



使用者指南

AWS Organizations



AWS Organizations: 使用者指南

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

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

Table of Contents

什麼是 AWS Organizations ?	1
功能	2
使用案例	3
術語與概念	4
可用的功能集	5
組織結構	5
邀請和交握	8
組織政策	9
配額和服務限制	10
命名指導方針	10
考量事項	10
最大值和最小值	10
交握過期時間	14
您可以連接實體的政策數量	14
調節限制	16
區域支援	19
可用區域的清單	20
帳單和定價	24
付款責任	24
付款結構	24
支援和意見回饋	24
其他 AWS 資源	24
最佳實務	26
帳戶和登入資料	26
啟用根存取管理，以簡化管理成員帳戶的根使用者憑證	26
讓聯絡電話號碼維持在最新狀態	26
使用適用於所有根帳戶的群組電子郵件地址	27
組織結構和工作負載	27
在單一組織內管理您的帳戶	27
根據業務目的而非報告結構來群組工作負載	27
使用多個帳戶來組織您的工作負載	27
服務和成本管理	28
使用 AWS 服務主控台或 API/CLI 操作在組織層級啟用服務	28
使用帳單工具追蹤成本並最佳化資源用量	28

在組織資源中規劃標記策略並強制執行標籤	28
開始使用	29
註冊 AWS	29
註冊 AWS 帳戶	29
建立具有管理存取權的使用者	30
存取 AWS Organizations	31
教學：建立和設定組織	32
先決條件	33
步驟 1：建立您的組織	34
步驟 2：建立組織單位	36
步驟 3：建立服務控制政策	38
步驟 4：測試您組織的政策	43
教學課程：使用 Amazon EventBridge 監控組織	43
先決條件	44
步驟 1：設定追蹤記錄與事件選擇器	45
步驟 2：設定 Lambda 函數	46
步驟 3：建立傳送電子郵件給訂閱者的 Amazon SNS 主題	47
步驟 4：建立 Amazon EventBridge 規則	48
步驟 5：測試 Amazon EventBridge 規則	48
清除：移除不再需要的資源	50
使用 AWS SDKs	51
管理整個組織	52
建立組織	52
建立組織	52
驗證您的電子郵件地址	56
驗證電子郵件地址	57
重新傳送驗證電子郵件	57
變更您的電子郵件地址	57
啟用所有功能	58
考量事項	59
標準遷移程序	60
輔助遷移程序	68
檢視組織的詳細資訊	68
刪除組織	70
考量事項	70
刪除組織	71

管理組織中的帳戶	74
管理帳戶	74
管理帳戶的最佳實務	74
關閉管理帳戶	76
成員帳戶	77
成員帳戶最佳實務	77
建立成員帳戶	80
存取成員帳戶	85
關閉成員帳戶	90
保護成員帳戶以免遭關閉	92
移除成員帳戶	93
從成員帳戶離開組織	98
更新成員帳戶的帳戶名稱	101
更新成員帳戶的根使用者電子郵件	101
帳戶邀請	101
考量事項	102
傳送邀請	104
管理擱置的邀請	106
接受或拒絕邀請	111
遷移 帳戶	115
預遷移	115
遷移	118
遷移後	118
檢視帳戶的詳細資訊	119
匯出帳戶詳細資訊	120
匯出組織中所有 AWS 帳戶 的清單	121
更新帳戶的替代聯絡人	122
更新帳戶的主要聯絡人	122
AWS 區域 帳戶的更新	122
組織單位 (OUs)	123
OUs 的最佳實務	124
了解 AWS Organizations	124
建議的基礎 OUs	125
建議的額外 OUs	126
結論	127
導覽根目錄和樹狀目錄	128

檢視 OU 的詳細資訊	129
建立 OU	131
重新命名 OU	135
標記 OU	136
在 OUs 之間移動帳戶	138
檢視根的詳細資訊	139
刪除 OU	140
組織政策	144
政策類型	144
授權政策	144
管理政策	145
授權政策	147
SCPs和 RCPs之間的差異	147
使用 SCPs和 RCPs	147
服務控制政策	149
資源控制政策	197
管理政策	210
先決條件和許可	211
了解政策繼承	212
檢視有效政策	227
宣告式政策	229
備份政策	247
標籤政策	285
聊天應用程式政策	322
AI 服務選擇退出政策	335
Security Hub 政策	344
的委派管理員 AWS Organizations	353
建立以資源為基礎的委派政策	354
更新以資源為基礎的委派政策	358
檢視以資源為基礎的委派政策	363
刪除以資源為基礎的委派政策	363
啟用政策類型	365
停用政策類型	366
考量事項	366
停用政策類型	366
建立 政策	368

建立服務控制政策 (SCP)	368
建立資源控制政策 (RCP)	372
建立宣告政策	376
建立備份政策	378
建立標籤政策	382
建立聊天應用程式政策	386
建立 AI 服務選擇退出政策	390
建立 Security Hub 政策	392
更新政策	394
更新服務控制政策 (SCP)	395
更新資源控制政策 (RCP)	397
更新宣告政策	400
更新備份政策	402
更新標籤政策	405
更新聊天應用程式政策	408
更新 AI 服務選擇退出政策	410
更新 Security Hub 政策	413
編輯連接至政策的標籤	414
編輯連接至服務控制政策 (SCP) 的標籤	415
編輯連接至資源控制政策 (RCP) 的標籤	416
編輯連接至宣告政策的標籤	417
編輯連接至備份政策的標籤	418
編輯連接至標籤政策的標籤	420
編輯連接至聊天應用程式政策的標籤	421
編輯連接至 AI 服務選擇退出政策的標籤	422
編輯連接至 Security Hub 政策的標籤	423
連接政策	424
連接政策	424
分離政策	435
分離政策	435
取得政策詳細資訊	445
列出所有政策	446
列出連接的政策	450
列出所有連接	451
取得關於政策的詳細資訊	453
刪除政策	455

刪除政策	456
標記 資源	462
考量事項	462
使用標籤	463
新增、更新和移除標籤	463
建立資源時新增標籤	463
新增或更新現有資源的標籤	464
多方核准	466
使用其他 AWS 服務	467
啟用信任的存取所需的許可	467
停用信任的存取所需的許可	468
如何啟用或停用信任的存取	469
AWS Organizations 和服務連結角色	471
使用 AWSServiceRoleForDeclarativePoliciesEC2Report 服務連結角色	472
搭配 Organizations 運作的服務	472
AWS 帳戶管理	510
AWS Application Migration Service	513
AWS Artifact	518
AWS Audit Manager	521
AWS Backup	524
AWS 帳單與成本管理	526
AWS CloudFormation StackSets	528
AWS CloudTrail	531
Amazon CloudWatch	535
AWS Compute Optimizer	539
AWS Config	543
AWS 成本最佳化中心	545
AWS Control Tower	548
Amazon Detective	550
Amazon DevOps Guru	554
AWS Directory Service	557
Amazon Elastic Compute Cloud	559
Amazon Elastic Kubernetes Service	561
AWS Firewall Manager	563
Amazon GuardDuty	567
AWS Health	569

AWS Identity and Access Management	572
Amazon Inspector	574
AWS License Manager	578
AWS Managed Services (AMS) 自助服務報告 (SSR)	581
Amazon Macie	583
AWS Marketplace	585
AWS Marketplace 私有市場	588
AWS Marketplace 採購洞察儀表板	591
AWS Network Manager	594
Amazon Q Developer	597
AWS Resource Access Manager	598
AWS 資源總管	602
AWS Security Hub	605
Amazon S3 Storage Lens	608
AWS 安全事件回應	611
Amazon Security Lake	615
AWS Service Catalog	619
Service Quotas	623
AWS IAM Identity Center	624
AWS Systems Manager	628
AWS 使用者通知	632
標籤政策	634
AWS Trusted Advisor	635
AWS Well-Architected Tool	638
Amazon VPC IP 地址管理員 (IPAM)	641
Amazon VPC Reachability Analyzer	644
整合式 的委派管理員 AWS 服務	647
授與委派管理員帳戶的權限	648
安全	650
AWS PrivateLink	650
的限制和 的限制 AWS PrivateLinkAWS Organizations	651
建立一個 VPC 端點	651
建立 VPC 端點政策	652
身分和存取權管理	652
目標對象	653
使用身分驗證	653

使用政策管理存取權	656
AWS Organizations 如何使用 IAM	658
管理組織的存取許可	664
身分型政策範例	671
資源型政策範例	677
AWS 受管政策	685
包含標籤的以屬性為基礎的存取控制	689
故障診斷	693
日誌記錄和監控	695
AWS CloudTrail	695
Amazon EventBridge	705
法規遵循驗證	706
恢復能力	706
基礎架構安全	707
疑難排解	708
疑難排解一般問題	708
向 提出請求時，我會收到「存取遭拒」訊息 AWS Organizations	708
當我使用臨時安全憑證來發出請求時，出現「存取遭拒」訊息	708
嘗試以成員帳戶身分離開組織或以管理帳戶身分移除成員帳戶時遇到「存取遭拒」訊息	709
當我試著新增帳戶到我的組織時，出現「超過配額」訊息	709
我在新增或移除帳戶時遇到「此操作需要一段等待時間」訊息	709
嘗試新增帳戶到我的組織時遇到「組織仍在初始化」訊息	709
當我嘗試邀請帳戶加入我的組織時，收到「邀請已停用」訊息。	710
我所做的變更不一定都會立即顯示	710
當我嘗試存取已屬於組織的帳戶時，會收到「完成註冊」訊息	710
提出 HTTP 查詢請求	711
端點	711
必要的 HTTPS	711
簽署 AWS Organizations API 請求	712
程式碼範例	713
基本概念	713
動作	714
文件歷史紀錄	750
.....	dcclxi

什麼是 AWS Organizations ？

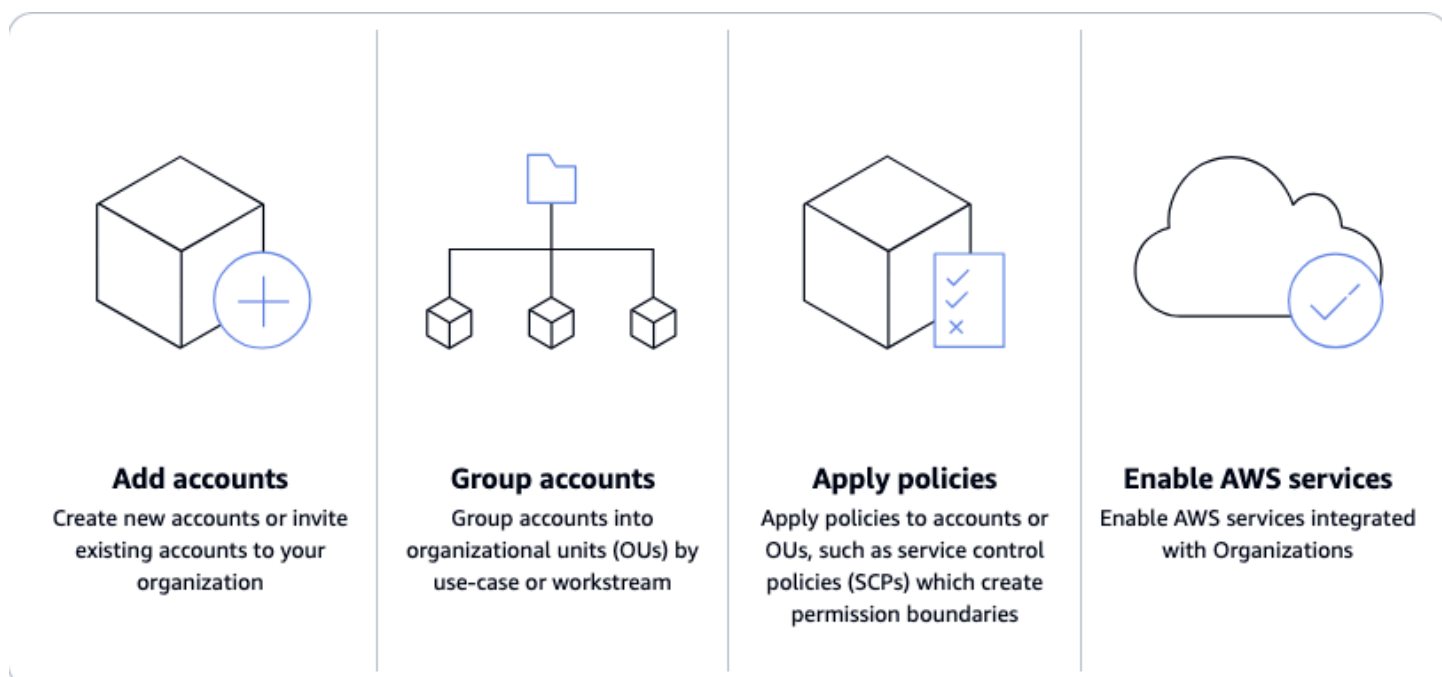
在擴展 AWS 資源時集中管理您的環境

AWS Organizations 可協助您在 AWS 資源成長和擴展時，集中管理和控管您的環境。使用 Organizations，您可以建立帳戶並配置資源、將帳戶分組以組織工作流程、套用控管政策，以及使用所有帳戶的單一付款方式簡化計費。

Organizations 與其他 整合 AWS 服務，因此您可以定義組織中帳戶之間的中央組態、安全機制、稽核需求和資源共用。如需詳細資訊，請參閱[與其他 AWS Organizations 搭配使用 AWS 服務](#)。

下圖顯示如何使用 的高階說明 AWS Organizations：

- 新增帳戶
- 群組帳戶
- 套用政策
- 啟用 AWS 服務。



主題

- [的功能 AWS Organizations](#)
- [的使用案例 AWS Organizations](#)

- [的術語和概念 AWS Organizations](#)
- [的配額和服務限制 AWS Organizations](#)
- [的區域支援 AWS Organizations](#)
- [的帳單和定價 AWS Organizations](#)
- [的支援和意見回饋 AWS Organizations](#)

的功能 AWS Organizations

AWS Organizations 提供下列功能：

管理您的 AWS 帳戶

AWS 帳戶 是許可、安全性、成本和工作負載的自然界限。在擴展雲端環境時，使用多帳戶環境是建議的最佳實務。您可以使用 AWS Command Line Interface (AWS CLI)、SDKs 或 APIs 以程式設計方式建立新帳戶，並集中佈建建議的資源和許可給使用 [AWS CloudFormation StackSets](#) 的帳戶，以簡化帳戶建立。

定義和管理組織

建立新帳戶時，您可以將它們分組為組織單位 (OUs)，或提供單一應用程式或服務的帳戶群組。套用標籤政策來分類或追蹤組織中的資源，並為使用者或應用程式提供屬性型存取控制。此外，您可以將支援的責任委派 AWS 服務給帳戶，讓使用者可以代表您的組織管理這些帳戶。

保護和監控您的帳戶

您可以集中提供工具和存取權給您的安全團隊，以代表組織管理安全需求。例如，您可以跨帳戶提供唯讀安全存取、使用 [Amazon GuardDuty](#) 偵測和緩解威脅、使用 [IAM Access Analyzer](#) 檢閱意外存取資源，以及使用 [Amazon Macie](#) 保護敏感資料。

控制存取和許可

設定 [AWS IAM Identity Center](#) 以使用作用中目錄提供對 AWS 帳戶和資源的存取，並根據個別任務角色自訂許可。您也可以將[組織政策](#)套用至使用者、帳戶或 OUs。例如，[服務控制政策 SCPs](#)可讓您控制對組織內 AWS 資源、服務和區域的存取。[資源控制政策 RCPs](#)可讓您集中防止意外使用 AWS 資源。[聊天應用程式政策](#)可讓您從 Slack 和 Microsoft Teams 等聊天應用程式控制對組織帳戶的存取。

跨帳戶共用資源

您可以使用 [AWS Resource Access Manager \(AWS RAM\)](#) 在組織內共用 AWS 資源。例如，您可以建立一次 [Amazon Virtual Private Cloud \(Amazon VPC\)](#) 子網路，並在組織中共用它們。您也

可以透過 集中同意軟體授權[AWS License Manager](#)，並透過 跨帳戶共用 IT 服務和自訂產品的目錄[AWS Service Catalog](#)。

稽核您的環境是否符合規範

您可以[AWS CloudTrail](#)跨帳戶啟用，這會建立雲端環境中所有活動的記錄，而成員帳戶無法關閉或修改。此外，您可以設定 政策，以使用 強制備份，[AWS Backup](#)或定義跨帳戶和 AWS 區域 的資源的建議組態設定[AWS Config](#)。

集中管理帳單和成本

Organizations 為您提供單一合併帳單。此外，您可以檢視跨帳戶資源的使用量，使用 追蹤成本[AWS Cost Explorer](#)，並使用 最佳化運算資源的使用量[AWS Compute Optimizer](#)。

的使用案例 AWS Organizations

以下是一些使用案例 AWS Organizations：

自動化工作負載的建立 AWS 帳戶 和分類

您可以自動建立 AWS 帳戶，以快速啟動新的工作負載。將帳戶新增至使用者定義的群組，以進行即時安全政策應用程式、非接觸式基礎設施部署和稽核。建立個別的群組，將開發和生產帳戶分類，並使用 [AWS CloudFormation StackSets](#) 為每個群組佈建服務和許可。

定義和強制執行稽核和合規政策

您可以套用服務控制政策 (SCPs)，以確保您的使用者僅執行符合您安全和合規要求的動作。使用 建立整個組織執行的所有動作的中央日誌[AWS CloudTrail](#)。檢視和強制執行跨帳戶和 AWS 區域 使用的標準資源組態[AWS Config](#)。使用 自動套用一般備份[AWS Backup](#)。使用 [AWS Control Tower](#) 為您的 AWS 工作負載套用安全、操作和合規的預先封裝控管規則。

為您的安全團隊提供工具和存取權，同時鼓勵開發

建立安全群組，並提供所有 資源的唯讀存取權，以識別和緩解安全問題。您可以允許該群組管理 [Amazon GuardDuty](#)，以便主動監控和緩解對工作負載的威脅，以及 [IAM Access Analyzer](#) 快速識別對 資源的意外存取。

跨帳戶共用常用資源

Organizations 可讓您輕鬆地跨帳戶共用重要的中央資源。例如，您可以共用您的中央，[AWS Directory Service for Microsoft Active Directory](#)讓應用程式可以存取您的中央身分存放區。

跨您的帳戶共用重要的中央資源

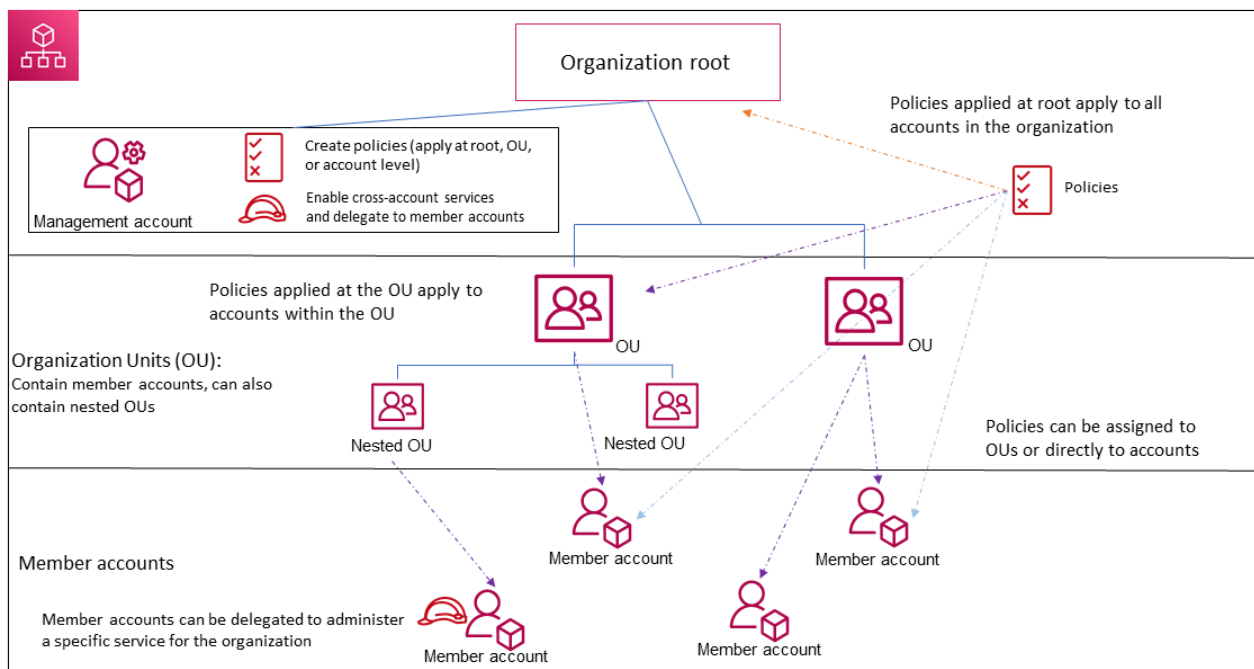
將 [AWS Directory Service for Microsoft Active Directory](#) 共用為應用程式的中央身分存放區。使用 [AWS Service Catalog](#) 在指定的帳戶中共用 IT 服務，讓使用者可以快速探索和部署核准的服務。透過集中定義一次應用程式資源，並使用 [\(\)](#) 在整個組織中共用，確保應用程式資源是在 [Amazon Virtual Private Cloud \(Amazon VPC\)](#) [AWS Resource Access Manager \(AWS RAM\)](#) 子網路上建立。

的術語和概念 AWS Organizations

本主題說明 的一些重要概念 AWS Organizations。

下圖顯示由五個帳戶組成的組織，這些帳戶在根目錄下組織成四個組織單位 (OUs)。組織也有數個政策連接到其中的部分 OU 或直接連接至帳戶。

對於每個項目的描述，請參閱本主題中的定義。



主題

- [可用的功能集](#)
- [組織結構](#)
- [邀請和交握](#)

- [組織政策](#)

可用的功能集

所有功能（建議）

所有功能都是 可用的預設功能集 AWS Organizations。您可以設定整個組織的中央政策和組態需求、在組織內建立自訂許可或功能、在單一帳單下管理和組織您的帳戶，以及代表組織將責任委派給其他帳戶。您也可以使用與其他 的整合 AWS 服務 來定義組織中所有成員帳戶的中央組態、安全機制、稽核需求和資源共用。如需詳細資訊，請參閱[與其他 AWS Organizations 搭配使用 AWS 服務](#)。

所有功能模式都提供合併帳單的所有功能以及管理功能。

合併帳單

合併帳單是提供共用帳單功能的功能集，但不包含 的更進階功能 AWS Organizations。例如，您無法讓其他 AWS 服務與您的組織整合，以跨其所有帳戶運作，或使用 政策來限制不同帳戶中的使用者和角色可以執行的操作。

您可以為原本僅支援合併帳單功能的組織啟用所有功能。若要啟用所有功能，所有獲邀請的成員帳戶必須透過接受在管理帳戶啟動程序時傳送的邀請來核准變更。如需詳細資訊，請參閱[使用 為組織啟用所有功能 AWS Organizations](#)。

組織結構

組織

組織是 的集合[AWS 帳戶](#)，您可以集中管理，並組織成階層式的樹狀結構，[其中根](#)位於根目錄頂端，而[組織單位](#)巢狀在根目錄下。每個帳戶都可以直接放在根帳戶中，或放在階層中的其中一個 OU 中。

每個組織包含：

- [管理帳戶](#)
- 零個或多個[成員帳戶](#)
- 零個或多個[組織單位 OUs](#)
- 零或多個[政策](#)。

組織具有的功能取決於您啟用的[功能集](#)。

根帳戶

管理[帳戶中包含管理根](#)（根），是組織的起點[AWS 帳戶](#)。根是組織階層中最上層的容器。在此根目錄下，您可以建立[組織單位 \(OUs\)](#)，以邏輯方式將帳戶分組，並將這些 OUs 組織到最符合您需求的階層中。

如果您將[管理政策](#)套用至根帳戶，則其會套用至所有[組織單位 OUs](#) 和[帳戶](#)，包括組織的管理帳戶。

如果您將授權政策（例如，服務控制政策 (SCP)）套用至根帳戶，則會套用至組織中的所有組織單位 (OUs) 和[成員帳戶](#)。它不適用於組織中的管理帳戶。

Note

建立組織時，您只能有一個 root. AWS Organizations automatic 為您建立根。

組織單位 (OU)

組織單位 (OU) 是[AWS 帳戶](#)組織內的群組。OU 也可以包含其他 OUs，讓您建立階層。例如，您可以將屬於相同部門的所有帳戶分組為部門 OU。同樣地，您可以將執行安全服務的所有帳戶分組為安全 OU。

當您需要將相同的控制項套用至組織中的帳戶子集時，OUs非常有用。巢狀 OUs可啟用較小的管理單位。例如，您可以為每個工作負載建立 OUs，然後在每個工作負載 OUs 中建立兩個巢狀 OU，以將生產工作負載從生產前分割出來。除了直接指派給團隊層級 OU 的任何控制項之外，這些 OU 還會繼承父系 OU OUs 的政策。包含[根](#)並在最低OUs 中 AWS 帳戶 建立，您的階層可以有五個層級的深度。

AWS 帳戶

AWS 帳戶 是 AWS 資源的容器。您可以在 中建立和管理 AWS 資源 AWS 帳戶，並提供存取和計費的 AWS 帳戶 管理功能。

使用多個 AWS 帳戶 是擴展您環境的最佳實務，因為它提供成本的帳單界限、隔離資源以確保安全、提供彈性或個人和團隊，以及適應新程序。

 Note

AWS 帳戶與使用者不同。[使用者](#)是您使用 AWS Identity and Access Management (IAM) 建立的身分，採用[具有長期憑證的 IAM 使用者](#)或[具有短期憑證的 IAM 角色](#)的形式。單一 AWS 帳戶可以且通常包含許多使用者和角色。

組織中有兩種類型的帳戶：指定為[管理帳戶](#)的單一帳戶，以及一或多個[成員帳戶](#)。

管理帳戶

管理帳戶是您 AWS 帳戶 用來建立組織的。從管理帳戶，您可以執行下列動作：

- 在組織中建立其他帳戶
- [邀請和管理](#)其他帳戶的邀請以加入您的組織
- 指定[委派管理員帳戶](#)
- 從組織移除帳戶
- 將政策連接到實體，例如[根](#)、[組織單位 \(OUs\)](#) 或組織內的帳戶
- 啟用與支援服務的整合 AWS，以跨組織中的所有帳戶提供服務功能。

管理帳戶是組織的最終擁有者，擁有對安全、基礎設施和財務政策的最終控制權。此帳戶具有付款人帳戶的角色，並負責支付其組織中帳戶產生的所有費用。

 Note

您無法變更組織中的哪個帳戶是管理帳戶。

成員帳戶

成員帳戶是 AWS 帳戶，管理帳戶除外，這是組織的一部分。如果您是組織的[管理員](#)，您可以在組織中建立成員帳戶，並邀請現有帳戶加入組織。您也可以將政策套用至成員帳戶。

 Note

成員帳戶一次只能屬於一個組織。您可以指定要委派管理員帳戶的成員帳戶。

委派的管理員

我們建議您僅將 管理帳戶及其使用者和角色用於必須由該帳戶執行的任務。我們建議您將 AWS 資源存放在組織內其他成員帳戶中，且將其保存在管理帳戶之外。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中任何使用者或角色。將資源與管理帳戶分開，也可協助您瞭解發票上的費用。從組織的管理帳戶中，您可以將一或多個成員帳戶指定為委派管理員帳戶以協助您實作此建議。委派管理員有兩種類型：

- Organizations 的委派管理員：您可以從這些帳戶管理組織政策，並將政策附加至組織內的實體 (根、OU 或帳戶)。管理帳戶可以在細微層級控制委派權限。如需詳細資訊，請參閱[委派管理員 AWS Organizations](#)。
- AWS 服務的委派管理員：您可以從這些帳戶管理與 Organizations 整合 AWS 的服務。管理帳戶可以根據需要將不同的會員帳戶註冊為委派管理員。這些帳戶具有特定服務的管理權限，以及 Organizations 唯讀動作的權限。如需詳細資訊，請參閱[AWS 服務 該 的委派管理員與 Organizations 搭配使用](#)

邀請和交握

邀請

邀請是由組織的管理帳戶向另一個[帳戶](#)提出的請求。例如，要求獨立帳戶加入[組織](#)的程序是邀請。

邀請會實作為[交握](#)。您在 AWS Organizations 主控台可能看不到交握。但是，如果您使用 AWS CLI 或 AWS Organizations API，則必須直接使用交握。

交握

交握是兩個 AWS 帳戶之間的安全資訊交換：寄件者和收件人。

支援下列交握：

- INVITE：交握傳送到獨立帳戶，以便加入寄件者的組織。
- ENABLE_ALL_FEATURES：交握已傳送至受邀成員帳戶，以啟用組織的所有功能。
- APPROVE_ALL_FEATURES：當所有受邀成員帳戶已核准啟用所有功能時，將交握傳送至管理帳戶。

您通常只有在使用 AWS Organizations API 或 等命令列工具時，才需要直接與交握互動 AWS CLI。

組織政策

政策是具有「一或多個陳述式」的「文件」，可定義您要套用至 群組的控制項 AWS 帳戶。AWS Organizations 支援授權政策和管理政策。

授權政策

授權政策可協助您集中管理 AWS 帳戶 整個組織的安全性。

服務控制政策 (SCP)

服務控制政策是一種政策類型，可集中控制組織中 IAM 使用者和 IAM 角色的可用許可上限。

這表示 SCPs 指定以主體為中心的控制項。SCPs 會建立許可護欄，或設定成員帳戶中主體可用的許可上限限制。當您想要對組織中的主體集中強制執行一致的存取控制時，您可以使用 SCP。

這可能包括指定您的 IAM 使用者和 IAM 角色可以存取的服務、他們可以存取的資源，或他們可以提出請求的條件（例如，來自特定區域或網路）。如需詳細資訊，請參閱 [SCPs](#)。

資源控制政策 (RCP)

資源控制政策是一種政策類型，可集中控制組織中資源的可用許可上限。

這表示 RCPs 指定以資源為中心的控制項。RCPs 會針對成員帳戶中資源可用的許可上限建立許可護欄或設定限制。當您想要在組織中跨資源集中強制執行一致的存取控制時，請使用 RCP。

這可能包括限制對資源的存取，以便只能由屬於您組織的身分存取，或指定組織外部身分可以存取您資源的條件。如需詳細資訊，請參閱 [RCPs](#)。

管理政策

管理政策可協助您集中設定和管理整個組織的 AWS 服務 及其功能。

宣告政策

宣告式政策是一種政策，可讓您集中宣告和強制執行整個組織中指定 AWS 服務 規模的所需組態。連接後，當服務新增新功能或 APIs 時，一律會維護組態。如需詳細資訊，請參閱 [宣告政策](#)。

備份政策

備份政策是一種政策類型，可讓您集中管理和將備份計劃套用至組織帳戶 AWS 的資源。如需詳細資訊，請參閱 [備份政策](#)。

標籤政策

標籤政策是一種政策類型，可讓您標準化連接至組織帳戶中 AWS 資源的標籤。如需詳細資訊，請參閱[標籤政策](#)。

聊天應用程式政策

聊天應用程式政策是一種政策類型，可讓您控制從 Slack 和 Microsoft Teams 等聊天應用程式對組織帳戶的存取。如需詳細資訊，請參閱[聊天應用程式政策](#)。

AI 服務選擇退出政策

AI 服務選擇退出政策是一種政策，可讓您控制組織中所有帳戶 AWS AI 服務的資料收集。如需詳細資訊，請參閱[AI 服務選擇退出政策](#)。

的配額和服務限制 AWS Organizations

本主題說明 的配額和服務限制 AWS Organizations。

命名指導方針

以下是您在其中建立的名稱準則 AWS Organizations，包括帳戶、組織單位 (OUs)、根和政策的名称：

- 名稱必須由 Unicode 字元組成。
- 名稱的最大字串長度因物件而異。如需有關每個物件實際限制的資訊，請參閱 [AWS Organizations API 參考](#)並尋找建立物件的 API 操作，並查看該操作Name參數的詳細資訊。例如：[Account name](#) (帳戶名稱) 或 [OU name](#) (OU 名稱)。

考量事項

由於更新，服務配額代碼可能會隨著時間而變更。這不會影響配額值或名稱。若要尋找特定配額的配額代碼，請使用 [ListServiceQuotas](#) 操作，並在您想要的配額輸出中尋找QuotaCode回應。

最大值和最小值

以下是 中實體的預設上限 AWS Organizations。

Note

請考慮下列 AWS Organizations 有關配額的資訊：

- 您可以使用 [Service Quotas 主控台](#)，請求增加某些值。
- AWS Organizations 除非另有說明，否則 限制適用於組織層級。許多配額僅適用於從 AWS Organizations 管理帳戶執行的動作。
- AWS Organizations 是一項全球服務，實際託管於美國東部（維吉尼亞北部）區域 (us-east-1)。因此，在使用 Service Quotas 主控台 AWS CLI、或 AWS SDK 時，您必須使用 us-east-1 來存取這些配額。

描述	限制
預設帳戶數量上限	10 – 組織中允許的預設帳戶上限。此配額可調整，而且可以使用 Service Quotas 主控台 增加。 注意：只有組織的管理帳戶可以提交此配額增加請求。根據客戶資格和要求，最多可授予 10,000 個帳戶提高限制。新建立的帳戶和組織可能會遇到低於預設值 10 個帳戶的配額。 傳送給帳戶的邀請計入此配額。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會退回計數。 當帳戶關閉時，在永久關閉之前，不會停止計入此配額。如需帳戶永久關閉時間的詳細資訊，請參閱《AWS 帳戶管理 參考指南》中的 關閉後期間。 有些服務的帳戶限制與組織中允許的帳戶數量上限不同。如需詳細資訊，請參閱 AWS 服務的限制。
移除已建立帳戶的最短存留期	每個支援的 區域：7 — 建立的帳戶必須存在的天數下限，然後才能將其從組織中移除。
組織中根帳戶的數量	1
組織中 OU 的數量	2000
組織中每個類型的政策數目	服務控制政策：10,000 資源控制政策：1000

描述	限制
	宣告政策：1000 備份政策：1000 標籤政策：1000 聊天應用程式政策：1000 AI 服務選擇退出政策：1000 Security Hub 政策：1000
政策文件的大小上限	服務控制政策：5120 個字元 資源控制政策：5120 個字元 宣告政策：10,000 個字元 備份政策：10,000 個字元 聊天應用程式政策：10,000 個字元 AI 服務選擇退出政策：2500 個字元 標籤政策：10,000 個字元 Security Hub 政策：10,000 個字元 注意：如果您使用 儲存政策 AWS Management Console，則 JSON 元素與引號外部之間的額外空格（例如空格和換行符號）會被移除且不計算在內。如果您使用 SDK 操作或 儲存政策 AWS CLI，則政策會完全按照您提供的方式儲存，而不會自動移除字元。
在根帳戶中形成巢狀的最大 OU 數量	在根帳戶下可以有 5 個層級的 OU。

描述	限制
您在 24 小時期間內可執行的邀請嘗試上限	您的組織允許的帳戶為 20 或數目上限，以較大者為準。已接受的邀請不會計入此限制之內。一旦有邀請被接受，當天即可以傳送另一個邀請。 如果組織中允許的帳戶數目上限少於 20，如果您嘗試邀請的帳戶超過組織所能包含的帳戶數目時，則會出現「超出帳戶限制」例外狀況。不過，您可以在一天內取消邀請並傳送新邀請，最多可嘗試 20 次。
您可以同時建立的成員帳戶數量	5 個 – 一旦一個完成，您便可以開始另一個，但一次只能有 5 個進行中。
您可以在 30 天內關閉的帳戶數量	組織中 10% 的成員帳戶，上限為 1000。此配額不可調整。 • 小於 100 個帳戶 – 您最多可以關閉 10 個成員帳戶 • 100 - 10,000 個帳戶 – 您可以關閉最多 10% 的成員帳戶 • > 10,000 個帳戶 – 您可以關閉最多 1000 個成員帳戶 達到此配額後，您可以關閉其他帳戶或等待配額重設。如需詳細資訊，請參閱 《AWS 帳戶管理指南》中的關閉AWS 帳戶。
您可以同時關閉的成員帳戶數量	3 個，一次只能關閉三個帳戶。完成後，您便可關閉另一個帳戶。
您可以連接政策的目標實體數目	無限制
您可以連接至根、OU 或帳戶的標籤數目	50
以資源為基礎的委派政策大小上限	40,000 個字元

依 AWS 服務劃分的限制

大多數 AWS 服務 支援您在組織中可以擁有的指定帳戶數量上限。不過，某些服務的帳戶限制與組織中允許的帳戶數量上限不同。

下表顯示具有個別帳戶限制的服務。

AWS 服務	限制	可以提高
AWS IAM Identity Center	3000	是
AWS Application Migration Service	5000	否
AWS Directory Service	250	是

如需詳細資訊，請參閱《IAM Identity Center 使用者指南》中的[AWS IAM Identity Center 配額](#)和《Application Migration Service 使用者指南》中的[AWS MGN 服務配額限制](#)。

交握過期時間

以下是 中交握的逾時 AWS Organizations。

描述	限制
邀請加入組織	15 天
請求啟用組織中的所有功能	90 天
刪除交握並且不再顯示在清單中	完成交握之後的 30 天

您可以連接實體的政策數量

下限和上限取決於政策類型和您要連接政策的目標實體。下表顯示每個政策類型，以及您可以連接每個類型的目標實體數量。

Note

這些數目只適用於那些直接連接至 OU 或帳戶的政策。透過繼承影響 OU 或帳戶的政策並未根據這些限制計數。所有政策限制都是硬性限制。

Policy type (政策類型)	連接至實體的數目下限	連接至根的數目上限	每個 OU 的連接數目上限	每個帳戶的連接數目上限
服務控制政策	1 — 當您啟用 SCP 時，每個實體都必須隨時連接至少一個 SCPs。您無法從實體移除最後一個 SCP。	5	5	5
資源控制政策	1 — 當您啟用 RCPs 時，RCPFullAWSAccess 政策會自動連接到根帳戶、每個 OU 和組織中的每個帳戶。您無法分離此政策，且會計入 5 個政策配額。	5	5	5
宣告政策	0	10	10	10
備份政策	0	10	10	10
標籤政策	0	10	10	10
聊天應用程式政策	0	5	5	5
AI 服務選擇退出政策	0	5	5	5
Security Hub 政策	0	10	10	10

 Note

組織中只能有一個根。

調節限制

下表依管理類別列出 AWS Organizations APIs，並在帳戶和組織層級顯示其各自的調節速率。

AWS Organizations 使用[字符儲存貯體演算法](#)來實作 API 限流。透過此演算法，您的帳戶會有一個儲存貯體，其中包含特定數量的字符。儲存貯體中的字符數量代表您在任何指定秒的限流配額。

速率是字符每秒新增到字符儲存貯體的固定速度。

爆量是可新增的字符數量上限，以及每秒可使用的字符數量上限。

例如，DescribeAccountAPI 的基準速率限制為每秒 1 AWS 帳戶 到 20 個請求，爆量速率限制為每秒 30 個請求。每秒 30 個請求的爆量速率可讓您暫時超過每秒 20 個請求的基準速率。

您可以在第一秒提出 20 個請求，也就是基準率。在接下來的一秒，您可以提出 30 個請求，超過基準但保持在 30 的爆量率內。不過，在第三秒內，如果您嘗試提出超過 20 個請求，將會調節您，因為您已超過基準速率且已使用高載容量。

高載速率可讓您在不受調節的情況下處理流量中的暫時峰值，只要每秒的平均請求隨著時間保持在基準限制內。

帳戶管理限制

下表列出帳戶管理 AWS Organizations APIs。

AWS Organizations API	每個帳戶限制（速率、爆量）	每個組織限制（速率、爆量）
CloseAccount	.05、1	
CreateAccount、CreateGovCloudAccount	0.1、3	
DescribeAccount	20、30	24、36
DescribeCreateAccountStatus	2、2	2、3
LeaveOrganization	1、1	
ListCreateAccountStatus	5、8	6、10

交握管理限制

下表列出帳戶交握 AWS Organizations APIs。

AWS Organizations API	每個帳戶限制 (速率、爆量)	每個組織限制 (速率、爆量)
AcceptHandshake	1、2	5、5
DescribeHandshake	1、2	6、10
CancelHandshake	2、3	
DeclineHandshake	1、1	5、5
InviteAccountToOrganization	3、5	
ListHandshakesForAccount、ListHandshakesForOrganization	5、8	6、10

組織管理限制

下表列出組織管理 AWS Organizations APIs。

AWS Organizations API	每個帳戶限制 (速率、爆量)	每個組織限制 (速率、爆量)
CreateOrganization、DeleteOrganization、EnableFullControl	1、1	
CreateOrganizationalUnit、DescribeOrganization	1、2	
MoveAccount、UpdateOrganizationalUnit、DeleteOrganizationalUnit	2、3	
DescribeOrganizationalUnit	2、2	2、3
ListAccounts	8、12	9、15

AWS Organizations API	每個帳戶限制 (速率、爆量)	每個組織限制 (速率、爆量)
ListChildren	6、10	7、12
ListParents、ListAccountsForParent、ListOrganizationalUnitsForParent	5、8	6、10
ListRoots	1、2	1、3
ListTagsForResource	10、15	12、18
RemoveAccountFromOrganization	2、2	
TagResource、UntagResource	4、6	

政策管理限制

下表列出政策管理 AWS Organizations APIs。

AWS Organizations API	每個帳戶限制 (速率、爆量)	每個組織限制 (速率、爆量)
CreatePolicy、DeletePolicy、AttachPolicy、DetachPolicy	2、3	
DescribePolicy	2、2	2、3
DisablePolicyType、EnablePolicyType	1、1	
ListPolicies、ListPoliciesForTarget、ListTargetsForPolicy	5、8	6、10
UpdatePolicy	2、3	

服務管理限制

下表列出服務管理 AWS Organizations APIs。

AWS Organizations API	每個帳戶限制 (速率、爆量)	每個組織限制 (速率、爆量)
EnableAWSServiceAccess、DisableAWSServiceAccess	1、2	
ListAWSServiceAccessForOrganization、ListDelegatedServicesForAccount	1、3	1、4
ListDelegatedAdministrators	5、8	6、10
RegisterDelegatedAdministrator、DeregisterDelegatedAdministrator	1、2	

的區域支援 AWS Organizations

AWS Organizations 適用於所有 AWS 商業區域 AWS GovCloud (US) Regions和中國區域。

如需 中的功能差異清單 AWS GovCloud (US) Regions，請參閱 [AWS Organizations 中的 AWS GovCloud \(US\)](#)。

如需中國區域的功能差異清單，請參閱[AWS Organizations 中國的](#)。

Organizations 的服務端點位於：

- 美國東部（維吉尼亞北部）的商業組織
- AWS GovCloud (US) 組織的 In AWS GovCloud（美國西部）
- 中國組織的中國（寧夏），由寧夏西部雲端資料技術公司營運。 Ltd (NWCD)。

所有組織實體都可以全域存取，但中國管理的組織除外，類似於 AWS Identity and Access Management (IAM) 現在的運作方式。當您建立和管理組織 AWS 區域時，您不需要指定，但您需要

為中國使用的 帳戶建立個別的組織。您 中的使用者可以 AWS 服務 在提供服務的任何地理區域 AWS 帳戶 使用。

Note

標籤政策僅在區域子集中受支援

標籤政策是協助您將組織帳戶中各資源的標籤標準化的一種政策。標籤政策僅在支援 Organizations 的 區域子集中支援。如需支援標籤政策的區域清單，請參閱[標籤政策 | 支援區域](#)。

可用的 清單 AWS 區域

下表列出所有可用的 AWS 區域。

區域名稱	區域	端點	通訊協定
美國東部 (俄亥俄)	us-east-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
美國東部 (維吉尼亞北部)	us-east-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
美國西部 (奧勒岡)	us-west-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
非洲 (開普敦)	af-south-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
亞太區域 (香港)	ap-east-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS

區域名稱	區域	端點	通訊協定	
亞太區域 (海德拉巴)	ap-south-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (雅加達)	ap-southeast-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太地區 (馬來西亞)	ap-southeast-5	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (墨爾本)	ap-southeast-4	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (孟買)	ap-south-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (大阪)	ap-northeast-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (首爾)	ap-northeast-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (新加坡)	ap-southeast-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (雪梨)	ap-southeast-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	

區域名稱	區域	端點	通訊協定	
亞太區域 (台北)	ap-east-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (泰國)	ap-southeast-7	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
亞太區域 (東京)	ap-northeast-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
加拿大 (中部)	ca-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
加拿大西部 (卡加利)	ca-west-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
歐洲 (法蘭克福)	eu-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
歐洲 (愛爾蘭)	eu-west-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
歐洲 (倫敦)	eu-west-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
歐洲 (米蘭)	eu-south-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
歐洲 (巴黎)	eu-west-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	

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

區域名稱	區域	端點	通訊協定
AWS GovCloud (美國西部)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS

的帳單和定價 AWS Organizations

AWS Organizations 免費提供。您只需支付成員帳戶中使用者和角色使用 AWS 的資源費用。例如，您需針對您的成員帳戶中的使用者或角色使用的 Amazon EC2 執行個體支付標準費用。如需其他服務定價的資訊 AWS，請參閱[AWS 定價](#)。

誰會支付我組織中 AWS 成員帳戶下使用者所產生的用量？

[管理帳戶](#)的擁有者負責支付組織中帳戶使用的所有用量、資料和資源。

我的帳單是否反映我在組織中建立的組織單位結構？

您的帳單不會反映您在組織中定義的結構。您可以在個人中使用[成本分配標籤](#) AWS 帳戶 來分類和追蹤您的 AWS 成本，而此分配會顯示在組織的合併帳單中。

的支援和意見回饋 AWS Organizations

我們誠摯歡迎您提供意見回饋。您可將意見傳送至 feedback-awsorganizations@amazon.com。您也可以將意見回饋和問題發佈到 [AWS Organizations 支援論壇](#)。如需 AWS 支援論壇的詳細資訊，請參閱[論壇說明](#)。

其他 AWS 資源

- [AWS 訓練和課程](#) – 角色型和特殊課程的連結，以及可自行安排進度的實驗室，以協助強化您的 AWS 技能並取得實際經驗。
- [AWS 開發人員工具](#) – 連結至開發人員工具與資源，其提供文件、程式碼範例、版本備註與其他資訊，以協助您使用 AWS 來建置創新的應用程式。
- [AWS 支援中心](#) – 建立和管理 AWS 支援案例的中樞。同時包含與其他實用資源的連結，例如論壇、常見技術問答集、服務運作狀態，以及 AWS Trusted Advisor。

- [AWS 支援](#) – Support 相關資訊的主要網頁 AWS ，這是一個one-on-one、快速回應的支援管道，可協助您在雲端中建置和執行應用程式。
- [聯絡我們](#) – 有關 AWS 帳單、帳戶、事件、濫用和其他問題的查詢的中央聯絡窗口。
- [AWS 網站條款](#) – 有關我們的著作權和商標、您的帳戶、授權和網站存取，以及其他主題的詳細資訊。

多帳戶環境的最佳實務

請遵循這些建議，協助您逐步設定和管理多帳戶環境 AWS Organizations。

主題

- [帳戶和登入資料](#)
- [組織結構和工作負載](#)
- [服務和成本管理](#)

帳戶和登入資料

啟用根存取管理，以簡化管理成員帳戶的根使用者憑證

我們建議您啟用根存取管理，以協助您監控和移除成員帳戶的根使用者憑證。根存取管理可防止復原根使用者憑證，從而改善組織中的帳戶安全性。

- 移除成員帳戶的根使用者憑證，以防止 登入根使用者。這也可防止成員帳戶復原根使用者。
- 擔任特殊權限工作階段，在成員帳戶上執行下列任務：
 - 移除設定錯誤的儲存貯體政策，此政策拒絕所有主體存取 Amazon S3 儲存貯體。
 - 刪除拒絕所有主體存取 Amazon SQS 佇列的 Amazon Simple Queue Service 資源型政策。
 - 允許成員帳戶復原其根使用者憑證。有權存取成員帳戶根使用者電子郵件收件匣的人員可以重設根使用者密碼，並以成員帳戶根使用者身分登入。

啟用根存取管理後，新建立的成員帳戶預設是secure-by-default，沒有根使用者憑證，因此不需要額外的安全性，例如佈建後的 MFA。

如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[集中成員帳戶的根使用者憑證](#)。

讓聯絡電話號碼維持在最新狀態

若要復原對您的存取權 AWS 帳戶，請務必擁有有效且作用中的聯絡電話號碼，以允許您接收文字訊息或通話。我們建議您使用專用電話號碼，以確保 AWS 可以聯絡您以取得帳戶支援和復原。您可以透過 AWS Management Console 或帳戶管理 APIs 輕鬆檢視和管理您的帳戶電話號碼。

有多種方式可以取得專用電話號碼，確保 AWS 可以與您聯絡。我們強烈建議您購買專用的 SIM 卡和實體電話。長期安全地存放手機和 SIM 卡，確保電話號碼仍可用於帳戶復原。還要確保負責行動帳單的團隊瞭解此號碼的重要性，即使號碼長時間不使用。您必須在組織內將此電話號碼保密以獲得額外的保護。

在 AWS 聯絡資訊主控台頁面中記錄電話號碼，並與組織中必須知道該電話號碼的特定團隊分享其詳細資訊。此方法有助於將電話號碼轉移到其他 SIM 卡的相關風險降至最低。根據您現有的資訊安全政策存放手機。不過，請勿將手機存放在與其他相關憑證資訊相同的位置。應記錄並監控任何對手機的存取或其儲存位置。如果與帳戶關聯的電話號碼有所更動，請實作程序以更新現有文件中的電話號碼。

使用適用於所有根帳戶的群組電子郵件地址

使用由您的企業管理的電子郵件地址。使用電子郵件地址，直接將收到的訊息轉寄給使用者群組。如果 AWS 必須聯絡帳戶的擁有者，例如，為了確認存取，電子郵件訊息會分發給多方。這種方法有助於減少回應延遲的風險，即使個人在度假、請病假或離開公司。

組織結構和工作負載

在單一組織內管理您的帳戶

我們建議您建立單一組織，並管理您在此組織內的所有帳戶。組織是一種安全性界限，可讓您在環境中維持各個帳戶之間的一致性。您可以跨組織內的帳戶集中套用政策或服務層級組態。如果您想要在多帳戶環境中啟用一致的政策、集中式可見性和程式設計控制，最好在單一組織中達成此目標。

根據業務目的而非報告結構來群組工作負載

我們建議您將生產工作負載環境和資料隔離在頂層工作負載導向 OU 下。您的 OU 應以一組通用的控制項為基礎，而非仿照公司的報告結構。除了生產 OU 之外，我們建議您定義一或多個非生產 OU，其中包含用於開發和測試工作負載的帳戶和工作負載環境。如需其他指引，請參閱「[組織以工作負載為導向的 OU](#)」。

使用多個帳戶來組織您的工作負載

為您的 AWS 資源 AWS 帳戶 提供自然安全、存取和計費界限。使用多個帳戶有好處，因為它可以讓您分配帳戶級別配額和 API 請求率限制，並且享有此處列出的[其他好處](#)。我們建議您使用一些[全組織的基本帳戶](#)，例如安全性、記錄和基礎架構的帳戶。對於工作負載帳戶，您應該在[不同帳戶中將生產工作負載與測試/開發工作負載分開](#)。

服務和成本管理

使用 AWS 服務主控台或 API/CLI 操作在組織層級啟用服務

最佳實務是，建議您 AWS Organizations 使用服務主控台或 API 操作/CLI 命令對等項目，啟用或停用您想要與整合的任何服務。使用此方法，AWS 服務可以為您的組織執行所有必要的初始化步驟，例如建立任何必要的資源，並在停用服務時清除資源。AWS 帳戶管理 是唯一需要使用 AWS Organizations 主控台或 APIs 啟用的服務。若要檢閱與整合的服務清單 AWS Organizations，請參閱 [AWS 服務 您可以搭配 使用 AWS Organizations](#)。

使用帳單工具追蹤成本並最佳化資源用量

管理組織時，您會收到一份合併帳單，其中涵蓋了組織中帳戶的所有費用。對於需要存取成本可見度的企業使用者，您可以在管理帳戶中提供具有受限唯讀權限的角色來檢閱帳單和成本工具。例如，您可以 [建立可存取帳單報告的權限集](#)，或使用 AWS Cost Explorer Service (檢視一段時間內成本趨勢的工具) 和成本效益服務 (例如 [Amazon S3 Storage Lens](#) 和 [AWS Compute Optimizer](#))。

在組織資源中規劃標記策略並強制執行標籤

隨著帳戶和工作負載的擴展，標籤對於成本追蹤、存取控制和資源管理來說是一項實用的功能。對於標記命名策略，請遵循[標記 AWS 資源](#)中的指導。除了資源之外，您還可以在組織根目錄、帳戶、OU 和政策上建立標籤。請參閱「[擬定您的標記策略](#)」以取得其他資訊。

入門 AWS Organizations

下列主題提供的資訊可協助您開始使用 AWS Organizations。您也可以使用下列教學課程，開始使用執行任務 AWS Organizations。

[教學：建立和設定組織](#)

依據逐步說明立即開始建立您的組織、邀請第一位成員帳戶加入、建立包含您的帳戶的 OU 階層，並且套用部分服務控制政策 (SCP)。

[教學課程：使用 Amazon EventBridge 監控您組織的重要變更](#)

當您指定的動作在組織內發生時，設定 Amazon EventBridge 來觸發以電子郵件形式、SMS 文字訊息或日誌項目顯示的警示電子郵件，以監控組織內的金鑰變更。例如，許多組織希望在建立新帳戶時、或是當帳戶嘗試離開組織時收到通知。

主題

- [註冊 AWS](#)
- [存取 AWS Organizations](#)
- [教學：建立和設定組織](#)
- [教學課程：使用 Amazon EventBridge 監控您組織的重要變更](#)
- [AWS Organizations 搭配 AWS SDK 使用](#)

註冊 AWS

主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。

2. 請遵循線上指示進行。

註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者[AWS Management Console](#)身分登入。在下一頁中，輸入您的密碼。

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

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的[為您的 AWS 帳戶 根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的[使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

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

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

- 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

- 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

存取 AWS Organizations

您可以透過下列 AWS Organizations 任何方式使用：

AWS Management Console

[AWS Organizations 主控台](#)是瀏覽器型界面，可用來管理組織和資源 AWS。您可以使用主控台在您的組織中執行任何任務。

AWS 命令列工具

使用 AWS 命令列工具，您可以在系統的命令列發出命令，以執行 AWS Organizations 和 AWS 任務。使用命令列比使用主控台更快、更方便。若您想要建構執行 AWS 任務的指令碼，命令列工具也非常實用。

AWS 提供兩組命令列工具：

- [AWS Command Line Interface](#)

AWS Command Line Interface (AWS CLI) 是管理 的統一工具 AWS 服務。只需一個工具即可下載和設定，您可以從命令列控制多個 AWS 服務，並透過指令碼將其自動化。

如需安裝和使用 的詳細資訊 AWS CLI，請參閱[AWS Command Line Interface 《使用者指南》](#)。

- [AWS Tools for Windows PowerShell](#)

適用於 Windows PowerShell 的工具可讓開發人員和管理員在 PowerShell 指令碼環境中管理其 AWS 服務和資源。您可以使用用來管理 Windows、Linux 和 MacOS 環境的相同 PowerShell 工具來管理您的 AWS 資源。

如需安裝和使用 Tools for Windows PowerShell 的詳細資訊，請參閱 [AWS Tools for Windows PowerShell 使用者指南](#)。

AWS SDKs

AWS SDKs 由各種程式設計語言和平台（例如 Java、Python、Ruby、.NET、iOS 和 Android）的程式庫和範本程式碼組成。SDK 會負責的工作諸如以密碼演算法簽署請求、管理錯誤以及自動重試請求。如需 AWS SDKs 的詳細資訊，包括如何下載和安裝，請參閱 [適用於 Amazon Web Services 的工具](#)。

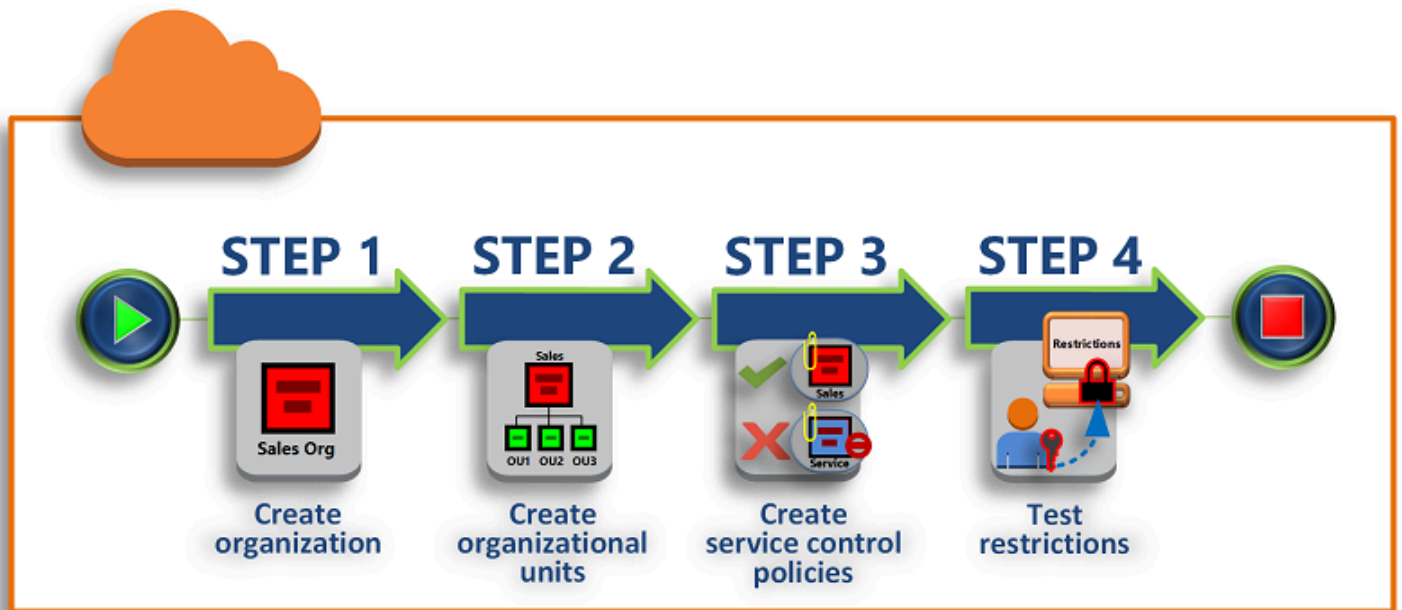
AWS Organizations HTTPS 查詢 API

AWS Organizations HTTPS 查詢 API 可讓您以程式設計方式存取 AWS Organizations 和 AWS。HTTPS 查詢 API 可讓您直接向該服務發出 HTTPS 請求。當您使用 HTTPS API 時，必須包含使用您的憑證來數位簽署請求的程式碼。如需詳細資訊，請參閱 [執行 HTTP 查詢請求來呼叫 API](#) 和 [AWS Organizations API 參考](#)。

教學：建立和設定組織

在本教學課程中，您會建立您的組織，並使用兩個 AWS 成員帳戶進行設定。您會在您的組織中建立其中一個成員帳戶，及邀請其他帳戶加入您的組織。接著，您會使用 [允許清單](#) 技術，以指定帳戶管理員僅可以委派明確列出的服務和動作。這可讓管理員驗證 AWS 引進的任何新服務，再允許公司內的任何其他人員使用。如此一來，如果 AWS 引入新的服務，則仍然禁止，直到管理員將服務新增至適當政策中的允許清單。本教學課程也說明如何使用 [拒絕清單](#)，以確保成員帳戶中的使用者可以變更所 AWS CloudTrail 建立稽核日誌的組態。

下圖顯示教學的主要步驟。



步驟 1：建立您的組織

在此步驟中，您會使用目前的 AWS 帳戶 做為管理帳戶來建立組織。您也可以邀請一個 AWS 帳戶加入您的組織，並將第二個帳戶建立為成員帳戶。

步驟 2：建立組織單位

接著，您可以在新組織中建立兩個組織單位 (OU)，並將這些成員帳戶放入 OU 中。

步驟 3：建立服務控制政策

您可以使用[服務控制政策 \(SCP\)](#)，將限制套用到可委派給成員帳戶中使用者及角色的動作。在此步驟中，您會建立兩個 SCP 並將他們連接到組織中的 OU。

步驟 4：測試您組織的政策

您可以以使用者身分從各測試帳戶登入，查看 SCP 對帳戶產生的影響。

本教學課程中的所有步驟都不會產生 AWS 帳單費用。AWS Organizations 是一項免費服務。

先決條件

本教學假設您能夠存取兩個現有 AWS 帳戶（在本教學課程中建立第三個），而且可以以管理員身分登入每個。

此教學會提到如下的帳戶：

- 111111111111 – 您用來建立組織的帳戶。此帳戶會成為管理帳戶。此帳戶擁有者的電子郵件地址為 OrgAccount111@example.com。
- 222222222222 – 您邀請加入組織作為成員帳戶的帳戶。此帳戶擁有者的電子郵件地址為 member222@example.com。
- 333333333333 – 您建立為組織成員的帳戶。此帳戶擁有者的電子郵件地址為 member333@example.com。

將上面的值替換成與您測試帳戶關聯的值。我們建議您不要在本教學中使用生產帳戶。

步驟 1：建立您的組織

在此步驟中，您會以管理員身分登入帳戶 111111111111、以管理帳戶身分使用該帳戶來建立組織，然後邀請現有帳戶 222222222222 加入為成員帳戶。

AWS Management Console

1. 以帳戶 111111111111 的管理員 AWS 身分登入，然後開啟 [AWS Organizations 主控台](#)。
2. 在簡介頁面上，選擇 Create organization (建立組織)。
3. 在確認對話方塊中，選擇 Create an organization (建立組織)。

Note

在預設情況下，您建立的組織會啟用所有功能。您也可以建立組織，但選擇僅啟用[合併帳戶功能](#)。

AWS 會建立組織並顯示[AWS 帳戶](#)頁面。如果您在不同的頁面上，則選擇左側導覽窗格中的 AWS 帳戶。

如果您使用的帳戶從未經由 AWS 驗證其電子郵件，則會自動傳送一封驗證電子郵件到與您的管理帳戶關聯的地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。

4. 請在 24 小時內驗證您的電子郵件地址。如需詳細資訊，請參閱[使用的電子郵件地址驗證 AWS Organizations](#)。

您的組織現已建立，其唯一成員即為您個人的帳戶。此為組織的管理帳戶。

邀請現有的帳戶加入您的組織

現在您已有了組織，就可以開始填入帳戶。在本節中的步驟，您會邀請現有帳戶加入為您組織的成員。

AWS Management Console

邀請現有的帳戶加入

1. 導覽至 [AWS 帳戶](#) 頁面，然後選擇 Add AWS 帳戶 (新增 AWS 帳戶帳戶)。
2. 在 [新增 AWS 帳戶](#) 頁面上，選擇邀請現有的 AWS 帳戶。
3. 在 Email address or account ID of an AWS 帳戶 to invite (待邀請的 AWS 帳戶 帳戶的電子郵件地址或帳戶 ID) 方塊中，輸入您要邀請的帳戶擁有者電子郵件地址，如下所示：**member222@example.com**。或者，如果您知道 AWS 帳戶 ID 號碼，則可以改為輸入。
4. 在 Message to include in the invitation email message (要包含在邀請電子郵件訊息中的訊息) 方塊中，輸入您所需的任何文字。此文字包含在傳送到帳戶擁有者的電子郵件中。
5. 選擇傳送邀請。將邀請 AWS Organizations 傳送給帳戶擁有者。

Important

如果收到指示，請展開錯誤訊息。如果錯誤指出您已超出組織的帳戶限制，或是組織仍在初始化，因此無法新增帳戶，請在建立組織後等待一小時，然後再試一次。如果錯誤仍然存在，請聯絡 [AWS Support](#)。

6. 針對此教學的目的，您現在需要接受自己的邀請。執行以下其中一項，以進入主控台內的 Invitations (邀請) 頁面：
 - 開啟從管理帳戶 AWS 傳送的電子郵件，然後選擇連結以接受邀請。提示您登入時，請以獲邀請成員帳戶中的管理員身分執行。
 - 開啟 [AWS Organizations 主控台](#)，導覽至 [Invitations](#) (邀請) 頁面。
7. 在 [AWS 帳戶](#) 頁面上，選擇 Accept (接受)，然後選擇 Confirm (確認)。

Tip

邀請可能會延遲接收，您可能需要等待一段時間才能接受邀請。

8. 從您的帳戶成員登出，並再次在您的管理帳戶中以管理員身分登入。

建立成員帳戶

在本節的步驟中，您會建立 AWS 帳戶 自動成為組織成員的。我們在本教學中提到的帳戶為 333333333333。

AWS Management Console

建立成員帳戶

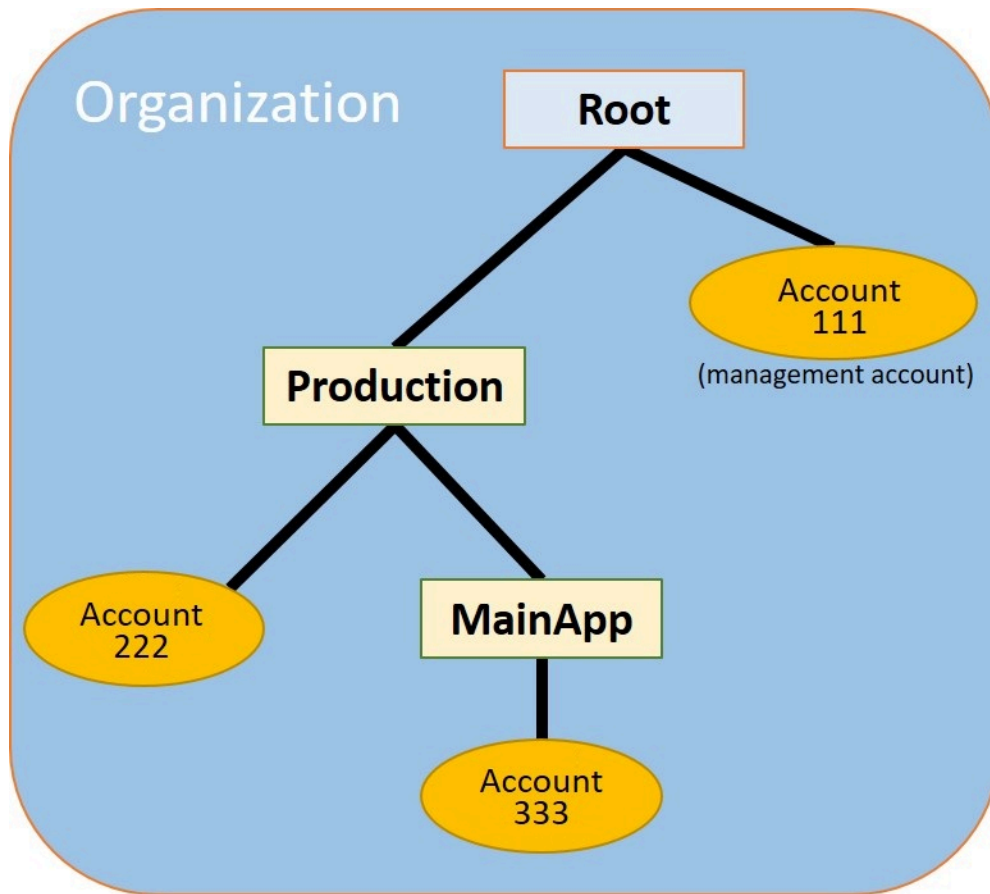
1. 在 AWS Organizations 主控台的[AWS 帳戶](#)頁面上，選擇新增 AWS 帳戶。
2. 在 [Add an AWS 帳戶](#) (新增 AWS 帳戶帳戶) 頁面上，選擇 Create an AWS 帳戶 (建立 AWS 帳戶帳戶)。
3. 針對 AWS 帳戶 name (AWS 帳戶 帳戶名稱)，輸入帳戶的名稱，例如 **MainApp Account**。
4. 針對 Email address of the account's root user (帳戶根使用者的電子郵件地址)，輸入要為帳戶接收通訊的個人電子郵件地址。此值必須在全域必須是唯一的。沒有任兩個帳戶可以有相同的電子郵件地址。例如，您可以使用類似 **mainapp@example.com** 的內容。
5. 針對 IAM role name (IAM 角色名稱)，您可以將它保留空白，以自動使用 OrganizationAccountAccessRole 的預設角色名稱，或者您可以提供自己的名稱。此角色可讓您在以管理帳戶中 IAM 使用者的身分登入時存取新成員帳戶。在本教學中，請將它保留空白，以指示 AWS Organizations 使用預設名稱建立角色。
6. 選擇 Create AWS 帳戶 (建立)。您可能需要稍待片刻並重新整理頁面，才會看見新帳戶顯示在 [AWS 帳戶](#) 頁面。

Important

如果您收到錯誤，指出您已超出組織的帳戶限制，或是因為您的組織仍在初始化，所以無法新增帳戶，請在建立組織後等待 1 小時，然後再試一次。如果錯誤仍然存在，請聯絡 [AWS Support](#)。

步驟 2：建立組織單位

在本節的步驟中，您會建立組織單位 (OU)，並將您的成員帳戶置放在其中。當您完成時，您的階層看起來會與下圖相似。管理帳戶會留在根中。一個成員帳戶已移至生產 OU，而另一個成員帳戶已移到生產的子系 MainApp OU 中。



AWS Management Console

若要建立並填入 OU

Note

在接下來的步驟中，您可以與物件互動，您可以選擇物件本身的名稱或物件旁的選項按鈕。

- 如果您選擇物件的名稱，則會開啟顯示物件詳細資訊的新頁面。
- 如果您選擇物件旁邊的選項按鈕，則會識別要由其他動作執行的物件，例如選擇選單選項。

接下來的步驟會讓您選擇選項按鈕，以便您可以隨後透過選擇選單選項來處理關聯的物件。

1. 在 [AWS Organizations 主控台](#) 上，導覽至 [AWS 帳戶](#) 頁面。

2. 選擇 Root (根) 容器旁邊的核取方塊



3. 選擇動作下拉式清單，然後在組織單位下，選擇建立新。

4. 在 Create organizational unit in Root (在根中建立組織單位) 頁面，針對 Organizational unit name (組織單位名稱)，輸入 **Production**，然後選擇 Create organizational unit (建立組織單位)。

5. 選擇您的新 Production (生產) OU 旁邊的核取方塊



6. 選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Create new (建立新的)。

7. 在 Create organizational unit in Production (在生產中建立組織單位) 頁面，針對第二個 OU 的名稱，輸入 **MainApp**，然後選擇 Create organizational unit (建立組織單位)。

現在您可以將您的成員帳戶移到這些 OU。

8. 返回 [AWS 帳戶](#) 頁面，然後選擇 Production (生產) OU 旁邊的三角形



，以展開其下的樹狀目錄。這會顯示 MainApp OU 作為生產的子項。

9. 在 333333333333 旁邊，選擇核取方塊



(而不是其名稱)，選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Move (移動)。

10. 在移動 AWS 帳戶 '333333333333' 頁面上，選擇生產旁的三角形來展開。在 MainApp (主應用程式) 旁邊，選擇單選按鈕



(而不是其名稱)，然後選擇 Move AWS 帳戶 (移動)。

11. 在 222222222222 旁邊，選擇核取方塊



(而不是其名稱)，選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Move (移動)。

12. 在 Move AWS 帳戶 '222222222222' 頁面上，在 Production 旁，選擇選項按鈕 (而非其名稱)，然後選擇 Move AWS 帳戶。

步驟 3：建立服務控制政策

在本節的步驟中，您會建立三個[服務控制政策 \(SCP\)](#)，並將他們連接到根和 OU，以限制組織帳戶中的使用者可以執行的作業。第一個 SCP 可防止任何成員帳戶中的任何人建立或修改您設定的任何 AWS

CloudTrail 日誌。管理帳戶不受任何 SCP 影響，因此在您套用 CloudTrail SCP 之後，您必須從管理帳戶建立任何日誌。

啟用組織的服務控制政策類型

在可以將任何類型的政策連接到根或根內的任何 OU 之前，您必須先啟用該組織的政策類型。預設不會啟用政策類型。本節中的步驟會說明如何為組織啟用服務控制政策 (SCP) 類型。

AWS Management Console

為組織啟用 SCP。

1. 導覽至 [Policies](#) (政策) 頁面，然後選擇 Service control policies (服務控制政策)。
2. 在 [Service control policies](#) (服務控制政策) 頁面中，選擇 Enable service control policies (啟用服務控制政策)。

綠色橫幅即會出現，通知您現在可以在組織中建立 SCP。

建立 SCP

現在，組織中已啟用服務控制政策，您可以建立本教學課程所需的三項政策。

AWS Management Console

建立封鎖 CloudTrail 設定動作的第一個 SCP

1. 導覽至 [Policies](#) (政策) 頁面，然後選擇 Service control policies (服務控制政策)。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇 Create policy (建立政策)。
3. 針對 Policy name (政策名稱)，輸入 **Block CloudTrail Configuration Actions**。
4. 在 Policy (政策) 區段的右側服務清單中，針對服務選取 CloudTrail。然後選擇下列動作：AddTags、CreateTrail、DeleteTrail、RemoveTags、StartLogging、StopLogging 和 UpdateTrail。
5. 在右側窗格中選擇 Add resource (新增資源)，並指定 CloudTrail 和 All Resources (所有資源)。然後選擇 Add resource (新增資源)。

左側的政策陳述式看起來與以下內容相似。

```
{  
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Sid": "Stmt1234567890123",
        "Effect": "Deny",
        "Action": [
          "cloudtrail:AddTags",
          "cloudtrail:CreateTrail",
          "cloudtrail>DeleteTrail",
          "cloudtrail:RemoveTags",
          "cloudtrail:StartLogging",
          "cloudtrail:StopLogging",
          "cloudtrail:UpdateTrail"
        ],
        "Resource": [
          "*"
        ]
      }
    ]
  }
}

```

6. 選擇 建立政策。

第二個政策會定義您要為生產 OU 中使用者和角色啟用的所有服務及動作[允許清單](#)。完成之後，生產 OU 中的使用者便只會存取列出的服務和動作。

AWS Management Console

建立會為生產 OU 將核准的服務列入允許清單的第二個政策

1. 在 [Service control policies \(服務控制政策\)](#) 頁面中，選擇 Create policy (建立政策)。
2. 針對 Policy name (政策名稱)，輸入 **Allow List for All Approved Services**。
3. 將您的游標置放在 Policy (政策) 區段的右側窗格中，然後貼上政策，如下所示。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1111111111111",
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "elasticloadbalancing:*"
      ]
    }
  ]
}

```

```

        "codecommit:*",
        "cloudtrail:*",
        "codedeploy:*"
    ],
    "Resource": [ "*" ]
}
]
}

```

4. 選擇 建立政策。

最終政策會提供服務的[拒絕清單](#)，這些服務會遭到封鎖而無法在 MainApp OU 中使用。在本教學中，您會封鎖 MainApp OU 中的任何帳戶對 Amazon DynamoDB 的存取。

AWS Management Console

建立第三個政策來拒絕無法在 MainApp OU 中使用之服務的存取權

1. 在 [Service control policies \(服務控制政策\)](#) 頁面中，選擇 Create policy (建立政策)。
2. 針對 Policy name (政策名稱)，輸入 **Deny List for MainApp Prohibited Services**。
3. 在左側的 Policy (政策) 區段中，選取 Amazon DynamoDB 作為服務。針對動作，選擇 All actions (所有動作)。
4. 在左側窗格中選擇 Add resource (新增資源)，並指定 DynamoDB 和 All Resources (所有資源)。然後選擇 Add resource (新增資源)。

右側的政策陳述式會進行更新，看起來與以下內容相似。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [ "dynamodb:*" ],
      "Resource": [ "*" ]
    }
  ]
}

```

5. 選擇 Create policy (建立政策) 來儲存 SCP。

將 SCP 連接到您的 OU

現在 SCP 已存在，並且已為您的根帳戶啟用，您可以將它們連接到根帳戶和 OU。

AWS Management Console

將政策連接到根和 OU

1. 導覽至 [AWS 帳戶](#) 頁面。
2. 在 [AWS 帳戶](#) 頁面中，選擇 Root (根) (其名稱，而非單選按鈕)，以導覽至其詳細資訊頁面。
3. 在 Root (根) 詳細資訊頁面中，選擇 Policies (政策) 索引標籤，然後在 Service Control Policies (服務控制政策) 中，選擇 Attach (連接)。
4. 在 Attach a service control policy (連接服務控制政策) 頁面上，選擇名稱為 Block CloudTrail Configuration Actions 的 SCP 旁邊的選項按鈕，然後選擇 Attach (連接)。在此教學中，您會將其連接至根，從而會影響所有成員帳戶，以防止任何人改變您設定 CloudTrail 的方式。

在 Root (根) 詳細資訊頁面，Policies (政策) 索引標籤現在會顯示連接至根的兩個 SCP：您剛剛連接的 SCP 和預設的 FullAWSAccess SCP。

5. 導覽回 [AWS 帳戶](#) 頁面，然後選擇 Production (生產) OU (其名稱，而非單選按鈕)，以導覽至其詳細資訊頁面。
6. 在 Production (生產) OU 的詳細資訊頁面中，選擇 Policies (政策) 索引標籤。
7. 在 Service Control Policies (服務控制政策) 中，選擇 Attach (連接)。
8. 在 Attach a service control policy (連接服務控制政策) 頁面上，選擇名 Allow List for All Approved Services 旁邊的選項按鈕，然後選擇 Attach (連接)。這可讓使用者或 Production (生產) OU 中成員帳戶的使用者或角色來存取核准的服務。
9. 選擇 Policies (政策) 索引標籤，查看連接至 OU 的那兩個 SCP：您剛剛連接的 SCP 和預設的 FullAWSAccess SCP。不過，因為 FullAWSAccess SCP 也在允許所有服務和動作的允許清單中，所以您現在必須分離此 SCP，以確保僅允許您所核准的服務。
10. 若要從 Production (生產) OU 移除預設政策，選擇 FullAWSAccess 選項按鈕，選擇 Detach (分離)，然後在確認對話方塊中，選擇 Detach policy (分離政策)。

移除此預設政策後，您在前面步驟中所連接允許清單 SCP 中的所有動作和服務，將立即無法提供 Production (生產) OU 下所有成員帳戶存取。任何對於使用不在 Allow List for All Approved Services (所有核准服務的允許清單) SCP 中之動作的請求都會遭到拒絕。即使帳戶中的管理員將 IAM 許可政策連接到其中一個成員帳戶的使用者，也是如此。

11. 現在您可以連接名為 Deny List for MainApp Prohibited services 的 SCP，防止 MainApp OU 中帳戶內的任何人使用任何受限制的服務。

若要執行此動作，導覽至 [AWS 帳戶](#) 頁面，選擇三角形圖示以展開 Production (生產) OU 的分支，然後選擇 MainApp OU (其名稱，而非單選按鈕)，以導覽至其內容。

12. 在 MainApp 詳細資訊頁面，選擇 Policies (政策) 索引標籤。
13. 在 Service Control Policies (服務控制政策)，選擇 Attach (連接)，然後在可用政策的清單中，選擇 Deny List for MainApp Prohibited Services (拒絕 MainApp 禁止服務清單)，然後選擇 Attach policy (連接政策)。

步驟 4：測試您組織的政策

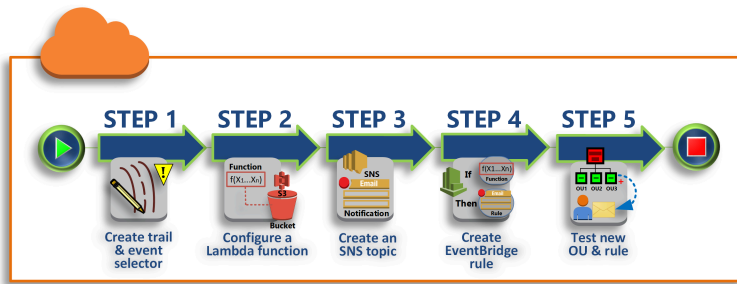
您現在可以以任何成員帳戶中的使用者身分[登入](#)，並嘗試執行各種 AWS 動作：

- 若您以管理帳戶中的使用者身分登入，您可以執行您 IAM 許可政策允許的任何操作。SCP 不會影響管理帳戶中的任何使用者或角色，無論帳戶位在哪一個根或 OU。
- 如果您在帳戶 222222222222 中以使用者身分登入，您可以執行允許清單允許的任何動作。AWS Organizations 會拒絕嘗試在不在允許清單中的任何服務中執行動作。此外，會 AWS Organizations 拒絕嘗試執行其中一個 CloudTrail 組態動作。
- 如果您以帳戶 333333333333 中的使用者身分登入，您可以執行允許清單所允許，且未被拒絕清單所封鎖的任何動作。AWS Organizations 會拒絕所有嘗試執行不在允許清單的任何動作、以及在拒絕清單政策任何動作。此外，會 AWS Organizations 拒絕嘗試執行其中一個 CloudTrail 組態動作。

教學課程：使用 Amazon EventBridge 監控您組織的重要變更

本教學課程說明如何設定 Amazon EventBridge、先前的 Amazon CloudWatch Events 來監控您組織的變更。首先設定規則，此規則會在使用者叫用特定 AWS Organizations 操作時觸發。接下來，您將 Amazon EventBridge 設定為在規則觸發時執行 AWS Lambda 函數，並將 Amazon SNS 設定為傳送電子郵件，其中包含事件的詳細資訊。

下圖顯示教學的主要步驟。



步驟 1：設定追蹤記錄與事件選擇器

在 中建立名為線索的日誌 AWS CloudTrail。您可以設定日誌來擷取所有 API 呼叫。

步驟 2：設定 Lambda 函數

建立 AWS Lambda 函數，將事件的詳細資訊記錄到 S3 儲存貯體。

步驟 3：建立傳送電子郵件給訂閱者的 Amazon SNS 主題

建立 Amazon SNS 主題，此主題會發送電子郵件給其訂閱者，然後讓訂閱者自行訂閱該主題。

步驟 4：建立 Amazon EventBridge 規則

建立規則，此規則會讓 Amazon EventBridge 將特定 API 呼叫的詳細資訊，傳給 Lambda 函數和 SNS 主題的訂閱者。

步驟 5：測試 Amazon EventBridge 規則

藉由執行其中一項受監控的操作，來測試您的新規則。在本教學課程中，受監控的操作會建立組織單位 (OU)。您可檢視 Lambda 函數所建立的日誌記錄，和檢視 Amazon SNS 傳送給訂閱者的電子郵件。

秘訣

您也可以使用此教學作為設定類似操作 (例如在帳戶建立完成時傳送電子郵件通知) 的指南。由於帳戶建立是非同步的操作，當它完成時，您預設不會收到通知。如需搭配使用 AWS CloudTrail 和 Amazon EventBridge 的詳細資訊 AWS Organizations，請參閱 [在中記錄和監控 AWS Organizations](#)。

先決條件

本教學課程的假設如下：

- 您可以從組織中的管理帳戶以 IAM 使用者 AWS Management Console 身分登入。IAM 使用者必須擁有許可，以在 CloudTrail 中建立日誌、在 Lambda 中建立函數、在 Amazon SNS 中建立主題，以及在 Amazon EventBridge 中建立規則，並進行設定。如需關於授與許可的詳細資訊，請參閱 IAM 使用者指南中的[存取管理](#)，或針對您想要設定其存取的服務，參閱該服務的指南。
- 您可以存取現有的 Amazon Simple Storage Service (Amazon S3) 儲存貯體 (或者您擁有建立儲存貯體的許可)，來接收您在步驟 1 中所設定的 CloudTrail 日誌。

Important

目前，AWS Organizations 僅託管在美國東部（維吉尼亞北部）區域（即使它可在全球使用）。若要執行本教學課程中的步驟，您必須設定 AWS Management Console 以使用該區域。

步驟 1：設定追蹤記錄與事件選擇器

在此步驟中，您會登入管理帳戶，並且在 中設定日誌 (稱為追蹤記錄 AWS CloudTrail)。您也會設定針對追蹤的事件選擇器，以擷取所有讀取/寫入 API 呼叫，以便 Amazon EventBridge 具有要觸發的呼叫。

若要建立追蹤記錄

1. 以組織管理帳戶的管理員 AWS 身分登入，然後在 開啟 CloudTrail 主控台<https://console.aws.amazon.com/cloudtrail/>。
2. 在主控台右上角的導覽列中，選擇美國東部 (維吉尼亞北部) 區域。如果您選擇不同的區域，AWS Organizations 不會在 Amazon EventBridge 組態設定中顯示為選項，而且 CloudTrail 不會擷取有關的資訊 AWS Organizations。
3. 在導覽窗格中，選擇 Trails (追蹤記錄)。
4. 選擇 Create trail (建立追蹤)。
5. 針對 Trail name (追蹤名稱)，輸入 **My-Test-Trail**。
6. 執行以下其中一個選項，指定 CloudTrail 交付其日誌的位置：
 - 如果您需要建立儲存貯體，請選擇 Create new S3 bucket (建立新的 S3 儲存貯體)，然後針對 Trail log bucket and folder (追蹤日誌儲存貯體和資料夾)，輸入新儲存貯體的名稱。

 Note

S3 儲存貯體名稱必須在「全域」必須是唯一的。

- 如果您已經擁有儲存貯體，請選擇 Use existing S3 bucket (使用現有的 S3 儲存貯體)，然後從 S3 bucket (S3 儲存貯體) 清單中選擇儲存貯體的名稱。
7. 選擇 Next (下一步)。
 8. 在 Choose log events (選擇日誌事件) 頁面的 Management events (管理事件) 區段中，選擇 Read (讀取) 和 Write (寫入)。
 9. 選擇 Next (下一步)。
 10. 檢閱選項，然後選擇 Create trail (建立追蹤)。

Amazon EventBridge 可讓您從幾種不同的方法中選擇其一，用來在警示規則符合傳入的 API 呼叫時傳送提醒。本教學示範兩種方法：叫用可以記錄 API 呼叫的 Lambda 函數，以及傳送資訊至 Amazon SNS 主題，而此主題會發送電子郵件或文字訊息給該主題的訂閱者。在接下來的兩個步驟中，會建立所需的元件：Lambda 函數和 Amazon SNS 主題。

步驟 2：設定 Lambda 函數

在此步驟中會建立 Lambda 函數，其中記錄根據 Amazon EventBridge 規則 (您稍後會進行設定) 傳送給該函數的 API 活動。

建立記錄 Amazon EventBridge 事件的 Lambda 函數

1. 在開啟 AWS Lambda 主控台 <https://console.aws.amazon.com/lambda/>。
2. 如果您是初次使用 Lambda，請選擇歡迎頁面上的 Get Started Now (立即開始使用)；否則請選擇 Create function (建立函數)。
3. 在 Create function (建立函數) 頁面上，選擇 Use a blueprint (使用藍圖)。
4. 從 Blueprints (藍圖) 搜尋方塊中，針對篩選條件輸入 **hello**，並選擇 hello-world 藍圖。
5. 選擇設定。
6. 在 Basic information (基本資訊) 頁面上，執行以下作業：
 - a. 對於 Lambda 函數名稱，在 Name (名稱) 文字方塊中輸入 **LogOrganizationEvents**。

- b. 針對 Role (角色)，選擇 Create a new role with basic Lambda permissions (建立具備基本 Lambda 許可的新角色)。此角色會授予許可給您的 Lambda 函數，讓函數存取所需的資訊和寫入其輸出日誌。
7. 如下列範例所示，編輯 Lambda 函數程式碼。

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1; // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

此範本程式碼會記錄具有 **LogOrganizationsEvents** 標記字串的事件，後面接續構成事件的 JSON 字串。

8. 選擇 Create function (建立函數)。

步驟 3：建立傳送電子郵件給訂閱者的 Amazon SNS 主題

在此步驟中，您會建立一個 Amazon SNS 主題，此主題會透過電子郵件來傳送資訊給其訂閱者。這會讓此主題成為之後所建立 Amazon EventBridge 規則的目標。

若要建立 Amazon SNS 主題來傳送電子郵件給訂閱者

1. 在 <https://console.aws.amazon.com/sns/v3/> 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇 Topics (主題)。
3. 請選擇 Create new topic (建立新主題)。
 - a. 針對 Topic name (主題名稱)，輸入 **OrganizationsCloudWatchTopic**。
 - b. 針對 Display name (顯示名稱)，輸入 **OrgsCWEvnt**。
 - c. 請選擇建立主題。
4. 現在您可以建立該主題的訂閱。針對剛才所建立的主題，來選擇 ARN。
5. 選擇 Create subscription (建立訂閱)。
 - a. 在 Create subscription (建立訂閱) 頁面上，針對 Protocol (通訊協定) 選擇 Email (電子郵件)。
 - b. 針對 Endpoint (端點)，輸入電子郵件地址。

- c. 選擇建立訂閱。將電子郵件 AWS 傳送至您在上一個步驟中指定的電子郵件地址。請等待該電子郵件送達，然後選取電子郵件中的 Confirm subscription (確認訂閱) 連結，來確認您已成功收到電子郵件。
- d. 返回主控台並重新整理頁面。Pending confirmation (待確認) 訊息會關閉，改而顯示目前有效的訂閱 ID。

步驟 4：建立 Amazon EventBridge 規則

現在您帳戶中已經存在所需的 Lambda 函數，您可以建立 Amazon EventBridge 規則，以在規則中的條件滿足時叫用該函數。

若要建立 EventBridge 規則

1. 在 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。
2. 將主控台設定為 US East (N. Virginia) (美國東部 (維吉尼亞北部)) 區域，否則組織的相關資訊將不可用。在主控台右上角的導覽列中，選擇美國東部 (維吉尼亞北部) 區域。
3. 如需建立規則的說明，請參閱《[Amazon EventBridge 使用者指南](#)》中的 [Amazon EventBridge](#) 中的規則。EventBridge

步驟 5：測試 Amazon EventBridge 規則

在此步驟中，您會建立組織單位 (OU)、觀察 Amazon EventBridge 規則、產生日誌項目，並將電子郵件傳送給您自己，其中包含該事件的相關詳細資訊。

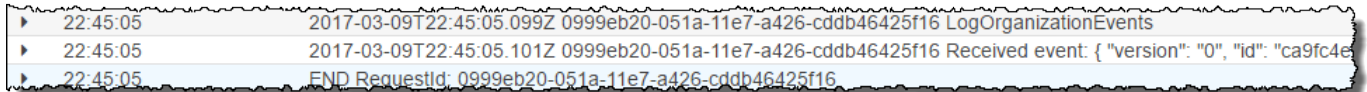
AWS Management Console

建立組織單位 (OU)

1. 開啟 AWS Organizations 主控台至 [AWS 帳戶頁面](#)。
2. 選擇核取方塊
☒
Root (根) OU，選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Create new (建立新的)。
3. 針對 OU 的名稱，輸入 **TestCWE0U**，然後選擇 Create organizational unit (建立組織單位)。

查看 EventBridge 日誌項目

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽頁面中，選擇 Logs (日誌)。
3. 在 Log Groups (日誌群組) 下方，選擇與您的 Lambda 函數：`/aws/lambda/LogOrganizationEvents` 關聯的群組。
4. 每個群組包含一或多個串流，而今天應該會有一個群組。請選擇此群組。
5. 檢視日誌。您應該會看到與以下內容相似的資料列。



```

22:45:05      2017-03-09T22:45:05.099Z 0999eb20-051a-11e7-a426-cddb46425f16 LogOrganizationEvents
22:45:05      2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event: { "version": "0", "id": "ca9fc4e
22:45:05      END RequestId: 0999eb20-051a-11e7-a426-cddb46425f16

```

6. 選取項目的中間資料列，檢視所接收事件的完整 JSON 文字。在輸出的 `requestParameters` 和 `responseElements` 片段中，可以看到 API 請求的所有詳細資訊。

```

2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
  "version": "0",
  "id": "123456-EXAMPLE-GUID-123456",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.organizations",
  "account": "123456789012",
  "time": "2017-03-09T22:44:26Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.04",
    "userIdentity": {
      ...
    },
    "eventTime": "2017-03-09T22:44:26Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent": "AWS Organizations Console, aws-internal/3",
    "requestParameters": {
      "parentId": "r-exampleRootId",
      "name": "TestCWEOU"
    },
    "responseElements": {

```

```
    "organizationalUnit": {
      "name": "TestCWE0U",
      "id": "ou-exampleRootId-example0UId",
      "arn": "arn:aws:organizations::1234567789012:ou/o-example0rgId/ou-
exampleRootId-exampe0UId"
    },
    "requestID": "123456-EXAMPLE-GUID-123456",
    "eventID": "123456-EXAMPLE-GUID-123456",
    "eventType": "AwsApiCall"
  }
}
```

7. 檢查您的電子郵件帳戶，看看是否有來自 OrgsCWEvnt (您 Amazon SNS 主題的顯示名稱) 的訊息。電子郵件的內文中，包含了與先前步驟所示日誌記錄相同的 JSON 文字輸出。

清除：移除不再需要的資源

為了避免產生費用，您應該刪除在本教學課程中建立的任何您不想保留 AWS 的資源。

清除您的 AWS 環境

1. 使用 [CloudTrail 主控台](#)，來刪除您在步驟 1 中所建立的名稱為 **My-Test-Trail** 的追蹤。
2. 如果您在步驟 1 中建立了 Amazon S3 儲存貯體，則使用 [Amazon S3 主控台](#) 來刪除該儲存貯體。
3. 使用 [Lambda 主控台](#)，來刪除您在步驟 2 中所建立名為 **LogOrganizationEvents** 的函數。
4. 使用 [Amazon SNS 主控台](#)，來刪除您在步驟 3 中所建立的名稱為 **OrganizationsCloudWatchTopic** 的 Amazon SNS 主題。
5. 使用 [CloudWatch 主控台](#)，刪除您在步驟 4 中建立的名為 **OrgsMonitorRule** 的 EventBridge 規則。
6. 最後，使用 [Organizations 主控台](#)，來刪除您在步驟 5 中所建立名為 **TestCWE0U** 的 OU。

到此為止。在本教學課程中，您設定了 EventBridge 來監控組織的變更。您設定了規則，此規則會在使用者叫用特定 AWS Organizations 操作時觸發。此規則會執行記錄事件的 Lambda 函數，並傳送電子郵件，其中包含關於事件的詳細資訊。

AWS Organizations 搭配 AWS SDK 使用

AWS 軟體開發套件 (SDKs) 適用於許多熱門的程式設計語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

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

可用性範例

找不到所需的內容嗎？請使用本頁面底部的提供意見回饋連結申請程式碼範例。

使用 管理組織 AWS Organizations

組織是 的集合 AWS 帳戶，您可以集中管理，並整理成階層式的樹狀結構，其中根位於根目錄頂端，而組織單位巢狀在根目錄下。每個帳戶都可以直接放在根帳戶中，或放在階層中的其中一個 OU 中。

每個組織都包含：

- 管理帳戶
- 零個或多個成員帳戶
- 零個或多個組織單位 OUs)
- 零或多個政策。

組織具有的功能取決於您啟用的[功能集](#)。

主題

- [使用 建立組織 AWS Organizations](#)
- [使用 的電子郵件地址驗證 AWS Organizations](#)
- [使用 重新傳送驗證電子郵件 AWS Organizations](#)
- [使用 變更組織的電子郵件地址 AWS Organizations](#)
- [使用 為組織啟用所有功能 AWS Organizations](#)
- [從管理帳戶檢視組織的詳細資訊](#)
- [使用 刪除組織 AWS Organizations](#)

使用 建立組織 AWS Organizations

您可以使用 AWS 帳戶 做為管理帳戶來建立組織。建立組織時，您可以選擇組織支援[所有功能（建議）](#)還是僅[合併帳單](#)。根據預設，您建立的組織支援所有功能。

建立組織

您可以使用 或使用 AWS Management Console 中的命令 AWS CLI 或其中一個 SDK APIs，來建立組織。

最低許可

若要使用您目前的 建立組織 AWS 帳戶，您必須具有下列許可：

- `organizations:CreateOrganization`
- `iam:CreateServiceLinkedRole`

您可以將此許可限制為僅限服務委託人 `organizations.amazonaws.com`。

AWS Management Console

建立組織

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在預設情況下，您建立的組織會啟用所有功能。但是，您可以選擇下列其中一個步驟：
 - 若要建立已啟用所有功能的組織，在簡介頁面上，選擇 Create an organization (建立組織)。
 - 若要建立僅具有合併帳單功能的組織，請在「簡介」頁面和 Create an organization (建立組織) 下，選擇 consolidated billing features (合併帳單功能)，然後在 Confirmation (確認) 對話方塊中，選擇 Create an organization (建立組織)。

如果您不小心選擇了錯誤的選項，您可以立即前往 [Settings](#) (設定) 頁面，然後選擇 Delete organization (刪除組織)，並重新開始

3. 組織會隨即建立，且 [AWS 帳戶](#) 頁面會隨即出現。唯一存在的帳戶是您的管理帳戶，並且其目前存放在 [根組織單位 \(OU\)](#)。

如有必要，Organizations 會自動傳送驗證電子郵件至與您管理帳戶關聯的地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。請在 24 小時內驗證您的電子郵件地址。如需詳細資訊，請參閱 [使用的電子郵件地址驗證 AWS Organizations](#)。您可以建立帳戶以發展您的組織，而不驗證您的管理帳戶的電子郵件地址。不過，若要邀請現有的帳戶，您必須先完成電子郵件驗證。

Note

如果此帳戶之前已驗證其電子郵件地址，則在您使用該帳戶建立組織時，就不會再發生這種情況。

AWS CLI & AWS SDKs

下列程式碼範例示範如何使用 `CreateOrganization`。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
        {
            FeatureSet = "ALL",
        });

        Organization newOrg = response.Organization;

        Console.WriteLine($"Organization: {newOrg.Id} Main Account:
{newOrg.MasterAccountId}");
    }
}
```



```
}  
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [CreateOrganization](#)。

CLI

AWS CLI

範例 1：建立新組織

Bill 想要使用帳戶 111111111111 的登入資料來建立組織。下列範例顯示帳戶成為新組織中的主要帳戶。由於他未指定功能集，因此新組織預設為啟用的所有功能，且服務控制政策會在根上啟用。

```
aws organizations create-organization
```

輸出包含組織物件，其中包含新組織的詳細資訊：

```
{  
  "Organization": {  
    "AvailablePolicyTypes": [  
      {  
        "Status": "ENABLED",  
        "Type": "SERVICE_CONTROL_POLICY"  
      }  
    ],  
    "MasterAccountId": "111111111111",  
    "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-exampleorgid/111111111111",  
    "MasterAccountEmail": "bill@example.com",  
    "FeatureSet": "ALL",  
    "Id": "o-exampleorgid",  
    "Arn": "arn:aws:organizations::111111111111:organization/o-exampleorgid"  
  }  
}
```

範例 2：建立僅啟用合併帳單功能的新組織

下列範例會建立僅支援合併帳單功能的組織：

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

輸出包含組織物件，其中包含新組織的詳細資訊：

```
{
  "Organization": {
    "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
    "AvailablePolicyTypes": [],
    "Id": "o-exampleorgid",
    "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
    "MasterAccountEmail": "bill@example.com",
    "MasterAccountId": "111111111111",
    "FeatureSet": "CONSOLIDATED_BILLING"
  }
}
```

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的建立組織。

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [CreateOrganization](#)。

建立組織之後，您可以透過下列方式從管理帳戶將帳戶新增至組織：

- [建立會自動新增至組織作為成員帳戶的其他 AWS 帳戶](#) 帳戶
- [驗證您的電子郵件地址](#) 後，請[邀請現有的 AWS 帳戶](#) 以成員帳戶身分加入您的組織。

使用 的電子郵件地址驗證 AWS Organizations

在您建立組織之後，以及在您可以邀請帳戶加入之前，必須驗證您擁有組織中為管理帳戶提供的電子郵件地址。

當您建立組織時，如果管理帳戶先前尚未經過驗證，AWS 會自動將驗證電子郵件傳送至指定的電子郵件地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。

驗證電子郵件地址

請在 24 小時內，遵循電子郵件中的指示來驗證您的電子郵件地址。如果超過 24 小時，請參閱[重新傳送驗證電子郵件](#)。

使用 重新傳送驗證電子郵件 AWS Organizations

如果您未在 24 小時內驗證您的電子郵件地址，您可以重新傳送驗證請求。驗證您的電子郵件地址後，您可以邀請其他人 AWS 帳戶 加入您的組織。如果您未收到驗證電子郵件，請檢查您的電子郵件地址是否正確，並在必要時修改。

- 若要進一步了解與您的管理帳戶關聯的電子郵件地址，請參閱[從管理帳戶檢視組織的詳細資訊](#)。
- 若要變更與您的管理帳戶關聯的電子郵件地址，請參閱AWS Billing 使用者指南中的[管理 AWS 帳戶](#)。

AWS Management Console

重新傳送驗證請求

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 導覽至 [Settings](#) (設定) 頁面，然後選擇 Send verification request (傳送驗證請求)。只有在未驗證管理帳戶時，才會出現此選項。
3. 請在 24 小時內驗證您的電子郵件地址。

驗證您的電子郵件地址後，您將可邀請其他 AWS 帳戶 加入您的組織。如需詳細資訊，請參閱[使用 管理帳戶邀請 AWS Organizations](#)。

使用 變更組織的電子郵件地址 AWS Organizations

若要變更與管理帳戶相關聯的電子郵件地址，請參閱 AWS 帳戶管理 參考指南中的[更新根使用者 AWS 帳戶 的名稱、電子郵件地址或密碼](#)。

若您變更管理帳戶的電子郵件地址，帳戶的狀態會回復到「電子郵件未驗證」，而您必須完成新電子郵件地址的驗證程序。

Note

如果您在變更管理帳戶的電子郵件地址之前邀請帳戶加入組織，而且尚未接受這些邀請，則在您驗證管理帳戶的新電子郵件地址之前，都無法接受這些邀請。您必須先[重新傳送驗證請求](#)。在您回覆電子郵件完成程序後，您邀請的帳戶可以接受邀請。

使用 為組織啟用所有功能 AWS Organizations

AWS Organizations 有兩個可用的功能集：

- [所有功能](#) – 此功能集是使用 的偏好和預設方式 AWS Organizations，其中包含合併帳單的所有功能。當您建立組織時，根據預設會啟用所有功能。啟用所有功能後，您可以使用 Organizations 中可用的進階帳戶管理功能，例如[與支援的 AWS 服務和組織政策整合](#)。
- [合併帳單功能](#) – 此功能集僅限於跨組織產生單一帳單。沒有其他管理功能可用於合併帳單。

如果您使用合併帳單功能集建立組織，您稍後可以啟用所有功能。不過，您無法在所有功能啟用後，從所有功能遷移到合併帳單。

標準遷移和輔助遷移

遷移至所有功能的兩種方法是標準遷移和輔助遷移。

標準遷移是所有 AWS Organizations 客戶可用的自助式程序，可啟用所有功能模式。

協助遷移是 Enterprise Support 計劃客戶可請求將其組織 AWS 遷移到代表您的所有功能模式的程序。

Note

單向程序和復原程序

- 從合併帳單功能到所有功能的移轉是單向的。啟用組織的所有功能之後，您就無法切換回僅具備合併帳單功能。
- 在您開始輔助遷移程序之後，就無法復原。如果您想要改用標準程序，則需要等待 90 天直到程序過期。

主題

- [考量事項](#)
- [使用 Organizations 啟用所有功能的標準遷移程序](#)
- [協助遷移程序，以使用 Organizations 啟用所有功能](#)

考量事項

從僅支援合併帳單功能的組織變更為支援所有功能的組織之前，請考慮下列事項：

受邀帳戶必須核准遷移

當您開始啟用所有功能的程序時，會將請求 AWS Organizations 傳送至您邀請加入組織的每個成員帳戶。每個獲邀請的帳戶必須透過接受請求來核准啟用所有功能。只有這樣，您才能完成啟用組織中的所有功能的程序。如果帳戶拒絕請求，您必須從組織移除帳戶或重新傳送請求。您必須先接受請求，才能完成啟用所有功能的程序。您使用 AWS Organizations 建立的帳戶不會收到請求，因為他們不需要核准額外的控制。

邀請的帳戶會收到通知，告知目前已啟用哪些功能集

受邀帳戶的擁有者會收到邀請通知，無論他們是加入僅合併帳單的組織，還是啟用了所有功能。您可以在啟用所有功能的同時，繼續邀請帳戶加入您的組織。

如果您在啟用所有功能的程序期間邀請帳戶，邀請會指出他們所加入的組織已啟用所有功能。如果您在帳戶接受邀請之前取消啟用所有功能的程序，則該邀請會被取消。您必須再次邀請帳戶成為僅具備合併帳單功能之組織成員。

如果您邀請帳戶但尚未接受邀請之前，您就會開始啟用所有功能的程序，該邀請會被取消，因為邀請指出該組織只有合併帳單功能。您必須再次邀請帳戶成為已啟用所有功能之組織的成員。

在組織中建立帳戶的程序不受遷移影響

您可以繼續在組織中建立帳戶。該程序不會受到此變更的影響。

服務連結角色 **AWSServiceRoleForOrganizations** 為必要項目

AWS Organizations 驗證每個成員帳戶是否具有名為 的服務連結角色 **AWSServiceRoleForOrganizations**。所有帳戶中均必須有此角色，才能啟用所有功能。如果您刪除獲邀請帳戶中的該角色，接受邀請會啟用重新建立角色的所有功能。如果您在使用 建立的帳戶中刪除角色 AWS Organizations，該帳戶會收到專門重新建立該角色的邀請。所有的邀請都必須獲得接受，組織才能完成啟用所有功能的程序。

使用 Organizations 啟用所有功能的標準遷移程序

本主題說明如何使用標準遷移程序啟用所有功能。

步驟 1：請求受邀帳戶核准遷移（管理帳戶）

當您使用組織管理帳戶登入時，您可以開始啟用所有功能的程序。若要執行此動作，請執行下列步驟。

最低許可

若要啟用組織中的所有功能，您必須擁有下列許可：

- `organizations:EnableAllFeatures`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

要求獲邀請的成員帳戶接受啟用組織中的所有功能

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Settings \(設定\)](#) 頁面中，選擇 `Begin process to enable all features` (開始啟用所有功能的程序)。
3. 在 [Enable all features](#) (啟用所有功能) 頁面上，確認您了解在切換後透過選擇 `Begin process to enable all features` (開始程序以啟用所有功能)，無法傳回僅合併帳單功能。

AWS Organizations 會傳送請求至組織中每個受邀（未建立）帳戶，要求核准以啟用組織中的所有功能。如果您有任何使用建立的帳戶，AWS Organizations 且成員帳戶管理員已刪除名為 `服務連結角色AWSServiceRoleForOrganizations`，會 AWS Organizations 傳送請求給該帳戶以重新建立角色。

主控台會隨即顯示受邀帳戶的請求核准狀態清單。

Tip

若要稍後返回此頁面，請開啟 [Settings \(設定\)](#) 頁面，並在 `Request sent date` (已傳送請求日期) 區段中，選擇 `View status` (檢視狀態)。

4. [Enable all features](#) (啟用所有功能) 頁面會顯示組織中每個帳戶目前的請求狀態。已接受請求的帳戶會顯示 ACCEPTED (已接受) 狀態。尚未同意的帳戶會顯示 OPEN (未決) 狀態。

AWS CLI & AWS SDKs

要求獲邀請的成員帳戶接受啟用組織中的所有功能

您可以使用下列其中一項命令來啟用組織中的所有功能：

- AWS CLI: [enable-all-features](#)

下列命令會開始在組織中啟用所有功能的程序。

```
$ aws organizations enable-all-features
{
  "Handshake": {
    "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ],
    "State": "REQUESTED",
    "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
    "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
    "Action": "ENABLE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "o-a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ]
  }
}
```

輸出會顯示受邀成員帳戶必須同意的交握詳細資訊。

- AWS SDKs : [EnableAllFeatures](#)

❗ 備註

- 當請求傳送到成員帳戶時，即開始 90 天的倒數計時。所有帳戶必須在該時間內核准請求，否則請求會過期。如果請求過期，與此嘗試相關的所有請求都會取消，而且您必須從步驟 2 重新開始。
- 一旦您要求啟用所有功能，現有未接受的帳戶邀請將全部遭到取消。
- 在所有功能遷移過程中，您仍然可以啟動新帳戶邀請和建立新帳戶。

在組織中的所有受邀帳戶核准其請求之後，您就可以完成程序並啟用所有功能。如果您的組織沒有任何受邀成員帳戶，您也可以立即完成程序。若要完成此程序，請繼續[步驟 3：完成遷移程序以啟用所有功能（管理帳戶）](#)。

