性、危及安全性或消耗過多資源的常見 Web 入侵。透過定義可自訂的 Web 安全規則，AWS WAF 您可以控

制 Web 應用程式要允許或封鎖哪些流量。您可以使用 AWS WAF 建立自訂規則來封鎖常見的攻擊模式，例如 SQL Injection 或跨網站指令碼；以及專為您的特定應用程式設計的規則。

若要進一步了解，請參閱 [AWS WAF - Web Application Firewall](#)。

AMS 不支援監控 (CloudWatch 警示/事件/MS 警示) AWS WAF。由於的性質 AWS WAF，您必須為您的應用程式建立自訂規則；AMS 無法在沒有應用程式內容的情況下為您量化和建立警示。若要進一步了解，請參閱 [AWS WAF - Web Application Firewall](#)。

AWS WAF 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何 AWS WAF 請求在我的 AMS 帳戶中設定？

透過使用 管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 (ct-1w8z66n899dct) 提交 RFC AWS WAF 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：customer_waf_role。在您的帳戶中佈建 AWS WAF IAM 角色之後，您必須在聯合解決方案中加入該角色。

問：使用 有哪些限制 AWS WAF？

佈建許可後，您即可擁有的完整功能 AWS WAF。

問：要使用哪些先決條件或相依性 AWS WAF？

AWS WAF 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS Well-Architected Tool 在您的 AMS 帳戶中佈建

使用 AMS 自助式佈建 (SSP) 模式直接存取 AMS 受管帳戶中 AWS Well-Architected Tool 的功能。AWS Well-Architected Tool 可協助您檢閱工作負載的狀態，並將其與最新的 AWS 架構最佳實務進行比較。此工具以 [AWS Well-Architected Framework](#) 為基礎，旨在協助雲端架構師建置安全、高效能、彈性且高效率的應用程式基礎設施。此架構為您提供評估架構的一致方法，已在解決方案架構團隊執行 AWS 的數萬個工作負載檢閱中使用，並提供指引，以協助實作可隨時間擴展應用程式需求的設計。如需詳細資訊，請參閱 [AWS Well-Architected Tool](#)。

AWS WA Tool 在 AWS Managed Services 常見問答集中

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS Well-Architected Tool 的？

透過使用 [管理 | AWS 服務 | 自行佈建服務 | 新增變更類型 \(ct-1w8z66n899dct\)](#) 提交 RFC AWS Well-Architected Tool 來請求存取。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_well_architected_tool_console_admin_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

問：AWS Well-Architected Tool 在我的 AMS 帳戶中使用 有哪些限制？

完整功能 AWS Well-Architected Tool 可在您的 AMS 帳戶中使用。

問：AWS Well-Architected Tool 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS Well-Architected Tool 您的 AMS 帳戶中沒有要使用的先決條件或相依性。

使用 AMS SSP AWS X-Ray 在您的 AMS 帳戶中佈建

使用 AMS 自助式服務佈建 (SSP) 模式直接在您的 AMS 受管帳戶中存取 AWS X-Ray (X-Ray) 功能。AWS X-Ray 可協助開發人員分析和偵錯生產、分散式應用程式，例如使用微服務架構建置的應用程式。透過 X-Ray，您可以了解應用程式及其基礎服務的效能，以識別效能問題和錯誤的根本原因並進行故障診斷。X-Ray 會在請求通過您的應用程式時提供請求的 end-to-end 檢視，並顯示應用程式基礎元件的映射。您可以使用 X-Ray 來分析開發中和生產中的應用程式，從簡單的三層應用程式到由數千種服務組成的複雜微服務應用程式。如需詳細資訊，請參閱 [AWS X-Ray](#)。

AWS Managed Services 常見問答集中的 X-Ray

常見問題和解答：

問：如何請求存取 AMS 帳戶中 AWS X-Ray 的？

透過提交 [管理 | AWS 服務 | 自助佈建服務 | 新增 \(ct-1w8z66n899dct\)](#) 變更類型來請求存取權。此 RFC 會將下列 IAM 角色佈建至您的帳戶：`customer_xray_console_role`。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。此外，您必須擁有 `customer_xray_daemon_write_instance_profile`，才能將資料從 Amazon EC2 執行個體推送至 X-Ray。當您收到時，就會建立此執行個體描述檔 `customer_xray_console_role`。

您可以向 AMS Operations 提交服務請求，將 `customer_xray_daemon_write_policy` 指派給現有的執行個體描述檔，也可以使用 AMS Operations 為您啟用 X-Ray 時建立的執行個體描述檔。

問：AWS X-Ray 在我的 AMS 帳戶中使用 有哪些限制？

除了使用 AWS KMS 金鑰 (KMS 金鑰) 加密之外，您的 AMS 帳戶中 AWS X-Ray 提供的完整功能。預設會 AWS X-Ray 加密所有追蹤資料。根據預設，X-Ray 會加密追蹤和靜態相關資料。如果您需要使

用金鑰加密靜態資料，您可以選擇受管 KMS 金鑰 AWS(aws/xray) 或 KMS 客戶受管金鑰。對於適用於 X-Ray 加密的 KMS 客戶受管金鑰，請提交管理 | 其他 | 其他 | 建立變更類型 (ct-1e1xtak34nx76)。

問：AWS X-Ray 在我的 AMS 帳戶中使用 的先決條件或相依性是什麼？

AWS X-Ray 具有對 Amazon S3、CloudWatch 和 CloudWatch Logs 的相依性，這些日誌已在 AMS 帳戶中實作。暫時性相依性會根據資料來源和功能可能互動 AWS AWS X-Ray 的其他服務（例如 Amazon Redshift、Amazon RDS、Athena）而有所不同。

使用 AMS SSP 在您的 AMS 帳戶中佈建 VM Import/Export

使用 AMS 自助式佈建 (SSP) 模式，直接在您的 AMS 受管帳戶中存取 VM Import/Export capabilities。VM Import/Export 可讓您輕鬆地將虛擬機器映像從現有環境匯入 Amazon EC2 執行個體，並將其匯出回內部部署環境。此服務可讓您利用在已建置的虛擬機器中現有的投資，將這些虛擬機器作為 ready-to-use 型執行個體帶入 Amazon EC2，以滿足 IT 安全性、組態管理和合規要求。您也可以將匯入的執行個體匯出回現場部署虛擬化基礎設施，讓您跨 IT 基礎設施部署工作負載。若要進一步了解，請參閱 [VM Import/Export](#)。

AWS Managed Services 常見問答集中的 VM Import/Export

常見問題和解答：

問：如何請求存取 AMS 帳戶中的 VM Import/Export？

透過使用 Management | AWS service | Self-visioned service | Add change type (ct-1w8z66n899dct) 提交 RFC，請求存取 VM Import/Export。此 RFC 會將下列 IAM 政策佈建至您的帳戶：customer_vmimport_policy。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。

需要額外的角色，即 VM Import/Export Service 角色，服務才能在您的帳戶中執行動作。

問：在我的 AMS 帳戶中使用 VM Import/Export 有哪些限制？

- AMS VM Import/Export 提供匯入自訂機器映像和資料磁碟區的功能。不過，已縮小 S3 的許可範圍，將動作限制為符合名稱的儲存貯體，customer-vmimport-* 以限制對帳戶內資訊的存取。
- AMS VM Import/Export 支援映像和快照匯入。不過，由於安全措施，執行個體匯入和執行個體匯出功能無法使用。
- 此外，匯出功能已停用，以降低匯出受限和敏感資料的風險。

問：在我的 AMS 帳戶中使用 VM Import/Export 的先決條件或相依性是什麼？

- 您必須提供支援的磁碟映像，才能匯入 AWS 環境。如需詳細資訊，請參閱 [VM Import/Export Requirements](#)。
- VM Import/Export 無法透過 AWS 主控台存取。您必須透過 AWS CLI AWS Tools for PowerShell 或 AWS SDKs 存取此服務。或者，您可以透過提交變更類型 `ct-117rmp64d5mvb` 來請求執行個體描述檔：部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立 EC2 執行個體描述檔。此執行個體描述檔可讓工具從執行個體執行命令。

客戶受管模式

AWS Managed Services (AMS) 客戶受管模式提供靈活且可根據您的需求進行調整的控管模型。對於 AMS 無法為您操作的服務和應用程式，這可以被視為備用選項。AMS 不會操作在此模式下建立之帳戶中託管的基礎設施。不過，您可以在此模式中利用集中式多帳戶管理。在此模式下，可以使用下列多帳戶登陸區域功能：

- 自動化帳戶部署
- 網路帳戶中透過 Transit Gateway 的連線
- AMS Config 規則程式庫
- 將日誌副本儲存在日誌帳戶中
- 將客戶受管 Guard Duty 警示彙總至安全帳戶
- Consolidated Billing (合併帳單)
- 啟用自訂服務控制政策。

例如：如果您想要在 Ubuntu Pro 上執行工作負載，而 Ubuntu Pro 不是由 AMS 管理的作業系統，您可以使用客戶受管帳戶來託管它。您也可以透過客戶受管帳戶合併工作負載，以利用透過跨 AWS 組織共用提供的預留執行個體/共享計劃的大量折扣。

Customer Managed 模式入門

AMS 客戶受管模式可透過特殊的多帳戶登陸區域應用程式帳戶使用。

如需詳細資訊，包括如何建立客戶受管應用程式帳戶，請參閱[客戶受管應用程式帳戶](#)。

AMS 和 AWS Service Catalog

AWS Managed Services (AMS) 中的 Service Catalog 可讓組織建立和管理 AWS 資訊技術 (IT) 服務的目錄，並讓 IT 管理員建立、管理已核准產品的目錄，並將其分發給帳戶中的最終使用者，然後他們可

以在個人化的服務入口網站中存取他們所需的產品。管理員可以控制哪些使用者可以存取每個產品，以強制執行組織業務政策的合規性。管理員也可以設定角色，讓最終使用者只需要 IAM 存取 Service Catalog，即可部署核准的資源。Service Catalog 可讓您的組織受益於更高的敏捷性和降低成本，因為最終使用者只能從您控制的目錄中找到並啟動他們所需的產品。

Service Catalog 為您提供 AMS 變更請求 (RFC) 程序的替代方案，以佈建和更新 AMS 受管帳戶中的資源。AMS 會針對透過 Service Catalog 佈建的所有基礎設施資源，管理大規模執行 AWS 所需的所有基礎設施操作任務，包括安全性、合規性、佈建、可用性、修補程式、監控、提醒、報告、事件回應和成本最佳化。在您的 AMS 受管帳戶中使用 Service Catalog 可為您提供一種機制，以集中管理經常部署的 IT 服務，並協助您實現一致的控管，同時允許使用者僅將他們所需的已核准 IT 服務快速部署到其受管環境中。

Service Catalog 入門

若要開始使用 AMS 中的 Service Catalog，請透過 AMS 主控台提交服務請求，以請求存取 Service Catalog。提交請求時，三個 IAM 角色將部署到您的帳戶（以及包含叫用 AMS Transform 的 CloudFormation 巨集）的 AMS 受管堆疊中，以便我們可以在系統中註冊產品，並對透過 Service Catalog 佈建的基礎設施執行操作。部署的三個 IAM 角色包括 IT 管理員以 Service Catalog 管理員身分管理產品的角色；應用程式擁有者和最終使用者設定、啟動和管理產品的角色；以及將用作啟動限制的角色，定義 Service Catalog 在啟動或更新產品時將使用的許可。

開始之前，AMS 中的 Service Catalog

Service Catalog 是否會取代現有的 AMS 變更請求 (RFC) 程序？

在啟用 Service Catalog 的帳戶中，它將充當變更管理系統，您可以在其中透過預先定義的產品目錄在 AMS 帳戶中佈建和更新 IT 服務；AMS 將提供預設產品組合/產品目錄，而且您的 IT 管理員可以建立和設定您自己的。Service Catalog 只會認可透過 Service Catalog 佈建的堆疊。同樣地，透過 Service Catalog 佈建的服務將無法透過 AMS RFC 程序進行修改，因為在 Service Catalog 之外進行修改會將堆疊偏離核准的產品組態。

我可以在 AMS 主控台中查看透過服務目錄佈建的堆疊嗎？

是。您可以在 AMS 主控台中檢視透過服務目錄佈建的所有堆疊。透過服務目錄佈建的堆疊可透過「SC-」的堆疊 ID 輕鬆識別。雖然堆疊可在 AMS 主控台中檢視，但您將無法透過 AMS RFC 程序進行更新。AMS 變更管理系統 (RFCs 的存取權僅限於存取請求、修補程式協同運作和備份 RFCs。

如果我透過 Service Catalog 佈建和/或更新堆疊，AMS 主控台中是否會有對應的 RFC？

AMS 主控台中顯示的唯一 RFC 是在最初佈建堆疊時向 AMS 註冊堆疊的 RFC。透過 Service Catalog 啟動堆疊時觸發的 AMS 驗證程序會自動提交此 RFC。所有其他佈建和變更都會直接在

Service Catalog 中追蹤，並且可以在 Service Catalog 主控台中檢視。此外，您可以使用 Service Catalog 中的佈建產品計畫功能，檢視在佈建或更新產品之前將對資源進行的變更清單。

我是否必須執行在 AMS 受管帳戶中佈建產品的特定動作？

是。在 AMS 帳戶中佈建的所有 Service Catalog 產品都必須在定義該產品的 CFN 範本中包含此行 JSON：

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

此 CloudFormation 程式碼片段會觸發在 AMS 受管帳戶中佈建資源之前所需的 AMS 驗證。您有責任將此程式碼行包含在產品定義中。如果未包含，佈建將會失敗，並顯示下列錯誤訊息：「無法建立產品。此帳戶由 AMS 管理。AMS 帳戶中的所有產品都必須在範本中具有 AMS Transform 程式碼。」

AMS 客戶在啟動時是否有任何 Service Catalog 功能無法使用和/或受限？

是，下列 SC 功能在初始啟動時不適用於 AMS 客戶：

- 透過 Service Catalog 建立帳戶
- 能夠在 AMS 受管帳戶中透過 Service Catalog 啟動所有 AWS 服務。AWS 服務可用性僅限於 AMS 支援的服務（受管和自行佈建）。如需 AMS 支援服務的詳細資訊，請參閱 AMS 服務描述。
- Service Catalog IT Service Manager (ITSM) 連接器不會與 AMS 事件報告和服務請求通訊。
- 能夠利用 Service Catalog 快速啟動和參考架構，無需修改。請記住，適用於 AMS 帳戶的 Service Catalog 產品必須包含此行 JSON 程式碼：

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

CNF 範本中的。請注意，此行不是典型 AWS CloudFormation 範本的一部分，必須明確新增。

- AMS 目前不支援佈建 Service Catalog 產品的 Terraform。
- AMS 不支援 AWS CFN 堆疊集。
- 您無法建立自訂 IAM 角色。
- 服務動作僅限於：
 - [AWS-RebootRdsInstance](#)
 - [AWS-RestartEC2Instance](#)

- [AWS-StartEC2Instance](#)
- [AWS-StartRdsInstance](#)
- [AWS-StopEC2Instance](#)
- [AWS-StopRdsInstance](#)
- [AWS-CreatelImage](#)
- [AWS-CreateRdsSnapshot](#)
- [AWS-CreateSnapshot](#)

 Note

建立服務動作時，您可以將執行角色設定為最終使用者的許可、啟動角色或您選擇的自訂 IAM 角色。選取的執行角色必須具有足夠的許可才能執行服務動作，並具有 TrustPolicy，允許 Service Catalog 擔任該角色，否則該服務動作會在執行時失敗。我們建議使用 AWSManagedServicesServiceCatalogLaunchRole，它具有正確的許可和信任政策，可用作服務動作。

使用 AMS RFC 系統所需的用途為何？

在一般可用性 (GA) 時，您仍然需要使用 RFCS 來執行下列動作：

- 設定修補程式協調器
- 設定備份政策
- 請求執行個體存取
- 建立和指派 AMS 準則以外的安全群組。
- 執行工作負載擷取 (WIGS)
- 建立 IAM 角色

我可以使用 Service Catalog CLI 來存取 AMS 受管帳戶中的 Service Catalog 嗎？

是，可透過 CLI 使用並啟用 Service Catalog APIs。可透過佈建和終止這些成品來管理 Service Catalog 成品的動作可供使用。如需詳細資訊，請參閱 [AWS Service Catalog 資源](#)，或下載最新的 AWS 開發套件或 CLI。

誰會建立、管理和分發客戶的核准產品目錄？

客戶的目錄管理員和/或 IT 管理員或指派的資源負責管理您的 Service Catalog 目錄和核准的產品。

我可以使用 AMS AMIs嗎？

2020 年 3 月之後提供的 AMS AMIs 可透過 AWS Service Catalog 部署。

如何使用 Service Catalog 遷移至 AMS？

若要使用 Service Catalog 將工作負載遷移至 AMS，請先依照[工作負載擷取](#) (WIGs) 程序在 AMS 中建立 AMI。您可以使用 WIGS 產生的 AMI 在 Service Catalog 中建立產品。如何執行此操作，請參閱 [AWS Service Catalog - 入門](#)。

尋找您需要的資料 (SKMS)、AMS

在 AMS 服務知識管理或 SKMS 系統上使用 AWS Managed Services (AMS) 帳戶呼叫時，尋找您需要的資料。AMS。

SKMS 代表服務知識管理系統，並參考所有與客戶 AWS Managed Services (AMS) 服務相關的資訊。AMS 具有用於尋找資料的 SKMS API。

主題

- [什麼是服務知識管理？](#)
- [在 AMS 中尋找 VPC IDs](#)
- [在 AMS 中尋找子網路 IDs](#)
- [尋找 AMI IDs、AMS](#)
- [尋找安全群組 \(SG\) IDs、AMS](#)
- [在 AMS 中尋找 IAM 實體](#)
- [在 AMS 中尋找堆疊 IDs](#)
- [在 AMS 中尋找執行個體 IDs 或 IP 地址](#)
- [在 AMS 中尋找 Amazon Resource Name \(ARNs\)](#)
- [在 AMS 中依 ARN 尋找資源](#)
- [尋找 AMS 帳戶設定](#)

什麼是服務知識管理？

服務知識管理是 AMS 帳戶上所有資訊的存放區。下列相關資訊可透過 AMS 服務知識管理系統 (SKMS)、AMS SKMS API 或 AMS 主控台取得：

- VPC
- 受管子網路
- 堆疊和堆疊元件，包括 Amazon EC2 執行個體和其他資源
- Amazon Machine Images (AMI)

您可以從 SKMS 使用資訊來了解受管基礎設施，並做為輸入來變更管理和服務請求，以建立、變更或移除基礎設施。

Note

所有 AMS SKMS API 呼叫都會記錄在其中 AWS CloudTrail。

透過 AMS SKMS API 存取 SKMS，該 API 提供用於探索可部署環境 (VPCs 和子網路) 和應用程式資源 (堆疊、Amazon EC2 執行個體和執行個體映像或 AMIs) 相關資訊的操作。

VPCs 和執行個體映像是在帳戶中設定，具有必要的存取許可。建立後，您可以使用變更管理系統，將工作堆疊填入 VPCs。

在 AMS 中尋找 VPC IDs

虛擬私有雲端 (VPC) 具有一或多個子網路。在 AMS 中，您的 VPC 位於中 AWS 區域，而且您擁有私有和公有子網路。

另請參閱[在 AMS 中尋找子網路 IDs](#)。

有些 CTs 需要 VpcId。若要尋找 VPC ID，您可以使用 AMS 主控台或 API/CLI。

AMS 主控台：

在導覽窗格中，選取 VPCs 和相關的 VPC。所選 VPC 的 VPC 詳細資訊頁面會開啟，其中包含 VPC ID 等資訊。

AMS SKMS API ListVpcSummaries 或 CLI：

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 us-east-1。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

1. 在下列範例中，第一個命令會請求帳戶中所有 VPCs 的摘要清單。第二個命令會請求 VPCs 清單，具有查詢篩選條件，以僅列出 2016 年建立 VPCs，並輸出 CreatedTime、VpcId 和 Name。

Note

您可以透過 AMS 主控台開發人員資源頁面取得 AMS SKMS CLI。

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               ListVPCSummaries                               |
+-----+
|                               VPCSummaries                               |
|+-----+-----+
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name       | 952444781316-initial-vpc |
|+-----+-----+
|                               Visibility                               |
|+-----+-----+
| Id          | PrivateAndPublic |
| Name       | PrivateAndPublic |
|+-----+-----+
```

2. 這次使用查詢：

```
aws amsskms list-vpc-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

```

-----
|                                     ListVPCSummaries                                     |
+-----+-----+-----+-----+
| 2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |
+-----+-----+-----+-----+

```

在 AMS 中尋找子網路 IDs

數個資源需要在組態時間指定子網路或子網路清單。若要尋找子網路，您可以使用 AMS 主控台或 AMS SKMS API/CLI。請注意，AMS SKMS API/CLI 是私有的，必須先安裝才能使用。

AMS 主控台：

1. 在導覽窗格中，選取 VPCs 和相關的 VPC。所選 VPC 的 VPC 詳細資訊頁面會開啟子網路資料表，按一下子網路 ID 以開啟詳細資訊頁面並尋找 ID。

AMS SKMS API ListSubnetSummaries 或 CLI：

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

若要尋找 VPC 的子網路，您可以使用 `list-subnet-summaries` 命令進行搜尋，如下所示。

Note

如果您要尋找不在 AMS 帳戶中的子網路，您可以嘗試 `aws ec2 describe-subnets --region us-west-2`。

1. SKMS API/CLI ListSubnetSummaries 操作：

簡單清單：

```
aws amsskms list-subnet-summaries
```

輸出至資料表：

```
aws amsskms list-subnet-summaries --output table
```

2. SKMS API ListSubnetSummaries 操作具有根據可見性縮小結果範圍的參數。此外，您可以根據名稱**篩選**結果。如果您使用的是 CLI，您也可以使用 `--query` 選項來縮小輸出或搜尋部分值。例如，若要尋找特定 VPC 的所有子網路，您可以使用此命令：

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
  output table
```

這會傳回如下內容：

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

如需使用 CLI 查詢的相關資訊，請參閱[如何使用 --query Option 篩選輸出](#)，以及查詢語言參考[JMESPath Specification](#)。

3. 如果您有多個 VPCs，請在 命令中包含 VPC 篩選條件，然後為每個 VPC 執行 命令。例如：

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. 在 AWS 中，使用 [describe-subnets](#)。

如需使用 CLI 查詢的相關資訊，請參閱[如何使用 --query Option 篩選輸出](#)，以及查詢語言參考[JMESPath Specification](#)。

子網路名稱

從您收集輸入並新增至系統之後，系統會自動建立您的 AMS 子網路。AMS 使用公式來建立子網路名稱：***ACCOUNT_ID-SUBNET-TYPE-AZ-IDENTIFIER***。子網路類型為 dmz、shared-services 或 customer-application。如果您有多個客戶應用程式子網路，在帳戶 ID 之後，可能會將選用的識別符新增至子網路名稱，以指出子網路是「額外」或「預留」子網路。

尋找 AMI IDs、AMS

Amazon Machine Image 或 AMI 是從 Amazon EC2 執行個體建立的 Amazon EC2 執行個體範本。每個月 AWS 都會提供更新的 AMIs（例如，使用修補程式）；不過，AWS Managed Services (AMS) 需要 AMIs。AMS 會發行新的 AMIs，您可以在每月修補程式週二之後不久使用。

Amazon Machine Image (AMIs) 是用來在 AWS 中建立 EC2 執行個體的執行個體組態範本。AMS 要求將特定 AMIs 用於 AMS 受管資源。建立 EC2 執行個體和 EC2 Auto Scaling 群組的變更類型需要您為 AMS 指定 AMI，以用作變更類型建立之執行個體的基礎。AMS 建議您一律選取可用的最新 AMI。

若要進一步了解 AWS AMIs，請參閱 [AWS AMI 設計](#)。

為您的 AMS 帳戶建立 Amazon EC2 堆疊或 Amazon EC2 Auto Scaling 群組時，您必須依 Amild 指定 AMI。您僅限於以「customer-」開頭 AMIs，我們建議您一律選擇最新的 AMI。

若要尋找您帳戶的最新 AMI，您可以使用 AMS SKMS CLI 命令進行搜尋，或使用 AMS 主控台詳細資訊頁面以取得相關 VPC：

- 使用 AMS 主控台：可用的 AMIs 會列在 AMS 主控台的 AMI 頁面上。從名稱開頭為「customer-」的 AMIs 中選取。
- 使用 AMS SKMS API/CLI ListAmis 操作。

 Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

以下是 CLI 範例，其中包含將結果限制為客戶 AMIs 的選項：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

此範例使用 `filter` 選項搭配 `query` 選項來尋找開頭為「客戶」AMIs：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- 如需使用 CLI 查詢的相關資訊，請參閱[如何使用 --query Option 篩選輸出](#)，以及查詢語言參考[JMESPath Specification](#)。

尋找安全群組 (SG) IDs、AMS

Amazon EC2 建立和 OpenSearch 建立網域 CTs 需要安全群組 ID。這將採用格式 `sg-02ce123456e7893c7`。您的帳戶至少有兩個預設安全群組；請參閱[安全群組](#)。此外，您可能還有針對特定用途建立的安全群組。若要探索您的安全群組：

- AWS 主控台：使用 EC2 或 VPC 主控台檢視所選 VPC 的所有安全群組。
- API/CLI（登入您的 AMS 帳戶時）：

列出您的安全群組：

```
aws ec2 describe-security-groups
```

在 AMS 中尋找 IAM 實體

您的帳戶具有預設 IAM 角色和政策；請參閱 [AMS 中的 IAM 使用者角色](#) 和預設 IAM 執行個體描述檔；請參閱 [EC2 IAM 執行個體描述檔](#) 搭配預設政策。若要探索您的 IAM 角色和政策：

- 主控台：使用 IAM 主控台檢視您帳戶的所有 IAM 政策和角色。
- API/CLI（登入您的 AMS 帳戶時）：

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

列出您的角色：

```
aws --profile saml iam list-roles
```

列出您的政策：

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

在 AMS 中尋找堆疊 IDs

若要尋找堆疊 ID，您可以使用 Amazon EC2 主控台、AMS 主控台或 AMS SKMS API/CLI。

AMS 主控台：

- 在導覽窗格中，選取 RFCs，然後按一下建立堆疊的 RFC。使用頂端的篩選條件選項來減少清單。RFC 詳細資訊頁面隨即開啟，並包含具有堆疊 ID 的執行輸出。
- 或者，您可以在導覽窗格中選取堆疊以開啟堆疊清單頁面，然後將堆疊清單翻頁至您感興趣的堆疊。如果您知道要尋找的堆疊主體，此方法會更實用。

Amazon EC2 主控台：

在導覽窗格中，選取執行個體或負載平衡器或 Auto Scaling 群組。

AMS SKMS API ListStackSummaries 或 CLI：

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

若要檢視目前帳戶中的堆疊清單，請執行 SKMS API 的 ListStackSummaries 操作 (CLI: `list-stack-summaries`)。若要透過 StackId 取得特定堆疊執行個體的完整資訊，請執行 GetStack。

- 在下列範例中，第一個命令會請求帳戶中所有堆疊執行個體的摘要清單。第二個命令會請求堆疊執行個體的清單，具有查詢篩選條件，以僅列出特定堆疊範本的執行個體，並輸出 VpcId、Name 和 StackId。

```
aws amsskms list-stack-summaries --output table
```

```
-----
|                               ListStackSummaries                               |
|                               StackSummaries                                |
+-----+-----+-----+-----+
| VpcId   | StackId   | StackTemplateId | Name   |
+-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
```

```
|vpc-0123abcd|stack-8323cc0e12345678|stm-s2b72beb123456789|S3 store|
|vpc-0123abcd|stack-2309fa0712345678|stm-sdhopvbb123456789|ELB      |
|vpc-0123abcd|stack-5e61a70512345678|stm-sdpabqbb123456789|PatchSim|
|vpc-0123abcd|stack-bd0e080d12345678|stm-s2b72beb123456789|CLI demo|
+-----+-----+-----+-----+-----+
```

如需使用 CLI 查詢的相關資訊，請參閱[如何使用 --query Option 篩選輸出](#)，以及查詢語言參考[JMESPath Specification](#)。

Note

如需使用執行個體 IDs 進行存取的資訊，另請參閱[使用堡壘存取執行個體](#)。

在 AMS 中尋找執行個體 IDs 或 IP 地址

- 若要請求存取執行個體、登入執行個體或建立 AMI，您必須擁有執行個體 ID。對於 EC2 執行個體（獨立執行個體或堆疊的一部分）或資料庫執行個體，您可以透過幾種不同的方式找到 ID：
 - ASG 堆疊中執行個體的 AMS 主控台：查看建立堆疊之 RFC 的 RFC 詳細資訊頁面。在執行輸出區段中，您會找到 ASG 堆疊的堆疊 ID，然後您可以前往 EC2 Console Auto Scaling Groups 頁面，搜尋該堆疊 ID 並尋找其執行個體。當您找到執行個體時，請選取它，並在頁面底部開啟包含詳細資訊的區域，包括 IP 地址。
 - 獨立 EC2 或資料庫（資料庫）執行個體的 AMS 主控台：查看建立 EC2 堆疊或資料庫執行個體之 RFC 的 RFC 詳細資訊頁面。在執行輸出區段中，您會找到執行個體 ID 和 IP 地址。
 - AWS EC2 主控台：
 - 在導覽窗格中，選取 Instances (執行個體)。執行個體頁面隨即開啟。
 - 按一下您想要 ID 的執行個體。執行個體詳細資訊頁面隨即開啟，並顯示 ID 和 IP 地址。
 - AWS 資料庫主控台：
 - 在首頁上，選取資料庫執行個體。執行個體頁面隨即開啟。
 - 篩選您要為其 ID 的資料庫執行個體。執行個體詳細資訊頁面隨即開啟，並顯示 ID。
 - AMS CLI/API。

Note

必須安裝 AMS CLI，這些命令才能運作。若要安裝 AMS API 或 CLI，請前往 AMS 主控台開發人員資源頁面。如需 AMS CM API 或 AMS SKMS API 的參考資料，請參閱《使用者指南》中的 AMS 資訊資源一節。您可能需要新增身分驗證 `--profile` 選項，例如 `aws amsskms ams-cli-command --profile SAML`。您可能還需要新增 `--region` 選項，因為所有 AMS 命令都用盡 `us-east-1`；例如 `aws amscm ams-cli-command --region=us-east-1`。

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 `us-east-1`。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

執行下列命令以取得堆疊執行輸出詳細資訊：

```
aws amsskms get-stack --stack-id STACK_ID
```

輸出看起來像這樣，`InstanceId` 出現在底部下方 `Outputs`（顯示的值為範例）：

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
    ],
  },
}
```

```
{
  {
    "Value": "subnet-01234567890abcdef",
    "Key": "InstanceSubnetId"
  },
  {
    "Value": "t2.large",
    "Key": "InstanceType"
  },
  {
    "Value": "ami-01234567890abcdef",
    "Key": "InstanceAmiId"
  }
],
"Tags": [],
"Outputs": [
  {
    "Value": "i-0b22a22eec53b9321",
    "Key": "InstanceId"
  },
  {
    "Value": "10.0.5.000",
    "Key": "InstancePrivateIP"
  }
],
"StackTemplateId": "stm-s6xvs0000000000000",
"CreatedTime": "1486584508416",
"Name": "Amazon"
}
```

在 AMS 中尋找 Amazon Resource Name (ARNs)

Amazon Resource Name (ARN) 是可唯一識別 AWS 資源的字串，例如 EC2 執行個體、S3 儲存貯體、帳戶、Lambda 函數等。當您想要在所有 IAM 政策、Amazon Relational Database Service (Amazon RDS) 標籤和 API 呼叫中明確指定資源時 AWS，AWS 需要 ARN。ARNs 是從指定服務、區域、帳戶和其他資訊的識別符建構而成。有三種 ARN 格式：

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

ARN 的確切格式取決於服務和資源類型。若要進一步了解 ARNs，請參閱 [Amazon Resource Name \(ARNs\) AWS 和服務命名空間](#) 和 [ARN 格式](#)。

如需依資源的 ARN 格式範例，請參閱 AWS 服務授權參考[資源類型表格](#)。

尋找 AWS 物件的 ARN 可能很困難。以下是三種嘗試方法：

- AWS 服務主控台：前往相關的 AWS 服務主控台、尋找資源，並在資源的詳細資訊中尋找 ARN。
- AWS API/CLI（您必須先安裝 AWS CLI）：在 [AWS CLI 命令參考](#) 中尋找相關服務，然後視 AWS 服務而定，尋找相關操作，例如 describe、get 或等。例如，對於所有 IAM 角色、政策和使用者，您可以從 CLI 的輸出中取得 ARN：

```
aws iam get-role --role-name EMR_DefaultRole
```

- 根據相關格式建構 ARN：尋找資源的 ARN 格式、查看 [AWS 服務的動作、資源和條件索引鍵](#) 頁面、尋找相關服務，然後尋找相關動作，然後向下切入資源 ARN 格式。取得格式後，請將變數取代為相關設定。

您可以遵循適當的格式（每個服務和資源類型的格式變更）並填入資訊，自行建構 ARN。以下是一些 ARN 範例：

- AWS 帳戶 ARN 具有下列語法：

```
arn:aws:iam::ACCOUNT-ID:root
```

- S3 ARN 具有儲存貯體和相關聯物件的平面階層：

```
arn:aws:s3:::ams-bucket
```

- EC2 ARN 具有子資源類型，例如映像、安全群組、執行個體等。此範例包含結尾的執行個體 ID：

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Lambda ARN 具有資源 ID 部分的函數名稱，您可能需要在結尾包含版本編號，如本範例所示：

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```


AWS Key Management Service 服務提供此資訊：[尋找金鑰 ID 和金鑰 ARN](#)。

若要尋找 DynamoDB 資料表的 ARN，請使用 DynamoDB [describe-table](#) CLI。

如需外部人員查看 AWS ARNs請參閱 [AWS ARN 說明：Amazon Resource Name Guide](#)。

在 AMS 中依 ARN 尋找資源

Amazon Resource Name (ARNs)可唯一識別 AWS 資源。若要了解 ARNs 和 ARN 格式，請參閱 [Amazon Resource Name \(ARNs\) AWS 和服務命名空間](#)和 [ARN 格式](#)。

Note

若要從資源 ARN 取得資源的詳細資訊，您必須能夠存取建立資源的帳戶。

中沒有從資源 ARN AWS 查詢所有資源詳細資訊的直接路徑，因為 服務具有多種具有各種相關資訊的資源類型。如果您有資源的 ARN，您可以判斷：

- 相關 AWS 服務（第三個 ARN 區段）會告訴您要查看哪些 AWS 主控台來尋找資源
- 資源 ID（第六個或第七個 ARN 區段）會確認您找到正確的資源

或者，您可以在 AWS CLI 命令[AWS 參考中尋找該服務可用的 CLI 命令](#)，以取得有關取得資源詳細資訊的資訊。

例如，從下列 ARN，您可以判斷服務是 lambda，帳戶是 123456789012，資源類型是 function，而函數的名稱是 TestFunction。

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

您可以從中檢閱 [AWS Lambda 服務的 CLI 文件](#)，了解如何使用各種命令擷取更多詳細資訊，例如 get-function和 get-function-configuration。

例如，如果您有 Lambda 函數的名稱或 ARN，您可以使用下列命令來取得其詳細資訊：

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

尋找 AMS 帳戶設定

帳戶設定，用於建立 AMS RFCs、設定排程，以及判斷誰會收到通知。

某些設定會在加入期間建立，並要求變更服務請求。您應該記下這些帳戶的詳細資訊，因為您將在與 AMS 通訊時使用它們：

- 登入資料：如果您需要擷取 AMS 使用者名稱或密碼，請聯絡本機 IT 管理員--AMS 使用您的公司 Active Directory。
- Cloud Service Delivery Manager (CSDM)：此人員是您與 AMS 的聯絡人，可用於回答服務問題。您在加入時會收到此人員的聯絡資訊，而且應該讓組織中與 AMS 互動的所有人員都能使用。您可以預期從此人員收到有關 AMS 服務的每月報告。
- 主控台存取：您可以在專門為您的帳戶設定的 URL 中存取 AMS 主控台。您可以從 CSDM 取得 URL。
- AMS CLI：您可以透過 AMS 主控台開發人員的資源頁面或您從 CSDM 取得的可分發套件來取得 AMS CLI。在您擁有可分發套件之後，請遵循[安裝或升級 AMS CLI](#)中概述的步驟。
- 維護時段：維護時段會決定 EC2 執行個體何時進行修補。AWS Managed Services 維護時段（或維護時段）會執行 AWS Managed Services (AMS) 的維護活動，並在每個月的第二個星期四太平洋時間下午 3 點至下午 4 點重複執行。AMS 可能會變更維護時段，但需提前 48 小時通知。您可能已在加入時選擇不同的時段 -- 保留所選維護時段的記錄。
- 監控：AMS 預設提供一組 CloudWatch 指標，但您也可以請求其他指標。如果您這樣做，請保留這些記錄。
- 日誌：根據預設，您的日誌會存放在 `ams-a-ACCOUNT_ID-log-management-REGION`，其中 **REGION** 是產生日誌的區域。
- 緩解：加入時，AMS 會記錄您選擇的緩解動作，以防發現對資源的惡意軟體攻擊。例如，聯絡特定人員。將此資訊提供給組織中與 AMS 互動的所有人員。
- 區域：您可以在 AMS 主控台中查看 VPC 詳細資訊頁面。您也可以在安裝 AMS SKMS CLI 之後執行此命令（此命令使用 SAML 設定檔，如果您的身分驗證方法不同，請移除）：

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

 Important Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 us-east-1。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

在 AMS 中尋找 FQDNs

AWS Managed Services (AMS) 存取變更類型 (CTs) 需要 AMS 信任網域的完整網域名稱或 FQDN，格式為 `C844273800838.amazonaws.com`。若要探索您的 AWS FQDN，請執行下列其中一項操作：

- AWS 主控台：查看目錄名稱欄中的 AWS Directory Service 主控台。
- CLI：登入您的網域時，請使用下列命令：

Windows (傳回使用者和 FQDN)：

```
whoami /upn
```

或 (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux：

```
hostname --fqdn
```

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 us-east-1。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

在 AMS 中尋找可用區域 AZs)

可用區域：所有帳戶至少有兩個可用區域。若要準確尋找您的可用區域名稱，您必須先知道相關聯的子網路 ID。

- AMS 主控台：在導覽窗格中按一下 VPCs，然後視需要按一下相關的 VPC。在 VPCs 詳細資訊頁面上，選取子網路資料表中的相關子網路，以使用相關聯的可用區域名稱開啟子網路詳細資訊頁面。
- AMS SKMS API/CLI：

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 us-east-1。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

在 AMS 中尋找 SNS 主題

您的 SNS 主題會決定在各種情況下收到通知的人員。AMS 提供 AMI 通知的 SNS 主題（請參閱[使用 SNS 的 AMS AMI 通知](#)）、CloudWatch 警示和 EC2 資源（請參閱[接收 AMS 產生的提醒](#)）等。若要探索現有的 SNS 主題：

- AWS 主控台：使用 SNS 主控台檢視所有主題、應用程式和訂閱，以及訊息圖表。同時建立、刪除、訂閱和發佈至主題。
- API/CLI（登入您的 AMS 帳戶時，需要 AWS CLI）：

列出您的 SNS 主題：

```
aws sns list-topics
```

列出您的 SNS 訂閱：

```
aws sns list-subscriptions
```

Note

AMS API/CLI (amscm 和 amsskms) 端點位於 AWS N. Virginia 區域 us-east-1。根據身分驗證的設定方式，以及您的帳戶和資源所在的 AWS 區域，您可能需要在發出命令 `--region us-east-1` 時新增。如果這是您的身分驗證方法 `--profile saml`，您可能還需要新增。

在 AMS 中尋找備份設定

備份和快照是由 AMS 透過原生 [AWS Backup](#) 服務管理。

組態是透過 AWS Backup 計劃管理。您可以有多個 AWS Backup 計劃，將標記的資源與備份排程和保留政策建立關聯。若要尋找您的 AMS 帳戶 AWS Backup 設定，請使用 <https://console.aws.amazon.com/backup> 主控台或 [備份](#) 命令的 AWS CLI 命令參考。

如需 AMS 和 的詳細資訊 AWS Backup，請參閱 [持續性管理](#)。

AMS 中的存取管理

了解如何使用 SSH 或遠端桌面通訊協定 (RDP) 存取資源，以及如何使用堡壘。

AWS Managed Services (AMS) 存取管理系統是在加入期間設定。只有透過 AMS 聯合的 AMS IAM 使用者角色使用者可以存取帳戶中的 AMS 資源。

除了接下來所述的聯合信任之外，AMS 安全群組是私有和公有應用程式存取的重要元素。如需 AMS 安全群組以及如何變更安全群組的詳細資訊，請參閱 [安全群組](#)。

主題

- [什麼是 Access Management ?](#)
- [在 AMS 中使用根使用者帳戶的方式和時間](#)
- [AMS Advanced 主控台和 Amazon EC2 存取](#)
- [存取 AWS Management 主控台和 AMS 主控台](#)
- [使用堡壘存取執行個體](#)

什麼是 Access Management ?

存取管理是 AMS 透過僅允許授權和驗證的存取來保護資源的方式。AMS 使用預設 IAM 使用者角色和執行個體描述檔，以及多重驗證、安全群組、適合 DNS 的堡壘名稱等，來保護您的資源。

AMS 著重於需要管理的三種存取類型：

- 主控台存取：利用聯合，帳戶 Active Directory 中的使用者可以使用單一登入 (SSO) 存取主控台。如果您為這些帳戶設定了多重驗證，您可以繼續要求 MFA 存取主控台。
- 使用 RDP 或 SSH 存取執行個體：利用 Active Directory 信任，帳戶現有 Active Directory 中的使用者可以請求存取執行個體，然後使用其現有的公司登入資料成功驗證堡壘和執行個體。如果您為這些帳戶設定了多重驗證，您可以繼續要求 MFA 請求存取執行個體。AMS 使用自己的 MFA 解決方案來限制 AMS 工程師存取執行個體。
- 應用程式存取：依使用案例而異。

主題

- [AMS 存取您帳戶的原因和時間](#)

AMS 存取您帳戶的原因和時間

AWS Managed Services (AMS) 會管理您的 AWS 基礎設施，有時基於特定原因，AMS 運算子和管理員會存取您的帳戶。這些存取事件會記錄在 AWS CloudTrail (CloudTrail) 日誌中。

下列主題說明 AMS 為何、何時以及如何存取您的帳戶。

AMS 客戶帳戶存取觸發條件

AMS 客戶帳戶存取活動由觸發程序驅動。今天的觸發條件是在問題管理系統中建立的 AWS 票證，以回應 Amazon CloudWatch (CloudWatch) 警示和事件，以及您提交的事件報告或服務請求。每個存取可能會執行多個服務呼叫和主機層級活動。

下表列出存取理由、觸發條件和觸發條件的啟動者。

存取觸發程序

存取	啟動者	觸發條件
修補	AMS	修補程式問題
基礎設施部署	AMS	部署問題
內部問題調查	AMS	問題（已識別為系統性的問題）
警示調查和修復	AMS	AWS Systems Manager 操作工作項目 (SSM OpsItems)
手動 RFC 執行	您	變更請求 (RFC) 問題。（非自動化 RFCs 可能需要 AMS 存取您的資源）
事件調查和修復	您	傳入支援案例（您提交的事件或服務請求）
傳入服務請求履行	您	

AMS 客戶帳戶存取 IAM 角色

觸發時，AMS 會使用 AWS Identity and Access Management (IAM) 角色存取客戶帳戶。就像您帳戶中的所有活動一樣，角色及其用量都會記錄在 CloudTrail 中。

⚠ Important

請勿修改或刪除這些角色。

AMS 存取客戶帳戶的 IAM 角色

角色名稱	帳戶類型 (SALZ、MALZ 管理、MALZ 應 用程式等)	描述
ams-service-admin	SALZ、MALZ	AMS Service 自動化存取和自動化基礎設施部署，例如修補程式、備份、自動化修復。
ams-application-infra-read-only	SALZ、MALZ 應 用程式、MALZ 工具應用程式	運算子唯讀存取
ams-application-infra-operations		事件/服務請求的運算子存取權
ams-application-infra-admin		AD 管理員存取權
ams-primary-read-only	MALZ 管理	運算子唯讀存取
ams-primary-operations		事件/服務請求的運算子存取權
ams-primary-admin		AD 管理員存取權
ams-logging-read-only	MALZ 記錄	運算子唯讀存取
ams-logging-operations		事件/服務請求的運算子存取權
ams-logging-admin		AD 管理員存取權
ams-networking-read-only	MALZ 網路	運算子唯讀存取
ams-networking-operations		事件/服務請求的運算子存取權
ams-networking-admin		AD 管理員存取權

角色名稱	帳戶類型 (SALZ、MALZ 管理、MALZ 應 用程式等)	描述
ams-shared-services-read-only	MALZ 共用服務	運算子唯讀存取
ams-shared-services-operations		事件/服務請求的運算子存取權
ams-shared-services-admin		AD 管理員存取權
ams-security-read-only	MALZ 安全性	運算子唯讀存取
ams-security-operations		事件/服務請求的運算子存取權
ams-security-admin		AD 管理員存取權
ams-access-security-analyst	SALZ、MALZ 應 用程式、MALZ Tools-App lication、MALZ Core	AMS 安全存取
ams-access-security-analyst-read-only		AMS 安全，唯讀存取
Sentinel_AdminUser_Role_PXHazRQadu0PVcCDcMbHE	SALZ	【BreakGlassRole】 用於將 breakGlass客戶帳戶
Sentinel_PowerUser_Role_wZuPuS0ROOI0IazDbRI9	SALZ、MALZ	Poweruser 存取客戶帳戶以進行 RFC 執行
Sentinel_ReadOnlyUser_Role_Pd4L6Rw9RD0InLkD5JOo		ReadOnly 存取客戶帳戶以進行 RFC 執行
ams_admin_role		客戶帳戶 RFC 執行的管理員存取權

角色名稱	帳戶類型 (SALZ、MALZ 管理、MALZ 應 用程式等)	描述
AWSManagedServices_Provisioning_CustomerStacksRole		用於透過 CloudFormation Ingest 代表客戶啟動和更新 CFN 堆疊
customer_ssm_automation_role		CT 執行傳遞給 SSM Automation 以執行 Runbook 的角色
ams_ssm_automation_role	SALZ、MALZ 應用程式、MALZ Core	AMS 服務傳遞給 SSM Automation 以執行 Runbook 的角色
ams_ssm_iam_deployment_role	MALZ 應用程式	IAM 目錄使用的角色
ams_ssm_shared_services_intermediary_role	MALZ 共用服務	應用程式 ams_ssm_automation_role 用來在共用服務帳戶中執行特定 SSM 文件的角色
AmsOpsCenterRole	SALZ、MALZ	用來在客戶帳戶中建立和更新 OpsItems
AMSOpsItemAutoExecutionRole		用來取得 SSM 文件、描述資源標籤、更新 OpsItems，以及啟動自動化
customer-mc-ec2-instance-profile		預設客戶 EC2 執行個體描述檔 (角色)

請求執行個體存取

若要存取資源，您必須先提交該存取的變更請求 (RFC)。您可以請求兩種類型的存取：admin（讀取/寫入許可）和唯讀（標準使用者存取）。根據預設，存取會持續八小時。此為必要資訊：

- 您要存取之執行個體或執行個體的堆疊 ID 或一組堆疊 IDs。
- AMS 信任網域的完整網域名稱。
- 想要存取的人員的 Active Directory 使用者名稱。

- 您要存取之堆疊所在的 VPC ID。

獲得存取權後，您可以視需要更新請求。

如需如何請求存取的範例，請參閱[堆疊管理員存取 | 授予](#)或[堆疊唯讀存取 | 授予](#)。

在 AMS 中使用根使用者帳戶的方式和時間

[根使用者](#)是您帳戶中的超級使用者 AWS。AMS 會監控根用量。我們建議您僅將根用於需要它的一些任務，例如：變更您的帳戶設定、啟用 AWS Identity and Access Management (IAM) 對帳單和成本管理的存取、變更根密碼，以及啟用多重要素驗證 (MFA)。請參閱 AWS Identity and Access Management 《使用者指南》中的[需要根使用者憑證](#)的任務。

Note

MFA 會在 AMS 進階加入期間啟用，以特別不允許根使用者存取。AMS 受管帳戶中的根存取權與其他 AWS 帳戶不同，對於整個 AMS 受管環境的安全性至關重要。設定的 MFA 是虛擬 MFA，並使用 AMS 擁有的裝置執行。在 AMS 的協助下設定虛擬 MFA 之後，虛擬字符會立即刪除。這可確保您和 AMS 都無法以根使用者身分登入帳戶。根登入只能在特殊請求上重新啟用（接下來說明），且 AMS 預期只有在絕對必要時才能使用此類存取。如需有關 MFA 的資訊，請參閱[使用多重要素驗證保護新帳戶](#)。

根存取一律會觸發 AMS Security and Operations 團隊回應。AMS 會監控 API 呼叫的根存取，並在偵測到此類存取時觸發警示。

AMS 帳戶類型之間的請求根存取權略有不同。

使用 AMS 進階單一帳戶登陸區域的根存取權：

如果您有單一帳戶登陸區域，請聯絡您的雲端服務交付管理員 (CSDM) 和雲端架構師 (CAs)，告知他們您需要的根存取工作。最好在提議的活動之前 24 小時發出通知。

使用 AMS 進階多帳戶登陸區域的根存取權：

對於多帳戶登陸區域應用程式、共享服務、安全或聯網帳戶，請使用 Management | Other | Other (ct-1e1xtak34nx76) 變更類型。包含日期、時間和使用根使用者登入資料的目的，並排定 RFC，以確保在提議的活動前 24 小時發出通知。使用您的多帳戶登陸區域管理帳戶來提交 RFC。

此外，請提前 24 小時聯絡您的 CSDM 和 CAs，告知他們您需要的根存取工作。

根用量的 AMS 操作和安全性回應：

使用根使用者帳戶時，AMS 會收到警示。如果根登入資料使用量未排定，他們會聯絡 AMS 安全團隊和您的客戶團隊，以確認是否為預期的活動。如果不是預期的活動，AMS 會與您的安全團隊一起調查問題。

AMS Advanced 主控台和 Amazon EC2 存取

存取 AMS Advanced 主控台。

存取您的 Amazon EC2 執行個體。

提交存取請求：

登入您的 AMS Amazon EC2 執行個體：

存取 AWS Management 主控台和 AMS 主控台

在加入期間，您會收到 AWS Management 主控台的登入（權限有限：您可以寫入 AMS 主控台，以及客戶資訊頁面中的某些欄位）。您可以在 AWS 管理主控台中選取 Managed Services 連結來存取 AMS 主控台。聯合存取或共用登入資料（使用者名稱/密碼）會依照 IT 管理團隊的協議進行準備。如需進一步建立帳戶或群組，請向 AMS 提交服務請求。

如需有關存取 AWS 管理主控台的資訊，請參閱[使用 AWS 管理主控台](#)。

如需使用 AMS 主控台的一些秘訣，請參閱[使用 AMS 主控台](#)。

暫時 AMS 主控台存取

如果您尚未設定身分提供者（例如 SAML）來向 AMS 進行身分驗證，您可以暫時存取 AMS 主控台。請聯絡您的 CSDM，以使用下列值代表您提交部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策變更請求 (ct-3dpd8mdd9jn1r)：

- UserName：您正在建立之 IAM 使用者實體的名稱

- AccessType：「主控台存取」
- UserPermissions：「*USERNAME* 的臨時 AMS 主控台存取權（您想要擁有臨時存取權的人員）」
- 電子郵件通知：您的電子郵件地址，因此當 AMS 請求您

Note

此臨時 AMS 主控台存取的 RFC 需要您內部安全團隊和 AMS 全球安全部門的安全審查和接受。

此請求完成後，您可以登入後，您必須核准已建立的 RFC，以追蹤核准並允許 AMS 團隊關閉工作。若要核准 RFC，請在 RFC 的清單頁面中找到它（旁邊會有待核准旗標），選取它以開啟該 RFC 的 RFC 詳細資訊頁面，然後選擇核准。請注意，在 RFC 核准之前，您將無法使用 AMS。

當 RFC 成功完成時，AMS 操作會為您提供新的 IAM 使用者和密碼。然後遵循下列步驟：

1. 前往 AWS 管理主控台，並使用提供的登入資料登入。系統會要求您建立新密碼。您也必須在登入時設定多重要素驗證 (MFA)；若要進一步了解如何執行此操作，請參閱[在中使用 Multi-Factor Authentication \(MFA\) AWS](#)。
2. 在 AWS 管理主控台中，變更為提供的 IAM 角色 (customer_*CustomerCode*_readonly_user_role)。
3. 開啟 AMS 受管服務主控台。

Note

暫時存取預設為 60 天；不過，您可以聯絡 CSDM 請求三十天延長。

使用堡壘存取執行個體

客戶和 AMS 運算子對 AMS 受管帳戶內資源的所有存取，都是使用堡壘主機來鎖定。我們維護 Linux 和 Windows RDP 堡壘，以存取多帳戶登陸區域 (MALZ) 和單一帳戶登陸區域 (SALZ) AMS Advanced 帳戶。

您的堡壘只能透過私有連線 (VPN 或 AWS Direct Connect)DX 存取。除了防火牆以防止傳入流量之外，堡壘也會定期依固定排程重新佈建（使用現有登入資料）。

Note

如需將檔案移至 EC2 執行個體的資訊，請參閱[檔案傳輸：本機 Windows 或 MAC PC 到 Linux Amazon EC2](#)。

MALZ

您可以使用 Active Directory (AD) 登入資料登入堡壘執行個體，以存取您的帳戶執行個體。Amazon 使用位於周邊網路 VPC（網路帳戶）中的堡壘，而您可以使用位於共用服務帳戶中客戶堡壘子網路中的客戶堡壘。

當您的 AMS 環境最初加入時，您有兩個 SSH 堡壘和兩個 RDP 堡壘，取決於您的選擇。

SALZ

您可以使用 Active Directory (AD) 登入資料登入堡壘執行個體，以存取您的帳戶執行個體。AMS 使用位於周邊網路子網路中的堡壘，而您使用位於私有子網路中的堡壘。

當您的帳戶最初加入時，預設會有兩個 RDP 和兩個 SSH 堡壘。

Note

做為單一帳戶登陸區域的一部分，AMS 同時提供 RDP (Windows) 和 SSH (Linux) 堡壘來存取堆疊；不過，您可以選擇只想要 RDP 堡壘還是只想要 SSH 堡壘。若要請求僅維護 RDP 或僅維護 SSH 堡壘，請提交服務請求。

若要存取執行個體，您需要：

- 授予堆疊的存取權。若要取得堆疊的存取權，請參閱[堆疊管理員存取權 | 授予](#)或[堆疊唯讀存取權 | 授予](#)。
- 您要存取的堆疊 ID，以便授予您存取執行個體的權限。若要尋找堆疊 ID，請參閱[在 AMS 中尋找堆疊 IDs](#)。
- 您要存取的執行個體 IP。若要尋找執行個體 IP，請參閱[在 AMS 中尋找執行個體 IDs 或 IP 地址](#)。
- DNS 易記堡壘名稱或堡壘 IP。接下來將說明如何使用 DNS 易記的堡壘名稱，以及如何尋找堡壘 IP。

DNS 易記堡壘名稱

AWS Managed Services (AMS) 使用 DNS 易記的堡壘名稱。

MALZ

對於多帳戶登陸區域 (MALZ)，系統會為 AMS 受管 Active Directory 的 FQDN 中的堡壘建立 DNS 記錄。AMS 會視需要取代 Linux 和 Windows 堡壘。例如，如果有新的堡壘 AMI 必須部署，堡壘 DNS 記錄會動態更新，以指向新的有效堡壘。

1. 若要存取 SSH (Linux) 堡壘，請使用如下所示的 DNS 記錄：

`sshbastion(1-4).Your_Domain.com`

例如，其中網域為 `Your_Domain`：

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. 若要存取 RDP (Windows) 堡壘，請使用如下所示的 DNS 記錄：`rdp-Username.Your_Domain.com`。

例如，其中使用者名稱為 `alex`、`demo`、`test` 或 `bob`，網域為 `Your_Domain.com`：

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`
- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

單一帳戶登陸區域 (SALZ) 會視需要取代 Linux 和 Windows 堡壘。例如，如果有新的堡壘 AMI 必須部署，堡壘 DNS 記錄會動態更新，以指向新的有效堡壘。

1. 若要存取 SSH (Linux) 堡壘，請使用如下所示的 DNS 記錄：

`sshbastion(1-4).AAccountNumber.amazonaws.com`。

例如，其中 `123456789012` 是帳戶號碼：

- sshbastion1.A123456789012.amazonaws.com
- sshbastion2.A123456789012.amazonaws.com
- sshbastion3.A123456789012.amazonaws.com
- sshbastion4.A123456789012.amazonaws.com

2. 若要存取 RDP (Windows) 堡壘，請使用如下所示的 DNS 記錄：rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com。

例如，其中 123456789012 是帳戶號碼：

- rdpbastion1.A123456789012.amazonaws.com
- rdpbastion2.A123456789012.amazonaws.com
- rdpbastion3.A123456789012.amazonaws.com
- rdpbastion4.A123456789012.amazonaws.com

節省單一帳戶登陸區域 (SALZ) 堡壘的成本

AMS 在預設組態中提供兩個 SSH 堡壘和兩個 RDP 堡壘，供您連線至 Amazon EC2 執行個體，並在服務操作的預設組態中部署兩個 DMZ 堡壘。根據預設，堡壘會使用 m4. large Amazon EC2 執行個體。您可以選擇將堡壘使用的 Amazon EC2 執行個體變更為 t3.small，並節省成本。

如果您使用隨需執行個體、Spot 執行個體或節省計劃，您應該考慮此功能並節省成本。如果您使用預留執行個體，請考慮使用 t3.small 執行個體是否會降低您的成本。若要變更執行個體類型，請從 AMS 帳戶提交 RFC 與管理 | 進階堆疊元件 | EC2 執行個體堆疊 | 調整大小 (ct-15mazj88xc69) CT。

如有其他問題，請聯絡您的雲端服務交付管理員 (CSDM)，或檢查您是否可以從此功能中受益。

使用堡壘 IP 地址

AMS 客戶可以使用先前[DNS 易記堡壘名稱](#)所述的 SSH 和 RDP 堡壘，或堡壘 IP 地址。

若要尋找您帳戶的堡壘 IP 地址、SSH 和 RDP：

1. 僅適用於多帳戶登陸區域：登入共用服務帳戶。
2. 開啟 EC2 主控台，然後選擇執行中的執行個體。

執行個體頁面隨即開啟。

3. 在頂端的篩選方塊中，輸入 ssh-bastion 或 rdp-bastion。

在頂端的篩選方塊中，輸入 customer-ssh 或 customer-rdp。

顯示您帳戶的 SSH 和/或 RDP 堡壘。

請注意，除了 SSH 堡壘之外，您可能會在清單中看到無法使用的 AMS 周邊網路堡壘。

4. 選取 SSH 或 RDP 堡壘。如果您使用 Windows 電腦並想要登入 Linux 執行個體，請使用 SSH 堡壘。如果您想要登入 Windows 執行個體，請使用 RDP 堡壘。如果您使用 Linux 作業系統並想要登入 Windows 執行個體，您可以透過 RDP 通道使用 SSH 堡壘（這樣您就可以存取 Windows 桌面）。若要從 Linux 作業系統存取 Linux 執行個體，請使用 SSH 堡壘。

AMS 中的執行個體存取範例

這些範例示範如何在透過 RFC 授予存取權之後，使用堡壘登入 AMS 帳戶中的執行個體。如需取得授予存取權的詳細資訊，請參閱 [請求執行個體存取](#)。

Note

如需將檔案移至 EC2 執行個體的資訊，請參閱[檔案傳輸：本機 Windows 或 MAC PC 到 Linux Amazon EC2](#)。

必要資料：

- 堡壘 DNS 易記名稱或 IP 地址：如 中所述使用 DNS 易記名稱，[DNS 易記堡壘名稱](#)或如 中所述尋找堡壘 IP 地址[使用堡壘 IP 地址](#)。

Note

透過 Amazon EC2 Auto Scaling 群組建立的 Amazon EC2 執行個體將具有循環進出的 IP 地址，您必須使用 Amazon EC2 主控台來尋找該 IP 地址。

- 使用者名稱（例如 `DOMAIN_FQDN\USERNAME`）和密碼：帳戶的登入資料。`USERNAME` 必須是您的 Active Directory 使用者名稱。

請注意，可以使用格式為 `username@customerdomain.com` 的使用者名稱，但可能會導致 PBIS 設定發生問題。

- 堆疊 IP 地址：查看您提交以啟動堆疊之 RFC 的執行輸出，或在 Amazon EC2 主控台中查詢 Amazon EC2 執行個體 IP 地址，以找出此問題。對於單一 Amazon EC2 執行個體，您也可以使用

AMS SKMS 命令 `ListStackSummaries` 來尋找堆疊 ID，然後使用 `GetStack` 來尋找堆疊 IP 地址。如需 AMS SKMS API 參考，請參閱 AWS 成品主控台中的報告索引標籤。

視需要存取堡壘 IP 地址，可以是 SSH 或 RDP，並使用下列其中一個程序登入。

Note

RDP 堡壘僅允許兩個同時連線。因此，在最佳情況下，只有 4 個管理員可以同時連線到 Windows 堆疊。如果您需要更多 RDP 連線，請參閱 [AMS 加入指南中的應用程式遷移/加入期間的 AMS 堡壘選項](#)。

Linux 電腦到 Linux 執行個體

使用 SSH 連接到 SSH 堡壘，然後連接到 Linux 執行個體。

MALZ

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 堡壘](#)。

若要連線到 Linux 執行個體，您必須先連線到 SSH 堡壘。

1. 開啟 shell 視窗並輸入：

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

如果您的 `Domain_FQDN` 是 "corp.domain.com"、您的帳號是 "123456789123"、您的 `_Domain` 是 "amazonaws.com"、您選擇堡壘 "4"，且您的使用者名稱是 "JoeSmith"，則看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 使用您的公司 Active Directory 登入資料登入。
3. 當出現 Bash 提示時，SSH 會傳入執行個體，然後輸入：

```
ssh Domain_FQDN\\Username@Instance_IP
```

或者，您可以使用登入旗標 (-l)：

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 堡壘](#)。

若要連線到 Linux 執行個體，您必須先連線到 SSH 堡壘。

1. 開啟 shell 視窗並輸入：

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

如果您的帳號是 123456789123，您可以選擇堡壘 4，而您的使用者名稱是 JoeSmith，這看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 使用您的公司 Active Directory 登入資料登入。
3. 當出現 Bash 提示時，SSH 會傳入執行個體，然後輸入：

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

或者，您可以使用登入旗標 (-l)：

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 電腦到 Windows 執行個體

使用 SSH 通道和 RDP 用戶端從 Linux 電腦連線至 Windows 執行個體。

MALZ

此程序需要適用於 Linux 的遠端桌面連線用戶端；範例使用 Microsoft 遠端桌面（連線至 Windows 遠端桌面服務的開放原始碼 UNIX 用戶端）。Rdesktop 是替代方案。

Note

登入 Windows 執行個體的方式可能會根據使用的遠端桌面用戶端而有所不同。

首先建立 SSH 通道，然後登入。

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 易記堡壘名稱](#)。

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱[存取請求](#)。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).Your_Domain
```

如果您的 Domain_FQDN 是 "corp.domain.com"、您的 AMS 受管 Your_Domain 是 "amazonaws.com"、您選擇堡壘 "4"，且您的使用者名稱是 "JoeSmith"，則看起來像這樣：

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱[尋找執行個體 ID 或 IP 地址](#)。
1. 從 Linux 桌面到 Windows 執行個體透過 SSH 通道設定 RDP。為了發出具有正確值的 ssh 命令，有幾種方式可以繼續：
 - 在 Linux shell 中，設定變數，然後輸入 SSH 連線命令：

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"  
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

範例，如果使用下列值：

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 將變數值直接新增至ssh命令。

在任何一種情況下，這就是轉譯的請求（假設相同的變數值集）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. 兩者之一：開啟遠端桌面用戶端，輸入迴路地址和連接埠 127.0.0.1 : 3389，然後開啟連線。

或者，從新的 Linux 桌面 shell 登入 Windows 執行個體。如果您使用 RDesktop，命令如下所示：

```
rdesktop 127.0.0.1:3389
```

Windows 執行個體的遠端桌面視窗會顯示在您的 Linux 桌面上。

Tip

如果遠端桌面工作階段無法啟動，請確認步驟 1 中的連接埠 3389 允許從 SSH 堡壘連線至 Windows 執行個體 (private_ip_address_of_windows_instance 正確取代)：

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功：

```
nc 172.16.0.83 3389 -v -z
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```


SALZ

單一帳戶登陸區域的此程序需要 Linux 的遠端桌面連線用戶端；範例使用 Microsoft 遠端桌面（連線至 Windows 遠端桌面服務的開放原始碼 UNIX 用戶端）。Rdesktop 是替代方案。

Note

登入 Windows 執行個體的方式可能會根據使用的遠端桌面用戶端而有所不同。

首先建立 SSH 通道，然後登入。

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 易記堡壘名稱](#)。

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱[存取請求](#)。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

如果您的帳號是 123456789123 且您選擇堡壘 4，則看起來像這樣：

```
sshbastion4.A123456789123.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱[尋找執行個體 ID 或 IP 地址](#)。
1. 從 Linux 桌面到 Windows 執行個體透過 SSH 通道設定 RDP。為了發出具有正確值的ssh命令，有幾種方式可以繼續：
 - 在 Linux shell 中，設定變數，然後輸入 SSH 連線命令：

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"  
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"  
AD="AD_ACCOUNT_NUMBER"  
USER="AD_USERNAME"  
ssh -L 3389:$WINDOWS:3389 A$AD\\$USER@$BASTION
```

範例，如果使用下列值：

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 將變數值直接新增至ssh命令。

在任何一種情況下，這就是轉譯的請求（假設相同的變數值集）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 兩者之一：開啟遠端桌面用戶端，輸入迴路地址和連接埠 127.0.0.1 : 3389，然後開啟連線。

或者，從新的 Linux 桌面 shell 登入 Windows 執行個體。如果您使用 RDesktop，命令如下所示：

```
rdesktop 127.0.0.1:3389
```

Windows 執行個體的遠端桌面視窗會顯示在您的 Linux 桌面上。

Tip

如果遠端桌面工作階段無法啟動，請確認步驟 1 中的連接埠 3389 允許從 SSH 堡壘連線至 Windows 執行個體 (`private_ip_address_of_windows_instance` 正確取代)：

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功：

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp      0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Windows 電腦到 Windows 執行個體

使用 Windows 遠端桌面連線用戶端從 Windows 電腦連線至 Windows 執行個體。

MALZ

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 易記堡壘名稱](#)。

1. 開啟遠端桌面連線程式，這是標準的 Windows 程式，然後在主機名稱欄位中輸入 Windows 堡壘的易記 DNS 名稱。

2. 選擇連線。遠端桌面連線會嘗試與堡壘建立 RDP 連線。

如果成功，會開啟登入資料對話方塊。若要取得存取權，請使用您的公司 Active Directory 登入資料，就像使用 Windows 執行個體一樣。

3. 在堡壘上開啟遠端桌面連線程式，然後輸入您要連線的 Windows 執行個體 IP 地址（例如 10.0.0.100），然後選擇連線。連線至 Windows 執行個體之前，需要再次使用您的公司 Active Directory 登入資料。

SALZ

如需易記堡壘名稱的詳細資訊，請參閱 [DNS 易記堡壘名稱](#)。

1. 開啟遠端桌面連線程式，這是標準的 Windows 程式，並在主機名稱欄位中輸入 Windows 堡壘的易記 DNS 名稱；例如，如果您的帳戶號碼為 123456789123 且您選擇堡壘 4，`rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`則會像這樣 `rdpbastion4.A123456789123.amazonaws.com`。

2. 選擇連線。遠端桌面連線會嘗試與堡壘建立 RDP 連線。

如果成功，會開啟登入資料對話方塊。若要取得存取權，請使用您的公司 Active Directory 登入資料，就像使用 Windows 執行個體一樣。

3. 在堡壘上開啟遠端桌面連線程式，然後輸入您要連線的 Windows 執行個體 IP 地址（例如 10.0.0.100），然後選擇連線。連線至 Windows 執行個體之前，需要再次使用您的公司 Active Directory 登入資料。

Windows 電腦到 Linux 執行個體

若要從 Windows 環境 RDP 到 SSH 堡壘，請遵循下列步驟。

MALZ

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱[存取請求](#)。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).YOUR_DOMAIN
```

如果 YOUR_DOMAIN 是 myamsaddomain.com：// 且您選擇堡壘 4：

```
sshbastion4.myamsaddomain.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱[尋找執行個體 ID 或 IP 地址](#)。

若要從 Windows 機器連線至 Linux 執行個體，您必須先連線至 SSH 堡壘。

使用原生 Windows [OpenSSH 用戶端](#)，或在本機電腦上安裝 [PuTTY](#)。若要進一步了解 OpenSSH，請參閱 [Windows 中的 OpenSSH](#)。

