



開發人員指南

AWS 網路安全管理員



AWS 網路安全管理員: 開發人員指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS Network Security Manager ?	1
AWS Network Security Manager 的運作方式一目了然	1
AWS Network Security Manager 的功能	1
使用案例	2
相關服務	2
存取 AWS Network Security Manager	3
定價	4
您是第一次使用 的新手嗎 ?	4
AWS Network Security Manager 的運作方式	5
AWS Network Security Manager 資源模型	5
AWS Network Security Manager 資源生命週期、合併和同步	6
草稿和作用中生命週期	6
版本控制	7
優先順序型政策合併	7
使用 Config AWS 進行資源探索	8
同步和修復	9
管理員和成員帳戶	10
服務連結角色	10
設定 AWS Network Security Manager	12
選擇您的組織模型	12
設定 供單一帳戶使用	12
設定 以搭配 AWS Organizations 使用多帳戶	12
建立 AWS Network Security Manager 管理員帳戶	13
使用 AWS Network Security Manager 許可建立 IAM 身分	15
註冊 AWS 帳戶	16
在預設停用的區域中使用 AWS Network Security Manager	16
教學課程：部署您的第一個網路安全保護	17
先決條件	17
步驟 1：建立規則	17
步驟 2：建立範本	19
步驟 3：建立政策	19
步驟 4：建立範圍	20
步驟 5：建立和發佈部署	21
步驟 6：監控同步狀態	22

步驟 7：清除	22
後續步驟	24
管理防火牆和安全服務	25
管理 AWS WAF ACLs	25
AWS WAF 概念	25
快速建立 AWS WAF	28
AWS WAF 的標準建立程序	32
管理 Shield Advanced AWS 的 DDoS 保護	37
Shield Advanced AWS 的快速建立	37
Shield Advanced AWS 的標準建立程序	40
AWS Network Security Manager 和 Firewall Manager	44
與 AWS Firewall Manager 共存	44
修復期間的優先順序	44
從 AWS Firewall Manager 的計劃遷移	44
安全	45
資料保護	45
靜態加密	46
傳輸中加密	46
金鑰管理	46
身分與存取管理	47
目標對象	47
使用身分驗證	47
使用政策管理存取權	48
AWS Network Security Manager 如何與 IAM 搭配使用	50
身分型政策範例	55
疑難排解	58
服務連結角色	60
服務連結角色許可	60
建立服務連結角色	71
編輯服務連結角色	71
刪除服務連結角色	71
支援的區域	72
法規遵循驗證	72
恢復能力	72
基礎設施安全性	73
安全最佳實務	73

預防性控制	73
偵測性控制	73
監控 AWS Network Security Manager	74
監控同步狀態	74
同步狀態操作	74
了解同步狀態值	74
了解評估時間戳記	75
跨帳戶可見性	75
診斷out-of-sync的資源	75
CloudTrail 日誌	76
AWS CloudTrail 中的 Network Security Manager 資訊	76
範例：CreatePolicy 事件	77
配額	80
資源配額	80
資源合成配額	80
範圍組態配額	81
管理員帳戶配額	81
API 分頁配額	81
配額調整性	82
文件歷史紀錄	83
.....	lxxxiv

什麼是 AWS Network Security Manager ?

使用 AWS Network Security Manager，您可以在組織中的一或多個帳戶和資源中集中定義和部署網路安全保護，例如 AWS WAF 和 AWS Shield Advanced 規則。您不需要個別使用每個資源，而是定義可重複使用的政策物件（規則、範本和政策）一次，並大規模部署它們，並持續監控以偵測和修復政策偏離。

AWS Network Security Manager 的運作方式一目了然

您可以定義一組階層政策物件，並將其套用至目標範圍。最低層級的政策物件是規則。您可以將規則分組為範本，您可以將這些範本結合為具有優先順序衝突解決的政策。然後，您可以選取要使用範圍保護的帳戶和資源，並透過發佈部署來強制執行您的政策。

部署之後，AWS Network Security Manager 會持續監控範圍環境和部署的政策，以檢查是否符合預期的定義。如果沒有，AWS Network Security Manager 可以選擇性地修復偏離預期組態的資源。如需資源模型、生命週期和架構的完整詳細資訊，請參閱 [AWS Network Security Manager 的運作方式](#)。