步驟 2：核准啟用所有功能或重新建立服務連結角色（邀請帳戶）的請求

以其中一個組織的受邀成員帳戶登入時，您可以從管理帳戶核准請求。如果您的帳戶原先獲邀請加入組織，該邀請是要啟用所有功能並隱含包含核准重新建立 `AWSServiceRoleForOrganizations` 角色 (必要時)。如果您的帳戶是使用 建立的，AWS Organizations 而且您刪除了 `AWSServiceRoleForOrganizations` 服務連結角色，則您只會收到重新建立角色的邀請。若要執行此動作，請執行下列步驟。

⚠ Important

如果您啟用所有功能，則組織中的管理帳戶可以對您的成員帳戶套用以政策為基礎的控制。對於使用者，甚至身為管理員的您，這些控制可以限制在您的帳戶中能夠執行什麼動作。這類限制可能會使您的帳戶無法離開組織。

❗ 最低許可

若要核准為您的成員帳戶啟用所有功能的請求，成員帳戶必須具有下列許可：

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListHandshakesForAccount` – 僅在使用 Organizations 主控台時才需要

- `iam:CreateServiceLinkedRole` – 只有在必須在成員帳戶中重新建立 `AWSServiceRoleForOrganizations` 角色時才為必要

AWS Management Console

接受在組織中啟用所有功能的請求

1. 在 AWS Organizations 主控台登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 ([不建議](#))。
2. 了解接受組織中所有功能對您的帳戶所代表的意義，然後選擇 `Accept` (接受)。此頁面會繼續將程序顯示為未完成，直到組織中的所有帳戶接受請求，並且管理帳戶的管理員完成程序為止。

AWS CLI & AWS SDKs

接受在組織中啟用所有功能的請求

若要接受請求，您必須接受與 `"Action": "APPROVE_ALL_FEATURES"` 的交握。

- AWS CLI:
 - [accept-handshake](#)
 - [list-handshakes-for-account](#)

下列範例顯示如何列出帳戶可用的交握。輸出的第四行中 `"Id"` 的值是下一個命令所需的值。

```
$ aws organizations list-handshakes-for-account
{
  "Handshakes": [
    {
      "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
      "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
      "Parties": [
        {
          "Id": "a1b2c3d4e5",
          "Type": "ORGANIZATION"
        },
        {
          "Id": "111122223333",
          "Type": "ACCOUNT"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "State": "OPEN",
  "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
  "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
  "Action": "APPROVE_ALL_FEATURES",
  "Resources": [
    {
      "Value": "c440da758cab44068cdafc812EXAMPLE",
      "Type": "PARENT_HANDSHAKE"
    },
    {
      "Value": "o-aa111bb222",
      "Type": "ORGANIZATION"
    },
    {
      "Value": "111122223333",
      "Type": "ACCOUNT"
    }
  ]
}
]
}

```

下列範例會使用上一個命令的交握 ID 來接受交握。

```

$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
  "Handshake": {
    "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "111122223333",
        "Type": "ACCOUNT"
      }
    ]
  },

```

```

    "State": "ACCEPTED",
    "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
    "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
    "Action": "APPROVE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "c440da758cab44068cdafc812EXAMPLE",
        "Type": "PARENT_HANDSHAKE"
      },
      {
        "Value": "o-aa111bb222",
        "Type": "ORGANIZATION"
      },
      {
        "Value": "111122223333",
        "Type": "ACCOUNT"
      }
    ]
  }
}

```

- AWS SDKs :
 - [list-handshakes-for-account](#)
 - [AcceptHandshake](#)

步驟 3：完成遷移程序以啟用所有功能（管理帳戶）

所有獲邀的成員帳戶都需核准請求，才能啟用所有功能。如果組織中沒有任何獲邀請的成員帳戶，Enable all features progress (啟用組織中的所有功能進度) 頁面會以綠色橫幅表示您可以完成程序。

最低許可

若要完成啟用組織中的所有功能的程序，您必須擁有下列許可：

- organizations:AcceptHandshake
- organizations:ListHandshakesForOrganization
- organizations:DescribeOrganization – 僅在使用 Organizations 主控台時才需要

AWS Management Console

完成啟用所有功能的程序

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Settings](#) (設定) 頁面上，如果所有受邀帳戶接受啟用所有功能的請求，頁面上方會出現綠色方塊，以便通知您。在綠色方塊中，選擇 Go to finalize (前往完成)。
3. 在 [Enable all features](#) (啟用所有功能) 頁面中，選擇 Finalize (完成)，然後在確認對話方塊中，選擇 Finalize (完成)。
4. 組織現在已啟用所有功能。

AWS CLI & AWS SDKs

完成啟用所有功能的程序

若要完成該程序，您必須接受與 "Action": "ENABLE_ALL_FEATURES" 的交握。

- AWS CLI:
 - [list-handshakes-for-organization](#)
 - [accept-handshake](#)

```
$ aws organizations list-handshakes-for-organization
{
  "Handshakes": [
    {
      "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
      "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
      "Parties": [
        {
          "Id": "a1b2c3d4e5",
          "Type": "ORGANIZATION"
        }
      ],
      "State": "OPEN",
      "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
      "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
      "Action": "ENABLE_ALL_FEATURES",
      "Resources": [
```

```

        {
            "Value": "o-aa111bb222",
            "Type": "ORGANIZATION"
        }
    ]
}

```

下列範例示範如何列出組織可用的交握。輸出的第四行中 "Id" 的值是下一個命令所需的值。

```

$ aws organizations accept-handshake \
  --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
  "Handshake": {
    "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ],
    "State": "ACCEPTED",
    "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
    "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
    "Action": "ENABLE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "o-aa111bb222",
        "Type": "ORGANIZATION"
      }
    ]
  }
}

```

- AWS SDKs :
 - [ListHandshakesForOrganization](#)
 - [AcceptHandshake](#)

協助遷移程序，以使用 Organizations 啟用所有功能

如果您是企業客戶，由於您可能管理的帳戶數量龐大，因此可能很難完成標準遷移程序。例如，您可能難以取得遷移大型組織中所有受邀帳戶的核准。

協助遷移有助於此程序，讓客戶擁有企業支援計劃，以請求將其組織 AWS 遷移到代表您的所有功能。此程序需要您簽署一份協議合約，確認您擁有所有帳戶，然後是 14 天的等待期。如果帳戶想要在遷移到所有功能生效之前離開組織，此等待期間會提供帳戶離開組織的時間。

AWS Management Console

使用輔助遷移遷移至所有功能

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [設定](#) 頁面上，選擇啟用所有功能，然後選擇輔助遷移。
3. 閱讀協議的條款與條件，選擇接受並選擇開始程序，以啟用所有功能來開始遷移。

Note

開始輔助遷移程序會覆寫標準遷移程序

如果您目前正在使用標準遷移程序啟用所有功能，則會取消，輔助遷移程序也會開始。

輔助遷移程序是單向的，無法復原

在您開始輔助遷移程序之後，就無法復原。如果您想要改用標準程序，則需要等待 90 天直到程序過期。

如果您使用輔助遷移，則不需要擔心以根使用者身分存取受邀帳戶，以接受所有功能的遷移。

您可以聯絡您的技術客戶經理 (TAM)，以取得協助遷移的確切詳細資訊、進度和時間表。

從管理帳戶檢視組織的詳細資訊

在 [AWS Organizations 主控台](#) 登入組織的管理帳戶時，您可以檢視組織的詳細資訊。

最低許可

若要檢視組織的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeOrganization`

AWS Management Console

檢視您的組織的詳細資訊

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 瀏覽至 [Settings](#) (設定) 頁面。此頁面會顯示有關組織的詳細資訊，包括組織 ID、帳戶名稱和指派給組織管理帳戶的電子郵件地址。

AWS CLI & AWS SDKs

檢視您的組織的詳細資訊

您可以使用下列其中一項命令來檢視組織的詳細資訊：

- AWS CLI: [describe-organization](#)

以下範例顯示此命令輸出中包含的資訊。

```
$ aws organizations describe-organization
{
  "Organization": {
    "Id": "o-aa111bb222",
    "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
    "FeatureSet": "ALL",
    "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-aa111bb222/123456789012",
    "MasterAccountId": "123456789012",
    "MasterAccountEmail": "admin@example.com",
    "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
  }
}
```

 Important

該 AvailablePolicyTypes 欄位已棄用，並且不包含有關在您的組織中啟用政策的準確資訊。若要查看實際針對組織啟用的準確且完整的政策類型清單，請使用 ListRoots 命令，如以下章節 AWS CLI 部分中所述。

- AWS SDKs : [DescribeOrganization](#)

使用 刪除組織 AWS Organizations

當您不再需要您的組織時，可以將它刪除。刪除組織並不會關閉管理帳戶，而是會從組織移除管理帳戶並刪除組織本身。

先前的管理帳戶會成為不再由 AWS 帳戶 管理的獨立帳戶 AWS Organizations。然後，您有三個選項：

- 您可以繼續將其用作獨立帳戶
- 您可以使用它來建立不同的組織
- 您可以接受來自另一個組織的邀請，以將帳戶新增至該組織做為成員帳戶。

主題

- [考量事項](#)
- [刪除組織](#)

考量事項

已刪除的組織無法復原

如果您刪除某個組織，則無法復原該組織。如果您已在組織內建立任何政策，則也會將它們刪除且無法對其復原。

只有在移除所有成員帳戶後，才能刪除組織

只有在從組織移除所有成員帳戶之後，您才能夠刪除該組織。如果您使用 建立一些成員帳戶 AWS Organizations，則可能會封鎖您移除這些帳戶。只有在成員帳戶具有以獨立 AWS 帳戶形式運作所需的

所有資訊時，您才可以移除該成員帳戶。如需有關如何提供該資訊和移除帳戶的詳細資訊，請參閱[使用從成員帳戶離開組織 AWS Organizations](#)。

無法從組織中移除處於「暫停」狀態的成員帳戶

如果您在將成員帳戶從組織中移除之前，已關閉成員帳戶，它會進入「暫停」狀態一段時間，而且在最終關閉之前，您無法從組織中移除該帳戶。這最多可能需要 90 天的時間，而且可能會讓您在此之前無法刪除組織，直至所有成員帳戶都完全關閉。

透過刪除組織從組織移除管理帳戶，可能會以下列方式影響帳戶：

- 該帳戶只負責支付自己的費用，並且不再負責其他任何帳戶衍生的費用。
- 與其他服務的整合可能會停用。例如，AWS IAM Identity Center 需要一個組織才能運作，因此，如果您從支援 IAM Identity Center 的組織中移除帳戶，則該帳戶中的使用者就無法再使用該服務。

組織的管理帳戶絕不會受到服務控制政策 (SCP) 的影響，因此在 SCP 不再可用之後，許可中沒有變更。

備份所有報告

請務必從管理帳戶匯出或備份報告，尤其是帳單報告。當您刪除組織時，不會儲存組織層級報告和歷史記錄。所有成本資料（例如 Cost Explorer 資料集）都會遭到刪除。建議您完整匯出所有帳單歷史記錄。

如需詳細資訊，請參閱[成本和用量報告](#)、[Cost Explorer 報告](#)、[S Savings Plans 報告](#)，以及[預留執行個體 \(RI\) 使用率和涵蓋範圍](#)。

刪除組織

使用下列程序來刪除將先前的管理帳戶還原為不再由 AWS 帳戶 管理的獨立組織 AWS Organizations。

最低許可

若要刪除組織，您必須以管理帳戶中的使用者或角色的身分登入，且您必須擁有以下許可：

- `organizations:DeleteOrganization`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

若要刪除組織

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在您能夠刪除組織之前，您必須先從組織移除所有帳戶。如需詳細資訊，請參閱[使用 從組織移除成員帳戶 AWS Organizations](#)。
3. 導覽至 [Settings](#) (設定) 頁面，然後選擇 Delete organization (刪除組織)。
4. 在 Delete organization (刪除組織) 確認對話方塊中，輸入顯示在文字方塊上方行中的組織 ID。然後，選擇 Delete organization (刪除組織)。

Important

此作業不會關閉管理帳戶，但會將其退回至獨立帳戶 AWS 帳戶。若要關閉帳戶，請遵循[使用 關閉組織中的成員帳戶 AWS Organizations](#) 中的步驟。

AWS CLI & AWS SDKs

下列程式碼範例示範如何使用 DeleteOrganization。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to delete an existing organization using the AWS
```

```

    /// Organizations Service.
    /// </summary>
    public class DeleteOrganization
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
}

```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [DeleteOrganization](#)。

CLI

AWS CLI

刪除組織

下列範例示範如何刪除組織。若要執行此操作，您必須是組織中主要帳戶的管理員。此範例假設您先前已從組織移除所有成員帳戶、OUs 和政策：

```
aws organizations delete-organization
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [DeleteOrganization](#)。

使用 管理組織中的帳戶 AWS Organizations

AWS 帳戶 是 AWS 資源的容器。您可以在 中建立和管理 AWS 資源 AWS 帳戶。

本主題說明如何管理 的帳戶 AWS Organizations。

主題

- [使用 管理管理帳戶 AWS Organizations](#)
- [使用 管理成員帳戶 AWS Organizations](#)
- [使用 管理帳戶邀請 AWS Organizations](#)
- [使用 將帳戶遷移至另一個組織 AWS Organizations](#)
- [在 中檢視帳戶的詳細資訊 AWS Organizations](#)
- [匯出 中所有帳戶的詳細資訊 AWS Organizations](#)
- [更新 中帳戶的替代聯絡人 AWS Organizations](#)
- [更新 中帳戶的主要聯絡資訊 AWS Organizations](#)
- [中的帳戶更新 AWS 區域AWS Organizations](#)

使用 管理管理帳戶 AWS Organizations

管理帳戶是您 AWS 帳戶 用來建立組織的 。

管理帳戶是組織的最終擁有者，可最終控制安全、基礎設施和財務政策。此帳戶具有付款人帳戶的角色，並負責支付其組織中帳戶產生的所有費用。

本主題說明如何使用 管理 帳戶 AWS Organizations。

主題

- [管理帳戶的最佳實務](#)
- [關閉組織中的管理帳戶](#)

管理帳戶的最佳實務

請遵循這些推薦，協助保護 AWS Organizations中管理帳戶的安全。這些推薦假設，您同時遵守[僅將根使用者用於那些真正需要它的任務的最佳實務](#)。

主題

- [限制有權存取管理帳戶的使用者](#)
- [審查並追蹤誰擁有存取權](#)
- [管理帳戶僅用於需要管理帳戶的任務](#)
- [避免將工作負載部署到組織的管理帳戶](#)
- [委派管理帳戶以外的職責來進行去集中化](#)

限制有權存取管理帳戶的使用者

管理帳戶是所有上述管理任務的關鍵，例如帳戶管理、政策、與其他 AWS 服務的整合、合併帳單等。因此，您應該限制管理帳戶的存取權，並將此存取權侷限在需要權限來對組織進行變更的管理員使用者。

審查並追蹤誰擁有存取權

為確保您仍擁有管理帳戶的存取權，請定期檢閱您企業內有權存取與其關聯之電子郵件地址、密碼、MFA 和電話號碼的人員。將您的審查與現有的商業程序保持一致。為了確保只有正確的使用者才能存取，請新增此資訊的每月或每季審查。請確定，復原或重設根使用者憑證存取權的程序不依賴於任何特定個人來完成。所有程序都應解決人們無法使用的預期。

管理帳戶僅用於需要管理帳戶的任務

我們建議您僅將該管理帳戶及其使用者和角色用於必須僅由該帳戶執行的任務。將您的所有 AWS 資源存放在組織中的其他 AWS 帳戶中，並將其保留在管理帳戶中。將資源保存在其他帳戶的一個重要原因是，因為 Organizations 服務控制政策 (SCP) 無法限制管理帳戶中的任何使用者或角色。將資源與管理帳戶分開，也會協助您瞭解發票上的費用。

如需必須從管理帳戶呼叫的任務清單，請參閱[只能從組織的管理帳戶呼叫的操作](#)。

避免將工作負載部署到組織的管理帳戶

獲得授權的作業可以在組織的管理帳戶內執行，SCP 不適用於管理帳戶。這就是為什麼您應該將管理帳戶中包含的雲端資源和資料限制為只能在管理帳戶中管理的資源和資料。

委派管理帳戶以外的職責來進行去集中化

如果可能的話，我們建議在管理帳戶之外委派職責和服務。為您的團隊提供自己帳戶中的權限，以便管理組織的需求，而無需存取管理帳戶。此外，您可以為支援此功能的服務註冊多個委派管理員，

例如用於跨組織 AWS Service Catalog 共用軟體，或用於撰寫和部署堆疊的 AWS CloudFormation StackSets。

如需詳細資訊，請參閱[安全參考架構](#)、[使用多個帳戶組織您的 AWS 環境](#)，以及將成員帳戶註冊為各種 AWS 服務的委派管理員[AWS 服務 您可以搭配 使用 AWS Organizations](#)的建議。

如需設定委派管理員的詳細資訊，請參閱[為 AWS 帳戶管理啟用委派的管理員帳戶](#)和 [的委派管理員 AWS Organizations](#)。

關閉組織中的管理帳戶

若要關閉組織中的管理帳戶，您必須先[關閉](#)或[移除](#)組織中的所有成員帳戶。關閉管理帳戶的行為也會刪除 執行個體，AWS Organizations 以及您在[關閉後期間](#)過後在該組織內建立的任何政策。

關閉管理帳戶

使用下列程序來關閉管理帳戶。

Important

在您關閉管理帳戶之前，強烈建議您檢閱考量事項，並了解關閉帳戶的影響。如需詳細資訊，請參閱 [帳戶管理指南中的關閉帳戶前須知事項](#)和[關閉帳戶後須知事項](#)。AWS

AWS Management Console

從帳戶頁面關閉管理帳戶

Note

您無法直接從 AWS Organizations 主控台關閉管理帳戶。

1. 以您要關閉之管理帳戶的[根使用者 AWS Management Console 身分登入](#)。以 IAM 使用者或角色身分登入時，您無法關閉帳戶。
2. 確認您的組織中沒有剩餘的作用中成員帳戶。若要執行此操作，請前往 [AWS Organizations 主控台](#)。如果您的成員帳戶仍然處於作用中狀態，您將需要遵循 [使用 關閉組織中的成員帳戶 AWS Organizations](#)或 中提供的指引[從組織移除成員帳戶](#)，才能移至下一個步驟。
3. 在右上角的導覽列上，選擇您的帳戶名稱或號碼，然後選擇帳戶。

4. 在[帳戶頁面上](#)，選擇關閉帳戶按鈕。閱讀並確保您了解帳戶關閉指南。
5. 選擇關閉帳戶按鈕以啟動帳戶關閉程序。
6. 您應該會在幾分鐘內收到電子郵件確認，指出您的帳戶已關閉。

AWS CLI & AWS SDKs

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS Management Console。

使用 管理成員帳戶 AWS Organizations

成員帳戶是管理帳戶 AWS 帳戶以外的，屬於組織的一部分。

本主題說明如何使用 管理成員帳戶 AWS Organizations。

主題

- [成員帳戶最佳實務](#)
- [使用 在組織中建立成員帳戶 AWS Organizations](#)
- [使用 存取組織中的成員帳戶 AWS Organizations](#)
- [使用 關閉組織中的成員帳戶 AWS Organizations](#)
- [使用 保護成員帳戶免於關閉 AWS Organizations](#)
- [使用 從組織移除成員帳戶 AWS Organizations](#)
- [使用 從成員帳戶離開組織 AWS Organizations](#)
- [使用 更新成員帳戶的帳戶名稱 AWS Organizations](#)
- [使用 更新成員帳戶的根使用者電子郵件地址AWS Organizations](#)

成員帳戶最佳實務

請遵循這些推薦，協助保護組織中成員帳戶的安全。這些推薦假設，您同時遵守[僅將根使用者用於那些真正需要它的任務的最佳實務](#)。

主題

- [定義帳戶名稱和屬性](#)

- [有效率地擴展您的環境和帳戶使用情況](#)
- [啟用根存取管理，以簡化管理成員帳戶的根使用者憑證](#)

定義帳戶名稱和屬性

對於您的會員帳戶，請使用反映帳戶使用情況的命名結構和電子郵件地址。例如，Workloads+fooA+dev@domain.com 用於 WorkloadsFooADev，Workloads+fooB+dev@domain.com 用於 WorkloadsFooBDev。如果您已為組織定義了自訂標籤，建議您在反映帳戶使用情況、成本中心、環境和專案的帳戶上指派這些標籤。如此可讓您更容易識別、組織和搜尋帳戶。

有效率地擴展您的環境和帳戶使用情況

當您擴展時，在建立新帳戶之前，請確保不存在類似需求的帳戶，以避免不必要的重複。AWS 帳戶應基於常見的存取需求。如果您打算重複使用這些帳戶（例如沙盒帳戶或同等帳戶），建議您清除帳戶中不需要的資源或工作負載，但儲存帳戶以供日後使用。

關閉帳戶之前，請注意，這些帳戶必須遵守關閉帳戶配額限制。如需詳細資訊，請參閱[配額和服務限制 AWS Organizations](#)。考慮實作清理過程以重複使用帳戶，而不是關閉帳戶，並在可能的情況下建立新帳戶。如此一來，您就可以避免因執行資源而產生成本，並達到 [CloseAccount API](#) 限制。

啟用根存取管理，以簡化管理成員帳戶的根使用者憑證

我們建議您啟用根存取管理，以協助您監控和移除成員帳戶的根使用者憑證。根存取管理可防止復原根使用者憑證，從而改善組織中的帳戶安全性。

- 移除成員帳戶的根使用者憑證，以防止登入根使用者。這也可防止成員帳戶復原根使用者。
- 擔任特殊權限工作階段，在成員帳戶上執行下列任務：
 - 移除設定錯誤的儲存貯體政策，此政策拒絕所有主體存取 Amazon S3 儲存貯體。
 - 刪除拒絕所有主體存取 Amazon SQS 佇列的 Amazon Simple Queue Service 資源型政策。
 - 允許成員帳戶復原其根使用者憑證。有權存取成員帳戶根使用者電子郵件收件匣的人員可以重設根使用者密碼，並以成員帳戶根使用者身分登入。

啟用根存取管理後，新建立的成員帳戶預設是secure-by-default，沒有根使用者憑證，因此不需要額外的安全性，例如佈建後的 MFA。

如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[集中成員帳戶的根使用者憑證](#)。

使用 SCP 來限制成員帳戶中根使用者可執行的動作

建議您在組織中建立服務控制政策 (SCP)，並將其附加至組織的根，以便套用至所有成員帳戶。如需詳細資訊，請參閱[保護您的 Organizations 帳戶的根使用者登入資料](#)。

您可以拒絕所有根動作，唯必須在成員帳戶中執行的特定僅限根動作除外。例如，下列 SCP 可防止任何成員帳戶中的根使用者進行任何 AWS 服務 API 呼叫，除了「更新設定錯誤且拒絕存取所有主體的 S3 儲存貯體政策」（需要根登入資料的動作之一）。如需詳細資訊，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
      }
    }
  ]
}
```

在大多數情況下，任何管理任務都可由成員帳戶中具有相關管理員許可的 AWS Identity and Access Management (IAM) 角色執行。任何此類角色均應將套用適當的控制，以限制、記錄和監控活動。

使用 在組織中建立成員帳戶 AWS Organizations

本主題說明如何 AWS 帳戶 在組織中建立 AWS Organizations。如需建立單一 的相關資訊 AWS 帳戶，請參閱 [入門資源中心](#)。

建立成員帳戶之前的考量事項

Organizations 會自動**OrganizationAccountAccessRole**為成員帳戶建立 IAM 角色

當您在組織中建立成員帳戶時，Organizations 會自動**OrganizationAccountAccessRole**在成員帳戶中建立 IAM 角色，讓管理帳戶中的使用者和角色能夠對成員帳戶執行完整的管理控制。每當政策更新時，連接到相同受管政策的任何其他帳戶都會自動更新。這個角色會受限於套用至成員帳戶的任何[服務控制政策 \(SCP\)](#)。

Organizations 會自動**AWSServiceRoleForOrganizations**為成員帳戶建立服務連結角色

當您在組織中建立成員帳戶時，Organizations 會自動**AWSServiceRoleForOrganizations**在成員帳戶中建立服務連結角色，以啟用與特定 AWS 服務的整合。您必須設定其他服務以允許整合。如需詳細資訊，請參閱[AWS Organizations 和服務連結角色](#)。

成員帳戶只能在組織的根目錄中建立

組織中的成員帳戶只能在組織的根目錄中建立。建立組織的成員帳戶根之後，您可以在 OUs 之間移動它。如需詳細資訊，請參閱[使用 將帳戶移至組織單位 \(OU\) 或根和 OUs 之間 AWS Organizations](#)。

連接到根的政策會立即套用

如果您有任何連接到根的政策，這些政策會立即套用到所建立帳戶中的所有使用者和角色。

如果您已為 [AWS 組織啟用其他服務的服務信任](#)，則該信任的服務可以建立服務連結角色，或在組織中任何成員帳戶中執行動作，包括您建立的帳戶。

成員帳戶必須選擇接收行銷電子郵件

您建立做為組織一部分的成員帳戶不會自動訂閱 AWS 行銷電子郵件。若要選擇加入您的帳戶以接收行銷電子郵件，請參閱<https://pages.awscloud.com/communication-preferences>。

由 管理的組織成員帳戶 AWS Control Tower 應在 中建立 AWS Control Tower

如果您的組織由 管理 AWS Control Tower，我們建議您使用 AWS Control Tower 主控台下的帳戶工廠或使用 AWS Control Tower APIs來建立您的成員 AWS Control Tower 帳戶。

如果您在 Organizations 中於組織管理組織時建立成員帳戶 AWS Control Tower，該帳戶將不會向註冊 AWS Control Tower。如需詳細資訊，請參閱AWS Control Tower 使用者指南中的[參照 AWS Control Tower外部資源](#)。

建立成員帳戶

登入組織的管理帳戶後，您可以建立屬於組織一部分的成員帳戶。

當您使用下列程序建立帳戶時，AWS Organizations 會自動將下列主要聯絡資訊從管理帳戶複製到新成員帳戶：

- 電話號碼
- 公司名稱
- 網站 URL
- Address

Organizations 也會從管理帳戶複製通訊語言和 Marketplace 資訊（某些帳戶的供應商 AWS 區域）。

最低許可

若要在您的組織中建立成員帳戶，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:CreateAccount`
- `iam:CreateServiceLinkedRole`

AWS Management Console

建立自動 AWS 帳戶 成為您組織一部分的

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，選擇新增 AWS 帳戶。
3. 在[新增 AWS 帳戶](#) 頁面上，選擇建立 AWS 帳戶(預設會選擇該項)。
4. 在[建立 AWS 帳戶](#) 頁面，針對AWS 帳戶 名稱，輸入您要指派給帳戶的名稱。此名稱可協助您區分該帳戶與組織中的所有其他帳戶，並且與 IAM 別名或擁有者的電子郵件名稱不同。

5. 針對帳戶擁有者的電子郵件地址，輸入帳戶擁有者的電子郵件地址。此電子郵件地址無法與另一個電子郵件地址建立關聯，AWS 帳戶 因為它會成為帳戶根使用者的使用者名稱憑證。
6. (選用) 指定要在新帳戶中自動建立、要指派給 IAM 角色的名稱。此角色會授予組織的管理帳戶許可，以存取新建立的成員帳戶。如果您未指定名稱，會將預設名稱 AWS Organizations 提供給角色 `OrganizationAccountAccessRole`。建議您在所有帳戶中使用預設名稱以確保一致性。

⚠ Important

請記住此角色名稱。稍後您會需要它，以便為管理帳戶中的使用者和角色授予新帳戶的存取權。

7. (選用) 在 Tags (標籤) 區段中，透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至新帳戶。將值留空會將其設定為空白字串；而不是 null。您可以在帳戶中連接最多 50 個標籤。
8. 選擇建立 AWS 帳戶。
 - 如果您收到錯誤，指出您已超出組織的帳戶配額，請參閱[當我試著新增帳戶到我的組織時，出現「超過配額」訊息](#)。
 - 如果您收到錯誤，指出因為您的組織仍在初始化，您無法新增帳戶，請等候一小時然後重試。
 - 您也可以檢查 AWS CloudTrail 日誌，以取得帳戶建立是否成功的相關資訊。如需詳細資訊，請參閱[在中記錄和監控 AWS Organizations](#)。
 - 如果錯誤仍存在，請聯絡 [AWS 支援](#)。

出現 [AWS 帳戶](#) 頁面時，將您的新帳戶新增至清單。

9. 現在帳戶已存在，並且具有的 IAM 角色可授予管理員存取給管理帳戶中的使用者，您可以遵循 [使用 存取組織中的成員帳戶 AWS Organizations](#) 中的步驟來存取帳戶。

AWS CLI & AWS SDKs

下列程式碼範例示範如何使用 `CreateAccount`。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;

        Console.WriteLine($"The status of {status.AccountName} is {status.State}.");
    }
}
```

```
}
```

- 如需 API 詳細資訊，請參閱適用於 .NET 的 AWS SDK 《API 參考》中的 [CreateAccount](#)。

CLI

AWS CLI

建立自動成為組織一部分的成員帳戶

下列範例顯示如何在 組織中建立成員帳戶。成員帳戶是以生產帳戶名稱和 susan@example.com 的電子郵件地址設定。Organizations 會使用 OrganizationAccountAccessRole 的預設名稱自動建立 IAM 角色，因為未指定 roleName 參數。此外，由於未指定 iamUserAccessToBilling 參數，因此允許具有足夠許可存取帳戶帳單資料的 IAM 使用者或角色的設定會設定為預設值 ALLOW。Organizations 會自動傳送「歡迎 AWS」電子郵件給 Susan：

```
aws organizations create-account --email susan@example.com --account-name "Production Account"
```

輸出包含一個請求物件，顯示狀態現在為 IN_PROGRESS：

```
{
  "CreateAccountStatus": {
    "State": "IN_PROGRESS",
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

您稍後可以透過將 Id 回應值作為 create-account-request-id 參數的值提供給 describe-create-account-status 命令來查詢請求的目前狀態。

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的在您的組織中建立 AWS 帳戶。

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [CreateAccount](#)。

使用 存取組織中的成員帳戶 AWS Organizations

當您在組織中建立帳戶時，除了根使用者之外，AWS Organizations 還會自動建立名為 `OrganizationAccountAccessRole` 的 IAM 角色。您可以在建立時指定不同的名稱，但我們建議您在所有帳戶中一致命名。AWS Organizations 不會建立任何其他使用者或角色。

若要存取組織中的帳戶，您必須使用以下其中一個方法：

最低許可

若要 AWS 帳戶 從組織中的任何其他帳戶存取，您必須具有下列許可：

- `sts:AssumeRole` – Resource 元素必須設為星號 (*) 或需要存取新成員帳戶之使用者帳戶的帳戶 ID

Using the root user (Not recommended for everyday tasks)

當您在組織中建立新的成員帳戶時，該帳戶預設沒有根使用者登入資料。成員帳戶無法登入其根使用者，也無法為其根使用者執行密碼復原 (除非啟用帳戶復原)。

您可以[集中成員帳戶的根存取權](#)，以移除組織中現有成員帳戶的根使用者憑證。刪除根使用者憑證會移除根使用者密碼、存取金鑰、簽署憑證，並停用多重驗證 (MFA)。這些成員帳戶沒有根使用者憑證，無法以根使用者身分登入，而且無法復原根使用者密碼。您在 Organizations 中建立的新帳戶預設沒有根使用者憑證。

如果您需要在不存在根使用者憑證的成員帳戶上執行需要根使用者憑證的任務，請聯絡您的管理員。

若要以根使用者的身分存取您的成員帳戶，您必須完成密碼復原程序。如需詳細資訊，請參閱 AWS 登入使用者指南中的[我忘記 的根使用者密碼 AWS 帳戶](#)。

如果您必須使用根使用者存取成員帳戶，請遵循下列最佳實務：

- 除了建立具有更有限許可的其他使用者和角色之外，請勿使用根使用者來存取您的帳戶。然後，以這些使用者或角色身分登入。
- 在[根使用者上啟用多重驗證 \(MFA\)](#)。重設密碼，並[將 MFA 裝置指派給根使用者](#)。

如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。如需其他根使用者安全建議，請參閱《IAM 使用者指南》中的[的根使用者最佳實務 AWS 帳戶](#)。

Using trusted access for IAM Identity Center

使用 [AWS IAM Identity Center](#) 並啟用 IAM Identity Center 的受信任存取 AWS Organizations。這可讓使用者使用其公司登入資料登入 AWS 存取入口網站，並存取其指派管理帳戶或成員帳戶中的資源。

如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[多帳戶許可](#)。如需設定 IAM Identity Center 的受信任存取的詳細資訊，請參閱 [AWS IAM Identity Center](#) 和 [AWS Organizations](#)。

Using the IAM role OrganizationAccountAccessRole

如果您使用提供的工具來建立帳戶 AWS Organizations，您可以使用您以此方式建立的所有新帳戶中，名為 OrganizationAccountAccessRole 的預先設定角色來存取帳戶。如需詳細資訊，請參閱[使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations](#)。

若是邀請現有帳戶加入組織，而該帳戶也接受邀請，您可以選擇建立 IAM 角色，以允許管理帳戶存取受邀的成員帳戶。此角色與 AWS Organizations 建立的帳戶中自動新增的角色完全相同。

若要建立角色，請參閱[使用 為受邀帳戶建立 OrganizationAccountAccessRole AWS Organizations](#)。

在您建立角色後，您便可以使用[使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations](#)中的步驟來存取它。

主題

- [使用 為受邀帳戶建立 OrganizationAccountAccessRole AWS Organizations](#)
- [使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations](#)

使用 為受邀帳戶建立 OrganizationAccountAccessRole AWS Organizations

依預設，如果您隨著組織建立成員帳戶，AWS 會自動在帳戶中建立一個角色，為管理帳戶中可以擔任該角色的 IAM 使用者授予管理員許可。在預設情況下，該角色名為 OrganizationAccountAccessRole。如需詳細資訊，請參閱[使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations](#)。

不過，您邀請加入組織的成員帳戶，不會自動建立管理員角色。您可以手動執行此動作，如以下程序所示。這基本上會複製自動為已建立帳戶設定的角色。我們建議您為手動建立的角色使用相同的名稱 `OrganizationAccountAccessRole`，以保有一致性並方便記住。

AWS Management Console

在成員帳戶中建立 AWS Organizations 管理員角色

1. 登入 IAM 主控台，網址為 <https://console.aws.amazon.com/iam/>。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 ([不建議](#))。使用者或角色必須具有建立 IAM 角色和政策的許可。
2. 在 IAM 主控台中，導覽至角色，然後選擇建立角色。
3. 選擇 AWS 帳戶，然後選擇另一個 AWS 帳戶。
4. 輸入您要授予管理員存取權之管理帳戶的 12 位數帳戶 ID 號碼。在選項下，請注意下列事項：
 - 針對此角色，因為帳戶是公司內部帳戶，您不應該選擇 Require external ID (需要外部 ID)。如需外部 ID 選項的詳細資訊，請參閱《IAM 使用者指南》中的[何時應使用外部 ID？](#)。
 - 如果您已啟用和設定 MFA 身分驗證，您可以選擇性地要求使用 MFA 裝置進行身分驗證。如需 MFA 的詳細資訊，請參閱《IAM 使用者指南》中的[使用多重要素驗證 \(MFA\) AWS](#)。
5. 選擇 Next (下一步)。
6. 在新增許可頁面上，選擇名為 `AdministratorAccess` 的 AWS 受管政策，然後選擇下一步。
7. 在名稱、檢閱和建立頁面上，指定角色名稱和選用描述。為求與新帳戶中指派給角色的預設名稱一致，建議您使用 `OrganizationAccountAccessRole`。若要遞交您的變更，請選擇 Create role (建立角色)。
8. 您的新角色會顯示在可用的角色清單中。選擇新角色的名稱來檢視其詳細資訊，特別注意提供的連結 URL。將此 URL 提供給成員帳戶中，需要存取角色的使用者。此外，請記下 Role ARN (角色 ARN)，因為您在步驟 15 中將需要它。
9. 登入 IAM 主控台，網址為 <https://console.aws.amazon.com/iam/>。這時，以管理帳戶中擁有許可可能建立政策和將政策指派給使用者或群組的使用者身分登入。
10. 導覽至政策，然後選擇建立政策。
11. 針對 Service (服務)，選擇 STS。
12. 針對動作，首先在篩選條件方塊中輸入 **AssumeRole**，然後在出現時選中旁邊的核取方塊。
13. 在資源下，確定已選取特定，然後選擇新增 ARNs。

14. 輸入 AWS 成員帳戶 ID 號碼，然後輸入您先前在步驟 1–8 中建立的角色名稱。選擇新增 ARN。
15. 如果您要授予許可以擔任多個成員帳戶中的角色，請對每個帳戶重複步驟 14 和 15。
16. 選擇 Next (下一步)。
17. 在檢閱和建立頁面上，輸入新政策的名稱，然後選擇建立政策以儲存變更。
18. 在導覽窗格中選擇使用者群組，然後選擇您要用來委派成員帳戶管理的群組名稱（而非核取方塊）。
19. 選擇許可索引標籤標籤。
20. 選擇新增許可，選擇連接政策，然後選擇您在步驟 11–18 中建立的政策。

所選取群組成員的使用者現在可以使用您在步驟 9 中擷取的 URL 來存取每個成員帳戶的角色。他們可以透過您在組織中所建立帳戶的相同方式存取這些成員帳戶。如需使用角色來管理成員帳戶詳細資訊，請參閱[使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations](#)。

使用 存取具有 OrganizationAccountAccessRole 的成員帳戶 AWS Organizations

當您使用 AWS Organizations 主控台建立成員帳戶時，AWS Organizations 會自動在帳戶中建立名為 OrganizationAccountAccessRole 的 IAM 角色。此角色擁有成員帳戶內的完整管理許可。此角色的存取範圍包括管理帳戶中的所有主體，因此該角色設定為授予對該組織管理帳戶的存取權。

您可以遵循 [使用 為受邀帳戶建立 OrganizationAccountAccessRole AWS Organizations](#) 中的步驟，為獲邀請成員帳戶建立完全相同的角色。

若要使用此角色來存取成員帳戶，您必須以管理帳戶帳戶中擁有擔任此角色許可的使用者身分登入。若要設定這些許可，請執行下列程序。我們建議您將許可授予群組，而不是使用者，以方便維護。

AWS Management Console

授予管理帳戶中 IAM 群組成員的許可以存取角色

1. 登入 IAM 主控台 (<https://console.aws.amazon.com/iam/>)，以管理帳戶中擁有管理員許可的使用者身分。需要此項，才能將許可委派給其使用者將存取成員帳戶中角色的 IAM 群組。
2. 透過建立您稍後在[???](#)中需要的受管理政策來開始。

在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。

3. 在視覺化編輯器索引標籤上，選擇選擇服務，STS 在搜尋方塊中輸入 以篩選清單，然後選擇 STS 選項。

4. 在動作區段**assume**中，在搜尋方塊中輸入 以篩選清單，然後選擇 AssumeRole 選項。
5. 在資源區段中，選擇特定，選擇新增 ARNs
6. 在指定 ARN (s) 區段中，選擇其他帳戶以用於其中的資源。
7. 輸入您剛建立的成員帳戶的 ID
8. 對於具有路徑的資源角色名稱，輸入您在上一節中建立的角色名稱（建議將其命名為 OrganizationAccountAccessRole）。
9. 當對話方塊顯示正確的 ARNs 時，選擇新增 ARN。
10. (選擇性) 如果您想要要求多重因素認證 (Multi-Factor Authentication, MFA)，或限制來自指定 IP 地址範圍的角色存取，請展開「請求條件」區段，然後選取您要強制執行的選項。
11. 選擇 Next (下一步)。
12. 在檢閱和建立頁面上，輸入新政策的名稱。例如：**GrantAccessToOrganizationAccountAccessRole**。您也可以加入選用說明。
13. 選擇 Create policy (建立政策) 以儲存您的新受管政策。
14. 現在有了可用的政策，您就可以將其連接到群組。

在導覽窗格中，選擇使用者群組，然後選擇您要能夠擔任成員帳戶中角色之成員的群組名稱（而非核取方塊）。如果需要，您可以建立新群組。

15. 選擇 許可 標籤、選擇 新增許可，然後選擇 連接政策。
16. (選擇性) 在 Search (搜尋) 方塊中，您可以開始輸入政策名稱以篩選清單，直到您可以看到剛剛在[Step 2](#) 到[Step 13](#) 建立的政策名稱為止。您也可以選擇所有類型，然後選擇客戶 AWS 受管，篩選掉所有受管政策。
17. 勾選政策旁的方塊，然後選擇連接政策。

屬於群組成員的 IAM 使用者現在具有許可，可以使用下列程序在 AWS Organizations 主控台中切換到新角色。

AWS Management Console

切換到成員帳戶的角色

使用角色時，使用者擁有新成員帳戶中的管理員許可。指示身為群組成員的 IAM 使用者，執行下列動作切換到新的角色。

1. 從 AWS Organizations 主控台的右上角，選擇包含您目前登入名稱的連結，然後選擇切換角色。

2. 輸入管理員提供的帳戶 ID 號碼和角色名稱。
3. 對於 Display Name (顯示名稱)，輸入您要在右上角導覽列中顯示的文字，以在您使用該角色時取代您的使用者名稱。您可以選擇性地選擇顏色。
4. 選擇 Switch Role (切換角色)。現在您執行的所有動作，都是使用授予您切換目標角色的許可所完成。在您切換回去之前，您將不再擁有與原始 IAM 使用者建立關聯的許可。
5. 在您完成需要角色許可的執行動作後，您便可以切換回您的一般 IAM 使用者。在右上角 (任何您指定為 Display Name (顯示名稱) 的項目) 選擇角色名稱，然後選擇 Back to **UserName** (切換回 UserName)。

使用 關閉組織中的成員帳戶 AWS Organizations

如果您不再需要組織中的成員帳戶，您可以按照本主題中的指示，從[AWS Organizations 主控台](#)將其關閉。如果您的組織處於[所有功能](#)模式，您只能使用 AWS Organizations 主控台關閉成員帳戶。

您也可以在以根使用者身分登入 AWS Management Console 後 AWS 帳戶，直接從 中的[帳戶頁面](#)關閉。如需step-by-step說明，請參閱《AWS 帳戶管理指南》中的[關閉 AWS 帳戶](#)。

若要關閉管理帳戶，請參閱 [關閉組織中的管理帳戶](#)。

關閉成員帳戶

登入組織的管理帳戶時，您可以關閉屬於組織一部分的成員帳戶。若要執行此動作，請執行下列步驟。

Important

在關閉您的成員帳戶之前，強烈建議您檢閱考量事項，並了解關閉帳戶的影響。如需詳細資訊，請參閱 [《帳戶管理指南》中的關閉帳戶前的須知事項](#)和[關閉帳戶後的須知事項](#)。AWS

AWS Management Console

從 AWS Organizations 主控台關閉成員帳戶

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者身分登入，或以組織的管理帳戶中的根使用者身分登入 ([不建議](#))。
2. 在 [AWS 帳戶](#) 頁面上，尋找並選擇您要關閉的成員帳戶名稱。您可以導覽 OU 階層，或查看沒有 OU 結構的帳戶平面清單。

3. 選擇頁面頂端帳戶名稱旁的 Close (關閉)。只有在組織處於[所有功能](#)模式時，AWS 才能使用此選項。

 Note

如果您的組織使用[合併帳單](#)模式，您將無法在主控台中看到關閉按鈕。若要以合併帳單模式關閉帳戶，請登入您要以根使用者身分關閉的帳戶。在帳戶頁面上，選擇關閉帳戶按鈕，輸入您的帳戶 ID，然後選擇關閉帳戶按鈕。

4. 閱讀並確保您了解帳戶關閉指引。
5. 輸入成員帳戶 ID，然後選擇關閉帳戶。

 Note

您關閉的任何成員帳戶會在其帳戶名稱旁，於 AWS Organizations 主控台中顯示 SUSPENDED 標籤，最長至原始關閉日期後 90 天。90 天後，成員帳戶將不再顯示在 AWS Organizations。

從帳戶頁面關閉成員帳戶

或者，您也可以直接從 中的帳戶頁面關閉 AWS 成員帳戶 AWS Management Console。如需 step-by-step 指引，請遵循《AWS 帳戶管理指南》中[關閉 AWS 帳戶](#) 中的指示。

AWS CLI & AWS SDKs

關閉 AWS 帳戶

您可以使用下列其中一項命令來關閉 AWS 帳戶：

- AWS CLI：[close-account](#)。

```
$ aws organizations close-account \
  --account-id 123456789012
```

此命令成功後就不會產生輸出。

- AWS SDKs：[CloseAccount](#)

使用 保護成員帳戶免於關閉 AWS Organizations

為了保護成員帳戶免於意外關閉，請建立 IAM 政策，指定哪些帳戶可豁免。此政策可防止關閉受保護的成員帳戶。

建立 IAM 政策以使用下列其中一種方法拒絕帳戶關閉：

- 使用政策的 ARNs 明確列出政策Resource元素中的受保護帳戶。
- 標記個別帳戶並使用aws:ResourceTag全域條件金鑰，以防止關閉已標記的帳戶。

服務控制政策無法保護成員帳戶

服務控制政策 (SCPs) 無法辨識成員帳戶SCPs 不會影響管理帳戶中的 IAM 主體。

防止關閉成員帳戶的範例 IAM 政策

下列程式碼範例顯示兩種不同的方法來限制成員帳戶關閉其帳戶。

Prevent member accounts with tags from getting closed

您可以將以下政策連接至管理帳戶中的身分。此政策可防止管理帳戶中的主體關閉任何加上aws:ResourceTag 標籤全域條件金鑰、AccountType 索引鍵和 Critical 標籤值的成員帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventCloseAccountForTaggedAccts",
      "Effect": "Deny",
      "Action": "organizations:CloseAccount",
      "Resource": "*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
      }
    }
  ]
}
```

Prevent member accounts listed in this policy from getting closed

您可以將以下政策連接至管理帳戶中的身分。此政策可防止管理帳戶中的主體關閉 Resource 元素中明確指定的成員帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventCloseAccount",
      "Effect": "Deny",
      "Action": "organizations:CloseAccount",
      "Resource": [
        "arn:aws:organizations::555555555555:account/o-12345abcdef/123456789012",
        "arn:aws:organizations::555555555555:account/o-12345abcdef/123456789014"
      ]
    }
  ]
}
```

使用 從組織移除成員帳戶 AWS Organizations

移除成員帳戶並不會關閉帳戶，而是會從組織移除成員帳戶。前成員帳戶會成為 AWS 帳戶 不再由管理的獨立帳戶 AWS Organizations。

之後，該帳戶不再受任何政策的約束，並負責自己的帳單支付。從組織移除帳戶後，該組織的管理帳戶不會再針對該帳戶所累積的任何費用收費。

考量事項

管理帳戶建立的 IAM 存取角色不會自動刪除

當您從組織中移除成員帳戶時，不會自動刪除為啟用組織管理帳戶存取權而建立的任何 IAM 角色。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

只有在帳戶擁有以獨立帳戶運作所需的資訊時，您才能從組織移除帳戶

只有在帳戶具有讓它以獨立帳戶形式運作所需的資訊時，您才能從組織移除帳戶。當您使用 AWS Organizations 主控台、API 或 AWS CLI 命令在組織中建立帳戶時，不會自動收集獨立帳戶所需的所有資訊。

對於您要獨立建立的每個帳戶，您必須選擇支援計畫、提供並驗證所需的聯絡資訊，並提供目前的付款方式。AWS 會使用 付款方式來收取帳戶未連接到組織時所發生的任何計費（非 AWS 免費方案）AWS 活動的費用。若要移除尚未取得此資訊的帳戶，請依照 [使用 從成員帳戶離開組織 AWS Organizations](#) 中的步驟執行。

您必須等到帳戶建立後至少七天

若要移除您在組織中建立的帳戶，您必須等到帳戶建立後至少七天。受邀的帳戶不受此等待期限的限制。

離開的帳戶擁有者會負責所有累積的新成本

帳戶成功離開組織時，的擁有者 AWS 帳戶 會負責所有累積的新 AWS 成本，並使用帳戶的付款方式。組織的管理帳戶不再負責。

帳戶不能是為組織啟用的任何 AWS 服務的委派管理員帳戶

您要移除的帳戶不得是為組織啟用的任何 AWS 服務的委派管理員帳戶。如果帳戶是委派的系統管理員，您必須先將委派的管理員帳戶變更為組織中剩餘的另一個帳戶。如需如何停用或變更 AWS 服務委派管理員帳戶的詳細資訊，請參閱該服務的文件。

帳戶不再有權存取成本和用量資料

當成員帳戶離開組織時，該帳戶就不再能夠帳戶存取作為組織成員期間的成本和使用狀況資料。不過，組織的管理帳戶仍然可以存取資料。如果帳戶重新加入組織，帳戶便能再次存取資料。

會刪除連接至帳戶的標籤

當成員帳戶離開組織時，會刪除連接至該帳戶的所有標籤。

帳戶中的主體不再受到任何組織政策的影響

帳戶中的委託人不再受組織中套用的任何[政策](#)的影響。這表示 SCP 實施的限制將不再有效，而帳戶中的使用者和角色可能會較以前具有更多的許可。其他組織政策類型無法再強制執行或處理。

組織協議不再涵蓋該帳戶

如果成員帳戶被從組織中移除，該成員帳戶即不再涵蓋於組織協議中。管理帳戶管理員應在從組織移除成員帳戶之前，與成員帳戶溝通此事，以便在必要時成員帳戶可以簽訂新的協議。您可以在 [Organization Agreements](#) 頁面的 AWS Artifact 主控台中檢視作用中組織協議的清單。 [AWS Artifact](#)

可能會停用與其他 服務的整合

與其他服務的整合可能會停用。如果您從已啟用與服務整合的組織中移除帳戶 AWS，則該帳戶中的使用者將無法再使用該服務。

從組織移除成員帳戶

登入組織的管理帳戶時，您可以從組織移除您不再需要的成員帳戶。若要這麼做，請執行下列作業：此程序僅適用於成員帳戶。若要移除管理帳戶，您必須[刪除組織](#)。

最低許可

若要從組織中移除一個或多個成員帳戶，您必須以管理帳戶中具有以下許可的使用者或角色身分登入：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:RemoveAccountFromOrganization`

如果您在步驟 5 中選擇以成員帳戶中的使用者或角色的身分登入，則該使用者或角色必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:LeaveOrganization` – 請注意，組織管理員可以套用會移除此許可的政策到您的帳戶，以防止您從您的組織移除帳戶。
- 如果您以 IAM 使用者的身分登入，而且帳戶缺少付款資訊，則使用者必須擁有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 許可 (若該帳戶尚未遷移至精細許可) 或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 許可 (若該帳戶已遷移至精細許可)。此外，成員帳戶必須已啟用 IAM 使用者對帳單的存取權。如果尚未啟用，請參閱 AWS Billing 使用者指南中的[啟用帳單和成本管理主控台的存取權](#)。

AWS Management Console

從組織移除成員帳戶

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，尋找並選擇您要從您的組織移除的每個成員帳戶旁白的核取方塊



您可以導覽 OU 階層，或 AWS 帳戶 僅啟用檢視，以查看沒有 OU 結構的帳戶清單。如果您有許多帳戶，您可能需要在清單底部選擇載入更多採用 'ou-name' 的帳戶，以尋找您想要移動的所有內容。

在 [AWS 帳戶](#) 頁面上，尋找並選擇您要從您的組織移除的成員帳戶的名稱。您可能需要展開 OU (選擇



以尋找您想要的帳戶。

3. 選擇 Actions (動作)，然後在 AWS 帳戶 下，選擇 Remove from organization (從組織中移除)。
4. 在 Remove account 'account-name' (#account-id-num) from organization? (從組織中移除帳戶 'account-name' (#account-id-num)) 對話方塊中，選擇 Remove account (移除帳戶)。
5. 如果 AWS Organizations 無法移除一或多個帳戶，通常是因為您尚未提供帳戶作為獨立帳戶運作所需的全部資訊。執行以下步驟：
 - a. 登入失敗的帳戶。我們建議您透過選擇 Copy link (複製連結)，然後將連結貼到新無痕瀏覽器視窗的網址列來登入成員帳戶。如果您沒有看到複製連結，請使用[此連結](#)前往註冊 AWS 頁面並完成缺少的註冊步驟。如果您不使用無痕視窗，系統會將您從管理帳戶登出，並且將無法瀏覽回此對話方塊。
 - b. 您的瀏覽器會帶領您直接前往註冊程序，以完成此帳戶遺漏的任何步驟。完成提示的所有步驟。它們可能包含下列項目：
 - 提供聯絡資訊
 - 提供有效的付款方法
 - 驗證電話號碼
 - 選取支援計劃選項
 - c. 完成最後一個註冊步驟後，AWS 會自動將您的瀏覽器重新導向至成員帳戶的 AWS Organizations 主控台。選擇 Leave organization (離開組織)，然後在確認對話方塊中確認

您的選擇。系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視任何擱置邀請，以便帳戶加入其他組織的。

- d. 從組織移除授予帳戶存取權的 IAM 角色。

 Important

如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

AWS CLI & AWS SDKs

從組織移除成員帳戶

您可以使用下列其中一項命令來移除成員帳戶：

- AWS CLI: [remove-account-from-organization](#)

```
$ aws organizations remove-account-from-organization \
  --account-id 123456789012
```

此命令成功後就不會產生輸出。

- AWS SDKs : [RemoveAccountFromOrganization](#)

從組織移除帳戶之後，請確保從組織移除授予此帳戶存取權的 IAM 角色。

 Important

如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶

的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

會員帳戶可以使用 [leave-organization](#) 來移除自己。如需詳細資訊，請參閱[使用 從成員帳戶離開組織 AWS Organizations](#)。

使用 從成員帳戶離開組織 AWS Organizations

當您登入成員帳戶時，您可以離開組織。管理帳戶無法使用此技術來離開組織。若要移除管理帳戶，您必須[刪除組織](#)。

考量事項

具有組織的帳戶狀態會影響可見的成本和用量資料

如果成員帳戶離開組織而成為獨立帳戶，則帳戶一旦是組織之成員就無法再存取時間範圍內的成本和用量資料。帳戶只能存取做為獨立帳戶時所產生的資料。

如果成員帳戶離開組織 A 而加入組織 B，則此帳戶就無法再存取其做為組織 A 成員之時間範圍內來自組織 A 的成本和用量資料。帳戶只能存取做為組織 B 成員時所產生的資料。

如果帳戶重新加入先前所屬的組織，此帳戶會重新獲得對其過去成本與使用狀況資料的存取權。

該帳戶不再受代表其接受的組織協議所涵蓋

如果您離開某個組織，您將不再受到組織的管理帳戶代表您接受的組織協議的涵蓋。您可以在 Organization Agreements 頁面的 AWS Artifact 主控台中檢視這些[AWS Artifact 組織協議](#)的清單。離開組織之前，您應該判斷 (適當時，在您的法律、隱私權或合規團隊的協助下) 是否有必要設立新的協議。

從成員帳戶離開組織

若要離開組織，請完成下列程序。

最低許可

若要離開 組織，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

- `organizations:LeaveOrganization` – 請注意，組織管理員可以套用會移除此許可的政策到您的帳戶，以防止您從您的組織移除帳戶。
- 如果您以 IAM 使用者的身分登入，而且帳戶缺少付款資訊，則使用者必須擁有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 許可 (若該帳戶尚未遷移至精細許可) 或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 許可 (若該帳戶已遷移至精細許可)。此外，成員帳戶必須已啟用 IAM 使用者對帳單的存取權。如果尚未啟用，請參閱AWS Billing 使用者指南中的[啟用帳單和成本管理主控台的存取權](#)。

AWS Management Console

若要從成員帳戶離開組織

1. 在 AWS Organizations 主控台登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者的身分登入，擔任 IAM 角色，或以成員帳戶中的根使用者身分登入 ([不建議](#))。

根據預設，您無法存取使用 建立之成員帳戶中的根使用者密碼 AWS Organizations。如有需要，請依照 中的使用根使用者（不建議用於日常任務）中的步驟來復原根使用者密碼[使用 存取組織中的成員帳戶 AWS Organizations](#)。

2. 在[組織儀表板](#)頁面上，選擇離開此組織。
3. 在確認離開組織？對話方塊中，選擇離開組織。收到提示時，確認選擇移除帳戶。確認之後，系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視帳戶加入其他組織的任何待處理邀請。

如果顯示您目前無法離開組織訊息，表示您的帳戶沒有以獨立帳戶運作所需的完整資訊。如果是這種情況，請繼續下一個步驟。

4. 如果確認離開組織？對話方塊顯示您目前無法離開組織訊息，請選擇完成帳戶註冊步驟連結。

如果您沒有看到完成帳戶註冊步驟連結，請使用[此連結](#)前往註冊 AWS頁面完成缺少的註冊步驟。

5. 在註冊 AWS 頁面上，輸入成為獨立帳戶所需的所有必要資訊。可能包括以下資訊類型：

- 聯絡人姓名及地址
- 有效的付款方式
- 電話號碼驗證
- 支援計劃選項

6. 看到說明註冊程序完成的對話方塊時，請選擇 **Leave organization** (離開組織)。

出現確認對話方塊。確認選擇移除帳戶。系統會將您重新導向至 AWS Organizations 主控台的入門頁面，您可以在其中檢視帳戶加入其他組織的任何待處理邀請。

7. 從組織移除授予帳戶存取權的 IAM 角色。

Important

如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

AWS CLI & AWS SDKs

以成員帳戶的身分離開組織

您可以使用下列其中一項命令來離開組織：

- AWS CLI: [leave-organization](#)

下列範例會造成使用其憑證執行命令的帳戶離開組織。

```
$ aws organizations leave-organization
```

此命令成功後就不會產生輸出。

- AWS SDKs : [LeaveOrganization](#)

成員帳戶離開組織後，請確保從組織移除授予此帳戶存取權的 IAM 角色。

Important

如果您的帳戶是在組織中建立的，則 Organizations 會自動在帳戶中建立 IAM 角色，使組織的管理帳戶具有存取權。如果帳戶是受邀加入，則 Organizations 不會自動建立此類角色，但是您或其他管理員可能已建立此類角色以獲得相同的利益。無論是哪一種情況，當您從組織移除帳戶時，任何此類角色都不會自動刪除。如果您想要終止之前的組織管理帳戶

的這種存取權，就必須手動刪除此 IAM 角色。如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

管理帳戶中的使用者也可以改用 [remove-account-from-organization](#) 來移除成員帳戶。如需詳細資訊，請參閱[從組織移除成員帳戶](#)。

使用 更新成員帳戶的帳戶名稱 AWS Organizations

當您登入組織的管理帳戶時，您可以更新成員帳戶的帳戶名稱。若要了解如何更新成員帳戶名稱，請遵循《AWS 帳戶管理 參考指南》[AWS 帳戶 中更新組織中任何的帳戶名稱](#)中的步驟。

使用 更新成員帳戶的根使用者電子郵件地址 AWS Organizations

為了提高安全性和管理彈性，管理帳戶中的 IAM 主體（具有必要的 IAM 許可）可以集中更新其任何成員帳戶的根使用者電子郵件地址（也稱為主要電子郵件地址），而不必個別登入每個帳戶。這可讓管理帳戶（或委派管理員帳戶）中的管理員對其成員帳戶擁有更多控制權。它還確保來自中任何成員帳戶的根使用者電子郵件地址 AWS Organizations 可以保持最新狀態，即使您可能無法存取原始根使用者電子郵件地址或管理登入資料。

當根使用者電子郵件地址由管理帳戶管理員集中變更時，密碼和 MFA 組態將保持與變更之前相同。請注意，控制帳戶的根使用者電子郵件地址和主要聯絡電話號碼的使用者可以略過 MFA。

若要更新組織中成員帳戶的根使用者電子郵件地址，您的組織先前必須啟用[所有功能](#)模式。在合併帳單模式或非組織一部分的帳戶 AWS Organizations 中，無法集中更新其根使用者電子郵件地址。想要變更 API 不支援之帳戶的根使用者電子郵件地址的使用者，應繼續使用帳單主控台來管理其根使用者電子郵件地址。

如需如何更新成員帳戶根使用者電子郵件地址step-by-step說明，請參閱《AWS 帳戶管理 參考指南》[AWS 帳戶 中的為組織中的任何 更新根使用者電子郵件](#)。

使用 管理帳戶邀請 AWS Organizations

在您[建立組織並驗證您擁有與管理帳戶相關聯的電子郵件地址](#)後，您可以邀請現有的 AWS 帳戶 加入您的組織。使用 AWS Organizations 主控台來啟動和管理您傳送給其他帳戶的邀請。您只能從組織的管理帳戶傳送邀請給其他帳戶。

當您邀請帳戶時，AWS Organizations 會傳送邀請給帳戶擁有者，他們可以決定接受或拒絕邀請。

如果您是的管理員 AWS 帳戶，您也可以接受或拒絕來自組織的邀請。如果您接受，您的帳戶會變成該組織的成員。

若要建立自動成為組織一部分的帳戶，請參閱 [使用 在組織中建立成員帳戶 AWS Organizations](#)。

Important

組織中的所有帳戶都必須來自與管理帳戶相同的 AWS 分割區。商業 AWS 區域 分割區中的帳戶不能位於具有來自中國區域分割區或 AWS GovCloud (US) 區域分割區中帳戶的組織。

主題

- [考量事項](#)
- [使用 傳送帳戶邀請 AWS Organizations](#)
- [使用 管理待定帳戶邀請 AWS Organizations](#)
- [使用 接受或拒絕帳戶邀請 AWS Organizations](#)

考量事項

您每天可傳送的邀請數量限制

如需每天可傳送的邀請數量限制，請參閱[最大值和最小值](#)。已接受的邀請不會計入此限制之內。一旦有邀請被接受，當天即可以傳送另一個邀請。必須在 15 天內回應每個邀請，否則邀請會過期。

傳送到帳戶的邀請會計入組織中的帳戶配額。如果受邀帳戶拒絕、管理帳戶取消邀請或邀請過期，則會重設計數。

帳戶只能加入一個組織

帳戶只能加入一個組織。如果您收到多個邀請，您只能接受一個邀請。

帳單歷史記錄和報告會保留在 管理帳戶

所有帳戶的帳單歷史記錄和報告都會保留在 組織中的管理帳戶。將帳戶移至新的組織之前，請匯出或備份任何帳單，並報告您要保留的任何成員帳戶歷史記錄。這可能包括[成本和用量報告](#)、[Cost Explorer報告](#)、[S Savings Plans 報告](#)，以及[預留執行個體 \(RI\) 使用率和涵蓋範圍](#)。

管理帳戶負責成員帳戶產生的所有費用

帳戶接受加入組織的邀請後，組織的管理帳戶會負責支付新成員帳戶產生的所有費用。不再使用連接至成員帳戶的付款方式。而是連接至組織管理帳戶的付款方式來支付成員帳戶產生的所有費用。

Organizations 會自動建立服務連結角色 `AWSServiceRoleForOrganizations`

AWS Organizations 會建立名為 的服務連結角色 [AWSServiceRoleForOrganizations](#)，以支援 AWS Organizations 與其他 AWS 服務之間的整合。如需詳細資訊，請參閱 [AWS Organizations 和服務連結角色](#)。如果您的組織支援 [所有功能](#)，受邀帳戶必須具有此角色。如果組織僅支援 [合併帳單](#) 功能集，您可以刪除此角色。如果您刪除此角色，並在之後啟用組織中的所有功能，會為帳戶 AWS Organizations 重新建立此角色。

Organizations 不會自動建立 IAM 角色 `OrganizationAccountAccessRole`

對於受邀的成員帳戶，AWS Organizations 不會自動建立 IAM 角色 [OrganizationAccountAccessRole](#)。該角色會授予管理帳戶中的使用者存取成員帳戶的管理權限。如果想要啟用對邀請帳戶的該層級管理控制，可以手動新增該角色。如需詳細資訊，請參閱 [使用為受邀帳戶建立 OrganizationAccountAccessRole AWS Organizations](#)。

Note

當您在組織中建立帳戶，而不是邀請現有帳戶加入時，`OrganizationAccountAccessRole` 預設 AWS Organizations 會自動建立 IAM 角色。

連接到包含帳戶的根或 OU 的政策會立即套用

如果您有任何政策連接到包含受邀帳戶的根或組織單位 (OU)，這些政策會立即套用至受邀帳戶中的所有使用者和角色。

您可以 [AWS 為組織啟用其他服務的服務信任](#)。當您這麼做時，該受信任的服務就可以在組織中的任何成員帳戶 (包括受邀的帳戶) 中，建立服務連結角色或執行動作。

只有合併帳單功能集的組織仍可邀請帳戶

您可以邀請帳戶加入只啟用合併帳單功能的組織。如果您稍後想要為組織啟用所有功能，受邀帳戶必須核准變更。

使用 傳送帳戶邀請 AWS Organizations

若要邀請帳戶加入您的組織，您必須先驗證您擁有與管理帳戶關聯的電子郵件地址。如需詳細資訊，請參閱[使用的電子郵件地址驗證 AWS Organizations](#)。在您驗證電子郵件地址之後，請完成下列步驟來邀請帳戶加入您的組織。

最低許可

若要邀請 AWS 帳戶 加入您的組織，您必須具有下列許可：

- `organizations:DescribeOrganization` (僅限主控台)
- `organizations:InviteAccountToOrganization`

AWS Management Console

邀請另一個帳戶加入組織

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 如果您已使用 驗證您的電子郵件地址 AWS，請略過此步驟。

如果您尚未驗證您的電子郵件地址，請在建立組織後 24 小時內遵循[驗證電子郵件](#)中的指示。在您收到驗證電子郵件訊息之前，可能會有一些延遲的時間。驗證您的電子郵件地址之前，您不可邀請帳戶加入您的組織。

3. 導覽至 [AWS 帳戶](#) 頁面，然後選擇 Add an AWS account (新增 AWS 帳戶)。
4. 在 [Add an AWS 帳戶](#) (新增) 頁面中，選擇 Invite an existing AWS account (邀請現有的 AWS 帳戶)。
5. 在[邀請現有 AWS](#)頁面上，針對 AWS 帳戶 要邀請的電子郵件地址或帳戶 ID，輸入與要邀請的帳戶相關聯的電子郵件地址，或其帳戶 ID 號碼。
6. (選用) 對於要包含在邀請電子郵件訊息中的訊息，輸入您要包含在傳送給受邀帳戶擁有者電子郵件邀請中的任何文字。
7. (選用) 在 Add tags (新增標籤) 區段中，指定一個或多個在帳戶管理員接受邀請後自動套用至帳戶的標記。若要執行此操作，請選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值。將值留空會將其設定為空白字串；而不是 null。您可以在 AWS 帳戶中連接最多 50 個標籤。
8. 選擇傳送邀請。

⚠ Important

如果您收到訊息，說明您已超出組織的帳戶配額，或因為您的組織仍在初始化而無法新增帳戶，請聯絡 [AWS 支援](#)。

9. 主控台會將您重新導向至[邀請](#)頁面，您可以在此處檢視所有開啟和已接受的邀請。您剛建立的邀請會出現在清單上方，並且其狀態設定為 OPEN (開啟中)。

AWS Organizations 會將邀請傳送至您邀請加入組織之帳戶擁有者的電子郵件地址。此電子郵件訊息包含 AWS Organizations 主控台的連結，帳戶擁有者可以檢視詳細資訊，並選擇接受或拒絕邀請。或者，受邀帳戶的擁有者可以略過電子郵件訊息、直接前往 AWS Organizations 主控台、檢視邀請，以及接受或拒絕邀請。

對此帳戶的邀請會立即計入您在組織中可以具有的帳戶數量上限。AWS Organizations 不會等候直到帳戶接受邀請。如果獲邀請的帳戶拒絕，則管理帳戶會取消邀請。如果獲邀請的帳戶未在指定的時間期間內回應，則邀請會過期。在這兩種情況下，邀請不會計入您的配額。

AWS CLI & AWS SDKs

邀請另一個帳戶加入組織

您可以使用以下其中一個命令來邀請另一個帳戶加入您的組織：

- AWS CLI: [invite-account-to-organization](#)

```
$ aws organizations invite-account-to-organization \
  --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
  --notes "This is a request for Juan's account to join Bill's organization."
{
  "Handshake": {
    "Action": "INVITE",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
    "ExpirationTimestamp": 1482952459.257,
    "Id": "h-examplehandshakeid111",
    "Parties": [
      {
        "Id": "o-exampleorgid",
        "Type": "ORGANIZATION"
      }
    ]
  }
}
```

```

        {
            "Id": "juan@example.com",
            "Type": "EMAIL"
        }
    ],
    "RequestedTimestamp": 1481656459.257,
    "Resources": [
        {
            "Resources": [
                {
                    "Type": "MASTER_EMAIL",
                    "Value": "bill@amazon.com"
                },
                {
                    "Type": "MASTER_NAME",
                    "Value": "Management Account"
                },
                {
                    "Type": "ORGANIZATION_FEATURE_SET",
                    "Value": "FULL"
                }
            ],
            "Type": "ORGANIZATION",
            "Value": "o-exampleorgid"
        },
        {
            "Type": "EMAIL",
            "Value": "juan@example.com"
        }
    ],
    "State": "OPEN"
}

```

- AWS SDKs : [InviteAccountToOrganization](#)

使用 管理待定帳戶邀請 AWS Organizations

登入到您的管理帳戶時，您可以檢視組織中的所有連結的 AWS 帳戶，以及取消任何等待中 (開啟) 的邀請。若要執行此動作，請執行下列步驟。

最低許可

若要管理組織的等待中邀請，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

AWS Management Console

檢視或取消從您的組織傳送到其他帳戶的邀請

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 導覽至[邀請](#)頁面。

此頁面顯示從您的組織傳送的所有邀請及其目前狀態。

如果您看不到邀請，請檢查受邀帳戶是否為另一個組織的管理帳戶。只有成員帳戶和獨立帳戶才能接收邀請。管理帳戶無法接收邀請。

如果您想要邀請另一個組織中管理帳戶的帳戶，建議您將該帳戶設為獨立帳戶。

Note

已接受、已取消和已拒絕的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

3. 選擇您希望取消邀請旁邊的選項按鈕



然後選擇 `Cancel invitation` (取消邀請)。如果選項按鈕呈現灰色，則無法取消該邀請。

邀請的狀態會從 `Open` (開啟) 變更為 `Canceled` (已取消)。

AWS 會傳送電子郵件訊息給帳戶擁有者，說明您已取消邀請。除非您傳送新的邀請，否則該帳戶不再可以加入組織。

AWS CLI & AWS SDKs

檢視或取消從您的組織傳送到其他帳戶的邀請

您可以使用以下命令來檢視或取消邀請：

- AWS CLI: [list-handshakes-for-organization](#), [cancel-handshake](#)
- 下列範例顯示此組織傳送給其他帳戶的邀請。

```
$ aws organizations list-handshakes-for-organization
{
  "Handshakes": [
    {
      "Action": "INVITE",
      "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
      "ExpirationTimestamp": 1482952459.257,
      "Id": "h-examplehandshakeid111",
      "Parties": [
        {
          "Id": "o-exampleorgid",
          "Type": "ORGANIZATION"
        },
        {
          "Id": "juan@example.com",
          "Type": "EMAIL"
        }
      ],
      "RequestedTimestamp": 1481656459.257,
      "Resources": [
        {
          "Resources": [
            {
              "Type": "MASTER_EMAIL",
              "Value": "bill@amazon.com"
            },
            {
              "Type": "MASTER_NAME",
              "Value": "Management Account"
            },
            {
              "Type": "ORGANIZATION_FEATURE_SET",
              "Value": "FULL"
            }
          ]
        }
      ]
    }
  ]
}
```

```

        }
      ],
      "Type": "ORGANIZATION",
      "Value": "o-exampleorgid"
    },
    {
      "Type": "EMAIL",
      "Value": "juan@example.com"
    },
    {
      "Type": "NOTES",
      "Value": "This is an invitation to Juan's account to join
Bill's organization."
    }
  ],
  "State": "OPEN"
},
{
  "Action": "INVITE",
  "State": "ACCEPTED",
  "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
  "ExpirationTimestamp": 1.471797437427E9,
  "Id": "h-examplehandshakeid222",
  "Parties": [
    {
      "Id": "o-exampleorgid",
      "Type": "ORGANIZATION"
    },
    {
      "Id": "anika@example.com",
      "Type": "EMAIL"
    }
  ],
  "RequestedTimestamp": 1.469205437427E9,
  "Resources": [
    {
      "Resources": [
        {
          "Type": "MASTER_EMAIL",
          "Value": "bill@example.com"
        },
        {
          "Type": "MASTER_NAME",

```

```

        "Value": "Management Account"
      }
    ],
    "Type": "ORGANIZATION",
    "Value": "o-exampleorgid"
  },
  {
    "Type": "EMAIL",
    "Value": "anika@example.com"
  },
  {
    "Type": "NOTES",
    "Value": "This is an invitation to Anika's account to join
Bill's organization."
  }
]
}
]
}

```

下列範例顯示如何取消對帳戶的邀請。

```

$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
  "Handshake": {
    "Id": "h-examplehandshakeid111",
    "State": "CANCELED",
    "Action": "INVITE",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
    "Parties": [
      {
        "Id": "o-exampleorgid",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "susan@example.com",
        "Type": "EMAIL"
      }
    ],
    "Resources": [
      {
        "Type": "ORGANIZATION",

```



```

        "Value": "o-exampleorgid",
        "Resources": [
            {
                "Type": "MASTER_EMAIL",
                "Value": "bill@example.com"
            },
            {
                "Type": "MASTER_NAME",
                "Value": "Management Account"
            },
            {
                "Type": "ORGANIZATION_FEATURE_SET",
                "Value": "CONSOLIDATED_BILLING"
            }
        ]
    },
    {
        "Type": "EMAIL",
        "Value": "anika@example.com"
    },
    {
        "Type": "NOTES",
        "Value": "This is a request for Susan's account to join Bob's
organization."
    }
],
"RequestedTimestamp": 1.47008383521E9,
"ExpirationTimestamp": 1.47137983521E9
}
}

```

- AWS SDKs : [ListHandshakesForOrganization](#)、[CancelHandshake](#)

使用 接受或拒絕帳戶邀請 AWS Organizations

如果您收到加入組織的邀請，您可以接受或拒絕邀請。

考量事項

組織帳戶的狀態會影響可看見的成本和用量資料

如果成員帳戶離開組織而成為獨立帳戶，則帳戶一旦是組織之成員就無法再存取時間範圍內的成本和用量資料。帳戶只能存取做為獨立帳戶時所產生的資料。

如果成員帳戶離開組織 A 而加入組織 B，則此帳戶就無法再存取其做為組織 A 成員之時間範圍內來自組織 A 的成本和用量資料。帳戶只能存取做為組織 B 成員時所產生的資料。

如果帳戶重新加入先前所屬的組織，此帳戶會重新獲得對其過去成本與使用狀況資料的存取權。

只有成員帳戶和獨立帳戶可以接受或拒絕邀請

只有成員帳戶和獨立帳戶可接受或拒絕加入組織的邀請。如果向成員帳戶傳送邀請，該帳戶應先離開目前組織，才能接受邀請。如果邀請已傳送至已屬於組織的管理帳戶，則該帳戶將無法檢視邀請，直到他們[從組織移除所有成員帳戶並刪除組織](#)為止。

接受或拒絕帳戶邀請

若要接受或拒絕邀請，請完成下列步驟。

最低許可

若要接受或拒絕加入 組織的邀請，您必須擁有以下許可：

- `organizations:ListHandshakesForAccount` – 在 AWS Organizations 主控台中查看邀請清單時必填。
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole` – 只有在接受邀請需要在成員帳戶中建立服務連結角色以支援與其他整合時才需要 AWS 服務。如需詳細資訊，請參閱[AWS Organizations 和服務連結角色](#)。

AWS Management Console

接受或拒絕邀請

1. 加入組織的邀請會傳送到帳戶擁有者的電子郵件地址。如果您是帳戶擁有者，而且您收到邀請電子郵件訊息，請依照電子郵件邀請中的指示，或前往您的瀏覽器中的 [AWS Organizations 主控台](#)，然後選擇 [Invitations \(邀請\)](#)，或直接前往[成員帳戶的邀請](#)頁面。
2. 如果提示，請以擔任 IAM 角色的 IAM 使用者身分登入或以帳戶的根使用者身分登入 ([不建議](#)) 獲邀請的帳戶。
3. [會員帳戶的邀請](#)頁面顯示您的帳戶加入組織的未結邀請。

選擇 **Accept invitation** (接受邀請) 或 **Decline invitation** (拒絕邀請)。

- 如果您在之前的步驟中選擇 **Accept invitation** (接受邀請)，主控台會將您重新導向至 [Organization 概觀](#) 頁面，其中含有您的帳戶現在為其成員的組織的詳細資訊。您可以檢視組織的 ID 和擁有者的電子郵件地址。

 Note

已接受的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

AWS Organizations 會自動在新成員帳戶中建立服務連結角色，以支援 AWS Organizations 和其他 之間的整合 AWS 服務。如需詳細資訊，請參閱 [AWS Organizations 和服務連結角色](#)。

AWS 會傳送電子郵件訊息給組織的管理帳戶擁有者，說明您已接受邀請。它還會傳送一封電子郵件訊息給帳戶擁有者，說明帳戶現在為組織的成員。

- 如果您在前面的步驟中選擇 **Decline** (拒絕)，則您的帳戶會維持在列出任何其他等待中邀請的 [成員帳戶邀請](#) 頁面上。

AWS 會傳送電子郵件訊息給組織的管理帳戶擁有者，說明您拒絕邀請。

 Note

已拒絕的邀請會繼續在清單中顯示 30 天。之後便會刪除它們，不再顯示在清單中。

AWS CLI & AWS SDKs

接受或拒絕邀請

您可以使用以下命令來接受或拒絕邀請：

- AWS CLI: [accept-handshake](#), [decline-handshake](#)

下列範例顯示如何接受對加入組織的邀請。

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
```

```
"Handshake": {
  "Action": "INVITE",
  "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
  "RequestedTimestamp": 1481656459.257,
  "ExpirationTimestamp": 1482952459.257,
  "Id": "h-examplehandshakeid111",
  "Parties": [
    {
      "Id": "o-exampleorgid",
      "Type": "ORGANIZATION"
    },
    {
      "Id": "juan@example.com",
      "Type": "EMAIL"
    }
  ],
  "Resources": [
    {
      "Resources": [
        {
          "Type": "MASTER_EMAIL",
          "Value": "bill@amazon.com"
        },
        {
          "Type": "MASTER_NAME",
          "Value": "Management Account"
        },
        {
          "Type": "ORGANIZATION_FEATURE_SET",
          "Value": "ALL"
        }
      ],
      "Type": "ORGANIZATION",
      "Value": "o-exampleorgid"
    },
    {
      "Type": "EMAIL",
      "Value": "juan@example.com"
    }
  ],
  "State": "ACCEPTED"
}
```

```
}
```

下列範例顯示如何拒絕對加入組織的邀請。

- AWS SDKs : [AcceptHandshake](#)、[DeclineHandshake](#)

使用 將帳戶遷移至另一個組織 AWS Organizations

您可以隨時 AWS 帳戶 將從一個組織遷移到另一個組織。例如，當您需要將一或多個 AWS 帳戶 來自多個組織的合併到一個組織時，遷移帳戶在合併和取得時很有幫助。

無論您的使用案例為何，在組織之間遷移帳戶需要您從舊組織中移除帳戶、讓帳戶成為獨立帳戶，以及讓帳戶接受來自新組織的邀請以加入新組織。在遷移期間，您的工作負載和服務將繼續根據您的規格運作。不過，請務必注意組織中可能擁有的任何相依性。

Note

已關閉或暫停的帳戶無法遷移

您無法遷移已關閉或暫停的帳戶。若要回應帳戶，請聯絡 [支援](#)。

七天的存留期要求

若要遷移您在組織中建立的帳戶，您必須等到帳戶建立後至少七天。受邀的帳戶不受此等待期限的限制。

在帳戶之間複寫資料

下列 AWS 規範性指引提供在下列之間複寫資料的策略相關資訊 AWS 帳戶：[資源複寫或在其
中遷移 AWS 帳戶](#)。

遷移帳戶之前需要執行的動作

將 AWS 帳戶 遷移到另一個組織之前，請確定您已完成下列步驟。

步驟 1：檢查您是否具有遷移 帳戶所需的 IAM 許可

步驟 1

請確定您已套用將帳戶遷移至個別組織的必要許可。

若要離開組織，您必須擁有下列許可：

- `organizations:DescribeOrganization` (僅限主控台)

- `organizations:LeaveOrganization`

如需詳細資訊，請參閱[從您的成員帳戶離開組織](#)。

若要邀請 AWS 帳戶 加入組織，您必須擁有下列許可：

- `organizations:DescribeOrganization` (僅限主控台)
- `organizations:InviteAccountToOrganization`

如需詳細資訊，請參閱[邀請 AWS 帳戶 加入您的組織](#)。

若要遷移帳戶，您無法擁有防止遷移的 IAM 政策或服務控制政策

如果您是管理帳戶或委派管理員，您可以透過將許可政策連接到組織內的 IAM 身分（使用者、群組和角色）來控制對 AWS 資源的存取。如需詳細資訊，請參閱 [的 IAM 政策 AWS Organizations](#)。

在遷移帳戶之前：

- 檢查沒有阻止您遷移帳戶的 IAM 政策或服務控制政策 (SCPs)。
- 識別您在遷移帳戶的組織需要複寫的現有 IAM 政策和服務控制政策 (SCPs)。
- 識別指定組織 ID 的現有 IAM 政策。例如 [aws:PrincipalOrgID](#)。

如需詳細資訊，請參閱 [《IAM 使用者指南》和服務控制政策 \(SCP\) 中的管理 IAM 政策 SCPs](#)。

步驟 2：檢查您是否已移除允許存取舊管理帳戶的 IAM 許可

步驟 2

請確定您已移除 IAM 許可，以允許存取舊的管理帳戶，例如 `OrganizationAccountAccessRole`。

當您從組織移除成員帳戶時，為啟用組織管理帳戶存取而建立的任何 IAM 角色都不會自動刪除。如果您想要終止之前的組織管理帳戶的這種存取權，就必須手動刪除 IAM 角色。

如需關於如何刪除角色的詳細資訊，請參閱 IAM 使用者指南中的[刪除角色或執行個體設定檔](#)。

步驟 3：檢查您的手機驗證和付款方式

步驟 3

遷移帳戶必須做為獨立帳戶運作一段時間，才能遷移至新組織。

若要允許 帳戶以獨立帳戶的形式運作，請檢查下列項目：

- 請確定您的手機驗證是up-to-date。
- 請確定 已為帳戶新增有效的付款方式，以解決帳戶遷移時產生的任何費用。
- 如果您使用 付款方式的發票，請確定您的發票是up-to-date。

步驟 4：備份所有報告

步驟 4

請務必從管理帳戶匯出或備份報告，尤其是帳單報告。當您遷移帳戶時，不會儲存組織層級報告和歷史記錄。建議您執行所有帳單歷史記錄的完整匯出。您仍然可以存取成員帳戶的報告，例如 AWS CloudTrail 事件歷史記錄和帳戶帳單歷史記錄。

Important

從組織移除帳戶後，所有組織層級的報告和歷史記錄，例如管理帳戶中的組織帳單資訊都會遭到刪除。

如需詳細資訊，請參閱[成本和用量報告](#)、[Cost Explorer管報告](#)、[Savings Plans 報告](#)，以及[預留執行個體 \(RI\) 使用率和涵蓋範圍](#)。

步驟 5：檢查組織相依性

步驟 5

請確定遷移帳戶沒有任何與組織相關的相依性。

要檢查的相依性：

- 如果帳戶是委派管理員，則必須先取消註冊委派管理員許可，才能遷移帳戶。如需詳細資訊，請參閱[您可以使用的服務 AWS Organizations](#)。
- 如果帳戶是管理帳戶，您必須從組織移除所有成員帳戶，並在遷移之前刪除組織。刪除組織之後，您的管理帳戶將做為獨立帳戶運作。遷移後，管理帳戶將成為新組織的成員帳戶。如需詳細資訊，請參閱[刪除組織](#)。
- 如果任何 IAM 許可取決於帳戶，則在您將帳戶遷移至新組織之後，您將需要調整舊組織的許可，以便舊組織如往常一樣運作。如需詳細資訊，請參閱[管理組織的存取許可](#)。

- 如果您使用任何帳戶或組織單位 (OU) 標籤，則需要在新組織中重新建立標籤。

(選用) 步驟 6：如果您使用 [AWS Control Tower](#)，請檢閱指引 [AWS Control Tower](#)

(選用) 步驟 6

如果您要將帳戶遷移至 管理的組織或從中遷移 AWS Control Tower，請檢閱下列 AWS 規範性指引：[將 AWS 成員帳戶從 遷移 AWS Organizations 至 AWS Control Tower](#)。

遷移帳戶時需要執行的動作

遷移程序要求新組織向遷移帳戶傳送邀請、讓舊組織移除遷移帳戶，以及讓遷移帳戶接受來自新組織的邀請，以加入新組織。

遷移 帳戶

1. 從新組織的管理帳戶傳送邀請到遷移帳戶。您應該在邀請離開舊組織之前，將邀請傳送到帳戶。這有助於將遷移帳戶暫時作為獨立帳戶運作時產生的成本降至最低。如需邀請帳戶的相關資訊，請參閱[邀請 AWS 帳戶 加入您的組織](#)。
2. 從舊組織移除遷移帳戶。您可以使用管理[帳戶從組織移除成員帳戶](#)，或[將組織從 中移除為成員帳戶](#)。
3. 接受加入新組織的邀請。如需詳細資訊，請參閱[接受來自組織的邀請](#)。從另一個組織遷移到另一個組織的帳戶會自動新增至新組織的根目錄。將帳戶移至新組織中的組織單位 (OU) 之前，建議您檢查遷移帳戶是否具有適當的組織政策和 OU 許可。
4. 如果您想要遷移管理帳戶，您必須從組織[移除所有成員帳戶](#)，並在[將管理帳戶遷移至新組織之前刪除組織](#)。刪除舊組織後，您的管理帳戶將作為獨立帳戶運作，並且可以接受來自新組織的邀請，以加入新組織。如果您接受邀請，管理帳戶將是新組織的成員帳戶。

遷移 帳戶後需要執行的動作

將您的帳戶從一個組織遷移到另一個組織之後，請確定您已完成以下步驟。

遷移後檢閱

1. 評估遷移帳戶的所有[帳單工具組態](#)，例如成本類別、預算和帳單警示。
2. 針對您從一個組織遷移到另一個組織的任何帳戶，檢閱並更新下列貨幣資訊：
 - a. 如有必要，[請更新帳戶的稅務設定](#)。
 - b. 確定遷移帳戶的[支援 計劃](#)符合新組織的付款人帳戶。

- c. 檢閱您可能想要套用至您遷移帳戶的任何可能[免稅](#)。
3. 驗證並確認遷移帳戶的現有 IAM 政策和服務控制政策 (SCPs)。例如，您可能需要更新某些 IAM 政策的組織 ID，以反映新組織。
4. 更新您遷移帳戶之新組織的[成本分配標籤](#)。您將需要更新您遷移帳戶收集的所有先前成本分配標籤。
5. 任何[預留執行個體](#)和 [Save Plans](#) 都會與 帳戶一起遷移。這些不會保留在舊組織中。支援 如果需要將這些項目轉移到舊組織，請聯絡。

在 中檢視帳戶的詳細資訊 AWS Organizations

當您在[AWS Organizations 主控台](#)中登入組織的管理帳戶時，您可以檢視成員帳戶的詳細資訊。

最低許可

若要檢視 的詳細資訊 AWS 帳戶，您必須具有下列許可：

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListAccounts` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視 的詳細資訊 AWS 帳戶

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 導覽至 [AWS 帳戶](#) 頁面，然後選擇您要檢查的帳戶名稱 (而非選項按鈕)。如果您所需的帳戶是 OU 的子項，您可能需要選擇三角形圖示

 以將其展開並查看其子項。重複此步驟，直到找到帳戶為止。

Account details (帳戶詳細資訊) 方塊會顯示帳戶的相關資訊。

AWS CLI & AWS SDKs

檢視 的詳細資訊 AWS 帳戶

您可以使用下列命令來檢視帳戶的詳細資訊：

- AWS CLI:
 - [list-accounts](#) – 列出組織中所有帳戶的詳細資訊
 - [describe-account](#) – 僅列出指定帳戶的詳細資訊

這兩個命令會針對回應中包含的每個帳戶傳回相同的詳細資訊。

以下範例顯示如何擷取指定帳戶的詳細資訊。

```
$ aws organizations describe-account --account-id 123456789012

{
  "Account": {
    "Id": "123456789012",
    "Arn": "arn:aws:organizations::123456789012:account/o-aa111bb222/123456789012",
    "Email": "admin@example.com",
    "Name": "Example.com Organization's Management Account",
    "Status": "ACTIVE",
    "JoinedMethod": "INVITED",
    "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
  }
}
```

- AWS SDKs :
 - [ListAccounts](#)
 - [DescribeAccount](#)

匯出 中所有帳戶的詳細資訊 AWS Organizations

透過 AWS Organizations，組織的管理帳戶使用者和委派管理員可以匯出 .csv 檔案，其中包含組織內的所有帳戶詳細資訊。因此，組織管理員可以輕鬆檢視帳戶並依狀態進行篩選：ACTIVE、SUSPENDED 或 PENDING。如果您的組織有許多帳戶，.csv 檔案下載選項提供一種在試算表中輕鬆檢視及排序帳戶詳細資訊的方法。

Note

只有管理帳戶中的主體可以下載帳戶清單。

匯出組織中所有 AWS 帳戶 的清單

登入組織的管理帳戶時，您可以取得屬於組織一部分的所有帳戶的清單，格式為會 .csv 檔案。清單包含個別帳戶詳細資訊；但其未指出帳戶所屬的組織單位 (OU)。

.csv 檔案內含每個帳戶的以下資訊：

- Account ID (帳戶 ID) – 帳戶識別碼。例如：123456789012
- ARN – 帳戶的 Amazon 資源名稱。例如：
arn:aws:organizations::123456789012:account/o-o1gb0d1234/123456789012
- Email – 與帳戶相關聯的電子郵件地址。例如：marymajor@example.com
- Name (名稱) – 帳戶建立者提供的帳戶名稱。例如：階段測試帳戶
- Status (狀態) – 組織內的帳戶狀態。此值可以是 PENDING、ACTIVE 或 SUSPENDED。
- Joined method (加入的方法) – 指定帳戶的建立方式。此值可以是 INVITED 或 CREATED。
- Joined timestamp (加入時的時間戳記) – 帳戶加入組織的日期和時間。

最低許可

若要匯出您組織中所有成員帳戶的 .csv 檔案，您必須擁有以下許可：

- organizations:DescribeOrganization
- organizations:ListAccounts

AWS Management Console

匯出 AWS 帳戶 組織中所有 的 .csv 檔案

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇 Actions (動作)，然後針對 AWS 帳戶 選擇 Export account list (匯出帳戶清單)。頁面頂端的藍色橫幅指示 "Export is in progress!" (「匯出進行中！」)
3. 當檔案準備就緒時，橫幅會變成綠色，並指示："Download is ready!" (「下載已準備就緒！」) 選擇下載 CSV。檔案 Organization_accounts_information.csv 下載到您的裝置。

AWS CLI & AWS SDKs

匯出含有帳戶詳細資訊的 .csv 檔案的唯一方法是使用 AWS Management Console。您無法使用 AWS CLI 匯出帳戶清單 .csv 檔案。

更新 中帳戶的替代聯絡人 AWS Organizations

您可以使用 Organizations 主控台，或以程式設計方式使用 CLI AWS 或 AWS SDKs 更新組織內 AWS 帳戶的替代聯絡人。若要了解如何更新替代聯絡人，請參閱 AWS 《帳戶管理參考》[AWS 帳戶 中的更新組織中任何 的替代聯絡人](#)。

更新 中帳戶的主要聯絡資訊 AWS Organizations

您可以使用 Organizations 主控台，或以程式設計方式使用 CLI AWS 或 AWS SDKs 更新組織內 AWS 帳戶的主要聯絡資訊。若要了解如何更新主要聯絡人資訊，請參閱 AWS 《帳戶管理參考》[AWS 帳戶 中的更新組織中任何 的主要聯絡人](#)。

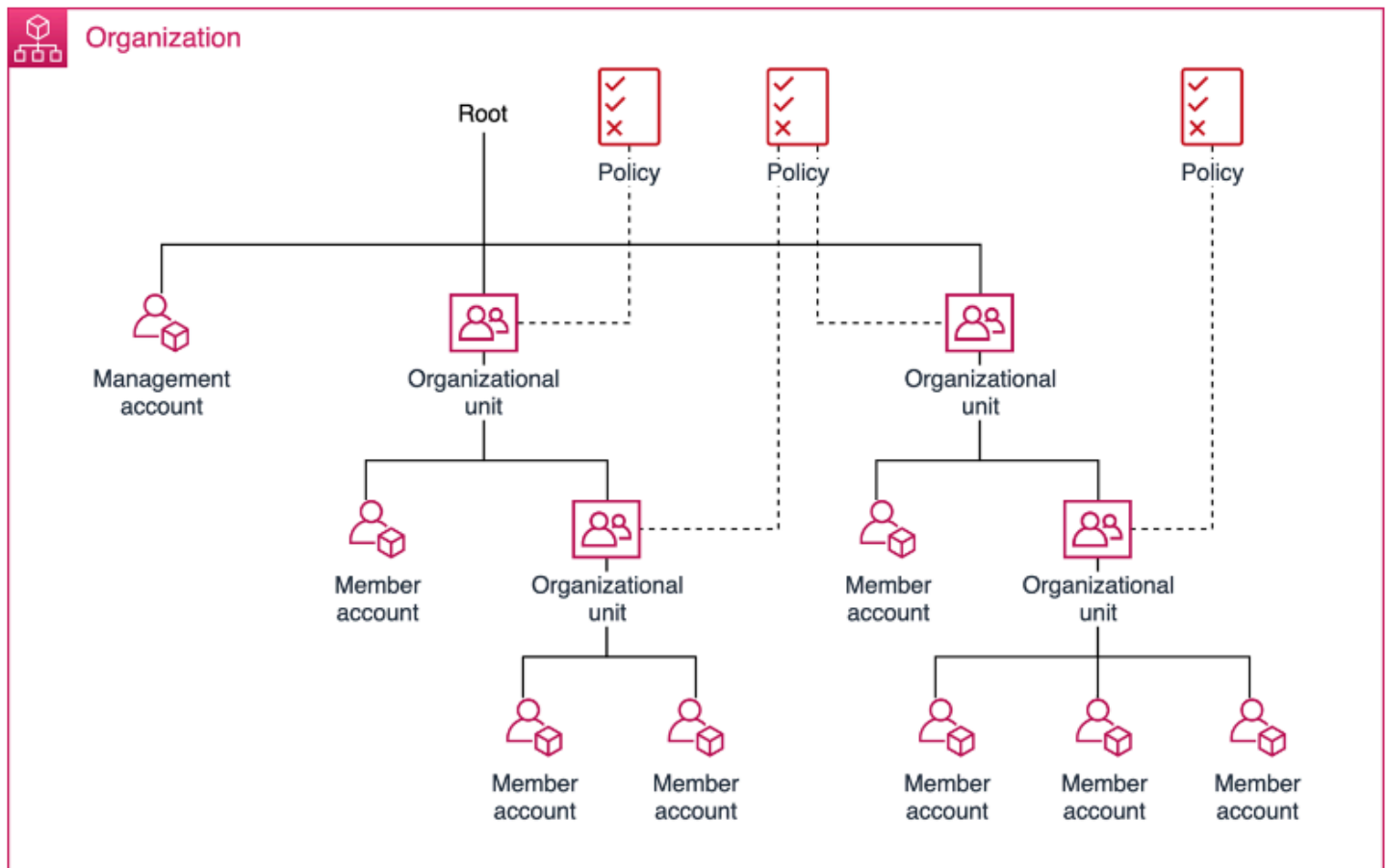
中的帳戶更新 AWS 區域AWS Organizations

您可以使用 AWS Organizations 主控台 AWS 區域 更新組織中帳戶已啟用的。若要了解如何更新已啟用 AWS 區域，請參閱 [《帳戶管理參考 AWS 區域》中的在帳戶中啟用或停用](#)。AWS

使用 管理組織單位 OUs) AWS Organizations

您可以使用組織單位 (OU) 將帳戶群組在一起，以單一單位的形式進行管理。這可大幅簡化帳戶的管理。例如，您可以將以政策為基礎的控制連接到 OU，而 OU 內的所有帳戶會自動繼承政策。您可以在單一組織內建立多個 OU，您也可以在其他 OU 內建立 OU。每個 OU 可以包含多個帳戶，而且您可以在 OU 之間移動帳戶。但是，OU 的名稱在父系 OU 或根中必須是唯一的。

下圖顯示由七個帳戶組成的組織，這些帳戶在根目錄下組織成四個 OUs。組織也有一些政策會套用至 OUs。



Note

組織中有一個根，在您第一次設定組織時為您 AWS Organizations 建立。

主題

- [使用 管理組織單位 \(OUs最佳實務 AWS Organizations\)](#)

- [使用 導覽根和組織單位 \(OU\) 階層 AWS Organizations](#)
- [使用 檢視組織單位 \(OU\) 的詳細資訊 AWS Organizations](#)
- [使用 建立組織單位 \(OU\) AWS Organizations](#)
- [使用 重新命名組織單位 \(OU\) AWS Organizations](#)
- [使用 標記組織單位 \(OU\) AWS Organizations](#)
- [使用 將帳戶移至組織單位 \(OU\) 或根和 OUs 之間 AWS Organizations](#)
- [使用 檢視根的詳細資訊 AWS Organizations](#)
- [使用 刪除組織單位 \(OU\) AWS Organizations](#)

使用 管理組織單位 (OUs最佳實務 AWS Organizations

請遵循這些建議，以協助您使用 AWS Organizations 組織單位 (OUs) 在 中管理多帳戶環境。

主題

- [了解 AWS Organizations](#)
- [建議的基礎組織單位 OUs\)](#)
- [建議的額外組織單位 OUs\)](#)
- [結論](#)

了解 AWS Organizations

架構良好的多帳戶 AWS 環境的基礎是 AWS Organizations，可讓您集中管理多個帳戶。組織單位 (OU) 是組織中帳戶的邏輯群組。OUs可讓您將帳戶組織成階層，並協助您套用管理控制項。Organizations [政策](#)定義您可以套用至 群組的控制項 AWS 帳戶。例如，[服務控制政策](#) (SCP) 是定義組織中帳戶可執行之 AWS 服務 動作的政策，例如 Amazon EC2 Run Instance。

雖然您可以從單一帳戶開始您的 AWS 旅程，但 AWS 建議您隨著工作負載的大小和複雜性增加而設定多個帳戶。使用多帳戶環境是 AWS 最佳實務，可以提供數種好處：

- 具有各種需求的快速創新：您可以將 配置 AWS 帳戶 給公司內不同的團隊、專案或產品，以協助確保他們都能快速創新，同時允許自己的安全需求。
- 簡化帳單：使用多個 AWS 帳戶 可以簡化如何配置 AWS 成本，方法是協助識別哪些產品或服務項目負責 AWS 收費。

- 彈性的安全控制：您可以使用多個 AWS 帳戶 來隔離具有特定安全需求的工作負載或應用程式，或需要符合嚴格的合規準則，例如 HIPAA 或 PCI。
- 適應業務流程：您可以 AWS 帳戶 採用最能反映公司業務流程之各種需求的方法來組織多個 ，這些業務流程具有不同的營運、法規和預算需求。

建議的基礎組織單位 OUs)

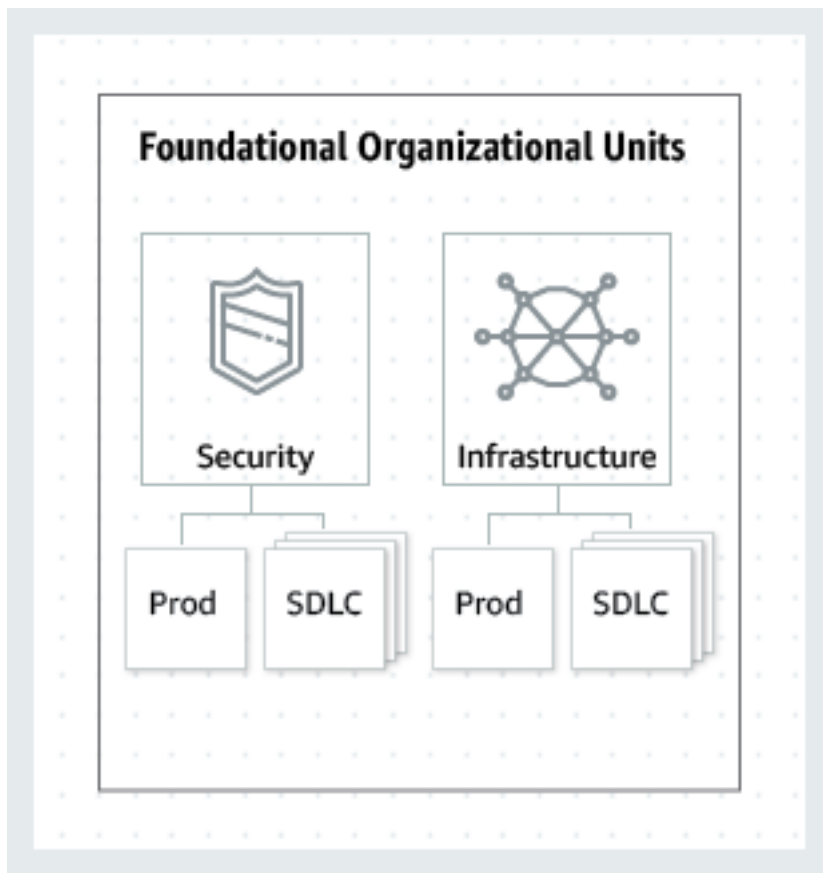
您的組織單位 OUs) 應該以函數或常用的控制項為基礎，而不是鏡射公司的報告結構。AWS 建議您從安全和基礎設施開始。大多數企業都有集中式團隊，可為整個組織提供滿足這些需求的服務。我們建議為這些特定函數建立一組基礎 OUs：

- 安全：用於安全服務。建立日誌封存、安全唯讀存取、安全工具和破解玻璃的帳戶。
- 基礎設施：用於共用基礎設施服務，例如聯網和 IT 服務。為您需要的每種基礎設施服務類型建立帳戶。

由於大多數公司對於生產工作負載都有不同的政策要求，基礎設施和安全性可以有非生產 (SDLC) 和生產 (Prod) 的巢狀 OUs。SDLC OU 主機非生產工作負載中的帳戶，不應具有來自其他帳戶的生產相依性。如果生命週期階段之間的 OU 政策存在變化，SDLC 可以分割為多個 OUs (例如，開發和預生產)。Prod OU 中的帳戶託管生產工作負載。

在 OU 層級套用政策，以根據您的需求管理 Prod 和 SDLC 環境。一般而言，在 OU 層級套用政策是比個別帳戶層級更好的做法，因為它可簡化政策管理和任何潛在的故障診斷。

下圖顯示安全性和基礎設施的基礎 OUs(Prod 和 SDLC)：



建議的額外組織單位 OUs)

中央服務到位後，我們建議建立與建置或執行您的產品或服務直接相關的 OUs。許多 AWS 客戶會在建立基礎之後建置下列 OUs：

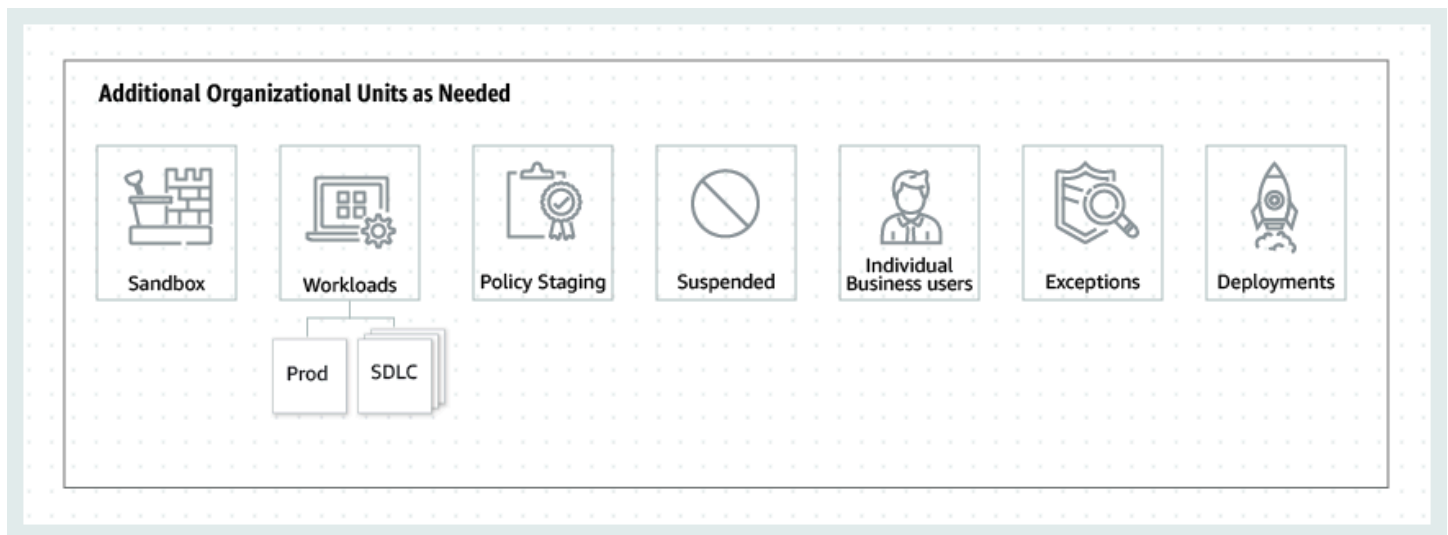
- 沙盒：保留個別開發人員可用來實驗 AWS 帳戶的 AWS 服務。請確定這些帳戶可與內部網路分離。
- 工作負載：包含託管對外應用程式服務的 AWS 帳戶。您應該在 SDLC 和 Prod 環境（類似基礎 OU）OUs 下建構 OUs，以隔離和緊密控制生產工作負載。

我們也建議根據您的特定需求，新增額外的 OUs 以進行維護和持續擴展。以下是根據現有 AWS 客戶實務的一些常見主題：

- 政策預備：保留帳戶，您可以在 AWS 其中測試提議的政策變更，然後再將其廣泛套用至組織。首先在預期 OU 的帳戶層級實作變更，然後慢慢地在其他帳戶、OUs 和整個組織中的其餘部分進行訓練。
- 已暫停：包含已關閉且正在等待從組織中刪除 AWS 帳戶的。將 SCP 連接至此 OU，以拒絕所有動作。如果需要還原帳戶，請確定帳戶已加上可追蹤性的詳細資訊。

- 個別商業使用者：包含的有限存取 OU，AWS 帳戶適用於可能需要建立業務生產力相關應用程式的商業使用者（而非開發人員），例如設定 S3 儲存貯體與合作夥伴共用報告或檔案。
- 例外狀況：AWS 帳戶用於具有高度自訂安全性或稽核需求的業務使用案例的保留，與工作負載 OU 中定義的保留不同。例如，針對機密的新應用程式或功能設定 AWS 帳戶。在帳戶層級使用 SCPs 以滿足自訂需求。考慮使用 [Amazon EventBridge](#) 和 [AWS Config 規則](#) 設定 Detect and React 系統。
- 部署：包含適用於持續整合和持續交付/部署 (CI/CD 部署) AWS 帳戶的。與工作負載 OU (Prod 和 SDLC) 中的帳戶相比，如果您有不同的 CI/CD 部署控管和操作模型，則可以建立此 OUs。CI/CD 的分佈有助於減少對中央團隊所操作之共用 CI/CD 環境的組織相依性。對於工作負載 AWS 帳戶 OU 中應用程式的每個一組 SDLC/Prod，請在部署 OU 下建立 CI/CD 帳戶。
- 轉換：這在將現有帳戶和工作負載移至組織的標準區域之前，會用作現有帳戶和工作負載的暫時保留區域。這可能是因為帳戶是資料擷取的一部分、先前由第三方管理，或是舊組織結構中的舊版帳戶。