1. 使用原生 Windows 或開啟 PuTTY，然後輸入 SSH 堡壘主機名稱或 SSH 堡壘的 IP 地址。例如，10.65.2.214 (22 是用於 SSH 的連接埠，預設為)。
2. OpenSSH 或 PuTTY 會嘗試 SSH 連線到堡壘，並開啟 shell 視窗。
3. 像使用 RDP 主機一樣使用您的公司 Active Directory 登入資料來取得存取權。
4. 當出現 Bash 提示時，SSH 會進入執行個體。輸入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

開始之前：

- 請求存取您要連線的執行個體；如需資訊，請參閱[存取請求](#)。
- 選擇要連線的易記 DNS SSH 堡壘名稱；例如：

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

如果您的帳號是 123456789123 且您選擇堡壘 4，則看起來像這樣：

```
sshbastion4.A123456789123.amazonaws.com
```

- 尋找您要連線之執行個體的 IP 地址；如需資訊，請參閱[尋找執行個體 ID 或 IP 地址](#)。

若要從 Windows 機器連線至 Linux 執行個體，您必須先連線至 SSH 堡壘。

使用原生 Windows [OpenSSH 用戶端](#)，或在本機電腦上安裝 [PuTTY](#)。若要進一步了解 OpenSSH，請參閱 [Windows 中的 OpenSSH](#)。

1. 使用原生 Windows 或開啟 PuTTY，然後輸入 SSH 堡壘主機名稱或 SSH 堡壘的 IP 地址。例如，10.65.2.214 (22 是用於 SSH 的連接埠，預設為)。
2. OpenSSH 或 PuTTY 會嘗試 SSH 連線到堡壘，並開啟 shell 視窗。
3. 像使用 RDP 主機一樣使用您的公司 Active Directory 登入資料來取得存取權。
4. 當出現 Bash 提示時，SSH 會進入執行個體。輸入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

AMS 帳戶中以團隊或角色為基礎的存取控制

案例：兩個應用程式團隊 A 和 B 分別針對其應用程式「AA」和「BB」使用單一 AMS 帳戶。團隊 A 只想要存取應用程式「AA」的資源，而團隊 B 只想要存取應用程式「BB」的資源。如何設定？

使用其 ITSM 的工具實作以團隊為基礎的存取控制 (TBAC)。例如，您可以使用 AMS ServiceNow Connector 應用程式與 AMS APIs 整合。如需此實作的高階指引，請聯絡您的 CSDM。

AMS Advanced 中的自動化執行個體組態

AMS Advanced 自動化執行個體組態服務會每天執行，並自動掃描和更新受管 EC2 執行個體上的 SSM 和 CloudWatch 代理程式和組態檔案。更新會視需要套用，以：

- SSM 和 CloudWatch 代理程式
- CloudWatch 組態檔案

這些更新可讓 AMS 存取您的 AMS 受管 EC2 執行個體，並設定您的執行個體以發出適當的[日誌](#)和指標。

主題

- [自動化執行個體組態的先決條件](#)
- [SSM Agent 自動安裝](#)
- [自動化變更](#)

自動化執行個體組態的先決條件

對於使用變更管理部署執行個體的 AMS Advanced 客戶，必須符合下列先決條件：

- SSM 代理程式已安裝，且處於受管狀態。
- 執行個體會標記為受管執行個體。(aws:cloudformation:stack-name標籤具有以 stack-或開頭的值sc-。)

如果您的執行個體尚未安裝 SSM 代理程式，您可以使用 AMS SSM 代理程式自動安裝功能進行安裝。如需詳細資訊，請參閱[SSM Agent 自動安裝](#)。

或者，您可以手動安裝 SSM 代理程式。如需詳細資訊，請參閱下列內容：

- Linux：[在 Linux 的 EC2 執行個體上手動安裝 SSM 代理程式 - AWS Systems Manager](#)
- Windows：[在適用於 Windows Server 的 EC2 執行個體上手動安裝 SSM 代理程式 - AWS Systems Manager](#)

如需 SSM 代理程式的詳細資訊，請參閱[使用 SSM 代理程式](#)的 AWS 文件。

SSM Agent 自動安裝

若要讓 AMS 管理您的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，您必須在每個執行個體上安裝 AWS Systems Manager SSM Agent。如果您的執行個體未安裝 SSM Agent，您可以使用 AMS SSM Agent 自動安裝功能。

Note

- 此功能僅適用於不在 Auto Scaling 群組中且執行 AMS 支援的 Linux 作業系統的 EC2 執行個體。
- AMS SSM 代理程式自動安裝功能預設為停用。若要啟用此功能，請聯絡您的 CA 或 CSDM。

SSM Agent 使用的先決條件

- 確定與目標執行個體相關聯的執行個體描述檔具有下列其中一個政策（或與其允許清單相同的許可）：
 - AmazonSSMManagedEC2InstanceDefaultPolicy
 - AmazonSSMManagedInstanceCore
- 請確定 AWS Organizations 層級沒有明確拒絕前述政策中所列許可的服務控制政策。

如需詳細資訊，請參閱[設定 Systems Manager 所需的執行個體許可](#)。

- 若要封鎖傳出流量，請確定已在目標執行個體所在的 VPC 上啟用下列界面端點（適當地取代 URL 中的「區域」）：
 - ssm.<region>.amazonaws.com
 - ssmmessages.<region>.amazonaws.com
 - ec2messages.<region>.amazonaws.com

如需詳細資訊，請參閱[使用適用於 Systems Manager 的 VPC 端點來改善 EC2 執行個體的安全性](#)。

如需啟用或停用受管節點可用性疑難排解的一般秘訣，請參閱[解決方案 2：確認已為執行個體指定 IAM 執行個體描述檔（僅限 EC2 執行個體）](#)。

 Note

AMS 會在自動安裝程序中停止和啟動每個執行個體。當執行個體停止時，存放在執行個體儲存體磁碟區中的資料和存放在 RAM 上的資料都會遺失。如需詳細資訊，請參閱[停止執行個體時會發生的情況](#)。

請求在您的執行個體上自動安裝 SSM Agent

如果您的帳戶已加入 AMS Accelerate Patch Add-On，請為執行個體設定修補程式維護時段 (MW)。需要有效的 SSM 代理程式才能完成修補程序。如果執行個體上缺少 SSM 代理程式，則 AMS 會嘗試在修補程式維護時段期間自動安裝它。

 Note

AMS 會在自動安裝程序中停止和啟動每個執行個體。當執行個體停止時，存放在執行個體儲存體磁碟區中的資料和存放在 RAM 上的資料都會遺失。如需詳細資訊，請參閱[停止執行個體時會發生的情況](#)。

SSM Agent 自動安裝的運作方式

AMS 使用 EC2 使用者資料在您的執行個體上執行安裝指令碼。若要新增使用者資料指令碼並在執行個體上執行，AMS 必須停止並啟動每個執行個體。

如果您的執行個體已有現有的使用者資料指令碼，則 AMS 會在自動安裝程序期間完成下列步驟：

1. 建立現有使用者資料指令碼的備份。
2. 以 SSM Agent 安裝指令碼取代現有的使用者資料指令碼。
3. 重新啟動執行個體以安裝 SSM Agent。
4. 停止執行個體並還原原始指令碼。
5. 使用原始指令碼重新啟動執行個體。

自動化變更

AMS Advanced 自動化執行個體組態服務會視需要變更 EC2 執行個體。

有哪些變更：

- [在 Linux 執行個體上自動更新程式碼](#)
- [在 Linux 執行個體上自動更新 PBIS](#)
- [自動更新 SSM 和 CloudWatch 代理程式的最低版本](#)
- [CloudWatch 組態檔案、更新詳細資訊](#)
- [自動設定的日誌](#)

在 Linux 執行個體上自動更新程式碼

AMS 會自動更新 Linux 執行個體上的執行個體程式碼。這有助於改善 AMS 元件和環境的操作穩定性和安全性。

常見問答集：

Linux 上的執行個體上程式碼 (OIC) 包含哪些內容？

OIC 包含 `ams-toolkit` 套件，以及一些組態檔案和 Cron 任務。AMS 需要這些檔案和套件才能整合 (Active Directory、CloudFormation 和其他相依性)。我們將這些檔案預先封裝至 AMS 提供的 AMIs，或在工作負載擷取期間安裝到您的執行個體。

AMS 何時會更新 OIC？

當我們發行具有錯誤修正或其他改進的新版本時，AMS 會更新 OIC。檢查 OIC 版本和更新的工作流程會每天執行。

在 Linux 執行個體上自動更新 PBIS

AMS 使用 Power Broker Identity Service (PBIS) 模組將 Linux 執行個體加入 AMS 受管 Active Directory。

AMS 會自動更新 Linux 執行個體上的 PBIS。

常見問答集：

AMS 何時會更新 PBIS？

AMS 會在重新啟動時開啟 PBIS 更新。如果有可用的新 PBIS 版本，則 AMS 會在下次執行個體重啟時嘗試安裝新版本。

PBIS 更新可以關閉嗎？

您可以在執行個體或帳戶層級關閉 PBIS 更新：

- 帳戶層級：在 SSM 參數存放區中建立參數：名稱：`/ams/skip-pbis-update`、值：`true`（任何案例）。

Note

執行個體描述檔必須具有讀取 SSM 參數的許可。如果缺少 旗標，則預設行為是執行更新。

- 執行個體層級：
 - 標籤型：將下列標籤新增至執行個體：金鑰：`skip_pbis_update`、值：`true`（任何案例）。
 - Config 檔案：將下列旗標新增至 `/opt/aws/ams/etc/ams.conf.d/state.ini` 檔案：`skip_pbis_update = true`。

Note

標籤的優先順序高於 SSM 參數。您可以透過 參數關閉帳戶層級的 PBIS 更新，但透過新增標籤 (Key: `skip_pbis_update`) 將其用於單一（或多個）執行個體 Value: `false`。

若要設定任何描述的選項，請遵循 AMS 環境中的標準變更管理程序。

自動更新 SSM 和 CloudWatch 代理程式的最低版本

AMS Advanced 最低版本 (SSM 或 CloudWatch 代理程式的版本) 是經過 AMS 服務團隊測試並針對您的作業系統預先核准的版本。我們會嘗試保持主動性並執行最新穩定且相容的版本，因此版本編號會隨著時間而變更。您可以透過向 AMS 提出服務請求來尋找目前的最低版本。

• SSM 代理程式管理

Amazon SSM Agent 負責在執行個體上執行遠端命令。執行個體組態自動化可確保 SSM Agent 正在執行最低版本。

• Cloudwatch 代理程式管理

Amazon CloudWatch Agent 負責發出作業系統日誌和指標。自動化執行個體組態會執行下列動作：

- 如有需要，會停用舊版 CloudWatch Log 代理程式，並將組態遷移至新的統一 CloudWatch 代理程式
- 如果您的執行個體正在執行舊版 CloudWatch Log Agent，自動化執行個體組態會停用舊版 CloudWatch Log Agent 服務，並將其組態遷移至統一的 CloudWatch 代理程式。
- 自訂 CloudWatch 組態以發出適當的日誌和指標。

受影響的檔案和目錄：

- Windows
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch 組態檔案、更新詳細資訊

我們從下列 CloudWatch 目錄讀取您的自訂 CloudWatch 組態（僅限 JSON）（請參閱[建議的目錄](#)），並將其與標準 AMS CloudWatch 組態合併：CloudWatch

- CloudWatch 檔案
 - 在執行個體上：
 - Windows
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
 - %ProgramFiles%\WindowsPowerShell\Modules\AWSManagedServices.Logging.Utilities\Files\Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
 - 在 Amazon S3 上：
 - Windows：
 - https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json

- https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json

自動設定的日誌

我們會設定您的執行個體以寫入下列日誌。

- Windows :
 - AmazonSSMAgentLog
 - AmazonCloudWatchAgentLog
 - AmazonSSMErrorLog
 - AmazonCloudFormationLog
 - ApplicationEventLog
 - EC2ConfigServiceEventLog
 - MicrosoftWindowsAppLockerEXEAndDLLEventLog
 - MicrosoftWindowsAppLockerMSIAndScriptEventLog
 - MicrosoftWindowsGroupPolicyOperationalEventLog
 - SecurityEventLog
 - SystemEventLog
- Linux :
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit.log
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler
 - /var/log/syslog

- /var/log/yum.log
- /var/log/zypper.log

AMS 中的監控和事件管理

主題

- [什麼是監控？](#)
- [AMS 監控系統監控什麼？](#)
- [監控的運作方式](#)
- [檢視 AMS 帳戶的監控組態](#)
- [變更 AMS 帳戶的監控組態](#)
- [AMS 中的應用程式感知事件通知](#)
- [在 AMS 中使用 OpsCenter](#)
- [來自 AMS 的提醒通知](#)
- [在 AMS 中建立其他 CloudWatch 警示](#)
- [在 AMS 中建立自訂 CloudWatch 指標和警示](#)
- [在 AMS 中使用適用於 .Net 和 SQL 伺服器的 CloudWatch Application Insights](#)
- [在 AMS 中使用 Amazon EventBridge 受管規則](#)
- [AMS 中的信任修復程式](#)

AWS Managed Services (AMS) 監控系統可監控您的 AMS 資源是否有故障、效能降低和安全問題。AMS 監控系統倚賴 Amazon CloudWatch(CloudWatch)、Amazon GuardDuty、Amazon Macie 和等 AWS 服務 AWS Health。除了監控系統之外，AMS 還部署 TrendMicro DeepSecurity 以防止 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上的惡意軟體，如需端點安全 (EPS) 預設值的相關資訊，請參閱 [端點安全 \(EPS\)](#)。

AMS 監控提供下列優點：

- 監控基準，即使您未為受管帳戶設定任何其他監控，也能獲得預設層級的保護。如需相關資訊，請參閱[AMS 中基準監控的提醒](#)。
- 調查提醒以判斷適當的動作。例如，如果 GuardDuty 找到指出對 Amazon EC2 執行個體強制嘗試暴力的活動，則 AMS 會分析 VPC 流量日誌，以了解活動的來源和內容。
- 盡可能修復提醒，以防止或減少對應用程式的影響。例如，如果您使用獨立的 Amazon EC2 執行個體，但系統運作狀態檢查失敗，則 AMS 會停止並重新啟動執行個體，以嘗試復原執行個體。如需詳細資訊，請參閱[AMS 自動修復提醒](#)。

- 使用 OpsCenter 對作用中和先前已解決的警示進行透明度。例如，如果您在 Amazon EC2 執行個體上有非預期的高 CPU 使用率，您可以請求存取 AWS Systems Manager 主控台（包括存取 OpsCenter 主控台），並直接在 OpsCenter 主控台中檢視 OpsItem。OpsCenter

什麼是監控？

AMS 監控系統可監控您的 AWS 資源是否有故障、效能降低和安全問題。作為受管帳戶，AMS 會設定和部署適用 AWS 資源的警示、監控警示，並在適用時執行修復。

AMS 監控系統會根據您帳戶中的監控組態產生警示。帳戶的監控組態是指帳戶中建立提醒的所有資源參數；如需資源參數的相關資訊，請參閱 [AMS 中基準監控的提醒](#)。帳戶的監控組態包括 CloudWatch 警示定義，以及產生警示的 CloudWatch 事件規則（警示或事件）。

基準監控組態是由 AMS 策劃的一組警示定義 ([AMS 中基準監控的提醒](#))，用於監控受管帳戶中的資源。由於您請求的變更，帳戶的監控組態可能與基準組態不同。

帳戶中所設定之基準監控所產生的立即、持續、下降或潛在故障、效能降低或安全問題的通知，稱為警示。警示的範例包括 Amazon CloudWatch 警示、Amazon CloudWatch 事件、事件或 AWS 服務的問題清單，例如 Amazon GuardDuty，以及 Trend Micro Deep Security 的事件或警示。

來自 Amazon GuardDuty、Amazon Macie 或 Trend Micro Deep Security 等安全相關 AWS 服務的提醒稱為安全提醒，以區分它們與其他類型的提醒。

AMS 監控提供下列優點：

- 自訂基準資源警示以符合您的需求的能力。
- 盡可能自動修復提醒，以防止或降低對應用程式的影響。例如，如果您使用獨立的 Amazon EC2 執行個體，但系統運作狀態檢查失敗，則 AMS 會停止並重新啟動執行個體，以嘗試復原執行個體。如需詳細資訊，請參閱 [AMS 自動修復提醒](#)。
- 使用 OpsCenter 對作用中和先前已解決的警示進行透明度。例如，如果您在 Amazon EC2 執行個體上有非預期的高 CPU 使用率，您可以請求存取 主控台 AWS Systems Manager（包括存取 OpsCenter 主控台），並直接在 OpsCenter 主控台中檢視 OpsItem。OpsCenter
- 調查警示以判斷適當的動作。
- 根據您帳戶中的組態和支援的 AWS 服務產生的提醒。帳戶的監控組態是指帳戶中建立提醒的所有資源參數。帳戶的監控組態包括 CloudWatch 警示定義，以及產生警示的 EventBridge（先前稱為 CloudWatch Events）（警示或事件）。如需資源參數的詳細資訊，請參閱 [AMS 中基準監控的提醒](#)。

- 通知即將發生、持續發生、下降或潛在的故障；效能降低；或帳戶中設定的基準監控所產生的安全問題（稱為警示）。警示的範例包括 CloudWatch 警示、事件或來自 AWS 服務的調查結果，例如 GuardDuty 或 AWS Health。

AMS 監控系統監控什麼？

為了與 AWS Managed Services (AMS) 共享服務責任模型保持一致，AMS 監控系統會監控您的 AWS 基礎設施。如需 AMS 中基準監控的詳細資訊，包括監控的 AWS 資源和每個資源的提醒類型，請參閱 [AMS 中基準監控的提醒](#)。對於 Amazon EC2 執行個體，AMS 會監控作業系統，並根據 CPU 使用率和根磁碟區用量等作業系統指標提供基準監控。

我們建議您使用專為應用程式量身打造的 AWS 服務來補充 AMS 監控與額外監控。如需監控可用性的指引，請參閱本白皮書 [可靠性支柱](#) 中的「監控和警示」一節。您可以設定自己的監控以符合您的操作需求；在 [AMS 中建立其他 CloudWatch 警示](#) 和 會討論如何執行此操作在 [AMS 中建立自訂 CloudWatch 指標和警示](#)。

AMS 中 Active Directory Trust 的單一帳戶登陸區域主動監控

AMS 單一帳戶登陸區域 (SALZ) 會監控 AMS 受管帳戶中受管 Active Directory (AD) 與公司網域之間的單向信任狀態。與 Managed AD 的單向信任對於存取請求和執行個體登入請求至關重要。透過這項新的監控，AMS 現在會主動回應信任相關問題，並縮短偵測存取相關事件的平均時間。

此功能會在您的 AWS Managed Services (AMS) 帳戶中自動啟用。

對成本的影響很小。此功能使用四個 AWS CloudWatch 指標，以及兩個 AWS CloudWatch 警示做為一個信任。

監控的運作方式

請參閱下列 AWS Managed Services (AMS) 中監控架構的圖形。

下圖提供 AMS 多帳戶登陸區域和 AMS 單一帳戶登陸區域監控工作流程的高階概觀。

- 產生：在帳戶加入時，AMS 會為您在受管帳戶中建立的所有資源設定基準監控 (CloudWatch (CW) 警示和 CW 事件規則的組合)。基準監控組態會在觸發 CW 警示或產生 CW 事件時產生警示。
- 彙總：
 - 多帳戶登陸區域：提醒是由您在應用程式和核心組織單位帳戶中的資源產生，並透過安全帳戶引導它們傳送至 AMS 監控系統。

- 單一帳戶登陸區域：您的資源所產生的所有提醒都會透過導向至帳戶中的 SNS 主題，傳送至 AMS 監控系統。
- 您也可以設定 AMS 如何將 EC2 分組在一起。AMS 會將與相同 EC2 執行個體相關的所有警示分組為單一事件，或根據您的偏好設定，為每個警示建立一個事件。您可以隨時使用 Cloud Service Delivery Manager 或 Cloud Architect 來變更此組態。無論您使用的是多帳戶登陸區域或單一帳戶登陸區域，其運作方式都相同。
- 處理：AMS 會分析警示，並根據其影響的可能性進行處理。警示的處理方式如下。
- 具有已知客戶影響的提醒：這些提醒會導致建立新的事件報告，而 AMS 會遵循事件管理程序；如需事件管理的相關資訊，請參閱 [AMS 事件回應](#)。

範例提醒：Amazon EC2 執行個體未通過系統運作狀態檢查，AMS 會停止並重新啟動執行個體以嘗試復原執行個體。

- 具有不確定客戶影響的提醒：對於這些類型的提醒，AMS 會傳送事件報告，在許多情況下會要求您在 AMS 採取動作之前驗證影響。不過，如果基礎設施相關的檢查通過，則 AMS 不會將事件報告傳送給您。

例如：Amazon EC2 執行個體上 >85% CPU 使用率超過 10 分鐘的提醒無法立即分類為事件，因為根據用量，可能預期會發生此行為。在此範例中，AMS Automation 會對資源執行基礎設施相關檢查。如果這些檢查通過，即使 CPU 用量超過 99%，AMS 也不會傳送提醒通知。如果自動化偵測到資源上的基礎設施相關檢查失敗，則 AMS 會傳送提醒通知，並檢查是否需要緩解。本節會詳細討論提醒通知。AMS 會在通知中提供緩解選項。當您回覆確認警示是事件 AMS 的通知時，會建立新的事件報告，並開始 AMS 事件管理程序。收到「無客戶影響」或三天內完全沒有回應的服務通知會標記為已解析，而對應的提醒會標記為已解析。

- 沒有客戶影響的提醒：如果在評估之後，AMS 判斷提醒沒有客戶影響，則提醒會關閉。

例如，AWS Health 通知需要替換的 EC2 執行個體，但該執行個體已終止。

EC2 執行個體分組通知

您可以設定 AMS 監控，將來自相同 EC2 執行個體的警示分組為單一事件。您的 Cloud Service Delivery Manager 或 Cloud Architect 可以為您設定。您可以為每個 AMS 受管帳戶設定四個參數。

1. 範圍：選擇全帳戶或以標籤為基礎的。

- 若要指定適用於該帳戶中每個 EC2 執行個體的組態，請選擇範圍 = 整個帳戶。
- 若要指定僅適用於該帳戶中具有特定標籤之 EC2 執行個體的組態，請選擇範圍 = 標籤型。

2. 分組規則：選擇傳統或執行個體。

- 若要為帳戶中的每個資源設定執行個體層級分組，請選擇範圍 = 全帳戶和分組規則 = 執行個體。
 - 若要將帳戶中的特定資源設定為使用執行個體層級分組，請標記這些執行個體，然後選擇範圍 = 標籤型和分組規則 = 執行個體層級。
 - 若要不要將執行個體分組用於帳戶中的提醒，請選擇分組規則 = 傳統。
3. 參與選項：選擇無、僅報告或預設。
- 若要讓 AMS 在組態處於作用中狀態時，不為這些資源的警示建立事件或執行自動化，請選擇無。
 - 若要讓 AMS 在組態處於作用中狀態時，不為這些資源的警示建立事件或執行自動化，也不要執行自動修復 Systems Manager 文件，但若要在報告中包含這些事件的記錄，請僅選擇報告。如果您想要減少與之互動的事件支援案例數量，以及某些資源的某些事件不需要立即關注，例如非生產帳戶中的事件，這可能會很有用。
 - 若要讓 AMS 處理您的提醒、執行自動化，並在需要時建立事件案例，請選擇預設值。
4. 解決時間：選擇 24 小時、48 小時或 72 小時。最後，設定事件案例自動關閉的時間。如果上次案例通訊的時間在值後達到設定的解析，則事件會關閉。

提醒通知

在警示處理過程中，AWS Managed Services (AMS) 會根據影響分析建立事件，並在可以判斷影響時啟動事件管理程序以進行修復。如果無法判斷影響，則 AMS 會透過服務通知，將提醒通知傳送至與您帳戶相關聯的電子郵件地址。在某些情況下，不會傳送此提醒通知。例如，如果基礎設施相關的檢查傳遞高 CPU 使用率提醒，則不會傳送提醒通知給您。如需詳細資訊，請參閱 [中警示處理程序的 AMS 監控架構圖表](#) [監控的運作方式](#)。

標籤型提醒通知

使用標籤將資源的提醒通知傳送到不同的電子郵件地址。最佳實務是使用標籤型提醒通知，因為當多個開發人員團隊使用相同的帳戶時，傳送至單一電子郵件地址的通知可能會導致混淆。標籤型提醒通知不受您選擇的 [EC2 執行個體分組通知](#) 設定影響。

透過標籤型提醒通知，您可以：

- 將提醒傳送至特定電子郵件地址：使用 key = OwnerTeamEmail 標記具有提醒的資源，這些提醒必須傳送至特定電子郵件地址 value = **EMAIL_ADDRESS**。
- 傳送提醒到多個電子郵件地址：若要使用多個電子郵件地址，請指定以逗號分隔的值清單。
例如 key = **OwnerTeamEmail** 和 value = **EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...**。值欄位的字元總數不能超過 260。

- 使用自訂標籤金鑰：若要使用自訂標籤金鑰，請在明確同意啟用標籤型通訊自動通知的電子郵件中提供自訂標籤金鑰名稱給 CSDM。最佳實務是針對所有執行個體和資源的聯絡標籤使用相同的標記策略。

Note

OwnerTeamEmail 的鍵值不必在駝色案例中。不過，標籤區分大小寫，最佳實務是使用建議的格式。

電子郵件地址必須完整指定，並帶有「簽署時」(@)，以將本機部分與網域分隔。無效的電子郵件地址範例：*Team.AppATabc.xyz* 或 *john.doe*。如需標記策略的一般指引，請參閱[標記 AWS 資源](#)。請勿在標籤中新增個人身分識別資訊 (PII)。盡可能使用分發清單或別名。

來自下列 Amazon Services 的資源支援標籤型提醒通知：EC2、Elastic Block Store (EBS)、Elastic Load Balancing (ELB)、Application Load Balancer (ALB)、Network Load Balancer、Relational Database Service (RDS)、OpenSearch、Elastic File System (EFS)、FSx 和 Site-to-Site VPN。

檢視 AMS 帳戶的監控組態

您可以檢視的帳戶監控組態有兩個關鍵部分：

- CloudWatch 警示：您可以前往 CloudWatch 主控台並選擇其他感興趣的服務，以檢視帳戶中的所有 CW 警示。
- CloudWatch 事件：
 - 多帳戶登陸區域：透過使用字串 篩選所有 CW 事件規則，即可找到帳戶中監控的 CloudWatch Events"ams-"。
 - 單一帳戶登陸區域：透過使用字串 篩選所有 CW 事件規則，即可找到帳戶中監控的 CloudWatch Events"mc-"。

變更 AMS 帳戶的監控組態

您可以變更 Amazon EC2 資源的基準監控組態。如需可設定的提醒，請參閱[AMS 中基準監控的提醒](#)。您可以變更警示定義、警示目的地，或選擇退出基準監控的警示通知，讓警示符合您應用程式的操作需求。您可以提交管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k) 並附上下列詳細資訊，以請求任何或所有先前提及的變更。

- 執行個體 IDs 【如果未提及，則帳戶中的所有執行個體都在範圍內】
- CloudWatch 指標名稱，例如 CPU 使用率/交換免費/IOwait
- 目標 - SMS/SNS 主題的電子郵件 ID/電話號碼

若要進一步了解您可以在基準監控組態中請求的變更類型，請參閱 [Amazon CloudWatch 文件](#)。

AMS 中的應用程式感知事件通知

使用應用程式感知自動事件通知，針對 AMS 代表您建立的支援案例自訂您的通訊體驗。當您使用此功能時，AMS 會從 [AWS Service Catalog AppRegistry](#) 擷取自訂工作負載偏好設定，以充實 AMS 事件與應用程式中繼資料的通訊，並自訂 AMS 代表您建立的支援案例嚴重性。若要使用此功能，您必須先在 AMS 帳戶中使用 provision AWS Service Catalog AppRegistry。

若要進一步了解 AMS 監控預設值，請參閱 [AMS 中的監控和事件管理](#)。

在您的 AMS 帳戶中佈建 AppRegistry 並建立應用程式

AppRegistry 服務可在 AMS 帳戶的自助式佈建 (SSP) 模式中使用。如需如何請求存取權的指示，請參閱 [使用 AMS SSP 在您的 AWS Service Catalog AppRegistry AMS 帳戶中佈建](#)。

佈建 AppRegistry 之後，請使用下列其中一種方法來建立應用程式：

1. AWS 主控台：若要進一步了解如何透過 AWS 主控台在 AppRegistry 中建立應用程式，請參閱 [AWS Service Catalog AppRegistry 管理員指南](#) 中的 [建立應用程式](#)。
2. CloudFormation：您可以定義 AppRegistry 應用程式，就像定義任何其他資源一樣。如需詳細資訊，請參閱 AWS CloudFormation 《使用者指南》中的 [AWS Service Catalog AppRegistry 資源類型參考](#)。

建立標籤以啟用案例擴充

您必須先標記應用程式，AMS 才能存取應用程式中繼資料。下表列出所需的標籤。

標籤鍵	標籤值
ams 受管	true

為您的應用程式自訂 AMS 支援案例嚴重性

您可以指定應用程式對組織的重要性，以自訂 AMS 建立支援案例的嚴重性。此設定是由 AppRegistry 中與您的應用程式相關聯的屬性群組所控制。屬性群組名稱的名稱必須符合下列模式：

```
AMS.<ApplicationName>.CommunicationOptions
```

在上述模式中，當您建立應用程式時，ApplicationName 必須符合 AppRegistry 中使用的名稱。

範例內容：

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

這會決定您正在使用的結構描述版本，以及可用的功能子集。

結構描述版本	功能
1.0	根據 Criticality 值自訂支援案例嚴重性

重要性

此應用程式的重要性決定了 AMS 自動化系統所建立支援案例的嚴重性。

有效值：

```
low|normal|high|urgent|critical
```

如需嚴重性等級的詳細資訊，請參閱 AWS 支援 API 參考中的 [SeverityLevel](#)。

必要：是

檢閱必要的許可

若要使用此功能，AMS 需要存取下列 AWS Identity and Access Management 許可：

- iam : ListRoleTags
- iam : ListUserTags
- resourcegroupstaggingapi : GetResources
- servicecatalog-appregistry : GetApplication
- servicecatalog-appregistry : ListAssociatedAttributeGroups
- servicecatalog-appregistry : GetAttributeGroup

Important

請確定沒有拒絕上述動作的 IAM 政策或服務控制政策 (SCP)。

API 呼叫是由 `ams-access-admin` 角色進行。以下是您可能會看到的範例：

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

在 AMS 中使用 OpsCenter

AWS Managed Services (AMS) Operations 團隊使用 [AWS Systems Manager OpsCenter](#) 來診斷和修復與資源相關的許多提醒。

使用 OpsCenter 可減少平均解決時間 (MTTR)，同時提供 AMS 操作團隊操作佇列的透明檢視。

透過 OpsCenter，除了自動化解決方案之外，AMS 還為您提供操作工作項目的透明檢視，也稱為 [OpsItems](#)，AMS 團隊正在積極處理。

若要進一步了解 OpsCenter 和 OpsItems，請參閱 [AWS Systems Manager OpsCenter](#)。如需有關存取 AWS 管理主控台的資訊，請參閱[使用 AWS 管理主控台](#)。從 AWS 管理主控台，您可以導覽至 AWS Systems Manager 主控台和 OpsCenter；如需進一步了解，請參閱[AWS Systems Manager 工作階段管理員](#)。OpsCenter 也提供您可以使用的 API；如需詳細資訊，請參閱[進一步了解 OpsCenter](#)。

OpsCenter 是價格合理的功能，具有成本低於 10 USD 的 ~1000 OpsItems。如需相關資訊，請參閱 [AWS Systems Manager 定價](#)。

來自 AMS 的提醒通知

在警示處理過程中，AWS Managed Services (AMS) 會根據影響分析建立事件，並在可以判斷影響時啟動事件管理程序以進行修復。如果無法判斷影響，AMS 會透過服務通知將警示通知傳送至與您的帳戶相關聯的電子郵件地址；請參閱 [中警示處理程序的 AMS 監控架構圖表](#) [監控的運作方式](#)。

接收 AMS 產生的提醒

AWS Managed Services (AMS) 可讓您直接接收 Amazon EC2 資源的提醒通知，以減少通訊延遲。若要直接接收 Amazon EC2 提醒，請使用 [管理 | 監控和通知 | SNS | 訂閱變更類型 \(ct-3rc19u1k017wu\)](#)，將您的目標（偏好電子郵件）訂閱 Amazon SNS 主題 Direct-Customer-Alerts。

Note

根據預設，並非所有基準提醒都會傳送至 Direct-Customer-Alerts 主題。若要查看 AMS 監控系統產生的所有提醒，請訂閱 AMS 監控系統的 Amazon SNS 主題。在請求中，要求「AMS 監控主題」，指定訂閱管道來接收提醒 (Lambda、Amazon SQS、HTTP/S、電子郵件或 SMS)，並指定將接收提醒的端點（例如，電子郵件地址，如果您選擇電子郵件通訊協定）。AMS 監控主題會接收 AMS 共用服務所使用的警示，因此可能會有雜訊。

若要進一步了解，請參閱《Amazon Simple Notification Service [Subscribe](#) API 參考》中的訂閱一節。

如需 AMS 提供的基準提醒清單，請參閱 [AMS 中基準監控的提醒](#)。

AMS 中的標籤型提醒通知

使用標籤將資源的提醒通知傳送到不同的電子郵件地址。最佳實務是使用標籤型提醒通知，因為當多個開發人員團隊使用相同的帳戶時，傳送至單一電子郵件地址的通知可能會導致混淆。

Important

標籤型提醒通知僅適用於與 Amazon EC2、Amazon EBS、Elastic Load Balancing、Network Load Balancer、Application Load Balancer、Amazon RDS、Amazon Redshift 和 OpenSearch 相關的通知。

請勿在標籤中新增個人身分識別資訊 (PII)。

將提醒傳送至特定電子郵件地址

使用 `key = OwnerTeamEmail`、標記具有必須傳送至特定電子郵件地址之提醒的資源 `value = EMAIL_ADDRESS`。

傳送提醒到多個電子郵件地址

若要使用多個電子郵件地址，請指定以逗號分隔的值清單。例如 `key = OwnerTeamEmail` 和 `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`。值欄位的字元總數不能超過 260。

使用自訂標籤金鑰

若要使用自訂標籤金鑰，請在電子郵件中提供自訂標籤金鑰名稱給 CSDM，以同意啟用標籤型通訊的自動通知。最佳實務是針對所有執行個體和資源的聯絡標籤使用相同的標記策略。

電子郵件地址必須完整指定，並帶有「簽署時」(`@`)，以將本機部分與網域分隔。無效的電子郵件地址範例：`Team.AppATabc.xyz` 或 `john.doe`。如需標記策略的一般指引，請參閱[使用標籤](#)。若要標記現有資源，請使用部署 | 進階堆疊元件 | 標籤 | 建立（自動）(ct-3cx7we852p3af) 變更類型提交 RFC。

Note

`OwnerTeamEmail` 索引鍵值不必在駝色案例中。不過，標籤區分大小寫，最佳實務是使用建議的格式。

AMS 自動修復提醒

驗證後，AWS Managed Services (AMS) 會根據本節所述的特定條件和程序，自動修復特定提醒。

提醒名稱	描述	閾值	動作
中斷的安全頻道	當執行個體與 AD 網域控制器失去連線時，會在 Windows EC2 執行個體上觸發中斷的安全頻道警示。	閾值在過去 15 分鐘內超過定義的值 10 次。	AMS 自動修復會驗證執行個體是否在 SSM 中上線、主機名稱是否重複，以及 AD 電腦物件是否與 CloudFormation 堆疊對齊。修復會修復安全通道連線，以還原對執行個體的存取。

提醒名稱	描述	閾值	動作
狀態檢查失敗	可能的硬體故障或執行個體的故障狀態。	系統在過去 15 分鐘內至少偵測到一次失敗狀態。	AMS 自動修復會先驗證執行個體是否可存取。如果無法存取執行個體，則會停止並重新啟動執行個體。停止和啟動可讓執行個體遷移至新的基礎硬體。如需詳細資訊，請參閱下列「EC2 狀態檢查失敗修復自動化」一節。
AMSLinuxDiskUsage	在 EC2 執行個體上 1 個掛載點（磁碟區上的指定空間）的磁碟用量填滿時觸發。	閾值在過去 30 分鐘超過定義的值 6 次。	AMS 自動修復會先刪除暫存檔案。如果這無法釋放足夠的磁碟空間，它會擴展磁碟區，以防止在磁碟區已滿時停機。
AMSWindowsDiskUsage	當 EC2 執行個體上 1 個掛載點（磁碟區上的指定空間）的磁碟用量填滿時。	閾值在過去 30 分鐘內超過定義的值 6 次。	AMS 自動修復會先刪除暫存檔案。如果這無法釋放足夠的磁碟空間，它會擴展磁碟區，以防止在磁碟區已滿時停機。

提醒名稱	描述	閾值	動作
RDS-EVENT-0089	資料庫執行個體已消耗超過其分配儲存容量的 90%。	儲存空間配置超過 90%。	AMS 自動修復會先驗證資料庫是否處於可修改且可用或完整儲存狀態。然後，它會嘗試透過 CloudFormation 變更集增加配置的儲存、IOPS 和儲存輸送量。如果偵測到堆疊偏離，則會回到 RDS API 以防止停機時間。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

提醒名稱	描述	閾值	動作
RDS-EVENT-0007	資料庫執行個體的配置儲存體已用盡。若要解決此問題，請配置額外的儲存空間。	儲存空間是 100% 配置。	AMS 自動修復會先驗證資料庫是否處於可修改且可用或完整儲存狀態。然後，它會嘗試透過 CloudFormation 變更集增加配置的儲存、IOPS 和儲存輸送量。如果偵測到堆疊偏離，則會回到 RDS API 以防止停機時間。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

提醒名稱	描述	閾值	動作
RDS-EVENT-0224	請求的已配置儲存達到或超過設定的最大儲存閾值。	資料庫執行個體的最大儲存閾值已用盡，或大於或等於請求的已配置儲存。	AMS 自動修復會先驗證請求的 RDS 儲存量是否超過最大儲存閾值。如果確認，AMS 會嘗試使用 CloudFormation 變更集將最大儲存閾值提高 30%，如果資源未透過 CloudFormation 佈建，則請直接 RDS API。 將下列標籤新增至 RDS 資料庫執行個體，即可選擇退出此功能： "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

提醒名稱	描述	閾值	動作
RDS-Stora ge-Capaci ty	少於 1GB 會保留在資料庫 執行個體的配置儲存體中 。	已配置 99% 的儲存空間。	AMS 自動修復會先驗 證資料庫是否處於可修 改且可用或完整儲存狀 態。然後，它會嘗試透過 CloudFormation 變更集增 加配置的儲存、IOPS 和 儲存輸送量。如果偵測到 堆疊偏離，則會回到 RDS API 以防止停機時間。 將下列標籤新增至 RDS 資料庫執行個體，即可選 擇退出此功能： "Key: ams:rt:ams-rds- max-allocated- storage-policy, Value: ams-opt-o ut".

Amazon EC2 中斷安全通道：修復自動化備註

在 AWS Managed Services (AMS) 自動修復對 Amazon EC2 Windows 中斷安全通道問題執行修復之前，自動化會執行下列預先檢查，並建立事件報告以進行進一步調查：

- 驗證 Amazon EC2 執行個體 SSM 狀態是否為「線上」。
- 驗證 Amazon EC2 執行個體是否屬於 Auto Scaling 群組，以及 Auto Scaling 群組中的所有執行個體是否具有相同的主機名稱。
- 檢查 Amazon EC2 執行個體是否為用來佈建的 CloudFormation 堆疊的一部分。如果執行個體已從 CloudFormation 堆疊中移除，自動化會驗證相關聯的 Active Directory 組織單位 (OU) 是否仍在參考堆疊。

通過上述驗證後，自動化會繼續修復中斷的安全頻道。

修復步驟：

- 自動修復會嘗試修復 EC2 執行個體和 AD 網域之間的安全通道，還原對執行個體的存取。
- 修復後，自動化會檢查是否已建立安全頻道。如果失敗，AMS 會建立事件並委託 AMS 操作進行調查。

EC2 狀態檢查失敗：修復自動化備註

AMS 自動修復如何與 EC2 狀態檢查失敗問題搭配使用：

- 如果您的 Amazon EC2 執行個體無法連線，執行個體必須停止並再次啟動，才能遷移至新的硬體並復原。
- 如果問題的根目錄在作業系統中（缺少 fstab 中的裝置、核心損毀等），則自動化無法復原您的執行個體。
- 如果您的執行個體屬於 Auto Scaling 群組，自動化不會採取任何動作，AutoScalingGroup 擴展動作會取代執行個體。
- 如果您的執行個體已啟用 EC2 Auto Recovery，則修復不會採取動作。

EC2 磁碟區用量修復自動化

AWS Managed Services (AMS) 自動修復如何解決 EC2 磁碟區用量問題：

- 自動化會先驗證是否需要磁碟區擴展，以及是否可以執行。如果認為擴展是適當的，自動化可以增加磁碟區容量。此自動化程序會平衡成長需求與受控制、有限的擴展。
- 在擴展磁碟區之前，自動化會在執行個體上執行清除任務 (Windows：磁碟清理程式、Linux：Logrotate + Simple Service Manager 代理程式日誌移除)，以嘗試釋放空間。

Note

清理任務不會在 EC2 "T" 系列執行個體上執行，因為它們依賴 CPU 點數來持續運作。

- 在 Linux 上，自動化僅支援擴展類型為 EXT2, EXT3, EXT4 和 XFS 的檔案系統。
- 在 Windows 上，自動化僅支援新技術檔案系統 (NTFS) 和彈性檔案系統 (ReFS)。
- 自動化不會擴展屬於邏輯磁碟區管理員 (LVM) 或 RAID 陣列一部分的磁碟區。
- 自動化不會擴展執行個體存放區磁碟區。
- 如果受影響的磁碟區已大於 2 TiB，則自動化不會採取動作。
- 透過自動化的擴展限制為每週最多三次，系統生命週期內總計五倍。

- 如果先前的擴展在過去六小時內發生，自動化不會擴展磁碟區。

當這些規則阻止自動化採取動作時，AMS 會透過傳出服務請求與您聯絡，以決定要採取的下一個動作。

Amazon RDS 低儲存事件修復自動化

AWS Managed Services (AMS) 自動修復如何與 Amazon RDS 低儲存體事件問題搭配使用：

- 在嘗試擴展 Amazon RDS 執行個體儲存體之前，自動化會執行多項檢查，以確保 Amazon RDS 執行個體處於可修改且可用，或儲存已滿的狀態。
- 在偵測到 CloudFormation 堆疊偏離之處，修復會透過 Amazon RDS API 進行。
- 修復動作不會在下列情況下執行：
 - Amazon RDS 執行個體狀態不是「可用」或「完整儲存」。
 - Amazon RDS 執行個體儲存體目前無法修改（例如在過去六小時內修改儲存體時）。
 - Amazon RDS 執行個體已啟用自動擴展儲存。
 - Amazon RDS 執行個體不是 CloudFormation 堆疊中的資源。
- 修補限制為每六小時一次擴展，且在滾動十四天期間內不超過三次擴展。
- 當這些案例發生時，AMS 會透過傳出事件與您聯絡，以判斷下一個動作。

在 AMS 中建立其他 CloudWatch 警示

您可以使用 AWS Managed Services (AMS) 部署 | 監控和通知 | CloudWatch | 建立警示變更類型來建立新的 CloudWatch 警示。

Important

AMS 不會監控您建立的 CloudWatch 警示。

針對 Amazon EC2 執行個體使用自訂 CloudWatch 指標和警示（僅適用於不依賴部署至 Auto Scaling 群組 AMIs 的可變部署）：

1. 產生您的應用程式監控指令碼和自訂指標。如需範例指令碼的詳細資訊和存取權，請參閱[監控 Amazon EC2 Linux 執行個體的記憶體和磁碟指標](#)。Linux Amazon EC2 執行個體的 Amazon CloudWatch 監控指令碼示範如何產生和使用 Amazon CloudWatch 自訂指標。Amazon EC2 這些

- 範例 Perl 指令碼包含功能完整的範例，可報告 Linux 執行個體的記憶體、交換和磁碟空間使用率指標。
- 上傳您的監控指令碼。若要將監控指令碼上傳至 Auto Scaling 群組或 Amazon EC2 執行個體組態，您可以在設定 Auto Scaling 群組或 Amazon EC2 執行個體時使用 UserData，或者，如果您的應用程式是使用 CodeDeploy 部署，您可以使用部署 | 應用程式 | CodeDeploy 應用程式 | 部署 CT (ct-2edc3sd1sqmrb) 修改組態。
 - 將自訂指標發佈至 CloudWatch（第一次發佈新自訂指標的資料點時，即會建立），請參閱[發佈自訂指標](#)。
 - 建立 CloudWatch 警示，請參閱[建立執行個體的 CloudWatch 警示](#)。

Important

監控資料必須傳送至此路徑 **【infra/INSTANCE_ID/YOUR_CUSTOM_METRIC】**

若要修改或刪除 CloudWatch 警示，請使用 Management | Other | Other | Create change type (ct-1e1xtak34nx76) 提交 RFC，其中包含完成動作所需的參數，如 Amazon CloudWatch API 參考 [PutMetricAlarm](#) 中所述。

您可以使用 CloudWatch 事件串流。AMS 已與 CloudWatch 整合，您可以請求任何 AWS API 呼叫觸發 CloudWatch 事件。

若要這樣做，請提交管理 | 其他 | 其他 | 使用您感興趣的 API 呼叫更新 CT (ct-0xdawir96cy7k)。AMS 運算子將與您交談以收集需求。若要進一步了解，請參閱 [Amazon CloudWatch 文件](#)。

若要存取 CloudWatch 事件串流，請提交管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k)，將一方新增至 SNS 通知主題。AMS 運算子將與您交談以收集需求。

在 AMS 中建立自訂 CloudWatch 指標和警示

您可以在 Amazon CloudWatch 中存放您的業務和應用程式指標。您可以檢視圖形，並根據這些指標設定警示，就像 CloudWatch 為 AWS Managed Services (AMS) 資源存放的指標一樣。若要進一步了解 CloudWatch，請參閱 [Amazon CloudWatch 概念](#)。

Amazon SNS 允許應用程式針對發佈警示的 AMS 受管監控系統或 MMS、Amazon SNS (SNS) 主題，透過「推送」機制，將時間關鍵訊息傳送給多個訂閱者；在此情況下，為 MMS 和您的 SQS 佇列。您

可以使用 CloudWatch 來建立自訂指標，並透過 SNS 主題適當設定 AMS 警示。若要執行此操作，請遵循下列步驟。

Note

此程序不適用於依賴部署至 Auto Scaling 群組AMI的不可變部署，適用於可變應用程式（非 ASG）部署。

在 AMS Advanced 的限制內設定自訂指標是一項複雜的任務。如需 CloudWatch 的範例，請參閱[範例：計算字詞的出現次數](#)。

1. 產生您的應用程式監控指令碼和自訂指標（例如計數出現範例）。如需範例指令碼的詳細資訊和存取權，請參閱[監控 Amazon EC2 Linux 執行個體的記憶體和磁碟指標](#)。
2. 上傳您的監控指令碼。若要將監控指令碼上傳至 Auto Scaling 群組或 Amazon EC2 執行個體組態，您可以在設定 Auto Scaling 群組或 Amazon EC2 執行個體時使用 UserData，或者，如果您的應用程式是使用 CodeDeploy 部署，您可以使用部署 | 應用程式 | CodeDeploy 應用程式 | 部署 CT (ct-2edc3sd1sqmrb) 修改組態。
3. 將自訂指標發佈至 CloudWatch（第一次發佈新自訂指標的資料點時，即會建立），請參閱[發佈自訂指標](#)。
4. 若要將客戶指標與您的應用程式監控系統整合，請請求 AMS 透過使用部署 | 監控和通知 | SNS | 建立變更類型 (ct-3dfnglm4ombbs) 提交 RFC 來建立指標的 SNS 主題。
5. 建立 CloudWatch 警示，請參閱[建立 Amazon CloudWatch 警示](#)。

Important

監控資料必須傳送至此路徑 **【infra/*INSTANCE_ID*/*YOUR_CUSTOM_METRIC*】**。

在 AMS 中使用適用於 .Net 和 SQL 伺服器的 CloudWatch Application Insights

您可以使用 Amazon CloudWatch Application Insights 為您的 AWS Managed Services (AMS) 應用程式資源設定監視器，以持續分析資料是否有應用程式問題跡象，並在疑難排解應用程式問題時縮短平均修復時間 (MTTR)。如需 CloudWatch Application Insights 的詳細資訊，請參閱[適用於 .NET 和 SQL Server 的 CloudWatch Application Insights](#)。

⚠ Important

AMS 不會監控 CloudWatch Application Insights 的問題，因為它們適用於由您控制的應用程式程式碼。

若要使用 CloudWatch Application Insights，請提交 RFC 與 部署 | 進階堆疊元件 | Identity and Access Management (IAM) | 建立實體或政策（需要檢閱）變更類型 (ct-3dpd8mdd9jn1r)，並提出建立 IAM 角色的請求，以提供您設定 CloudWatch Application Insights 的許可。有兩種接收已識別問題的選項：透過 SNS 主題或在 CloudWatch Event 規則中使用目標。在 RFC 中，指定您想要的。如果您打算使用 CloudWatch Event 規則，也請在 RFC 中指定規則定義。設定 CloudWatch Application Insights 之後，您會收到潛在問題的通知，包括指向可能根本原因的洞見。

若要了解如何擔任角色，請參閱 AMS 加入指南 [將 Active Directory 與 AMS IAM 角色聯合](#)。

在 AMS 中使用 Amazon EventBridge 受管規則

AMS Advanced 使用 Amazon EventBridge 受管規則。受管規則是直接連結至 AMS 的唯一規則類型。這些規則符合傳入事件，並將其傳送至目標進行處理。受管規則由 AMS 預先定義，並包含服務管理客戶帳戶所需的事件模式，除非另有定義，否則只有擁有的服務可以利用這些受管規則。

AMS 受管規則會連結到events.managedservices.amazonaws.com服務主體。這些受管規則是透過[AWSServiceRoleForManagedServices_Events服務連結角色](#)進行管理。若要刪除這些規則，客戶需要特別確認。如需詳細資訊，請參閱[刪除 AMS 的受管規則](#)。

如需規則的詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的[規則](#)。

AMS 部署的 Amazon EventBridge 受管規則

Amazon EventBridge 受管規則

規則名稱	描述	定義
AMSAdvancedCoreRule	此規則會將 Amazon CloudWatch 警示轉送至 AMS 監控。Amazon	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"],</pre>

規則名稱	描述	定義
	CloudWatch 事件會監控 CloudWatch 警示。	<pre>} }</pre>

建立 AMS 的受管規則

您不需要手動建立 Amazon EventBridge 受管規則。當您在 AWS 管理主控台 AWS CLI、或 AWS API 中加入 AMS 時，AMS 會為您建立它們。

編輯 AMS 的受管規則

AMS 不允許您編輯受管規則。AMS 會預先定義每個受管規則的名稱和事件模式。

刪除 AMS 的受管規則

您不需要手動刪除 受管規則。當您在 AWS 管理主控台 AWS CLI、或 AWS API 中從 AMS 離職時，AMS 會為您清除資源並刪除 AMS 擁有的所有受管規則。

如果 AMS 無法在離職期間移除受管規則，您也可以使用 Amazon EventBridge 主控台、AWS CLI 或 AWS API 手動刪除受管規則。若要這樣做，您必須先從 AMS 離職，並強制刪除受管規則。

AMS 中的信任修復程式

Trusted Remediator 是一種 AWS Managed Services 解決方案，可自動修復 [AWS Trusted Advisor](#)和 [AWS Compute Optimizer](#)建議。當 Trusted Advisor 和 Compute Optimizer 指出降低成本、改善系統可用性、最佳化效能或填補安全漏洞的機會時，信任的修復程式會建立建議 AWS 帳戶。透過 Trusted Remediator，您可以透過使用已建立最佳實務的安全標準化方式，處理這些安全性、效能、成本最佳化、容錯能力和服務限制建議。Trusted Remediator 可讓您設定修復解決方案，並依照您建立的排程自動執行，簡化修復程序。這種簡化方法可以一致、有效率地解決問題，無需手動介入。

信任的修復程式主要優點

以下是信任的修復程式的主要優點：

- 改善安全性、效能和成本最佳化：信任的補救措施可協助您增強帳戶的整體安全狀態、最佳化資源使用率，以及降低營運成本。

- 自助式設定和組態：您可以設定信任的修復程式，以符合您的需求和偏好設定。
- 自動化 Trusted Advisor 檢查和 AWS Compute Optimizer 建議修復：設定之後，信任的修復程式會自動執行所選檢查的修復動作。此自動化不需要手動介入。
- 最佳實務實作：修補動作是以已建立的最佳實務為基礎，因此問題會以標準化且有效的方式解決。
- 排程執行：您可以選擇與day-to-day操作工作流程一致的修復排程。

Trusted Remediator 可讓您主動解決 AWS 環境中已識別的問題，協助您遵守最佳實務，並維護安全、高效能且符合成本效益的雲端基礎設施。

可信任修復程式的運作方式

以下是信任修復程式工作流程的圖例：

Trusted Remediator 會評估的 Trusted Advisor 和 Compute Optimizer 建議，AWS 帳戶並在 OpsCenter 中建立 AWS Systems Manager OpsItems。 [OpsItems](#) OpsCenter 然後，您可以使用信任的修復程式自動化文件自動或手動修復 OpsItems。以下是每種修復類型的詳細資訊：

- 自動化修復：信任的修復程式會執行自動化文件並監控執行。自動化文件完成後，信任的修復程式會解析 Opsitem。
- 手動修復：信任的修復程式會建立 OpsItem 供您檢閱。檢閱之後，您可以建立自動化 RFC、[信任的修復程式 | 尋找 | 修復](#)、變更類型以修復資源。如需手動修復步驟的詳細資訊，請參閱 [在信任的修復程式中執行手動修復](#)。

修復日誌存放在 Amazon S3 儲存貯體中。您可以使用 S3 儲存貯體中的資料來建置自訂 QuickSight 儀表板以進行報告。AMS 也為信任的修復程式提供隨需報告。若要接收這些報告，請聯絡您的 CSDM。

Trusted Remediator 的關鍵術語

以下是在 AMS 中使用受信任修復程式時，有助於了解的術語：

- AWS Trusted Advisor 和 AWS Compute Optimizer：AWS和 Trusted Advisor Compute Optimizer 提供的雲端最佳化服務會 AWS 檢查您的環境，並根據以下六個類別的最佳實務提供建議：
 - 成本最佳化
 - 效能
 - 安全性
 - 容錯能力

- 卓越營運
- 服務限制

如需詳細資訊，請參閱[AWS Trusted Advisor](#)及[AWS Compute Optimizer](#)。

- 信任的修復程式：適用於[Trusted Advisor](#)檢查和[AWS Compute Optimizer](#)建議的 AMS 修復解決方案。Trusted Remediator 可協助您使用已知的最佳實務安全地修復 Trusted Advisor 檢查和 Compute Optimizer 建議，以改善安全性、效能並降低成本。可信任的修復程式易於設定。您設定一次，信任的修復程式會根據您偏好的排程（每日或每週）執行修復。
- AWS Systems Manager SSM 文件：JSON 或 YAML 檔案，定義對 AWS 資源 AWS Systems Manager 執行的動作。SSM 文件可做為宣告性規格，以自動化跨多個 AWS 資源和執行個體的操作任務。
- AWS Systems Manager OpsCenter OpsItem：一種雲端操作問題管理資源，可協助您追蹤和解決環境中 AWS 的操作問題。OpsItems 為跨 和資源的操作資料和問題提供集中式檢視 AWS 服務 和管理系統。每個 OpsItem 都代表一個操作問題，例如潛在的安全風險、效能問題或操作事件。
- 組態：組態是一組儲存在 中的屬性[AWS AppConfig](#)，即 的功能 [AWS Systems Manager](#)。中的信任修復程式應用程式 AWS AppConfig 有助於在帳戶層級設定修復。
- 執行模式：執行模式是一種組態屬性，可決定如何針對每個 Trusted Advisor 檢查結果執行修復。支援四種執行模式：自動化、手動、條件式、非作用中。
- 資源覆寫：此功能使用資源標籤覆寫特定資源的組態。
- 修復項目日誌：信任的修復程式修復 S3 日誌儲存貯體中的日誌檔案。修復項目日誌會在修復 OpsItems 建立時建立。此日誌檔案包含手動執行修復 OpsItems 和自動執行修復 OpsItems。使用此日誌檔案來追蹤所有修復項目。
- 自動化修復執行日誌：信任的修復器修復 S3 日誌儲存貯體中的日誌檔案。自動執行 SSM 文件時，會建立自動修復執行日誌。此日誌包含自動執行修復 OpsItems 的 SSM 執行詳細資訊。使用此日誌檔案來追蹤自動化修復。

在 AMS 中開始使用信任的修復程式

可信任的修復程式可在 AMS 中使用，無需額外費用。Trusted Remediator 支援單一帳戶和多帳戶組態。

加入信任的修復程式

若要將您的 AMS 帳戶加入信任的修復程式，請傳送電子郵件給 Cloud Architects 或 Cloud Service Delivery Manager (CSDMs)。在電子郵件中，包含以下資訊：

- **AWS 帳戶：**12 位數帳戶識別號碼。您想要加入信任的修復程式的所有帳戶都必須屬於相同的 AMS Advanced 客戶。
- **委派管理員帳戶：**用於單一或多個帳戶的 Trusted Advisor 和 Compute Optimizer 檢查組態的帳戶。
- **成員帳戶：**這些是連結至委派管理員帳戶的帳戶。這些帳戶會從委派的管理員帳戶繼承組態。您可以有一個成員帳戶或多個成員帳戶。

Note

成員帳戶會從委派的管理員帳戶繼承組態。如果您需要特定帳戶的不同組態，請使用您偏好的組態加入多個委派管理員帳戶。在加入之前，請與您的 Cloud Architects 規劃帳戶結構和組態。

- **AWS 區域：**AWS 區域 您的資源所在的。如需的清單 AWS 區域，請參閱[AWS 服務 依區域](#)。
- **修補排程和時間：**您偏好的修補排程（每日或每週）。Trusted Remediator 會收集 Trusted Advisor 檢查並在排程時間啟動修復。例如，您可以設定每週週日凌晨 1：00 的修復排程，澳洲東部標準時間。
- **通知電子郵件：**信任的修復程式會使用通知電子郵件，在有修復時每天通知您。通知電子郵件主旨是「可信修復摘要」，內容提供過去 24 小時內執行的可信任修復的資訊。

Note

每次排定的修補後，請檢閱您的應用程式和資源。如需其他支援，請聯絡 AMS。

在您向 CA 或 CSDM 提交包含必要詳細資訊的加入請求之後，AMS 會將您的帳戶加入信任的修復程式。Trusted Remediator 使用 AWS AppConfig 的功能 AWS Systems Manager 來定義 Trusted Advisor 檢查的組態。這些組態是一組存放在其中的屬性 AWS AppConfig。為了防止您的資源產生未經授權的費用，所有支援的 Trusted Advisor 檢查都會在帳戶加入信任的修復程式時設定為非作用中。這些組態可協助您自動修復特定 Trusted Advisor 檢查，或評估和手動修復剩餘的檢查。這些組態可高度自訂，可讓您為每個 Trusted Advisor 檢查套用組態。如需詳細資訊，請參閱[在信任的修復程式中設定 Trusted Advisor 檢查修復](#)。

在 中設定信任的修復程式 AWS 帳戶

加入完成時，您的 CA 或 CSDM 會通知您，並在委派管理員中建立預設組態 AWS 帳戶。組態會存放在信任的修復程式應用程式 AWS AppConfig 下的 中。您可以使用 RFC [管理 | 信任的修復程式 | 修復](#)

[組態 | 更新](#)以請求組態更新。如需詳細資訊，請參閱[在信任的修復程式中設定 Trusted Advisor 檢查修復](#)。

若要檢視預設的可信任修復程式組態，請完成下列步驟：

1. 在 <https://console.aws.amazon.com/systems-manager/> 開啟 AWS Systems Manager 主控台。

 Note

請確定您在委派的管理員帳戶中。

2. 選擇應用程式管理、AppConfig。
3. 從應用程式清單中選取信任的修復程式。

以下是顯示受信任修復程式組態的 AWS AppConfig 主控台範例：

選擇要修復的檢查和建議

根據預設，修復執行模式對於組態中的所有 Trusted Advisor 檢查和 Compute Optimizer 建議都是非作用中的。這可防止未經授權的修復並保護資源。AMS 提供精選的 SSM 自動化文件，用於 Trusted Advisor 檢查修復。

若要選取您想要使用信任的修復程式修復的檢查，請完成下列步驟：

1. 檢閱支援的 [Trusted Advisor 和 Compute Optimizer 建議清單或相關聯的 SSM 自動化文件名稱](#)，以決定您要使用信任的修復程式修復哪些檢查和建議。
2. 提交[管理 | 信任的修復程式 | 修復組態 | 更新](#)請求以更新所選 Trusted Advisor 檢查的組態。如需如何選取檢查的指示，請參閱 [在信任的修復程式中設定 Trusted Advisor 檢查修復](#)。

在信任的修復程式中追蹤您的修復

在您更新帳戶層級組態之後，信任的修復程式會為每個修復建立 OpsItems。Trusted Remediator 會執行 SSM 文件，以根據您的修復排程自動修復 OpsItems。如需如何從 Systems Manager OpsCenter 主控台檢視所有修復 OpsItems 的說明，請參閱 [在信任的修復程式中追蹤修復](#)。OpsCenter

在信任的修復程式中執行手動修復

您可以使用自動 RFC 手動修復 Trusted Advisor 檢查。當您選擇手動修復時，信任的修復程式會建立手動執行 OpsItem。如需詳細資訊，請參閱[在信任的修復程式中執行手動修復](#)。

受信任修復程式支援的 Compute Optimizer 建議

下表列出支援的 Compute Optimizer 建議、SSM 自動化文件、預先設定的參數，以及自動化文件的預期結果。在啟用 SSM 自動化文件進行檢查修復之前，請檢閱預期成果，以協助您根據您的業務需求了解可能的風險。

對於您要啟用修復的支援檢查，請確定每個 Compute Optimizer 檢查的對應組態規則都存在。如需詳細資訊，請參閱[選擇 AWS Compute Optimizer 接受 Trusted Advisor 檢查](#)。

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
精簡化		
Amazon EC2 執行個體建議	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation 根據 Compute Optimizer 建議更新 Amazon EC2 執行個體類型。如果選項存在，則會選擇最佳選項，同時維護相同的平台參數（架構、Hypervisor、網路介面、虛擬化類型等）。	- MinimumDaysSinceLastChange：指定自上次執行個體類型變更以來最短天數的參數。預設值是 7 天。 無限制條件 - CreateAMIBeforeResize：若要在調整大小之前將執行個體 AMI 建立為備份，請將設定為 'True'。若要不建立備份，請將設定為 'False'。預設為 'True'。 無限制條件
Amazon EBS 磁碟區建議	AWSManagedServices-ModifyEBSVolume Amazon EBS 磁碟區會根據 Compute Optimizer 建議進行修改。修改可能包括磁碟區類型、大小、IOPS、磁碟區產生 (gp2、gp3 等)。	CreateSnapshot：若要在修改磁碟區之前建立快照，請將設定為 'True'。若要不建立快照，請將設定為 'False'。預設值為 'True'。 無限制條件

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
		- VolumeType：所需的磁碟區類型。如果未指定類型，則會保留現有類型。 無限制條件 - VolumeSize：磁碟區所需的大小，以 GiB 為單位。目標磁碟區大小必須大於或等於磁碟區的現有大小。如果未指定大小，則會保留現有的大小。 無限制條件 - lops：每秒請求的 I/O 操作數 (IOPS)。此參數僅適用於 io1、io2 和 gp3 磁碟區。 無限制條件 - 輸送量：為磁碟區佈建的輸送量，上限為 1000 MiB/s。此參數僅適用於 gp3 磁碟區。 無限制條件 - RemediateStackDrift：若要啟動偏離修復，如果任何偏離是由磁碟區修改造成，請將 設為 'True'。若要不嘗試漂移修復，請將 設定為 'False'。預設為 'True'。 無限制條件
Lambda 函數建議	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda 根據 Compute Optimizer 建議最佳化 函數記憶體。	RecommendedMemorySize：如果與建議選項不同，則為自訂記憶體大小。 無限制條件

最佳化選項	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
閒置資源		
閒置 Amazon EBS 磁碟區	AWSManagedServices-DeleteUnusedEBSVolume 未連接的 Amazon EBS 磁碟區將被刪除。	• CreateSnapshot：若要在刪除磁碟區之前建立快照，請將設為 'True'。若要不建立快照，請將設定為 'False'。預設值為 'True'。 無限制條件 • MinimumUnattachedDays：要刪除的 Amazon EBS 磁碟區未連接天數下限，最長可達 62 天。預設為 7。 無限制條件
閒置 Amazon EC2 執行個體	AWSManagedServices-StopEC2Instance 閒置的 Amazon EC2 執行個體將會停止。	ForceStopWithInstanceStore：若要針對使用執行個體存放區的執行個體強制停止，請將設為 'True'。若要不強制停止，請將設為 'False'。預設值 'False' 可防止執行個體停止。 無限制條件
閒置 Amazon RDS 執行個體	AWSManagedServices-StopIdleRDSInstance 停止閒置的 Amazon RDS 執行個體。支援的引擎包括：MariaDB、Microsoft SQL Server、MySQL、Oracle、PostgreSQL。本文件不適用於 Aurora MySQL 和 Aurora PostgreSQL。執行個體最多會停止 7 天，並自動重新啟動。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的檢查

下表列出支援的 Trusted Advisor 檢查、SSM 自動化文件、預先設定的參數，以及自動化文件的預期結果。在啟用 SSM 自動化文件進行檢查修復之前，請檢閱預期成果，以協助您根據您的業務需求了解可能的風險。

請確定您要啟用修復之支援檢查的每個 Trusted Advisor 檢查都有對應的組態規則。如需詳細資訊，請參閱[檢視 支援的 AWS Trusted Advisor 檢查 AWS Config](#)。如果檢查有對應的 AWS Security Hub 控制項，請確定 Security Hub 控制項已啟用。如需詳細資訊，請參閱在[Security Hub 中啟用控制項](#)。如需管理預先設定參數的資訊，請參閱[在信任的修復程式中設定 Trusted Advisor 檢查修復](#)。