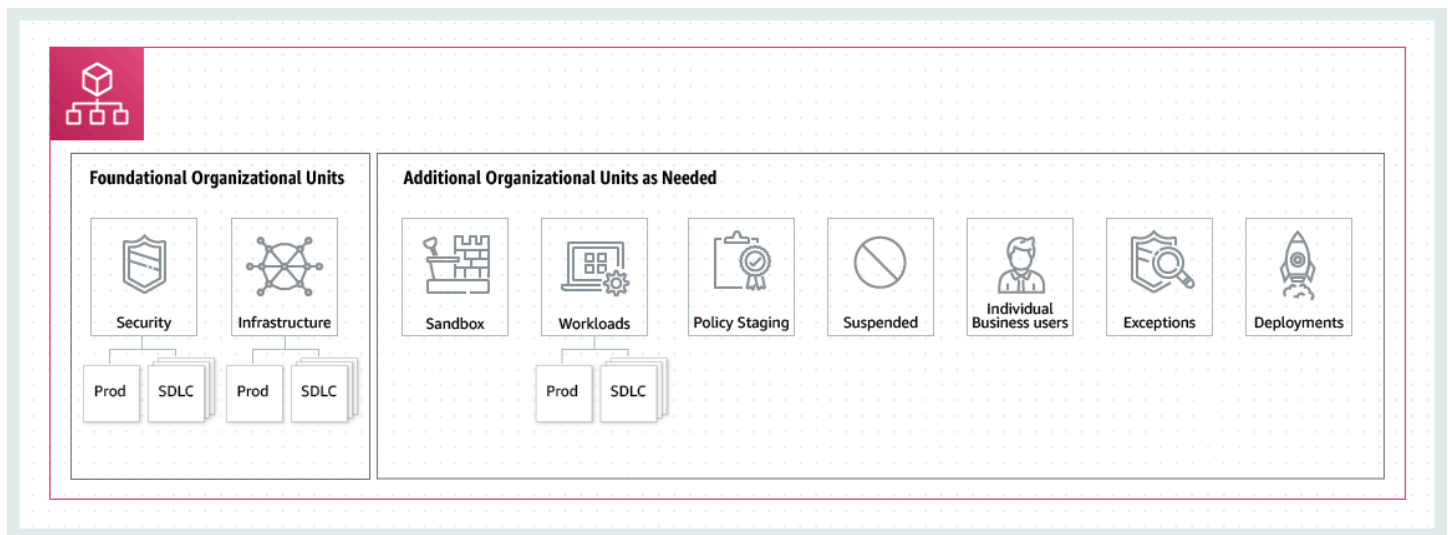
下圖顯示沙盒、工作負載、政策預備、暫停、個別商業使用者、例外狀況、部署和轉換帳戶的其他 OUs：



結論

架構良好的多帳戶策略可協助您創新 AWS，同時有助於確保您符合安全和可擴展性需求。本主題中描述的架構代表 AWS 最佳實務，您應將其用作 AWS 旅程的起點。

下圖顯示建議的基礎 OUs 和其他 OUs：



使用 導覽根和組織單位 (OU) 階層 AWS Organizations

在移動帳戶或連接政策時，若要導覽至不同的 OU 或導覽至根，您可以使用預設「樹狀目錄」檢視。

AWS Management Console

將組織作為「樹狀目錄」導覽

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面 Organization (組織) 區段的頂部，選取Hierarchy (階層) 切換 (而不是List (清單))。
3. 樹狀目錄一開始會顯示根，僅顯示子 OU 和帳戶的第一層。若要展開樹狀目錄以顯示更深的層級，請選擇任何父實體旁的展開圖示 (▶)。
若要降低雜亂和收合樹狀目錄的分支，請選擇已展開的父實體旁的折疊圖示 (▼)。
4. 選擇 OU 或根的名稱，以檢視其詳細資訊並執行特定操作。或者，您可以選擇名稱旁的選項按鈕，並在 Actions (動作) 選單中執行對該實體的特定操作。

您還可以僅以表格形式檢視組織中帳戶的清單，而不必先導覽至 OU 來尋找它們。在此檢視中，您無法看到任何 OU，或操控連接到它們的政策。

AWS Management Console

以沒有階層的平面帳戶清單來檢視組織

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面的組織區段頂端，選擇 AWS 帳戶 僅檢視切換圖示以開啟它。

3. 不含任何階層的帳戶清單會隨即顯示。

使用 檢視組織單位 (OU) 的詳細資訊 AWS Organizations

在 [AWS Organizations 主控台](#) 登入組織的管理帳戶時，您可以檢視組織中 OU 的詳細資訊。

最低許可

若要檢視組織單位 (OU) 的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListOrganizationsUnitsForParent` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視 OU 的詳細資訊

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，選擇您要檢查的 OU (而非選項按鈕) 名稱。如果您所需的 OU 是另一個 OU 的子項，選擇其父項 OU 旁邊的三角形圖示以將其展開，並查看階層下一級中的那些項目。重複此操作，直至您找到所需的 OU。

Organizational unit details (組織單位詳細資訊) 方塊會顯示 OU 的相關資訊。

AWS CLI & AWS SDKs

檢視 OU 的詳細資訊

您可以使用下列命令來檢視 OU 的詳細資訊：

- AWS CLI , AWS SDKs
 - [list-roots](#)
 - [list-children](#)
 - [describe-organizational-unit](#)

以下範例顯示如何使用 AWS CLI 來尋找 OU 的 ID。您可以透過從 `list-roots` 命令開始周遊階層，然後在根上執行 `list-children` 並對其每個子項反覆執行，來尋找 OU ID，直至找到您所需的一個。

```
$ aws organizations list-roots
{
  "Roots": [
    {
      "Id": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "PolicyTypes": []
    }
  ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type ORGANIZATIONAL_UNIT
{
  "Children": [
    {
      "Id": "ou-a1b2-f6g7h111",
      "Type": "ORGANIZATIONAL_UNIT"
    }
  ]
}
```

取得 OU ID 之後，下列範例顯示如何擷取 OU 的詳細資訊。

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-f6g7h111
```

```
{
  "OrganizationalUnit": {
    "Id": "ou-a1b2-f6g7h111",
    "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h111",
    "Name": "Production-Apps"
  }
}
```

- AWS SDKs :
 - [ListRoots](#)
 - [ListChildren](#)
 - [DescribeOrganizationalUnit](#)

使用 建立組織單位 (OU) AWS Organizations

登入您的組織的管理帳戶時，您可以在組織的根建立一個 OU。OU 可以建立最多達五層的巢狀。若要建立您的第一個 OU，請完成以下步驟。

Important

如果此組織是使用 管理 AWS Control Tower，請使用 AWS Control Tower 主控台或 APIs 建立您的 OUs。如果您在 Organizations 中建立 OU，則該 OU 不會註冊 AWS Control Tower。如需詳細資訊，請參閱AWS Control Tower 使用者指南中的[參照 AWS Control Tower外部資源](#)。

最低許可

若要在您的組織的根帳戶內建立 OU，您必須擁有以下許可：

- organizations:DescribeOrganization – 僅在使用 Organizations 主控台時才需要
- organizations>CreateOrganizationalUnit

AWS Management Console

建立組織單位 (OU)

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 導覽至 [AWS 帳戶](#) 頁面。

主控台會顯示根及其內容。第一次瀏覽根時，主控台會在該最上層檢視中顯示所有的 AWS 帳戶。如果您之前建立了 OU，並將帳戶移至其中，主控台只會顯示最上層 OU 以及尚未移至 OU 的任何帳戶。

3. (選用) 如果您想要在現有 OU 內建立 OU，請透過選擇子 OU 的名稱 (而不是核取方塊)，或在樹狀檢視中選擇 OU 旁白的



直至看到您所需的 OU，然後選擇其名稱，來[導覽至子 OU](#)。

4. 當您在階層中選取正確的父 OU 時，請在 Actions (動作) 選單的 Organizational Unit (組織單位) 下方，選擇 Create new (建立新的)
5. 在 Create organizational unit (建立組織單位) 對話方塊中，輸入您要建立的 OU 名稱。
6. (選用) 選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來新增一個或多個標籤。將值留空會將其設定為空白字串；而不是 null。您可以在 OU 中連接最多 50 個標籤。
7. 最後，選擇 Create organizational unit (建立組織單位)。

您的新 OU 會顯示在父系內。您現在可以[將帳戶移至此 OU](#)，或將政策連接至此 OU。

AWS CLI & AWS SDKs

建立 OU

下列程式碼範例示範如何使用 `CreateOrganizationalUnit`。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```

        Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
        Console.WriteLine($"Organizational unit {orgUnitName} Details");
        Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
    }
    else
    {
        Console.WriteLine("Could not create new organizational unit.");
    }
}
}

```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [CreateOrganizationalUnit](#)。

CLI

AWS CLI

在根或父 OU 中建立 OU

下列範例示範如何建立名為 AccountingOU 的 OU：

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --name AccountingOU
```

輸出包含 organizationalUnit 物件，其中包含新 OU 的詳細資訊：

```

{
    "OrganizationalUnit": {
        "Id": "ou-examplerootid111-exampleouid111",
        "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-examplerootid111-exampleouid111",
        "Name": "AccountingOU"
    }
}

```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [CreateOrganizationalUnit](#)。

使用 重新命名組織單位 (OU) AWS Organizations

登入您的組織的管理帳戶時，您可以重新命名 OU。若要執行此動作，請執行下列步驟。

最低許可

若要在您的 組織的根帳戶內重新命名 OU，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

重新命名 OU

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，[導覽至](#)您要重新命名的 OU，然後執行以下其中一個步驟：
 - 選擇想要重新命名的 OU 旁邊的選項按鈕 。
然後，在 Actions (動作) 選單的 Organizational unit (組織單位) 中，選擇 Rename (重新命名)。
 - 選擇 OU 的名稱，以存取 OU 的詳細資訊頁面。然後，在頁面頂端選擇 Rename (重新命名)。
3. 在 Rename organizational unit (重新命名組織單位) 對話方塊中，輸入新名稱，然後選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

重新命名 OU

您可以使用下列其中一項命令來重新命名 OU：

- AWS CLI: [update-organizational-unit](#)

下列範例顯示如何將 OU 重新命名。

```
$ aws organizations update-organizational-unit \
  --organizational-unit-id ou-a1b2-f6g7h222 \
  --name "Renamed-OU"
{
  "OrganizationalUnit": {
    "Id": "ou-a1b2-f6g7h222",
    "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h222",
    "Name": "Renamed-OU"
  }
}
```

- AWS SDKs : [UpdateOrganizationalUnit](#)

使用 標記組織單位 (OU) AWS Organizations

登入您的組織的管理帳戶時，您可以新增或移除連接至 OU 的標籤。若要執行此動作，請執行下列步驟。

最低許可

若要編輯連接至您 組織的根內 OU 的標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribeOrganizationalUnit` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 OU 的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，[導覽至您要編輯其標籤的 OU](#) 並選擇其名稱。
3. 在 OU 的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。

4. 您可以在此索引標籤上執行以下任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 透過選擇您要移除的標籤旁邊的 Remove (移除)，移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至 OU 的標籤

您可以使用下列其中一項命令來變更連接至 OU 的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)

下列範例會將標籤 "Department"="12345" 連接至 OU。請注意，Key 和 Value 區分大小寫。

```
$ aws organizations tag-resource \  
  --resource-id ou-a1b2-f6g7h222 \  
  --tags Key=Department,Value=12345
```

此命令成功後就不會產生輸出。

下列範例會從 OU 中移除 Department 標記。

```
$ aws organizations untag-resource \  
  --resource-id ou-a1b2-f6g7h222 \  
  --tag-keys Department
```

此命令成功後就不會產生輸出。

- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

使用 將帳戶移至組織單位 (OU) 或根和 OUs 之間 AWS Organizations

登入到您的組織的管理帳戶時，您可以將您的組織中的帳戶從根移至 OU，在 OU 間移動，或從 OU 回到根。將帳戶放置在 OU 內，可讓它受限於連接至父 OU 和父系鏈結中任何 OU 的任何政策。如果帳戶不在 OU 中，則僅受限於直接連接至根政策，以及直接連接帳戶的任何政策。若要移動帳戶，請完成以下步驟。

最低許可

若要將帳戶移至 OU 階層中的新位置，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:MoveAccount`

AWS Management Console

將帳戶移至 OU

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，尋找您要移動的一個或多個帳戶。您可以導覽 OU 階層，或啟用僅檢視 AWS 帳戶，以查看沒有 OU 結構的帳戶平面清單。如果您有許多帳戶，您可能需要在清單底部選擇載入更多採用 'ou-name' 的帳戶，以尋找您想要移動的所有內容。
3. 選擇您要移動的每個帳戶名稱旁邊的核取方塊
 
4. 在 Actions (動作) 選單的 AWS 帳戶 下，選擇 Move (移動)。
5. 在 Move AWS 帳戶 (啟動 AWS 帳戶帳戶) 對話方塊中，導覽至至您要移動帳戶的目標 OU 或根並選擇，然後選擇 Move AWS 帳戶(移動 AWS 帳戶帳戶)。

AWS CLI & AWS SDKs

將帳戶移至 OU

您可以使用下列其中一項命令來移動帳戶：

- AWS CLI: [move-account](#)

下列範例會將 AWS 帳戶 從根目錄移至 OU。請注意，您必須指定來源和目的地容器的 ID。

```
$ aws organizations move-account \
  --account-id 111122223333 \
  --source-parent-id r-a1b2 \
  --destination-parent-id ou-a1b2-f6g7h111
```

此命令成功後就不會產生輸出。

- AWS SDKs : [MoveAccount](#)

使用 檢視根的詳細資訊 AWS Organizations

當您在[AWS Organizations 主控台](#)中登入組織的管理帳戶時，您可以檢視管理根的詳細資訊。

最低許可

若要檢視根的詳細資訊，您必須擁有以下許可：

- `organizations:DescribeOrganization` (僅限主控台)
- `organizations:ListRoots`

根是組織單位 (OU) 階層中最上層的容器，而且通常會像 OU 一樣運作。不過，作為階層最上方的容器，對根的變更會影響 AWS 帳戶 組織中的所有其他 OU 和每個。

AWS Management Console

檢視根的詳細資訊

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 導覽至 [AWS 帳戶](#) 頁面，然後選擇 Root (根) OU (其名稱，而非選項按鈕)。
3. Root (根) 詳細資訊會隨即出現，並顯示根的詳細資訊。

AWS CLI & AWS SDKs

檢視根的詳細資訊

您可以使用下列其中一項命令來檢視根帳戶的詳細資訊：

- AWS CLI: [list-roots](#)

以下範例顯示如何擷取根的詳細資訊，包括目前在組織中啟用的政策類型：

```
$ aws organizations list-roots
{
  "Roots": [
    {
      "Id": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "PolicyTypes": [
        {
          "Type": "BACKUP_POLICY",
          "Status": "ENABLED"
        }
      ]
    }
  ]
}
```

- AWS SDKs : [ListRoots](#)

使用 刪除組織單位 (OU) AWS Organizations

登入到您的組織的管理帳戶時，您可以刪除不再需要的任何 OU。

您必須先將所有帳戶從 OU 和任何子 OU 移出，然後才能刪除子 OU。

最低許可

若要刪除 OU，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations>DeleteOrganizationalUnit`

AWS Management Console

刪除 OU

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，尋找您要刪除的 OU，然後選擇每個 OU 名稱旁邊的核取方塊 ☒。
3. 選擇 Actions (動作)，然後在 Organizational unit (組織單位) 下，選擇 Delete (刪除)。
4. 若要確認您要刪除 OU，請輸入 OU 的名稱 (如果您選擇僅刪除一個 OU) 或 'delete' 一詞 (如果您選擇多個 OU)，然後選擇 Delete (刪除)。

AWS Organizations 會刪除 OUs 並從清單中移除它們。

AWS CLI & AWS SDKs

刪除 OU

下列程式碼範例示範如何使用 DeleteOrganizationalUnit。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
```

```
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-000000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [DeleteOrganizationalUnit](#)。

CLI

AWS CLI

刪除 OU

下列範例顯示如何刪除 OU。此範例假設您先前已從 OUs 移除所有帳戶和其他 OU：

```
aws organizations delete-organizational-unit --organizational-unit-id ou-  
examplerootid111-exampleouid111
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [DeleteOrganizationalUnit](#)。

使用 管理組織政策 AWS Organizations

中的政策 AWS Organizations 可讓您將其他類型的管理套用至組織中 AWS 帳戶 的。只有在您[啟用組織中的所有功能](#)時，才可以使用這些政策。

AWS Organizations 主控台會顯示每個政策類型的啟用或停用狀態。在 Organize accounts (組織帳戶) 索引標籤中，選擇左側導覽窗格中的 Root。畫面右側的詳細資訊窗格顯示所有可用的政策類型。此清單指出組織根中已啟用和已停用哪些政策類型。如果顯示 Enable (啟用) 類型的選項，則該類型目前已停用。如果顯示 Disable (停用) 類型的選項，則該類型目前已啟用。

主題

- [政策類型](#)
- [中的授權政策 AWS Organizations](#)
- [中的管理政策 AWS Organizations](#)
- [的委派管理員 AWS Organizations](#)
- [啟用政策類型](#)
- [停用政策類型](#)
- [使用 建立組織政策 AWS Organizations](#)
- [使用 更新組織政策 AWS Organizations](#)
- [使用 編輯連接至組織政策的標籤 AWS Organizations](#)
- [使用 連接組織政策 AWS Organizations](#)
- [使用 分離組織政策 AWS Organizations](#)
- [取得組織政策的相關資訊](#)
- [使用 刪除組織政策 AWS Organizations](#)

政策類型

Organizations 提供下列兩大類別的政策類型：

授權政策

授權政策可協助您集中管理整個組織的安全性 AWS 帳戶。

- [服務控制政策 SCPs](#) 可集中控制組織中 IAM 使用者和 IAM 角色的最大可用許可。

- [資源控制政策 RCPs](#) 提供對組織中資源可用許可上限的中央控制。

管理政策

管理政策可協助您集中設定和管理整個組織的 AWS 服務 及其功能。

- [宣告政策](#)可讓您集中宣告和強制執行跨組織 AWS 服務 大規模指定 所需的組態。連接後，當服務新增新功能或 APIs 時，一律會維護組態。
- [備份政策](#)可讓您集中管理備份計劃，並將備份計劃套用至整個組織帳戶的 AWS 資源。
- [標籤政策](#)可讓您標準化連接至組織帳戶中 AWS 資源的標籤。
- [聊天應用程式政策](#)可讓您從 Slack 和 Microsoft Teams 等聊天應用程式控制對組織帳戶的存取。
- [AI 服務選擇退出政策](#)可讓您控制組織中所有帳戶的 AWS AI 服務資料收集。
- [Security Hub 政策](#)可讓您解決與組織安全需求相符的安全涵蓋範圍差距，並將它們集中套用至整個組織。

下表總結了每個政策類型的某些特性。如需這些政策類型的其他特性，請參閱 [的配額和服務限制 AWS Organizations](#)。

Policy type (政策類型)	政策類別	影響管理帳戶	可以連接至 根、OU 或帳戶的 數目上限	大小上限	支援檢視 OU 或帳戶的有效 政策
SCP	授權	 否	5	5120 個字元	 否
RCP	授權	 否	5	5120 個字元	 否

Policy type (政策類型)	政策類別	影響管理帳戶	可以連接至 根、OU 或帳 戶的數目上限	大小上限	支援檢視 OU 或帳戶的有效 政策
宣告政策	管理	 是	10	10,000 個字 元	 是
備份政策	管理	 是	10	10,000 個字 元	 是
標籤政策	管理	 是	10	10,000 個字 元	 是
聊天應用程式 政策	管理	 是	5	10,000 個字 元	 是
AI 服務選擇退 出政策	管理	 是	5	2500 個字元	 是
Security Hub 政策	管理	 是	10	10,000 個字 元	 是

中的授權政策 AWS Organizations

中的授權政策 AWS Organizations 可讓您集中設定和管理成員帳戶中主體和資源的存取權。這些政策如何影響您套用它們的組織單位 (OUs) 和帳戶，取決於您套用的授權政策類型。

在 中有兩種不同類型的授權政策 AWS Organizations：服務控制政策 (SCPs) 和資源控制政策 (RCPs)。

主題

- [SCPs和 RCPs之間的差異](#)
- [使用 SCPs和 RCPs](#)
- [服務控制政策 \(SCP\)](#)
- [資源控制政策 RCPs\)](#)

SCPs和 RCPs之間的差異

SCPs是以主體為中心的控制項。SCPs 會針對成員帳戶中的主體可用的許可上限建立許可護欄或設定限制。當您想要對組織中的主體集中強制執行一致的存取控制時，您可以使用 SCP。這可能包括指定您的 IAM 使用者和 IAM 角色可以存取的服務、他們可以存取的資源，或是他們可以提出請求的條件（例如，來自特定區域或網路）。

RCPs是以資源為中心的控制項。RCPs 會針對成員帳戶中資源可用的許可上限建立許可護欄或設定限制。當您想要在組織中跨資源集中強制執行一致的存取控制時，可以使用 RCP。這可能會限制對資源的存取，以便只能由屬於您組織的身分存取，或指定組織外部身分可存取您資源的條件。

某些控制項可以透過 SCPs 和 RCPs 以類似方式套用。例如，您可能想要[防止使用者將未加密的物件上傳到 S3](#)，該物件可以寫入 SCP，以對主體可以對 S3 儲存貯體採取的動作強制執行控制。此控制項也可以寫入 RCP，以便在任何主體將物件上傳至 S3 儲存貯體時要求加密。如果您的儲存貯體允許第三方廠商等組織外部的實體將物件上傳至 S3 儲存貯體，則可能會偏好第二個選項。不過，某些控制項只能在 RCP 中實作，而某些控制項只能在 SCP 中實作。如需詳細資訊，請參閱[SCPs和 RCPs的一般使用案例](#)。

使用 SCPs和 RCPs

SCPs和 RCPs是獨立的控制項。您可以選擇只啟用 SCPs或 RCPs，或同時使用兩種政策類型。透過同時使用 SCPs 和 RCPs，您可以建立圍繞身分和資源的[資料周邊](#)。

SCPs可讓您控制身分可存取的資源。例如，您可能想要允許身分存取 AWS 組織中的資源。不過，您可能想要防止身分存取組織外部的資源。您可以使用 SCPs強制執行此控制項。

RCPs提供控制哪些身分可以存取您的資源的能力。例如，您可能想要允許組織中的身分存取組織中的資源。不過，您可能想要防止組織外部的身分存取您的資源。您可以使用 RCPs強制執行此控制項。RCPs可讓您為組織外部存取資源的主體，提供影響有效許可的能力。SCPs只能影響 AWS 組織內主體的有效許可。

SCPs和 RCPs的一般使用案例

下表詳細說明使用 SCP 和 RCPs的一般使用案例

使用案例	政策類型	影響			
		您的身分	外部身分	您的資源	外部資源 (請求的目標)
Restrict which services or actions your identities can use	SCP	X		X	X
Restrict which resources your identities can access	SCP	X		X	X
Enforce requirements on how your identities can access resources	SCP	X		X	X
Restrict which identities can access your resources	RCP	X	X	X	

影響				
Protect sensitive resources in your organization	RCP	X	X	X
Enforce requirements on how your resources can be accessed	RCP	X	X	X

服務控制政策 (SCP)

服務控制政策 (SCP) 是一種組織政策類型，可用來管理您的組織中的許可。SCPs 可讓您集中控制組織中 IAM 使用者和 IAM 角色的最大可用許可。SCP 可協助您確保您的帳戶符合組織的存取控制指導方針。SCP 只有在[啟用所有功能](#)的組織中才能使用。若您的組織只啟用了合併帳單功能，便無法使用 SCP。如需啟用 SCP 的說明，請參閱[啟用政策類型](#)。

SCPs 不會將許可授予組織中的 IAM 使用者和 IAM 角色。SCP 沒有授予與任何許可。SCP 會針對組織中 IAM 使用者和 IAM 角色可執行的動作，定義許可護欄或設定限制。若要授予許可，管理員必須連接政策來控制存取，例如連接到 IAM 使用者和 IAM 角色的身分型政策，以及連接到您帳戶中資源的資源型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[身分型政策和資源型政策](#)。

[有效許可](#)是 SCP 和資源[控制政策 \(RCPs\)](#) 允許的內容與身分型和資源型政策允許的內容之間的邏輯交集。

SCPs 不會影響管理帳戶中的使用者或角色

SCP 不會影響管理帳戶中的使用者或角色。它們只會影響組織中的成員帳戶。這也表示 SCPs 適用於指定為委派管理員的成員帳戶。

本頁主題

- [測試 SCP 的效果](#)

- [SCP 的大小上限](#)
- [將 SCP 連接至組織中的不同層級](#)
- [SCP 對許可的影響](#)
- [使用存取資料來改進 SCP](#)
- [任務和實體不受 SCP 的限制](#)
- [SCP 評估](#)
- [SCP 語法](#)
- [服務控制政策範例](#)
- [使用 對服務控制政策 SCPs\) 進行故障診斷 AWS Organizations](#)

測試 SCP 的效果

AWS 強烈建議您不要在未徹底測試政策對帳戶的影響的情況下，將 SCPs 連接到組織的根目錄。而是建立一個 OU，讓您一次將一個帳戶 (或至少為少量帳戶) 移至其中，確保您不會不慎將使用者鎖在重要服務之外。判斷服務是否正由帳戶使用的其中一種方法是檢查 [IAM 中上次存取資料的服務](#)。另一種方法是[使用 AWS CloudTrail 記錄 API 層級的服務用量](#)。

Note

您不應移除 FullAWSAccess 政策，除非您使用允許的動作對其進行修改或取代為單獨的政策，否則來自成員帳戶的所有 AWS 動作均將失敗。

SCP 的大小上限

您 SCP 中所有的字元都會計入其[大小上限](#)。本指南中範例顯示的 SCP 格式具有額外的空格，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

Tip

使用視覺化編輯器建置您的 SCP。它會自動移除額外空格。

將 SCP 連接至組織中的不同層級

如需 SCP 運作方式的詳細說明，請參閱 [SCP 評估](#)。

SCP 對許可的影響

SCPs類似於 AWS Identity and Access Management 許可政策，並使用幾乎相同的語法。但是，SCP 永遠不會授予許可。反之，SCPs是存取控制，可指定組織中 IAM 使用者和 IAM 角色的最大可用許可。如需詳細資訊，請參閱 IAM 使用者指南中的[政策評估邏輯](#)。

- SCP 只會影響由屬於組織一部分的帳戶管理的 IAM 使用者和角色。SCP 不會直接影響資源型政策。也不會影響來自組織外部帳戶的使用者或角色。例如，假設組織中的帳戶 A 擁有一個 Amazon S3 儲存貯體。儲存貯體政策 (資源型政策) 會授予來自組織外部帳戶 B 的使用者存取。帳戶 A 有連接一個 SCP。SCP 不會套用至帳戶 B 中的外部使用者。SCP 僅會套用至組織中帳戶 A 管理的使用者。
- SCP 會限制 IAM 使用者和成員帳戶中 IAM 使用者和角色的許可，包括成員帳戶的根使用者。任何帳戶只會擁有其上「每個」父系允許的許可。如果帳戶上方的任何層級封鎖了許可，無論是隱含 (不包含在 Allow 政策陳述式中) 或是明確 (包含在 Deny 政策陳述式中)，受影響的帳戶中的使用者或角色都將無法使用該許可，即使帳戶管理員將具備 */* 許可的 AdministratorAccess IAM 政策連接到使用者也一樣。
- SCP 僅影響組織中的成員帳戶。它們對管理帳戶中的使用者或角色沒有影響。這也表示 SCPs適用於指定為委派管理員的成員帳戶。如需詳細資訊，請參閱[管理帳戶的最佳實務](#)。
- 使用者和角色仍必須使用適當的 IAM 許可政策授予許可。沒有任何 IAM 許可政策的使用者將不具備存取權，即使適用的 SCP 允許所有服務和動作。
- 如果使用者或角色擁有的 IAM 許可政策，會授予存取適用 SCP 也允許的動作，使用者或角色即可執行該動作。
- 如果使用者或角色擁有的 IAM 許可政策，會授予存取權給適用的 SCP 不允許或明確拒絕的動作，使用者或角色即無法執行該動作。
- SCP 會影響連接的帳戶中的所有使用者和角色，包括根帳戶使用者。唯一的例外狀況，詳述於[任務和實體不受 SCP 的限制](#)。
- SCP 不會影響任何服務連結角色。服務連結角色可讓其他 與 AWS 服務 整合 AWS Organizations，且無法受到 SCPs限制。
- 當您停用根中的 SCP 政策類型時，所有 SCPs都會自動與該根中的所有 AWS Organizations 實體分離。AWS Organizations 實體包括組織單位、組織和帳戶。如果您在根帳戶重新啟用 SCP，該根帳戶只會還原為根帳戶中自動連接到所有實體的預設 FullAWSAccess 政策。停用 SCP 之前對 AWS Organizations 實體的任何 SCP 連接都會遺失，並且無法自動復原，雖然您可以手動重新連接他們。
- 若許可邊界 (進階 IAM 功能) 和 SCP 同時存在，則邊界、SCP 和身分類型政策必須全部允許動作。

使用存取資料來改進 SCP

使用管理帳戶登入資料登入時，您可以在 IAM 主控台的 AWS Organizations 區段中檢視 AWS Organizations 實體或政策的[服務上次存取資料](#)。您也可以使用 IAM 中的 AWS Command Line Interface (AWS CLI) 或 AWS API 來擷取服務上次存取的資料。此資料包含有關 AWS Organizations IAM 使用者和角色上次嘗試存取之允許的服務，以及何時存取的資訊。您可以使用此資訊來找出未使用的許可，以便微調您的 SCP，使其更完善地遵循[最低權限](#)的原則。

例如，您可能有一個[拒絕清單 SCP](#)，禁止存取三個 AWS 服務。未列在 SCP Deny 陳述式中的所有服務都可獲允。IAM 中的服務上次存取資料會告訴您 SCP AWS 服務 允許但從未使用過哪些資料。有了該資訊，您可以更新 SCP 以拒絕存取您不需要的服務。

如需詳細資訊，請參閱《IAM 使用者指南》中的以下主題：

- [檢視 Organizations 的 Organizations 服務上次存取資料](#)
- [使用資料來調整組織單位的許可](#)

任務和實體不受 SCP 的限制

您無法使用 SCP 限制下列任務：

- 管理帳戶執行的任何動作
- 任何使用連接到服務連結角色之許可所執行的動作
- 以根帳戶使用者身分註冊企業支援計劃
- 為 CloudFront 私有內容提供可信簽署者功能
- 將 Amazon Lightsail 電子郵件伺服器和 Amazon EC2 執行個體的反向 DNS 設定為根使用者
- 某些 AWS 相關服務的任務：
 - Alexa Top Sites
 - Alexa Web Information Service
 - Amazon Mechanical Turk
 - Amazon 產品行銷 API

SCP 評估

Note

本節中的資訊不適用於管理政策類型，包括備份政策、標籤政策、聊天應用程式政策或 AI 服務選擇退出政策。如需詳細資訊，請參閱[理解管理政策繼承](#)。

由於可以在 AWS Organizations 中連接不同層級的多個服務控制政策 (SCP)，因此理解 SCP 的評估方式可協助您撰寫產生正確結果的 SCP。

主題

- [SCP 如何使用允許陳述式](#)
- [SCP 如何使用拒絕陳述式](#)
- [使用 SCP 的策略](#)

SCP 如何使用允許陳述式

對於為特定帳戶允許的許可，每個層級都必須有明確的 **Allow** 陳述式，範圍從根目錄到帳戶直接路徑中的每個 OU (包括目標帳戶本身)。因此，當您啟用 SCPs 時，會 AWS Organizations 連接名為 [FullAWSAccess](#) 的 AWS 受管 SCP 政策，以允許所有服務和動作。如果移除此政策且未在組織的任何層級取代，則該層級下的所有 OU 和帳戶都會遭到封鎖，無法執行任何動作。

例如，讓我們逐步瀏覽圖 1 和圖 2 中顯示的場景。對於在帳戶 B 中允許的許可或服務，應將允許此許可或服務的 SCP 連接至根、生產 OU 和帳戶 B 本身。

SCP 評估遵循預設拒絕模型，這意味著 SCP 中未明確允許的任何許可都將被拒絕。如果在 SCP 中的任何層級 (例如根目錄、生產 OU 或帳戶 B) 均沒有允許陳述式，則會拒絕存取。

備註

- SCP 中的 Allow 陳述式允許 Resource 元素只有一個 "*" 項目。
- SCP 中的 Allow 陳述式完全不能有 Condition 元素。

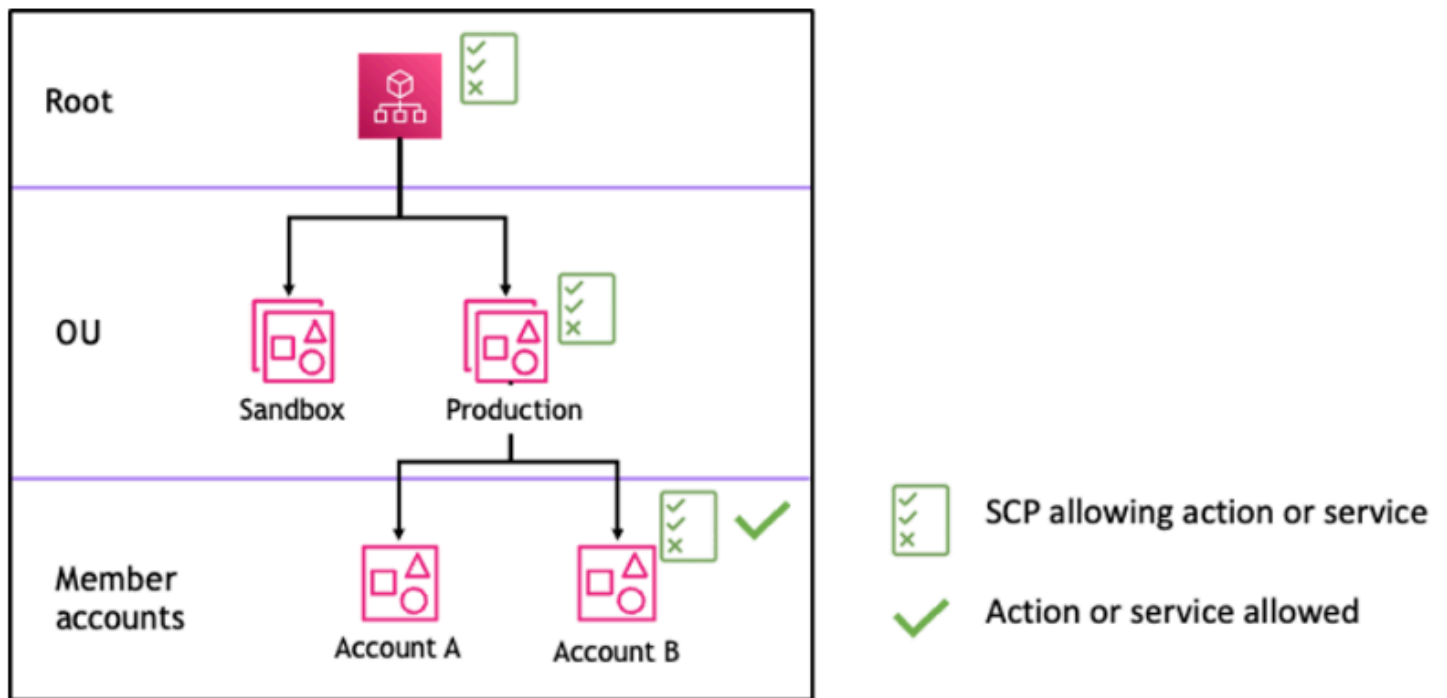


圖 1：在根、生產 OU 和帳戶 B 中連接 *Allow* 陳述式的範例組織結構

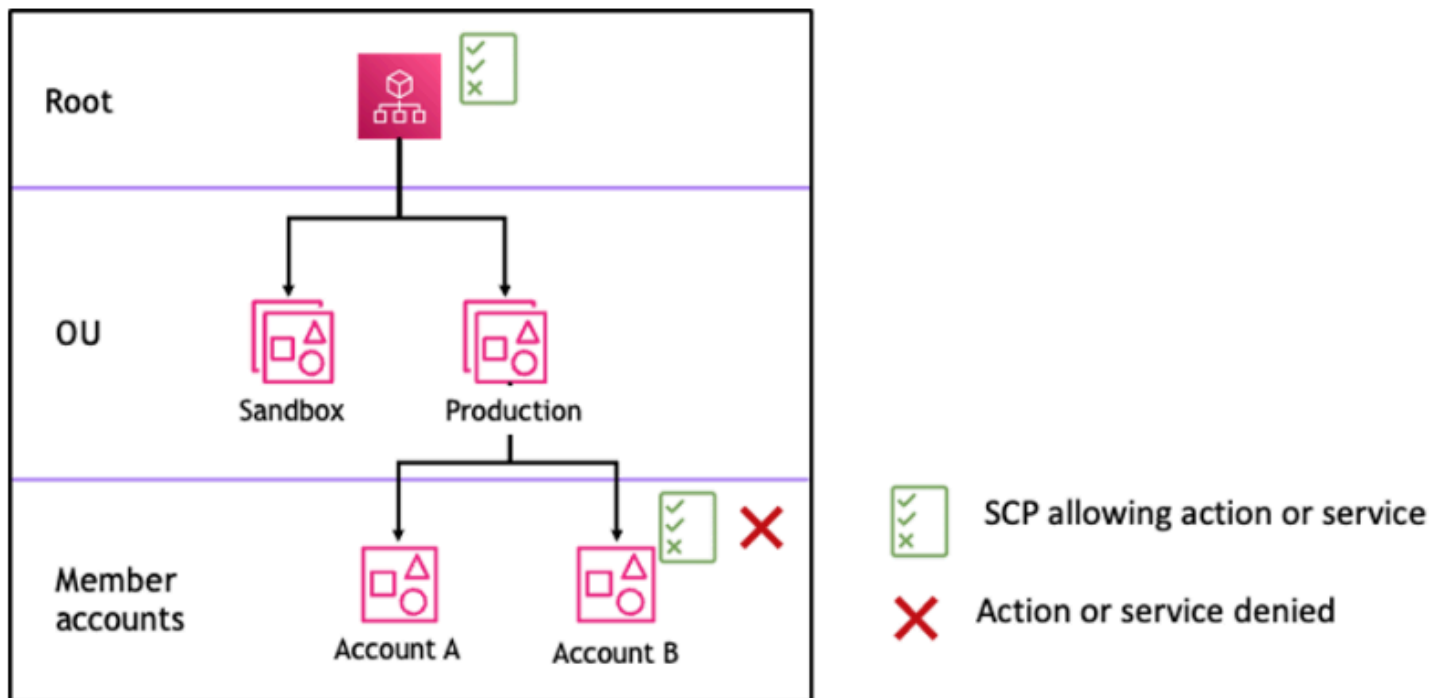


圖 2：生產 OU 中缺少 *Allow* 陳述式的範例組織結構及其對帳戶 B 的影響

SCP 如何使用拒絕陳述式

對於為特定帳戶拒絕的許可，從根目錄到帳戶直接路徑中的每個 OU (包括目標帳戶本身) 的任何 SCP 都可以拒絕該許可。

例如，假設有一個 SCP 連接至生產 OU，該 SCP 具有針對特定服務指定的明確 Deny 陳述式。剛好有另一個 SCP 連接至根和帳戶 B，其明確允許存取該相同的服務，如圖 3 所示。因此，帳戶 A 和帳戶 B 都會遭到拒絕存取該服務，因為系統會針對所有 OU 和成員帳戶評估連接至組織中任何層級的拒絕政策。

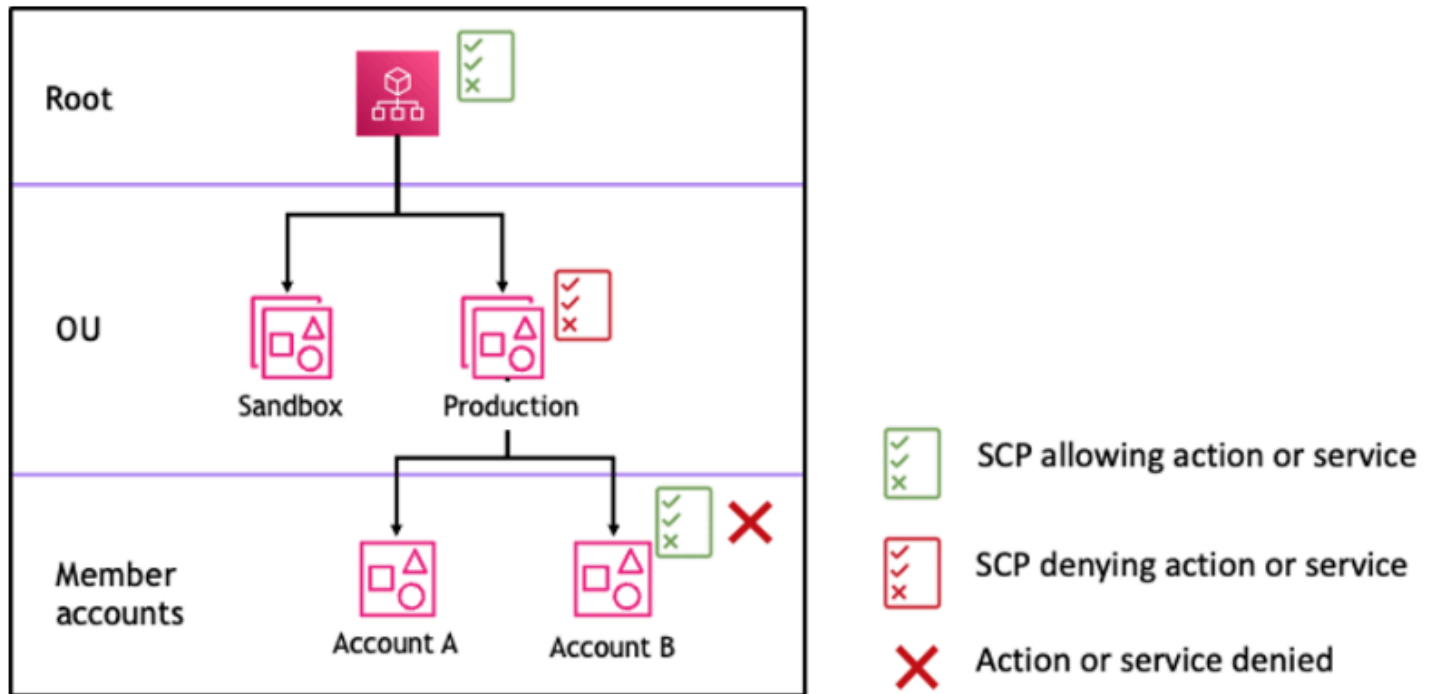


圖 3：在生產 OU 中連接 Deny 陳述式的範例組織結構及其對帳戶 B 的影響

使用 SCP 的策略

撰寫 SCP 時，您可以使用 Allow 和 Deny 陳述式的組合，以允許組織中預期的動作和服務。Deny 陳述式是實作限制的強大方法，這些限制對於組織或 OU 的較廣泛部分來說應該有效，因為在根層級或 OU 層級套用時，它們會影響其下的所有帳戶。

例如，您可以使用 Deny 陳述式 [防止成員帳戶離開組織](#)。在根層級對實作政策，這將對組織中的所有帳戶有效。拒絕陳述式也支援可協助建立例外狀況的條件元素。

Tip

您可以使用 [IAM](#) 中的 [服務上次存取資料](#) 來更新您的 SCPs，以限制僅存取您需要的 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的 [檢視 Organizations 的 Organizations 服務上次存取資料](#)。

AWS Organizations 建立時，會將名為 [FullAWSAccess](#) 的 AWS 受管 SCP 連接至每個根目錄、OU 和帳戶。此政策會允許所有服務和動作。您可以將 FullAWSAccess 取代為僅允許一組服務的政策，因此 AWS 服務不允許新的，除非更新 SCPs 明確允許。例如，如果您的組織只想要允許在環境中使用服務子集，可以使用 Allow 陳述式來僅允許特定的服務。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "cloudwatch:*",
        "organizations:*"
      ],
      "Resource": "*"
    }
  ]
}
```

結合這兩種陳述式的政策可能如以下範例所示，其中會阻止成員帳戶離開組織並允許使用所需的 AWS 服務。組織管理員可以分離 FullAWSAccess 政策，並改為連接此政策。

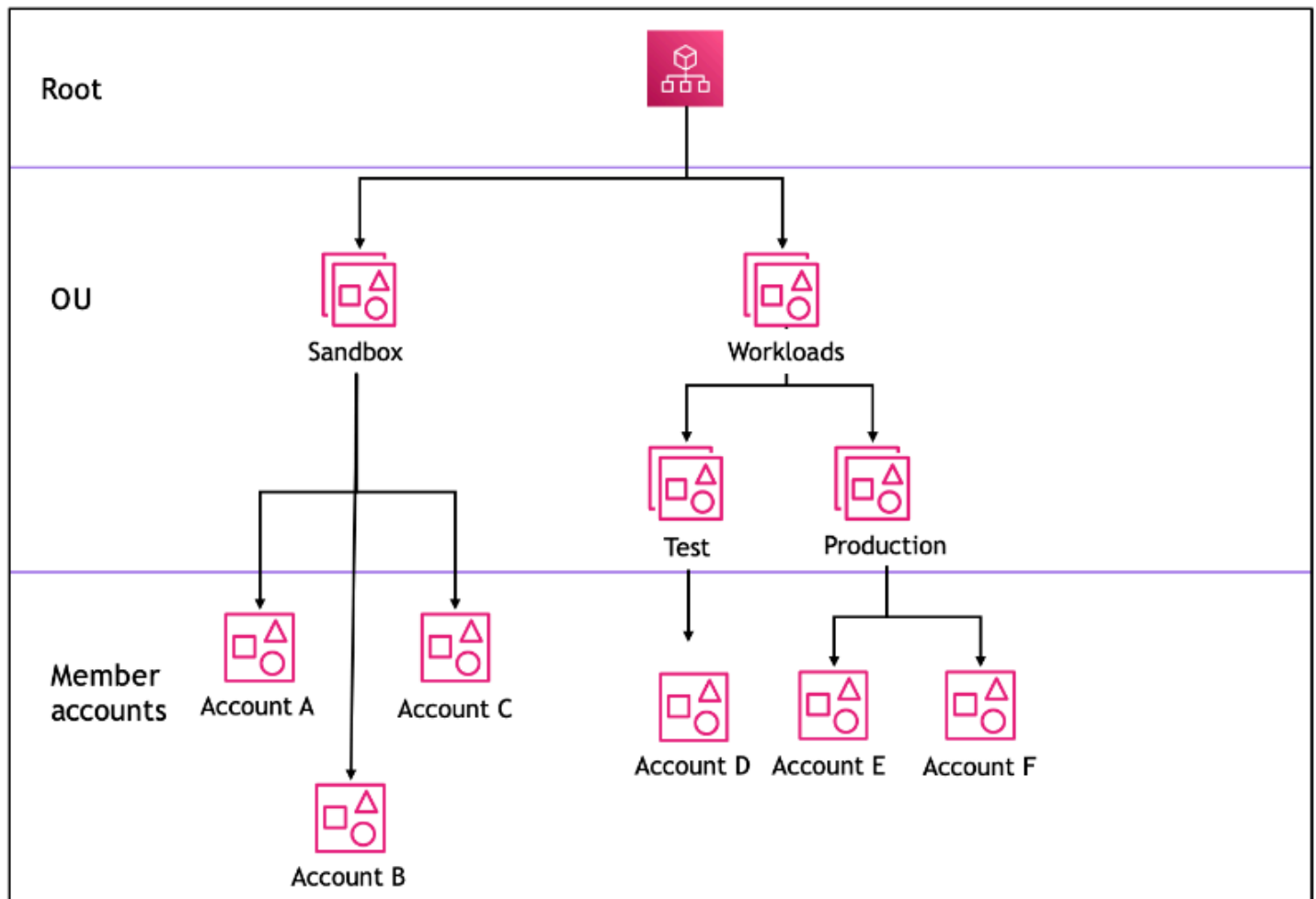
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "cloudwatch:*",
        "organizations:*"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Effect": "Deny",
      "Action": "organizations:LeaveOrganization",
      "Resource": "*"
    }
  ]
}

```

現在，請考慮下列範例組織結構，以理解如何在組織中的不同層級套用多個 SCP。



如下資料表顯示沙盒 OU 中的有效政策。

案例	根中的 SCP	沙盒 OU 中的 SCP	帳戶 A 中的 SCP	帳戶 A 中的產生政策	帳戶 B 和帳戶 C 中的產生政策
1	完整 AWS 存取	完整 AWS 存取 + 拒絕 S3 存取	完整 AWS 存取 + 拒絕 EC2 存取	無 S3 存取， 無 EC2 存取	無 S3 存取
2	完整 AWS 存取	允許 EC2 存取	允許 EC2 存取	允許 EC2 存取	允許 EC2 存取
3	拒絕 S3 存取	允許 S3 存取	完整 AWS 存取	無服務存取	無服務存取

如下資料表顯示工作負載 OU 中的有效政策。

案例	根中的 SCP	工作負載 OU 中的 SCP	測試 OU 中的 SCP	帳戶 D 中的產生政策	生產 OU、帳戶 E 和帳戶 F 中的產生政策
1	完整 AWS 存取	完整 AWS 存取	完整 AWS 存取 + 拒絕 EC2 存取	無 EC2 存取	完整 AWS 存取
2	完整 AWS 存取	完整 AWS 存取	允許 EC2 存取	允許 EC2 存取	完整 AWS 存取
3	拒絕 S3 存取	完整 AWS 存取	允許 S3 存取	無服務存取	無 S3 存取

SCP 語法

服務控制政策 (SCPs) 使用的語法與 AWS Identity and Access Management (IAM) 許可政策和資源型政策（例如 Amazon S3 儲存貯體政策）使用的語法類似。如需 IAM 政策及其語法的詳細資訊，請參閱 IAM 使用者指南中的 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html 指南中的 IAM 政策概觀。

SCP 是根據 [JSON](#) 規則進行結構化的純文字檔。本主題描述它使用的元素。

 Note

您 SCP 中所有的字元都會計入其[大小上限](#)。本指南中範例顯示的 SCP 格式具有額外的空格，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

如需 SCP 的一般資訊，請參閱[服務控制政策 \(SCP\)](#)。

元素摘要

下表摘要說明您可以在 SCP 中使用的政策元素。有些政策元素僅能在拒絕動作的 SCP 中使用。Supported effects (支援效果) 欄會列出您在 SCP 中可搭配每個政策元素使用的效果類型。

Element	用途	支援效果
Action	指定 SCP 允許或拒絕 AWS 的服務和動作。	Allow, Deny
效果	定義 SCP 陳述式是要 允許 還是 拒絕 存取帳戶中的 IAM 使用者和角色。	Allow, Deny
Statement	做為政策元素的容器。SCP 中可包含	Allow, Deny

Element	用途	支援效果
	多個陳述式。	
Statement ID (Sid)	(選用) 提供陳述式的易記名稱。	Allow, Deny
版本	指定用於處理政策的語言語法規則。	Allow, Deny
Condition	指定決定陳述式生效時機的條件。	Deny
NotAction	指定從 SCP 豁免 AWS 的服務和動作。使用此項目以取代 Action 元素。	Deny
Resource	指定 SCP 套用 AWS 的資源。	Deny

下列各節提供如何在 SCP 中使用政策元素的更多資訊及範例。

主題

- [Action 和 NotAction 元素](#)

- [Condition 元素](#)
- [Effect 元素](#)
- [Resource 元素](#)
- [Statement 元素](#)
- [Statement ID \(Sid\) 元素](#)
- [Version 元素](#)
- [不支援的元素](#)

Action 和 NotAction 元素

每個陳述式都必須包含以下其中一個項目：

- 在允許和拒絕陳述式中，必須包含一個 Action 元素。
- 針對拒絕陳述式 (Effect 元素的值為 Deny)，必須包含一個 Action 「或」 NotAction 元素。

Action 或 NotAction 元素的值是字串的清單 (JSON 陣列)，可識別 陳述式允許或拒絕 AWS 的服務和動作。

每個字串都包含服務的縮寫 (例如 "s3"、"ec2"、"iam" 或 "organizations")，採用全部小寫，後面接著冒號，然後是來自該服務的動作。動作和註解不區分大小寫。一般而言，它們都是以每個字開頭，以大寫字母和小寫字母開頭。例如："s3:ListAllMyBuckets"。

您也可以在 SCP 中使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 作為萬用字元，以比對部分名稱相同的多個動作。值 "s3:*" 表示 Amazon S3 服務中的所有動作。值 "ec2:Describe*" 只會符合開頭為 "Describe" 的 EC2 動作。
- 使用問號 (?) 萬用字元來比對單一字元。

Note

在 SCP 中，Action 或 NotAction 元素中的萬用字元 (*) 和 (?) 只能單獨使用或用在字串結尾。它不能出現在字串開頭或中間。因此，在 SCP 中，"servicename:action*" 有效，但 "servicename:*action" 和 "servicename:some*action" 都無效。

如需在 AWS Organizations SCPs 和 IAM 許可政策中支援的所有服務和動作清單，請參閱《IAM 使用者指南》中的[AWS 服務的動作、資源和條件金鑰](#)。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：動作](#)和 [IAM JSON 政策元素：NotAction](#)。

Action 元素的範例

以下範例顯示的 SCP 包含一個陳述式，允許帳戶管理員委派帳戶中 EC2 執行個體的描述、啟動、停止和終止許可。這是[允許名單](#)的範例，當預設的 Allow * 政策未連接時非常有用，使得依預設會隱含拒絕許可。若預設的 Allow * 政策仍然連接到以下政策所連接的根、OU 或帳戶，則該政策不會有任何作用。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
      "ec2:RunInstances",
      "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
    ],
    "Resource": "*"
  }
}
```

以下範例示範如何將您不要在連接帳戶中使用的服務[加入拒絕清單](#)。它會假設預設的 "Allow *" SCP 仍連接到所有 OU 和根帳戶。此範例政策可防止連接的帳戶中的帳戶管理員針對 IAM、Amazon EC2 和 Amazon RDS 服務委派任何許可。可以委派來自其他服務的任何動作，只要沒有連接的另一個附加政策拒絕他們。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [ "iam:*", "ec2:*", "rds:*" ],
    "Resource": "*"
  }
}
```

NotAction 元素的範例

下列範例示範如何使用 NotAction 元素，將 AWS 服務排除在政策的影響之外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
      }
    }
  ]
}
```

透過此陳述式，受影響的帳戶僅限於在指定的 AWS 區域，除非在使用 IAM 動作。

Condition 元素

您可以在 SCP 中的拒絕陳述式內指定 Condition 元素。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "cloudfront:*",
        "iam:*",
        "route53:*",
        "support:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
```

```

}
]
}
}
}
]
"eu-central-1",
"eu-west-1"
]

```

除了所列服務中的動作外，此 SCP 會拒絕存取任何位於 eu-central-1 和 eu-west-1 區域外的操作。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)

Effect 元素

每個陳述式必須包含一個 Effect 元素。此值可以是 Allow 或 Deny。它會影響任何相同陳述式中列出的動作。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：效果](#)。

```
"Effect": "Allow"
```

以下範例會顯示一個具備陳述式的 SCP，該陳述式中包含了值為 Allow 的 Effect 元素，允許帳戶使用者執行 Amazon S3 服務的動作。此範例在使用 [允許清單策略](#) 的組織中很有用 (默認 FullAWSAccess 政策全部分離，因為這樣就能讓許可按預設隱含獲得拒絕)。結果是，陳述式 [允許](#) 任何連接帳戶的 Amazon S3 許可：

```
{
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

即使此陳述式使用與 IAM 許可政策相同的 Allow 值關鍵字，在 SCP 中，它仍不會實際授予使用者執行任何動作的許可。而 SCP 會充當篩選條件，為組織、組織單位 (OU) 或帳戶中的帳戶指定最大許可。在上述範例中，即使帳戶中的使用者已有連接的 AdministratorAccess 受管政策，此 SCP 仍會將受影響帳戶中的所有使用者限制為僅能存取 Amazon S3 動作。

"Effect": "Deny"

在 Effect 元素的值為 Deny 的陳述式中，您也可以將存取限制在特定資源，或是定義決定 SCP 何時生效的條件。

以下顯示範例，示範如何在拒絕陳述式中使用條件金鑰。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": "t2.micro"
      }
    }
  }
}
```

此 SCP 中的陳述式會設定一個防撞欄，防止受影響的帳戶 (其中 SCP 已連接到帳戶本身，或是連接到包含帳戶的組織根或 OU) 在 Amazon EC2 執行個體的類型並未設為 t2.micro 時啟動 Amazon EC2 執行個體。即使允許此動作的 IAM 政策已連接到帳戶，SCP 建立的防撞欄也會防止該操作。

Resource 元素

在 Effect 元素的值為 Allow 的陳述式中，您只能在 SCP 的 Resource 元素內指定 "*"。您無法指定個別資源的 Amazon 資源名稱 (ARN)。

您也可以使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 作為萬用字元，以比對部分名稱相同的多個動作。
- 使用問號 (?) 萬用字元來比對單一字元。

在 Effect 元素的值為 Deny 的陳述式中，您「可以」指定個別 ARN，如以下範例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
```

```

    "Effect": "Deny",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
    ],
    "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
    ]
  }
]
}

```

此 SCP 會限制受影響帳戶中的 IAM 使用者和角色，對您組織中所有帳戶內建立的常見管理 IAM 角色進行變更。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：資源](#)。

Statement 元素

SCP 包含一或多個 Statement 元素。您在政策中只能有一個 Statement 關鍵字，但其值可以是 JSON 陣列的陳述式 (加上 [] 字元)。

以下範例顯示單一陳述式，其中包含單一 Effect、Action 和 Resource 元素。

```

"Statement": {
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*"
}

```

以下範例包含兩個陳述式，在一個 Statement 元素內有陣列清單。第一個陳述式會允許所有動作，第二個則會拒絕任何 EC2 動作。其結果是帳戶中的管理員可委派除了 Amazon Elastic Compute Cloud (Amazon EC2) 之外的任何許可。

```

"Statement": [

```



```
{
  "Effect": "Allow",
  "Action": "*",
  "Resource": "*"
},
{
  "Effect": "Deny",
  "Action": "ec2:*",
  "Resource": "*"
}
]
```

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：陳述式](#)。

Statement ID (**Sid**) 元素

Sid 是一種您可以為政策陳述式提供的選用識別符。您可以將 Sid 值指派給陳述式陣列中的每個陳述式。以下範例 SCP 會顯示範例 Sid 陳述式。

```
{
  "Statement": {
    "Sid": "AllowsAllActions",
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*"
  }
}
```

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：ID](#)。

Version 元素

每個 SCP 必須包含具有值 "2012-10-17" 的 Version 元素。這是與 IAM 許可政策的最新版本相同的版本值。

```
"Version": "2012-10-17",
```

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：版本](#)。

不支援的元素

SCP 不支援以下元素：

- Principal
- NotPrincipal
- NotResource

服務控制政策範例

本主題中顯示的範例[服務控制政策 \(SCP\)](#) 僅供參考。

使用這些範例之前

您在組織中使用這些範例 SCP 前，請執行下列操作：

- 詳閱及自訂 SCP，使其符合您的獨特需求。
- 使用 [AWS SCP 範例](#)，徹底測試您環境中 AWS 服務的 SCPs。

本節中的範例政策示範 SCP 的實作與使用。他們並非闡述為完全如圖所示實作的官方 AWS 建議或最佳實務。您有責任仔細測試任何拒絕型政策是否適合解決您環境的商業需求。除非您將必要的例外狀況新增至政策，AWS 服務 否則拒絕型服務控制政策可能會意外限制或封鎖您對 的使用。如需此類例外狀況的範例，請參閱第一個範例，該範例會豁免全域服務，而這些規則會封鎖對不需要的存取 AWS 區域。

- 請記住，SCP 會影響其連接到每個帳戶中的每個使用者、角色，包括根使用者。
- 請記住，SCP 不會影響服務連結角色。服務連結角色可讓其他 與 AWS 服務 整合 AWS Organizations，且無法受到 SCPs 限制。

Tip

您可以使用 [IAM](#) 中的 [服務上次存取資料](#) 來更新您的 SCPs，以限制僅存取您需要的 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的 [檢視 Organizations 的 Organizations 服務上次存取資料](#)。

以下每一個政策都是[拒絕清單政策](#)策略的範例。拒絕清單政策必須隨著在受影響帳戶中允許已核准動作的其他政策連接。例如，預設的 FullAWSAccess 政策會允許使用帳戶中的所有服務。此政策預設連接到根帳戶、所有組織單位 (OU) 和所有帳戶。它不會實際授予許可；沒有任何 SCP 會這麼做。相反地，它可讓該帳戶中的管理員將標準 AWS Identity and Access Management (IAM) 許可政策連接至帳

戶中的使用者、角色或群組，以委派對這些動作的存取。然後，這些拒絕清單政策會個別藉由封鎖對指定的服務或動作的存取，來覆寫任何政策。

範例

- 一般範例
 - AWS 根據請求拒絕對 的存取 AWS 區域
 - 防止 IAM 使用者和角色進行某些變更
 - 防止 IAM 使用者和角色進行指定變更，且指定的管理員角色除外
 - 需要 MFA 才能執行 API 操作
 - 封鎖根使用者的服務存取
 - 防止成員帳戶離開組織。
- 聊天應用程式中 Amazon Q Developer SCPs
 - 拒絕所有 IAM 操作
 - 拒絕 S3 儲存貯體放置來自指定 Slack 頻道的請求
- Amazon CloudWatch 範例 SCP
 - 防止使用者停用 CloudWatch 或更改其組態
- AWS Config 的範例 SCP
 - 防止使用者停用 AWS Config 或變更其規則
- Amazon Elastic Compute Cloud (Amazon EC2) 的範例 SCP
 - 要求 Amazon EC2 執行個體使用特定類型
 - 防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體
 - 防止停用預設的 Amazon EBS 加密
 - 防止建立和連接非 gp3 磁碟區
- Amazon GuardDuty 的範例 SCP
 - 防止使用者停用 GuardDuty 或修更其組態
- 的範例 SCPs AWS Resource Access Manager
 - 防止外部共享
 - 允許特定帳戶僅共享指定的資源類型
 - 防止與組織或組織單位 (OU) 共享
 - 僅允許與指定的 IAM 使用者和角色共享
- Amazon Application Recovery Controller (ARC) SCPs

- [防止使用者更新 ARC 路由控制狀態](#)
- [適用於 Amazon S3 的 SCP 範例](#)
 - [防止 Amazon S3 未加密物件上傳](#)
- [標記資源的 SCP 範例](#)
 - [需要在建立的指定資源上使用標籤](#)
 - [防止標籤被授權委託人以外的人員修改](#)
- [Amazon Virtual Private Cloud \(Amazon VPC\) 的範例 SCP](#)
 - [防止使用者刪除 Amazon VPC 流程日誌](#)
 - [防止尚沒有網際網路存取的任何 VPC 取得存取](#)

一般範例

AWS 根據請求拒絕對 的存取 AWS 區域

此 SCP 拒絕存取任何位於指定區域外的操作。eu-west-1 將 eu-central-1 和 取代為 AWS 區域您想要使用的。它為核准之全域服務中的操作提供豁免。此範例也顯示了如何豁免由兩個指定的管理員角色之一所提出的請求。

Note

若要搭配 使用區域拒絕 SCP AWS Control Tower，請參閱《AWS Control Tower 控制參考指南》中的[AWS 根據請求拒絕對 的存取 AWS 區域](#)。

此政策會使用此 Deny 效果，來拒絕存取不以兩個核准區域 (eu-central-1 和 eu-west-1) 之一為目標之操作的所有請求。[NotAction](#) 元素可讓您列出服務，這些服務的操作 (或個別操作) 都免受此限制的約束。由於全域服務具有由 us-east-1 區域實體託管的端點，因此必須以這種方式豁免這些端點。透過以這種方式結構化的 SCP，如果要求的服務包含在 NotAction 元素中，則允許對 us-east-1 區域內全域服務提出的請求。此範例政策會拒絕任何其他對 us-east-1 區域內服務的請求。

Note

此範例可能不會包含所有最新的全域 AWS 服務 或操作。請將服務和營運項目清單替換成您組織中帳戶所使用的全球服務。

秘訣

您可以[在 IAM 主控台中檢視服務上次存取的資料](#)，以判斷您的組織使用的全域服務。IAM 使用者、群組或角色詳細資訊頁面上的 Access Advisor 索引標籤會顯示該實體已使用的 AWS 服務，按最近存取排序。

考量事項

- AWS KMS 和 AWS Certificate Manager 支援區域端點。然而，如果您想要將其與全域服務 (例如 Amazon CloudFront) 搭配使用，則必須將其包含在下列範例 SCP 的全域服務排除清單中。像 Amazon CloudFront 這樣的全球服務通常需要存取相同區域中的 AWS KMS 和 ACM，而對於全球服務而言，該服務是美國東部（維吉尼亞北部）區域 (us-east-1)。
- 根據預設，AWS STS 是全域服務，且必須包含在全域服務排除清單中。不過，您可以讓 AWS STS 使用區域端點，而不是單一全域端點。如果您執行此操作，可從下列範例 SCP 的全域服務豁免清單中移除 STS。如需詳細資訊，請參閱在 [AWS STS 中管理 AWS 區域](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "a4b:*",
        "acm:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "budgets:*",
        "ce:*",
        "chime:*",
        "cloudfront:*",
        "config:*",
        "cur:*",
        "directconnect:*",
        "ec2:DescribeRegions",
```

```

        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnGateways",
        "fms:*",
        "globalaccelerator:*",
        "health:*",
        "iam:*",
        "importexport:*",
        "kms:*",
        "mobileanalytics:*",
        "networkmanager:*",
        "organizations:*",
        "pricing:*",
        "route53:*",
        "route53domains:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "s3:GetAccountPublic*",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:PutAccountPublic*",
        "shield:*",
        "sts:*",
        "support:*",
        "trustedadvisor:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*"
    ],
    "Resource": "*",
    "Condition": {
        "StringNotEquals": {
            "aws:RequestedRegion": [
                "eu-central-1",
                "eu-west-1"
            ]
        },
        "ArnNotLike": {
            "aws:PrincipalARN": [
                "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
            ]
        }
    }
}

```

```

    }
  }
]
}

```

防止 IAM 使用者和角色進行某些變更

此 SCP 會限制 IAM 使用者和角色，對您組織中所有帳戶內建立的指定 IAM 角色進行變更。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}

```

防止 IAM 使用者和角色進行指定變更，且指定的管理員角色除外

此 SCP 是以前一個範例為基礎，為管理員設置了例外狀況。它會防止受影響帳戶中 IAM 使用者和角色，對您組織中所有帳戶內建立的常見管理 IAM 角色進行變更，但使用指定角色的管理員則除外。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "DenyAccessWithException",
    "Effect": "Deny",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
    ],
    "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
    ],
    "Condition": {
        "ArnNotLike": {
            "aws:PrincipalARN": "arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
    }
}
]
}

```

需要 MFA 才能執行 API 操作

使用如下的 SCP，來要求先啟用多重要素驗證 (MFA)，IAM 使用者和角色才能停止執行動作。在此範例中，動作是停止 Amazon EC2 執行個體。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}

```



```
}  
]  
}
```

封鎖根使用者的服務存取

下列政策會限制對成員帳戶中[根使用者](#)的所有存取。若您希望防止您的帳戶以特定方式使用根憑證，請將您自己的動作新增到此政策。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RestrictEC2ForRoot",  
      "Effect": "Deny",  
      "Action": [  
        "ec2:*"  
      ],  
      "Resource": [  
        "*"   
      ],  
      "Condition": {  
        "StringLike": {  
          "aws:PrincipalArn": [  
            "arn:aws:iam::*:root"  
          ]  
        }  
      }  
    }  
  ]  
}
```

防止成員帳戶離開組織。

下列政策會封鎖使用 LeaveOrganization API 操作，讓成員帳戶的管理員無法從組織中移除其帳戶。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Action": [  
        "iam:LeaveOrganization"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

```

        "organizations:LeaveOrganization"
      ],
      "Resource": "*"
    }
  ]
}

```

聊天應用程式中 Amazon Q Developer SCPs

此類別中的範例

- [拒絕所有 IAM 操作](#)
- [拒絕 S3 儲存貯體放置來自指定 Slack 頻道的請求](#)

拒絕所有 IAM 操作

下列 SCP 拒絕透過聊天應用程式組態中的所有 Amazon Q Developer 調用的所有 IAM 操作。

```

{
  "Effect": "Deny",
  "Action": "iam:*",
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:ChatbotSourceArn": "arn:aws:chatbot:*:*:*"
    }
  }
}

```

拒絕 S3 儲存貯體放置來自指定 Slack 頻道的請求

下列政策拒絕 S3 對來自 Slack 頻道的所有請求的指定儲存貯體提出請求。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleS3Deny",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {

```

```

        "StringLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot:*:chat-configuration/
slack-channel/*"
        }
    }
}
]
}

```

Amazon CloudWatch 範例 SCP

此類別中的範例

- [防止使用者停用 CloudWatch 或更改其組態](#)

防止使用者停用 CloudWatch 或更改其組態

較低級別的 CloudWatch 操作人員需要監控儀表板和警報。然而，操作人員必須無法刪除或變更資深人員可能會設置的任何儀表板或警示。此 SCP 可防止任何受影響帳戶中的使用者或角色執行可能刪除或變更儀表板或警示的任何 CloudWatch 命令。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}

```

AWS Config的範例 SCP

此類別中的範例

- [防止使用者停用 AWS Config 或變更其規則](#)

防止使用者停用 AWS Config 或變更其規則

此 SCP 可防止任何受影響帳戶中的使用者或角色執行可能停用 AWS Config 或修改其規則或觸發程序 AWS Config 的操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Elastic Compute Cloud (Amazon EC2) 的範例 SCP

此類別中的範例

- [要求 Amazon EC2 執行個體使用特定類型](#)
- [防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體](#)
- [防止停用預設的 Amazon EBS 加密](#)
- [防止建立和連接非 gp3 磁碟區](#)

要求 Amazon EC2 執行個體使用特定類型

使用這項 SCP，任何未使用 t2.micro 執行個體類型啟動的執行個體都會遭到拒絕。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "RequireMicroInstanceType",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringNotEquals": {
            "ec2:InstanceType": "t2.micro"
        }
    }
}
]
}

```

防止在沒有 IMDSv2 的情況下啟動 EC2 執行個體

以下政策限制所有使用者在沒有 IMDSv2 的情況下啟動 EC2 執行個體。

```

[
  {
    "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": "2"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
  }
]

```

```

    "Condition":{
      "NumericLessThan":{
        "ec2:RoleDelivery":"2.0"
      }
    },
    {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
    }
  ]

```

以下政策限制所有使用者在沒有 IMDSv2 的情況下啟動 EC2 執行個體，但允許特定 IAM 身分修改執行個體中繼資料選項。

```

[
  {
    "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": "2"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {

```

```

        "ec2:RoleDelivery": "2.0"
    }
}
},
{
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
        "ArnNotLike": {
            "aws:PrincipalARN": [
                "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
            ]
        }
    }
}
}
]

```

防止停用預設的 Amazon EBS 加密

以下政策限制所有使用者停用預設的 Amazon EBS 加密。

```

{
    "Effect": "Deny",
    "Action": [
        "ec2:DisableEbsEncryptionByDefault"
    ],
    "Resource": "*"
}

```

防止建立和連接非 gp3 磁碟區

下列政策會限制所有使用者建立或連接不屬於 gp3 磁碟區類型的任何 Amazon EBS 磁碟區。如需詳細資訊，請參閱 [Amazon EBS 磁碟區類型](#)。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
            "Effect": "Deny",
            "Action": [

```

```

        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
        "StringNotEquals": {
            "ec2:VolumeType": "gp3"
        }
    }
}
]
}

```

這有助於在整個組織中強制執行標準化磁碟區組態。

不會阻止磁碟區類型修改

您不能限制使用 SCPs 將現有 gp3 磁碟區修改為其他類型的 Amazon EBS 磁碟區的動作。例如，此 SCP 不會阻止您將現有的 gp3 磁碟區修改為 gp2 磁碟區。這是因為條件金鑰會在修改磁碟區之前 ec2:VolumeType 檢查磁碟區類型。

Amazon GuardDuty 的範例 SCP

此類別中的範例

- [防止使用者停用 GuardDuty 或修更其組態](#)

防止使用者停用 GuardDuty 或修更其組態

此 SCP 可防止任何受影響帳戶中的使用者或角色停用 GuardDuty，或更改其組態，無論直接以命令形式或透過主控台。它有效地啟用對 GuardDuty 資訊和資源的唯讀存取。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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:DisassociateFromMasterAccount",
        "guardduty:DisassociateMembers",
        "guardduty:InviteMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:TagResource",
        "guardduty:UnarchiveFindings",
        "guardduty:UntagResource",
        "guardduty:UpdateDetector",
        "guardduty:UpdateFilter",
        "guardduty:UpdateFindingsFeedback",
        "guardduty:UpdateIPSet",
        "guardduty:UpdatePublishingDestination",
        "guardduty:UpdateThreatIntelSet"
    ],
    "Resource": "*"
}
]
}

```

的範例 SCPs AWS Resource Access Manager

此類別中的範例

- [防止外部共享](#)
- [允許特定帳戶僅共享指定的資源類型](#)
- [防止與組織或組織單位 \(OU\) 共享](#)
- [僅允許與指定的 IAM 使用者和角色共享](#)

防止外部共享

下列範例 SCP 可防止使用者建立資源共享，以允許與不屬於組織的 IAM 使用者和角色共享。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "ram:RequestedAllowsExternalPrincipals": "true"
        }
      }
    }
  ]
}
```

允許特定帳戶僅共享指定的資源類型

下列 SCP 允許帳戶 111111111111 和 222222222222 以建立共享字首清單的資源共享，並將字首清單與現有的資源共享關聯。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OnlyNamedAccountsCanSharePrefixLists",
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "111111111111",

```

```

        "222222222222"
      ]
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:PrefixList"
    }
  }
}
]
}

```

防止與組織或組織單位 (OU) 共享

下列 SCP 可防止使用者建立與組織或 OUs 共用資源的資源共用。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "ram:Principal": [
            "arn:aws:organizations::*:organization/*",
            "arn:aws:organizations::*:ou/*"
          ]
        }
      }
    }
  ]
}

```

僅允許與指定的 IAM 使用者和角色共享

下列範例 SCP 允許使用者僅與組織 o-12345abcdef、組織單位 ou-98765fedcba，以及帳戶 111111111111 共享資源。

```

{

```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Deny",
        "Action": [
          "ram:AssociateResourceShare",
          "ram:CreateResourceShare"
        ],
        "Resource": "*",
        "Condition": {
          "ForAnyValue:StringEquals": {
            "ram:Principal": [
              "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
              "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
              "111111111111"
            ]
          }
        }
      }
    ]
  }
}

```

Amazon Application Recovery Controller (ARC) SCPs

此類別中的範例

- [防止使用者更新 ARC 路由控制狀態](#)

防止使用者更新 ARC 路由控制狀態

較低層級的 ARC 運算子需要監控儀表板和檢視 ARC 資訊。不過，運算子必須無法更新路由控制，使其無法將應用程式從一個容錯移轉 AWS 區域 到另一個，因為資深運算子可能會允許。此 SCP 可防止任何受影響帳戶中的使用者或角色執行更新 ARC 路由控制的 ARC 操作。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAll",
      "Effect": "Deny",
      "Action": [

```

```

        "route53-recovery-cluster:UpdateRoutingControlState",
        "route53-recovery-cluster:UpdateRoutingControlStates"
    ],
    "Resource": "*",
    "Condition": {
        "ArnNotLike": {
            "aws:PrincipalARN": [
                "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
            ]
        }
    }
}
]
}

```

適用於 Amazon S3 的 SCP 範例

Note

Amazon Simple Storage Service (Amazon S3) 會自動將伺服器端加密 (SSE-S3) 套用至每個新物件，除非您指定不同的加密選項。如需詳細資訊，請參閱 [《Amazon S3 使用者指南》中的 Amazon S3 現在會自動加密所有新物件](#)。Amazon S3

此類別中的範例

- [防止 Amazon S3 未加密物件上傳](#)

防止 Amazon S3 未加密物件上傳

以下政策限制所有使用者將未加密的物件上傳至 S3 儲存貯體。

```

{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}

```

```
}
```

以下政策限制所有使用者將未加密的物件上傳至 S3 儲存貯體，並強制執行指定的加密類型 (AES256 或 aws:kms)，以便在其儲存貯體中進行物件上傳。

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

標記資源的 SCP 範例

此類別中的範例

- [需要在建立的指定資源上使用標籤](#)
- [防止標籤被授權委託人以外的人員修改](#)

需要在建立的指定資源上使用標籤

如果請求未包含指定的標籤，下列 SCP 可防止受影響帳戶中的 IAM 使用者和角色建立某些資源類型。

⚠ Important

請記得透過您在環境中使用的服務來測試拒絕型政策。下列範例是建立未標記機密或執行未標記 Amazon EC2 執行個體的簡單區塊，且不包含任何例外狀況。

下列範例政策與 AWS CloudFormation 不相容，因為該服務會建立秘密，然後將其標記為兩個不同的步驟。此範例政策可有效地 AWS CloudFormation 封鎖在堆疊中建立秘密，因為這類動作會導致在未視需要加上標籤的秘密中短暫發生。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
```

```

        "Null": {
            "aws:RequestTag/CostCenter": "true"
        }
    },
    {
        "Sid": "DenyRunInstanceWithNoCostCenterTag",
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Condition": {
            "Null": {
                "aws:RequestTag/CostCenter": "true"
            }
        }
    }
]
}

```

如需在 AWS Organizations SCPs 和 IAM 許可政策中支援的所有服務和動作清單，請參閱《IAM 使用者指南》中的[適用於的動作、資源和條件金鑰 AWS 服務](#)。

防止標籤被授權委託人以外的人員修改

下列 SCP 顯示政策如何僅允許授權委託人修改連接至您資源的標籤。這是使用屬性型存取控制 (ABAC) 作為 AWS 雲端安全策略的一部分的重要部分。該政策允許呼叫者僅修改以下資源上的標籤：其授權標籤 (在本例中為 `access-project`) 與連接至發出請求的使用者或角色的相同授權標籤完全相符。該政策也會防止授權使用者變更為用於授權的標籤值。呼叫委託人必須具有授權標籤，才能完全進行任何變更。

該政策只會阻止未經授權的使用者變更標記。未被此政策封鎖的授權使用者仍必須具有單獨的 IAM 政策，明確授予相關標記 API 上的 Allow 許可。舉例來說，如果您的使用者具有 Allow `/*/*` 的管理員政策 (允許所有服務和所有操作)，則組合會導致允許管理員使用者僅變更以下標籤：具有與連接至使用者委託人的授權標籤值相符的授權標籤值。這是因為該政策中的明確 Deny 會覆寫管理員政策中的明確 Allow。

Important

這並非完整的政策解決方案，不應如此處所示使用。此範例僅用於說明 ABAC 策略的一部分，且需要針對生產環境進行自訂與測試。

如需完整的政策及其運作方式的詳細分析，請參閱[AWS Organizations中的使用服務控制政策來保護用於授權的資源標籤](#)

請記得透過您在環境中使用的服務來測試拒絕型政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
        },
        "Null": {
          "ec2:ResourceTag/access-project": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```

```

        "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}]",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "access-project"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
        },
        "Null": {
            "aws:PrincipalTag/access-project": true
        }
    }
}
]
}

```

Amazon Virtual Private Cloud (Amazon VPC) 的範例 SCP

此類別中的範例

- [防止使用者刪除 Amazon VPC 流程日誌](#)
- [防止尚沒有網際網路存取的任何 VPC 取得存取](#)

防止使用者刪除 Amazon VPC 流程日誌

此 SCP 可防止任何受影響帳戶中的使用者或角色刪除 Amazon Elastic Compute Cloud (Amazon EC2) 流程日誌或 CloudWatch 日誌群組或日誌串流。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
}
```

防止尚沒有網際網路存取的任何 VPC 取得存取

此 SCP 可防止任何受影響帳戶中的使用者或角色變更您的 Amazon EC2 Virtual Private Cloud (VPC) 的組態，以授予它們網際網路的直接存取。它不會封鎖現有的直接存取，或透過您的現場部署網路環境路由的任何存取。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

使用 對服務控制政策 (SCPs) 進行故障診斷 AWS Organizations

使用此處的資訊來協助您診斷和修正服務控制政策 (SCPs) 中常見的錯誤。

中的服務控制政策 (SCPs) AWS Organizations 類似於 IAM 政策，並共用通用語法。此語法的開頭為 [JavaScript 物件標記法 \(JSON\)](#) 規則。JSON 描述物件，其具有的名稱和值組會構成物件。[IAM 政策文法](#) 以該文法為基礎，定義哪些名稱和值具有意義，且可由使用政策授予許可 AWS 服務 的理解。

AWS Organizations 使用 IAM 語法和語法的子集。如需詳細資訊，請參閱 [SCP 語法](#)。

常見的政策錯誤

- [多個政策物件](#)
- [多個陳述式元素](#)
- [政策文件大小超過上限](#)

多個政策物件

一個 SCP 必須僅包含一個 JSON 物件。可在兩旁放置 {} 括弧來表示物件。雖然您可以在外側括弧對中嵌入額外的 {} 括弧以在 JSON 物件中巢套其他物件，但是一個政策只能包含一個最外層的 {} 括弧對。以下範例不正確，因為它在最上層包含兩個物件 (以 ## 標示)：

```
{
  "Version": "2012-10-17",
  "Statement":
  {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  }
}
{
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
}
```

不過，您可以使用正確的政策語法來達成前述範例的意圖。可以將兩個資料塊合併到單個 Statement 元素中，而非包含兩個各自擁有 Statement 元素的完整政策物件。Statement 元素將兩個物件組成的陣列作為其值，如以下範例所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

此範例無法進一步的壓縮到具有一個元素的 Statement，因為這兩個元素有不同的效果。一般而言，只有在每個陳述式中的 Effect 和 Resource 元素完全相同時，您才可以結合陳述式。

多個陳述式元素

此錯誤可能會先以上一章節中錯誤的變異顯示。但是，它在語法上是不同類型的錯誤。在以下範例中，頂層只有一個政策物件，由單一 {} 括弧組表示。但是，該物件包含兩個 Statement 元素。

一個 SCP 只能包含一個 Statement 元素，名稱 (Statement) 在冒號左側，它的值在冒號右側。Statement 元素的值必須是物件，以 {} 括弧表示，其中包含一個 Effect 元素、一個 Action 元素和一個 Resource 元素。以下範例不正確，因為在政策物件中包含兩個 Statement 元素：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
```

```
"Action": "s3:*",  
"Resource": "*" }  
}
```

由於值物件可以是多個值物件的陣列，您可以將兩個 Statement 元素結合到具有物件陣列的一個元素來解決這個問題，如以下範例所示：

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:Describe*",  
      "Resource": "*" }  
    ,  
    {  
      "Effect": "Deny",  
      "Action": "s3:*",  
      "Resource": "*" }  
  ]  
}
```

Statement 元素的值是一種物件陣列。此範例中的陣列包含兩個物件，每個物件是 Statement 元素的正確值。陣列中的每個物件之間用逗號隔開。

政策文件大小超過上限

SCP 文件的大小上限是 5,120 個字元。此大小上限包括所有字元 (包含空格)。若要減少 SCP 的大小，您可以移除引號外部的所有空格字元 (例如空格和換行字元)。

Note

如果您使用 儲存政策 AWS Management Console，則會移除 JSON 元素和引號外部的額外空格，而不會計入。如果您使用 SDK 操作或 儲存政策 AWS CLI，則政策會完全按照您提供的方式儲存，不會自動移除字元。

資源控制政策 RCPs)

Note

服務控制政策 (SCPs) 和資源控制政策 (RCPs)

當您需要限制組織成員帳戶中 IAM 主體的許可時，請使用 SCP。

當您需要限制組織帳戶外部的 IAM 主體，請求存取組織成員帳戶中的資源時，請使用 RCP。

如需詳細資訊，請參閱[了解 SCPs和 RCPs](#)。

資源控制政策 (RCPs) 是一種組織政策，可用來管理組織中的許可。RCPs可讓您集中控制組織中資源的最大可用許可。RCPs可協助您確保帳戶中的資源符合組織的存取控制準則。RCPs僅適用於[已啟用所有功能的](#)組織。如果您的組織只啟用合併帳單功能，則無法使用 RCPs。如需啟用 RCPs的說明，請參閱[啟用政策類型](#)。

僅 RCPs 不足以將許可授予組織中的資源。RCP 不會授予任何許可。RCP 會針對身分可對組織中資源採取的動作，定義許可護欄或設定限制。管理員仍然必須將身分型政策連接到 IAM 使用者或角色，或將資源型政策連接到您帳戶中的資源，以實際授予許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[身分型政策和資源型政策](#)。

[有效許可](#)是 RCPs [和服務控制政策 \(SCPs\)](#) 允許的內容與身分型和資源型政策允許的內容之間的邏輯交集。

RCPs不會影響管理帳戶中的資源

RCPs不會影響管理帳戶中的資源。它們只會影響組織中成員帳戶中的資源。這也表示 RCPs適用於指定為委派管理員的成員帳戶。

本頁主題

- [AWS 服務 支援 RCPs 清單](#)
- [測試 RCPs的效果](#)
- [RCPs的大小上限](#)
- [將 RCPs連接到組織中的不同層級](#)
- [RCP 對許可的影響](#)
- [不受 RCPs 限制的資源和實體](#)
- [RCP 評估](#)

- [RCP 語法](#)
- [資源控制政策範例](#)

AWS 服務 支援 RCPs 清單

RCPs適用於下列項目的動作 AWS 服務：

- [Amazon Simple Storage Service \(Amazon S3\)](#)
- [AWS Security Token Service](#)
- [AWS Key Management Service](#)
- [Amazon SQS](#)
- [AWS Secrets Manager](#)
- [Amazon Elastic Container Registry](#)
- [Amazon OpenSearch Serverless](#)

測試 RCPs的效果

AWS 強烈建議您不要在不徹底測試政策對您帳戶中資源的影響的情況下，將 RCPs 連接到組織的根目錄。您可以先將 RCPs 連接至個別測試帳戶、將其移至階層中較低的 OUs，然後視需要逐步完成組織結構。判斷影響的一種方法是檢閱拒絕存取錯誤的 AWS CloudTrail 日誌。

RCPs的大小上限

RCP 中的所有字元都會計入其[大小上限](#)。本指南中的範例顯示以額外空格格式化的 RCPs，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

Tip

使用視覺化編輯器來建置 RCP。它會自動移除額外空格。

將 RCPs連接到組織中的不同層級

您可以直接將 RCPs 連接到個別帳戶、OUs 或組織根目錄。如需 RCPs運作方式的詳細說明，請參閱[RCP 評估](#)。

RCP 對許可的影響

RCPs AWS Identity and Access Management (IAM) 政策。它們與以[資源為基礎的政策](#)最密切相關。不過，RCP 永遠不會授予許可。反之，RCPs是存取控制，可指定組織中資源的可用許可上限。如需詳細資訊，請參閱 IAM User Guide 中的 [Policy evaluation logic](#)。

- RCPs適用於子集的資源 AWS 服務。如需詳細資訊，請參閱[AWS 服務 支援 RCPs 清單](#)。
- RCP 只會影響由屬於已連接 RCP 之組織一部分的帳戶管理的資源。RCPs 它們不會影響來自組織外部帳戶的資源。例如，請考慮組織中帳戶 A 擁有的 Amazon S3 儲存貯體。儲存貯體政策（以資源為基礎的政策）會將存取權授予組織外部帳戶 B 的使用者。帳戶 A 已連接 RCP。即使由帳戶 B 的使用者存取，該 RCP 也適用於帳戶 A 中的 S3 儲存貯體。不過，當帳戶 A 中的使用者存取時，該 RCP 不適用於帳戶 B 中的資源。
- RCP 會限制成員帳戶中資源的許可。帳戶中的任何資源都只有其上方每個父系允許的這些許可。如果許可在帳戶上方的任何層級遭到封鎖，受影響帳戶中的資源就沒有該許可，即使資源擁有者附加以資源為基礎的政策，允許任何使用者完整存取。
- RCPs適用於在操作請求中授權的資源。您可以在[服務授權參考](#)中動作資料表的「資源類型」欄中找到這些資源。如果在「資源類型」欄中指定資源，則會套用呼叫主體帳戶的 RCPs。例如，會s3:GetObject授權物件資源。每當提出GetObject請求時，就會套用適用的 RCP 來判斷請求委託人是否可以叫用 GetObject操作。適用的 RCP 是已連接到帳戶、組織單位 (OU) 或擁有所存取資源之組織的根目錄的 RCP。
- RCPs只會影響組織中成員帳戶中的資源。它們不會影響管理帳戶中的資源。這也表示 RCPs適用於指定為委派管理員的成員帳戶。如需詳細資訊，請參閱[管理帳戶的最佳實務](#)。
- 當委託人請求存取具有連接 RCP（具有適用 RCP 的資源）的帳戶內的資源時，RCP 會包含在政策評估邏輯中，以判斷委託人是否被允許或拒絕存取。
- RCPs會影響主體嘗試使用適用的 RCP 存取成員帳戶中資源的有效許可，無論主體是否屬於相同的組織。這包括根使用者。例外狀況是委託人是服務連結角色，因為 RCPs不適用於由服務連結角色進行的呼叫。服務連結角色 AWS 服務 可讓代表您執行必要的動作，且不受 RCPs限制。
- 使用者和角色仍然必須獲得具有適當 IAM 許可政策的許可，包括身分型和資源型政策。沒有任何 IAM 許可政策的使用者或角色無法存取，即使適用的 RCP 允許所有服務、所有動作和所有資源。

不受 RCPs 限制的資源和實體

您無法使用 RCPs來限制下列項目：

- 管理帳戶中資源的任何動作。

- RCPs不會影響任何服務連結角色的有效許可。服務連結角色是一種獨特的 IAM 角色類型，可直接連結至 AWS 服務，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。RCPs 無法限制服務連結角色的許可。RCP 也不會影響 AWS 服務擔任服務連結角色的能力；也就是說，服務連結角色的信任政策也不會受到 RCPs的影響。
- RCPs不適用於 [AWS 受管金鑰AWS Key Management Service](#)。AWS 受管金鑰 是由 代表您建立、管理和使用 AWS 服務。您無法變更或管理其許可。
- RCPs不會影響下列許可：

服務	API	RCPs未授權的資源
AWS Key Management Service	kms:RetireGrant	RCPs不會影響 kms:RetireGrant 許可。如需如何kms:RetireGrant 確定許可的詳細資訊，請參閱《AWS KMS 開發人員指南》中的 淘汰和撤銷授予 。

RCP 評估

Note

本節中的資訊不適用於管理政策類型，包括備份政策、標籤政策、聊天應用程式政策或 AI 服務選擇退出政策。如需詳細資訊，請參閱[理解管理政策繼承](#)。

由於您可以在 的不同層級連接多個資源控制政策 (RCPs) AWS Organizations，因此了解 RCPs的評估方式可協助您撰寫可產生正確結果RCPs。

使用 RCPs的策略

RCPFullAWSAccess 政策是 AWS 受管政策。當您啟用資源控制政策 (RCPs) 時，它會自動連接到組織根目錄、每個 OU，以及您組織中的每個帳戶。您無法分離此政策。此預設 RCP 允許所有委託人和動作存取通過 RCP 評估，這表示在您開始建立和連接 RCPs 之前，所有現有的 IAM 許可都會繼續如預期般運作。此 AWS 受管政策不會授予存取權。

您可以使用 Deny陳述式來封鎖對組織中資源的存取。若要針對特定帳戶中的資源拒絕許可，從根到帳戶（包括目標帳戶本身）直接路徑中每個 OU 的任何 RCP 都可以拒絕該許可。

Deny 陳述式是實作限制的強大方式，對於您組織的更廣泛部分應該是如此。例如，您可以連接政策，以協助防止組織外部的身份存取您的資源根層級，這對於組織中的所有帳戶都有效。AWS 強烈建議您不要在未徹底測試政策對您帳戶中資源的影響的情況下，將 RCPs 連接到組織的根目錄。如需詳細資訊，請參閱[測試 RCPs 的效果](#)。

在圖 1 中，有一個連接到生產 OU 的 RCP，該生產 OU 具有為指定服務指定的明確 Deny 陳述式。因此，帳戶 A 和帳戶 B 都會遭到拒絕存取該服務，因為系統會針對所有 OU 和成員帳戶評估連接至組織中任何層級的拒絕政策。

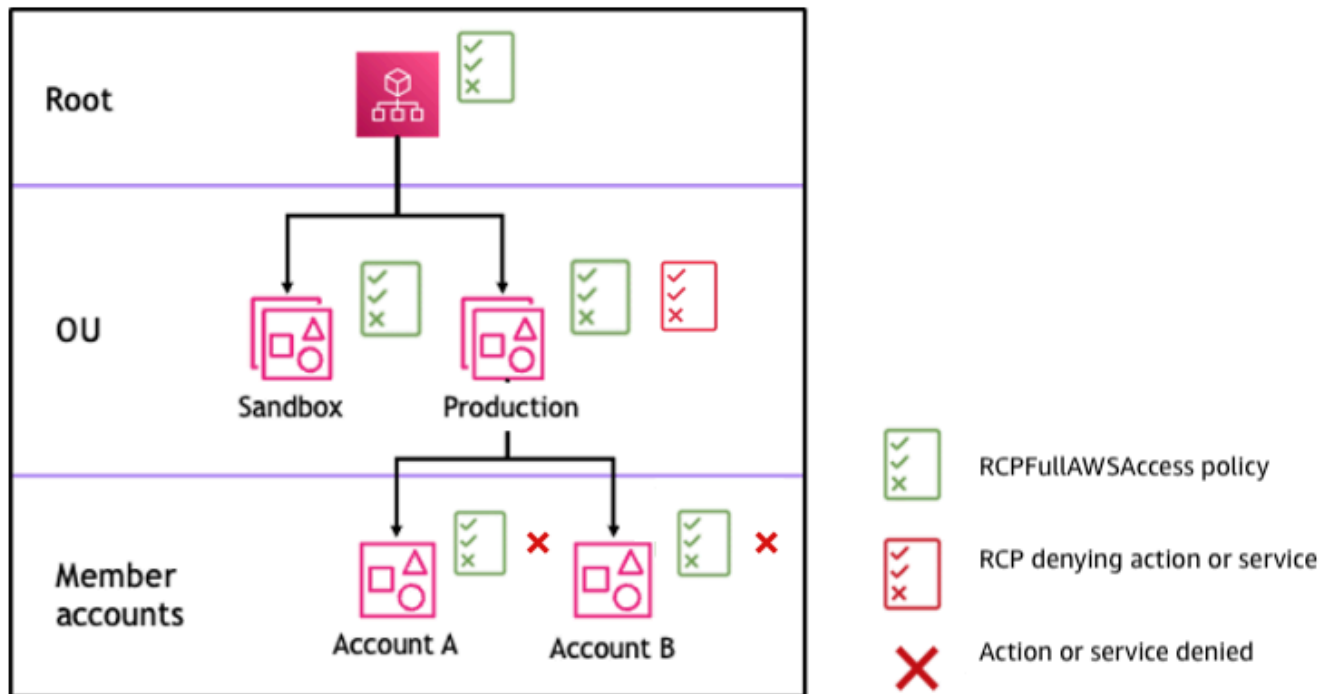


圖 1：在生產 OU 附加 Deny 陳述式的組織結構範例及其對帳戶 A 和帳戶 B 的影響

RCP 語法

資源控制政策 (RCPs) 使用的語法與以[資源為基礎的政策](#)類似。如需 IAM 政策及其語法的詳細資訊，請參閱 IAM 使用者指南中的 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html 指南中的 IAM 政策概觀。

RCP 是根據 [JSON](#) 規則所建構。本主題描述它使用的元素。

Note

RCP 中的所有字元都會計入其[大小上限](#)。本指南中的範例顯示以額外空格格式化的 RCPs，以改善其可讀性。不過，若您的政策大小接近大小上限，為了節省空間，您可以刪除引號外部的任何空格，例如空格字元和換行字元。

如需 RCPs 一般資訊，請參閱 [資源控制政策 RCPs](#)。

元素摘要

下表摘要說明您可以在 RCPs 中使用的政策元素。

Note

只有 **RCPFullAWSAccess** 政策 **Allow** 支援 的效果

只有 **RCPFullAWSAccess** 政策 **Allow** 支援 的效果。當您啟用資源控制政策 (RCPs) 時，此政策會自動連接到組織根目錄、每個 OU 以及組織中的每個帳戶。您無法分離此政策。此預設 RCP 允許所有委託人和動作存取通過 RCP 評估，這表示在您開始建立和連接 RCPs 之前，所有現有的 IAM 許可都會繼續如預期般運作。這不會授予存取權。

Element	用途
版本	指定用於處理政策的語言語法規則。
Statement	做為政策元素的容器。您可以在 RCPs 中擁有多個陳述式。
Statement ID (Sid)	(選用) 提供陳述式的易記名稱。
效果	定義 RCP 陳述式是否拒絕存取帳戶中的資源。

Element	用途	
Principal	指定允許或拒絕存取帳戶中資源的委託人。	
Action	指定 RCP 允許或拒絕 AWS 的服務和動作。	
Resource	指定 RCP 套用 AWS 的資源。	
NotResource	指定 RCP 豁免 AWS 的資源。使用此項目以取代 Resource 元素。	
Condition	指定決定陳述式生效時機的條件。	

主題

- [Version 元素](#)
- [Statement 元素](#)
- [Statement ID \(Sid\) 元素](#)
- [Effect 元素](#)
- [Principal 元素](#)
- [Action 元素](#)
- [Resource 和 NotResource 元素](#)
- [Condition 元素](#)
- [不支援的元素](#)

Version 元素

每個 RCP 必須包含值為 `Version` 元素 "2012-10-17"。這是與 IAM 許可政策的最新版本相同的版本值。

```
"Version": "2012-10-17",
```

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：版本](#)。

Statement 元素

RCP 包含一或多個 `Statement` 元素。您在政策中只能有一個 `Statement` 關鍵字，但其值可以是 JSON 陣列的陳述式 (加上 `[]` 字元)。

下列範例顯示由單一 `Effect`、`Action`、`Principal` 和 `Resource` 元素組成的單一陳述式。

```
{
  "Statement": {
    "Effect": "Deny",
    "Principal": "*",
    "Action": "*",
    "Resource": "*"
  }
}
```

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：陳述式](#)。

Statement ID (Sid) 元素

`Sid` 是一種您可以為政策陳述式提供的選用識別符。您可以將 `Sid` 值指派給陳述式陣列中的每個陳述式。下列範例 RCP 顯示範例 `Sid` 陳述式。

```
{
  "Statement": {
    "Sid": "DenyAllActions",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "*",
    "Resource": "*"
  }
}
```

如需詳細資訊，請參閱《[IAM 使用者指南](#)》中的 [IAM JSON 政策元素：Sid](#)。

Effect 元素

每個陳述式必須包含一個 Effect 元素。使用 Effect 元素 Deny 中的 值，您可以限制對特定資源的存取，或定義 RCPs 何時生效的條件。對於您建立 RCPs，值必須是 Deny。如需詳細資訊，請參閱《IAM 使用者指南》中的 [RCP 評估](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_effect.html) 和 IAM JSON 政策元素：效果。 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_effect.html

Principal 元素

每個陳述式必須包含 Principal 元素。您只能在 RCP 的 Principal 元素中指定「*」。使用 Conditions 元素來限制特定委託人。

如需詳細資訊，請參閱《[IAM 使用者指南](#)》中的 [IAM JSON 政策元素：主體](#)。

Action 元素

每個陳述式必須包含 Action 元素。

Action 元素的值是字串或字串清單 (JSON 陣列)，可識別陳述式允許或拒絕 AWS 的服務和動作。

每個字串都由服務（例如 "s3"、"sqs" 或 "sts"）的縮寫組成，所有小寫字母後面接著冒號，然後是該服務的動作。一般而言，它們都會以每個字輸入，開頭為大寫字母和小寫。例如："s3:ListAllMyBuckets"。

您也可以使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 作為萬用字元，以比對部分名稱相同的多個動作。值 "s3:*" 表示 Amazon S3 服務中的所有動作。此值僅 "sts:Get*" 比對以「取得」開頭 AWS STS 的動作。
- 使用問號 (?) 萬用字元來比對單一字元。

Note

萬用字元 (*) 和問號 (?) 可用於動作名稱中的任何位置
與 SCPs 不同，您可以在動作名稱的任何位置使用萬用字元，例如星號 (*) 或問號 (?)。

如需支援 RCPs 的服務清單，請參閱 [AWS 服務 支援 RCPs 清單](#)。如需 AWS 服務 支援的動作清單，請參閱 [AWS 《服務授權參考》中的 服務的動作、資源和條件金鑰](#)。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 原則元素：動作](#)。

Resource 和 NotResource 元素

每個陳述式必須包含 Resource 或 NotResource 元素。

您可以在資源元素中使用萬用字元，例如星號 (*) 或問號 (?)：

- 使用星號 (*) 做為萬用字元，以符合共用部分名稱的多個資源。
- 使用問號 (?) 萬用字元來比對單一字元。

如需詳細資訊，請參閱《[IAM 使用者指南](#)》中的 [IAM JSON 政策元素：資源](#) 和 [IAM JSON 政策元素：NotResource](#)。

Condition 元素

您可以在 RCP 的拒絕陳述式中指定 Condition 元素。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

此 RCP 拒絕存取 Amazon S3 操作和資源，除非請求是透過安全傳輸發生（請求是透過 TLS 傳送）。

如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)

不支援的元素

RCPs 不支援下列元素：

- NotPrincipal

- NotAction

資源控制政策範例

本主題中顯示的範例[資源控制政策 \(RCPs\)](#) 僅供參考。如需資料周邊範例，請參閱 GitHub 中的[資料周邊政策範例](#)。

使用這些範例之前

在組織中使用這些範例 RCPs 之前，請執行下列動作：

- 仔細檢閱和自訂 RCPs 以滿足您的唯一需求。
- 使用您使用 AWS 的服務，徹底測試您環境中的 RCPs。

本節中的範例政策示範 RCPs 的實作和使用。他們並非闡述為完全如圖所示實作的官方 AWS 建議或最佳實務。您有責任仔細測試任何政策是否適合解決您環境的業務需求。除非您將必要的例外狀況新增至政策，否則拒絕型資源控制政策可能會意外限制或封鎖您使用 AWS 服務。

一般範例

主題

- [RCPFullAWSAccess](#)
- [跨服務混淆代理人保護](#)
- [限制只能存取資源的 HTTPS 連線](#)
- [一致的 Amazon S3 儲存貯體政策控制](#)

RCPFullAWSAccess

當您啟用資源控制政策 (RCPs) 時，下列政策是 AWS 受管政策，會自動連接到組織根目錄、每個 OU 和組織中的每個帳戶。您無法分離此政策。此預設 RCP 允許所有主體和動作存取您的資源，這表示直到您開始建立和連接 RCPs 為止，您所有現有的 IAM 許可都會繼續如預期般運作。您不需要測試此政策的效果，因為它會允許現有授權行為繼續您的資源。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*"
}
```

跨服務混淆代理人保護

Some AWS 服務（呼叫服務）使用其 AWS 服務委託人從其他 AWS 服務（稱為服務）存取 AWS 資源。當無意存取 AWS 資源的演員嘗試使用 AWS 服務委託人的信任來與無意存取的資源互動時，稱為跨服務混淆代理人問題。如需詳細資訊，請參閱《IAM 使用者指南》中的[混淆代理人問題](#)

下列政策要求存取資源的 AWS 服務委託人僅代表組織的請求執行此操作。此政策只會將控制項套用至aws:SourceAccount已存在的請求，因此不需要使用的服務整合aws:SourceAccount不會受到影響。如果請求內容中存在aws:SourceAccount，則Null條件將評估為true，導致強制執行aws:SourceOrgID金鑰。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceConfusedDeputyProtection",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:*",
        "sqs:*",
        "kms:*",
        "secretsmanager:*",
        "sts:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceOrgID": "my-org-id",
          "aws:SourceAccount": [
            "third-party-account-a",
            "third-party-account-b"
          ]
        }
      }
    }
  ],
}
```

```

        "Bool": {
            "aws:PrincipalIsAWSService": "true"
        },
        "Null": {
            "aws:SourceArn": "false"
        }
    }
}
]
}

```

限制只能存取資源的 HTTPS 連線

下列政策要求只有透過 HTTPS (TLS) 的加密連線才能存取您的 資源。這可協助您防止潛在攻擊者操控網路流量。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceSecureTransport",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "sts:*",
        "s3:*",
        "sqs:*",
        "secretsmanager:*",
        "kms:*"
      ],
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}

```

一致的 Amazon S3 儲存貯體政策控制

下列 RCP 包含多個陳述式，可對組織中的 Amazon S3 儲存貯體強制執行一致的存取控制。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceS3TlsVersion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericLessThan": {
          "s3:TlsVersion": [
            "1.2"
          ]
        }
      }
    },
    {
      "Sid": "EnforceKMSEncryption",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
        }
      }
    }
  ]
}
```

- 陳述式 ID EnforceS3TlsVersion – 需要 1.2 的最低 TLS 版本，才能存取 S3 儲存貯體。
- 陳述式 ID EnforceKMSEncryption – 要求使用 KMS 金鑰加密物件的伺服器端。

中的管理政策 AWS Organizations

管理政策可讓您集中設定和管理 AWS 服務 及其功能。政策究竟如何影響繼承它們的 OU 和帳戶，取決於在 AWS Organizations 中套用的管理政策類型。檢閱本區段中的主題，以理解有關管理政策的相關術語和概念。

主題

- [的管理政策的先決條件和許可 AWS Organizations](#)
- [理解管理政策繼承](#)
- [檢視有效的管理政策](#)
- [宣告式政策](#)
- [備份政策](#)
- [標籤政策](#)
- [聊天應用程式政策](#)
- [AI 服務選擇退出政策](#)
- [Security Hub 政策](#)

的管理政策的先決條件和許可 AWS Organizations

此頁面說明 管理政策的先決條件和必要許可 AWS Organizations。

主題

- [管理政策的先決條件](#)
- [管理政策的許可](#)

管理政策的先決條件

為組織使用管理政策需要下列項目：

- 您的組織必須[啟用所有功能](#)。
- 您必須登入組織的管理帳戶，或是委派管理員。
- 您的 AWS Identity and Access Management (IAM) 使用者或角色必須具有下一節所列的許可。

管理政策的許可

下列範例 IAM 政策提供許可，以使用組織中管理政策的所有層面。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "OrganizationPolicies",
    "Effect": "Allow",
    "Action": [
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations>DeletePolicy",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DetachPolicy",
        "organizations:DisableAWSServiceAccess",
        "organizations:DisablePolicyType",
        "organizations:EnableAWSServiceAccess",
        "organizations:EnablePolicyType",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListCreateAccountStatus",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTargetsForPolicy",
        "organizations:UpdatePolicy"
    ],
    "Resource": "*"
}
]
}

```

如需有關 IAM 政策和許可的詳細資訊，請參閱 [IAM 使用者指南](#)。

理解管理政策繼承

Important

本節中的資訊不適用於授權政策：服務控制政策 (SCPs) 和資源控制政策 (RCPs)。如需 SCPs 和 RCPs 如何在 AWS Organizations 階層中運作的詳細資訊，請參閱 [SCP 評估](#) 和 [RCP 評估](#)。

您可以在組織中將這些管理政策連接至組織實體 (組織根、組織單位 (OU) 或帳戶)：

- 當您將管理政策連接至組織根時，組織中的所有 OU 和帳戶都會繼承該政策。
- 當您將管理政策連接至特定 OU 時，直屬於該 OU 或任何子 OU 的帳戶會繼承此政策。
- 當您將管理政策連接至特定帳戶時，它只會影響該帳戶。

因為您可以將管理政策連接至組織中的多個層級，所以帳戶可以繼承多個政策。

下列主題說明如何將父政策和子政策處理為帳戶的有效政策。

主題

- [繼承術語](#)
- [政策語法與管理政策類型的繼承](#)
- [繼承運算子](#)
- [繼承範例](#)

繼承術語

本主題在討論管理政策繼承時會使用下列術語。

政策繼承

組織不同層級的政策互動，從組織的頂層根下移至組織單位 (OU) 階層，再到個別帳戶。

您可以將政策連接至組織根、OU、個別帳戶，以及這些組織實體的任何組合。政策繼承是指連接至組織根或 OU 的管理政策。在連接管理政策的組織根目錄或 OU 中，所有成員帳戶都繼承該政策。

例如，當管理政策連接至組織根時，組織中的所有帳戶都會繼承該政策。這是因為組織中的所有帳戶永遠都在組織根下。當您將標籤政策連接至特定 OU 時，直屬於該 OU 或任何子 OU 的帳戶會繼承該政策。因為您可以將政策連接至組織中的多個層級，所以帳戶可能會繼承單一政策類型的多個政策文件。

父政策

在組織樹狀結構中較上方連接的政策，高於樹狀結構中連接至較低實體的政策。

例如，如果您將管理政策 A 連接至組織根，就只是政策而已。如果您也將政策 B 連接至該根下的 OU，而政策 A 是政策 B 的父政策。政策 B 是政策 A 的子政策。政策 A 和政策 B 合併，為 OU 中的帳戶建立有效的標籤政策。

子政策

在組織樹狀結構中比父政策更低的層級上連接的政策。

有效政策

指定規則以套用至帳戶的最終單一政策文件。帳戶繼承的任何政策，加上直接連接至帳戶的任何政策，聚集而成有效政策。如需詳細資訊，請參閱[檢視有效的管理政策](#)。

繼承運算子

控制繼承的政策如何合併成為單一有效政策的運算子。這些運算子視為進階功能。經驗豐富的政策作者可以使用這些運算子，限制子政策可以進行哪些變更和政策中的設定如何合併。如需詳細資訊，請參閱[繼承運算子](#)。

政策語法與管理政策類型的繼承

政策究竟如何影響繼承它們的 OU 和帳戶，取決於所選管理政策的類型。管理政策類型包括：

- [宣告式政策](#)
- [備份政策](#)
- [標籤政策](#)
- [聊天應用程式政策](#)
- [AI 服務選擇退出政策](#)

管理政策類型的語法包含[繼承運算子](#)，可讓您精細地指定要套用父政策中的哪些元素，以及哪些元素在被子 OU 和帳戶繼承時可以被覆寫或修改。

有效政策是從組織根和 OU 繼承的一組規則，以及直接連接到帳戶的規則。有效政策會指定套用至帳戶的最終規則集。您可以檢視帳戶的有效政策，其中包含所套用政策中所有繼承運算子的效果。如需詳細資訊，請參閱[檢視有效的管理政策](#)。

繼承運算子

繼承運算子可控制繼承的政策和帳戶政策如何合併成為帳戶的有效政策。這些運算子包括值-設定運算子和子控制運算子。

當您在 AWS Organizations 主控台中使用視覺化編輯器時，您只能使用 @assign 運算子。其他運算子視為進階功能。若要使用其他運算子，您必須手動撰寫 JSON 政策。經驗豐富的政策作者可以使用繼承運算子，控制哪些值套用至有效的政策，並限制子政策可以進行哪些變更。

如需政策繼承如何在組織中運作的詳細資訊，請參閱 [繼承範例](#)。

值-設定運算子

您可以使用下列值-設定運算子來控制政策與其父政策的互動方式。

- `@assign` – 使用指定的設定覆寫任何繼承的政策設定。如果未繼承指定的設定，此運算子會將其新增至有效政策。此運算子可套用至任何類型的任何政策設定。
 - 對於單值設定，此運算子會以指定的值取代繼承的值。
 - 對於多值設定 (JSON 陣列)，此運算子會移除任何繼承的值，並取代為此政策指定的值。
- `@append` – 將指定的設定 (不刪除任何項目) 新增至繼承的設定。如果未繼承指定的設定，此運算子會將其新增至有效政策。此運算子只能與多值設定一起使用。
 - 此運算子會將指定的值新增至繼承陣列中的任何值。
- `@remove` – 從有效政策中移除指定的繼承設定 (如果存在)。此運算子只能與多值設定一起使用。
 - 此運算子會從繼承自父政策的值陣列中，只移除指定的值。其他值可以繼續存在於陣列中，而且可以由子政策繼承。

子控制運算子

可自行決定是否使用子控制運算子。您可以使用 `@operators_allowed_for_child_policies` 運算子來控制子政策可以使用哪些值-設定運算子。您可以允許所有運算子、某些特定運算子或不允許運算子。根據預設，允許所有運算子 (`@all`)。

- `"@operators_allowed_for_child_policies":["@all"]` – 子 OU 和帳戶可以在政策中使用任何運算子。根據預設，子政策中允許所有運算子。
- `"@operators_allowed_for_child_policies":["@assign", "@append", "@remove"]` – 子 OU 和帳戶在子政策中只能使用指定的運算子。您可以在此子控制運算子中指定一或多個值-設定運算子。
- `"@operators_allowed_for_child_policies":["@none"]` – 子 OU 和帳戶在政策中無法使用運算子。您可以使用此運算子，有效封鎖父政策中定義的值，讓子政策無法新增、附加或移除這些值。

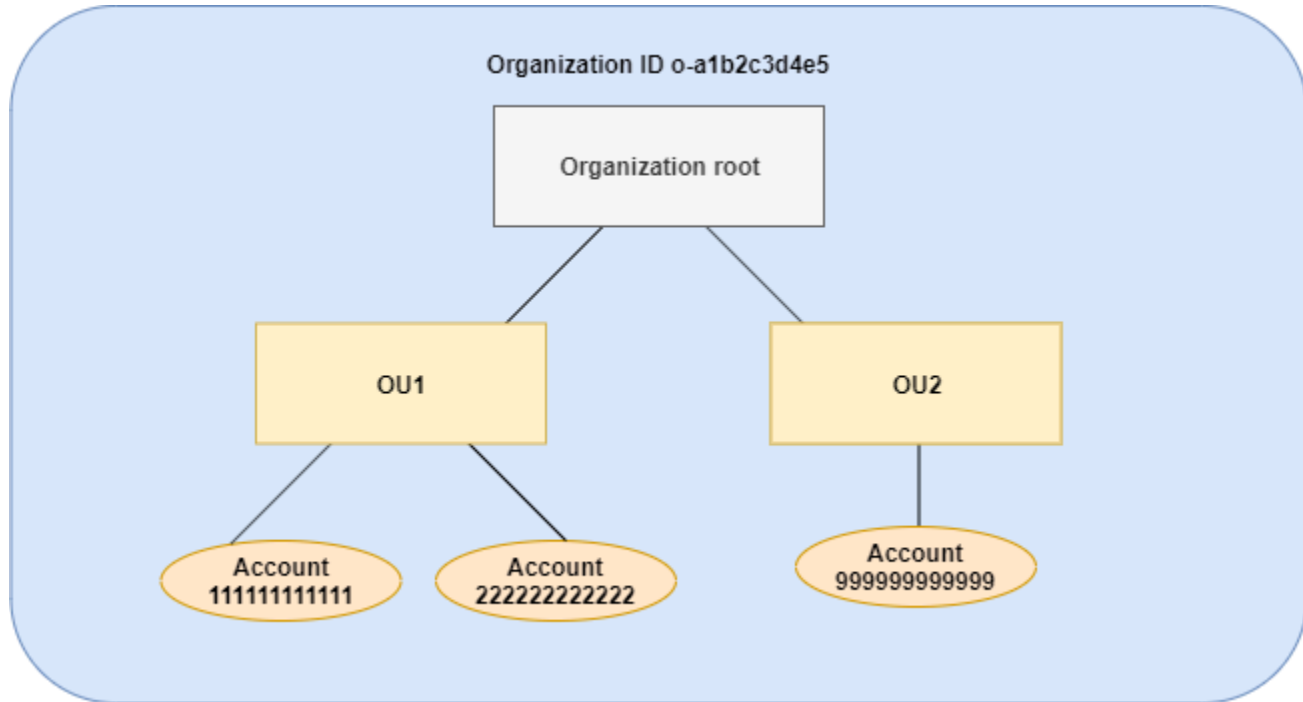
Note

如果繼承的子控制運算子禁止使用某個運算子，則您無法在子政策中反轉該規則。如果您將子控制運算子包含在父政策中，則會限制所有子政策中的值-設定運算子。

繼承範例

這些範例顯示父標籤和子標籤政策如何合併成為帳戶的有效標籤政策，以示範政策繼承的運作方式。

這些範例假設您有如下圖所示的組織結構。



範例

- [範例 1：允許子政策只覆寫標籤值](#)
- [範例 2：將新值附加到繼承的標籤](#)
- [範例 3：從繼承的標籤中移除值](#)
- [範例 4：限制對子政策的變更](#)
- [範例 5：與子控制運算子衝突](#)
- [範例 6：與相同階層層級上附加的值衝突](#)

範例 1：允許子政策只覆寫標籤值

下列標籤政策定義 CostCenter 標籤鍵和兩個可接受的值 (Development 和 Support)。如果您將此政策連接至組織根，則會對組織中的所有帳戶產生效果。

政策 A – 組織根標籤政策

```
{
```

```

    "tags": {
      "costcenter": {
        "tag_key": {
          "@@assign": "CostCenter"
        },
        "tag_value": {
          "@@assign": [
            "Development",
            "Support"
          ]
        }
      }
    }
  }
}

```

假設您希望 OU1 中的使用者對某個索引鍵使用不同的標籤值，而且想要針對特定的資源類型強制執行標籤政策。因為政策 A 未指定允許哪些子控制運算子，所以允許所有運算子。您可以使用 @@assign 運算子，並建立如下的標籤政策以連接至 OU1。

政策 B – OU1 標籤政策

```

{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "Sandbox"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "redshift:*",
          "dynamodb:table"
        ]
      }
    }
  }
}

```

當政策 A 和政策 B 合併以形成帳戶的有效標籤政策時，為標籤指定 @@assign 運算子會執行以下操作：

- 政策 B 覆寫父政策 (政策 A) 中指定的兩個標籤值。結果是 Sandbox 是 CostCenter 標籤鍵的唯一合規值。
- 新增的 enforced_for 指定在所有 Amazon Redshift 資源和 Amazon DynamoDB 資料表上，CostCenter 標籤必須使用指定的標籤值。

如圖所示，OU1 包含兩個帳戶：111111111111 和 222222222222。

帳戶 111111111111 和 222222222222 所產生的有效標籤政策

Note

您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
  "tags": {
    "costcenter": {
      "tag_key": "CostCenter",
      "tag_value": [
        "Sandbox"
      ],
      "enforced_for": [
        "redshift:*",
        "dynamodb:table"
      ]
    }
  }
}
```

範例 2：將新值附加到繼承的標籤

在某些情況下，您希望組織中的所有帳戶以簡短的可接受值清單來指定標籤鍵。對於一個 OU 中的帳戶，在建立資源時，您可能想要允許只有這些帳戶才可以指定的額外值。此範例指出如何利用 @@append 運算子來這樣做。@@append 運算子是進階功能。

與範例 1 一樣，此範例一開始也以政策 A 當作組織根標籤政策。

政策 A – 組織根標籤政策

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "Development",
          "Support"
        ]
      }
    }
  }
}
```

在此範例中，將政策 C 連接至 OU2。此範例的差異在於，在政策 C 中使用 @@append 運算子會新增至 (而非覆寫) 可接受的值清單和 enforced_for 規則。

政策 C – OU2 標籤政策，用於附加值

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@append": [
          "Marketing"
        ]
      },
      "enforced_for": {
        "@@append": [
          "redshift:*",
          "dynamodb:table"
        ]
      }
    }
  }
}
```

```
}
```

當政策 A 和政策 C 合併形成帳戶的有效標籤政策時，將政策 C 連接至 OU2 會產生下列效果：

- 因為政策 C 包含 `@append` 運算子，所以允許新增至 (而非覆寫) 政策 A 中指定的可接受標籤值清單。
- 與政策 B 一樣，新增的 `enforced_for` 指定在所有 Amazon Redshift 資源和 Amazon DynamoDB 資料表上，`CostCenter` 標籤必須做為指定的標籤值。如果父政策不含子控制運算子來限制子政策可指定的內容，則覆寫 (`@assign`) 和新增 (`@append`) 有相同的效果。

如圖所示，OU2 包含一個帳戶：999999999999。政策 A 和政策 C 合併，為帳戶 999999999999 建立有效的標籤政策。

帳戶 999999999999 的有效標籤政策

Note

您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
  "tags": {
    "costcenter": {
      "tag_key": "CostCenter",
      "tag_value": [
        "Development",
        "Support",
        "Marketing"
      ],
      "enforced_for": [
        "redshift:*",
        "dynamodb:table"
      ]
    }
  }
}
```

範例 3：從繼承的標籤中移除值

在某些情況下，連接至組織的標籤政策所定義的標籤值，可能超過您希望帳戶使用的數量。此範例說明如何使用 `@@remove` 運算子修訂標籤政策。`@@remove` 是進階功能。

與其他範例一樣，此範例一開始也以政策 A 當作組織根標籤政策。

政策 A – 組織根標籤政策

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "Development",
          "Support"
        ]
      }
    }
  }
}
```

在此範例中，將政策 C 連接至帳戶 999999999999。

政策 D – 帳戶 999999999999 標籤政策，用於移除值

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@remove": [
          "Development",
          "Marketing"
        ],
        "enforced_for": {
          "@@remove": [
            "redshift:*",
            "dynamodb:table"
          ]
        }
      }
    }
  }
}
```

```
]
}
}
}
```

當政策 A、政策 C 和政策 D 合併形成有效的標籤政策時，將政策 D 連接至帳戶 999999999999 會產生下列效果：

- 假設您已執行所有先前的範例，則政策 B、C 和 C 是 A 的子政策。政策 B 只連接至 OU1，因此不影響帳戶 99999999999999。
- 對於帳戶 99999999999999，CostCenter 標籤鍵唯一可接受的值是 Support。
- 不強制 CostCenter 標籤鍵合規。

帳戶 999999999999 新的有效標籤政策

 Note

您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
  "tags": {
    "costcenter": {
      "tag_key": "CostCenter",
      "tag_value": [
        "Support"
      ]
    }
  }
}
```

如果您稍後將更多帳戶新增至 OU2，其有效的標籤政策將與帳戶 999999999999 有所不同。這是因為更嚴格的政策 D 只在帳戶層級連接，而不是連接至 OU。

範例 4：限制對子政策的變更

在某些情況下，您可能想要限制子政策中的變更。此範例說明如何利用子控制運算子來這樣做。

此範例從新的組織根標籤政策開始，並假設標籤政策尚未連接至組織實體。

政策 E – 組織根標籤政策，用於限制子政策中的變更

```
{
  "tags": {
    "project": {
      "tag_key": {
        "@operators_allowed_for_child_policies": ["@none"],
        "@assign": "Project"
      },
      "tag_value": {
        "@operators_allowed_for_child_policies": ["@append"],
        "@assign": [
          "Maintenance",
          "Escalations"
        ]
      }
    }
  }
}
```

當您將政策 E 連接至組織根時，政策即可防止子政策變更 Project 標籤鍵。不過，子政策可以覆寫或附加標籤值。

假設您接著將下列政策 F 連接至 OU。

政策 F – OU 標記政策

```
{
  "tags": {
    "project": {
      "tag_key": {
        "@assign": "PROJECT"
      },
      "tag_value": {
        "@append": [
          "Escalations - research"
        ]
      }
    }
  }
}
```

合併政策 E 和政策 F 會對 OU 的帳戶產生下列效果：

- 政策 F 是政策 E 的子政策。
- 政策 F 試圖變更大小寫處理，但無法這樣做。這是因為政策 E 在標籤鍵中包含 `"@operators_allowed_for_child_policies": ["@none"]` 運算子。
- 不過，政策 F 可以為索引鍵附加標籤值。這是因為政策 E 在標籤值中包含 `"@operators_allowed_for_child_policies": ["@append"]`。

OU 中帳戶的有效政策

Note

您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```
{
  "tags": {
    "project": {
      "tag_key": "Project",
      "tag_value": [
        "Maintenance",
        "Escalations",
        "Escalations - research"
      ]
    }
  }
}
```

範例 5：與子控制運算子衝突

子控制運算子可以存在於組織階層中相同層級上連接的標籤政策中。在此情況下，政策合併形成帳戶的有效政策時會使用允許運算子的交集。

假設政策 G 和政策 H 連接至組織根。

政策 G – 組織根標籤政策 1

```
{
  "tags": {
```

```

    "project": {
      "tag_value": {
        "@operators_allowed_for_child_policies": ["@append"],
        "@assign": [
          "Maintenance"
        ]
      }
    }
  }
}

```

政策 H – 組織根標籤政策 2

```

{
  "tags": {
    "project": {
      "tag_value": {
        "@operators_allowed_for_child_policies": ["@append", "@remove"]
      }
    }
  }
}

```

在此範例中，組織根上的一個政策定義只能附加標籤鍵的值。連接至組織根的其他政策允許子政策附加和移除值。這兩個許可的交集用於子政策。結果是子政策可以附加值，但不能移除值。因此，子政策可以將值附加至標籤值清單，但無法移除 Maintenance 值。

範例 6：與相同階層層級上附加的值衝突

您可以將多個標籤政策連接至每個組織實體。當您這麼做時，連接至相同組織實體的標籤政策可能包含衝突的資訊。這些政策是根據連接至組織實體時的順序來評估。若要變更先評估哪個政策，您可以分離政策，再重新連接。

假設政策 J 最先連接至組織根，然後政策 K 才連接至組織根。

政策 J – 連接至組織根的第一個標籤政策

```

{
  "tags": {
    "project": {
      "tag_key": {
        "@assign": "PROJECT"
      }
    }
  }
}

```

```

        },
        "tag_value": {
            "@append": ["Maintenance"]
        }
    }
}
}

```

政策 K – 連接至組織根的第二個標籤政策

```

{
  "tags": {
    "project": {
      "tag_key": {
        "@assign": "project"
      }
    }
  }
}

```

在此範例中，有效的標籤政策中會使用標籤鍵 PROJECT，因為定義此標籤鍵的政策最先連接至組織根。

政策 JK – 帳戶的有效標籤政策

帳戶的有效政策如下。

Note

您無法直接使用顯示的有效政策的內容作為新政策的內容。語法不包括控制與其他子政策和父政策合併所需的運算子。顯示有效政策僅用於了解合併的結果。

```

{
  "tags": {
    "project": {
      "tag_key": "PROJECT",
      "tag_value": [
        "Maintenance"
      ]
    }
  }
}

```

```
}  
}
```

檢視有效的管理政策

決定組織中帳戶的有效管理政策。

什麼是有效的管理政策？

有效政策會指定適用於 AWS 帳戶 管理政策類型的最終規則。這是帳戶繼承的管理政策彙總，加上直接連接到帳戶之該管理政策類型的任何政策。當您將管理政策連接到組織的根目錄時，它適用於組織中的所有帳戶。當您將管理政策連接到組織單位 (OU) 時，它適用於屬於 OUs 的所有帳戶和 OU。當您直接將管理政策連接到帳戶時，它僅適用於該帳戶 AWS 帳戶。

如需有關如何將 AI 服務選擇退出政策合併成最終有效政策的資訊，請參閱[理解管理政策繼承](#)。

備份政策範例

連接至組織根目錄的備份政策可能會指定組織中的所有帳戶，以每週一次的預設備份頻率備份所有 Amazon DynamoDB 資料表。如果個別備份政策直接連接至一個成員帳戶，且在資料表中有重要資訊，則可以覆寫為每天一次的頻率值。這些備份政策的組合包含有效的備份政策。此有效備份政策針對組織中的每個帳戶而個別決定。在此範例中，結果是組織中的所有帳戶每週備份一次 DynamoDB 資料表，例外的是有一個帳戶每天都備份資料表。

標籤政策範例

連接到組織根目錄的標籤政策可能會定義具有四個合規值的 CostCenter 標籤。連接至帳戶的另一個標籤政策，可能限制 CostCenter 索引鍵只能有四個合規值之中的兩個。這些標籤政策的組合構成有效的標籤政策。結果是組織根標籤政策中定義的四個合規標籤值之中，只有兩個是帳戶的合規值。

聊天應用程式政策範例

聊天應用程式中的 Amazon Q Developer 會根據有效的聊天應用程式政策，重新評估聊天應用程式中組態中先前建立的任何 Amazon Q Developer，並在符合有效政策中允許的設定和護欄時拒絕任何先前允許的動作。成員帳戶的有效政策會定義允許的設定和護欄。例如，如果將拒絕公開 Slack 頻道存取的聊天應用程式政策套用至成員帳戶，則成員帳戶中公開 Slack 頻道聊天應用程式組態中的現有 Amazon Q Developer 將被停用。聊天應用程式中的 Amazon Q Developer 不會傳送通知，且頻道成員將無法在封鎖的頻道中執行任何任務。聊天應用程式主控台 Amazon Q Developer 會將受影響的頻道標記為已停用，並在旁邊加上適當的錯誤訊息。

AI 服務選擇退出範例

連接到組織根目錄的 AI 服務選擇退出政策可能會指定組織中的所有帳戶選擇退出所有 AWS 機器學習服務使用內容。直接連接至一個成員帳戶的單獨 AI 服務選擇退出政策，會指定其選擇加入僅針對 Amazon Rekognition 使用的內容。這些 AI 服務選擇退出政策的組合包括有效的 AI 服務選擇退出政策。結果是組織中的所有帳戶都選擇退出所有帳戶 AWS 服務，但選擇加入 Amazon Rekognition 的一個帳戶除外。

如何檢視有效的管理政策

您可以從 [AWS Organizations 主控台](#)、AWS Management Console AWS API 或 檢視帳戶管理政策類型的有效政策 AWS Command Line Interface。

最低許可

若要檢視帳戶管理政策類型的有效政策，您必須具有執行下列動作的許可：

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

檢視帳戶管理政策類型的有效政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在頁面上 [AWS 帳戶](#)，選擇您要檢視有效政策的帳戶名稱。您可能需要展開 OU (選擇 )，以尋找您想要的帳戶。
3. 在政策索引標籤上，選擇您要檢視有效政策的管理政策類型。
4. 選擇檢視有效政策 AWS 帳戶。

主控台會顯示套用至指定帳戶的有效政策。

Note

如果沒有重大變更，則您無法複製和貼上有效的政策，並將其用作另一個政策的 JSON。政策文件必須包含 [繼承運算子](#)，指定每個設定合併到最終有效政策的方式。

AWS CLI & AWS SDKs

檢視帳戶管理政策類型的有效政策

您可以使用下列其中一項來檢視有效政策：

- AWS CLI: [describe-effective-policy](#)

下列範例顯示帳戶的有效 AI 服務選擇退出政策。

```
$ aws organizations describe-effective-policy \
  --policy-type AISERVICES_OPT_OUT_POLICY \
  --target-id 123456789012
{
  "EffectivePolicy": {
    "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":\n\"optOut\"}, ....TRUNCATED FOR BREVITY.... \"opt_out_policy\":{\"optIn\"}}}\",
    \"LastUpdatedTimestamp\": \"2020-12-09T12:58:53.548000-08:00\",
    \"TargetId\": \"123456789012\",
    \"PolicyType\": \"AISERVICES_OPT_OUT_POLICY\"
  }
}
```

- AWS SDKs : [DescribeEffectivePolicy](#)

宣告式政策

宣告政策可讓您集中宣告和強制執行整個組織中指定 AWS 服務 之 所需的組態。連接後，當服務新增新功能或 APIs 時，一律會維護組態。使用宣告式政策來防止不合規的動作。例如，您可以封鎖整個組織的 Amazon VPC 資源的公有網際網路存取。

使用宣告政策的主要優點如下：

- 易用性：您可以使用 AWS Organizations 和 AWS Control Tower 主控台 中的 AWS 服務 幾個選項，或使用 AWS CLI & AWS SDKs 的幾個命令，強制執行 的基準組態。
- 設定一次並忘記：即使服務引入新功能或 APIs，AWS 服務 的基準組態也會一律維持。將新帳戶新增至組織或建立新主體和資源時，也會維護基準組態。
- 透明度：帳戶狀態報告可讓您檢閱範圍內帳戶宣告政策支援的所有屬性的目前狀態。您也可以建立可自訂的錯誤訊息，這可協助管理員將最終使用者重新導向至內部 wiki 頁面，或提供描述性訊息，以協助最終使用者了解動作失敗的原因。

如需支援 AWS 服務 和 屬性的完整清單，請參閱 [支援的 AWS 服務 和 屬性](#)。

主題

- [宣告政策的運作方式](#)
- [宣告政策的自訂錯誤訊息](#)
- [宣告政策的帳戶狀態報告](#)
- [支援的 AWS 服務 和 屬性](#)
- [宣告式政策入門](#)
- [使用宣告式政策的最佳實務](#)
- [產生宣告政策的帳戶狀態報告](#)
- [宣告性政策語法和範例](#)

宣告政策的運作方式

在服務的控制平面中強制執行宣告政策，這是與[授權政策的重要區別](#)，例如[服務控制政策 \(SCPs\)](#) 和 [資源控制政策 \(RCPs\)](#)。雖然授權政策會規範對 APIs 存取，但宣告政策會直接在服務層級套用，以強制執行持久的意圖。這可確保始終強制執行基準組態，即使服務引入了新功能或 APIs。

下表有助於說明此區別，並提供一些使用案例。

	服務控制政策	資源控制政策	宣告式政策		
為什麼？	集中大規模定義和強制執行主體（例如 IAM 使用者和 IAM 角色）的一致存取控制。	集中定義和強制執行大規模資源的一致存取控制	集中定義和強制執行大規模 AWS 服務的基準組態。		
如何？	透過在 API 層級控制主體的可用存取許可上限。	透過控制 API 層級之資源的可用存取許可上限。	透過強制執行的所需組態，AWS 服務 而不使用 API 動作。		

	服務控制政策	資源控制政策	宣告式政策		
管理服務連結角色？	否	否	是		
回饋機制	不可自訂的存取遭拒 SCP 錯誤。	不可自訂的存取遭拒 RCP 錯誤。	可自訂的錯誤訊息。如需詳細資訊，請參閱 宣告政策的自訂錯誤訊息 。		
範例 政策	AWS 根據請求拒絕對的存取 AWS 區域	限制只能存取資源的 HTTPS 連線	允許的影像設定		

在您[建立](#)並[連接](#)宣告政策之後，它會在您的組織中套用和強制執行。宣告政策可以套用至整個組織、組織單位 (OUs) 或帳戶。加入組織的帳戶會自動繼承組織中的宣告政策。如需詳細資訊，請參閱[理解管理政策繼承](#)。

有效政策是從組織根和 OU 繼承的一組規則，以及直接連接到帳戶的規則。有效政策會指定套用至帳戶的最終規則集。如需詳細資訊，請參閱[檢視有效的管理政策](#)。

如果已[分離](#)宣告政策，則屬性狀態會在連接宣告政策之前回復為先前的狀態。

宣告政策的自訂錯誤訊息

宣告式政策可讓您建立自訂錯誤訊息。例如，如果 API 操作因為宣告性政策而失敗，您可以設定錯誤訊息或提供自訂 URL，例如內部 wiki 的連結或描述失敗的訊息連結。如果您未指定自訂錯誤訊息，AWS Organizations 會提供下列預設錯誤訊息：Example: This action is denied due to an organizational policy in effect。

您也可以稽核建立宣告政策、更新宣告政策，以及使用刪除宣告政策的程序 AWS CloudTrail。CloudTrail 可能會因為宣告性政策而標記 API 操作失敗。如需詳細資訊，請參閱[記錄和監控](#)。

⚠ Important

請勿在自訂錯誤訊息中包含個人身分識別資訊 (PII) 或其他敏感資訊。PII 包含一般資訊，可用於識別或尋找個人。它涵蓋財務、醫療、教育或僱用等記錄。PII 範例包括地址、銀行帳戶號碼和電話號碼。

宣告政策的帳戶狀態報告

帳戶狀態報告可讓您檢閱範圍內帳戶宣告政策支援的所有屬性的目前狀態。您可以選擇要包含在報告範圍中的帳戶和組織單位 (OUs)，或選取根來選擇整個組織。

此報告透過提供區域明細，以及屬性的目前狀態跨帳戶（透過）是否一致或不一致（透過），來協助您評估整備程度 `numberOfUnmatchedAccounts`。 `numberOfMatchedAccounts` 您也可以查看最常見的值，這是 屬性最常觀察到的組態值。

在圖 1 中，有產生的帳戶狀態報告，顯示下列屬性的跨帳戶一致性：VPC 封鎖公開存取和映像封鎖公開存取。這表示，對於每個屬性，範圍內的所有帳戶都有該屬性的相同組態。

產生的帳戶狀態報告會顯示下列屬性的不一致帳戶：允許的映像設定、執行個體中繼資料預設值、序列主控台存取和快照封鎖公開存取。在此範例中，帳戶不一致的每個屬性都是因為有一個帳戶具有不同的組態值。

如果有最常見的值，則會顯示在其個別欄中。如需每個屬性控制項的詳細資訊，請參閱[宣告式政策語法和範例政策](#)。

您也可以展開屬性以查看區域明細。在此範例中，映像區塊公開存取已擴展，而且在每個區域中，您可以看到帳戶之間也有一致性。

附加宣告政策以強制執行基準組態的選擇取決於您的特定使用案例。使用帳戶狀態報告，協助您在連接宣告政策之前評估準備程度。

如需詳細資訊，請參閱[產生帳戶狀態報告](#)。

Account status report				
		Updated last Monday at 12:40 PM		Generate status report View report in S3
Attribute	Region	Uniform across accounts	Inconsistent accounts	Most frequent value
▶ Allowed Images Settings	All Regions	⚠ No	1	
▶ Instance Metadata Defaults	All Regions	⚠ No	1	{"HttpTokens":"requi
▶ Serial Console Access	All Regions	⚠ No	1	false
▶ VPC Block Public Access	All Regions	✅ Yes	0	{"State":"default-sta
▶ Snapshot Block Public Access	All Regions	⚠ No	1	unblocked
▼ Image Block Public Access	All Regions	✅ Yes	0	block-new-sharing
	eu-west-3	✅ Yes	0	
	eu-north-1	✅ Yes	0	

圖 1：VPC Block Public Access 和 Image Block Public Access 帳戶間的統一帳戶狀態報告範例。

支援的 AWS 服務 和 屬性

EC2 宣告政策支援的屬性

下表顯示 Amazon EC2 相關服務支援的屬性。

EC2 的宣告政策

AWS 服務	屬性	政策效果	政策內容	其他資訊
Amazon VPC	VPC 封鎖公開存取	控制 Amazon VPCs 和子網路中的資源是否可以透過網際網路閘道 (IGWs) 連線到網際網路。	檢視政策	如需詳細資訊，請參閱《Amazon VPCs 使用者指南》中的封鎖對 VPC 和子網路的公開存取。
Amazon EC2	序列主控台存取	控制 EC2 序列主控台是否可存取。	檢視政策	如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指

AWS 服務	屬性	政策效果	政策內容	其他資訊
				南》中的 設定 EC2 序列主控台的存取權 。
	映像區塊公開存取	控制 Amazon Machine Image (AMIs) 是否可公開共用。	檢視政策	如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 了解 AMIs 的封鎖公開存取 。
	允許的影像設定	使用允許的 AMI 控制 Amazon EC2 中 Amazon Machine Image (AMIs) 探索和使用的。	檢視政策	如需詳細資訊，請參閱《 Amazon Elastic Compute Cloud 使用者指南 》中的 Amazon Machine Image (AMIs) 。
	執行個體中繼資料預設值	控制所有新 EC2 執行個體啟動的 IMDS 預設值。	檢視政策	如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 設定新執行個體的執行個體中繼資料選項 。

AWS 服務	屬性	政策效果	政策內容	其他資訊
Amazon EBS	快照區塊公開存取	控制 Amazon EBS 快照是否可公開存取。	檢視政策	如需詳細資訊，請參閱《 Amazon Elastic Block Store 使用者指南 》中的 封鎖 Amazon EBS 快照的公開存取 。

宣告式政策入門

請依照下列步驟開始使用宣告式政策。

1. [了解您必須執行宣告性政策任務的許可](#)。
2. [為您的組織啟用宣告政策](#)。

Note

需要啟用信任存取

您必須為宣告政策將強制執行基準組態的服務啟用受信任存取。這會建立唯讀服務連結角色，用於產生您組織中帳戶現有組態的帳戶狀態報告。

使用主控台

如果您使用 Organizations 主控台，此步驟是啟用宣告政策程序的一部分。

使用 AWS CLI

如果您使用 AWS CLI，則有兩個不同的 APIs：

- [EnablePolicyType](#)，您用來啟用宣告政策。
- [EnableAWSServiceAccess](#)，您用來啟用受信任存取。

如需如何使用 啟用特定服務的受信任存取的詳細資訊 AWS CLI，[AWS 服務 請參閱 與 搭配使用 AWS Organizations](#)。

3. [執行帳戶狀態報告](#)。
4. [建立宣告政策](#)。
5. [將宣告政策連接至組織的根、OU 或帳戶](#)。
6. [檢視套用至 帳戶的合併有效宣告政策](#)。

對於所有這些步驟，請以 IAM 使用者身分登入、擔任 IAM 角色，或以組織管理帳戶中的根使用者身分登入 ([不建議](#))。

其他資訊

- [了解宣告政策語法並查看範例政策](#)

使用宣告式政策的最佳實務

AWS 建議使用宣告式政策的下列最佳實務。

利用整備度評估

使用宣告政策帳戶狀態報告，評估範圍內帳戶宣告政策支援的所有屬性的目前狀態。您可以選擇要包含在報告範圍中的帳戶和組織單位 (OUs)，或選取根來選擇整個組織。

此報告透過提供區域明細，以及屬性的目前狀態跨帳戶 (透過) 是否一致或不一致 (透過)，來協助您評估整備程度 `numberOfUnmatchedAccounts`。 `numberOfMatchedAccounts` 您也可以查看最常見的值，這是 屬性最常觀察到的組態值。

附加宣告政策以強制執行基準組態的選擇取決於您的特定使用案例。

如需詳細資訊和說明範例，請參閱 [宣告政策的帳戶狀態報告](#)。

從小開始，然後擴展

若要簡化偵錯，請從測試政策開始。每次變更後，請先驗證變更的行為和影響，再繼續變更。此方法可減少發生錯誤或意外結果時，您必須考量的變數數量。

例如，您可以從連接到非關鍵測試環境中單一帳戶的測試政策開始。確認其適用於您的規格後，您可以逐步將政策向上移動到更多帳戶和更多組織單位 OUs)。

建立審核程序

實作程序來監控新的宣告屬性、評估政策例外狀況，並進行調整，以維持與您的組織安全和營運需求的一致性。

使用 驗證變更 `DescribeEffectivePolicy`

對宣告性政策進行變更後，請檢查您進行變更之層級下代表帳戶的有效政策。您可以使用 [，或使用 `DescribeEffectivePolicy` API 操作或其中一個 或 SDK 變體來檢視有效政策 AWS Management Console](#)。 [DescribeEffectivePolicy](#) AWS CLI AWS 請確定您所做的變更對有效政策產生預期的影響。

通訊和訓練

確保您的組織了解宣告政策的目的是和影響。提供有關預期行為以及如何處理因政策強制執行而失敗的明確指引。

產生宣告政策的帳戶狀態報告

帳戶狀態報告可讓您檢閱範圍內帳戶宣告政策支援的所有屬性的目前狀態。您可以選擇要包含在報告範圍中的帳戶和組織單位 (OUs)，或選取根來選擇整個組織。

此報告透過提供區域明細，以及屬性的目前狀態跨帳戶（透過）是否一致或不一致（透過），來協助您評估整備程度 `numberOfUnmatchedAccounts`。 `numberOfMatchedAccounts` 您也可以查看最常見的值，這是 屬性最常觀察到的組態值。

附加宣告政策以強制執行基準組態的選擇取決於您的特定使用案例。

如需詳細資訊和說明範例，請參閱 [宣告政策的帳戶狀態報告](#)。

先決條件

您必須先執行下列步驟，才能產生帳戶狀態報告

1. 只有管理帳戶或組織的委派管理員才能呼叫 `StartDeclarativePoliciesReport` API。
2. 您必須先擁有 S3 儲存貯體，才能產生報告（建立新的報告或使用現有的報告），它必須位於提出請求的相同區域中，而且必須具有適當的 S3 儲存貯體政策。如需範例 S3 政策，請參閱《Amazon EC2 API 參考》中範例下的範例 Amazon S3 政策 https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_StartDeclarativePoliciesReport.html#API_StartDeclarativePoliciesReport_Examples Amazon EC2
3. 您必須為宣告政策將強制執行基準組態的服務啟用受信任存取。這會建立唯讀服務連結角色，用於產生您組織中帳戶現有組態的帳戶狀態報告。

使用主控台

針對 Organizations 主控台，此步驟是啟用宣告政策程序的一部分。

使用 AWS CLI

對於 AWS CLI，請使用 [EnableAWSServiceAccess](#) API。

如需如何使用 啟用特定服務的受信任存取的詳細資訊 AWS CLI，[AWS 服務 請參閱](#)。 [AWS Organizations](#)

4. 每個組織一次只能產生一個報告。在另一個報告進行時嘗試產生報告將導致錯誤。

存取合規狀態報告

最低許可

若要產生合規狀態報告，您需要執行下列動作的許可：

- `ec2:StartDeclarativePoliciesReport`
- `ec2:DescribeDeclarativePoliciesReports`
- `ec2:GetDeclarativePoliciesReportSummary`
- `ec2:CancelDeclarativePoliciesReport`
- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:DescribeOrganizationalUnit`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListAWSServiceAccessForOrganization`
- `s3:PutObject`

Note

如果您的 Amazon S3 儲存貯體使用 SSE-KMS 加密，您還必須在政策中包含 `kms:GenerateDataKey` 許可。

AWS Management Console

使用下列程序來產生帳戶狀態報告。

產生帳戶狀態報告

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在政策頁面上，選擇 EC2 的宣告政策。

3. 在 EC2 宣告政策頁面上，從動作下拉式功能表中選擇檢視帳戶狀態報告。
4. 在檢視帳戶狀態報告頁面上，選擇產生狀態報告。
5. 在組織結構小工具中，指定您要包含在報告中的組織單位 OUs)。
6. 選擇提交。

AWS CLI & AWS SDKs

產生帳戶狀態報告

使用下列操作來產生合規狀態報告、檢查其狀態，以及檢視報告：

- `ec2:start-declarative-policies-report`：產生帳戶狀態報告。報告會以非同步方式產生，可能需要數小時才能完成。如需詳細資訊，請參閱《Amazon EC2 API 參考》中的 [StartDeclarativePoliciesReport](#)。
- `ec2:describe-declarative-policies-report`：描述帳戶狀態報告的中繼資料，包括報告的狀態。如需詳細資訊，請參閱《Amazon EC2 API 參考》中的 [DescribeDeclarativePoliciesReports](#)。
- `ec2:get-declarative-policies-report-summary`：擷取帳戶狀態報告的摘要。如需詳細資訊，請參閱《Amazon EC2 API 參考》中的 [GetDeclarativePoliciesReportSummary](#)。
- `ec2:cancel-declarative-policies-report`：取消產生帳戶狀態報告。如需詳細資訊，請參閱《Amazon EC2 API 參考》中的 [CancelDeclarativePoliciesReport](#)。

在產生報告之前，授予 EC2 宣告政策委託人存取將存放報告的 Amazon S3 儲存貯體。若要執行此作業，請將下列政策連接至 儲存貯體。將 `amzn-s3-demo-bucket` 為您實際的 Amazon S3 儲存貯體名稱，並將 `identity_ARN` 取代為用於呼叫 `StartDeclarativePoliciesReport` API 的 IAM 身分。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DeclarativePoliciesReportDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": "identity_ARN"
      },
      "Action": [
        "s3:PutObject"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringEquals": {
            "aws:CalledViaLast": "report.declarative-policies-
ec2.amazonaws.com"
        }
    }
}
]
}

```

宣告性政策語法和範例

此頁面說明宣告式政策語法並提供範例。

考量事項

- 當您使用宣告性政策設定服務屬性時，可能會影響多個 APIs。任何不合規動作都將失敗。
- 帳戶管理員將無法修改個別帳戶層級的服務屬性值。

宣告式政策的語法

宣告政策是根據 [JSON](#) 規則建構的純文字檔案。宣告政策的語法遵循所有管理政策類型的語法。如需該語法的完整討論，請參閱[管理政策類型的政策語法和繼承](#)。本主題著重於將該一般語法套用至宣告政策類型的特定需求。

下列範例顯示基本宣告政策語法：

```

{
  "ec2_attributes": {
    "exception_message": {
      "@@assign": "Your custom error message.https://myURL"
    },
    ...

    [Insert supported service attributes]

    ...
  }
}

```

```
}
```

- `ec2_attributes` 欄索引鍵名稱。宣告政策一律以指定的固定金鑰名稱開頭 AWS 服務。這是上面範例政策的第一行。目前宣告政策僅支援 Amazon EC2 相關服務。
- 在下 `ec2_attributes`，您可以使用 `exception_message` 來設定自訂錯誤訊息。如需詳細資訊，請參閱 [宣告政策的自訂錯誤訊息](#)。
- 在下 `ec2_attributes`，您可以插入一或多個支援的宣告政策。如需這些結構描述，請參閱 [支援的宣告政策](#)。

支援的宣告政策

以下是宣告政策支援的 AWS 服務 和 屬性。在下列某些範例中，可能會壓縮 JSON 空白格式以節省空間。

- VPC 封鎖公開存取
- 序列主控台存取
- 映像區塊公開存取
- 允許的影像設定
- 執行個體中繼資料預設值
- 快照區塊公開存取

VPC Block Public Access

政策效果

控制 Amazon VPCs 和子網路中的資源是否可以透過網際網路閘道 (IGWs) 連線到網際網路。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 [網際網路存取組態](#)。

政策內容

```
"vpc_block_public_access": {
  "internet_gateway_block": { // (optional)
    "mode": { // (required)
      "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
    },
    "exclusions_allowed": { // (required)
      "@@assign": "enabled" // enabled | disabled
    }
  }
}
```

```
}
}
```

以下是此屬性的可用欄位：

- "internet_gateway":
 - "mode":
 - "off"：未啟用 VPC BPA。
 - "block_ingress"：所有至 VPCs 網際網路流量（排除 VPCs 或子網路除外）都會遭到封鎖。僅允許進出 NAT 閘道和僅輸出網際網路閘道的流量，因為這些閘道僅允許建立傳出連線。
 - "block_bidirectional"：往返網際網路閘道和輸出限定網際網路閘道（排除 VPCs 和子網路除外）的所有流量都會遭到封鎖。
- "exclusions_allowed"：排除是一種模式，可套用至單一 VPC 或子網路，其會將其從帳戶的 VPC BPA 模式排除，並允許雙向或僅輸出存取。
 - "enabled"：排除可由帳戶建立。
 - "disabled"：帳戶無法建立排除項目。

Note

您可以使用 屬性來設定是否允許排除，但無法使用此屬性本身建立排除。若要建立排除項目，您必須在擁有 VPC 的帳戶中建立排除項目。如需建立 VPC BPA 排除的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [建立和刪除排除](#)。

考量

如果您在宣告式政策中使用此屬性，則無法使用下列操作來修改範圍內帳戶的強制執行組態。此清單並不詳盡：

- ModifyVpcBlockPublicAccessOptions
- CreateVpcBlockPublicAccessExclusion
- ModifyVpcBlockPublicAccessExclusion

Serial Console Access

政策效果

控制 EC2 序列主控台是否可存取。如需 EC2 序列主控台的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [EC2 序列主控台](#)。

政策內容

```
"serial_console_access": {
  "status": { // (required)
    "@@assign": "enabled" // enabled | disabled
  }
}
```

以下是此屬性的可用欄位：

- "status":
 - "enabled"：允許 EC2 序列主控台存取。
 - "disabled"：EC2 序列主控台存取遭到封鎖。

考量

如果您在宣告式政策中使用此屬性，則無法使用下列操作來修改範圍內帳戶的強制執行組態。此清單並不詳盡：

- EnableSerialConsoleAccess
- DisableSerialConsoleAccess

Image Block Public Access

政策效果

控制 Amazon Machine Image (AMIs) 是否可公開共用。如需 AMIs 的詳細資訊，請參閱《[Amazon Elastic Compute Cloud 使用者指南](#)》中的 [Amazon Machine Image \(AMIs\)](#)。

政策內容

```
"image_block_public_access": {
  "state": { // (required)
    "@@assign": "block_new_sharing" // unblocked | block_new_sharing
  }
}
```

以下是此屬性的可用欄位：

- "state":
 - "unblocked" : AMIs的公開共用沒有限制。
 - "block_new_sharing" : 封鎖 AMIs的新公開共用。已公開共用AMIs 仍可公開使用。

考量

如果您在宣告式政策中使用此屬性，則無法使用下列操作來修改範圍內帳戶的強制執行組態。此清單並不詳盡：

- EnableImageBlockPublicAccess
- DisableImageBlockPublicAccess

Allowed Images Settings

政策效果

使用允許的 AMI 控制 Amazon EC2 中 Amazon Machine Image (AMIs)。如需 AMIs 的詳細資訊，請參閱 [《Amazon Elastic Compute Cloud 使用者指南》中的 Amazon Machine Image \(AMIs\)](#)。

政策內容

以下是此屬性的可用欄位：

```
"allowed_images_settings": {
  "state": { // (required)
    "@@assign": "enabled" // enabled | disabled | audit_mode
  },
  "image_criteria": { // (optional)
    "criteria_1": {
      "allowed_image_providers": { // limit 200
        "@@append": [
          "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
digit account ID
        ]
      }
    }
  }
}
```

- "state":
 - "enabled" : 屬性為作用中且強制執行。
 - "disabled" : 屬性為非作用中且未強制執行。
 - "audit_mode" : 屬性處於稽核模式。這表示它會識別不合規的映像，但不會封鎖其使用。
- "image_criteria" : 定義允許 AMI 來源的 `allowed_image_providers` 物件清單。
- "allowed_image_providers" : 以逗號分隔的提供者名稱或帳戶 IDs 清單。

考量

如果您在宣告式政策中使用此屬性，則無法使用下列操作來修改範圍內帳戶的強制執行組態。此清單並不詳盡：

- `EnableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`
- `DisableAllowedImagesSettings`

Instance Metadata Defaults

政策效果

控制所有新 EC2 執行個體啟動的 IMDS 預設值。請注意，此組態只會設定預設值，不會強制執行 IMDS 版本設定。如需 IMDS 預設值的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [IMDS](#)。

政策內容

以下是此屬性的可用欄位：

```
"instance_metadata_defaults": {
  "http_tokens": { // (required)
    "@@assign": "required" // no_preference | required | optional
  },
  "http_put_response_hop_limit": { // (required)
    "@@assign": "4" // -1 | 1 -> 64
  },
  "http_endpoint": { // (required)
    "@@assign": "enabled" // no_preference | enabled | disabled
  },
}
```

```
"instance_metadata_tags": { // (required)
    "@@assign": "enabled" // no_preference | enabled | disabled
}
}
```

- "http_tokens":
 - "no_preference" : 其他預設值適用。例如，如果適用，AMI 會預設為。
 - "required" : 必須使用 IMDSv2。不允許 IMDSv1。
 - "optional" : 允許 IMDSv1 和 IMDSv2。

 Note

中繼資料版本

http_tokens 將設定為 required (必須使用 IMDSv2) 之前，請確定您的所有執行個體都不會進行 IMDSv1 呼叫。

- "http_put_response_hop_limit":
 - "*Integer*" : 從 -1 到 64 的整數值，代表中繼資料字符可以移動的躍點數目上限。若要表示沒有偏好設定，請指定 -1。

 Note

跳轉限制

如果 http_tokens 設為 required，建議將 http_put_response_hop_limit 設為最少 2。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[執行個體中繼資料存取考量](#)事項。

- "http_endpoint":
 - "no_preference" : 其他預設值適用。例如，如果適用，AMI 會預設為。
 - "enabled" : 可存取執行個體中繼資料服務端點。
 - "disabled" : 無法存取執行個體中繼資料服務端點。
- "instance_metadata_tags":
 - "no_preference" : 其他預設值適用。例如，如果適用，AMI 會預設為。
 - "enabled" : 可從執行個體中繼資料存取執行個體標籤。
 - "disabled" : 無法從執行個體中繼資料存取執行個體標籤。

Snapshot Block Public Access

政策效果

控制 Amazon EBS 快照是否可公開存取。如需 EBS 快照的詳細資訊，請參閱《[Amazon Elastic Block Store 使用者指南](#)》中的 [Amazon EBS 快照](#)。

政策內容

```
"snapshot_block_public_access": {
  "state": { // (required)
    "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
    block_all_sharing
  }
}
```

以下是此屬性的可用欄位：

- "state":
 - "block_all_sharing"：封鎖快照的所有公開共用。已公開共用的快照會被視為私有，不再公開。
 - "block_new_sharing"：封鎖快照的新公開共用。已公開共用的快照仍可公開使用。
 - "unblocked"：不限制公開共用快照。

考量

如果您在宣告式政策中使用此屬性，則無法使用下列操作來修改範圍內帳戶的強制執行組態。此清單並不詳盡：

- EnableSnapshotBlockPublicAccess
- DisableSnapshotBlockPublicAccess

備份政策

備份政策可讓您集中管理備份計劃，並將備份計劃套用至組織帳戶的 AWS 資源。

[AWS Backup](#) 可讓您建立 [備份計劃](#)，以定義如何備份 AWS 資源。計劃中的規則包括各種設定，例如備份頻率、備份發生的時間範圍、AWS 區域 包含要備份之資源的，以及存放備份的保存庫。然後，

您可以將備份計劃套用到使用標籤識別 AWS 的資源群組。您還必須識別 AWS Identity and Access Management (IAM) 角色，其授予 AWS Backup 代表您執行備份操作的許可。

中的備份政策會將所有這些片段 AWS Organizations 合併為 [JSON](#) 文字文件。您可以將備份政策連接至組織結構中的任何元素，例如根、組織單位 (OU) 和個別帳戶。Organizations 會套用繼承規則，以合併組織根、任何父 OU 或連接至帳戶的政策。這樣會為每個帳戶產生[有效備份政策](#)。此有效政策會指示 AWS Backup 如何自動備份您的 AWS 資源。

備份政策的運作方式

備份政策可讓您精細控制在組織所需的任何層級上備份資源。例如，您可以在連接至組織根的政策中指定必須備份所有 Amazon DynamoDB 資料表。該政策可以包含預設備份頻率。然後，您可以將備份政策連接至 OU，以根據每個 OU 的需求來覆寫備份頻率。例如，Developers OU 可能指定備份頻率為每週一次，而 Production OU 指定每天一次。

您可以建立部分備份政策，僅個別包含成功備份資源所需的部分資訊。您可以將這些政策連接至組織樹狀結構的不同部分，例如根或父 OU，讓較低層級的 OU 和帳戶繼承這些部分政策。當 Organizations 使用繼承規則合併帳戶的所有政策時，產生的有效政策必須具有所有必要的元素。否則，AWS Backup 請考慮政策無效，且不會備份受影響的資源。

Important

AWS Backup 只有在具有所有必要元素的完整有效政策調用時，才能執行成功的備份。

雖然前述的部分政策策略沒問題，但如果帳戶的有效政策並不完整，則會導致錯誤或無法成功備份資源。另一種策略是考慮要求所有備份政策本身必須完整且有效。使用階層中較高層級連接的政策所提供的「預設」值，然後視需要在子政策中包含[繼承子控制運算子](#)，以覆寫這些預設值。

AWS 帳戶 組織中每個 的有效備份計畫，AWS Backup 會在主控台中顯示為該帳戶的不可變計畫。可檢視但不能變更。不過，您可以使用 [TagResource](#) 和 [UntagResource](#) APIs 或移除備份計畫標籤。

當 根據政策建立的備份計畫 AWS Backup 開始備份時，您可以在 AWS Backup 主控台中查看備份任務的狀態。成員帳戶中的使用者可以看到該成員帳戶中各備份任務的狀態和任何錯誤。如果您也使用啟用受信任的服務存取 AWS Backup，則組織管理帳戶中的使用者可以看到組織中所有備份任務的狀態和錯誤。如需詳細資訊，請參閱AWS Backup 開發人員指南中的[啟用跨帳戶管理](#)。

備份政策入門

請依照下列步驟開始使用備份政策。

1. [了解執行備份政策任務所需的許可](#)
2. [了解使用備份政策時建議的一些最佳實務。](#)
3. [為組織啟用備份政策。](#)
4. [建立備份政策。](#)
5. [將備份政策連接至組織的根、OU 或帳戶。](#)
6. [檢視套用至帳戶的合併有效備份政策。](#)

對於所有這些步驟，請以 IAM 使用者身分登入、擔任 IAM 角色，或以組織管理帳戶中的根使用者身分登入 ([不建議](#))。

其他資訊

- [了解備份政策語法和查看政策範例](#)

使用備份政策的最佳實務

AWS 建議使用下列備份政策的最佳實務。

決定備份政策策略

您建立的備份政策可以是不完整的片段，經過繼承和合併後，形成每個成員帳戶的完整政策。如果這樣做，假設您在某個層級變更，但未仔細考量低於該層級的所有帳戶所受的影響，最後可能產生不完整的有效政策。為了避免這種情況，建議您確保在所有層級實作的備份政策本身是完整的。將父政策視為預設政策，可由子政策中指定的設定來覆寫。如此一來，即使子政策不存在，繼承的政策仍然完整並使用預設值。您可以使用[子控制繼承運算子](#)，以控制子政策可新增、變更或移除哪些設定。

使用 **GetEffectivePolicy** 驗證備份政策的變更

變更備份政策後，在低於您進行變更的層級之下，請檢查代表性帳戶的有效政策。您可以使用 [_](#)，或[使用 GetEffectivePolicy API 操作或其其中一個 或 SDK 變體來檢視有效政策 AWS Management Console](#)。 [GetEffectivePolicy](#) AWS CLI AWS 請確定您所做的變更對有效政策產生預期的影響。

簡單開始，小小改變

若要簡化偵錯，請從簡單的政策開始，然後一次變更一項。每次變更後，請先驗證變更的行為和影響，再繼續變更。在發生錯誤或意外的結果時，此方法可減少您必須考慮的變數。

將備份的副本存放在組織中的其他 AWS 區域 和 帳戶中

若要改善災難復原位置，您可以存放備份的複本。

- 不同的區域 – 如果您將備份複本存放在其他區域 AWS 區域，則有助於保護備份免於原始區域中意外損毀或刪除。使用政策的 `copy_actions` 區段，以在執行備份計劃相同帳戶的一個或多個區域中指定保存庫。若要執行此操作，當您指定用於存放備份複本的備份保存庫 ARN 時，請使用 `$account` 變數來識別帳戶。`$account` 變數會在執行時間自動取代為執行備份政策的帳戶 ID。
- 不同的帳戶 – 如果您將備份複本存放在中 AWS 帳戶，您可以新增安全障礙，協助防止惡意演員入侵您的其中一個帳戶。使用政策的 `copy_actions` 區段，以在組織中的一個或多個帳戶中指定保存庫，與執行的備份計劃帳戶分開。若要執行此操作，當您指定用於存放備份複本的備份保存庫 ARN 時，請使用其實際帳戶 ID 來識別帳戶。

限制每個政策的計劃數目

包含多個計劃的政策在疑難排解時較複雜，因為有大量的輸出必須全部驗證。應該讓每個政策只包含一個備份計劃，以簡化偵錯和疑難排解。然後，您可以新增更多政策來包含其他計劃，以符合其他需求。此方法有助於將計劃的任何問題隔離在一個政策中，在對其他政策及其計劃的問題在疑難排解時，才不會因為這些問題而變得更複雜。

使用堆疊集建立必要的備份保存庫和 IAM 角色

使用 AWS CloudFormation 堆疊集與 Organizations 整合，在您的組織中的每個成員帳戶中自動建立所需的備份文件庫和 AWS Identity and Access Management (IAM) 角色。您可以建立堆疊集，其中包含您希望 AWS 帳戶 組織中每個 自動可用的資源。此方法可讓您執行備份計劃時確保已符合相依性。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的[建立具有自我管理許可的堆疊集](#)。

檢閱每個帳戶中建立的第一個備份來檢查結果

當您變更政策時，請檢查該變更之後建立的下一個備份，以確保變更產生預期的影響。此步驟不僅止於查看有效的政策，還可確保 AWS Backup 解譯您的政策，並按照您預期的方式實作備份計劃。

使用 AWS CloudTrail 事件來監控組織中的備份政策

您可以使用 AWS CloudTrail 事件來監控備份政策何時從組織中的任何帳戶建立、更新或刪除，或何時存在無效的組織備份計劃。如需詳細資訊，請參閱 AWS Backup 開發人員指南中的[記錄跨帳戶管理事件](#)。

備份政策語法和範例

此頁面說明備份政策語法並提供範例。

備份政策的語法

備份政策是根據 [JSON](#) 規則建構的純文字檔。備份政策的語法遵循所有管理政策類型的語法。如需詳細資訊，請參閱 [管理政策類型的政策語法和繼承](#)。本主題著重於以該一般語法滿足備份政策類型的特定需求。

如需 AWS Backup 計劃的詳細資訊，請參閱《AWS Backup 開發人員指南》中的 [CreateBackupPlan](#)。

考量事項

政策語法

JSON 中將拒絕重複的金鑰名稱。

政策必須指定要備份的 AWS 區域 和資源。

政策必須指定 AWS Backup 擔任的 IAM 角色。

在相同層級使用@assign運算子可以覆寫現有的設定。如需詳細資訊，請參閱[子政策覆寫父政策中的設定](#)。

繼承運算子可控制繼承的政策和帳戶政策如何合併成為帳戶的有效政策。這些運算子包括值-設定運算子和子控制運算子。

如需詳細資訊，請參閱[繼承運算子](#)和[備份政策範例](#)。

IAM 角色

第一次建立備份計劃時，IAM 角色必須存在。

IAM 角色必須具有存取標籤查詢所識別資源的許可。

IAM 角色必須具有執行備份的許可。

備份保存庫

保存庫必須存在於每個指定的 中，AWS 區域 備份計畫才能執行。

每個接收有效政策 AWS 的帳戶都必須有保存庫。如需詳細資訊，請參閱《AWS Backup 開發人員指南》中的[備份保存庫建立和刪除](#)。

我們建議您使用 AWS CloudFormation 堆疊集及其與 Organizations 的整合，為組織中的每個成員帳戶自動建立和設定備份保存庫和 IAM 角色。如需詳細資訊，請參閱AWS CloudFormation 使用者指南中的[建立具有自我管理許可的堆疊集](#)。

配額

如需配額清單，請參閱《AWS Backup 開發人員指南》中的[AWS Backup 配額](#)。

備份語法：概觀

備份政策語法包含下列元素：

```
{
  "plans": {
    "PlanName": {
      "rules": { ... },
      "regions": { ... },
      "selections": { ... },
      "advanced_backup_settings": { ... },
      "backup_plan_tags": { ... }
    }
  }
}
```

備份政策元素

Element	描述	必要
規則	備份規則的清單。每個規則會定義備份何時開始，以及 regions 和 selections 元素中指定資源的執行時段。	是
區域	備份政策可保護資源 AWS 區域 的清單。	是
選項	備份rules保護regions之指定 內的一或多個資源類型。	是
advanced_backup_settings	特定備份案例的組態選項。 目前，支援的唯一進階備份設定是為在 Amazon EC2 執行個體上執行的 Windows 或 SQL Server 啟用 Microsoft Volume Shadow Copy Service (VSS) 備份。	否
backup_plan_tags	您要與備份計畫建立關聯的標籤。每個標籤都是由使用者定義的金鑰和值組成的標籤。	否

Element	描述	必要
	標籤可協助您管理、識別、組織、搜尋和篩選備份計劃。	

備份語法：規則

rules 政策金鑰會指定在所選資源上執行的排程備份任務 AWS Backup。

備份規則元素

Element	描述	必要
schedule_expression	UTC 中的 Cron 表達式，指定何時 AWS Backup 啟動備份任務。 如需 cron 表達式的資訊，請參閱《Amazon EventBridge 使用者指南》中的 使用 cron 和 rate 表達式來排程規則 。	是
target_backup_vault_name	存放備份的備份保存庫。 備份保存庫是由用於建立它們的帳戶及其建立 AWS 區域 位置的唯一名稱所識別。	是
start_backup_window_minutes	如果備份任務未成功啟動，則會取消在取消備份任務之前等待的分鐘數。 若包含此值，則其必須至少為 60 分鐘以避免發生錯誤。	否
complete_backup_window_minutes	備份任務成功啟動後，必須完成或由 取消前的 N 分鐘數 AWS Backup。	否
enable_continuous_backup	指定 是否 AWS Backup 建立連續備份。 True 會 AWS Backup 讓 建立能夠point-in-time 還原 (PITR) 的連續備份。False (或未指定) AWS Backup 會讓 建立快照備份。	否

Element	描述	必要
	如需持續備份的詳細資訊，請參閱AWS Backup 開發人員指南中的 point-in-time 恢復。 注意：啟用 PITR 的備份保留期上限為 35 天。	
lifecycle	指定何時將備份 AWS Backup 轉換為冷儲存，以及何時過期。 AWS Backup 開發人員指南中，可轉換為冷儲存的資源類型會依資源表的功能可用性依資源的功能可用性列出。 每個生命週期都包含下列元素： • <code>move_to_cold_storage_after_days</code>：在將復原點 AWS Backup 移至冷儲存之前，備份發生後的天數。 • <code>delete_after_days</code>：在 AWS Backup 刪除復原點之前，備份發生後的天數。 • <code>opt_in_to_archive_for_supported_resources</code>：如果將此值指派為 <code>true</code>，則備份計畫會根據您的生命週期設定，將支援的資源轉換為封存（冷）儲存層。 注意：轉換為冷儲存的備份必須存放在冷儲存中至少 90 天。 這表示 <code>delete_after_days</code> 必須大於 90 天 <code>move_to_cold_storage_after_days</code>。	否

Element	描述	必要
copy_actions	指定 是否將備份 AWS Backup 複製到一或多個其他位置。 每個複製動作都包含下列元素： - target_backup_vault_arn : 存放額外備份複本的保存庫 AWS Backup。 - 針對相同帳戶複本\$account使用 - 使用跨帳戶複本的實際帳戶 ID - lifecycle : 指定 何時將備份 AWS Backup 轉換為冷儲存，以及何時過期。 每個生命週期都包含下列元素： - move_to_cold_storage_after_days : 在將復原點移至冷儲存之前 AWS Backup，備份發生後的天數。 - delete_after_days : 在 AWS Backup 刪除復原點之前，備份發生後的天數。 注意：轉換為冷儲存的備份必須存放在冷儲存中至少 90 天。 這表示 delete_after_days 必須大於 90 天move_to_cold_storage_after_days。	否
recovery_point_tags	您要指派給從備份還原之資源的標籤。 每個標籤都包含下列元素： - tag_key : 標籤名稱（區分大小寫） - tag_value : 標籤值（區分大小寫）	否

Element	描述	必要
index_actions	指定 是否 AWS Backup 建立 Amazon EBS 快照和/或 Amazon S3 備份的備份索引。建立備份索引是為了搜尋備份的中繼資料。如需備份索引建立和備份搜尋的詳細資訊，請參閱備份搜尋。 注意：建立 Amazon EBS 快照備份索引需要其他 IAM 角色許可。 每個索引動作都包含下列元素：resource_types 其中支援編製索引的資源類型為 Amazon EBS 和 Amazon S3。此參數會指定要選擇加入索引的資源類型。	否

備份語法：區域

regions 政策金鑰指定 AWS 區域 AWS Backup 查找哪些 來尋找符合selections金鑰中條件的資源。

備份區域元素

Element	描述	必要
regions	指定 AWS 區域 代碼。例如：["us-east-1", "eu-north-1"] 。	是

備份語法：選取項目

selections 政策金鑰指定由備份政策中的規則所備份的資源。

有兩種互斥元素：tags和 resources。有效的政策必須在選擇resources中have標籤或 才有效。

如果您想要同時具有標籤條件和資源條件的選擇，請使用 resources金鑰。

備份選擇元素：標籤

Element	描述	必要
iam_role_arn	AWS Backup 擔任的 IAM 角色可跨指定區域查詢、探索和備份資源。 角色必須有足夠的許可，才能根據標籤條件查詢資源，並對相符的資源執行備份操作。	是
tag_key	要搜尋的標籤索引鍵名稱。	是
tag_value	必須與相符 tag_key 相關聯的值。 AWS Backup 只有在 tag_key 和 tag_value 相符（區分大小寫）時，才會包含資源。	是
conditions	您要包含或排除的標籤索引鍵和值 使用 string_equals 或 string_not_equals 來包含或排除完全相符的標籤。 使用 string_like 和 string_not_like 來包含或排除包含或不包含特定字元的標籤 注意：每個選擇僅限 30 個條件。	否

備份選擇元素：資源

Element	描述	必要
iam_role_arn	AWS Backup 擔任的 IAM 角色可跨指定區域查詢、探索和備份資源。 角色必須有足夠的許可，才能根據標籤條件查詢資源，並對相符的資源執行備份操作。 注意：在 中 AWS GovCloud (US) Regions，您必須將分割區的名稱新增至 ARN。	是

Element	描述	必要
	例如, "arn:aws:ec2:*:*:volume/* " 必須是 "arn:aws-us-gov:ec2:*:*:volume/* "。	
resource_types	要包含在備份計畫中的資源類型。	是
not_resource_types	從備份計畫中排除的資源類型。	否
conditions	標記您要包含或排除的索引鍵和值 使用 string_equals 或 string_not_equals 來包含或排除完全相符的標籤。 使用 string_like 和 string_not_like 來包含或排除包含或不包含特定字元的標籤 注意：每個選擇僅限 30 個條件。	否

支援的資源類型

Organizations 支援 resource_types 和 not_resource_types 元素的下列資源類型：

- AWS Backup gateway 虛擬機器： "arn:aws:backup-gateway:*:*:vm/*"
- AWS CloudFormation 堆疊： "arn:aws:cloudformation:*:*:stack/*"
- Amazon DynamoDB 資料表： "arn:aws:dynamodb:*:*:table/*"
- Amazon EC2 執行個體： "arn:aws:ec2:*:*:instance/*"
- Amazon EBS 磁碟區： "arn:aws:ec2:*:*:volume/*"
- Amazon EFS 檔案系統： "arn:aws:elasticfilesystem:*:*:file-system/*"
- Amazon Aurora/Amazon DocumentDB/Amazon Neptune 叢集：
"arn:aws:rds:*:*:cluster:"
- Amazon RDS 資料庫： "arn:aws:rds:*:*:db:"
- Amazon Redshift 叢集： "arn:aws:redshift:*:*:cluster:"
- Amazon S3： "arn:aws:s3:::"
- 適用於 SAP 的 AWS Systems Manager HANA 資料庫： "arn:aws:ssm-sap:*:*:HANA/*"

- AWS Storage Gateway 閘道： "arn:aws:storagegateway:*:*:gateway/*"
- Amazon Timestream 資料庫： "arn:aws:timestream:*:*:database/*"
- Amazon FSx 檔案系統： "arn:aws:fsx:*:*:file-system/*"
- Amazon FSx 磁碟區： "arn:aws:fsx:*:*:volume/*"

程式碼範例

如需詳細資訊，請參閱[使用標籤區塊指定資源](#)和[使用資源區塊指定資源](#)。

備份語法：進階備份設定

`advanced_backup_settings` 金鑰指定特定備份案例的組態選項。每個設定都包含下列元素：

進階備份設定元素

Element	描述	必要
<code>advanced_backup_settings</code>	指定特定備份案例的設定。此索引鍵包含一個或多個設定。每個設定都是包含下列元素的 JSON 物件字串： 目前支援的唯一進階備份設定是為在 Amazon EC2 執行個體上執行的 Windows 或 SQL Server 啟用 Microsoft Volume Shadow Copy Service (VSS) 備份。 每個進階備份都會設定下列元素： • <code>Object key name</code>：指定下列進階設定適用的資源類型的字串。 金鑰名稱必須是 "ec2" 資源類型	否

Element	描述	必要
	Object value : Dtring , 其中包含一或多個特定於相關聯資源類型的備份設定。 值指定"windows_vss" 支援在 disabled Amazon EC2 執行個體上執行的備份為 enabled或。	

範例：

```
"advanced_backup_settings": {
  "ec2": {
    "windows_vss": {
      "@@assign": "enabled"
    }
  }
},
```

備份語法：備份計畫標籤

backup_plan_tags 政策金鑰會指定連接至備份計畫本身的標籤。這不會影響為 rules或 指定的標籤selections。

備份計畫標籤元素

Element	描述	必要
backup_plan_tags	每個標籤都是由使用者定義的索引鍵和值組成的標籤： - tag_key：標記要搜尋的金鑰名稱。值會區分大小寫。 - tag_value：附加至備份計畫並與相關聯的值tag_key。值會區分大小寫。	否

備份政策範例

接下來的備份政策範例僅供參考。在下列某些範例中，可能會壓縮 JSON 空白格式以節省空間。

- [範例 1：指派給父節點的政策](#)
- [範例 2：父政策與子政策合併](#)
- [範例 3：父政策可防止子政策的任何變更](#)
- [範例 4：父政策可防止子政策變更一個備份計畫](#)
- [範例 5：子政策覆寫父政策中的設定](#)
- [範例 6：使用標籤區塊指定資源](#)
- [範例 7：使用資源區塊指定資源](#)

範例 1：指派給父節點的政策

下列範例顯示備份政策指派給帳戶的其中一個父節點。

父政策 – 此政策可以連接至組織的根，或任何 OU (所有預定帳戶的父系)。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@@assign": [
          "ap-northeast-2",
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 5/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "480"
          },
          "complete_backup_window_minutes": {
            "@@assign": "10080"
          },
          "lifecycle": {
            "move_to_cold_storage_after_days": {
```

```

        "@@assign": "180"
      },
      "delete_after_days": {
        "@@assign": "270"
      },
      "opt_in_to_archive_for_supported_resources": {
        "@@assign": "false"
      }
    },
    "target_backup_vault_name": {
      "@@assign": "FortKnox"
    },
    "index_actions": {
      "resource_types": {
        "@@assign": [
          "EBS",
          "S3"
        ]
      }
    },
    "copy_actions": {
      "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
        "target_backup_vault_arn": {
          "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
        },
        "lifecycle": {
          "move_to_cold_storage_after_days": {
            "@@assign": "30"
          },
          "delete_after_days": {
            "@@assign": "120"
          },
          "opt_in_to_archive_for_supported_resources": {
            "@@assign": "false"
          }
        }
      }
    },
    "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
      "target_backup_vault_arn": {
        "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
      }
    }
  }
}

```



```

        },
        "lifecycle": {
            "move_to_cold_storage_after_days": {
                "@@assign": "30"
            },
            "delete_after_days": {
                "@@assign": "120"
            },
            "opt_in_to_archive_for_supported_resources": {
                "@@assign": "false"
            }
        }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": {
                    "@@assign": "arn:aws:iam::${account}:role/MyIamRole"
                },
                "tag_key": {
                    "@@assign": "data_type"
                },
                "tag_value": {
                    "@@assign": [
                        "PII",
                        "RED"
                    ]
                }
            }
        }
    },
    "advanced_backup_settings": {
        "ec2": {
            "windows_vss": {
                "@@assign": "enabled"
            }
        }
    }
}

```

```
}
```

如果沒有其他政策繼承或連接到帳戶，則每個適用的有效政策轉譯 AWS 帳戶 如下範例所示。CRON 運算式導致每小時整點執行一次備份。帳戶 ID 123456789012 將是每個帳戶的實際帳戶 ID。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
      ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",
          "target_backup_vault_name": "FortKnox",
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "delete_after_days": "2",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
          },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
              "target_backup_vault_arn": {
                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
              },
              "lifecycle": {
                "delete_after_days": "28",
                "move_to_cold_storage_after_days": "180",
                "opt_in_to_archive_for_supported_resources": "false"
              }
            }
          }
        }
      }
    }
  }
}
```

```

        },
        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
            "target_backup_vault_arn": {
                "@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
            },
            "lifecycle": {
                "delete_after_days": "28",
                "move_to_cold_storage_after_days": "180",
                "opt_in_to_archive_for_supported_resources": "false"
            }
        }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                "tag_key": "dataType",
                "tag_value": [
                    "PII",
                    "RED"
                ]
            }
        }
    },
    "advanced_backup_settings": {
        "ec2": {
            "windows_vss": "enabled"
        }
    }
}

```

範例 2：父政策與子政策合併

在下列範例中，繼承的父政策和子政策會繼承或直接連接到 AWS 帳戶 合併，以形成有效的政策。

父政策 – 此政策可以連接至組織的根或任何父 OU。

```
{
```

```

    "plans": {
      "PII_Backup_Plan": {
        "regions": { "@@append": [ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
        "rules": {
          "Hourly": {
            "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
            "start_backup_window_minutes": { "@@assign": "60" },
            "target_backup_vault_name": { "@@assign": "FortKnox" },
            "index_actions": {
              "resource_types": {
                "@@assign": [
                  "EBS",
                  "S3"
                ]
              }
            },
            "lifecycle": {
              "move_to_cold_storage_after_days": { "@@assign": "28" },
              "delete_after_days": { "@@assign": "180" },
              "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
            },
            "copy_actions": {
              "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                "target_backup_vault_arn" : {
                  "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                },
                "lifecycle": {
                  "move_to_cold_storage_after_days": { "@@assign":
"28" },
                  "delete_after_days": { "@@assign": "180" },
                  "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
                }
              }
            }
          },
          "selections": {
            "tags": {
              "datatype": {

```

```
    "iam_role_arn": { "@@assign": "arn:aws:iam::${account}:role/  
MyIamRole" },  
  
    "tag_key": { "@@assign": "dataType" },  
    "tag_value": { "@@assign": [ "PII", "RED" ] }  
  }  
}  
}  
}  
}
```

子政策 – 此政策可以直接連接至帳戶，或父政策所連接 OU 之下任何層級的 OU。

```
{
  "plans": {
    "Monthly_Backup_Plan": {
      "regions": {
        "@@append": [ "us-east-1", "eu-central-1" ] },
      "rules": {
        "Monthly": {
          "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
          "start_backup_window_minutes": { "@@assign": "480" },
          "target_backup_vault_name": { "@@assign": "Default" },
          "lifecycle": {
            "move_to_cold_storage_after_days": { "@@assign": "30" },
            "delete_after_days": { "@@assign": "365" },
            "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
          },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
              "target_backup_vault_arn" : {
                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
              },
              "lifecycle": {
                "move_to_cold_storage_after_days": { "@@assign":
"30" },
                "delete_after_days": { "@@assign": "365" },
                "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
              }
            }
          }
        }
      }
    }
  }
}
```

```

    }
  },
  "selections": {
    "tags": {
      "MonthlyDatatype": {
        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/MyMonthlyBackupIamRole" },
        "tag_key": { "@@assign": "BackupType" },
        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
      }
    }
  }
}

```

產生的有效政策 – 套用至帳戶的有效政策包含兩個計劃，每個計劃各自有一組規則和一組要套用規則的資源。

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",
          "target_backup_vault_name": "FortKnox",
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "delete_after_days": "2",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
          }
        }
      }
    }
  }
}

```

```

        "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                "target_backup_vault_arn" : {
                    "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                },
                "lifecycle": {
                    "move_to_cold_storage_after_days": "28",
                    "delete_after_days": "180",
                    "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
                }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                    "tag_key": "dataType",
                    "tag_value": [ "PII", "RED" ]
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {

```

```

    "@@assign" : "arn:aws:backup:us-east-1:$account:backup-vault:Default"
  },
  "lifecycle": {
    "move_to_cold_storage_after_days": "30",
    "delete_after_days": "365",
    "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
  }
}
},
"selections": {
  "tags": {
    "monthlydatatype": {
      "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;role/MyMonthlyBackupIamRole",
      "tag_key": "BackupType",
      "tag_value": [ "MONTHLY", "RED" ]
    }
  }
}
}
}
}

```

範例 3：父政策防止子政策做出任何變更

在下列範例中，繼承的父政策使用[子控制運算子](#)來強制執行所有設定，並防止子政策變更或覆寫這些設定。

父政策 – 此政策可以連接至組織的根或任何父 OU。政策的每個節點上都出現

"@operators_allowed_for_child_policies": ["@none"]，表示子政策完全無法變更計劃。子政策也無法將其他計劃新增至有效政策。此政策成為所連接的 OU 之下每個 OU 和帳戶的有效政策。

```
{
  "plans": {
    "@operators_allowed_for_child_policies": ["@none"],
    "PII_Backup_Plan": {
      "@operators_allowed_for_child_policies": ["@none"],
      "regions": {
```



```

    "@operators_allowed_for_child_policies": ["@none"],
    "@append": [
        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
    ]
},
"rules": {
    "@operators_allowed_for_child_policies": ["@none"],
    "Hourly": {
        "@operators_allowed_for_child_policies": ["@none"],
        "schedule_expression": {
            "@operators_allowed_for_child_policies": ["@none"],
            "@assign": "cron(0 0/1 ? * * *)"
        },
        "start_backup_window_minutes": {
            "@operators_allowed_for_child_policies": ["@none"],
            "@assign": "60"
        },
        "target_backup_vault_name": {
            "@operators_allowed_for_child_policies": ["@none"],
            "@assign": "FortKnox"
        },
        "index_actions": {
            "@operators_allowed_for_child_policies": ["@none"],
            "resource_types": {
                "@assign": [
                    "EBS",
                    "S3"
                ]
            }
        },
        "lifecycle": {
            "@operators_allowed_for_child_policies": ["@none"],
            "move_to_cold_storage_after_days": {
                "@operators_allowed_for_child_policies": ["@none"],
                "@assign": "28"
            },
            "delete_after_days": {
                "@operators_allowed_for_child_policies": ["@none"],
                "@assign": "180"
            },
            "opt_in_to_archive_for_supported_resources": {
                "@operators_allowed_for_child_policies": ["@none"],

```

```

        "@@assign": "false"
      }
    },
    "copy_actions": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "target_backup_vault_arn": {
          "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
          "@@operators_allowed_for_child_policies": ["@@none"]
        },
        "lifecycle": {
          "@@operators_allowed_for_child_policies": ["@@none"],
          "delete_after_days": {
            "@@operators_allowed_for_child_policies":
["@@none"],
            "@@assign": "28"
          },
          "move_to_cold_storage_after_days": {
            "@@operators_allowed_for_child_policies":
["@@none"],
            "@@assign": "180"
          },
          "opt_in_to_archive_for_supported_resources": {
            "@@operators_allowed_for_child_policies":
["@@none"],
            "@@assign": "false"
          }
        }
      }
    }
  },
  "selections": {
    "@@operators_allowed_for_child_policies": ["@@none"],
    "tags": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "datatype": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "iam_role_arn": {
          "@@operators_allowed_for_child_policies": ["@@none"],
          "@@assign": "arn:aws:iam::$account:role/MyIamRole"
        }
      }
    }
  }
}

```

```
    },
    "tag_key": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "@@assign": "dataType"
    },
    "tag_value": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "@@assign": [
        "PII",
        "RED"
      ]
    }
  }
},
{
  "advanced_backup_settings": {
    "@@operators_allowed_for_child_policies": ["@@none"],
    "ec2": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "windows_vss": {
        "@@assign": "enabled",
        "@@operators_allowed_for_child_policies": ["@@none"]
      }
    }
  }
}
}
```

產生的有效政策 – 忽略任何存在的子備份政策，父政策會成為有效政策。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
      ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",

```

```

        "target_backup_vault_name": "FortKnox",
        "index_actions": {
            "resource_types": {
                "@@assign": [
                    "EBS",
                    "S3"
                ]
            }
        },
        "lifecycle": {
            "delete_after_days": "2",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
        },
        "copy_actions": {
            "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
            "lifecycle": {
                "move_to_cold_storage_after_days": "28",
                "delete_after_days": "180",
                "opt_in_to_archive_for_supported_resources": "false"
            }
        }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                "tag_key": "dataType",
                "tag_value": [
                    "PII",
                    "RED"
                ]
            }
        }
    },
    "advanced_backup_settings": {
        "ec2": {"windows_vss": "enabled"}
    }
}

```

範例 4：父政策防止子政策變更備份計劃

在下列範例中，繼承的父政策使用[子控制運算子](#)來強制執行單一計劃的設定，並防止子政策變更或覆寫這些設定。子政策仍然可以新增其他計劃。

父政策 – 此政策可以連接至組織的根或任何父 OU。此範例與上一個範例類似，一樣都封鎖所有子繼承運算子，但 plans 最上層除外。該層級的 @@append 設定可讓子政策將其他計劃新增至有效政策中的集合。仍然完全禁止變更繼承的計劃。

為了清楚起見，已截斷計劃中的區段。

```
{
  "plans": {
    "@@operators_allowed_for_child_policies": ["@@append"],
    "PII_Backup_Plan": {
      "@@operators_allowed_for_child_policies": ["@none"],
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}
```

子政策 – 此政策可以直接連接至帳戶，或父政策所連接 OU 之下任何層級的 OU。這個子政策定義新的計劃。

為了清楚起見，已截斷計劃中的區段。

```
{
  "plans": {
    "MonthlyBackupPlan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}
```

產生的有效政策 – 有效政策包含這兩個計劃。

```
{
  "plans": {
```

```

    "PII_Backup_Plan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    },
    "MonthlyBackupPlan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}

```

範例 5：子政策覆寫父政策中的設定

在下列範例中，子政策使用[值設定運算子](#)來覆寫從父政策繼承的某些設定。

父政策 – 此政策可以連接至組織的根或任何父 OU。子政策可以覆寫任何設定，因為沒有[子控制運算子](#)出面禁止，所以預設行為允許子政策 @@assign、@@append 或 @@remove。父政策包含有效備份計劃的所有必要元素，因此，只要原封不動繼承，就會成功備份資源。

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@@append": [
          "us-east-1",
          "ap-northeast-3",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
          "start_backup_window_minutes": {"@@assign": "60"},
          "target_backup_vault_name": {"@@assign": "FortKnox"},
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          }
        }
      }
    }
  }
}

```

```

        },
        "lifecycle": {
            "delete_after_days": {"@@assign": "2"},
            "move_to_cold_storage_after_days": {"@@assign": "180"},
            "opt_in_to_archive_for_supported_resources": {"@@assign":
false}
        },
        "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                "lifecycle": {
                    "move_to_cold_storage_after_days": {"@@assign": "28"},
                    "delete_after_days": {"@@assign": "180"},
                    "opt_in_to_archive_for_supported_resources":
{"@@assign": false}
                }
            }
        }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                "tag_key": {"@@assign": "dataType"},
                "tag_value": {
                    "@@assign": [
                        "PII",
                        "RED"
                    ]
                }
            }
        }
    }
}

```

子政策 – 子政策只能包含的設定必須不同於繼承的父政策。合併到有效政策時，必須有繼承的父政策提供其他必要的設定。否則，有效的備份政策會包含無效的備份計劃，而無法如預期般備份資源。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@@assign": [
          "us-west-2",
          "eu-central-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
          "start_backup_window_minutes": {"@@assign": "80"},
          "target_backup_vault_name": {"@@assign": "Default"},
          "lifecycle": {
            "move_to_cold_storage_after_days": {"@@assign": "30"},
            "delete_after_days": {"@@assign": "365"},
            "opt_in_to_archive_for_supported_resources": {"@@assign":
false}
          }
        }
      }
    }
  }
}
```

產生的有效政策 – 有效政策包含兩個政策的設定，而子政策所提供的設定會覆寫從父政策繼承的設定。此範例中有下列變更：

- 區域清單換成完全不同的清單。如果您要將區域新增至繼承的清單，請在子政策中使用 @@append，而不是 @@assign。
- AWS Backup 每隔一小時執行一次，而不是每小時執行一次。
- AWS Backup 允許 80 分鐘開始備份，而不是 60 分鐘。
- AWS Backup 使用保存Default庫而非 FortKnox。
- 生命週期延長，而得以轉移至不常用的儲存體及最終刪除備份。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
```



```

        "us-west-2",
        "eu-central-1"
    ],
    "rules": {
        "hourly": {
            "schedule_expression": "cron(0 0/2 ? * * *)",
            "start_backup_window_minutes": "80",
            "target_backup_vault_name": "Default",
            "index_actions": {
                "resource_types": {
                    "@@assign": [
                        "EBS",
                        "S3"
                    ]
                }
            },
            "lifecycle": {
                "delete_after_days": "365",
                "move_to_cold_storage_after_days": "30",
                "opt_in_to_archive_for_supported_resources": "false"
            },
            "copy_actions": {
                "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                    "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": "28",
                        "delete_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    }
                }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                    "tag_key": "dataType",
                    "tag_value": [
                        "PII",
                        "RED"
                    ]
                }
            }
        }
    }
}

```

```
]
}
}
}
}
```

範例 6：使用 **tags** 區塊指定資源

下列範例包含所有具有 `tag_key = "env"` 和 `tag_value = "prod"` 的資源 "gamma"。此範例會排除具有 `tag_key = "backup"` 和 `tag_value = "false"` 的資源 "false"。

```
...
"selections":{
  "tags":{
    "selection_name":{
      "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
      "tag_key":{"@@assign": "env"},
      "tag_value":{"@@assign": ["prod", "gamma"]},
      "conditions":{
        "string_not_equals":{
          "condition_name1":{
            "condition_key": { "@@assign": "aws:ResourceTag/backup" },
            "condition_value": { "@@assign": "false" }
          }
        }
      }
    }
  }
},
...
},
...
```

範例 7：使用 **resources** 區塊指定資源

以下是使用 `resources` 區塊來指定資源的範例。

Example: Select all resources in my account

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 區塊使用布林值AND來合併資源類型。

...

```

"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@@assign": [
        "*"
      ]
    }
  }
},
...

```

Example: Select all resources in my account, but exclude Amazon EBS volumes

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 和 "not_resource_types" 區塊使用布林值AND來結合資源類型。

```

...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@@assign": [
        "*"
      ]
    },
    "not_resource_types":{
      "@@assign": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  }
},
...

```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 和 "not_resource_types" 區塊使用布林值AND來結合資源類型。"conditions" 區塊使用布林值AND。

```

...
"resources":{

```

```

    "resource_selection_name":{
      "iam_role_arn":{"@@assign": "arn:aws:iam::${account}:role/IAMRole"},
      "resource_types":{
        "@@assign": [
          "*"
        ]
      },
      "not_resource_types":{
        "@@assign": [
          "arn:aws:ec2:*:*:volume/*"
        ]
      },
      "conditions":{
        "string_equals":{
          "condition_name1":{
            "condition_key": { "@@assign":"aws:ResourceTag/backup"},
            "condition_value": { "@@assign":"true" }
          }
        }
      }
    }
  },
  ...

```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 區塊使用布林值AND來合併資源類型。"conditions" 區塊使用布林值AND來結合資源類型和標籤條件。

```

...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::${account}:role/IAMRole"},
    "resource_types":{
      "@@assign": [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:rds:*:*:db:*"
      ]
    },
    "conditions":{
      "string_equals":{
        "condition_name1":{

```

```

        "condition_key":{"@assign":"aws:ResourceTag/backup"},
        "condition_value":{"@assign":"true"}
    },
    "condition_name2":{
        "condition_key":{"@assign":"aws:ResourceTag/stage"},
        "condition_value":{"@assign":"prod"}
    }
}
}
},
...

```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 區塊使用布林值AND來合併資源類型。"conditions" 區塊使用布林值AND來結合資源類型和標籤條件。

```

...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@assign":"true"}
                }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@assign":"test"}
                }
            }
        }
    }
}

```

```

    }
  },
  ...

```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 區塊使用布林值AND來合併資源類型。"conditions" 區塊使用布林值AND來結合資源類型和標籤條件。

在此範例中，請注意在 include*、*exclude*和 (*)中使用萬用字元arn:aws:rds:*:*:db:*。您可以在字串(*)的開頭、結尾和中間使用萬用字元。

```

...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@assign": [
        "*"
      ]
    },
    "conditions":{
      "string_like":{
        "condition_name1":{
          "condition_key":{"@assign":"aws:ResourceTag/key1"},
          "condition_value":{"@assign":"include*"}
        }
      },
      "string_not_like":{
        "condition_name2":{
          "condition_key":{"@assign":"aws:ResourceTag/key2"},
          "condition_value":{"@assign":"*exclude*"}
        }
      }
    }
  }
},
...

```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

布林值邏輯類似於您可能會在 IAM 政策中使用的邏輯。"resource_types" 和 "not_resource_types" 區塊使用布林值AND來結合資源類型。"conditions" 區塊使用布林值AND來結合資源類型和標籤條件。

```
...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@@assign": [
        "*"
      ]
    },
    "not_resource_types":{
      "@@assign":[
        "arn:aws:fsx::*:file-system/*",
        "arn:aws:rds::*:db:*"
      ]
    },
    "conditions":{
      "string_equals":{
        "condition_name1":{
          "condition_key":{"@@assign":"aws:ResourceTag/backup"},
          "condition_value":{"@@assign":"true"}
        }
      }
    }
  }
},
...
```

標籤政策

標籤政策可讓您標準化連接到組織帳戶中 AWS 資源的標籤。

您可以使用標籤政策來維護標籤的一致性，包括標籤索引鍵和標籤值的慣用大小寫處理。

什麼是標籤？

標籤是您指派或 AWS 指派給 AWS 資源的自訂屬性標籤。每個標籤有兩個部分：

- 標籤鍵 (例如, CostCenter、Environment 或 Project)。標籤鍵會區分大小寫。
- 選用欄位，稱為標籤值 (例如 111122223333 或 Production)。忽略標籤值基本上等同於使用空字串。與標籤鍵相同，標籤值會區分大小寫。

此頁面的其餘部分說明標籤政策。如需標籤的詳細資訊，請參閱下列來源：

- 如需標記的一般資訊，包括命名和使用慣例，請參閱[標記 AWS 資源使用者指南](#)。
- 關於支援標記的服務清單，請參閱[Resource Groups 標記 API 參考](#)。
- 如需有關使用標籤來分類資源的資訊，請參閱[標記 AWS 資源的最佳實務白皮書](#)。
- 如需有關標記 Organizations 資源的資訊，請參閱[標記 AWS Organizations 資源](#)。
- 如需在其他 中標記資源的詳細資訊 AWS 服務，請參閱該服務的文件。

什麼是標籤政策？

標籤政策是協助您將組織帳戶中各資源的標籤標準化的一種政策。在標籤政策中，您指定在標記資源時適用的標記規則。

例如，標籤政策可以指定當 CostCenter 標籤連接至資源時，必須使用標籤政策所定義的大小寫處理和標籤值。標籤政策也可以指定在指定的資源類型上，強制執行不合規的標記操作。換句話說，防止完成指定的資源類型上不合規的標記請求。對於未標記的資源或標籤政策中未定義的標籤，不會評估是否符合標籤政策。

使用標籤政策涉及使用多個 AWS 服務：

- 使用 AWS Organizations 管理標籤政策。登入組織的管理帳戶時，您可以使用 Organizations 來啟用標籤政策功能。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。然後，您就可以建立標籤政策並連接至組織實體，使這些標記規則生效。
- 使用 AWS Resource Groups 管理是否符合標籤政策。登入組織中的帳戶時，您可以使用 Resource Groups 在帳戶中的資源上尋找不合規標籤。您可以在建立資源的 AWS 服務中更正不合規標籤。您也可以使用[標籤編輯器](#)和[資源群組標記](#) API 來標記和取消標記來自多個 服務的資源。

如果您登入組織中的管理帳戶，您可以檢視組織所有帳戶的合規資訊。

只有在[已啟用所有功能](#)的組織中，才能使用標籤政策。如需使用標籤政策所需條件的詳細資訊，請參閱[管理政策的先決條件和許可 AWS Organizations](#)。

Important

若要開始使用標籤政策，AWS 強烈建議您遵循 中描述的範例工作流程，[開始使用標籤政策](#) 然後再繼續進行更進階的標籤政策。將標籤政策擴及整個 OU 或組織之前，最好先了解將簡單標籤政策連接至單一帳戶的效果。在您強制符合任何標籤政策之前，尤其要了解標籤政策的效果。[開始使用標籤政策](#) 頁面上的表格也提供連結來說明更進階政策的相關任務。

使用標籤政策的最佳實務

AWS 建議使用下列標籤政策的最佳實務。

決定標籤大寫策略

決定標籤如何使用大寫，並對所有資源類型一致地實作該策略。例如，決定要使用 Costcenter、costcenter 還是 CostCenter，並針對所有標籤使用相同的慣例。為了讓合規報告產生一致的結果，請避免使用大小寫處理不一致的相似標籤。此策略可協助您定義組織的標籤政策。

使用建議的工作流程

從小的開始，建立簡單的標籤政策。然後連接至可用於測試的成員帳戶。使用[開始使用標籤政策](#)中所述的工作流程。

決定標籤規則

這將取決於您組織的需求。例如，您可能想要指定當CostCenter標籤連接至 AWS Secrets Manager 秘密時，必須使用指定的大小寫處理。建立標籤政策來定義合規標籤，並將標籤政策連接至您希望這些標記規則生效的組織實體。

教導帳戶管理員

當您準備擴大使用標籤政策時，請教導帳戶管理員，如下所示：

- 傳達您的標記策略。
- 強調指出管理員需要在特定資源類型上使用標籤。

這很重要，因為未標記的資源在合規結果中不會顯示為不合規。

- 提供指引來檢查是否符合標籤政策。指示管理員使用標記資源使用者指南中的[評估帳戶的合規](#)中所述程序，在其帳戶中尋找和更正資源的不合規標籤。AWS 讓他們知道您希望他們多久檢查一次合規性。

強制合規性時請小心。

強制合規性可能會使組織帳戶中的使用者無法標記他們所需的資源。檢閱[了解強制](#)中的資訊。另請參閱[開始使用標籤政策](#)中所述的工作流程。

考慮建立 SCP 以防護資源建立請求

從未貼上標籤的資源在報告中不會顯示為不合規。帳戶管理員仍然可以建立未標記的資源。在某些情況下，您可以使用服務控制政策 (SCP) 來為資源建立請求設定防護。如需 SCP 範例，請參閱[需要在建立的指定資源上使用標籤](#)。

若要了解 AWS 服務是否支援使用標籤控制存取，請參閱《[AWS 服務 IAM 使用者指南](#)》中的使用 IAM。在 ABAC（根據標籤授權）欄中尋找具有是 的服務。選擇服務的名稱，以檢視該服務的授權和存取控制文件。

開始使用標籤政策

使用標籤政策涉及使用多個 AWS 服務。若要開始使用，請檢閱下列頁面。然後遵循此頁面上的工作流程，熟悉標籤政策及其效果。

- [的管理政策的先決條件和許可 AWS Organizations](#)
- [使用標籤政策的最佳實務](#)

第一次使用標籤政策

請依照下列步驟，開始首次使用標籤政策。

任務	要登入的帳戶	AWS 要使用的服務主控台
步驟 1： 為您的組織啟用標籤政策。	組織的管理帳戶。 ¹	AWS Organizations
步驟 2： 建立標籤政策。 讓第一個標籤政策保持簡單。 以您要使用的大小寫處理輸入	組織的管理帳戶。 ¹	AWS Organizations

任務	要登入的帳戶	AWS 要使用的服務主控台
一個標籤鍵，所有其他選項都保留預設值。		
步驟 3：將標籤政策連接至可用於測試的單一成員帳戶。 您在下一個步驟必須登入此帳戶。	組織的管理帳戶。 ¹	AWS Organizations
步驟 4：建立一些含有合規標籤的資源，也建立一些含有不合規標籤的資源。	您用於測試的成員帳戶。	您感到自在的任何 AWS 服務。例如，您可以使用 AWS Secrets Manager 並遵循 建立基本秘密 中的程序，建立含有合規和不合規秘密的秘密。
步驟 5： 檢視有效的標籤政策並評估帳戶的合規狀態。	您用於測試的成員帳戶。	資源群組和建立資源 AWS 的服務。 如果您建立的資源含有合規和不合規標籤，您在結果中應該會看到不合規標籤。
步驟 6：重複過程來尋找並更正合規問題，直到測試帳戶中的資源符合標籤政策為止。	您用於測試的成員帳戶。	資源群組 和建立資源 AWS 的服務。
您可以隨時 評估組織整體合規性 。	組織的管理帳戶。 ¹	資源群組

¹ 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

擴大使用標籤政策

您可以依任何順序執行下列任務，以擴大使用標籤政策。

進階任務	要登入的帳戶	AWS 要使用的服務主控台
建立更進階的標籤政策。 請遵循與新手使用者相同的程序，但嘗試其他任務。例如，定義其他鍵或值，或為標籤鍵指定不同的大小寫處理方式。 您可以使用 理解管理政策繼承 和 標籤政策語法 中的資訊，建立更詳細的標籤政策。	組織的管理帳戶。 ¹	AWS Organizations
將標籤政策連接至其他帳戶或 OU。 將更多政策連接至帳戶，或帳戶隸屬的任何 OU 之後，請檢查 帳戶的有效標籤政策。	組織的管理帳戶。 ¹	AWS Organizations
建立 SCP 以在任何人建立新資源時要求標籤。如需範例，請參閱「需要在建立的指定資源上使用標籤」。	組織的管理帳戶。 ¹	AWS Organizations
當帳戶的合規狀態改變時，根據有效的標籤政策，持續評估帳戶的合規狀態。更正不合規標籤。	含有效標籤政策的成員帳戶。	資源群組 和建立資源 AWS 的服務。
評估組織整體合規性 。	組織的管理帳戶。 ¹	資源群組

¹ 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

第一次強制執行標籤政策

若要第一次強制執行標籤政策，請遵循類似於第一次使用標籤政策的工作流程，並使用測試帳戶。

⚠ Warning

強制合規性時請小心。請確定您了解使用標籤政策的效果，並遵循建議的工作流程。在擴大強制更多帳戶之前，請先在測試帳戶上測試強制的效果。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。如需詳細資訊，請參閱[了解強制](#)。

強制任務	要登入的帳戶	AWS 要使用的服務主控台
步驟 1： 建立標籤政策。 讓第一個強制的標籤政策保持簡單。以您要使用的大小寫處理輸入一個標籤鍵，然後選擇 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作) 選項。然後指定一個要強制執行標籤政策的資源類型。延續先前的範例，您可以選擇對 Secrets Manager 秘密強制執行標籤政策。	組織的管理帳戶。 ¹	AWS Organizations
步驟 2： 將標籤政策連接至單一測試帳戶。	組織的管理帳戶。 ¹	AWS Organizations
步驟 3：嘗試建立一些含有合規標籤的資源，也建立一些含有不合規標籤的資源。如果資源是含不合規標籤的標籤政策中所指定的類型，應該就不允許您在此資源上建立標籤。	您用於測試的成員帳戶。	您感到自在的任何 AWS 服務。例如，您可以使用 AWS Secrets Manager 並遵循 建立基本秘密 中的程序，建立含有合規和不合規秘密的秘密。
步驟 4： 根據有效的標籤政策，評估帳戶的合規狀態，並更正不合規標籤。	您用於測試的成員帳戶。	資源群組 和建立資源 AWS 的服務。

強制任務	要登入的帳戶	AWS 要使用的服務主控台
步驟 5：重複過程來尋找並更正合規問題，直到測試帳戶中的資源符合標籤政策為止。	您用於測試的成員帳戶。	資源群組 和建立資源 AWS 的服務。
您可以隨時 評估組織整體合規性 。	組織的管理帳戶。 ¹	資源群組

¹ 您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

使用 Amazon EventBridge 監控不合規標籤

您可以使用 Amazon EventBridge、先前的 Amazon CloudWatch Events 監控何時引入不合規標籤。在下列範例事件中，tag-policy-compliant 的 "false" 值表示新標籤不符合有效的標籤政策。

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-00000000aaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

您可以訂閱事件，並指定要監控的字串或模式。如需詳細資訊，請參閱 [《Amazon EventBridge 使用者指南》](#)。

了解強制

標籤政策可以指定在指定的資源類型上，強制執行不合規的標記操作。換句話說，防止完成指定的資源類型上不合規的標記請求。

Important

強制對於未使用標籤來建立的資源沒有影響。

若要強制要求符合標籤政策，請在[建立標籤政策](#)時執行下列其中一項動作：

- 從 Visual editor (視覺化編輯器) 索引標籤中，選取 [Prevent noncompliant operations for this tag \(防止對此標籤執行不合規操作\)](#)。
- 從 JSON 索引標籤中，使用 `enforced_for` 欄位。如需標籤政策語法的相關資訊，請參閱[標籤政策語法和範例](#)。

遵循以下最佳實務來強制符合標籤政策：

- 強制合規性時請小心 – 確定您了解使用標籤政策的效果，並遵循 [開始使用標籤政策](#) 中所述的建議工作流程。在擴大強制更多帳戶之前，請先在測試帳戶上測試強制的效果。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。
- 注意您可以強制的資源類型 – 您只能在[支援的資源類型](#)上強制符合標籤政策。當您使用視覺化編輯器建置標籤政策時，將會列出支援強制合規的資源類型。
- 了解與某些服務的互動 – 有些 AWS 服務 服務具有類似容器的資源群組，可自動為您建立資源，而標籤可以從一個服務中的資源傳播到另一個服務。例如，Amazon EC2 Auto Scaling 群組和 Amazon EMR 叢集上的標籤可自動傳播至包含的 Amazon EC2 執行個體。相較於 Auto Scaling 群組或 EMR 叢集，您對於 Amazon EC2 的標籤政策可能更嚴格。如果您啟用強制，標籤政策會防止標記資源，還可能禁止動態擴展和佈建。

下列各節說明如何尋找不符合規資源，並將其修正為合規。

主題

- [尋找帳戶的不合規資源 AWS Organizations](#)
- [使用更正資源中的不合規標籤 AWS Organizations](#)
- [使用產生整個組織的合規報告 AWS Organizations](#)

- [支援強制執行的服務和資源類型](#)

尋找帳戶的不合規資源 AWS Organizations

針對每個帳戶，您可以取得不合規資源的相關資訊。您應該從帳戶資源所在的每個區域執行此命令。

若要尋找具有標籤政策之帳戶的不合規資源，請執行下列命令，將結果儲存至 檔案：

```
$ aws resourcegroupstaggingapi get-resources --region us-east-1 \
  --include-compliance-details \
  --exclude-compliant-resources > outputfile.txt
```

使用 更正資源中的不合規標籤 AWS Organizations

找到不合規標籤後，請使用下列任何方法來更正。您登入的帳戶中，資源必須有不合規標籤：

- 使用建立不合規資源之 AWS 服務的主控制台或標記 API 操作。
- 使用 AWS Resource Groups [TagResources](#) 和 [UntagResources](#) 操作來新增符合有效政策的標籤，或移除不合規的標籤。

使用 產生整個組織的合規報告 AWS Organizations

您可以隨時產生報告，列出 AWS 帳戶 整個組織中 中所有已標記的資源。此報告顯示每個資源是否符合有效標籤政策。請注意，您對標籤政策或資源所做的變更，可能需要經過長達 48 小時，才會反映在組織整體合規報告中。例如，假設您有一個標籤政策為某個資源類型定義新的標準化標籤。如果該類型的資源沒有此標籤，則在報告中會顯示為合規，時間長達 48 小時。

只要組織的管理帳戶具有 Amazon S3 儲存貯體的存取權，您可以在 us-east-1 區域中從該帳戶產生報告。儲存貯體必須具有連接的儲存貯體政策，如[用於存放報告的 Amazon S3 儲存貯體政策](#)中所示。若要產生報告，請執行下列命令：

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

您每次可以產生一個報告。

此報告可能需要一些時間才能完成。您可以執行下列命令來檢查狀態：

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
  "Status": "SUCCEEDED"
```


}

當上述命令傳回 SUCCEEDED 時，您可以從 Amazon S3 儲存貯體開啟報告。

支援強制執行的服務和資源類型

下列服務和資源類型支援強制符合標籤政策功能：

服務名稱	資源類型	JSON 語法
Amazon API Gateway	- API 金鑰 - 網域名稱 - REST API 操作 - 階段	"apigateway:apikeys" "apigateway:domainnames" "apigateway:restapis" "apigateway:restapis/stages"
AWS Amplify	- 元件 - 主題	"amplifyuibuilder:app/environment/components" "amplifyuibuilder:app/environment/themes"
AWS AppConfig	- 應用程式 - 組態設定檔 - 部署 - 部署策略 - 環境	"appconfig:application" "appconfig:application/configurationprofile" "appconfig:application/environment/deployment" "appconfig:deploymentstrategy" "appconfig:application/environment"
AWS App Mesh	- 全部 - 閘道路由 - 網格 - 路由 - 虛擬閘道 - 虛擬節點	"appmesh:*" "appmesh:mesh/virtualGateway/gatewayRoute" "appmesh:mesh" "appmesh:mesh/virtualRouter/route" "appmesh:mesh/virtualGateway"

服務名稱	資源類型	JSON 語法
	• 虛擬路由器 • 虛擬服務	• "appmesh:mesh/virtualNode" • "appmesh:mesh/virtualRouter" • "appmesh:mesh/virtualService"
Amazon Athena	• 全部 • 工作群組	• "athena:*" • "athena:workgroup"
AWS Audit Manager	• 評估 • 評定架構 • 控制項	• "auditmanager:assessment " • "auditmanager:assessmentFramework " • "auditmanager:control "
AWS Backup	• 備份計劃 • 保存庫 • 閘道 • Hypervisor • VM	• "backup:backup-plan" • "backup:backup-vault" • "backup-gateway:gateway" • "backup-gateway:hypervisor" • "backup-gateway:vm"
AWS Batch	• 任務 • 任務定義 • 任務佇列	• "batch:job" • "batch:job-definition" • "batch:job-queue"
AWS BugBust	• 事件	• "bugbust:event"
AWS Certificate Manager	• 全部 • 憑證 • Private certificate authority	• "acm:*" • "acm:certificate" • "acm-pca:certificate-authority"

服務名稱	資源類型	JSON 語法
Amazon Chime	- 應用程式執行個體 - 頻道 - 媒體管道 - 會議 - SIP 媒體應用程式 - 使用者應用程式執行個體 - 語音連接器	"chime:app-instance" "chime:app-instance/channel" "chime:media-pipeline" "chime:meeting" "chime:sma" "chime:app-instance/user" "chime:vc"
AWS Clean Rooms	- 協作 - 設定的資料表 - 成員資格 - 設定的資料表關聯	"cleanrooms:collaboration" "cleanrooms:configuredtable" "cleanrooms:membership" "cleanrooms:membership/configuredtableassociation"
AWS Cloud9	環境	"cloud9:environment"
Amazon CloudFront	- 全部 - 發佈	"cloudfront:*" "cloudfront:distribution"
AWS CloudTrail	- 全部 - 追蹤	"cloudtrail:*" "cloudtrail:trail"
Amazon CloudWatch	- 全部 - 警示 - Contributor Insights 規則 - 指標串流	"cloudwatch:*" "cloudwatch:alarm" "cloudwatch:insight-rule" "cloudwatch:metric-stream"
Amazon CloudWatch Internet Monitor	監控	"internetmonitor:monitor"

服務名稱	資源類型	JSON 語法
Amazon CloudWatch Logs	- 目的地 - 日誌群組	"logs:destination" "logs:log-group"
Amazon CloudWatch Observability Access Manager	- 連結 - 接收	"oam:link" "oam:sink"
AWS CodeBuild	- 全部 - 專案	"codebuild:*" "codebuild:project"
Amazon CodeCatalyst	連線	"codecatalyst:connections"
AWS CodeCommit	- 全部 - 儲存庫	"codecommit:*" "codecommit:repository"
AWS CodePipeline	- 全部 - 動作類型 - 管道 - Webhook	"codepipeline:*" "codepipeline:actiontype" "codepipeline:pipeline" "codepipeline:webhook"
Amazon Cognito 身分	- 全部 - 身分集區	"cognito-identity:*" "cognito-identity:identitypool"
Amazon Cognito 使用者集區	- 全部 - 使用者集區	"cognito-idp:*" "cognito-idp:userpool"
Amazon Comprehend	- 全部 - 文件分類器 - 實體辨識器	"comprehend:*" "comprehend:document-classifier" "comprehend:entity-recognizer"

服務名稱	資源類型	JSON 語法
AWS Config	• 全部 • 彙整授權 • Config 彙整工具 • Config 規則	• "config:* • "config:aggregation-authori zation" • "config:config-aggregator" • "config:config-rule"
Amazon CodeGuru Reviewer	• 關聯	• "codeguru-reviewer:associat ion"
Amazon CodeGuru Security	• Scan	• "codeguru-security:scans"
CodeConnections	• 連線 • 主機	• "codestar-connections:conne ction" • "codestar-connections:host"
Amazon Connect	• 聯絡流程 • 整合關聯 • 佇列 • Quick Connect • 轉接設定檔 • 使用者	• "connect:instance/contact-f low" • "connect:instance/integration- association" • "connect:instance/queue" • "connect:instance/transfer- destination" • "connect:instance/routing-p rofile" • "connect:instance/agent"
Amazon Connect Wisdom	• 助理 • 關聯 • 內容 • 知識庫 • Session (工作階段)	• "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"

服務名稱	資源類型	JSON 語法
AWS Database Migration Service	• 全部 • 端點 • ES • Rep • Subgrp • 任務	• "dms:*" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"
Amazon Data Lifecycle Manager	• 政策	• "dlm:policy"
AWS Direct Connect	• 全部 • Dxcon • Dxlagn • Dxvif	• "directconnect:*" • "directconnect:dxcon" • "directconnect:dxlagn" • "directconnect:dxvif"
Amazon DynamoDB	• 全部 • 資料表	• "dynamodb:*" • "dynamodb:table"