Trusted Advisor Trusted Remediator 支援的成本最佳化檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Z4AUBRNSmz 無關聯彈性 IP 地址	AWSManagedServices-TrustedRemediatorReleaseElasticIP 釋出與任何資源無關的彈性 IP 地址。	不允許預先設定的參數。 無限制條件
c18d2gz150 - Amazon EC2 執行個體已停止	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - Amazon EC2 執行個體已停止幾天。	• CreateAMIBeforeTermination：若要在終止 Amazon EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 true。若要在終止之前不建立備份，請選擇 false。預設值為 true。 • AllowedDays：執行個體在終止前處於停止狀態的天數。預設值為 30。 無限制條件
c18d2gz128 未設定生命週期政策的 Amazon ECR 儲存庫	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 如果生命週期政策尚未存在，請為指定的儲存庫建立生命週期政策。	ImageAgeLimit：Amazon ECR 儲存庫中「任何」映像的最大存留期限限制，以天 (1-365) 為單位。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
DAvU99Dc4C 利用率過低的 Amazon EBS 磁碟區	AWSManagedServices-DeleteUnusedEBSVolume 如果過去 7 天內未連接磁碟區，則刪除未充分利用的 Amazon EBS 磁碟區。預設會建立 Amazon EBS 快照。	• CreateSnapshot：如果設定為 true，則自動化會在刪除之前建立 Amazon EBS 磁碟區的快照。預設設定為 true。有效值為 true 和 false（區分大小寫）。 • MinimumUnattachedDays：EBS 磁碟區的刪除未連接天數下限，最長可達 62 天。如果設定為 0，則 SSM 文件不會檢查未連接的期間，如果磁碟區目前未連接，則刪除磁碟區。預設值為 7。 無限制條件
hjLMh88uM8 閒置負載平衡器	AWSManagedServices-DeleteIdleClassicLoadBalancer 如果閒置的 Classic Load Balancer 未使用且未註冊任何執行個體，則會將其刪除。	IdleLoadBalancerDays：Classic Load Balancer 在考慮閒置之前有 0 個請求連線的天數。預設值為七天。 如果啟用自動執行，如果沒有作用中的後端執行個體，自動化會刪除閒置的 Classic Load Balancer。對於具有作用中後端執行個體但沒有運作狀態良好的後端執行個體的所有閒置 Classic Load Balancer，不會使用自動修復，並會建立用於手動修復 OpsItems。
Ti39halfu8 Amazon RDS 閒置資料庫執行個體	AWSManagedServices-StopIdleRDSInstance 過去七天處於閒置狀態的 Amazon RDS 資料庫執行個體會停止。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
COr6dfpM05 AWS Lambda 記憶體大小過度佈建的函數	AWSManagedServices-ResizeLambdaMemory AWS Lambda 函數的記憶體大小會調整為 提供的建議記憶體大小 Trusted Advisor。	RecommendedMemorySize : Lambda 函數的建議記憶體配置。值範圍介於 128 和 10240 之間。 如果在自動化執行之前修改 Lambda 函數大小，則此自動化可能會以 建議的值覆寫設定 Trusted Advisor。
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-StopEC2Instance (自動和手動執行模式的預設 SSM 文件)。 低使用率的 Amazon EC2 執行個體會停止。	ForceStopWithInstanceStore : 設定為 true 以使用執行個體存放區強制停止執行個體。否則，請設定為 false。的預設值false可防止執行個體停止。有效值為 true 或 false (區分大小寫)。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 執行個體的大小會由相同執行個體系列類型的一個執行個體類型縮減。執行個體會在調整大小操作期間停止和啟動，並在 SSM 文件執行完成後回到初始狀態。此自動化不支援調整 Auto Scaling 群組中的執行個體大小。	- MinimumDaysSinceLastChange：自上次執行個體類型變更以來的天數下限。如果在指定的時間內修改執行個體類型，則不會變更執行個體類型。使用 0 略過此驗證。預設值為 7。 - CreateAMIBeforeResize：若要在調整大小之前建立執行個體 AMI 做為備份，請選擇 true。若要不建立備份，請選擇 false。預設值為 false。有效值為 true 和 false (區分大小寫)。 - ResizeIfStopped：若要繼續變更執行個體大小，即使執行個體處於停止狀態，請選擇 true。如果執行個體處於停止狀態，若要不自動調整其大小，請選擇 false。有效值為 true 和 false (區分大小寫)。 無限制條件
Qch7DwouX1 Amazon EC2 執行個體低使用率	AWSManagedServices-TerminateInstance 如果不屬於 Auto Scaling 群組，且未啟用終止保護，則會終止低使用率的 Amazon EC2 執行個體。預設會建立 AMI。	CreateAMIBeforeTermination：將此選項設定為 true 或 false，以在終止 EC2 執行個體之前建立執行個體 AMI 做為備份。預設值為 true。有效值為 true 和 false (區分大小寫)。 無限制條件
G31sQ1E9U 利用率過低的 Amazon Redshift 叢集	AWSManagedServices-PauseRedshiftCluster Amazon Redshift 叢集已暫停。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1cj39rr6v Amazon S3 不完整的分段上傳中止組態	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 儲存貯體已設定生命週期規則，以中止在特定天後仍未完成的分段上傳。	DaysAfterInitiation : Amazon S3 停止未完成分段上傳的天數。預設值設定為 7 天。 無限制條件
c1z7kmr00n 執行個體的 Amazon EC2 成本最佳化建議	使用 Amazon EC2 執行個體建議和來自的閒置 Amazon EC2 執行個體 受信任修復程式支援的 Compute Optimizer 建議 。	不允許預先設定的參數。 無限制條件
c1z7kmr02n 磁碟區的 Amazon EBS 成本最佳化建議	使用 Amazon EBS 磁碟區建議和來自的閒置 Amazon EBS 磁碟區 受信任修復程式支援的 Compute Optimizer 建議 。	不允許預先設定的參數。 無限制條件
c1z7kmr03n 資料庫執行個體的 Amazon RDS 成本最佳化建議	從使用閒置 Amazon RDS 執行個體 受信任修復程式支援的 Compute Optimizer 建議 。	不允許預先設定的參數。 無限制條件
c1z7kmr05n AWS Lambda 函數的成本最佳化建議	使用來自的 Lambda 函數建議 受信任修復程式支援的 Compute Optimizer 建議 。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的安全檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
12Fnkpl8Y5 存取金鑰已暴露	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 公開的 IAM 存取金鑰已停用。	不允許預先設定的參數。 使用公開的 IAM 存取金鑰設定的應用程式無法驗證。
Hs4Ma3G127 - 應啟用 API Gateway REST 和 WebSocket API 執行記錄 對應的 AWS Security Hub 檢查： APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging 執行記錄會在 API 階段上啟用。	LogLevel：記錄層級以啟用執行記錄，ERROR - 僅針對錯誤啟用記錄。INFO- 為所有事件啟用記錄。 您必須授予 API Gateway 許可，以讀取和寫入您帳戶的日誌至 CloudWatch，以啟用執行日誌，請參閱在 API Gateway 中設定 REST APIs 的 CloudWatch 日誌 記錄以取得詳細資訊。
Hs4Ma3G129 - API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤 對應的 AWS Security Hub 檢查： APIGateway.3	AWSManagedServices-EnableAPIGatewayXRayTracing 在 API 階段上啟用 X-Ray 追蹤。	不允許預先設定的參數。 無限制條件
Hs4Ma3G202 - API Gateway REST API 快取資料應靜態加密 對應的 AWS Security Hub 檢查	AWSManagedServices-EnableAPIGatewayCacheEncryption 如果 API Gateway REST API 階段已啟用快取，請啟用 API Gateway REST API 快取資料的靜態加密。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
查：APIGateway.5 Hs4Ma3G177 - 對應的 AWS Security Hub 檢查 - 與負載平衡器相關聯的自動擴展群組應使用負載平衡器運作狀態檢查 AutoScaling.1	AWSManagedServices-TrustedRolemediatorEnableAutoScalingGroupELBHealthCheck Auto Scaling 群組已啟用 Elastic Load Balancing 運作狀態檢查。	HealthCheckGracePeriod：Auto Scaling 在檢查已開始服務的 Amazon Elastic Compute Cloud 執行個體的運作狀態之前等待的時間，以秒為單位。 如果連接到 Auto Elastic Load Balancing 群組的任何 Elastic Load Balancing 負載平衡器回報運作狀態不佳，開啟 Elastic Load Balancing 運作狀態檢查可能會導致取代執行中的執行個體。Auto Scaling 如需詳細資訊，請參閱將 Elastic Load Balancing 負載平衡器連接至 Auto Scaling 群組
Hs4Ma3G245 - AWS CloudFormation 堆疊應與 Amazon Simple Notification Service 整合 對應的 AWS Security Hub 檢查：CloudFormation.1	AWSManagedServices-EnableCFNStackNotification 將 CloudFormation 堆疊與 Amazon SNS 主題建立關聯以進行通知。	NotificationARNs：要與所選 CloudFormation 堆疊建立關聯的 Amazon SNS 主題 ARNs。 若要啟用自動修復，必須提供 NotificationARNs 預先設定的參數。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G210 - CloudFront 分佈應該已啟用記錄 對應的 AWS Security Hub 檢查：CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging Amazon CloudFront 分佈已啟用記錄功能。	• BucketName：您要存放存取日誌的 Amazon S3 儲存貯體名稱。 • S3KeyPrefix：theAmazonCloudFront 分發日誌 S3 儲存貯體中位置的字首。 • IncludeCookies：指出是否要在存取日誌中包含 Cookie。 若要啟用自動修復，必須提供下列預先設定的參數： • BucketName • S3KeyPrefix • IncludeCookies 如需此修復限制，請參閱如何開啟 CloudFront 分佈的記錄功能？
Hs4Ma3G109 - 應啟用 CloudTrail 日誌檔案驗證 對應的 AWS Security Hub 檢查：CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLoggingValidation 啟用 CloudTrail 追蹤日誌驗證。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G108 - CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合 對應的 AWS Security Hub 檢查：CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 已與 CloudWatch Logs 整合。	- CloudWatchLogsLogGroupName：交付 CloudTrail 日誌的 CloudWatch Logs 日誌群組名稱。CloudTrail 您必須使用帳戶中存在的日誌群組。 - CloudWatchLogsRoleName：CloudWatch Logs 端點的 IAM 角色名稱，以假設寫入使用者的日誌群組。您必須使用帳戶中存在的角色。 若要啟用自動修復，必須提供下列預先設定的參數： - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName
Hs4Ma3G217 - CodeBuild 專案環境應具有記錄 AWS 組態 對應的 AWS Security Hub 檢查：CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig 啟用 CodeBuild 專案的記錄。	不允許預先設定的參數。 無限制條件
Hs4Ma3G306 - Neptune 資料庫叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot 從 Amazon DocumentDB 手動叢集快照移除公有存取權。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G308 - Amazon DocumentDB 叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：DocumentDB B.5	AWSManagedServices-TrustedR emediatorEnableDocumentDBClusterDeletionProtection 啟用 Amazon DocumentDB 叢集的刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G323 - DynamoDB 資料表應該啟用刪除保護 對應的 AWS Security Hub 檢查：DynamoDB.6	AWSManagedServices-TrustedR emediatorEnableDynamoDBTableDeletionProtection 啟用非 AMS DynamoDB 資料表的刪除保護。	不允許預先設定的參數。 無限制條件
ePs02jT06w - Amazon EBS 公有快照	AWSManagedServices-TrustedR emediatorDisablePublicAccessOnEBSSnapshot Amazon EBS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G118 - VPC 預設安全群組不應允許傳入或傳出流量 對應的 AWS Security Hub 檢查：EC2.2	AWSManagedServices-TrustedR emediatorRemoveAllRulesFromDefaultSG 預設安全群組中的所有輸入和輸出規則都會移除。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G117 - 連接的 EBS 磁碟區應該靜態加密 對應的 AWS Security Hub 檢查：EC2.3	AWSManagedServices-EncryptInstanceVolume 執行個體上連接的 Amazon EBS 磁碟區已加密。	- KMSKeyId：AWS KMS key ID 或 ARN 來加密磁碟區。 - DeleteStaleNonEncryptedSnapshotBackups：決定是否應刪除舊未加密磁碟區的快照備份的旗標。 作為修復的一部分，執行個體會重新啟動，如果 DeleteStaleNonEncryptedSnapshotBackups 設定為 false，則復原可以協助還原。
Hs4Ma3G120 - 在指定時段後應移除已停止的 EC2 執行個體 對應的 AWS Security Hub 檢查：EC2.4	AWSManagedServices-TerminateInstance（自動和手動執行模式的預設 SSM 文件） Amazon EC2 執行個體已停止 30 天。	CreateAMIBeforeTermination：。若要在終止 EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 true。若要在終止之前不建立備份，請選擇 false。預設值為 true。 無限制條件
Hs4Ma3G120 - 在指定時段後應移除已停止的 EC2 執行個體 對應的 AWS Security Hub 檢查：EC2.4	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - 在 Security Hub 中定義的天數內停止的 Amazon EC2 執行個體（預設值為 30）會終止。	CreateAMIBeforeTermination：若要在終止 EC2 執行個體之前建立執行個體 AMI 做為備份，請選擇 true。若要在終止之前不建立備份，請選擇 false。預設值為 true。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G121 - 應啟用 EBS 預設加密 對應的 AWS Security Hub 檢查：EC2.7	AWSManagedServices-EncryptEBSByDefault Amazon EBS 加密預設為針對特定 啟用 AWS 區域	不允許預先設定的參數。 預設加密是區域特有設定。如果您為區域啟用此功能，則無法針對該區域中的個別磁碟區或快照停用此功能。
Hs4Ma3G124 - Amazon EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2) 對應的 AWS Security Hub 檢查：EC2.8	AWSManagedServices-TrustedRemediatorEnableEC2InstanceIMDSv2 Amazon EC2 執行個體使用執行個體中繼資料服務第 2 版 (IMDSv2)。	- IMDSv1MetricCheckPeriod：在 CloudWatch 中分析 IMDSv1 用量指標的天數 (42-455)。如果 Amazon EC2 執行個體是在指定的期間內建立，則分析會從執行個體的建立日期開始。 - HttpPutResponseHopLimit：執行個體中繼資料字符允許的網路跳轉數目上限。此值可在 1 和 2 躍點之間設定。的跳轉限制會將字符存取 1 限制為直接在執行個體上執行的程序，而 的跳轉限制則 2 允許從執行個體上執行的容器存取。 無限制條件
Hs4Ma3G207 - EC2 子網路不應自動指派公有 IP 地址 對應的 AWS Security Hub 檢查：EC2.15	AWSManagedServices-UpdateAutoAssignPublicIPv4Addresses VPC 子網路設定為不會自動指派公有 IP 地址。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G209 - 移除未使用的網路存取控制清單 對應的 AWS Security Hub 檢查：EC2.16	AWSManagedServices-DeleteUnusedNACL 刪除未使用的網路 ACL	不允許預先設定的參數。 無限制條件
Hs4Ma3G215 - 應移除未使用的 Amazon EC2 安全群組 對應的 AWS Security Hub 檢查：EC2.22	AWSManagedServices-DeleteSecurityGroups 刪除未使用的安全群組。	不允許預先設定的參數。 無限制條件
Hs4Ma3G247 - Amazon EC2 Transit Gateway 不應自動接受 VPC 連接請求 對應的 AWS Security Hub 檢查：EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach - 停用自動接受指定非 AMS Amazon EC2 Transit Gateway 的 VPC 連接請求。	不允許預先設定的參數。 無限制條件
Hs4Ma3G235 - ECR 私有儲存庫應設定標籤不可變性 對應的 AWS Security Hub 檢查：ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability 將指定儲存庫的影像標籤可變性設定設定為 IMMUTABLE。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G216 - ECR 儲存庫應至少設定一個生命週期政策 對應的 AWS Security Hub 檢查：ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 儲存庫已設定生命週期政策。	LifecyclePolicyText：要套用至儲存庫的 JSON 儲存庫政策文字。 若要啟用自動修復，必須提供下列預先設定的參數： LifecyclePolicyText
Hs4Ma3G325 - EKS 叢集應該啟用稽核記錄 對應的 AWS Security Hub 檢查：EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog EKS 叢集已啟用稽核日誌。	不允許預先設定的參數。 無限制條件
Hs4Ma3G183 - 應用程式負載平衡器應設定為捨棄 HTTP 標頭 對應的 AWS Security Hub 檢查：ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer 設定為無效的標頭欄位。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G18 4 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄 對應的 AWS Security Hub 檢 查：ELB.5	AWSManagedServices-EnableELBLogging (自動和手動執行模式的預設 SSM 文件) Application Load Balancer 和 Classic Load Balancer 記錄已啟用。	• BucketName：儲存貯體名稱 (非 ARN)。請確定儲存貯體政策已正確設定以供記錄。 • S3KeyPrefix：Elastic Load Balancing 日誌的 Amazon S3 儲存貯體中位置的字首。 若要啟用自動修復，必須提供下列預先設定的參數： • BucketName • S3KeyPrefix Amazon S3 儲存貯體必須有儲存貯體政策，授予 Elastic Load Balancing 將存取日誌寫入儲存貯體的許可。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G18 4 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄 對應的 AWS Security Hub 檢 查：ELB.5	AWSManagedServices-EnableELBLoggingV2 Application Load Balancer 和 Classic Load Balancer 記錄已啟用。	- TargetBucketTagKey：用於識別目標 Amazon S3 儲存貯體的標籤名稱（區分大小寫）。將此與 搭配使用TargetBucketTagValue，以標記將做為存取記錄目的地儲存貯體的儲存貯體。 - TargetBucketTagValue：用於識別目標 Amazon S3 儲存貯體的標籤值（區分大小寫）。將此與 搭配使用TargetBucketTagKey，以標記將做為存取記錄目的地儲存貯體的儲存貯體。 - S3BucketPrefix：Amazon S3 儲存貯體的字首（邏輯階層）。您指定的字首不得包含字串 AWSLogs。如需詳細資訊，請參閱使用字首組織物件。 若要啟用自動修復，必須提供下列預先設定的參數： - TargetBucketTagKey - TargetBucketTagValue - S3BucketPrefix Amazon S3 儲存貯體必須有儲存貯體政策，授予 Elastic Load Balancing 將存取日誌寫入儲存貯體的許可。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G326 - 應啟用 Amazon EMR 封鎖公開存取設定 對應的 AWS Security Hub 檢查：EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess 帳戶已開啟 Amazon EMR 封鎖公開存取設定。	不允許預先設定的參數。 無限制條件
Hs4Ma3G135 - AWS KMS 金鑰不應意外刪除 對應的 AWS Security Hub 檢查：KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 金鑰刪除已取消。	不允許預先設定的參數。 無限制條件
Hs4Ma3G299 - Amazon DocumentDB 手動叢集快照不應公開 對應的 AWS Security Hub 檢查：Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection 啟用 Amazon Neptune 叢集的刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G319 - Network Firewall 防火牆應該已啟用刪除保護 對應 AWS Security Hub 檢查：NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection - 啟用 AWS Network Firewall 的刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G223 - OpenSearch 網域應該加密節點之間傳送的資料 對應的 AWS Security Hub 檢查：OpenSearch.h.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 網域已啟用節點對節點加密。	不允許預先設定的參數。 啟用node-to-node加密後，您無法停用設定。反之，請手動擷取加密網域的快照、建立另一個網域、遷移您的資料，然後刪除舊網域。
Hs4Ma3G222 - 應啟用記錄至 CloudWatch Logs 的 OpenSearch 網域錯誤 對應的 AWS Security Hub 檢查：Opensearch.h.4	AWSManagedServices-EnableOpenSearchLogging OpenSearch 網域已啟用錯誤記錄。	CloudWatchLogGroupArn：anAmazon CloudWatch Logs 日誌群組的 ARN。 若要啟用自動修復，必須提供下列預先設定的參數：CloudWatchLogGroupArn。 Amazon CloudWatch 資源政策必須設定許可。如需詳細資訊，請參閱《Amazon OpenSearch Service 使用者指南》中的啟用稽核日誌
Hs4Ma3G221 - OpenSearch 網域應該啟用稽核記錄 對應的 AWS Security Hub 檢查：Opensearch.h.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 網域設定為啟用稽核記錄。	CloudWatchLogGroupArn：要發佈日誌的 CloudWatch Logs 群組 ARN。 若要啟用自動修復，必須提供下列預先設定的參數：CloudWatchLogGroupArn Amazon CloudWatch 資源政策必須設定許可。如需詳細資訊，請參閱《Amazon OpenSearch Service 使用者指南》中的啟用稽核日誌

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G220 - 應使用 TLS 1.2 加密與 OpenSearch 網域的連線 對應的 AWS Security Hub 檢查：Opensearch.h.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 政策設定為 `Policy-Min-TLS-1-2-2019-07`，且僅允許透過 HTTPS (TLS) 的加密連線。	不允許預先設定的參數。 使用 TLS 1.2 需要連線至 OpenSearch 網域。加密傳輸中的資料可能會影響效能。使用此功能測試您的應用程式，以了解效能描述檔和 TLS 的影響。
Hs4Ma3G194 - Amazon RDS 快照應為私有 對應的 AWS Security Hub 檢查：RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G192 - RDS 資料庫執行個體應禁止公開存取，如 PubliclyAccessible AWS 組態所決定 對應的 AWS Security Hub 檢查：RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance 在 RDS 資料庫執行個體上停用公有存取。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G189 - 針對 Amazon RDS 資料庫執行個體設定增強型監控 對應的 AWS Security Hub 檢查：RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring 啟用 Amazon RDS 資料庫執行個體的增強型監控	- MonitoringInterval：針對資料庫執行個體收集增強型監控指標的點之間的間隔，以秒為單位。有效間隔為 0、1、5、10、15、30 和 60。若要停用收集增強型監控指標，請指定 0。 - MonitoringRoleName：允許 Amazon RDS 將增強型監控指標傳送至 Amazon CloudWatch Logs 的 IAM 角色名稱。如果未指定角色，則會 rds-monitoring-role 使用或建立預設角色，如果該角色不存在。 如果在自動化執行之前啟用增強型監控，則此自動化可能會使用預先設定參數中設定的 MonitoringInterval 和 MonitoringRoleName 值來覆寫設定。
Hs4Ma3G190 - Amazon RDS 叢集應該啟用刪除保護 對應的 AWS Security Hub 檢查：RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 叢集已啟用刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G198 - Amazon RDS 資料庫執行個體應啟用刪除保護 對應的 AWS Security Hub 檢查：RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 執行個體已啟用刪除保護。	不允許預先設定的參數。 無限制條件
Hs4Ma3G199 - RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs 對應的 AWS Security Hub 檢查：RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports 已針對 RDS 資料庫執行個體或 RDS 資料庫叢集啟用 RDS 日誌匯出。	不允許預先設定的參數。 服務連結角色 AWSServiceRoleForRDS 為必要項目。
Hs4Ma3G160 - 應為 RDS 執行個體設定 IAM 身分驗證 對應的 AWS Security Hub 檢查：RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management 已為 RDS 執行個體啟用身分驗證。	ApplyImmediately：指出是否盡快非同步套用此請求中的修改和任何待定修改，若要立即套用變更，請選擇 true。若要排程下一個維護時段的變更，請選擇 false。 無限制條件
Hs4Ma3G161 - 應為 RDS 叢集設定 IAM 身分驗證 對應的 AWS Security Hub 檢查：RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication RDS 叢集已啟用 IAM 身分驗證。	ApplyImmediately：指出此請求中的修改和任何待定修改是否以非同步方式盡快套用，若要立即套用變更，請選擇 true。若要排程下一個維護時段的變更，請選擇 false。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G162 - 應啟用 RDS 自動次要版本升級 對應的 AWS Security Hub 檢查：RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS 的自動次要版本升級組態已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於 available 狀態，才能進行此修復。
Hs4Ma3G163 - RDS 資料庫叢集應設定為將標籤複製到快照 對應的 AWS Security Hub 檢查：RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagToSnapshot Amazon RDS 叢集的設定已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於可用狀態，才能進行此修復。
Hs4Ma3G164 - RDS 資料庫執行個體應設定為將標籤複製到快照 對應的 AWS Security Hub 檢查：RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot Amazon RDS 的設定已啟用。	不允許預先設定的參數。 Amazon RDS 執行個體必須處於可用狀態，才能進行此修復。
rSs93HQwa1 Amazon RDS 公有快照	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公開存取已停用。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G103 - Amazon Redshift 叢集應禁止公開存取 對應的 AWS Security Hub 檢查：Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Amazon Redshift 叢集上的公開存取已停用。	不允許預先設定的參數。 停用公有存取會封鎖來自網際網路的所有用戶端。而且 Amazon Redshift 叢集處於修改狀態幾分鐘，而修復會停用叢集上的公有存取。
Hs4Ma3G106 - Amazon Redshift 叢集應該啟用稽核記錄 對應的 AWS Security Hub 檢查：Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging 稽核記錄會在維護時段期間啟用到您的 Amazon Redshift 叢集。	不允許預先設定的參數。 若要啟用自動修復，必須提供下列預先設定的參數。 BucketName：儲存貯體必須位於相同的中 AWS 區域。叢集必須具有讀取儲存貯體並放置物件許可。 如果在自動化執行之前啟用 Redshift 叢集記錄，則記錄設定可能會由此自動化覆寫，並在預先設定的參數中設定 BucketName 和 S3KeyPrefix 值。
Hs4Ma3G105 - Amazon Redshift 應已啟用自動升級至主要版本 對應的 AWS Security Hub 檢查：Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade - 主要版本升級會在維護時段期間自動套用至叢集。Amazon Redshift 叢集不會立即停機，但如果升級到主要版本，您的 Amazon Redshift 叢集可能會在維護時段期間停機。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G104 - Amazon Redshift 叢集應使用增強型 VPC 路由 對應的 AWS Security Hub 檢查：Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Amazon Redshift 叢集已啟用增強型 VPC 路由。	不允許預先設定的參數。 無限制條件
Hs4Ma3G173 - 應在儲存貯體層級啟用 S3 封鎖公開存取設定 對應的 AWS Security Hub 檢查：S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 儲存貯體層級的公有存取區塊會套用至 Amazon S3 儲存貯體。	不允許預先設定的參數。 此修復可能會影響 S3 物件可用性。如需 Amazon S3 如何評估存取權的資訊，請參閱封鎖對 Amazon S3 儲存體的公開存取權。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G230 - 應啟用 S3 儲存貯體伺服器存取記錄 對應的 AWS Security Hub 檢查：S3.9	AWSManagedServices-EnableBucketAccessLogging (自動和手動執行模式的預設 SSM 文件) Amazon S3 伺服器存取記錄已啟用。	- TargetBucket：儲存伺服器存取日誌的 S3 儲存貯體名稱。 - TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式 (值區分大小寫)。若要針對日誌物件使用 S3 金鑰的簡單格式，請選擇 SimplePrefix。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 PartitionedPrefixEventTime。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 PartitionedPrefixDeliveryTime。有效值為 SimplePrefix、PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime。 若要啟用自動修復，必須提供下列預先設定的參數：TargetBucket。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G230 – 應啟用 S3 儲存貯體伺服器存取記錄 對應的 AWS Security Hub 檢查：S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccess LoggingV2 - 已啟用 Amazon S3 儲存貯體記錄。	- TargetBucketTagKey：用於識別目標儲存貯體的標籤名稱（區分大小寫）。使用此和 TargetBucketTagValue 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 - TargetBucketTagValue：用於識別目標儲存貯體的標籤值（區分大小寫），請使用此值和 TargetBucketTagKey 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 - TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式（值區分大小寫）：若要將 S3 金鑰的簡單格式用於日誌物件，請選擇 SimplePrefix。若要將分割 S3 金鑰用於日誌物件，並將 EventTime 用於分割字首，請選擇 PartitionedPrefixEventTime。若要將分割 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割字首，請選擇 PartitionedPrefixDeliveryTime。預設值為 PartitionedPrefixEventTime。 若要啟用自動修復，必須提供下列參數：TargetBucketTagKey 和 TargetBucketTagValue。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Pfx0RwqBli Amazon S3 儲存貯體許可	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 封鎖公有存取權	不允許預先設定的參數。 此檢查包含多個提醒條件。此自動化可修復公有存取問題。不支援修復 Trusted Advisor 標記的其他組態問題。此修復支援修復 AWS 服務已建立的 S3 儲存貯體（例如 cf-templates-0000000000000）。
Hs4Ma3G272 - 使用者不應具有 SageMaker 筆記本執行個體的根存取權 對應的 AWS Security Hub 檢查： SageMaker .3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess SageMaker 筆記本執行個體已停用使用者的根存取權。	不允許預先設定的參數。 如果 SageMaker 筆記本執行個體處於 InService 狀態，則此修復會導致中斷。
Hs4Ma3G179 - SNS 主題應使用靜態加密 AWS KMS 對應的 AWS Security Hub 檢查： SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest SNS 主題是以伺服器端加密設定。	KmsKeyId：Amazon SNS 的 AWS 受管客戶主金鑰 (CMK) 或自訂 CMK 的 ID，用於伺服器端加密 (SSE)。預設值設為 alias/aws/sns。 如果使用自訂 AWS KMS 金鑰，則必須設定正確的許可。如需詳細資訊，請參閱 啟用 Amazon SNS 主題的伺服器端加密 (SSE)

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
Hs4Ma3G158 - SSM 文件不應公開 對應的 AWS Security Hub 檢查：SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing - 停用 SSM 文件的公開共用。	不允許預先設定的參數。 無限制條件
Hs4Ma3G136 - Amazon SQS 佇列應靜態加密 對應的 AWS Security Hub 檢查：SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Amazon SQS 中的訊息會加密。	• SqsManagedSseEnabled：設定為 true 以使用 Amazon SQS 擁有的加密金鑰啟用伺服器端佇列加密，設定為 false 以使用 AWS KMS 金鑰啟用伺服器端佇列加密。 • KMSKeyId：Amazon SQS 的 AWS 受管客戶主金鑰 (CMK) 或自訂 CMK 的 ID 或別名，用於佇列的伺服器端加密。如果未提供，則會使用 alias/aws/sqs。 • KmsDataKeyReusePeriodSeconds：Amazon SQS 可以在 AWS KMS 再次呼叫之前重複使用資料金鑰來加密或解密訊息的時間長度，以秒為單位。代表秒數的整數，介於 60 秒 (1 分鐘) 和 86,400 秒 (24 小時) 之間。如果 SqsManagedSseEnabled 設定為 true，則會忽略此設定。 對加密佇列的匿名 SendMessage 和 ReceiveMessage 請求會遭到拒絕。所有對啟用 SSE 之佇列的請求都必須使用 HTTPS 和簽章版本 4。

Trusted Advisor Trusted Remediator 支援的容錯能力檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz138 Amazon DynamoDB 時間 點復原	AWSManagedServices-TrustedRemediatorEnableDDBPITR 啟用 DynamoDB 資料表的 point-in-time 復原。	不允許預先設定的參數。 無限制條件
R365s2Qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Amazon S3 儲存貯體版本控制已啟用。	不允許預先設定的參數。 此修復不支援修復 AWS 服務已建立的 S3 儲存貯體（例如 cf-templates-0000000000000）。
BueAdJ7NrP Simple Storage Service (Amazon S3) 儲存貯體記錄	AWSManagedServices-EnableBucketAccessLogging Amazon S3 儲存貯體記錄已啟用。	• TargetBucket：儲存伺服器存取日誌的 S3 儲存貯體名稱。 • TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式，若要將 S3 金鑰的簡單格式用於日誌物件，請選擇 SimplePrefix。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 PartitionedPrefixEventTime。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 PartitionedPrefixDeliveryTime。預設值為 PartitionedPrefixEventTime。有效值為 SimplePrefix、PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime（區分大小寫）。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
		若要啟用自動修復，必須提供下列預先設定的參數： • TargetBucket 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域 且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。
f2iK5R6Dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedR emediatorEnableRDSMultiAZ 已啟用多可用區域部署。	不允許預先設定的參數。 在此變更期間，可能會發生效能降低。
H7lgTzjTYb Amazon EBS 快照	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot Amazon EBSsnapshots 已建立。	不允許預先設定的參數。 無限制條件
opQPADkZvH RDS 備份	AWSManagedServices-EnableRD SBackupRetention 資料庫已啟用 Amazon RDS 備份保留。	• BackupRetentionPeriod：保留自動備份的天數 (1-35)。 • ApplyImmediately：指出是否盡快非同步套用 RDS 備份保留變更和任何待定修改。選擇立即true套用變更，或false選擇排程下一個維護時段的變更。 如果 ApplyImmediately 參數設定為 true，則 db 上的待定變更會與 RDSBackup 保留設定一起套用。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt013 Amazon RDS 資料庫執行個體已關閉儲存體自動調整規模	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling - 針對 Amazon RDS 資料庫執行個體啟用儲存體自動擴展。	MaxAllocatedStorageIncreasePercentage：目前 Allocated Storage 的增加百分比，以設定 MaxAllocatedStorage。預設值設為 26。 您必須將最大儲存閾值設定為比目前配置的儲存多至少 10%。最佳實務是將最大儲存閾值設定為至少多 26%。如需詳細資訊，請參閱使用 Amazon Relational Database Service 儲存體自動擴展自動管理容量。 無限制條件
7qGXsKIUw Classic Load Balancer 連線耗盡	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Classic Load Balancer 已啟用連線耗盡。	ConnectionDrainingTimeout：取消註冊執行個體之前，保持現有連線開啟的最長時間，以秒為單位。預設值設為 300 秒。 無限制條件
c18d2gz106 AWS Backup 計劃中不包含 Amazon EBS	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS 包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon EBS 磁碟區。標籤對必須符合的標籤型資源選擇條件 AWS Backup。 - TagKey - TagValue 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz107 AWS Backup 計劃中不包含 Amazon DynamoDB 資料表	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlanAddDynamoDBToBackupPlan Amazon DynamoDB 資料表包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon DynamoDB。標籤對必須符合的標籤型資源選擇條件 AWS Backup。 • TagKey • TagValue 無限制條件
c18d2gz117 AWS Backup 計劃中不包含 Amazon EFS	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS 包含在 AWS Backup 計劃中。	修復會使用下列標籤對來標記 Amazon EFS。標籤對必須符合的標籤型資源選擇條件 AWS Backup。 • TagKey • TagValue 無限制條件
c18d2gz105 跨負載平衡的 Network Load Balancer	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Network Load Balancer 上已啟用跨區域負載平衡。	不允許預先設定的參數。 無限制條件
c1qf5bt026 Amazon RDS synchronous_commit 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的參數 synchronous_commit 已開啟。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt030 Amazon RDS innodb_flush_log_at_trx_commit 參數不是 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 1 的 參數innodb_flush_log_at_trx_commit 設定為。	不允許預先設定的參數。 無限制條件
c1qf5bt031 Amazon RDS sync_binlog 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 參數sync_binlog 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt036 Amazon RDS innodb_default_row_format 參數設定不安全	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS DYNAMIC 的 參數innodb_default_row_format 設定為。	不允許預先設定的參數。 無限制條件
c18d2gz144 未啟用 Amazon EC2 詳細監控	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Amazon EC2 已啟用詳細監控。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的效能檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
COr6dfpM06	AWSManagedServices-ResizeLambdaMemory	RecommendedMemorySize : Lambda 函數的建議記憶體配置。值範圍介於 128 和 10240 之間。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
AWS Lambda 記憶體大小的佈建不足函數	Lambda 函數的記憶體大小會調整為 提供的建議記憶體大小 Trusted Advisor。	如果在自動化執行之前修改 Lambda 函數大小，則此自動化可能會以 建議的值覆寫設定 Trusted Advisor。
ZRxQIPsb6c Amazon EC2 執行個體高使用率	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 執行個體的大小由相同執行個體系列類型的一個執行個體類型調整。執行個體會在調整大小操作期間停止和啟動，並在執行完成後返回初始狀態。此自動化不支援調整 Auto Scaling 群組中的執行個體大小。	• MinimumDaysSinceLastChange：自上次執行個體類型變更以來的天數下限。如果在指定的時間內修改執行個體類型，則不會變更執行個體類型。使用 0 略過此驗證。預設值為 7。 • CreateAMIBeforeResize：若要在調整大小之前建立執行個體 AMI 做為備份，請選擇 true。若要不建立備份，請選擇 false。預設值為 false。有效值為 true 和 false (區分大小寫)。 • ResizeIfStopped：若要繼續變更執行個體大小，即使執行個體處於停止狀態，請選擇 true。如果執行個體處於停止狀態，若要不自動調整其大小，請選擇 false。有效值為 true 和 false (區分大小寫)。 無限制條件
c1qf5bt021 使用低於最佳值的 Amazon RDS innodb_change_buffering 參數	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 innodb_change_buffering 參數值設定為 NONE。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt025 Amazon RDS autovacuum 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 參數autovacuum 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt028 Amazon RDS enable_indexonlyscan 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 參數enable_indexonlyscan 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt029 Amazon RDS enable_indexscan 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 參數enable_indexscan 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt032 Amazon RDS innodb_stats_persistent 參數已關閉	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的 參數innodb_stats_persistent 已開啟。	不允許預先設定的參數。 無限制條件
c1qf5bt037 Amazon RDS general_logging 參數已開啟	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的參數general_logging 已關閉。	不允許預先設定的參數。 無限制條件

Trusted Advisor Trusted Remediator 支援的服務限制檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
IN7RR0I7J9 EC2-VPC 彈性 IP 地址	AWSManagedServices-UpdateVpcElasticIPQuota 系統會請求 EC2-VPC 彈性 IP 地址的新限制。根據預設，限制會增加 3。	增量：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
kM7QQ0I7J9 VPC 網際網路閘道	AWSManagedServices-IncreaseServiceQuota - 請求 VPC 網際網路閘道的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
jL7PP0I7J9 VPC	AWSManagedServices-IncreaseServiceQuota 已請求 VPC 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
fW7HH0I7J9 Auto Scaling 群組	AWSManagedServices-IncreaseServiceQuota 已請求 Auto Scaling 群組的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
3Njm0DJQO9 RDS 選項群組	AWSManagedServices-IncreaseServiceQuota 已請求 Amazon RDS 選項群組的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
EM8b3yLRTr ELB Application Load Balancer	AWSManagedServices-Increase ServiceQuota 會請求 ELB Application Load Balancer 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。
8wlqYSt25K ELB Network Load Balancer	AWSManagedServices-Increase ServiceQuota 會請求 ELB Network Load Balancer 的新限制。根據預設，限制會增加 3。	增加：增加目前配額的數字。預設值為 3。 如果此自動化在 Trusted Advisor 檢查更新為 OK 狀態之前執行多次，則可能會提高限制。

Trusted Advisor Trusted Remediator 支援的卓越營運檢查

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c18d2gz125 Amazon API Gateway 未記錄執行日誌	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging 執行記錄會在 API 階段上啟用。	不允許預先設定的參數。 您必須授予 API Gateway 許可，以讀取和寫入您帳戶的日誌至 CloudWatch，以啟用執行日誌，請參閱在 API Gateway 中設定 REST APIs 的 CloudWatch 日誌 記錄以取得詳細資訊。
c18d2gz168 未針對負載平衡器啟用 Elastic Load Balancing 刪除保護	為 Elastic Load Balancer 開啟 AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection - 刪除保護。	不允許預先設定的參數。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1qf5bt012 Amazon RDS Performance Insights 已關閉	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights Amazon RDS 的績效詳情已開啟。	- PerformanceInsightsRetentionPeriod：保留績效詳情資料的天數。有效值：7或月 * 31，其中月是從 1-23 的月數。範例：93 (3 個月 * 31)、341(11 個月 * 31)、589(19 個月 * 31) 或 731。 - PerformanceInsightsKMSKeyId：Performance Insights 資料的加密 AWS KMS 金鑰 ID。如果您未指定 PerformanceInsightsKMSKeyId 的值，則 Amazon RDS 會使用預設 AWS KMS 金鑰。 無限制條件

檢查 ID 和名稱	SSM 文件名稱和預期結果	支援的預先設定參數和限制條件
c1fd6b96l4 已啟用 Amazon S3 存取日誌	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Amazon S3 儲存貯體存取記錄已啟用。	- TargetBucketTagValue：用於識別目標儲存貯體的標籤值（區分大小寫），請使用此值和 TargetBucketTagKey 來標記要用作存取記錄目的地儲存貯體的儲存貯體。 - TargetObjectKeyFormat：日誌物件的 Amazon S3 金鑰格式（值區分大小寫）。若要針對日誌物件使用 S3 金鑰的簡單格式，請選擇 SimplePrefix。若要將分割的 S3 金鑰用於日誌物件，並將 EventTime 用於分割的字首，請選擇 PartitionedPrefixEventTime。若要將分割的 S3 金鑰用於日誌物件，並將 DeliveryTime 用於分割的字首，請選擇 PartitionedPrefixDeliveryTime。有效值為 SimplePrefix、PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime。 若要啟用自動修復，必須提供下列預先設定的參數：TargetBucketTagKey 和 TargetBucketTagValue。 目的地儲存貯體必須與來源儲存貯體位於相同 AWS 帳戶 AWS 區域且具有正確的日誌交付許可。如需詳細資訊，請參閱啟用 Amazon S3 伺服器存取記錄。

在信任的修復程式中設定 Trusted Advisor 檢查修復

組態會存放在 `中 AWS AppConfig`，做為信任的修復程式應用程式的一部分。每個 Trusted Advisor 檢查類別都有單獨的組態描述檔。如需 Trusted Advisor 類別的詳細資訊，請參閱[檢視檢查類別](#)。

您可以請求根據每個資源或每個 Trusted Advisor 檢查來設定修復。您可以使用資源標籤套用例外狀況。

Note

問題 Trusted Advisor 清單的修復目前使用 `設定 AWS AppConfig`，且此功能目前完全支援。AMS 預期這會在未來變更。最佳實務是避免建置依賴的自動化 AWS AppConfig，因為此方法可能會有所變更。請注意，為了實現相容性，您可能需要更新或修改以目前 AWS AppConfig 實作為基礎的自動化。

Compute Optimizer -> EC2 執行個體功能旗標具有額外的參數：

- `allow-upscale` 允許升級佈建不足的非最佳化 EC2 執行個體。預設值為 `"false"`。
- `min-savings-opportunity-percentage` 自動化修復的最低節省百分比機會。預設值為 10%

預設修復組態

個別 Trusted Advisor 檢查的組態會儲存為 AWS AppConfig 旗標。旗標名稱符合檢查名稱。每個檢查組態都包含下列屬性：

- `execution-mode`：決定信任的修復程式如何執行預設修復：
 - 自動化：信任的修復程式會自動修復資源，方法是建立 OpsItem、執行 SSM 文件，然後在成功執行後解決 OpsItem。
 - 手動：OpsItem 已建立，但 SSM 文件不會自動執行。您可以檢閱 OpsItem，並使用自動化 RFC 執行修復。如需詳細資訊，請參閱[在信任的修復程式中使用修復](#)。
 - 條件式：修補預設為停用。您可以使用標籤為特定資源啟用它。如需詳細資訊，請參閱下列各節[使用資源標籤自訂修復](#)和[使用資源覆寫標籤自訂修復](#)。
 - 非作用中：不會發生修復，也不會建立 OpsItem。您無法覆寫設定為非作用中之 Trusted Advisor 檢查的執行模式。
- `pre configured-parameters`：輸入自動化修復所需的 SSM 文件參數值，格式為 `Parameter=Value`，以逗號 (,) 分隔。如需每個檢查之相關聯 SSM 文件的支援預先設定參數，[Trusted Advisor](#) [Trusted Remediator 支援的檢查](#)請參閱。

- `alternative-automation-document`：此屬性有助於使用另一個支援的文件（如果適用於特定檢查）覆寫現有的自動化文件。根據預設，不會選取此屬性。

Note

`alternative-automation-document` 屬性不支援自訂自動化文件。您可以使用 中列出的現有支援信任的修復程式自動化文件 [Trusted Advisor Trusted Remediator 支援的檢查](#)。例如，針對檢查 Qch7DwouX1，有三個相關聯的 SSM 文件：AWSManagedServices-StopEC2Instance、AWSManagedServices-ResizeInstanceByOneLevel 和 AWSManagedServices-TerminateInstance。的值 `alternative-automation-document` 可以是 AWSManagedServices-ResizeInstanceByOneLevel 或 AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance 是要修復的預設 SSM 文件 Qch7DwouX1)。

每個屬性的值必須符合該屬性的限制。

Tip

套用 Trusted Advisor 檢查的預設組態之前，最佳實務是考慮使用下列各節所述的資源標記和資源覆寫功能。預設組態會套用至帳戶內的所有資源，這在所有情況下可能並不理想。

以下是範例主控台螢幕擷取畫面，其中執行模式設定為手動，且屬性符合其限制條件。

使用資源標籤自訂修復

檢查組態中的 `automated-for-tagged-only` 和 `manual-for-tagged-only` 屬性可讓您指定資源標籤，以用於如何修復個別檢查。當您需要將一致的修補行為套用至共用相同標籤的資源群組時，最佳實務是使用此方法。以下是這些標籤的說明：

- `automated-for-tagged-only`：指定資源標籤（一或多個標籤對，以逗號分隔），讓檢查自動修復，無論預設執行模式為何。
- `manual-for-tagged-only`：為應手動執行的修復指定資源標籤（一或多個標籤對，逗號分隔），無論預設執行模式為何。

例如，如果您想要為所有非生產資源啟用自動修復，並強制執行生產資源的手動修復，您可以設定組態，如下所示：

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

在您的資源上設定上述組態後，請檢查修復行為，如下所示：

- 標記 'Environment=Non-Production' 的資源會自動修復。
- 標記為 'Environment=Production' 的資源需要手動介入才能修復。
- 沒有 'Environment' 標籤的資源遵循預設執行模式（在此情況下為 'Conditional'）。因此，不會對剩餘的資源採取任何動作）。

如需組態的其他支援，請聯絡您的 Cloud Architect。

使用資源覆寫標籤自訂修復

資源覆寫標籤可讓您自訂個別資源的修補行為，無論其標籤為何。透過將特定標籤新增至資源，您可以覆寫該資源的預設執行模式和 Trusted Advisor 檢查。資源覆寫標籤優先於預設組態和資源標記設定。因此，如果您使用資源覆寫標籤將資源的預設執行模式設定為自動、手動或條件式，則會覆寫預設執行模式和任何資源標記組態。

若要覆寫資源的執行模式，請完成下列步驟：

1. 識別您要覆寫修復組態的資源。
2. 決定您要覆寫之 Trusted Advisor 檢查的檢查 ID。您可以在 [中找到受支援檢查 IDs](#) [Trusted Advisor](#) [Trusted Remediator 支援的檢查](#)。Trusted Advisor
3. 使用標籤 [| 更新](#) 或 [標籤 | 大量更新](#) 變更類型，將標籤新增至具有下列索引鍵和值的資源：
 - 標籤索引鍵：TR-*Trusted Advisor check ID*-Execution-Mode（區分大小寫）

在上述標籤索引鍵範例中，Trusted Advisor check ID 將取代為您要覆寫之 Trusted Advisor 檢查的唯一識別。

- 標籤值：將下列其中一個值用於標籤值：
 - 自動化：信任的修復程式會自動修復此 Trusted Advisor 檢查的資源。
 - 手動：為資源建立 OpsItem，但不會自動執行修復。您可以使用 自動化來檢閱和執行修復。
- 如需詳細資訊，請參閱[在信任的修復程式中使用修復](#)。

- 非作用中：不會為此資源和指定的 Trusted Advisor 檢查執行修復和 OpsItem 建立。

例如，若要使用 Trusted Advisor 檢查 ID 自動修復 Amazon EBS 磁碟區 DAvU99Dc4C，請將標籤新增至 EBS 磁碟區。標籤索引鍵為 TR-DAvU99Dc4C-Execution-Mode，標籤值為 Automated。

以下是顯示標籤區段的主控制台範例：

執行模式決策工作流程

有多個層級可為您的資源和每個 Trusted Advisor 檢查設定執行模式。下圖顯示 Trusted Remediator 如何根據您的組態決定要使用的執行模式：

設定修復教學課程

下列教學課程提供在信任的修復程式中建立常見修復的範例

手動修復所有資源

此範例會設定 Trusted Advisor 檢查 ID DAvU99Dc4C（未充分利用的 Amazon EBS 磁碟區）的所有 Amazon EBS 磁碟區的手動修復。

使用檢查 ID DAvU99Dc4C 設定 Amazon EBS 磁碟區的手動修復

1. 使用修復組態|更新，變更類型以請求組態更新。
2. 輸入下列參數：
 - CheckIds：DAvU99Dc4C
 - ExecutionMode：手動

Note

您可以在單一請求中設定多個檢查。對於需要相同組態的檢查，請在 CheckIds 參數中包含多個檢查 IDs。對於需要不同組態的檢查，建立新的 RemediationConfiguration 物件。

3. 提交 RFC。

自動修復所有資源，但選取的資源除外

此範例會為具有 Trusted Advisor 檢查 ID DAvU99Dc4C（未充分利用的 Amazon EBS 磁碟區）的所有 Amazon EBS 磁碟區設定自動修復，但不會修復的指定磁碟區（指定為非作用中）除外。

使用檢查 ID DAvU99Dc4C 設定 Amazon EBS 磁碟區的自動修復，所選非作用中資源除外

1. 覆寫所選 Amazon EBS 磁碟區的自動修復：

使用[標籤 | 更新](#)或[標籤 | 大量更新](#)變更類型，為要從自動修復排除的磁碟區套用下列標籤：

- 金鑰：TR-DAvU99Dc4C-Execution-Mode
- 值：非作用中

2. 使用修復組態|更新變更類型來請求組態更新。

3. 輸入下列參數：

- CheckIds：DAvU99Dc4C
- ExecutionMode：自動化

4. 提交 RFC。

自動修復已標記的資源

此範例會針對具有 Trusted Advisor 檢查 ID DAvU99Dc4C（未充分利用的 Amazon EBS 磁碟區）Stage=NonProd標籤的所有 Amazon EBS 磁碟區設定自動修復。沒有此標籤的所有其他資源都無法修復。

使用檢查 ID DAvU99Dc4C 的標籤**Stage=NonProd**設定 Amazon EBS 磁碟區的自動修復

1. 使用[修復組態 | 更新](#)、變更類型來請求組態更新。

2. 輸入下列參數：

- CheckIds：DAvU99Dc4C
- ExecutionMode：條件式
- AutomatedForTaggedOnly：{"Stage": "NonProd"}

Note

AutomatedForTaggedOnly 參數指定的值會覆寫先前設定的值。若要保留現有的標籤，請將它們包含在新值中。

3. 提交 RFC。

將組態重設為預設值

此範例會移除檢查 Hs4Ma3G104 的現有 automated-for-tagged-only 組態。若要移除先前套用的標籤組態，請將 AutomatedForTaggedOnly 參數值設定為 {}。

將檢查 Hs4Ma3G104 的組態重設為預設值

1. 使用 [修復組態 | 更新](#) 變更類型來請求組態更新。
2. 輸入下列參數：
 - CheckIds : Hs4Ma3G104
 - ExecutionMode : 輸入目前使用的值
 - AutomatedForTaggedOnly : {}
3. 提交 RFC。

在信任的修復程式中使用修復

在信任的修復程式中追蹤修復

若要追蹤 OpsItems 修補，請完成下列步驟：

1. 在 <https://console.aws.amazon.com/systems-manager/> 開啟 AWS Systems Manager 主控台。
2. 選擇 Operations Management、OpsCenter。
3. (選用) 依 Source=Trusted Remediator 篩選清單，以在清單中僅包含 Trusted Remediator OpsItems。

以下是由 Source=Trusted Remediator 篩選的 OpsCenter 畫面範例：

 Note

除了從 OpsCenter 檢視 OpsItems 之外，您還可以在 AMS S3 儲存貯體中檢視修復日誌。OpsCenter 如需詳細資訊，請參閱[信任的修復程式中的修復日誌](#)。

在信任的修復程式中執行手動修復

Trusted Remediator 會為設定為手動修復的檢查建立 OpsItems。您必須檢閱這些檢查，並手動開始修復程序。

若要手動修復 OpsItem，請完成下列步驟：

1. 在 <https://console.aws.amazon.com/systems-manager/> 開啟 AWS Systems Manager 主控台。
2. 選擇 Operations Management、OpsCenter。
3. (選用) 依 Source=Trusted Remediator 篩選清單，以在清單中僅包含 Trusted Remediator OpsItems。
4. 選擇您要檢閱的 OpsItem。
5. 檢閱 OpsItem 的操作資料。操作資料包含下列項目：
 - trustedAdvisorCheckCategory：Trusted Advisor 檢查 ID 的類別。例如，容錯能力
 - trustedAdvisorCheckId：唯一的 Trusted Advisor 檢查 ID。
 - trustedAdvisorCheckMetadata：資源中繼資料，包括資源 ID。
 - trustedAdvisorCheckName：Trusted Advisor 檢查的名稱。
 - trustedAdvisorCheckStatus：針對資源偵測到的 Trusted Advisor 檢查狀態。
 - trustedAdvisorCheckManualRemediation：提供手動修復參考詳細資訊的自訂資料。
 - ManualExecutionInput：定義參數的物件，您可以在執行手動修復時修改的值。
 - DocumentName：Runbook 的名稱 (SSM 文件)。
 - CustomizableParameters：您可以修改的參數名稱。
 - DefaultInput：定義參數名稱和值的物件，用於手動修復。值會根據預先設定的參數填入。
6. 若要手動修復 OpsItem，請完成下列步驟：
 - a. 使用[信任的修復程式 | 調查結果 | 修復 ct-1c7ch8z5phrjp](#) 變更類型
 - b. 輸入下列參數的值：

- `DocumentName`：必須是 `AWSManagedServices-RemediateTrustedRemediatorFinding`。
- 區域：AWS 區域，格式為 `us-east-1`。
- 參數：輸入手動修復參數：
 - `OpsItemId`：Ops 項目的 ID。
 - `RemediationDocumentName`：要使用的 SSM 自動化文件名稱。文件必須與操作項目相關聯。如果多個文件與操作項目相關聯，則必須指定 `DocumentName`。
 - `RemediationParameters`：自動化執行參數的索引鍵/值映射，格式為：`{\"ParameterName1\": [\"ParameterValue1\"], \"ParameterName2\": [\"ParameterValue2\"]}`。您只能使用存在於 Ops Item `trustedAdvisorCheckManualRemediation CustomizableParameters` 中的參數。如果未指定，則會從操作項目擷取參數和值。
- c. 選擇執行。如果沒有錯誤，則 RFC 成功建立的頁面會顯示已提交的 RFC 詳細資訊，以及初始的執行輸出。
- d. 監控 RFC 執行的進度。
- e. 執行完成後，OpsItem 就會解決。如果 RFC 失敗，請遵循中的步驟[對信任的修復程式中的修復進行故障診斷](#)。如需其他故障診斷支援，請聯絡 AMS。

對信任的修復程式中的修復進行故障診斷

如需手動修復和修復失敗的協助，請聯絡 AMS。

若要檢視修復狀態和結果，請完成下列步驟：

1. 在 <https://console.aws.amazon.com/systems-manager/> 開啟 AWS Systems Manager 主控台。
2. 選擇 Operations Management、OpsCenter。
3. （選用）依 `Source=Trusted Remediator` 篩選清單，只將 Trusted Remediator OpsItems 包含在清單中。
4. 選擇您要檢閱的 OpsItem。
5. 在自動化執行區段中，檢閱文件名稱、狀態和結果。
6. 檢閱下列常見的自動化失敗。如果您的問題未列在此處，請聯絡您的 CSDM 尋求協助。

常見的修復錯誤

自動化執行中未列出任何執行

沒有與 OpsItem 相關聯的執行可能表示執行因不正確的參數值而無法啟動。

疑難排解步驟

1. 在操作資料中，檢閱 `trustedAdvisorCheckAutoRemediation` 屬性值。
2. 驗證 `DocumentName` 和參數值是否正確。如需正確的值，[在信任的修復程式中設定 Trusted Advisor 檢查修復](#)請檢閱 以取得如何設定 SSM 參數的詳細資訊。若要檢閱支援的檢查參數，請參閱 [Trusted Advisor Trusted Remediator 支援的檢查](#)
3. 驗證 SSM 文件中的值是否符合允許的模式。若要檢視文件內容中的參數詳細資訊，請在 Runbooks 區段中選取文件名稱。
4. 在您檢閱和更正參數之後，請手動修復 OpsItem。如需修復步驟，請參閱 [在信任的修復程式中執行手動修復](#)。
5. 若要防止此錯誤再次發生，請確定您使用組態中的正確參數值來設定修復。如需詳細資訊，請參閱[在信任的修復程式中設定 Trusted Advisor 檢查修復](#)

自動化執行中失敗的執行

修復文件包含多個步驟，與透過 APIs AWS 服務 執行各種動作互動。若要識別失敗的特定原因，請完成下列步驟：

疑難排解步驟

1. 若要檢視個別執行步驟，請選擇執行 ID、自動化執行區段中的連結。以下是 Systems Manager 主控台的範例，顯示所選自動化的執行步驟：
2. 選擇狀態為失敗的步驟。以下是錯誤訊息範例：

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

此錯誤表示在修復組態的預先設定參數中指定了不正確的儲存貯體名稱。

若要解決此錯誤，請使用正確的儲存貯體名稱[手動執行自動化](#)。為避免此問題再次發生，[請使用正確的儲存貯體名稱更新修復組態](#)。

- DB instance my-db-instance-1 is not in available status for modification.

此錯誤表示自動化無法進行預期的變更，因為資料庫執行個體處於無效狀態。

若要解決此錯誤，[請手動執行自動化](#)。

信任的修復程式中的修復日誌

Trusted Remediator 會以 JSON 格式建立日誌，並將其上傳至 Amazon Simple Storage Service。日誌檔案會上傳至 AMS 建立且名為的 S3 儲存貯體 `ams-trusted-remediator-{your-account-id}-logs`。AMS 會在委派管理員帳戶中建立 S3 儲存貯體。您可以將日誌檔案匯入 QuickSight，以產生自訂的修補報告。

修復項目日誌

建立修復 OpsItem Remediation item log 時，信任的修復程式會建立。此日誌包含手動修復 OpsItem 和自動修復 OpsItem。您可以使用 Remediation item log 來追蹤所有修補的概觀。

Compute Optimizer 建議的修復項目日誌位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-Resource ID.json
```

Trusted Advisor 檢查的修復項目日誌位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-Resource ID.json
```

修復項目日誌範例檔案 URL

```
s3:///ams-trusted-remediator-111122223333-logs/  
remediation_items/2023-02-06/1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json
```

Compute Optimizer Remediation 項目日誌格式

```
{
```



```
"AccountID": "Account_ID",
"ComputeOptimizerCheckID": "Compute Optimizer check ID",
"ComputeOptimizerCheckName": "Compute Optimizer check name",
"ResourceID": "Resource ID",
"RemediationTime": Remediation creation time,
"ExecutionMode": "Automated or Manual",
"OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 修復項目日誌格式

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Compute Optimizer Remediation 項目日誌格式範例內容

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 修復項目日誌格式範例內容

```
{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}
```

```
}
```

自動化修復執行日誌、Compute Optimizer 和 Trusted Advisor

當自動化 SSM 文件執行完成 Automated remediation execution log 時，信任的修復程式會建立。此日誌僅包含自動修復 OpsItem 的 SSM 執行詳細資訊。您可以使用此日誌檔案來追蹤自動化修復。

Compute Optimizer 自動化修復日誌位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Compute Optimizer recommendation  
ID.json
```

Trusted Advisor 自動化修復日誌位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource  
ID.json
```

Compute Optimizer 自動化修復日誌位置範例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/1750908858-123456789012-compute-  
optimizer-ec2-i-1235173471d2cd789.json
```

Trusted Advisor 自動化修復日誌位置範例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

自動化修復日誌格式範例內容

```
{  
  "OpsItemID": "oi-767c77e05301",  
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
  "SSMExecutionStatus": "Success"}
```

Trusted Remediator 中的最佳實務

以下是協助您使用受信任修復程式的最佳實務：

- 如果您不確定修復結果，請從手動執行模式開始。有時候，從一開始針對修復套用自動執行可能會導致非預期的結果。
- 每週審查補救措施和 OpsItems，以取得信任的補救措施結果的洞察。
- 成員帳戶會從委派的管理員帳戶繼承組態。因此，以協助您使用相同組態管理多個帳戶的方式建構帳戶非常重要。您可以使用標籤從預設組態中豁免資源。

信任的修復程式FAQs

以下是有關信任修復程式的常見問題：

什麼是 Trusted Remediator，它如何使我受益？

當 Compute Optimizer 識別出不合規 Trusted Advisor 或發出建議時，信任的補救措施會根據您指定的偏好設定回應，方法是套用補救措施、透過手動補救措施尋求核准，或在即將到來的每月商業審查 (MBR) 期間報告補救措施。修補會在您偏好的修補時間或排程進行。Trusted Remediator 可讓您自行處理 Trusted Advisor 檢查，並靈活地設定和修復個別或大量檢查。透過經過測試的修補文件程式庫，AMS 會持續套用安全檢查並遵循 AWS 最佳實務來提高您的帳戶。只有在組態中指定這麼做時，您才會收到通知。AMS 使用者可以選擇加入 Trusted Remediator，無需額外費用。

信任的修復程式與其他 有何關聯和搭配 AWS 服務？

您可以在現有的企業支援計劃中存取 Trusted Advisor 檢查和 Compute Optimizer 建議。Trusted Remediator 與 Trusted Advisor 和 Compute Optimizer 整合，以利用現有的 AMS 自動化功能。具體而言，AMS 使用 AWS Systems Manager 自動化文件（執行手冊）進行自動化修復。AWS AppConfig 用於設定修復工作流程。您可以透過 Systems Manager OpsCenter 檢視所有目前和過去的修補。修復日誌存放在 Amazon S3 儲存貯體中。您可以使用日誌在 QuickSight 中匯入和建置自訂報告儀表板。

誰會設定修補？

您擁有帳戶中的組態。管理您的組態是您的責任。您也可以聯絡 AMS 以取得組態變更、支援和手動修復，以及對修復失敗進行疑難排解。

如何安裝 SSM 自動化文件？

SSM 自動化文件會自動與加入的 AMS 帳戶共用。

AMS 擁有的資源是否也會修復？

AMS 擁有的資源不會由信任的修復程式標記。Trusted Remediator 僅專注於您的 資源。

AWS 區域 什麼是 中的可信任修復程式，以及誰可以使用它？

信任的修復程式可供 AMS Advanced 客戶使用。如需支援區域的最新清單，請參閱[AWS 服務 依區域](#)。

信任的修復程式會造成資源漂移嗎？

由於 SSM 自動化文件會透過 AWS API 直接更新資源，因此可能會發生資源偏離。您可以使用標籤來隔離透過現有 CI/CD 套件建立的資源。您可以設定信任的修復程式來忽略標記的資源，同時仍然修復其他資源。

如何暫停或停止信任的修復程式？

使用 [管理 | 信任的修復程式 | 狀態 | 啟用或停用](#)變更類型來停止信任的修復程式服務。使用相同的變更類型重新啟用信任的修復程式。

如何修復受信任修復程式不支援的檢查？

您可以繼續透過 Operations On Demand (OOD) 聯絡 AMS 以進行不支援的檢查。AMS 可協助您修復這些檢查。如需詳細資訊，請參閱[隨需操作](#)。

信任的修復程式會將哪些資源部署到您的帳戶？

Trusted Remediator 會在 Trusted Remediator 委派管理員帳戶中部署下列資源：

- 名為 `ams-trusted-remediator-{your-account-id}-logs` 的 Amazon S3 儲存貯體。建立修復 OpsItem 時，信任的修復程式會以 Remediation item log JSON 格式建立，並將日誌檔案上傳至此儲存貯體。
- 保留支援 Trusted Advisor 檢查修復組態和 Compute Optimizer 建議的 AWS AppConfig 應用程式。

Trusted Remediator 不會在 Trusted Remediator 成員帳戶中部署資源。

日誌管理

主題

- [什麼是日誌管理？](#)
- [AMS 記錄的運作方式](#)
- [存取您的日誌](#)
- [自訂您的日誌組態](#)

AMS 日誌管理會從受管帳戶收集、彙總和控制日誌的保留。AWS 日誌管理會將帳戶中 AWS 部署的 Amazon EC2 執行個體和資源的日誌彙總到 CloudWatch Logs。您可以在 [中找到目前彙總日誌的服務完整清單](#)[AMS 彙總服務日誌](#)。

什麼是日誌管理？

日誌管理是處理執行個體、應用程式和 AWS 服務所產生的日誌事件的程序。此功能定義 AMS 如何處理、存放和輪換您受管 AWS 帳戶中產生的日誌事件。基礎設施日誌會在事件解決期間使用，並支援系統稽核。

AMS 記錄的運作方式

AMS 單一帳戶登陸區域 (SALZ) 日誌管理使用各種預先安裝的代理程式和工具，這些代理程式和工具會在執行個體和應用程式加入或佈建時實作。

記錄是在帳戶加入程序和啟動堆疊時設定。

執行個體和 AWS 服務產生的 AMS 多帳戶登陸區域 (MALZ) 日誌可在由 AMS 管理的每個帳戶中的 CloudWatch Logs 或 Amazon Simple Storage Service (Amazon S3) 中取得。AMS 多帳戶登陸區域提供中央記錄帳戶，可做為個別應用程式帳戶產生之部分日誌的中央彙總位置。

[存取您的日誌](#) 子區段中的資料表說明個別帳戶中可用的日誌，以及中央記錄帳戶中可用的日誌。

存取您的日誌

若要存取您的日誌，請確定您擁有其中一個必要的 IAM 角色，且位於您的 AMS 帳戶中。然後導覽至顯示的目錄。

Multi-Account Landing Zone (MALZ)

提供五個預設 IAM 角色，每個角色都允許存取您帳戶中的所有日誌（全部都以開頭AWSManagedServices）：

- AdminRole
- CaseRole
- ChangeManagementRole
- ReadOnlyRole
- SecurityOpsRole

對這些角色的存取是透過聯合設定，每個角色都會映射到 Active Directory 網域中的群組。

若要進一步了解這些角色，請參閱 [AMS 中的 IAM 使用者角色](#)。

Single-Account Landing Zone (SALZ)

Customer_ReadOnly_Role AMS 單一帳戶登陸區域的預設值可讓您存取帳戶內的所有日誌。使用映射至 Active Directory 群組的 AWS Identity and Access Management (IAM) 角色來控制對日誌的存取。

AMS 彙總服務日誌

每個 AWS 服務都會記錄到 CloudWatch Logs 或 Amazon S3 儲存貯體中的特定位置。

Note

除非特別說明，否則所有日誌位置皆為產生日誌之帳戶的本機位置，不會彙總到中央日誌帳戶。

若要在 SALZ 和 MALZ 帳戶中尋找預設 AMS CloudTrail 線索名稱，請前往 CloudTrail 的 AWS 主控台，然後前往線索頁面並搜尋 AMS。由於 AMS 資源有標籤，因此您可以用這種方式找到線索。AMS CloudTrail 標籤範例：

```
Environment    AMSInfrastructure
```

若要存取您的日誌，請確定您擁有其中一個必要的 IAM 角色，且位於您的 AMS 帳戶中。然後導覽至顯示的目錄。

Multi-Account Landing Zone

AMS 多帳戶登陸區域彙總服務日誌

	服務名稱	日誌詳細資訊	日誌位置
1	Amazon Aurora	一般、慢查詢和錯誤日誌。	CloudWatch LogGroup : /aws/rds/cluster/{ <i>database_name</i> }/ { <i>log_name</i> }
2	AWS CloudFormation (CFN)	僅限 API 呼叫記錄。	AWS CloudFormation API 呼叫是透過 CloudTrail 記錄，它會將其日誌傳送至 CloudWatch LogGroup，然後將日誌同步到 S3 儲存貯體。日誌預設會保留在 CloudWatch LogGroup 中 14 天，並無限期保留在 S3 儲存貯體中。 CloudWatch LogGroup : / CloudTrail/Landing-Zone-Logs S3 儲存貯體 【在中央記錄帳戶中】 : aws-landing-zone-logs-ams-a{ <i>account_ID</i> }-log-management-{ <i>region</i> } 路徑 : /AWSLogs/{ <i>account_ID</i> }/CloudTrail/
3	Amazon CloudFront (CloudFront)	使用者請求記錄。CloudFront 記錄必須明確啟用。如需相關資訊，請參閱 啟用支援服務的記錄 。	S3 儲存貯體 : ams-a{ <i>account_ID</i> }-log-management-{ <i>region</i> } 路徑 : AWS/RedShift/{ <i>CloudFront ## ID</i> }
4	Amazon CloudWatch (CloudWatch)	僅限 API 呼叫記錄。	CloudWatch LogGroup : / CloudTrail/Landing-Zone-Logs

	服務名稱	日誌詳細資訊	日誌位置
			S3 儲存貯體 【在中央記錄帳戶中】：aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路徑：/AWSLogs/{ <i>account_ID</i> }/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	EBS 服務不會產生日誌。	不適用
6	Amazon Elastic Compute Cloud (Amazon EC2)	系統和應用程式日誌。 如需資訊，請參閱「 Amazon Elastic Compute Cloud (Amazon EC2) - 系統層級日誌 」。	CloudWatch Logs：/{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	僅限 API 呼叫記錄。	CloudWatch LogGroup：/ CloudTrail/Landing-Zone-Logs S3 儲存貯體 【在中央記錄帳戶中】：aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路徑：/AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	服務名稱	日誌詳細資訊	日誌位置
8	Elastic Load Balancing (ELB)	存取和錯誤日誌項目。 彈性負載平衡器會記錄所有傳送給他們的請求，包括未路由至後端執行個體的請求。例如，如果用戶端傳送格式不正確的請求，或沒有運作狀態良好的執行個體可回應，則仍會記錄請求。 如需 Elastic Load Balancing 日誌項目的詳細資訊，請參閱 - Classic Load Balancer：存取日誌項目。 - Application Load Balancer：存取日誌項目。 - Network Load Balancer：存取日誌項目。	API 呼叫日誌： CloudWatch LogGroup： CloudTrail/Landing-Zone-Logs S3 儲存貯體【在中央記錄帳戶中】： <code>aws-landing-zone-logs-{account_ID}-{region}</code> 路徑：<code>/AWSLogs/{account_ID}/CloudTrail/</code> 存取日誌： S3 儲存貯體：<code>mc-a{account_ID}-logs{region}</code> 路徑：<code>aws/elbaccess</code>
9	Amazon OpenSearch Service (OpenSearch Service)	服務錯誤日誌。 您必須明確啟用 OpenSearch 記錄。如需相關資訊，請參閱啟用支援服務的記錄。	CloudWatch LogGroup： CloudTrail/Landing-Zone-Logs S3 儲存貯體【在中央記錄帳戶中】： <code>aws-landing-zone-logs-{account_ID}-{region}</code> 路徑：<code>/AWSLogs/{account_ID}/CloudTrail/</code>