服務名稱	資源類型	JSON 語法
Amazon EC2	• 容量保留 • 容量保留機群 • 電信業者閘道 • 用戶端 VPN 端點 • CoIP 集區 • 客戶閘道 • 專用主機 • DHCP 選項 • 出口限定網際網路閘道 • 彈性 IP • 事件視窗 • 匯出映像任務 • 匯出執行個體任務 • 機群 • FPGA Image • 主機保留 • 映像 • 匯入映像任務 • 匯入快照任務 • 執行個體 • Instance Connect Endpoint • 網際網路閘道 • IP 地址管理員 • IP Address Manager 外部資源驗證權杖 • IP Address Manager 集區	• "ec2:capacity-reservation" • "ec2:capacity-reservation-fleet" • "ec2:carrier-gateway" • "ec2:client-vpn-endpoint" • "ec2:coip-pool" • "ec2:customer-gateway" • "ec2:dedicated-host" • "ec2:dhcp-options" • "ec2:egress-only-internet-gateway" • "ec2:elastic-ip" • "ec2:instance-event-window" • "ec2:export-image-task" • "ec2:export-instance-task" • "ec2:fleet" • "ec2:fpga-image" • "ec2:host-reservation" • "ec2:image" • "ec2:import-image-task" • "ec2:import-snapshot-task" • "ec2:instance" • "ec2:instance-connect-endpoint" • "ec2:internet-gateway" • "ec2:ipam" • "ec2:ipam-external-resource-verification-token" • "ec2:ipam-pool"

服務名稱	資源類型	JSON 語法
	- IP Address Manager 資源探索 - IP Address Manager 資源探索關聯 - IP Address Manager 範圍 - IPv4 集區 - 金鑰對 - 啟動範本 - 本機閘道路由表 - 本機閘道路由表虛擬介面群組關聯 - 本機閘道路由表 VPC 關聯 - NAT 閘道 - 網路 ACL - 網路介面 - Network Insights 存取範圍 - Network Insights 存取範圍分析 - Network Insights 分析 - Network Insights 路徑 - 置放群組 - 字首清單 - 取代根磁碟區任務 - 預留執行個體	"ec2:ipam-resource-discovery" "ec2:ipam-resource-discovery-association" "ec2:ipam-scope" "ec2:ipv4pool-ec2" "ec2:key-pair" "ec2:launch-template" "ec2:local-gateway-route-table" "ec2:local-gateway-route-table-virtual-interface-group-association" "ec2:local-gateway-route-table-vpc-association" "ec2:natgateway" "ec2:network-acl" "ec2:network-interface" "ec2:network-insights-access-scope" "ec2:network-insights-access-scope-analysis" "ec2:network-insights-analysis" "ec2:network-insights-path" "ec2:placement-group" "ec2:prefix-list" "ec2:replace-root-volume-task" "ec2:reserved-instances" "ec2:route-table" "ec2:security-group"

服務名稱	資源類型	JSON 語法
	• 路由表 • 安全群組 • 快照 • Spot 機群請求 • Spot 執行個體請求 • 子網路 • 子網路 CIDR 保留 • 流量鏡像篩選條件 • 流量鏡像工作階段 • 流量鏡像目標 • 轉換閘道 • 傳輸閘道附件 • Transit Gateway Connect 對等 • Transit Gateway 多點傳送網域 • 傳輸閘道政策表 • 傳輸閘道路由表 • 傳輸閘道路由表公告 • 已驗證的存取端點 • 已驗證的存取群組 • 已驗證的存取執行個體 • 已驗證的存取信任提供者 • 資料量 • VPC 流程日誌 • VPC • VPC 端點	• "ec2:snapshot" • "ec2:spot-fleet-request" • "ec2:spot-instances-request" • "ec2:subnet" • "ec2:subnet-cidr-reservation" • "ec2:traffic-mirror-filter" • "ec2:traffic-mirror-session" • "ec2:traffic-mirror-target" • "ec2:transit-gateway" • "ec2:transit-gateway-attachment" • "ec2:transit-gateway-connect-peer" • "ec2:transit-gateway-multicast-domain" • "ec2:transit-gateway-policy-table" • "ec2:transit-gateway-route-table" • "ec2:transit-gateway-route-table-announcement" • "ec2:verified-access-endpoint" • "ec2:verified-access-group" • "ec2:verified-access-instance" • "ec2:verified-access-trust-provider" • "ec2:volume" • "ec2:vpc-flow-log" • "ec2:vpc" • "ec2:vpc-endpoint"

服務名稱	資源類型	JSON 語法
	• VPC 端點服務 • VPC 對等連線 • VPN 連接 • VPN 閘道	• "ec2:vpc-endpoint-service" • "ec2:vpc-peering-connection" • "ec2:vpn-connection" • "ec2:vpn-gateway"
Amazon EC2 資源回收筒	• 規則	• "rbin:rule"
AWS Elastic Beanstalk	• 應用程式 • 應用程式版本 • 組態範本 • 平台	• "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic Container Registry	• 儲存庫	• "ecr:repository"
Amazon Elastic Container Service	• 容量提供者 • 叢集 • 服務 • 任務定義 • 任務集	• "ecs:capacity-provider" • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"
Amazon Elastic File System	• 全部 • 檔案系統	• "elasticfilesystem:*" • "elasticfilesystem:file-system"
Amazon Elastic Kubernetes Service	• 叢集	• "eks:cluster"
Amazon Elastic 搜尋	• 網域	• "es:domain"

服務名稱	資源類型	JSON 語法
Amazon EMR	- 叢集 - 編輯器	"elasticmapreduce:cluster" "elasticmapreduce:editor"
Amazon EMR Serverless	應用程式	"emr-serverless:applications"
AWS 實體解析	- 匹配流程 - 結構描述映射	"entityresolution:matchingworkflow" "entityresolution:schemamapping"
Amazon ElastiCache	叢集	"elasticache:cluster"
Amazon EventBridge	- 全部 - 事件匯流排 - 規則	"events:*" "events:event-bus" "events:rule"
Amazon EventBridge Pipes	管道	"pipes:pipe"
Amazon EventBridge 排程器	排程群組	"scheduler:schedule-group"
Amazon Fraud Detector	- 偵測器 - 偵測器版本 - 模型 - 規則 - 變數	"frauddetector:detector" "frauddetector:detector-version" "frauddetector:model" "frauddetector:rule" "frauddetector:variable"
Amazon Global Accelerator	加速器	"globalaccelerator:accelerator"

服務名稱	資源類型	JSON 語法
Elastic Load Balancing	• 全部 • 接聽程式 • 接聽程式規則 • 負載平衡器 • 目標群組	• "elasticloadbalancing:*" • "elasticloadbalancing:listener" • "elasticloadbalancing:listener-rule" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"
Amazon FSx	• 全部 • 備份 • 檔案系統	• "fsx:*" • "fsx:backup" • "fsx:file-system"
Amazon GuardDuty	• 偵測器 • 篩選條件 • IP 集合 • 威脅情資集合	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"
AWS HealthLake	• 資料儲存	• "healthlake:datastore"

服務名稱	資源類型	JSON 語法
AWS HealthOmics	- 註解存放區 - 註解存放區版本 - 參考存放區 - 參考資料 - 執行 - 執行群組 - 序列存放區 - 讀取集合 - 變量存放區 - 工作流程	"omics:annotationStore" "omics:annotationStore/version" "omics:referenceStore" "omics:referenceStore/reference" "omics:run" "omics:runGroup" "omics:sequenceStore" "omics:sequenceStore/readSet" "omics:variantStore" "omics:workflow"
Amazon Inspector	篩選條件	"inspector2:filter "
AWS Identity and Access Management	- 執行個體描述檔 - MFA - OIDC 供應商 - 政策 - SAML 供應商 - 伺服器憑證	"iam:instance-profile" "iam:mfa" "iam:oidc-provider" "iam:policy" "iam:saml-provider" "iam:server-certificate"
AWS IoT Analytics	- 全部 - 頻道 - 資料集 - 資料儲存 - 管道	"iotanalytics:*" "iotanalytics:channel" "iotanalytics:dataset" "iotanalytics:datastore" "iotanalytics:pipeline"
AWS IoT Events	- 全部 - 偵測器模型 - 輸入	"iotevents:*" "iotevents:detectorModel" "iotevents:input"

服務名稱	資源類型	JSON 語法
AWS IoT Fleet Hub	應用程式	"iotfleethub:application"
AWS IoT SiteWise	- 資產 - 資產模型	"iotsitewise:asset" "iotsitewise:asset-model "
AWS IoT Greengrass	- 大量部署 - 連接器定義 - 核心定義 - 裝置定義 - 函數定義 - 記錄器定義 - 資源定義 - 訂閱定義	"greengrass:bulk" "greengrass:connectorsDefinition" "greengrass:coresDefinition" "greengrass:devicesDefinition" "greengrass:functionsDefinition" "greengrass:loggersDefinition" "greengrass:resourcesDefinition" "greengrass:subscriptionsDefinition"
AWS Key Management Service	- 全部 - 金鑰	"kms:*" "kms:key"
Amazon Kinesis	- 全部 - 應用程式	"kinesisanalytics:*" "kinesisanalytics:application"
Amazon Data Firehose	- 全部 - 交付串流	"firehose:*" "firehose:deliverystream"
AWS Lambda	- 全部 - 函式	"lambda:*" "lambda:function"
Amazon Macie	自訂資料識別碼	"macie2:custom-data-identifier"
Amazon MediaStore	容器	"mediastore:container"

服務名稱	資源類型	JSON 語法
Amazon MQ	- 代理程式 - 組態	"mq:broker" "mq:configuration"
Amazon Network Firewall	- 防火牆 - 防火牆政策 - 狀態規則群組 - 無狀態規則群組	"network-firewall:firewall" "network-firewall:firewall-policy" "network-firewall:stateful-rulegroup" "network-firewall:stateless-rulegroup"
Amazon OpenSearch Serverless	收集	"aoss:collection"
AWS Organizations	- 帳戶 - Organizational Unit (組織單位) - 政策 - 根帳戶	"organizations:account" "organizations:ou" "organizations:policy" "organizations:root"
Amazon Pinpoint SMS Voice V2	- 組態集合 - 選擇退出清單 - 電話號碼 - 集區 - 寄件者 Id	"sms-voice:configuration-set" "sms-voice:opt-out-list" "sms-voice:phone-number" "sms-voice:pool" "sms-voice:sender-id"

服務名稱	資源類型	JSON 語法
Amazon RDS	- 叢集參數群組 - 叢集端點 - 事件訂閱 - 資料庫選項群組 - DB parameter group (資料庫參數群組) - 資料庫代理 - 資料庫代理端點 - 預留資料庫執行個體 - 資料庫安全群組 - DB subnet group (資料庫子網路群組) - 目標群組	"rds:cluster-pg" "rds:cluster-endpoint" "rds:es" "rds:og" "rds:pg" "rds:db-proxy" "rds:db-proxy-endpoint" "rds:ri" "rds:secgrp" "rds:subgrp" "rds:target-group"
Amazon Redshift	- 全部 - 叢集 - 事件訂閱 - HSM 用戶端憑證 - HSM 組態 - 參數群組 - 快照 - 快照複製授予 - 快照排程 - 子網路群組	"redshift:*" "redshift:cluster" "redshift:eventsubscription" "redshift:hsmclientcertificate" "redshift:hsmconfiguration" "redshift:parametergroup" "redshift:snapshot" "redshift:snapshotcopygrant" "redshift:snapshotschedule" "redshift:subnetgroup"

服務名稱	資源類型	JSON 語法
Amazon Redshift Serverless	- 命名空間 - 工作群組	"redshift-serverless:namespace" "redshift-serverless:workgroup"
AWS Resource Access Manager	- 全部 - 資源共享	"ram:*" "ram:resource-share"
AWS Resource Groups	- 全部 - 群組	"resource-groups:*" "resource-groups:group"
Amazon Route 53	託管區域	"route53:hostedzone"
Amazon Route 53 Resolver	- 全部 - 解析程式端點 - 解析程式規則	"route53resolver:*" "route53resolver:resolver-endpoint" "route53resolver:resolver-rule"
Amazon S3	- 儲存貯體 - Storage Lens - Storage Lens 群組	"s3:bucket" "s3:storage-lens" "s3:storage-lens-group"

服務名稱	資源類型	JSON 語法
Amazon SageMaker AI	- App Image Config - Artifact - Context - 訓練工作 - 正在處理任務 - 模型套件群組 - 人力任務 UI - 模型套件 - 動作 - 管道 - 實驗 - 流程定義 - 專案	"sagemaker:app-image-config" "sagemaker:artifact" "sagemaker:context" "sagemaker:training-job" "sagemaker:processing-job " "sagemaker:model-package-group" "sagemaker:human-task-ui" "sagemaker:model-package" "sagemaker:action" "sagemaker:pipeline" "sagemaker:experiment" "sagemaker:flow-definition" "sagemaker:project"
AWS Secrets Manager	- 全部 - 秘密	"secretsmanager:*" "secretsmanager:secret"
AWS 安全湖	- 資料湖 - Subscriber	"securitylake:data-lake" "securitylake:subscriber"
AWS Service Catalog	- 應用程式 - 屬性群組 - 產品組合 - 產品	"servicecatalog:applications" "servicecatalog:attribute-groups " "catalog:portfolio " "catalog:product "
Amazon Simple Notification Service (SNS)	主題	"sns:topic"

服務名稱	資源類型	JSON 語法
Amazon Simple Queue Service (SQS)	佇列	"sqs:queue"
Amazon States Language	- 全部 - 活動 - State Machine (狀態機器)	"states:*" "states:activity" "states:stateMachine"
AWS Step Functions	活動	"states:activity"
AWS Storage Gateway	- 全部 - 閘道 - Share (分享) - 磁帶 - 資料量	"storagegateway:*" "storagegateway:gateway" "storagegateway:share" "storagegateway:tape" "storagegateway:gateway/volume"
AWS Systems Manager	- 關聯 - 自動化執行 - 文件 - 維護時段 - 受管的執行個體 - Ops 項目 - 修補基準 - 聯絡人	"ssm:association" "ssm:automation-execution" "ssm:document" "ssm:maintenancewindow" "ssm:managed-instance" "ssm:opsitem" "ssm:patchbaseline" "ssm-contacts:contact"
Amazon Textract	- 轉接器 - 版本	"textract:adapters" "textract:adapters/versions"
AWS 轉移系列	- Server - 使用者 - 工作流程	"transfer:server" "transfer:user" "transfer:workflow"

服務名稱	資源類型	JSON 語法
Amazon Well-Architected	工作負載	"wellarchitected:workload"
AWS Wickr	網路	"wickr:network"
Amazon WorkSpaces	- 全部 - 連線別名 - 目錄 - 工作空間 - WorkSpaces 服務包 - WorkSpaces 映像 - WorkSpaces IP 群組	"workspaces:*" "workspaces:connectionalias" "workspaces:directory" "workspaces:workspace" "workspaces:workspacebundle" "workspaces:workspaceimage" "workspaces:workspaceipgroup"

標籤政策語法和範例

此頁面說明標籤政策語法並提供範例。

標籤政策語法

標籤政策是根據 [JSON](#) 規則建構的純文字檔。標籤政策的語法遵循管理政策類型的語法。如需該語法的完整討論，請參閱[理解管理政策繼承](#)。本主題著重於以該一般語法滿足標籤政策類型的特定需求。

下列標籤政策顯示基本的標籤政策語法：

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "100",
          "200"
        ]
      }
    }
  }
}
```

```
    },
    "enforced_for": {
      "@@assign": [
        "secretsmanager:*"
      ]
    }
  }
}
```

標籤政策語法包括下列元件：

- `tags` 欄索引鍵名稱。標籤政策一律以此固定索引鍵名稱開頭。這是上面範例政策的第一行。
- 唯一識別政策陳述式的政策索引鍵。必須符合「標籤鍵」的值 (大小寫處理除外)。政策值區分大小寫。

在此範例中，`costcenter` 是政策索引鍵。

- 至少有一個標籤鍵，指定允許的標籤鍵含有您希望資源符合的大寫。如果沒有定義大小寫處理，則小寫為標籤鍵的預設大小寫處理。標籤鍵的值必須符合政策鍵的值。但由於政策索引鍵值不區分大小寫，大寫可能有所不同。

在此範例中，`CostCenter` 是標籤鍵。這是符合標籤政策規範的大小寫處理。此標籤鍵具有替代大小寫處理的資源，不符合標籤政策規範。

您可以在標籤政策中定義多個標籤鍵。

- (選用) 標籤鍵可接受的一或多個標籤值的清單。如果標籤政策未指定標籤鍵的標籤值，則任何值 (包括完全沒有值) 都視為合規。

在此範例中，`CostCenter` 標籤鍵的可接受值為 100 和 200。

- (選用) `enforced_for` 選項，指出是否防止對指定的服務和資源執行任何不合規的標記操作。在主控台，這是視覺化編輯器中用於建立標籤政策的 Prevent noncompliant operations for this tag (防止對此標籤執行不合規操作) 選項。此選項的預設設定為 `null`。

標籤政策範例指定所有 AWS Secrets Manager 資源上傳遞的 `CostCenter` 標籤必須符合此政策。

Warning

只有在您使用標籤政策很有經驗時，才應該變更此選項的預設值。否則，可能會使組織帳戶中的使用者無法建立他們所需的資源。

- 運算子，指定標籤政策如何與組織樹狀結構中的其他標籤政策合併，以建立帳戶的[有效的標籤政策](#)。此範例中使用 `@@assign`，將字串指定給 `tag_key`、`tag_value` 和 `enforced_for`。如需運算子的詳細資訊，請參閱 [繼承運算子](#)。
- – 您可以在標籤值和 `enforced_for` 欄位中使用 * 萬用字元：
 - 每個標籤值中只能使用一個萬用字元。例如，允許 `*@example.com`，但不允許 `*@*.com`。
 - 對於 `enforced_for`，您可以對某些服務搭配使用 `<service>:*`，以對該服務的所有資源啟用強制執行。如需支援 `enforced_for` 的服務和資源類型清單，請參閱 [支援強制執行的服務和資源類型](#)。

萬用字元無法用來指定所有服務，也無法用來指定所有服務的某些資源。

標籤政策範例

接下來的範例[標籤政策](#)僅供參考。

Note

在您嘗試在組織中使用這些範例標籤政策之前，請注意下列事項：

- 請確定您已按照[建議的工作流程](#)開始使用標籤政策。
- 您應該仔細檢閱和自訂這些標籤政策，以滿足您的獨特需求。
- 標籤政策中的所有字元都受制於[大小上限](#)。本指南中的範例添加額外空格來顯示標籤政策，以改善可讀性。不過，如果政策大小接近大小上限，為了節省空間，您可以刪除任何空格。空白字元的例子包括引號外面的空格字元和換行符號。
- 未標記的資源由於不合規而無法出現在結果中。

範例 1：定義整個組織的標籤鍵大小寫

下列範例顯示的標籤政策只定義兩個標籤鍵，以及您希望組織中的帳戶標準化所依據的大小寫。

政策 A – 組織根標籤政策

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter",
```

```

        "@operators_allowed_for_child_policies": ["@none"]
    },
    "Project": {
        "tag_key": {
            "@assign": "Project",
            "@operators_allowed_for_child_policies": ["@none"]
        }
    }
}

```

此標籤政策定義兩個標籤鍵：CostCenter 和 Project。將此標籤政策連接至組織根，會產生下列影響：

- 組織中的所有帳戶都會繼承此標籤政策。
- 組織中所有帳戶都必須使用已定義的大小寫處理以符合規範。具有 CostCenter 和 Project 標籤的資源符合規範。標籤鍵具有替代大小寫處理的資源 (例如 costcenter、Costcenter 或 COSTCENTER) 不符合規範。
- "@operators_allowed_for_child_policies": ["@none"] 行會封鎖標籤鍵。在組織樹狀結構中較下方連接的標籤政策 (子政策)，不能使用值-設定運算子來變更標籤鍵 (包括其大小寫處理)。
- 與所有標籤政策一樣，對於未標記的資源或標籤政策中未定義的標籤，不會評估是否符合標籤政策規範。

AWS 建議您使用此範例做為為您要使用的標籤金鑰建立類似標籤政策的指南。將此標籤政策連接至組織根目錄。然後，建立類似於下一個範例的標籤政策，只為已定義的標籤鍵定義可接受的值。

下一步：定義值

假設您已將先前的標籤政策連接至組織根。接下來，您可以建立如下所示的標籤政策，並連接至帳戶。此政策定義 CostCenter 和 Project 標籤鍵可接受的值。

政策 B – 帳戶標籤政策

```

{
    "tags": {
        "CostCenter": {
            "tag_value": {

```

```

        "@@assign": [
            "Production",
            "Test"
        ]
    },
    "Project": {
        "tag_value": {
            "@@assign": [
                "A",
                "B"
            ]
        }
    }
}

```

如果您將政策 A 連接至組織根，將政策 B 連接至帳戶，則這些政策合併起來，為帳戶建立下列有效的標籤政策：

政策 A + 政策 B = 帳戶的有效標籤政策

```

{
  "tags": {
    "Project": {
      "tag_value": [
        "A",
        "B"
      ],
      "tag_key": "Project"
    },
    "CostCenter": {
      "tag_value": [
        "Production",
        "Test"
      ],
      "tag_key": "CostCenter"
    }
  }
}

```

如需政策繼承的詳細資訊，包括繼承運算子運作方式的範例，以及有效的標籤政策範例，請參閱 [理解管理政策繼承](#)。

範例 2：禁止使用標籤鍵

若要禁止使用標籤鍵，您可以將如下所示的標籤政策連接至組織實體。

此範例政策指定 Color 標籤鍵不接受任何值。也會指定在子標籤政策中不允許[運算子](#)。因此，在受影響帳號中，資源上的任何 Color 標籤都會被系統視為不相容。然而，enforced_for 選項實際上會阻止受影響帳戶僅標記使用 Color 標籤的 Amazon DynamoDB 資料表。

```
{
  "tags": {
    "Color": {
      "tag_key": {
        "@operators_allowed_for_child_policies": [
          "@none"
        ],
        "@assign": "Color"
      },
      "tag_value": {
        "@operators_allowed_for_child_policies": [
          "@none"
        ],
        "@assign": []
      },
      "enforced_for": {
        "@assign": [
          "dynamodb:table"
        ]
      }
    }
  }
}
```

支援地區

下列區域可使用標籤政策功能：

區域名稱	區域參數
美國東部 (維吉尼亞北部) 區域 ¹	us-east-1
美國東部 (俄亥俄) 區域	us-east-2

區域名稱	區域參數
美國西部 (加利佛尼亞北部) 區域	us-west-1
美國西部 (奧勒岡) 區域	us-west-2
非洲 (開普敦) 區域 ²	af-south-1
亞太區域 (香港) 區域 ²	ap-east-1
亞太 (孟買) 區域	ap-south-1
亞太區域 (海德拉巴) 2	ap-south-2
亞太區域 (東京) 區域	ap-northeast-1
亞太區域 (首爾) 區域	ap-northeast-2
亞太 (大阪) 區域	ap-northeast-3
亞太區域 (新加坡) 區域	ap-southeast-1
亞太區域 (雪梨) 區域	ap-southeast-2
亞太區域 (雅加達) 區域 2	ap-southeast-3
亞太區域 (馬來西亞) 區域	ap-southeast-5
亞太區域 (墨爾本) 2	ap-southeast-4
亞太區域 (泰國)	ap-southeast-7
加拿大 (中部) 區域	ca-central-1
加拿大西部 (卡加利) 2	ca-west-1
中國 (北京) 區域	cn-north-1
中國 (寧夏) 區域	cn-northwest-1
歐洲 (法蘭克福) 區域	eu-central-1

區域名稱	區域參數
歐洲 (蘇黎世) 區域 2	eu-central-2
歐洲 (米蘭) 區域 ²	eu-south-1
歐洲 (西班牙) 2	eu-south-2
歐洲 (愛爾蘭) 區域	eu-west-1
歐洲 (倫敦) 區域	eu-west-2
歐洲 (巴黎) 區域	eu-west-3
歐洲 (斯德哥爾摩) 區域	eu-north-1
墨西哥 (中部) 區域	mx-central-1
中東 (巴林) 區域 ²	me-south-1
南美洲 (聖保羅) 區域	sa-east-1
以色列 (特拉維夫) 2	il-central-1
AWS GovCloud (美國東部) 區域	us-gov-east-1
AWS GovCloud (美國西部) 區域	us-gov-west-1

¹呼叫下列 Organizations 操作時，您必須指定 **us-east-1** 區域：

- [DeletePolicy](#)
- [DisablePolicyType](#)
- [EnablePolicyType](#)
- 在組織根上的任何其他操作，例如 [ListRoots](#)。

呼叫下列 Resource Groups 標記 API 操作時 (標籤政策功能的一部分)，您也必須指定 **us-east-1** 區域：

- [DescribeReportCreation](#)

- [GetComplianceSummary](#)
- [StartReportCreation](#)

Note

若要評估整個組織是否符合標籤政策，您還必須具有美國東部 (維吉尼亞北部) 區域中 Amazon S3 儲存貯體的存取權以便儲存報告。如需詳細資訊，請參閱《標記 AWS 資源使用者指南》中的[報告儲存的 Amazon S3 儲存貯體政策](#)。

²必須手動啟用這些區域。若要進一步了解如何啟用和停用 AWS 區域，請參閱[《帳戶管理參考指南》中的指定您的帳戶可以使用哪些 AWS 區域](#)。AWS 在這些區域中無法使用 Resource Groups 主控台。

聊天應用程式政策

中的聊天應用程式政策 AWS Organizations 可讓您控制從聊天應用程式存取組織的帳戶，例如 Slack 和 Microsoft Teams。

[聊天應用程式中的 Amazon Q Developer](#) AWS 是一項服務，可讓 DevOps 和軟體開發團隊使用簡訊程式聊天室來監控和回應其中的操作事件 AWS 雲端。聊天應用程式中的 Amazon Q Developer 會處理來自 Amazon Simple Notification Service (Amazon SNS) 的 AWS 服務通知，並將其轉送至聊天室，讓團隊可以立即分析並採取行動，無論位置為何。

聊天應用程式政策的運作方式

使用聊天應用程式政策，組織的管理帳戶或委派管理員可以在組織中執行下列動作：

- 強制執行可以使用哪些支援的聊天應用程式 (Amazon Chime、Microsoft Teams 和 Slack)。
- 限制聊天用戶端存取特定工作區 (Slack) 和團隊 (Microsoft Teams)。
- 將 Slack 頻道可見性限制為公有或私有頻道。
- 設定和強制執行特定[角色設定](#)。

聊天應用程式政策會限制並優先於帳戶層級設定，例如[角色設定](#)和[頻道護欄政策](#)。您可以在聊天應用程式或 Organizations 主控台中，從 Amazon Q Developer 存取和修改聊天應用程式政策。

政策連接到帳戶和組織單位 (OU) 之後，範圍內帳戶聊天應用程式組態中的任何目前和未來 Amazon Q Developer 將自動符合控管和許可設定。如需詳細資訊，請參閱[了解管理政策繼承](#)。

如果您嘗試執行受聊天應用程式政策限制的動作，錯誤訊息會通知您，由於聊天應用程式政策建議聯絡組織的管理帳戶或委派管理員，不允許該動作。

Note

聊天應用程式政策會在執行時間驗證。這表示會持續檢查現有資源的合規性。由於目前不支援在聊天應用程式中傳送通知或與 Amazon Q Developer 互動的執行時間型 IAM 許可，因此不會與現有的 IAM 許可重疊。

聊天應用程式政策入門

請依照下列步驟開始使用聊天應用程式政策。

1. [了解執行聊天應用程式政策任務所需的許可](#)。
2. [為您的組織啟用聊天應用程式政策](#)。
3. [建立聊天應用程式政策](#)。
4. [將聊天應用程式政策連接至組織的根、OU 或帳戶](#)。
5. [檢視套用至 帳戶的合併有效聊天應用程式政策](#)。

對於所有這些步驟，請以 IAM 使用者身分登入、擔任 IAM 角色，或以組織管理帳戶中的根使用者身分登入 ([不建議](#))。

其他資訊

- [了解聊天應用程式政策語法，並查看範例政策](#)

聊天應用程式政策語法和範例

本主題說明聊天應用程式政策語法並提供範例。

聊天應用程式政策的語法

聊天應用程式政策是根據 [JSON](#) 規則建構的純文字檔案。聊天應用程式政策的語法遵循管理政策類型的語法。如需該語法的完整討論，請參閱[理解管理政策繼承](#)。本主題著重於將該一般語法套用至聊天應用程式政策類型的特定需求。

下列範例顯示聊天應用程式政策的基本語法：

```

{
  "chatbot":{
    "platforms":{
      "slack":{
        "client":{
          "@@assign":"enabled" // enabled | disabled
        },
        "workspaces": { // limit 255
          "@@assign":[
            "Slack-Workspace-Id"
          ]
        },
        "default":{
          "supported_channel_types":{
            "@@assign":[
              "private" // public | private
            ]
          },
          "supported_role_settings":{
            "@@assign":[
              "user_role" // user_role | channel_role
            ]
          }
        },
        "overrides":{ // limit 255
          "Slack-Workspace-Id":{
            "supported_channel_types":{
              "@@assign":[
                "public" // public | private
              ]
            },
            "supported_role_settings":{
              "@@assign":[
                "user_role" // user_role | channel_role
              ]
            }
          }
        }
      },
      "microsoft_teams":{
        "client":{
          "@@assign":"enabled"
        },

```

```

    "tenants":{ // limit 36
      "Microsoft-Teams-Tenant-Id":{ // limit 36
        "@@assign":[
          "Microsoft-Teams-Team-Id"
        ]
      }
    },
    "default":{
      "supported_role_settings":{
        "@@assign":[
          "user_role" // user_role | channel_role
        ]
      }
    },
    "overrides":{ // limit 36
      "Microsoft-Teams-Tenant-Id":{ // limit 36
        "Microsoft-Teams-Team-Id":{
          "supported_role_settings":{
            "@@assign":[
              "user_role" // user_role | channel_role
            ]
          }
        }
      }
    },
    "chime":{
      "client":{
        "@@assign":"disabled" // enabled | disabled
      }
    },
    "default":{
      "client":{
        "@@assign":"disabled" // enabled | disabled
      }
    }
  }
}

```

此聊天應用程式政策包含下列元素：

- chatbot 欄索引鍵名稱。聊天應用程式政策一律從此固定金鑰名稱開始。這是此範例政策的頂端。

- 在下 chatbot 有一個 platforms 區塊，其中包含不同支援聊天應用程式的組態：Slack、Microsoft Teams 和 Amazon Chime。
- 對於 Slack，可使用下列欄位：
 - "client":
 - "enabled"：Slack 用戶端已啟用。允許 Slack 整合。
 - "disabled"：Slack 用戶端已停用。不允許 Slack 整合。
 - "workspaces"：允許 Slack 工作區的逗號分隔清單。在此範例中，允許的 Slack 工作區為 *Slack-Workspace-Id1* 和 *Slack-Workspace-Id2*。
 - "default"：Slack 工作區的預設設定。
 - "supported_channel_types":
 - "public"：範圍內的 Slack 工作區預設允許公有 Slack 頻道。
 - "private"：範圍內的 Slack 工作區預設允許私有 Slack 頻道。
 - supported_role_settings:
 - "user_role"：範圍內的 Slack 工作區預設允許使用者層級 IAM 角色。
 - "channel_role"：範圍內的 Slack 工作區預設允許頻道層級 IAM 角色。
 - "overrides"：Slack 工作區的覆寫設定。
 - *Slack-Workspace-Id2*：以逗號分隔的 Slack 工作區清單，其中套用覆寫設定。在此範例中，Slack 工作區為 *Slack-Workspace-Id2*。
 - "supported_channel_types":
 - "public"：覆寫範圍內的 Slack 工作區是否允許公有 Slack 頻道的設定。
 - "private"：覆寫範圍內的 Slack 工作區是否允許私有 Slack 頻道的設定。
 - supported_role_settings:
 - "user_role"：覆寫範圍內的 Slack 工作區是否允許使用者層級 IAM 角色的設定。
 - "channel_role"：覆寫範圍內的 Slack 工作區是否允許頻道層級 IAM 角色的設定。
- 對於 Microsoft Teams，可使用下列欄位：
 - "client":
 - "enabled"：Microsoft Teams 用戶端已啟用。允許 Microsoft Teams 整合。
 - "disabled"：Microsoft Teams 用戶端已停用。不允許 Microsoft Teams 整合。
 - "tenants"：允許 Microsoft Teams 租用戶的逗號分隔清單。在此範例中，允許的租用戶為 *Microsoft-Teams-Tenant-Id*。

- *Microsoft-Teams-Tenant-Id*：租用戶內允許的團隊逗號分隔清單。在此範例中，允許的團隊為 *Microsoft-Teams-Team-Id*。
- "default"：租用戶內團隊的預設設定。
 - supported_role_settings:
 - "user_role"：範圍內的團隊預設允許使用者層級 IAM 角色。
 - "channel_role"：範圍內的團隊預設允許頻道層級 IAM 角色。
 - "overrides"：Microsoft Teams 租用戶的覆寫設定。
 - *Microsoft-Teams-Tenant-Id*：以逗號分隔的租用戶清單，其中套用覆寫設定。在此範例中，租用戶為 *Microsoft-Teams-Tenant-Id*。
 - *Microsoft-Teams-Team-Id*：以逗號分隔租用戶內的團隊清單。在此範例中，允許的團隊為 *Microsoft-Teams-Team-Id*。
 - supported_role_settings:
 - "user_role"：覆寫範圍內的團隊是否允許使用者層級 IAM 角色的設定。
 - "channel_role"：覆寫範圍內的團隊是否允許頻道層級 IAM 角色的設定。
 - 對於 Amazon Chime，可使用下列欄位：
 - "client":
 - "enabled"：Amazon Chime 用戶端已啟用。允許 Amazon Chime 整合。
 - "disabled"：Amazon Chime 用戶端已停用。不允許 Amazon Chime 整合。
 - 在下 chatbot，有一個 default 區塊，除非在較低層級覆寫，否則會停用整個組織中聊天應用程式中的 Amazon Q Developer。此預設值也會停用聊天應用程式中 Amazon Q Developer 支援的任何新聊天應用程式。例如，如果聊天應用程式中的 Amazon Q Developer 支援新的聊天應用程式，則此預設也會停用該新支援的聊天應用程式。

Note

如需頻道層級 IAM 角色和使用者層級 IAM 角色的詳細資訊，請參閱 [《聊天應用程式管理員指南》](#) 中的 [了解聊天應用程式中的 Amazon Q 開發人員許可](#)。

聊天應用程式政策範例

接下來的政策範例僅供參考。

範例 1：僅允許特定工作區中的私有 Slack 頻道、停用 Microsoft Teams、所有支援的身分驗證模式

下列政策著重於控制 Slack 和 Microsoft Teams 聊天機器人整合的允許組態。

```
{
  "chatbot": {
    "platforms": {
      "slack": {
        "client": {
          "@@assign": "enabled"
        },
        "workspaces": {
          "@@assign": [
            "Slack-Workspace-Id"
          ]
        },
        "default": {
          "supported_channel_types": {
            "@@assign": [
              "private"
            ]
          },
          "supported_role_settings": {
            "@@assign": [
              "channel_role",
              "user_role"
            ]
          }
        }
      }
    },
    "microsoft_teams": {
      "client": {
        "@@assign": "disabled"
      }
    },
    "chime": {
      "client": {
        "@@assign": "disabled"
      }
    },
    "default": {
      "client": {
        "@@assign": "disabled"
      }
    }
  }
}
```

```
}  
  }  
}  
}
```

對於 Slack

- Slack 用戶端已啟用。
- 僅允許特定的 Slack 工作區 *Slack-Workspace-Id*。
- 預設設定為僅允許私有 Slack 頻道、頻道層級 IAM 角色和使用者層級 IAM 角色。

適用於 Microsoft 團隊

- Microsoft Teams 用戶端已停用。

對於 Amazon Chime

- Amazon Chime 用戶端已停用。

其他詳細資訊

- 底部的 default 區塊會將用戶端設定為停用，這會停用整個組織中聊天應用程式中的 Amazon Q Developer，除非在較低層級覆寫。此預設值也會停用聊天應用程式中 Amazon Q Developer 支援的任何新聊天應用程式。例如，如果聊天應用程式中的 Amazon Q Developer 支援新的聊天應用程式，則此預設也會停用該新支援的聊天應用程式。

範例 2：僅允許與使用者層級 IAM 角色的 Slack 整合

下列政策對 Slack 採取更寬鬆的方法，允許所有 Slack 工作區，但將身分驗證模式限制為僅限使用者層級 IAM 角色。

```
{  
  "chatbot":{  
    "platforms":{  
      "slack":{  
        "client":{  
          "@@assign":"enabled"  
        },  
      },  
    },  
  },  
}
```

```

        "workspaces":
        {
            "@@assign":[
                "*"
            ]
        },
        "default":{
            "supported_role_settings":{
                "@@assign":[
                    "user_role"
                ]
            }
        }
    },
    "microsoft_teams":{
        "client":{
            "@@assign":"disabled"
        }
    },
    "chime":{
        "client":{
            "@@assign":"disabled"
        }
    }
},
"default":{
    "client":{
        "@@assign":"disabled"
    }
}
}
}

```

對於 Slack

- Slack 用戶端已啟用。
- 沒有使用萬用字元 定義特定的 Slack 工作區 "*"，因此允許所有工作區。
- 預設設定為僅允許使用者層級 IAM 角色。

適用於 Microsoft 團隊

- Microsoft Teams 用戶端已停用。

對於 Amazon Chime

- Amazon Chime 用戶端已停用。

其他詳細資訊

- 底部的 default 區塊會將用戶端設定為停用，這會停用整個組織中聊天應用程式中的 Amazon Q Developer，除非在較低層級覆寫。此預設值也會停用聊天應用程式中 Amazon Q Developer 支援的任何新聊天應用程式。例如，如果聊天應用程式中的 Amazon Q Developer 支援新的聊天應用程式，則此預設也會停用該新支援的聊天應用程式。

範例 3：只允許特定租用戶中的 Microsoft Teams 整合

下列範例政策會鎖定組織，僅允許 Microsoft Teams 聊天機器人在指定的租用戶內整合，同時完全封鎖 Slack 整合。

```
{
  "chatbot": {
    "platforms": {
      "slack": {
        "client": {
          "@@assign": "disabled"
        },
      },
      "microsoft_teams": {
        "client": {
          "@@assign": "enabled"
        },
        "tenants": {
          "Microsoft-Teams-Tenant-Id": {
            "@@assign": [
              "*"
            ]
          }
        }
      },
    },
    "chime": {
      "client": {
        "@@assign": "disabled"
      }
    }
  }
}
```

```
}  
}  
}
```

對於 Slack

- Slack 用戶端已停用。

適用於 Microsoft 團隊

- 僅允許特定租用戶 *Microsoft-Teams-Tenant-Id*，使用萬用字元 "*" 允許該租用戶中的所有團隊。

對於 Amazon Chime

- Amazon Chime 用戶端已停用。

其他詳細資訊

- 底部的 default 區塊會將用戶端設定為停用，這會停用整個組織中聊天應用程式中的 Amazon Q Developer，除非在較低層級覆寫。此預設值也會停用聊天應用程式中 Amazon Q Developer 支援的任何新聊天應用程式。例如，如果聊天應用程式中的 Amazon Q Developer 支援新的聊天應用程式，則此預設也會停用該新支援的聊天應用程式。

範例 4：允許聊天應用程式中受限的 Amazon Q Developer 存取 Slack 工作區和 Microsoft Teams 租用戶

下列政策允許聊天應用程式中受限的 Amazon Q Developer 存取所選 Slack 工作區和 Microsoft Teams 租用戶。

```
{  
  "chatbot": {  
    "platforms": {  
      "slack": {  
        "client": {  
          "@@assign": "enabled"  
        },  
        "workspaces": {  
          "@@assign": [  

```

```

        "Slack-Workspace-Id1",
        "Slack-Workspace-Id2"
    ]
},
"default":{
    "supported_channel_types":{
        "@@assign":[
            "private"
        ]
    },
    "supported_role_settings":{
        "@@assign":[
            "user_role"
        ]
    }
},
"overrides":{
    "Slack-Workspace-Id2":{
        "supported_channel_types":{
            "@@assign":[
                "public",
                "private"
            ]
        },
        "supported_role_settings":{
            "@@assign":[
                "channel_role",
                "user_role"
            ]
        }
    }
},
"microsoft_teams":{
    "client":{
        "@@assign":"enabled"
    },
    "tenants":{
        "Microsoft-Teams-Tenant-Id":{
            "@@assign":[
                "Microsoft-Teams-Team-Id"
            ]
        }
    }
},

```

```

    "default":{
      "supported_role_settings":{
        "@@assign":[
          "user_role"
        ]
      }
    },
    "overrides":{
      "Microsoft-Teams-Tenant-Id":{
        "Microsoft-Teams-Team-Id":{
          "supported_role_settings":{
            "@@assign":[
              "channel_role",
              "user_role"
            ]
          }
        }
      }
    }
  },
  "default":{
    "client":{
      "@@assign":"disabled"
    }
  }
}

```

對於 Slack

- Slack 用戶端已啟用。
- 允許 Slack 工作區為 *Slack-Workspace-Id1* 和 *Slack-Workspace-Id2*。
- Slack 的預設設定為僅允許私有頻道和使用者層級 IAM 角色。
- 工作區 *Slack-Workspace-Id2* 有一個覆寫，允許公有和私有頻道，以及頻道層級 IAM 角色和使用者層級 IAM 角色。

適用於 Microsoft 團隊

- Microsoft Teams 已啟用。
- 允許團隊租用戶為 *Microsoft-Teams-Tenant-Id*，團隊為 *Microsoft-Teams-Team-Id*。

- 預設設定為僅允許使用者層級 IAM 角色。
- 租用戶 *Microsoft-Teams-Tenant-Id* 有覆寫，允許團隊 *Microsoft-Teams-Team-Id* 的頻道層級 IAM 角色和使用者層級 IAM 角色。

其他詳細資訊

- 底部的 default 區塊會將用戶端設定為停用，這會停用整個組織中聊天應用程式中的 Amazon Q Developer，除非在較低層級覆寫。這表示在此範例中已停用 Amazon Chime。此預設值也會停用聊天應用程式中 Amazon Q Developer 支援的任何新聊天應用程式。例如，如果聊天應用程式中的 Amazon Q Developer 支援新的聊天應用程式，則此預設也會停用該新支援的聊天應用程式。

AI 服務選擇退出政策

AI 服務選擇退出政策可讓您控制組織中所有帳戶的 AWS AI 服務資料收集。

AWS AI 服務可能會使用和存放客戶內容，以改善服務。服務改進是使用和儲存非[個人資料](#)的內容，以開發和改善 AWS 和附屬機器學習和人工智慧技術。因此，我們可能會將內容存放在 AWS 區域 您使用服務的 AWS 區域 外部。身為 AWS 客戶，您可以隨時選擇不讓內容用於改善服務。

您可以為個別 AI 服務或 AI 服務選擇退出政策支援的所有服務建立選擇退出政策。您也可以查詢適用於每個帳戶的有效政策，以查看設定選項的效果。

如需詳細資訊，請參閱《AWS 服務條款》中的[AWS Machine Learning和人工智慧服務](#)。如需 AI 服務選擇退出政策支援的服務清單，請參閱[支援的 AI 服務清單](#)。

主題

- [使用 AI 服務選擇退出政策時的考量事項](#)
- [開始使用 AI 服務選擇退出政策](#)
- [選擇退出所有支援的 AWS AI 服務](#)
- [AI 服務選擇退出政策語法和範例](#)

使用 AI 服務選擇退出政策時的考量事項

選擇退出會刪除所有相關聯的歷史內容

當您選擇退出 AWS AI 服務的內容使用時，該服務會刪除在您設定 選項 AWS 之前與 共用的所有相關歷史內容。此刪除僅限於儲存的資料，而這些資料並非提供服務功能的必要項目。

例如，您在選擇加入時使用服務。該服務可能會儲存該內容的複本，以改善服務。您選擇退出。服務為了改善服務而存放的任何副本都會遭到刪除，但不會刪除用來為您提供服務的任何資料。

開始使用 AI 服務選擇退出政策

請依照下列步驟開始使用人工智慧 (AI) 服務選擇退出政策。

1. [了解執行備份政策任務所需的許可](#)
2. [為您的組織啟用 AI 服務選擇退出政策。](#)
3. [建立 AI 服務選擇退出政策。](#)
4. [將 AI 服務選擇退出政策連接至組織的根、OU 或帳戶。](#)
5. [檢視套用至帳戶的合併有效 AI 服務選擇退出政策。](#)

對於所有這些步驟，您以 AWS Identity and Access Management (IAM) 使用者身分登入、擔任 IAM 角色，或以組織的管理帳戶中的根使用者身分登入 ([不建議](#))。

其他資訊

- [了解 AI 服務選擇退出政策的政策語法，並查看政策範例](#)

選擇退出所有支援的 AWS AI 服務

在本主題中：

- 您可以在 AWS Organizations 主控台中選擇不接收按鈕。
- 您可以使用 AWS CLI & AWS SDKs 連接提供的範例政策來選擇退出。
- 您可以檢視 AI 服務選擇退出政策 AWS 服務 支援的 清單。

選擇退出所有支援的 AI 服務

您可以透過建立和連接 AI 服務選擇退出政策，選擇不讓組織將其內容用於改善服務。此政策適用於所有目前和未來支援的 AWS AI 服務。成員帳戶無法更新政策。

AWS Management Console

選擇退出所有 AI 服務

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI 服務選擇退出政策](#) 頁面上，選擇選擇退出所有服務。
3. 在選擇退出所有服務確認頁面上，選擇選擇退出所有服務。

AWS CLI & AWS SDKs

選擇退出所有 AI 服務

1. 複製「範例 1：選擇退出組織中所有帳戶的所有 [AI 服務](#)」的 [AI 服務選擇退出範例](#)。
2. 遵循[連接和分離 AI 服務選擇退出](#)中的指示。

Note

選擇退出 Amazon Monitron 需要其他步驟。如需詳細資訊，請參閱 [AWS 服務條款](#)。

AI 服務選擇退出政策支援的 服務清單

以下是 AI 服務選擇退出政策 AWS 服務 支援的 清單：

- [Amazon AI 操作](#)
- [Amazon Chime SDK 語音分析](#)
- [Amazon CloudWatch](#)
- [Amazon CodeGuru Profiler](#)
- [Amazon CodeWhisperer](#) (現在是 [Amazon Q Developer](#) 的一部分)
- [Amazon Comprehend](#)
- [Amazon Connect](#)
- [Amazon Connect 最佳化](#)
- [Amazon Connect Contact Lens](#)
- [AWS 資料庫遷移服務](#)

- [Amazon DataZone](#)
- [AWS Entity Resolution](#)
- [Amazon Fraud Detector](#)
- [AWS Glue](#)
- [Amazon GuardDuty](#)
- [Amazon Lex](#)
- [Amazon Polly](#)
- [Amazon Q](#)
- [Amazon QuickSight](#)
- [Amazon Rekognition](#)
- [Amazon Security Lake](#)
- [AWS Supply Chain](#)
- [Amazon Textract](#)
- [Amazon Transcribe](#)
- [AWS Transform \(變形\)](#)
- [Amazon Translate](#)

AI 服務選擇退出政策語法和範例

本主題說明人工智慧 (AI) 服務選擇退出政策語法，並提供了範例。

AI 服務選擇退出政策的語法

AI 服務選擇退出政策是根據 [JSON](#) 規則建構的純文字檔。AI 服務選擇退出政策的語法遵循管理政策類型的語法。如需該語法的完整討論，請參閱[理解管理政策繼承](#)。本主題著重於以該一般語法滿足 AI 服務選擇退出政策類型的特定需求。

Important

本節中討論的值的大小寫很重要。輸入具有大小寫字母的值，如本主題所示。如果您使用未預期的大小寫，政策將無法運作。

下列政策顯示基本的 AI 服務選擇退出政策語法。如果此範例直接連接至帳戶，則該帳戶會明確選擇退出某項服務，並選擇加入至另一項服務。從較高層級 (OU 或根政策) 繼承的政策可以選擇加入或選擇退出其他服務。

```
{
  "services": {
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "lex": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

想像下列連接至組織根的範例政策。它會設定組織選擇退出所有 AI 服務的預設值。這會自動包含任何未明確豁免的 AI 服務，包括 AWS 未來可能會部署的任何 AI 服務。您可以將子政策連接至 OU 或直接連接至帳戶，以覆寫除 Amazon Comprehend 之外的任何 AI 服務的此設定。下列範例中的第二個項目使用 @@operators_allowed_for_child_policies 來設定 none 以防止被覆寫。範例中的第三個項目會針對 Amazon Rekognition 進行整個組織的豁免。它在整個組織中選擇使用該服務，但正確確實允許子政策在適用時覆寫。

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "comprehend": {
      "opt_out_policy": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "@@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

```

    }
  }
}

```

AI 服務選擇退出政策語法包含下列元素：

- **services** 元素。透過此固定名稱，AI 服務選擇退出政策將識別為包含元素的最外層 JSON。

AI 服務選擇退出政策可在 **services** 元素下具有一個或多個陳述式。每個陳述式均包含下列要素：

- 識別 AWS AI 服務的服務名稱金鑰。以下鍵名稱是該欄位的有效值：
 - **default** – 代表所有目前可用的 AI 服務，並隱含且自動包含未來可能新增的任何 AI 服務。
 - aiops
 - awssupplychain
 - chimesdkvoiceanalytics
 - cloudwatch
 - codeguruprofiler
 - codewhisperer
 - comprehend
 - connectamd
 - connectoptimization
 - contactlens
 - datazone
 - dms
 - entityresolution
 - frauddetector
 - glue
 - guardduty
 - lex
 - polly
 - q
 - quicksight
 - rekognition

- securitylake
- textract
- transcribe
- transform
- translate

透過服務名稱鍵識別的每個政策陳述式都可以包含下列元素：

- `opt_out_policy` 索引鍵。此鍵必須存在。這是您可以放置在服務名稱鍵下的唯一鍵。

`opt_out_policy` 鍵可以僅包含 `@@assign` 運算子 (具有下列其中一個值)：

- `optOut` – 您選擇退出指定 AI 服務使用的內容。
- `optIn` – 您選擇加入指定 AI 服務使用的內容。

 備註

- 您無法使用 `@@append` 和 `@@remove` AI 服務選擇退出政策中的繼承運算子。
- 您無法使用 AI 服務選擇退出政策中的 `@@enforced_for` 運算子。

- 在任何層級，您都可以指定 `@@operators_allowed_for_child_policies` 運算子，來控制子政策可以執行哪些動作來覆寫父政策強加的設定。您可以指定下列其中一個值：
 - `@@assign` – 此政策的子政策可以使用 `@@assign` 運算子，以不同的值覆蓋繼承的值。
 - `@@none` – 此政策的子政策無法變更值。

`@@operators_allowed_for_child_policies` 的行為取決於您放置它的位置。您可以在下列位置使用：

- 在 `services` 鍵下方 – 控制子政策是否可以在有效政策中新增或變更服務清單。
- 在特定 AI 服務的鍵下，或 `default` 鍵 – 控制子政策是否可以新增或變更此特定項目下的鍵清單。
- 在特定服務的 `opt_out_policies` 鍵下 – 控制子政策是否只能變更此特定服務的設定。

AI 服務選擇退出政策範例

接下來的政策範例僅供參考。

範例 1：選擇退出組織中所有帳戶的所有 AI 服務

下列範例顯示您可以連接至組織根的政策，以選擇退出組織中帳戶的 AI 服務。

Tip

如果您使用範例右上角的「複製」按鈕來複製下列範例，則複本不會包含行號。已經準備貼上。

```
[1] | {
    |   "services": {
    |     "@operators_allowed_for_child_policies": ["@none"],
    |     "default": {
[2] |       "@operators_allowed_for_child_policies": ["@none"],
    |       "opt_out_policy": {
[3] |         "@operators_allowed_for_child_policies": ["@none"],
    |         "@assign": "optOut"
    |       }
    |     }
    |   }
  | }
```

- [1] – "@operators_allowed_for_child_policies": ["@none"] 在 services 下，可防止任何子政策針對個別服務新增已經存在的 default 區段之外的任何新區段。Default 代表「所有 AI 服務」的預留位置。
- [2] – "@operators_allowed_for_child_policies": ["@none"] 在 default 下，可防止任何子政策新增已經存在的 opt_out_policy 區段之外的任何新區段。
- [3] – "@operators_allowed_for_child_policies": ["@none"] 在 opt_out_policy 下，可防止子政策變更 optOut 設定的值或新增任何其他設定。

範例 2：為所有服務設定組織預設設定，但允許子政策覆寫個別服務的設定

下列範例政策會為所有 AI 服務設定整個組織的預設值。default 的值，可防止子政策變更服務 default 的 optOut 值，這是所有 AI 服務的預留位置。如果將此政策連接至根或 OU，以將其套用為父政策，則子政策仍然可以變更個別服務的選擇退出設定，如第二項政策所示。

- 因為沒有 "@operators_allowed_for_child_policies": ["@none"] 在 services 鍵下，子政策可以為個別服務新增區段。

- "`@operators_allowed_for_child_policies`": [`"@none"`] 在 `default` 下，可防止任何子政策新增已經存在的 `opt_out_policy` 區段之外的任何新區段。
- "`@operators_allowed_for_child_policies`": [`"@none"`] 在 `opt_out_policy` 下，可防止子政策變更 `optOut` 設定的值或新增任何其他設定。

組織根使用者 AI 服務選擇退出父政策

```
{
  "services": {
    "default": {
      "@operators_allowed_for_child_policies": ["@none"],
      "opt_out_policy": {
        "@operators_allowed_for_child_policies": ["@none"],
        "@assign": "optOut"
      }
    }
  }
}
```

下列範例政策假設之前的範例政策已連接至組織根或父 OU，並且您將此範例連接至受父政策影響的帳戶。它會覆寫預設的選擇退出設定，並明確選擇僅使用 Amazon Lex 服務。

AI 服務選擇退出子政策

```
{
  "services": {
    "lex": {
      "opt_out_policy": {
        "@assign": "optIn"
      }
    }
  }
}
```

產生的有效政策 AWS 帳戶 是帳戶只選擇加入 Amazon Lex，並且因為父政策的繼承 `default` 選擇退出設定而選擇退出所有其他 AWS AI 服務。

範例 3：針對單一服務定義整個組織的 AI 服務選擇退出政策

下列範例顯示 AI 服務選擇退出政策，定義單一 AI 服務的 optOut 設定。如果此政策連接至組織的根，它會防止任何子政策覆寫這一項服務的 optOut 設定。其他服務並未透過此政策解決，但可能會受其他 OU 或帳戶中的子政策的影響。

```
{
  "services": {
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optOut",
        "@@operators_allowed_for_child_policies": ["@none"]
      }
    }
  }
}
```

Security Hub 政策

AWS Security Hub 政策為安全團隊提供集中式方法來管理整個安全組態 AWS Organizations。透過利用這些政策，您可以透過中央組態機制建立和維護一致的安全控制。此整合可讓您建立符合您組織安全需求的政策，並將這些政策集中套用至帳戶和組織單位 (OUs)，以解決安全涵蓋範圍漏洞。

Security Hub 政策已與完全整合 AWS Organizations，允許管理帳戶或委派管理員定義和強制執行安全組態。當帳戶加入您的組織時，他們會根據其在組織階層中的位置自動繼承適用的政策。這可確保您的安全標準會隨著組織的成長而一致套用。這些政策會遵守現有的組織結構，並在安全組態的分佈方式方面提供彈性，同時維持對關鍵安全設定的集中控制。

主要功能和優點

Security Hub 政策提供一組完整的功能，可協助您在整個 AWS 組織中管理和強制執行安全組態。這些功能可簡化安全管理，同時確保對多帳戶環境的一致控制。

- 在您的組織中跨帳戶和區域集中[啟用 Security Hub](#)
- 建立安全政策，以跨帳戶和 OUs 定義您的安全組態
- 加入您的組織時，自動將安全組態套用至新帳戶
- 確保整個組織的安全設定一致
- 防止成員帳戶修改組織層級的安全組態

什麼是 Security Hub 政策？

Security Hub 政策是 AWS Organizations 政策，可讓您集中控制整個組織帳戶的安全組態。這些政策可與無縫搭配 AWS Organizations，協助您在整個多帳戶環境中建立和維護一致的安全標準。

當您實作 Security Hub 政策時，您可以定義特定安全組態，以自動在整個組織中傳播。這可確保所有帳戶，包括新建立的帳戶，都符合您組織的安全需求和最佳實務。

這些政策也透過強制執行一致的安全控制，並防止個別帳戶修改組織層級的安全設定，來協助您維持合規。這種集中式方法可大幅降低管理大型複雜 AWS 環境中安全組態的管理開銷。

Security Hub 政策的運作方式

當您將 Security Hub 政策連接至組織或組織單位時，AWS Organizations 會自動評估政策，並根據您定義的範圍套用政策。政策強制執执行程序遵循特定的衝突解決規則：

當區域同時出現在啟用和停用清單中時，停用組態優先。例如，如果啟用和停用組態中同時列出一個區域，則 Security Hub 將在該區域中停用。

當 ALL_SUPPORTED 指定為啟用時，除非明確停用，否則所有目前和未來的區域都會啟用 Security Hub。這可讓您在 AWS 擴展到新區域時維持全面的安全涵蓋範圍。

子政策可以使用繼承運算子修改父政策設定，允許在不同組織層級進行精細控制。這種階層方法可確保特定組織單位可以自訂其安全設定，同時維護基準控制。

術語

本主題會在討論 Security Hub 政策時使用下列術語。

Security Hub 政策術語

術語	定義
有效政策	合併所有繼承的政策後，套用至帳戶的最終政策。
政策繼承	帳戶從父組織單位繼承政策的程序。
委派的管理員	指定代表組織管理 Security Hub 政策的帳戶。
服務連結角色	允許 Security Hub 與其他 AWS 服務互動的 IAM 角色。

Security Hub 政策的使用案例

Security Hub 政策可解決多帳戶環境中常見的安全管理挑戰。下列使用案例示範組織通常如何實作這些政策，以增強其安全狀態。

範例使用案例：區域合規要求

跨國公司需要不同地理區域的不同 Security Hub 組態。他們會使用 在所有區域中建立啟用 Security Hub 的父政策ALL_SUPPORTED，然後使用子政策來停用需要不同安全控制的特定區域。這可讓他們保持符合區域法規，同時確保全面的安全涵蓋範圍。

範例使用案例：開發團隊安全標準

軟體開發組織實作 Security Hub 政策，在生產區域中啟用監控，同時不管理開發區域。他們在政策中使用明確的區域清單ALL_SUPPORTED，而不是維持對安全監控涵蓋範圍的精確控制。這種方法允許他們在生產環境中強制執行更嚴格的安全控制，同時在開發領域保持靈活性。

政策繼承和強制執行

了解政策如何繼承和強制執行對於整個組織的有效安全管理至關重要。繼承模型遵循 AWS Organizations 階層，確保可預測且一致的政策應用程式。

- 連接到根層級的政策適用於所有帳戶
- 帳戶從其父組織單位繼承政策
- 多個政策可以套用至單一帳戶
- 更具體的政策（更接近階層中的帳戶）優先

政策驗證

建立 Security Hub 政策時，會發生下列驗證：

- 區域名稱必須是有效的 AWS 區域識別符
- Security Hub 必須支援區域
- 政策結構必須遵循 AWS Organizations 政策語法規則
- enable_in_regions 和 disable_in_regions清單都必須存在，但可以是空的

區域考量事項和支援的區域

Security Hub 政策跨多個區域運作，需要仔細考慮您的全球安全需求。了解區域行為可協助您在整個組織的全球足跡中實作有效的安全控制。

- 政策強制執行會在每個區域中獨立執行
- 您可以指定要在政策中包含或排除的區域
- 使用 ALL_SUPPORTED 選項時，會自動包含新區域
- 政策僅適用於可使用 Security Hub 的區域

後續步驟

若要開始使用 Security Hub 政策：

1. 檢閱 Security Hub 政策入門中的先決條件
2. 使用我們的最佳實務指南來規劃您的政策策略
3. 了解政策語法並檢視範例政策

Security Hub 政策入門

設定 Security Hub 政策之前，請確定您了解先決條件和實作需求。本主題會引導您在組織中設定和管理這些政策的程序。

開始之前

在實作 Security Hub 政策之前，請檢閱下列要求：

- 您的帳戶必須是 AWS Organizations 組織的一部分
- 您必須以下列其中一種身分登入：
 - 組織的管理帳戶
 - 具有管理 Security Hub 政策許可的委派管理員帳戶
- 您必須為組織中的 Security Hub 啟用受信任存取
- 您必須在組織的根目錄中啟用 Security Hub 政策類型

此外，請確認：

- 您要套用政策的區域支援 Security Hub
- 您的管理帳戶中已設定AWSServiceRoleForSecurityHubV2服務連結角色。若要驗證此角色是否存在，請執行 `aws iam get-role --role-name AWSServiceRoleForSecurityHubV2`。如果您需要建立此角色，您可以從管理帳戶 `aws securityhub enable-security-hub-v2` 在任何區域中執行，或執行 `aws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com`。

實作步驟

若要有效實作 Security Hub 政策，請依序遵循這些步驟。每個步驟可確保適當的組態，並有助於防止設定期間的常見問題。管理帳戶或委派管理員可以透過 AWS Organizations 主控台、AWS 命令列界面 (AWS CLI) 或 AWS SDKs 執行這些步驟。

1. [啟用 Security Hub 的受信任存取](#)。
2. [為您的組織啟用 Security Hub 政策](#)。
3. [建立 Security Hub 政策](#)。
4. [將 Security Hub 政策連接至組織的根、OU 或帳戶](#)。
5. [檢視套用至 帳戶的合併有效 Security Hub 政策](#)。

對於所有這些步驟，您以 AWS Identity and Access Management (IAM) 使用者身分登入、擔任 IAM 角色，或以組織的管理帳戶中的根使用者身分登入 ([不建議](#))。

其他資訊

- [了解 Security Hub 政策的政策語法，並查看政策範例](#)

使用 Security Hub 政策的最佳實務

在整個組織中實作 Security Hub 政策時，遵循已建立的最佳實務有助於確保安全組態的成功部署和維護。這些指導方針特別說明 Security Hub 政策管理和強制執行的獨特層面 AWS Organizations。

政策設計原則

建立 Security Hub 政策之前，請為您的政策結構建立明確的原則。保持政策簡單，並避免複雜的跨屬性或巢狀規則，以致難以判斷最終結果。從組織根層級的廣泛政策開始，並視需要透過子政策進行精簡。

考慮以策略方式使用空白區域清單。當您只需要在特定區域中停用 Security Hub 時，您可以保留 `enable_in_regions` 空白，或保留 `disable_in_regions` 空白，讓區域不受政策管理。此彈性可協助您精確控制安全監控涵蓋範圍。

區域管理策略

透過 Security Hub 政策管理區域時，請考慮這些經過驗證的方法。當您想要在安全涵蓋範圍內自動包含未來區域 `ALL_SUPPORTED` 時，請使用 `ALL_SUPPORTED`。對於更精細的控制，請明確列出區域，而不是依賴 `ALL_SUPPORTED`，尤其是當不同的區域需要不同的安全組態時。

記錄您的區域特定需求，特別是：

- 需要特定組態的合規規定區域
- 開發與生產環境的差異
- 選擇加入具有特殊考量的區域
- Security Hub 必須保持停用的區域

政策繼承規劃

仔細規劃您的政策繼承結構，以維持有效的安全控制，同時允許必要的彈性。記錄哪些組織單位可以修改繼承的政策，以及允許哪些修改。當您需要強制執行嚴格的安全控制時，請考慮在父層級限制繼承運算子 (`@@assign`、`@@append`、`@@remove`)。

監控和驗證

實作定期監控實務，以確保您的政策保持有效。定期檢閱政策附件，尤其是在組織變更之後。驗證區域組態是否符合您的預期安全涵蓋範圍，特別是在使用 `ALL_SUPPORTED` 或 管理多個區域清單時。

故障診斷策略

疑難排解 Security Hub 政策時，請先專注於政策優先順序和繼承。請記住，當區域出現在兩個清單中時，停用組態優先於啟用組態。檢查政策繼承鏈，以了解父系和子系政策如何結合，以為每個帳戶建立有效的政策。

Security Hub 政策語法和範例

Security Hub 政策遵循標準化的 JSON 語法，該語法定義了在整個組織中啟用和設定 Security Hub 的方式。了解政策結構可協助您為您的安全需求建立有效的政策。

考量事項

建立 Security Hub 政策之前，請先了解政策語法的這些要點：

- 政策中需要 `enable_in_regions` 和 `disable_in_regions` 清單，但它們可以是空的
- 處理有效政策時，`disable_in_regions` 優先於 `enable_in_regions`
- 除非明確限制，否則子政策可以使用繼承運算子修改父政策
- `ALL_SUPPORTED` 指定項目包括目前和未來的區域
- 區域名稱必須在 Security Hub 中有效且可用

基本政策結構

Security Hub 政策使用以下基本結構：

```
{
  "securityhub":{
    "enable_in_regions":[
      "us-east-1",
      "us-west-2"
    ],
    "disable_in_regions":[
      "eu-central-1"
    ]
  }
}
```

政策元件

Security Hub 政策包含下列重要元件：

`securityhub`

政策設定的頂層容器

所有 Security Hub 政策都需要

`enable_in_regions`

應啟用 Security Hub 的區域清單

可包含特定區域名稱或 `ALL_SUPPORTED`

必要欄位，但可為空白

使用 時ALL_SUPPORTED， 包含未來的區域

disable_in_regions

應停用 Security Hub 的區域清單

可包含特定區域名稱或 ALL_SUPPORTED

必要欄位，但可為空白

當區域出現在兩個清單中enable_in_regions時，優先考慮

繼承運算子

@@指派 - 覆寫繼承的值

@@附加 - 將新值新增至現有值

@@移除 - 從繼承的設定中移除特定值

Security Hub 政策範例

下列範例示範常見的 Security Hub 政策組態。

以下範例會在所有目前和未來的區域中啟用 Security Hub。透過ALL_SUPPORTED在enable_in_regions清單中使用 並保持disable_in_regions空白，此政策可在新區域可用時確保全面的安全涵蓋範圍。

```
{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
      ]
    }
  }
}
```

此範例會在所有區域中停用 Security Hub，包括任何未來區域，因為disable_in_regions清單的優先順序高於 enable_in_regions。

```
{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "us-east-1",
        "us-west-2"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    }
  }
}
```

下列範例示範子政策如何使用繼承運算子修改父政策設定。此方法允許精細控制，同時維護整體政策結構。子政策會將新區域新增至 enable_in_regions並從 disable_in_regions中移除區域。

```
{
  "securityhub":{
    "enable_in_regions":{
      "@@append":[
        "eu-central-1"
      ]
    },
    "disable_in_regions":{
      "@@remove":[
        "us-west-2"
      ]
    }
  }
}
```

此範例示範如何在多個特定區域中啟用 Security Hub，而不使用 ALL_SUPPORTED。這可讓您精確控制哪些區域已啟用 Security Hub，同時讓未指定的區域不受政策管理。

```
{
  "securityhub":{
```

```

    "enable_in_regions":{
      "@@assign":[
        "us-east-1",
        "us-west-2",
        "eu-west-1",
        "ap-southeast-1"
      ]
    },
    "disable_in_regions":{
      "@@assign":[

      ]
    }
  }
}

```

下列範例示範如何透過在大多數區域中啟用 Security Hub 來處理區域合規要求，同時在特定位置明確停用它。disable_in_regions 清單優先，確保 Security Hub 在這些區域中保持停用狀態，無論其他政策設定為何。

```

{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
        "ap-east-1",
        "me-south-1"
      ]
    }
  }
}

```

的委派管理員 AWS Organizations

我們建議您僅將 AWS Organizations 管理帳戶及其使用者和角色用於該帳戶必須執行的任務。我們也建議您將 AWS 資源存放在組織內其他成員帳戶中，且將其保存在管理帳戶之外。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中的使用者或角色。

從組織的管理帳戶，您可以將 Organizations 的政策管理委派給指定的成員帳戶，以執行預設僅適用於管理帳戶的政策動作。

如需以資源為基礎的委派政策範例，請參閱 [資源型政策範例 AWS Organizations](#)。

主題

- [使用 建立資源型委派政策 AWS Organizations](#)
- [使用 更新資源型委派政策 AWS Organizations](#)
- [使用 檢視資源型委派政策 AWS Organizations](#)
- [使用 刪除資源型委派政策 AWS Organizations](#)

使用 建立資源型委派政策 AWS Organizations

從管理帳戶中，為您的組織建立以資源為基礎的委派政策，並新增指定哪些成員帳戶可以對政策執行動作的陳述式。您可以在政策中新增多個陳述式，以表示成員帳戶的不同許可集。

最低許可

若要建立以資源為基礎的委派政策，您需要執行下列動作的許可：

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

此外，您必須授與委派管理員帳戶中的角色和使用者對應的 IAM 許可，以執行必要動作。如果沒有 IAM 許可，則假設呼叫主體沒有管理 AWS Organizations 政策所需的許可。

AWS Management Console

使用以下其中一個方法，在 AWS Management Console 中將陳述式新增至以資源為基礎的委派政策：

- JSON 政策 – 貼上並自訂要在帳戶中使用的範例資源型委派政策，或在 JSON 編輯器中輸入您自己的 JSON 政策文件。
- 視覺化編輯器 – 在視覺化編輯器中建構新的委派政策，此政策會引導您建立委派政策，而不需要撰寫 JSON 語法。

使用 JSON 政策編輯器來建立委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 AWS Organizations 的委派管理員區段中，選擇委派以建立 Organizations 委派政策。
4. 輸入 JSON 政策文件。如需有關 IAM 政策語言的詳細資訊，請參閱 [IAM JSON 政策參考](#)。
5. 解決政策驗證期間產生的任何[安全性警告、錯誤或一般性警告](#)，然後選擇 Create policy (建立政策) 以儲存工作。

使用視覺化編輯器來建立委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 AWS Organizations 的委派管理員區段中，選擇委派以建立 Organizations 委派政策。
4. 在 Create Delegation policy (建立委派政策) 頁面上，選擇 Add new statement (新增陳述式)。
5. 將 Effect (效果) 設定為 Allow。
6. 新增 Principal 以定義您要委派的成員帳戶。
7. 從 Actions (動作) 清單中，選擇您要委派的動作。您可使用 Filter actions (篩選動作)，以縮減選項。
8. 若要指定委派的成員帳戶是否可將政策連接至組織根目錄或組織單位 (OU)，請設定 Resources。您也必須選取 policy 作為資源類型。您可採用以下方式來指定資源：
 - 選擇 Add a resource (新增資源)，並按照對話方塊中的提示建構 Amazon Resource Name (ARN)。
 - 在編輯器中手動列出資源 ARN。如需 ARN 語法的詳細資訊，請參閱 AWS 一般參考指南中的 [Amazon Resource Name \(ARN\)](#)。如需有關在政策資源元素中使用 ARN 的詳細資訊，請參閱 [IAM JSON 政策元素：Resource](#)。
9. 選擇 Add a condition (新增條件) 以指定其他條件，包括您要委派的政策類型。選擇條件的 Condition key (條件索引鍵)、Tag key (標籤索引鍵)、Qualifier (修飾詞) 以及 Operator (運算子)，然後輸入 **Value**。完成時，請選擇 Add condition (新增條件)。如需有關 Condition (條件) 元素的詳細資訊，請參閱 IAM JSON 政策參考中的 [IAM JSON 政策元素：Condition](#)。

10. 若要新增更多許可區塊，請選擇 Add new statement (新增陳述式)。針對每個區塊皆重複步驟 5 到 9。
11. 解決[政策驗證](#)期間產生的任何安全性警告、錯誤或一般性警告，然後選擇 Create policy (建立政策) 以儲存工作。

AWS CLI & AWS SDKs

建立委派政策

您可以使用下列命令來建立委派政策：

- AWS CLI : [put-resource-policy](#)

下列範例會建立委派政策。

```
$ aws organizations put-resource-policy --content
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Fully_manage_backup_policies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "135791357913"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": [
        "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
        "arn:aws:organizations::246802468024:ou/o-abcdef/*",
        "arn:aws:organizations::246802468024:account/o-abcdef/*",
        "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
      ],
    }
  ]
}
```

```
    "Condition": {
      "StringLikeIfExists": {
        "organizations:PolicyType": [
          "BACKUP_POLICY"
        ]
      }
    }
  }
]
```

- AWS 開發套件：[PutResourcePolicy](#)

支援的委派政策動作

委派政策支援下列動作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization

- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

支援的條件金鑰

只有 支援的條件金鑰 AWS Organizations 可用於委派政策。如需詳細資訊，請參閱 [服務授權參考中的條件金鑰 AWS Organizations](#)。

使用 更新資源型委派政策 AWS Organizations

從管理帳戶中，更新您組織的資源型委派政策，並新增指定哪些成員帳戶可以對政策執行動作的陳述式。您可以在政策中新增多個陳述式，以表示成員帳戶的不同許可集。

最低許可

若要更新以資源為基礎的委派政策，您需要執行下列動作的許可：

- organizations:PutResourcePolicy
- organizations:DescribeResourcePolicy

此外，您必須授與委派管理員帳戶中的角色和使用者對應的 IAM 許可，以執行必要動作。如果沒有 IAM 許可，則假設呼叫主體沒有管理 AWS Organizations 政策所需的許可。

AWS Management Console

使用以下其中一個方法，在 AWS Management Console 中將陳述式新增至以資源為基礎的委派政策：

- JSON 政策 – 貼上並自訂要在帳戶中使用的範例資源型委派政策，或在 JSON 編輯器中輸入您自己的 JSON 政策文件。
- 視覺化編輯器 – 在視覺化編輯器中建構新的委派政策，此政策會引導您建立委派政策，而不需要撰寫 JSON 語法。

使用 JSON 政策編輯器來更新委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 的委派管理員 AWS Organizations 區段中，選擇編輯以更新 Organizations 委派政策。
4. 輸入 JSON 政策文件。如需有關 IAM 政策語言的詳細資訊，請參閱 [IAM JSON 政策參考](#)。
5. 解決政策驗證期間產生的任何[安全警告、錯誤或一般警告](#)，然後選擇建立政策。

使用視覺化編輯器更新委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 的委派管理員 AWS Organizations 區段中，選擇編輯以更新 Organizations 委派政策。
4. 在 Create Delegation policy (建立委派政策) 頁面上，選擇 Add new statement (新增陳述式)。
5. 將 Effect (效果) 設定為 Allow。
6. 新增 Principal 以定義您要委派的成員帳戶。
7. 從 Actions (動作) 清單中，選擇您要委派的動作。您可使用 Filter actions (篩選動作)，以縮減選項。

8. 若要指定委派的成員帳戶是否可將政策連接至組織根目錄或組織單位 (OU)，請設定 Resources。您也必須選取 policy 作為資源類型。您可採用以下方式來指定資源：
 - 選擇 Add a resource (新增資源)，並按照對話方塊中的提示建構 Amazon Resource Name (ARN)。
 - 在編輯器中手動列出資源 ARN。如需 ARN 語法的詳細資訊，請參閱 AWS 一般參考指南中的 [Amazon Resource Name \(ARN\)](#)。如需有關在政策資源元素中使用 ARN 的詳細資訊，請參閱 [IAM JSON 政策元素：Resource](#)。
9. 選擇 Add a condition (新增條件) 以指定其他條件，包括您要委派的政策類型。選擇條件的 Condition key (條件索引鍵)、Tag key (標籤索引鍵)、Qualifier (修飾詞) 以及 Operator (運算子)，然後輸入 **Value**。完成時，請選擇 Add condition (新增條件)。如需有關 Condition (條件) 元素的詳細資訊，請參閱 IAM JSON 政策參考中的 [IAM JSON 政策元素：Condition](#)。
10. 若要新增更多許可區塊，請選擇 Add new statement (新增陳述式)。針對每個區塊皆重複步驟 5 到 9。
11. 解決[政策驗證](#)期間產生的任何安全警告、錯誤或一般警告，然後選擇儲存政策。

AWS CLI & AWS SDKs

建立或更新委派政策

您可以使用下列命令來建立或更新委派政策：

- AWS CLI：[put-resource-policy](#)

以下範例會建立或更新委派政策。

```
$ aws organizations put-resource-policy --content
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Fully_manage_backup_policies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "135791357913"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:CreatePolicy",
```

```

        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
    ],
    "Resource": [
        "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
        "arn:aws:organizations::246802468024:ou/o-abcdef/*",
        "arn:aws:organizations::246802468024:account/o-abcdef/*",
        "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": [
                "BACKUP_POLICY"
            ]
        }
    }
}
]
}

```

- AWS 開發套件：[PutResourcePolicy](#)

支援的委派政策動作

委派政策支援下列動作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization

- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

支援的條件金鑰

只有 支援的條件金鑰 AWS Organizations 可用於委派政策。如需詳細資訊，請參閱服務授權參考中的 [的條件金鑰 AWS Organizations](#)。

使用 檢視資源型委派政策 AWS Organizations

在管理帳戶中，檢視組織的以資源為基礎的委派政策，以了解哪些委派管理員有存取權，可管理哪些政策類型。

最低許可

若要檢視以資源為基礎的委派政策，您需要具有下列動作的執行許可：`organizations:DescribeResourcePolicy`。

AWS Management Console

檢視委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 AWS Organizations 的委派管理員區段中，捲動以檢視完整的委派政策。

AWS CLI & AWS SDKs

檢視委派政策

您可以使用下列命令來檢視委派政策：

- AWS CLI：[describe-resource-policy](#)

以下範例會擷取政策。

```
$ aws organizations describe-resource-policy
```

- AWS SDK：[DescribeResourcePolicy](#)

使用 刪除資源型委派政策 AWS Organizations

當您不再需要委派組織中的政策管理時，可以從組織的管理帳戶中刪除以資源為基礎的委派政策。

 Important

如果刪除以資源為基礎的委派政策，則無法將其復原。

 最低許可

若要刪除以資源為基礎的委派政策，您需要具有下列動作的執行許可：`organizations:DeleteResourcePolicy`。

AWS Management Console

刪除委派政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 選擇設定。
3. 在 AWS Organizations 的委派管理員區段，選擇刪除。
4. 在 Delete policy (刪除政策) 確認對話方塊中，輸入 **delete**。然後，選擇 Delete policy (刪除政策)。

AWS CLI & AWS SDKs

刪除委派政策

您可以使用下列項命令來刪除委派政策：

- AWS CLI : [delete-resource-policy](#)

以下範例會刪除政策。

```
$ aws organizations delete-resource-policy
```

- AWS SDK : [DeleteResourcePolicy](#)

啟用政策類型

建立政策並將其連接至組織之前，必須先啟用該政策類型以供使用。啟用政策類型是在組織根執行的一次性任務。您只能從組織的管理帳戶或指定為委派管理員的成員帳戶啟用政策類型。

最低許可

若要啟用政策類型，您必須有執行下列動作的許可：

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

啟用政策類型

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Policies](#) (政策) 頁面上，選擇您要啟用的政策類型的名稱。
3. 在 Policy type (政策類型) 頁面上，選擇啟用 **Policy type** (政策類型)。

此頁面會由指定類型的可用政策清單所取代。

AWS CLI & AWS SDKs

啟用政策類型

您可以使用下列其中一項命令來啟用政策類型：

- AWS CLI: [enable-policy-type](#)

下列範例顯示如何啟用組織的備份政策。請注意，您必須指定組織根的 ID。

```
$ aws organizations enable-policy-type \
  --root-id r-a1b2 \
  --policy-type BACKUP_POLICY
{
```

```
"Root": {
  "Id": "r-a1b2",
  "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
  "Name": "Root",
  "PolicyTypes": [
    {
      "Type": "BACKUP_POLICY",
      "Status": "ENABLED"
    }
  ]
}
```

輸出中 PolicyTypes 的清單現在包含指定的政策類型且具有ENABLEDStatus。

- AWS SDKs : [EnablePolicyType](#)

停用政策類型

如果不想再在組織中使用特定政策類型，可以停用該類型以防止意外使用。您只能從組織的管理帳戶或指定為委派管理員的成員帳戶停用政策類型。

考量事項

停用的政策會與所有實體分離，但不會刪除

當您停用政策類型時，所指定類型的所有政策都會自動與組織根的所有實體分離。這些政策不會被刪除。

(僅限服務控制政策類型) 根中的所有實體最初只會連接到預設 **FullAWSAccess** SCP

(僅限服務控制政策類型) 如果您稍後重新啟用 SCP 政策類型，組織根中的所有實體一開始只會連接至預設 FullAWSAccess SCP。在組織中停用 SCP 時，SCP 到實體的連接會中斷。如果您稍後想要重新啟用 SCP，必須視需要將其重新連接至組織的根、OU 和帳戶。

停用政策類型

最低許可

若要停用 SCP，您需要具有執行下列動作的許可：

- organizations:DisablePolicyType

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:ListRoots` – 僅在使用 Organizations 主控台時才需要

AWS Management Console

停用政策類型

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Policies](#) (政策) 頁面上，選擇您要停用的政策類型的名稱。
3. 在 Policy type (政策類型) 頁面上，選擇停用 **Policy type** (政策類型)。
4. 在確認對話方塊上，輸入字詞 **disable**，然後選擇 Disable (停用)。

指定類型的可用政策清單會消失。

AWS CLI & AWS SDKs

停用政策類型

您可以使用下列其中一項命令來停用政策類型：

- AWS CLI: [disable-policy-type](#)

下列範例顯示如何停用組織的備份政策。請注意，您必須指定組織根的 ID。

```
$ aws organizations disable-policy-type \
  --root-id r-a1b2 \
  --policy-type BACKUP_POLICY
{
  "Root": {
    "Id": "r-a1b2",
    "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
    "Name": "Root",
    "PolicyTypes": []
  }
}
```

輸出中 PolicyTypes 的清單不再包含指定的政策類型。

- AWS SDKs : [DisablePolicyType](#)

使用 建立組織政策 AWS Organizations

為組織[啟用政策](#)後，您可以建立政策。

本主題說明如何使用 建立政策 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [建立服務控制政策 \(SCP\)](#)
- [建立資源控制政策 \(RCP\)](#)
- [建立宣告政策](#)
- [建立備份政策](#)
- [建立標籤政策](#)
- [建立聊天應用程式政策](#)
- [建立 AI 服務選擇退出政策](#)
- [建立 Security Hub 政策](#)

建立服務控制政策 (SCP)

最低許可

若要建立 SCP，您需要具有執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

建立服務控制政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇 Create policy (建立政策)。

3. 在 [Create policy \(建立政策\) 頁面上](#)，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來新增一個或多個標籤。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱[標記 AWS Organizations 資源](#)。

 Note

在接下來的大部分步驟中，我們會討論使用 JSON 編輯器右側的控制項，逐元素建構政策。或者，您可以隨時在視窗左側的 JSON 編輯器中輸入文字。您可以直接輸入，或者可以使用複製和貼上。

5. 若要建置政策，您的下一個步驟會因您是否希望新增陳述式，[拒絕](#)或[允許](#)存取而有所不同。如需詳細資訊，請參閱[SCP 評估](#)。您可以使用 Deny 陳述式，您可以擁有額外的控制，因為您可以限制存取特定資源、定義 SCP 生效的條件，以及使用 [NotAction](#) 元素。如需語法的詳細資訊，請參閱[SCP 語法](#)。

新增「拒絕」存取的陳述式：

- a. 在編輯器的右側編輯陳述式窗格中，在新增動作下，選擇 AWS 服務。

在您選擇右側的選項時，JSON 編輯器會隨即更新，在左側顯示相應的 JSON 政策。

- b. 選取服務之後，包含該服務可用動作的清單即會開啟。您可以選擇 All actions (所有動作)，或選擇您要拒絕的一個或多個個別動作。

左側的 JSON 會隨即更新，以包含您選取的動作。

 Note

如果您選取個別動作，然後返回上一步並選取 All actions (所有動作)，**servicename:*** 的預期項目會新增至 JSON，但您之前選取的個別動作會留在 JSON 中，而不會移除。

- c. 如果您想要從其他服務新增動作，可以選擇 Statement (陳述式) 方塊頂部的 All Services (所有服務)，然後視需要重複之前的兩個步驟。
- d. 指定要包含在陳述式中的資源。
 - 在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。

- 在 Add resource (新增資源) 對話方塊，從清單中選擇您要控制其資源的服務。您只能從在上一步選擇的服務中進行選擇。
- 在 Resource Type (資源類型) 下，選擇您要控制的資源類型。
- 最後，完成 Resource ARN (資源 ARN) 中的 Amazon 資源名稱 (ARN)，以識別您要控制存取的特定資源。您必須取代由大括號 {} 包圍的所有預留位置。您可以指定資源類型的 ARN 語法允許的萬用字元 (*)。如需有關可以在何處使用萬用字元的資訊，請參閱文件以取得特定資源類型。
- 選擇 Add resource (新增資源)，以儲存您對政策的新增。JSON 中的 Resource 元素會反映您的新增或變更。資源元素為必要項目。

 Tip

如果您想要為所選取的服務指定所有資源，請選擇 All resources (所有資源) 選項，或 JSON 中直接編輯 Resource 語句來讀取 "Resource": "*"。

- e. (選用) 若要指定在政策陳述式生效時限制的條件，請在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。
- 條件索引鍵 – 從清單中，您可以選擇所有 AWS 服務可用的任何條件索引鍵（例如 `aws:SourceIp`），或只針對您為此陳述式選取的其中一個服務選擇服務特定的索引鍵。
 - 限定詞 – (選用) 當請求具有多值內容索引鍵的多個值時，您可以指定 [限定詞](#) 來根據值測試請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [單一值與多值內容索引鍵](#)。若要檢查請求是否可以有多個值，請參閱服務授權參考中的 [的動作、資源和條件索引鍵 AWS 服務](#)。
 - 預設值 – 針對政策中的條件索引鍵值，測試請求中的單一值。如果請求中的值符合政策中的值，則條件會傳回 true。如果政策指定多個值，則會將其視為「或」測試，如果請求值符合任何政策值，則條件會傳回 true。
 - 對於請求中的任意值 – 當請求可以有多个值時，此選項會測試是否至少一個請求值符合政策中至少其中一個條件索引鍵值。如果請求中任一鍵值符合政策中的任一條件值，則條件會傳回 true。如果沒有相符金鑰或為 null 資料集，則條件會傳回 false。
 - 對於請求中的所有值 – 當請求可以有多个值時，此選項會測試是否每一個請求值均符合政策中的條件索引鍵值。如果請求中每個鍵值至少符合政策中的一個值，則條件會傳回 true。如果請求中沒有鍵，或鍵值解析為 null 資料集 (例如空白字串)，則也會傳回 true。

- 運算子 – [運算子](#) 指定要進行的比較類型。顯示的選項取決於條件索引鍵的資料類型。例如，`aws:CurrentTime` 全域條件索引鍵可讓您從任何日期比較運算子中選擇，或 `Null`，您可以用於測試該值是否存在於請求中。

針對除 `Null` 測試之外的任何條件運算子，您可以選擇 [IfExists](#) 選項。

- 數值 – (選用) 指定您要測試請求的一個或多個值。

選擇新增條件。

如需有關條件索引鍵的詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。

6. 新增「允許」存取的陳述式：

- a. 在左側的 JSON 編輯器中，將行 `"Effect": "Deny"` 變更為 `"Effect": "Allow"`。

在您選擇右側的選項時，JSON 編輯器會隨即更新，在左側顯示相應的 JSON 政策。

- b. 選取服務之後，包含該服務可用動作的清單即會開啟。您可以選擇 All actions (所有動作)，或選擇您要允許的一個或多個個別動作。

左側的 JSON 會隨即更新，以包含您選取的動作。

 Note

如果您選取個別動作，然後返回上一步並選取 All actions (所有動作)，`servicename:*` 的預期項目會新增至 JSON，但您之前選取的個別動作會留在 JSON 中，而不會移除。

- c. 如果您想要從其他服務新增動作，可以選擇 Statement (陳述式) 方塊頂部的 All Services (所有服務)，然後視需要重複之前的兩個步驟。

7. (選用) 若要將另一個陳述式新增到政策，請選擇 Add statement (新增陳述式) 並使用視覺編輯器來建置下一個陳述式。
8. 當您完成新增陳述式後，請選擇 Create policy (建立政策) 來儲存完成的 SCP。

您的新 SCP 會出現在組織的政策清單中。您現在可以[將 SCP 連接至根、OU 或帳戶](#)。

AWS CLI & AWS SDKs

建立服務控制政策

您可以使用下列其中一項命令來建立 SCP：

- AWS CLI: [create-policy](#)

以下範例假設您已有名為 Deny-IAM.json 的檔案，且包含 JSON 政策文字。它會使用該檔案來建立新的服務控制政策。

```
$ aws organizations create-policy \
  --content file://Deny-IAM.json \
  --description "Deny all IAM actions" \
  --name DenyIAMSCP \
  --type SERVICE_CONTROL_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/service_control_policy/p-i9j8k7l6m5",
      "Name": "DenyIAMSCP",
      "Description": "Deny all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\": \"Statement1\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]} ]}"
  }
}
```

- AWS SDKs : [CreatePolicy](#)

Note

遇到管理帳戶與少數其他幾種情況時，SCP 沒有任何作用。如需詳細資訊，請參閱[任務和實體不受 SCP 的限制](#)。

建立資源控制政策 (RCP)

最低許可

若要建立 RCPs，您需要執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

建立資源控制政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在資源控制政策頁面上，選擇建立政策。
3. 在 [建立新的資源控制政策頁面上](#)，輸入政策名稱和選用的政策描述。
4. (選用) 選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來新增一個或多個標籤。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱 [標記 AWS Organizations 資源](#)。

Note

在接下來的大部分步驟中，我們會討論使用 JSON 編輯器右側的控制項，逐元素建構政策。或者，您可以隨時在視窗左側的 JSON 編輯器中輸入文字。您可以直接輸入，或者可以使用複製和貼上。

5. 若要新增陳述式：
 - a. 在編輯器的右側編輯陳述式窗格中，在新增動作下，選擇 AWS 服務。

在您選擇右側的選項時，JSON 編輯器會隨即更新，在左側顯示相應的 JSON 政策。

- b. 選取服務之後，包含該服務可用動作的清單即會開啟。您可以選擇 All actions (所有動作)，或選擇您要拒絕的一個或多個個別動作。

左側的 JSON 會隨即更新，以包含您選取的動作。

Note

如果您選取個別動作，然後返回上一步並選取 All actions (所有動作)，`servicename:*` 的預期項目會新增至 JSON，但您之前選取的個別動作會留在 JSON 中，而不會移除。

- c. 如果您想要從其他服務新增動作，可以選擇 Statement (陳述式) 方塊頂部的 All Services (所有服務)，然後視需要重複之前的兩個步驟。
- d. 指定要包含在陳述式中的資源。
 - 在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。
 - 在 Add resource (新增資源) 對話方塊，從清單中選擇您要控制其資源的服務。您只能從在上一步選擇的服務中進行選擇。
 - 在 Resource Type (資源類型) 下，選擇您要控制的資源類型。
 - 完成資源 ARN 中的 Amazon Resource Name (ARN)，以識別您要控制存取的特定資源。您必須取代由大括號 { } 包圍的所有預留位置。您可以指定資源類型的 ARN 語法允許的萬用字元 (*)。如需您可在何處使用萬用字元的相關資訊，請參閱特定資源類型的[文件](#)。
 - 選擇 Add resource (新增資源)，以儲存您對政策的新增。JSON 中的 Resource 元素會反映您的新增或變更。資源元素為必要項目。

 Tip

如果您想要為所選取的服務指定所有資源，請選擇 All resources (所有資源) 選項，或 JSON 中直接編輯 Resource 語句來讀取 "Resource": "*"。

- e. (選用) 若要指定在政策陳述式生效時限制的條件，請在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。
 - 條件索引鍵 – 從清單中，您可以選擇所有 AWS 服務可用的任何條件索引鍵 (例如 aws:SourceIp)，或只針對您為此陳述式選取的其中一個服務選擇服務特定的索引鍵。
 - 限定詞 – (選用) 當請求具有多值內容索引鍵的多個值時，您可以指定[限定詞](#)以根據值測試請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[單一值與多值內容索引鍵](#)。若要檢查請求是否可以有多個值，請參閱服務授權參考中的[的動作、資源和條件索引鍵 AWS 服務](#)。
 - 預設值 – 針對政策中的條件索引鍵值，測試請求中的單一值。如果請求中的值符合政策中的值，則條件會傳回 true。如果政策指定多個值，則會將其視為「或」測試，如果請求值符合任何政策值，則條件會傳回 true。

- 對於請求中的任意值 – 當請求可以有多個值時，此選項會測試是否至少一個請求值符合政策中至少其中一個條件索引鍵值。如果請求中任一鍵值符合政策中的任一條件值，則條件會傳回 true。如果沒有相符金鑰或為 null 資料集，則條件會傳回 false。
- 對於請求中的所有值 – 當請求可以有多個值時，此選項會測試是否每一個請求值均符合政策中的條件索引鍵值。如果請求中每個鍵值至少符合政策中的一個值，則條件會傳回 true。如果請求中沒有鍵，或鍵值解析為 null 資料集 (例如空白字串)，則也會傳回 true。
- 運算子 – [運算子](#) 指定要進行的比較類型。顯示的選項取決於條件索引鍵的資料類型。例如，aws:CurrentTime 全域條件索引鍵可讓您從任何日期比較運算子中選擇，或 Null，您可以用於測試該值是否存在於請求中。

針對除 Null 測試之外的任何條件運算子，您可以選擇 [IfExists](#) 選項。

- 數值 – (選用) 指定您要測試請求的一個或多個值。

選擇新增條件。

如需有關條件索引鍵的詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。

- f. (選用) 若要使用 NotAction 元素拒絕存取除指定動作之外的所有動作，請在左側窗格中，將 "Effect": "Deny", 元素之後的 Action 替換為 NotAction。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：NotAction](#)。
6. (選用) 若要將另一個陳述式新增到政策，請選擇 Add statement (新增陳述式) 並使用視覺編輯器來建置下一個陳述式。
 7. 完成新增陳述式後，請選擇建立政策以儲存完成的 RCP。

您的新 RCP 會出現在組織的政策清單中。您現在可以[將 RCP 連接至根帳戶、OUs 帳戶或帳戶](#)。

AWS CLI & AWS SDKs

建立資源控制政策

您可以使用下列其中一個命令來建立 RCP：

- AWS CLI: [create-policy](#)

以下範例假設您已有名為 Deny-IAM.json 的檔案，且包含 JSON 政策文字。它使用該檔案來建立新的資源控制政策。

```
$ aws organizations create-policy \
  --content file://Deny-IAM.json \
  --description "Deny all IAM actions" \
  --name DenyIAMRCP \
  --type RESOURCE_CONTROL_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/resource_control_policy/p-i9j8k7l6m5",
      "Name": "DenyIAMRCP",
      "Description": "Deny all IAM actions",
      "Type": "RESOURCE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\": \"Statement1\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]} ]}"
  }
}
```

- AWS SDKs : [CreatePolicy](#)

Note

RCPs 不會對管理帳戶和少數其他情況生效。如需詳細資訊，請參閱[不受 RCPs 限制的資源和實體](#)。

建立宣告政策

最低許可

若要建立宣告政策，您需要執行下列動作的許可：

- organizations:CreatePolicy

AWS Management Console

建立宣告政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在[宣告政策](#)頁面上，選擇建立政策。
3. 在[為 EC2 建立新的宣告政策頁面上](#)，輸入政策名稱和選用的政策描述。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱[標記 AWS Organizations 資源](#)。
5. 您可以使用 Visual editor (視覺化編輯器) 建置政策，如本程序所述。您也可以直接在 JSON 索引標籤中輸入或貼上政策文字。如需宣告政策語法的詳細資訊，請參閱 [宣告性政策語法和範例](#)。

如果您選擇使用視覺化編輯器，請選取您要包含在宣告政策中的服務屬性。如需詳細資訊，請參閱[支援的 AWS 服務 和 屬性](#)。

6. 選擇新增服務屬性，然後根據您的規格設定 屬性。如需每個效果的詳細資訊，請參閱 [宣告性政策語法和範例](#)。
7. 當政策編輯完成時，請在頁面的右下角選擇 Create policy (建立政策)。

AWS CLI & AWS SDKs

建立宣告政策

您可以使用下列其中一項來建立宣告政策：

- AWS CLI: [create-policy](#)

1. 建立如下所示的宣告式政策，並將其存放在文字檔案中。

```
{
  "ec2_attributes": {
    "image_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

此宣告政策指定必須設定受政策影響的所有帳戶，以便新的 Amazon Machine Image (AMIs) 不可公開共享。如需宣告政策語法的詳細資訊，請參閱 [宣告性政策語法和範例](#)。

2. 匯入 JSON 政策檔案，以在組織中建立新的政策。在此範例中，之前的 JSON 檔案名稱為 `policy.json`。

```
$ aws organizations create-policy \
  --type DECLARATIVE_POLICY_EC2 \
  --name "MyTestPolicy" \
  --description "My test policy" \
  --content file://policy.json
{
  "Policy": {
    "Content": "{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":\n{\"@@assign\":\"block_new_sharing\"}}}}\".",
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5"
      "Arn": "arn:aws:organizations::o-aa111bb222:policy/\ndeclarative_policy_ec2/p-i9j8k7l6m5",
      "Description": "My test policy",
      "Name": "MyTestPolicy",
      "Type": "DECLARATIVE_POLICY_EC2"
    }
  }
}
```

- AWS SDKs : [CreatePolicy](#)

後續作業

建立宣告政策後，請使用[帳戶狀態報告](#)評估準備程度。然後，您可以強制執行基準組態。若要執行該操作，您可以[連接政策](#)至組織根、組織單位 (OU)、組織內的 AWS 帳戶，或這三者全部的組合。

建立備份政策

最低許可

若要建立備份政策，您需要具有執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

您可以透過下列兩種方式 AWS Management Console 之一，在 中建立備份政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 [@@assign 值設定運算子](#)，完全不支援存取[子控制運算子](#)。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

建立備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Backup policies](#) (備份政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create policy (建立政策) 頁面上，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。
5. 您可以使用 Visual editor (視覺化編輯器) 建置政策，如本程序所述。您也可以使用 JSON 索引標籤中輸入或貼上政策文字。如需備份政策語法的相關資訊，請參閱[備份政策語法和範例](#)。

如果您選擇使用 Visual editor (視覺化編輯器)，請選取適合您情境的備份選項。備份計劃由三個部分組成。如需這些備份計劃元素的詳細資訊，請參閱 AWS Backup 開發人員指南中的[建立備份計劃](#)和[指派資源](#)。

a. 備份計劃一般詳細資訊

- Backup plan name (備份計劃名稱) 只能由英數字元、連字號和底線字元組成。
- 您必須從清單中至少選取一個 Backup plan region (備份計劃區域)。計劃只能備份選取的 AWS 區域。

b. 一或多個備份規則，指定 AWS Backup 的運作方式和時機。每個備份規則定義下列項目：

- 包含備份頻率以及進行備份的時段的排程。

- 要使用的備份保存庫名稱。Backup vault name (備份保存庫名稱)只能由英數字元、連字號和底線字元組成。備份保存庫必須先存在，計劃才能順利執行。使用 AWS Backup 主控台或 AWS CLI 命令建立保存庫。
- (選用) 一或多個 Copy to region (複製到區域)規則，也將備份複製到其他 AWS 區域中的保存庫。
- 一或多個標籤鍵和值配對，連接至每次執行此備份計劃時建立的備份復原點。
- 生命週期選項，指定備份何時轉移至不常用的儲存體及備份何時到期。

選擇 Add rule (新增規則)，將您需要的每個規則新增至計劃。

如需關於備份規則的詳細資訊，請參閱 AWS Backup 開發人員指南中的[備份規則](#)。

- c. 資源指派，指定 AWS Backup 應該按照此計劃而備份的資源。指派是透過指定 AWS Backup 用於尋找和比對資源的標籤對來進行

- Resource assignment name (資源指派名稱)只能由英數字元、連字號和底線字元組成。
- 指定 IAM 角色，以便 AWS Backup 用於依名稱執行備份。

在主控台，您不需要指定整個 Amazon 資源名稱 (ARN)。角色名稱及其前綴 (指定角色類型) 都必須包括在內。前綴通常是 role 或 service-role，並以正斜線 (/) 與角色名稱分隔。例如，您可以輸入 role/MyRoleName 或 service-role/MyManagedRoleName。存放在基礎 JSON 中可轉換為完整 ARN。

 Important

指定的 IAM 角色必須已存在於套用政策的帳戶中。否則，雖然備份計劃可能成功啟動備份任務，但這些備份任務會失敗。

- 指定一個或多個資源標籤標籤鍵和標籤值組，以識別您想要備份的資源。如果有多個標籤值，請以逗號分隔值。

選擇 Add assignment (新增指派)，將每個設定的資源指派新增至備份計劃。

如需詳細資訊，請參閱AWS Backup 開發人員指南中的[將資源指派至備份計劃](#)。

6. 政策建立完成時，請選擇 Create policy (建立政策)。政策會出現在可用的備份政策清單中。

AWS CLI & AWS SDKs

建立備份政策

您可以使用下列其中一項來建立備份政策：

- AWS CLI: [create-policy](#)

將備份計劃建立為類似以下內容的 JSON 文字，並將其存放在文字檔案中。如需語法的完整規則，請參閱[備份政策語法和範例](#)。

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-north-1" ] },
      "rules": {
        "Hourly": {
          "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
          "start_backup_window_minutes": { "@@assign": "480" },
          "complete_backup_window_minutes": { "@@assign": "10080" },
          "lifecycle": {
            "move_to_cold_storage_after_days": { "@@assign": "180" },
            "delete_after_days": { "@@assign": "270" }
          },
          "target_backup_vault_name": { "@@assign": "FortKnox" },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:secondary-vault": {
              "lifecycle": {
                "move_to_cold_storage_after_days": { "@@assign": "10" },
                "delete_after_days": { "@@assign": "100" }
              }
            }
          }
        },
        "selections": {
          "tags": {
            "datatype": {
              "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/MyIamRole" },
              "tag_key": { "@@assign": "dataType" },
              "tag_value": { "@@assign": [ "PII" ] }
            }
          }
        }
      }
    }
  }
}
```

```

    }
  }
}

```

此備份計畫指定 AWS Backup 應備份受影響 中所有資源 AWS 帳戶，這些資源位於指定的 中，AWS 區域 且標籤的值 dataType 為 PII。

然後，匯入 JSON 政策檔案備份計畫，以在組織中建立新的政策備份計畫。請注意輸出中的政策 ARN 結尾的政策 ID。

```

$ aws organizations create-policy \
  --name "MyBackupPolicy" \
  --type BACKUP_POLICY \
  --description "My backup policy" \
  --content file://policy.json{
  "Policy": {
    "PolicySummary": {
      "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
      "Description": "My backup policy",
      "Name": "MyBackupPolicy",
      "Type": "BACKUP_POLICY"
    }
    "Content": "...a condensed version of the JSON policy document you
provided in the file...",
  }
}

```

- AWS SDKs : [CreatePolicy](#)

建立標籤政策

最低許可

若要建立標籤政策，您需要具有執行下列動作的許可：

- organizations:CreatePolicy

您可以透過下列兩種方式 AWS Management Console 之一，在 中建立標籤政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 [@@assign 值設定運算子](#)，完全不支援存取[子控制運算子](#)。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

AWS Management Console

您可以透過下列兩種方式 AWS Management Console 之一，在 中建立標籤政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 [@@assign 值設定運算子](#)，完全不支援存取[子控制運算子](#)。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

建立標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Tag policies](#) (標籤政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 Create policy (建立政策) 頁面上，輸入政策的 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以將一個或多個標籤新增至政策物件本身。這些標籤不是政策的一部分。若要執行此操作，請選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱[標記 AWS Organizations 資源](#)。
5. 您可以使用 Visual editor (視覺化編輯器) 建立標籤政策，如本程序所述。您也可以直接在 JSON 索引標籤中輸入或貼上標籤政策。如需標籤政策語法的相關資訊，請參閱[標籤政策語法](#)。

如果您選擇使用視覺化編輯器，請指定下列項目：

6. 針對 New Tag Key 1(新標籤鍵 1)，指定要新增的標籤鍵名稱。

7. 對於合規選項，您可以選取下列選項：

- a. 使用您在上面為標籤索引鍵指定的大寫 — 保持此選項清除（預設值），以指定如果有繼承的父標籤政策，應該定義標籤索引鍵的案例處理方式。

如果您要使用此政策來強制標籤鍵的特定大寫，請啟用此選項。如果您選取此選項，您為 Tag Key (標籤鍵) 指定的大寫，將覆寫父政策中指定的大小寫處理。

如果父政策不存在且您未選取此選項，則只有完全小寫字元的標籤鍵才視為合規。如需父政策中有關繼承的詳細資訊，請參閱[理解管理政策繼承](#)。

Tip

在建立標籤政策來定義標籤鍵及其大小寫處理時，請考慮使用[範例 1：定義整個組織的標籤鍵大小寫](#)中顯示的範例標籤政策作為指南。將此標籤政策連接至組織根目錄。稍後，您可以建立額外的標籤政策，並連接至 OU 或帳戶，以建立其他標記規則。

- b. 指定此標籤索引鍵的允許值 — 如果您想要將此標籤索引鍵的允許值新增至從父政策繼承的任何值，請啟用此選項。

依預設會清除此選項，這表示只有從父政策定義和繼承的那些值才視為合規。如果父政策不存在或未指定標籤值，則任何值 (包括完全沒有值) 都視為合規。

若要更新可接受的標籤值清單，請選取 Specify allowed values for this tag key (指定此標籤鍵的允許值)，然後選取 Specify values (指定值)。出現提示時，輸入新的值 (每個方塊一個值)，然後選擇 Save changes (儲存變更)。

8. 對於要強制執行的資源類型，您可以為此標籤選取防止不合規操作。

我們建議您清除此選項（預設值），除非您在使用標籤政策時有經驗。請確定您已檢閱[了解強制](#)中的建議，並全面測試。否則，可能會使組織帳戶中的使用者無法標記他們所需的資源。

如果您確實想要強制此標籤鍵合規，請選取此核取方塊，然後選取 Specify resource types (指定資源類型)。提示後，請選取要包含在政策中的資源類型。接著選擇 Save changes (儲存變更)。

⚠ Important

選取此選項後，任何操縱指定類型資源標籤的操作，僅在操作使標籤符合政策時才會成功。

9. (選用) 若要將另一個標籤鍵新增至此標籤政策，請選擇 Add tag key (新增標籤鍵)。然後執行步驟 6–9 來定義標籤鍵。
10. 標籤政策建置完成時，請選擇 Save Changes (儲存變更)。

AWS CLI & AWS SDKs

建立標籤政策

您可以使用下列其中一項來建立標籤政策：

- AWS CLI: [create-policy](#)

您可以使用任何文字編輯器來建立標籤政策。使用 JSON 語法，並在您選擇的位置中，以任何名稱和副檔名將標籤政策儲存為檔案。標籤政策最多可包含 2,500 個字元，包括空格。如需標籤政策語法的相關資訊，請參閱[標籤政策語法](#)。

建立標籤政策

1. 文字檔案中建立看起來類似下列內容的標籤政策：

testpolicy.json 的內容：

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      }
    }
  }
}
```

此標籤政策定義 CostCenter 標籤鍵。標籤可以接受或不接受任何值。這樣的政策表示，帶有 CostCenter 標籤的資源 (無論是否連接任何值) 都符合規定。

2. 建立包含檔案中政策內容的政策。為了便於閱讀，輸出中的額外空白字元已被截斷。

```
$ aws organizations create-policy \
  --name "MyTestTagPolicy" \
  --description "My Test policy" \
  --content file://testpolicy.json \
  --type TAG_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-a1b2c3d4e5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-a1b2c3d4e5",
      "Name": "MyTestTagPolicy",
      "Description": "My Test policy",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\n\n\"CostCenter\"\n}\n}\n}\n}"
  }
}
```

- AWS SDKs : [CreatePolicy](#)

建立聊天應用程式政策

最低許可

若要建立聊天應用程式政策，您需要執行下列動作的許可：

- `organizations:CreatePolicy`

AWS Management Console

您可以透過下列兩種方式 AWS Management Console 之一，在 中建立聊天應用程式政策：

- 視覺化編輯器，可讓您選擇選項，然後為您產生 JSON 政策文字。
- 文字編輯器，可讓您直接建立 JSON 政策文字。

視覺化編輯器讓程序變簡單，但彈性受限。若要建立第一個政策並熟悉使用政策，這是好方法。在了解政策的運作方式，並開始覺得受限於視覺化編輯器後，您可以自行編輯 JSON 政策文字，將進階功能新增至政策。視覺化編輯器只使用 [@@assign 值設定運算子](#)，完全不支援存取[子控制運算子](#)。只有在手動編輯 JSON 政策文字時，才能新增子控制運算子。

建立聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Chatbot 政策](#) 頁面上，選擇建立政策。
3. 在[建立新的聊天應用程式政策頁面上](#)，輸入政策名稱和選用的政策描述。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱[標記 AWS Organizations 資源](#)。
5. 您可以使用 Visual editor (視覺化編輯器) 建置政策，如本程序所述。您也可以使用 JSON 索引標籤輸入或貼上政策文字。如需聊天應用程式政策語法的詳細資訊，請參閱 [聊天應用程式政策語法和範例](#)。

如果您選擇使用視覺化編輯器，請透過指定聊天用戶端的存取控制來設定聊天應用程式政策。

- a. 為設定 Amazon Chime 聊天用戶端存取選擇下列其中一項
 - 拒絕鈴聲存取。
 - 允許 Chime 存取。
- b. 選擇下列設定 Microsoft Teams 聊天用戶端存取權的選項
 - 拒絕存取所有 Teams
 - 允許存取所有 Teams
 - 限制對具名 Teams 的存取
- c. 為設定 Slack 聊天用戶端存取選擇下列其中一項
 - 拒絕存取所有 Slack 工作區
 - 允許存取所有 Slack 工作區
 - 限制對具名 Slack 函式的存取

 Note

此外，您可以在聊天應用程式中選取將 Amazon Q Developer 用量限制為僅限私有 Slack 頻道。

d. 為設定 IAM 許可類型選取下列選項

- 啟用頻道層級 IAM 角色 — 所有頻道成員共用在頻道中執行任務的 IAM 角色許可。如果頻道成員需要相同的許可，則頻道角色是適當的。
- 啟用使用者層級 IAM 角色 — 頻道成員必須選擇 IAM 使用者角色才能執行動作（需要主控台存取權才能選擇角色）。如果頻道成員需要不同的許可，並且可以選擇其使用者角色，則使用者角色是適當的。

6. 政策建立完成時，請選擇 Create policy (建立政策)。此政策會出現在聊天機器人備份政策清單中。

AWS CLI & AWS SDKs

建立聊天應用程式政策

您可以使用下列其中一項來建立聊天應用程式政策：

- AWS CLI: [create-policy](#)

您可以使用任何文字編輯器來建立聊天應用程式政策。使用 JSON 語法，並將聊天應用程式政策儲存為檔案，並在您選擇的位置使用任何名稱和副檔名。聊天應用程式政策最多可有 ？ 個字元，包括空格。如需標籤政策語法的相關資訊，請參閱[聊天應用程式政策語法和範例](#)。

建立聊天應用程式政策

1. 在類似以下內容的文字檔案中建立聊天應用程式政策：

testpolicy.json 的內容：

```
{
  "chatbot": {
    "platforms": {
      "slack": {
        "client": {
          "@@assign": "enabled"
        },

```

```

        "workspaces": {
            "@@assign": [
                "Slack-Workspace-Id"
            ]
        },
        "default": {
            "supported_channel_types": {
                "@@assign": [
                    "private"
                ]
            }
        }
    },
    "microsoft_teams": {
        "client": {
            "@@assign": "disabled"
        }
    }
}
}
}

```

此聊天應用程式政策僅允許特定工作區中的私有 Slack 頻道、停用 Microsoft Teams，並支援所有[角色設定](#)。

2. 建立包含檔案中政策內容的政策。為了便於閱讀，輸出中的額外空白字元已被截斷。

```

$ aws organizations create-policy \
  --name "MyTestChatbotPolicy" \
  --description "My Test policy" \
  --content file://testpolicy.json \
  --type CHATBOT_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-a1b2c3d4e5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/chatbot_policy/p-a1b2c3d4e5",
      "Name": "MyTestChatApplicationsPolicy",
      "Description": "My Test policy",
      "Type": "CHATBOT_POLICY",
      "AwsManaged": false
    },

```

```
"Content": "{ \"chatbot\": { \"platforms\": { \"slack\": { \"client\": { \"@@assign\": \"enabled\" }, \"workspaces\": { \"@@assign\": [ \"Slack-Workspace-Id\" ] }, \"supported_channel_types\": { \"@@assign\": [ \"private\" ] } }, \"microsoft_teams\": { \"client\": { \"@@assign\": \"disabled\" } } } } } }
```

- AWS SDKs : [CreatePolicy](#)

建立 AI 服務選擇退出政策

最低許可

若要建立 AI 服務選擇退出政策，您需要具有執行下列動作的許可：

- organizations:CreatePolicy

AWS Management Console

建立 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI services opt-out policies](#) (AI 服務選擇退出政策) 頁面上，選擇 Create policy (建立政策)。
3. 在 [Create new AI services opt-out policy \(建立新的 AI 服務選擇退出政策\)](#) 頁面上，輸入 Policy name (政策名稱) 與選用的 Policy description (政策描述)。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱[標記 AWS Organizations 資源](#)。
5. 在 JSON 索引標籤中輸入或貼上政策文字。如需 AI 服務選擇退出政策語法的相關資訊，請參閱[AI 服務選擇退出政策語法和範例](#)。例如，您可以用作起點的政策，請參閱[AI 服務選擇退出政策範例](#)。
6. 當政策編輯完成時，請在頁面的右下角選擇 Create policy (建立政策)。

AWS CLI & AWS SDKs

建立 AI 服務選擇退出政策

您可以使用下列其中一項來建立標籤政策：

- AWS CLI: [create-policy](#)

1. 建立如下所示的 AI 服務選擇退出政策，並將其存放在文字檔案中。請注意，"optOut" 和 "optIn" 區分大小寫。

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

此 AI 服務選擇退出政策規定，除了 Amazon Rekognition 以外，受政策影響的所有帳戶都選擇退出所有 AI 服務。

2. 匯入 JSON 政策檔案，以在組織中建立新的政策。在此範例中，之前的 JSON 檔案名稱為 `policy.json`。

```
$ aws organizations create-policy \
  --type AISERVICES_OPT_OUT_POLICY \
  --name "MyTestPolicy" \
  --description "My test policy" \
  --content file://policy.json
{
  "Policy": {
    "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign\":"
    "\":\"optOut\"}}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":"
    "\":\"optIn\"}}}}",
    "PolicySummary": {
```

```
    "Id": "p-i9j8k7l6m5"
    "Arn": "arn:aws:organizations::o-aa111bb222:policy/aiservices_opt_out_policy/p-i9j8k7l6m5",
    "Description": "My test policy",
    "Name": "MyTestPolicy",
    "Type": "AISERVICES_OPT_OUT_POLICY"
  }
}
```

- AWS SDKs : [CreatePolicy](#)

建立 Security Hub 政策

最低許可

若要建立 Security Hub 政策，您需要執行下列動作的許可：

- organizations:CreatePolicy

AWS Management Console

建立 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Security Hub 政策](#) 頁面上，選擇建立政策。
3. 在 [建立新的 Security Hub 政策頁面上](#)，輸入政策名稱和選用的政策描述。
4. (選用) 您可以透過選擇 Add tag (新增標籤)，然後輸入一個鍵和一個選用值，來將一個或多個標籤新增至政策。將值留空會將其設定為空白字串；而不是 null。您可以在政策中連接最多 50 個標籤。如需詳細資訊，請參閱 [標記 AWS Organizations 資源](#)。
5. 在 JSON 程式碼方塊中輸入或貼上政策文字。如需 Security Hub 政策語法的相關資訊，請參閱 [Security Hub 政策語法和範例](#)。例如，您可以用作起點的政策，請參閱 [Security Hub 政策範例](#)。
6. 當政策編輯完成時，請在頁面的右下角選擇 Create policy (建立政策)。

AWS CLI & AWS SDKs

建立 Security Hub 政策

您可以使用下列其中一項來建立 Security Hub 政策：

- AWS CLI: [create-policy](#)

範例：建立在所有支援區域中啟用 Security Hub 的政策

以下範例假設您已有名為 `testPolicy_enableAllSupportedRegions.json` 的檔案，且包含 JSON 政策文字。它使用該檔案來建立新的 Security Hub 政策。

```
$ aws organizations create-policy \
  --content file:///./testPolicy_enableAllSupportedRegions.json \
  --name "testPolicy_enableAllSupportedRegions" \
  --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
  --type SECURITYHUB_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66ev7hgcvj",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/securityhub_policy/p-66ev7hgcvj",
      "Name": "testPolicy_enableAllSupportedRegions",
      "Description": "Test policy to enable securityhub in ALL_SUPPORTED Regions",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":\n  {\n    \"@@assign\": [\n      \"ALL_SUPPORTED\"\n    ]\n  },\n  \"disable_in_regions\": {\n    \"@@assign\": []\n  }\n}\n}"
  }
}
```

範例：建立政策，在所有支援的區域中啟用 Security Hub，但在 us-east-1 區域中停用

以下範例假設您已有名為 `testPolicy_enableAllSupportedRegions_Disable_us-east-1.json` 的檔案，且包含 JSON 政策文字。它使用該檔案來建立新的 Security Hub 政策。

```
$ aws organizations create-policy \
```

```

--content file:///./testPolicy_enableAllSupportedRegions_Disable_us-east-1.json
\
--name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
--description "Test policy to enable securityhub in ALL_SUPPORTED Regions but
disable in us-east-1 Region" \
--type SECURITYHUB_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66217dwpos",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66217dwpos",
      "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
      "Description": "Test policy to enable securityhub in ALL_SUPPORTED
Regions but disable in us-east-1 Region",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
{\n      \"@@assign\": [\n        \"ALL_SUPPORTED\"\n      ],\n    },\n
  \"disable_in_regions\": {\n    \"@@assign\": [\n      \"us-east-1\"\n    ]\n
  }\n }"
  }
}

```

- AWS SDKs : [CreatePolicy](#)

使用 更新組織政策 AWS Organizations

當您的政策需求變更時，您可以更新現有的政策。

本主題說明如何使用 更新政策 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [更新服務控制政策 \(SCP\)](#)
- [更新資源控制政策 \(RCP\)](#)
- [更新宣告政策](#)
- [更新備份政策](#)
- [更新標籤政策](#)

- [更新聊天應用程式政策](#)
- [更新 AI 服務選擇退出政策](#)
- [更新 Security Hub 政策](#)

更新服務控制政策 (SCP)

登入到您組織的管理帳戶時，您可以重新命名或變更政策的內容。變更 SCP 的內容會立即影響所有連接帳戶中的任何使用者、群組和角色。

最低許可

若要更新 SCP，您需要具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
4. 進行下列任一或所有變更：
 - 您可以在 Policy name (政策名稱) 中輸入新名稱，來重新命名政策。
 - 您可以在 Policy description (政策描述) 輸入新文字，來變更描述。
 - 您可以在左側窗格中以 JSON 格式編輯政策，來編輯政策文字。或者，您可以在右側的編輯器中選擇陳述式，同時使用控制項來變更其元素。如需每個控制項的詳細資訊，請參閱本主題稍早介紹的[建立 SCP 程序](#)。
5. 完成時，請選擇儲存變更。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項命令來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "MyRenamedPolicy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "Blocks all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\\\"*\\\"]}]}"
  }
}
```

下列範例會新增或變更服務控制政策的描述。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new policy description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
```

```

    "AwsManaged": false
  },
  "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\": \"Statement1\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]} ]}"
}

```

下列範例會指定包含新 JSON 政策文字的檔案，以變更 SCP 的政策文件。

```
$ aws organizations update-policy \
  --policy-id p-zlfw1r64
  --content file://MyNewPolicyText.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
  }
}
```

- AWS SDKs : `UpdatePolicy`

更新資源控制政策 (RCP)

登入到您組織的管理帳戶時，您可以重新命名或變更政策的內容。變更 RCP 的內容會立即影響所有連接帳戶中的任何資源。

 最低許可

若要更新 RCP，您需要執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在資源控制政策頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
4. 進行下列任一或所有變更：
 - 您可以在 Policy name (政策名稱) 中輸入新名稱，來重新命名政策。
 - 您可以在 Policy description (政策描述) 輸入新文字，來變更描述。
 - 您可以在左側窗格中以 JSON 格式編輯政策，來編輯政策文字。或者，您可以在右側的編輯器中選擇陳述式，同時使用控制項來變更其元素。如需每個控制項的詳細資訊，請參閱本主題稍早的[建立 RCP 程序](#)。
5. 完成時，請選擇儲存變更。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項命令來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "MyRenamedPolicy"
{
  "Policy": {
```



```

    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "Blocks all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\\\"*\\\"]}]}"
  }
}

```

下列範例會新增或變更資源控制政策的描述。

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new policy description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\\\"*\\\"]}]}"
  }
}

```

下列範例透過指定包含新 JSON 政策文字的檔案來變更 RCP 的政策文件。

```

$ aws organizations update-policy \
  --policy-id p-zlfw1r64
  --content file://MyNewPolicyText.json
{
  "Policy": {

```

```

    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\": [{\"Sid\":
\\\"AModifiedPolicy\\\",\\\"Effect\\\":\\\"Deny\\\",\\\"Action\\\": [\\\"iam:*\\\"],\\\"Resource\\\": [\\\"*
\\\"]}]}"
  }
}

```

- AWS SDKs : [UpdatePolicy](#)

更新宣告政策

最低許可

若要更新宣告式政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `"*`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `"*`) 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新宣告式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [宣告政策](#) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
4. 您可以輸入新的政策名稱、策略說明，或編輯 JSON 政策文字。如需宣告政策語法的詳細資訊，請參閱 [宣告性政策語法和範例](#)。

5. 政策更新完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名宣告式政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/declarative_policy_ec2/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Type": "DECLARATIVE_POLICY_EC2",
      "AwsManaged": false
    },
    "Content": "{\"ec2-configuration\":{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":{\"@assign\":\"block_new_sharing\"}}}}\"."
  }
}
```

下列範例會新增或變更宣告政策的描述。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/declarative_policy_ec2/p-i9j8k7l6m5",
      "Name": "Renamed policy",
```

```
        "Description": "My new description",
        "Type": "DECLARATIVE_POLICY_EC2",
        "AwsManaged": false
    },
    "Content": "{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":
{\"@@assign\":\"block_new_sharing\"}}}}\".
    }
}
```

- AWS SDKs : [UpdatePolicy](#)

更新備份政策

登入組織的管理帳戶後，您可以在組織中編輯需要變更的政策。

最低許可

若要更新備份政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在同一政策陳述式中指定 `Resource` 元素，其中包含要更新的政策 ARN (或「*」)
- `organizations:DescribePolicy`，並在同一政策陳述式中指定 `Resource` 元素，其中包含要更新的政策 ARN (或「*」)

AWS Management Console

更新備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Backup policies](#) (備份政策) 頁面上，選擇您要更新的政策名稱。
3. 選擇 Edit Policy (編輯政策)。
4. 您可以輸入新的政策名稱、政策描述。您可以使用視覺化編輯器，或直接編輯 JSON，來變更政策內容。
5. 政策更新完成時，請選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

建立備份政策

您可以使用下列其中一項來備份政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名備份政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Type": "BACKUP_POLICY",
      "AwsManaged": false
    },
    "Content": "{\\"plans\\":{\\"TestBackupPlan\\":{\\"regions\\":{\\"@@assign\\":
....TRUNCATED FOR BREVITY....  \\"@@assign\\":[\\"Yes\\"]}}}}}"
  }
}
```

下列範例會新增或變更備份政策的描述。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "BACKUP_POLICY",
      "AwsManaged": false
    }
  }
}
```

```

    },
    "Content": "{\\"plans\\":{\\"TestBackupPlan\\":{\\"regions\\":{\\"@@assign\\":
....TRUNCATED FOR BREVITY....  "@@assign\\":[\\"Yes\\"]}}}}}"
  }
}

```

下列範例會變更連接至備份政策的 JSON 政策文件。在此範例中，內容擷取自名為 `policy.json` 的檔案，其中包含以下文字：

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
      "rules": {
        "Hourly": {
          "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
          "start_backup_window_minutes": { "@@assign": "480" },
          "complete_backup_window_minutes": { "@@assign": "10080" },
          "lifecycle": {
            "move_to_cold_storage_after_days": { "@@assign": "180" },
            "delete_after_days": { "@@assign": "270" },
            "opt_in_to_archive_for_supported_resources": {"@@assign":
false}
          },
          "target_backup_vault_name": { "@@assign": "FortKnox" },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
              "lifecycle": {
                "move_to_cold_storage_after_days": { "@@assign":
"10" },
                "delete_after_days": { "@@assign": "100" },
                "opt_in_to_archive_for_supported_resources":
{"@@assign": false}
              }
            }
          }
        },
        "selections": {
          "tags": {
            "datatype": {

```

```
MyIamRole" },  
    "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/  
    "tag_key": { "@@assign": "dataType" },  
    "tag_value": { "@@assign": [ "PII" ] }  
  }  
}  
}  
}  
}
```

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "BACKUP_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"plans\":{\n\"TestBackupPlan\":{\n\"regions\":{\n\"@@assign\":
....TRUNCATED FOR BREVITY....    \"@@assign\":[\"Yes\"]}}}}}}}"
  }
}
```

- AWS SDKs : `UpdatePolicy`

更新標籤政策

 最低許可

若要更新標籤政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

- `organizations:DescribePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Tag policies](#) (標籤政策) 頁面上，選擇您要更新的標籤政策。
3. 選擇 Edit Policy (編輯政策)。
4. 您可以輸入新的政策名稱、政策描述。可以使用視覺化編輯器或直接編輯 JSON，來變更政策內容。
5. 標籤政策更新完成時，請選擇 Save Changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名標籤政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed tag policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
  },
}
```



```

      "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":\n\"CostCenter\"\n}\n}\n}\n\n"
    }
  }
}

```

下列範例會新增或變更標籤政策的描述。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new tag policy description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Description": "My new tag policy description",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\\n\\\"tags\\\":{\\n\\\"CostCenter\\\":{\\n\\\"tag_key\\\":{\\n\\\"@@assign\\\":
\\\"CostCenter\\\"\\n}\\n}\\n}\\n\\n\"
  }
}
```

下列範例會變更連接至 AI 服務選擇退出政策的 JSON 政策文件。在此範例中，內容擷取自名為 `policy.json` 的檔案，其中包含以下文字：

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
}
}
```

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Description": "My new tag policy description",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":{\"@@assign\":[\"ec2:instance\"]}}}}"
```

- AWS SDKs : [UpdatePolicy](#)

更新聊天應用程式政策

最低許可

若要更新聊天應用程式政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `"*`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `"*`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [聊天機器人政策](#) 頁面上，選擇您要更新的聊天應用程式政策。
3. 選擇 Edit Policy (編輯政策)。
4. 您可以輸入新的政策名稱、政策描述。可以使用視覺化編輯器或直接編輯 JSON，來變更政策內容。
5. 標籤政策更新完成時，請選擇 Save Changes (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名聊天應用程式政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed chat applications policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
      "Name": "Renamed chat applications policy",
      "Type": "CHATBOT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"chatbot\":{\"platforms\":{\"slack\":{\"client\":
{\"@@assign\":\"enabled\"},\"workspaces\":{\"@@assign\":[\"Slack-Workspace-Id\"]},\"default\":
{\"supported_channel_types\":{\"@@assign\":[\"private\"]}}},\"microsoft_teams\":{\"client\":
{\"@@assign\":\"disabled\"}}}}}"
  }
}
```

```
}
```

- AWS SDKs : [UpdatePolicy](#)

更新 AI 服務選擇退出政策

最低許可

若要更新 AI 服務選擇退出政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `"**"`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `"**"`) 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI services opt-out policies](#) (AI 服務選擇退出政策) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 `Edit policy` (編輯政策)。
4. 您可以輸入新的政策名稱、策略說明，或編輯 JSON 政策文字。如需 AI 服務選擇退出政策語法的相關資訊，請參閱 [AI 服務選擇退出政策語法和範例](#)。例如，您可以用作起點的政策，請參閱 [AI 服務選擇退出政策範例](#)。
5. 政策更新完成時，請選擇 `Save changes` (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名 AI 服務選擇退出政策。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
....TRUNCATED FOR BREVITY... :{\"@@assign\":{\"optIn\"}}}}}"
  }
}
```

下列範例會新增或變更 AI 服務選擇退出政策的描述。

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
....TRUNCATED FOR BREVITY... :{\"@@assign\":{\"optIn\"}}}}}"
  }
}
```

下列範例會變更連接至 AI 服務選擇退出政策的 JSON 政策文件。在此範例中，內容擷取自名為 `policy.json` 的檔案，其中包含以下文字：

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "comprehend": {
      "opt_out_policy": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "@@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"services\": {\n\"default\": {\n\"    ....TRUNCATED FOR BREVITY....    \"optIn\"\n}\n}\n}"
  }
}
```

- AWS SDKs : [UpdatePolicy](#)

更新 Security Hub 政策

最低許可

若要更新 Security Hub 政策，您必須具有執行下列動作的許可：

- `organizations:UpdatePolicy`，並在包含指定政策 (或 `"**"`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素
- `organizations:DescribePolicy`，並在包含指定政策 (或 `"**"`) 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

更新 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Security Hub 政策](#) 頁面上，選擇您要更新的政策名稱。
3. 在政策的詳細資訊頁面上，選擇 `Edit policy` (編輯政策)。
4. 您可以輸入新的政策名稱、策略說明，或編輯 JSON 政策文字。如需 Security Hub 政策語法的相關資訊，請參閱 [Security Hub 政策語法和範例](#)。例如，您可以用作起點的政策，請參閱 [Security Hub 政策範例](#)。
5. 政策更新完成時，請選擇 `Save changes` (儲存變更)。

AWS CLI & AWS SDKs

更新政策

您可以使用下列其中一項來更新政策：

- AWS CLI: [update-policy](#)

下列範例會重新命名 Security Hub 政策。

```
$ aws organizations update-policy \
  --policy-id p-66ev7hgcvj \
  --name "Renamed policy"
{
```

```

    "Policy": {
      "PolicySummary": {
        "Id": "p-66ev7hgcvj",
        "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
        "Name": "Renamed policy",
        "Type": "SECURITYHUB_POLICY",
        "AwsManaged": false
      },
      "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
{\n      \"@assign\": [\n        \"ALL_SUPPORTED\"\n      ],\n    },\n  \"disable_in_regions\": {\n    \"@assign\": []\n  }\n}\n"
    }
  }
}

```

下列範例會新增或變更 Security Hub 政策的描述。

```

$ aws organizations update-policy \
  --policy-id p-66ev7hgcvj \
  --name "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66ev7hgcvj",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
      "Name": "My new description",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
{\n      \"@assign\": [\n        \"ALL_SUPPORTED\"\n      ],\n    },\n  \"disable_in_regions\": {\n    \"@assign\": []\n  }\n}\n"
    }
  }
}

```

- AWS SDKs : [UpdatePolicy](#)

使用 編輯連接至組織政策的標籤 AWS Organizations

本主題說明如何使用 編輯附加政策的標籤 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [編輯連接至服務控制政策 \(SCP\) 的標籤](#)
- [編輯連接至資源控制政策 \(RCP\) 的標籤](#)
- [編輯連接至宣告政策的標籤](#)
- [編輯連接至備份政策的標籤](#)
- [編輯連接至標籤政策的標籤](#)
- [編輯連接至聊天應用程式政策的標籤](#)
- [編輯連接至 AI 服務選擇退出政策的標籤](#)
- [編輯連接至 Security Hub 政策的標籤](#)

編輯連接至服務控制政策 (SCP) 的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至 SCP 的標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接至您組織的 SCP 的標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 SCP 的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在政策詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 進行下列任一或所有變更：

- 透過在舊值上輸入新值來變更標籤的值。您無法直接修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，然後新增含有新標籤鍵的標籤。
- 選擇 Remove (移除) 以移除現有的標籤。
- 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。

5. 完成時，請選擇儲存變更。

AWS CLI & AWS SDKs

編輯連接至 SCP 的標籤

您可以使用下列其中一項命令來編輯連接至 SCP 的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至資源控制政策 (RCP) 的標籤

當您登入組織的管理帳戶時，您可以新增或移除連接到 RCP 的標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接至 AWS 組織中 RCP 的標籤，您必須具有下列許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 RCP 的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在資源控制政策頁面上，選擇具有您要編輯之標籤的政策名稱。
3. 在政策詳細資訊頁面上，選擇標籤索引標籤，然後選擇管理標籤。
4. 進行下列任一或所有變更：
 - 透過在舊值上輸入新值來變更標籤的值。您無法直接修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，然後新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 完成時，請選擇儲存變更。

AWS CLI & AWS SDKs

編輯連接至 RCP 的標籤

您可以使用下列其中一個命令來編輯連接至 RCP 的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至宣告政策的標籤

當您登入組織的管理帳戶時，您可以新增或移除連接到宣告政策的標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接到 AWS 組織中宣告政策的標籤，您必須具有下列許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接到宣告政策的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [宣告政策](#) 頁面上，選擇具有您要編輯之標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接到宣告政策的標籤

您可以使用下列其中一個命令來編輯連接到宣告政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至備份政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至備份政策的標籤。如需標記的相關資訊，請參閱 [標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接至您組織的備份政策標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` (僅限主控台 – 導覽至政策)

- `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至備份政策的標記

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. [備份政策](#) 頁面
3. 選擇您要編輯其標籤的政策名稱。

政策詳細資訊頁面會隨即出現。

4. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
5. 您可以在此頁面上執行任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
6. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至備份政策的標記

您可以使用下列其中一項命令來編輯連接至備份政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至標籤政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至標籤政策的標籤。若要執行此動作，請執行下列步驟。

最低許可

若要編輯連接至您組織的標籤政策標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` (僅限主控台 – 導覽至政策)
- `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至標籤政策的標記

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Tag policies](#) (標籤政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至標籤政策的標記

您可以使用下列其中一項命令來編輯連接至標籤政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至聊天應用程式政策的標籤

當您登入組織的管理帳戶時，您可以新增或移除連接到聊天應用程式政策的標籤。若要執行此動作，請執行下列步驟。

最低許可

若要編輯連接到組織中聊天應用程式政策的標籤，您必須具有下列許可：

- `organizations:DescribeOrganization` (僅限主控台 – 導覽至政策)
- `organizations:DescribePolicy` (僅限主控台 – 導覽至政策)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至聊天應用程式政策的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Chatbot 政策](#) 頁面上，選擇具有您要編輯之標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。

5. 在您完成所有要進行的新增、移除和編輯之後，選擇 **Save changes** (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至聊天應用程式政策的標籤

您可以使用下列其中一個命令來編輯連接至聊天應用程式政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至 AI 服務選擇退出政策的標籤

登入您的組織的管理帳戶時，您可以新增或移除連接至 AI 服務選擇退出政策的標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接至您組織的 AI 服務選擇退出政策標籤，您必須擁有以下許可：

- `organizations:DescribeOrganization` – 僅在使用 Organizations 主控台時才需要
- `organizations:DescribePolicy` – 僅在使用 Organizations 主控台時才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

編輯連接至 AI 服務選擇退出政策的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI services opt-out policies](#) (AI 服務選擇退出政策) 頁面上，選擇您要編輯的附有標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 **Tags** (標籤) 索引標籤，然後選擇 **Manage tags** (管理標籤)。
4. 您可以在此頁面上執行任一動作：

- 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接至 AI 服務選擇退出政策的標籤

您可以使用下列其中一項命令來編輯連接至 AI 服務選擇退出政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

編輯連接至 Security Hub 政策的標籤

當您登入組織的管理帳戶時，您可以新增或移除連接到 Security Hub 政策的標籤。如需標記的相關資訊，請參閱[標記 AWS Organizations 資源](#)。

最低許可

若要編輯連接到組織中 Security Hub 政策的標籤，您必須具有下列許可：

- organizations:DescribeOrganization – 僅在使用 Organizations 主控台時才需要
- organizations:DescribePolicy – 僅在使用 Organizations 主控台時才需要
- organizations:TagResource
- organizations:UntagResource

AWS Management Console

編輯連接到 Security Hub 政策的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在 [Security Hub 政策](#) 頁面上，選擇具有您要編輯之標籤的政策名稱。
3. 在所選政策的詳細資訊頁面上，選擇 Tags (標籤) 索引標籤，然後選擇 Manage tags (管理標籤)。
4. 您可以在此頁面上執行任一動作：
 - 透過在舊值上輸入新值來編輯任何標籤的值。您無法修改標籤鍵。若要變更標籤鍵，您必須刪除含有舊標籤鍵的標籤，並新增含有新標籤鍵的標籤。
 - 選擇 Remove (移除) 以移除現有的標籤。
 - 新增標籤鍵值組。選擇 Add tag (新增標籤)，然後在提供的方塊中輸入新的標籤鍵名稱和選用值。如果您將 Value (值) 方塊保留空白，則值為空白字串；而不是 null。
5. 在您完成所有要進行的新增、移除和編輯之後，選擇 Save changes (儲存變更)。

AWS CLI & AWS SDKs

編輯連接到 Security Hub 政策的標籤

您可以使用下列其中一個命令來編輯連接到 Security Hub 政策的標籤：

- AWS CLI: [tag-resource](#) and [untag-resource](#)
- AWS SDKs : [TagResource](#) 和 [UntagResource](#)

使用 連接組織政策 AWS Organizations

本主題說明如何使用 連接政策 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [使用 連接政策 AWS Organizations](#)

使用 連接政策 AWS Organizations

最低許可

若要連接政策，您必須具有執行下列動作的許可：

- `organizations:AttachPolicy`

最低許可

若要將授權政策 (SCP 或 RCP) 連接至根帳戶、OU 或帳戶，您需要執行下列動作的許可：

- `organizations:AttachPolicy`，並在包含 "*" 或指定政策的 Amazon Resource Name (ARN) 和您要連接政策的根、OU 或帳戶的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

Service control policies (SCPs)

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接 SCP 政策。

導覽至根、OU 或帳戶以連接 SCP 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接 SCP 的根、OU 或帳戶旁邊的核取方塊，然後選擇。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 Service control policies (服務控制政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

Policies (政策) 索引標籤上的連接的 SCP 清單會更新，以包含新的新增項目。政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可。

導覽至政策以連接 SCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。

4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

Targets (目標) 索引標籤上的連接的 SCP 清單會更新，以包含新的新增項目。政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可。

Resource control policies (RCPs)

您可以透過導覽至政策或要連接政策的根帳戶、OU 或帳戶來連接 RCP。

若要透過導覽至根、OU 或帳戶來連接 RCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在頁面上 [AWS 帳戶](#)，導覽至 ，然後選擇您要連接 RCP 的根帳戶、OU 帳戶或帳戶旁的核取方塊。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在政策索引標籤中，在資源控制政策的項目中，選擇連接。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

政策索引標籤上連接的 RCPs 清單會更新為包含新的新增項目。政策變更會立即生效，影響連接帳戶中的資源許可，或連接根帳戶或 OU 下的所有帳戶許可。

導覽至政策以連接 RCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在資源控制政策頁面上，選擇要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

目標索引標籤上連接的 RCPs 清單會更新為包含新增項目。政策變更會立即生效，影響連接帳戶中的資源許可，或連接根帳戶或 OU 下的所有帳戶許可。

Declarative policies

您可以透過導覽至政策或要連接政策的根帳戶、OU 或帳戶來連接宣告性政策。

若要透過導覽至根、OU 或帳戶來連接宣告政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在政策索引標籤的宣告政策項目中，選擇連接。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

政策索引標籤上連接的宣告政策清單會更新為包含新的新增項目。政策變更會立即生效。

導覽至政策以連接宣告式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [宣告政策](#) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

目標索引標籤上連接的宣告政策清單會更新為包含新的新增項目。政策變更會立即生效。

Backup policies

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接備份政策。

導覽至根、OU 或帳戶以連接備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 Backup policies (備份政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

Policies (政策) 索引標籤上的連接的備份政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Backup policies \(備份政策\)](#) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

Targets (目標) 索引標籤上的連接的備份政策清單會更新，以包含新的新增項目。政策變更會立即生效。

Tag policies

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接標籤政策。

導覽至根、OU 或帳戶以連接標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。

3. 在 Policies (政策) 索引標籤的 Tag policies (標籤政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

Policies (政策) 索引標籤上的連接的標籤政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Tag policies](#) (標籤政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。

5. 選擇連接政策。

Targets (目標) 索引標籤上的連接的標籤政策清單會更新，以包含新的新增項目。政策變更會立即生效。

Chat applications policies

您可以透過導覽至政策或要連接政策的根帳戶、OU 或帳戶，來連接聊天應用程式政策。

導覽至根、OU 或帳戶來連接聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。

3. 在政策索引標籤的聊天應用程式政策項目中，選擇連接。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

政策索引標籤上連接的聊天應用程式政策清單會更新為包含新增項目。政策變更會立即生效。

導覽至政策以連接聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Chatbot 政策](#) 頁面上，選擇要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

目標索引標籤上連接的聊天應用程式政策清單會更新為包含新增項目。政策變更會立即生效。

AI services opt-out policies

您可以導覽至政策或連接政策的根、OU 或帳戶，以連接 AI 服務選擇退出政策。

導覽至根、OU 或帳戶以連接 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在 Policies (政策) 索引標籤的 AI service opt-out policies (AI 服務選擇退出政策) 項目中，選擇 Attach (連接)。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

Policies (政策) 索引標籤上的連接的 AI 服務選擇退出政策清單會更新，以包含新的新增項目。政策變更會立即生效。

導覽至政策以連接 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI services opt-out policies](#) (AI 服務選擇退出政策) 頁面上，選擇您要連接的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

Targets (目標) 索引標籤上的連接的 AI 服務選擇退出政策清單會更新，以包含新的新增項目。政策變更會立即生效。

Security Hub policies

您可以透過導覽至政策或要連接政策的根帳戶、OU 或帳戶，來連接 Security Hub 政策。

若要透過導覽至根、OU 或帳戶來連接 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面上，導覽至您要連接政策的根、OU 或帳戶的名稱並選擇。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
3. 在政策索引標籤中，在 Security Hub 政策的項目中，選擇連接。
4. 尋找您所需的政策，然後選擇 Attach policy (連接政策)。

政策索引標籤上連接的 Security Hub 政策清單會更新為包含新的新增項目。政策變更會立即生效。

導覽至政策以連接 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Security Hub 政策](#) 頁面上，選擇要連接的政策名稱。

3. 在 Targets (目標) 索引標籤上，選擇 Attach (連接)。
4. 選擇您要連接政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
5. 選擇連接政策。

目標標籤上連接的 Security Hub 政策清單會更新，以包含新增項目。政策變更會立即生效。

AWS CLI & AWS SDKs

連接政策

下列程式碼範例示範如何使用 AttachPolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
```

```
{
    IAmazonOrganizations client = new AmazonOrganizationsClient();
    var policyId = "p-000000000";
    var targetId = "r-0000";

    var request = new AttachPolicyRequest
    {
        PolicyId = policyId,
        TargetId = targetId,
    };

    var response = await client.AttachPolicyAsync(request);

    if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
    {
        Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
    }
    else
    {
        Console.WriteLine("Was not successful in attaching the policy.");
    }
}
}
```

- 如需 API 詳細資訊，請參閱適用於 .NET 的 AWS SDK 《API 參考》中的 [AttachPolicy](#)。

CLI

AWS CLI

將政策連接至根帳戶、OU 或帳戶

範例 1

下列範例示範如何將服務控制政策 (SCP) 連接至 OU：

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id ou-examplerootid111-exampleouid111
```

範例 2

下列範例示範如何將服務控制政策直接連接至 帳戶：

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id 333333333333
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [AttachPolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
    or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- 如需 API 詳細資訊，請參閱《適用於 AWS Python (Boto3) 的 SDK API 參考》中的 [AttachPolicy](#)。

政策變更會立即影響連接的帳戶中 IAM 使用者和角色或連接的根或 OU 下所有帳戶的許可

使用 分離組織政策 AWS Organizations

本主題說明如何使用 分離政策 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [使用 分離政策 AWS Organizations](#)

使用 分離政策 AWS Organizations

最低許可

若要從組織根目錄、OU 或帳戶分離政策，您必須具有執行下列動作的許可：

- `organizations:DetachPolicy`

Note

您無法從根、OU 或 帳戶分離最後一個授權政策 (SCP 或 RCP)。每個根目錄、OU 和帳戶都必須至少連接一個 SCP 和 RCP。

AWS Management Console

Service control policies (SCPs)

您可以導覽至政策或您要分離政策的根、OU 或帳戶，以分離 SCP 政策。

導覽至連接的目標根、OU 或帳戶以分離 SCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在 Policies (政策) 索引標籤上，選擇您要分離的 SCP 旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的 SCP 清單隨即更新。分離 SCP 導致的 SCP 變更會立即生效。例如，對於先前連接的帳戶，或先前連接的根或 OU 下的帳戶，分離 SCP 會立即影響其中 IAM 使用者和角色的許可。

導覽至政策以分離 SCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的 SCP 清單隨即更新。分離 SCP 導致的 SCP 變更會立即生效。例如，對於先前連接的帳戶，或先前連接的根或 OU 下的帳戶，分離 SCP 會立即影響其中 IAM 使用者和角色的許可。

Resource control policies (RCPs)

您可以透過導覽至政策或要從中分離政策的根帳戶、OU 或帳戶來分離 RCP。從實體分離 RCP 之後，該 RCP 不再適用於受現在分離的實體影響的任何資源。

Note

您無法分離 `RCPFullAWSAccess` 政策

RCPFullAWSAccess 政策會自動連接到根、每個 OU，以及您組織中的每個帳戶。您無法分離此政策。

透過導覽至其連接的根帳戶、OU 或帳戶來分離 RCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在政策索引標籤上，選擇您要分離的 RCP 旁的選項按鈕，然後選擇分離。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的 RCPs 清單已更新。分離 RCP 所造成的政策變更會立即生效。例如，分離 RCP 會立即影響先前連接之帳戶或先前連接之組織根帳戶或 OU 下的 IAM 使用者和角色的許可。

導覽至政策以分離 RCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在資源控制政策頁面上，選擇要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的 RCPs 清單已更新。分離 RCP 所造成的政策變更會立即生效。例如，分離 RCP 會立即影響先前連接之帳戶或先前連接之組織根帳戶或 OU 下的 IAM 使用者和角色的許可。

Declarative policies

您可以透過導覽至政策或要從中分離政策的根帳戶、OU 或帳戶，來分離宣告性政策。

導覽至其連接的根帳戶、OU 或帳戶，以分離宣告政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在政策索引標籤上，選擇您要分離的宣告政策旁的選項按鈕，然後選擇分離。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的宣告政策清單已更新。政策變更會立即生效。

導覽至政策以分離宣告政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [宣告政策](#) 頁面上，選擇要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的宣告政策清單已更新。政策變更會立即生效。

Backup policies

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離備份政策。

導覽至連接的根、OU 或帳戶以分離備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。

3. 在 Policies (政策) 索引標籤上，選擇您要分離的備份政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的備份政策清單會隨即更新。政策變更會立即生效。

導覽至政策以分離備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Backup policies](#) (備份政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的備份政策清單會隨即更新。政策變更會立即生效。

Tag policies

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離標籤政策。

導覽至連接的根、OU 或帳戶以分離標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在 Policies (政策) 索引標籤上，選擇您要分離的標籤政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的標籤政策清單會隨即更新。政策變更會立即生效。

導覽至標籤政策以分離備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Tag policies](#) (標籤政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的標籤政策清單會隨即更新。政策變更會立即生效。

Chat applications policies

您可以透過導覽至政策或要從中分離政策的根帳戶、OU 或帳戶，來分離聊天應用程式政策。

導覽至其連接的根帳戶、OU 或帳戶，以分離聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在政策索引標籤上，選擇您要分離的聊天應用程式政策旁的選項按鈕，然後選擇分離。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

已更新連接的聊天應用程式政策清單。政策變更會立即生效。

導覽至政策以分離聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Chatbot 政策](#) 頁面上，選擇要從根、OU 或帳戶分離的政策名稱。

3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。

4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

已更新連接的聊天應用程式政策清單。政策變更會立即生效。

AI services opt-out policies

您可以導覽至政策或分離接政策的根、OU 或帳戶，以分離 AI 服務選擇退出政策。

導覽至連接的根、OU 或帳戶以分離 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。

3. 在 Policies (政策) 索引標籤上，選擇您要分離的 AI 服務選擇退出政策旁邊的選項按鈕，然後選擇 Detach (分離)。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

已更新連接 AI 服務選擇退出政策的清單。政策變更會立即生效。

導覽至政策以分離 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AI services opt-out policies](#) (AI 服務選擇退出政策) 頁面上，選擇您要從根、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇



以尋找您所需的 OU 和帳戶。

4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

已更新連接 AI 服務選擇退出政策的清單。政策變更會立即生效。

Security Hub policies

您可以透過導覽至政策或要從中分離政策的根帳戶、OU 或帳戶，來分離 Security Hub 政策。

導覽至其連接的根帳戶、OU 或帳戶，以分離 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [AWS 帳戶](#) 頁面導覽至您要從中分離政策的根、OU 或帳戶。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。選擇根、OU 或帳戶的名稱。
3. 在政策索引標籤上，選擇您要分離的 Security Hub 政策旁的選項按鈕，然後選擇分離。
4. 在確認對話方塊中，選擇 Detach policy (分離政策)。

連接的 Security Hub 政策清單已更新。政策變更會立即生效。

導覽至政策以分離 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Security Hub 政策](#) 頁面上，選擇要從根帳戶、OU 或帳戶分離的政策名稱。
3. 在 Targets (目標) 索引標籤上，選擇您要分離政策的根、OU 或帳戶旁的選項按鈕。您可能需要展開 OU (選擇 )，以尋找您所需的 OU 和帳戶。
4. 請選擇分離。
5. 在確認對話方塊中，選擇 Detach (分離)。

連接的 Security Hub 政策清單已更新。政策變更會立即生效。

AWS CLI & AWS SDKs

連接政策

下列程式碼範例示範如何使用 DetachPolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
```

```
};

var response = await client.DetachPolicyAsync(request);

if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
{
    Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
}
else
{
    Console.WriteLine("Could not detach the policy.");
}
}
```

- 如需 API 詳細資訊，請參閱適用於 .NET 的 AWS SDK 《API 參考》中的 [DetachPolicy](#)。

CLI

AWS CLI

從根帳戶、OU 或帳戶分離政策

下列範例示範如何從 OU 分離政策：

```
aws organizations detach-policy --target-id ou-examplerootid111-exampleouid111
--policy-id p-examplepolicyid111
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [DetachPolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
    attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- 如需 API 詳細資訊，請參閱《適用於 AWS Python (Boto3) 的 SDK API 參考》中的 [DetachPolicy](#)。

政策變更會立即生效，如果適用，會影響連接帳戶或連接根帳戶或 OU 下所有帳戶的 IAM 使用者、角色和資源的許可。

取得組織政策的相關資訊

本主題說明各種取得組織中政策詳細資訊的方法。這些程序適用於所有政策類型。您必須在組織根上啟用政策類型，才能將該類型的政策連接至該組織根中的任何實體。

主題

- [列出所有政策](#)
- [列出連接到根、OU 或帳戶的政策](#)
- [列出政策連接的所有根帳戶、OU 和帳戶](#)
- [取得關於政策的詳細資訊](#)

列出所有政策

最低許可

若要列出您的組織內的政策，您必須擁有以下許可：

- `organizations:ListPolicies`

您可以在 [中](#) 或使用 AWS Command Line Interface (AWS CLI) 命令 `AWS Management Console` 或 AWS SDK 操作來檢視組織中的政策。

AWS Management Console

列出組織中的所有政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Policies](#) (政策) 頁面上，選擇您要列出的政策類型。

如果已啟用指定的政策類型，主控台會顯示組織中目前可用的所有該類型政策的清單。

3. 返回 [Policies](#) (政策) 頁面，然後針對每個政策類型重複執行此操作。

AWS CLI & AWS SDKs

下列程式碼範例示範如何使用 `ListPolicies`。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
using System;  
using System.Threading.Tasks;  
using Amazon.Organizations;
```



```
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };

        var response = new ListPoliciesResponse();
        try
        {
            do
            {
                response = await client.ListPoliciesAsync(request);
                response.Policies.ForEach(p => DisplayPolicies(p));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            }
            while (response.NextToken is not null);
        }
        catch (AWSOrganizationsNotInUseException ex)
```

```

        {
            Console.WriteLine(ex.Message);
        }
    }

    /// <summary>
    /// Displays information about the Organizations policies associated
    /// with an organization.
    /// </summary>
    /// <param name="policy">An Organizations policy summary to display
    /// information on the console.</param>
    private static void DisplayPolicies(PolicySummary policy)
    {
        string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

        Console.WriteLine(policyInfo);
    }
}

```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API Reference 中的 [ListPolicies](#)。

CLI

AWS CLI

擷取特定類型組織中所有政策的清單

下列範例示範如何取得篩選條件參數所指定的 SCPs 清單：

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

輸出包含具有摘要資訊的政策清單：

```

{
    "Policies": [
        {
            "Type": "SERVICE_CONTROL_POLICY",
            "Name": "AllowAllS3Actions",
            "AwsManaged": false,
            "Id": "p-examplepolicyid111",

```

```

        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
        "Description": "Enables account admins to delegate
permissions for any S3 actions to users and roles in their accounts."
    },
    {
        "Type": "SERVICE_CONTROL_POLICY",
        "Name": "AllowAllEC2Actions",
        "AwsManaged": false,
        "Id": "p-examplepolicyid222",
        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
        "Description": "Enables account admins to delegate
permissions for any EC2 actions to users and roles in their accounts."
    },
    {
        "AwsManaged": true,
        "Description": "Allows access to every operation",
        "Type": "SERVICE_CONTROL_POLICY",
        "Id": "p-FullAWSAccess",
        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
        "Name": "FullAWSAccess"
    }
]
}

```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [ListPolicies](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```

def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

```

```

:param policy_filter: The kind of policies to return.
:param orgs_client: The Boto3 Organizations client.
:return: The list of policies found.
"""
try:
    response = orgs_client.list_policies(Filter=policy_filter)
    policies = response["Policies"]
    logger.info("Found %s %s policies.", len(policies), policy_filter)
except ClientError:
    logger.exception("Couldn't get %s policies.", policy_filter)
    raise
else:
    return policies

```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API Reference 中的 [ListPolicies](#)。

列出連接到根、OU 或帳戶的政策

最低許可

若要列出連接到您組織內的根、組織單位 (OU) 或帳戶的政策，您必須擁有以下許可：

- `organizations:ListPoliciesForTarget`，並在包含指定目標 (或 `"*"`) 的 Amazon 資源名稱 (ARN) 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

列出直接連接到指定的根、OU 或帳戶的所有政策

- 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
- 在 [AWS 帳戶](#) 頁面上，選擇您要檢視其政策的根、OU 或帳戶的名稱。您可能需要展開 OU (選擇



以尋找您想要的 OU。

) ,

3. 在根、OU 或帳戶頁面上，選擇 Policies (政策) 索引標籤。

Policies (政策) 索引標籤會顯示連接至該根、OU 或帳戶的所有政策，並依政策類型分組。

AWS CLI & AWS SDKs

列出直接連接到指定的根、OU 或帳戶的所有政策

您可以使用下列其中一項命令來列出連接到實體的政策：

- AWS CLI: [list-policies-for-target](#)

下列範例會列出連接至指定 OU 的所有服務控制政策。您必須同時指定根、OU 或帳戶的 ID，以及您想要列出的政策類型。

```
$ aws organizations list-policies-for-target \
  --target-id ou-a1b2-f6g7h222 \
  --filter SERVICE_CONTROL_POLICY
{
  "Policies": [
    {
      "Id": "p-FullAWSAccess",
      "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess",
      "Name": "FullAWSAccess",
      "Description": "Allows access to every operation",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": true
    }
  ]
}
```

- AWS SDKs : [ListPoliciesForTarget](#)

列出政策連接的所有根帳戶、OU 和帳戶

最低許可

若要列出政策連接的實體，您必須擁有以下許可：

- `organizations:ListTargetsForPolicy`，並在包含指定政策 (或 `"*"`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

列出已連接指定政策的所有根、OU 和帳戶

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在[政策](#)頁面上，選擇政策類型，然後選擇您要檢查其附件的政策名稱。
3. 選擇 Targets (目標)索引標籤，以顯示所選政策連接的每個根、OU 和帳戶的資料表。

AWS CLI & AWS SDKs

列出已連接指定政策的所有根、OU 和帳戶

您可以使用下列其中一項命令來列出擁有政策的實體：

- AWS CLI: [list-targets-for-policy](#)

下列範例顯示指定政策的根、OU 和帳戶的所有連接。

```
$ aws organizations list-targets-for-policy \
  --policy-id p-FullAWSAccess
{
  "Targets": [
    {
      "TargetId": "ou-a1b2-f6g7h111",
      "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h111",
      "Name": "testou2",
      "Type": "ORGANIZATIONAL_UNIT"
    },
    {
      "TargetId": "ou-a1b2-f6g7h222",
      "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h222",
      "Name": "testou1",
      "Type": "ORGANIZATIONAL_UNIT"
    }
  ]
}
```

```

    },
    {
      "TargetId": "123456789012",
      "Arn": "arn:aws:organizations::123456789012:account/o-aa111bb222/123456789012",
      "Name": "My Management Account (bisdavid)",
      "Type": "ACCOUNT"
    },
    {
      "TargetId": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "Type": "ROOT"
    }
  ]
}

```

- AWS SDKs : [ListTargetsForPolicy](#)

取得關於政策的詳細資訊

最低許可

若要顯示政策的詳細資訊，您必須擁有以下許可：

- `organizations:DescribePolicy`，並在包含指定政策 (或 `""`) 的 ARN 的相同政策陳述式中具有 `Resource` 元素

AWS Management Console

取得關於政策的詳細資訊

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Policies](#) (政策) 頁面上，選擇您要檢查的政策類型，然後選擇政策名稱。

政策頁面顯示關於政策的可用資訊，包括其 ARN、描述和連接的目標。

- **Content** (內容) 索引標籤會以 JSON 格式顯示政策的目前內容。
- **Targets** (目標) 索引標籤會顯示政策連接的根、OU 和帳戶的清單。

- Tags (標籤) 索引標籤會顯示附加至政策的標籤。注意：Tags (標籤) 索引標籤不適用於 AWS 受管政策。

若要編輯政策，請選擇 Edit policy (編輯政策)。由於每個政策類型都有不同的編輯需求，因此，請參閱建立和更新指定政策類型之政策的指示。

AWS CLI & AWS SDKs

下列程式碼範例示範如何使用 DescribePolicy。

CLI

AWS CLI

取得政策的相關資訊

下列範例示範如何請求政策的相關資訊：

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

輸出包含政策物件，其中包含政策的詳細資訊：

```
{
  "Policy": {
    "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*\"\n    }\n  ]\n}",
    "PolicySummary": {
      "Arn": "arn:aws:organizations::111111111111:policy/o-exampleorgid/service_control_policy/p-examplepolicyid111",
      "Type": "SERVICE_CONTROL_POLICY",
      "Id": "p-examplepolicyid111",
      "AwsManaged": false,
      "Name": "AllowAllS3Actions",
      "Description": "Enables admins to delegate S3 permissions"
    }
  }
}
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [DescribePolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API 參考中的 [DescribePolicy](#)。

使用 刪除組織政策 AWS Organizations

如果您不再需要某項政策，則將該政策從所有 OU 和帳戶中分離後，即可刪除政策。

本主題說明如何使用 刪除政策 AWS Organizations。政策會定義您要套用至 群組的控制項 AWS 帳戶。

主題

- [使用 刪除政策 AWS Organizations](#)

使用 刪除政策 AWS Organizations

登入到您的組織的管理帳戶時，您可以刪除在您的組織中不再需要的政策。

您必須先將政策從所有連接的實體分離，才能刪除政策。

Note

- 您無法刪除任何 AWS 受管 SCP，例如名為的 `SCPFullAWSAccess`。
- 您無法刪除任何 AWS 受管 RCP，例如名為的 `RCPRCPFullAWSAccess`。

最低許可

若要刪除政策，您需要執行下列動作的許可：

- `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

刪除 SCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Service control policies](#) (服務控制政策) 頁面上，選擇您要刪除的 SCP 名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Resource control policies (RCPs)

刪除 RCP

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [資源控制政策](#) 頁面上，選擇您要刪除的 RCP 名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Declarative policies

刪除宣告政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [宣告政策](#) 頁面上，選擇您要刪除的政策名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Backup policies

刪除備份政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 從 [Backup policies \(備份政策\)](#) 頁面中，選擇您要刪除的備份政策名稱。
3. 您必須先將您要刪除的備份政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。

4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Tag policies

刪除標籤政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [標籤政策](#) 頁面上，選擇您要刪除的政策。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Chat applications policies

刪除聊天應用程式政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Chatbot 政策](#) 頁面上，選擇您要刪除的政策名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AI services opt-out policies

刪除 AI 服務選擇退出政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在 [AI 服務選擇退出政策](#) 頁面上，選擇您要刪除的政策名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

Security Hub policies

刪除 Security Hub 政策

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Security Hub 政策](#) 頁面上，選擇您要刪除的政策名稱。
3. 您必須先將您要刪除的政策從所有根、OU 和帳戶分離。選擇 Targets (目標) 索引標籤，再選擇每個根、OU 或顯示於 Targets (目標) 清單中帳戶旁邊的選項按鈕，然後選擇 Detach (分離)。在確認對話方塊中，選擇 Detach (分離)。重複操作，直至移除所有目標。
4. 在頁面頂端，選擇 Delete (刪除)。
5. 在確認對話方塊中，輸入政策的名稱，然後選擇 Delete (刪除)。

AWS CLI & AWS SDKs

刪除政策

下列程式碼範例示範如何使用 DeletePolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
using System;
```

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

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API Reference 中的 [DeletePolicy](#)。

CLI

AWS CLI

刪除政策

下列範例示範如何從組織刪除政策。此範例假設您之前已從所有實體分離政策：

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [DeletePolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def delete_policy(policy_id, orgs_client):  
    """  
    Deletes a policy.  
  
    :param policy_id: The ID of the policy to delete.  
    :param orgs_client: The Boto3 Organizations client.  
    """  
    try:  
        orgs_client.delete_policy(PolicyId=policy_id)  
        logger.info("Deleted policy %s.", policy_id)  
    except ClientError:  
        logger.exception("Couldn't delete policy %s.", policy_id)  
        raise
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API Reference 中的 [DeletePolicy](#)。

標記 AWS Organizations 資源

標籤是您新增至 AWS 資源的自訂屬性標籤，可讓您更輕鬆地識別、組織和搜尋資源。每個標籤有兩個部分：

- 標籤鍵 (例如，CostCenter、Environment 或 Project)。標籤鍵最大長度為 128 個字元且區分大小寫。
- 標籤值 (例如 111122223333 或 Production)。標籤值最大長度為 256 個字元，且與標籤鍵一樣需要區分大小寫。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。忽略標籤值基本上等同於使用空字串。

如需標籤鍵或值中允許哪些字元的詳細資訊，請參閱 Resource Groups 標記 API 參考中的[標籤 API 的標籤參數](#)。

您可使用標籤來依照用途、擁有者、環境或其他條件分類資源。如需詳細資訊，請參閱[標記 AWS 資源的最佳實務](#)。

Tip

使用[標籤政策](#)，協助將組織帳戶中各資源的標籤實作標準化。

主題

- [考量事項](#)
- [使用標籤](#)
- [新增、更新和移除標籤](#)

考量事項

AWS Organizations 當您登入管理帳戶時，支援下列標記操作：

您可以將標籤新增至下列組織資源

- AWS 帳戶
- 組織單位

- 組織的根
- 政策

您可以在下列時間新增標籤

- [建立資源時](#) – 在 Organizations 主控台中指定標籤，或使用 Tags 參數與其中一個 Create API 操作來指定標籤。這不適用於組織的根。
- [建立資源之後](#) – 使用 Organizations 主控台，或呼叫 [TagResource](#) 操作。

其他考量事項

您可以使用 主控台或呼叫 [ListTagsForResource](#) 操作 AWS Organizations，在 中檢視任何可標記資源上的標籤。

您可以使用主控台或呼叫 [UntagResource](#) 操作指定要移除的鍵，來從資源中移除標籤。

使用標籤

標籤可讓您按對您有用的任何類別分組資源，從而協助您整理組織中的資源。例如，您可以指派追蹤擁有部門的「部門」標記。您可以指派「環境」標籤，來追蹤指定的資源是否屬於 alpha、beta、gamma 或生產環境的一部分。

您也可以使用標籤執行以下動作：

- [在您的資源上強制執行標記標準。](#)
- [控制誰可以存取您的資源。](#)

新增、更新和移除標籤

登入您的組織的管理帳戶時，您可以為組織中的資源新增標籤。

建立資源時新增標籤

最低許可

若要在建立資源時將標籤新增至資源，您需要具有以下許可：

- 建立指定類型之資源的許可
- `organizations:TagResource`
- `organizations:ListTagsForResource` – 僅在使用 Organizations 主控台時才需要

您可以在建立以下資源時包含連接至該資源的標籤鍵和值。

- AWS 帳戶
 - [建立的帳戶](#)
 - [受邀帳戶](#)
- [組織單位 \(OU\)](#)
- 政策
 - [服務控制政策](#)
 - [資源控制政策](#)
 - [宣告政策](#)
 - [備份政策](#)
 - [標籤政策](#)
 - [聊天應用程式政策](#)
 - [AI 服務選擇退出政策](#)

組織根會在您初始建立組織時建立，因此，您只能將標籤作為現有資源新增至組織。

新增或更新現有資源的標籤

您還可以新增標籤或更新連接至現有資源的標籤值。

最低許可

若要將標籤新增或更新至組織中的資源，您需要具有以下許可：

- `organizations:TagResource`
- `organizations:ListTagsForResource` – 僅在使用 Organizations 主控台時才需要

若要從組織的資源中移除標籤，您需要具有以下許可：

- `organizations:UntagResource`

AWS Management Console

新增、更新或移除現有資源的標籤

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 導覽並選擇帳戶、根、OU 或政策，然後按一下其名稱以開啟其詳細資訊頁面。
3. 在 Tags (標籤) 索引標籤上，選擇 Manage tags (管理標籤)。
4. 您可以新增標籤、修改現有標籤的值或移除標籤。

若要新增標籤，請選擇 Add tag (新增標籤)，然後輸入標籤的 Key (鍵) 和選用的 Value (值)。

若要移除標籤，請選擇 Remove (移除)。

標籤鍵與值皆區分大小寫。使用您要標準化的大小寫。您還必須遵守任何適用標籤政策的要求。

5. 視需要重複上一個步驟。
6. 選擇儲存變更。

AWS CLI & AWS SDKs

將標籤新增或更新至現有資源

您可以使用下列其中一個命令，將標籤新增至組織中的可標記資源：

- AWS CLI : [tag-resource](#)
- AWS SDKs : [TagResource](#)

從組織的資源中刪除標籤

您可以使用下列其中一項命令來刪除標籤：

- AWS CLI : [untag-resource](#)
- AWS SDKs : [UntagResource](#)

的多方核准 AWS Organizations

多方核准是 的一項功能[AWS Organizations](#)，可讓您透過分散式核准程序保護預先定義的操作清單。使用多方核准來建立核准工作流程，並將安全程序轉換為以團隊為基礎的決策。

何時使用多方核准：

- 您需要符合「絕不信任，一律驗證」的零信任原則
- 您需要確保正確的人能夠以正確的方式存取正確的事物
- 您需要對敏感或關鍵操作進行分散式決策
- 您需要防範敏感或關鍵資源的意外操作
- 您需要針對稽核或合規原因進行正式審核和核准

如需詳細資訊，請參閱 [《多方核准使用者指南》中的什麼是多方核准](#)。

與其他 AWS Organizations 搭配使用 AWS 服務

您可以使用受信任存取來啟用您指定的支援 AWS 服務，稱為受信任服務，以代表您在組織及其帳戶中執行任務。這包括授予許可給信任的服務，但不會影響使用者或角色的許可。啟用存取權後，受信任的服務可在需要該角色時，在您組織的每個帳戶中建立一個稱為服務連結角色的 IAM 角色。該角色擁有的許可政策，會允許信任的服務執行該服務文件中所述的任務。這可讓您指定您想要信任的服務代表您在組織的帳戶中維護的設定和組態詳細資訊。受信任的服務只有在需要於帳戶上執行管理動作時，才會建立服務連結角色，而且不一定會在組織的所有帳戶中執行。

Important

我們強烈建議您，當選項可用時，請僅使用信任服務的主控制台，或其 AWS CLI 或 API 操作對等項目來啟用和停用信任存取。這可讓受信任的服務在啟用受信任的存取時執行任何必要的初始化，例如在停用受信任的存取時，建立任何必要的資源和任何必要的資源清除。

如需如何使用受信任的服務來啟用或停用組織的受信任服務存取的相關資訊，請參閱 [AWS 服務您可以搭配使用 AWS Organizations](#) 的支援受信任的存取欄下方的進一步了解連結。

如果您使用 Organizations 主控台、CLI 命令或 API 操作來停用存取權，則會導致發生下列動作：

- 服務無法再在您組織的帳戶中建立服務連結角色。這意味著服務無法代表您在組織的任何新帳戶上執行操作。服務仍然可以在較舊的帳戶中執行操作，直至服務完成從 AWS Organizations 中清除。
- 除非附加至您角色的 IAM 政策明確允許這些操作，否則服務無法再在組織的成員帳戶中執行任務。這包括從成員帳戶到管理帳戶，或委派管理員帳戶 (如相關) 的任何資料彙總。
- 某些服務會偵測到這一點，並清除與整合相關的任何剩餘的資料或資源，而其他服務會停止存取組織，但會保留任何歷史資料和組態，以針對可能的重新啟用整合提供支援。

而使用其他服務的主控制台或命令來停用整合，可確保其他服務可以清除僅用於整合所需的任何資源。服務如何清除組織帳戶中的資源取決於該服務。如需詳細資訊，請參閱其他 AWS 服務的安全文件。

啟用信任的存取所需的許可

受信任存取需要兩個服務的許可：AWS Organizations 和受信任的服務。若要啟用信任的存取，請選擇以下其中一個案例：

- 如果您的登入資料同時具有 AWS Organizations 和信任服務的許可，請使用信任服務提供的工具（主控台或 AWS CLI）來啟用存取。這可讓服務 AWS Organizations 代表您在 中啟用受信任存取，並建立服務在組織中操作所需的任何資源。

這些登入資料的最低許可如下：

- `organizations:EnableAWSServiceAccess`. 您也可以使用 `organizations:ServicePrincipal` 條件金鑰搭配此操作，來限制這些操作對核准的服務委託人名稱清單所做的請求。如需詳細資訊，請參閱[條件索引鍵](#)。
- `organizations:ListAWSServiceAccessForOrganization` – 如果您使用 AWS Organizations 主控台，則為必要項目。
- 信任的服務所需的最低許可取決於服務。如需詳細資訊，請參閱信任的服務的文件。
- 如果一個人擁有 中具有許可的登入資料，AWS Organizations 但其他人擁有信任服務中具有許可的登入資料，請依序執行這些步驟：
 1. 擁有 中具有許可的登入資料的人員 AWS Organizations 應使用 AWS Organizations 主控台 AWS CLI、或 AWS SDK 來啟用受信任服務的受信任存取。在執行以下步驟 (步驟 2) 時，這會授予其他服務的許可，以在組織中執行所需的組態。

最低 AWS Organizations 許可如下：

- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` – 只有在您使用 AWS Organizations 主控台時才需要

如需在 中啟用信任存取的步驟 AWS Organizations，請參閱 [如何啟用或停用信任的存取](#)。

2. 擁有信任的服務中許可的憑證的人員，可讓該服務與 AWS Organizations 搭配使用。這會指示服務執行任何必要的初始化，例如建立讓信任的服務在組織中操作所需的任何資源。如需詳細資訊，請參閱服務特定指示，位於[AWS 服務 您可以搭配 使用 AWS Organizations](#)。

停用信任的存取所需的許可

當您不想允許信任的服務在您的組織上或其帳戶上運作，請選擇以下其中一個案例。

Important

停用信任的服務存取不會防止具有適當的許可的使用者和角色使用該服務。若要完全封鎖使用者和角色存取 AWS 服務，您可以移除授予該存取權的 IAM 許可，也可以在其中使用[服務控制政策 SCPs](#) AWS Organizations。

您只能將 SCP 套用至成員帳戶。SCP 不會套用至管理帳戶。建議您[不要在管理帳戶中執行服務](#)。而是在成員帳戶中執行，您可以在這裡使用 SCP 控制安全性。

- 如果您的登入資料同時具有 AWS Organizations 和信任服務的許可，請使用信任服務可用的工具（主控台或 AWS CLI）來停用存取。此服務會藉由移除不再需要的資源，以及代表您停用 AWS Organizations 中服務的信任的存取來進行清理。

這些登入資料的最低許可如下：

- `organizations:DisableAWSServiceAccess`。您也可以使用 `organizations:ServicePrincipal` 條件金鑰搭配此操作，來限制這些操作對核准的服務委託人名稱清單所做的請求。如需詳細資訊，請參閱[條件索引鍵](#)。
- `organizations:ListAWSServiceAccessForOrganization` – 如果您使用 AWS Organizations 主控台，則為必要項目。
- 信任的服務所需的最低許可取決於服務。如需詳細資訊，請參閱信任的服務的文件。
- 如果中具有許可的登入資料 AWS Organizations 不是信任服務中具有許可的登入資料，請依下列順序執行這些步驟：
 - 擁有信任的服務中許可的人員會先使用該服務停用存取。這會指示信任的服務透過移除信任的存取所需的資源來進行清理。如需詳細資訊，請參閱服務特定指示，位於[AWS 服務 您可以搭配使用 AWS Organizations](#)。
 - 具有許可的人員接著 AWS Organizations 可以使用 AWS Organizations 主控台 AWS CLI 或 AWS SDK 來停用受信任服務的存取。這會從組織及其帳戶移除信任的服務的許可。

最低 AWS Organizations 許可如下：

- `organizations:DisableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` – 只有在您使用 AWS Organizations 主控台時才需要

如需在 中停用信任存取的步驟 AWS Organizations，請參閱 [如何啟用或停用信任的存取](#)。

如何啟用或停用信任的存取

如果您只有 的許可，AWS Organizations 而且想要代表其他服務的管理員啟用或停用對組織的信任存取 AWS，請使用下列程序。

Important

我們強烈建議您，當選項可用時，請僅使用信任服務的主控制台，或其 AWS CLI 或 API 操作對等項目來啟用和停用信任存取。這可讓受信任的服務在啟用受信任的存取時執行任何必要的初始化，例如在停用受信任的存取時，建立任何必要的資源和任何必要的資源清除。

如需如何使用受信任的服務來啟用或停用組織的受信任服務存取的相關資訊，請參閱 [AWS 服務 您可以搭配 使用 AWS Organizations](#) 的支援受信任的存取欄下方的進一步了解連結。

如果您使用 Organizations 主控台、CLI 命令或 API 操作來停用存取權，則會導致發生下列動作：

- 服務無法再在您組織的帳戶中建立服務連結角色。這意味著服務無法代表您在組織的任何新帳戶上執行操作。服務仍然可以在較舊的帳戶中執行操作，直至服務完成從 AWS Organizations 中清除。
- 除非附加至您角色的 IAM 政策明確允許這些操作，否則服務無法再在組織的成員帳戶中執行任務。這包括從成員帳戶到管理帳戶，或委派管理員帳戶 (如相關) 的任何資料彙總。
- 某些服務會偵測到這一點，並清除與整合相關的任何剩餘的資料或資源，而其他服務會停止存取組織，但會保留任何歷史資料和組態，以針對可能的重新啟用整合提供支援。

而使用其他服務的主控制台或命令來停用整合，可確保其他服務可以清除僅用於整合所需的任何資源。服務如何清除組織帳戶中的資源取決於該服務。如需詳細資訊，請參閱其他服務的文件 AWS。

AWS Management Console

啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [服務](#) 頁面，尋找您要啟用的服務的資料列，然後選擇其名稱。
3. 選擇 Enable trusted access (啟用信任存取)。
4. 在確認對話方塊中，勾選顯示啟用受信任的存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任存取。
5. 如果您啟用存取，請告訴 AWS 其他服務的管理員，他們現在可以讓其他服務使用 AWS Organizations。

若要停用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在[服務](#)頁面，尋找您要停用的服務的資料列，然後選擇其名稱。
3. 請等候直到其他服務的管理員告知您已停用服務並且已清除資源為止。
4. 在確認對話方塊中，輸入 **disable**，然後選擇停用受信任的存取。

AWS CLI, AWS API

啟用或停用受信任的服務存取

您可以使用下列 AWS CLI 命令或 API 操作來啟用或停用信任的服務存取：

- AWS CLI：AWS organizations [enable-aws-service-access](#)
- AWS CLI：AWS organizations [disable-aws-service-access](#)
- AWS API：[EnableAWSServiceAccess](#)
- AWS API：[DisableAWSServiceAccess](#)

AWS Organizations 和服務連結角色

AWS Organizations 使用 [IAM 服務連結角色](#)，讓信任的服務能夠在組織的成員帳戶中代表您執行任務。設定信任的服務並授權它來與您的組織整合時，該服務可以請求 AWS Organizations 在其成員帳戶中建立服務連結角色。信任的服務會視需要以非同步方式執行此動作，但不一定會同時在組織的所有帳戶中建立。服務連結角色具有預先定義的 IAM 許可，允許受信任的服務僅在該帳戶內執行特定任務。一般而言，AWS 會管理所有服務連結角色，這表示您通常無法更改角色或連接的政策。

為了讓它可行，當您在組織中建立帳戶或接受將您的現有帳戶加入組織的邀請時，AWS Organizations 會為該成員帳戶佈建名為 `AWSServiceRoleForOrganizations` 的服務連結角色。只有 AWS Organizations 服務本身可以擔任此角色。角色具有允許 AWS Organizations 為其他角色建立服務連結角色的許可 AWS 服務。此服務連結角色會出現在所有組織中。

雖然我們不建議這麼做，如果您的組織只啟用了[合併帳單功能](#)，則絕不會使用名為 `AWSServiceRoleForOrganizations` 的服務連結角色，您可以將其刪除。如果您稍後想要在組織中啟用[所有功能](#)，則需要該角色，您必須將它還原。當您開始啟用所有功能的程序時，會發生下列檢查：

- 對於獲邀加入組織的每個成員帳戶 – 帳戶管理員會收到請求，請求接受啟用所有功能。若要成功同意請求，管理員必須同時擁有 `organizations:AcceptHandshake` 和 `iam:CreateServiceLinkedRole` 許可，如果服務連結角色 (`AWSServiceRoleForOrganizations`) 尚不存在。如果 `AWSServiceRoleForOrganizations` 角色已存在，管理員只需要 `organizations:AcceptHandshake` 許可即可接受請求。當管理員同意請求時，如果服務連結角色不存在，會 AWS Organizations 建立該角色。
- 對於在組織中建立的每個成員帳戶 – 帳戶管理員會收到請求，請求重新建立服務連結角色。(成員帳戶的管理員不會收到啟用所有功能的請求，因為管理帳戶 (之前稱為「主帳戶」) 的管理員會被視為建立成員帳戶的擁有者。) 當成員帳戶管理員接受請求時，AWS Organizations 會建立服務連結角色。管理員必須同時擁有 `organizations:AcceptHandshake` 和 `iam:CreateServiceLinkedRole` 許可，才能成功接受交握。

在組織中啟用所有功能之後，您不再可以從任何帳戶刪除 `AWSServiceRoleForOrganizations` 服務連結角色。

 Important

AWS Organizations SCPs 永遠不會影響服務連結角色。這些角色不受任何 SCP 的限制。

使用 `AWSServiceRoleForDeclarativePoliciesEC2Report` 服務連結角色

Organizations `AWSServiceRoleForDeclarativePoliciesEC2Report` 會使用服務連結角色來描述成員帳戶的帳戶屬性狀態，以建立宣告政策報告。角色的許可是在 中定義 [AWS 受管政策：DeclarativePoliciesEC2Report](#)。

AWS 服務 您可以搭配 使用 AWS Organizations

透過 AWS Organizations，您可以將多個 合併 AWS 帳戶 為單一組織，大規模執行帳戶管理活動。合併帳戶可簡化您使用其他的方式 AWS 服務。您可以使用 中的多帳戶管理服務 AWS Organizations 搭配 select AWS 服務，對組織成員的所有帳戶執行任務。

下表列出 AWS 服務 您可以與 搭配使用的 AWS Organizations，以及在全組織層級使用每個服務的好處。

受信任的存取 – 您可以啟用相容的 AWS 服務，以跨 AWS 帳戶 組織中的所有 執行操作。如需詳細資訊，請參閱[與其他 AWS Organizations 搭配使用 AWS 服務](#)。

的委派管理員 AWS 服務 – 相容 AWS 服務可以將組織中 AWS 的成員帳戶註冊為該服務中組織帳戶的管理員。如需詳細資訊，請參閱[AWS 服務 該 的委派管理員與 Organizations 搭配使用](#)。

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS 帳戶管理 管理 AWS 帳戶 組織所有的詳細資訊和中繼資料。	管理 AWS 帳戶 組織中所有的帳戶詳細資訊、替代聯絡人和區域。	 是 進一步了解	 是 進一步了解	
AWS Application Migration Service AWS Application Migration Service 可讓公司在無相容性問題、效能中斷或長切換時段的情況下，lift-and-shift AWS 大量實體、虛擬或雲端伺服器。	您可以管理跨多個帳戶的大規模遷移。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
AWS Artifact 下載 AWS 安全合規報告，例如 ISO 和 PCI 報告。	可以代表組織中的所有成員帳戶接受協議。	 是 進一步了解	 否	
AWS Audit Manager 自動化持續收集證據，協助您稽核雲端服務的使用情況。	持續稽核組織中多個帳戶的 AWS 使用情形，以簡化您評估風險與合規的方式。	 是 進一步了解	 是 進一步了解	
AWS Backup 管理及監視組織中所有帳戶的備份。	您可以為整個組織或組織單位 (OU) 中的帳戶群組設定及管理備份計劃。您可以集中監視所有帳戶的備份。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS 帳單與成本管理 提供 AWS 雲端財務管理資料的概觀，並協助您更快、更明智地做出決策。	如果適用，允許分割成本分配資料擷取 AWS Organizations 資訊，並針對您已選擇使用的分割成本分配資料服務收集遙測資料。 如需詳細資訊，請參閱 Billing and Cost Management 使用者指南中的 什麼是 AWS 帳單與成本管理？ 。	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
AWS CloudFormation Stacksets 以單一操作建立、更新或刪除跨多個帳戶與區域的堆疊。	管理帳戶或委派管理員帳戶中的使用者可以建立具有服務受管許可的堆疊集，將堆疊執行個體部署至組織中的帳戶。	 是 進一步了解	 是 進一步了解	
AWS CloudTrail 針對帳戶啟用監管、合規、操作和風險稽核。	管理帳戶或委派管理員帳戶中的使用者可以建立組織追蹤或事件資料存放區，其中會記錄組織中所有成員帳戶的所有事件。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
Amazon CloudWatch AWS 即時監控您的 AWS 資源和您在 上執行的應用程式。您可以使用 CloudWatch 來收集和追蹤指標，這些指標是您可以針對資源和應用程式測量的變數。	與 Organizations 整合在 CloudWatch 中有兩個優點。首先，透過與 Organizations 整合，您可以使用 CloudWatch 從 CloudWatch 主控台的中央檢視探索和了解 AWS 資源的遙測組態狀態。 其次，當您可以在 CloudWatch 中使用網路流量監視器來取得網路	是 進一步了解	是 進一步了解	

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
	效能指標的可見性時，透過與 Organizations 整合，您可以檢視多個帳戶中資源的網路效能資訊，而不只是一個帳戶。			

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Compute Optimizer 取得 AWS 運算最佳化建議。	您可以分析您組織帳戶中的所有資源以獲得最佳化建議。 如需詳細資訊，請參閱AWS Compute Optimizer 使用者指南中的 Compute Optimizer 支援的帳戶。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Config 評定、稽核和評估 AWS 資源的組態。	您可以取得整個組織的合規狀態檢視。您也可以使用 AWS Config API 操作 來管理組織中所有 AWS 帳戶的 AWS Config 規則和一致性套件。 您可以使用委派的管理員帳戶，從 AWS Organizations 中組織的所有成員帳戶彙總資源組態與合規資料。如需詳細	 是 進一步了解	 是 進一步了解： Config 規則 一致性套件 多帳戶多區域資料彙整	

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
	資訊，請參閱 AWS Config 《開發人員指南》中的 註冊委派管理員 。			

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Control Tower 設定和管控安全、合規的多帳戶 AWS 環境。	您可以設定登陸區域，這是所有 AWS 資源的多帳戶環境。此環境包含組織和組織實體。您可以使用此環境來強制執行所有的合規法規 AWS 帳戶。 如需詳細資訊，請參閱 AWS Control Tower 使用者指南中的 如何 AWS Control Tower 以及 透過 AWS Organizat	 是 進一步了解	 否	

AWS 服務	搭配使用的優點	支援受信任存取	支援委派的管理員	
	AWS Organizations 管理帳戶。			
AWS 成本最佳化中心 收集跨 AWS 最佳化產品的成本建議。	您可以輕鬆識別、篩選和彙總 AWS Organizations 成員帳戶和 AWS 區域中 AWS 的成本最佳化建議。 如需詳細資訊，請參閱 Cost Optimization Hub 使用者指南中的 Cost Optimization Hub。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
Amazon Detective 從日誌資料產生視覺化效果，以便分析、調查並快速識別安全問題清單或可疑活動的根本原因。	您可以整合 Amazon Detective 與 AWS Organizations，以確保您的 Detective 行為圖表可讓您了解所有組織帳戶的活動。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
Amazon DevOps Guru 分析營運資料和應用程式指標與事件，以識別與正常操作模式不同的行為。當 DevOps Guru 檢測到操作問題或風險時，會通知使用者。	您可以與整合 AWS Organizations，以管理整個組織中所有帳戶的洞見。您可以委派管理員檢視、排序和篩選來自所有帳戶的洞察，以取得所有受監控應用程式的組織範圍運作狀態。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Directory Service 在 AWS 雲端中設定和執行目錄，或將您的 AWS 資源與現有的內部部署 Microsoft Active Directory 連線。	您可以將 AWS Directory Service 與整合 AWS Organizations，跨多個帳戶和區域中的任何 VPC 無縫共用目錄。	 是 進一步了解	 否	

AWS 服務	搭配 使用的優點 AWS Organizations	支援受信 信任存取	支援委派的管理員	
Amazon EventBridge AWS 即時監控您的 AWS 資源和您在 上執行的應用程式。	您可以啟用在組織中的所有 Amazon EventBridge Events、先前的 Amazon CloudWatch Events 帳戶共享。 如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 在 AWS 帳戶之間傳送和接收 Amazon EventBridge 事件 。	 否	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon Elastic Compute Cloud Amazon VPC IP Address Manager (IPAM) 在 AWS 雲端中提供隨需、可擴展的運算容量。	讓 Organizations 管理員在使用宣告性政策功能時，建立其組織中帳戶現有組態的報告。	 是 進一步了解	 否	
Amazon Elastic Kubernetes Service Amazon EKS 儀表板提供跨 AWS 雲端 Kubernetes 叢集的彙總可見性和管理。	讓 Organizations 管理員檢視叢集資源的合併儀表板資料，包括整個組織的版本分佈、運作狀態和升級需求。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS Firewall Manager 跨帳戶和應用程式，集中設定和管理 web 應用程式的防火牆規則。	您可以集中設定和管理組織中所有帳戶的 AWS WAF 規則。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon GuardDuty GuardDuty 是持續性的安全監控服務，可分析和處理來自各種資料來源的資訊。它使用威脅智慧饋送和機器學習) 以在您的 AWS 環境中識別意外和可能未經授權且惡意的活動。	您可以指定一個成員帳戶，代表組織中的所有帳戶來檢視和管理 GuardDuty。新增成員帳戶會自動為所選中的這些帳戶啟用 GuardDuty AWS 區域。您也可以為新增至組織的帳戶自動啟用 GuardDuty。 如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使 用 的優 點 AWS Organizat ions	支援受信 任存取	支援委派的管理員	
	GuardDuty 和 Organizat ions 。			
AWS Health 了解可能影響 您的資源效能 或可用性問題 的事件 AWS 服 務。	您可以在 組織中 跨帳戶彙 總 AWS Health 事 件。	 是 進一 步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
AWS Identity and Access Management 安全地控制對 AWS 資源的存取。	您可以在 IAM 中使用 上次存取的服務資料 ，以協助您更好地了解整個組織的 AWS 活動。您可以使用此資料來建立和更新 服務控制政策 (SCP) ，將存取限制在僅限您組織帳戶所用的 AWS 服務。 如需範例，請參閱 IAM 使用者指南中的 使用資料來精簡組織	 是 進一步了解	 是 進一步了解	

IAM Access Analyzer	分析您 AWS 環境中以資源為基礎的政策，以識別授予信任區域外委託人存取權的任何政策。	您可以將成員帳戶指定為 IAM Access Analyzer 的管理員。 如需詳細資訊，請參閱 IAM 使用者指南中的啟用 Access Analyzer。	 是	進一步了解
			 是	進一步了解

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
Amazon Inspector 自動掃描 AWS 工作負載是否有漏洞，以探索位於 Amazon ECR 中的 Amazon EC2 執行個體和容器映像是否有軟體漏洞和意外的網路暴露。	委派管理員啟用或停用成員帳戶掃描、檢視整個組織的彙總問題清單資料、建立和管理隱藏規則。 如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的 使用 AWS Organizations 管理多個帳戶 。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS License Manager 簡化將軟體授權轉送到雲端的程序。	您可啟用跨帳戶探索組織中的運算資源。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
Amazon Macie 使用機器學習探索並分類您的關鍵商業內容，以協助您符合資料安全性和隱私權需求。它會持續評估您儲存在 Amazon S3 中的內容並通知您潛在的問題。	您可以為組織中的所有帳戶設定 Amazon Macie，以便從指定的 Macie 管理員帳戶中，在所有帳戶中的 Amazon S3，取得所有資料的合併檢視。您可以將 Macie 設定為在組織成長時自動保護新帳戶中的資源。系統會警示您修復整個組織中 S3 儲存體的	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
政策配置不當。				
AWS Managed Services (AMS) 自助服務報告 (SSR) 從各種原生 AWS 服務收集資料，並提供存取主要 AMS 產品報告的權限。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。	您可以啟用彙總 SSR，這項功能可讓客戶透過您的管理帳戶或委派管理員帳戶，檢視整個組織的合併自助式報告。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使用的優點 AWS Organizations	支援受信 信任存取	支援委派的管理員	
AWS Marketplace 經策管數位目錄，您可以用於尋找、購買、部署和管理第三方軟體、資料和服務，而您需要這些軟體、資料和服務，來建置解決方案並執行您的業務。	您可以跨組織中的帳戶共用 AWS Marketplace 訂閱和購買的授權。	 是 進一步了解	 否	

AWS 服務	搭配 使用 的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS Marketplace 私有市集 為您提供廣泛的 產品 目錄 AWS Marketplace，以及這些產品的精細控制。	可讓您建立與整個組織、一或多個 OUs 或組織中一或多個帳戶相關聯的多個私有市場體驗，每個帳戶都有自己的一組核准產品。您的 AWS 管理員也可以使用公司或團隊的標誌、訊息和顏色方案，將公司品牌套用到每個私有市場體驗。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使用的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS Marketplace 採購洞察儀表板 可讓您檢視 AWS 組織中帳戶間所有 AWS Marketplace 購買項目的協議和成本分析資料。	AWS Marketplace 採購洞察儀表板會聆聽組織變更，例如加入組織的帳戶，並彙總其對應協議的資料，以建置其儀表板。	 是 進一步了解	 是 進一步了解	
AWS Network Manager 可讓您跨 AWS 帳戶、區域和內部部署位置集中管理 AWS Cloud WAN 核心網路和 AWS Transit Gateway 網路。	您可以使用傳輸閘道及其連接的資源，在組織內的多個 AWS 帳戶中集中管理和監控您的全球網路。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配 使用 的優 點 AWS Organizat ions	支援受信 任存取	支援委派的管理員	
Amazon Q Developer Amazon Q Developer 是生成式 AI 支援的對話式助理，可協助您了解、建置、擴展和操作 AWS 應用程式。	Amazon Q Developer 的付費訂閱版本需要 Organizations 整合。	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Resource Access Manager 與其他帳戶共用您擁有的指定 AWS 資源。	您可以在組織內共用資源，完全無需交換額外的邀請。您可以共享的資源包括 Route 53 解析程式規則、隨需容量保留等。 如需共用容量保留的相關資訊，請參閱 Amazon EC2 使用者指南 或 Amazon EC2 使用者指南。 如需可共享資源的清單，請參閱AWS	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
	RAM 使用者指南中的 可共享資源 。			
AWS 資源總管 在類似網際網路搜尋引擎的體驗中探索您的資源	啟用多帳戶搜尋。	 是 進一步了解	 是 進一步了解	
AWS Security Hub 在 中檢視您的安全狀態 AWS ，並根據安全產業標準和最佳實務檢查您的環境。	您可以為組織的所有帳戶自動啟用 Security Hub，包括新增的新帳戶。這會增加 Security Hub 檢查和問題清單的涵蓋範圍，從而提供更準確的整體安全狀態。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信存取	支援委派的管理員	
Amazon S3 Storage Lens 透過可執行的建議來最佳化儲存，取得 Amazon S3 儲存用量和活動指標的可見性。	設定 Amazon S3 Storage Lens 以了解 Amazon S3 儲存用量和活動趨勢，以及針對您組織中所有成員帳戶的建議。	 是 進一步了解	 是 進一步了解	
AWS 安全事件回應 AWS 安全服務提供全年無休的即時、人力輔助安全事件支援，協助客戶快速回應網路安全事件，例如憑證遭竊和勒索軟體攻擊。	整個組織的安全涵蓋範圍。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon Security Lake Amazon Security Lake 將來自雲端、內部部署和自訂來源的安全資料，集中到存放在您的帳戶的資料湖中。	建立可跨帳戶收集日誌和事件的資料湖。	 是 進一步了解	 是 進一步了解	
AWS Service Catalog 建立和管理已核准在 AWS 上使用的 IT 服務型錄。	您可以更輕鬆地跨帳戶複製共用產品組合和複製產品，無需共用產品組合 ID。	 是 進一步了解	 是 進一步了解	
Service Quotas 集中檢視和管理您的服務配額 (也稱為限制)。	您可以建立配額請求範本，以便於組織中建立帳戶時自動請求提高配額。	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS IAM Identity Center 為所有帳戶和雲端應用程式提供單一登入存取。	使用者可以使用其公司登入資料登入 AWS 存取入口網站，並存取其指派管理帳戶或成員帳戶中的資源。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Systems Manager 啟用 AWS 資源的可見性和控制。	您可以使用 Systems Manager Explorer 同步 AWS 帳戶組織中所有的操作資料。 您可以使用 Systems Manager 變更管理員，從委派的系統管理員帳戶來管理組織中所有成員帳戶的變更範本、核准和報告。	 是 進一步了解	 是 進一步了解	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信 任存取	支援委派的管理員	
AWS 使用者通知 AWS 通知的中央位置。	您可以集中設定和檢視組織中各帳戶的通知。	 是 進一步了解	 是 進一步了解	
標籤政策 使用組織帳戶中各資源的標準化標籤。	您可以建立標籤政策來定義特定資源和資源類型的標記規則，並將這些政策連接至組織單位和帳戶，以強制執行這些規則。	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
AWS Trusted Advisor Trusted Advisor 會檢查您的 AWS 環境，並在有機會節省成本、改善系統可用性和效能，或協助填補安全漏洞時提出建議。	執行 AWS 帳戶組織中所有的 Trusted Advisor 檢查。	 是 進一步了解	 是 進一步了解	
AWS Well-Architected Tool AWS Well-Architected Tool 可協助您記錄工作負載的狀態，並將其與最新的 AWS 架構最佳實務進行比較。	可讓 AWS WA Tool 和 Organizations 客戶簡化與其他成員共用 AWS WA Tool 資源的程序。	 是 進一步了解	 否	

AWS 服務	搭配使用的優點 AWS Organizations	支援受信任存取	支援委派的管理員	
Amazon VPC IP 地址管理員 (IPAM) IPAM 是一種 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控 AWS 工作負載的 IP 地址。	監控整個組織的 IP 地址使用情況，並在成員帳戶之間共用 IP 地址集區。	 是 進一步了解	 是 進一步了解	
Amazon VPC Reachability Analyzer Reachability Analyzer 是一種組態分析工具，可讓您在虛擬私有雲端 (VPC) 中的來源資源和目的地資源之間執行連線測試。	追蹤組織中跨帳戶的路徑。	 是 進一步了解	 是 進一步了解	

AWS 帳戶管理 和 AWS Organizations

AWS 帳戶管理 可協助您管理 AWS 帳戶 組織中所有的帳戶資訊和中繼資料。您可以設定、修改或刪除組織每個成員帳戶的替代聯絡人資訊。如需詳細資訊，請參閱 AWS 帳戶管理 使用者指南中的[在組織中使用 AWS 帳戶管理](#)。

使用下列資訊來協助您 AWS 帳戶管理 整合 AWS Organizations。

使用 Account Management 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

帳戶管理需要信任的 存取權 AWS Organizations，才能將成員帳戶指定為組織的此服務委派管理員。

您只能使用 Organizations 工具啟用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS 帳戶管理 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS 帳戶管理對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS 帳戶管理，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS 帳戶管理 為信任的服務。

```
$ aws organizations enable-aws-service-access \
  --service-principal account.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Account Management 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS 帳戶管理。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS 帳戶管理 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS 帳戶管理對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS 帳戶管理，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS 帳戶管理 為信任的服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal account.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Account Management 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中進行 Account Management 的委派管理員。

如需關於如何設定委派政策的一般指示，請參閱 [使用 建立資源型委派政策 AWS Organizations](#)。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal account.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 account.amazonaws.com 為參數。

AWS Application Migration Service（應用程式遷移服務）和 AWS Organizations

AWS Application Migration Service 簡化、加速和降低遷移應用程式的成本 AWS。透過與 Organizations 整合，您可以使用全域檢視功能來管理跨多個帳戶的大規模遷移。如需詳細資訊，請參閱《Application Migration Service 使用者指南》中的 [設定您的 AWS Organizations](#)。

使用下列資訊來協助您 AWS Application Migration Service 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 Application Migration Service 在您的組織中的帳戶內執行支援的操作。

只有在您停用 Application Migration Service 和 Organizations 之間的受信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

- `AWSServiceRoleForApplicationMigrationService`

Application Migration Service 所使用的服務主體

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Application Migration Service 所使用的服務連結角色會授予下列服務主體存取權：

- `mgn.amazonaws.com`

使用 Application Migration Service 啟用受信任存取

當您使用 Application Migration Service 啟用受信任存取時，您可以使用全域檢視功能，這可讓您管理跨多個帳戶的大規模遷移。全域檢視提供可見性和功能，可在不同 AWS 帳戶中對來源伺服器、應用程式和波浪執行特定動作。如需詳細資訊，請參閱《AWS Application Migration Service 使用者指南》中的[設定您的 AWS Organizations](#)。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Application Migration Service 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Application Migration Service 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Application Migration Service 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Application Migration Service 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Application Migration Service 主控台或工具啟用受信任存取，則不需要完成這些步驟。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Application Migration Service 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Application Migration Service 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Application Migration Service，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Application Migration Service 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal mgn.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Application Migration Service 停用受信任存取

只有 Organizations 管理帳戶中的管理員可以使用 Application Migration Service 停用受信任存取。

您可以使用 AWS Application Migration Service 或 AWS Organizations 工具停用受信任存取。

⚠ Important

我們強烈建議您盡可能使用 AWS Application Migration Service 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Application Migration Service 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Application Migration Service 提供的工具停用整合時，才能繼續執行這些步驟。

如果您使用 AWS Application Migration Service 主控台或工具來停用受信任存取，則不需要完成這些步驟。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Application Migration Service 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Application Migration Service 對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Application Migration Service，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Application Migration Service 為信任的服務。

```
$ aws organizations disable-aws-service-access \
```

```
--service-principal mgn.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Application Migration Service 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以為 Application Migration Service 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Application Migration Service 的管理分開。如需詳細資訊，請參閱《Application Migration Service 使用者指南》中的[設定您的 AWS Organizations](#)。

最低許可

只有 Organizations 管理帳戶中的使用者或角色可以將成員帳戶設定為組織中 Application Migration Service 的委派管理員

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal mgn.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務識別 mgn.amazonaws.com 為參數。

停用 Application Migration Service 的委派管理員

只有 Organizations 管理帳戶中的管理員才能移除 Application Migration Service 的委派管理員。您可以使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作來移除委派管理員。

AWS Artifact 和 AWS Organizations

AWS Artifact 是一項服務，可讓您下載 AWS 安全合規報告，例如 ISO 和 PCI 報告。使用時 AWS Artifact，組織管理帳戶中的使用者可以代表組織中的所有成員帳戶自動接受協議，即使新增了新的報告和帳戶。成員帳戶使用者可以檢視和下載協議。如需詳細資訊，請參閱《AWS Artifact 使用者指南》中的[管理 AWS Artifact 中多個帳戶的協議](#)。

使用下列資訊來協助您 AWS Artifact 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許在您的組織中的帳戶內 AWS Artifact 執行支援的操作。

只有在您停用 AWS Artifact 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

雖然如果您從組織中移除成員帳戶就能刪除或修改此角色，但我們不建議這樣做。

不建議修改角色，因為其可能會導致安全問題，如跨服務混淆代理人。如需進一步了解如何預防混淆代理人，請參閱《AWS Artifact 使用者指南》中的[預防跨服務代理人](#)。

- `AWSServiceRoleForArtifact`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Artifact 授予下列服務主體存取權的服務連結角色：

- `artifact.amazonaws.com`

使用 AWS Artifact 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具啟用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Artifact 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Artifact對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Artifact，他們現在可以從服務主控台 啟用該服務。AWS Organizations

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Artifact 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal artifact.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Artifact停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任的存取 AWS Artifact。

您只能使用 Organizations 工具停用受信任的存取。

AWS Artifact 需要 的信任存取，AWS Organizations 才能使用組織協議。如果您在使用 AWS Artifact 進行組織協議 AWS Organizations 時停用的受信任存取，它會停止運作，因為它無法存取組織。您

在 中接受但無法存取的任何組織協議都會 AWS Artifact 保留 AWS Artifact。AWS Artifact 建立 AWS Artifact 的角色會保留。如果您之後重新啟用信任的存取，AWS Artifact 會繼續如之前般運作，而不需重新設定服務。

從組織移除的獨立帳戶不再可存取任何組織協議。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Artifact 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Artifact對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Artifact，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Artifact 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal artifact.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

AWS Audit Manager 和 AWS Organizations

AWS Audit Manager 可協助您持續稽核 AWS 用量，以簡化評估風險的方式，以及是否符合法規和產業標準。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。需要稽核時，Audit Manager 可協助您管理對控制的利害關係人審查，並協助您以較少的手動工作來建立稽核就緒報表。

當您將 Audit Manager 與整合時 AWS Organizations，您可以透過在評估範圍內包含來自組織的多個 AWS 帳戶，從更廣泛的來源收集證據。

如需詳細資訊，請參閱 Audit Manager 使用者指南中的[啟用 AWS 組織](#)。

使用下列資訊來協助您 AWS Audit Manager 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Audit Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Audit Manager 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

如需 Audit Manager 如何使用此角色的詳細資訊，請參閱AWS Audit Manager 使用者指南中的[使用服務連結角色](#)。

- `AWSServiceRoleForAuditManager`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Audit Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `auditmanager.amazonaws.com`

使用 Audit Manager 來啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

Audit Manager 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的委派管理員。

您可以使用 AWS Audit Manager 主控台或 AWS Organizations 主控台啟用受信任存取。

⚠ Important

我們強烈建議您盡可能使用 AWS Audit Manager 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Audit Manager 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Audit Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Audit Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Audit Manager 主控台來啟用受信任的存取

如需啟用受信任存取的相關指示，請參閱AWS Audit Manager 使用者指南中的[設定](#)。

i Note

如果您使用 AWS Audit Manager 主控台設定委派管理員，AWS Audit Manager 會自動為您啟用信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將啟用 AWS Audit Manager 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Audit Manager 來停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS Audit Manager。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Audit Manager 為信任的服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal auditmanager.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

為 Audit Manager 啟用委派的管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Audit Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Audit Manager 的管理分開。

最低許可

只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Audit Manager 的委託管理員：

`audit-manager:RegisterAccount`

如需啟用 Audit Manager 委派管理員帳戶的指示，請參閱AWS Audit Manager 使用者指南中的[設定](#)。

如果您使用 AWS Audit Manager 主控台設定委派管理員，則 Audit Manager 會自動為您啟用信任的存取。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws audit-manager register-account \
  --delegated-admin-account 123456789012
```

- AWS SDK：呼叫 RegisterAccount 操作，並提供 delegatedAdminAccount 參數來委派管理員帳戶。

AWS Backup 和 AWS Organizations

AWS Backup 是一項服務，可讓您管理和監控組織中 AWS Backup 的任務。使用時 AWS Backup，如果您以組織管理帳戶中的使用者身分登入，您可以啟用整個組織的備份保護和監控。它可協助您使用[備份政策](#)，將 AWS Backup 計劃集中套用至組織中所有帳戶的資源，以達成合規。當您同時使用 AWS Backup 和時 AWS Organizations，可以獲得下列優點：

保護

您可以在組織中[啟用備份政策類型](#)，然後[建立備份政策](#)以連接至組織的根、OU 或帳戶。備份政策結合了 AWS Backup 計劃與自動將計劃套用至您的帳戶所需的其他詳細資訊。直接連接到帳戶的政策會與[繼承](#)自組織的根目錄和任何父 OUs 的政策合併，以建立適用於該帳戶的[有效政策](#)。此政策包含 IAM 角色的 ID，該角色具有在您帳戶中資源 AWS Backup 上執行的許可。AWS Backup 會使用 IAM 角色，依照有效政策中的備份計劃所指定，代表您執行備份。

監控

當您在組織中[啟用 AWS Backup 受信任的存取](#)時，您可以使用 AWS Backup 主控台，檢視組織中任何帳戶中的備份、還原和複製任務的詳細資訊。如需詳細資訊，請參閱 AWS Backup 開發人員指南中的[監控您的備份任務](#)。

如需詳細資訊 AWS Backup，請參閱 [AWS Backup 開發人員指南](#)。

使用下列資訊來協助您 AWS Backup 整合 AWS Organizations。

使用 AWS Backup 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Backup 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Backup 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Backup 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Backup 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。如果您使用 AWS Backup 主控台或工具啟用受信任存取，則不需要完成這些步驟。

若要使用 啟用受信任存取 AWS Backup，請參閱《AWS Backup 開發人員指南》中的在[多個中啟用備份 AWS 帳戶](#)。

使用 AWS Backup 停用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

AWS Backup 需要 的受信任存取 AWS Organizations，才能監控您組織帳戶中的備份、還原和複製任務。如果您停用受信任的存取 AWS Backup，則無法檢視目前帳戶以外的任務。AWS Backup 建立 AWS Backup 的角色會保留。如果您稍後重新啟用受信任存取，會 AWS Backup 繼續像以前一樣運作，而不需要重新設定服務。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Backup 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal backup.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 的委派管理員帳戶 AWS Backup

請參閱《AWS Backup 開發人員指南》中的[委派管理員](#)。

AWS 帳單與成本管理 和 AWS Organizations

AWS 帳單與成本管理 提供一組功能，可協助您設定帳單、擷取和支付發票，以及分析、整理、規劃和最佳化成本。當您搭配 Billing and Cost Management 使用時，AWS Organizations 您可以允許[分割成本分配資料](#)擷取 AWS Organizations 資訊，並在適用情況下收集您選擇的分割成本分配資料服務的遙測資料。

使用下列資訊來協助您 AWS 帳單與成本管理 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色可讓 Billing and Cost Management 在組織中的 帳戶內執行支援的操作。

只有在停用 Billing and Cost Management and Organizations 之間的受信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

如需詳細資訊，請參閱《[帳單和成本管理使用者指南](#)》中的[帳單和成本管理的服務連結角色許可](#)。

- `AWSServiceRoleForSplitCostAllocationData`

Billing and Cost Management 使用的服務主體

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Billing and Cost Management 使用的服務連結角色會授予下列服務主體存取權：

Billing and Cost Management 使用 `billing-cost-management.amazonaws.com`服務主體。

使用 Billing and Cost Management 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

透過管理帳戶啟用受信任存取，客戶可以利用 Billing and Cost Management 下的分割成本分配資料功能。當客戶啟用 Amazon Elastic Kubernetes Service 與 Amazon Managed Service for Prometheus 的分割成本分配資料時，系統會叫用受信任的存取，以為組織內的所有成員帳戶建立服務連結角色。這允

許分割成本分配資料從客戶的 Amazon Managed Service for Prometheus 工作空間收集遙測資料，並根據這些指標執行成本分配。

您只能使用 Organizations 工具啟用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS 帳單與成本管理 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal billing-cost-management.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

停用受信任存取權

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS 帳單與成本管理 為信任的服務。

```
$ aws organizations disable-aws-service-access \
```

```
--service-principal billing-cost-management.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

AWS CloudFormation StackSets 和 AWS Organizations

AWS CloudFormation StackSets 可讓您建立、更新或刪除跨多個 AWS 帳戶 和 AWS 區域 單一操作的堆疊。StackSets 與 AWS Organizations 整合，可讓您使用每個成員帳戶中具有相關許可的服務連結角色，建立具有服務管理許可的堆疊集。這可讓您將堆疊執行個體部署至組織中的成員帳戶。您不需要建立必要的 AWS Identity and Access Management 角色；StackSets 會代表您在每個成員帳戶中建立 IAM 角色。

您可以選擇自動部署到未來新增至組織的帳戶。啟用自動部署後，關聯堆疊集執行個體的角色和部署會自動新增至未來在該 OU 中新增的所有帳戶。

啟用 StackSets 和 Organizations 之間的受信任存取後，管理帳戶會擁有為您的組織建立和管理堆疊集的許可。管理帳戶最多可將五個成員帳戶註冊為委派管理員。啟用受信任存取之後，委派管理員也會擁有為您的組織建立和管理堆疊集的許可。具有服務管理許可的堆疊集是在管理帳戶中建立的，包括由委派管理員建立的堆疊集。

Important

委派管理員具有部署至組織中帳戶的完整許可。管理帳戶無法限制部署至特定 OU 或執行特定堆疊集操作的委派管理員許可。

如需將 StackSets 與 Organizations 整合的詳細資訊，請參閱AWS CloudFormation 《使用者指南》中的[使用 AWS CloudFormation StackSets](#)。

使用下列資訊來協助您整合 AWS CloudFormation StackSets 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 AWS CloudFormation Stacksets 在組織中的組織帳戶內執行支援的操作。

只有在您停用 AWS CloudFormation Stacksets 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- 管理帳戶：AWSServiceRoleForCloudFormationStackSetsOrgAdmin

若要為您組織中的成員帳戶建立服務連結角色

AWSServiceRoleForCloudFormationStackSetsOrgMember，您需要先在管理帳戶中建立堆疊集。此將建立一個堆疊集執行個體，然後在成員帳戶中建立角色。

- 成員帳戶：AWSServiceRoleForCloudFormationStackSetsOrgMember

如需建立堆疊集的詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的[使用 AWS CloudFormation StackSets](#)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Stacksets AWS CloudFormation 使用的服務連結角色會授予下列服務主體存取權：

- 管理帳戶：stacksets.cloudformation.amazonaws.com

只有在您停用 StackSets 和 Organizations 之間的受信任存取時，才能修改或刪除此角色。

- 成員帳戶：member.org.stacksets.cloudformation.amazonaws.com

只有在您首先停用 StackSets 和 Organizations 之間的受信任存取，或者首先從目標組織或組織單位 (OU) 中移除帳戶時，才能從帳戶中修改或刪除此角色。

使用 AWS CloudFormation Stacksets 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

只有 Organizations 管理帳戶中的管理員才具有許可，以使用其他服務啟用受信任存取 AWS。您可以使用 AWS CloudFormation 主控台或 Organizations 主控台來啟用信任存取。

您只能使用 AWS CloudFormation StackSets 啟用受信任存取。

若要使用 AWS CloudFormation Stacksets 主控台啟用受信任存取，請參閱 AWS CloudFormation 《使用者指南》中的[使用 啟用受信任存取 AWS Organizations](#)。

使用 AWS CloudFormation Stacksets 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 Organizations 管理帳戶中的管理員才具有使用其他服務停用信任存取的許可 AWS。您只能使用 Organizations 主控台來停用受信任的存取。如果您在使用 StackSets 時停用 Organizations 的受信任存取，則會保留所有先前建立的堆疊執行個體。不過，使用服務連結角色許可部署的堆疊集，無法再對 Organizations 管理的帳戶執行部署。

您可以使用 AWS CloudFormation 主控台或 Organizations 主控台來停用受信任存取。

Important

如果您以程式設計方式停用受信任存取（例如使用 AWS CLI 或 API），請注意，這會移除許可。最好使用 AWS CloudFormation 主控台停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信任停用的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 AWS CloudFormation StackSets。
4. 選擇停用受信任的存取。
5. 在停用受信任存取 for AWS CloudFormation StackSets 對話方塊中，輸入停用進行確認，然後選擇停用受信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴 AWS CloudFormation StackSets 的管理員，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，將 AWS CloudFormation StackSets 停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal stacksets.cloudformation.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Stacksets AWS CloudFormation 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 AWS CloudFormation Stacksets 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Stacksets AWS CloudFormation 的管理分開。

如需如何將成員帳戶指定為組織中 AWS CloudFormation Stacksets 的堆疊集，請參閱AWS CloudFormation 使用者指南中的[註冊委派管理員](#)。

AWS CloudTrail 和 AWS Organizations

AWS CloudTrail 是一項 AWS 服務，可協助您啟用的控管、合規和操作和風險稽核 AWS 帳戶。使用 AWS CloudTrail，管理帳戶中的使用者可以建立組織追蹤，記錄 AWS 帳戶 該組織中所有 事件。組織線索會自動套用到組織中的所有成員帳戶。成員帳戶可以查看組織線索，但無法進行修改或刪除。依預設，成員帳戶無法存取在 Amazon S3 儲存貯體中組織追蹤的日誌檔案。這個做法可協助您統一套用並強制執行組織中帳戶的事件日誌策略。

如需詳細資訊，請參閱AWS CloudTrail 使用者指南中的[建立組織追蹤](#)。

使用下列資訊來協助您 AWS CloudTrail 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 CloudTrail 在您組織的組織帳戶中執行支援的操作。

只有在您停用 CloudTrail 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能移除或修改此角色。

- AWSServiceRoleForCloudTrail

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。CloudTrail 使用的服務連結角色會將存取權授與下列服務委託人：

- `cloudtrail.amazonaws.com`

使用 CloudTrail 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

如果您透過從 AWS CloudTrail 主控台建立追蹤來啟用受信任存取，系統會自動為您設定受信任存取（建議）。您也可以使用 AWS Organizations 主控台啟用受信任存取。您必須使用 AWS Organizations 管理帳戶登入，才能建立組織追蹤。

如果您選擇使用 AWS CLI 或 AWS API 建立組織追蹤，則必須手動設定信任的存取。如需詳細資訊，請參閱AWS CloudTrail 使用者指南中的[啟用 CloudTrail 作為 AWS Organizations 中的受信任服務](#)。

Important

我們強烈建議您盡可能使用 AWS CloudTrail 主控台或工具來啟用與 Organizations 的整合。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS CloudTrail 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal cloudtrail.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 CloudTrail 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

AWS CloudTrail 需要 的信任存取，AWS Organizations 才能使用組織追蹤和組織事件資料存放區。如果您在使用時停用的 AWS Organizations 信任存取 AWS CloudTrail，則會刪除成員帳戶的所有組織追蹤，因為 CloudTrail 無法存取組織。所有管理帳戶組織追蹤和組織事件資料存放區都會轉換為帳戶層級追蹤和事件資料存放區。為 CloudTrail 與 之間的整合而建立 `AWSServiceRoleForCloudTrail` 的角色會 AWS Organizations 保留在帳戶中。如果您重新啟用受信任的存取，CloudTrail 將不會對現有追蹤和事件資料存放區採取動作。管理帳戶必須更新任何帳戶層級追蹤和事件資料存放區，才能將其套用至組織。

若要將帳戶層級追蹤或事件資料存放區轉換為組織追蹤或組織事件資料存放區，請執行下列動作：

- 從 CloudTrail 主控台更新[追蹤](#)或[事件資料存放](#)區，並選擇為組織中的所有帳戶啟用選項。
- 從中 AWS CLI，執行下列動作：
 - 若要更新追蹤，請執行 `update-trail` 命令並包含 `--is-organization-trail` 參數。
 - 若要更新事件資料存放區，請執行 `update-event-data-store` 命令並包含 `--organization-enabled` 參數。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS CloudTrail。您只能使用 Organizations 工具、使用 AWS Organizations 主控台、執行 Organizations CLI AWS 命令，或在其中一個 AWS SDKs 中呼叫 Organizations API 操作，來停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS CloudTrail 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS CloudTrail對話方塊中，輸入停用進行確認，然後選擇停用信任存取。