	服務名稱	日誌詳細資訊	日誌位置
10	Amazon ElastiCache	僅限 API 呼叫記錄。	CloudWatch LogGroup : //CloudTrail/Landing-Zone-Logs
11	Amazon GuardDuty		S3 儲存貯體 【在中央記錄帳戶中】 : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
12	Amazon Inspector		路徑 : /AWSLogs/{ <i>account_ID</i> }/CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	連線、使用者和活動日誌。 當您透過叫用建立 Redshift 叢集 CT (ct-1malj7snzxrkr) 來建立 Redshift 叢集時，預設會啟用記錄。 如需詳細資訊，請參閱資料庫稽核記錄。	S3 儲存貯體 : ams-a{<i>account_ID</i>}-log-management-{<i>region</i>} 路徑 : /AWS/RedShift/{ <i>CloudFront ## ID</i> }
15	Amazon Relational Database Service (RDS)	資料庫類型特定的日誌。 您必須明確啟用 RDS 記錄。如需相關資訊，請參閱啟用支援服務的記錄。 您只能透過預存程序存取 MSSQL 日誌；如需資訊，請參閱封存日誌檔案。	CloudWatch LogGroup : /aws/rds/({####或##})/{<i>database_name</i> }/{<i>log_name</i>}

	服務名稱	日誌詳細資訊	日誌位置
16	Amazon S3 (S3)	儲存貯體存取日誌。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊，例如請求者、儲存貯體名稱、請求時間、請求動作、回應狀態和錯誤碼（如果有的話）。存取記錄資訊在安全與存取稽核中相當實用。您也可藉由該資訊了解自己的客戶群，並掌握 Amazon S3 帳單相關資料。 如需 S3 存取日誌項目的詳細資訊，請參閱 S3 伺服器存取日誌格式。	S3 儲存貯體：mc-a{<i>account_ID</i>}-log-management-{<i>region</i>} 路徑：/aws/s3access/{<i>bucket_name</i>} S3 儲存貯體【在中央記錄帳戶中】：aws-landing-zone-s3-access-logs-{<i>account_ID</i>}-{<i>region</i>} 路徑：/
17	Amazon Simple Email Service (SES)	SES API 服務呼叫。	CloudWatch LogGroup：/ CloudTrail/Landing-Zone-Logs S3 儲存貯體【在中央記錄帳戶中】：aws-landing-zone-logs-{<i>account_ID</i>}-{<i>region</i>} 路徑：/AWSLogs/{<i>account_ID</i>}/CloudTrail/
18	Amazon Virtual Private Cloud (VPC)	VPC 流程資料（進出 VPC 網路介面的 IP 流量相關資訊）。	CloudWatch LogGroup： /aws/vpcflow/{ <i>VPC_ID</i> }
19	Auto Scaling	僅限 API 呼叫記錄。	CloudWatch LogGroup：/ CloudTrail/Landing-Zone-Logs
20	AWS Certificate Manager		S3 儲存貯體【在中央記錄帳戶中】：aws-landing-zone-logs-{<i>account_ID</i>}-{<i>region</i>} 路徑：/AWSLogs/{<i>account_ID</i>}/CloudTrail/

	服務名稱	日誌詳細資訊	日誌位置
21	AWS CodeDeploy	執行個體特定的部署日誌。	在執行個體上
22	AWS Config	AWS Config API 服務呼叫。	CloudWatch LogGroup : / CloudTrail/Landing-Zone-Logs S3 儲存貯體 【在中央記錄帳戶中】 : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路徑 : /AWSLogs/{ <i>account_ID</i> }/CloudTrail/
		資源組態變更，如 AWS Config 所追蹤。	S3 儲存貯體 【在中央記錄帳戶中】 : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路徑 : /AWSLogs/{ <i>account_ID</i> }/Config/
23	AWS Database Migration Service	資料庫遷移日誌。 如需詳細資訊，請參閱 AWS Database Migration Service 中的日誌管理簡介 。	資料庫遷移主控台
24	AWS Direct Connect (DX)	僅限 API 呼叫記錄。	CloudWatch LogGroup : / CloudTrail/Landing-Zone-Logs
25	AWS Glacier		S3 儲存貯體 【在中央記錄帳戶中】 : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
26	AWS IAM (IAM)		
27	AWS Key Management Service		路徑 : /AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	服務名稱	日誌詳細資訊	日誌位置
28	AWS 管理主控台 (主控台或 AWS 主控台)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Single-Account Landing Zone

AMS 單一帳戶登陸區域彙總服務日誌

	服務名稱	日誌詳細資訊	日誌位置
1	Amazon Aurora	一般、慢查詢和錯誤日誌。	CloudWatch LogGroup : /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	Amazon CloudFormation (CloudFormation 或 CFN)	僅限 API 呼叫記錄。	CloudFormation API 呼叫是透過 CloudTrail 記錄，其會將日誌傳送至 CloudWatch LogGroup，然後將日誌同步至 S3 儲存貯體。 CloudWatch LogGroup : /aws/ams/cloudtrail S3 儲存貯體 : <i>ams-a{account_ID }-log-management-{region}</i>
3	Amazon CloudFront (CloudFront)	使用者請求記錄。	S3 儲存貯體 : <i>ams-a{account_ID }-log-management-{region}</i>

	服務名稱	日誌詳細資訊	日誌位置
		您必須明確啟用 CloudFront 記錄。如需相關資訊，請參閱 啟用支援服務的記錄 。	路徑：AWS/RedShift/{ <i>CloudFront_distribution_ID</i> }
4	Amazon CloudWatch (CloudWatch)	僅限 API 呼叫記錄。	CloudWatch LogGroup：/aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	EBS 服務不會產生日誌。	不適用
6	Amazon Elastic Compute Cloud (EC2)	系統和應用程式日誌。 如需資訊，請參閱「 Amazon Elastic Compute Cloud (Amazon EC2) - 系統層級日誌 」。	CloudWatch Logs：/{ <i>instance_ID</i> }
7	Amazon Elastic File System (Amazon EFS)	僅限 API 呼叫記錄。	CloudWatch LogGroup：/aws/ams/cloudtrail

	服務名稱	日誌詳細資訊	日誌位置
8	Elastic Load Balancing (ELB)	存取和錯誤日誌項目。 彈性負載平衡器會記錄所有傳送給他們的請求，包括未路由至後端執行個體的請求。例如，如果用戶端傳送格式不正確的請求，或沒有運作狀態良好的執行個體可回應，則仍會記錄請求。 如需彈性負載平衡器日誌項目的詳細資訊，請參閱 - Classic Load Balancer：存取日誌項目。 - Application Load Balancer：存取日誌項目。 - Network Load Balancer：存取日誌項目。	CloudWatch LogGroup：<code>/aws/ams/cloudtrail</code> S3 儲存貯體：<code>mc-a{<i>account_ID</i>}-logs-{<i>region</i>}</code> 路徑：<code>aws/elbaccess</code>
9	Amazon OpenSearch Service (OpenSearch Service)	服務錯誤日誌。 您必須明確啟用 OpenSearch 記錄。如需相關資訊，請參閱啟用支援服務的記錄。	CloudWatch LogGroup： <code>/aws/ams/cloudtrail</code>
10	Amazon ElastiCache	僅限 API 呼叫記錄。	CloudWatch LogGroup： <code>/aws/ams/cloudtrail</code>
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		

	服務名稱	日誌詳細資訊	日誌位置
14	Amazon Redshift	連線、使用者和活動日誌。 當您叫用建立 Redshift 叢集 CT (ct-1malj7snzxrkr) 來建立 Redshift 叢集時，預設會啟用記錄。 如需詳細資訊，請參閱資料庫稽核記錄。	S3 儲存貯體：ams-a{<i>account_ID</i>}-log-management-{<i>region</i>} 路徑：/AWS/RedShift/{<i>CloudFront_Distribution_ID</i>}
15	Amazon Relational Database Service (RDS)	資料庫類型特定的日誌。 必須明確啟用 RDS 記錄。如需相關資訊，請參閱啟用支援服務的記錄。 您只能透過預存程序存取 MSSQL 日誌；如需資訊，請參閱封存日誌檔案。	CloudWatch LogGroup：/aws/rds/(instance cluster)/(database name)/(log name)
16	Amazon S3 (S3)	儲存貯體存取日誌。每個存取日誌記錄都會提供有關單一存取請求的詳細資訊，例如：請求者、儲存貯體名稱、請求時間、請求動作、回應狀態和錯誤碼（如果有的話）。存取日誌資訊在安全性和存取稽核中很有用；它也可以協助您了解您的客戶群並了解您的 Amazon S3 帳單。 如需 S3 存取日誌項目的詳細資訊，請參閱S3 伺服器存取日誌格式。	S3 儲存貯體：mc-a{<i>account_ID</i>}-log-management-{<i>region</i>} 路徑：/aws/s3access/{<i>bucket_name</i>}

	服務名稱	日誌詳細資訊	日誌位置
17	Amazon Simple Email Service (SES)	SES API 服務呼叫。	CloudWatch LogGroup : /aws/ams/cloudtrail S3 儲存貯體 : ams-a{ <i>account_ID</i> }-log-management-{ <i>region</i> } 路徑 : AWS/CloudTrail/AWSLogs/{ <i>account_ID</i> }/CloudTrail/{ <i>region</i> }
18	Amazon Virtual Private Cloud (VPC)	VPC 流程資料 (進出 VPC 網路介面的 IP 流量相關資訊) 。	CloudWatch LogGroup : /aws/vpcflow/{vpc_id}
19	Auto Scaling	僅限 API 呼叫記錄。	CloudWatch LogGroup : /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	執行個體特定的部署日誌。	在執行個體上
22	AWS Config	AWS Config API 服務呼叫。	CloudWatch LogGroup : /aws/ams/cloudtrail S3 儲存貯體 : ams-a{ <i>account_ID</i> }-log-management-{ <i>region</i> } 路徑 : AWS/CloudTrail/AWSLogs/{ <i>account_ID</i> }/CloudTrail/{ <i>region</i> }
23	AWS Database Migration Service	資料庫遷移日誌。 如需詳細資訊，請參閱 AWS Database Migration Service 中的日誌管理簡介 。	資料庫遷移主控台

	服務名稱	日誌詳細資訊	日誌位置
24	AWS Direct Connect (DX)	僅限 API 呼叫記錄。	CloudWatch LogGroup : /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM (IAM)		
27	AWS Key Management Service		
28	AWS 管理主控台 (主控台或 AWS 主控台)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

AMS 共用服務日誌

下表說明您帳戶中 AMS Shared Services 的日誌和日誌位置。

若要存取您的日誌，請確定您擁有其中一個必要的 IAM 角色，且位於您的 AMS 帳戶中。然後導覽至顯示的目錄。

AMS 單一帳戶登陸區域共享服務記錄

	共用服務名稱	日誌詳細資訊	日誌位置
1	防禦主機	有關存取堡壘主機之使用者的資訊。	Linux 堡壘： CloudWatch Logs : /{instance id}/var/log/secure

	共用服務名稱	日誌詳細資訊	日誌位置
			CloudWatch Logs : <code>/{{instance id}}/var/log/audit/audit.log</code> Windows 堡壘 : CloudWatch Logs : <code>/{{instance id}}/SecurityEventLog</code>
2	管理主機	指令碼的輸出，可協助帳戶內的自動存取管理動作。	CloudWatch Logs : <code>/{{instance id}}/ApplicationEventLog</code>
4	EPS 主機 (DSM)	有關在 Deep Security Management 平台上註冊執行個體的資訊。	CloudWatch Logs : <code>/{{instance id}}/var/log/DSM.log</code>
5	目錄服務	帳戶登入、帳戶管理、詳細追蹤、物件存取、政策變更和帳戶目錄中權限使用的相關資訊。 您必須明確啟用 Directory Services 記錄。如需相關資訊，請參閱 啟用支援服務的記錄 。	CloudWatch Logs : <code>/aws/directoryservice/{{directory id}}-{{directory dns name}}</code>
6	Lambdas	各種 Lambda 的輸出，可協助帳戶內的自動化操作動作。	CloudWatch Logs : <code>/aws/lambda/{{lambda name}}</code>

AMS 多帳戶登陸區域共享服務記錄

	共用服務名稱	日誌詳細資訊	日誌位置
1	堡壘	執行個體登入和身分驗證失敗的輸出。	Linux Bastions CloudWatch Logs : <code>/{{<i>instance_ID</i>}}/var/log/secure.log</code>

	共用服務名稱	日誌詳細資訊	日誌位置
			Windows Bastions CloudWatch Logs : <code>/{{<i>instance_ID</i> }}/SecurityEventLog</code>
2	管理主機	指令碼系統的輸出，可協助帳戶內的自動存取管理動作。	CloudWatch Logs : <code>/{{<i>instance_ID</i> }}/ApplicationEventLog</code>
3	EPS 主機 (DSM)	有關在 Deep Security Management 平台上註冊執行個體的資訊。	CloudWatch Logs : <code>/{{<i>instance_ID</i> }}/var/log/DSM.log</code>
4	目錄服務	帳戶登入、帳戶管理、詳細追蹤、物件存取、政策變更和帳戶目錄中權限使用的相關資訊。 您必須明確啟用 Directory Services 記錄。如需相關資訊，請參閱啟用支援服務的記錄。	CloudWatch Logs : <code>/aws/directoryservice/{{<i>directory_ID</i> }}-{{<i>directory_DNS_name</i> }}</code>
5	Lambdas	各種 Lambda 的輸出，可協助帳戶內的自動化操作動作。	CloudWatch Logs : <code>/aws/lambda/{{<i>Lambda_name</i> }}</code>

Amazon Elastic Compute Cloud (Amazon EC2) - 系統層級日誌

執行個體日誌是由在執行個體上執行的 CloudWatch Logs 代理程式收集，並且可以透過與執行個體同名的 CloudWatch Log 群組存取。例如，如果執行個體 ID 為 `i-0123456789abcdef0` 且日誌檔案名稱為 `/var/log/messages`，則日誌群組將為 `i-0123456789abcdef0` 和日誌串流 `/var/log/messages`。

另請參閱[AMS 彙總服務日誌](#)。

若要存取您的日誌，請確定您擁有其中一個必要的 IAM 角色，且位於您的 AMS 帳戶中。然後導覽至顯示的目錄。

 Note

根據預設，會收集下列日誌。

Amazon Linux / Red Hat Linux / Centos Linux / Ubuntu / SUSE Linux

日誌檔案/日誌串流

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

 Note

如需有關存取 Amazon Linux 2023 日誌的資訊，請參閱[為什麼 /var/log 目錄在我的 EC2 Amazon Linux 2023 執行個體中缺少日誌？](#)

Windows

日誌檔案/日誌串流

SecurityEventLog


```
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

與 Splunk 整合

AMS 支援以 AWS Lambda 為基礎的推送到客戶日誌分析服務，例如 Splunk。

AMS 利用適用於 Amazon Web 服務的 Splunk 附加元件，允許將 AWS 資料串流至 Splunk。請參閱[硬體和軟體需求](#)。

請參閱此 Splunk 部落格文章[如何將 AWS CloudWatch Logs 串流至 Splunk \(提示：比您想像的更容易\)](#)。由於 AMS 客戶預設會啟用 CloudWatch 日誌串流，因此 AMS 會為您設定 AWS Lambda 函數，不過您需要設定 Splunk HTTP 事件收集器 (HEC) 輸入，並向 AMS 提交新增功能的請求。

以下是資料輸入設定的外觀：

自訂您的日誌組態

您可以變更 CloudWatch 日誌的日誌資料保留，也可以啟用其他 AWS 服務的日誌記錄。

更改 CloudWatch 日誌保留

您可以變更 CloudWatch 日誌的日誌資料保留設定。根據預設，日誌將無限期保留且永遠不會過期。您可以調整每個日誌群組的保留政策，維持無限期保留，或選擇保留期間為 1 天至 10 年。若要在 AMS 中檢視允許的最短保留期間，請參閱可透過 AWS Artifact 取得的 AMS 技術標準文件。若要存取 AWS Artifact，請聯絡您的 CSDM 以取得指示，或前往[AWS Artifact 入門](#)。

CloudWatch Logs 日誌保留功能會根據保留政策刪除串流中的日誌事件。它不會刪除日誌串流或日誌群組。如需一般資訊，請參閱 Amazon CloudWatch Logs 使用者指南[什麼是 Amazon CloudWatch Logs ?](#)。

如需自訂日誌保留期間的資訊，以及進一步了解，請參閱在[CloudWatch Logs 中變更日誌資料保留](#)。

啟用支援服務的記錄

有些 服務預設未啟用記錄，且需要明確啟用。

若要啟用 CloudFront、OpenSearch、Amazon RDS 和 Route53 的記錄，請使用下列值提交 RFC 與 Management | Other | Other | Create change type (ct-1e1xtak34nx76)，視需要取代##：

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

安全管理

AWS Managed Services (AMS) 安全管理是 AMS 識別組織資產並實作政策和程序以保護這些資產的程序。

Note

AMS 現在具有變更類型 (CT)、部署 | 進階堆疊元件 | ACM 憑證搭配其他 SANs | 建立 (ct-3l14e139i5p50)，可用來提交 AWS Certificate Manager 憑證的請求。如需詳細資訊，請參閱 [AWS::CertificateManager::Certificate](#)。此 CT 提供建立其他主體替代名稱 (SAN)。

若要進一步了解一般 AWS 安全性，請參閱[安全性、身分和合規的最佳實務](#)。

AMS 將安全風險分類如下：

- 反惡意軟體偵測到的已知風險，惡意軟體緩解程序會處理這些風險。
- 安全事件，包括安全事件管理程序處理的存取違規。

主題

- [AMS 中的資料保護](#)
- [身分與存取管理](#)
- [AMS 中的安全事件回應](#)
- [在 AMS Advanced 中變更請求安全性審查](#)

AMS 中的資料保護

AMS 會利用 Amazon GuardDuty、Amazon Macie（選用）和其他內部專屬工具和程序等原生 AWS 服務，持續監控您的受管帳戶。觸發警示後，AMS 會承擔初始分類和警示回應的責任。我們的回應程序是以 NIST 標準為基礎。AMS 會定期使用安全事件回應模擬測試其回應程序，讓您的工作流程與現有的客戶安全回應計劃保持一致。

當 AMS 偵測到或您的安全政策的任何違規 AWS 或即將發生的違規威脅時，我們會收集資訊，包括受影響的資源和任何組態相關變更。AMS 每週 365 天、每天 24 小時全年無休 follow-the-sun 支援，專門的運算子會積極審查和調查所有受管帳戶的監控儀表板、事件佇列和服務請求。AMS 會與我們的安全專家調查調查結果，以分析活動，並透過您帳戶中列出的安全呈報聯絡人通知您。

根據我們的調查結果，AMS 會主動與您互動。如果您認為活動未經授權或可疑，AMS 會與您一起調查並修復或包含問題。GuardDuty 會產生某些問題清單類型，要求您先確認影響，AMS 才能採取任何動作。例如，GuardDuty 調查結果類型 UnauthorizedAccess : IAMUser/ConsoleLogin 表示您的其中一個使用者已從異常位置登入；AMS 會通知您，並要求您檢閱調查結果以確認此行為是否合法。

Amazon Macie

AWS Managed Services 建議您使用 Macie 來偵測大量且完整的敏感資料清單，例如個人健康資訊 (PHI)、個人身分識別資訊 (PII) 和財務資料。

Macie 可以設定為在任何 Amazon S3 儲存貯體上定期執行，隨著時間的推移，自動評估儲存貯體中的任何新物件或修改物件。產生安全調查結果時，AMS 會通知您，並視需要與您合作進行修復。

如需詳細資訊，請參閱[分析 Amazon Macie 調查結果](#)。

Amazon Macie 安全性

Macie 是一種人工智慧/AI 支援的安全服務，可透過自動探索、分類和保護存放在 AWS 中的敏感資料，協助您防止資料遺失。Macie 使用機器學習來識別敏感資料，例如個人身分識別資訊 (PII) 或智慧財產權、指派商業價值，並提供這些資料存放位置和組織中使用方式的可見性。Macie 會持續監控資料存取活動是否有異常，並在偵測到未經授權存取或意外資料外洩的風險時傳送提醒。Macie 服務支援 Amazon S3 和 AWS CloudTrail 資料來源。

AMS 會持續監控來自 Macie 的提醒，如果收到提醒，會採取快速動作來保護您的資源和帳戶。隨著 Macie 加入 AMS 支援的服務清單，我們現在也負責根據您的指示，在所有帳戶中啟用和設定 Macie。您可以在 Macie 提醒和我們的動作在 AWS 主控台或支援的整合中展開時加以檢視。在帳戶加入期間，您可以指定用來存放 PII 的帳戶。對於具有 PII 的所有新帳戶，建議使用 Macie。對於具有 PII 的現有帳戶，請聯絡我們，我們將在您的帳戶中將其開啟。因此，您可以獲得多一層的保護，並享受 AMS 管理之 AWS 環境中 Macie 的所有優點。

AMS Macie FAQs

- 當所有 AMS 帳戶都啟用 Trend Micro 和 GuardDuty 時，為什麼我需要 Macie？

Macie 可協助您對 Amazon S3 中的資料進行分類、資料對業務具有的值，以及與該資料存取相關聯的行為，以協助您保護 Amazon S3 中的資料。Amazon GuardDuty 透過協助識別威脅行為者偵察、執行個體問題和有問題的帳戶活動等威脅，為您的 AWS 帳戶、工作負載和資料提供廣泛的保護。這兩種服務都整合了使用者行為分析、機器學習和異常偵測，以偵測其各自類別中的威脅。Trend Micro 不會專注於識別 PII 和來自它們的威脅。

- 如何在我的 AMS 帳戶中開啟 Macie？

如果您的帳戶中存放 PII/PHI，或打算存放 PII/PHI，請聯絡您的 CSDM 或提出服務請求，為 AMS 管理的新帳戶或現有帳戶啟用 Macie。

- 在我的 AMS 帳戶中啟用 Macie 的成本影響是什麼？

Macie 定價適用於類似 Amazon Elastic Compute Cloud (Amazon EC2) 等其他服務的 AMS。您根據用量和根據 SLAs 的 AMS 提升來支付 Amazon Macie。Macie 費用是根據用量而定，請參閱以 AWS CloudTrail 事件和 [Amazon S3 儲存體為基礎的 Amazon Macie 定價](#)。Amazon S3 請注意，Macie 費用通常會在啟用後第二個月扁平化，因為它會根據新增至 Amazon S3 儲存貯體的增量資料收費。

若要進一步了解 Macie，請參閱 [Amazon Macie](#)。

GuardDuty

GuardDuty 是一種持續的安全監控服務，使用威脅情報摘要，例如惡意 IP 地址和網域的清單，以及機器學習，以識別 AWS 環境中非預期和可能未經授權的惡意活動。這可能包括權限提升、使用公開的登入資料，或與惡意 IP 地址或網域通訊等問題。GuardDuty 也會監控 Amazon Web Services 帳戶存取行為是否有入侵跡象，例如未經授權的基礎設施部署，例如部署在從未使用過的區域中的執行個體，或是不尋常的 API 呼叫，例如變更密碼政策以降低密碼強度。如需詳細資訊，請參閱 [GuardDuty 使用者指南](#)。

若要檢視和分析 GuardDuty 調查結果，請使用下列程序。

1. 開啟 [GuardDuty 主控台](#)。
2. 選擇問題清單，然後選擇特定問題清單以檢視詳細資訊。每個調查結果的詳細資訊會根據調查結果類型、涉及的資源和活動的性質而有所不同。

如需可用調查結果欄位的詳細資訊，請參閱 [GuardDuty 調查結果詳細資訊](#)。

GuardDuty 安全性

Amazon GuardDuty 提供威脅偵測，可讓您持續監控和保護您的 AWS 帳戶和工作負載。Amazon GuardDuty 會分析從您的帳戶產生的中繼資料連續串流，以及事件、Amazon VPC 流程日誌和網域名稱系統 (DNS) 日誌中找到 AWS CloudTrail 的網路活動。它還使用整合的威脅情報，例如已知的惡意 IP 地址、異常偵測和機器學習，以更準確地識別威脅。GuardDuty 是受監控的 AMS 服務。若要進一步了解 Amazon GuardDuty 監控，請參閱 [GuardDuty 監控](#)。若要進一步了解 GuardDuty，請參閱 [Amazon GuardDuty](#)。

所有新的 AMS 帳戶預設都已啟用 GuardDuty。AMS 會在帳戶加入期間設定 GuardDuty。您可以隨時提交變更請求來修改設定。GuardDuty 定價適用於 AMS，類似於其他服務，例如 Amazon Elastic Compute Cloud (Amazon EC2)。您需要根據用量和根據 SLAs 的 AMS 提升來支付 GuardDuty。GuardDuty 費用是根據用量 ([Amazon GuardDuty 定價](#))，根據 Amazon VPC Flow 日誌 AWS CloudTrail 的事件和數量來衡量。

針對 AMS 中的 GuardDuty，會啟用下列主要偵測類別：

- Reconnaissance -- 建議威脅行為者進行偵察的活動，例如異常 API 活動、VPC 內連接埠掃描、失敗的登入請求異常模式，或從已知的不良 IP 探勘的未封鎖連接埠。
- 執行個體問題 -- 有問題的執行個體活動，例如加密貨幣挖掘、使用網域產生演算法 (DGA) 的惡意軟體、傳出拒絕服務活動、異常大量的網路流量、異常網路通訊協定、與已知惡意 IP 的傳出執行個體通訊、外部 IP 地址使用的臨時 Amazon EC2 登入資料，以及使用 DNS 的資料外洩。
- 帳戶活動 -- 帳戶活動的常見模式包括來自異常地理位置或匿名代理的 API 呼叫、嘗試停用 AWS CloudTrail 記錄、異常執行個體或基礎設施啟動、異常 AWS 區域中的基礎設施部署，以及來自已知惡意 IP 地址的 API 呼叫。

AMS 會在您的受管帳戶中使用 GuardDuty 來持續監控 GuardDuty 的調查結果和提醒，如果收到提醒，AMS 操作會採取主動動作來保護您的資源和帳戶。您可以在 GuardDuty 調查結果和我們的動作在 AWS 主控台或支援的整合中展開時加以檢視。

GuardDuty 可與帳戶中的 Trend Micro Deep Security Manager 搭配使用。Trend Micro Deep Security Manager 提供主機型入侵偵測/入侵防護服務。Trend Micro Web Reputation 服務與 GuardDuty 有一些重疊，能夠偵測主機何時嘗試與已知為威脅的主機或 Web 服務通訊。不過，GuardDuty 提供額外的威脅偵測類別，並透過監控網路流量來達成此目的，這是一種與 Trend Micro 主機型偵測互補的方法。以網路為基礎的威脅偵測，如果主機出現有問題的行為，則不允許控制失敗，從而提高安全性。AMS 建議您在所有 AMS 帳戶中使用 GuardDuty。

若要進一步了解 Trend Micro，請參閱 [Trend Micro Deep Security Help Center](#)；請注意，非 Amazon 連結可能會變更，恕不另行通知。

GuardDuty 監控

GuardDuty 透過產生 AMS 擷取且可發出提醒的[安全調查結果](#)，通知您 AWS 環境的狀態。

Amazon GuardDuty 會透過分析和處理 VPC 流程日誌、AWS CloudTrail 事件日誌和網域名稱系統日誌，來監控 AWS 環境的安全性。您可以將 GuardDuty 設定為也使用您自己的自訂、信任 IP 清單和威脅清單，以擴展此監控範圍。

- 信任的 IP 清單包含您已允許與 AWS 基礎設施和應用程式進行安全通訊的 IP 地址。GuardDuty 不會針對信任 IP 清單中的 IP 地址產生問題清單。在任何指定的時間內，您在每一個區域的每一個 AWS 帳戶中僅能上傳一份信任 IP 清單。
- 威脅清單包含已知的惡意 IP 地址。GuardDuty 會根據威脅清單產生調查結果。在任何指定的時間內，您在每一個區域的每一個 AWS 帳戶中可以上傳六份威脅清單。

若要實作 GuardDuty，請使用 AMS CT 部署 | 監控和通知 | GuardDuty IP 組 | 建立 (ct-08avsj2e9mc7g) 來建立一組核准的 IP 地址。您也可以使用 AMS CT 部署 | 監控和通知 | GuardDuty 威脅 intel 集 | 建立 (ct-25v6r7t8gvkq5) 來建立一組遭拒的 IP 地址。

如需 AMS 監控的服務清單，請參閱 [AMS 監控系統監控什麼？](#)。

Amazon Route 53 Resolver DNS 防火牆

Amazon Route 53 Resolver 會以遞迴方式回應來自公開記錄、Amazon VPC 特定 DNS 名稱和 Amazon Route 53 私有託管區域的 AWS 資源的 DNS 查詢，且預設可在所有 VPCs 中使用。使用 Route 53 Resolver DNS 防火牆，您可以篩選和調節 Virtual Private Cloud (VPC) 的傳出 DNS 流量。為此，您可以在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合、將規則群組與 VPC 產生關聯，然後監控 DNS 防火牆日誌和指標中的活動。根據活動，您可以相應地調整 DNS 防火牆的行為。如需詳細資訊，請參閱[使用 DNS 防火牆篩選傳出 DNS 流量](#)。

若要檢視和管理 Route 53 Resolver DNS 防火牆組態，請使用下列程序：

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/vpc/>：// 開啟 Amazon VPC 主控台。
2. 在 DNS 防火牆下，選擇規則群組。
3. 檢閱、編輯或刪除現有的組態，或建立新的規則群組。如需詳細資訊，請參閱 [Route 53 Resolver DNS Firewall 的運作方式](#)。

Amazon Route 53 Resolver DNS 防火牆監控和安全性

Amazon Route 53 DNS Firewall 使用規則關聯、規則動作和規則評估優先順序的概念。網域清單是一組可重複使用的網域規格，可在規則群組的 DNS Firewall 規則中使用。當您將規則群組與 VPC 建立關聯時，DNS 防火牆會比較您的 DNS 查詢與規則中使用的網域清單。如果 DNS 防火牆找到相符項目，則會根據相符規則的動作來處理 DNS 查詢。如需規則群組和規則的詳細資訊，請參閱 [DNS 防火牆規則群組和規則](#)。

網域清單可分為兩個主要類別：

- 受管網域清單，可為您 AWS 建立和維護。
- 您自己的網域清單，由您建立和維護。

規則群組會根據其關聯優先順序索引進行評估。

根據預設，AMS 會部署基準組態，其中包含下列規則和規則群組：

- 一個名為的規則群組DefaultSecurityMonitoringRule。規則群組具有最高關聯優先順序，可在建立時針對每個啟用的每個現有 VPC 使用 AWS 區域。
- 一個在規則群組中DefaultSecurityMonitoringRule以優先順序 1 命名的DefaultSecurityMonitoringRule規則，使用AWSManagedDomainsAggregateThreatList受管網域清單搭配動作 ALERT。

如果您有現有的組態，則會以低於現有組態的優先順序部署基準組態。您現有的組態是預設值。如果您現有的組態不提供如何處理查詢解析的較高優先順序指示，則可以使用 AMS 基準組態做為全部截獲。若要變更或移除基準組態，請執行下列其中一項操作：

- 請聯絡您的 Cloud Service Delivery Manager (CSDM) 或 Cloud Architect (CA)。
- 使用 [Management | Other | Other | Create CT \(ct-1e1xtak34nx76\) 建立變更請求 \(RFC\)](#)。
- 建立服務請求。

如果您的帳戶是在開發人員模式或直接變更模式下操作，您可以自行執行變更。

AWS Certificate Manager (ACM) 憑證

AMS 具有 CT、部署 | 進階堆疊元件 | ACM 憑證搭配其他 SANs | 建立 (ct-3l14e139i5p50)，可用來提交 AWS Certificate Manager 憑證的請求，以及最多五個額外的主體替代名稱 (SAN) (例如 example.com、example.net 和 example.org)。如需詳細資訊，請參閱[什麼是 AWS Certificate Manager ?](#) 和 [ACM 憑證特性](#)。

Note

此逾時設定不僅與執行有關，也與透過電子郵件驗證 ACM 憑證的驗證有關。如果沒有您的驗證，RFC 會失敗。

AMS 中的資料加密

AMS 使用多項 AWS 服務進行資料加密，特別是 Amazon Simple Storage Service、AWS Key Management Service (AWS KMS)、Amazon Elastic Block Store、Amazon Relational Database Service Amazon Redshift Amazon ElastiCache AWS Lambda 和 Amazon OpenSearch Service。

Amazon Simple Storage Service (Amazon S3)

Amazon S3 提供多種物件加密選項，可保護傳輸中和靜態資料。伺服器端加密會先加密您的物件，再將該物件儲存至其資料中心內的磁碟，接著在下載物件時予以解密。只要您驗證要求並具備存取許可，存取加密物件或未加密物件的方式並無不同。如需詳細資訊，請參閱 [Amazon S3 中的資料保護](#)。

Amazon EBS

使用 Amazon EBS 加密，您不需要建置、維護和保護自己的金鑰管理基礎設施。Amazon EBS 加密會在建立加密磁碟區和快照時使用 AWS KMS 金鑰。加密操作會在託管 Amazon EC2 執行個體的伺服器上進行。這是為了確保執行個體與其連接的 Amazon EBS 儲存體之間的 data-at-rest 和 data-in-transit 都是安全的。您可以將加密和未加密磁碟區同時連接到執行個體。如需詳細資訊，請參閱 [Amazon EBS 加密](#)。

Amazon RDS

Amazon RDS 可以加密 Amazon RDS 資料庫執行個體。靜態加密的資料包括資料庫執行個體的基本儲存體、其自動備份、僅供讀取複本和快照。Amazon RDS 加密資料庫執行個體使用業界標準的 AES-256 加密演算法，在託管 Amazon RDS 資料庫執行個體的伺服器上加密您的資料。加密資料後，Amazon RDS 會以透明的方式處理資料的存取和解密身分驗證，且對效能的影響最小。您不需要修改資料庫用戶端應用程式即可使用加密。如需詳細資訊，請參閱 [加密 Amazon RDS 資源](#)。

Amazon Simple Queue Service

除了預設的 Amazon SQS 受管伺服器端加密 (SSE) 選項之外，Amazon SQS 受管 SSE (SSE-SQS) 還可讓您建立自訂受管伺服器端加密，使用 Amazon SQS 受管加密金鑰來保護透過訊息佇列傳送的敏感資料。伺服器端加密 (SSE) 可讓您在加密佇列中傳輸敏感資料。SSE 會使用 Amazon SQS 受管加密金鑰 (SSE-SQS) 或 AWS KMS (SSE-KMS) 中管理的金鑰來保護佇列中的訊息內容。如需有關使用管理 SSE 的資訊 AWS Management Console，請參閱 [靜態加密](#)。

靜態資料加密

OpenSearch Service 網域提供靜態資料加密，這是一種安全功能，可協助防止未經授權存取您的資料。此功能使用 AWS Key Management Service (AWS KMS) 來存放和管理加密金鑰，並使用 256 位

元金鑰 (AES-256) 的進階加密標準演算法來執行加密。如需詳細資訊，請參閱 [Amazon OpenSearch Service 的靜態資料加密](#)。

金鑰管理

AWS KMS 是一項受管服務，可讓您輕鬆地建立和控制客戶主金鑰 (CMKs)，用來加密資料的加密金鑰。AWS KMS CMKs 受到 FIPS 140-2 密碼編譯模組驗證計畫驗證的硬體安全模組 (HSMs) 保護，但中國（北京）和中國（寧夏）區域除外。如需詳細資訊，請參閱 [什麼是 AWS Key Management Service？](#)

身分與存取管理

AWS Identity and Access Management (IAM) 是一種 Web 服務，可協助您安全地控制對 AWS 資源的存取。您可以使用 IAM 來控制 (已登入) 的身分驗證和授權使用資源的 (許可)。在 AMS 加入期間，您有責任在每個受管帳戶中建立跨帳戶 IAM 管理員角色。

多帳戶登陸區域 (MALZ) IAM 防護措施

AMS 多帳戶登陸區域 (MALZ) 需要 Active Directory (AD) 信任作為 AMS 存取管理的主要設計目標，以允許每個組織（包括 AMS 和客戶）管理其身分的生命週期。這樣就不需要在彼此的目錄中擁有登入資料。已設定單向信任，因此中的受管 Active Directory AWS 帳戶信任客戶擁有或受管 AD 來驗證使用者。由於信任只是一種方式，並不表示 Managed AD 受客戶 Active Directory 信任。

在此組態中，管理使用者身分的客戶目錄稱為使用者樹系，而連接 Amazon EC2 執行個體的受管 AD 稱為資源樹系。這是 Windows 身分驗證常用的 Microsoft 設計模式；如需詳細資訊，請參閱 [樹系設計模型](#)。

此模型可讓這兩個組織自動化各自的生命週期，並允許 AMS 和您在員工離開組織時快速撤銷存取權。如果沒有此模型，如果兩個組織都使用通用目錄（或在彼此的目錄中建立使用者/群組），則兩個組織都必須放入其他工作流程和使用者同步，以考慮員工開始和離開。這會帶來風險，因為該程序具有延遲，而且可能容易出錯。

MALZ 存取先決條件

存取 AWS/AMS 主控台、CLI、軟體開發套件的 MALZ Identity Provider Integration。

您 AMS 帳戶中 Amazon EC2 執行個體的單向信任。

使用身分驗證

AMS 使用 IAM 角色，這是一種 IAM 身分。IAM 角色與使用者非常類似，因為它是具有許可政策的身分，可決定身分在 中可以和不可以執行的動作 AWS。不過，角色沒有與其相關聯的登入資料，而不是唯一地與一個人相關聯，任何需要該角色的人都可以擔任該角色。IAM 使用者可擔任一個角色，為了特定任務來臨時採用不同許可。

存取角色由內部群組成員資格控制，由 Operations Management 管理並定期審查。

AMS 中的 IAM 使用者角色

IAM 角色類似於 IAM 使用者，因為它是具有許可政策的 AWS 身分，可決定身分在其中可以和不可以執行的動作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。

對於標準 AMS 帳戶，目前有一個 AMS 預設使用者角色 `Customer_ReadOnly_Role`，對於具有 Managed Active Directory `customer_managed_ad_user_role` 的 AMS 帳戶，則有一個額外的角色。

角色政策會設定 CloudWatch 和 Amazon S3 日誌動作、AMS 主控台存取、大多數的唯讀限制 AWS 服務、帳戶 S3 主控台的限制存取，以及 AMS 變更類型存取的許可。

此外，`Customer_ReadOnly_Role` 具有變動的 `reserved-instances` 許可，可讓您保留執行個體。它有一些節省成本的值，因此，如果您知道需要長時間特定數量的 Amazon EC2 執行個體，您可以呼叫這些 APIs。若要進一步了解，請參閱 [Amazon EC2 預留執行個體](#)。

Note

為 IAM 使用者建立自訂 IAM 政策的 AMS 服務層級目標 (SLO) 為四個工作天，除非將重複使用現有政策。如果您想要修改現有的 IAM 使用者角色，或新增新的角色，請分別提交 [IAM：更新實體](#) 或 [IAM：建立實體](#) RFC。

如果您不熟悉 Amazon IAM 角色，請參閱 [IAM 角色](#) 以取得重要資訊。

多帳戶登陸區域 (MALZ)：若要查看 AMS 多帳戶登陸區域預設、非自訂的使用者角色政策，請參閱 [MALZ：預設 IAM 使用者角色](#)，下一步。

MALZ：預設 IAM 使用者角色

預設多帳戶 AMS 多帳戶登陸區域使用者角色的 JSON 政策陳述式。

Note

使用者角色是可自訂的，而且可能因帳戶而異。提供尋找角色的說明。

這些是預設 MALZ 使用者角色的範例。為了確保您已設定所需的政策，請執行 AWS 命令 [get-role](#) 或登入 AWS Management -> [IAM 主控台](#)，然後在導覽窗格中選擇角色。

核心 OU 帳戶角色

核心帳戶是 MALZ 管理的基礎設施帳戶。AMS 多帳戶登陸區域 核心帳戶包括管理帳戶和聯網帳戶。

核心 OU 帳戶：常用角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公有 AWS 受管政策)。
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess (公有 AWS 受管政策)。
AWSManagedServicesChangeManagementRole (核心帳戶版本)	ReadOnlyAccess AWSSupportAccess AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy

核心 OU 帳戶：管理帳戶角色和政策

角色	政策或政策
AWSManagedServicesBillingRole	AMSBillingPolicy (AMSBillingPolicy)。
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公有 AWS 受管政策)。
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess (公有 AWS 受管政策)。

角色	政策或政策
AWSManagedServicesChangeManagementRole (管理帳戶版本)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

核心 OU 帳戶：聯網帳戶角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公有 AWS 受管政策)。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess (公有 AWS 受管政策)。
AWSManagedServicesChangeManagementRole (網路帳戶版本)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

應用程式帳戶角色

應用程式帳戶角色會套用至您的應用程式特定帳戶。

應用程式帳戶：角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公有 AWS 受管政策)。
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess (公有 AWS 受管政策)。 此政策提供所有支援操作和資源的存取權。如需詳細資訊，請參閱 AWS Support 入門 。
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSSupportAccess 範例 此政策提供所有支援操作和資源的存取權。 AWSCertificateManagerFullAccess 資訊，(公有 AWS 受管政策) AWSWAFFullAccess 資訊，(公有 AWS 受管政策)。此政策授予 AWS WAF 資源的完整存取權。 AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (應用程式帳戶版本)	ReadOnlyAccess AWSSupportAccess (公有 AWS 受管政策)。 此政策提供所有支援操作和資源的存取權。如需詳細資訊，請參閱 AWS Support 入門 。 AMSSecretsManagerSharedPolicy AMSChangeManagementPolicy AMSReservedInstancesPolicy AMSS3Policy

角色	政策或政策
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccess
	AMSCheckManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSCheckManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Policy
	AMSReservedInstancesPolicy

政策範例

範例適用於大多數使用的政策。若要檢視 `ReadOnlyAccess` 政策（這是提供所有 AWS 服務的唯讀存取權的頁面），如果您有作用中的 AWS 帳戶：[ReadOnlyAccess](#)，您可以使用此連結。此外，此處也包含精簡版本。

AMSBillingPolicy

AMSBillingPolicy

您的會計部門可以使用新的帳單角色來檢視和變更 管理帳戶中的帳單資訊或帳戶設定。若要存取替代聯絡人、檢視帳戶資源用量，或保留帳單標籤，或甚至修改您的付款方式等資訊，您可以使用此角色。此新角色包含 [AWS Billing IAM 動作網頁](#) 中列出的所有許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Action": [
    "aws-portal:ViewBilling",
    "aws-portal:ModifyBilling"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToBilling"
},
{
  "Action": [
    "aws-portal:ViewAccount",
    "aws-portal:ModifyAccount"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToAccountSettings"
},
{
  "Action": [
    "budgets:ViewBudget",
    "budgets:ModifyBudget"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToAccountBudget"
},
{
  "Action": [
    "aws-portal:ViewPaymentMethods",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToPaymentMethods"
},
{
  "Action": [
    "aws-portal:ViewUsage"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToUsage"
},
}
```

```
{
  "Action": [
    "cur:DescribeReportDefinitions",
    "cur:PutReportDefinition",
    "cur>DeleteReportDefinition",
    "cur:ModifyReportDefinition"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToCostAndUsageReport"
},
{
  "Action": [
    "pricing:DescribeServices",
    "pricing:GetAttributeValues",
    "pricing:GetProducts"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToPricing"
},
{
  "Action": [
    "ce:*",
    "compute-optimizer:*"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToCostExplorerComputeOptimizer"
},
{
  "Action": [
    "purchase-orders:ViewPurchaseOrders",
    "purchase-orders:ModifyPurchaseOrders"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToPurchaseOrders"
},
{
  "Action": [
    "redshift:AcceptReservedNodeExchange",
    "redshift:PurchaseReservedNodeOffering"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "AllowAccessToRedshiftReservedNodes"
```

```
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToRedshiftAction"
    },
    {
        "Action": "savingsplans:*",
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AWSSavingsPlansFullAccess"
    }
]
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

檢視所有 AMS 變更類型的許可，以及所請求變更類型的歷史記錄。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

請求部署 | 受管登陸區域 | 管理帳戶 | 建立應用程式帳戶 (使用 VPC) 變更類型的許可。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

請求部署 | 受管登陸區域 | 網路帳戶 | 建立應用程式路由表變更類型的許可。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (適用於管理 | 其他 | CTs)

請求管理 | 其他 | 其他 | 建立和管理 | 其他 | 其他 | 更新變更類型的許可。

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

檢視 AMS 透過 共用之秘密密碼/雜湊的許可 AWS Secrets Manager (例如，稽核基礎設施的密碼)。

建立秘密密碼/雜湊以與 AMS 共用的許可 (例如，需要部署之產品的授權金鑰)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
```

AMSCChangeManagementPolicy

AMSCChangeManagementPolicy

請求和檢視所有 AMS 變更類型的許可，以及請求變更類型的歷史記錄。

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

管理 Amazon EC2 預留執行個體的許可；如需定價資訊，請參閱 [Amazon EC2 預留執行個體](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}
```

AMSS3Policy

AMSS3Policy

從現有 Amazon S3 儲存貯體建立和刪除檔案的許可。

Note

這些許可不會授予建立 S3 儲存貯體的能力；必須使用部署 | 進階堆疊元件 | S3 儲存 | 建立變更類型來完成。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",

```

```
        "s3:DeleteObject",
        "s3:PutObject"
    ],
    "Resource": "*"
}
]
```

AWSSupportAccess

AWSSupportAccess

完整存取 支援。如需詳細資訊，請參閱 [入門 支援](#)。如需 Premium Support 資訊，請參閱 [支援](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ],
    "Resource": "*"
  }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions (公有 AWS 受管政策)

訂閱、取消訂閱和檢視 AWS Marketplace 訂閱的許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
```



```
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
],
"Effect": "Allow",
"Resource": "*"
}]
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

完整存取 AWS Certificate Manager。如需詳細資訊，請參閱[AWS Certificate Manager](#)。

[AWSCertificateManagerFullAccess](#) 資訊，（公有 AWS 受管政策）。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
    "Resource": "*"
  }]
}
```

AWSWAFFullAccess

AWSWAFFullAccess

完整存取 AWS WAF。如需詳細資訊，請參閱 [AWS WAF - Web Application Firewall](#)。

[AWSWAFFullAccess](#) 資訊（公有 AWS 受管政策）。此政策授予 AWS WAF 資源的完整存取權。

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [{
  "Action": [
    "waf:*",
    "waf-regional:*",
    "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
}]
}
```

ReadOnlyAccess

ReadOnlyAccess

在 AWS 主控台上唯讀存取所有 AWS 服務和資源。AWS 啟動新服務時，AMS 會更新 ReadOnlyAccess 政策，為新服務新增唯讀許可。更新的許可會套用於政策連接到的所有主體實體。

這不會授予登入 EC2 主機或資料庫主機的能力。

如果您有作用中的 AWS 帳戶，則可以使用此連結 [ReadOnlyAccess](#) 來檢視整個 ReadOnlyAccess 政策。整個 ReadOnlyAccess 政策只要提供所有的唯讀存取權即可 AWS 服務。以下是 ReadOnlyAccess 政策的部分摘錄。

單一帳戶登陸區域 (SALZ)：若要查看 AMS 單一帳戶登陸區域預設、非自訂的使用者角色政策，請參閱 [SALZ：預設 IAM 使用者角色](#)，下一步。

SALZ：預設 IAM 使用者角色

預設 AMS 單一帳戶登陸區域使用者角色的 JSON 政策陳述式。

Note

SALZ 預設使用者角色可自訂，且可能因帳戶而異。提供尋找角色的說明。

以下是預設 SALZ 使用者角色的範例。若要確保您已為您設定政策，請執行 [get-role](#) 命令。或者，前往 <https://console.aws.amazon.com/iam/> 登入 AWS Identity and Access Management 主控台，然後選擇角色。

客戶唯讀角色是多個政策的組合。角色 (JSON) 的明細如下。

Managed Services 稽核政策：

Managed Services IAM ReadOnly 政策

Managed Services 使用者政策

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
```

```
"Effect": "Allow",
"Action": [
  "s3:GetObject"
],
"Resource": [
  "arn:aws:s3:::mc-a*-logs-*/aws/*",
  "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
]
},
{
  "Sid": "AllowAccessToOtherObjects",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject",
    "s3:Get*",
    "s3:List*",
    "s3:PutObject"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCustomerToListTheLogBucketRoot",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ],
  "Condition": {
    "StringEquals": {
      "s3:prefix": [
        "",
        "/"
      ]
    }
  }
},
{
  "Sid": "AllowCustomerCWLConsole",
  "Effect": "Allow",
  "Action": [
```

```

        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
    ]
},
{
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
        "amscm:*",
        "amsskms:*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "ModifyAWSBillingPortal",
    "Effect": "Allow",
    "Action": [
        "aws-portal:Modify*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "DenyDeleteCWL",

```

```
"Effect": "Deny",
"Action": [
  "logs:DeleteLogGroup",
  "logs:DeleteLogStream"
],
"Resource": [
  "arn:aws:logs:*:*:log-group:*"
]
},
{
  "Sid": "DenyMCCWL",
  "Effect": "Deny",
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents",
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/mc/*"
  ]
},
{
  "Sid": "DenyS3MCNamespace",
  "Effect": "Deny",
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
    "arn:aws:s3:::mc-a*-logs-*/mc/*",
    "arn:aws:s3:::mc-a*-logs-*--audit/*",
    "arn:aws:s3:::mc-a*-internal-*/*",
    "arn:aws:s3:::mc-a*-internal-*"
  ]
},
{
  "Sid": "ExplicitDenyS3CfnBucket",
  "Effect": "Deny",
  "Action": [
    "s3:*"
  ],

```

```
"Resource": [
  "arn:aws:s3:::cf-templates-*"
],
{
  "Sid": "DenyListBucketS3LogsMC",
  "Action": [
    "s3:ListBucket"
  ],
  "Effect": "Deny",
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ],
  "Condition": {
    "StringLike": {
      "s3:prefix": [
        "auditlog/*",
        "encrypted/mc/*",
        "mc/*"
      ]
    }
  }
},
{
  "Sid": "DenyS3LogsDelete",
  "Effect": "Deny",
  "Action": [
    "s3:Delete*",
    "s3:Put*"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*/*"
  ]
},
{
  "Sid": "DenyAccessToKmsKeysStartingWithMC",
  "Effect": "Deny",
  "Action": [
    "kms:*"
  ],
  "Resource": [
    "arn:aws:kms::*:key/mc-*",
    "arn:aws:kms::*:alias/mc-*"
  ]
}
```



```
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Customer Secrets Manager 共用政策

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Sid": "AllowSecretsManagerListSecrets",
"Effect": "Allow",
"Action": "secretsmanager:listSecrets",
"Resource": "*"
},
{
  "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
  "Effect": "Allow",
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ]
},
{
  "Sid": "DenyCustomerGetSecretCustomerNamespace",
  "Effect": "Deny",
  "Action": "secretsmanager:GetSecretValue",
  "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
},
{
  "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
  "Effect": "Deny",
  "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
  ],
  "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
}
]
}
```

Customer Marketplace 訂閱政策

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
```

```
"Effect": "Allow",
"Action": [
    "aws-marketplace:ViewSubscriptions",
    "aws-marketplace:Subscribe"
],
"Resource": [
    "*"
]
}
```

安全事件記錄和監控

AMS 會持續監控受管環境是否有安全威脅。AMS 或您可能會偵測到安全事件。AMS 會根據國家標準技術研究所 (NIST) 的電腦安全事件處理指南，定期更新其自動化程序，以更好地偵測安全威脅。

端點安全 (EPS)

您在 AMS Advanced 環境中佈建的資源會自動包含端點安全 (EPS) 監控用戶端的安裝。此程序可確保 24 小時全年無休監控和支援 AMS 進階受管資源。此外，AMS Advanced 會監控所有代理程式活動，並在偵測到任何安全事件時建立事件。

Note

安全事件會視為事件處理；如需詳細資訊，請參閱[事件回應](#)。

端點安全提供反惡意軟體保護，特別是支援下列動作：

- EC2 執行個體向 EPS 註冊
- EC2 執行個體從 EPS 取消註冊
- EC2 執行個體即時反惡意軟體保護
- EPS 代理程式起始的心跳
- EPS 還原隔離的檔案
- EPS 事件通知
- EPS 報告

AMS Advanced 使用 Trend Micro 進行端點安全 (EPS)。這些是預設的 EPS 設定。若要進一步了解 Trend Micro，請參閱 [Trend Micro Deep Security Help Center](#)；請注意，非 Amazon 連結可能會變更，恕不另行通知。

AMS 進階多帳戶登陸區域 (MALZ) 預設設定如下列各節所述；對於非預設 AMS 多帳戶登陸區域 EPS 設定，請參閱 [AMS 進階多帳戶登陸區域 EPS 非預設設定](#)。

Note

您可以自備 EPS，請參閱 [AMS 自備 EPS](#)。

一般 EPS 設定

端點安全一般網路設定。

EPS 預設值

設定	預設
防火牆連接埠（執行個體的安全群組）	EPS Deep Security Manager 代理程式 (DSMs) 必須針對 Agent/Relay to Manager 通訊開啟連接埠 4120，以及針對 Manager Console 開啟連接埠 4119。EPS 轉送必須開啟連接埠 4122，管理員/客服人員才能轉送通訊。客戶執行個體傳入通訊不應開啟任何特定連接埠，因為客服人員會啟動所有請求。
通訊方向	代理程式/應用程式啟動
活動訊號間隔	十分鐘
警示之前的遺失活動訊號數目	Two
伺服器時間之間允許的偏離上限（差異）	無限制
為非作用中（已註冊但未上線）虛擬機器引發離線錯誤	否
預設政策	基本政策（接下來說明）

設定	預設
啟用具有相同主機名稱的多部電腦	允許
已提出待定更新的提醒	七天後
更新排程	AMS 以 Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) 軟體更新的每月發行週期為目標。不過，AMS 不會維護更新用的 SLA。AMS 開發人員團隊會在部署期間在整個機群中執行更新。 DSA/DSA 更新會記錄在 Trend Micro DSM 系統事件中，AMS 預設會在本機保留 13 週。如需廠商文件，請參閱 Trend Micro Deep Security Help Center 中的系統事件。日誌也會匯出至 Amazon CloudWatch 中的日誌群組 <code>/aws/ams/eps/var/log/DSM.log</code>。
更新來源	Trend Micro Update Server (https://ipv6-iaus.trendmicro.com/iau_server.dll/ : //)
事件或日誌資料刪除	事件和日誌會在七天後從 DSM 資料庫刪除。
保留代理程式軟體版本	最多五個
保留最新的規則更新	最多十個
日誌儲存	根據預設，日誌檔案會安全地存放在 Amazon S3 中，但您也可以將其封存至 Amazon Glacier，以協助滿足稽核和合規要求。

基本政策

端點安全基礎政策預設設定。

EPS 基本政策

設定	預設
已啟用的模組	反惡意軟體
已停用的模組	Web 評價
	防火牆
	入侵保護
	完整性監控
	日誌檢查
	應用程式控制

反惡意軟體

端點安全反惡意軟體設定。

EPS 反惡意軟體預設值

設定	預設	備註
即時掃描	掃描所有項目	隔離所有可疑病毒。 啟用 IntelliTrap 和間諜軟體/灰色軟體保護。 間諜軟體和灰色軟體會觸發反惡意軟體，並導致項目隔離。
	每天/全天 (24 小時)	
手動掃描	掃描所有項目	必須請求，然後遵循預設的即時掃描組態。

設定	預設	備註
排程掃描	掃描所有項目	為每月最後一個星期日上午 6 點進行設定。
智慧保護	已停用	N/A
隔離的檔案	Trend Micro Deep Security Manager (DSM)	大約保留 1GB 的磁碟進行隔離。
掃描限制	Trend Micro DSM	掃描所有大小的檔案。
允許的間諜軟體或灰色軟體	無	N/A
本機事件通知	是	N/A

惡意軟體緩解程序

AMS 使用 Trend Micro 的 Deep Security Platform（反惡意軟體系統）來偵測和回應 AMS 受管執行個體上的惡意軟體。根據預設，針對 Windows 和 Linux 作業系統，Trend Micro 偵測代理程式會在所有 Amazon EC2 執行個體上執行，包括共用服務和私有子網路中的執行個體。反惡意軟體系統會連線至 AMS 監控，以便在偵測到惡意軟體時產生事件。如果有客戶影響，事件會呈報至事件管理程序（如需詳細資訊，請參閱 [AMS 事件回應](#)）。雖然 AMS 會評估影響，但會通知您，並嘗試減輕影響。

當 Trend Micro 發佈更新時，會自動更新 Trend Micro 反惡意軟體定義。

在應用程式加入期間，您會指出在執行個體上發現惡意軟體時，您希望 AMS 採取的動作：

- 確定隔離的檔案在允許清單上，將其從隔離中移除並傳回至檔案系統。
- 刪除隔離的檔案，將其從執行個體中移除。
- 暫停執行個體並加以取代。然後，暫停的執行個體可供您掛載以進行鑑識研究。

應用程式加入後：

- 當反惡意軟體系統在執行個體上發現惡意軟體時，AMS 會自動隔離惡意軟體。這會觸發事件和後續調查。

- AMS 透過服務通知通知您事件，並開始遵循您選取的預設緩解動作。
- 如果您尚未選擇預設動作，AMS 會詢問您要採取的動作。收到指示後，AMS 會執行選取的動作並通知您。如果適用，AMS 會在動作完成後再次通知您，包括鑑識分析所需的詳細資訊。

在 Trend Micro Deep Security 中啟用 IDS 和 IPS

您可以請求 AMS 為您的帳戶啟用 Trend Micro 入侵偵測系統 (IDS) 和入侵保護系統 (IPS)，非預設功能。

若要這樣做，請提交更新請求（管理 | 其他 | 其他 | 更新），並包含接收 IDS 和 IPS 通知的電子郵件地址清單。這些地址會新增至您帳戶中的 SNS 主題，AMS 會為您建立該主題。

Note

AMS 無法新增任何可能干擾我們提供其他 AMS 服務能力的 Trend Micro 服務。

完整系統惡意軟體掃描

支付卡產業資料安全標準 (PCI DSS) 需要完整的系統惡意軟體掃描，這些掃描預設為在您的 AMS 受管 VPC 上啟用。完整系統掃描設定為在 2AM 點（在伺服器上設定的時區）進行，因為它們使用大量的 CPU。除了一般惡意軟體掃描之外，還需使用大量 CPU。

有新的管理變更類型 (CT) 停用惡意軟體掃描，可讓您停用完整的系統惡意軟體掃描。您可以在 管理 | 主機安全 | 完整系統掃描 | 停用分類、變更 ID ct-1pybwg08h8qsz 中找到 CT。若要重新啟用掃描，請使用管理 | 其他 | 其他 | 更新 CT。停用完整系統掃描不會停用您的一般惡意軟體掃描。

Amazon Inspector 安全性

Amazon Inspector 服務會監控 AMS 受管堆疊的安全性。Amazon Inspector 是一種自動化安全評估服務，可協助識別部署在 上之基礎設施的安全性和合規性漏洞 AWS。Amazon Inspector 安全評估可讓您檢查 Amazon EC2 執行個體中的意外網路可存取性和漏洞，以自動評估堆疊是否存在暴露、漏洞和與最佳實務的偏差。執行評估後，Amazon Inspector 會依據嚴重性層級，產生詳細的安全調查結果清單。Amazon Inspector 評估會以映射至常見安全最佳實務和定義的預先定義規則套件提供。AWS 安全研究人員會定期更新這些規則。如需 Amazon Inspector 的詳細資訊，請前往 [Amazon Inspector](#)。

AMS Amazon Inspector FAQs

- 根據預設，Amazon Inspector 是否安裝在我的 AMS 帳戶中？

否。Amazon Inspector 不屬於預設 AMI 建置或工作負載擷取。

- 如何存取和安裝 Amazon Inspector？

提交 RFC（管理 | 其他 | 其他 | 建立）以向 Inspector 請求帳戶存取和安裝，而 AMS 操作團隊將修改 Customer_ReadOnly_Role 以提供 Amazon Inspector 主控台存取（沒有 SSM 存取）。

- 是否必須在要評估的所有 Amazon EC2 執行個體上安裝 Amazon Inspector Agent？Amazon EC2

否，任何 Amazon EC2 執行個體都可以在沒有代理程式的情況下執行具有網路連線能力規則套件的 Amazon Inspector 評估。Amazon EC2 主機評估規則套件需要代理程式。如需代理程式安裝的詳細資訊，請參閱[安裝 Amazon Inspector Agents](#)。

- 此服務是否需要支付額外費用？

是。您可以在 Amazon Inspector 定價網站上找到 [Amazon Inspector 定價](#)。

- 什麼是 Amazon Inspector 調查結果？

調查結果是在所選評估目標的 Amazon Inspector 評估期間發現的潛在安全問題。調查結果會顯示在 Amazon Inspector 主控台或 API 中，並同時包含安全問題的詳細說明和解決這些問題的建議。

- 是否提供 Amazon Inspector 評估的報告？

是。評估報告詳細說明了評估過程中的測試內容和評估結果。您的評估結果是標準格式的報告，您可以在團隊內分享修復動作的成果，豐富合規稽核資料或儲存以供將來參考。成功完成 Amazon Inspector 評估報告後，即可為評估執行產生該報告。

- 我可以使用標籤來識別要執行 Amazon Inspector 報告的堆疊嗎？

是。

- AMS Operations 團隊是否可以存取 Amazon Inspector 評估結果？

是。有權存取 AWS 中 Amazon Inspector 主控台的任何人都可以檢視問題清單和評估報告。

- AMS Operations 團隊是否會根據 Amazon Inspector 報告的調查結果建議或採取動作？

否。如果您想要根據 Amazon Inspector 報告的調查結果進行變更，必須透過 RFC（管理 | 其他 | 其他 | 更新）請求變更。

- 當我執行 Amazon Inspector 報告時，是否會通知 AMS？

當您請求 Amazon Inspector 存取時，執行 RFC 的 AMS Operator 會向您的 CSDM 通知請求。

如需詳細資訊，請參閱 [Amazon Inspector FAQs](#)。

AMS 事件回應

AMS 使用傳統的 IT 服務管理 (ITSM) 事件管理最佳實務，在需要時盡快還原服務。

我們透過全球各地的多個操作中心提供全年無休follow-the-sun支援，讓專屬的操作員主動監控儀表板和事件佇列。

我們的營運工程師使用內部事件追蹤工具來識別、記錄、分類、排定優先順序、診斷、解決和關閉事件，並透過 AMS 主控台或透過 支援 API 提供所有這些活動的更新。我們的運算子，其中許多已在各種技術設定檔和角色中花費 AWS Premium Support 的時間，利用各種內部 支援 工具來協助處理所有這些活動。這些運算子非常熟悉 AMS 支援的基礎設施，並具備專家層級的技術技能來解決所有已識別的支援問題。在極少數情況下，我們的營運商需要協助，Premium Support and AWS Service 團隊可視需要提供協助。

在高優先順序事件影響關鍵工作負載的情況下，AMS 會建議基礎設施還原。疑難排解問題或從已知的良好備份還原之間，通常存在權衡，而客戶因服務停機時間的風險和影響是決定因素。如果您有時間對問題進行故障診斷，AMS 會為您提供協助，但如果急迫性很高，我們可以立即啟動還原。

Note

不屬於堆疊範本或資料還原的暫時性資料會遺失。AMS 會盡合理努力在 AWS 服務方案無法使用時執行基礎設施還原。一旦 AWS 服務方案可用，基礎設施還原即完成。

如果您未依照 AMS 的建議授權基礎設施還原，則不符合事件解決時間的 AMS 服務承諾的服務額度資格。

法規遵循驗證

AMS 部署和管理 AWS Config 規則和修補動作的程式庫，以防止可能降低帳戶安全性和操作完整性的錯誤設定。

例如，建立 Amazon S3 儲存貯體時，AWS Config 可以根據要求 Amazon S3 儲存貯體拒絕公開讀取存取的規則來評估 Amazon S3 儲存貯體。如果 Amazon S3 儲存貯體政策或儲存貯體存取控制清單 (ACL) 允許公開讀取存取，會將儲存貯體和規則 AWS Config 標記為不合規。這些會根據資源的評估結果，將資源 AWS Config 規則 標記為合規、不合規或不適用。如需 AWS Config 服務的詳細資訊，請參閱 [AWS Config 開發人員指南](#)。

您可以使用 AWS Config 主控台、AWS CLI 或 AWS Config API 來檢視您帳戶中部署的規則，以及規則和資源的合規狀態。如需詳細資訊，請參閱 AWS Config 文件：[檢視組態合規](#)。

Note

如需本主題的其他資訊，請參閱 AWS Artifact 報告。如需詳細資訊，請參閱在 [AWS Artifact 中下載報告](#)。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。此資訊不包含在本使用者指南中，因為它包含敏感的安全內容。

檢視您 合規狀態的多帳戶登陸區域 AWS Config 規則

AMS 多帳戶登陸區域會利用 AWS Config 彙整工具服務，建立所有帳戶的合規集中檢視。這表示您可以在安全帳戶中的彙總工具下，查看 AMS 多帳戶登陸區域環境中 AWS Config 規則 所有 AWS Config 的合規狀態。

以下是 AWS Config 彙總工具的範例，顯示 AWS Config 規則 跨 帳戶的中央合規狀態。

如需詳細資訊，請參閱 [Config Aggregator](#) 的 AWS 文件。

- AMS 如何使用 AWS Config 規則？

AMS 會建立 AWS Config 規則，以便根據規則中指定的條件來查看 AWS 資源的組態。如果規則不合規，您可以請求變更，AMS Ops 團隊將與您合作採取更正動作。

- 在這種情況下，您會在 AMS 帳戶中看到下列變更：
 - AWS Config 規則 在 AWS Config > 規則下
 - 包含其 Lambda 函數的自訂 Config 規則存在於您的帳戶中
 - 安全帳戶中的 Config 彙總器和所有帳戶中的 Config 授權（僅限多帳戶登陸區域）

以下是 的範例 AWS Config 規則，其合規評估結果如下所示：

若要進一步了解 AWS Config，請參閱：

- AWS Config：[什麼是 Config？](#)
- AWS Config 規則：[使用規則評估資源](#)
- AWS Config 規則：[動態合規檢查：AWS Config 規則 – 雲端資源的動態合規檢查](#)
- AWS Config 彙總工具：[多帳戶多區域資料彙總](#)

AMS 多帳戶登陸區域服務控制政策限制

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

恢復能力

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。AWS 區域 提供多個實體分隔和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

基礎架構安全

Note

如需本主題的其他資訊，請參閱 AWS Artifact 報告。如需詳細資訊，請參閱[在 AWS Artifact 中下載報告](#)。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。此資訊不包含在本使用者指南中，因為它包含敏感的安全內容。

end-of-support作業系統的安全控制

在作業系統製造商「end-of-support」或 EOS 一般支援期間之外且未收到安全更新的作業系統，會有更高的安全風險。

AWS 提供一些 服務，以協助處理end-of-support作業系統。如需 Windows end-of-support的相關資訊，請參閱 [Windows Server End-of-Support遷移計劃](#)。

Note

如需本主題的其他資訊，請參閱 AWS Artifact 報告。如需詳細資訊，請參閱[在 AWS Artifact 中下載報告](#)。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。此資訊不包含在本使用者指南中，因為它包含敏感的安全內容。

使用安全群組

安全群組可做為一種虛擬防火牆，控制一或多個執行個體的流量。AMS 安全群組可讓您設定執行個體層級的傳入流量規則和傳出流量規則。您可以建立安全群組，並指定 AMS 帳戶、Amazon EC2 執行個體、Amazon RDS 資料庫執行個體、負載平衡器、Deep Security Manager (DSM) 複寫執行個體、EFS 掛載目標和 ElastiCache 叢集中的資源，以與安全群組建立關聯。建立關聯後，安全群組中設定的規則會限制往返這些執行個體的流量。

若要進一步了解一般 AWS 安全性，請參閱 [Linux 執行個體的安全性、身分與合規最佳實務](#) 和 [Amazon EC2 安全群組](#)。

AMS 現在有一組用於建立和管理安全群組的變更類型：

- 部署 | 進階堆疊元件 | 安全群組 | 建立 (ct-10xx2g2d7hc90)
- 管理 | 進階堆疊元件 | 安全群組 | 刪除 (ct-3cp96z7r065e4)
- 管理 | 進階堆疊元件 | 安全群組 | 更新 (ct-3memthlcmvc1b)

如需範例，請參閱[安全群組](#)。

安全群組

在 AWS VPCs 中，AWS 安全群組充當虛擬防火牆，控制一或多個堆疊（執行個體或一組執行個體）的流量。啟動堆疊時，它會與一或多個安全群組相關聯，以決定允許哪些流量到達該群組：

- 對於公有子網路中的堆疊，預設安全群組接受來自所有位置（網際網路）的 HTTP (80) 和 HTTPS (443) 流量。堆疊也接受來自您公司網路和 AWS 堡壘的內部 SSH 和 RDP 流量。然後，這些堆疊可以透過任何連接埠輸出到網際網路。它們也可以輸出到您的私有子網路和公有子網路中的其他堆疊。
- 私有子網路中的堆疊可以輸出到私有子網路中的任何其他堆疊，而堆疊中的執行個體可以完全透過任何通訊協定互相通訊。

Important

私有子網路上堆疊的預設安全群組允許私有子網路中的所有堆疊與該私有子網路中的其他堆疊通訊。如果您想要限制私有子網路中堆疊之間的通訊，您必須建立新的安全群組來描述限制。例如，如果您想要限制與資料庫伺服器的通訊，以便該私有子網路中的堆疊只能透過特定連接埠從特定應用程式伺服器通訊，請請求特殊安全群組。本節將說明如何執行此操作。

預設安全群組

MALZ

下表說明堆疊的預設傳入安全群組 (SG) 設定。SG 名為「SentinelDefaultSecurityGroupPrivateOnly-vpc-ID」，其中 *ID* 是 AMS 多帳戶登陸區域帳戶中的 VPC ID。允許所有流量透過此安全群組傳出至 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"（允許堆疊子網路中的所有本機流量）。

第二個安全群組「SentinelDefaultSecurityGroupPrivateOnly」允許所有流量傳出至 0.0.0.0/0。

 Tip

如果您要為 AMS 變更類型選擇安全群組，例如 EC2 建立或 OpenSearch 建立網域，您可以使用此處所述的其中一個預設安全群組，或您建立的安全群組。您可以在 AWS EC2 主控台或 VPC 主控台中找到每個 VPC 的安全群組清單。

還有其他預設安全群組用於內部 AMS 用途。

AMS 預設安全群組（傳入流量）

類型	通訊協定	連接埠範圍	來源
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnly（限制相同安全群組成員的傳出流量）
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制傳出流量）
HTTP、HTTPS、SSH、	TCP	80 / 443（來源 0.0.0.0/0） 允許從堡壘存取 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制傳出流量）
MALZ 堡壘：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客戶提供的內部部署 CIDRs

類型	通訊協定	連接埠範圍	來源
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	

SALZ 堡壘：

SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

下表說明堆疊的預設傳入安全群組 (SG) 設定。SG 名為 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-**ID**"，其中 **ID** 是唯一的識別符。允許所有流量透過此安全群組傳出至 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"（允許堆疊子網路中的所有本機流量）。

第二個安全群組 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-ID" 允許所有流量傳出至 0.0.0.0/0。

Tip

如果您要為 AMS 變更類型選擇安全群組，例如 EC2 建立或 OpenSearch 建立網域，您可以使用此處所述的其中一個預設安全群組，或您建立的安全群組。您可以在 AWS EC2 主控台或 VPC 主控台中找到每個 VPC 的安全群組清單。

還有其他預設安全群組用於內部 AMS 用途。

AMS 預設安全群組（傳入流量）

類型	通訊協定	連接埠範圍	來源
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnly（限制相同安全群組成員的傳出流量）
所有流量	全部	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制傳出流量）
HTTP、HTTPS、SSH、	TCP	80 / 443（來源 0.0.0.0/0） 允許從堡壘存取 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制傳出流量）
MALZ 堡壘：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客戶提供的內部部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡壘：			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

建立、變更或刪除安全群組

您可以請求自訂安全群組。如果預設安全群組不符合應用程式或組織的需求，您可以修改或建立新的安全群組。這類請求會被視為需要核准，並由 AMS 操作團隊審核。

若要在堆疊和 VPCs 外部建立安全群組，請使用 `Deployment | Advanced stack components | Security group | Create (review required)` 變更類型 (ct-10xx2g2d7hc90) 提交 RFC。

針對 Active Directory (AD) 安全群組修改，請使用下列變更類型：

- 若要新增使用者：使用 `Management | Directory Service | 使用者和群組 | 新增使用者至群組` 【ct-24pi85mjtza8k】 提交 RFC
- 若要移除使用者：使用 `管理 | Directory Service | 使用者和群組 | 從群組移除使用者` 【ct-2019s9y3nfm14】 提交 RFC

Note

使用「需要檢閱」CTs時，AMS 建議您使用 ASAP 排程選項（在主控台中選擇 ASAP，在 API/CLI 中保留開始和結束時間空白），因為這些 CTs 需要 AMS 運算子來檢查 RFC，並在核准和執行之前與您通訊。如果您排程這些 RFCs，請務必至少允許 24 小時。如果未在排定的開始時間之前進行核准，則會自動拒絕 RFC。

尋找安全群組

若要尋找連接到堆疊或執行個體的安全群組，請使用 EC2 主控台。找到堆疊或執行個體後，您可以看到連接到該堆疊或執行個體的所有安全群組。

如需在命令列尋找安全群組並篩選輸出的方法，請參閱 [describe-security-groups](#)。

AMS 預防性和偵測性控制程式庫

AWS Managed Services (AMS) 為您提供經過驗證的服務控制政策 (SCPs) 和 ConfigRules 的精選程式庫/目錄，可用於改善您的安全狀態並減輕 AMS 帳戶中的合規差距。

主題

- [統籌 SCPs 和 Config 規則](#)
- [Config 規則的自訂通知](#)

統籌 SCPs 和 Config 規則

AMS Advanced 的統籌 SCPs 和 Config 規則。

- 服務控制政策 (SCPs)：提供的 SCPs 是預設 AMS 政策的補充。

您可以將這些程式庫控制與預設的程式庫控制搭配使用，以滿足特定的安全需求。

- 組態規則：AMS 建議除了預設 AMS 組態規則之外，還要套用一致性套件（請參閱 [AWS Config 指南中的一致性套件](#)）（如需預設規則，請參閱 AMS 成品）。一致性套件涵蓋大部分的合規要求，AWS 會定期更新這些要求。

此處列出的規則可用於涵蓋 Conformance Packs 未涵蓋的使用案例特定差距

Note

隨著 AMS 預設規則和一致性套件隨著時間更新，您可能會看到這些規則的重複。

AMS 建議定期清除重複的 Config 規則。

對於 AMS Advanced，Config 規則不應使用自動修復（請參閱 [透過 AWS Config 規則修復不合規 AWS 資源](#)），以避免 out-of-band 變更。

SCP-AMS-001：限制 EBS 建立

如果您未啟用加密，請防止建立 EBS 磁碟區。

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002：限制 EC2 啟動

如果未加密 EBS 磁碟區，請防止 EC2 執行個體啟動。這包括拒絕從未加密 AMIs 啟動 EC2，因為此 SCP 也適用於根磁碟區。

```
{
  "Condition": {
```

```
    "Bool": {
      "ec2:Encrypted": "false"
    },
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Effect": "Deny"
  }
}
```

SCP-ADV-001：限制 RFC 提交

限制預設 AMS 角色提交特定的自動化 RFCs 例如建立 VPC 或刪除 VPC。如果您想要將更精細的許可套用至聯合角色，這會很有幫助。

例如，您可能希望預設值 `AWSManagedServicesChangeManagement Role` 能夠提交大多數可用的 RFCs，但允許建立和刪除 VPC、建立其他子網路、停止應用程式帳戶、更新或刪除 SAML 身分提供者的 RFC 除外：

SCP-AMS-003：限制在 AMS 中建立 EC2 或 RDS

防止建立沒有特定標籤的 Amazon EC2 和 RDS 執行個體，同時允許 AMS 預設 `AMS Backup IAM` 角色這樣做。這是災難復原或 DR 所需的。

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

```
    }  
  }  
}
```

SCP-AMS-004：限制 S3 上傳

防止上傳未加密的 S3 物件。

```
{  
    "Sid": "DenyUnencryptedS3Uploads",  
    "Effect": "Deny",  
    "Action": "s3:PutObject",  
    "Resource": "*",  
    "Condition": {  
        "StringNotLike": {  
            "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]  
        },  
        "Null": {  
            "s3:x-amz-server-side-encryption": "false"  
        }  
    }  
}
```

SCP-AMS-005：限制 API 和主控台存取

針對來自己知不良 IP 地址的請求，防止 AWS 主控台和 API 存取，視客戶 InfoSec 的判斷而定。

SCP-AMS-006：防止 IAM 實體從組織中移除成員帳戶

防止 AWS Identity and Access Management 實體從組織中移除成員帳戶。

```
{  
    "Effect": "Deny",  
    "Action": ["organizations:LeaveOrganization"],  
    "Resource": ["*"]  
}
```

SCP-AMS-007：防止與組織外部帳戶共用資源

防止與 AWS 組織外部帳戶共用資源

```
{
  "Effect": "Deny",
  "Action": [
    "ram:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
      "ram:AllowsExternalPrincipals": "true"
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:UpdateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "ram:RequestedAllowsExternalPrincipals": "true"
    }
  }
}
```

SCP-AMS-008：防止與組織或組織單位 (OUs) 共用

防止與組織中的帳戶和/或 OU 共用資源。

```
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
```



```
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
    ]
}
}
```

SCP-AMS-009：防止使用者接受資源共享邀請

防止成員帳戶接受來自 AWS RAM 加入資源共享的邀請。此 API 不支援任何條件，並防止僅從外部帳戶共用。

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010：防止帳戶區域啟用和停用動作

防止啟用或停用您 AWS 帳戶的任何新 AWS 區域。

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011：防止帳單修改動作

防止對帳單和付款組態進行修改。

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ]
}
```

```
],  
  "Resource": "*" }  
}
```

SCP-AMS-012：防止刪除或修改特定 CloudTrails

防止修改特定 AWS CloudTrail 線索。

```
{  
  "Effect": "Deny",  
  "Action": [  
    "cloudtrail:DeleteEventDataStore",  
    "cloudtrail:DeleteTrail",  
    "cloudtrail:PutEventSelectors",  
    "cloudtrail:PutInsightSelectors",  
    "cloudtrail:UpdateEventDataStore",  
    "cloudtrail:UpdateTrail",  
    "cloudtrail:StopLogging"  
  ],  
  "Resource": [  
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"  
  ]  
}
```

SCP-AMS-013：防止停用預設 EBS 加密

防止停用預設 Amazon EBS 加密。

```
{  
  "Effect": "Deny",  
  "Action": [  
    "ec2:DisableEbsEncryptionByDefault"  
  ],  
  "Resource": "*" }  
}
```

SCP-AMS-014：防止建立預設 VPC 和子網路

防止建立預設 Amazon VPC 和子網路。

```
{  
  "Effect": "Deny",  
  "Action": [  
    "ec2:CreateVpc",  
    "ec2:CreateSubnet"  
  ],  
  "Resource": "*" }  
}
```

```
"Action": [  
  "ec2:CreateDefaultSubnet",  
  "ec2:CreateDefaultVpc"  
],  
"Resource": "*"   
}
```

SCP-AMS-015：防止停用和修改 GuardDuty

防止修改或停用 Amazon GuardDuty。

```
{  
  "Effect": "Deny",  
  "Action": [  
    "guardduty:AcceptInvitation",  
    "guardduty:ArchiveFindings",  
    "guardduty:CreateDetector",  
    "guardduty:CreateFilter",  
    "guardduty:CreateIPSet",  
    "guardduty:CreateMembers",  
    "guardduty:CreatePublishingDestination",  
    "guardduty:CreateSampleFindings",  
    "guardduty:CreateThreatIntelSet",  
    "guardduty:DeclineInvitations",  
    "guardduty>DeleteDetector",  
    "guardduty>DeleteFilter",  
    "guardduty>DeleteInvitations",  
    "guardduty>DeleteIPSet",  
    "guardduty>DeleteMembers",  
    "guardduty>DeletePublishingDestination",  
    "guardduty>DeleteThreatIntelSet",  
    "guardduty:DisableOrganizationAdminAccount",  
    "guardduty:DisassociateFromMasterAccount",  
    "guardduty:DisassociateMembers",  
    "guardduty:InviteMembers",  
    "guardduty:StartMonitoringMembers",  
    "guardduty:StopMonitoringMembers",  
    "guardduty:TagResource",  
    "guardduty:UnarchiveFindings",  
    "guardduty:UntagResource",  
    "guardduty:UpdateDetector",  
    "guardduty:UpdateFilter",  
    "guardduty:UpdateFindingsFeedback",  
    "guardduty:UpdateIPSet",  
  ]  
}
```

```
"guardduty:UpdateMalwareScanSettings",
"guardduty:UpdateMemberDetectors",
"guardduty:UpdateOrganizationConfiguration",
"guardduty:UpdatePublishingDestination",
"guardduty:UpdateThreatIntelSet"
],
"Resource": "*"
}
```

SCP-AMS-016：防止根使用者活動

防止根使用者執行任何動作。

```
{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017：防止為根使用者建立存取金鑰

防止為根使用者建立存取金鑰。

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018：防止停用 S3 帳戶公有存取區塊

防止停用 Amazon S3 帳戶公有存取區塊。這可防止帳戶中的任何儲存貯體變成公有。

```
{
  "Effect": "Deny",
```

```
"Action": "s3:PutAccountPublicAccessBlock",
"Resource": "*"
}
```

SCP-AMS-019：防止停用 AWS Config 或修改 Config 規則

防止停用或修改 AWS Config 規則。

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020：防止所有 IAM 動作

防止所有 IAM 動作。

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021：防止刪除 CloudWatch Logs 群組和串流

防止刪除 Amazon CloudWatch Logs 群組和串流。

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
}
```

```
"Resource": "*"
}
```

SCP-AMS-022 : 防止 Glacier 刪除

防止刪除 Amazon Glacier。

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023 : 防止刪除 IAM Access Analyzer

防止刪除 IAM Access Analyzer。

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024 : 防止修改 Security Hub

防止刪除 AWS Security Hub。

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

```
}
```

SCP-AMS-025：防止在 Directory Service 下刪除

防止刪除 下的資源 AWS Directory Service。

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026：防止使用列入拒絕清單的服務

防止使用拒絕清單的服務。

Note

將 *service1* 和 *service2* 取代為您的服務名稱。*Access-analyzer* 或 *IAM* 範例。

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027：防止在特定區域中使用列入拒絕清單的服務

防止在特定 AWS 區域中使用列入拒絕清單的服務。

Note

將 *service1* 和 *service2* 取代為您的服務名稱。*Access-analyzer* 或 *IAM* 範例。
將 *region1* 和 *region2* 取代為您的服務名稱。範例 *us-west-2* 或 *use-east-1*。

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:*", "service2:*"],
  "Condition": {
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028：防止修改標籤，授權委託人除外

防止授權委託人以外的任何使用者修改標籤。使用授權標籤來授權委託人。授權標籤必須與資源和主體建立關聯。只有在資源和委託人上的標籤都相符時，使用者/角色才會被視為已授權。如需詳細資訊，請參閱下列資源：

- [使用 中的服務控制政策保護用於授權的資源標籤 AWS Organizations](#)
- [防止修改標籤，但授權委託人除外](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
```

```
    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
  },
  "Null": {
    "ec2:ResourceTag/access-project": false
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
```

```
}  
}  
}
```

SCP-AMS-029：防止使用者刪除 Amazon VPC 流程日誌

防止刪除 Amazon VPC 流程日誌。

```
{  
  "Action": [  
    "ec2:DeleteFlowLogs",  
    "logs:DeleteLogGroup",  
    "logs:DeleteLogStream",  
    "s3:DeleteBucket",  
    "s3:DeleteObject",  
    "s3:DeleteObjectVersion",  
    "s3:PutLifecycleConfiguration",  
    "firehose:DeleteDeliveryStream"  
  ],  
  "Resource": "*",  
  "Effect": "Deny"  
}
```

SCP-AMS-030：防止與網路帳戶以外的帳戶共用 VPC 子網路

防止與網路帳戶以外的帳戶共用 Amazon VPC 子網路。

Note

將 **NETWORK_ACCOUNT_ID** 取代為您的網路帳戶 ID。

```
{  
  "Effect": "Deny",  
  "Action": [  
    "ram:AssociateResourceShare",  
    "ram:CreateResourceShare"  
  ],  
  "Resource": "*",  
  "Condition": {  
    "StringNotEquals": {  
      "ram:Principal": "NETWORK_ACCOUNT_ID"  
    }  
  }  
}
```

```

    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}

```

SCP-AMS-031：防止使用禁止的執行個體類型啟動執行個體

防止延遲禁止的 Amazon EC2 執行個體類型。

Note

將 *instance_type1* 和 *instance_type2* 取代為您想要限制的執行個體類型，例如 *t2.micro* 或萬用字元字串，例如 **.nano#*

```

{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}

```

SCP-AMS-032：防止在沒有 IMDSv2 的情況下啟動執行個體

防止沒有 IMDSv2 的 Amazon EC2 執行個體。IMDSv2

```

[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",

```

```
"Condition": {
  "StringNotEquals": {
    "ec2:MetadataHttpTokens": "required"
  }
},
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "NumericGreaterThan": {
      "ec2:MetadataHttpPutResponseHopLimit": "3"
    }
  }
},
{
  "Effect": "Deny",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "NumericLessThan": {
      "ec2:RoleDelivery": "2.0"
    }
  }
},
{
  "Effect": "Deny",
  "Action": "ec2:ModifyInstanceMetadataOptions",
  "Resource": "*"
}
]
```

SCP-AMS-033：防止修改特定 IAM 角色

防止修改指定的 IAM 角色。

```
{
  "Action": [
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
```

```

    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

SCP-AMS-034：防止在特定 IAM 角色上修改 AssumeRolePolicy

防止修改指定 IAM 角色的 AssumeRolePolicy。

```

{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

ConfigRule：必要標籤

檢查 EC2 執行個體是否有您需要的自訂標籤。除了 InfoSec 之外，這也適用於您的成本管理

```

ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS

```

```
SourceIdentifier: REQUIRED_TAGS
```

ConfigRule : 已輪換存取金鑰

檢查存取金鑰是否在指定的期間內輪換。根據典型的合規要求，這通常設定為 90 天。

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
  maxAccessKeyAge number of days.
InputParameters:
  maxAccessKeyAge: '90'
Source:
  Owner: AWS
  SourceIdentifier: ACCESS_KEYS_ROTATED
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule : AMS 中的 IAM 根存取金鑰

檢查帳戶中沒有根存取金鑰。對於 AMS Advanced 帳戶，預期這是out-of-the-box可用的合規。

```
ConfigRuleName: iam-root-access-key-check
Description: >-
  A config rule that checks whether the root user access key is available. The
  rule is COMPLIANT if the user access key does not exist.
Source:
  Owner: AWS
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule : SSM 受管 EC2

檢查您的 EC2s是否由 SSM Systems Manager 管理。

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
```



```
- 'AWS::EC2::Instance'
- 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule : AMS 中未使用的 IAM 使用者

檢查是否有指定期間內未使用的 IAM 使用者登入資料。如同金鑰輪換檢查，這通常會根據一般合規要求預設為 90 天。

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule : S3 儲存貯體記錄

檢查帳戶中的 S3 儲存貯體是否已啟用記錄。

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule : S3 儲存貯體版本控制

檢查是否已啟用所有 S3 儲存貯體的版本控制和 MFA-delete (選用)

```
ConfigRuleName: s3-bucket-versioning-enabled
```

```
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule : S3 公有存取

檢查公有存取設定（公有 ACL、公有政策、公有儲存貯體）是否在帳戶間受到限制

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
  Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

ConfigRule : 非封存的 GuardDuty 調查結果

檢查是否有任何非封存的 GuardDuty 調查結果早於指定的持續時間。預設持續時間為低 sev 30 天，中 sev 7 天，高 sev 問題清單 1 天。

```
ConfigRuleName: guardduty-non-archived-findings
Description: >-
  A Config rule that checks whether the Amazon GuardDuty has findings that
  are non archived. The rule is NON_COMPLIANT if GuardDuty has non
  archived low/medium/high severity findings older than the specified number.
InputParameters:
```

```
daysLowSev: '30'
daysMediumSev: '7'
daysHighSev: '1'
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule : CMK 刪除

檢查是否有任何已排程（也稱為待定）要刪除的 AWS Key Management Service 自訂主金鑰 (CMKs)。這一點至關重要，因為 CMK 刪除的不知道可能會導致資料無法復原

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule : CMK 輪換

檢查帳戶中的每個 CMK 是否已啟用自動輪換

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Config 規則的自訂通知

可能會發生重大不合規的 Config 規則，需要直接向您的 InfoSec 和領導團隊提高提升意識。針對這類案例，AMS 建議您設定不合規事件驅動的自訂通知。

例如：

```
ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the mandated tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
            - RequiredEC2Tags
            - Arn
    Targets:
      - Id: RemediationNotification
        Arn:
          Ref: SnsTopic
        InputTransformer:
          InputTemplate: >-
            "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
            COST_CENTER, APP_ID, Name, and Backup."
          InputPathsMap:
```

```
        instance_id: $.detail.resourceId
SnsTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: Cloud_Ops_Leaders@customer.com
        Protocol: email
    TopicName: noncompliant-instance-notification
SnsTopicPolicy:
  Type: 'AWS::SNS::TopicPolicy'
  Properties:
    PolicyDocument:
      Statement:
        - Sid: __default_statement_ID
          Effect: Allow
          Principal:
            AWS: '*'
          Action:
            - 'SNS:GetTopicAttributes'
            - 'SNS:SetTopicAttributes'
            - 'SNS:AddPermission'
            - 'SNS:RemovePermission'
            - 'SNS:DeleteTopic'
            - 'SNS:Subscribe'
            - 'SNS:ListSubscriptionsByTopic'
            - 'SNS:Publish'
            - 'SNS:Receive'
          Resource:
            Ref: SnsTopic
        Condition:
          StringEquals:
            'AWS:SourceOwner':
              Ref: 'AWS::AccountId'
        - Sid: TrustCWEToPublishEventsToMyTopic
          Effect: Allow
          Principal:
            Service: events.amazonaws.com
          Action: 'sns:Publish'
          Resource:
            Ref: SnsTopic
  Topics:
    - Ref: SnsTopic
```

AMS Advanced 的 Amazon EventBridge 規則服務連結角色

AMS Advanced 使用名為 `AWSServiceRoleForManagedServices_Events` 的服務連結角色 (SLR) – 此角色信任其中一個 AWS Managed Services 服務主體 (`events.managedservices.amazonaws.com : //`) 為您擔任該角色。服務會使用 角色來建立 EventBridge 受管規則。此規則是您 AWS 帳戶中將警示狀態變更資訊從您的帳戶交付至 AWS Managed Services 所需的基礎設施。

AMS Advanced 的 EventBridge SLR 許可

`AWSServiceRoleForManagedServices_Events` 服務連結角色信任下列服務擔任該角色：

- `events.managedservices.amazonaws.com`

連接至此角色是 `AWSManagedServices_EventsServiceRolePolicy` AWS 受管政策（請參閱 [AWS 受管政策：AWSManagedServices_EventsServiceRolePolicy](#)）。服務會使用 角色，將警示狀態變更資訊從您的帳戶傳遞至 AWS Managed Services。您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的 [服務連結角色許可](#)。

您可以在此 ZIP：`EventsServiceRolePolicy.zip` 中下載 JSON

`AWSManagedServices_EventsServiceRolePolicy`。 [EventsServiceRolePolicy.zip](#)

建立 AMS Advanced 的 EventBridge SLR

您不需要手動建立一個服務連結角色。當您在 AWS 管理主控台 AWS CLI、或 AWS API 中加入 AMS 時，AMS Advanced 會為您建立服務連結角色。

Important

如果您在 2023 年 2 月 7 日之前使用 AMS Advanced 服務，此服務連結角色會出現在您的帳戶中，當它開始支援服務連結角色時，AMS Accelerate 會在您的帳戶中建立 `AWSServiceRoleForManagedServices_Events` 角色。若要進一步了解，請參閱 [我的 IAM 帳戶中出現的新角色](#)。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您加入 AMS 時，AMS Advanced 會再次為您建立服務連結角色。

編輯 AMS Advanced 的 EventBridge SLR

AMS Advanced 不允許您編輯 `AWSServiceRoleForManagedServices_Events` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。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」](#) 的編輯服務連結角色。

刪除 AMS Advanced 的 EventBridge SLR

您不需要手動刪除 `AWSServiceRoleForManagedServices_Events` 角色。當您在 AWS 管理主控台、AWS CLI 或 AWS API 中從 AMS 離職時，AMS Advanced 會為您清除資源並刪除服務連結角色。

您也可以使用 IAM 主控台、AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

Note

如果您嘗試刪除資源時，AMS Advanced 服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 `AWSServiceRoleForManagedServices_Events` 服務連結角色所使用的 AMS Advanced 資源

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、或 AWS API 來刪除 `AWSServiceRoleForManagedServices_Events` 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](#)。

安全最佳實務

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

AMS 多帳戶登陸區域 EPS 非預設設定

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

AMS 護欄

護欄是為整體 AMS 環境提供持續控管的高階規則。

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

MALZ Service 控制政策

本節已修訂，因為它包含敏感的 AMS 安全相關資訊。此資訊可透過 AMS 主控台文件取得。若要存取 AWS Artifact，您可以聯絡 CSDM 以取得指示，或前往 [AWS Artifact 入門](#)。

AMS 中的安全事件回應

安全是 AWS Managed Services (AMS) 的首要任務。AMS 會在您的帳戶中部署資源和控制項來管理這些資源和控制項。AWS 具有共同的責任模型：AWS 管理雲端的安全性，而您需負責雲端的安全性。AMS 會使用安全控制和主動監控安全問題，來保護您的資料和資產，並協助確保 AWS 基礎設施的安全。這些功能可協助您為在 AWS 雲端中執行的應用程式建立安全基準。AMS 透過安全事件回應與您合作來評估效果，然後根據最佳實務建議執行遏制和修復。

發生與基準的偏差時，例如組態錯誤或外部因素變更，您需要回應和調查。若要成功執行此作業，您需要了解 AMS 環境中安全事件回應的基本概念。您還必須了解在發生安全問題之前準備、教育和培訓雲端團隊的需求。請務必了解您可以使用的控制項和功能、準備常見安全問題的回應計畫，例如使用者帳戶入侵或濫用特權帳戶，以及識別使用自動化來改善回應速度和一致性的修補方法。此外，您需要了解您的合規和法規要求，因為它們與建置安全事件回應計劃相關，以滿足這些要求。

安全事件回應可能很複雜，但透過實作反覆方法，您可以簡化程序，並允許事件回應團隊透過提供早期和持續的偵測和回應來保持資產利益相關者的滿意度。在本指南中，我們會為您提供 AMS 用於事件回應的方法、AMS 責任矩陣 (RACI)、如何為安全事件做好準備、如何在安全事件期間與 AMS 互動，以及 AMS 使用的一些事件回應執行手冊。

AMS 安全事件回應的運作方式

AWS Managed Services 符合 NIST 800-61 [電腦安全事件處理指南](#) 的安全事件回應。透過符合此產業標準，我們提供一致的安全事件管理方法，並遵循最佳實務來保護和回應雲端中的安全事件。

事件回應生命週期

當偵測識別並產生安全提醒，或您請求安全協助時，AWS Managed Services Operations 團隊會確保及時調查、執行自動化以執行資料收集、分類和分析、通知您分析、執行調查和任何遏制活動，然後發佈事件分析。

在事件回應期間執行的資料收集、分類、分析和遏制活動會根據正在調查的安全事件類型而有所不同。特定案例的安全事件回應工作流程範例位於本文件結尾。

在事件期間，AMS 會動態判斷正確的動作過程，這可能會導致適當時重新排序或繞過記錄的步驟，以確保產生正確的結果。

準備

隨著威脅態勢的演進，AMS 持續擴展偵測和回應功能。隨著新增偵測，AMS 會將來自這些新偵測的提醒納入偵測和回應平台。AMS 安全回應者經過訓練，可調查並在整個安全事件回應生命週期中與您合作。

由於這種合作夥伴關係，您的安全與應用程式團隊必須準備好與 AMS 互動，在這些事件發生時處理安全事件。本文件說明安全事件期間預期會發生的情況，並協助您準備在安全事件發生時快速回應。

本文件使用事件的 NIST 800-61 定義做為系統或網路中任何可觀察到的事件，並將事件做為違反或即將發生的違反政策、可接受的使用政策或標準安全實務威脅。

準備作業核對清單

與您的 AMS 雲端解決方案交付管理員 (CSDM) 和 AMS 雲端架構師 (CA) 一起完成下列檢查清單：

- 了解哪些 帳戶中正在執行哪些工作負載。
- 了解哪些內部團隊負責各種工作負載，並在工作負載中適當標記這些工作負載。
- 為在安全事件調查期間可能需要的其他團隊和遏制決策保留內部聯絡詳細資訊。
- 確認安全聯絡人是最新的，並新增至所有受管 AWS 帳戶。聯絡人是以每個帳戶為基礎進行管理。
- 了解如何向 AMS 引發安全事件，並熟悉嚴重性和預期的回應時間。
- 確保收到安全通知時，它們會路由到適當的人員和系統，例如分頁器或您的安全操作中心。
- 了解您可以使用哪些日誌來源、這些來源儲存在您的帳戶中，以及誰可以存取它們。
- 了解如何在調查期間使用 CloudWatch Insights 查詢日誌。
- 了解資源 (EC2、IAM、S3 和 on) 可用的抑制選項，以及抑制時工作負載可用性的後果。

偵測

在管理 AWS 您的帳戶期間，AMS 會使用從偵測來源和控制項收集的資料來監控使用者行為、帳戶活動和潛在安全事件的異常，包括但不限於 Amazon CloudWatch、Amazon GuardDuty、VPC Flow Logs、Amazon Macie AWS Config 和 Amazon 內部威脅情報摘要。

AMS 同時使用原生 AWS 服務和其他偵測技術來回應由下列人員建立的安全事件：

- 組態一致性調查結果類型
- GuardDuty 調查結果類型
- Macie 調查結果類型
- Amazon Route 53 Resolver DNS 防火牆事件
- AMS 安全事件（雲端監看警示）

隨著服務、產品和威脅生態系統的演進，會新增其他問題清單。

向 AMS 報告安全事件

透過 AMS 支援入口網站或 支援 中心引發事件，以通知 AMS 安全事件或請求調查。

分析

識別並報告安全事件後，下一個步驟是分析報告的事件是誤報還是實際事件。AMS 使用自動化和手動調查技術來處理安全事件。分析包括調查來自不同偵測來源的日誌，例如網路流量日誌、主機日誌、CloudTrail 事件、AWS 服務日誌等。分析也會尋找透過相互關聯顯示異常行為的模式。

需要您的合作夥伴關係，才能了解帳戶環境的特定內容，並確定帳戶和工作負載的正常情況。這有助於 AMS 更快地識別異常並加速事件回應。

處理來自 AMS 有關安全事件的通訊

AMS 透過事件票證與您的安全聯絡人互動，在調查期間通知您。您的 AMS 雲端服務交付管理員 (CSDM) 和 AMS 雲端架構師 (CA) 是主動安全調查期間任何通訊的聯絡窗口。

通訊包括產生安全提醒時的自動通知、事件分析後的通訊、建立呼叫橋接和持續交付成品，例如日誌檔案、受感染資源的快照，以及在安全事件期間取得調查結果。

AMS 安全性提醒通知中包含的標準欄位如下所列。這些欄位為您提供資訊，讓您可以將事件路由到組織內的適當團隊以進行修復。

- 問題清單類型
- 問題清單識別符（相關）
- 問題清單嚴重性
- 問題清單描述
- 調查結果建立的日期和時間

- AWS 帳戶 ID
- 區域 (在相關區域)
- AWS 資源 (IAM user/role/policy、EC2、S3、EKS)

根據調查結果類型提供其他欄位，例如 EKS 調查結果，包括 Pod、容器和叢集詳細資訊。

包含

AMS 的遏制方法是與您建立合作夥伴關係。您了解您的業務以及因網路隔離、IAM 使用者或角色取消佈建、執行個體重新建置等遏制活動而可能發生的工作負載影響。

抑制的重要部分是決策。例如，關閉系統、隔離資源與網路，或關閉存取或結束工作階段。如果有預先決定的策略和程序來包含事件，這些決策會更容易做出。AMS 提供遏制策略，然後在您考慮實作遏制動作所涉及的風險之後，實作解決方案。

根據分析中的資源，有不同的遏制選項。AMS 預期在事件調查期間會同時部署多種類型的遏制。其中一些範例包括：

- 套用保護規則來封鎖未經授權的流量 (安全群組、NACL、WAF 規則、SCP 規則、拒絕清單、將簽章動作設定為隔離或封鎖)
- 資源隔離
- 網路隔離
- 停用 IAM 使用者、角色和政策
- 修改/減少 IAM 使用者、角色權限
- 終止/暫停/刪除運算資源
- 限制來自受影響資源的公開存取
- 輪換存取金鑰、API 金鑰和密碼
- 刷新已公開的登入資料和敏感資訊

AMS 鼓勵您考慮在其風險偏好範圍內的每個主要事件類型的遏制策略類型，並清楚記錄有助於在事件發生時做出決策的條件。決定適當策略的條件包括：

- 資源可能受損
- 保留證據
- 服務無法使用 (例如，網路連線、提供給外部各方的服務)

- 實作策略所需的時間和資源
- 策略的有效性（例如，部分遏制、完全遏制）
- 解決方案的持久性（例如，單向門與雙向門決策）
- 解決方案的持續時間（例如，四小時內要移除的緊急解決方法、兩週內要移除的暫時解決方法、永久解決方案）。
- 套用您可以開啟的安全控制，以降低風險，並留出時間來定義和實作更有效的遏制。

遏制的速度至關重要，AMS 建議分階段方法，透過制定短期和長期方法的策略來實現高效和有效的遏制。

使用本指南來考慮根據資源類型涉及不同技術的遏制策略。

- 遏制策略
 - AMS 是否可以識別安全事件的範圍？
 - 如果是，請識別所有資源（使用者、系統、資源）。
 - 如果否，請平行調查並對已識別的資源執行下一個步驟。
 - 資源可以隔離嗎？
 - 如果是，請繼續隔離受影響的資源。
 - 如果否，則與系統擁有者和管理員合作，以決定包含問題所需的進一步動作。
 - 是否將所有受影響的資源與未受影響的資源隔離？
 - 如果是，請繼續下一個步驟。
 - 如果否，則繼續隔離受影響的資源，直到完成短期遏制，以防止事件進一步升級。
- 系統備份
 - 是否為進一步分析而建立受影響系統的備份副本？
 - 鑑識複本是否加密並存放在安全的位置？
 - 如果是，請繼續下一個步驟。
 - 如果否，請加密鑑識影像，然後將它們存放在安全的位置，以防止意外使用、損壞和竄改。

根除

包含事件之後，可能需要消除威脅來源，才能保護系統，然後再繼續進行下一個復原階段。根除步驟可能包括刪除惡意軟體和移除遭入侵的使用者帳戶，以及識別和緩解所有遭到利用的漏洞。在根除期間，請務必識別環境中所有受影響的帳戶、資源和執行個體，以便進行修復。

最佳實務是以分階段方法完成根除和復原，以排定修復步驟的優先順序。對於大規模事件，復原可能需要幾個月的時間。早期階段的用意必須是透過相對快速（數天到數週）的高價值變更來提高整體安全性，以防止未來發生事件。後期階段必須專注於長期變更（例如基礎設施變更）和持續工作，以盡可能確保企業的安全。

對於某些事件，不需要根除或在復原期間執行。

考慮下列各項：

- 系統是否可以重新製作映像，然後使用修補程式或其他對策進行強化，以防止或降低攻擊風險？
- 攻擊者留下的所有惡意軟體和其他成品是否已移除，且受影響的系統是否進一步強化以抵禦攻擊？

復原

AMS 會與您合作，將系統還原至正常操作、確認系統正常運作，以及（如適用）修復漏洞以防止類似事件。

考慮下列各項：

- 受影響的系統是否已修補和強化（針對最近的攻擊和可能的未來攻擊）？
- 何時可以將受影響的系統還原到生產環境？
- 您將使用哪些工具來測試、監控和驗證您還原至生產環境的系統是否不容易受到初始攻擊技術的影響？

事件後報告

在事件發生後，AMS 會針對所有安全事件執行調查審查程序。此外，AMS 會啟動錯誤校正 (COE) 程序，以解決系統造成的安全事件，或可合理改善的程序遺漏。AMS 會與您合作，持續改善安全調查體驗。COE 程序可協助 AMS 識別影響客戶事件的促成因素，並將這些原因連接到下一個動作項目，以防止類似事件重複發生，或協助減輕影響的持續時間或層級。

安全性事件的調查審查程序會處理下列項目，以識別改進的機會：

- 從事件開始到事件探索、初始影響評估，以及事件處理程序的每個階段（例如，遏制、復原）經過了多少時間？
- 事件回應團隊需要多長時間才能回應事件的初始報告？
- 執行初始影響分析需要多長時間？
- 這可以預防嗎？如何預防？是否有可以防止這種情況的工具或程序？

- 我們可以更快地及如何偵測到此問題嗎？
- 什麼可以讓調查更快進行？
- 是否遵循記錄的事件回應程序？它們是否足夠？
- 與其他利益相關者的資訊共用是否及時完成 如何改進？
- 與其他團隊 (AWS 安全、客戶團隊、AWS 開發團隊和客戶安全團隊) 的協作是否有效？如果沒有，可以改善哪些項目？
- 缺少哪些可能有幫助的準備步驟、呈報矩陣、RACI、共同責任模型等？是否需要更新任何 Runbook？
- 初始影響評估和最終影響評估之間的差異是什麼？我們可以如何改善事件回應中稍早評估的準確性？
- 所學課程的動作項目有哪些？

AMS 中的安全事件回應 Runbook

本節包含兩個 Runbook：

- [對根使用者活動的回應](#)
- [回應惡意軟體事件](#)

對根使用者活動的回應

[根使用者](#)是您 AWS 帳戶中的超級使用者。請注意，AMS 會監控根用量。最佳實務是僅針對需要根使用者的少數任務使用根使用者，例如變更您的帳戶設定、啟用 AWS Identity and Access Management (IAM) 存取帳單和成本管理、變更根密碼，以及開啟多重要素驗證 (MFA)。如需詳細資訊，請參閱[需要根使用者憑證的任務](#)。

如需如何通知 AMS 計劃根用量的詳細資訊，請參閱[何時以及如何在 AMS 中使用根帳戶](#)。

偵測到根使用者活動時，嘗試登入失敗，可能表示成功登入後帳戶中發生暴力攻擊或活動，會產生事件，並將事件傳送至您定義的安全聯絡人。

AWS Managed Services Operations 會調查計劃外的根使用者活動、執行資料收集、分類和分析，以及依照您的方向執行遏制活動，然後執行事件後分析。

如果您有 AMS Advanced 操作模型，您會收到來自 AMS CSDM 和 AMS Ops 工程師的額外通訊，以確認意外的根使用者活動，因為 AMS 有責任保護根使用者憑證。AMS 會調查根使用者活動，直到您確認路徑向前為止。

準備

向 AMS 告知任何計劃使用的根使用者，方法是使用計劃事件的資料和時間提交 AMS 服務請求，以防止不必要的事件回應活動。

定期使用 AMS 執行 GameDays，以驗證 AMS 的客戶事件回應程序、人員和系統是最新的，並與負責的人員建立肌肉記憶體，以實現更快的事件回應。

階段 A：偵測

AMS 透過偵測來源監控帳戶中的根活動，包括 GuardDuty 和 AMS 監控。

如果您有 AMS Accelerate，操作模型會回應請求調查非預期根使用者活動的事件。發生這種情況時，AMS Operations 會啟動遭入侵的帳戶 Runbook。

如果您有 AMS Advanced，操作模型會回應事件，或通知 CSDM 任何計劃根使用者活動，以終止作用中的帳戶入侵調查。

階段 B：分析

當判斷活動未獲授權時，AMS 會對根使用者事件進行徹底調查。使用自動化和 AMS 安全回應團隊，會針對根使用者的異常和非預期行為分析日誌和事件。日誌會提供給您，以協助判斷活動是否未知、是否為授權的根使用者事件，或是否需要進一步調查。

調查期間為支援內部檢查而提供的資訊範例包括：

- 帳戶資訊：根帳戶用於哪個帳戶？
- 根使用者的電子郵件地址：每個根使用者都與您組織的電子郵件地址相關聯
- 身分驗證詳細資訊：根使用者從何處和何時存取您的環境？
- 活動記錄：使用者以根登入時做了什麼？這些記錄的形式為 CloudWatch 事件。了解如何讀取這些日誌有助於調查。

這是最佳實務，您已準備好接收分析資訊，並規劃如何聯絡組織內帳戶的授權聯絡人。由於根使用者未命名為個人，因此判斷誰可以存取組織中用於帳戶的根電子郵件地址，有助於快速在內部路由問題。

階段 C：包含和消除

AMS 與您的安全團隊合作，在您授權的客戶安全聯絡人指示下執行遏制。遏制選項包括：

- 輪換適當的登入資料和金鑰。

- 終止對帳戶和資源的作用中工作階段。
- 消除已建立的資源。

在遏制活動期間，AMS 會與您的安全團隊緊密合作，以確保工作負載的任何中斷都降到最低，並且根憑證會受到適當的保護。

完成遏制計畫後，您可以視需要與 AMS 營運團隊合作執行任何復原動作。

事件後報告

AMS 會視需要啟動調查審查程序，以識別學到的任何教訓。在完成 COE 的過程中，AMS 會將任何相關調查結果傳達給受影響的客戶，以協助他們改善事件回應程序。

AMS 會記錄調查的所有最終詳細資訊、收集適當的指標，然後將事件報告給需要資訊的任何 AMS 內部團隊，包括您指派的 CSDM 和 CA。

回應惡意軟體事件

Amazon EC2 執行個體用於託管各種工作負載，包括第三方軟體和由組織內應用程式團隊部署的自訂開發軟體。AMS 提供並鼓勵您在 AMS 持續修補和維護的映像上部署工作負載。

在執行個體操作期間，AMS 會透過各種安全偵測控制來監控行為或活動的異常，包括 Amazon GuardDuty、端點保護、網路流量和 Amazon 內部威脅情報摘要。

具有 AMS Advanced 操作模型的 AMS 客戶會自動在佈建的資源上安裝端點安全 (EPS) 監控用戶端。這可確保資源 24 小時全年無休受到監控和支援，包括在偵測到事件時建立安全事件。

AMS 也會監控 GuardDuty 惡意軟體調查結果。如果啟用，這些都可以在 AMS Advanced 和 AMS Accelerate 上使用。如需詳細資訊，請參閱 [Amazon GuardDuty 中的惡意軟體防護](#)。

Note

如果您選擇[使用自有 EPS](#)，則事件回應的程序會與此頁面上概述的程序不同。如需詳細資訊，請參閱參考的文件。

偵測到惡意軟體時，會建立事件並通知您該事件。此通知後面接著發生的任何修復活動。AMS Operations 會調查、執行資料收集、分類和分析，然後依照您的方向執行遏制活動，接著執行事件後分析。

階段 A：偵測

AMS 會使用 GuardDuty 和端點安全解決方案監控來監控執行個體上的事件。AMS 會決定適當的擴充和分類活動，以協助您根據調查結果或提醒類型做出遏制或風險接受決策。

資料收集是根據調查結果類型執行。資料收集涉及查詢受影響帳戶內部和外部的多個資料來源，以建立觀察到的活動或關注組態的影像。

AMS 會執行調查結果與任何受影響帳戶或 AMS 威脅情報平台之任何其他警示和警示或遙測的相互關聯。

階段 B：分析

收集資料後，會對其進行分析，以識別任何活動或關注指標。在調查的這個階段，AMS 會與您合作，整合執行個體和工作負載的商業和網域知識，以協助了解預期事項和異常情況。

調查期間為支援內部檢查而提供的資訊範例包括：

- 帳戶資訊：在哪個帳戶上觀察到惡意軟體活動？
- 執行個體詳細資訊：哪些（些）執行個體與惡意軟體事件有關？
- 事件時間戳記：警示何時觸發？
- 工作負載資訊：執行個體上執行什麼項目？
- 惡意軟體詳細資訊，如果相關：惡意軟體系列和有關惡意軟體的開放原始碼資訊。
- 使用者或角色詳細資訊：哪些使用者或角色受到活動的影響和參與活動？
- 活動記錄：執行個體上會記錄哪些活動？這些是 CloudWatch 事件的形式，以及來自執行個體的系統事件。了解如何讀取這些日誌將協助您進行調查
- 網路活動：哪些端點正在連接到執行個體、執行個體正在連接到什麼，以及流量分析是什麼？

最佳實務是準備接收調查資訊，並規劃如何聯絡組織內帳戶、執行個體和工作負載的適當聯絡窗口。了解您的網路拓撲和預期的連線有助於加速影響分析。了解環境中規劃的滲透測試，以及應用程式擁有者執行的最新部署，也可以加速調查。

如果您確定活動已規劃並授權，則會更新事件並結束調查。如果已確認入侵，您和 AMS 會決定適當的遏制計畫。

階段 C：包含和消除

AMS 會與您合作，根據收集的資料和已知資訊來判斷適當的遏制活動。遏制選項包括但不限於：

- 透過快照保留資料
- 修改網路規則以限制傳入或傳出執行個體的流量
- 修改 SCP、IAM 使用者和角色政策以限制存取
- 終止、暫停或關閉執行個體
- 終止任何持久性連線
- 輪換適當的登入資料/金鑰

如果您選擇對執行個體執行根除活動，則 AMS 會支援您達成此目標。選項包括但不限於：

- 移除任何不需要的軟體
- 從乾淨的完全修補映像重建執行個體，並重新部署應用程式和組態
- 從先前的備份還原執行個體
- 將應用程式和服務部署到您帳戶中可能適合託管工作負載的另一個執行個體。

在還原服務之前，請務必判斷惡意軟體在執行個體上交付和執行的方式，以確保套用任何其他控制，以防止執行個體上的惡意軟體再次發生。AMS 會視需要為您的鑑識合作夥伴或團隊提供額外的洞見或資訊，以支援鑑識。

此時，您會使用 AMS Operations 進行復原活動。AMS 與您緊密合作，將對工作負載的干擾降至最低，並保護執行個體。

事件後報告

AMS 會視需要啟動調查審查程序，以識別學到的經驗教訓。在完成 COE 的過程中，AMS 會與您溝通相關調查結果，以協助您改善事件回應程序。

AMS 會記錄調查的最終詳細資訊、收集適當的指標，並向需要資訊的 AMS 內部團隊報告事件，包括您指派的 CSDM 和 CA。

在 AMS Advanced 中變更請求安全性審查

AWS Managed Services 變更請求審核程序可確保 AMS 在代表您在帳戶中實作請求的變更時，對請求的變更執行安全審核。

[AMS Advanced 技術標準](#) 定義最低安全標準、組態和程序，以建立帳戶的基準安全性。當 AMS 實作請求的變更時，我們會遵循這些標準。

AMS 會根據 AMS 技術標準評估所有變更請求。任何可能因為偏離技術標準而降低您帳戶安全性狀態的變更都會經過安全性審查程序。在此過程中，AMS 會反白顯示相關風險，並由您的授權風險核准者審查和核准，以平衡安全和業務需求。

客戶安全風險管理程序

AMS 進階客戶安全風險管理 (CSRM) 程序有助於清楚地識別風險，並向正確的擁有者傳達風險。此程序可將環境中的安全風險降至最低，並減少已識別風險的持續營運開銷。

根據預設，當組織的人員請求 AMS 對您的受管環境實作變更時，AMS 會檢閱變更，以判斷請求是否超出技術標準，這可能會改變您帳戶的安全狀態。如果存在高或非常高的安全風險，則您的授權安全人員會接受或拒絕變更審查。對於 AMS 操作帳戶的能力，也會評估請求的變更是否有負面影響。如果審查發現可能的負面影響，則需要在 AMS 內進行額外的審查和核准。

對於高風險或極高風險，您可以在 CSRM 程序中選擇退出核准型工作流程。若要將特定帳戶的 CSRM 選項從標準 CSRM 變更為僅限通知，請與您的 Cloud Service Delivery Manager 合作建立一次性風險接受。如果您選擇繼續僅通知選項，則無論風險類別為何，AMS 都會實作請求的變更。此外，AMS 會向您的授權風險核准者傳送風險通知，而不是在變更實作之前尋求核准。如需 AMS CSRM 程序、如何在加入新的 AMS 帳戶時變更預設 CSRM 選項，或如何更新現有帳戶的詳細資訊，請洽詢您的 Cloud Architects 或 Cloud Service Delivery Manager。

Note

AMS 強烈建議您在所有帳戶中使用標準 CSRM 的預設選項。

AMS Advanced 技術標準

以下是 AMS Advanced 技術標準類別：

ID	類別
AMS-STD-001	標記組態
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	網路安全
AMS-STD-004	滲透測試

ID	類別
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	主機安全性
AMS-STD-007	日誌
AMS-STD-008	AMS-MAD
AMS-STD-009	其他事項

AMS Advanced 中的標準控制項

以下是 AMS 中的標準控制項：

AMS-STD-001 - 標記組態

以下是 001 - 標記組態的標準控制項。

1. AMS 團隊用於操作和管理目的所需的所有 AWS 資源都必須具有下列鍵值對。
 - AppId= AMSInfrastructure
 - 環境 = AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=True
2. 除了先前列出的標籤外，AMS 團隊所需的所有標籤都必須具有 AMS 字首清單中提及的字首（請參閱備註）。
3. AMS 團隊 (AppId、Environment 和 AppName) 所需的標籤值，可以在您根據變更請求建立的任何資源上進行變更。
4. 不得根據您的變更請求刪除 AMS 所需堆疊上的任何標籤。
5. 您無法為您的基礎設施使用 AMS 標籤命名慣例，如第 2 點所述。
6. 您可以在 AMS 所需的資源中建立自訂標籤（通常用於計費和成本報告使用案例）。如果資源是透過堆疊更新而非更新範本來更新，則會保留自訂標籤。

 Note

AMS 字首清單

1. ams-*
2. AWSManagedServices*
3. /ams/*
4. ams*
5. AMS*
6. Ams*
7. mc*
8. MC*
9. Mc*
- 10.sentinel*
- 11.Sentinel*
- 12.Managed_Services*
- 13.NewAMS*
- 14.AWS_*
- 15.aws*
- 16.VPC_*
- 17.CloudTrail*
- 18.Cloudtrail*
- 19/aws_reserved/
- 20.輸入*
- 21.EPSDB*
- 22.MMS*
- 23.TemplateId*
- 24.StackSet-ams*
- 25.StackSet-AWS-Landing-Zone
- 26.IAMPolicy*

28根*

29LandingZone*

30StateMachine*

31codedeploy_service_role

32managementhost

33https : //sentinel.int。

34eps

35.UnhealthyInServiceBastion

36毫秒-

AMS-STD-002 - AWS Identity and Access Management (IAM)

ID	技術標準
1.0	逾時持續時間
1.1	聯合身分使用者預設逾時工作階段為一小時，最多可增加四個小時。
1.2	預設堆疊存取時間為 12 小時。
2.0	AWS 根帳戶用量
2.1	如果根帳戶因任何原因使用，Amazon GuardDuty 必須設定為產生相關調查結果。
2.2	對於單一帳戶登陸區域 (SALZ) 帳戶和多帳戶登陸區域 (MALZ) 管理帳戶（先前稱為主帳戶/帳單帳戶），根使用者帳戶必須啟用虛擬 MFA，並在帳戶加入期間捨棄 MFA 軟字符，因此 AMS 和客戶都無法登入為根帳戶。標準 AWS 根密碼遺失程序必須與 AMS Cloud Service Delivery Manager (CSDM) 一起遵循。此組態必須在 AMS 受管帳戶的生命週期期間保留。

ID	技術標準
2.3	您不得為根帳戶建立存取金鑰。
3.0	使用者建立和修改
3.1	可以建立具有程式設計存取和唯讀許可的 IAM 使用者/角色，無需任何時間限制政策。不過，不允許在帳戶中所有 Amazon Simple Storage Service 儲存貯體中讀取物件（例如 S3 : GetObject) 的許可。
3.1.1	用於主控台存取和具有唯讀許可的 IAM 人類使用者可以使用時間限制政策（最多 180 天）建立，而removal/renewal/extension時間限制政策將導致風險通知。不過，不允許讀取帳戶中所有 S3 儲存貯體中物件（例如 S3 : GetObject) 的許可。 S3
3.2	在沒有接受風險的情況下，不得在客戶帳戶中建立具有任何基礎設施變更許可（寫入和許可管理）的主控台和程式設計存取的 IAM 使用者和角色。S3 物件層級寫入許可存在例外狀況，只要特定儲存貯體位於非 AMS 相關標籤的範圍和標記操作中，這些許可就可以接受而不接受風險。
3.3	可以在 SALZ 或 MALZ 應用程式帳戶customer_servicenow_user 和 *core 帳戶* 中建立名為且customer_servicenow_logging_user 需要 ServiceNow 整合的程式設計存取 IAM 使用者，無需任何時間限制政策。

ID	技術標準
3.4	您可以建立在 SALZ customer_cloud_endure_policy 和 MALZ 帳戶中使用 CloudEndure 整合所需的和 customer_cloud_endure_deny_policy (具有唯讀存取權) 具有程式設計存取權的 IAM 使用者，但在計劃的遷移期間需要有時間限制的政策。時間限制的最長期間為 180 天，不含任何 RA。SCP 也獲授權變更 MALZ 帳戶，以允許這些政策在所需期間內運作。您可以根據您的需求定義適當的遷移時段，並視需要調整。
4.0	政策、動作和 APIs
4.1	SALZ 帳戶中的所有 IAM 使用者和角色都必須連接預設的客戶拒絕政策 (CDP)，以保護 AMS 基礎設施免於意外或故意損壞。
4.2	AMS SCPs 必須在 MALZ 中的所有 AMS 受管帳戶中啟用。
4.3	能夠在 KMS 金鑰上執行管理動作的身分，例如 PutKeyPolicy、和 ScheduleKeyDeletion，必須僅限於 AMS 運算子和自動化主體。
4.4	政策不得以等同於「效果」：「允許」搭配「動作」：「*」而非「資源」：「*」的陳述式提供管理員存取權，而不接受風險。
4.5	IAM 政策不得包含任何動作，包含動作 允許 S3：*** 在任何儲存貯體上，而不接受風險。
4.6	客戶 IAM 政策中不得針對 AMS 基礎設施金鑰對 KMS 金鑰政策進行 API 呼叫。

ID	技術標準
4.7	不允許繞過變更管理程序 (RFC) 的動作，例如啟動或停止執行個體、建立 S3 儲存貯體或 RDS 執行個體等。
4.8	不允許對 Amazon Route 53 中的 AMS 基礎設施 DNS 記錄進行變更的動作。
4.9	在遵循到期程序後建立主控台存取權的 IAM 人工使用者，除了信任政策、擔任角色和時間有限的政策之外，不得直接連接任何政策。
4.10	您可以在相同帳戶中建立具有特定秘密或命名空間讀取存取權 AWS Secrets Manager 的 Amazon EC2 執行個體描述檔。
4.11	AWS Managed Services Change Management (AMSCM) 或 AWS Managed Services Service 知識管理系統 (AMSSKMS) 許可可以新增至任何角色（可開啟 SR/Incident/RFC 的）。
4.12	IAM 政策不得包含任何動作，其中包括在任何 AMS Amazon CloudWatch 日誌群組上允許 log : DeleteLogGroup 和 logs : DeleteLogStream 的動作。
4.13	不允許建立多區域金鑰的許可。
4.14	若要提供尚未在帳戶中建立之 S3 儲存貯 ARNs 的存取權，請使用服務特定的 S3 條件金鑰 <code>s3:ResourceAccount</code> 來指定帳戶號碼。
4.15	您可以檢視、建立、列出和刪除自訂儀表板的存取權，但只能在 Amazon CloudWatch 儀表板上檢視和列出存取權。
4.15.1	您可以檢視、建立、列出和刪除對 S3 儲存鏡頭自訂儀表板的存取權。

ID	技術標準
4.16	可以將 SQL Workbench 相關的完整許可授予角色/使用者，以便在 Amazon Redshift 資料庫上運作。
4.17	可將任何 AWS CloudShell 許可授予客戶角色，做為 CLI 的替代方案。
4.18	以 AWS 服務 做為信任委託人的 IAM 角色也必須符合 IAM 技術標準。
4.19	服務連結角色 (SLRs) 不受 AMS IAM 技術標準的約束，因為它們是由 IAM 服務團隊建置和維護。
4.20	IAM 政策不得允許對帳戶中所有儲存貯體的 Amazon S3 儲存貯體物件（例如 Amazon S3 : GetObject) 進行不受限制的讀取存取： • 在開發人員模式帳戶中：違規會導致風險通知 • 在非開發人員模式帳戶中：違規需要接受風險
4.21	資源類型 "savingsplan" 的所有 IAM 許可都可以授予客戶。
4.22	AMS 工程師不允許在任何資料儲存服務中手動複製或移動客戶資料（檔案、S3 物件、資料庫），例如 Amazon S3、Amazon Relational Database Service、Amazon DynamoDB 等，或在作業系統檔案系統中。
4.23	不得修改 SCP 政策，以允許在任何 AMS 受管帳戶中進行任何其他存取。
4.24	不允許 SCP 政策中可能破壞 AMS 基礎設施或管理功能的任何變更。（注意：AMS 資源具有標籤 AppId= AMSInfrastructure ，並遵循 AMS Protected Namespace)。

ID	技術標準
4.25	AMS 自動化 IAM 佈建功能必須在您的帳戶中啟用，做為選擇加入功能。
4.26	AMS 人工擔任的角色或使用者不得存取 S3、RDS、DynamoDB、Redshift、Elasticache、EFS 和 FSx 中的客戶內容。此外，在運算子角色中，必須明確拒絕對其他發佈的已知新 APIs 的任何存取 AWS 服務，以授予對客戶內容的存取。
5.0	聯合
5.1	必須使用 AMS 受管帳戶中的聯合身分來設定身分驗證。
5.2	只能有從 AMS AD 到作用中目錄的單向傳出信任 (AMS AD 信任內部部署 AD)。
5.3	用於向 AMS 進行身分驗證的身分存放區不得存在於 AMS 受管應用程式帳戶中。
6.0	跨帳戶政策
6.1	您可以根據客戶記錄設定屬於相同客戶的 AMS 帳戶之間的 IAM 角色信任政策。
6.2	只有在非 AMS 帳戶由相同 AMS 客戶擁有時 (透過確認其位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱相符)，才能設定 AMS 和非 AMS 帳戶之間的 IAM 角色信任政策。
6.3	未經風險接受，不得設定 AMS 帳戶與第三方帳戶之間的 IAM 角色信任政策。
6.4	您可以設定跨帳戶政策，在相同客戶的 AMS 帳戶之間存取任何客戶管理的 CMKs。

ID	技術標準
6.5	您可以設定跨帳戶政策，以透過 AMS 帳戶存取非 AMS 帳戶中的任何 KMS 金鑰。
6.6	在未接受風險的情況下，不允許跨帳戶政策存取第三方帳戶在 AMS 帳戶中的任何 KMS 金鑰。
6.6.1	只有在非 AMS 帳戶由相同 AMS 客戶擁有時，才能設定跨帳戶政策以存取 AMS 帳戶內的任何 KMS 金鑰。
6.7	您可以設定跨帳戶政策，在相同客戶的 AMS 帳戶之間存取可存放資料的任何 S3 儲存貯體資料或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.8	可從具有唯讀存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或資源的跨帳戶政策，其中的資料可存放在非 AMS 帳戶中（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.9	存取任何 S3 儲存貯體資料或資源的跨帳戶政策（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift），其具有從 AMS 到非 AMS 帳戶（或非 AMS 到 AMS 帳戶）的寫入許可，只有在非 AMS 帳戶是同一 AMS 客戶所擁有（透過確認他們位於相同的 AWS Organizations 帳戶或將電子郵件網域與客戶的公司名稱相符）時，才必須設定。
6.10	跨帳戶政策，可從具有唯讀存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或可存放資料的資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。

ID	技術標準
6.11	從具有寫入存取權的 AMS 帳戶存取任何 S3 儲存貯體資料或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）的跨帳戶政策不得設定。
6.12	在未接受風險的情況下，不得設定來自第三方帳戶的跨帳戶政策來存取可存放資料的 AMS 客戶 S3 儲存貯體或資源 (asAmazon RDS、Amazon DynamoDB 或 Amazon Redshift)。
7.0	User Groups (使用者群組)
7.1	允許具有唯讀和非變動許可的 IAM 群組。
8.0	以資源為基礎的政策
8.1	AMS 基礎設施資源必須透過附加以資源為基礎的政策，不受未經授權的身分管理。
8.2	您的資源必須使用最低權限的資源型政策設定，除非您明確指定不同的政策。
9.0	自助式佈建服務 (SSPS)
9.1	AMS 預設 IAM 角色或政策（包括執行個體描述檔、SSPS、模式）不得修改，無論是否接受任何風險接受。允許（不接受風險）信任政策的例外狀況。預設 SSP 角色也允許標記角色、政策或使用者變更。
9.3	Systems Manager Automation 主控台角色的 SSPS 政策無法連接到預設角色以外的任何自訂角色。其他 SSPS 政策只有在確保將政策連接至自訂角色時，才能連接至自訂 IAM 角色，而不會為預設 SSPS 服務提供預期設計以外的額外許可。

AMS-STD-003 - 網路安全

以下是 003 - Network Security 的標準控制項：

ID	技術標準
	聯網
1.0	所有 EC2 執行個體只能透過堡壘主機、堡壘主機 VPC CIDR 範圍或從相同的執行個體 VPC CIDR 範圍透過 SSH 或 RDP 存取。
2.0	允許 EC2 執行個體上的彈性 IP
3.0	必須使用 AMS 控制平面和資料平面 TLS 1.2+ 中的延伸。
4.0	所有輸出流量必須使用帳戶 IGW 或 TGW 傳遞。
5.0	如果根據 9.0 未連接到負載平衡器，則安全群組在傳入規則中不得具有 0.0.0.0/0 的來源
6.0	未經風險接受，不得公開 S3 儲存貯體或物件。
7.0	連接埠 SSH/22 或 SSH/2222（非 SFTP/2222）、TELNET/23、RDP/3389、WinRM/5985-5986、VNC/5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 RPC/135、NETBIOS/137-139 上的伺服器管理存取權不得透過安全群組從 VPC 外部進行。
8.0	連接埠 (MySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433) 或自訂連接埠上的資料庫管理存取權，不得允許來自未透過 DX、VPC 對等或 VPN 透過安全群組路由至 VPC 的公有 IPs。

ID	技術標準
8.1	任何可存放客戶資料的資源都不應直接公開至公有網際網路。
9.0	透過連接埠 HTTP/80、HTTPS/8443 和 HTTPS/443 從網際網路存取的直接應用程式，只允許載入平衡器，但不允許直接存取任何運算資源，例如 EC2 執行個體、ECS/EKS/Fargate 容器等。
10.0	允許從客戶私有 IP 範圍透過連接埠 HTTP/80 和 HTTPS/443 存取應用程式。
11.0	未經風險接受，不得允許對控制 AMS 基礎設施存取的安全群組進行任何變更。
12.0	AMS Security 是指每次請求將安全群組連接到執行個體時的標準。
13.0	連接埠 3389 和 22 上的客戶堡壘存取必須只允許來自透過 DX、VPC 對等或 VPN 路由至 VPC 的私有 IP 範圍。
14.0	只有在相同 AMS 客戶擁有非 AMS 帳戶時（透過確認它們位於相同的 AWS Organization 帳戶下，或將電子郵件網域與客戶的公司名稱相符），才能使用內部工具，設定私有託管區域與 VPCs 從 AMS 到非 AMS 帳戶（或非 AMS 到 AMS 帳戶）的跨帳戶關聯。
15.0	您可以允許屬於相同客戶之帳戶之間的 VPC 對等互連。
16.0	AMS 基礎 AMIs 可以使用內部工具與非 AMS 帳戶共用，只要這兩個帳戶都由同一客戶擁有（透過確認它們位於相同 AWS Organizations 帳戶下，或將電子郵件網域與客戶的公司名稱相符）。

ID	技術標準
17.0	未經風險接受，不得在任何安全群組中設定 FTP 連接埠 21。
18.0	只要客戶擁有所有帳戶，就可以透過傳輸閘道進行跨帳戶網路連線。
19.0	不允許將私有子網路設為公有
20.0	不允許與第三方帳戶（非客戶擁有）的 VPC 互連連線。
21.0	不允許使用第三方帳戶（非客戶擁有）的 Transit Gateway 連接。
22.0	AMS 為客戶提供服務所需的任何網路流量，不得在客戶網路輸出點遭到封鎖。
23.0	允許與同一客戶 AWS 帳戶擁有的 共用解析程式規則，並發出風險通知
19.0	ICMP
19.1	從客戶基礎設施向 Amazon EC2 發出的傳入 ICMP 請求將需要風險通知。
19.2	允許透過 DX、VPC 對等或 VPN 透過安全群組路由至 Amazon VPC 的公IPs 傳入請求。
19.3	未透過 DX、VPC 對等或 VPN 透過安全群組路由至 Amazon VPC 的公IPs 傳入請求需要接受風險。
19.4	允許從 Amazon EC2 到任何目的地的傳出 ICMP 請求。
20.0	安全群組共用

ID	技術標準
20.1	如果安全群組符合此安全標準，則可以在相同帳戶中VPCs 之間共用，以及在相同組織中的帳戶之間共用。
20.2	如果安全群組不符合此標準，且此安全群組先前需要接受風險，則不允許在相同帳戶中的 VPCs 之間或相同組織中的 帳戶之間使用安全群組共用功能，而不接受該 VPC 或帳戶的新帳戶的風險。

AMS-STD-004 - 滲透測試

以下是 004 - 滲透測試的標準控制項

1. AMS 不支援 pentest 基礎設施。這是客戶的責任。例如，Kali 不是 Linux 的 AMS 支援發行版本。
2. 客戶需要遵守[滲透測試](#)。
3. 如果客戶想要在帳戶中執行基礎設施滲透測試，AMS 會提前 24 小時預先通知。
4. AMS 會根據客戶在變更請求或服務請求中明確陳述的客戶需求，佈建客戶滲透基礎設施。
5. 客戶滲透基礎設施的身分管理是客戶的責任。

AMS-STD-005 - GuardDuty

以下是 005 - GuardDuty 的標準控制項

1. GuardDuty 必須隨時在所有客戶帳戶中啟用。
2. MALZ 中客戶受管應用程式帳戶 (CMA) 的 GuardDuty 調查結果不會導致 ops 團隊發出警示。
3. GuardDuty 提醒必須存放在相同帳戶或相同組織下的任何其他受管帳戶中。
4. 不得使用 GuardDuty 的信任 IP 清單功能。反之，自動封存可以用作替代方案，這適用於稽核目的。
5. GuardDuty 管理員委派不得在 MALZ 中啟用，因為委派管理員可以執行高權限動作，例如在其他帳戶中停用 GuardDuty，而無需接受風險。
6. GuardDuty Auto Archive Filters 應使用最大傳回的最小範圍。例如，如果 AMS 會在不同的 CIDR 區塊中看到多個無法預測IPs，且有適合使用的公司 ASN，請使用 ASN。不過，如果您的範圍可以縮小到特定範圍或 /32 地址，則範圍可以縮小到這些範圍。

AMS-STD-006 - 主機安全

以下是 006 - Host Security 的標準控制項

- 防毒代理程式必須隨時在所有 EC2 執行個體上執行。（例如，Trend Micro DSM）。
- 必須啟用反惡意軟體模組。
- EPS 代理程式必須包含要掃描的所有目錄和檔案。
- 由防毒解決方案隔離的檔案可以隨需與您共用。
- 不應安裝第三方端點安全解決方案。
- 防毒簽章更新頻率必須設定為每天至少一次。
- 排定的掃描頻率必須設定為每月至少一次。
- 必須隨時啟用和執行即時（存取中）掃描。
- AMS 不得在您的執行個體上執行任何非 AMS 所擁有或撰寫的自訂指令碼。（注意：您可以透過堆疊管理員存取 CT 或使用[AWS Systems Manager 自動化 \(AMS SSPS\)](#) 來使用堆疊管理員存取。
- 不得在 Windows 主機上停用網路層級驗證 (NLA)。
- 根據設定的修補程式週期，主機作業系統必須具有最新的安全修補程式。
- AMS 受管帳戶不得在帳戶中有未受管的執行個體。
- 不允許 AMS 在執行個體上建立本機管理員帳戶。
- 不得在 EC2 上建立金鑰對。
- 您不得使用宣告為生命週期結束 (EOL) 的作業系統，而且廠商或第三方不提供進一步的安全支援。

AMS-STD-007 - 記錄

以下是 007 - 記錄的標準控制項

ID	技術標準
1.0	日誌類型
1.1	作業系統日誌：所有主機必須至少記錄主機身分驗證事件、所有使用提升權限的存取事件，以及所有存取和權限組態變更的存取事件，包括成功和失敗。

ID	技術標準
1.2	AWS CloudTrail：必須啟用並設定 CloudTrail 管理事件記錄，才能將日誌交付至 S3 儲存貯體。
1.3	VPC 流程日誌：所有網路流量日誌都必須透過 VPC 流程日誌記錄。
1.4	Amazon S3 伺服器存取記錄：存放日誌的 AMS 強制 S3 儲存貯體必須啟用伺服器存取記錄。
1.5	AWS Config 快照：AWS Config 必須記錄所有區域中所有支援資源的組態變更，並將組態快照檔案至少每天交付至 S3 儲存貯體一次。
1.6	Endpoint Protection System (EPS) 日誌：必須啟用並設定 EPS 解決方案日誌，才能將日誌交付至 CloudWatch Logs 日誌群組。
1.7	應用程式日誌：客戶有權在其應用程式中啟用記錄，並存放在 CloudWatch Logs 日誌群組或 S3 儲存貯體中。
1.8	S3 物件層級記錄：客戶有權在其 S3 儲存貯體中啟用物件層級記錄。
1.9	服務記錄：客戶有權啟用和轉送 SSPS 服務的日誌，例如任何核心服務。
1.10	Elastic Load Balancing(Classic/Application Load Balancer/Network Load Balancer) 日誌：存取和錯誤日誌項目必須存放在 AMS 2.0 受管 S3 儲存貯體中。
2.0	存取控制

ID	技術標準
2.1	您不得在存放日誌和 CloudWatch Logs 日誌群組的 AMS 所需的 S3 儲存貯體中擁有寫入或刪除存取權。
2.2	您必須擁有您帳戶中所有日誌的唯讀存取權。
2.3	存放日誌的 AMS 授權 S3 儲存貯體不允許第三方將使用者視為儲存貯體政策中的原則。
2.4	未經您授權的安全聯絡人明確核准，不得刪除來自 CloudWatch Logs 日誌群組的日誌。
3.0	日誌保留
3.1	AMS 授權的 CloudWatch Logs 日誌群組在日誌上必須至少保留 90 天。
3.2	存放日誌的 AMS 授權 S3 儲存貯體在日誌上必須至少保留 18 個月。
3.3	AWS Backup 快照應可在支援的資源上至少保留 31 天。
4.0	加密
4.1	必須在存放日誌的 AMS 團隊所需的所有 S3 儲存貯體中啟用加密。
4.2	任何從客戶帳戶轉送到任何其他帳戶的日誌都必須加密。
5.0	完整性
5.1	必須啟用日誌檔案完整性機制。必須在 AMS 團隊所需的 AWS CloudTrail 線索中設定「記錄檔案驗證」。
6.0	日誌轉送

ID	技術標準
6.1	任何日誌都可以從一個 AMS 帳戶轉送到相同客戶的另一個 AMS 帳戶。
6.2	只有在相同 AMS 客戶擁有非 AMS 帳戶時，才能從 AMS 轉送任何日誌至非 AMS 帳戶。
6.3	來自客戶帳戶的任何日誌都不得轉發到第三方帳戶（非由客戶擁有）。

AMS-STD-008 - AMS-MAD

以下是 008 - AMS-MAD 的標準控制項

ID	技術標準
1.0	存取管理
1.1	只有具有互動式登入和自動化任務的 AMS 特殊權限使用者才能登入管理主機，以在客戶帳戶中管理受管 AD。
1.2	AD 管理員只能擁有委派管理員權限 (AMS 委派管理員群組)。
1.3	登入客戶 AD 環境（管理主機或執行個體）的工程師必須具有有時間限制的存取權。
1.4	客戶在 EC2 執行個體中使用遠端伺服器管理員工具可以唯讀存取 AD 物件。
1.5	不得允許 Active Directory 使用者或群組的管理權限。
1.6	AWS 允許與相同客戶 AWS 帳戶擁有的共用目錄，並發出風險通知。
2.0	服務帳戶

ID	技術標準
2.1	群組受管服務帳戶 (gMSA) 必須在應用程式支援的位置使用，而不是標準服務帳戶。
2.2	所有其他服務帳戶必須在風險接受程序之後建立。
2.3	除非客戶明確要求，否則不得重複使用 AD 安全群組。應建立新的 AD 群組。請求存取服務帳戶的電腦物件必須新增至新的安全群組。
2.4	任何 gMSA 服務帳戶都必須新增至「受管服務帳戶」組織單位 (OU) 下。
2.5	任何非 gMSA 服務帳戶都必須新增至「使用者→服務帳戶」OU 下。
3.0	群組政策物件 (GPO)
3.1	如果「Windows 設定 > 安全設定」GPO 下的任何設定以任何方式從目前狀態降低帳戶的安全狀態，則不得修改。
3.2	在 MALZ 中，從請求 GPO 建立的應用程式帳戶提交的 RFCs，必須將 GPO 連結至對應至應用程式帳戶的 OU。任何會影響所有帳戶的 GPOs 都必須來自共用服務帳戶。
3.3	對於作用中目錄網域下的所有伺服器，預設 RDP 閒置工作階段逾時必須設定為 15 分鐘。
4.0	Active Directory 信任
4.1	如果條件式轉寄站IPs 透過 DX、VPC 對等或 VPN 路由至 VPC，則允許單向傳出信任 (AMS 託管目錄至客戶目錄)。
5.0	其他

ID	技術標準
5.1	必須啟用日誌檔案完整性機制。必須在 AMS 團隊所需的 AWS CloudTrail 線索中設定「記錄檔案驗證」。
6.0	日誌轉送
6.1	客戶使用者、群組、電腦物件、OU 或其他實體不得根據 AMS 命名慣例使用 AMS 命名慣例。
6.2	所有 OUs 都必須由 AMS 管理。

AMS-STD-009 - 其他

以下是 009 - 其他 的標準控制項

- 如果在資源、物件、資料庫或檔案系統中啟用加密，則不得停用。

在您的環境中帶來高或極高安全風險的變更

下列變更會在您的環境中帶來高或非常高的安全風險：

AWS Identity and Access Management

- High_Risk-IAM-001：建立根帳戶的存取金鑰
- High_Risk-IAM-002：修改 SCP 政策以允許其他存取
- High_Risk-IAM-003：修改 SCP 政策可能會破壞 AMS 基礎設施
- High_Risk-IAM-004：在客戶帳戶中建立具有基礎設施變動許可（寫入、許可管理或標記）的角色/使用者
- High_Risk-IAM-005：IAM 角色信任 AMS 帳戶與第三方帳戶之間的政策（非客戶所擁有）
- High_Risk-IAM-006：跨帳戶政策，透過第三方帳戶從 AMS 帳戶存取任何 KMS 金鑰
- High_Risk-IAM-007：來自第三方帳戶的跨帳戶政策，用於存取可存放資料的 AMS 客戶 S3 儲存貯體或資源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）
- High_Risk-IAM-008：指派具有客戶帳戶中任何基礎設施變動許可的 IAM 許可
- High_Risk-IAM-009：允許列出和讀取帳戶中的所有 S3 儲存貯體

- High_Risk-IAM-010：具有讀取/寫入許可的自動化 IAM 佈建

網路安全

- High_Risk-NET-001：從網際網路開啟作業系統管理連接埠 SSH/22 或 SSH/2222（非 SFTP/2222）、TELNET/23、RDP/3389、WinRM/5985-5986、VNC/5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 NETBIOS/137-139
- High_Risk-NET-002：從網際網路開啟資料庫管理連接埠 MySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433 或任何管理客戶連接埠
- High_Risk-NET-003：直接在任何運算資源上開啟應用程式連接埠 HTTP/80、HTTPS/8443 和 HTTPS/443。例如，EC2 執行個體、ECS/EKS/Fargate 容器等來自網際網路
- High_Risk-NET-004：安全群組的任何變更，可控制對 AMS 基礎設施的存取
- High_Risk-NET-006：VPC 與第三方帳戶互連（非客戶擁有）
- High_Risk-NET-007：新增客戶防火牆作為所有 AMS 流量的輸出點
- High_Risk-NET-008：不允許與第三方帳戶連接 Transit Gateway
- High_Risk-S3-001：在 S3 儲存貯體中佈建或啟用公開存取

日誌

- High_Risk-LOG-001：停用 CloudTrail。(Ops Site Manager 需要核准)
- High_Risk-LOG-002：停用 VPC 流程日誌。(Ops Site Manager 需要核准)
- High_Risk-LOG-003：透過任何方法 (S3 事件通知、SIEM 代理程式提取、SIEM 代理程式推送等) 將日誌從 AMS 受管帳戶轉送至第三方帳戶（非客戶擁有）
- High_Risk-LOG-004：針對 CloudTrail 使用非 AMS 追蹤

主機安全性

- High_Risk-HOST-001：因任何原因停用帳戶中的端點安全。(Ops Site Manager 需要核准)
- High_Risk-HOST-002：停用資源或帳戶層級的修補。
- High_Risk-HOST-003：在帳戶中部署未受管的 EC2 執行個體。
- High_Risk-HOST-004：執行客戶提供的自訂指令碼。
- High_Risk-HOST-005：在執行個體上建立本機管理員帳戶。
- High_Risk-HOST-006：Trend Micro EPS 檔案類型/延伸掃描排除或停用端點上的惡意軟體保護。

 Note

與滲透測試、漏洞掃描或服務影響事件/已知需要主動採取行動的效能問題相關的 EPS 反惡意軟體排除或 GuardDuty 抑制規則不需要接受風險。在這些情況下，風險通知就足夠了。

- High_Risk-HOST-007：建立 EC2 的 KeyPair
- High_Risk-HOST-008：在 EC2 中停用端點安全
- High_Risk-HOST-009：使用生命週期結束 (EOL) 作業系統的帳戶

Miscellaneous (其他)

- High_Risk-ENC-001：啟用任何資源時停用加密

受管 Active Directory

- High_Risk-AD-001：提供管理員權限給作用中的目錄使用者或群組
- High_Risk-AD-002：能夠降低帳戶安全狀態的 GPO 政策

AMS Advanced 中的持續性管理

作為持續性管理的一部分，AWS Managed Services (AMS) 會使用 AWS Backup 提供原生服務的自動存取 AWS。這有助於存取支援 Amazon EBS、Amazon EC2、Amazon RDS、Amazon EFS 等的服務。

若要進一步了解，請參閱 [AWS Backup：運作方式](#)。

主題

- [什麼是持續性管理？](#)
- [持續性管理的運作方式](#)
- [災難復原回應](#)
- [災難復原規劃](#)

什麼是持續性管理？

持續性管理是 AMS 為您的帳戶提供備份和快照的程序。

AMS AWS Backup 透過您用來建立和管理備份任務和計劃的變更類型，提供 的存取權。

持續性管理的運作方式

AMS 使用 [AWS Backup](#) 進行持續性管理。

開始在 AMS AWS Backup 中使用 時：

1. 執行隨需備份
2. 建立備份計畫（選用，AMS 提供預設備份計畫）
3. 使用預設 AMS 備份保存庫（選用）
4. 管理（執行、精簡、刪除等）備份計畫和復原點

AMS 備份計畫

備份計畫是一種政策表達式，可定義您希望備份支援的 AWS 資源的時間和方式，例如 RDS 資料庫、EBS 磁碟區、DynamoDB 資料表和 EFS 檔案系統。排程和保留政策是透過自訂備份計劃進行管理，您可以使用變更類型 (CT) 搭配 AMS Advanced 或 AWS Backup 搭配 AMS Accelerate 使用 來建

立。使用標籤將資源指派給備份計劃，並根據定義的備份計劃 AWS Backup 自動備份和保留已指派資源的備份。如果您擁有的工作負載有不同的備份需求，則可以建立多個備份計劃。

備份計畫最多可以有六個備份規則，定義排程和保留期間，以及其他詳細資訊。備份排程會決定何時 AWS Backup 啟動備份任務，以及建立備份的頻率。您可以選擇每小時、每日、每週或每月的頻率。刪除天數設定會決定快照在自動刪除前的儲存天數。

Note

AMS 進階：如果您從舊版 AMS 備份系統遷移，AMS 會建立預設備份計劃以回溯相容性。此案例中的 key : value 對是 Backup : True。為了支援回溯相容性，這裡的值不區分大小寫，因此 Backup : True 或 Backup : TRUE 都是有效的標籤。所有其他索引鍵：值對都區分大小寫。

AWS Backup 可以在 EBS 磁碟區層級或 Amazon EC2 執行個體層級操作，但請勿同時操作兩者，因為這可能會導致競爭條件，其中備份可能會衝突。

預設備份計劃，多帳戶登陸區域

在新帳戶建立 RFC 期間，AMS 會確保帳戶層級有整體的預設備份計劃，以保護工作負載。預設會設定必要欄位的值，如下節所示：

預設 AMS 備份計畫

default-backup-plan

TAG 金鑰：Backup

TAG 值：True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
```



```
RuleForYearlyBackups delete after years: 2 years
```