- 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS CloudTrail，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS CloudTrail 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal cloudtrail.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 CloudTrail 委派管理員帳戶

當您將 CloudTrail 與 Organizations 一起使用時，您可以在組織內註冊任何帳戶以作為 CloudTrail 委派管理員，以代表組織管理組織的追蹤和事件資料存放區。委派管理員是組織中的成員帳戶，可以在 CloudTrail 中執行與管理帳戶相同的管理工作。

最低許可

只有組織管理帳戶中的管理員可以註冊 CloudTrail 的委派管理員。

您可以使用 CloudTrail 主控台，或使用 Organizations RegisterDelegatedAdministrator CLI 或 SDK 操作，註冊委派管理員帳戶。若要使用 CloudTrail 主控台註冊委派管理員，請參閱 [Add a CloudTrail delegated administrator](#) (新增 CloudTrail 委派管理員)。

停用 CloudTrail 委派管理員

只有組織管理帳戶中的管理員可以移除 CloudTrail 的委派管理員。您可以使用 CloudTrail 主控台或使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作，移除委派管理員。

如需有關如何使用 CloudTrail 主控台移除委派管理員的資訊，請參閱 [Remove a CloudTrail delegated administrator](#) (移除 CloudTrail 委派管理員)。

Amazon CloudWatch 和 AWS Organizations

您可以針對下列使用案例使用 AWS Organizations 的 Amazon CloudWatch：

- 從 CloudWatch 主控台的中央檢視探索並了解資源 AWS 的遙測組態狀態。這可簡化稽核您 AWS 組織或帳戶中多個資源類型的遙測收集組態的程序。您必須開啟受信任的存取，才能在整個組織中使用遙測組態。

如需詳細資訊，請參閱《Amazon [CloudWatch 使用者指南](#)》中的稽核 [CloudWatch 遙測組態](#)。
Amazon CloudWatch

- 在 Network Flow Monitor 中使用多個帳戶，這是 Amazon CloudWatch Network Monitoring 的一項功能。Network Flow Monitor 為 Amazon EC2 執行個體之間的流量提供近乎即時的網路效能可見性。開啟信任的存取以與 Organizations 整合後，您可以建立監視器，將多個帳戶的網路效能詳細資訊視覺化。

如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[初始化多帳戶監控的網路流量監控](#)。

使用以下資訊來協助您整合 Amazon CloudWatch 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

在組織的管理帳戶中建立下列[服務連結角色](#)。當您啟用受信任存取時，服務連結角色會自動在成員帳戶中建立。此角色可讓 CloudWatch 在組織中的組織帳戶中執行支援的操作。只有在您停用 CloudWatch 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForObservabilityAdmin`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。CloudWatch 使用的服務連結角色會將存取權授予下列服務主體：

- `observabilityadmin.amazonaws.com`
- `networkflowmonitor.amazonaws.com`

- `topology.networkflowmonitor.amazonaws.com`

使用 CloudWatch 啟用受信任存取

如需開啟受信任存取所需的許可資訊，請參閱 [啟用信任的存取所需的許可](#)。

您可以使用 Amazon CloudWatch 主控台或 主控台來啟用受信任存取 AWS Organizations。

Important

我們強烈建議您盡可能使用 Amazon CloudWatch 主控台或工具來啟用與 Organizations 的整合。這可讓 Amazon CloudWatch 執行所需的任何組態，例如建立服務所需的資源。只有在您無法使用 Amazon CloudWatch 提供的工具啟用整合時，才能繼續進行這些步驟。如需詳細資訊，請參閱 [本說明](#)。

如果您使用 Amazon CloudWatch 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 CloudWatch 主控台開啟受信任存取

請參閱《Amazon [CloudWatch 使用者指南](#)》中的開啟 [CloudWatch 遙測稽核](#)。Amazon CloudWatch

當您在 CloudWatch 中開啟受信任的存取時，您可以啟用遙測稽核，並且可以在網路流量監視器中使用多個帳戶。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon CloudWatch。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 Amazon CloudWatch 的受信任存取對話方塊中，輸入啟用以確認，然後選擇啟用受信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴 Amazon CloudWatch 的管理員，他們現在可以從服務主控台 啟用該服務來使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用下列 AWS CLI 命令或 API 操作來啟用受信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令以啟用 Amazon CloudWatch 做為 Organizations 的受信任服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal observabilityadmin.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 CloudWatch 關閉受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您可以使用 Amazon CloudWatch 或 AWS Organizations 工具來停用受信任存取。

Important

我們強烈建議您盡可能使用 Amazon CloudWatch 主控台或工具來停用與 Organizations 的整合。這可讓 Amazon CloudWatch 執行其所需的任何清除，例如刪除資源或服務不再需要的存取角色。只有在您無法使用 Amazon CloudWatch 提供的工具停用整合時，才能繼續進行這些步驟。

如果您使用 Amazon CloudWatch 主控台或工具停用受信任存取，則不需要完成這些步驟。

使用 CloudWatch 主控台關閉受信任存取

請參閱《Amazon [CloudWatch 使用者指南](#)》中的關閉 [CloudWatch 遙測稽核](#) Amazon CloudWatch

當您在 CloudWatch 中關閉受信任存取時，遙測稽核不再處於作用中狀態，您無法再使用網路流量監視器中的多個帳戶。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用下列 AWS CLI 命令或 API 操作來停用受信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令來停用 Amazon CloudWatch 做為 Organizations 的受信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal observabilityadmin.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

註冊 CloudWatch 的委派管理員帳戶

當您將成員帳戶註冊為組織的委派管理員帳戶時，該帳戶的使用者和角色可以為 CloudWatch 執行管理動作，否則只能由使用組織的管理帳戶登入的使用者或角色執行。使用委派管理員帳戶可協助您將組織的管理與 CloudWatch 中的功能管理分開。

最低許可

只有 Organizations 管理帳戶中的管理員可以將成員帳戶註冊為組織中 CloudWatch 的委派管理員帳戶。

您可以使用 CloudWatch 主控台註冊委派管理員帳戶，或使用 Organizations RegisterDelegatedAdministrator API 操作搭配 AWS Command Line Interface 或 SDK。

如需有關如何使用 CloudWatch 主控台註冊委派管理員帳戶的資訊，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[開啟 CloudWatch 遙測稽核](#)。Amazon CloudWatch

當您在 CloudWatch 中註冊委派管理員帳戶時，您可以使用該帳戶進行管理操作，搭配遙測稽核和 Network Flow Monitor。

取消註冊 CloudWatch 的委派管理員

最低許可

只有使用 Organizations 管理帳戶登入的管理員才能取消組織中 CloudWatch 的委派管理員帳戶註冊。

您可以使用 CloudWatch 主控台，或使用 Organizations DeregisterDelegatedAdministrator API 操作搭配 AWS Command Line Interface 或 SDK 來取消註冊委派管理員帳戶。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[取消註冊委派管理員帳戶](#)。

當您在 CloudWatch 中取消註冊委派管理員帳戶時，您無法再使用帳戶進行遙測稽核和網路流量監控的管理操作。

AWS Compute Optimizer 和 AWS Organizations

AWS Compute Optimizer 是一種服務，可分析 AWS 資源的組態和使用率指標。資源範例包括 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和 Auto Scaling 群組。Compute Optimizer 會報告您的資源是否最佳化並產生最佳化推薦，以降低成本並改善工作負載的效能。如需有關 Compute Optimizer 的詳細資訊，請參閱[AWS Compute Optimizer 使用者指南](#)。

使用下列資訊來協助您 AWS Compute Optimizer 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Compute Optimizer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Compute Optimizer 和 Organizations 之間的信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForComputeOptimizer`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Compute Optimizer 使用的服務連結角色會將存取權授予下列服務委託人：

- `compute-optimizer.amazonaws.com`

使用 Compute Optimizer 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Compute Optimizer 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Compute Optimizer 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Compute Optimizer 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Compute Optimizer 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Compute Optimizer 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Compute Optimizer 主控台來啟用受信任存取

您必須使用組織的管理帳戶登入 Compute Optimizer 主控台。請遵循 AWS Compute Optimizer 使用者指南中的[選擇加入您的帳戶](#)，代表您的組織選擇加入。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Compute Optimizer 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Compute Optimizer 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Compute Optimizer，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Compute Optimizer 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Compute Optimizer 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS Compute Optimizer。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Compute Optimizer 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Compute Optimizer 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Compute Optimizer 的委派管理員

如需啟用 Compute Optimizer 委派管理員帳戶的說明，請參閱《AWS Compute Optimizer 使用者指南》中的 <https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html>。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 account.amazonaws.com 為參數。

停用 Compute Optimizer 的委派管理員帳戶

只有組織管理帳戶中的管理員可以設定 Compute Optimizer 的委派管理員。

若要使用 Compute Optimizer 主控台停用委派管理員 Compute Optimizer 帳戶，請參閱《AWS Compute Optimizer 使用者指南》中的 <https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html>。

若要使用 移除委派管理員 AWS CLI，請參閱 AWS CLI 命令參考中的 [deregister-delegated-administrator](#)。

AWS Config 和 AWS Organizations

中的多帳戶、多區域資料彙總 AWS Config 可讓您將來自多個帳戶和 AWS Config 的資料彙總到單一帳戶。多帳戶多區域資料彙總對中央 IT 管理員監控企業中多個 AWS 帳戶的合規性非常有用。彙總器是 中的資源類型 AWS Config，AWS Config 可從多個來源帳戶和區域收集資料。在您要查看彙總 AWS Config 資料的區域中建立彙總工具。建立彙總工具時，您可以選擇新增個別帳戶 ID 或您的組織。如需詳細資訊 AWS Config，請參閱 [AWS Config 開發人員指南](#)。

您也可以使用 [AWS Config APIs](#) 來管理 AWS Config 組織中所有 AWS 帳戶的規則。如需詳細資訊，請參閱《AWS Config 開發人員指南》[中的在您的組織中所有帳戶中啟用 AWS Config 規則](#)。

使用下列資訊來協助您 AWS Config 整合 AWS Organizations。

服務連結角色

下列[服務連結角色](#)允許 在您的組織中的帳戶內 AWS Config 執行支援的操作。

- AWSServiceRoleForConfig

進一步了解如何在 AWS Config 開發人員指南中 [，在指派給的 IAM 角色許可中建立此角色 AWS Config](#)

進一步了解 AWS Config 開發人員指南中的 AWS Config 如何在使用的服務連結角色中使用[服務連結角色 AWS Config](#)

只有在您停用 AWS Config 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

使用 AWS Config 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Config 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Config 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Config 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Config 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。如果您使用 AWS Config 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Config 主控台啟用受信任存取

若要啟用對 AWS Organizations 的信任存取 AWS Config，請建立多帳戶彙總器並新增組織。如需有關如何設定多帳戶彙總器的資訊，請參閱《AWS Config 開發人員指南》中的[建立彙總器](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Config 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Config 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Config，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Config 為信任的服務。

```
$ aws organizations enable-aws-service-access \
  --service-principal config.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Config 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Config 為信任的服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal config.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

AWS 成本最佳化中心 和 AWS Organizations

AWS 成本最佳化中心 是一項 AWS Billing and Cost Management 功能，可協助您整合和排定 AWS 帳戶和 AWS 區域的成本最佳化建議優先順序，以便充分利用您的 AWS 支出。當您將 Cost Optimization Hub 與 AWS Organizations 搭配使用時，您可以輕鬆地識別、篩選和彙總 Organizations 成員帳戶和 AWS 區域中 AWS 的成本最佳化建議。

如需詳細資訊，請參閱AWS Cost Management 《使用者指南》中的[成本最佳化中樞](#)。

使用下列資訊來協助您 AWS 成本最佳化中心 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 Cost Optimization Hub 在您組織中的組織帳戶中執行支援的操作。

只有在您停用 Cost Optimization Hub 和 Organizations 之間的受信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

如需詳細資訊，請參閱AWS Cost Management 《使用者指南》中的 [Cost Optimization Hub 的服務連結角色許可](#)。

- AWSServiceRoleForCostOptimizationHub

Cost Optimization Hub 使用的服務主體

Cost Optimization Hub 使用 `cost-optimization-hub.bcm.amazonaws.com`服務主體。

使用 Cost Optimization Hub 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

當您選擇使用組織的管理帳戶，並包含組織中的所有成員帳戶時，組織帳戶中會自動啟用 Cost Optimization Hub 的受信任存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS 成本最佳化中心 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS 成本最佳化中心對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS 成本最佳化中心，他們現在可以從服務主控台 啟用該服務來使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS 成本最佳化中心 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

停用受信任存取權

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

Important

如果您在選擇加入後停用 Cost Optimization Hub 受信任存取，Cost Optimization Hub 會拒絕存取您組織成員帳戶的建議。此外，組織內的成員帳戶不會選擇加入 Cost Optimization Hub。如需進一步了解，請參閱 AWS Cost Management 使用者指南中的 [Cost Optimization Hub and Organizations 受信任存取](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS 成本最佳化中心 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Cost Optimization Hub 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，指定的帳戶可以擷取您組織下所有帳戶的成本最佳化中心建議，並管理成本最佳化中心偏好設定，讓您擁有更大的彈性，以集中識別資源最佳化機會。

最低許可

只有具有下列許可的組織管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Cost Optimization Hub 的委派管理員：

如需為 Cost Optimization Hub 啟用委派管理員帳戶的指示，請參閱AWS Cost Management 《使用者指南》中的[委派管理員帳戶](#)。

停用 Cost Optimization Hub 的委派管理員

只有 Organizations 管理帳戶中的管理員才能移除 Cost Optimization Hub 的委派管理員。

若要使用 Cost Optimization Hub 主控台停用委派的管理員成本最佳化中樞帳戶，請參閱AWS Cost Management 《使用者指南》中的[委派管理員帳戶](#)。

若要使用 CLI AWS 移除委派管理員，請參閱 AWS Config CLI 參考[deregister-delegated-administrator](#)中的。

AWS Control Tower 和 AWS Organizations

AWS Control Tower 提供一種直接的方式來設定和管理 AWS 多帳戶環境，遵循規範最佳實務。AWS Control Tower 協調擴展了 的功能 AWS Organizations。AWS Control Tower 套用預防性和偵測性控制（護欄），以協助您的組織和帳戶避免與最佳實務（偏離）有所分歧。

AWS Control Tower 協調擴展 的功能 AWS Organizations。

如需詳細資訊，請參閱 [AWS Control Tower 使用者指南](#)。

使用下列資訊來協助您 AWS Control Tower 整合 AWS Organizations。

進行整合時所需要的角色

所有已註冊的帳戶中都必須存在有 `AWSControlTowerExecution` 角色。它允許 AWS Control Tower 管理您的個別帳戶，並將其相關資訊報告給您的 Audit and Log Archive 帳戶。

若要進一步了解 使用的角色 AWS Control Tower，請參閱 [AWS Control Tower 如何使用角色來建立和管理帳戶](#)，以及[使用 以身分為基礎的政策 \(IAM 政策 \) AWS Control Tower](#)。

使用的服務主體 AWS Control Tower

AWS Control Tower 使用 `controltower.amazonaws.com`服務主體。

使用 AWS Control Tower啟用受信任的存取

AWS Control Tower 使用信任的存取來偵測偏離以進行預防性控制，以及追蹤導致偏離的帳戶和 OU 變更。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具啟用受信任的存取。

若要從 Organizations 主控台啟用受信任存取，請選擇 AWS Control Tower 旁的 **Enable access**。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Control Tower 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal controltower.amazonaws.com
```


此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Control Tower 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

Important

停用 AWS Control Tower 受信任的存取會導致 AWS Control Tower 登陸區域中的漂移。修正此漂移問題的唯一方法是使用 AWS Control Tower 的登陸區域修復。在 Organizations 中重新啟用受信任的存取權並不能修正此漂移。在 AWS Control Tower 用戶指南中[進一步了解漂移](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Control Tower 為信任的服務。

```
$ aws organizations disable-aws-service-access \  
--service-principal controltower.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

Amazon Detective 和 AWS Organizations

Amazon Detective 會使用您的日誌資料產生視覺化效果，以便您分析、調查並識別安全問題清單或可疑活動的根本原因。

使用 AWS Organizations 可讓您確保 Detective 行為圖表可讓您查看所有組織帳戶的活動。

當您向 Detective 授予受信任存取權時，Detective 服務可以自動對組織成員身分的變更做出反應。委派管理員可以在行為圖中將任何組織帳戶作為成員帳戶啟用。Detective 還可以自動將新組織帳戶作為成員帳戶啟用。組織帳戶無法將自己與行為圖解除關聯。

如需詳細資訊，請參閱《Amazon Detective 管理指南》中的[在組織中使用 Amazon Detective](#)。

使用以下資訊來協助您整合 Amazon Detective 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 Detective 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Detective 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForDetective`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Detective 使用的服務連結角色會將存取權授予下列服務委託人：

- `detective.amazonaws.com`

使用 Detective 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

Note

當您指定 Amazon Detective 的委派管理員時，Detective 會自動啟用組織中 Detective 的受信任存取。

Detective 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的此服務委派管理員。

您只能使用 Organizations 工具啟用受信任的存取。

您可以使用 AWS Organizations 主控台啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon Detective。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 Amazon Detective 的信任存取對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告知 Amazon Detective 的管理員，他們現在可以 AWS Organizations 從服務主控台 啟用該服務。

使用 Detective 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 Amazon Detective 停用受信任存取。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任的存取。

AWS Management Console

使用 Organizations 主控台來受信任停用的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon Detective。
4. 選擇停用受信任的存取。
5. 在停用 Amazon Detective 的受信任存取對話方塊中，輸入停用進行確認，然後選擇停用受信任存取。

- 如果您只是的管理員 AWS Organizations，請告訴 Amazon Detective 的管理員，他們現在可以使用服務 AWS Organizations 主控台或工具停用該服務。

啟用 Detective 的委派管理員帳戶

Detective 的委派管理員帳戶是 Detective 行為圖的管理員帳戶。委派管理員會判斷要在該行為圖中啟用和停用哪些作為成員帳戶的組織帳戶。委派管理員可以設定 Detective，使其在將新的組織帳戶新增到組織時自動將其作為成員帳戶啟用。如需委派管理員如何管理組織帳戶的資訊，請參閱《Amazon Detective 管理指南》中的[將組織帳戶作為成員帳戶管理](#)。

只有組織管理帳戶中的管理員可以設定 Detective 的委派管理員。

您可以從 Detective 主控台或 API，或使用 Organizations CLI 或 SDK 操作，指定委派的管理員帳戶。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Detective 的委派管理員

若要使用 Detective 主控台或 API 設定委派管理員，請參閱《Amazon Detective 管理指南》中的[為組織指定 Detective 管理員帳戶](#)。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal detective.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 account.amazonaws.com 為參數。

停用 Detective 的委派管理員

您可以使用 Detective 主控台或 API，或透過使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作，移除委派管理員。關於如何使用

Detective 主控台或 API 或 Organizations API 移除委派管理員的資訊，請參閱《Amazon Detective 管理指南》中的[為組織指定 Detective 管理員帳戶](#)。

Amazon DevOpsGuru 和 AWS Organizations

Amazon DevOps Guru 分析營運資料和應用程式指標與事件，以識別與正常操作模式不同的行為。當 DevOps Guru 檢測到操作問題或風險時，會通知使用者。

使用 DevOpsGuru 可透過 支援多帳戶 AWS Organizations，因此您可以指定成員帳戶來管理整個組織的洞見。然後，此委派管理員可以檢視、排序和篩選組織內所有帳戶的洞察，以便從整體上了解組織內所有受監控應用程式的運作狀態，而無需進行任何其他自訂。

如需詳細資訊，請參閱《Amazon DevOps Guru 使用者指南》中的[監控組織中的帳戶](#)。

使用下列資訊來協助您整合 Amazon DevOpsGuru 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 DevOps Guru 在您組織的組織帳戶中執行支援的操作。

只有在您停用 DevOps Guru 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForDevOpsGuru`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。DevOps Guru 使用的服務連結角色會將存取權授予下列服務委託人：

- `devops-guru.amazonaws.com`

如需詳細資訊，請參閱《Amazon DevOps Guru 使用者指南》中的[將服務連結角色用於 DevOps Guru](#)。

使用 DevOps Guru 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

 Note

當您指定 Amazon DevOps Guru 的委派管理員時，DevOps Guru 會自動啟用組織中 DevOps Guru 的受信任存取。

DevOpsGuru 需要信任的存取，AWS Organizations 才能將成員帳戶指定為組織的此服務委派管理員。

 Important

強烈建議您盡可能使用 Amazon DevOps Guru 主控台或工具來啟用與 Organizations 的整合。這可讓 Amazon DevOps Guru 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 Amazon DevOps Guru 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

您可以使用 AWS Organizations 主控台或 DevOpsGuru 主控台來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在 [Services](#) (服務) 頁面上，尋找 Amazon DevOps Guru 列，選擇服務的名稱，然後選擇 Enable trusted access (啟用受信任存取)。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是的管理員 AWS Organizations，請告訴 Amazon DevOpsGuru 的管理員，他們現在可以使用其主控台啟用該服務 AWS Organizations。

DevOps Guru console

使用 DevOps Guru 主控台來啟用受信任服務存取

1. 在管理帳戶中以管理員身分登入並開啟 DevOps Guru 主控台：[Amazon DevOps Guru 主控台](#)
2. 選擇 Enable trusted access (啟用信任存取)。

使用 DevOps Guru 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 Amazon DevOpsGuru 停用受信任存取。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任的存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon DevOpsGuru。
4. 選擇停用受信任的存取。
5. 在停用 Amazon DevOpsGuru 的受信任存取對話方塊中，輸入停用進行確認，然後選擇停用受信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴 Amazon DevOpsGuru 的管理員，他們現在可以使用服務 AWS Organizations 主控台或工具停用該服務。

啟用 DevOps Guru 的委派管理員帳戶

DevOps Guru 的委派管理員帳戶可以查看所有成員帳戶中的洞察資料，這些帳戶是從組織加入 DevOps Guru。如需委派管理員如何管理組織帳戶的資訊，請參閱《Amazon DevOps Guru 使用者指南》中的[監控組織中的帳戶](#)。

只有組織管理帳戶中的管理員可以設定 DevOps Guru 的委派管理員。

您可以從 DevOps Guru 主控台，或使用 Organizations RegisterDelegatedAdministratorCLI 或 SDK 操作，指定委派管理員帳戶。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 DevOps Guru 的委派管理員

DevOps Guru console

在 DevOps Guru 主控台中設定委派管理員

1. 在管理帳戶中以管理員身分登入並開啟 DevOps Guru 主控台：[Amazon DevOps Guru 主控台](#)
2. 選擇 Register delegated administrator (註冊委派管理員)。您可以選擇管理帳戶或任何成員帳戶作為委派管理員。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 account.amazonaws.com 為參數。

停用 DevOps Guru 的委派管理員

您可以使用 DevOps Guru 主控台或使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作，移除委派管理員。如需有關如何使用 DevOps Guru 主控台移除委派管理員的資訊，請參閱《Amazon DevOps Guru 使用者指南》中的[監控組織中的帳戶](#)。

AWS Directory Service 和 AWS Organizations

AWS Directory Service for Microsoft Active Directory，或 AWS Managed Microsoft AD 可讓您以受管服務的形式執行 Microsoft Active Directory (AD)。AWS Directory Service 可讓您輕鬆地在 AWS 雲端中設定和執行目錄，或將 AWS 資源與現有的內部部署 Microsoft Active Directory 連線。AWS Managed Microsoft AD 也與緊密整合 AWS Organizations，以允許跨區域中的多個 AWS 帳戶和任何 VPC 無縫共用目錄。如需詳細資訊，請參閱[AWS Directory Service 管理員指南](#)。

若要 AWS Directory Service 跨組織共用，組織必須啟用所有功能，且目錄必須位於組織管理帳戶中。

使用下列資訊來協助您 AWS Directory Service 整合 AWS Organizations。

使用 AWS Directory Service 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Directory Service 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Directory Service 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Directory Service 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Directory Service 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Directory Service 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Directory Service 主控台啟用受信任存取

若要共享自動啟用受信任存取的目錄，請參閱 AWS Directory Service 管理指南中的[共享您的目錄](#)。如需 step-by-step 說明，請參閱[教學課程：共用您的 AWS 受管 Microsoft AD 目錄](#)。

您可以使用 AWS Organizations 主控台啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Directory Service 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Directory Service 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Directory Service，他們現在可以 AWS Organizations 從服務主控台 啟用該服務與 搭配使用。

使用 AWS Directory Service 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

如果您在使用 AWS Organizations 時停用 的信任存取 AWS Directory Service，則所有先前共用的目錄都會繼續正常操作。不過，您不再能夠以在組織內共享新目錄，直到您重新啟用信任的存取為止。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台來停用受信任的存取。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Directory Service 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Directory Service對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Directory Service，他們現在可以使用服務 AWS Organizations 主控台或工具停用該服務。

Amazon Elastic Compute Cloud 和 AWS Organizations

Amazon Elastic Compute Cloud 在 AWS 雲端中提供隨需、可擴展的運算容量。當您搭配 Organizations 使用 Amazon EC2 時，您可以讓 Organizations 管理員在使用 Amazon EC2 的[宣告政策](#)功能後，建立其組織中帳戶現有組態的報告。

使用以下資訊來協助您整合 Amazon Elastic Compute Cloud 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 Amazon EC2 在您組織中的組織帳戶內執行支援的操作。

只有在您停用 Amazon EC2 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Amazon EC2 使用的服務主體

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon EC2 使用的服務連結角色會將存取權授予下列服務主體：

- `ec2.amazonaws.com`

使用 Amazon EC2 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

若要讓 Organizations 管理員建立其組織中帳戶現有組態的報告，您必須啟用受信任的存取。

您只能使用 Organizations 工具啟用受信任存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon Elastic Compute Cloud。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 Amazon Elastic Compute Cloud 的受信任存取對話方塊中，輸入啟用以確認，然後選擇啟用受信任的存取。
6. 如果您只是的管理員 AWS Organizations，請告訴 Amazon Elastic Compute Cloud 的管理員，他們現在可以從服務主控台 啟用該服務。AWS Organizations

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用下列 AWS CLI 命令或 API 操作來啟用受信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以啟用 Amazon Elastic Compute Cloud 做為 Organizations 的受信任服務。

```
$ aws organizations enable-aws-service-access \
  --service-principal ec2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

停用受信任存取權

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令來停用 Amazon Elastic Compute Cloud 做為 Organizations 的受信任服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal ec2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

Amazon Elastic Kubernetes Service 和 AWS Organizations

Amazon Elastic Kubernetes Service Dashboard 是合併的儀表板，可用來監控、管理和了解跨多個 AWS 區域和 AWS 帳戶的 Kubernetes 叢集。EKS 儀表板透過集中式界面，為您的 Amazon EKS 基礎設施提供全面的控制和洞察。

Amazon Elastic Kubernetes Service Dashboard 可讓您追蹤排程升級的叢集、專案控制平面成本、檢閱叢集洞見，以及監控整個組織的節點群組分佈。您的 AWS 管理員可以透過圖形、資源清單和地理地

圖等不同的視覺化選項，檢視叢集資源的彙總資料，包括運作狀態、版本分佈和附加元件組態。儀表板會與 AWS Organizations 整合，以提供 EKS 資源的安全跨帳戶和跨區域可見性。

使用以下資訊來協助您整合 Amazon Elastic Kubernetes Service 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您使用 Amazon Elastic Kubernetes Service 主控台啟用受信任存取時，系統會自動在組織的管理帳戶中建立下列服務連結角色。此角色可讓 Amazon EKS 在您組織中的組織帳戶中執行支援的操作。只有在您停用 Amazon Elastic Kubernetes Service 和 Organizations 之間的受信任存取時，才能刪除或修改此角色。

如果您直接從 Organizations 主控台、CLI 或 SDK 啟用受信任存取，則不會自動建立服務連結角色。

- `AWSServiceRoleForAmazonEKSDashboard`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon EKS 使用的服務連結角色會將存取權授予下列服務主體：

- `dashboard.eks.amazonaws.com`

使用 Amazon EKS 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

使用 Amazon EKS 主控台啟用受信任存取

請參閱《Amazon EKS 使用者指南》中的[啟用受信任存取](#)。

使用 Amazon EKS 停用受信任存取

使用 Amazon EKS 主控台停用受信任存取

請參閱《Amazon EKS 使用者指南》中的[停用受信任存取](#)。

啟用 Amazon EKS 的委派管理員帳戶

管理帳戶管理員可以將 Amazon EKS 管理許可委派給稱為委派管理員的指定成員帳戶。

管理帳戶和委派管理員帳戶可以檢視 Amazon EKS 儀表板。

啟用委派管理員帳戶

請參閱《Amazon EKS 使用者指南》中的[啟用委派管理員帳戶](#)。

停用 Amazon EKS 的委派管理員

只有組織管理帳戶中的管理員可以設定 Amazon EKS 的委派管理員。

停用委派管理員帳戶

請參閱《Amazon EKS 使用者指南》中的[停用委派管理員帳戶](#)。

AWS Firewall Manager 和 AWS Organizations

AWS Firewall Manager 是一項安全管理服務，您可用來集中設定和管理組織中 和 AWS 帳戶 應用程式的防火牆規則和其他保護。使用 Firewall Manager，您可以推出 AWS WAF 規則、建立 AWS Shield Advanced 保護、設定和稽核 Amazon Virtual Private Cloud (Amazon VPC) 安全群組，以及部署 AWS Network Firewall。只需使用 Firewall Manager 設定一次防護，並將它們在您的組織內的所有帳戶和資源間自動套用，甚至是新增了新資源和帳戶亦然。如需詳細資訊 AWS Firewall Manager，請參閱 [AWS Firewall Manager 開發人員指南](#)。

使用下列資訊來協助您 AWS Firewall Manager 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Firewall Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Firewall Manager 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForFMS`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Firewall Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `fms.amazonaws.com`

使用 Firewall Manager 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Firewall Manager 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Firewall Manager 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Firewall Manager 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Firewall Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Firewall Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

您必須使用 AWS Organizations 管理帳戶登入，並將組織內的帳戶設定為 AWS Firewall Manager 管理員帳戶。如需詳細資訊，請參閱 AWS Firewall Manager 開發人員指南中的[設定 AWS Firewall Manager 管理員帳戶](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Firewall Manager 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Firewall Manager 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Firewall Manager，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Firewall Manager 為信任的服務。

```
$ aws organizations enable-aws-service-access \
  --service-principal fms.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Firewall Manager 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您可以使用 AWS Firewall Manager 或 AWS Organizations 工具來停用受信任的存取。

Important

我們強烈建議您盡可能使用 AWS Firewall Manager 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Firewall Manager 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Firewall Manager 提供的工具停用整合成時，才能繼續執行這些步驟。

如果您使用 AWS Firewall Manager 主控台或工具來停用受信任存取，則不需要完成這些步驟。

使用 Firewall Manager 主控台來停用受信任的存取

您可以依照 AWS Firewall Manager AWS Firewall Manager 開發人員指南中[將不同帳戶指定為管理員帳戶的指示](#)，來變更或撤銷 AWS Firewall Manager 管理員帳戶。

如果您撤銷管理員帳戶，您必須登入 AWS Organizations 管理帳戶，並設定新的管理員帳戶 AWS Firewall Manager。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Firewall Manager 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Firewall Manager 對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Firewall Manager，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Firewall Manager 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal fms.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Firewall Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Firewall Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Firewall Manager 的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Firewall Manager 的委託管理員。

如需如何將成員帳戶指定為組織的 Firewall Manager 管理員的說明，請參閱《AWS Firewall Manager 開發人員指南》中的[設定 AWS Firewall Manager 管理員帳戶](#)。

Amazon GuardDuty 和 AWS Organizations

Amazon GuardDuty 是持續性安全監控服務，可分析和處理各種資料來源，並使用威脅智慧饋送和機器學習技術來識別您的 AWS 環境中的非預期和可能未經授權的惡意活動。這可能包括權限升級、使用暴露的憑證、與惡意 IP 地址、URL 或網域的通訊，或者 Amazon Elastic Compute Cloud 執行個體和容器工作負載中出現惡意軟體等問題。

您可以透過 Organizations 管理組織中所有帳戶的 GuardDuty，來協助簡化 GuardDuty 的管理。

如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的[使用 AWS Organizations 管理 GuardDuty 帳戶](#)

使用下列資訊來協助您整合 Amazon GuardDuty AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。這些角色允許 GuardDuty 在您組織的組織帳戶中執行支援的操作。只有在您停用 GuardDuty 與 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除此角色。

- 會在已將 GuardDuty 與 Organizations 整合的帳戶中自動建立 `AWSServiceRoleForAmazonGuardDuty` 服務連結角色。如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的[使用 Organizations 管理 GuardDuty 帳戶](#)
- 會在已啟用 GuardDuty 惡意軟體防護的帳戶中自動建立 `AmazonGuardDutyMalwareProtectionServiceRolePolicy` 服務連結角色。如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南中的[用於 GuardDuty 惡意軟體防護的服務連結角色許可](#)

服務連結角色所使用的服務委託人

- guardduty.amazonaws.com，由 AWSServiceRoleForAmazonGuardDuty 服務連結角色使用。
- malware-protection.guardduty.amazonaws.com，由 AmazonGuardDutyMalwareProtectionServiceRolePolicy 服務連結角色使用。

使用 GuardDuty 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Amazon GuardDuty 啟用受信任存取。

Amazon GuardDuty 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的 GuardDuty 管理員。如果您使用 GuardDuty 主控台設定委派管理員，則 GuardDuty 會自動為您啟用受信任的存取。

不過，如果您想要使用 AWS CLI 或其中一個 AWS SDKs 來設定委派管理員帳戶，則必須明確呼叫 [EnableAWSServiceAccess](#) 操作，並提供服務主體做為參數。然後，可以呼叫 [EnableOrganizationAdminAccount](#)，來委派 GuardDuty 管理員帳戶。

使用 GuardDuty 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 停用 Amazon GuardDuty 做為信任的服務。

```
$ aws organizations disable-aws-service-access \  
--service-principal guardduty.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 GuardDuty 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 GuardDuty 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 GuardDuty 的管理分開。

最低許可

如需將成員帳戶指定為委派管理員所需許可的相關資訊，請參閱Amazon GuardDuty 使用者指南中的[指定委派管理員所需的許可](#)

將成員帳戶指定為 GuardDuty 的委派管理員

請參閱[指定委派的管理員並新增成員帳戶 \(主控台\)](#)和[指定委派的管理員並新增成員帳戶 \(API\)](#)

AWS Health 和 AWS Organizations

AWS Health 可讓您持續了解資源效能，以及 AWS 服務和帳戶的可用性。當您 AWS 的資源和服務受到問題影響或即將受到變更影響時 AWS Health，會交付事件。啟用組織檢視後，組織管理帳戶中的使用者可以彙總組織中所有帳戶 AWS Health 的事件。組織檢視只會顯示啟用此功能後交付 AWS Health 的事件，並保留 90 天。

您可以使用 AWS Health 主控台、AWS Command Line Interface (AWS CLI) 或 AWS Health API 來啟用組織檢視。

如需詳細資訊，請參閱AWS Health 《使用者指南》中的[彙總 AWS Health 事件](#)。

使用下列資訊來協助您 AWS Health 整合 AWS Organizations。

整合的服務連結角色

AWSServiceRoleForHealth_Organizations 服務連結角色允許 在您的組織中的 帳戶內 AWS Health 執行支援的操作。

當您透過呼叫 [EnableHealthServiceAccessForOrganization](#) API 操作來啟用受信任存取時，系統會在組織的管理帳戶中自動建立此角色。否則，請使用 AWS Health 主控台、API 或 CLI 建立角色，如 [IAM 使用者指南](#) 中的 [建立服務連結角色](#) 所述。

只有在停用 AWS Health 和 Organizations 之間的信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Health 授予下列服務主體存取權的服務連結角色：

- `health.amazonaws.com`

使用 AWS Health 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱 [啟用信任的存取所需的許可](#)。

當您為 啟用組織檢視功能時 AWS Health，也會自動為您啟用受信任的存取。

您可以使用 AWS Health 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Health 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Health 執行其所需的任何組態，例如建立 服務所需的資源。只有在您無法使用 AWS Health 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱 [本說明](#)。如果您使用 AWS Health 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Health 主控台啟用受信任存取

您可以使用 AWS Health 和下列其中一個選項來啟用信任存取：

- 使用 AWS Health 主控台。如需詳細資訊，請參閱 [AWS Health 使用者指南](#) 中的 [組織檢視 \(主控台\)](#)。
- 使用 AWS CLI。如需詳細資訊，請參閱 [AWS Health 使用者指南](#) 中的 [組織檢視 \(CLI\)](#)。
- 呼叫 [EnableHealthServiceAccessForOrganization](#) API 操作。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Health 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal health.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Health 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

停用組織檢視功能後，會 AWS Health 停止您組織中所有其他帳戶的彙總事件。這也會為您自動停用受信任存取。

您可以使用 AWS Health 或 AWS Organizations 工具來停用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Health 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Health 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Health 提供的工具停用整合時，才能繼續執行這些步驟。

如果您使用 AWS Health 主控台或工具來停用受信任存取，則不需要完成這些步驟。

使用 AWS Health 主控台停用信任存取

您可以使用以下其中一個選項來停用受信任存取：

- 使用 AWS Health 主控台。如需詳細資訊，請參閱AWS Health 使用者指南中的[停用組織檢視 \(主控台\)](#)。
- 使用 AWS CLI。如需詳細資訊，請參閱AWS Health 使用者指南中的[停用組織檢視 \(CLI\)](#)。

- 呼叫 [DisableHealthServiceAccessForOrganization](#) API 操作。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Health 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal health.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 的委派管理員帳戶 AWS Health

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 AWS Health 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 AWS Health 的管理分開。

將成員帳戶指定為 AWS Health 的委派管理員

參見 [註冊委派管理員以進行組織檢視](#)

移除 AWS Health 的委派管理員

參見 [移除組織檢視中的委派管理員](#)

AWS Identity and Access Management 而且 AWS Organizations

AWS Identity and Access Management 是一種 Web 服務，可安全地控制對 AWS 服務的存取。

您可以在 IAM 中使用 [上次存取的服務資料](#)，以協助您更好地了解整個組織的 AWS 活動。您可以使用此資料來建立和更新 [服務控制政策 \(SCP\)](#)，將存取限制在僅限您組織帳戶所用的 AWS 服務。

如需範例，請參閱 IAM 使用者指南中的[使用資料來精簡組織單位的許可](#)中的

IAM 可讓您集中管理根使用者憑證，並在成員帳戶上執行特權任務。在您啟用根存取管理，以啟用 IAM 的信任存取後 AWS Organizations，您可以集中保護成員帳戶的根使用者憑證。成員帳戶無法登入其根使用者，也無法為其根使用者執行密碼復原。IAM 的管理帳戶或委派管理員帳戶也可以使用短期根存取對成員帳戶執行一些特殊權限任務。短期特權工作階段會為您提供臨時憑證，以便您可以確定相關範圍，對組織中的成員帳戶採取特權動作。

如需詳細資訊，請參閱《IAM 使用者指南》中的[集中管理成員帳戶的根存取權](#)。

使用下列資訊來協助您 AWS Identity and Access Management 整合 AWS Organizations。

使用 IAM 啟用受信任存取

當您啟用根存取管理時，會為 IAM in 啟用受信任存取 AWS Organizations。

使用 IAM 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS Identity and Access Management。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Identity and Access Management 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Identity and Access Management對話方塊中，輸入停用進行確認，然後選擇停用信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Identity and Access Management，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Identity and Access Management 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal iam.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 IAM 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對成員帳戶執行特權任務，否則只能由組織管理帳戶中的使用者或角色執行。如需詳細資訊，請參閱《IAM 使用者指南》中的[在 Organizations 成員帳戶上執行特權任務](#)。

只有組織管理帳戶中的管理員可以設定 IAM 的委派管理員。

您可以從 IAM 主控台或 API，或使用 Organizations CLI 或 SDK 操作來指定委派管理員帳戶。

停用 IAM 的委派管理員

只有 Organizations 管理帳戶或 IAM 委派管理員帳戶中的管理員，才能從組織中移除委派管理員帳戶。您可以使用 Organizations CLI 或 SDK `DeregisterDelegatedAdministrator` 操作來停用委派的管理。

Amazon Inspector 和 AWS Organizations

Amazon Inspector 是一項自動化漏洞管理服務，可持續掃描 Amazon EC2 和容器工作負載，以尋找軟體漏洞和意外的網路暴露。

使用 Amazon Inspector，您只需委派 Amazon Inspector 的管理員帳戶，AWS Organizations 即可管理透過 建立關聯的多個帳戶。委派管理員管理組織的 Amazon Inspector，並被授予代表組織執行任務所需的特殊許可，例如：

- 啟用或停用成員帳戶掃描
- 檢視整個組織的彙總問題清單資料
- 建立和管理隱藏規則

如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的[使用 AWS Organizations 管理多個帳戶](#)。

使用下列資訊來協助您整合 Amazon Inspector AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 Amazon Inspector 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Amazon Inspector 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForAmazonInspector2`

如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的[將服務連結角色用於 Amazon Inspector](#)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon Inspector 使用的服務連結角色會將存取權授予下列服務委託人：

- `inspector2.amazonaws.com`

使用 Amazon Inspector 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

Amazon Inspector 需要信任的 存取權 AWS Organizations，才能將成員帳戶指定為組織的此服務委派管理員。

當您指定 Amazon Inspector 的委派管理員時，Amazon Inspector 會自動啟用組織中 Amazon Inspector 的受信任存取。

不過，如果您想要使用 AWS CLI 或其中一個 AWS SDKs 來設定委派管理員帳戶，則必須明確呼叫 `EnableAWSServiceAccess` 操作，並提供 服務主體做為 參數。然後，您可以呼叫 `EnableDelegatedAdminAccount` 以委派 Inspector 管理員帳戶。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以啟用 Amazon Inspector 做為 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \  
    --service-principal inspector2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

Note

如果您使用 `EnableAWSServiceAccess` API，您還需要呼叫 [EnableDelegatedAdminAccount](#) 以委派 Inspector 管理員帳戶。

使用 Amazon Inspector 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 Amazon Inspector 停用受信任存取。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，將 Amazon Inspector 停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Amazon Inspector 的委派管理員帳戶

使用 Amazon Inspector，您可以使用委派管理員 AWS Organizations 與服務來管理組織中的多個帳戶。

AWS Organizations 管理帳戶會將組織內的帳戶指定為 Amazon Inspector 的委派管理員帳戶。委派管理員管理組織的 Amazon Inspector，並被授予代表組織執行任務所需的特殊許可，例如：啟用或停用成員帳戶掃描、檢視整個組織的彙總問題清單資料，以及建立和管理隱藏規則

如需有關委派管理員如何管理組織帳戶的資訊，請參閱《Amazon Inspector 使用者指南》中的[了解管理員和成員帳戶之間的關係](#)。

只有組織管理帳戶中的管理員可以設定 Amazon Inspector 的委派管理員。

您可以從 Amazon Inspector 主控台或 API，或使用 Organizations CLI 或 SDK 操作，指定委派管理員帳戶。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Amazon Inspector 的委派管理員

若要使用 Amazon Inspector 主控台設定委派管理員，請參閱《Amazon Inspector 使用者指南》中的[步驟 1：啟用 Amazon Inspector - 多帳戶環境](#)。

Note

您必須在您使用 Amazon Inspector 的每個區域中呼叫 `inspector2:enableDelegatedAdminAccount`。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal inspector2.amazonaws.com
```

- AWS SDK：呼叫 `Organizations RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 `account.amazonaws.com` 為參數。

停用 Amazon Inspector 的委派管理員

只有 AWS Organizations 管理帳戶中的管理員才能從組織中移除委派的管理員帳戶。

您可以使用 Amazon Inspector 主控台或 API，或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，移除委派管理員。若要使用 Amazon Inspector 主控台移除委派管理員，請參閱《Amazon Inspector 使用者指南》中的[移除委派管理員](#)。

AWS License Manager 和 AWS Organizations

AWS License Manager 簡化將軟體廠商授權帶入雲端的程序。當您在建置雲端基礎設施時 AWS，您可以使用 `bring-your-own-license (BYOL)` 機會來節省成本，也就是說，您可以重新使用現有的授權庫存，以搭配雲端資源使用。有了規則為基礎的授權消費限制，管理員即可針對現有雲端部署設定嚴格或寬鬆的限制，藉此預防不合規伺服器使用情形發生。

如需有關 License Manager 的詳細資訊，請參閱 [License Manager 使用者指南](#)。

透過將 License Manager 與連結 AWS Organizations，您可以：

- 在組織中實現運算資源的跨帳戶探索。
- 檢視和管理您擁有的並在 AWS 上執行的商業 Linux 訂閱。如需詳細資訊，請參閱 [AWS License Manager 中的 Linux 訂閱](#)。

使用下列資訊來協助您 AWS License Manager 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。這些角色允許 License Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 License Manager 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改角色。

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

如需詳細資訊，請參閱 [License Manager – 管理帳戶角色](#)、[License Manager – 成員帳戶角色](#)和 [License Manager – Linux 訂閱角色](#)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。License Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

使用 License Manager 來啟用受信任存取

您只能使用 啟用受信任的存取 AWS License Manager。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

使用 License Manager 來啟用受信任存取

您必須使用您的 AWS Organizations 管理帳戶登入 License Manager 主控台，並將其與您的 License Manager 帳戶建立關聯。如需詳細資訊，請參閱 [中的設定 AWS License Manager](#)。

使用 License Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

您可以執行下列命令，將 停用 AWS License Manager 為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal license-manager.amazonaws.com
```

此命令成功後就不會產生輸出。

若要停用 Linux 訂閱的受信任存取，請使用：

```
$ aws organizations disable-aws-service-access \
  --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWS API : [DisableAWSServiceAccess](#)

啟用 License Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 License Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 License Manager 的管理分開。

若要將成員帳戶委派為 License Manager 的管理員，請遵循 License Manager 使用者指南中的[註冊委派管理員](#)。

AWS Managed Services (AMS) 自助服務報告 (SSR) 和 AWS Organizations

[AWS Managed Services \(AMS\) 自助式服務報告 \(SSR\)](#) 會從各種原生 AWS 服務收集資料，並提供主要 AMS 產品的報告存取權。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。

與整合後 AWS Organizations，您可以啟用彙總自助式報告 (SSR)。這是 AMS 功能，可讓進階和加速客戶檢視其在組織層級跨帳戶彙總的現有自助式服務報告。這可讓您了解關鍵操作指標，例如修補程式合規、備份涵蓋範圍，以及其中所有 AMS 受管帳戶的事件 AWS Organizations。

使用下列資訊來協助您整合 AWS Managed Services (AMS) 自助服務報告 (SSR) AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色可讓 AMS 在您的組織中的帳戶內執行支援的操作。

只有在停用 AMS 和 Organizations 之間的信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AMS 使用的服務連結角色會將存取權授予下列服務主體：

- `selfservicereporting.managedservices.amazonaws.com`

使用 AMS 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 AWS Managed Services (AMS) 自助式服務報告 (SSR) 啟用為信任的服務。

```
$ aws organizations enable-aws-service-access \  
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AMS 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 AWS Managed Services (AMS) 自助式服務報告 (SSR) 停用為信任的服務。

```
$ aws organizations disable-aws-service-access \  
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 AMS 的委派管理員帳戶

委派管理員帳戶可以在 AMS 主控台的單一彙總檢視中檢視所有帳戶的 AMS 報告（例如修補程式和備份）。

您可以使用 AMS 主控台或 API，或使用 Organizations CLI 或 SDK `RegisterDelegatedAdministrator` 操作來新增委派管理員。

停用 AMS 的委派管理員

只有組織管理帳戶中的管理員可以設定 AMS 的委派管理員。

您可以使用 AMS 主控台或 API，或使用 Organizations CLI 或 SDK `DeregisterDelegatedAdministrator` 操作來移除委派管理員。

Amazon Macie 和 AWS Organizations

Amazon Macie 是一種全受管資料安全和資料隱私權服務，該服務使用機器學習和模式比對來探索、監控和協助您保護 Amazon Simple Storage Service (Amazon S3) 中的敏感資料。Macie 會自動探索敏感資料，例如個人身分識別資訊 (PII) 和智慧財產權，讓您更清楚了解組織在 Amazon S3 中存放在的資料。

如需詳細資訊，請參閱[Amazon Macie 使用者指南](#)中的[使用 AWS Organizations 管理 Amazon Macie 帳戶](#)。

使用下列資訊來協助您整合 Amazon Macie 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會自動為您組織的委派 Macie 管理員帳戶建立以下[服務連結角色](#)。該角色允許 Macie 為您組織的帳戶執行支援的操作。

只有在您停用 Macie 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能刪除此角色。

- `AWSServiceRoleForAmazonMacie`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Macie 使用的服務連結角色會將存取權授予下列服務委託人：

- `macie.amazonaws.com`

使用 Macie 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 Amazon Macie 主控台或 AWS Organizations 主控台來啟用受信任存取。

Important

強烈建議您盡可能使用 Amazon Macie 主控台或工具來啟用與 Organizations 整合。這可讓 Amazon Macie 執行其需要的任何組態，例如建立服務所需的資源。只有在您無法使用 Amazon Macie 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 Amazon Macie 主控台或工具啟用受信任的存取，則不需要完成這些步驟。

使用 Amazon Macie 主控台來啟用受信任存取

Amazon Macie 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的 Macie 管理員。如果您使用 Macie 管理主控台設定委派管理員，則 Macie 會自動為您啟用受信任的存取。

如需詳細資訊，請參閱 Amazon Macie 使用者指南中的[在 Amazon Macie 中整合和設定組織](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，讓 Amazon Macie 成為 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal macie.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

啟用 Macie 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Macie 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Macie 的管理分開。

最低許可

只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Macie 的委託管理員：

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

將成員帳戶指定為 Macie 的委派管理員

Amazon Macie 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的 Macie 管理員。如果您使用 Macie 管理主控台設定委派管理員，則 Macie 會自動為您啟用受信任的存取。

如需詳細資訊，請參閱 <https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin>

AWS Marketplace 和 AWS Organizations

AWS Marketplace 是精選的數位目錄，可用來尋找、購買、部署和管理第三方軟體、資料和服務，而您需要這些軟體、資料和服務來建置解決方案並執行您的企業。

AWS Marketplace 會使用 建立和管理授權 AWS License Manager，以用於 中的購買 AWS Marketplace。當您與組織中的其他帳戶共享您的授權 (授予存取權) 時，AWS Marketplace 會為這些帳戶建立和管理新的授權。

如需詳細資訊，請參閱 AWS Marketplace 買家指南中的 [AWS Marketplace 的服務連結角色](#)。

使用下列資訊來協助您 AWS Marketplace 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下 [服務連結角色](#)。此角色允許 在您的組織中的 帳戶內 AWS Marketplace 執行支援的操作。

只有在您停用 AWS Marketplace 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForMarketplaceLicenseManagement`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS Marketplace 授予下列服務主體存取權的服務連結角色：

- `license-management.marketplace.amazonaws.com`

使用 AWS Marketplace 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Marketplace 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Marketplace 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Marketplace 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Marketplace 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Marketplace 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS Marketplace 主控台啟用受信任存取

請參閱《AWS Marketplace 買方指南》中的[為 建立服務連結角色 AWS Marketplace](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。

2. 在導覽窗格中，選擇服務。
3. AWS Marketplace 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Marketplace對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Marketplace，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Marketplace 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Marketplace停用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具啟用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Marketplace 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

AWS Marketplace 私有 Marketplace 和 AWS Organizations

AWS Marketplace 是精選的數位目錄，可用來尋找、購買、部署和管理第三方軟體、資料和服務，而您需要這些軟體、資料和服務來建置解決方案並執行您的企業。私有市場為您提供廣泛的產品目錄 AWS Marketplace，以及這些產品的精細控制。

AWS Marketplace Private Marketplace 可讓您建立與整個組織、一或多個 OUs 或組織中一或多個帳戶相關聯的多個私有市場體驗，每個帳戶都有自己的核准產品集。您的 AWS 管理員也可以使用公司或團隊的標誌、訊息和顏色方案，將公司品牌套用到每個私有市場體驗。

如需詳細資訊，請參閱《AWS Marketplace 買方指南》中的[使用角色在中設定私有 Marketplace AWS Marketplace](#)。

使用以下資訊來協助您整合 AWS Marketplace Private Marketplace 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您使用 AWS Marketplace Private Marketplace 主控台啟用信任存取時，系統會自動在組織的管理帳戶中建立下列服務連結角色。此角色允許 Private Marketplace 在組織中的組織帳戶中執行支援的操作。只有在您停用 AWS Marketplace Private Marketplace 和 Organizations 之間的受信任存取，並取消組織中的所有私有市集體驗的關聯時，才能刪除或修改此角色。

如果您直接從 Organizations 主控台、CLI 或 SDK 啟用受信任存取，則不會自動建立服務連結角色。

- `AWSServiceRoleForPrivateMarketplaceAdmin`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Private Marketplace 使用的服務連結角色會將存取權授予下列服務主體：

- `private-marketplace.marketplace.amazonaws.com`

使用 Private Marketplace 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Marketplace Private Marketplace 主控台或 主控台來啟用受信任存取 AWS Organizations 。

Important

我們強烈建議您盡可能使用 AWS Marketplace Private Marketplace 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Marketplace Private Marketplace 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Marketplace Private Marketplace 提供的工具啟用整合時，才能繼續進行這些步驟。如需詳細資訊，請參閱[本說明](#)。如果您使用 AWS Marketplace Private Marketplace 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Private Marketplace 主控台啟用受信任存取

請參閱 AWS Marketplace 購買者指南中的[私有市集入門](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在 服務清單中選擇 AWS Marketplace 私有 Marketplace。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 AWS Marketplace Private Marketplace 的信任存取對話方塊中，輸入啟用以進行確認，然後選擇啟用信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴 AWS Marketplace Private Marketplace 的管理員，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 AWS Marketplace Private Marketplace 啟用為信任的服務。

```
$ aws organizations enable-aws-service-access \
  --service-principal private-marketplace.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Private Marketplace 停用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 停用 AWS Marketplace Private Marketplace 做為信任的服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal private-marketplace.marketplace.amazonaws.com
```


此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

為 Private Marketplace 啟用委派管理員帳戶

管理帳戶管理員可以將 Private Marketplace 管理許可委派給稱為委派管理員的指定成員帳戶。若要將帳戶註冊為私有市集的委派管理員，管理帳戶管理員必須確保啟用信任的存取和服務連結角色，選擇註冊新的管理員，提供 12 位數 AWS 的帳號，然後選擇提交。

管理帳戶和委派管理員帳戶可以執行 Private Marketplace 管理任務，例如建立體驗、更新品牌設定、關聯或取消關聯對象、新增或移除產品，以及核准或拒絕待處理的請求。

若要使用 Private Marketplace 主控台設定委派管理員，請參閱 AWS Marketplace 買方指南中的[建立和管理私有市集](#)。

您也可以使用 Organizations `RegisterDelegatedAdministrator` API 來設定委派管理員。如需詳細資訊，請參閱 Organizations Command Reference (Organizations 命令參考) 中的[RegisterDelegatedAdministrator](#)。

停用 Private Marketplace 的委派管理員

只有組織管理帳戶中的管理員可以設定 Private Marketplace 的委派管理員。

您可以使用 Private Marketplace 主控台或 API，或使用 Organizations CLI 或 SDK `DeregisterDelegatedAdministrator` 操作來移除委派管理員。

若要使用 Private Marketplace 主控台停用委派的管理員私有 Marketplace 帳戶，請參閱 AWS Marketplace 買方指南中的[建立和管理私有市集](#)

AWS Marketplace 採購洞察儀表板和 AWS Organizations

您可以使用 AWS Marketplace 採購洞察儀表板來檢視組織中所有 AWS 帳戶的協議和成本分析資料。與 Organizations 整合時，AWS Marketplace 採購洞見儀表板會接聽組織變更，例如加入組織的帳戶，並彙總其對應協議的資料以建置其儀表板。

如需詳細資訊，請參閱 AWS Marketplace 買方指南中的[採購洞察](#)。

使用下列資訊，協助您整合 AWS Marketplace 採購洞見儀表板 AWS Organizations。

啟用整合時建立的服務連結角色和受管政策

當您啟用 AWS Marketplace 採購洞見儀表板時，即會建立 [AWSServiceRoleForProcurementInsightsPolicy](#) 服務連結角色和 [AWSServiceRoleForProcurementInsightsPolicy](#) AWS 受管政策。

使用 AWS Marketplace 採購洞見啟用受信任的存取

啟用信任存取可讓 AWS Marketplace 採購洞見儀表板與客戶的 Organizations 服務整合。AWS Marketplace 採購洞見儀表板會聆聽組織變更，例如加入組織的帳戶，並彙總其對應協議的資料以建置其儀表板。

如需啟用受信任存取所需許可的資訊，請參閱 [啟用信任的存取所需的許可](#)。

您可以使用 AWS Marketplace 採購洞見儀表板主控台或主控台來啟用受信任存取 AWS Organizations。

Important

我們強烈建議您盡可能使用 AWS Marketplace 採購洞見儀表板主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Marketplace 採購洞見儀表板執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Marketplace 採購洞見儀表板提供的工具啟用整合時，才能繼續進行這些步驟。如需詳細資訊，請參閱 [本說明](#)。

如果您使用 AWS Marketplace 採購洞見儀表板主控台或工具啟用受信任存取，則不需要完成這些步驟。

啟用 AWS Marketplace 採購洞見儀表板以啟用受信任的存取

請參閱《AWS Marketplace 買方指南》中的 [啟用 AWS Marketplace 採購洞見儀表板](#)。

使用 Organizations 工具啟用受信任存取

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇AWS Marketplace 採購洞察儀表板。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 AWS Marketplace 採購洞見儀表板的信任存取對話方塊中，輸入啟用以進行確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告知 AWS Marketplace 採購洞見儀表板的管理員，他們現在可以從服務主控台 啟用該服務來使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以透過 Organizations 將 AWS Marketplace 採購洞見儀表板啟用為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal procurement-insights.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS Marketplace 採購洞見停用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具停用受信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，將 AWS Marketplace 採購洞見儀表板停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal procurement-insights.marketplace.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用委派管理員帳戶以取得 AWS Marketplace 採購洞見

若要在 AWS Marketplace 採購洞見主控台中設定委派管理員，請參閱《AWS Marketplace 買方指南》中的[註冊委派管理員](#)。

您也可以使用 Organizations RegisterDelegatedAdministrator API 來設定委派管理員。如需詳細資訊，請參閱 Organizations Command Reference (Organizations 命令參考) 中的[RegisterDelegatedAdministrator](#)。

停用委派管理員以取得 AWS Marketplace 採購洞見

只有組織管理帳戶中的管理員可以設定委派管理員以取得 AWS Marketplace 採購洞見。

若要透過 AWS Marketplace 採購洞見主控台移除委派管理員，請參閱 AWS Marketplace 買方指南中的[取消註冊委派管理員](#)。

您也可以使用 Organizations CLI 或 SDK DeregisterDelegatedAdministrator 操作來移除委派管理員。

AWS Network Manager 和 AWS Organizations

Network Manager 可讓您跨 AWS 帳戶、區域和 AWS 內部部署位置集中管理 AWS Cloud WAN 核心網路和 Transit Gateway 網路。透過多帳戶支援，您可以為任何 AWS 帳戶建立單一全域網路，並使用 Network Manager 主控台註冊從多個帳戶到全球網路的傳輸閘道。

啟用 Network Manager 和 Organizations 之間受信任的存取權後，已註冊的委派管理員和管理帳戶可以利用成員帳戶中部署的服務連結角色來描述連接至全域網路的資源。在 Network Manager 主控台中，註冊的委派管理員和管理帳戶可以承擔在成員帳戶中部署的自訂 IAM 角色：CloudWatch-CrossAccountSharingRole 用於多帳戶監控和事件，以及 IAMRoleForAWSNetworkManagerCrossAccountResourceAccess 用於主控台交換機角色存取權限，以查看和管理多帳戶資源。

Important

- 我們強烈建議使用 Network Manager 主控台來管理多帳戶設定 (啟用/停用受信任的存取權，以及註冊/取消註冊委派管理員)。若從主控台管理這些設定，即會自動將所有必需的服務連結角色和自訂 IAM 角色部署和管理至多帳戶存取所需的成員帳戶。
- 當您在 Network Manager 主控台中啟用 Network Manager 的信任存取時，主控台也會啟用 AWS CloudFormation StackSets 服務。Network Manager 使用 StackSets 部署多帳戶管理所需的自訂 IAM 角色。

如需有關將 Network Manager 與組織整合的詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 AWS Organizations 管理多個 Network Manager 中的帳戶](#)。

使用下列資訊協助您整合 AWS Network Manager 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在列出的組織帳戶中自動建立以下[服務連結角色](#)。這些角色允許 Network Manager 在您組織的帳戶中執行支援的操作。如果停用受信任的存取，Network Manager 將不會從組織中的帳戶刪除這些角色。您可以使用 IAM 主控台手動將其刪除。

管理帳戶

- AWSServiceRoleForNetworkManager
- AWSServiceRoleForCloudFormationStackSetsOrgAdmin
- AWSServiceRoleForCloudWatchCrossAccount

成員帳戶

- AWSServiceRoleForNetworkManager

- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

當您將成員帳戶註冊為委派管理員時，將在委派管理員帳戶中自動建立以下附加角色：

- `AWSServiceRoleForCloudWatchCrossAccount`

服務連結角色所使用的服務委託人

服務連結角色只能由依據角色定義的信任關係所授權的服務主體來假設。

- 對於 `AWSServiceRoleForNetworkManager` service-linked 角色，`networkmanager.amazonaws.com` 是唯一具有存取權限的服務主體。
- 對於 `AWSServiceRoleForCloudFormationStackSetsOrgMember` 服務連結角色，`member.org.stacksets.cloudformation.amazonaws.com` 是唯一具有存取權限的服務主體。
- 對於 `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` 服務連結角色，`stacksets.cloudformation.amazonaws.com` 是唯一具有存取權限的服務主體。
- 對於 `AWSServiceRoleForCloudWatchCrossAccount` 服務連結角色，`cloudwatch-crossaccount.amazonaws.com` 是唯一具有存取權限的服務主體。

刪除這些角色將影響 Network Manager 的多帳戶功能。

使用 Network Manager 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

只有 Organizations 管理帳戶中的管理員才具有許可，以使用其他服務啟用受信任存取 AWS。請務必使用 Network Manager 主控台來啟用受信任的存取，以避免權限問題。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 AWS Organizations 管理多個 Network Manager 中的帳戶](#)。

使用 Network Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 Organizations 管理帳戶中的管理員才具有使用其他服務停用信任存取的許可 AWS。

Important

我們強烈建議您使用 Network Manager 主控台來停用受信任的存取。如果您以任何其他方式停用受信任存取，例如使用 AWS CLI、搭配 API 或 AWS CloudFormation 主控台，則部署的 AWS CloudFormation StackSets 和自訂 IAM 角色可能無法正確清除。若要停用受信任的服務存取，請登入 [Network Manager 主控台](#)。

為 Network Manager 啟用委派的管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Network Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Network Manager 的管理分開。

如需如何將成員帳戶指定為組織中 Network Manager 的委派管理員，請參閱 Amazon VPC 使用者指南中的 [註冊委派管理員](#)。

Amazon Q 開發人員和 AWS Organizations

Amazon Q Developer 是生成式 AI 支援的對話助理，可協助您了解、建置、延伸和操作 AWS 應用程式。它也是一般用途、採用機器學習技術的程式碼產生器，可即時為您提供程式碼建議。Amazon Q Developer 的付費訂閱版本需要 Organizations 整合。如需詳細資訊，請參閱 [《Amazon Q 使用者指南》中的帳戶、IAM Identity Center 和 Organizations 設定](#)。

使用以下資訊來協助您整合 Amazon Q Developer 與 AWS Organizations。

服務連結角色

AWSServiceRoleForAmazonQDeveloper 服務連結角色可讓 Amazon Q Developer 在您的組織內執行支援的操作。使用 Amazon Q Developer 主控台、API 或 CLI 建立角色，如 [IAM 使用者指南](#) 中的 [建立服務連結角色](#) 所述。

如果您使用的是成員帳戶，則只有在停用 Amazon Q Developer 和 Organizations 之間的受信任存取，或是從組織移除成員帳戶時，才能刪除或修改此角色。

Amazon Q Developer 使用的服務主體

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon Q Developer 使用的服務連結角色會授予下列服務主體存取權：

- `q.amazonaws.com`

使用 Amazon Q Developer 啟用受信任存取

Amazon Q Developer Pro 使用受信任的存取權，將 Organizations 管理帳戶中所做的設定與相同組織中的成員帳戶共用。

例如，在 Organizations 管理帳戶中工作的 Amazon Q Developer Pro 管理員可以使用程式碼參考來啟用建議。如果啟用信任存取，則該組織中所有成員帳戶也會啟用具有程式碼參考的建議。

您只能使用 Amazon Q Developer 啟用受信任存取。

若要啟用 Amazon Q Developer 的信任存取，請使用此程序。

1. 在 Amazon Q 開發人員設定頁面的成員帳戶設定下，選擇編輯。
2. 在快顯視窗中，選取開啟。
3. 選擇 Save (儲存)。

如需詳細資訊，請參閱《Amazon Q Developer 使用者指南》中的[啟用信任存取](#)。

使用 Amazon Q Developer 停用受信任存取

您只能使用 Amazon Q 開發人員工具停用受信任存取。

若要停用 Amazon Q Developer 的信任存取，請使用此程序。

1. 在 Amazon Q 開發人員設定頁面的成員帳戶設定下，選擇編輯。
2. 在快顯視窗中，選取關閉。
3. 選擇 Save (儲存)。

如需詳細資訊，請參閱《Amazon Q Developer 使用者指南》中的[啟用信任存取](#)。

AWS Resource Access Manager 和 AWS Organizations

AWS Resource Access Manager (AWS RAM) 可讓您與其他 共用您擁有的指定 AWS 資源 AWS 帳戶。這是一種集中式服務，可提供一致的體驗，以在多個帳戶中共享不同類型的 AWS 資源。

如需詳細資訊 AWS RAM，請參閱 [AWS RAM 使用者指南](#)。

使用下列資訊來協助您 AWS Resource Access Manager 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 在您的組織中的 帳戶內 AWS RAM 執行支援的操作。

只有在您停用 AWS RAM 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForResourceAccessManager`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS RAM 授予下列服務主體存取權的服務連結角色：

- `ram.amazonaws.com`

使用 AWS RAM 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Resource Access Manager 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Resource Access Manager 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Resource Access Manager 執行其所需的任何組態，例如建立 服務所需的資源。只有在您無法使用 AWS Resource Access Manager 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Resource Access Manager 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS RAM 主控台或 CLI 啟用受信任存取

請參閱 AWS RAM 使用者指南中的[啟用與 AWS Organizations 共享](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Resource Access Manager 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Resource Access Manager 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Resource Access Manager，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Resource Access Manager 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal ram.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS RAM 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您可以使用 AWS Resource Access Manager 或 AWS Organizations 工具來停用受信任的存取。

Important

我們強烈建議您盡可能使用 AWS Resource Access Manager 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Resource Access Manager 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Resource Access Manager 提供的工具停用整合時，才能繼續執行這些步驟。

如果您使用 AWS Resource Access Manager 主控台或工具來停用受信任存取，則不需要完成這些步驟。

使用 AWS Resource Access Manager 主控台或 CLI 停用受信任存取

請參閱AWS RAM 使用者指南中的[啟用與 AWS Organizations 共享](#)。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信任停用的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Resource Access Manager 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Resource Access Manager對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Resource Access Manager，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Resource Access Manager 為信任的服務。

```
$ aws organizations disable-aws-service-access \  
    --service-principal ram.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

AWS 資源總管 和 AWS Organizations

AWS 資源總管 是一項資源搜尋和探索服務。憑藉 Resource Explorer，您可以在類似網際網路搜尋引擎的體驗中探索您的資源，例如 Amazon Elastic Compute Cloud 執行個體、Amazon Kinesis Data Streams 或 Amazon DynamoDB 資料表。您可以使用名稱、標籤和 ID 等資源中繼資料來搜尋資源。Resource Explorer 可跨您帳戶中 AWS 的區域運作，以簡化跨區域工作負載。

當您將 Resource Explorer 與 整合時 AWS Organizations，您可以透過在評估範圍內包含來自您組織的多個 AWS 帳戶，從更廣泛的來源收集證據。

使用下列資訊來協助您 AWS 資源總管 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Resource Explorer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Resource Explorer 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

如需有關 Resource Explorer 如何使用此角色的詳細資訊，請參閱《AWS 資源總管 使用者指南》中的[使用服務連結角色](#)。

- `AWSServiceRoleForResourceExplorer`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Resource Explorer 使用的服務連結角色會將存取權授予下列服務主體：

- `resource-explorer-2.amazonaws.com`

若要啟用 AWS 資源總管的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

Resource Explorer 需要信任的 存取權 AWS Organizations，才能將成員帳戶指定為組織的委派管理員。

您可以使用 Resource Explorer 主控台或 Organizations 主控台來啟用受信任存取。我們強烈建議您盡可能使用 Resource Explorer 主控台或工具來啟用與 Organizations 整合。這可讓 AWS 資源總管 執行其所需的任何組態，例如建立 服務所需的資源。

若要使用 Resource Explorer 主控台來啟用受信任存取

如需有關啟用受信任存取的說明，請參閱《AWS 資源總管 使用者指南》中的[使用 Resource Explorer 的先決條件](#)。

Note

如果您使用 AWS 資源總管 主控台設定委派管理員，AWS 資源總管 會自動為您啟用信任的存取。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS 資源總管 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

若要停用 Resource Explorer 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 停用受信任存取 AWS 資源總管。

您可以使用 AWS 資源總管 或 AWS Organizations 工具來停用受信任的存取。

Important

我們強烈建議您盡可能使用 AWS 資源總管 主控台或工具來停用與 Organizations 的整合。這可讓 AWS 資源總管 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS 資源總管提供的工具停用整合時，才能繼續執行這些步驟。

如果您使用 AWS 資源總管 主控台或工具來停用受信任存取，則不需要完成這些步驟。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS 資源總管 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Resource Explorer 的委派管理員帳戶

使用您的委派管理員帳戶建立多帳戶資源檢視畫面，然後將範圍調整為組織單位或您的整個組織。您可以透過 AWS Resource Access Manager 建立資源共用，與組織中的任何帳戶共用多帳戶檢視。

最低許可

只有具有下列許可之 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Resource Explorer 的委派管理員：

`resource-explorer:RegisterAccount`

如需有關啟用 Resource Explorer 委派管理員帳戶的說明，請參閱《AWS 資源總管 使用者指南》中的[設定](#)。

如果您使用 AWS 資源總管 主控台設定委派管理員，Resource Explorer 會自動為您啟用信任的存取。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務識別 `resource-explorer-2.amazonaws.com` 為參數。

停用 Resource Explorer 的委派管理員

只有 Organizations 管理帳戶或 Resource Explorer 委派管理員帳戶中的管理員可以移除 Resource Explorer 的委派管理員。您可以使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作停用受信任存取。

AWS Security Hub 和 AWS Organizations

AWS Security Hub 可讓您全面檢視的安全狀態，AWS 並協助您根據安全產業標準和最佳實務來檢查環境。

Security Hub 會從 AWS 帳戶、AWS 服務您使用的和支援的第三方合作夥伴產品收集安全資料。它可協助您分析安全趨勢，並識別最高優先級的安全問題。

當您同時使用 Security Hub 和 AWS Organizations 時，您可以為所有帳戶自動啟用 Security Hub，包括新增的新帳戶。這會增加 Security Hub 檢查和問題清單的涵蓋範圍，從而提供更全面和準確的整體安全狀態。

如需有關 Security Hub 的詳細資訊，請參閱 [AWS Security Hub 使用者指南](#)。

使用下列資訊來協助您 AWS Security Hub 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Security Hub 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Security Hub 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForSecurityHub`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Security Hub 使用的服務連結角色會將存取權授予下列服務委託人：

- `securityhub.amazonaws.com`

使用 Security Hub 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

當您指定 Security Hub 的委派管理員時，Security Hub 會自動啟用組織中 Security Hub 的受信任存取。

使用 Security Hub 停用受信任存取

如需停用信任存取所需的許可資訊，請參閱AWS Organizations 《使用者指南》中的[停用信任存取所需的許可](#)。

在您停用信任的存取之前，建議您與組織的委派管理員合作，以停用成員帳戶中的 Security Hub，並清除這些帳戶中的 Security Hub 資源。

您可以使用 AWS Organizations 主控台、Organizations API 或來停用受信任的存取 AWS CLI。只有 Organizations 管理帳戶的管理員可以使用 Security Hub 停用受信任存取。

如需使用 Security Hub 停用受信任存取的指示，請參閱[停用 Security Hub 整合 AWS Organizations](#)。

啟用 Security Hub 的委派管理員

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Security Hub 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Security Hub 的管理分開。

如需相關資訊，請參閱AWS Security Hub 使用者指南中的[指定 Security Hub 管理員帳戶](#)。

將成員帳戶指定為 Security Hub 的委派管理員

1. 使用 Organizations 管理帳戶登入。
2. 執行下列其中一項：
 - 如果您的管理帳戶未啟用 Security Hub，則在 Security Hub 主控台上選擇 Go to Security Hub (移至 Security Hub)。
 - 如果您的管理帳戶已啟用 Security Hub，則在 Security Hub 主控台上，一般選擇設定下。
3. 在 Delegated Administrator (委派的管理員) 下，輸入帳戶 ID。

停用 Security Hub 的委派管理員

只有組織管理帳戶可以移除委派的 Security Hub 管理員帳戶。

若要變更委派的 Security Hub 管理員，您必須先移除目前的委派管理員帳戶，然後指定新的管理員帳戶。

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

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

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

如需停用委派 Security Hub 管理員的指示，請參閱[移除或變更委派管理員](#)。

Amazon S3 Storage Lens 與 AWS Organizations

透過授予 Amazon S3 Storage Lens 對組織的信任存取權，您可以允許它收集和彙總組織中所有 AWS 帳戶的指標。S3 Storage Lens 會透過存取屬於您組織的帳戶清單，收集並分析所有這些帳戶的儲存體、用量和活動指標來執行此操作。

如需詳細資訊，請參閱《Amazon S3 Storage Lens 使用者指南》中的[使用 Amazon S3 Storage Lens 的服務連結角色](#)。

使用下列資訊來協助您整合 Amazon S3 Storage Lens AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取，且 Storage Lens 組態已套用至您的組織時，會自動在您組織的委派管理員帳戶建立以下[服務連結角色](#)。該角色允許 Amazon S3 Storage Lens 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Amazon S3 Storage Lens 和 Organizations 之間的受信任存取，或從組織中移除該成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForS3StorageLens`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon S3 Storage Lens 使用的服務連結角色會將存取權授予下列服務委託人：

- `storage-lens.s3.amazonaws.com`

啟用 Amazon S3 Storage Lens 的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 Amazon S3 Storage Lens 主控台或 AWS Organizations 主控台來啟用受信任存取。

Important

強烈建議您盡可能使用 Amazon S3 Storage Lens 主控台或工具來啟用與 Organizations 整合。這可讓 Amazon S3 Storage Lens 執行其需要的任何組態，例如建立服務所需的資源。只

有在您無法使用 Amazon S3 Storage Lens 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 Amazon S3 Storage Lens 主控台或工具啟用受信任的存取，則不需要完成這些步驟。

使用 Amazon S3 主控台來啟用受信任存取

請參閱《Amazon Simple [Storage Service 使用者指南](#)》中的[啟用 S3 Storage Lens 的受信任存取](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon S3 Storage Lens。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 Amazon S3 Storage Lens 的受信任存取對話方塊中，輸入啟用以確認，然後選擇啟用受信任存取。
6. 如果您只是的管理員 AWS Organizations，請告知 Amazon S3 Storage Lens 的管理員，他們現在可以從服務主控台 啟用該服務。AWS Organizations

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以啟用 Amazon S3 Storage Lens 做為 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \
```

```
--service-principal storage-lens.s3.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

停用 Amazon S3 Storage Lens 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 Amazon S3 Storage Lens 工具停用受信任的存取。

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS SDKs 來停用受信任存取。

使用 Amazon S3 主控台來停用受信任存取

請參閱《Amazon Simple [Storage Service 使用者指南](#)》中的[停用 S3 Storage Lens 的受信任存取](#)。

啟用 Amazon S3 Storage Lens 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Amazon S3 Storage Lens 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Amazon S3 Storage Lens 的管理分開。

最低許可

只有具有下列許可的 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Amazon S3 Storage Lens 的委託管理員：

```
organizations:RegisterDelegatedAdministrator  
organizations:DeregisterDelegatedAdministrator
```

Amazon S3 Storage Lens 最多可支援您組織中的 5 個委派管理員帳戶。

將成員帳戶指定為 Amazon S3 Storage Lens 的委派管理員

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS SDKs 註冊委派管理員。若要使用 Amazon S3 主控台將成員帳戶註冊為組織的委派管理員帳戶，請參閱《Amazon Simple Storage Service 使用者指南》中的[註冊 S3 Storage Lens 的委派管理員](#)。

取消註冊 Amazon S3 Storage Lens 的委派管理員。

您可以使用 Amazon S3 主控台、AWS CLI 或任何 AWS SDKs 取消註冊委派管理員。若要使用 Amazon S3 主控台取消註冊委派管理員，請參閱《Amazon Simple Storage Service 使用者指南》中的[取消註冊 S3 Storage Lens 的委派管理員](#)。

AWS 安全事件回應和 AWS Organizations

AWS 安全事件回應是一項安全服務，提供全年無休的即時、人為輔助安全事件支援，協助客戶快速回應憑證遭竊和勒索軟體攻擊等網路安全事件。透過與 Organizations 整合，您可以為整個組織啟用安全涵蓋範圍。如需詳細資訊，請參閱《[AWS 安全事件回應使用者指南](#)》中的[使用 管理 AWS Organizations](#)安全事件回應帳戶。

使用以下資訊來協助您整合 AWS 安全事件回應 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下服務連結角色。

- `AWSServiceRoleForSecurityIncidentResponse` - 用於建立安全事件回應成員資格 - 透過 訂閱服務 AWS Organizations。
- `AWSServiceRoleForSecurityIncidentResponse_Triage` - 只有在註冊期間啟用分類功能時才會使用。

安全事件回應所使用的服務主體

上一節中的服務連結角色只能由角色所定義的信任關係授權的服務主體擔任。安全事件回應所使用的服務連結角色會將存取權授予下列服務主體：

- `security-ir.amazonaws.com`

啟用安全事件回應的信任存取

啟用安全事件回應的受信任存取權可讓服務追蹤組織的結構，並確保組織中的所有帳戶都有作用中的安全事件涵蓋範圍。當您啟用分類功能時，它也允許服務在成員帳戶中使用服務連結角色來分類功能。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS 安全事件回應主控台或主控台來啟用受信任存取 AWS Organizations。

Important

我們強烈建議您盡可能使用 AWS 安全事件回應主控台或工具來啟用與 Organizations 的整合。這可讓 AWS 安全事件回應執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS 安全事件回應提供的工具啟用整合時，才繼續進行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS 安全事件回應主控台或工具啟用受信任存取，則不需要完成這些步驟。

當您使用安全事件回應主控台進行設定和管理時，Organizations 會自動啟用 Organizations 受信任的存取。如果您使用安全事件回應 CLI/SDK，則必須使用 [EnableAWSServiceAccess API](#) 手動啟用信任存取。若要了解如何透過安全事件回應主控台啟用受信任存取，請參閱《安全事件回應使用者指南》中的[為 AWS 帳戶管理啟用受信任存取](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 AWS 安全事件回應。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 AWS 安全事件回應的信任存取對話方塊中，輸入啟用以進行確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴 AWS 安全事件回應的管理員，他們現在可以從服務主控台 啟用該服務來使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 AWS 安全事件回應啟用為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal security-ir.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用安全事件回應停用受信任存取

只有 Organizations 管理帳戶中的管理員可以使用安全事件回應來停用受信任的存取。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇AWS 安全事件回應。
4. 選擇停用受信任的存取。
5. 在停用 AWS 安全事件回應的受信任存取對話方塊中，輸入停用進行確認，然後選擇停用受信任存取。
6. 如果您只是的管理員 AWS Organizations，請告知 AWS 安全事件回應的管理員，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，將 AWS 安全事件回應停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \  
--service-principal security-ir.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

為安全事件回應啟用委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以針對安全事件回應執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與安全事件回應的管理分開。如需詳細資訊，請參閱《[AWS 安全事件回應使用者指南](#)》中的[使用 管理 AWS Organizations 安全事件回應帳戶](#)。

最低許可

只有 Organizations 管理帳戶中的使用者或角色才能將成員帳戶設定為組織中安全事件回應的委派管理員

若要了解如何透過安全事件回應主控台設定委派管理員，請參閱《[安全事件回應使用者指南](#)》中的[指定委派安全事件回應管理員帳戶](#)。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \  
--account-id 123456789012 \  
--service-principal security-ir.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務識別 security-ir.amazonaws.com 為參數。

針對安全事件回應停用委派管理員

Important

如果成員資格是從委派管理員帳戶建立的，則取消註冊委派管理員是一項破壞性動作，並會導致服務中斷。若要重新註冊 DA：

1. 登入 <https://console.aws.amazon.com/security-ir/home#/membership/settings> 的安全事件回應主控台
2. 從服務主控台取消成員資格。成員資格會保持作用中狀態，直到帳單週期結束為止。
3. 一旦取消成員資格，即會停用透過 Organizations 主控台、CLI 或 SDK 存取服務。

只有 Organizations 管理帳戶中的管理員可以移除安全事件回應的委派管理員。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作來移除委派管理員。

Amazon Security Lake 和 AWS Organizations

Amazon Security Lake 將來自雲端、內部部署和自訂來源的安全資料，集中到存放在您的帳戶的資料湖中。透過與 Organizations 整合，您可以建立資料湖來收集跨帳戶的日誌和事件。如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 [使用 AWS Organizations 管理多個帳戶](#)。

使用下列資訊協助您整合 Amazon Security Lake 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您呼叫 [RegisterDataLakeDelegatedAdministrator](#) API 時，系統會自動在組織的管理帳戶中建立下列 [服務連結角色](#)。此角色可讓 Amazon Security Lake 在您的組織中的帳戶內執行支援的操作。

只有在您停用 Amazon Security Lake 和 Organizations 之間的受信任存取，或是從組織移除成員帳戶時，您才可以刪除或修改此角色。

- `AWSServiceRoleForSecurityLake`

- ⚠ 建議：**使用 Security Lake 的 RegisterDataLakeDelegatedAdministrator API 來允許 Security Lake 存取您的 Organization 並註冊 Organizations 的委派管理員
- 如果您使用 Organizations 的 APIs 註冊委派管理員，則可能不會成功建立 Organizations 的服務連結角色。若要確保完整功能，請使用 Security Lake APIs。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Amazon Security Lake 使用的服務連結角色會授予下列服務主體存取權：

- securitylake.amazonaws.com

使用 Amazon Security Lake 啟用受信任存取

當您使用 Security Lake 啟用受信任存取時，Security Lake 可以自動對組織成員資格的變更做出回應。委派管理員可以從任何組織帳戶中的支援服務啟用 AWS 日誌收集。如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 [Amazon Security Lake 的服務連結角色](#)。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具啟用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon Security Lake。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 Amazon Security Lake 的信任存取對話方塊中，輸入啟用進行確認，然後選擇啟用信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴 Amazon Security Lake 的管理員，他們現在可以從服務主控台 啟用該服務。AWS Organizations

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以啟用 Amazon Security Lake 做為 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Amazon Security Lake 停用受信任存取

只有 Organizations 管理帳戶中的管理員可以使用 Amazon Security Lake 停用受信任存取。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信任停用的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在服務清單中選擇 Amazon Security Lake。
4. 選擇停用受信任的存取。
5. 在停用 Amazon Security Lake 的受信任存取對話方塊中，輸入停用進行確認，然後選擇停用受信任存取。

6. 如果您只是的管理員 AWS Organizations，請告訴 Amazon Security Lake 的管理員，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 停用 Amazon Security Lake 做為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Amazon Security Lake 的委派管理員帳戶

Amazon Security Lake 委派管理員會將組織中的其他帳戶新增為成員帳戶。委派的管理員可以啟用 Amazon Security Lake 並為成員帳戶設定 Amazon Security Lake 設定。委派管理員可以在啟用 Amazon Security Lake 的所有 AWS 區域中（無論您目前正在使用哪個區域端點），跨組織收集日誌。

您還可以設定委派管理員在組織中自動將新帳戶新增為成員。Amazon Security Lake 委派管理員可存取關聯成員帳戶中的日誌和事件。因此，您可以設定 Amazon Security Lake 來收集關聯成員帳戶擁有的資料。您還可以授權訂閱用戶取用關聯成員帳戶擁有的資料。

如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的 [使用 AWS Organizations 管理多個帳戶](#)。

最低許可

只有 Organizations 管理帳戶中的管理員可以將成員帳戶設定為組織中 Amazon Security Lake 的委派管理員

您可以使用 Amazon Security Lake 主控台、Amazon Security Lake `CreateDataLakeDelegatedAdmin` API 操作或 CLI `create-datalake-delegated-admin` 命令來指定委派的管理員帳戶。或者，您可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作。如需為 Amazon Security Lake 啟用委派管理員帳戶的指示，請參閱《Amazon Security Lake 使用者指南》中的[指定委派的 Security Lake 管理員和新增成員帳戶](#)。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK：呼叫 `Organizations RegisterDelegatedAdministrator` 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 `account.amazonaws.com` 為參數。

停用 Amazon Security Lake 的委派管理員

只有 Organizations 管理帳戶或 Amazon Security Lake 委派管理員帳戶中的管理員，才能從組織中移除委派管理員帳戶。

您可以使用 Amazon Security Lake `DeregisterDataLakeDelegatedAdministrator` API 操作、CLI `deregister-data-lake-delegated-administrator` 命令，或使用 Organizations CLI 或 SDK `DeregisterDelegatedAdministrator` 操作來移除委派的管理員帳戶。若要使用 Amazon Security Lake 移除委派管理員，請參閱《[Amazon Security Lake 使用者指南](#)》中的[移除 Amazon Security Lake 委派管理員](#)。

AWS Service Catalog 和 AWS Organizations

Service Catalog 可讓您建立和管理已核准在 AWS 上使用的 IT 服務目錄。

將 Service Catalog 與 AWS Organizations 整合，可簡化整個組織的產品組合共用和產品複製。Service Catalog 管理員可以在共用產品組合 AWS Organizations 時參考中的現有組織，而且可以與組織樹狀結構中的任何信任組織單位 (OU) 共用產品組合。這會消除共用產品組合 ID 的需求，且接收帳戶可在匯入產品組合時手動參考產品組合 ID。透過此機制共用的產品組合會列在 Service Catalog 中管理員之 Imported Portfolio (匯入產品組合) 檢視的共用帳戶中。

如需有關 Service Catalog 的詳細資訊，請參閱 [《Service Catalog 管理員指南》](#)。

使用下列資訊來協助您 AWS Service Catalog 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

AWS Service Catalog 不會建立任何服務連結角色，做為啟用受信任存取的一部分。

用於授予許可的服務委託人

若要啟用受信任存取，必須指定下列服務委託人：

- `servicecatalog.amazonaws.com`

使用 Service Catalog 啟用可信存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Service Catalog 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Service Catalog 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Service Catalog 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Service Catalog 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Service Catalog 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 Service Catalog CLI 或 AWS SDK 啟用受信任存取

呼叫以下其中一個命令或一項操作：

- AWS CLI: [aws servicecatalog enable-aws-organizations-access](#)
- AWS SDKs : [AWSServiceCatalog : EnableAWSOrganizationsAccess](#)

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Service Catalog 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Service Catalog 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Service Catalog，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Service Catalog 為信任的服務。

```
$ aws organizations enable-aws-service-access \  
--service-principal servicecatalog.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Service Catalog 停用可信存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

如果您在使用 Service Catalog AWS Organizations 時停用使用的受信任存取，則不會刪除目前的共用，但會讓您無法在整個組織中建立新的共用。如果呼叫此動作導致目前共享變更，將不會在您的組織結構中同步。

使用 Service Catalog CLI 或 AWS SDK 停用受信任存取

呼叫以下其中一個命令或一項操作：

- AWS CLI: [aws servicecatalog disable-aws-organizations-access](#)
- AWS SDKs : [DisableAWSOrganizationsAccess](#)

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Service Catalog 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Service Catalog 對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Service Catalog，他們現在可以使用服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Service Catalog 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

Service Quotas 與 AWS Organizations

Service Quotas 是一種 AWS 服務，可讓您從中央位置檢視和管理配額。「配額」也稱為限制，即您的 AWS 帳戶中的資源、動作與項目的最大值。

當 Service Quotas 與 建立關聯時 AWS Organizations，您可以建立配額請求範本，以在建立帳戶時自動請求增加配額。

如需 Service Quotas 的詳細資訊，請參閱 [Service Quotas 使用者指南](#)。

使用以下資訊來協助您整合 Service Quotas 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Service Quotas 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Service Quotas 和 Organizations 之間的受信任存取，或從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForServiceQuotas`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Service Quotas 使用的服務連結角色會將存取權授予下列服務委託人：

- `servicequotas.amazonaws.com`

啟用受信任存取與其他 Service Quotas 服務

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Service Quotas 啟用受信任存取。

您可以使用 Service Quotas 主控台 AWS CLI 或 SDK 啟用受信任存取：

- 使用 Service Quotas 主控台來啟用受信任存取。

使用您的 AWS Organizations 管理帳戶登入，然後在 Service Quotas 主控台上設定範本。如需詳細資訊，請參閱 Service Quotas 使用者指南中的[使用 Service Quota 範本](#)。

- 使用 Service Quotas AWS CLI 或 SDK 啟用受信任存取

呼叫以下命令或操作：

- AWS CLI: [aws service-quotas associate-service-quota-template](#)
- AWS SDKs : [AssociateServiceQuotaTemplate](#)

AWS IAM Identity Center 和 AWS Organizations

AWS IAM Identity Center 提供所有 AWS 帳戶 和雲端應用程式的單一登入存取。它透過 與 Microsoft Active Directory 連線 AWS Directory Service，以允許該目錄中的使用者使用其現有的 Active Directory 使用者名稱和密碼登入個人化 AWS 存取入口網站。從 AWS 存取入口網站，使用者可以存取他們擁有許可的所有 AWS 帳戶 和 雲端應用程式。

如需 IAM Identity Center 的詳細資訊，請參閱 [《AWS IAM Identity Center 使用者指南》](#)。

使用下列資訊來協助您 AWS IAM Identity Center 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 IAM Identity Center 在您組織的組織帳戶中執行支援的操作。

只有在您停用 IAM Identity Center 與 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForSSO`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。IAM Identity Center 使用的服務連結角色會將存取權授予下列服務主體：

- `sso.amazonaws.com`

使用 IAM Identity Center 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS IAM Identity Center 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS IAM Identity Center 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS IAM Identity Center 執行其所需的任何組態，例如建立 服務所需的資源。只有在您無法使用 AWS IAM Identity Center 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS IAM Identity Center 主控台或工具啟用受信任存取，則不需要完成這些步驟。

IAM Identity Center 需要 的信任存取 AWS Organizations 才能運作。當您設定 IAM Identity Center 時會啟用受信任的存取。如需詳細資訊，請參閱AWS IAM Identity Center 使用者指南中的[入門 – 步驟 1：啟用 AWS IAM Identity Center](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS IAM Identity Center 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS IAM Identity Center 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS IAM Identity Center，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS IAM Identity Center 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal sso.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 IAM Identity Center 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

IAM Identity Center 需要 的信任存取 AWS Organizations 才能操作。如果您在使用 IAM Identity Center AWS Organizations 時停用 的受信任存取，它會因為無法存取組織而停止運作。使用者無法使用 IAM Identity Center 來存取帳戶。會保留 IAM Identity Center 建立的任何角色，但 IAM Identity Center 服務無法加以存取。會保留 IAM Identity Center 服務連結角色。如果您重新啟用受信任存取，IAM Identity Center 會繼續如之前般運作，而不需重新設定服務。

如果從您的組織移除帳戶，IAM Identity Center 自動會清理任何中繼資料和資源，例如其服務連結角色。從組織移除的獨立帳戶，不再能與 IAM Identity Center 搭配使用。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信停用任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。

3. AWS IAM Identity Center 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS IAM Identity Center 對話方塊中，輸入停用進行確認，然後選擇停用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS IAM Identity Center，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS IAM Identity Center 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal sso.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 IAM Identity Center 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 IAM Identity Center 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 IAM Identity Center 的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 IAM Identity Center 的委派管理員。

如需有關如何為 IAM Identity Center 啟用委派管理員帳戶的說明，請參閱 AWS IAM Identity Center 使用者指南中的[委派的管理員](#)。

AWS Systems Manager 和 AWS Organizations

AWS Systems Manager 是一組功能，可讓您掌握和控制 AWS 資源。在您組織的所有 AWS 帳戶中，以下 Systems Manager 功能皆可與 Organizations 搭配使用：

- Systems Manager Explorer 是可自訂的操作儀表板，可報告 AWS 資源的相關資訊。您可以使用 Organizations and Systems Manager Explorer 來同步 AWS 帳戶組織中所有的操作資料。如需詳細資訊，請參閱AWS Systems Manager 使用者指南中的 [Systems Manager Explorer](#)。
- Systems Manager Change Manager 是一個企業變更管理架構，用於請求、核准、實作和報告應用程式組態和基礎結構的操作變更。如需詳細資訊，請參閱AWS Systems Manager 使用者指南中的 [AWS Systems Manager Change Manager](#)。
- Systems Manager OpsCenter 提供中央位置，讓營運工程師和 IT 專業人員可以檢視、調查和解決與 AWS 資源相關的操作工作項目 (OpsItems)。當您將 OpsCenter 與 Organizations 搭配使用時，其支援在單一工作階段期間從管理帳戶 (Organizations 管理帳戶或 Systems Manager 委派的管理員帳戶) 與另一個帳戶使用 OpsItems。設定完成後，使用者可以執行以下類型的動作：
 - 在另一個帳戶中建立、檢視和更新 OpsItems。
 - 檢視其他帳戶中 OpsItems 中指定的 AWS 資源詳細資訊。
 - 啟動 Systems Manager Automation Runbook，以修復另一個帳戶中 AWS 資源的問題。

如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 [AWS Systems Manager OpsCenter](#)。

- 使用快速設定，以建議的最佳實務快速設定常用 AWS 服務和功能。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 [AWS Systems Manager 快速設定](#)。

當您註冊 Systems Manager 的 AWS Organizations 委派管理員帳戶時，您可以建立、更新、檢視和刪除以組織中組織單位為目標的 Quick Setup 組態管理員。請參閱 AWS Systems Manager 使用者指南中的 [使用委派管理員進行快速設定](#)。

- 當您設定 Systems Manager 的整合式主控台時，您會輸入委派管理員帳戶。此帳戶用於向 Quick Setup、Explorer、CloudFormation StackSets 和 Resource Explorer 註冊 AWS Organizations 委派管理員帳戶。如需進一步了解，請參閱為 [組織設定 Systems Manager 整合式主控台](#) [AWS Systems Manager 使用者指南](#)。

使用下列資訊來協助您 AWS Systems Manager 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Systems Manager 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Systems Manager 和 Organizations 之間的受信任存取，或是從組織中移除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Systems Manager 使用的服務連結角色會將存取權授予下列服務委託人：

- `ssm.amazonaws.com`

使用 Systems Manager 來啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 Organizations 工具啟用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Systems Manager 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Systems Manager 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Systems Manager，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Systems Manager 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal ssm.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 Systems Manager 來停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

Systems Manager 需要與 的信任存取 AWS Organizations，才能同步組織中 AWS 帳戶 的操作資料。如果您停用信任存取，則 Systems Manager 無法同步操作資料，還會報告錯誤。

您只能使用 Organizations 工具停用受信任的存取。

您可以使用 AWS Organizations 主控台、執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS Management Console

使用 Organizations 主控台來受信任停用的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. AWS Systems Manager 在服務清單中選擇。
4. 選擇停用受信任的存取。
5. 在停用信任存取的 AWS Systems Manager對話方塊中，輸入停用進行確認，然後選擇停用信任存取。

- 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Systems Manager，他們現在可以使用 服務 AWS Organizations 主控台或工具 停用該服務。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Systems Manager 為信任的服務。

```
$ aws organizations disable-aws-service-access \
  --service-principal ssm.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 Systems Manager 的委派管理員帳戶

當您將成員帳戶指定為組織的委派管理員時，該帳戶的使用者和角色可以對 Systems Manager 執行管理動作，否則只能由組織管理帳戶中的使用者或角色執行。這可協助您將組織的管理與 Systems Manager 的管理分開。

如果您在整個組織中使用 Change Manager，則會使用委派管理員帳戶。這是 AWS 帳戶 指定為在 Change Manager 中管理變更範本、變更請求、變更執行手冊和核准工作流程的帳戶。委派的帳戶會管理整個組織的變更活動。當您設定組織以配合 Change Manager 使用時，可以指定哪些帳號擔任此角色。它不必是組織的管理帳戶。如果您僅以單一帳戶使用 Change Manager，則不需要委派管理員帳戶。

若要將成員帳戶指定為委派管理員，請查看《AWS Systems Manager 使用者指南》中的以下主題：

- 關於 Explorer 和 OpsCenter，請參閱 [《設定委派管理員》](#)。
- 關於 Systems Manager Change Manager，請參閱 [設定 Change Manager 的組織和委派帳戶](#)。
- 如需快速設定，請參閱 [註冊 Quick Setup 的委派管理員](#)。

停用 Systems Manager 的委派管理員帳戶

若要取消註冊委派管理員，請參閱 AWS Systems Manager 使用者指南中的下列主題：

- 對於 Explorer 和 OpsCenter，請參閱[取消註冊 Explorer 委派管理員](#)。
- 關於 Systems Manager Change Manager，請參閱[設定 Change Manager 的組織和委派帳戶](#)。
- 如需快速設定，請參閱[取消註冊 Quick Setup 的委派管理員](#)。

AWS 使用者通知 和 AWS Organizations

[AWS 使用者通知](#) 是 AWS 通知的中央位置。

與 整合後 AWS Organizations，您可以集中設定和檢視組織中各帳戶的通知。

使用下列資訊來協助您 AWS 使用者通知 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 在您的組織中的 帳戶內 使用者通知 執行支援的操作。

只有在您停用 使用者通知 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- AWSServiceRoleForAWSUserNotifications

如需詳細資訊，請參閱AWS 使用者通知 《使用者指南》中的[使用服務連結角色](#)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。 使用者通知 授予下列服務主體存取權的服務連結角色：

- notifications.amazon.com

使用 使用者通知啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 啟用受信任的存取 AWS 使用者通知。

若要使用 使用者通知 主控台啟用受信任存取，請參閱使用者通知 《使用者指南》中的在 [AWS Organizations 中啟用 AWS 使用者通知](#)。

使用 使用者通知停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您只能使用 啟用受信任的存取 AWS 使用者通知。

若要使用 使用者通知 主控台停用受信任存取，請參閱使用者通知 《使用者指南》中的在 [AWS Organizations 中啟用 AWS 使用者通知](#)。

啟用 的委派管理員帳戶 使用者通知

管理帳戶管理員可以將 使用者通知 管理許可委派給稱為委派管理員的指定成員帳戶。若要將帳戶註冊為私有市集的委派管理員，管理帳戶管理員必須確保啟用信任的存取和服務連結角色，選擇註冊新的管理員，提供 12 位數 AWS 的帳號，然後選擇提交。

管理帳戶和委派的管理員帳戶可以執行 使用者通知 管理任務，例如建立體驗、更新品牌設定、關聯或取消關聯對象、新增或移除產品，以及核准或拒絕待處理的請求。

若要使用 使用者通知 主控台設定委派管理員，請參閱使用者通知 《使用者指南》中的在 [中註冊委派管理員 AWS 使用者通知](#)。

您也可以使用 Organizations RegisterDelegatedAdministrator API 來設定委派管理員。如需詳細資訊，請參閱 Organizations Command Reference (Organizations 命令參考) 中的 [RegisterDelegatedAdministrator](#)。

停用 的委派管理員 使用者通知

只有組織管理帳戶中的管理員可以設定委派管理員 使用者通知。

您可以使用 使用者通知 主控台或 API，或使用 Organizations CLI 或 SDK DeregisterDelegatedAdministrator 操作來移除委派管理員。

若要使用 使用者通知 主控台停用委派管理員 使用者通知 帳戶，請參閱使用者通知 《使用者指南》中的在 [中移除委派管理員 AWS 使用者通知](#)。

標籤政策和 AWS Organizations

標籤政策是 中的一種政策類型 AWS Organizations ，可協助您在組織帳戶中跨資源標準化標籤。如需標籤政策的詳細資訊，請參閱[標籤政策](#)。

使用下列資訊協助您整合標籤政策 AWS Organizations。

服務連結角色所使用的服務委託人

Organizations 使用下列服務委託人與連接至您資源的標籤互動。

- `tagpolicies.tag.amazonaws.com`

啟用標籤政策的受信任存取

您可以在組織中啟用標籤政策或使用 AWS Organizations 主控台來啟用受信任存取。

Important

強烈建議您透過啟用標記政策來啟用受信任存取。這可讓 Organizations 執行必要的設定任務。

您可以在 AWS Organizations 主控台中啟用標籤政策類型，來啟用標籤政策的受信任存取。如需詳細資訊，請參閱[啟用政策類型](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。
3. 在 服務清單中選擇標籤政策。
4. 選擇 Enable trusted access (啟用信任存取)。

5. 在啟用標籤政策的信任存取對話方塊中，輸入啟用以進行確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴標籤政策的管理員，他們現在可以從服務主控台 啟用該服務來使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，將標籤政策啟用為 Organizations 的信任服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal tagpolicies.tag.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用標籤政策來停用受信任存取

您可以在 AWS Organizations 主控台中停用標籤政策類型，以停用標籤政策的信任存取。如需詳細資訊，請參閱[停用政策類型](#)。

AWS Trusted Advisor 和 AWS Organizations

AWS Trusted Advisor 會檢查您的 AWS 環境，並在有機會節省成本、改善系統可用性和效能，或協助消除安全漏洞時提出建議。與 Organizations 整合時，您可以接收組織中所有帳戶的 Trusted Advisor 檢查結果，並下載報告，以檢視您的檢查摘要和任何受影響的資源。

如需詳細資訊，請參閱AWS 支援 使用者指南中的 [AWS Trusted Advisor的 組織檢視](#)。

使用下列資訊來協助您 AWS Trusted Advisor 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。此角色允許 在您的組織中的 帳戶內 Trusted Advisor 執行支援的操作。

只有在您停用 Trusted Advisor 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- `AWSServiceRoleForTrustedAdvisorReporting`

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Trusted Advisor 授予下列服務主體存取權的服務連結角色：

- `reporting.trustedadvisor.amazonaws.com`

使用 Trusted Advisor 啟用受信任的存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您只能使用 啟用受信任的存取 AWS Trusted Advisor。

使用 Trusted Advisor 主控台啟用受信任存取

請參閱AWS 支援 使用者指南中的[啟用組織檢視](#)。

使用 Trusted Advisor 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

停用此功能後，會 Trusted Advisor 停止記錄組織中所有其他帳戶的檢查資訊。您無法檢視或下載現有的報告或建立新的報告。

您可以使用 AWS Trusted Advisor 或 AWS Organizations 工具來停用受信任的存取。

Important

我們強烈建議您盡可能使用 AWS Trusted Advisor 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Trusted Advisor 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Trusted Advisor 提供的工具停用整合時，才能繼續執行這些步驟。

如果您使用 AWS Trusted Advisor 主控台或工具來停用受信任存取，則不需要完成這些步驟。

使用 Trusted Advisor 主控台停用受信任存取

請參閱AWS 支援 使用者指南中的[停用組織檢視](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Trusted Advisor 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 的委派管理員帳戶 Trusted Advisor

當您將成員帳戶指定為組織的委派管理員時，來自指定帳戶的使用者和角色可以為組織中的其他成員帳戶管理 AWS 帳戶 中繼資料。如果您未啟用委派系統管理員帳戶，則只有組織的管理帳戶才能執行這任務。這可協助您將組織的管理與帳戶詳細資訊的管理分開。

最低許可

只有 Organizations 管理帳戶中的使用者或角色可以將成員帳戶設定為 Trusted Advisor 組織中的委派管理員

如需啟用委派管理員帳戶的指示 Trusted Advisor，請參閱支援 《使用者指南》中的[註冊委派管理員](#)。

AWS CLI, AWS API

如果您想要使用 AWS CLI 或其中一個 AWS SDKs 設定委派管理員帳戶，您可以使用下列命令：

- AWS CLI:


```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK：呼叫 Organizations RegisterDelegatedAdministrator 操作和成員帳戶的 ID 號碼，並將帳戶服務主體識別 account.amazonaws.com 為參數。

停用 的委派管理員 Trusted Advisor

您可以使用 Trusted Advisor 主控台，或使用 Organizations CLI 或 SDK

DeregisterDelegatedAdministrator 操作來移除委派管理員。如需有關如何使用 Trusted Advisor 主控台停用委派管理員 Trusted Advisor 帳戶的資訊，請參閱 [支援 使用者指南中的取消註冊委派管理員](#)。

AWS Well-Architected Tool 和 AWS Organizations

AWS Well-Architected Tool 可協助您記錄工作負載的狀態，並將其與最新的 AWS 架構最佳實務進行比較。

AWS Well-Architected Tool 搭配 Organizations 使用 可讓 AWS Well-Architected Tool 和 Organizations 客戶簡化與其組織其他成員共用 AWS Well-Architected Tool 資源的程序。

如需詳細資訊，請參閱 AWS Well-Architected Tool 使用者指南中的 [共用 AWS Well-Architected Tool 資源](#)。

使用下列資訊來協助您 AWS Well-Architected Tool 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下 [服務連結角色](#)。此角色允許 在您的組織中的 帳戶內 AWS WA Tool 執行支援的操作。

只有在您停用 AWS WA Tool 和 Organizations 之間的受信任存取，或者從組織中刪除成員帳戶時，才能移除或修改此角色。

- AWSServiceRoleForWellArchitected

服務角色政策為 AWSWellArchitectedOrganizationsServiceRolePolicy

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。AWS WA Tool 授予下列服務主體存取權的服務連結角色：

- `wellarchitected.amazonaws.com`

使用 AWS WA Tool 啟用受信任的存取

允許更新 AWS WA Tool 以反映組織中的階層變更。

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

您可以使用 AWS Well-Architected Tool 主控台或 AWS Organizations 主控台啟用受信任存取。

Important

我們強烈建議您盡可能使用 AWS Well-Architected Tool 主控台或工具來啟用與 Organizations 的整合。這可讓 AWS Well-Architected Tool 執行其所需的任何組態，例如建立服務所需的資源。只有在您無法使用 AWS Well-Architected Tool 提供的工具啟用整合時，才能繼續執行這些步驟。如需詳細資訊，請參閱[本說明](#)。

如果您使用 AWS Well-Architected Tool 主控台或工具啟用受信任存取，則不需要完成這些步驟。

使用 AWS WA Tool 主控台啟用受信任存取

請參閱 AWS Well-Architected Tool 《使用者指南》中的[共用您的 AWS Well-Architected Tool 資源](#)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在導覽窗格中，選擇服務。

3. AWS Well-Architected Tool 在服務清單中選擇。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用信任存取的 AWS Well-Architected Tool 對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。
6. 如果您只是的管理員 AWS Organizations，請告訴管理員 AWS Well-Architected Tool，他們現在可以從服務主控台 啟用該服務與 搭配使用 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

執行下列命令，以 Organizations 將 啟用 AWS Well-Architected Tool 為信任的服務。

```
$ aws organizations enable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

使用 AWS WA Tool 停用受信任的存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您可以使用 AWS Well-Architected Tool 或 AWS Organizations 工具來停用受信任的存取。

Important

我們強烈建議您盡可能使用 AWS Well-Architected Tool 主控台或工具來停用與 Organizations 的整合。這可讓 AWS Well-Architected Tool 執行其所需的任何清除，例如刪除資源或存取服務不再需要的角色。只有在您無法使用 AWS Well-Architected Tool 提供的工具停用整合成時，才能繼續執行這些步驟。

如果您使用 AWS Well-Architected Tool 主控台或工具來停用受信任存取，則不需要完成這些步驟。

使用 AWS WA Tool 主控台停用受信任存取

請參閱AWS Well-Architected Tool 《使用者指南》中的[共用您的 AWS Well-Architected Tool 資源](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，以 Organizations 將 停用 AWS Well-Architected Tool 為信任的服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