預設 AMS 備份計畫	開始時間	Retention
hourly backup	N/A	N/A
daily backup	daily 11:30PM UTC	7 days
weekly backup	weekly 11:30PM UTC, only on Saturday	4 weeks
monthly backup	monthly 11:30 PM UTC, on day 1 of the month	26 weeks
yearly backup	11:30 PM UTC, on day 1 of the month	2 years

增強型預設 AMS 備份計畫

該計畫是用於防範勒索軟體攻擊的 AWS Backup 最佳實務藍圖。它實作每日、每週、每月和每年備份策略。在[支援的資源](#)上啟用 AWS Backup [連續備份](#)，並具有最大保留期 (31 天)。

ams-enhanced-default-backup-plan

TAG 金鑰：backup-orchestrator-enhanced

TAG 值：true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
  UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
  UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
  02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
  UTC time on day 1 of the month, only in January)
```

```
RuleForYearlyBackups delete after years: 2 years
```

增強型 AMS 備份計劃	開始時間	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	31 days
weekly backup	Saturday, 2:00 UTC	6 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

資料敏感 AMS 備份計畫

該計畫是 AWS Backup 最佳實務的藍圖，可防止資料敏感型應用程式的勒索軟體攻擊。它實作每小時、每日、每週、每月和每年備份策略。AWS Backup [連續備份](#)會在[支援的資源](#)上啟用最大保留期 (31 天)。

ams-data-sensitive-backup-plan

TAG 金鑰：backup-orchestrator-data-sensitive

TAG 值：true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

資料敏感 AMS 備份計畫	開始時間	Retention
hourly backup	at the hour mark	7 days
daily backup	daily 4:00 UTC	31 days
weekly backup	Saturday, 2:00 UTC	6 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

AMS 備份保存庫

AWS Backup 會將快照組織到稱為保存庫的邏輯儲存單位。

您可以使用標籤，在個別保存庫層級控制備份保存庫通知。您可以新增 標籤，AMSNotificationOptOut並將 值設定為特定保存庫True上的，以選擇不接收特定保存庫的通知。若要繼續從保存庫取得通知，請移除 標籤。

若要檢視 AMS 備份的清單，請開啟 [AWS Backup 主控台](#)。在導覽窗格中，選擇備份保存庫，然後從下表中選取其中一個 AMS 備份保存庫。在備份區段中，檢視備份文件庫中所有備份的清單。選取要編輯、刪除或還原的備份。

AMS 備份計劃的保存庫

AMS 保存庫名稱	描述
ams-automated-backups	This vault receives all recovery points taken by the AMS Advanced default AWS Backup plan default-backup-plan.
ams-automated-enhanced-backups	This vault receives all recovery points taken by AMS Advanced enhanced default AWS Backup plan ams-enhanced-default-backup-plan.
ams-automated-data-sensitive-backups	This vault receives all recovery points taken by AMS Advanced AWS Backup plan ams-data-sensitive-backup-plan.

AMS 保存庫名稱	描述
ams-manual-backups	This is the default location for all backups from Start Backup Job RFC (ct-2hhud2lx01tq7) backup plans, if no vault name is defined.
ams-custom-backups	This is the default location for the snapshots AMS takes prior to patching an instance using Patch Orchestrator or the monthly patch activities. These are automatically removed according to the AMS patch lifecycle default policy of 60 days.

AMS 備份變更類型

AMS 提供多種 CTs，供您建立和使用備份計畫。

Important

請勿編輯您的 AMS 預設備份計畫，因為您的變更可能會遺失。反之，請為您的自訂組態建立新的計畫。

- [備份計畫：建立](#)
- [備份任務：開始](#)
- [備份任務：停止](#)
- [復原點：刪除](#)
- [DynamoDB | 從備份建立](#)
- [EBS 磁碟區：從備份建立](#)
- [Amazon Elastic File System \(EFS\)：從備份建立](#)

AMS 備份監控和報告

Important

AMS 備份監控和報告僅適用於 AMS 支援的區域。這些是美國東部（維吉尼亞）、美國西部（加利佛尼亞北部）、美國西部（奧勒岡）、美國東部（俄亥俄）、加拿大（中部）、南美洲（聖保羅）、歐洲（愛爾蘭）、歐洲（法蘭克福）、歐洲（倫敦）、歐洲（巴黎）、亞太區域（孟買）、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）。

AMS 會產生每日自助式報告，以及資源涵蓋範圍和備份任務狀態的每月報告。每月報告會在每月商業審核 (MBRs) 中共用。若要進一步了解每日備份報告，請參閱[每日備份報告](#)。

AMS 專家會監控您使用設定的所有備份任務 AWS Backup。如果備份失敗，AMS 會調查失敗，並在可用時通知您根本原因和修復選項。為了避免警示雜訊，在您的帳戶中造成大量備份失敗的事件期間，AMS 會透過 CSDM 提出集體建議，而不是針對每個個別失敗通知您。

請注意，AMS 不會監控使用 AWS 服務的獨立備份功能設定的任何備份。

災難復原回應

除了以下各節所述的選項之外，建議您了解使用 AMS 啟動災難復原 (DR) 時應採取哪些步驟。

如果您遇到災難且需要啟動復原，請遵循下列一般準則：

1. 使用可用性類別開啟高優先順序事件。AMS 將開啟會議橋接器，並邀請您的團隊加入。
2. 了解您需要復原的資源清單。
3. 了解您需要復原的目標登陸區域 (LZ)（例如，相同的帳戶、不同的可用區域或不同的帳戶和不同的區域）。
4. 提交目標登陸區域中每個資源的復原請求。請遵循您現有的 DR 計畫，或參閱下一節中的選項（例如 [在 AMS 上使用 EBS 快照保護 EC2 的災難](#) 或 [在 AMS 上使用彈性災難復原來保護 EC2 的災難](#)）。
5. 還原應用程式功能並使用 AMS 協助來疑難排解基礎設施相關問題。

AMS 可協助您準備此事件，並為您的組織建立 DR 計畫以涵蓋這些問題。如需詳細資訊，請聯絡您的雲端服務交付管理員 (CSDM) 或雲端架構師 (CA)。

災難復原規劃

災難復原 (DR) 是企業業務持續性和合規的關鍵服務。AMS 會與您合作，協助您規劃、實作和維護 AMS 上的 DR 策略。

AMS 登陸區域 (LZ)、多帳戶和單一帳戶，可為符合大多數災難保護案例的 AMS 基礎設施元件提供原生、多可用區域、高可用性。不過，視您企業的地理覆蓋範圍而定，您可能需要區域保護。對於跨區域可用性和 DR，不同區域需要另一個 AMS 帳戶（多帳戶登陸區域和單一帳戶登陸區域都是如此）。

AMS 符合本部落格中所述的 AWS DR 指引、在[災難中快速復原關鍵任務系統](#)，並支援下列四個選項：

- 多站台（或高可用性）
- 暖待命
- 指示燈
- 備份與恢復

以下各節會說明這些選項及其 AMS 支援。

多站台或高可用性 (HA)

HA 解決方案通常由應用程式的內建功能提供，例如叢集或同步複寫。使用者會導向至 Prod 和 HA/DR 節點。DNS 會直接指向節點，或透過彈性負載平衡器 (ELB) 指向節點。

您的 AMS 雲端架構師 (CA) 將與您合作，作為 Well-Architected-Review 和 DR 規劃的一部分。

HA DR 會利用應用程式和 AWS 原生服務和功能，如下圖所示：

DR 網站可以位於相同或不同位置 AWS 區域。

Note

不同的區域（跨區域）會有不同的 Active Directory 環境。

DR（容錯移轉）步驟：自動容錯移轉，不需要手動步驟。如果主要 LZ 發生故障，使用者會自動重新路由至 DR/HA 節點。這可透過 DNS 和應用程式組態達成。

HA DR 指標：

- 復原點目標 (RPO)：<5 分鐘
- 復原時間目標和 (RTO)：<5 分鐘
- 維護：高（兩個環境都需要同步變更，例如應用程式組態、修補、SG 或 ALB、憑證等）。
- 成本：高

暖待命

「暖待命」一詞用於描述災難復原 (DR) 案例，其中環境的縮減版本正在雲端中執行。

資料複寫通常由應用程式層非同步處理到線上執行個體，而其餘執行個體（例如應用程式和 Web 層）可能會關閉以節省成本。使用者只會導向生產網站。也可以在 DR 網站中預先佈建其他 AWS 資源，例如彈性負載平衡器 (ELB)。

您的 AMS Cloud Architect (CA) 將與您合作，作為 Well-Architected-Review 和 DR 規劃的一部分。

Warm Standby DR 會利用應用程式和 AWS 原生服務和功能，如下圖所示：

DR 網站可以位於相同或不同位置 AWS 區域。

Note

不同的區域（跨區域）會有不同的 Active Directory 環境。

DR（容錯移轉）步驟：

1. 啟動資料複寫，並將 DR 站點中的資料執行個體設為主要執行個體
2. 視需要更新應用程式組態（新的 IP、伺服器名稱等）
3. 將 DNS 重新導向至 DR 網站 (ELB)
4. 需要時的 AD 相依性（服務帳戶、SPNs、GPOs 等）

HA DR 指標：

- 復原點目標 (RPO)：<1 小時

- 復原時間目標和 (RTO) : <1 小時 (取決於執行個體數量和協同運作)
- 維護 : 高 (兩個環境都需要同步變更 , 例如應用程式組態、修補、安全群組 (SG) 或應用程式負載平衡器 (ALB)、憑證等) 。
- 成本 : 中型

指示燈

在此災難復原 (DR) 方法中 , 您會為有限的一組核心服務複寫部分 Prod 環境。您的基礎設施的一小部分一律在執行中 , 同時同步可變資料 (例如資料庫或文件) , 而基礎設施的其他部分則只會在測試期間關閉和使用。與備份和復原方法不同 , 您必須確保最重要的核心元素已在 DR 登陸區域 (指示燈) 中設定並執行。

您的 AMS Cloud Architect 將與您合作 , 作為 Well-Architected-Review 和 DR 規劃的一部分。

Pilot Light DR 利用應用程式和 AWS 原生服務和功能 , 如下圖所示 :

DR 網站可以位於相同或不同位置 AWS 區域。

Note

不同的區域 (跨區域) 會有不同的 Active Directory 環境。

DR (容錯移轉) 步驟 :

1. 啟動資料複寫 , 並將 DR 站點中的資料執行個體設為主要執行個體
2. 啟動已關閉的執行個體和基礎設施
3. 視需要更新應用程式組態 (新的 IP、伺服器名稱等)
4. 視需要將執行個體新增至 ELB
5. 將 DNS 重新導向至 DR 網站 (ELB)
6. 視需要的 AD 相依性 (服務帳戶、SPNs、GPOs 等)

指示燈 DR 指標 :

- 復原點目標 (RPO) : <1 小時

- 復原時間目標和 (RTO) : ~1 小時 (取決於執行個體數量和協同運作)
- 維護 : 中
- 成本 : 中型

備份和還原

這種簡單且低成本的災難復原 (DR) 方法可將您的資料和應用程式從任何地方備份到 DR 登陸區域，以便在從災難復原期間使用。

您的 AMS Cloud Architect 會與您合作，做為備份和 DR 規劃的一部分。

備份和還原 DR 使用 AMS 自動化工具和程序，如下圖所示：

可以使用兩種備份和複寫方法：

- EBS 快照 (復原點目標 (RPO) > 1 小時)，稱為「EBS」
- AWS Elastic Disaster Recovery (復原點目標 (RPO) ~ 0.25 小時)，稱為「DRS」

DR 網站可以位於相同 或不同 AWS 區域。

Note

不同的區域 (跨區域) 具有不同的 Active Directory 環境。

DR (容錯移轉) 步驟：

1. 從快照還原執行個體 (以預留位置執行個體為先的兩步驟程序)
2. 更新應用程式組態 (新的 IP、伺服器名稱等)
3. 視需要設定其他基礎設施 (SG、ELB 等)
4. 將 DNS 重新導向至 DR 網站 (ELB)
5. 視需要更新或還原 AD 相依性 (服務帳戶、服務主體名稱 SPNs)、群組政策物件 GPOs) 等)

備份和還原 DR 指標：

- 復原點目標 (RPO) : >1 小時或 ~0.25 小時 (取決於所選的解決方案 - EBS 或 DRE)
- 復原時間目標和 (RTO) : ~1 小時 (取決於執行個體數量和協同運作)
- 維護 : 高 (兩個環境都需要同步變更 , 例如應用程式組態、修補、安全群組或應用程式負載平衡器、憑證等。
- 成本 : 中型

在 AMS 上使用 EBS 快照保護 EC2 的災難

事前準備 :

- AMS 產品登陸區域 (來源)
- AMS DR 登陸區域 (DR 目標)
- EC2 執行個體已啟用 EBS 快照 (AWS Backup)

快照複寫解決方案 :

- 跨可用區域 : 不適用 - 依設計 , EBS 快照在 區域中高度可用
- 跨區域 : AWS Backup

下圖代表 AMS 上 EBS 快照的 EC2 還原程序 :

AMS 上的 EC2 DR 步驟 :

1. 提出 RFC 以與目標帳戶共用 EBS 快照 (跨區域 DR 需要)。

變更類型 : 管理、進階堆疊元件、EBS 快照、共用

2. 在目的地子網路 (DR 站點子網路) 中建立預留位置 EC2 AMS 堆疊。建議使用 CFN 擷取來建立堆疊 , 因為客戶可以在相同的堆疊中結合指派安全群組和其他 (例如將執行個體新增至 ELB) 的步驟。

變更類型 : 部署、擷取、CloudFormation 範本的堆疊、建立

3. 引發 RFC 以執行 EC2 堆疊磁碟區還原。

變更類型 : 管理、進階堆疊元件、EC2 執行個體堆疊、還原磁碟區。

CT 會從步驟 1 中共用的快照還原磁碟區 , 並連接至步驟 2 中建立的預留位置執行個體。

磁碟區還原 CT 功能：

- 關閉預留位置執行個體
- 從快照還原磁碟區
- 交換磁碟區
- 啟動執行個體
- 保留舊網域
- 變更主機名稱
- 重新啟動。AMS 引導指令碼會在啟動時將執行個體加入目標 (DR) 網域

磁碟區還原 CT 輸入：

- InstanceId (預留位置執行個體 ID)
- RootDeviceSnapshotId, 還原根磁碟區的 EBS 快照
- KMSKeyId、KMS 金鑰識別符或 ARN, 用於加密 EC2 執行個體上所有還原的磁碟區
- DeviceNames, 最多 25 個 (選用)
- SnapshotIds, 最多 25 個 (選用)。要還原之磁碟區的快照清單

在 AMS 上使用彈性災難復原來保護 EC2 的災難

事前準備：

- AMS 產品登陸區域 (來源)
- AMS DR 登陸區域 (DR 目標)
- 您必須先為計劃使用的所有 初始化 Elastic Disaster Recovery AWS 區域 服務。

在 DR 登陸區域 (LZ) 中建立 IAM 角色，以存取 Elastic Disaster Recovery 主控台。

- 重要：SSM 文件會在 DRS 中建立為啟動後動作。此動作必須在 PostLaunch 設定的所有伺服器上啟用。
- 目的地 (預留位置) 執行個體必須具有標籤索引鍵："AWSDRS", 值："AllowLaunchingIntoThisInstance"。預留位置執行個體必須處於停止狀態。否則，AMS 無法在啟動設定下選取預留位置執行個體，且 Elastic Disaster Recovery 無法在預留位置執行個體上方還原。

如需 AMS 上 EC2 彈性災難復原設定和還原程序的圖表，請參閱 [AWS Elastic Disaster Recovery \(AWS DRS\) 一般架構](#)。

在 AMS 上使用彈性災難復原的 EC2 DR 步驟：

1. 在具有適當標籤的目的地子網路 (DR 站點子網路) 中建立預留位置 EC2 AMS 堆疊，如需詳細資訊，請參閱上一節。我們建議您使用 CFN 擷取來建立堆疊，因為您可以結合在相同堆疊中指派安全群組和標記執行個體、EBS 磁碟區和其他 (例如將執行個體新增至 ELB) 的步驟。

變更類型：部署、擷取、CloudFormation 範本的堆疊、建立

2. 停止預留位置執行個體。

變更類型：管理、進階堆疊元件、EC2 執行個體、停止

3. 如果未在步驟 1 中完成，請使用索引鍵標記預留位置執行個體及其 EBS 磁碟區："AWSDRS"，值："AllowLaunchingIntoThisInstance"。

變更類型：管理、進階堆疊元件、標籤、更新。

4. 在啟動至執行個體 ID、來源伺服器的 DRS 啟動設定下，使用步驟 1 的預留位置執行個體做為目標。從來源伺服器的 Elastic Disaster Recovery 主控台啟動執行個體復原演練。

Note

預留位置執行個體磁碟區會保留在帳戶中。若要刪除這些磁碟區，請在災難復原操作結束時提交管理 | 進階堆疊元件 | EBS 磁碟區 | 刪除變更類型 (ct-3e3h8u0sp5z80)。

彈性災難復原還原工作流程：

- 目標 (預留位置) 執行個體必須處於停止狀態
- 交換磁碟區並刪除來源 (預留位置) 根磁碟區
- 啟動執行個體
- 執行啟動後動作以完成下列項目：
 - 啟用 SSM 代理程式。
 - 交換磁碟區並刪除來源 (預留位置) 根磁碟區。
 - 啟動執行個體
 - 執行 PostLaunchScript SSM 文件。本文件執行下列動作：
 1. 離開舊網域。

2. 變更主機名稱。
3. 重新啟動。AMS 引導指令碼會在啟動期間將執行個體加入目標 (DR) 網域。

AMS 中的修補程式管理

主題

- [AMS Patch Orchestrator：標籤型修補模型](#)
- [使用修補程式協調器](#)
- [隨需修補](#)
- [AMS 標準修補](#)
- [修補服務承諾](#)

在 AMS 中，修補程式管理是一項服務，可協助您在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上維護作業系統廠商更新。您可以自由自訂修補 Amazon EC2 執行個體的頻率和程序。

您可以在加入期間設定修補程式管理，並使用 RFC 程序進行更新。使用變更管理系統和修補程式相容的範本建立的堆疊（適用於 Amazon EC2、Auto Scaling 群組、HA 單層或雙層堆疊）會自動訂閱修補程式管理。

AMS 提供功能 Patch Orchestrator – 標籤型修補，用於設定修補。

如需修補詞彙的定義，請參閱 [AMS 金鑰術語](#)。

Important

- 如果建立堆疊的 AMS 範本與修補程式管理相容，則堆疊或堆疊的組成執行個體無法選擇退出修補程式管理。目前，修補與下列堆疊範本相容：
 - Amazon EC2 堆疊 | 建立和 Amazon EC2 堆疊 | 建立（使用其他磁碟區）
 - 使用擷取啟動的 Amazon EC2 AWS CloudFormation 執行個體
 - Auto Scaling 群組 | 建立（已修補群組中的 Amazon EC2 執行個體）
 - 高可用性單層堆疊 | 建立和高可用性雙層堆疊 | 建立
- 如果發生影響堆疊的持續事件，AMS 運算子可以重新排程或取消排定的修補。
- 根據預設，特定修補程式相容堆疊中的所有執行個體都會就地修補。若要使用最新/修補的 AMS AMI，使用 Amazon Machine Image (AMI) 取代來修補 Auto Scaling 群組，請提交服務請求。更新 AMIs 會每月共用給帳戶。

Important

您可以為受管節點指定替代修補程式儲存庫。當 AMS 實作您請求的修補程式組態時，您需負責選取和驗證所選儲存庫的安全性。您也必須接受使用這些儲存庫的任何風險，例如供應鏈風險。

以下是修補程式管理程序安全的最佳實務：

- 僅使用受信任且經過驗證的儲存庫來源
- 盡可能預設為標準作業系統廠商儲存庫
- 定期稽核自訂儲存庫組態

Tip

AMS 建議您為具有寶貴應用程式或服務的執行個體啟用備份。如需啟用備份的詳細資訊，請參閱 [AMS Advanced 中的持續性管理](#)。

AMS Patch Orchestrator：標籤型修補模型

如果您已加入新的 AMS Patch Orchestrator 標籤型修補模型，您可以使用標籤將修補程式組態套用至一組精確的資源，稱為修補程式群組，範圍從一個執行個體到所有執行個體。如需 AMS 標籤的相關資訊，請參閱[使用標籤](#)。下節提供設定 Patch Orchestrator 標籤的說明。

修補程式會在您使用 [SSM 修補程式視窗 | 建立定義的修補程式時段](#) 期間安裝。每個修補程式時段都是 AWS Systems Manager 維護時段，會依照您選擇的排程執行、有設定的持續時間，並套用至一個修補程式群組。不屬於明確修補程式時段的執行個體會在您加入 Patch Orchestrator 時所定義的預設維護時段進行修補。

Important

如果多個修補程式維護時段排定同時執行，則在任何指定時間必須處理少於 1001 個執行個體。這是 AWS Systems Manager 限制。AMS 建議每 50 個執行個體至少一個小時。

根據預設，所有作業系統 (OS) 供應商提供的修補程式都會在維護時段或隨需修補程式期間安裝。這稱為預設修補程式基準。如果您想要限制要安裝哪些修補程式，您可以使用其中一個修補程式基準建立

CTs (每個OSes) 來定義自訂修補程式基準，請參閱[修補子類別](#)。例如，您可以使用自訂修補程式基準，以便僅為一或多個修補程式群組安裝關鍵和重要的安全更新。

在執行個體上安裝修補程式後，執行個體會重新啟動。修補程式通知會在修補前後傳送，並在排程開始之前 96 小時內傳送額外的提醒。此外，AMS 會在選取的維護時段將更新套用至基礎設施管理工具（例如 AWS SSM 代理程式）。

Important

AMS 正在取代遺失修補程式之執行個體的每月修補程式合規報告，且不會傳送每月報告。有鑑於最近發佈的自助式操作報告，每 24 小時重新整理一次，並可供您隨需使用，並提供最新且精細的資料。若要進一步了解報告，請參閱自助式報告。若要進一步了解報告，請參閱 [自助式報告](#)。

如需通知的詳細資訊，請參閱 [修補程式通知](#)。

使用修補程式協調器

透過提交包含下列詳細資訊的服務請求，為您的帳戶啟用 AMS Patch Orchestrator：

- 類別：其他
- 主旨：加入修補程式協調器
- CC 電子郵件：此加入 RFC 狀態變更時，CC 電子郵件地址會收到通知
- 詳細資訊：將以下資訊貼到電子郵件中並提供您的值。請注意，ThirdTagKey 是選用的。如需建議和範例，請參閱下表。

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
Second Tag Key:
Third Tag Key:
```

下表說明所提供值的格式和建議。

修補程式協調器標籤型修補組態

參數的名稱	資訊	建議或範例
預設維護時段排程	預設維護時段的排程，以 Cron 或 Rate 表達式的形式顯示。例如： • <code>cron(0 3 ? * 6L *)</code>：每個月最後一個星期五上午 03：00 • <code>rate(7 days)</code>：每七天 如需建立 Cron 表達式以及 Cron 和 Rate 表達式資源連結的詳細資訊，請參閱維護時段的 Cron 和 Rate 表達式。	建議每個月至少在一致的工作日執行一次時段。
預設維護時段排程時區	預設維護時段執行的時區是以網際網路指派號碼授權機構 (IANA) 格式為基礎。	例如： • America/Los_Angeles • 等/UTC
預設維護時段持續時間	預設維護時段的持續時間，以小時為單位。	每 50 個執行個體至少 1 小時，加上截止 2 小時。
預設維護時段截止	預設維護時段結束前未啟動新修補命令的時數。此間隔存在，以便有足夠的時間在視窗結束之前完成修補。	至少 2 小時。
預設修補程式備份保留天數 (選用)	在修補執行個體之前，保留建立 EBS 還原點的預設時間，以天為單位。	我們建議保留預設值，即 60。
預設維護時段通知電子郵件	一到五個電子郵件地址或分發清單，用於接收預設維護時段修補狀態的通知。	建議使用群組分發清單，而非個別電子郵件。

參數的名稱	資訊	建議或範例
第一個標籤索引鍵	用來建立修補程式群組標籤值的第一個標籤索引鍵。	例如 AppId。如果您已使用修補程式群組標籤定義自己的修補程式群組，請指定 null。
第二個標籤索引鍵	用來建立修補程式群組標籤值的第二個標籤鍵。	例如，環境。如果您已使用修補程式群組標籤定義自己的修補程式群組，請指定 null。
第三個標籤金鑰（選用）	用於建立修補程式群組標籤值的選用第三個標籤索引鍵。	例如，群組。

在您加入新的 Patch Orchestrator 修補服務模型之後，帳戶中所有適當標記的執行個體都屬於具有修補程式群組標籤的修補程式群組。Patch Orchestrator 會使用您現有的修補程式群組標籤，或由您在 Patch Orchestrator 加入期間指定的兩個或三個串連標籤值組成的 AMS 建立標籤。例如，{*Tag Value 1*}-{*Tag Value 2*}-{*Tag Value 3*}。AMS 每 12 小時更新這些 AMS 套用的修補程式群組標籤。如有需要，您可以使用[標籤 | 更新（需要檢閱）](#)或[標籤 | 更新（需要檢閱）](#)變更類型來更新修補程式群組標籤值。

例如，如果您的 Amazon EC2 執行個體具有下列標籤索引鍵：值對：

- AppId:MyApplication
- Environment:Production
- Group:1

在加入期間，您指定了下列標籤索引鍵：

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS 會建立下列修補程式群組標籤，並將其套用至您的執行個體：Patch Group:MyApplication-Production-1。

 Note

如果執行個體的作業系統不受支援，或在維護時段內停止，則不會建立修補程式失敗提醒。

Patch Orchestrator 先決條件

Patch Orchestrator 工作流程以最新版 System Manager Automation Document : AWSManagedServices-PatchInstanceFromMaintenanceWindow 修補的 Amazon EC2 執行個體為目標。

在文件工作流程中，執行命令文件「AWS-RunPatchBaseline」會針對修補程式群組成員中的每個 Amazon EC2 執行個體執行。若要進一步了解，請參閱[關於 SSM 文件 AWS-RunPatchBaseline](#)。

使用要求：

- 從 AMS 提供的 Amazon Machine Image (AMI) 或是透過「遷移合作夥伴遷移執行個體的堆疊」CT (ct-257p9zjk14ija) 在 AMI 上部署的 Amazon EC2 執行個體。
- 輸出網際網路連線已啟用。對於防火牆/代理解決方案，要求允許 Windows 更新端點和/或 Linux 儲存庫鏡像端點、AWS 系統管理員代理設定和中繼資料代理組態。如需詳細資訊，請參閱[設定 SSM 代理程式以使用代理](#)和[使用 HTTP 代理](#)
- IAM 角色符合 IAM 角色 SSM customer-mc-ec2-instance-profile 服務的最低允許存取。
- 我們建議使用 10 GB 的可用根分割區空間。對於 Linux 作業系統，/var 分割區中至少有 2 GB 可用。
- 用於更新下載的有效憑證授權單位。
- Windows Server Update Services (WSUS) - 登錄檔，包括但不限於：
DisableWindowsUpdateAccess、NoWindowsUpdate；自動更新不得影響 Windows Update 程序的操作。

驗證：

- 對於使用 yum package Manager 的 Linux 作業系統執行個體，您可以透過執行來驗證更新的可用性
#yum check-update
- 對於 Linux OS RedHat 5.7 和更新版本、6.1 和更新版本，以及 7.0 和更新版本；Amazon EC2 執行個體透過「從遷移合作夥伴遷移執行個體的堆疊」CT (ct-257p9zjk14ija) 遷移到您的 AMS 帳戶，您需要驗證訂閱管理員狀態以獲得更新效能。

- 在 Windows 作業系統上，啟用 Windows Server Update Services (WSUS)。本機政策不應封鎖 WSUS 掃描或安裝更新的能力。以管理員身分登入後，您就可以從 Windows Update Service 主控台執行可用更新的掃描來驗證它。Windows Server 作業系統版本，包括 2012R2、2016 和 2019，都有預設的 Windows Update 設定可供下載和安裝。您可以在掃描之前設定所需的設定。在後續版本的作業系統上，此操作可以觸發安裝；事先設定所需的行為。
- 透過提交服務請求，向 AMS 操作團隊請求驗證：「AWSManagedServices-CheckPatchingPrerequisites 自動化文件，針對 Amazon EC2 執行個體執行，以評估修補程式準備程度。」

Note

如果執行個體的作業系統不受支援，或在維護時段內停止，則不會建立修補程式失敗提醒。

修補程式視窗

特定修補程式群組中的執行個體會在一或多個修補程式時段期間進行修補。修補程式時段會根據定義為 Cron 或 Rate 表達式的排程執行，並且具有可設定的持續時間，旨在將修補程式相關的中斷保持在所選時間間隔內。AMS 建議建立多個修補時段，以整體涵蓋所有執行個體，以符合組織的特定修補常式，並使用預設的維護時段做為備用。使用 RFC 變更類型部署 | 修補 | SSM 修補視窗 | 建立 (ct-0el2j07llrxs7) 建立修補程式視窗。所有不屬於修補程式時段的執行個體都會在加入期間建立的預設維護時段期間修補。

一般而言，修補程式時段不需要更新，即可包含新的執行個體。這通常是透過修改執行個體標籤來完成。例如，請考慮下列一系列事件：

1. 兩個執行個體會加上 AppId:MyApplication、Environment:Production、的標籤 Group:1。

這會在這些執行個體上產生標籤，假設建立 MyApplication-Production-1 修補程式群組的第一個標籤金鑰 = AppId、第二個標籤金鑰 = 環境、第三個標籤金鑰 = 群組和修補程式時段。

2. 再建立三個執行個體，並使用 AppId:MyApplication、Environment:Production、進行標記 Group:1。

這會產生修補程式群組：MyApplication-Production-1 的標籤。

不需要變更修補程式時段，因為它會在下一次排程執行時挑選所有五個執行個體。

如需使用此變更類型的更詳細討論和逐步解說，請參閱 [SSM 修補程式視窗 | 建立](#)。

修補程式通知

Important

從 2025 年 2 月 1 日開始，AMS 客戶將不再收到其受管帳戶中空修補程式維護 Windows 的通知。

訂閱的電子郵件地址（最多五個）會在修補程式維護時段開始之前收到類似以下內容的電子郵件：

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
  2020-02-21T12:02:18.196Z.
Details:
  Maintenance Window AccountId:  YOUR_ACCOUNT_ID
  Maintenance Window Region:     YOUR_ACCOUNT_REGION
  Maintenance Window Id:         THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:       THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  InstanceId      InstanceName      StackId
  -----
  THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME

A follow-up message with a detailed report is sent as soon as the maintenance window is
over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by
following this URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
  
```

在修補程式活動結束時，訂閱的電子郵件地址會收到類似以下的電子郵件：

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
  2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:    YOUR_ACCOUNT_REGION
  Maintenance Window Id:        THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  RfcId                InstanceId      InstanceName      StackId
  Status
  -----
  THE_RFC_ID          THE_INSTANCE_ID    THE_INSTANCE_NAME THE_STACK_NAME
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following
this URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR\_ACCOUNT\_REGION

Please raise an Incident if an issue is impacting one of your production applications
by following this URL:
https://console.aws.amazon.com/managedservices/incident/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

```

AMS 修補系統每 96 小時會識別該 96 小時內所有即將發生的修補程式受管維護時段，並傳送提醒通知給該 96 小時時段內的所有訂閱電子郵件地址。這可能是在窗口之前的一小時，或完整的 96 小時。例如：

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME will start at:
  2020-05-06T16:35:36.523Z.

```

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
 Maintenance Window Region: *YOUR_ACCOUNT_REGION*
 Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
 Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
 Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
 Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
 Maintenance Window Schedule: rate(24 hours)
 Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
 Amazon Managed Services
 Patch Team

修補基準

根據預設，所有作業系統 (OS) 供應商提供的修補程式都是使用 AMS 預設修補程式基準進行安裝。如果您想要限制已安裝的修補程式，您可以選擇使用 RFC 變更類型部署 | 修補 | SSM 修補程式基準 | 建立#### (CT ID 因作業系統而異) 來建立修補程式基準。

如需使用這些變更類型的詳細資訊，請參閱[修補子類別](#)。

Patch Orchestrator 預留標籤

Patch Orchestrator 也會產生下列無法修改的標籤：

- **AMSPatchGroup** – 此標籤用於產生修補程式群組標籤值。您不應修改 AMSPatchGroup。如果您想要使用自訂的「修補程式群組」值，您可以修改「修補程式群組」標籤。Patch Orchestrator 會根據加入期間提供的標籤索引鍵繼續產生 AMSPatchGroup 的值，但如果標籤值已設定為自訂值，則不會修改 "Patch Group" 標籤值。若要停止使用自訂的「修補程式群組」值，您可以設定「修補程式群組」的值以符合 AMSPatchGroup 標籤值。
- **AMSDefaultPatchGroup** – 此標籤指出執行個體是預設維護時段的一部分，其值為 True 或 False。如果執行個體的修補程式群組未指派給維護時段，則此值會設為 True。

隨需修補

AMS 具有可與修補程式基準搭配使用的變更類型，可讓您隨需執行修補程式。這可以是您在加入時設定的預設基準，也可以是您使用修補程式基準變更類型設定的修補程式 Orchestrator Systems Manager 修補程式基準 (CT ID 因作業系統而異)。

您可以使用隨需修補變更類型搭配或不搭配 Patch Orchestrator。

如需使用此變更類型的詳細資訊，請參閱[隨需修補 | 執行](#)。

Note

您無法在隨需修補變更類型中使用屬於 Auto Scaling 群組的執行個體。

AMS 標準修補

AMS 支援使用 AMS 標準修補模型的現有客戶，但此模型不適用於新客戶，並且正在淘汰以有利於 AMS Patch Orchestrator。

AMS 標準修補的一般修補程式內容包括支援作業系統的廠商更新，以及預先安裝支援作業系統的軟體（例如 IIS 和 Apache Server）。

在 AMS 加入期間，您可以指定修補需求、政策、頻率和偏好的修補時段。這些組態意味著您可以避免讓應用程式一次完全離線以進行基礎設施修補，因此您可以控制何時修補哪些基礎設施。

Note

本主題中所述的修補程序僅適用於您的堆疊。AMS 基礎設施會在個別程序期間修補。AWS Managed Services 維護時段（或維護時段）會執行 AWS Managed Services (AMS) 的維護活動，並在每個月的第二個星期四太平洋時間下午 3 點至下午 4 點重複執行。AMS 可能會變更維護時段，但需提前 48 小時通知。您可以在加入時設定 AMS 修補程式時段，或者核准或拒絕每月修補程式服務通知。

AMS 會定期掃描受管 Amazon EC2 執行個體，以透過作業系統更新功能取得更新。我們也定期更新環境中支援的 AMS 基礎 Amazon Machine Image AMIs)。

驗證後，AMS AMI 版本會與所有 AMS 帳戶共用。您可以使用 [DescribeImages](#) Amazon EC2 API 呼叫或使用 Amazon EC2 主控台來檢視可用的 AWS AMI 版本。若要尋找可用的 AMS AMIs，請參閱 [尋找 AMI IDs、AMS](#)。

AMS 只會在您要求時執行隨機操作修補排程。先前 AMS 會傳送通知；目前不會傳送通知。

Note

根據預設，AMS 會使用 Systems Manager 來套用修補程式，方法是讓套件管理員 (Linux) 或系統更新服務 (Windows) 查詢其預設儲存庫，以查看可用的新套件。如果在 day-to-day 操作過程中，您已使用預設套件管理員在 Linux 主機上安裝套件，該套件管理員也會在軟體可用時為該軟體挑選新套件。在這種情況下，您可能想要採取修補動作（本節說明）來選擇退出該執行個體。

支援的作業系統

支援的作業系統 (x86-64)

- Amazon Linux 2023

- Amazon Linux 2 (預期的 AMS 支援結束日期為 2026 年 6 月 30 日)
- Oracle Linux 9.x、8.x
- Red Hat Enterprise Linux (RHEL) 9.x、8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 及更新版本
- Microsoft Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

支援的作業系統 (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (預期的 AMS 支援結束日期為 2026 年 6 月 30 日)

支援的修補程式

AWS Managed Services 主要支援作業系統層級的修補。安裝的修補程式可能因作業系統而有所不同。

Important

所有更新都會從執行個體上設定的 Systems Manager 修補程式基準服務遠端儲存庫下載，並在本主題稍後說明。執行個體必須能夠連線到儲存庫，才能執行修補。
若要針對交付您要自行維護之套件的儲存庫選擇退出修補程式基準服務，請執行下列命令來停用儲存庫：

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

使用下列命令擷取目前設定的儲存庫清單：

```
yum repolist
```

- Amazon Linux 預先設定的儲存庫（通常是四個）：

儲存庫 ID	儲存庫名稱
amzn-main/latest	amzn-main-Base
amzn-updates/latest	amzn-updates-Base
epel/x86_64	Enterprise Linux 6 - x86_64 的額外套件
pbis	PBIS 套件更新

- Red Hat Enterprise Linux 預先設定的儲存庫（五個用於 Red Hat Enterprise Linux 7，五個用於 Red Hat Enterprise Linux 6）：

儲存庫 ID	儲存庫名稱
rhui-REGION-client-config-server-7/x86_64	Red Hat Update Infrastructure 2.0 用戶端組態伺服器
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux 伺服器 7
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux Server 7 RH Common(RPMs
epel/x86_64	適用於 Enterprise Linux 7 的額外套件 - x86_64
pbis	PBIS 套件更新

儲存庫 ID	儲存庫名稱
rhui-REGION-client-config-server-6	Red Hat 更新基礎設施 2.0
rhui-REGION-rhel-server-releases	Red Hat Enterprise Linux Server 6 (RPMs)
rhui-REGION-rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Common (RPMs)

儲存庫 ID	儲存庫名稱
Epel	Enterprise Linux 6 - x86_64 的額外套件
pbis	PBIS 套件更新

- CentOS 7 預先設定的儲存庫（通常五個）：

儲存庫 ID	儲存庫名稱
base/7/x86_64	CentOS-7 - 基礎
更新/7/x86_64	CentOS-7 - 更新
extras/7/x86_64	CentOS-7 - 額外項目
epel/x86_64	適用於 Enterprise Linux 7 的額外套件 - x86_64
pbis	PBIS 套件更新

- 對於 Microsoft Windows Server，所有更新都是使用 Windows Update Agent 進行偵測和安裝，其設定為使用 Windows Update 目錄（不包括 Microsoft Update 的更新）。

在 Microsoft Windows 作業系統上，修補程式管理員會使用 Microsoft 的 cab 檔案 wsusscn2.cab 作為可用作業系統安全性更新的來源。此檔案包含有關 Microsoft 發佈之安全相關更新的資訊。修補程式管理員會定期從 Microsoft 下載此檔案，並使用它來更新適用於 Windows 執行個體的修補程式集。此檔案僅包含 Microsoft 識別為與安全性相關的更新。修補程式管理員在處理檔案中的資訊時，也會移除已被較新的更新所取代的更新。因此，只有最新的更新會顯示出來並提供安裝。例如，如果 KB4012214 取代 KB3135456，則修補程式管理員中只會提供 KB4012214 做為更新。

若要進一步了解 wsusscn2.cab 檔案，請參閱 Microsoft 文章[使用 WUA 離線掃描更新](#)。

修補和基礎設施設計

AMS 根據您的基礎設施設計採用不同的修補方法：可變或不可變（如需詳細定義，請參閱[AMS 金鑰術語](#)）。

使用可變基礎設施時，修補作業會使用傳統就地方法，分別由 AMS 操作工程師安裝更新至 Amazon EC2 執行個體。此修補方法用於非 Auto Scaling 群組的堆疊，並包含單一 Amazon EC2 執行個體或數

個執行個體。在此案例中，取代執行個體或堆疊所依據的 AMI 會銷毀自第一次部署以來對該系統所做的所有變更，因此不會這麼做。更新會套用至執行中的系統，您可能會因為應用程式或系統重新啟動而發生系統停機（取決於堆疊組態）。這可以透過藍/綠更新策略來緩解。如需詳細資訊，請參閱[AWS CodeDeploy 介紹藍/綠部署](#)。

使用不可變的基礎設施時，修補方法是 AMI 取代。不可變執行個體會使用更新的 AMI 統一更新，以取代 Auto Scaling 群組組態中指定的 AMI。AMS 版本每月更新（即修補）AMI，通常是修補程式週二的一週。下一節說明運作方式。

AMS 標準修補的運作方式

AMS 使用 Systems Manager Run Command 服務定期排程每月和視需要的關鍵修補，具有兩種主要修補方法，即就地修補和替換 AMI，取決於您的基礎設施部署策略（可變與不可變）。本節說明 AMS 修補服務、類型、方法和程序。

AMS 定義兩種修補程式類型，以不同方式排程：

- 關鍵修補：在接受通知後，會盡快套用更新。
- 標準修補：定期更新並每月套用作業系統廠商。

透過就地修補或 AMI 替換（應請求）套用修補程式。

更新掃描

AMS 使用 [Amazon EC2 Run Command Service](#) 來聯絡您的 Amazon EC2 堆疊，並部署必要的掃描和修補指令碼。AMS 使用已安裝在支援的作業系統上的原生套件管理元件，在 Amazon EC2 堆疊上執行所有必要的掃描和修補行為。對於 Red Hat 和 Amazon Linux，服務使用 yum。對於 Windows，服務使用 Windows Update Agent。

每天使用 [SSM 維護時段](#) 和 AMS 預設 AWS-RunPatchBaseline 文件執行掃描。每個可連線的 Amazon EC2 堆疊都會使用 Linux 和 Windows 的更新儲存庫進行掃描。AMS 修補程序會偵測所有可連線的 Amazon EC2 堆疊，然後在批次程序中執行掃描，讓堆疊始終保持良好狀態，即使執行掃描時發生故障。接著會為每個 Amazon EC2 堆疊儲存掃描結果。

若要檢視堆疊或執行個體的掃描結果，請使用堆疊 ID 或執行個體 ID 提交服務請求。

預設 AMS 修補程序是安裝所有可用的修補程式，無論修補程式分類或嚴重性為何（例如，關鍵與標準）。例外狀況是您已明確排除堆疊的修補程式（不應排除 AMS 定義為強制性的修補程式）。

您會在建議的維護時段前 14 天收到修補服務通知。這可讓您有時間測試提議的修補程式，並接受或拒絕它們。如果您未回覆修補服務通知，則不會修補您的執行個體。當安裝修補程式時，AMS 會為每個堆疊建立變更請求 (RFC)，且該 RFC 會出現在您帳戶的 RFC 清單中。

AMS 設定的維護時段和通知

透過 AMS 設定的修補，每個帳戶都有每月維護時段，您可以在加入帳戶時定義此時段。AWS Managed Services 維護時段（或維護時段）會執行 AWS Managed Services (AMS) 的維護活動，並在每個月的第二個星期四太平洋時間下午 3 點至下午 4 點重複執行。AMS 可能會變更維護時段，但需提前 48 小時通知。

修補時段不同。修補傳出服務請求（也稱為服務通知）包含建議的修補時段。

Note

如需有關回覆修補服務通知的資訊，請參閱 [您可以在 AMS 標準修補中採取的動作](#)。

修補服務通知會透過電子郵件傳送至您帳戶存檔的聯絡電子郵件地址。通知包含 AWS Support 主控台的連結，您可以在其中回應它。您也可以使用 AMS 服務請求頁面來回應通知。服務通知包括：

- 套用到堆疊的更新 IDs (CSUs、IUs 和 OUs) 清單，以及您請求的更新不會修補（如果有的話）。
- 將受影響的執行個體 IDs。
- 套用更新的提議修補時段。您可以請求不同的修補時段。
- 您接受提議修補的請求，或要求其他資訊。AMS 可讓您有時間測試更新的影響，並核准或拒絕修補，或要求排除特定更新。如果您需要更多時間進行測試，並希望在測試後套用更新，請回應服務通知並描述您想要的內容，或根據先前 RFC 的詳細資訊提交新修補程式 RFC 的服務請求。如果您完全不回覆服務通知，則不會採取修補動作並取消 RFC。

如果您核准服務通知，AMS 會根據服務承諾，在同意的修補程式時段內執行修補程式 RFC 並套用更新。

修補完成後，AMS 會在服務請求中傳送通訊給您，其中包含修補活動的結果摘要（即成功或失敗）。

就地修補

就地修補是指 AMS 登入每個堆疊執行個體並套用修補程式的方法。

使用執行支援作業系統的 Amazon EC2 執行個體，在可變基礎設施上進行就地修補。修補會套用截至目前為止所有可用的非排除更新。發行關鍵修補程式時，會有一個額外的關鍵修補程序。

標準修補：就地

標準修補發生在修補程式服務通知中建議的約定修補程式排程上，並包含不視為關鍵的定期修補程式更新。

在建議的修補時段之前，以及您對通知的肯定回應，會建立修補程式 RFC，並顯示在 RFC 儀表板中。

關鍵修補：就地

當作業系統廠商發佈重大安全性更新時，AMS 會根據 AMS 服務承諾，傳送每個堆疊的服務通知（傳送至您帳戶的聯絡電子郵件），通知您修補程式 RFC。每次更新時，服務通知都會包含下列項目：

- 更新發行日期
- 更新重要性
- 更新詳細資訊 (KB 參考等)
- 受影響的堆疊 IDs

您可以測試通知中列出的更新，並透過回覆服務通知來核准或拒絕修補程式。如果您核准通知，則需要提供每個堆疊的特定修補程式時段來安裝更新。

Note

回應服務通知後 24 小時內的修補程式時段可能會根據可用容量重新排程。

如果您未在 10 天內回覆，或是拒絕建議的修補，則修補會取消。

如果您想要在允許的期間（在通知中提供）之後套用更新，請根據先前通知的詳細資訊提交新修補程式排程的服務請求。

如果您核准服務通知，AMS 會根據服務承諾，在您的指定修補程式時段內套用更新。

在多次更新的情況下，您可以透過指定要在對服務通知的回應中排除的更新，從修補中排除特定更新。

AMS 會針對每個堆疊傳送每次更新結果的服務通知（即成功或失敗）。

AMI 更新修補 (使用 Auto Scaling 群組 AMIs)

AMI 取代修補會在不可變的基礎設施上完成，方法是更新設定為在 Auto Scaling 群組中部署新 Amazon EC2 執行個體的 AMI ID。

Amazon Machine Image AMIs) 會針對支援的作業系統定期發行。作業系統廠商會定期發行新的修補程式。AMS 採用 Amazon 提供的 AMI、使用最新的修補程式進行更新，然後新增適當的元件，使其能夠在 AMS 環境中操作。然後，它透過將 AMI 共用到帳戶，讓所有 AMS 客戶都可以使用新的 AMS AMI。您可以使用這些新發行的 AMS AMIs，每月重新整理 Auto Scaling 群組堆疊。下圖說明 AMIs。

Auto Scaling 群組會根據為 Auto Scaling 群組設定的 AMI 建立其執行個體。當 AMS 共用更新的 AMIs 時，根據管理 AMI 更新的方式，您有下列選項：

- 如果您使用應用程式部署工具（例如 UserData、CodeDeploy 等），在執行個體建立後自動自訂執行個體，您可以執行下列動作：
 - 回覆修補服務通知，或提交服務請求，讓最新的 AMS AMI 取代您目前的 Auto Scaling 群組組態 AMI。取代 Auto Scaling 群組組態中的 AMI ID 後，AMS 會啟動執行個體的滾動更新，而 Auto Scaling 群組執行個體組態（例如安裝應用程式、開機指令碼等）會自動套用至使用新 AMS AMI 建立的新執行個體。
- 如果您在 Auto Scaling 群組的組態中使用自訂/黃金 AMI，您可以：
 - 使用新的 AMS AMI 建立執行個體、自訂執行個體並建立新的黃金 AMI。使用 Amazon EC2 主控台與 AMS 共用新的黃金 AMI，並向 AMS 提交服務請求，以更新 Auto Scaling 群組的組態，以使用新的自訂 AMI。
 - 使用 Amazon EC2 主控台與 AMS 共用您現有的黃金 AMI，並提交 AMS 的服務請求以更新您的黃金 AMI。為此，AMS 會從黃金 AMI 建立執行個體、將修補程式套用至該執行個體、為您建立新的黃金 AMI，然後更新 Auto Scaling 群組的組態以使用新的 AMI。此處的缺點是 AMS 無法測試您的新自訂 AMI 是否以您想要的方式運作。反之，您應該測試使用新 AMI 建立的執行個體，並在建立新的黃金 AMI、共用它，並請求 AMS 更新您的 Auto Scaling 群組之前，驗證一切是否正常運作。AMS 不建議此選項。

標準修補：AMI 更新

AMS 每月都會發行新的 Amazon Machine Image AMIs)，其中包含服務改進和適用於 AMIs 的新修補程式。

Note

從更新的 AWS AMIs 修補星期二之後，會產生新的 AMS AMIs。然後，AMS 會在提供它們之前對其進行測試。新的 AMIs 通過測試後，AMS 會將更新的 AMIs 分享給受管帳戶。

關鍵修補：AMI 更新

如有需要，AMS 會提供 AMIs 更新，其中包含自上次每月 AMI 發行以來發行的關鍵安全修補程式。

不可變基礎設施的關鍵安全更新程序與不可變基礎設施的每月 AMI 程序相同，但新的 AMS AMI 是在正常排程（修補程式週二）之外建立的，以發行新的關鍵更新為基礎。AMS 會根據您帳戶定義的服務水準協議 (SLAs)，提供具有關鍵安全修補程式的新 AMI。僅依請求更新 Auto Scaling 群組的 AMS 更新。使用服務請求來提交 AMI 替換請求。

AMS 標準修補失敗

如果更新失敗，AMS 會執行分析以了解失敗原因，並向您傳達分析結果。如果失敗可歸因於 AMS，則在維護時段內，我們會重試更新。否則，AMS 會為失敗的執行個體更新建立服務通知，並等待您的指示。

對於可歸因於您系統的故障，您可以提交具有新修補程式 RFC 的服務請求來更新執行個體。

您可以在 AMS 標準修補中採取的動作

除了測試新的 AMIs 之外，您還可以採取數種動作來管理基礎設施的修補：

- 如果測試更新的時間超過允許的修補程式時段，您可以提交服務請求（使用原始服務通知中的詳細資訊作為基礎），請求 AMS 套用當您準備好時取消的更新。
- 您可以提交服務請求，視需要提供更新清單、適用的執行個體和其他詳細資訊，以請求在下一個自動更新時段之前套用重要的更新 (IU) 或其他更新 (OU)。由於此 CT 並非自動化，因此排程和執行需要更長的時間。檢查服務層級目標 SLOs) 是否有適當的時間。如需詳細資訊，請參閱 [AMS 服務水準目標 SLOs](#)。

此外，您可以使用現有的修補 AMS AMIs 來建立自訂 AMIs。如需詳細資訊，請參閱 [AMI | Create](#)。

Note

您無法在下一個維護時段之前根據重要更新或其他更新來請求新的 AMS AMI，因為 AMS AMI 發行程序會遵循一致的節奏，以造福所有 AMS 客戶。

變更修補/選擇退出的項目

使用 AMS 設定的修補，在修補服務通知的回應中或服務請求中，您可以變更要修補的資源。您可以執行下列作業：

- 定義應該從修復、每個堆疊和每個作業系統中排除的修補程式清單。
- 定義應從特定修補程式或所有修補中排除的資源清單。
- 定義應一律從所有修補中排除的資源清單。
- 定義應該在特定日期和特定時間修補的資源清單（如果您尚未定義維護時段，則為佳）。

若要排除一或多個修補程式，請提交服務請求，或使用接下來提供的範本回應修補服務通知。請勿提交 RFC。在請求中包含您想要排除的修補程式名稱和原因。在服務請求中包含此資訊，如下所示：

- 名稱：修補程式的名稱。對於 Windows 修補程式，這是 KB 名稱，例如 KB3145384。對於 Linux 修補程式，這是套件名稱，例如 openssh-6.6.1p1-25.61.amzn1.x86_64。
- 原因：指出為什麼要排除修補程式的註解。
- 過期時間：排除過期的日期/時間。

如果已安裝排除的修補程式，則會將其移除。

如果排除這些修補程式會造成重大的安全風險，則運算子會檢閱請求，並與您進行討論。也會交涉已排除修補程式的過期日期。在同意的過期日期之後，排除會過期，並在任何後續修補上安裝修補程式。

如果適用，排除清單上的修補程式仍會在掃描結果中傳回。

Note

與 Windows 不同，Linux 修補程式是版本特定的。此區別很重要，因為未自動排除已排除修補程式的新版本。如果這是您想要執行的動作，您有責任通知 AMS 排除 Linux 修補程式的新版本。

修補程式服務通知回覆範本

您必須使用指定的格式回覆修補服務通知，才能在執行個體上執行修補。如果您尚未使用 AMS 設定維護時段，則應執行此操作。

當您回覆服務通知時，請使用指定的格式。

如果未設定維護時段，請告訴我們何時修補內容，如下所示：

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

如果您有設定的維護時段，並希望從特定修補程式中排除特定資源，請使用下列格式：

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

如果您有設定的維護時段，且希望一律排除特定資源，請使用下列格式：

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

準備修補

若要準備您的環境進行自動修補，建議您執行下列動作：

- 請確定您擁有所有要修補之執行個體的完整庫存。
- 確保在業務持續性策略中定期備份您的資源。額外的備份會建立為修補程式序列的一部分，並根據設定的修補程式協調器保留政策自動刪除這些備份（預設為 60 天）。
- 確保所有相關的授權都是最新的。
- 修改堆疊維護時段以交錯修補，以便在生產堆疊之前修補測試堆疊。如此一來，任何修補的錯誤都會在測試堆疊中找到，而且可以在修補生產堆疊之前識別。

檢視修補程式設定

若要了解您目前的修補組態，您可以執行下列動作：

- 使用查詢向 AMS 提交服務請求。
- 等待修補程式服務通知。修補通知會建議您要套用的所有修補程式和要修補的執行個體，並建議修補程式時段。

您可以提交服務請求來修改下列項目：

- 掃描間隔：在此堆疊執行個體上執行的合規掃描之間的時間，以分鐘為單位。
預設為 240(4 小時)。
- NotificationWindow：應該提前多久（以分鐘為單位）傳送排定的變更（修補）通知給您。
預設為 10080(7 天)。

AMS 標準修補FAQs

本節提供一些常見問題的答案。

- 問：如何選擇退出全域修補？

答：若要全域選擇退出修補，請提交服務請求。請注意，您無法選擇退出 AMS 強制修補程式。所有堆疊都會繼續掃描，以便我們報告漏洞。

- 問：如何排除特定堆疊的修補？

答：若要永久排除特定堆疊進行修補，請提交服務請求。若要從特定修補程式週期中排除特定堆疊，請使用要排除的堆疊清單來回應即將發生的修補通知。如需相關資訊，請參閱[變更修補/選擇退出的項目](#)。請注意，您無法選擇退出強制性修補程式。

- 問：如果我未核准修補服務通知，會發生什麼情況？

答：您有 14 天的時間核准標準修補服務請求，還有 10 天的時間核准關鍵修補通知。如果您未在期間內核准服務請求，服務承諾就會失效，而且不會發生修補。在強制修補的情況下，無論對服務請求的回應為何，都會套用修補程式。

- 問：如何排除特定修補程式和套件的安裝？

答：若要永久排除特定修補程式或套件，請提交服務請求。若要從特定修補程式週期中排除特定修補程式或套件，請使用要排除的修補程式或套件清單來回應即將到來的修補通知。如需詳細資訊，請參閱[變更修補/選擇退出的項目](#)。請注意，您無法選擇退出強制性修補程式。

- 問：如果系統因修補而失敗，會發生什麼情況？

答：AMS 會監控每個系統。AMS 會傳送每個堆疊和執行個體每次更新（即成功或失敗）結果的服務通知給您。如果偵測到故障，AMS 會調查、運作以還原執行個體，然後 AMS 操作工程師會嘗試手動修補。如需相關資訊，請參閱[AMS 標準修補失敗](#)。

- 問：哪些更新由 AMS 管理？

答：AMS 會管理 AMS 收到廠商通知的作業系統層級更新。如需詳細資訊，請參閱[支援的修補程式](#)。

- 問：哪些更新不是由 AMS 管理？

答：AMS 不會管理應用程式層級更新。

- 問：如何更新 Auto Scaling 群組？

答：Auto Scaling 群組會以 Auto Scaling 群組組態中的 AMI 取代更新，並執行滾動更新。滾動更新會觀察修補組態的 HealthyHostThreshold 設定，這會決定在修補期間必須保持作用中的堆疊中的 Amazon EC2 執行個體數量。如需詳細資訊，請參閱[AMI 更新修補（使用 Auto Scaling 群組 AMIs）](#)。

- 問：如何取得在正常週期外安裝的更新？

答：針對您想要在正常修補排程之外安裝的作業系統層級更新，請使用您收到的修補通知來提交服務請求。如果您測試建議的修補程式需要超過 21 天（標準修補程式）或 14 天（關鍵修補程式），則可能會發生這種情況。Out-of-band修補可在獨立 Amazon EC2 執行個體就地完成。

• 問：如何修補新部署的堆疊或執行個體？

答：建立新的 Amazon EC2 堆疊執行個體或 Auto Scaling 群組時，您應該一律指定最新的 AMS AMI，其中已有最新的修補程式。對於可變基礎設施，應在部署堆疊後立即執行內嵌修補。

修補服務承諾

根據您的基礎設施部署類型和更新的關鍵性，我們為可變和不可變基礎設施的關鍵安全更新，以及可變和不可變基礎設施的重要更新提供服務承諾。

標準修補

這些是標準修補的 AMS 服務承諾。

標準修補、可變基礎設施（就地修補）

事件/動作	服務承諾衡量
重要更新會在一個月內發佈。	時鐘啟動
從標準修補程式通知建立的十四天後，AMS 會透過服務通知和每個堆疊的電子郵件，通知您即將規劃的修補。服務通知包括： - 適用於 堆疊IDs (CSUs 和 IUs) 清單（需要和未套用），以及這些更新排除在修補之外 - 受影響的堆疊 IDs - 套用更新的維護時段	傳送服務通知後，時鐘會停止。
您會測試更新的影響，並核准或拒絕 RFC。如果您未在 14 天內回覆，或是在對服務通知的回應中拒絕修補，則不會採取任何動作。	如果您未在 14 天內核准或回覆，則會取消待定的變更，且更新的服務承諾不適用。

事件/動作	服務承諾衡量
如果您測試的時間超過 14 天，並且希望在 14 天期間之後套用更新，請根據先前 RFC 的詳細資訊提交新修補程式 RFC 的服務請求。	
如果您在 14 天內核准服務通知，AMS 會套用更新。 您可以選擇在對服務通知的回應中指定要排除的更新，以從 RFC 排除特定更新。	如果您在接收後 14 天內核准服務通知，時鐘就會開始。嘗試更新安裝後，時鐘會停止。
AMS 會傳送每次嘗試更新結果的服務通知給您。服務通知包含下列詳細資訊： - Amazon EC2 執行個體 ID - 更新 1 成功/失敗：ARN a1、ARN a2... - 更新 2 成功/失敗：ARN b1、ARN b2... - 更新 N 成功/失敗：ARN c1、ARN c2...	不適用。
如果更新失敗，AMS 會執行分析以了解失敗原因，並向您傳達分析結果。如果失敗可歸因於 AMS，則 AMS 會在維護時段內重試更新，否則 AMS 會為失敗的執行個體更新組合建立服務通知，並等待您在維護時段上的指示。	不適用。
對於可歸因於您的失敗，請提交新修補程式 RFC 的服務請求，以更新執行個體。	不適用。

關鍵修補

這些是關鍵安全性更新的 AMS 服務承諾。

關鍵安全性更新、可變基礎設施

事件/動作	服務承諾衡量
CSU 已發行。	時鐘啟動

事件/動作	服務承諾衡量
AMS 透過每個堆疊的服務通知（也會傳送電子郵件）通知您修補程式 RFC。服務通知包括： - 更新發行日期 - 更新重要性 - 更新詳細資訊：KB 參考，以此類推 - 受影響的堆疊 IDs	傳送服務通知後，時鐘會停止。
您可以測試 RFC 中列出的更新，並透過回覆服務通知在 10 天內核准或拒絕 RFC。 您可以提供特定的維護時段（每個堆疊）來安裝更新。在回覆服務通知的 24 小時內指定的維護時段可能會根據可用容量重新排程。 如果您未在 10 天內回覆，或者如果您拒絕修補程式 RFC，則會取消待定動作。 如果您想要在 14 天期間之後套用更新，請根據先前 RFC 的詳細資訊，提交新修補程式 RFC 的服務請求。	如果您未在 14 天內核准或回覆，則會取消待定的變更，且更新的服務承諾不適用。
如果您核准服務通知，AMS 會套用更新。 對於多個更新，您可以選擇指定要在對服務通知的回應中排除的更新，以從變更中排除特定更新。	如果所需的維護時段不在服務承諾時段內，則只有在 RFC 未在所需的維護時段內執行時，才會遺漏更新的服務承諾。
AMS 會傳送每個已套用更新結果的服務通知給您。服務通知包含下列詳細資訊： - Amazon EC2 執行個體 ID - 更新成功：ARN a1、ARN a2... - 更新失敗：ARN c1、ARN c2...	不適用。

事件/動作	服務承諾衡量
如果更新失敗，AMS 會執行分析以了解失敗原因，並向您傳達分析結果。如果故障可歸因於 AMS，則 AMS 會在維護時段內重試更新，否則 AMS 會為失敗的執行個體更新組合建立服務通知，並在新的維護時段等待您的指示。	不適用。
對於可歸因於您的失敗，請提交新修補程式 RFC 的服務請求，以更新執行個體。	不適用。

重大安全性更新、不可變的基礎設施

事件/動作	服務承諾衡量
CSU 已發行。	時鐘啟動
AMS 透過服務通知通知您下列事項： - 更新發行日期 - 更新重要性 - 更新詳細資訊 (KB 參考等) - 受影響的 AMS Amazon Machine Image (AMI) - 新更新 AMIs 的預期發佈日期和時間	時鐘會繼續執行。
AMS 會在受管帳戶中發行更新的 AMIs。	時鐘停止。
如果您核准服務通知，AMS 會套用更新。 AMS 會透過服務通知和電子郵件，通知您帳戶中共用 AMIs。	不適用。
如果測試新的 AMIs 所花費的時間超過配置的時間（一週），您可以向 AMS 提交服務請求，以使用新的 AMS AMI（原樣）更新 Auto Scaling 群組。如果您想要使用組態修改新的 AMS AMI，請使用 RFC 搭配 管理 其他 其他	不適用。

事件/動作	服務承諾衡量
更新 CT (ct-0xdawir96cy7k) 來請求我們更新您的 Auto Scaling 群組。	

報告和選項

AWS Managed Services (AMS) 會整理各種原生 AWS 服務的資料，以提供主要 AMS 產品的增值報告。

AMS 提供兩種類型的詳細報告：

- **請求報告：**您可以透過 Cloud Service Delivery Manager (CSDM) 臨時請求特定報告。這些報告沒有限制，因為您可能需要在加入或關鍵事件期間多次請求這些報告。不過，請注意，這些報告並非設計為按照每週報告等排程提供。若要進一步了解您的需求或使用自助式報告的詳細資訊，請聯絡您的 CSDM。
- **自助式報告：**AMS 自助式報告可讓您視需要隨時直接查詢和分析資料。使用自助式報告從 AMS 主控台存取報告，並透過 S3 儲存貯體（每個帳戶一個儲存貯體）報告資料集。這可讓您將資料整合到您偏好的商業智慧 (BI) 工具，以便根據您的需求自訂報告。

主題

- [隨需報告](#)
- [自助式報告](#)

隨需報告

主題

- [AMS 修補程式報告](#)
- [AMS 備份報告](#)
- [防止和監控熱門發言者報告的事件](#)
- [帳單費用詳細資訊報告](#)
- [信任的修復程式報告](#)

AMS 會整理來自各種原生 AWS 服務的資料，以提供主要 AMS 產品的附加價值報告。如需這些報告的副本，請向 Cloud Service Delivery Manager (CSDM) 提出請求。

AMS 修補程式報告

可用的報告

- [修補程式執行個體詳細資訊摘要報告](#)
- [修補程式詳細資訊報告](#)
- [遺漏修補程式報告的執行個體](#)
- [修補 SSM 涵蓋範圍報告](#)

修補程式執行個體詳細資訊摘要報告

修補程式執行個體詳細資訊摘要報告提供為已加入報告之執行個體收集的執行個體詳細資訊。這是資訊報告，可協助識別所有已加入的執行個體、帳戶狀態、執行個體詳細資訊、維護時段涵蓋範圍、維護時段執行時間、堆疊詳細資訊和平台類型。此報告提供下列項目：

1. 帳戶生產和非生產執行個體的資料。注意：生產和非生產階段衍生自帳戶名稱，而非執行個體標籤。
2. 依平台類型分佈執行個體的資料。注意：「N/A」平台類型是指無法擷取平台資訊的時間 AWS Systems Manager。
3. 執行個體狀態的分佈資料，以及執行、停止或終止的執行個體數量。

欄位名稱	定義
報告日期時間	產生報告的日期和時間。
帳戶 ID	執行個體 ID 所屬的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶名稱
生產帳戶	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。範例：PROD、NONPROD、無法使用
帳戶狀態	AMS 帳戶狀態。例如：ACTIVE、INTACTIVE
AMS 帳戶服務承諾	PREMIUM、PLUS
登陸區域	帳戶登陸區域類型的旗標。例如：MALZ、NON-MALZ
存取限制	限制存取的區域。例如：US SOIL

欄位名稱	定義
執行個體 ID	EC2 執行個體的 ID
執行個體名稱	EC2 執行個體的名稱
執行個體平台類型	作業系統 (OS) 類型。例如：Windows、Linux 等
執行個體平台名稱	作業系統 (OS) 名稱。例如：MicrosoftWindowsServer2012R2Standard、RedHatEnterpriseLinuxServer
堆疊名稱	包含執行個體的堆疊名稱
堆疊類型	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）。範例：AMS、CUSTOMER
Auto Scaling 群組名稱	包含執行個體的 Auto Scaling 群組 (ASG) 名稱
執行個體修補程式群組	用來將執行個體分組並套用相同維護時段的修補程式群組名稱。如果修補程式群組未指派，則值將為 "Unassigned"
執行個體修補程式群組類型	修補程式群組類型。 DEFAULT：具有預設維護時段的預設修補程式群組，由執行個體上的AMSDefaultPatchGroup:True 標籤決定。 CUSTOMER：客戶建立的修補程式群組。 NOT_ASSIGNED：未指派修補程式群組
執行個體狀態	EC2 執行個體生命週期內的狀態。範例：TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING。 如需詳細資訊，請參閱執行個體生命週期。

欄位名稱	定義
維護時段涵蓋範圍	如果此執行個體有未來的維護時段。範例： COVERED 或 NOT_COVERED
維護時段執行日期時間	下次預期執行維護時段時。如果為 NULL，則執行單一視窗，即非重複

修補程式詳細資訊報告

AWS Managed Services (AMS) 修補程式詳細資訊報告提供各種執行個體的修補程式詳細資訊和維護時段涵蓋範圍，包括：

1. 修補程式群組及其類型上的資料。
2. 維護時段、持續時間、截止日期、維護時段執行的未來日期（排程）和在每個時段中受影響的執行個體上的資料。
3. 帳戶下所有作業系統的資料，以及已安裝作業系統的執行個體數量。

欄位名稱	定義
報告日期時間	產生報告的日期和時間。
帳戶 ID	執行個體 ID 所屬的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶名稱
執行個體 ID	EC2 執行個體的 ID
生產帳戶	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。如果資料不可用，則值將為「不可用」
帳戶狀態	AMS 帳戶狀態。例如：ACTIVE、INTACTIVE
執行個體平台類型	作業系統 (OS) 類型。例如：Windows、Linux

欄位名稱	定義
執行個體平台名稱	作業系統 (OS) 名稱。例如：MicrosoftWindowsServer2012R2Standard、RedHatEnterpriseLinuxServer
堆疊類型	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）。例如：AMS、CUSTOMER
執行個體修補程式群組	用來將執行個體分組並套用相同維護時段的修補程式群組名稱。如果修補程式群組未指派，則值將為 "Unassigned"
執行個體修補程式群組類型	修補程式群組類型。 DEFAULT：具有預設維護時段的預設修補程式群組，由執行個體上的AMSDefaultPatchGroup:True 標籤決定 CUSTOMER：客戶建立的修補程式群組 UNASSIGNED：未指派修補程式群組
執行個體狀態	EC2 執行個體生命週期內的狀態。例如：TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING 如需詳細資訊，請參閱執行個體生命週期。
維護時段 ID	維護時段識別符
維護時段狀態	可能的值為 ENABLED 或 DISABLED。
維護時段類型	維護時段類型
維護時段下次執行日期時間	下次預期執行維護時段時。如果為 NULL，則執行單一視窗，即非重複
上次執行維護時段	執行維護時段的最新時間

欄位名稱	定義
維護時段持續時間 (小時)	維護時段的持續時間，以小時為單位
維護時段涵蓋範圍	維護時段涵蓋範圍
修補程式基準 ID	目前連接至執行個體的修補程式基準
修補程式狀態	整體修補程式合規狀態。例如：COMPLIANT、NON_COMPLIANT。如果至少有一個缺少的修補程式，執行個體會被視為不合規，否則會合規。
合規 - 總計	合規修補程式的計數 (所有嚴重性)
不合規 - 總計	不合規修補程式的計數 (所有嚴重性)
合規 - 關鍵	嚴重性為「關鍵」的合規修補程式計數
合規 - 高	嚴重性為「高」的合規修補程式計數
合規 - 中	嚴重性為 "medium" 的合規修補程式計數
合規 - 低	嚴重性為「低」的合規修補程式計數
合規 - 資訊性	具有「資訊」嚴重性的合規修補程式計數
合規 - 未指定	嚴重性為「未指定」的合規修補程式計數
不合規 - 關鍵	嚴重性為「關鍵」的不合規修補程式計數
不合規 - 高	嚴重性為「高」的不合規修補程式計數
不合規 - 中	嚴重性為 "medium" 的不合規修補程式計數
不合規 - 低	嚴重性為「低」的不合規修補程式計數
不合規 - 資訊性	具有「資訊」嚴重性的不合規修補程式計數
不合規 - 未指定	嚴重性為「未指定」的不合規修補程式計數

遺漏修補程式報告的執行個體

遺漏修補程式的 AWS Managed Services (AMS) 執行個體報告提供上次維護時段執行期間遺漏修補程式之執行個體的詳細資訊，包括：

1. 修補程式 ID 層級缺少修補程式的資料。
2. 至少有一個修補程式遺失的所有執行個體上的資料，以及修補程式嚴重性、未修補的天數、範圍和發行日期等屬性。

欄位名稱	定義
報告日期時間	產生報告的日期和時間。
帳戶 ID	執行個體 ID 所屬的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶名稱
生產帳戶	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。
帳戶狀態	AMS 帳戶狀態。例如：ACTIVE 或 INACTIVE
AMS 帳戶服務方案	PREMIUM 或 PLUS
執行個體 ID	EC2 執行個體的 ID
執行個體平台類型	作業系統 (OS) 類型。例如：Windows
執行個體狀態	EC2 執行個體生命週期的狀態。例如：TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING 如需詳細資訊，請參閱 執行個體生命週期 。
修補程式 ID	已發行修補程式的 ID。例如：KB3172729
修補程式嚴重性	每個發佈者的修補程式嚴重性。例如：CRITICAL、IMPORTANT、MODERATE、LOW、UNSPECIFIED

欄位名稱	定義
修補程式分類	每個發佈者的修補程式分類。例如：CRITICALUPDATES、SECURITYUPDATES、UPDATEROLLUPS、UPDATES、FEATUREPACKS
修補程式發行日期時間 (UTC)	每個發佈者的修補程式發行日期
修補程式安裝狀態	在每個 SSM 執行個體上安裝修補程式的狀態。例如：INSTALLED、MISSING、NOT applicable
未修補的天數	自上次 SSM 掃描以來執行個體未修補的天數
未修補範圍的天數	未修補天數的儲存貯體。例如：<30 天、30-60 天、60-90 天、90 天以上

修補 SSM 涵蓋範圍報告

AMS 修補 SSM 涵蓋範圍報告會通知您帳戶中的 EC2 執行個體是否已安裝 SSM 代理程式。

欄位名稱	定義
客戶名稱	有多個子客戶之情況的客戶名稱
資源區域	AWS 資源所在的區域
帳戶名稱	帳戶的名稱
AWS 帳戶 ID	AWS 帳戶的 ID
資源 ID	EC2 執行個體的 ID
資源名稱	EC2 執行個體的名稱
合規旗標	指出資源是否已安裝 SSM Agent (「合規」) (「NON_COMPLIANT」)

AMS 備份報告

可用的報告

- [備份任務成功/失敗報告](#)
- [備份摘要報告](#)
- [備份摘要/涵蓋報告](#)

備份任務成功/失敗報告

備份任務成功/失敗報告提供有關過去幾週內執行的備份的資訊。若要自訂報告，請指定您要擷取資料的週數。預設週數為 12。下表列出報告中包含的資料：

欄位名稱	定義
AWS 帳戶 ID	資源所屬的 AWS 帳戶 ID
帳戶名稱	AWS 帳戶名稱
備份任務 ID	Backup 任務的 ID
資源 ID	備份資源的 ID
資源類型	正在備份的資源類型
資源區域	備份資源 AWS 的區域
備份狀態	備份的狀態。如需詳細資訊，請參閱 備份任務狀態
復原點 ID	復原點的唯一識別符
狀態訊息	描述備份任務期間發生的錯誤或警告
備份大小	備份的大小，以 GB 為單位
復原點 ARN	已建立備份的 ARN
復原點存留期，以天為單位	自建立復原點以來經過的天數

欄位名稱	定義
不到 30 天	少於 30 天的備份指標

備份摘要報告

欄位名稱	定義
客戶名稱	多個子客戶的情況的客戶名稱
備份月份	備份的月份
備份年份	備份年份
資源類型	正在備份的資源類型
資源數量	已備份的資源數量
復原點的數量	不同快照的數量
少於 30 天的備份	少於 30 天的備份計數
最大復原點存留期	以天為單位的最舊復原點存留期
最小復原點存留期	最近的復原點存留期，以天為單位

備份摘要/涵蓋報告

備份摘要/涵蓋報告列出有多少資源目前不受任何 AWS Backup 計劃保護。與您的 CDSM 討論適當的計畫，以盡可能提高涵蓋範圍，並降低資料遺失的風險。

欄位名稱	定義
客戶名稱	多個子客戶的情況的客戶名稱
Region	AWS 資源所在的區域
帳戶名稱	帳戶的名稱

欄位名稱	定義
AWS 帳戶 ID	AWS 帳戶的 ID
資源類型	資源的類型。資源受 AWS Backup (Aurora、DocumentDB、DynamoDB、EBS、EC2、EFS、FSx、RDS 和 S3) 支援
資源 ARN	資源的 ARN
資源 ID	資源的 ID
涵蓋範圍	指出資源是否涵蓋 (「COVERED」或「NOT_COVERED」)
資源數量	帳戶中支援的資源數量
perc_coverage	過去 30 天內執行備份的支援資源百分比。

防止和監控熱門發言者報告的事件

可用的報告

- [已防止的事件報告](#)
- [監控熱門發言者報告](#)

已防止的事件報告

Incidents Prevented 報告會列出自動修復的 Amazon CloudWatch 警示，以防止可能發生的事件。若要進一步了解，請參閱[自動修復](#)。下表列出此報告中包含的資訊：

欄位名稱	定義
execution_start_time_utc	執行自動化的日期
customer_name	帳戶客戶名稱
account_name	帳戶的名稱

欄位名稱	定義
AwsAccountId	AWS 帳戶的 ID
document_name	執行的 SSM 文件或自動化名稱
duration_in_minutes	自動化的長度，以分鐘為單位
Region	AWS 資源所在的區域
automation_execution_id	執行的 ID
automation_execution_status	執行的狀態

監控熱門發言者報告

監控熱門發言者報告會顯示在特定期間內產生的 Amazon CloudWatch 警示數量，並提供產生最高數量警示的資源視覺化。此報告可協助您識別產生最高數量提醒的資源。這些資源可能是執行根本原因分析以修復問題或修改警示閾值的候選者，以防止沒有實際問題時不必要的觸發。下表列出此報告中包含的資訊：

欄位名稱	定義
客戶名稱	客戶名稱
AccountId	AWS 帳戶的 ID
警示類別	觸發的提醒類型
描述	提醒的描述
資源 ID	觸發提醒的資源 ID
資源名稱	觸發提醒的資源名稱
Region	AWS資源所在的區域
事件狀態	警示產生之事件的最新狀態
第一次出現	第一次觸發提醒

欄位名稱	定義
最近出現	觸發警示的最近時間
提醒計數	在第一次和最近出現之間產生的提醒數量

帳單費用詳細資訊報告

AWS Managed Services (AMS) 帳單費用詳細資訊報告提供連結帳戶和個別 AWS 服務的 AMS 帳單費用詳細資訊，包括：

- AMS 服務層級費用、提升百分比、帳戶層級 AMS 服務方案和 AMS 費用。
- 連結帳戶和 AWS 使用費

欄位名稱	定義
帳單月份	計費服務的月份和年份
付款人帳戶 ID	識別將負責支付 AMS 費用之帳戶的 12 位數 ID
連結的帳戶 ID	識別使用產生費用之服務的 AMS 帳戶的 12 位數 ID
AWS 服務名稱	已使用 AWS 的服務
AWS 費用	AWS 服務名稱中列出的 AWS 服務名稱 AWS 費用
定價計劃	與連結帳戶相關聯的定價計劃名稱
提升比例	根據 pricing_plan、SLA 和 AWS 服務的提升百分比（以小數 V.WXYZ 表示）
調整後 AWS 的費用	AWS 針對 AMS 調整的用量
調高的 AWS 費用	AMS ； $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$ 要收取的 AWS 費用百分比

欄位名稱	定義
執行個體 EC2 RDS 支出	EC2 和 RDS 執行個體上的支出
AMS 費用	產品的總 AMS 費用；uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
按比例分配的最低費用	我們為了符合合約下限而收取的金額
最低費用	AMS 最低費用（如適用）
連結的帳戶總 AMS 費用	linked_account 的所有費用總和
付款人帳戶 AMS 費用總計	付款人帳戶的所有費用總和

信任的修復程式報告

可用的報告

- [信任的修復程式修復摘要報告](#)
- [信任的修復程式組態摘要報告](#)
- [Trusted Advisor 檢查摘要報告](#)

信任的修復程式修復摘要報告

Trusted Remediator Remediation Status 報告提供先前修復週期中發生的修復的相關資訊。預設週數為 1。若要自訂報告，請根據您的修復排程指定週數。

欄位名稱	定義
日期	收集資料的日期。
帳戶 ID	資源所屬 AWS 的帳戶 ID
帳戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別

欄位名稱	定義
檢查名稱	修復的 Trusted Advisor 檢查名稱
檢查 ID	修復檢查的 ID Trusted Advisor
執行模式	針對特定 Trusted Advisor 檢查設定的執行模式
OpsItem ID	Trusted Advisor 為修復而建立的 OpsItem ID
OpsItem 狀態	報告 Trusted Advisor 時由 建立的 OpsItem 狀態
資源 ID	為修復而建立之資源的 ARN

信任的修復程式組態摘要報告

Trusted Remediator Configuration Summary 報告提供每個 Trusted Advisor 檢查目前 Trusted Remediator Remediation 組態的相關資訊。

欄位名稱	定義
日期	收集資料的日期。
帳戶 ID	套用組態 AWS 的帳戶 ID
帳戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別
檢查名稱	套用組態的修復 Trusted Advisor 檢查名稱
檢查 ID	套用組態的修復 Trusted Advisor 檢查 ID
執行模式	針對特定 Trusted Advisor 檢查設定的執行模式
覆寫至自動化	如果已設定標籤模式，將執行模式覆寫為自動化
覆寫為手動	如果已設定標籤模式，將執行模式覆寫為手動

Trusted Advisor 檢查摘要報告

Trusted Advisor 檢查摘要報告提供目前 Trusted Advisor 檢查的相關資訊。此報告會在每週修補排程之後收集資料。預設週數為 1。若要自訂報告，請根據您的修復週期指定週數。

欄位名稱	定義
日期	收集資料的日期。
帳戶 ID	套用組態 AWS 的帳戶 ID
客戶名稱	AWS 帳戶名稱
檢查類別	AWS Trusted Advisor 檢查類別
檢查名稱	套用組態的修復 Trusted Advisor 檢查名稱
檢查 ID	套用組態的修復 Trusted Advisor 檢查 ID
狀態	檢查的提醒狀態。可能的狀態為正常（綠色）、警告（黃色）、錯誤（紅色）或無法使用
資源已標記	由 Trusted Advisor 檢查標記（列出）AWS 的資源數量。
忽略的資源	由於 Trusted Advisor 您將其標記為已隱藏而忽略 AWS 的資源數量。
處於嚴重狀態的資源	處於嚴重狀態的資源數量
處於警告狀態的資源	處於警告狀態的資源數量

自助式報告

AWS Managed Services (AMS) 自助式報告 (SSR) 是一項功能，可從各種原生 AWS 服務收集資料，並提供主要 AMS 產品報告存取權。SSR 提供可用來支援操作、組態管理、資產管理、安全管理和合規的資訊。

使用 SSR 從 AMS 主控台存取報告，並透過 Amazon S3 儲存貯體（每個帳戶一個儲存貯體）報告資料集。您可以將資料插入您最愛的商業智慧 (BI) 工具，以根據您的獨特需求自訂報告。AMS 會在您的主要 AWS 區域中建立此 S3 儲存貯體 (S3 儲存貯體名稱：(ams-reporting-data-a<Account_ID>)，並從 us-east-1 區域中託管的 AMS 控制平面共用資料。

Important

若要存取此功能，您必須具有下列其中一個角色：

- 多帳戶登陸區域：AWSManagedServicesReadOnlyRole
- 單一帳戶登陸區域：Customer_ReadOnly_Role

Important

搭配使用自訂金鑰 AWS Glue

若要使用客戶受管 KMS 金鑰加密 AWS Glue 中繼資料，您必須執行下列額外步驟，以允許 AMS 從帳戶彙總資料：

1. 在 <https://console.aws.amazon.com/kms> 開啟 AWS Key Management Service 主控台，然後選擇客戶受管金鑰。
2. 選取您計劃用來加密 AWS Glue 中繼資料的金鑰 ID。
3. 選擇別名索引標籤，然後選擇建立別名。
4. 在文字方塊中，輸入 AmsReportingFlywheelCustomKey，然後選擇建立別名。

主題

- [內部 API 操作](#)
- [修補程式報告（每日）](#)
- [備份報告（每日）](#)
- [事件報告（每週）](#)
- [帳單報告（每月）](#)
- [彙總報告](#)
- [AMS 自助式報告儀表板](#)
- [資料保留政策](#)

- [從 SSR 離職](#)

內部 API 操作

如果您監控 API 操作，您可能會看到對下列僅限內部操作的呼叫：

- GetDashboardUrl
- ListReportsV2

內部 API 操作：GetDashboardUrl

當 AMS 主控台調用時，此操作會出現在系統日誌中。它沒有其他使用案例。它不適用於您的直接使用。

傳回對應報告的內嵌儀表板 URL。此操作接受 dashboardName 傳回的 ListReports。

請求語法

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

請求元素

dashboardName：請求 URL 的 QuickSight 儀表板名稱。儀表板名稱會在 ListReportsV2 中傳回。

類型：字串

回應語法

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。服務會傳回下列 JSON 格式的資料。

url：傳回所請求 的 QuickSight URLdashboardName。

類型：字串

錯誤

如需所有動作常見錯誤的相關資訊，請參閱[常見錯誤](#)。

BadRequestException:

提交的請求無效。例如，如果輸入不完整或不正確。如需詳細資訊，請參閱隨附的錯誤訊息。

HTTP 狀態碼：400

NotFoundException:

找不到請求的資源。請確定請求 URI 正確。

HTTP 狀態碼：404

TooManyRequestsException:

請求已達到其限流限制。在指定的時段後重試。

HTTP 狀態碼：429

UnauthorizedException:

請求遭拒，因為發起人沒有足夠的許可。

HTTP 狀態碼：401

內部 API 操作：ListReportsV2

當 AMS 主控台調用時，此 API 會出現在系統日誌中。它沒有其他使用案例。它不適用於您的直接使用。

傳回指定帳戶可用的操作報告清單。

請求語法

請求沒有請求內文。

回應語法

HTTP/1.1 200

```
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。服務會傳回下列 JSON 格式的資料。

reportsList：可用操作報告的清單。

類型：儀表板物件陣列

reportsType：指出是否跨多個帳戶彙總報告。

類型：字串

錯誤

如需所有動作常見錯誤的相關資訊，請參閱[常見錯誤](#)。

BadRequestException:

提交的請求無效。例如，輸入不完整或不正確。如需詳細資訊，請參閱隨附的錯誤訊息。

HTTP 狀態碼：400

NotFoundException:

找不到請求的資源。請確定請求 URI 正確。

HTTP 狀態碼：404

TooManyRequestsException:

請求已達到其限流限制。在指定的時段後重試。

HTTP 狀態碼：429

UnauthorizedException:

請求遭拒，因為發起人沒有足夠的許可。

HTTP 狀態碼：401

修補程式報告（每日）

可用的報告

-
- [修補程式詳細資訊](#)
- [遺漏修補程式的執行個體](#)

這是一個資訊報告，可協助識別所有加入 Patch Orchestrator (PO) 的執行個體、帳戶狀態、執行個體詳細資訊、維護時段涵蓋範圍、維護時段執行時間、堆疊詳細資訊和平台類型。

此資料集提供：

- 帳戶的生產和非生產執行個體上的資料。生產和非生產階段衍生自帳戶名稱，而非執行個體標籤。
- 依平台類型分佈執行個體的資料。當 AWS Systems Manager (SSM) 無法取得平台資訊時，就會發生「不適用」平台類型。
- 執行個體狀態分佈的資料、執行、停止或終止的執行個體數量。

主控台欄位名稱	資料集欄位名稱	定義
存取限制	access_restrictions	限制存取的區域
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱
帳戶狀態	account_status	AMS 帳戶狀態
	account_sla	AMS 帳戶服務承諾

主控台欄位名稱	資料集欄位名稱	定義
帳戶類型	malz_role	MALZ 角色
Auto Scaling 群組名稱	instance_asg_name	包含執行個體的 Auto Scaling 群組 (ASG) 名稱
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
執行個體修補程式群組	instance_patch_group	用來將執行個體分組並套用相同維護時段的修補程式群組名稱
執行個體修補程式群組類型	instance_patch_group_type	修補程式群組類型
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體平台名稱	instance_platform_name	作業系統 (OS) 名稱
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
登陸區域	malz_flag	MALZ 相關帳戶的旗標
維護時段涵蓋範圍	mw_covered_flag	如果執行個體至少有一個已啟用且具有未來執行日期的維護時段，則視為已涵蓋，否則未涵蓋
維護時段執行日期時間	earliest_window_execution_time	下次預期執行維護時段時
維護時段執行日期時間	earliest_window_execution_time	下次預期執行維護時段時

主控台欄位名稱	資料集欄位名稱	定義
生產帳戶	prod_account	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。
報告日期時間	dataset_datetime	產生報告的日期和時間。
堆疊名稱	instance_stack_name	包含執行個體的堆疊名稱
堆疊類型	instance_stack_type	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）

修補程式詳細資訊

此報告提供各種執行個體的修補程式詳細資訊和維護時段涵蓋範圍。

此報告提供：

- 修補程式群組及其類型上的資料。
- 維護時段、持續時間、截止日期、維護時段執行的未來日期（排程）和在每個時段中受影響的執行個體上的資料。
- 帳戶下所有作業系統的資料，以及安裝作業系統的執行個體數量。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
帳戶名稱	account_name	AWS 帳戶名稱
帳戶狀態	account_status	AMS 帳戶狀態

欄位名稱	資料集欄位名稱	定義
合規 - 關鍵	compliance_critical	嚴重性為「關鍵」的合規修補程式計數
合規 - 高	compliance_high	嚴重性為「高」的合規修補程式計數
合規 - 中	compliant_medium	嚴重性為 "medium" 的合規修補程式計數
合規 - 低	compliance_low	嚴重性為「低」的合規修補程式計數
合規 - 資訊性	compliant_informational	具有「資訊」嚴重性的合規修補程式計數
合規 - 未指定	compliant_unspecified	嚴重性為「未指定」的合規修補程式計數
合規 - 總計	compliant_total	合規修補程式計數（所有嚴重性）
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
	account_sla	AMS 帳戶服務方案
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體平台名稱	instance_platform_name	作業系統 (OS) 名稱

欄位名稱	資料集欄位名稱	定義
執行個體修補程式群組類型	instance_patch_group_type	DEFAULT：具有預設維護時段的預設修補程式群組，由執行個體上的 AMSDefaultPatchGroup : True 標籤決定 CUSTOMER：客戶建立的修補程式群組 NOT_ASSIGNED：未指派修補程式群組
執行個體修補程式群組	instance_patch_group	用來將執行個體分組並套用相同維護時段的修補程式群組名稱
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
上次執行維護時段	last_execution_window	執行維護時段的最新時間
維護時段 ID	window_id	維護時段 ID
維護時段狀態	window_state	維護時段狀態
維護時段類型	window_type	維護時段類型
維護時段下次執行日期時間	window_next execution_time	下次預期執行維護時段時
維護時段持續時間（小時）	window_duration	維護時段的持續時間，以小時為單位

欄位名稱	資料集欄位名稱	定義
維護時段涵蓋範圍	mw_covered_flag	如果執行個體至少有一個已啟用且具有未來執行日期的維護時段，則視為已涵蓋，否則未涵蓋
不合規 - 關鍵	noncompliant_critical	嚴重性為「關鍵」的不合規修補程式計數
不合規 - 高	noncompliant_high	嚴重性為「高」的不合規修補程式計數
不合規 - 中	noncompliant_medium	嚴重性為 "medium" 的不合規修補程式計數
不合規 - 低	noncompliant_low	嚴重性為「低」的不合規修補程式計數
不合規 - 資訊性	不合規 _資訊	具有「資訊」嚴重性的不合規修補程式計數
不合規 - 未指定	不合規 _未指定	嚴重性為「未指定」的不合規修補程式計數
不合規 - 總計	noncompliant_total	不合規修補程式的計數（所有嚴重性）
修補程式基準 ID	patch_baseline_id	目前連接至執行個體的修補程式基準
修補程式狀態	patch_status	整體修補程式合規狀態。如果至少有一個缺少的修補程式，則執行個體會被視為不合規，否則為合規。

欄位名稱	資料集欄位名稱	定義
生產帳戶	prod_account	AMS prod、非prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD'、'NONPROD'。
堆疊類型	instance_stack_type	AMS 堆疊（客戶帳戶中的 AMS 基礎設施）或客戶堆疊（支援客戶應用程式的 AMS 受管基礎設施）
	window_next_exec_yyyy	window_next_execution_time 的年份部分
	window_next_exec_mm	window_next_execution_time 的月份部分
	window_next_exec_D	window_next_execution_time 的天數部分
	window_next_exec_HHMM	Hour : Minute 部分 window_next_execution_time

遺漏修補程式的執行個體

此報告提供上次維護時段執行期間遺漏修補程式之執行個體的詳細資訊。

此報告提供：

- 修補程式 ID 層級缺少修補程式的資料。
- 至少有一個遺失修補程式和屬性的所有執行個體上的資料，例如修補程式嚴重性、未修補的天數、範圍和修補程式的發行日期。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間

欄位名稱	資料集欄位名稱	定義
帳戶 ID	aws_account_id	AWS 執行個體 ID 所屬的帳戶 ID
帳戶名稱	account_name	AWS 帳戶名稱
客戶名稱父系	customer_name_parent	
客戶名稱	customer_name	
生產帳戶	prod_account	AMS prod 或非 prod 帳戶的識別符，取決於帳戶名稱是否包含值 'PROD' 或 'NONPROD'。
帳戶狀態	account_status	AMS 帳戶狀態
帳戶類型	account_type	
	account_sla	AMS 帳戶服務方案
執行個體 ID	instance_id	EC2 執行個體的 ID
執行個體名稱	instance_name	EC2 執行個體的名稱
執行個體平台類型	instance_platform_type	作業系統 (OS) 類型
執行個體狀態	instance_state	EC2 執行個體生命週期內的狀態
執行個體標籤	ec2_tags	與 Amazon EC2 執行個體 ID 相關聯的標籤
修補程式 ID	patch_id	已發行修補程式的 ID
修補程式嚴重性	patch_sev	每個發佈者的修補程式嚴重性
修補程式分類	patch_class	每個修補程式發佈者的修補程式分類

欄位名稱	資料集欄位名稱	定義
修補程式發行日期時間 (UTC)	release_dt_utc	每個發佈者的修補程式發行日期
修補程式安裝狀態	install_state	每個 SSM 在執行個體上安裝修補程式的狀態
未修補的天數	days_unpatched	自上次 SSM 掃描以來執行個體未修補的天數
未修補範圍的天數	days_unpatched_bucket	未修補天數的儲存貯體

備份報告（每日）

備份報告涵蓋主要和次要（如適用）區域。它涵蓋備份（成功/失敗）的狀態，以及所拍攝快照上的資料。

此報告提供：

- 備份狀態
- 拍攝的快照數量
- 復原點
- 備份計畫和保存庫資訊

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	執行個體 ID 所屬的 AWS 帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱

欄位名稱	資料集欄位名稱	定義
帳戶 SLA	account_sla	AMS 帳戶服務承諾
	malz_flag	MALZ 相關帳戶的旗標
	malz_role	MALZ 角色
	access_restrictions	限制存取的區域
備份快照排程的開始日期時間	start_by_dt_utc	快照排程開始的時間戳記
備份快照實際開始日期時間	create_dt_utc	快照實際開始時的時間戳記
備份快照完成日期時間	completion_dt_utc	快照完成時的時間戳記
備份快照過期日期時間	expiration_dt_utc	快照過期時的時間戳記
備份任務狀態	backup_job_status	快照的狀態
備份類型	backup_type	備份類型
備份任務 ID	backup_job_id	備份任務的唯一識別符
位元組中的備份大小	backup_size_in_bytes	以位元組為單位的備份大小
備份計畫 ARN	backup_plan_arn	備份計畫 ARN
備份計畫 ID	backup_plan_id	備份計畫唯一識別符
備份計畫名稱	backup_plan_name	備份計畫名稱
備份計畫版本	backup_plan_version	備份計畫版本
備份規則 ID	backup_rule_id	備份規則 ID
備份保存庫 ARN	backup_vault_arn	備份保存庫 ARN
備份文件庫名稱	backup_vault_name	備份保存庫名稱
IAM 角色 ARN	iam_role_arn	IAM 角色 ARN

欄位名稱	資料集欄位名稱	定義
執行個體 ID	instance_id	唯一執行個體 ID
執行個體狀態	instance_state	執行個體狀態
執行個體標籤	ec2_tags	與 EC2 執行個體 ID 相關聯的標籤
資源 ARN	resource_arn	Amazon 資源名稱
資源 ID	resource_id	唯一資源識別符
資源區域	resource_region	資源的主要（和次要，如適用）區域。
資源類型	resource_type	資源的類型
復原點 ARN	recovery_point_arn	復原點的 ARN
復原點 ID	recovery_point_id	復原點的唯一識別符
復原點狀態	recovery_point_status	復原點狀態
在 天後刪除復原點	recovery_point_delete_after_days	天之後的復原點刪除
復原點會在 天後移至冷儲存	recovery_point_move_to_cold_storage_after_days	將備份快照移至冷儲存的完成日期後天數
復原點加密狀態	recovery_point_is_encrypted	復原點加密狀態
復原點加密金鑰 ARN	recovery_point_encryption_key_arn	復原點加密金鑰 ARN
堆疊 ID	stack_id	Cloudformation 堆疊唯一識別符
堆疊名稱	stack_name	堆疊名稱

欄位名稱	資料集欄位名稱	定義
標籤：AMS 預設修補程式群組	tag_ams_default_patch_group	標籤值：AMS 預設修補程式群組
標籤：應用程式 ID	tag_app_id	標籤值：應用程式 ID
標籤：應用程式名稱	tag_app_name	標籤值：應用程式名稱
標籤：備份	tag_backup	標籤值：備份
標籤：合規架構	tag_compliance_framework	標籤值：合規架構
標籤：成本中心	tag_cost_center	標籤值：成本中心
標籤：客戶	tag_customer	標籤值：客戶
標籤：資料分類	tag_data_classification	標籤值：資料分類
標籤：環境類型	tag_environment_type	標籤值：環境類型
標籤：營運時數	tag_hours_of_operation	標籤值：操作時數
標籤：擁有者團隊	tag_owner_team	標籤值：擁有者團隊
標籤：擁有者團隊電子郵件	tag_owner_team_email	標籤值：擁有者團隊電子郵件
標籤：修補程式群組	tag_patch_group	標籤值：修補程式群組
標籤：支援優先順序	tag_support_priority	標籤值：支援優先順序
磁碟區狀態	volume_state	磁碟區狀態

事件報告（每週）

此報告提供事件的彙總清單及其優先順序、嚴重性和最新狀態，包括：

- 分類為受管帳戶事件之支援案例資料
- 視覺化受管帳戶的事件指標所需的事件資訊
- 每個事件的事件類別和修復狀態資料

視覺化和資料都可以用於每週事件報告。

- 您可以透過 帳戶中的 AMS 主控台，透過報告頁面存取視覺化。
- 具有下列結構描述的資料集，可透過 受管帳戶中的 S3 儲存貯體存取。
- 使用提供的日期欄位，根據事件建立或解決的月、季、週和/或日來篩選事件。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間。
帳戶 ID	aws_account_id	AWS 事件所屬的帳戶 ID。
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
帳戶名稱	account_name	AWS 帳戶名稱。
案例 ID	case_id	事件的 ID。
建立月份	created_month	事件建立的月份。
優先順序	priority	事件的優先順序。
嚴重性	severity	事件的嚴重性。
狀態	status	事件的狀態。
類別	yuma_category	事件的類別。
建立日期	create_day	事件以 YYYY-MM-DD 格式建立的日期。
建立的週	created_wk	事件以 YYYY-WW 格式建立的一週。週日至週六視為一週的開始和結束。週是從 01 到 52。第 01 週一律是包含一年第一天的一週。例如，2023-12-31 和 2024-01-01 位於 2024 年 1 週。

欄位名稱	資料集欄位名稱	定義
建立的季度	created_qtr	事件以 YYYY-Q 格式建立的季度。01/01 至 03/31 定義為 Q1，以此類推。
已解決日期	resolved_day	事件以 YYYY-MM-DD 格式解決的日期。
已解決的週	resolved_wk	事件以 YYYY-WW 格式解決的一週。週日至週六視為一週的開始和結束。週是從 01 到 52。第 01 週一律是包含一年第一天的一週。對於 exmaple，2023-12-31 和 2024-01-01 位於 2024 年 1 週。
解析月份	resolved_month	事件以 YYYY-MM 格式解決的月份。
已解決的季度	resolved_qtr	事件以 YYYY-Q 格式解決的季度。01/01 至 03/31 定義為 Q1，以此類推。
建立的分組規則	grouping_rule	套用至事件的分組規則。"no_grouping" 或 "instance_grouping"。
執行個體 IDs	instance_ids	與事件相關聯的執行個體。
提醒數量	number_of_alerts	與該事件相關聯的提醒數量。如果您已啟用分組，則此數字可以大於 1。如果您沒有啟用分組，則一律為 1。
建立時間	created_at	建立事件時的時間戳記。

欄位名稱	資料集欄位名稱	定義
警示 ARNs	alarm_arns	與您的事件相關聯之警示的 Amazon Resource Name ("arn")。
相關警示	related_alarms	與事件關聯之所有警示的人類可讀取名稱。

帳單報告（每月）

帳單費用詳細資訊

此報告提供連結帳戶和個別 AWS 服務之 AMS 帳單費用的詳細資訊。

此報告提供：

- AMS 服務層級費用、提升百分比、帳戶層級 AMS 服務方案和 AMS 費用的資料。
- 連結帳戶和 AWS 使用費的資料。

Important

每月帳單報告僅適用於您的管理付款人帳戶 (MPA) 或您定義的費用帳戶。這些是傳送 AMS 每月帳單的帳戶。如果您找不到這些帳戶，請聯絡您的 Cloud Service Delivery Manager (CSDM) 尋求協助。

欄位名稱	資料集欄位名稱	定義
帳單日期	date	計費服務的月份和年份
付款人帳戶 ID	payer_account_id	識別負責支付 AMS 費用之帳戶的 12 位數 ID
連結的帳戶 ID	linked_account_id	識別使用產生擴展之服務的 AMS 帳戶的 12 位數 ID

欄位名稱	資料集欄位名稱	定義
AWS 服務名稱	product_name	已使用 AWS 的服務
AWS 費用	aws_charges	AWS 服務名稱中 AWS 服務名稱 AWS 的費用
定價計劃	pricing_plan	與連結帳戶相關聯的定價計劃
AMS 服務群組	tier_uplifting_groups	決定提升百分比的 AMS 服務群組程式碼
提升比例	uplift_percent	根據 pricing_plan、SLA AWS 和服務提升百分比（以小數 V.WXYZ 表示）
調整後 AWS 的費用	adjusted_aws_usage	AWS 針對 AMS 調整的用量
調高 AWS 費用	uplifted_aws_charges	AMS ; adjusted_aws_charges * uplift_percent AWS 要支付的費用百分比
執行個體 EC2 RDS 支出	instance_ec2_rds_spend	EC2 和 RDS 執行個體上的支出
預留執行個體費用	ris_charges	預留執行個體費用
提高預留執行個體費用	uplifted_ris	AMS 要收取的預留執行個體費用百分比 ; ris_charges * uplift_percent
Savings Plan 費用	sp_charges	SavingsPlan 使用費
提高的 Savings Plan 費用	uplifted_sp	AMS ; sp_charges * uplift_percent 需支付的節省計劃費用百分比

欄位名稱	資料集欄位名稱	定義
AMS 費用	ams_charges	產品的總 ams 費用； $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
按比例分配的最低費用	prorated_minimum	我們為了符合合約下限而收取的金額
連結的帳戶總 AMS 費用	linked_account_total ams_charges	linked_account 的所有費用總和
付款人帳戶 AMS 費用總計	payer_account_total ams_charges	付款人帳戶的所有費用總和
最低費用	minimum_fees	AMS 最低費用（如適用）
預留執行個體和 Savings Plan 折扣	adj_ri_sp_charges	要套用至 RI/SP 費用的 RI/SP 折扣（適用於特定情況）

彙總報告

彙總自助式報告 (SSR) 可讓您檢視組織層級、跨帳戶彙總的現有自助式報告。這可讓您查看 AMS 管理下的所有帳戶的關鍵操作指標，例如修補程式合規、備份涵蓋範圍和事件 AWS Organizations。

彙總 SSR 可在 AWS Managed Services 提供的所有商業 AWS 區域環境中使用。如需可用區域的完整清單，請參閱[區域資料表](#)。

啟用彙總報告

您必須從 AWS Organizations [管理帳戶](#) 管理彙總的 SSR。管理帳戶是您用來建立組織的 AWS 帳戶。

若要為已加入 AMS 的 AWS Organizations 管理帳戶啟用彙總 SSR，請存取您的 AMS 主控台並導覽至報告。選取 top-right-hand 的組織存取，開啟 [AWS Managed Services 主控台：組織檢視](#) 窗格。在此窗格中，您可以管理彙總的 SSR 功能。

AWS Organizations 未加入 AMS 的管理帳戶無法存取 AMS 主控台。若要為未加入 AMS 的 AWS Organizations 管理帳戶啟用彙總 SSR，請先向您的 進行身分驗證 AWS 帳戶，然後導覽至[AWS 主控台](#)並搜尋 Managed Services。這會開啟 AMS 行銷頁面。在此頁面上，選取導覽列中的組織存取連結以開啟 AWS Managed Services 主控台：Organization View，您可以在其中管理彙總 SSR 功能。

第一次存取 [AWS Managed Services主控台：Organization View](#) 時，請完成下列步驟：

1. 如果您尚未設定 AWS Organizations，請從主控台選擇啟用 AWS Organizations。如需設定的其他資訊 AWS Organizations，請參閱[AWS Organizations 《使用者指南》](#)。如果您已使用，可以略過此步驟 AWS Organizations。
2. 若要啟用彙總自助式報告服務，請選取在主控台上啟用受信任存取。
3. (選用) 註冊委派管理員，以擁有組織檢視的讀取存取權。

以委派管理員身分檢視彙總報告

委派管理員是您選擇擁有彙總報告讀取存取權的帳戶。委派管理員必須是加入 AMS 的帳戶，並且是唯一具有彙總報告讀取存取權的帳戶。

若要選擇委派管理員，請在 AWS Managed Services主控台：組織檢視的步驟 3 中輸入帳戶 ID。您一次只能註冊一個委派管理員帳戶。請注意，委派管理員帳戶必須是 AMS 受管帳戶。

若要更新委派管理員帳戶，請導覽至 [AWS Managed Services主控台：組織檢視](#)，然後選取移除委派管理員。主控台會提示您插入新的帳戶 ID，以註冊為委派管理員。

讀取彙總報告

如果您未註冊委派管理員，且您的 AWS Organizations 管理帳戶已加入 AMS，則 AWS Organizations 管理帳戶預設會取得彙總報告的讀取存取權。如果 AWS Organizations 管理帳戶不是由 AMS 管理，則您必須選擇委派管理員帳戶，才能讀取彙總報告。

在任何時候，只有加入 AMS 的單一帳戶才能讀取彙總報告，無論是 AWS Organizations 管理帳戶或註冊的委派管理員。組織內的所有其他成員帳戶 (並加入 AMS) 仍然只能存取每個個別帳戶的單一帳戶報告。

啟用彙總 SSR 後，導覽至您的[報告](#)。所有現有的自助式報告都會列在本節中，藍色標籤表示它們已彙總。請注意，您必須從您選擇的帳戶存取 AMS 主控台，才能讀取彙總報告。這是 AWS Organizations 管理帳戶或委派管理員帳戶。

啟用彙總 SSR 之後，即可從下一個報告週期開始取得彙總報告。

停用彙總報告

若要停用彙總 SSR，請開啟 [AWS Managed Services 主控台：組織檢視](#)。選取停用受信任存取。停用彙總 SSR 的受信任存取後，您的 AMS 自助式服務報告會在組織層級跨帳戶彙總。另請注意，停用會從下一個報告週期開始生效。

停用彙總 SSR 之後，在 AMS 主控台中的報告顯示為單一帳戶報告之前會有等待。發生此延遲是因為功能停用會從下一個報告週期開始生效。

AMS 自助式報告儀表板

AMS 自助式報告提供兩個儀表板：[Resource Tagger 儀表板](#)和 [安全組態規則儀表板](#)。

Resource Tagger 儀表板

AMS Resource Tagger Dashboard 提供 Resource Tagger 支援之資源的詳細資訊，以及 Resource Tagger 設定為套用至這些資源之標籤的目前狀態。

依資源類型劃分的資源交錯範圍

此資料集包含資源清單，其中包含由 Resource Tagger 管理的標籤。

依資源類型的資源涵蓋範圍視覺化為四個折線圖，描述下列指標：

- 資源計數：依資源類型區分，區域中的資源總數。
- 資源遺失受管標籤：區域中需要受管標籤但未由 Resource Tagger 標記的資源總數，依資源類型排序。
- 未受管資源：區域中資源的總數，依資源類型，這些資源類型未由 Resource Tagger 套用受管標籤。這通常表示這些資源不符合任何 Resource Tagger 組態，或明確地從組態中排除。
- 受管資源：與未受管資源指標 (資源計數 - 未受管資源) 相反。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間)
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID

欄位名稱	資料集欄位名稱	定義
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
資源計數	resource_count	在此區域中部署的資源數量 (指定資源類型的)。
ResourcesMissingManagedTags	resource_missing_managed_tags_count	根據組態描述檔，需要受管標籤但尚未由 Resource Tagger 標記的資源 (指定資源類型的) 數量。
UnmanagedResources	unmanaged_resource_count	資源數量 (指定資源類型的)，沒有由 Resource Tagger 套用的受管標籤。一般而言，這些資源不符合任何 Resource Tagger 組態區塊，或明確地從組態區塊中排除。

資源 Tagger 組態規則合規

此資料集包含 中 AWS 區域依資源類型列出的資源清單，這些資源已套用特定組態描述檔。它被視覺化為折線圖。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間)

欄位名稱	資料集欄位名稱	定義
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
組態設定檔 ID	configuration_profile_id	Resource Tagger 組態設定檔的 ID。組態設定檔用於定義用來標記資源的政策和規則。
MatchingResourceCount	resource_count	符合 Resource Tagger 組態設定檔 ID 的資源數量（指定資源類型的）。若要讓資源符合組態描述檔，必須啟用描述檔，且資源必須符合描述檔的規則。

Resource Tagger 不合規資源

此資料集包含單一 Resource Tagger 組態不合規的資源清單。此資料是資源合規的每日快照，顯示這些報告交付到客戶帳戶時客戶資源的狀態（沒有歷史檢視）。它被視覺化為樞紐分析表，由特定組態不合規的資源組成。

下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
報告日期時間	dataset_datetime	產生報告的日期和時間 (UTC 時間)
AWS 帳戶 ID	aws_account_id	AWS 帳戶 ID

欄位名稱	資料集欄位名稱	定義
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
Region	region	AWS 區域
資源類型	resource_type	此欄位可識別資源的類型。僅包含 Resource Tagger 支援的資源類型。
資源 ID	resource_id	Resource Tagger 支援之資源的唯一識別符。
涵蓋狀態	coverage_state	此欄位指出資源是否依 Resource Tagger 組態 ID 所設定進行標記。
組態設定檔 ID	configuration_profile_id	Resource Tagger 組態設定檔的 ID。組態設定檔用於定義用來標記資源的政策和規則。

安全組態規則儀表板

安全設定規則儀表板提供 AMS 帳戶資源和 AWS Config 規則合規性的深入檢視。您可以依規則嚴重性篩選報告，以排定最關鍵的問題清單的優先順序。下表列出此報告所提供的資料。

欄位名稱	資料集欄位名稱	定義
AWS 帳戶 ID	AWS 帳戶 ID	與相關資源繫結的帳戶 ID。
管理員帳戶 ID	aws_admin_account_id	由您啟用的信任 AWS Organizations 帳戶。
報告日期時間	報告日期	產生報告的日期和時間。
customer_name	客戶名稱	客戶名稱。
account_name	帳戶名稱	與帳戶 ID 相關聯的名稱

欄位名稱	資料集欄位名稱	定義
resource_id	資源 ID	資源的識別符。
resource_region	資源區域	AWS 區域 資源所在的 。
resource_type	資源類型	AWS 服務 或 資源類型。
resource_name	資源名稱	資源的名稱。
resource_ams_flag	資源 AMS 旗標	如果資源為 AMS 擁有，則此旗標設定為 TRUE。如果資源是客戶擁有，則此旗標設定為 FALSE。如果所有權不明，則此旗標會設為 UNKNOWN。
config_rule	Config 規則	組態規則不可自訂的名稱。
config_rule_description	組態規則描述	組態規則的描述。
source_identifier	來源識別符	受管組態規則的唯一識別符，而自訂組態規則沒有識別符。
compliance_flag	合規旗標	顯示資源是否符合組態規則。
rule_type	規則類型	指出規則是預先定義還是自訂建置。
exception_flag	例外狀況旗標	資源例外狀況旗標顯示對不合規資源接受的風險。如果資源的資源例外狀況旗標為 TRUE，則會豁免資源。如果例外狀況旗標為 NULL，則不會排除資源。
cal_dt	日期	規則的評估日期。
remediation_description	修復描述	如何修復規則合規的描述。

欄位名稱	資料集欄位名稱	定義
severity	嚴重性	組態規則嚴重性表示不合規的影響。
customer_action	客戶動作	修正 規則所需的動作。
建議	建議	組態規則檢查內容的描述。
remediation_category	修復類別	AMS 在此規則變得不合規時所採取的預設動作。

資料保留政策

在報告的期間之後，AMS SSR 每個報告都有資料保留政策，資料會清除且不再可用。

報告名稱	資料保留 SSR 主控台	資料保留 SSR S3 儲存貯體
執行個體詳細資訊摘要 (Patch Orchestrator)	2 個月	2 年
修補程式詳細資訊	2 個月	2 年
在維護時段執行期間遺漏修補程式的執行個體	2 個月	2 年
AMS 帳單費用詳細資訊	2 年	2 年
每日備份報告	1 個月	2 年
每週事件報告	2 個月	2 年
安全設定規則儀表板	3 個月	2 年
Resource Tagger 儀表板	1 年	2 年

從 SSR 離職

若要從 SSR 服務離職，請透過 AMS 主控台建立服務請求 (SR)。提交 SR 之後，AMS 操作工程師會協助您從 SSR 中離職。在 SR 中，提供您要離職的原因。

若要退出帳戶並執行資源清理，請透過 AMS 主控台建立 SR。提交 SR 之後，AMS 操作工程師會協助您刪除 SSR Amazon S3 儲存貯體。

如果您從 AMS 離職，您會自動從 AMS SSR 主控台離職。AMS 會自動停止將資料傳送至您的帳戶。AMS 會在離職程序中刪除您的 SSR S3 儲存貯體。

AMS 中的事件報告、服務請求和帳單問題

主題

- [事件管理](#)
- [服務請求管理](#)
- [帳單問題](#)

透過 AWS Managed Services (AMS)，您可以隨時透過 AMS 主控台請求操作問題和請求的協助。AMS 操作工程師全年無休回應您的事件和服務請求，回應時間服務水準協議 (SLAs) 和服務水準目標 (SLOs)，取決於您選取的帳戶服務層級 (Plus、Premium)。AMS 營運工程師會使用相同的機制，主動通知您重要的提醒和問題。

事件管理

主題

- [什麼是事件管理？](#)
- [事件管理服務承諾](#)
- [事件管理範例](#)

事件是影響受管環境 AWS 服務的效能問題，由 AWS Managed Services (AMS) 或您決定。AMS 團隊識別的事件會先收到「事件」：監控擷取的系統狀態變更。如果超過設定的閾值，事件會觸發警示，也稱為警示。AMS 操作團隊會判斷事件是否不受影響、事件（服務中斷或降級）或問題（一或多個已解決事件的根本原因）。

AMS 團隊也會透過 支援 中心或以程式設計方式使用服務代碼的 [AWS Support API](#) 來接收您識別的事件 `sentinel-report-incident`。

在 AMS 操作團隊收到您的事件後，會對其進行審核，以確保事件不會被歸類為服務請求。如果它應該分類為服務請求，它會立即重新分類，AMS 服務請求團隊會接管並通知您。如果事件可由接收運算子解決，則會立即採取步驟來解決事件。AMS 運算子會參考內部文件以取得解決方案，並視需要將事件呈報給其他支援資源，直到事件解決為止。若要在事件解決程序的每個步驟保持通知，請務必填寫 CC 電子郵件選項，如果您要透過聯合連線，請先登入，然後再遵循 AMS 傳送的電子郵件中的連結。解決後，AMS 操作團隊會記錄事件和解決方案以供日後使用。

如果事件解決需要變更基礎設施，可能需要安全審查。可能需要安全性審查的基礎設施變更包括與 IAM 或資源型政策或風險核准相關的變更。這些類型的事件需要 AMS Operations 工程師在進行變更之前建立 RFC，而且您需要核准該 RFC。例如，如果事件解決需要更新 IAM 政策，將會進行 AMS 安全審查，然後 AMS 操作工程師將使用 管理 | 進階堆疊元件 | Identity and Access Management (IAM) | 更新實體或政策變更類型 (ct-27tuth19k52b4) 建立 RFC，並等待您核准 RFC 再繼續。

Note

AMS 現在允許需要變更基礎設施的事件解決方案，而無需額外的 RFC 核准步驟。如果解決事件所需的變更不需要安全審查（變更與 IAM 或資源型政策或風險核准無關），則 AMS 可以根據您在事件中收到的核准進行變更，而無需在 RFC 中另行核准。

如需事件管理術語的定義，請參閱 [AMS 關鍵術語](#)。

若要了解事件的呈報路徑，請參閱[取得協助](#)。

如需事件的 AMS 回應說明，請參閱 [AMS 事件回應](#)。

什麼是事件管理？

事件管理是 AMS 用來記錄、處理、傳達作用中事件進度並提供通知的程序。

事件管理程序的目標是確保盡快還原受管服務的正常操作、將業務影響降至最低，並隨時通知所有相關各方。

事件的範例包括（但不限於）網路連線遺失或降級、無回應的程序或 API，或未執行的排程任務（例如備份失敗）。

下圖說明您向 AMS 報告之事件的工作流程。

此圖描述 AMS 向您報告之事件的工作流程。

事件優先順序

在 AWS Support 中心、主控台或 Support API (SAPI) 中建立的事件，其分類與在 AMS 主控台中建立的事件不同。

- 低：與 AWS 或 AMS 資源相關的業務服務或應用程式的非關鍵函數會受到影響。

- 中：與 AWS 和/或 AMS 資源相關的商業服務或應用程式受到中度影響，且運作狀態降低。
- 高：您的業務會受到重大影響。與 AWS 和/或 AMS 資源相關的應用程式重要功能無法使用。預留給影響生產系統的最重要中斷。

Note

AWS Support Console 提供五個層級的事件優先順序，我們可將其轉換為三個 AMS 層級。

問題與事件

當 AMS 認為事件顯示較大的瑕疵或組態錯誤，並且可能會再次發生時，它會被視為問題，而不只是事件。在這種情況下，AMS 會分析問題並提供解決問題的建議。

事件管理服務承諾

事件管理服務承諾

事件或動作	服務承諾衡量
案例 1：產生具有已知影響的事件。AMS 會開啟事件並通知您。	事件回應和事件解決的時鐘會在下列情況開始：
案例 2：AMS 會與您聯絡，以確認事件的影響。您確認事件是事件。	案例 1：AMS 會建立事件。
案例 3：您注意到問題並提交事件報告。	案例 2：您確認警示是事件。
	案例 3：您提交事件。
	服務承諾取決於所建立事件的優先順序。
如果您提交事件，AMS 會傳送回應以確認。	事件解決的時鐘會繼續刻度。
如果 AMS 代表您建立事件，則不會傳送個別的事件回應。	AMS 傳送事件確認時，事件回應時間的時鐘會停止。
	 Note 等待您輸入所花費的時間會排除在事件解決時間計算之外。對於 AMS 建立的

事件或動作	服務承諾衡量
對於有問題的資源/服務，AMS 會檢查運作狀態，以確認是否： - AMS 偵測到的事件或客戶提交的事件符合事件的資格，以及 - 事件已正確排定優先順序，且 如果您提交的事件未正確排定優先順序，AMS 會重新排定優先順序。如果 AMS 變更事件優先順序，則會傳送通知給您，以及優先順序變更背後的原因。在某些情況下，您提交的問題可能不符合事件的資格，具體取決於原因。在這些情況下，AMS 會關閉事件，並傳送通知給您，說明原因。無論事件分類為何，AMS 都會視需要協助您。 若要了解事件分類的規則，請參閱 事件優先順序。	事件，初始回應時間是為您建立初始事件通知的時間。 如果事件優先順序變更，則適用新優先順序的服務承諾；時鐘會繼續勾選。如果事件因為不符合事件的定義而關閉，則服務承諾不適用；時鐘會停止。
AMS 會在事件上運作，以在服務承諾內加以解決。在某些情況下，如果 AMS 判斷無法及時解決無法使用的堆疊或資源（多個），則 AMS 將提供基礎設施還原作為解決選項。基礎設施還原涉及根據受影響堆疊的範本重新部署現有堆疊（EBS/RDS 快照），並根據最後一個已知還原點（EBS/RDS 快照）啟動資料還原，除非您另有指定。個別 EC2 執行個體上的暫時性資料將會遺失。如果您未依 AWS 建議授權基礎設施還原，則不符合相關事件解決時間服務承諾的服務額度資格。	時鐘會在下列情況下停止： - AMS 已將與該事件相關的所有無法使用服務或資源還原為可用狀態，或 - 基礎設施還原已啟動。

事件或動作	服務承諾衡量
有時，除非您有預先定義的核准動作，否則 AMS 需要釐清事件解決工作，或讓 進行活動。因此，AMS 與您之間會進行通訊，以解決事件	當 AMS 正在等待您的回應或動作時，時鐘會停止。 時鐘會在下列情況下重新啟動：AMS 收到來自您的回應，或 AMS 要求您完成的動作。

Note

如需服務承諾的完整清單，請下載 [AMS 服務水準協議](#)。

事件管理範例

事件管理範例。

主題

- [事件測試](#)
- [報告事件](#)
- [監控和更新事件](#)
- [使用 AWS Support API 管理事件](#)
- [回應 AMS 產生的事件](#)

下列範例說明使用 AMS 主控台來提交事件。提交後，AMS 團隊會與您合作，根據您的服務水準協議 (SLA) 解決事件。

事件測試

測試 AMS 事件提交時，我們會要求您在主旨文字中包含此旗標：AMSTestNoOpsActionRequired。此旗標可讓 AMS 知道事件提交僅用於測試。當 AMS 操作工程師看到該旗標時，他們不會以任何方式回應事件提交。

報告事件

使用 AMS 主控台報告事件。請務必為每個新問題建立新的事件。開啟與舊查詢相關的案例時，包含相關的案例編號會很有幫助，以便我們可以參考先前的通訊。

 Note

如果案例通訊偏離原始問題，AMS 運算子可能會要求您報告新的事件。

若要使用 AMS 主控台報告事件：

1. 從左側導覽中，選擇事件

事件清單隨即開啟：

如果您的事件清單是空的，清除篩選條件選項會將篩選條件重設為任何狀態。

如果您知道要使用電話或聊天，請按一下支援中心中的建立事件，以在支援中心主控台中開啟事件建立頁面，自動填入 AMS 服務類型。

 Important

- 支援系統會記錄使用起始的通話，以改善回應。如果通話中斷，您必須透過支援中心案例回撥，AWS 沒有機制可以回撥給您。
- 電話和聊天支援旨在協助處理支援案例、事件和服務請求，而不是 RFC 或安全問題。
- 對於 RFC 問題，請使用相關 RFC 詳細資訊頁面上的通訊選項來聯絡 AMS 工程師。
- 針對安全問題，請建立高優先順序 (P1 或 P2) 支援案例。即時聊天功能不適用於安全事件。

2. 如果您想要尋找現有的事件，請在下拉式清單中選取事件狀態篩選條件。

- 所有尚未解決的事件。
- 尚未指派的新事件。
- 已指派的事件。
- 您重新開啟的事件。
- 指派的複雜事件。

- 在下一個步驟之前需要您的意見回饋的事件。
- 您最近提交資訊的事件。
- 已結束的事件。
- 帳戶中的所有事件。

3. 選擇建立。

建立事件頁面隨即開啟：

4. 選取優先順序：

- 低：與 AWS/AMS 資源相關的業務服務或應用程式的非關鍵函數會受到影響。
- 中：與 AWS/AMS 資源相關的商業服務或應用程式會受到中度影響，並在降級狀態下運作。
- 高：您的業務會受到重大影響。與 AWS/AMS 資源相關的應用程式關鍵函數無法使用。預留給影響生產系統的最重要中斷。

5. 選取類別。

Note

如果您要測試事件功能，請將無動作旗標 (AMSTestNoOpsActionRequired) 新增至您的事件標題。

6. 輸入以下資訊：

- 主旨：事件報告的描述性標題。
- CC 電子郵件：您想要通知有關事件報告和解決方案的人員的電子郵件地址清單。
- 詳細資訊：事件的完整描述、受影響的系統，以及解決方案的預期結果。回答預先設定的問題，或刪除它們並輸入任何相關資訊。

若要新增附件，請選擇新增附件，瀏覽至您想要的附件，然後按一下開啟。若要刪除附件，請按一下刪除圖示：

7. 選擇提交。

詳細資訊頁面隨即開啟，其中包含事件的相關資訊，例如類型、主旨、已建立、ID 和狀態，以及包含您所建立請求描述的通訊區域。

按一下回覆以開啟通訊區域，並提供其他詳細資訊或狀態更新。

事件解決後，請按一下關閉案例。

如果通訊數量超過一頁的數量，請按一下載入更多。

請不要忘記為通訊評分！

您的事件會顯示在事件清單頁面上。

YouTube 影片：[如何從 AWS Managed Services 主控台引發事件？](#)

監控和更新事件

您可以使用 AMS 主控台或以程式設計方式使用 支援 API 來更新、監控和檢閱事件報告和服務請求，這兩者稱為 案例。如需使用 支援 API 的資訊，請參閱 [DescribeCases](#) 操作。

若要使用 AMS 主控台監控案例、事件或服務請求，請遵循下列步驟。

1. 在 AMS 主控台事件報告或服務請求儀表板中，瀏覽至案例，然後選擇主旨以開啟包含目前狀態和通訊的詳細資訊頁面。

當 AMS 操作團隊更新報告的事件或服務請求案例時，您會收到電子郵件和 AMS 主控台中事件的連結，以便您可以回應。您無法透過回覆電子郵件來回應事件通訊。

Important

您必須輸入電子郵件地址，才能接收服務請求或事件案例的狀態變更通知。通知只會傳送至建立案例時新增至案例的電子郵件地址。

除非您在 AMS 聯合網路上使用電子郵件伺服器，否則通知電子郵件中的連結將無法運作。不過，您可以前往 AMS 主控台並使用案例詳細資訊頁面來回應通訊。

2. 如果清單中有許多案例，您可以使用篩選條件選項：

- 全部開啟（預設）：使用此篩選條件可查看所有尚未解決的案例。
 - 未指派：如果您剛提交案例，但未收到案例狀態已變更的任何通知，請使用。請注意，根據提交的優先順序（事件）或您的服務水準協議（服務請求），事件和服務請求案例會以不同的提示處理。
 - 開啟：如果您收到案例為「待定 Amazon」動作的通知，請使用；這表示案例已指派，但尚未開始運作。
 - 已重新開啟：如果您收到案例在解決後重新開啟的通知，請使用。
 - 進行中的工作：如果您收到操作員開始處理案例的通知，請使用。
 - 待定的客戶動作：如果您收到操作者請求，請使用。
 - 客戶動作已完成：如果您收到已處理案例動作的通知，請使用。
 - 已解決：使用來檢視您已知已解決的案例。已解決的案例會在歷史記錄中保留 12 個月。
 - 任何狀態：使用此篩選條件來查看所有案例，無論狀態為何。
3. 若要檢查最新狀態，請重新整理頁面。
 4. 如果有太多通訊無法全部顯示在頁面上，請選擇載入更多。
 5. 若要提供案例狀態的更新，請選擇回覆、輸入新的通訊，然後選擇提交。
 6. 若要在案例解決到滿意程度後關閉案例，請選擇關閉案例。