Amazon VPC IP Address Manager (IPAM) 和 AWS Organizations

Amazon VPC IP Address Manager (IPAM) 是一種 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控 AWS 工作負載的 IP 地址。

使用 AWS Organizations 可讓您監控整個組織的 IP 地址用量，並在成員帳戶之間共用 IP 地址集區。

如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的[整合 IPAM 與 AWS Organizations](#)。

使用下列資訊，協助您整合 Amazon VPC IP Address Manager (IPAM) 與 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

使用 IPAM 主控台或使用 IPAM 的 EnableIpamOrganizationAdminAccount API 將 IPAM 與 AWS Organizations 整合時，會在組織的管理帳戶和每個成員帳戶中自動建立下列服務連結角色。

- AWSServiceRoleForIPAM

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[IPAM 的服務連結角色](#)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。IPAM 使用的服務連結角色會授予存取權給下列服務委託人：

- `ipam.amazonaws.com`

使用 IPAM 啟用受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

Note

當您指定 IPAM 的委派管理員時，其會自動啟用組織中 IPAM 的受信任存取。IPAM 需要信任的存取權 AWS Organizations，才能將成員帳戶指定為組織的此服務委派管理員。

您只能使用 Amazon VPC IP 地址管理員 (IPAM) 工具啟用受信任存取。

如果您 AWS Organizations 使用 IPAM 主控台或使用 IPAM `EnableIpamOrganizationAdminAccount` API 整合 IPAM 與 `EnableIpamOrganizationAdminAccount`，則會自動授予 IPAM 受信任的存取權。授予受信任存取會在管理帳戶中和組織內所有成員帳戶中建立服務連結角色 `AWSServiceRoleForIPAM`。IPAM 使用服務連結角色來監控與組織中 EC2 聯網資源相關聯的 CIDR，並將與 IPAM 相關的指標存放在 Amazon CloudWatch 中。如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的[IPAM 的服務連結角色](#)。

如需啟用受信任存取的相關說明，請參閱 Amazon VPC IPAM 使用者指南中的[整合 IPAM 與 AWS Organizations](#)。

Note

您不能使用 AWS Organizations 主控台或 [EnableAWSServiceAccess](#) API 啟用 IPAM 的受信任存取。

使用 IPAM 停用受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

只有 AWS Organizations 管理帳戶中的管理員可以使用 API 停用 IPAM 的 AWS Organizations `disable-aws-service-access` 受信任存取。

如需停用 IPAM 帳戶許可和刪除服務連結角色的詳細資訊，請參閱 Amazon VPC 使用者指南中的 [IPAM 的服務連結角色](#)。

您可以透過執行 Organizations AWS CLI 命令，或呼叫其中一個 AWS SDKs。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來停用受信任服務存取

使用以下 AWS CLI 命令或 API 操作來停用信任的服務存取：

- AWS CLI: [disable-aws-service-access](#)

執行下列命令，將 Amazon VPC IP Address Manager (IPAM) 停用為 Organizations 的信任服務。

```
$ aws organizations disable-aws-service-access \
    --service-principal ipam.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [DisableAWSServiceAccess](#)

啟用 IPAM 的委派管理員帳戶

IPAM 的委派管理員帳戶負責建立 IPAM 和 IP 地址集區、管理和監控組織中 IP 地址的使用情況，並進行跨成員帳戶的 IP 地址集區共用。如需詳細資訊，請參閱 Amazon VPC IPAM 使用者指南中的 [整合 IPAM 與 AWS Organizations](#)。

只有組織管理帳戶中的管理員可以設定 IPAM 的委派管理員。

您可以從 IPAM 主控台或使用 `enable-ipam-organization-admin-account` API 指定委派的管
理員帳戶。如需詳細資訊，請參閱 AWS CLI 命令參考中的 [enable-ipam-organization-admin-account](#)。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 IPAM 的委託管理員。

若要使用 IPAM 主控台設定委派管理員，請參閱《Amazon VPC IPAM 使用者指南》中的[整合 IPAM 與 AWS Organizations](#)。

停用 IPAM 的委派管理員

只有組織管理帳戶中的管理員可以設定 IPAM 的委派管理員。

若要使用 移除委派管理員 AWS CLI，請參閱 AWS CLI 命令參考中的[disable-ipam-organization-admin-account](#)。

若要使用 IPAM 主控台停用委派管理員 IPAM 帳戶，請參閱《Amazon VPC IPAM 使用者指南》中的[整合 IPAM 與 AWS Organizations](#)。

Amazon VPC Reachability Analyzer 和 AWS Organizations

Reachability Analyzer 是一種組態分析工具，可讓您在虛擬私有雲端 (VPC) 中的來源資源和目的地資源之間執行連線測試。

AWS Organizations 搭配 Reachability Analyzer 使用 可讓您追蹤組織中帳戶間的路徑。

如需詳細資訊，請參閱 [Reachability Analyzer 使用者指南中的管理 Reachability Analyzer 中的委派管理員帳戶](#)。

使用下列資訊，協助您將 Reachability Analyzer 與 整合 AWS Organizations。

當您啟用整合時，即會建立服務連結角色。

當您啟用受信任存取時，會在您組織的管理帳戶中自動建立以下[服務連結角色](#)。該角色允許 Reachability Analyzer 在您組織的組織帳戶中執行支援的操作。

只有在您停用 Reachability Analyzer 和 Organizations 之間的受信任存取，或者從組織中移除成員帳戶時，才能刪除或修改此角色。

- `AWSServiceRoleForReachabilityAnalyzer`

如需詳細資訊，請參閱 [Reachability Analyzer user guide](#) (《Reachability Analyzer 使用者指南》) 中的 [Cross-account analyses for Reachability Analyzer](#) (Reachability Analyzer 的跨帳戶分析)。

服務連結角色所使用的服務委託人

上一節中的服務連結角色，只能由依據角色定義的信任關係所授權的服務委託人來假設。Reachability Analyzer 使用的服務連結角色會將存取權授予下列服務主體：

- `reachabilityanalyzer.networkinsights.amazonaws.com`

啟用 Reachability Analyzer 的受信任存取

如需啟用受信任存取所需許可的資訊，請參閱[啟用信任的存取所需的許可](#)。

當您指定 Reachability Analyzer 的委派管理員時，會自動啟用組織中 Reachability Analyzer 的受信任存取。

Reachability Analyzer 需要信任的 存取權 AWS Organizations，才能將成員帳戶指定為組織的此服務委派管理員。

Important

- 您可以使用 Reachability Analyzer 主控台或 Organizations 主控台來啟用受信任存取。但是，我們強烈建議您使用 Reachability Analyzer 主控台或 `EnableMultiAccountAnalysisForAwsOrganization` API 來啟用與 Organizations 的整合。這可讓 Reachability Analyzer 執行其需要的任何組態，例如建立服務所需的資源。
- 授予受信任存取會在管理帳戶中和組織內所有成員帳戶中建立服務連結角色 `AWSServiceRoleForReachabilityAnalyzer`。Reachability Analyzer 使用服務連結角色來允許管理，委派管理員則可以在組織中的任何資源之間執行連線分析。Reachability Analyzer 可拍攝組織中帳戶的網路元素快照，以回答連線查詢。
- 如需詳細資訊，以及有關透過 Reachability Analyzer 啟用受信任存取的指示，請參閱 [Reachability Analyzer user guide](#) (《Reachability Analyzer 使用者指南》) 中的 [Cross-account analyses for Reachability Analyzer](#) (Reachability Analyzer 的跨帳戶分析)。

您可以使用 AWS Organizations 主控台、執行 AWS CLI 命令，或呼叫其中一個 AWS SDKs 中的 API 操作，來啟用受信任存取。

AWS Management Console

使用 Organizations 主控台來啟用受信任的服務存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 ([不建議](#)) 身分登入。
2. 在[服務](#)頁面上，尋找 VPC Reachability Analyzer 列，選擇服務的名稱，然後選擇啟用受信任存取。
3. 在確認對話方塊中，啟用顯示啟用受信任存取選項，在方塊中輸入 **enable**，然後選擇啟用受信任的存取。
4. 如果您只是的管理員 AWS Organizations，請告知 Reachability Analyzer 的管理員，他們現在可以使用其主控台來啟用該服務 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 來啟用受信任服務存取

您可以使用下列 AWS CLI 命令或 API 操作來啟用信任的服務存取：

- AWS CLI: [enable-aws-service-access](#)

您可以執行下列命令來啟用 Reachability Analyzer，作為受信任服務搭配使用 Organizations。

```
$ aws organizations enable-aws-service-access \
    --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
```

此命令成功後就不會產生輸出。

- AWS API : [EnableAWSServiceAccess](#)

停用 Reachability Analyzer 的受信任存取

如需啟用受信任的存取所需許可的資訊，請參閱[停用信任的存取所需的許可](#)。

您可以使用 Reachability Analyzer 主控台 (建議) 或 Organizations 主控台來停用受信任存取。若要使用 Reachability Analyzer 主控台停用受信任存取，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》) 中的 [Cross-account analyses for Reachability Analyzer](#) (Reachability Analyzer 的跨帳戶分析)。

啟用 Reachability Analyzer 的委派管理員帳戶

委派管理員帳戶可以在組織中跨任何資源執行連線分析。如需詳細資訊，請參閱《Reachability Analyzer 使用者指南》中的[整合 Reachability Analyzer 與 AWS Organizations](#)。

只有組織管理帳戶中的管理員可以設定 Reachability Analyzer 的委派管理員。

您可以從 Reachability Analyzer 主控台或使用 RegisterDelegatedAdministrator API 指定委派管理員帳戶。如需詳細資訊，請參閱 Organizations Command Reference (Organizations 命令參考) 中的 [RegisterDelegatedAdministrator](#)。

最低許可

只有 Organizations 管理帳戶中的使用者或角色，才能將成員帳戶設定為組織中 Reachability Analyze 的委派管理員

若要使用 Reachability Analyzer 主控台設定委派管理員，請參閱《Reachability Analyzer 使用者指南》中的[整合 Reachability Analyzer 與 AWS Organizations](#)。

停用 Reachability Analyzer 的委派管理員

只有組織管理帳戶中的管理員可以設定 Reachability Analyzer 的委派管理員。

您可以使用 Reachability Analyzer 主控台或 API，或透過使用 Organizations DeregisterDelegatedAdministrator CLI 或 SDK 操作，移除委派管理員。

若要使用 Reachability Analyzer 主控台停用委派的管理員 Reachability Analyzer 帳戶，請參閱 Reachability Analyzer user guide (《Reachability Analyzer 使用者指南》) 中的 [Cross-account analyses for Reachability Analyzer](#) (Reachability Analyzer 的跨帳戶分析)。

AWS 服務 該 的委派管理員與 Organizations 搭配使用

我們建議您僅將 AWS Organizations 管理帳戶及其使用者和角色用於該帳戶必須執行的任務。我們也建議您將 AWS 資源存放在組織中的其他成員帳戶中，並將其保留在管理帳戶中。這是因為安全性功能 (例如 Organizations 服務控制政策 (SCP)) 不會限制管理帳戶中的使用者或角色。將資源與管理帳戶分開，也可協助您瞭解發票上的費用。

許多與 Organizations AWS 服務整合可讓您減少管理帳戶的用量。這些服務可讓您將一或多個成員帳戶註冊為管理員，以管理服務中使用的所有組織帳戶。這些帳戶稱為該特定服務的委派管理員。

透過將成員帳戶註冊為 AWS 服務的委派管理員，您可以讓該帳戶擁有該服務的某些管理權限，以及 Organizations 唯讀動作的權限。

在您將帳戶註冊為服務的委派管理員之前：

- 確認該服務支援委派管理員。請參閱 [AWS 服務 您可以搭配 使用 AWS Organizations](#) 的表格，瞭解哪些服務支援委派管理員。
- 為該服務啟用受信任存取。

 Note

若要瞭解如何為委派管理員啟用服務，請參閱 [AWS 服務 您可以搭配 使用 AWS Organizations](#) 中的表格，並在該服務的支援委派管理員直欄中，選取瞭解更多連結。

授與委派管理員帳戶的權限

每個服務特定的委派管理員帳戶都有該服務授與的權限。若要瞭解更多，請參閱 [AWS 服務 您可以搭配 使用 AWS Organizations](#) 中的表格，並在該服務的支援委派管理員直欄中，選取瞭解更多連結。

委派管理員帳戶也具有下列唯讀權限：

- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus

- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

這些權限可讓您檢視 (但不能變更) 這些主控台項目：

- 組織結構、所有帳戶與 OU，以及組織政策
- 成員資格
- 所有帳戶和 OU。
- 組織政策

中的安全性 AWS Organizations

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 和 之間的共同責任。[共同責任模型](#) 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 Cloud AWS 服務 AWS 中執行的基礎設施。AWS 也提供您可以安全使用的服務。在 [AWS 合規計畫](#) 中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用的合規計劃 AWS Organizations，請參閱[AWS 服務 合規計劃範圍中的](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Organizations 時套用共同責任模型。下列主題將示範如何設定 Organizations 以達到您的安全和合規目標。您也會了解如何使用其他 AWS 服務 來協助您監控和保護 Organizations 資源。

主題

- [AWS PrivateLink 適用於 AWS Organizations](#)
- [的身分和存取管理 AWS Organizations](#)
- [在 中記錄和監控 AWS Organizations](#)
- [AWS Organizations 的合規驗證](#)
- [中的彈性 AWS Organizations](#)
- [中的基礎設施安全性 AWS Organizations](#)

AWS PrivateLink 適用於 AWS Organizations

使用 AWS PrivateLink for AWS Organizations，您可以從虛擬私有雲端 (VPC) 內存取 AWS Organizations 服務，而不必跨公有網際網路。

Amazon VPC 可讓您在自訂虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需有關 Amazon VPC 的詳細資訊，請參閱 [《Amazon VPC 使用者指南》](#)。

若要將 Amazon VPC 連線到 AWS Organizations，您必須先定義介面 VPC 端點（介面端點）。介面端點由一個或多個彈性網路介面 (ENI) 來表示，這些是在 VPC 的子網路中指派的私有 IP 地址。從 VPC 到 AWS Organizations 介面端點的請求會保留在 Amazon 網路上。

如需介面端點的一般資訊，請參閱《Amazon [VPC 使用者指南](#)》中的使用介面 VPC 端點存取 AWS 服務。

主題

- [的限制和 的限制 AWS PrivateLinkAWS Organizations](#)
- [為 建立 VPC 端點 AWS Organizations](#)
- [為 AWS Organizations建立 VPC 端點政策](#)

的限制和 的限制 AWS PrivateLinkAWS Organizations

VPC 限制適用於 AWS PrivateLink 的 AWS Organizations。如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的使用介面 VPC 端點和配額存取 AWS 服務。 [AWS PrivateLink](#)此外，適用下列限制：

- 僅適用於 us-east-1 區域
- 不支援 Transport Layer Security (TLS) 1.1

為 建立 VPC 端點 AWS Organizations

您可以使用 Amazon VPC 主控台、AWS Command Line Interface (AWS CLI) 或在 VPC 中建立 AWS Organizations 端點 AWS CloudFormation。

如需有關使用 Amazon VPC 主控台或 建立和設定端點的資訊 AWS CLI，請參閱《Amazon [VPC 使用者指南](#)》中的[建立 VPC 端點](#)。如需有關使用 建立和設定端點的資訊 AWS CloudFormation，請參閱AWS CloudFormation 《使用者指南》中的 [AWS::EC2::VPCEndpoint](#) 資源。

當您建立 AWS Organizations 端點時，請使用下列 做為服務名稱：

```
com.amazonaws.us-east-1.organizations
```

如果您在存取時需要 FIPS 140-2 驗證的密碼編譯模組 AWS，請使用下列 AWS Organizations FIPS 服務名稱：

```
com.amazonaws.us-east-1.organizations-fips
```

為 AWS Organizations 建立 VPC 端點政策

您可以將端點政策連接至控制 Organizations 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[使用端點政策控制 VPC 端點的存取](#)。

範例：AWS Organizations 動作的 VPC 端點政策

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "Organizations:DescribeAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

的身分和存取管理 AWS Organizations

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可），以使用 Organizations 資源。IAM 是 AWS 服務您可以免費使用的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)

- [AWS Organizations 如何使用 IAM](#)
- [使用 管理組織的存取許可 AWS Organizations](#)
- [AWS Organizations的身分型政策範例](#)
- [的資源型政策範例 AWS Organizations](#)
- [AWS 的 受管政策 AWS Organizations](#)
- [使用 標籤的屬性型存取控制 AWS Organizations](#)
- [對 AWS Organizations 身分和存取進行故障診斷](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Organizations 中所做的工作。

服務使用者 – 如果您使用 Organizations 服務來執行您的任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 Organizations 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Organizations 中的功能，請參閱 [對 AWS Organizations 身分和存取進行故障診斷](#)。

服務管理員 – 如果您在公司負責 Organizations 資源，您可能可以完整存取 Organizations。您的任務是判斷您的服務使用者應存取哪些 Organizations 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Organizations 搭配使用，請參閱 [AWS Organizations 如何使用 IAM](#)。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Organizations 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Organizations 身分型政策範例，請參閱 [AWS Organizations的身分型政策範例](#)。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 (登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取時，您會間接擔任角色。

視您身分的使用者類型而定，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 登入 《使用者指南》中的[如何登入您的 AWS 帳戶](#)。

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的[適用於 API 請求的 AWS Signature 第 4 版](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的[多重要素驗證](#)和《IAM 使用者指南》中的[IAM 中的 AWS 多重要素驗證](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是，要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務與身分提供者聯合來存取。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、AWS Directory Service、身分中心目錄，或是 AWS 服務使用透過身分來源提供的憑證存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連接並同步到您自己的身分來源中的一組使用者和群組，以用於所有 AWS 帳戶和應用程式。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

[IAM 使用者](#)是 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 [IAM 使用者的使用案例](#)。

IAM 角色

[IAM 角色](#)是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從[使用者切換至 IAM 角色（主控台）](#)。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《[IAM 使用者指南](#)》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源 (而不是使用角色做為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 中的跨帳戶資源存取](#)。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。

- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可權給 AWS 服務](#)。
- 服務連結角色 – 服務連結角色是連結至的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式](#)。

使用政策管理存取權

您可以透過建立政策並將其連接至身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，AWS 當與身分或資源建立關聯時，會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的[JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 iam:GetRole 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、或 API AWS 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的[在受管政策和內嵌政策間選擇](#)。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCPs) – SCPs 是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的

許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs 的詳細資訊，包括支援 RCPs AWS 服務的清單，請參閱 AWS Organizations 《使用者指南》中的[資源控制政策 RCPs](#)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

AWS Organizations 如何使用 IAM

使用 IAM 管理 Organizations 的存取權之前，請先了解可與 Organizations 搭配使用的 IAM 功能。

IAM 功能	組織支援
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
暫時性憑證	否
轉送存取工作階段 (FAS)	是
服務角色	是

IAM 功能	組織支援
服務連結角色	是

若要深入了解 Organizations 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱 [《AWS IAM 使用者指南》中的與 IAM 搭配使用的服務](#)。

Organizations 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱 [《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱 [《IAM 使用者指南》中的 IAM JSON 政策元素參考](#)。

Organizations 的身分型政策範例

若要檢視 Organizations 身分型政策的範例，請參閱 [AWS Organizations 的身分型政策範例](#)。

Organizations 中的資源型政策

支援資源型政策：是

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予主體實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM 中的快帳戶資源存取](#)。

Organizations 服務僅支援一種名為資源型委派政策的資源型政策類型，指定哪些成員帳戶可以對政策執行動作。您可以在政策中新增多個陳述式，以表示成員帳戶的不同許可集。

如需詳細資訊，請參閱[委派管理員 AWS Organizations](#)。

Organizations 中的資源型政策範例

若要檢視 Organizations 資源型政策的範例，請參閱 [資源型政策範例 AWS Organizations](#)、

Organizations 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Organizations 動作的清單，請參閱服務授權參考中的 [定義的動作 AWS Organizations](#)。

Organizations 中的政策動作在動作之前使用下列字首：

```
organizations
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "organizations:action1",  
    "organizations:action2"  
]
```

若要檢視 Organizations 身分型政策的範例，請參閱 [AWS Organizations 的身分型政策範例](#)。

Organizations 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 Organizations 資源類型及其 ARNs 的清單，請參閱服務授權參考中的 [定義的資源 AWS Organizations](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Organizations 定義的動作](#)。

若要檢視 Organizations 身分型政策的範例，請參閱 [AWS Organizations 的身分型政策範例](#)。

Organizations 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，會使用邏輯 OR 操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

若要查看 Organizations 條件索引鍵的清單，請參閱服務授權參考中的 [的條件索引鍵 AWS Organizations](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [定義的動作 AWS Organizations](#)。

若要檢視 Organizations 身分型政策的範例，請參閱 [AWS Organizations 的身分型政策範例](#)。

Organizations ACLs

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 與 Organizations

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 AWS 中，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的 [使用屬性型存取控制 \(ABAC\)](#)。

搭配 Organizations 使用臨時登入資料

支援臨時登入資料：否

當您使用臨時登入資料登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱 [《AWS 服務 IAM 使用者指南》](#) 中的使用 IAM 的。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時登入資料。

當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的[從使用者切換至 IAM 角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱[IAM 中的暫時性安全憑證](#)。

轉送 Organizations 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的策略詳細資訊，請參閱[轉發存取工作階段](#)。

Organizations 的服務角色

支援服務角色：是

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可權給 AWS 服務](#)。

Warning

變更服務角色的許可可能會中斷 Organizations 功能。只有在 Organizations 提供指引時，才能編輯服務角色。

Organizations 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇 Yes (是) 連結，以檢視該服務的服務連結角色文件。

使用 管理組織的存取許可 AWS Organizations

組織中的所有 AWS 資源，包括根、OUs、帳戶和政策，都由 擁有 AWS 帳戶，而建立或存取資源的許可則受許可政策的管理。如果是組織，其管理帳戶擁有所有資源。帳戶管理員可以透過將許可政策連接至 IAM 身分（使用者、群組和角色）來控制對 AWS 資源的存取。

Note

帳戶管理員 (或管理員使用者) 是具有管理員許可的使用者。如需詳細資訊，請參閱《AWS 帳戶管理 參考指南》中的 [IAM 中的安全最佳實務](#)。

當您授予許可時，能夠決定取得許可的對象、這些對象取得的資源許可，以及可對上述資源進行的特定動作。

根據預設，IAM 使用者、群組和角色沒有許可。身為組織的管理帳戶中的管理員，您可以對管理帳戶中的其他 IAM 使用者或角色執行管理任務或委派管理員許可。若要委派許可，您必須將 IAM 許可政策附加到 IAM 使用者、群組或角色。根據預設，使用者不具任何許可；這種情況有時稱為隱含拒絕。政策會將隱含拒絕覆寫為明確允許，其指定使用者可以執行的動作，以及可以對其執行動作的資源。如果將許可授予角色，則組織中其他帳戶的使用者可以擔任該角色。

AWS Organizations 資源和操作

本節討論 AWS Organizations 概念如何對應至其 IAM 同等概念。

資源

在 中 AWS Organizations，您可以控制對下列資源的存取：

- 組成組織階層結構的根和 OU
- 屬於組織成員的帳戶
- 您連接到組織中實體的政策
- 您用來變更組織狀態的交握

這些資源中每一項都擁有一個相關聯的唯一 Amazon Resource Name (ARN)。您會在 IAM 許可政策的 Resource 元素中指定 ARN，藉此控制對資源的存取。如需 中所使用資源 ARN 格式的完整清單 AWS Organizations，請參閱《服務授權參考》中的 [定義的資源類型 AWS Organizations](#)。

作業

AWS 提供一組操作，以使用組織中的資源。它們可讓您執行建立、列出、修改、存取資源的內容、刪除資源等動作。大多數操作都在 IAM 政策的 Action 元素中參考，以控制能使用該操作的對象。如需可在 IAM 政策中用作許可 AWS Organizations 的操作清單，請參閱《服務授權參考》中的[組織定義的動作](#)。

當您在單一許可政策 Statement 中結合 Resource 和 Action 時，您可以控制可使用該特定動作所在的資源。

條件索引鍵

AWS 提供條件索引鍵供您查詢，以更精細地控制特定動作。您可以在 IAM 政策的 Condition 元素中參考這些條件金鑰，以指定必須符合陳述式才能被視為相符的額外情況。

下列條件索引鍵特別適用於 AWS Organizations：

- `aws:PrincipalOrgID` – 簡化在以資源為基礎的政策中指定 Principal 元素。此全球金鑰提供了列出組織中所有 AWS 帳戶的所有帳戶 ID 的替代方法。您可以在 Condition 元素中指定[組織 ID](#)，而不是列出組織成員的所有帳戶。

Note

此全域條件也適用於組織的管理帳戶。

如需詳細資訊，請參閱《IAM 使用者指南PrincipalOrgID》中的[AWS 全域條件內容索引鍵](#)中的說明。

- `aws:PrincipalOrgPaths` – 使用此條件金鑰來比對特定組織根、OU 或其子系的成員。當提出請求的委託人 (根使用者、IAM 使用者或角色) 位於指定的組織路徑時，`aws:PrincipalOrgPaths` 條件金鑰會傳回 true。路徑是 AWS Organizations 實體結構的文字表示。如需路徑的詳細資訊，請參閱《IAM 使用者指南》中的[了解 AWS Organizations 實體路徑](#)。如需使用此條件索引鍵的詳細資訊，請參閱 IAM 使用者指南中的 [aws:PrincipalOrgPaths](#)。

例如，下列條件元素符合相同組織中兩個 OU 之中任一個的成員。

```
"Condition": {
  "ForAnyValue:StringLike": {
    "aws:PrincipalOrgPaths": [
      "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
```

```

        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsdddd/"
    ]
}
}

```

- `organizations:PolicyType` – 您可以使用此條件金鑰，將 Organizations 政策相關 API 操作限制為僅在指定類型的 Organizations 政策上運作。您可以將此條件金鑰套用至任何政策陳述式，其中包含與 Organizations 政策互動的動作。

您可以搭配此條件金鑰使用下列值：

- `SERVICE_CONTROL_POLICY`
- `RESOURCE_CONTROL_POLICY`
- `DECLARATIVE_POLICY_EC2`
- `BACKUP_POLICY`
- `TAG_POLICY`
- `CHATBOT_POLICY`
- `AISERVICES_OPT_OUT_POLICY`

例如，下列範例政策允許使用者執行任何 Organizations 操作。不過，如果使用者執行一個採取政策引數的操作，則只有在指定的政策是標記政策時，才允許此操作。如果使用者指定任何其他類型的政策，則此操作會失敗。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": [ "TAG_POLICY" ]
        }
      }
    }
  ]
}

```

- `organizations:ServicePrincipal` – 如果您使用 [EnableAWSServiceAccess](#) 或 [DisableAWSServiceAccess](#) 操作以啟用或停用 [受信任存取](#) 與其他 AWS 服務。您可以使用 `organizations:ServicePrincipal` 來限制這些操作對核准的服務委託人名稱清單所做的請求。

例如，以下政策允許使用者只在使用 啟用和停用受信任存取 AWS Firewall Manager 時指定 AWS Organizations。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyAWSFirewallIntegration",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
        }
      }
    }
  ]
}
```

如需可在 IAM 政策中用作許可的所有 AWS Organizations 特定條件金鑰清單，請參閱《服務授權參考》中的 [的條件金鑰 AWS Organizations](#)。

了解資源所有權

AWS 帳戶 擁有在帳戶中建立的資源，無論誰建立資源。具體而言，資源擁有者是驗證資源建立請求 AWS 帳戶 的 [委託人實體](#)（即根使用者、IAM 使用者或 IAM 角色）的。對於組織，一律是管理帳戶。您無法呼叫從成員帳戶建立或存取組織資源的大多數操作。下列範例說明其如何運作：

- 如果您使用管理帳戶的根憑證來建立 OU，則您的管理帳戶即為資源的擁有者。（在 中 AWS Organizations，資源是 OU）。

- 如果您在管理帳戶中建立 IAM 使用者，並將建立 OU 的許可授予該使用者，則該使用者可以建立 OU。不過，使用者所屬的管理帳戶會擁有資源。
- 如果您在管理帳戶中建立 IAM 角色，並將建立 OU 的許可授予該角色，則任何可擔任該角色的人都能建立 OU。角色所屬的管理帳戶 (非擔任使用者) 會擁有該 OU 資源。

管理 資源的存取

許可政策描述誰可以存取哪些資源。下一節說明可用來建立許可政策的選項。

Note

本節討論在內容中使用 IAM AWS Organizations。它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參閱 [IAM 使用者指南](#)。如需 IAM 政策語法和說明的相關資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策參考](#)。

連接至 IAM 身分的政策稱為身分識別型政策 (IAM 政策)。連接到資源的政策稱為「資源類型」政策。

主題

- [身分型許可政策 \(IAM 政策\)](#)

身分型許可政策 (IAM 政策)

您可以將政策連接到 IAM 身分，以允許這些身分對 AWS 資源執行操作。例如，您可以執行下列動作：

- 將許可政策連接至您帳戶中的使用者或群組 – 若要授予使用者建立 AWS Organizations 資源的許可，例如[服務控制政策 \(SCP\)](#) 或 OU，您可以將許可政策連接至使用者或使用者所屬的群組。使用者或群組必須位在組織的管理帳戶中。
- 將許可政策連接至角色 (授予跨帳戶許可) – 您可以將以身分為基礎的許可政策連接至 IAM 角色，藉此對組織授予跨帳戶許可。例如，管理帳戶中的管理員可以建立角色，將跨帳戶許可授予成員帳戶中的使用者，如下所示：
 1. 管理帳戶管理員會建立 IAM 角色，並將會授予許可給組織資源的許可政策連接至該角色。
 2. 管理帳戶管理員將信任政策連接至角色，該角色會將成員帳戶 ID 識別為可以擔任角色的 Principal。

3. 然後成員帳戶管理員可以委派許可給成員帳戶中的任何使用者，以擔任該角色。這樣做可讓成員帳戶中的使用者可以在管理帳戶和組織中建立或存取資源。如果您想要授予 AWS 服務擔任角色的許可，則信任政策中的委託人也可以是 AWS 服務委託人。

如需使用 IAM 來委派許可的相關資訊，請參閱《IAM 使用者指南》中的[存取管理](#)。

以下為允許使用者在您的組織中執行 CreateAccount 動作的範例政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt10rgPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:CreateAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

您也可在政策的 Resource 元素中提供部分 ARN，用於指示資源的類型。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreatingAccountsOnResource",
      "Effect": "Allow",
      "Action": "organizations:CreateAccount",
      "Resource": "arn:aws:organizations::*:account/*"
    }
  ]
}
```

您也可以拒絕建立未將特定標籤納入正在建立的帳戶中的帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Sid": "DenyCreatingAccountsOnResourceBasedOnTag",
  "Effect": "Deny",
  "Action": "organizations:CreateAccount",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/key": "value"
    }
  }
}
```

如需使用者、群組、角色和許可的詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM 身分（使用者、使用者群組和角色）](#)。

指定政策元素：Actions、Conditions、Effects 和 Resources

對於每個 AWS Organizations 資源，服務會定義一組 API 操作或動作，以某種方式與該資源互動或操作該資源。若要授予這些操作的許可，AWS Organizations 會定義一組您可以在政策中指定的動作。例如，對於 OU 資源，AWS Organizations 定義如下的動作：

- AttachPolicy 和 DetachPolicy
- CreateOrganizationalUnit 和 DeleteOrganizationalUnit
- ListOrganizationalUnits 和 DescribeOrganizationalUnit

在某些情況下，執行 API 操作可能需要多個動作的許可，並且可能需要多個資源的許可。

以下是您可以在 IAM 許可政策中使用的最基本元素：

- 動作 – 使用此關鍵字，可辨識要允許或拒絕的操作 (動作)。例如，根據指定的 Effect，organizations:CreateAccount 允許或拒絕使用者執行 CreateAccount 操作的 AWS Organizations 許可。如需詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM JSON 政策元素：動作](#)。
- 資源 – 使用此關鍵字指定政策陳述式套用的資源的 ARN。如需詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM JSON 政策元素：資源](#)。

- 條件 – 使用此關鍵字，可指定必須達到才能套用政策陳述式的條件。Condition 通常會指定必須成立政策才會符合的額外情況。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 效果 – 使用此關鍵字，可指定政策陳述式應允許或拒絕對資源執行動作。如果您未明確授予存取 (或允許) 資源，則隱含地拒絕存取。您也可以明確拒絕存取資源，您可能會這樣做，以確保使用者無法對特定資源執行特定動作，即使另有其他政策授予存取。如需詳細資訊，請參閱《[IAM 使用者指南](#)》中的 [IAM JSON 政策元素：效果](#)。
- 委託人 – 在以身分為基礎的政策 (IAM 政策) 中，政策附加到的使用者會自動且隱含成為委託人。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。

若要進一步了解 IAM 政策語法和描述，請參閱《IAM [使用者指南](#)》中的 [IAM JSON 政策參考](#)。

AWS Organizations的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Organizations 資源的許可。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

如需 Organizations 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 [的動作、資源和條件索引鍵 AWS Organizations](#)。

主題

- [政策最佳實務](#)
- [使用 Organizations 主控台](#)
- [允許使用者檢視他們自己的許可](#)
- [提供完整管理員許可給使用者](#)
- [透過動作授予有限的存取](#)
- [授予對特定資源的存取](#)
- [授予對有限服務委託人啟用受信任存取的能力](#)

政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Organizations 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html 中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

使用 Organizations 主控台

若要存取 AWS Organizations 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 Organizations 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用 Organizations 主控台，請將 Organizations [AWSOrganizationsFullAccess](#) 或 [AWSOrganizationsReadOnlyAccess](#) AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的[新增許可到使用者](#)。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

提供完整管理員許可給使用者

您可以建立 IAM 政策，將完整的 AWS Organizations 管理員許可授予組織中的 IAM 使用者。您可以在 IAM 主控台中使用 JSON 政策編輯器來執行此操作。

若要使用 JSON 政策編輯器來建立政策

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在左側的導覽窗格中，選擇 Policies (政策)。

如果這是您第一次選擇 Policies (政策)，將會顯示 Welcome to Managed Policies (歡迎使用受管政策) 頁面。選擇 Get Started (開始使用)。

3. 在頁面頂端，選擇 Create policy (建立政策)。
4. 在政策編輯器中，選擇 JSON 選項。
5. 輸入下列 JSON 政策文件：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "organizations:*",
    "Resource": "*"
  }
}
```

6. 選擇 Next (下一步)。

Note

您可以隨時切換視覺化與 JSON 編輯器選項。不過，如果您進行變更或在視覺化編輯器中選擇下一步，IAM 就可能會調整您的政策結構，以便針對視覺化編輯器進行最佳化。如需詳細資訊，請參閱 IAM 使用者指南中的 [調整政策結構](#)。

7. 在檢視與建立頁面上，為您正在建立的政策輸入政策名稱與描述 (選用)。檢視此政策中定義的許可，來查看您的政策所授予的許可。
8. 選擇 Create policy (建立政策) 儲存您的新政策。

若要進一步了解如何建立 IAM 政策，請參閱 [《IAM 使用者指南》中的建立 IAM 政策](#)。

透過動作授予有限的存取

如果您想要授予有限的許可而非完整的許可，您可以建立一個政策，列出在 IAM 許可政策的 Action 元素中所允許的個別許可。如下列範例所示，您可以使用萬用字元 (*) 字元來授予 Describe* 和 List* 許可，也就是提供存取您的密碼的唯讀存取權：

Note

在服務控制政策 (SCP)，Action 元素中的萬用字元 (*) 字元只能單獨使用或用在字串結尾。它不能出現在字串開頭或中間。因此，在 SCP 中，"servicename:action*" 有效，但 "servicename:*action" 和 "servicename:some*action" 都無效。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "organizations:Describe*",
      "organizations:List*"
    ],
    "Resource": "*"
  }
}
```

如需可在 IAM 政策中指派的所有許可清單，請參閱服務授權參考中的 [AWS Organizations 定義的動作](#)。

授予對特定資源的存取

除了限制存取特定動作，您可以限制對阻止中特定實體的存取。在之前章節範例中的 Resource 元素皆指定萬用字元 («*»), 這表示「該動作可存取的任何資源」。反之，您可以以允許存取的特定實體之 Amazon Resource Name (ARN) 來取代 «*»。

範例：授予單一 OU 的存取許可

下列政策的第一個陳述式允許 IAM 使用者對整個組織的讀取存取，但第二個陳述式允許執行 AWS Organizations 管理動作的使用者只能在單一指定的組織單位 (OU) 中。這不會延伸至任何子項 OU。未授予帳單存取。請注意，這不會授予您 OU AWS 帳戶中的管理存取權。它只授予許可，以對指定 OU 內的帳戶執行 AWS Organizations 操作：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-<organizationalUnitId>"
    }
  ]
}
```

您可以從 AWS Organizations 主控台或呼叫 List* APIs 取得 OU 和組織的 IDs。您將此政策套用至其中的使用者或群組可以執行任何動作 ("organizations:*")，這直接包含在指定 OU 中的任何實體上。OU 依據 Amazon Resource Name (ARN) 識別。

如需各種資源 ARNs 的詳細資訊，請參閱服務授權參考中的 [定義的資源類型 AWS Organizations](#)。

授予對有限服務委託人啟用受信任存取的能力

您可以使用政策陳述式 Condition 元素，以進一步限制政策聲明符合的情況。

範例： 授予對一個指定服務啟用受信任存取的許可

下列陳述式顯示了如何限制只能對您指定的那些服務啟用受信任存取的能力。如果使用者嘗試使用與不同的服務主體呼叫 API AWS IAM Identity Center，則此政策不相符且請求遭拒：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*",
```

```
        "Condition": {
            "StringEquals" : {
                "organizations:ServicePrincipal" : "sso.amazonaws.com"
            }
        }
    ]
}
```

如需各種資源 ARNs 的詳細資訊，請參閱服務授權參考中的 [定義的資源類型 AWS Organizations](#)。

的資源型政策範例 AWS Organizations

下列程式碼範例示範如何使用以資源為基礎的委派政策。如需詳細資訊，請參閱[委派管理員 AWS Organizations](#)。

主題

- [範例：檢視組織、OU、帳戶和政策](#)
- [範例：建立、讀取、更新和刪除政策](#)
- [範例：標籤和取消標籤政策](#)
- [範例：將政策連接至單一 OU 或帳戶](#)
- [範例：用於管理組織備份政策的合併許可](#)

範例：檢視組織、OU、帳戶和政策

在委派政策管理之前，您必須委派導覽組織結構的許可，並查看組織單位 (OU)、帳戶及其附加的政策。

此範例顯示如何將這些許可納入成員帳戶 *AccountId* 的以資源為基礎的委派政策中。

Important

儘管您可以使用此政策委派任何 Organizations 唯讀動作，但建議您只包含範例中所示的最低必要動作的許可。

此委派政策範例授予從 AWS API 或以程式設計方式完成動作所需的許可 AWS CLI。若要使用此委派政策，請將 *AccountId* 的 AWS [預留位置文字](#) 取代為您自己的資訊。然後，依照 [的委派管理員 AWS Organizations](#) 中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

範例：建立、讀取、更新和刪除政策

您可以建立資源型委派政策，允許管理帳戶委派任何政策類型的 create、update、read 和 delete 動作。此範例示範如何將這些服務控制政策的動作委派給成員帳戶 *MemberAccountId*。範例中顯示的兩個資源分別授予客戶受管和 AWS 受管服務控制政策的存取權。

⚠ Important

此政策允許委派管理員對組織中任何帳戶建立的政策執行指定的動作，包括管理帳戶。它不允許委派管理員連接或分離政策，因為它不包含執行 `organizations:AttachPolicy` 和 `organizations:DetachPolicy` 動作所需的許可。

此委派政策範例授予從 AWS API 或 以程式設計方式完成動作所需的許可 AWS CLI。將 *MemberAccountId*、*ManagementAccountId* 和 *OrganizationId* 的預留 AWS 位置文字取代為您自己的資訊。然後，依照 [委派管理員 AWS Organizations](#) 中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "SERVICE_CONTROL_POLICY"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "DelegatingMinimalActionsForSCPs",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::MemberAccountId:root"
    },
    "Action": [
      "organizations:CreatePolicy",
      "organizations:DescribePolicy",
      "organizations:UpdatePolicy",
      "organizations>DeletePolicy"
    ],
    "Resource": [
      "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/  
service_control_policy/*",
      "arn:aws:organizations::aws:policy/service_control_policy/*"
    ]
  }
]
}

```

範例：標籤和取消標籤政策

此範例示範如何建立以資源為基礎的委派政策，允許委派管理員標記或取消標記備份政策。它授予從 AWS API 或 以程式設計方式完成動作所需的許可 AWS CLI。

若要使用此委派政策，請將 AWS *MemberAccountId*、*ManagementAccountId* 和 *OrganizationId* 的預留位置文字取代為您自己的資訊。然後，依照 [委派管理員 AWS Organizations](#) 中的指示操作。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",

```

```

        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "BACKUP_POLICY"
        }
    }
},
{
    "Sid": "DelegatingTaggingBackupPolicies",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
    },
    "Action": [
        "organizations:TagResource",
        "organizations:UntagResource"
    ],
    "Resource": "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
    backup_policy/*"
}
]
}

```

範例：將政策連接至單一 OU 或帳戶

此範例示範如何建立資源型委派政策，允許委派管理員從指定的組織單位 (OU) attach 或指定的帳戶，對或 detach Organizations 政策進行委派。委派這些動作之前，您必須委派許可來導覽組織的結構，並查看其下的帳戶。如需詳細資訊，請參閱[範例：檢視組織、OU、帳戶和政策](#)

⚠ Important

- 雖然此政策允許從指定的 OU 或帳戶連接或分離政策，但它排除子 OUs和子 OUs 下的帳戶。
- 此政策可讓委派管理員對組織中任何帳戶 (包括管理帳戶) 建立的政策執行指定的動作。

此委派政策範例授予從 AWS API 或 以程式設計方式完成動作所需的許可 AWS CLI。若要使用此委派政策，請將 *MemberAccountId*、*ManagementAccountId*、*OrganizationId* 和 *TargetAccountId* 的預留 AWS 位置文字取代為您自己的資訊。然後，依照 [的委派管理員 AWS Organizations](#) 中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
  ],
}
```

```

    "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::MemberAccountId:root"
    },
    "Action": [
      "organizations:AttachPolicy",
      "organizations:DetachPolicy"
    ],
    "Resource": [
      "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/ou-OUId",
      "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/TargetAccountId",
      "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/*"
    ]
  }
}

```

若要將連接和分離政策委派至組織中的任何 OU 或帳戶，請將先前範例中的資源取代為下列資源：

```

"Resource": [
  "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
  "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
  "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/*"
]

```

範例：用於管理組織備份政策的合併許可

此範例顯示如何建立以資源為基礎的委派政策，以允許管理帳戶委派在組織內管理備份政策所需的完整許可，包括 create、read、update 和 delete 動作，以及 attach 和 detach 政策動作。

Important

此政策可讓委派管理員對組織中任何帳戶 (包括管理帳戶) 建立的政策執行指定的動作。

此委派政策範例授予從 AWS API 或 以程式設計方式完成動作所需的許可 AWS CLI。若要使用此委派政策，請以您自己的資訊取代 *MemberAccountId*、*ManagementAccountId*、*OrganizationId* 和 *RootId* 的 AWS [預留位置文字](#)。然後，依照 [委派管理員 AWS Organizations](#) 中的指示操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
```

```

        "organizations:PolicyType": "BACKUP_POLICY"
    }
}
},
{
    "Sid": "DelegatingAllActionsForBackupPolicies",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
    },
    "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
    ],
    "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "BACKUP_POLICY"
        }
    }
}
]
}

```

AWS 的 受管政策 AWS Organizations

本節識別提供給您用於管理組織的受 AWS 管政策。您無法修改或刪除 AWS 受管政策，但您可以視需要將其連接至組織中的實體或將其分離。

AWS Organizations 與 AWS Identity and Access Management (IAM) 搭配使用的 受管政策

IAM 受管政策由 AWS 提供並維護。受管政策提供一般任務的許可，您可透過將受管政策連接至適當的 IAM 使用者或角色物件來指派給使用者。您不需要自行撰寫政策，而且在適當 AWS 更新政策以支援新服務時，您會自動並立即獲得更新的好處。

您可以在 IAM 主控台的 [Policies](#) (政策) 頁面中看到 AWS 受管政策清單。使用 Filter policies (篩選政策) 下拉式清單，以選取 AWS 受管。

您會使用下列受管政策，以將許可授予組織中的使用者和角色。

AWS 受管政策：AWSOrganizationsFullAccess

提供建立和完整管理組織所需的所有許可。

檢視政策：[AWSOrganizationsFullAccess](#)。

AWS 受管政策：AWSOrganizationsReadOnlyAccess

提供組織相關資訊的唯讀存取權。它不允許使用者進行任何變更。

檢視政策：[AWSOrganizationsReadOnlyAccess](#)。

AWS 受管政策：DeclarativePoliciesEC2Report

[AWSServiceRoleForDeclarativePoliciesEC2Report](#) 服務連結角色使用此政策，使其能夠描述成員帳戶的帳戶屬性狀態。

檢視政策：[DeclarativePoliciesEC2Report](#)。

Organizations AWS 受管政策的更新

下表詳細說明自此服務開始追蹤這些變更以來，AWS 受管政策的更新。如需有關此頁面變更的自動提醒，請訂閱 [文件歷史記錄頁面](#) 上的 RSS 摘要。

變更	描述	日期
AWSOrganizationsFullAccess – 已更新，允許透過 Organizations 主控台檢視或修改帳戶名稱所需的帳戶 API 許可。	新增 <code>account:GetAccount Information</code> 動作，以允許檢視組織中任何帳戶之帳戶名稱的存取權，以及 <code>account:PutAccount</code>	2025 年 4 月 22 日

變更	描述	日期
	Name 動作，以允許修改組織中任何帳戶名稱的存取權。	
DeclarativePoliciesEC2Report – 新的受管政策	新增DeclarativePoliciesEC2Report 政策以啟用AWSServiceRoleForDeclarativePoliciesEC2Report 服務連結角色的功能。	2024 年 11 月 22 日
AWSOrganizationsReadOnlyAccess – 已更新，允許檢視根使用者電子郵件地址所需的帳戶 API 許可。	新增 account:GetPrimaryEmail 動作，以允許檢視組織中任何成員帳戶的根使用者電子郵件地址的存取權，以及 account:GetRegionOptStatus 動作，以允許檢視組織中任何成員帳戶已啟用的區域。	2024 年 6 月 6 日
AWSOrganizationsFullAccess – 更新以包含描述政策陳述式的Sid元素。	新增 AWSOrganizationsFullAccess 受管政策的Sid元素。	2024 年 2 月 6 日
AWSOrganizationsReadOnlyAccess – 更新以包含描述政策陳述式的Sid元素。	新增 AWSOrganizationsReadOnlyAccess 受管政策的Sid元素。	2024 年 2 月 6 日
AWSOrganizationsFullAccess – 更新為允許透過 Organizations 主控台啟用或停用 AWS 區域 所需的帳戶 API 許可。	已將 account:ListRegions 、 account:EnableRegion 和 account:DisableRegion 動作新增至政策，以啟用寫入存取權來啟用或停用帳戶的 區域。	2022 年 12 月 22 日
AWSOrganizationsReadOnlyAccess – 已更新，允許 AWS 區域 透過 Organizations 主控台列出所需的帳戶 API 許可。	已將 account:ListRegions 動作新增至政策，以啟用檢視帳戶區域的權限。	2022 年 12 月 22 日

變更	描述	日期
AWSOrganizationsFullAccess – 更新為允許透過 Organizations 主控台新增或編輯帳戶聯絡人所需的帳戶 API 許可。	已將 <code>account:GetContactInformation</code> 和 <code>account:PutContactInformation</code> 動作新增至政策，以啟用寫入存取權來修改帳戶的聯絡人。	2022 年 10 月 21 日
AWSOrganizationsReadOnlyAccess – 更新為允許透過 Organizations 主控台檢視帳戶聯絡人所需的帳戶 API 許可。	已將 <code>account:GetContactInformation</code> 動作新增至政策，以啟用檢視帳戶聯絡人的存取權。	2022 年 10 月 21 日
AWSOrganizationsFullAccess – 更新以允許建立組織。	已將 <code>CreateServiceLinkedRole</code> 許可新增至政策，以啟用建立組織所需的服務連結角色。許可限於建立角色，該角色只能透過 <code>organizations.amazonaws.com</code> 服務使用。	2022 年 8 月 24 日
AWSOrganizationsFullAccess – 更新為允許透過 Organizations 主控台新增、編輯或刪除帳戶替代聯絡人所需的帳戶 API 許可。	已將 <code>account:GetAlternateContact</code> 、 <code>account>DeleteAlternateContact</code> 、 <code>account:PutAlternateContact</code> 動作新增至政策，以啟用寫入存取權來修改帳戶的替代聯絡人。	2022 年 2 月 7 日
AWSOrganizationsReadOnlyAccess – 更新為允許透過 Organizations 主控台檢視帳戶替代聯絡人所需的帳戶 API 許可。	已將 <code>account:GetAlternateContact</code> 動作新增至政策，以啟用檢視帳戶替代聯絡人的存取權。	2022 年 2 月 7 日

AWS 受管授權政策

[授權政策](#)類似於 IAM 許可政策，但是的功能，AWS Organizations 而非 IAM。您可以使用授權政策來集中設定和管理成員帳戶中主體和資源的存取權。

您可以在 Organizations 主控台的 [Policies](#) (政策) 頁面上，查看組織中的政策清單。

政策名稱	描述	ARN
FullAWSAccess	允許存取每個操作。	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess
RCPFullAWSAccess	允許存取每個資源。	arn:aws:organizations::aws:policy/resource_control_policy/p-RCPFullAWSAccess

使用 標籤的屬性型存取控制 AWS Organizations

[屬性型存取控制](#)可讓您使用管理員管理的屬性，例如連接至 AWS 資源和 AWS 身分的[標籤](#)，以控制對這些資源的存取。例如，您可以指定當使用者和資源對特定標籤具有相同的值時，使用者可以存取資源。

AWS Organizations 可標記的資源包括 AWS 帳戶組織的根、組織單位 OUs) 或政策。當您將標籤連接至 Organizations 資源時，您可以使用這些標籤來控制誰可以存取這些資源。您可以新增Condition元素到您的 AWS Identity and Access Management (IAM) 許可政策陳述式，在允許動作之前檢查是否存在特定標籤索引鍵和值，藉此執行此操作。這可讓您建立 IAM 政策，以有效地說明「允許使用者僅管理那些以鍵 X 和值 Y 來標記的 OU」或「允許使用者僅管理那些使用與使用者連接的 Z 標籤鍵具有相同值的鍵 Z 來標記的 OU。」

您可以根據 IAM 政策中不同類型的標籤參考來進行 Condition 測試。

- [檢查連接至請求中指定資源的標籤](#)
- [檢查連接至提出請求之 IAM 使用者或角色的標籤](#)
- [檢查請求中包含作為參數的標籤](#)

如需有關在政策中使用標籤進行存取控制的詳細資訊，請參閱[使用資源標籤來控制對 IAM 使用者和角色的存取](#)。如需 IAM 許可政策的完整語法，請參閱 [IAM JSON 政策參考](#)

檢查連接至請求中指定資源的標籤

當您使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或其中一個 AWS SDKs 提出請求時，您可以指定要使用該請求存取的資源。無論您是嘗試列出指定類型的可用資源、讀

取資源，或者寫入、修改或更新資源，都必須指定要存取的資源作為請求中的參數。這類請求由您連接至使用者和角色的 IAM 許可政策控制。在這些政策中，您可以比較連接至請求資源的標籤，並根據這些標籤的鍵和值選擇允許或拒絕存取。

若要檢查連接至資源的標籤，您可以使用以下字串前面的標籤鍵名稱參考 Condition 元素中的標籤：`aws:ResourceTag/`

例如，下列範例政策允許使用者或角色執行任何 AWS Organizations 操作，除非該資源具有包含鍵 `department` 和值 `security` 的標籤。如果該鍵和值存在，則政策會明確拒絕 `UntagResource` 操作。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "organizations:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/department" : "security"
        }
      }
    }
  ]
}
```

如需如何使用此元素的詳細資訊，請參閱 IAM 使用者指南中的[控制對資源的存取和 aws:ResourceTag](#)。

檢查連接至提出請求之 IAM 使用者或角色的標籤

您可以根據連接至該人員 IAM 使用者或角色的標籤，控制提出請求的人員 (委託人) 可執行的操作。若要執行此操作，請使用 `aws:PrincipalTag/key-name` 條件索引鍵來指定哪些標籤和值必須連接至呼叫的使用者或角色。

以下範例顯示如何僅在以下情況下允許動作：指定的標籤 (cost-center) 在呼叫操作的委託人和操作正在存取的資源上均具有相同的值。在此範例中，呼叫使用者只有在使用與使用者相同的 cost-center 值標記執行個體時，才會開始和停止 Amazon EC2 執行個體。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "ec2:startInstances",
      "ec2:stopInstances"
    ],
    "Resource": "*",
    "Condition": {"StringEquals":
      {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
  }
}
```

如需如何使用此元素的詳細資訊，請參閱 IAM 使用者指南中的[控制對 IAM 委託人的存取和 aws:PrincipalTag](#)。

檢查請求中包含作為參數的標籤

若干操作可讓您指定標籤作為請求的一部分。例如，當您建立資源時，可以指定連接至新資源的標籤。您可以指定 Condition 元素，其使用 aws:TagKeys 以根據請求中是否包含特定標籤鍵或一組鍵，來允許或拒絕操作。此比較運算子不關心標籤包含的值。它只檢查具有指定鍵的標籤是否存在。

若要檢查標籤鍵或標籤鍵清單，請指定具有以下語法的 Condition 元素：

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

您可以使用 [ForAllValues:](#) 以比較運算子為開頭，確保請求中的所有鍵都必須符合政策中指定的其中一個鍵。例如，以下範例政策只有在請求中存在的所有標籤都屬於此政策中三個標籤的子集時，才允許任何 Organizations 操作。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "organizations:*",
    "Resource": "*",
```

```

        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}

```

或者，您可以使用 [ForAnyValue](#)：以比較運算子為開頭，確保請求中的至少其中一個鍵必須符合政策中指定的其中一個鍵。例如，下列政策僅在至少一個指定標籤鍵均存在於請求中時，才會允許任何 Organizations 操作。

```

{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}

```

若干操作可讓您在請求中指定標籤。例如，當您建立資源時，可以指定連接至新資源的標籤。您可以將政策中的標籤鍵/值對與請求隨附的鍵/值對作比較。為此，透過在標籤鍵名稱前面加上以下字串來參考 Condition 元素中的標籤：`aws:RequestTag/key-name`，然後指定必須存在的標籤值。

例如，以下範例政策拒絕使用者或角色建立的任何請求，AWS 帳戶 其中請求遺失 `costcenter` 標籤，或提供該標籤的 值不是 1、2 或 3。

```

{

```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Deny",
    "Action": "organizations:CreateAccount",
    "Resource": "*",
    "Condition": {
      "Null": {
        "aws:RequestTag/costcenter": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "organizations:CreateAccount",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringNotEquals": {
        "aws:RequestTag/costcenter": [
          "1",
          "2",
          "3"
        ]
      }
    }
  }
]
}

```

如需如何使用這些元素的詳細資訊，請參閱 IAM 使用者指南中的 [aws:TagKeys](#) 和 [aws:RequestTag](#)。

對 AWS Organizations 身分和存取進行故障診斷

使用下列資訊來協助您診斷和修正使用 Organizations 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 Organizations 中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的 Organizations 資源](#)

我無權在 Organizations 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 `organizations:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
organizations:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 `organizations:GetWidget` 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，表示您無權執行 `iam:PassRole` 動作，則必須更新您的政策，以允許您將角色傳遞給 Organizations。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM marymajor 使用者嘗試使用主控台在 Organizations 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許以外的人員 AWS 帳戶 存取我的 Organizations 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Organizations 是否支援這些功能，請參閱 [AWS Organizations 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的[在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的[提供存取權給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的[將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 中的跨帳戶資源存取](#)。

在 中記錄和監控 AWS Organizations

最佳實務是應該監控您的組織，以確保所做的變更都會記錄。這可協助您確保可以調查任何非預期的變更，以及復原不需要的變更。AWS Organizations 目前支援兩個 AWS 服務，可讓您監控組織及其內發生的活動。

主題

- [使用 記錄 API AWS CloudTrail 呼叫 AWS Organizations](#)
- [Amazon EventBridge 和 AWS Organizations](#)

使用 記錄 API AWS CloudTrail 呼叫 AWS Organizations

AWS Organizations 已與 整合 AWS CloudTrail，此服務提供使用者、角色或服務在 AWS 中採取動作的記錄 AWS Organizations。CloudTrail 會將 的所有 API 呼叫擷取 AWS Organizations 為事件，包括來自 AWS Organizations 主控台的呼叫，以及來自對 AWS Organizations APIs 的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Organizations。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，您可以判斷提出的請求 AWS Organizations、提出的 IP 地址、提出者、提出的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

Important

您只能 AWS Organizations 在美國東部（維吉尼亞北部）區域檢視 的所有 CloudTrail 資訊。如果您在 CloudTrail 主控台中看不到 AWS Organizations 活動，請使用右上角的選單將主控台

設為美國東部（維吉尼亞北部）。如果您使用 AWS CLI 或 SDK 工具查詢 CloudTrail，請將您的查詢導向美國東部（維吉尼亞北部）端點。

AWS Organizations CloudTrail 中的資訊

建立帳戶 AWS 帳戶時，您的上會啟用 CloudTrail。當活動在 中發生時 AWS Organizations，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html>。

如需您 AWS 帳戶帳戶中正在進行事件的記錄 (包含 AWS Organizations 的事件)，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。當您的 中啟用 CloudTrail 記錄時 AWS 帳戶，對 AWS Organizations 動作發出的 API 呼叫會在 CloudTrail 日誌檔案中追蹤，並在其中寫入其他 AWS 服務記錄。您可以設定其他 AWS 服務來進一步分析 CloudTrail 日誌中收集的事件資料，並對其採取行動。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)

CloudTrail 會記錄所有 AWS Organizations 動作，並記錄在 [AWS Organizations API 參考](#) 中。例如，對 CreateAccount (包括 CreateAccountResult 事件)、ListHandshakesForAccount、CreatePolicy 及 InviteAccountToOrganization 的呼叫，都會在 CloudTrail 日誌檔案中產生項目。

每個日誌項目都會包含產生要求之人員的資訊。日誌記錄中的使用者身分資訊，可協助您判斷下列事項：

- 該請求是否使用根使用者或 IAM 使用者憑證提出
- 提出該請求時，是否使用了特定 [IAM 角色](#) 或 [聯合身分使用者](#) 的暫時安全憑證
- 該請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

了解 AWS Organizations 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

範例日誌項目：CloseAccount

下列範例顯示在呼叫 API 並且關閉帳戶的工作流程在後台開始處理時，所產生範例 CloseAccount 呼叫的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
    "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/my-admin-role",
        "accountId": "111122223333",
        "userName": "my-session-id"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2022-03-18T18:17:06Z"
      }
    }
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccount",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
  "requestParameters": {
    "accountId": "555555555555"
```

```

    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}

```

下列範例顯示關閉帳戶的後台工作流程成功完成後，CloseAccountResult 呼叫的 CloudTrail 日誌項目。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
  }
},

```

```

    "eventCategory": "Management"
  }

```

範例日誌項目：CreateAccount

下列範例顯示在呼叫 API 並且建立帳戶的工作流程在後台開始處理時，產生的範例 CreateAccount 呼叫的 CloudTrail 日誌項目。

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
    "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/my-admin-role",
        "accountId": "111122223333",
        "userName": "my-session-id"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-09-16T21:16:45Z"
      }
    }
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccount",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
  "requestParameters": {
    "tags": [],
    "email": "*****",
    "accountName": "*****"
  },
  "responseElements": {

```

```

    "createAccountStatus": {
      "accountName": "*****",
      "state": "IN_PROGRESS",
      "id": "car-examplecreateaccountrequestid111",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
    }
  },
  "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}

```

下列範例顯示了建立帳戶的後台工作流程成功完成後，CreateAccount 呼叫的 CloudTrail 日誌項目。

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "*****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}

```

```
}
}
```

下列範例顯示了建立帳戶的 CreateAccount 後台工作流程失敗後，產生的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "*****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": "Jun 21, 2018 10:06:27 PM",
      "completedTimestamp": "Jun 21, 2018 10:07:15 PM"
    }
  }
}
```

範例日誌項目：CreateOrganizationalUnit

下列範例顯示了範例 CreateOrganizationalUnit 呼叫的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
```

```

        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}

```

範例日誌項目：InviteAccountToOrganization

下列範例顯示了範例 InviteAccountToOrganization 呼叫的 CloudTrail 日誌項目。

```

{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",

```



```

    "userName": "diego"
  },
  "eventTime": "2017-01-18T21:41:17Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "InviteAccountToOrganization",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
  "requestParameters": {
    "notes": "This is a request for Mary's account to join Diego's organization.",
    "target": {
      "type": "ACCOUNT",
      "id": "111111111111"
    }
  },
  "responseElements": {
    "handshake": {
      "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
      "state": "OPEN",
      "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
      "id": "h-examplehandshakeid111",
      "parties": [
        {
          "type": "ORGANIZATION",
          "id": "o-aa111bb222"
        },
        {
          "type": "ACCOUNT",
          "id": "222222222222"
        }
      ],
      "action": "invite",
      "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
      "resources": [
        {
          "resources": [
            {
              "type": "MASTER_EMAIL",
              "value": "diego@example.com"
            },
            {
              "type": "MASTER_NAME",

```

```

        "value": "Management account for organization"
      },
      {
        "type": "ORGANIZATION_FEATURE_SET",
        "value": "ALL"
      }
    ],
    "type": "ORGANIZATION",
    "value": "o-aa111bb222"
  },
  {
    "type": "ACCOUNT",
    "value": "222222222222"
  },
  {
    "type": "NOTES",
    "value": "This is a request for Mary's account to join Diego's
organization."
  }
]
}
},
"requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}

```

範例日誌項目：AttachPolicy

下列範例顯示了範例 AttachPolicy 呼叫的 CloudTrail 日誌項目。回應表示呼叫失敗，因為請求的政策類型未於嘗試連接請求的根帳戶中啟用。

```

{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/diego",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "diego"
  },

```

```
"eventTime": "2017-01-18T21:42:44Z",
"eventSource": "organizations.amazonaws.com",
"eventName": "AttachPolicy",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
"errorCode": "PolicyTypeNotEnabledException",
"errorMessage": "The given policy type ServiceControlPolicy is not enabled on the current view",
"requestParameters": {
  "policyId": "p-examplepolicyid111",
  "targetId": "ou-examplerootid111-exampleouid111"
},
"responseElements": null,
"requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}
```

Amazon EventBridge 和 AWS Organizations

AWS Organizations 可以使用先前為 Amazon CloudWatch Events 的 Amazon EventBridge，在組織中發生管理員指定的動作時引發事件。例如，由於這類動作的靈敏度，多數管理員會想要在每次有人在組織中建立新帳戶，或在成員帳戶的管理員嘗試離開組織時收到警告。您可以設定尋找這些動作的 EventBridge 規則，然後將產生的事件傳送到管理員定義的目標。目標可以是傳送電子郵件或文字訊息給其訂閱者的 Amazon SNS 主題。您也可以建立 AWS Lambda 函式，記錄動作的詳細資訊以供日後審閱。

如需示範如何啟用 EventBridge 來監控組織內關鍵活動的教學資訊，請參閱[教學課程：使用 Amazon EventBridge 監控您組織的重要變更](#)。

Important

目前，AWS Organizations 僅託管在美國東部（維吉尼亞北部）區域（即使它可在全球使用）。若要執行本教學課程中的步驟，您必須設定 AWS Management Console 以使用該區域。

若要進一步了解 EventBridge (包括如何配置及啟用 CloudWatch Events)，請參閱 [Amazon EventBridge 使用者指南](#)。

AWS Organizations的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[在 中下載報告 AWS Artifact](#)。

您在使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- [安全合規與治理](#) - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- [HIPAA 合格服務參考](#) - 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- [AWS 合規資源](#) - 此工作手冊和指南的集合可能適用於您的產業和位置。
- [AWS 客戶合規指南](#) - 透過合規的角度了解共同責任模型。本指南摘要說明保護 的最佳實務，AWS 服務 並將指南映射到跨多個架構的安全控制（包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)）。
- AWS Config 開發人員指南中的[使用規則評估資源](#) - AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) - 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「[Security Hub 控制參考](#)」。
- [Amazon GuardDuty](#) - 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- [AWS Audit Manager](#) - 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

中的彈性 AWS Organizations

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 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠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、容錯能力和擴充能力，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](#)。

中的基礎設施安全性 AWS Organizations

作為受管服務，AWS Organizations 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Organizations。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過[AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-2 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

故障診斷 AWS Organizations

如果您在使用 時遇到問題 AWS Organizations，請參閱本節中的主題。

疑難排解一般問題

使用此處的資訊來協助您診斷和修正使用 時可能遇到的拒絕存取或其他常見問題 AWS Organizations。

主題

- [向 提出請求時，我會收到「存取遭拒」訊息 AWS Organizations](#)
- [當我使用臨時安全憑證來發出請求時，出現「存取遭拒」訊息](#)
- [嘗試以成員帳戶身分離開組織或以管理帳戶身分移除成員帳戶時遇到「存取遭拒」訊息](#)
- [當我試著新增帳戶到我的組織時，出現「超過配額」訊息](#)
- [我在新增或移除帳戶時遇到「此操作需要一段等待時間」訊息](#)
- [嘗試新增帳戶到我的組織時遇到「組織仍在初始化」訊息](#)
- [當我嘗試邀請帳戶加入我的組織時，收到「邀請已停用」訊息。](#)
- [我所做的變更不一定都會立即顯示](#)
- [當我嘗試存取已屬於組織的帳戶時，會收到「完成註冊」訊息](#)

向 提出請求時，我會收到「存取遭拒」訊息 AWS Organizations

- 確定您擁有許可來叫用所請求的動作和資源。管理員必須將 IAM 政策連接到您的使用者、群組或角色，以授予許可。如果授予這些許可的政策內容中包含了任何條件，例如時刻或 IP 地址的限制，則當您傳送請求時，也必須滿足這些要求。關於檢視或修改使用者、群組或角色的政策方面的相關資訊，請參閱《IAM 使用者指南》中的[政策的使用](#)。
- 如果您是手動簽署 API 請求 (而未使用 [AWS SDK](#))，請確認您已正確地[簽署請求](#)。

當我使用臨時安全憑證來發出請求時，出現「存取遭拒」訊息

- 確認您用來發出請求的 使用者或角色，擁有正確的許可。暫時安全登入資料的許可衍生自 使用者或角色，因此許可僅限於授予 使用者或角色的範圍。關於臨時安全憑證許可的決定方式，詳細資訊請參閱 IAM 使用者指南中的[控管臨時安全憑證的許可](#)。

- 確認您的請求正確簽署且請求的格式也正確。如需詳細資訊，請參閱 IAM 使用者指南中所選 SDK 的 [工具組](#) 文件 [或使用暫時安全登入資料來請求存取 AWS 資源](#)。
- 確認您的臨時安全憑證並未過期。如需詳細資訊，請參閱 IAM 使用者指南中的 [請求臨時安全憑證](#)。

嘗試以成員帳戶身分離開組織或以管理帳戶身分移除成員帳戶時遇到「存取遭拒」訊息

- 只有在您啟用 IAM 使用者存取成員帳戶中的帳單時，才可以移除成員帳戶。如需詳細資訊，請參閱 AWS Billing 使用者指南中的 [啟用帳單和成本管理主控台的存取權](#)。
- 只有在帳戶具有讓它以獨立帳戶形式運作所需的資訊時，您才能從組織移除帳戶。當您使用 AWS Organizations 主控台、API 或 AWS CLI 命令在組織中建立帳戶時，不會自動收集該資訊。對於您要獨立建立的帳戶，您必須接受 AWS 客戶協議、選擇支援計畫、提供和驗證所需的聯絡資訊，並提供目前的付款方式。AWS 會使用付款方式來收取帳戶未連接到組織時發生的任何計費（非 AWS 免費方案）AWS 活動的費用。如需詳細資訊，請參閱 [使用從成員帳戶離開組織 AWS Organizations](#)。

當我試著新增帳戶到我的組織時，出現「超過配額」訊息

組織中可以擁有的帳戶數量有上限。即使帳戶已刪除或關閉，仍會計入此配額。

加入的邀請會計入組織中的帳戶數量上限。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會退回計數。

- 關閉或刪除之前 AWS 帳戶，[請從組織中移除它](#)，使其不會繼續計入您的配額。
- 如需有關如何請求增加配額的資訊，請參閱 [最大值和最小值](#)。

我在新增或移除帳戶時遇到「此操作需要一段等待時間」訊息

由於帳戶配額，某些動作需要等待期間。例如，您無法立即移除新建立的帳戶。請在幾天後再嘗試該動作。

如需新增帳戶的問題，請參閱配額 [預設帳戶數量上限](#)。如需移除帳戶的問題，請參閱 [您在 30 天內可以關閉的帳戶配額](#)。

嘗試新增帳戶到我的組織時遇到「組織仍在初始化」訊息

如果您遇到此錯誤，而且在您建立組織後已超過一小時，請聯絡 [AWS 支援](#)。

當我嘗試邀請帳戶加入我的組織時，收到「邀請已停用」訊息。

當[啟用您組織中的所有功能](#)時，就會發生這種情況。此操作可能需要一些時間，並且需要所有成員帳戶有所回應。操作完成之前，您無法邀請新帳戶加入組織。

我所做的變更不一定都會立即顯示

為供全球各地資料中心的電腦存取服務，AWS Organizations 採用稱為[最終一致性](#)的分散式運算模式。您在 中所做的任何變更 AWS Organizations，都需要時間才能從所有可能的端點中顯示。從伺服器到伺服器或從複寫區域到複寫區域傳送資料所花費的時間，會產生一些延遲。AWS Organizations 也會使用快取來改善效能，但在某些情況下，這可能會增加時間。直到先前快取的資料逾時後，才能看到變更。

在設計您的全球應用程式時，請將這些可能的延遲納入考量，並確保即使在某地點所進行的變更不會立即顯示於其他位置時，這些應用程式也能如預期運作。

如需其他 如何受到此 AWS 服務 影響的詳細資訊，請參閱下列資源：

- Amazon Redshift 資料庫開發人員指南中的[管理資料一致性](#)
- Amazon Simple Storage Service 使用者指南中的 [Amazon S3 資料一致性模式](#)
- AWS 大數據部落格中的[將 Amazon S3 和 Amazon Elastic MapReduce 用於 ETL 工作流程時確保一致性](#)
- Amazon EC2 API 參考中的 [EC2 最終一致性](#)

當我嘗試存取已屬於組織的帳戶時，會收到「完成註冊」訊息

- 成員帳戶最多可能需要 48 小時才能繼承管理帳戶的帳單詳細資訊。
- 如果問題在 48 小時後仍存在，您可以向帳戶和帳單支援團隊開立支援案例。如需詳細資訊，請參閱[建立支援案例](#)。

提出 HTTP 查詢請求以呼叫 API

本節包含有關使用查詢 API 的一般資訊 AWS Organizations。如需 API 操作和錯誤的詳細資訊，請參閱 [AWS Organizations API 參考](#)。

Note

您可以使用其中一個 AWS SDKs，而不是直接呼叫 AWS Organizations 查詢 API。AWS SDKs 包含各種程式設計語言和平台 (Java、Ruby、.NET、iOS、Android 等) 的程式庫和範例程式碼。SDKs 提供便捷的方式，以建立 AWS Organizations 和 的程式設計存取 AWS。例如，開發套件會負責的工作諸如以密碼演算法簽署請求、管理錯誤以及自動重試請求。如需 AWS SDKs 的相關資訊，包括如何下載和安裝，請參閱 [適用於 Amazon Web Services 的工具](#)。

的查詢 API AWS Organizations 可讓您呼叫服務動作。查詢 API 請求是 HTTPS 請求，其中必須包含 Action 參數，以指出要執行的操作。AWS Organizations 支援所有操作的 GET 和 POST 請求。也就是說，API 不會要求您在某些動作上使用 GET，在其他動作上使用 POST。不過，GET 請求受限於 URL 的限制大小。此限制取決於瀏覽器，但一般限制為 2048 個位元組。因此，對於需要較大流量的查詢 API 請求，必須使用 POST 請求。

回應為 XML 文件。如需回應的詳細資訊，請參閱 [AWS Organizations API 參考](#) 中的個別動作頁面。

主題

- [端點](#)
- [必要的 HTTPS](#)
- [簽署 AWS Organizations API 請求](#)

端點

AWS Organizations 有一個託管在美國東部（維吉尼亞北部）區域的單一全域 API 端點。

如需所有服務的 AWS 端點和區域的詳細資訊，請參閱 [區域端點](#) AWS 一般參考。

必要的 HTTPS

由於查詢 API 會傳回安全憑證等敏感資訊，必須使用 HTTPS 加密所有 API 請求。

簽署 AWS Organizations API 請求

請求必須使用存取金鑰 ID 和私密存取金鑰簽署。強烈建議您不要將 AWS 帳戶根使用者 登入資料用於的日常作業 AWS Organizations。您可以使用使用者或角色的憑證。

若要簽署 API 請求，您必須使用 AWS Signature 第 4 版。如需使用 Signature 第 4 版的相關資訊，請參閱《IAM 使用者指南》中的[簽署 AWS API 請求](#)。

AWS Organizations 不支援舊版，例如 Signature 第 2 版。

如需詳細資訊，請參閱下列內容：

- [AWS 安全登入](#) 資料 – 提供您可以用來存取的登入資料類型的一般資訊 AWS。
- [IAM 中的安全最佳實務](#) – 提供使用 IAM 服務的建議，以協助保護您的 AWS 資源，包括 中的資源 AWS Organizations。
- [IAM 暫時性安全憑證](#) – 描述如何建立和使用暫時性安全憑證。

使用 AWS SDKs 的組織程式碼範例

下列程式碼範例示範如何使用 Organizations 搭配 AWS 軟體開發套件 (SDK)。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境中查看內容中的動作。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- [使用 AWS SDKs 的組織基本範例](#)
 - [使用 AWS SDKs 的組織動作](#)
 - [AttachPolicy 搭配 AWS SDK 或 CLI 使用](#)
 - [CreateAccount 搭配 AWS SDK 或 CLI 使用](#)
 - [CreateOrganization 搭配 AWS SDK 或 CLI 使用](#)
 - [CreateOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
 - [CreatePolicy 搭配 AWS SDK 或 CLI 使用](#)
 - [DeleteOrganization 搭配 AWS SDK 或 CLI 使用](#)
 - [DeleteOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
 - [DeletePolicy 搭配 AWS SDK 或 CLI 使用](#)
 - [DescribePolicy 搭配 AWS SDK 或 CLI 使用](#)
 - [DetachPolicy 搭配 AWS SDK 或 CLI 使用](#)
 - [ListAccounts 搭配 AWS SDK 或 CLI 使用](#)
 - [ListOrganizationalUnitsForParent 搭配 AWS SDK 或 CLI 使用](#)
 - [ListPolicies 搭配 AWS SDK 或 CLI 使用](#)

使用 AWS SDKs 的組織基本範例

下列程式碼範例示範如何 AWS Organizations 搭配 AWS SDKs 使用 的基本概念。

範例

- [使用 AWS SDKs 的組織動作](#)
 - [AttachPolicy 搭配 AWS SDK 或 CLI 使用](#)

- [CreateAccount 搭配 AWS SDK 或 CLI 使用](#)
- [CreateOrganization 搭配 AWS SDK 或 CLI 使用](#)
- [CreateOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
- [CreatePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DeleteOrganization 搭配 AWS SDK 或 CLI 使用](#)
- [DeleteOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
- [DeletePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DescribePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DetachPolicy 搭配 AWS SDK 或 CLI 使用](#)
- [ListAccounts 搭配 AWS SDK 或 CLI 使用](#)
- [ListOrganizationalUnitsForParent 搭配 AWS SDK 或 CLI 使用](#)
- [ListPolicies 搭配 AWS SDK 或 CLI 使用](#)

使用 AWS SDKs 的組織動作

下列程式碼範例示範如何使用 AWS SDKs 動作。每個範例均包含 GitHub 的連結，您可以在連結中找到設定和執行程式碼的相關說明。

下列範例僅包含最常使用的動作。如需完整清單，請參閱《[AWS Organizations API 參考](#)》。

範例

- [AttachPolicy 搭配 AWS SDK 或 CLI 使用](#)
- [CreateAccount 搭配 AWS SDK 或 CLI 使用](#)
- [CreateOrganization 搭配 AWS SDK 或 CLI 使用](#)
- [CreateOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
- [CreatePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DeleteOrganization 搭配 AWS SDK 或 CLI 使用](#)
- [DeleteOrganizationalUnit 搭配 AWS SDK 或 CLI 使用](#)
- [DeletePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DescribePolicy 搭配 AWS SDK 或 CLI 使用](#)
- [DetachPolicy 搭配 AWS SDK 或 CLI 使用](#)
- [ListAccounts 搭配 AWS SDK 或 CLI 使用](#)

- [ListOrganizationalUnitsForParent 搭配 AWS SDK 或 CLI 使用](#)
- [ListPolicies 搭配 AWS SDK 或 CLI 使用](#)

AttachPolicy 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 AttachPolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
```

```
        PolicyId = policyId,
        TargetId = targetId,
    };

    var response = await client.AttachPolicyAsync(request);

    if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
    {
        Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
    }
    else
    {
        Console.WriteLine("Was not successful in attaching the policy.");
    }
}
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [AttachPolicy](#)。

CLI

AWS CLI

將政策連接至根、OU 或帳戶

範例 1

下列範例示範如何將服務控制政策 (SCP) 連接至 OU：

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id ou-examplerootid111-exampleouid111
```

範例 2

下列範例示範如何將服務控制政策直接連接至 帳戶：

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
```

```
--target-id 333333333333
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [AttachPolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
    or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API 參考中的 [AttachPolicy](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

CreateAccount 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 CreateAccount。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;
```



```
        Console.WriteLine($"The status of {status.AccountName} is  
{status.State}.");  
    }  
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [CreateAccount](#)。

CLI

AWS CLI

建立自動成為組織一部分的成員帳戶

下列範例示範如何在 組織中建立成員帳戶。成員帳戶是以生產帳戶名稱和 `susan@example.com` 的電子郵件地址來設定。Organizations 會使用 `OrganizationAccountAccessRole` 的預設名稱自動建立 IAM 角色，因為未指定 `roleName` 參數。此外，由於未指定 `IamUserAccessToBilling` 參數，因此允許具有足夠存取帳戶帳單資料許可的 IAM 使用者或角色的設定會設定為預設值 `ALLOW`。組織會自動傳送「歡迎 AWS」電子郵件給 Susan：

```
aws organizations create-account --email susan@example.com --account-  
name "Production Account"
```

輸出包含一個請求物件，顯示狀態現在為 `IN_PROGRESS`：

```
{  
    "CreateAccountStatus": {  
        "State": "IN_PROGRESS",  
        "Id": "car-examplecreateaccountrequestid111"  
    }  
}
```

您稍後可以藉由提供 `Id` 回應值給 `describe-create-account-status` 命令做為 `create-account-request-id` 參數的值，來查詢請求的目前狀態。

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的在您的組織中建立 AWS 帳戶。

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [CreateAccount](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

CreateOrganization 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 CreateOrganization。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
    {
```

```
        FeatureSet = "ALL",
    });

    Organization newOrg = response.Organization;

    Console.WriteLine($"Organization: {newOrg.Id} Main Account:
{newOrg.MasterAccountId}");
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [CreateOrganization](#)。

CLI

AWS CLI

範例 1：建立新組織

Bill 想要使用來自帳戶 111111111111 的登入資料來建立組織。下列範例顯示帳戶成為新組織中的主要帳戶。由於他未指定功能集，因此新組織會預設為啟用的所有功能，且服務控制政策會在根上啟用。

```
aws organizations create-organization
```

輸出包含組織物件，其中包含新組織的詳細資訊：

```
{
  "Organization": {
    "AvailablePolicyTypes": [
      {
        "Status": "ENABLED",
        "Type": "SERVICE_CONTROL_POLICY"
      }
    ],
    "MasterAccountId": "111111111111",
    "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
    "MasterAccountEmail": "bill@example.com",
    "FeatureSet": "ALL",
```

```
        "Id": "o-exampleorgid",
        "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
    }
}
```

範例 2：建立僅啟用合併帳單功能的新組織

下列範例會建立僅支援合併帳單功能的組織：

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

輸出包含組織物件，其中包含新組織的詳細資訊：

```
{
  "Organization": {
    "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
    "AvailablePolicyTypes": [],
    "Id": "o-exampleorgid",
    "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
    "MasterAccountEmail": "bill@example.com",
    "MasterAccountId": "111111111111",
    "FeatureSet": "CONSOLIDATED_BILLING"
  }
}
```

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的建立組織。

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [CreateOrganization](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

CreateOrganizationalUnit 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 CreateOrganizationalUnit。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```

        Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
        Console.WriteLine($"Organizational unit {orgUnitName} Details");
        Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
    }
    else
    {
        Console.WriteLine("Could not create new organizational unit.");
    }
}
}

```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [CreateOrganizationalUnit](#)。

CLI

AWS CLI

在根或父 OU 中建立 OU

下列範例示範如何建立名為 AccountingOU 的 OU：

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

輸出包含一個 organizationalUnit 物件，其中包含新 OU 的詳細資訊：

```

{
    "OrganizationalUnit": {
        "Id": "ou-examplerootid111-exampleouid111",
        "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
        "Name": "AccountingOU"
    }
}

```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [CreateOrganizationalUnit](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

CreatePolicy 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 CreatePolicy。

.NET

適用於 .NET 的 SDK

 Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Creates a new AWS Organizations Policy.
/// </summary>
public class CreatePolicy
{
    /// <summary>
    /// Initializes the AWS Organizations client object, uses it to
    /// create a new Organizations Policy, and then displays information
    /// about the newly created Policy.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyContent = "{" +
            "  \"Version\": \"2012-10-17\", \" +
            "  \"Statement\" : [{\" +
            "    \"Action\" : [\"s3:*\"], \" +
            "    \"Effect\" : \"Allow\", \" +
            "    \"Resource\" : \"*\" \" +
            "  }]" +
```

```

        "});

        try
        {
            var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
            {
                Content = policyContent,
                Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                Name = "AllowAllS3Actions",
                Type = "SERVICE_CONTROL_POLICY",
            });

            Policy policy = response.Policy;
            Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
}

```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API Reference 中的 [CreatePolicy](#)。

CLI

AWS CLI

範例 1：使用 JSON 政策的文字來源檔案建立政策

下列範例示範如何建立名為 的服務控制政策 (SCP)AllowAllS3Actions。政策內容是從本機電腦上名為 的檔案取得policy.json。

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
delegation of all S3 actions"
```


輸出包含政策物件，其中包含新政策的詳細資訊：

```
{
  "Policy": {
    "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}\",
    "PolicySummary": {
      "Arn": "arn:aws:organizations::o-exampleorgid:policy/service_control_policy/p-examplepolicyid111",
      "Description": "Allows delegation of all S3 actions",
      "Name": "AllowAllS3Actions",
      "Type": "SERVICE_CONTROL_POLICY"
    }
  }
}
```

範例 2：使用 JSON 政策做為參數來建立政策

下列範例示範如何建立相同的 SCP，這次在參數中將政策內容內嵌為 JSON 字串。字串必須在雙引號之前以反斜線逸出，以確保它們在參數中被視為常值，而參數本身被雙引號包圍：

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}\" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

如需在組織中建立和使用政策的詳細資訊，請參閱《AWS Organizations 使用者指南》中的管理組織政策。

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [CreatePolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
    before
                    it is sent to AWS. The specific format depends on the policy
    type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API Reference 中的 [CreatePolicy](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

DeleteOrganization 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 DeleteOrganization。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine("Successfully deleted organization.");
        }
        else
        {
            Console.WriteLine("Could not delete organization.");
        }
    }
}
```

```
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [DeleteOrganization](#)。

CLI

AWS CLI

刪除組織

下列範例示範如何刪除組織。若要執行此操作，您必須是組織中主要帳戶的管理員。此範例假設您先前已從組織移除所有成員帳戶、OUs 和政策：

```
aws organizations delete-organization
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [DeleteOrganization](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

DeleteOrganizationalUnit 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 DeleteOrganizationalUnit。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
using System;  
using System.Threading.Tasks;  
using Amazon.Organizations;
```

```
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-000000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [DeleteOrganizationalUnit](#)。

CLI

AWS CLI

刪除 OU

下列範例顯示如何刪除 OU。此範例假設您先前已從 OUs 移除所有帳戶和其他 OU：

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [DeleteOrganizationalUnit](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

DeletePolicy 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 DeletePolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
```

```
/// <summary>
/// Initializes the Organizations client object and then uses it to
/// delete the policy with the specified policyId.
/// </summary>
public static async Task Main()
{
    // Create the client object using the default account.
    IAmazonOrganizations client = new AmazonOrganizationsClient();

    var policyId = "p-000000000";

    var request = new DeletePolicyRequest
    {
        PolicyId = policyId,
    };

    var response = await client.DeletePolicyAsync(request);

    if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
    {
        Console.WriteLine($"Successfully deleted Policy: {policyId}.");
    }
    else
    {
        Console.WriteLine($"Could not delete Policy: {policyId}.");
    }
}
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API Reference 中的 [DeletePolicy](#)。

CLI

AWS CLI

刪除政策

下列範例示範如何從組織刪除政策。此範例假設您先前已從所有實體分離政策：

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [DeletePolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API Reference 中的 [DeletePolicy](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

DescribePolicy 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 DescribePolicy。

CLI

AWS CLI

取得政策的相關資訊

下列範例示範如何請求政策的相關資訊：

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

輸出包含政策物件，其中包含政策的詳細資訊：

```
{
  "Policy": {
    "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*\"\n    }\n  ]\n}",
    "PolicySummary": {
      "Arn": "arn:aws:organizations::111111111111:policy/o-exampleorgid/service_control_policy/p-examplepolicyid111",
      "Type": "SERVICE_CONTROL_POLICY",
      "Id": "p-examplepolicyid111",
      "AwsManaged": false,
      "Name": "AllowAllS3Actions",
      "Description": "Enables admins to delegate S3 permissions"
    }
  }
}
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [DescribePolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API 參考中的 [DescribePolicy](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

DetachPolicy 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 DetachPolicy。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
using System;
```

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

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.DetachPolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
        }
        else
        {
            Console.WriteLine("Could not detach the policy.");
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [DetachPolicy](#)。

CLI

AWS CLI

從根、OU 或帳戶分離政策

下列範例示範如何從 OU 分離政策：

```
aws organizations detach-policy --target-id ou-examplerootid111-exampleouid111
--policy-id p-examplepolicyid111
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [DetachPolicy](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
    attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
```

```
raise
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API 參考中的 [DetachPolicy](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

ListAccounts 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 ListAccounts。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
    /// Creates the Organizations client and then calls its
    /// ListAccountsAsync method.
    /// </summary>
    public static async Task Main()
    {

```

```
// Create the client object using the default account.
IAmazonOrganizations client = new AmazonOrganizationsClient();

var request = new ListAccountsRequest
{
    MaxResults = 5,
};

var response = new ListAccountsResponse();
try
{
    do
    {
        response = await client.ListAccountsAsync(request);
        response.Accounts.ForEach(a => DisplayAccounts(a));
        if (response.NextToken is not null)
        {
            request.NextToken = response.NextToken;
        }
    }
    while (response.NextToken is not null);
}
catch (AWSOrganizationsNotInUseException ex)
{
    Console.WriteLine(ex.Message);
}

/// <summary>
/// Displays information about an Organizations account.
/// </summary>
/// <param name="account">An Organizations account for which to display
/// information on the console.</param>
private static void DisplayAccounts(Account account)
{
    string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

    Console.WriteLine(accountInfo);
}
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [ListAccounts](#)。

CLI

AWS CLI

擷取組織中所有帳戶的清單

下列範例示範如何請求組織中的帳戶清單：

```
aws organizations list-accounts
```

輸出包含帳戶摘要物件的清單。

```
{
  "Accounts": [
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481830215.45,
      "Id": "111111111111",
      "Name": "Master Account",
      "Email": "bill@example.com",
      "Status": "ACTIVE"
    },
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481835741.044,
      "Id": "222222222222",
      "Name": "Production Account",
      "Email": "alice@example.com",
      "Status": "ACTIVE"
    },
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481835795.536,
      "Id": "333333333333",
      "Name": "Development Account",
```

```
        "Email": "juan@example.com",
        "Status": "ACTIVE"
    },
    {
        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": 1481835812.143,
        "Id": "444444444444",
        "Name": "Test Account",
        "Email": "anika@example.com",
        "Status": "ACTIVE"
    }
]
}
```

- 如需 API 詳細資訊，請參閱 AWS CLI 命令參考中的 [ListAccounts](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

ListOrganizationalUnitsForParent 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 ListOrganizationalUnitsForParent。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

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

///  
<summary>
```



```
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var parentId = "r-0000";

        var request = new ListOrganizationalUnitsForParentRequest
        {
            ParentId = parentId,
            MaxResults = 5,
        };

        var response = new ListOrganizationalUnitsForParentResponse();
        try
        {
            do
            {
                response = await
client.ListOrganizationalUnitsForParentAsync(request);
                response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            } while (response.NextToken is not null);
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
}
```

```
/// <summary>
/// Displays information about an Organizations organizational unit.
/// </summary>
/// <param name="unit">The OrganizationalUnit for which to display
/// information.</param>
public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
{
    string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

    Console.WriteLine(accountInfo);
}
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API 參考中的 [ListOrganizationalUnitsForParent](#)。

CLI

AWS CLI

擷取父 OUs 或根中的 OU 清單

下列範例示範如何取得指定根中的 OUs 清單：

```
aws organizations list-organizational-units-for-parent --parent-id r-examplerootid111
```

輸出顯示指定的根包含兩個 OUs 並顯示每個的詳細資訊：

```
{
  "OrganizationalUnits": [
    {
      "Name": "AccountingDepartment",
      "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-examplerootid111/ou-examplerootid111-exampleouid111"
    },
    {
      "Name": "ProductionDepartment",
```

```

        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
        exempleroottid111/ou-exempleroottid111-exampleouid222"
    }
}
}

```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [ListOrganizationalUnitsForParent](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

ListPolicies 搭配 AWS SDK 或 CLI 使用

下列程式碼範例示範如何使用 ListPolicies。

.NET

適用於 .NET 的 SDK

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```

using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {

```

```

{
    // Create the client object using the default account.
    IAmazonOrganizations client = new AmazonOrganizationsClient();

    // The value for the Filter parameter is required and must be
    // one of the following:
    //     AISERVICES_OPT_OUT_POLICY
    //     BACKUP_POLICY
    //     SERVICE_CONTROL_POLICY
    //     TAG_POLICY
    var request = new ListPoliciesRequest
    {
        Filter = "SERVICE_CONTROL_POLICY",
        MaxResults = 5,
    };

    var response = new ListPoliciesResponse();
    try
    {
        do
        {
            response = await client.ListPoliciesAsync(request);
            response.Policies.ForEach(p => DisplayPolicies(p));
            if (response.NextToken is not null)
            {
                request.NextToken = response.NextToken;
            }
        }
        while (response.NextToken is not null);
    }
    catch (AWSOrganizationsNotInUseException ex)
    {
        Console.WriteLine(ex.Message);
    }
}

/// <summary>
/// Displays information about the Organizations policies associated
/// with an organization.
/// </summary>
/// <param name="policy">An Organizations policy summary to display
/// information on the console.</param>
private static void DisplayPolicies(PolicySummary policy)
{

```

```
        string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

        Console.WriteLine(policyInfo);
    }
}
```

- 如需 API 詳細資訊，請參閱 適用於 .NET 的 AWS SDK API Reference 中的 [ListPolicies](#)。

CLI

AWS CLI

擷取特定類型組織中所有政策的清單

下列範例示範如何取得篩選條件參數所指定的 SCPs 清單：

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

輸出包含具有摘要資訊的 政策清單：

```
{
  "Policies": [
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllS3Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid111",
      "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
      "Description": "Enables account admins to delegate
permissions for any S3 actions to users and roles in their accounts."
    },
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllEC2Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid222",
      "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",

```

```

        "Description": "Enables account admins to delegate
permissions for any EC2 actions to users and roles in their accounts."
    },
    {
        "AwsManaged": true,
        "Description": "Allows access to every operation",
        "Type": "SERVICE_CONTROL_POLICY",
        "Id": "p-FullAWSAccess",
        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
        "Name": "FullAWSAccess"
    }
]
}

```

- 如需 API 詳細資訊，請參閱《AWS CLI 命令參考》中的 [ListPolicies](#)。

Python

SDK for Python (Boto3)

Note

GitHub 上提供更多範例。尋找完整範例，並了解如何在 [AWS 程式碼範例儲存庫](#) 中設定和執行。

```

def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise

```

```
else:  
    return policies
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Python (Boto3) API Reference 中的 [ListPolicies](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [AWS Organizations 搭配 AWS SDK 使用](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

的文件歷史記錄 AWS Organizations

下表會說明 AWS Organizations 的主要文件更新。

- API 版本：2016-11-28
- 文件最近更新時間：2025 年 6 月 17 日

變更	描述	日期
新增 Security Hub 政策	您可以使用 Security Hub 政策來集中管理整個的 Security Hub 組態 AWS Organizations。這些政策可協助您在組織中的多個帳戶中啟用功能並維持一致的安全控制。	2025 年 6 月 17 日
已更新 AWSOrganizationsFullAccess 受管政策	新增 <code>account:GetAccountInformation</code> 動作，以允許檢視組織中任何帳戶之帳戶名稱的存取權，以及 <code>account:PutAccountName</code> 動作，以允許修改組織中任何帳戶名稱的存取權。	2025 年 4 月 22 日
Organizations 與整合 AWS 使用者通知	您可以使用使用者通知與整合 AWS Organizations，以集中設定和檢視組織中各帳戶的通知。	2025 年 1 月 24 日
組織與 AWS Managed Services (AMS) 自助服務報告 (SSR) 的整合	您可以將 AMS SSR 與整合 AWS Organizations，以啟用彙總自助式報告 (SSR)。這是一項 AMS 功能，可讓進階和加速客戶檢視他們在組織層級跨帳戶彙總的現有自助式服務報告。	2025 年 1 月 21 日

[新增宣告政策](#)

您可以使用宣告式政策來集中宣告和強制執行整個組織中 AWS 服務 大規模指定 所需的組態。連接後，當服務新增新功能或 APIs 時，一律會維護組態。

2024 年 12 月 1 日

[新的 AWS 受管政策](#)

新增 `DeclarativePoliciesEC2Report` 政策以啟用 `declarative-policies-ec2.amazonaws.com` 服務連結角色的功能。

2024 年 11 月 22 日

[已更新備份政策](#)

AWS Backup 政策已更新 `selections` 政策金鑰以包含 `conditions` 政策金鑰，並將新的 `resources` 政策金鑰新增至結構描述。透過新的結構描述，您可以更靈活地選擇備份政策的資源。

2024 年 11 月 14 日

[集中管理成員帳戶的根存取權](#)

您現在可以透過集中式根存取權，管理 AWS Organizations 中成員帳戶間的特權根使用者憑證。使用 集中保護 AWS 帳戶 受管 的根使用者憑證 AWS Organizations，以移除和防止根使用者憑證大規模復原和存取。

2024 年 11 月 14 日

[新增資源控制政策 \(RCPs\)](#)

您可以使用資源控制政策 (RCPs) 來控制組織中資源的可用許可上限。

2024 年 11 月 13 日

新增聊天應用程式政策	您可以使用聊天應用程式政策，從 Slack 和 Microsoft Teams 等聊天應用程式控制對組織帳戶的存取。	2024 年 9 月 26 日
案例驅動的內容更新	文件 AWS Organizations 已更新為在整個指南中更以案例為導向，且內容已重新組織以改善可讀性和探索。如果您對這些變更有意見回饋，請使用頁面底部的提供意見回饋按鈕。	2024 年 9 月 4 日
新增選擇退出所有 AI 服務主題	新增如何選擇退出所有支援 AWS AI 服務的文件。	2024 年 8 月 16 日
Organizations 現在支援組織中的 10,000 個帳戶	您現在可以在組織中管理最多 10,000 個成員帳戶，將先前的 5,000 個帳戶限制加倍。如果您有有效的需求和業務需求，您可以請求並核准 10,000 個帳戶配額，而不需要 Organizations 或其他整合帳戶的服務限制檢查 AWS 服務。	2024 年 8 月 14 日
新帳戶遷移主題	新增如何將帳戶從一個組織遷移到另一個組織的文件。	2024 年 8 月 1 日
已更新備份政策	AWS Backup 政策現在支援 Amazon Elastic Block Store (Amazon EBS) 快照封存。如需更新的範例，請參閱 更新備份政策和備份政策語法和範例 。	2024 年 7 月 9 日

更新 AWSOrganizationsReadOnlyAccess 受管政策	將 <code>account:GetPrimaryEmail</code> 動作新增至 <code>AWSOrganizationsReadOnlyAccess</code> 政策，該政策可讓存取檢視組織中任何成員帳戶的根使用者電子郵件地址，並新增 <code>account:GetRegionOptStatus</code> 動作，讓存取能夠檢視組織中任何成員帳戶已啟用的區域。	2024 年 6 月 6 日
新的更新根使用者電子郵件地址主題	<code>Organizations</code> 現在提供集中更新組織中任何成員帳戶的根使用者電子郵件地址的功能。	2024 年 6 月 6 日
已更新政策陳述式	已將新 <code>Sid</code> 元素新增至 <code>AWSOrganizations</code> 受管政策陳述式。	2024 年 2 月 6 日
新的關閉管理帳戶主題	新增了如何關閉管理帳戶之考量和詳細步驟的連結。	2024 年 2 月 1 日
更新的最佳實務	在最佳實務區段新增資訊，以協助符合 IAM 最佳實務。	2023 年 6 月 12 日
已更新 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess 受管政策	已更新這兩個受管政策，以啟用對帳戶聯絡人的寫入或讀取存取權。	2022 年 10 月 21 日
已更新 AWSOrganizationsFullAccess 受管政策	受管政策已更新，允許透過新增必要的許可，來建立新組織所需的服務連結角色，從而建立組織。	2022 年 8 月 24 日

[組織從 AWS Organizations 主控台關閉帳戶功能](#)

管理帳戶中的主體可從 AWS Organizations 主控台關閉成員帳戶，並使用 IAM 政策保護成員帳戶以免遭意外關閉。

2022 年 3 月 29 日

[已更新使用 AWS Organizations 主控台更新替代聯絡人的通知](#)

Organizations 現在可讓您使用 AWS Organizations 主控台更新組織內帳戶的替代聯絡人。宣佈新功能，並指向帳戶管理參考，以獲得指示。

2022 年 2 月 8 日

[Organizations 受管政策更新 - 更新至現有政策](#)

更新 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess 受管政策，以允許透過 AWS Organizations 主控台更新或檢視帳戶替代聯絡人所需的帳戶 API 許可。

2022 年 2 月 7 日

[Organizations 與 Amazon DevOps Guru 的整合](#)

您可以將 Amazon DevOpsGuru 與整合 AWS Organizations，以全面監控所有組織帳戶的應用程式運作狀態，並取得洞見。

2022 年 1 月 3 日

[Organizations 與 Amazon Detective 的整合](#)

您可以整合 Amazon Detective 與 AWS Organizations，以確保您的 Detective 行為圖表可讓您了解所有組織帳戶的活動。

2021 年 12 月 16 日

[Organizations 與 AWS Config 的整合 現在支援多帳戶多區域資料彙總。](#)

您可以使用委派的管理員帳戶，從組織的所有成員帳戶彙總資源組態與合規資料。如需詳細資訊，請參閱AWS Config 開發人員指南中的[多帳戶多區域資料彙總](#)。

2021 年 6 月 16 日

[與的組織整合 AWS Firewall Manager 現在包含對委派管理員的支援](#)

您現在可以將組織中的成員帳戶指定為整個組織的 Firewall Manager StackSets 管理員。這樣可以更好地將許可與組織的管理帳戶分離。

2021 年 4 月 30 日

[Organizations 備份政策現在支援持續備份](#)

您可以搭配組織的備份政策使用 AWS Backup 連續備份功能。

2021 年 3 月 10 日

[Organizations 與 AWS CloudFormation StackSets 的整合現在包含對委派管理員的支援](#)

您現在可以將組織中的成員帳戶指定為整個組織的 AWS CloudFormation StackSets 管理員。這樣可以更好地將許可與組織的管理帳戶分離。

2021 年 2 月 18 日

[啟用所有功能的同時繼續邀請帳戶](#)

AWS 已更新程序，以啟用組織中的所有功能。您現在可以繼續邀請新帳戶加入您的組織，同時等待現有帳戶回應其邀請。

2021 年 2 月 3 日

[推出 AWS Organizations 主控台的 2.0 版](#)

AWS 推出了新版的 AWS 主控台。所有文件已更新，以反映執行任務的新方式。

2021 年 1 月 21 日

[Organizations 現在支援與整合 AWS Marketplace](#)

您現在可以讓 AWS Marketplace 更輕鬆地在組織的所有帳戶中共用軟體授權。

2020 年 12 月 3 日

[Organizations 現在支援與 Amazon S3 Lens 整合](#)

Amazon S3 Lens 支援 Organizations 的受信任存取和委派管理員。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的 [Amazon S3 Storage Lens](#)。

2020 年 11 月 18 日

[跨帳戶備份複本](#)

當您使用備份政策來備份組織中的資源時，您現在可以將備份的副本存放在組織中的其他 AWS 帳戶 中。

2020 年 11 月 18 日

[AWS 區域 在中國，現在支援 AWS Resource Access Manager 做為 Organizations 信任的服務](#)

當您 AWS RAM 在中國使用 Organizations 和 時，您現在可以使用與 Organizations 整合 AWS RAM 的功能做為信任的服務。

2020 年 11 月 18 日

[Organizations 現在支援與 整合 AWS Security Hub](#)

您可以跨組織中的所有帳戶啟用 Security Hub，並將組織的其中一個成員帳戶指定為 Security Hub 的委派系統管理員帳戶。

2020 年 11 月 12 日

[已重新命名主要帳戶](#)

AWS Organizations 將「主要帳戶」的名稱變更為「管理帳戶」。這只是名稱變更，且功能沒有任何改變。

2020 年 10 月 20 日

[新增最佳實務區段和主題](#)

新增章節，以取得 AWS Organizations 的最佳實務。新章節包含討論管理帳戶和成員帳戶根使用者及密碼管理的最佳實務的主題。

2020 年 10 月 6 日

[新增最佳實務區段和前兩頁](#)

主體有一個新的章節，用於描述 AWS Organizations 的最佳實務。此更新包含組織管理帳戶的最佳實務主題，以及成員帳戶的最佳實務主題。

2020 年 10 月 2 日

[Organizations 備份政策現在使用 VSS \(磁碟區陰影複製服務\)，支援 Windows EC2 執行個體上應用程式一致的備份](#)

備份政策支援新的 advanced_backup_settings 區段。該新區段中的第一個項目是稱為 WindowsVSS 的 ec2 設定，您可以啟用或停用。如需詳細資訊，請參閱AWS Backup 開發人員指南中的[建立啟用 VSS 的 Windows Backup](#)。

2020 年 9 月 24 日

[Organizations 支援在建立時加註標籤和標籤型存取控制](#)

您可以在建立 Organizations 資源時向其新增標籤。您可以使用[標籤政策](#)來標準化 Organizations 資源的標籤使用情況。您可以使用[IAM 政策，來限制僅存取具有指定標籤鍵和值的資源](#)。

2020 年 9 月 15 日

[新增 AWS Health 為信任的服務](#)

您可以在組織中跨帳戶彙總 AWS Health 事件。

2020 年 8 月 4 日

[人工智慧 \(AI\) 服務選擇退出政策](#)

您可以使用 AI 服務選擇退出政策來控制 AWS AI 服務是否可以存放和使用這些服務處理的客戶內容 (AI 內容)，以開發和持續改善 AWS AI 服務和技術。

2020 年 7 月 8 日

[新增備份政策和與的整合 AWS Backup](#)

您可以使用備份政策，以建立和強制執行組織中所有帳戶的備份政策。

2020 年 6 月 24 日

[支援 IAM Access Analyzer 的委派管理](#)

您可將組織中 Access Analyzer 的管理存取權委派給指定的成員帳戶。

2020 年 3 月 30 日

與 AWS CloudFormation StackSets 整合	您可以建立服務管理的堆疊集，將堆疊執行個體部署到由 AWS Organizations 管理的帳戶。	2020 年 2 月 11 日
與 Compute Optimizer 整合	Compute Optimizer 已作為一項服務新增，可與您組織中的帳戶搭配運作。	2020 年 2 月 4 日
標籤政策	您可以使用標籤政策，協助將組織帳戶中各資源的標籤標準化。	2019 年 11 月 26 日
與 Systems Manager 整合	您可以在 Systems Manager Explorer AWS 帳戶 中同步組織中所有的操作資料。	2019 年 11 月 26 日
aws:PrincipalOrgPaths	新的全域條件金鑰會檢查提出請求的 IAM 使用者、IAM 角色或 AWS 帳戶 根使用者的 AWS Organizations 路徑。	2019 年 11 月 20 日
與 AWS Config 規則整合	您可以使用 AWS Config API 操作來管理組織中所有 AWS 帳戶 的 AWS Config 規則。	2019 年 7 月 8 日
用於受信任存取的新服務	新增了 Service Quotas 做為服務，可以與組織中的帳戶搭配運作。	2019 年 6 月 24 日
與 AWS Control Tower 整合	AWS Control Tower 已新增為可與組織中帳戶搭配使用的服務。	2019 年 6 月 24 日

與 整合 AWS Identity and Access Management	針對您的組織實體 (組織根、OU 和帳戶)，IAM 會提供服務上次存取的資料。您可以使用此資料來限制僅存取您需要 AWS 服務的。	2019 年 6 月 20 日
標記帳戶	您可以在您的組織中標記和取消標記帳戶，以及檢視組織中帳戶上的標籤。	2019 年 6 月 6 日
服務控制政策 (SCP) 中的資源、條件和 NotAction 元素	您現在可以在 SCP 中指定資源、條件及 NotAction 元素，拒絕您組織或組織單位 (OU) 中的跨帳戶存取。	2019 年 3 月 25 日
用於受信任存取的新服務	AWS License Manager 和 Service Catalog 已新增為可與組織中帳戶搭配使用的服務。	2018 年 12 月 21 日
用於受信任存取的新服務	AWS CloudTrail 和 AWS RAM 新增為可與組織中帳戶搭配使用的服務。	2018 年 12 月 4 日
用於受信任存取的新服務	AWS Directory Service 已新增做為可與組織中帳戶搭配使用的服務。	2018 年 9 月 25 日
電子郵件地址驗證	您必須先驗證您擁有與管理帳戶關聯的電子郵件地址，之後才可以邀請現有的帳戶加入您的組織。	2018 年 9 月 20 日
CreateAccount 通知	CreateAccount 通知會發佈到管理帳戶的 CloudTrail 日誌。	2018 年 6 月 28 日
用於受信任存取的新服務	AWS Artifact 已新增 做為可與組織中帳戶搭配使用的服務。	2018 年 6 月 20 日

用於受信任存取的新服務	AWS Config 和 AWS Firewall Manager 新增為可與組織中帳戶搭配使用的服務。	2018 年 4 月 18 日
受信任服務存取	您現在可以啟用或停用 Select 在組織中帳戶中 AWS 服務運作的存取權。IAM Identity Center 是一開始就支援的受信任服務。	2018 年 3 月 29 日
帳戶移除現在為自助服務	您現在可以從 內移除建立的帳戶，AWS Organizations 無需聯絡 AWS 支援。	2017 年 12 月 19 日
新增對新服務的支援 AWS IAM Identity Center	AWS Organizations 現在支援與 AWS IAM Identity Center (IAM Identity Center) 整合。	2017 年 12 月 7 日
AWS 已將服務連結角色新增至所有組織帳戶	名為 的服務連結角色AWSServiceRoleForOrganizations 會新增至組織中的所有帳戶，以啟用 AWS Organizations 與其他 之間的整合 AWS 服務。	2017 年 10 月 11 日
您現在可以移除已建立的帳戶	客戶現在可以透過 AWS 支援的協助，從組織中移除已建立的帳戶。	2017 年 6 月 15 日
服務啟動	隨附於新服務啟動 AWS Organizations 的文件初始版本。	2017 年 2 月 17 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。