請務必透過 1-5 星評分來評定服務，讓 AMS 知道我們的表現！

使用 AWS Support API 管理事件

[AWS Support API](#) 可讓您建立事件，並在問題調查以及與 AWS Support 人員的互動期間新增通訊。AWS Support API 會建立 [AWS Support Center](#) 大部分行為的模型。如需如何使用此 AWS 支援服務的詳細資訊，請參閱[程式設計 AWS 支援案例](#)。

Note

針對 AMS Advanced 事件使用 AWS Support API 或 SAPI 時，請使用此服務代碼：sentinel-report-incident。

回應 AMS 產生的事件

AMS 會主動監控您的資源；如需詳細資訊，請參閱[監控和事件管理](#)。有時 AMS 會識別並建立事件案例，通常是通知您事件。如果您必須採取動作來解決事件，AMS 會傳送通知給您為帳戶提供的聯絡資

訊。您回應此事件的方式與回應任何其他事件的方式相同。您通常會透過 AMS 主控台回應事件；在某些情況下，需要透過電子郵件或電話聯絡。

Note

AMS 會將通訊傳送到您 AWS 帳戶的主要電子郵件地址；我們建議您新增替代操作聯絡人電子郵件別名，以促進事件管理程序。這在 AMS 加入程序和相關加入文件期間涵蓋。如果您已在加入期間為 AMS 提供非資源型聯絡人（您通知 CSDM 的聯絡人），則會使用這些聯絡人。例如，您可以將名為「SecurityContacts」的聯絡人清單提供給 CSDMs/CAs 以用於安全相關事件或通知。如果您已同意 CSDM 使用標籤資訊，則執行個體/資源上的聯絡標籤會用於 AMS 產生的事件。

若要進一步了解此通知服務，請參閱[通知](#)。

服務請求管理

主題

- [何時使用服務請求](#)
- [服務請求管理的運作方式](#)
- [在 AMS 中測試服務請求](#)
- [在 AMS 中建立服務請求](#)
- [在 AMS 中監控和更新服務請求](#)
- [回應 AMS 產生的服務請求](#)

服務請求是您建立的 AMS 通訊，用於要求資訊或建議。標準服務請求的良好範例是提供設定 AMS 服務的指引或協助，例如 Alarm Manager、Patch Orchestrator 等。您也可以從 AMS 接收服務請求；這些稱為傳出服務請求或服務通知。若要查看 AMS 傳送給您的服務請求和傳出服務請求清單（服務通知），請查看 AMS 主控台的服務請求頁面。

若要進一步了解傳出服務請求，請參閱 [回應 AMS 產生的服務請求](#)。

您可以使用 AMS 主控台或使用 API 以程式設計方式建立 AWS Managed Services (AMS) 服務請求。支援 如需使用 API 的詳細資訊，請參閱 [支援 API](#)。針對 AMS，選擇 `sentinel-service-request` 服務代碼。

AMS 操作團隊收到您的服務請求後，會根據您的服務水準協議排定優先順序。若要在服務請求解決程序的每個步驟中隨時收到通知，請務必填寫 CC 電子郵件選項，如果您要透過聯合連線，請在遵循 AMS 傳送的電子郵件中的連結之前登入。

使用 AMS 主控台建立服務請求頁面來執行下列任務：

- 建立和更新服務請求
- 取得您目前所有服務請求的清單和詳細資訊
- 依日期和事件識別符縮小搜尋服務請求的範圍，包括已解決的請求
- 將通訊和檔案附件新增至您的請求，並新增電子郵件收件人以進行案例通訊
- 解決服務請求
- 評價服務請求通訊

何時使用服務請求

下列範例說明服務請求：

- AMS 或 AWS 一般指引
- 修補程式 MW 相關問題
- 備份排程相關問題
- 有關 AWS 服務功能的問題

以下是不應在服務請求中提出的範例：

- 存取問題
- 修補程式失敗
- 備份失敗
- RFC 失敗或造成業務中斷的 RFC（業務中斷的使用事件）
- RFC 問題或其他輸入或變更 RFC 範圍（使用 RFC 雙向通訊）

服務請求管理的運作方式

服務請求由待命 AMS 操作團隊處理。

AMS 操作團隊收到您的服務請求後，會對其進行審核，以確保請求不會更適當地分類為事件。如果它應該分類為事件，它會立即重新分類、AMS 事件管理團隊接管，而且會通知您。

如果可以透過提交 RFC 來解決服務請求，檢閱運算子會傳送一封電子郵件給您，要求您提交適當的 RFC（提供詳細資訊）。

如果 AMS 運算子可以解決服務請求，則會立即採取執行此操作的步驟。例如，如果服務請求是針對架構建議或其他資訊，則運算子會將您參考適當的資源或直接回答問題。

如果您的服務請求分析發現錯誤或功能請求，則 AMS 會透過服務請求傳送通知給您。由於功能請求或錯誤修正沒有 ETA，因此原始服務請求會關閉。如需與原始服務請求相關的後續問題，請聯絡您的 CSDM。

如果服務請求超出 AMS 操作的範圍，運算子會傳送請求給您的雲端服務交付管理員，以便他們可以與您或適當的 AWS 操作團隊通訊，並傳送電子郵件給您，以了解正在採取哪些步驟。

在您表示您對結果感到滿意之前，服務請求不會解決。

Note

我們建議在所有情況下提供聯絡人電子郵件、名稱和電話號碼，以促進通訊。

在 AMS 中測試服務請求

測試 AMS 服務請求時，我們會要求您在主旨文字中包含此標記：AMSTestNoOpsActionRequired，讓 AMS 知道該服務請求僅用於測試。當 AMS 操作工程師看到該旗標時，他們不會回應服務請求。

在 AMS 中建立服務請求

若要使用 AWS Managed Services (AMS) 主控台建立服務請求：

1. 從左側導覽中，選擇服務請求。

服務請求清單隨即開啟。

如果您的服務請求清單是空的，清除篩選條件選項會將篩選條件重設為任何狀態。

如果您知道要使用電話或聊天，請按一下支援中心中的建立服務請求，以在支援中心主控台中開啟服務請求建立頁面，自動填入 AMS 服務類型。

 Note

系統會記錄使用 支援 中心起始的通話，以改善回應。如果通話中斷，您必須透過支援中心案例回撥，AWS 沒有機制可以回撥給您。

 Important

電話和聊天支援旨在協助處理支援案例、事件和服務請求。對於 RFC 問題，請使用相關 RFC 詳細資訊頁面上的通訊選項來聯絡 AMS 工程師。

2. 如果您想要尋找現有的服務請求，請在下拉式清單中選取服務請求狀態篩選條件。

- 所有尚未解決的服務請求。
- 尚未指派的新服務請求。
- 已指派的服務請求。
- 您已重新開啟的服務請求。
- 已指派、複雜的服務請求。
- 在下一個步驟之前需要您的意見回饋的服務請求。
- 您最近提交資訊的服務請求。
- 已結束的服務請求。
- 帳戶中的所有服務請求。

3. 選擇建立。

建立服務請求頁面隨即開啟。

4. 選取類別。

 Note

如果您要測試服務請求功能，請將無動作旗標 `AMSTestNoOpsActionRequired` 新增至您的服務請求標題。

5. 輸入以下資訊：

- 主旨：這會建立清單頁面上服務請求詳細資訊的連結。
- CC 電子郵件：除了您的預設電子郵件聯絡人之外，這些電子郵件也會收到通訊。
- 詳細資訊：在此盡可能多提供資訊。

若要新增附件，請選擇新增附件，瀏覽至您想要的附件，然後按一下開啟。若要刪除附件，請按一下刪除圖示：

6. 選擇提交。

詳細資訊頁面隨即開啟，其中包含服務請求的相關資訊，例如類型、主旨、已建立、ID 和狀態，以及包含您建立之請求描述的通訊區域。

此外，您的服務請求會顯示在服務請求清單頁面上。當您有提醒但尚未收到 AMS 的通知時，請使用此選項。

按一下回覆以開啟通訊區域，並提供其他詳細資訊或狀態更新。

當服務請求已解決時，請按一下解決案例。

按一下載入更多以檢視不符合初始頁面的其他通訊。

請不要忘記為通訊評分！

對於帳單相關查詢，請從支援中心主控台建立服務請求案例。

YouTube 影片：[如何和何時從 AWS 主控台提出服務請求，以及服務水準目標是什麼？](#)

在 AMS 中監控和更新服務請求

您可以使用 AMS 主控台或以程式設計方式使用 支援 API 來更新、監控和檢閱事件報告和服務請求，兩者皆稱為案例。如需使用 支援 API 的資訊，請參閱 [DescribeCases](#) 操作。

若要使用 AMS 主控台監控案例、事件或服務請求，請遵循下列步驟。

1. 在 AMS 主控台事件報告或服務請求儀表板中，瀏覽至案例，然後選擇主旨以開啟包含目前狀態和通訊的詳細資訊頁面。

當 AMS 操作團隊更新報告的事件或服務請求案例時，您會收到電子郵件和 AMS 主控台中事件的連結，以便您可以回應。您無法透過回覆電子郵件來回應事件通訊。

Important

您必須輸入電子郵件地址，才能接收服務請求或事件案例的狀態變更通知。通知只會傳送至建立案例時新增至案例的電子郵件地址。

除非您在 AMS 聯合網路上使用電子郵件伺服器，否則通知電子郵件中的連結將無法運作。不過，您可以前往 AMS 主控台並使用案例詳細資訊頁面來回應通訊。

2. 如果清單中有許多案例，您可以使用篩選條件選項：
 - 全部開啟（預設）：使用此篩選條件可查看所有尚未解決的案例。
 - 未指派：如果您剛提交案例，但未收到案例狀態已變更的任何通知，請使用。請注意，根據提交的優先順序（事件）或您的服務水準協議（服務請求），事件和服務請求案例會以不同的提示處理。
 - 開啟：如果您收到案例「待定 Amazon」動作的通知，請使用；這表示案例已指派，但工作尚未開始。
 - 已重新開啟：如果您收到案例在解決後重新開啟的通知，請使用。
 - 進行中的工作：如果您收到操作員開始處理案例的通知，請使用。
 - 待定客戶動作：如果您收到操作者請求，請使用。
 - 客戶動作已完成：如果您已收到已處理案例動作的通知，請使用。
 - 已解決：使用來檢視您已知已解決的案例。已解決的案例會在歷史記錄中保留 12 個月。
 - 任何狀態：使用此篩選條件來查看所有案例，無論狀態為何。
3. 若要檢查最新狀態，請重新整理頁面。

4. 如果有許多通訊並未全部顯示在頁面上，請選擇載入更多。
5. 若要提供案例狀態的更新，請選擇回覆、輸入新的通訊，然後選擇提交。
6. 若要在案例解決到滿意程度後關閉案例，請選擇關閉案例。

請務必透過 1-5 星評分來評定服務，讓 AMS 知道我們的表現！

回應 AMS 產生的服務請求

AMS 修補程式管理會在設定維護時段之前傳送服務請求（也稱為服務通知）給您；如需詳細資訊，請參閱 [AMS 維護時段](#)。當您的基礎設施可能受到 AWS 服務的影響，或您的帳戶中的 EC2 執行個體可能需要重新啟動時，AMS 也會傳送服務通知給您；如需詳細資訊，請參閱 [服務通知](#)。

Note

AMS 會將通訊傳送到 AWS 您帳戶的主要電子郵件地址；我們建議您新增替代操作聯絡人電子郵件別名，以促進服務請求或服務通知管理程序。在 AMS 加入程序和相關的加入文件期間，會涵蓋這些電子郵件。

帳單問題

若要提交帳單相關問題，請完成下列步驟：

1. 在 <https://console.aws.amazon.com/support/home/> 開啟 [AWS 支援中心](#)。
2. 選擇帳戶和帳單。
3. 選擇建立案例。
4. 選擇帳戶和帳單，然後依照提示提交您的案例。

隨需操作

隨需操作 (OOD) 是一種 AWS Managed Services (AMS) 功能，可透過提供 AMS 操作計劃或 目前未原生提供的操作服務，來擴展 [AMS 操作計劃](#) 的標準範圍 AWS。選取後，目錄產品會透過自動化和高技能 AMS 資源的組合來交付。沒有長期承諾或其他合約，可讓您視需要擴展現有的 AMS 和 AWS 操作和功能。您同意每月購買每個區塊 20 小時的時數區塊 (OOD 區塊)。

您可以從標準化方案目錄中選取，並透過服務請求啟動新的 OOD 參與。OOD 產品的範例包括協助維護 Amazon EKS、操作 AWS Control Tower和管理 SAP 叢集。根據需求和我們最常看到的操作使用案例，定期新增新的目錄方案。

OOD 同時適用於 AMS Advanced 和 AMS Accelerate 操作計劃，並可在 AMS 提供的所有 [AWS 區域](#) 中使用。

AMS 會在實作您請求的變更時，執行客戶安全風險管理 (CSRM)。若要進一步了解 CSRM 程序，請參閱[變更請求安全性審查](#)。

隨需操作方案目錄

隨需操作 (OOD) 為您提供下表所述的服務。

 Note

如需金鑰術語的定義，請參閱 AWS Managed Services 文件[金鑰術語](#)。

營運計畫	標題	描述	預期結果
AMS Accelerate	Amazon EKS 叢集維護	AMS 透過處理 Amazon Elastic Kubernetes Service (Amazon EKS) 部署的持續維護，釋放您的容器開發人員。AMS 會執行更新叢集所需的end-to-end程序，以解決控制平面、附加元件和節點的元件。AMS 會執行受管節點類型的更新，以及一組精選的 Amazon EKS 和 Kubernetes 附加元件。	客戶團隊協助進行更新 Amazon EKS 叢集的基礎操作工作。

AMS Accelerate	AMI 建置和販賣	AMS 持續為客戶提供 AMI 建置和販賣的管理。 我們的工程師會執行每月發行的訂閱 AMIs、發行緊急修補活動的隨需 AMIs、使用 Runbook 管理變更，以及使用 CloudWatch Monitoring 監控 AMI 組建。我們也為指定帳戶中使用的所有 AMIs 提供故障診斷協助和詳細報告。此服務需要透過 EC2 Image Builder 部署 AMI build Pipelines。AMS 不支援與 EC2 Image Builder 互動的任何其他自動化或服務。	客戶安全狀態改善，客戶花費在建置和販賣 AMIs 上的時間減少。
AMS Accelerate	統籌變更執行	與我們的熟練營運工程師合作，將您的業務需求轉換為可在 AWS 環境中安全執行的已驗證變更請求。利用我們自動化的獨特方法和操作最佳實務的知識（例如，影響評估、轉返、兩人規則），無論是大規模的簡單變更，還是具有下游影響的複雜動作。	客戶協助定義、建立和執行自訂變更請求。變更可以是手動或自動化 (CloudFormation、SSM)。必要時，包括諮詢支援以取得組態指引。不適用於變更應用程式程式碼、應用程式安裝/部署、資料遷移或作業系統組態變更。

AMS Accelerate	AWS Network Firewall 操作	AMS 會與您合作加入防火牆，並實作和管理持續防火牆操作的政策和規則。我們的工程師會利用我們的營運最佳實務和自動化來設定標準化政策和規則，並啟用監控來偵測自動化程序外所做的變更，藉此達成此目的。AMS 會快速通知您不需要的變更，並在要求時提供包含這些變更的選項，或將帳戶還原至先前的組態，以確保您系統的整體穩定性。	客戶團隊透過快速偵測意外的網路防火牆變更來協助降低管理開銷，進而改善事件解決並縮短預期和非預期問題的根本原因分析時間。
AMS Accelerate	AWS Control Tower 操作	持續操作和管理 AWS Control Tower 登陸區域，包括 AWS Transit Gateway 和 AWS Organizations - 提供全面的登陸區域解決方案。我們透過自訂控制項和護欄程式庫來處理帳戶販賣、SCP 和 OU 管理、偏離修復、SSO 使用者管理和 AWS Control Tower 升級。	客戶團隊協助一些管理 AWS Control Tower、AWS Transit Gateway 和 的基礎操作工作 AWS Organizations。
AMS Accelerate	AWS 登陸區域加速操作	AMS 提供透過 AWS 登陸區域加速器 (LZA) 部署之 AWS 登陸區域的持續操作。 我們的工程師會處理組態檔案變更、AWS Control Tower (CT) 環境管理 (帳戶販賣、OU 建立、CT 護欄)、服務內容政策 (SCP) 管理、CT 偏離偵測和修復、網路組態管理，以及 CT 和 LZA 架構的更新。AWS LZA 提供一種方法來使用操作最佳實務和服務來設定和管理安全、多帳戶 AWS 環境，例如 AWS Control Tower。	客戶團隊協助持續操作和管理 AWS 登陸區域加速器解決方案。

AMS Accelerate	SAP 叢集協助	SAP 叢集的專用警示、監控、叢集修補、備份和事件修復。此目錄項目可讓您從 SAP 操作團隊卸載一些正在進行的操作工作，以便他們可以專注於容量管理和效能調校。	客戶或合作夥伴 SAP 團隊協助一些基礎操作工作。仍然需要客戶提供其他 SAP 功能，例如容量管理、效能調校、DBA 和 SAP 基礎管理。
AMS Accelerate	EC2 操作上的 SQL Server	AMS 會與您合作，以加入、實作和管理部署在 EC2 執行個體上 SQL Server 資料庫的持續操作。 我們的工程師利用我們的操作最佳實務和自動化，透過執行備份和修補等任務、將 AMS 操作支援延伸至 SQL Server 修補，以包含叢集感知的滾動更新、符合我們勒索軟體防禦策略的備份和還原服務，以及監控對客戶提供的備份和修補控制的遵守情況，來釋放資料庫團隊。	除了將自己的授權 (BYOL) 帶入 EC2 之外，SQL Server 客戶還協助卸載修補和備份資料庫操作，以提高工作負載的彈性和安全狀態。
AMS 進階	Amazon EKS 叢集維護	AMS 透過處理 Amazon Elastic Kubernetes Service (Amazon EKS) 部署的持續維護和運作狀態，釋放您的容器開發人員。AMS 會執行更新叢集所需的end-to-end程序，以解決控制平面、附加元件和節點的元件。AMS 會執行受管節點類型的更新，以及一組精選的 Amazon EKS 和 Kubernetes 附加元件。	客戶團隊協助進行更新 Amazon EKS 叢集的基礎操作工作。
AMS 進階	優先順序 RFC 執行	指定 AMS 操作工程師容量，以優先執行您的變更請求 (RFC)。透過 Amazon Chime 會議室直接與工程師互動，可以調整所有提交的回應層級和優先順序。	客戶會收到 RFCs 的 8 小時回應 SLO。

AMS 進階和 AMS 加速	舊版作業系統升級	將執行個體升級至支援的作業系統版本，以避免執行個體遷移。我們可以利用自動化和軟體廠商的升級功能（例如，Microsoft Windows 2008 R2 到 Microsoft Windows 2012 R2），在您選取的執行個體上執行就地升級。此方法非常適合無法輕鬆在新執行個體上重新安裝的舊版應用程式，並針對舊版作業系統上的已知和未緩解安全威脅提供額外的保護。 就地升級支援下列作業系統： • Microsoft Windows 2012 R2 到 Microsoft Windows 2016 及更高版本 • Microsoft Windows 2016 到 Microsoft Windows 2022 及更高版本 • Red Hat Enterprise Linux 7 到 Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 到 Red Hat Enterprise Linux 9 • Oracle Linux 7 到 Oracle Linux 8	此解決方案適用於無法再重新安裝在新執行個體上的應用程式（例如，遺失原始碼、ISV 停止營業等）。您可以將失敗的升級轉返至其原始狀態。從操作角度來看，回復是偏好的，因為它會使用最新的安全修補程式，將執行個體置於更可支援的狀態。

主題

- [隨需請求 AMS 操作](#)
- [變更隨需操作方案](#)

隨需請求 AMS 操作

AWS Managed Services (AMS) Operations on Demand (OOD) 適用於所有已加入 AMS AWS 帳戶的。若要利用隨需操作，請向雲端服務交付管理員 (CSDM)、解決方案架構師 (SA)、帳戶管理員或雲

端架構師 (CA) 請求其他資訊。可用的 OOD 方案會列在上述[方案的隨需操作目錄中](#)。業務開發範圍完成後，向 AMS Operations 提交服務請求，以啟動 OOD 業務開發。

每個 OOD 服務請求必須包含與參與相關的下列詳細資訊：

- 請求的特定 OOD 方案，以及每個特定 OOD 方案：
 - 要配置給特定 OOD 方案的區塊數量（一個區塊等於指定日曆月的 20 小時操作資源時間，以適用隨需操作方案 AWS 的當時標準費率收費）。
 - 請求特定 OOD 方案的每個 AWS Managed Services 帳戶的帳戶 ID。

您必須透過下列任一方式提交 OOD 服務請求：

- 接收適用隨需操作方案的 AWS Managed Services 帳戶，或
- 一種 AWS Managed Services 帳戶，在所有功能模式下為 AWS Organizations 管理帳戶，代表其屬於 AWS Managed Services 帳戶的任何成員帳戶。

收到 OOD 服務請求後，AMS Operations 會使用帳戶核准、部分核准或拒絕來檢閱和更新帳戶。

一旦 OOD 方案服務請求獲得核准，AMS 和您就會協調以開始參與。在服務請求獲得核准且約定參與開始日期之前，不會啟動 OOD 方案。

AMS 會使用 OOD 區塊的每月訂閱分配。我們會從參與開始日期開始，每月分配已核准的區塊數量，直到您透過新的服務請求請求退出為止。OOD 區塊在日曆月內有效。未使用的區塊或區塊部分不會轉換或轉送至未來幾個月。

無論實際使用多少小時，您每個月至少需要支付一個 OOD 區塊的費用。不使用任何額外、已配置的 OOD 區塊，則不會計費。

變更隨需操作方案

若要請求變更隨選操作 (OOD) 方案的持續參與，請提交包含以下資訊的服務請求：

- 正在請求的修改（和）
- 修改生效的請求日期。

收到 OOD 服務請求後，AMS Operations 會檢閱請求，並使用其核准進行更新，或請求指派的 CSDM 與您合作，以判斷修改的範圍和影響。如果判斷修改需要 CSDM 的範圍工作，您必須在範圍練習完成後提交第二個 OOD 服務請求，以啟動修改後的參與。

核准後，最新修改的區塊配置會變成並持續保持作用中狀態，取代任何先前的區塊配置，除非 AWS 和您另有同意。

文件歷史紀錄

下表說明 AMS 進階使用者指南每個版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- API 版本：2019-05-21
- 新增或更新的 CTs 和逐步解說：[AMS 進階變更類型參考文件歷史記錄](#)。
- 新的 AMS AMIs：[AMS Amazon Machine Image AMIs](#)。

變更	描述	日期
更新 AMS Advanced 區段中標準控制項的 AWS Identity and Access Management (IAM) 資料表	更新表格中有關 IAM 政策和 Amazon S3 儲存貯體存取權的資訊。	2025 年 9 月 25 日
更新帳單相關查詢的步驟	更新在 AMS 中建立服務請求一節中建立帳單相關查詢的服務請求的步驟。	2025 年 9 月 25 日
更新變更類型的電子郵件通知資訊	已更新設定 RFC 電子郵件通知（主控台）區段中新增變更類型電子郵件通知的資訊和範例。	2025 年 9 月 25 日
已更新變更類型	使用標記 AMS 建立的資源的變更類型更新 AMS 基礎設施自動標記區段。	2025 年 9 月 25 日
已更新 AWS Managed Services 常見問答集中的 VM Import/Export	更新了用於請求執行個體描述檔的 RFC，以允許工具從執行個體執行命令。	2025 年 9 月 24 日
更新啟動 SUSE Linux Enterprise Server for SAP Applications 15 SP6 執行個體的變更請求 (RFC)	更新步驟 2，說明如何使用正確的 RFC 啟動新的 SUSE Linux Enterprise Server for	2025 年 9 月 22 日

SAP Applications 15 SP6 執行個體。

[更新變更請求 \(RFC\)](#)

在 AWS Managed Services 常見問答集區段 AWS Elastic Disaster Recovery 中，使用正確的 RFC 更新，以在您的帳戶中建立所需的 IAM 角色。

2025 年 9 月 22 日

[新增 4 個受信任修復程式支援的新 Trusted Advisor 成本最佳化檢查](#)

新增下列成本最佳化檢查：

2025 年 9 月 22 日

- c1z7kmr00n - 執行個體的 Amazon EC2 成本最佳化建議
- c1z7kmr02n - 磁碟區的 Amazon EBS 成本最佳化建議
- c1z7kmr03n - 資料庫執行個體的 Amazon RDS 成本最佳化建議
- c1z7kmr05n - 函數 AWS Lambda 的成本最佳化建議

[更新可用區域 \(AZs\)的注意事項](#)

更新 AMS 中安全群組的相關資訊。

2025 年 9 月 5 日

[已更新變更類型](#)

已更新 AWS Managed Services 常見問答集區段中的 Amazon FSx，其中包含將 Managed AD 共用至應用程式帳戶的變更類型。

2025 年 9 月 5 日

[已更新變更類型](#)

已更新 AWS Managed Services 常見問答集區段中的 Amazon DocumentDB，其中包含使用刪除 APIs 的變更類型。

2025 年 9 月 5 日

已更新變更類型	將 AWS Managed Services 中的 Alexa for Business 常見問答集一節的變更類型更新為兩個有限存取的 IAM 使用者，用於安裝和操作 Alexa for Business 閘道。	2025 年 9 月 5 日
已更新變更類型	已更新 AWS Managed Services 常見問答集區段中的 AppStream 2.0，其中包含建立和選擇可在所有機群串流執行個體上使用的 IAM 角色的變更類型	2025 年 9 月 5 日
已更新變更類型	已更新 AWS Managed Services 常見問答集區段中的 EventBridge，其中包含變更類型，可在使用 EventBridge 觸發其他 AWS 資源之前請求 EventBridge 服務角色。	2025 年 9 月 5 日
更新受信任修復程式支援 Trusted Advisor 的安全性檢查	更新檢查 Hs4Ma3G108 支援的預先設定參數和限制條件 - CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	2025 年 9 月 5 日
受信任修復程式的更新 Trusted Advisor 安全性檢查支援	已更新 Trusted Advisor 安全性檢查以新增 Hs4Ma3G184 第 2 版 - 應啟用 Application Load Balancer 和 Classic Load Balancer 記錄	2025 年 9 月 5 日
更新受信任修復程式區段支援的卓越 Trusted Advisor 營運檢查	更新 Trusted Remediator 支援的卓越 Trusted Advisor 營運檢查區段，以新增啟用的新支援檢查 c1fd6b96l4 Amazon S3 存取日誌。	2025 年 8 月 28 日

已更新變更類型	自訂 IAM 角色的變更類型。	2025 年 8 月 25 日
在 AMS 章節中使用適用於 .Net 和 SQL 的 CloudWatch Application Insights 更新	修訂變更類型以使用 CloudWatch Application Insights。	2025 年 8 月 25 日
更新變更請求 (RFC)	請求變更 (RFC) 將更多標籤新增至 Amazon S3 儲存貯體。	2025 年 8 月 25 日
更新變更請求 (RFC)	請求變更 (RFC) 為管理目的標記 AMS 建立的所有資源。	2025 年 8 月 25 日
已更新 AWS Managed Services 常見問答集章節中的 Lambda	修訂了其他 AWS 服務的存取變更類型，以建立事件來源。	2025 年 8 月 25 日
已更新 AWS Managed Services 常見問答集章節中的 Lambda	修訂變更類型以佈建 Lambda 函數。	2025 年 8 月 25 日
已更新建立、變更或刪除安全群組區段	修訂變更類型，以在堆疊和 VPCs 外部建立安全群組。	2025 年 8 月 25 日
已更新 Trusted Remediation 區段，以包含 Compute Optimizer 的新內容	已更新信任的修復程式區段，以包含支援 AWS Compute Optimizer 建議的新內容。	2025 年 8 月 18 日
TOC 詞彙表連結已移除	AWS 詞彙表 。	2025 年 8 月 8 日
精確的變更類型建議	若要將客戶指標與您的應用程式監控系統整合，請請求 AMS 透過使用部署 監控和通知 Amazon SNS 建立 CT (ct-3dfnglm4ombbs) 提交 RFC 來建立指標的 Amazon SNS 主題。	2025 年 8 月 8 日

精確的變更類型建議	若要刪除預留位置執行個體磁碟區，請提交管理 進階堆疊元件 EBS 磁碟區 刪除變更類型 (ct-3e3h8u0sp5z80)。	2025 年 8 月 8 日
新的監控提醒：SecureChannelFailure 和中斷的安全通道	AMS AMS 自動修復警示中基準監控的警示。	2025 年 8 月 8 日
新的信任修復程式檢查	Trusted Advisor Trusted Remediator Hs4Ma3G120-AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime、Hs4Ma3G230-AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 和 c18d2gz150-AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime 支援的成本最佳化Trusted Advisor 檢查。 Hs4Ma3G120 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime Hs4Ma3G230AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime	2025 年 8 月 8 日
更新點 3.2 中的 IAM 標準	釐清語言並移除提及標記。	2025 年 7 月 25 日
更新提醒選擇退出選項	新增標籤可讓您選擇不接收額外的兩個提醒。	2025 年 7 月 25 日

自助式佈建服務棄用	CloudEndure 自助式佈建服務已棄用，以享有優惠 AWS Application Migration Service。	2025 年 7 月 25 日
備份的新功能	使用新標籤自訂備份文件庫上的通知。	2025 年 7 月 25 日
已更新控制表	已移除 AMS-STD-002 - AWS Identity and Access Management (IAM) 資料表區段中的一些重複控制項。	2025 年 6 月 26 日
已更新 SSP 服務 AWS Transfer Family 先決條件	已將資訊新增至先決條件區段。	2025 年 6 月 26 日
更新的 IAM 政策範例	依照建議，以更多限制更新 IAM 政策範例。	2025 年 6 月 26 日
更新的 AMI OSes	在 Ubuntu Linux 22.04 下新增 Ubuntu Linux 24.04，並將 SP5 的所有參考變更為 SP6。	2025 年 6 月 26 日
自助式佈建服務、MediaStore 已棄用	新增的棄用備註 AWS Elemental MediaStore。	2025 年 6 月 26 日
自助式佈建服務，Amazon Inspector Classic 已棄用	新增 Amazon Inspector Classic 的棄用備註。	2025 年 6 月 26 日
自助式佈建服務，Amazon Connect 已棄用	新增 Amazon Connect 的棄用備註。	2025 年 6 月 26 日
更新 AMS 中支援的組態章節	更新 AMS 中支援的作業系統和支援的終止支援 (EOS) 作業系統的支援組態。	2025 年 6 月 25 日
自助式佈建服務，已棄用 WorkDocs	已移除已取代 WorkDocs 的頁面和參考。	2025 年 6 月 19 日

替代修補程式儲存庫的修補程式管理重要安全注意事項	在 AMS 中使用替代修補程式儲存庫的重要安全注意事項和最佳實務。	2025 年 6 月 10 日
支援的作業系統更新	AMS Advanced 支援的作業系統已更新，有些已新增，有些已移除。	2025 年 5 月 22 日
僅限內部 APIs	某些 CloudWatch 日誌中出現的僅限APIs。	2025 年 5 月 22 日
AMS 信任的修復程式更新	如何使用新參數 <code>preconfigured-parameters</code> 來自訂信任的修復程式中的 Trusted Advisor 檢查。	2025 年 5 月 22 日
SSP Amazon Elastic Container Registry 更新	當您加入 Amazon ECR 服務時，會自動佈建更多角色。	2025 年 5 月 8 日
AMS Advanced Trusted Remediator 常見問答集和更新。	支援 Trusted Advisor 檢查的幾項更新、信任的修復程式常見問答集（新增「信任的修復程式部署到您的帳戶有哪些資源？」）等。另請參閱 Trusted Advisor Trusted Remediator 支援的檢查 。	2025 年 5 月 8 日
AMS 進階標準安全控制更新。	新增「安全群組共用」控制項。	2025 年 5 月 8 日
AMS 進階受保護命名空間。	已EPS新增 AMS 保護的命名空間 <code>EPSMarketplaceSubscriptionRole</code> 和。	2025 年 4 月 24 日
AMS 進階日誌位置。	已新增其他日誌位置。	2025 年 4 月 24 日

AppStream 2.0 先決條件更新的 AMS 進階自助式佈建模式。	已新增 AppStream 2.0 的先決條件：提交服務的佈建 RFC 時，您必須包含 Amazon S3 儲存貯體名稱。	2025 年 4 月 24 日
AMS 進階新 Amazon RDS 自動修復提醒。	警示 ID：- 0224，當請求的已配置儲存達到或超過設定的最大儲存閾值時觸發。	2025 年 3 月 27 日
AMS Advanced AWS 已關閉新客戶對 Amazon CloudSearch 的存取權，自 2024 年 7 月 25 日開始生效。	現有客戶仍然可以使用服務，但不會有新功能。	2025 年 3 月 27 日
AMS Advanced AWS 已關閉新客戶對的存取權 AWS CodeCommit，自 2024 年 7 月 25 日開始生效。	現有客戶仍然可以使用服務，但不會有新功能。	2025 年 3 月 27 日
Trusted Remediator 現已推出。	Trusted Remediator 是自動化 AWS Trusted Advisor 檢查修復的 AWS Managed Services 解決方案，現已推出。	2025 年 3 月 19 日
AMS 進階新自動修復 RDS 提醒。	已新增 RDS-EVENT-0224。	2025 年 3 月 17 日
AMS 進階新功能：事件通知。	您可以使用 AppRegistry 來建立應用程式，並自訂這些應用程式的事件通知。	2025 年 3 月 13 日
AMS Update to RDS 警示監控閾值。	RDS 平均 CPU 使用率警示閾值已從 75% 變更為 90%。	2025 年 2 月 20 日

[使用彙總報告檢視的新資料選項更新自助式報告](#)

新增資料選項以包含新的欄位名稱：Admin Account ID、資料集欄位名稱：aws_admin_account_id 和定義：Trusted AWS Organization account enabled by the customer適用於下列自助式報告：

- 修補程式報告（每日）
- 備份報告（每日）
- 事件報告（每週）

2025 年 1 月 28 日

[更新至 AWS Batch SSP](#)

您可以使用下列 RFC 在 AWS Batch AMS 帳戶中佈建：管理 | AWS 服務 | 自助佈建服務 | 新增 (ct-1w8z66n899dct)。

2025 年 1 月 28 日

[新的 AMS 功能：彙總自助服務報告](#)

彙總自助式報告 (SSR) 可讓您檢視組織層級跨帳戶彙總的現有自助式報告。

2025 年 1 月 21 日

[更新至預測 SSP 區段](#)

新增備註：AWS 自 2024 年 7 月 29 日起，已關閉新客戶對 Amazon Forecast 的存取權。Amazon Forecast 現有客戶可以繼續正常使用服務。

2025 年 1 月 10 日

[更新至 AMS 保護的命名空間區段](#)

已將遺失的受保護命名空間 (*mc、*MC 和 *Mc) 新增至 AMS 受保護命名空間清單。

2025 年 1 月 9 日

[更新至監控的運作方式區段](#)

新增新功能的相關資訊，依資源或執行個體 ID 而非依事件設定提醒通知。

2025 年 1 月 8 日

更新：標籤型更新內容	修正 keyname 中的錯別字和修正錯誤的組態檔案路徑。	2025 年 1 月 6 日
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	2024 年 11 月 21 日
已更新隨需操作方案資料表	就地升級支援下列作業系統： • Microsoft Windows 2016 到 Microsoft Windows 2022 及更高版本	2024 年 11 月 11 日
已更新隨需操作方案資料表	就地升級支援下列作業系統： • Microsoft Windows 2012 R2 到 Microsoft Windows 2016 及更高版本 • Red Hat Enterprise Linux 7 到 Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 到 Red Hat Enterprise Linux 9 • Oracle Linux 7 到 Oracle Linux 8	2024 年 11 月 1 日
已更新支援的組態	將支援的 Oracle Linux 作業系統更新為 9.0-9.3、8.0-8.9、7.5-7.9。	2024 年 10 月 24 日

[更新的 AMS Amazon Machine Image AMIs\)](#)

更新了 Windows 封裝的 AMIs 以移除 Windows 2012 和 2012 R2。更新以 Linux 為基礎的 AMIs，以移除已不再支援的數個 AMIs，並新增下列項目：

2024 年 10 月 24 日

- Amazon Linux 2 (ARM64)
- RHEL 9
- SUSE Linux Enterprise Server 15 SP5

[您現在可以在標籤型提醒中包含多個電子郵件地址。](#)

標籤型提醒現在支援多個電子郵件地址。

2024 年 9 月 20 日

[已新增變更請求安全性審查區段。](#)

已新增新區段，提供變更請求安全性審查程序的詳細資訊。

2024 年 9 月 17 日

[已新增 區段。](#)

說明變更請求安全性檢閱在 AMS Advanced 中如何發生的新章節現已推出。

2024 年 9 月 12 日

[AMS Advanced 支援的新服務。](#)

AWS Resilience Hub AMS Advanced 現在支援。

2024 年 8 月 30 日

[AMS Advanced 支援的新服務。](#)

AMS Advanced 現在支援五個新服務：

2024 年 8 月 21 日

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Amazon Managed Service for Prometheus

新的端點安全網路預設設定現已可用。	更新來源現在包含在 EPS 預設網路設定中。	2024 年 8 月 21 日
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	2024 年 7 月 30 日
AMS 現在支援 Amazon Route 53 Resolver DNS 防火牆。	AMS 現在支援 Amazon Route 53 Resolver DNS 防火牆	2024 年 7 月 30 日
AWS DataSync SSPS 更新	AWS DataSync 不再需要 Amazon S3 儲存貯體名稱上的「datasync-」字首。	2024 年 7 月 30 日
安全設定規則儀表板	安全設定規則儀表板現在可在自助式報告中使用。	2024 年 7 月 24 日
AMS 現在支援 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	AMS 現在支援 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	2024 年 7 月 5 日
Amazon Bedrock 現在可在自助式佈建模式中使用	您現在可以在 AMS SSP 模式下請求 Amazon Bedrock。	2024 年 6 月 27 日
安全事件回應中的 Amazon Route 53 Resolver DNS 防火牆事件	AMS 現在會在安全事件回應中監控 Amazon Route 53 Resolver DNS 防火牆事件	2024 年 6 月 21 日
新增有關如何啟用 AMS 帶來自己的 EPS (BYOEPS) 功能的其他資訊。	新增有關如何啟用 AMS 帶來自己的 EPS (BYOEPS) 功能的其他資訊。	2024 年 6 月 5 日
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	2024 年 5 月 23 日

在 AWS Amplify 自助式佈建模式下使用自訂角色（僅限 MALZ 環境）新增的資訊。	新增說明，說明 MALZ 環境如何在 AWS Amplify 自助式佈建模式中搭配使用自訂角色。	2024 年 5 月 23 日
Amazon Kendra 現在可在自助式佈建模式中使用。	Amazon Kendra 現在可在自助式佈建模式中使用。	2024 年 5 月 23 日
AMS Advanced 支援其他作業系統。	AMS Advanced 支援 Red Hat Enterprise Linux (RHEL) 9.x 和 Ubuntu 20.04 和 22.04。	2024 年 4 月 25 日
AMS Advanced 支援 Amazon Linux 2 的 ARM64 架構。	AMS Advanced 支援 Amazon Linux 2 的 ARM64 架構。	2024 年 4 月 25 日
已更新從多帳戶登陸區域 (MALZ) 登陸區域帳戶區段的離線。	新增如何從多帳戶登陸區域移出應用程式和核心帳戶的詳細資訊。	2024 年 4 月 11 日
已更新：服務請求管理描述。	更新了服務描述主題中的服務請求管理描述。	2024 年 3 月 21 日
已更新：事件管理服務承諾區段。	新增 AMS 服務水準協議的連結。	2024 年 3 月 21 日
更新：服務請求管理的運作方式區段。	新增有關 AMS 如何處理包含功能請求或錯誤之服務請求的說明。	2024 年 3 月 21 日
更新：取得支援區段。	已更新取得支援區段，以包含新的帳單問題區段。	2024 年 3 月 21 日
更新：AMS 自動化 IAM 佈建	使用自訂拒絕清單資訊更新 AMS 自動化 IAM 佈建	2024 年 3 月 21 日

舊版更新

下表說明 2024 年 3 月之前 AMS 進階指南文件的重要變更。

變更	描述	連結
2024 年 2 月		
更新支援的作業系統	更新支援的作業系統以包含 SUSE Linux Enterprise Server 15 SP5。	請參閱 支援的組態
新增 AMS 中基準監控提醒的注意事項。	已新增備註，指出 EC2 非根磁碟區用量的警示預設為停用。	請參閱 AMS 中基準監控的提醒
已新增 AMS Event Router 區段至監控和事件管理。	新增討論 AMS 進階事件路由器的新章節。	請參閱 在 AMS 中使用 Amazon EventBridge 受管規則
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	請參閱 AMIs.csv-and-notes .02.2024
2024 年 2 月		
新增 AMS Advanced Amazon EventBridge 規則服務連結角色的新區段	在基礎設施安全區段中新增 AMS Advanced 的 Amazon EventBridge 規則服務連結角色的新區段。	請參閱 AMS Advanced 的 Amazon EventBridge 規則服務連結角色
更新自助式服務佈建模式章節	新增了自助式佈建模式中 Amazon Inspector 的新章節。	請參閱 Amazon Inspector Classic (AMS SSPS)
2024 年 1 月		
更新計劃事件管理 (PEM) 章節	新增其他詳細資訊和 FAW 至計劃事件管理 (PEM)。	請參閱 AWS Managed Services 中的計劃事件管理
新增 SSM Agent 自動安裝的新章節	在自動化 EC2 執行個體組態中新增 SSM Agent 自動安裝的新章節。	請參閱 SSM Agent 自動安裝

變更	描述	連結
新增 AWS Resilience Hub (AMS SSPS)	新增了新的 SSPS 服務。	請參閱 使用 AMS SSP AWS Resilience Hub 在您的 AMS 帳戶中佈建
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	請參閱 AMIs.csv-and-notes .01.2024
2023 年 12 月		
更新 AMS 中的直接變更模式	在 AMS 中將新的子區段直接變更模式使用案例新增至直接變更模式。	請參閱 AMS 中的直接變更模式
Updated AWS Amplify (AMS SSPS)	更新常見問答集，釐清需要接受風險才能請求 Amplify。	請參閱 使用 AMS SSP AWS Amplify 在您的 AMS 帳戶中佈建
New AWS Elastic Disaster Recovery (AMS SSPS)	新增新的 SSPS 服務	請參閱 使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 帳戶中佈建
新的 Amazon Managed Service for Prometheus (AMS SSPS)	新增新的 SSPS 服務	請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Managed Service for Prometheus
更新持續性管理的運作方式章節。	新增了新的子區段，即 AMS 備份監控和報告。	請參閱 持續性管理的運作方式
新的 Amazon DevOpsGuru (AMS SSPS)	新增新的 SSPS 服務	請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon DocumentDB (與 MongoDB 相容)

變更	描述	連結
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	請參閱 AMIs.csv-and-notes .12.2023
2023 年 11 月		
已更新 Amazon CloudWatch Synthetics (AMS SSPS)	更新 FAQs 以使用正確的角色名稱。	請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon CloudWatch Synthetics
已更新 Amazon API Gateway 自助式佈建模式	已將其他角色 customer_apigateway_cloudwatch_role 新增至 API Gateway 區段。	請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon API Gateway
已將新服務新增至自助式佈建模式	已 AWS Service Catalog AppRegistry 新增至自助式佈建模式區段	請參閱 使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 帳戶中佈建
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	請參閱 AMIs.csv-and-notes .11.2023
2023 年 9 月		
新增使用 Patch Orchestrator 的備註	已將下列注意事項新增至使用修補程式協調器章節： 「不會為作業系統不支援或在維護時段內停止的執行個體建立修補程式失敗提醒」	請參閱 AMS 中的修補程式管理
使用其他服務更新資料加密	新增服務至 AMS 中的資料加密。	請參閱 AMS 中的資料保護

變更	描述	連結
新增段落至 RFC 錯誤訊息。	新增新段落以新增建立服務請求連結。	請參閱 針對 AMS 中的 RFC 錯誤進行故障診斷
更正 IAM 角色名稱。	更正 IAM 角色名稱 customer_emr_cluster_autoscaling_role。	請參閱 AMS 中的自助式佈建模式
更新 baselone 監控資訊	移除兩個已棄用警示 RDSReadLatencyAlarm 和 RDSWriteLatencyAlarm 的參考。	請參閱 AMS 中基準監控的提醒
2023 年 8 月		
新增：AMS 安全事件回應	新增使用 AMS 安全事件回應的文件。	請參閱 AMS 中的安全事件回應
2023 年 7 月		
新增：自動 IAM 佈建	新增使用自動化 IAM 佈建的文件。	請參閱 自動化 IAM 佈建 AMS
已更新：存取角色資料表	新增 AMS Access 的缺少角色。	請參閱 AMS 客戶帳戶存取 IAM 角色
2023 年 6 月		
已更新：監控 RDS 警示的清單。	更新了 AMS 基準監控的 RDS 警示清單。新增了 9 種新的 RDS 警示類型，並移除了 3 種現有的 RDS 警示類型。	請參閱 AMS 中基準監控的提醒 。
已更新：存取角色資料表	AMS Security 的新角色。	請參閱 AMS 客戶帳戶存取 IAM 角色
2023 年 5 月		

變更	描述	連結
已更新：服務帳單開始日期政策。	更新帳單開始日期的定義。	請參閱 AMS 金鑰術語 。
2023 年 4 月		
更新：每月帳單自助服務報告。	新增的備註：每月帳單報告僅適用於管理付款人帳戶 (AMS 進階多帳戶登陸區域)，但適用於所有連結的 AMS Accelerate 受管帳戶。	請參閱 帳單報告 (每月) 。
已更新：移除「標準修補」內容	AMS 使用 Patch Orchestrator。	AMS 中的修補程式管理
已更新：什麼是 AMS？	將先前在什麼是 AMS？下的一些主題移動為 AMS 服務描述的一部分。	服務描述
更新：離職多帳戶登陸區域	進行各種釐清。	從 AMS 多帳戶登陸區域帳戶離職
已更新：AWS Transfer Family (AMS SSPS)	新增傳輸設定教學課程的連結。	使用 AMS SSP AWS Transfer Family 在您的 AMS 帳戶中佈建
更新內容：自助式佈建	將 "CodeSuite" 取代為每個 AWS 法務的 "Code Services"。	使用 AMS SSP 在您的 AMS 帳戶中佈建 AMS Code 服務
更新內容：CloudWatch 指標和警示	新增 範例的連結：計算詞彙的出現次數 。	在 AMS 中建立自訂 CloudWatch 指標和警示
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.04.2023

變更	描述	連結
2023 年 3 月		
更新內容：從 AMS 離職	釐清在離開多帳戶登陸區域帳戶時要刪除的資源	從 AMS 多帳戶登陸區域帳戶離職
已更新：AMS AMIs	在文件歷史記錄區段中新增了每月 AMI ZIP 檔案的連結。	文件歷史紀錄
更新：自動修復	已移除 EC2 磁碟區自動化的 LVM 支援。	AMS 自動修復提醒
更新：修補程式 RACI	RACI 的多次更新和澄清以進行修補。	AMS 責任矩陣 (RACI)
更新內容：自助式佈建	新增常見問答集項目符號。若要啟動新的 AWS Datasync 代理程式，不需要 WIGS 擷取。	AMS 中的自助式佈建模式
更新內容：自助式佈建	新增常見問答集項目符號。若要啟動新的 AWS Datasync 代理程式，不需要 WIGS 擷取。	AMS 中的自助式佈建模式
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.03.2023
2023 年 2 月		
更新內容：從 AMS 離職	釐清如何卸任多帳戶登陸區域環境、VPCs 和應用程式帳戶	離線 AMS 帳戶
更新內容：尋找 ARNs	新增 DynamoDB describe-table CLI 以尋找 DynamoDB 資料表 ARN	在 AMS 中尋找 Amazon Resource Name (ARNs)

變更	描述	連結
更新內容：自助式佈建	已移除 AMS "CodeSuite" 選項，因為它不是實際的 SSPS。您仍然可以使用管理 AWS 服務 自行佈建服務 新增 (需要檢閱) (ct-3qe6io8t6jtny) 變更類型，並請求三種服務：CodeBuild、Code Deploy 和 CodePipeline。然後，AMS 會將下列 IAM 角色佈建至您的帳戶：customer_codedeploy_service_role、customer_codebuild_service_role 和 aws_code_pipeline_service_role。在帳戶中佈建之後，您必須在聯合解決方案中加入角色。	AMS 中的自助式佈建模式
更新內容：Secrets Manager 更新	更正多帳戶登陸區域 (MALZ) 與單一帳戶登陸區域 (SALZ) 所需的角色。	使用 Secrets Manager 共用金鑰常見問答集
更新內容：提醒的 AMS 自動修復	新增對邏輯磁碟區管理員 (LVM) 磁碟區的支援。	EC2 磁碟區用量修復自動化
更新內容：AMS Amazon Machine Image AMIs)	新增了使用範本程式碼將 AMIs 從您的帳戶中移除的離職 AMS AMIs 一節。	AMS Amazon Machine Image AMIs)
更新內容：IAM 使用者角色	已更新 IAM 政策：AMSBillingPolicy。	AMS 中的 IAM 使用者角色
新內容：不支援 OSes	新增 AMS 為不支援的作業系統 (OSes) 提供哪些服務的相關資訊。	AMS 中不支援作業系統的功能

變更	描述	連結
更新內容：隨需報告	某些隨需報告在 AMS Advanced 中不可用，並被錯誤顯示為可用。	隨需報告
更新內容：使 AMS 帳戶離職	說明將 MALZ 應用程式帳戶移出的指示。	離線 AMS 應用程式帳戶
更新內容：Secrets Manager	更正使用 Secrets Manager 所需的 IAM 角色名稱。	AWS Managed Services 常見問答集中的 Secrets Manager
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.02.2023
2023 年 1 月		
新內容：AWS Device Farm (AMS SSPS)	新增新的 SSPS 服務：AWS Device Farm。	使用 AMS SSP AWS Device Farm 在您的 AMS 帳戶中佈建
已更新：支援的 Windows 版本	新增對 Windows Server 2022 的支援。	AMS Amazon Machine Image AMIs)、支援的組態與使用 SNS 的 AMS AMI 通知
更新：持續性管理	更新預設 AMS 備份計畫中的規則。	預設備份計畫，多帳戶登陸區域
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.01.2023
2022 年 12 月		
更新：使用堡壘	已修正錯誤的連結。	使用堡壘存取執行個體

變更	描述	連結
已更新：資源排程器	針對更多內容，進行了幾項改善，並新增了 AWS 執行個體排程器的連結。	AWS Managed Services 資源排程器
更新：Windows AMIs 和支援的組態（適用於新的 Windows AMIs）	已更新從 EC2Launch (Windows Server 2016 和更新版本) 新增至 EC2Launch (Windows Server 2016 和 Windows Server 2019) 並新增 EC2LaunchV2 (Windows Server 2022 和更新版本) 的 AMS AMI 內容。將 Windows 型 AMIs 從 Microsoft Windows Server (2012、2012 R2、2016 和 2019) 更新為 Microsoft Windows Server (2012、2012 R2、2016、2019 和 2022)。	AMS Amazon Machine Image AMIs 和 服務描述
已更新：資源排程器區段	改善了部署和自訂 AMS 資源排程器的方法。	AWS Managed Services 資源排程器
已更新：設定 upu AMS：私有和公有 DNS	更新 DNS 架構圖。	設定私有和公有 DNS
已更新：MALZ 網路架構	更新圖表並新增加速應用程式帳戶的指導方針。	MALZ 網路架構
已更新：設定：使用標籤	新備註：僅 MALZ 應用程式帳戶支援自訂標記，不支援核心帳戶。	AMS 基礎設施自動標記
更新：存取管理：使用堡壘	更新包含 RDP 堡壘的簡介。	節省單一帳戶登陸區域 (SALZ) 堡壘的成本

變更	描述	連結
已更新：AMS 預設設定：警示	新增 EC2 執行個體：警示資料表的非根磁碟區用量。	AMS 中基準監控的提醒
更新：持續性管理	新增有關連續備份的指引。	持續性管理的運作方式
更新：自動化 EC2 執行個體組態	新增對 PowerBroker Identity Service (PBIS) 和執行個體代碼 (OIC) 的支援。	在 Linux 執行個體上自動更新 PBIS 和 在 Linux 執行個體上自動更新程式碼
更新：Secrets Manager 的自助式佈建	更新 CT 以將 Secrets Manager 新增至您的帳戶（在 FAQs 下）。	使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建
更新：日誌管理	更新 EC2 系統層級日誌的清單。	Amazon Elastic Compute Cloud (Amazon EC2) - 系統層級日誌
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.12.2022
2022 年 11 月		
已更新：AMS Amazon Machine Image AMIs)	更新支援的 SUSE Linux 版本。	AMS Amazon Machine Image AMIs)
已更新：MALZ 帳戶	新增刪除客戶受管應用程式帳戶的指引。	客戶受管應用程式帳戶
已更新：設定 AMS	新增了 customer-ams-amazon2-security-enhanced。	使用 SNS 的 AMS AMI 通知
更新：監控的運作方式	更新服務通知和事件報告的說明。	監控的運作方式

變更	描述	連結
已更新：MALZ 應用程式帳戶類型	已改善帳戶類型的說明。	應用程式帳戶類型
已更新：開發人員模式	新增有關開發人員模式的警告。	開始使用 AMS 開發人員模式之前
更新：計劃事件管理	新增章節：PEM 的類型	AWS Managed Services 中的計劃事件管理
已更新：Amazon Machine Image AMIs)	更新支援的 SUSE Linux 版本	AMS Amazon Machine Image AMIs)
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.11.2022
2022 年 10 月		
新增：自動化執行個體組態	新章節說明自動化執行個體組態程序。	AMS Advanced 中的自動化執行個體組態
新增：某些 SSPS 只接受手動 CT	更新了超過 50 個自助式佈建服務 FAQs，以使用手動 CT，而不是新增 SSPS 的自動 CT。	AMS 中的自助式佈建模式
更新：設定 AMS	已將兩個政策新增至 MALZ 的 Amazon EC2 IAM 執行個體描述檔。	EC2 IAM 執行個體描述檔
新增：自訂偵測和預防性規則的程式庫。	根據我們對多位客戶的學習，新增了一組範例服務控制政策 (SCPs) 和預防性 Config 規則控制。	統籌 SCPs 和 Config 規則

變更	描述	連結
更新：AWS Backup 警告	新增警告：「請勿編輯 AMS 備份計畫，因為您的變更可能會遺失。反之，請為您的自訂組態使用 ct-2hyozbpa0sx0m 建立新的備份計畫。」	持續性管理的運作方式
Update：AWS Backup 注意	新增有關將新 IAM 角色新增至聯合的備註。	在 AMS Advanced 中部署 IAM 資源
更新：監控管理	提醒會產生事件報告，而不是服務請求。	監控的運作方式
更新：自備 EPS	適用於 SALZ 和 MALZ。	AMS 自備 EPS
更新：加速應用程式帳戶	釐清您的 Accelerate 帳戶是應用程式帳戶。	應用程式帳戶類型
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.10.2022
2022 年 9 月		
已更新：用於尋找資源的 CLI 命令範例	新增了新範例，並且可能需要 --region 選項。	尋找您需要的資料 (SKMS)、AMS
已更新：佈建 IAM 角色	IAM 角色現在可以使用 建立和管理AWSManagedServices CloudFormationAdminRole 。	使用直接變更模式建立堆疊
已更新：AMS 技術標準	AMS-STD-007 記錄：(#20) 釐清轉送要求。	安全與合規
更新：持續性管理的運作方式	已將開始備份任務措辭修訂為「隨需」而非「現有」。	持續性管理的運作方式

變更	描述	連結
更新：安全性與合規性	更新標準 AMS-STD-007 編號 20 的說明和指引：在帳戶之間轉送日誌。	安全與合規
更新：變更管理使用案例	移除舊版變更管理使用者指南的中斷連結。	變更管理使用案例
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.09.2022
2022 年 8 月 11 日		

變更	描述	連結
更新：一致性和可讀性的章節標題，將一些主題子區段移至更適當的區段	「MALZ 網路架構」和「SALZ 網路架構」現在都是最上層「網路架構」區段的子區段，先前是「AMS 網路架構」區段 「變更管理模式」是「變更管理」的新標題 「預設設定」現在是「設定 AMS」的子區段 「AD FS 宣告規則和 SAML 設定」（先前稱為「Active Directory Federation Services (ADFS) 宣告規則和 SAML 設定」）現在是「設定 AMS」的子節 「存取管理」是「在 AMS 中存取」的新標題，並在 TOC 中向上移動 「尋找您需要的資料」是「服務知識管理」的新標題 「報告和選項」是「AMS 報告」的新標題，在 TOC 中較低 「隨需操作」現在是 TOC 中的最後一個主題	什麼是 AWS Managed Services ?
已更新：問題清單和 ARN，新增：使用 ARN 尋找資源	這兩個程序都會完全重寫，以確保實用性。	在 AMS 中尋找 Amazon Resource Name (ARNs) 與在 AMS 中依 ARN 尋找資源。

變更	描述	連結
已更新：將您的 CMA 與 Transit Gateway 連線	自動化不支援將路由新增至核心路由網域，以及需要更新的程序。	將您的 CMA 與 Transit Gateway 連線
更新：MALZ 基本元件定價	所有價格均以美元為單位，格式為美元符號。	AMS 環境基本元件
更新：AMS AMI 備註	Zip 檔案包含最新 AMS Amazon 機器映像 AMIs) 的備註，以及最新 AMIs 的 CSV 檔案。	AMIs.csv-and-notes.08.2022
2022 年 7 月 14 日		
更新：自助式報告	新增使用 KMS 金鑰加密 AWS Glue 中繼資料的指示。	自助式報告
更新：AMS 基準監控	新增 DeleteRecoveryPoint 備份提醒。	AMS 中基準監控的提醒
更新：支援的作業系統	新增 Amazon Linux 2 的終止支援日期。	支援的組態
已更新：自助式佈建	新增 AWS Transfer SSPS 的先決條件。	使用 AMS SSP AWS Transfer Family 在您的 AMS 帳戶中佈建
更新：AMS 報告	新增選擇加入區域的注意事項。	報告和選項
更新：RFC 通訊和連接	釐清允許的文字檔案類型；特別是 YAML 檔案必須以 .yaml (而非 .yml) 結尾。	新增 RFC 通訊和附件 (主控台)
2022 年 6 月 21 日		

變更	描述	連結
已更新內容	先前稱為「變更管理模式」或「標準 CM 模式」的 AMS 模式現在稱為「RFC 模式」。模式區段已展開。	模式概觀 .
新警示	新增 AWS Backup 警示。	AMS 中基準監控的提醒
2022 年 6 月 16 日		
新內容	事件管理。AMS 現在可以在事件報告中獲得您的核准，解決不屬於安全風險的事件，而且不需要單獨的 RFC 和核准。	事件管理
已更新內容	MALZ：更新網路架構圖。更新：應移除主帳戶 VPC 對共用服務 vpc 的 VPC 對等互連，因為它不存在。	網路帳戶架構
	Sagemaker 自助式佈建服務 (SSPS)。更新了在加入時新增的新 IAM 角色，以供 Sagemaker 使用。	使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon SageMaker AI

變更	描述	連結
	若要列出 SNS 通知支援的 AMIs：新增 customer-ams-sles12、Customer-ams-sles15、Customer-ams-amazon1-security-enhanced、Customer-ams-rhel8-security-enhanced、Customer-ams-ubuntu18、Customer-ams-windows2012、Customer-ams-windows2019 和 customer-ams-windows2019-security-enhanced。已移除 customer-ams-rhel6 和 customer-ams-rhel6-security-enhanced AMIs。	使用 SNS 的 AMS AMI 通知
	已移除呈報電子郵件。	在 AWS Managed Services 中取得說明
	已將主題清單移至開啟段落下方。	什麼是 AWS Managed Services ?
	更新了服務日誌，提供更好的負載封鎖日誌連結，也會重新格式化。	AMS 彙總服務日誌
EKS 自助式佈建服務 (SSPS)。新增在叢集中啟用信封秘密加密的相關資訊。	使用 AMS SSP 在您的 AMS 帳戶中 AWS Fargate 佈建 Amazon EKS	
2022 年 6 月 9 日		
已更新內容、取得說明	已移除呈報路徑電子郵件。AMS 透過事件報告、服務請求和 RFCs 提供通訊方法。	在 AWS Managed Services 中取得說明

變更	描述	連結
2022 年 5 月 12 日		
新內容、隨需操作 (OOD) 訂閱模式	AMS 已將隨需操作加入從目前的註冊和續約模型變更為訂閱配置和預設選擇加入模型。當您加入 AMS 帳戶時，您現在會自動註冊隨需操作。	隨需操作
2022 年 4 月 14 日		
新內容、成本最佳化	AMS 提供成本最佳化的建議。	AWS Managed Services 中的成本最佳化
已更新內容，在 MALZ 中加速帳戶	不正確的角色名稱 (Customer DefaultAdminRole) 已更新為正確的角色名稱 (AccelerateDefaultAdminRole)。	AMS Accelerate 帳戶 「存取您的 Accelerate 帳戶」區段。
已更新內容、AMS 存取 IAM 角色	新增用於存取您帳戶的其他 AMS IAM 角色。	AMS 存取您帳戶的原因和時間 「AMS 客戶帳戶存取 IAM 角色」區段。
已更新內容、AMS 備份計畫	新增 AMS 受管備份計畫。	AMS 備份計畫 和 AMS 備份保存庫
已更新內容，AWS Secrets Manager	已更新常見問答集。	使用 AMS SSP AWS Secrets Manager 在您的 AMS 帳戶中佈建
已更新內容、直接變更模式 (DCM) 加入	AMS 不支援將 Service Catalog 客戶加入 DCM。	直接變更模式入門

變更	描述	連結
已更新內容，服務描述	釐清支援的 服務區段： • AWS Fargate 上的 Amazon EKS -> Fargate 上的 Amazon Elastic Kubernetes Service • Amazon ECS for Fargate -> AWS Fargate 上的 Amazon Elastic Container Service • Amazon Kinesis -> Amazon Kinesis Data Streams	支援 AWS 的服務
已更新內容、卸任 MALZ 帳戶	更新以參考新變更類型，用於卸任應用程式帳戶。	離線 AMS 應用程式帳戶
已更新內容、開發人員模式事件管理	更新事件 SLA 描述為：AMS SLA 不適用於在 AMS 變更管理（包含開發人員模式）之外建立或更新的資源，因此，在開發人員模式中更新或建立的資源會自動降級為 P3，且支援會盡最大努力。	AMS 開發人員模式下的事件管理
已更新內容、DCM 加入	新 DCM 的 RFC 範本現在包含 SAML 提供者 ARN 的欄位。	直接變更模式入門
已更新內容，適用於的 DCM AWS CloudFormation	建立和更新 AWS CloudFormation 堆疊的說明現在包含 YAML 範例。	AMS 轉換
已更新內容，MALZ Tools 帳戶	遷移有新的 IAM 角色：AWSManagedServices MigrationRole。	AWS Application Migration Service (AWS MGN) 和 啟用對新 AMS 工具帳戶的存取

變更	描述	連結
新內容、多帳戶登陸區域帳戶	您可以在多帳戶登陸區域 AMS 管理帳戶中建立 Accelerate 帳戶。	AMS Accelerate 帳戶
已更新內容、API/CLI SDK 安裝	安裝指示會列出 Mac/Linux 安裝錯誤的檔案名稱，以及不正確的命令。已修正此問題。	使用 AMS API 和 CLI
已更新內容，在 MALZ 中加速帳戶	規則名稱不正確 (Customer DefaultAdminRole)，它已更新為正確的規則名稱 (AccelerateDefaultAdminRole)。	AMS Accelerate 帳戶 ，「存取您的 Accelerate 帳戶」區段
更新內容、監控	根用量監控從 85% 修改為 95%。	AMS 中基準監控的提醒
已更新內容、AMI 通知	您可以為新的 AMS AMIs 建立許多類型的 SNS 通知，我們已新增有關建立各種類型的資訊。	使用 SNS 的 AMS AMI 通知
已更新內容、AMS 預設設定	移除 Macie Classic 的參考，由 Macie 取代。	AMS 中基準監控的提醒
已更新內容、AMS 預留字首	保留字首清單的字母排序。	AMS 預留字首
已更新內容，服務描述	變更管理和自助式佈建的功能區段已更新，並提供 AMS 模式的詳細資訊。	AWS Managed Services (AMS) AMS 進階操作計劃功能
已更新內容，AWS Secrets Manager	使用 Secrets Manager 共用金鑰。	2022 年 2 月 10 日

變更	描述	連結
新內容、自助式佈建、Amazon Connect	新增了常見問答集，說明如何請求新增撥出或撥入通話的國家/地區清單。	2022 年 2 月 10 日
新內容、自助式佈建、Amazon EKS on Fargate	新增了 AMS 不支援透過 AWS 雲端開發套件 (CDK) 或 CloudFormation Ingest 部署 EKS 叢集的常見問答集限制。	2022 年 2 月 10 日
已變更內容、開發人員模式	更正，您不使用 RFC 或服務請求將使用者指派給聯合解決方案，您可以根據您的解決方案自行執行此操作。	2022 年 2 月 10 日
變更內容、直接變更模式 (DCM)	請注意，DCM 不支援 IAM。	2022 年 2 月 10 日
	DCM，請注意我們所做的驗證。	2022 年 2 月 10 日
	DCM，釐清不同角色的限制。	2022 年 2 月 10 日
變更內容、監控基準提醒	Redshift 叢集資源提醒已變更。	2022 年 2 月 10 日
變更內容、自助式報告	新增了確切的 s3 儲存貯體名稱 (ams-reporting-data-a<Account_ID>)，供客戶用來擷取報告。	2022 年 2 月 10 日

變更	描述	連結
變更內容、更新內容以參考自動變更類型，而非手動管理 其他 其他 (MOO)	更新多帳戶登陸區域 (MALZ) 應用程式帳戶內容，以參考自動變更類型 (三、「將 TGW 連接與路由表關聯」、「在 TGW 路由表中建立路由以連接到此 VPC」，以及「將 VPC 路由表設定為指向 AMS 多帳戶登陸區域傳輸閘道」)。 接收 AMS 產生的提醒 標籤型提醒通知	2022 年 2 月 10 日
變更內容：AMS AMIs。	新增有關安全增強型 AMIs 新資訊。請參閱 支援的組態、AMS Amazon Machine Image AMIs 和 安全性增強 AMIs。	2022 年 1 月 27 日
新內容：自助式佈建。	新增 Amazon Fsx for OpenZFS。請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon FSx for OpenZFS。	2022 年 1 月 27 日
變更內容：程式碼部署自助式佈建服務 (SSPS)。	其他角色名稱和其他限制備註。請參閱 使用 AMS SSP AWS CodeDeploy 在您的 AMS 帳戶中佈建。	2022 年 1 月 27 日
變更內容：更新連結。	修正中斷的連結：AMS-AMIs 尋找設定、尋找堆疊 ID、尋找 VPC ID、ListVpcSummaries、ListStackSummaries 和 GetStack APIs。如需範例，請參閱 在 AMS 中尋找堆疊 IDs。	2022 年 1 月 13 日

變更	描述	連結
變更內容：EKS 支援 Fargate	新增對FAQs的限制：不支援使用 EKS 建立或管理 EC2 節點群組。請參閱 使用 AMS SSP 在您的 AMS 帳戶中 AWS Fargate 佈建 Amazon EKS。	2022 年 1 月 13 日
變更內容：CloudFormation、直接變更模式 (DCM)	新增使用 AmsStackTransform 建立或更新 CF 堆疊的指示。請參閱 使用直接變更模式建立堆疊。	2022 年 1 月 13 日
變更內容：AWS 服務名稱的一致性	AMS 參考 AWS 服務 完全符合官方 AWS 標題或中繼資料。先前，有一些次要變化符合複雜的模式。如需範例，請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Alexa for Business 。	2022 年 1 月 13 日
變更內容：彈性容器登錄檔 (ECR) 的自助式佈建	新增使用 ECR 管理使用者許可的常見問答集項目。請參閱 使用 AMS SSP 在您的 AMS 帳戶中佈建 Amazon Elastic Container Registry。	2022 年 1 月 13 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。