AWS Network Security Manager 的功能

- 支援多種防火牆類型 – AWS Network Security Manager 支援適用於 Web ACL 組態和規則群組的 AWS WAF。受保護的資源類型包括 Amazon CloudFront 分佈、Application Load Balancer 和 Amazon API Gateway 階段。AWS Network Security Manager 也支援 AWS Shield Advanced for DDoS 保護 Amazon CloudFront 分佈、Application Load Balancer、Classic Load Balancer 和彈性 IP 地址。
- 可重複使用的安全組態 – 將政策物件定義為規則一次，將其分組為範本，並建立目標資源的範圍。在多個政策和部署中重複使用規則、範本和範圍。
- 優先順序型政策合併 – 當多個政策保護相同的資源時，AWS Network Security Manager 會根據政策優先順序合併其組態，提供可預測的衝突解決方案。
- 單一帳戶和多管理員支援 – 在單一帳戶中使用 AWS Network Security Manager，或指定多個管理員帳戶，每個帳戶都具有優先順序層級。當管理員的政策重疊時，AWS Network Security Manager 會先依管理員優先順序解決衝突，然後依每個帳戶內的政策優先順序解決衝突。
- 草稿和作用中狀態 – 每個 AWS Network Security Manager 資源，包括規則、範本、政策、範圍和部署，都支援草稿和作用中狀態。將資源儲存為草稿，而不會影響即時保護，然後在準備好強制執行它們時發佈。

- 版本化快照 – 每個 AWS Network Security Manager 資源，包括規則、範本、政策、範圍和部署，都支援不可變的版本編號快照。使用版本控制來保留已知良好的 AWS Network Security Manager 資源組態。
- Protected-resource 同步診斷 – 對於每個範圍內的資源，請參閱確切哪些設定不同步以及原因，以及與每個組態欄位的實際值相比的預期設定。
- 自動修復 – 選擇性地讓 AWS Network Security Manager 自動修復out-of-sync的資源，並將其與預期的組態保持一致，而無需手動介入。
- 自然語言規則產生 – 使用 GenerateRuleConfiguration操作以純語言描述規則，並接收由 Amazon Bedrock 提供支援的對應組態 JSON。

使用案例

以下是 AWS Network Security Manager 的常見使用案例：

- 跨所有帳戶強制執行基準 AWS WAF 規則 – 定義一組 AWS WAF 規則群組，每個面向網際網路的應用程式都必須使用，然後將其部署到整個組織中。AWS Network Security Manager 會自動將規則套用到新的範圍內資源。
- 跨特定資源建立特定的自訂或例外 AWS WAF 規則 – 定義一組 WAF AWS 規則，這些規則僅適用於一組特定的資源。此集可以是您透過 AWS 帳戶 ID、OU、標籤或 Amazon Resource Name (ARNs) 識別的特定業務單位或應用程式。
- 驗證面向網際網路的資源上的 DDoS 保護 – 建立範圍為公有資源類型的 AWS Shield Advanced 政策，並將其部署到整個組織，以便重要資源啟用 DDoS 保護。
- 偵測和修復組態偏離 – 使用同步狀態監控來識別防火牆組態已從預期狀態偏離的資源，並選擇性地啟用自動修復，使其恢復合規。
- 將安全管理委派給多個團隊 – 指定具有不同優先順序層級和特定帳戶、組織單位或防火牆類型範圍存取權的多個管理員帳戶，讓團隊能夠在定義的界限內管理自己的安全政策。

相關服務

- AWS WAF – 使用 AWS WAF 保護您的 Web 應用程式和 APIs 不受可能影響可用性、危及安全性或消耗過多資源的常見 Web 入侵和機器人影響。AWS Network Security Manager 使用 AWS WAF 為組織中的單一帳戶或跨帳戶的資源建立和管理 Web ACLs 和規則群組。

- AWS Shield Advanced – 受管 DDoS 保護服務，可為執行的應用程式提供擴充的保護 AWS。AWS Network Security Manager 使用 Shield Advanced 為單一帳戶或您組織中的帳戶中的資源提供 DDoS 保護。
- AWS Organizations – 協助您在 AWS 資源成長和擴展時集中管理環境。AWS Network Security Manager 需要 AWS Organizations 跨成員帳戶管理保護。
- AWS Config – 可讓您評估、稽核和評估 AWS 資源組態的服務。AWS Network Security Manager 使用服務連結 AWS 的 Config 記錄器來探索成員帳戶中的資源。

存取 AWS Network Security Manager

您可以透過下列界面存取 AWS Network Security Manager：

AWS 管理主控台

用於管理 AWS Network Security Manager 資源的 Web 型界面。

在 <https://console.aws.amazon.com/network-security-manager/> 開啟 AWS Network Security Manager 主控台。

AWS 命令列界面 (AWS CLI)

提供 AWS Network Security Manager 操作的命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

AWS SDKs

AWS 提供 SDKs 其中包含適用於各種程式設計語言和平台的程式庫和範本程式碼。SDKs 提供便捷的方式來建立對 AWS Network Security Manager 的程式設計存取。如需詳細資訊，請參閱 [Amazon Web Services 適用工具](#)。

AWS Network Security Manager API

透過 HTTPS 使用 JSON 的 REST API。API 端點格式為 `network-security-manager.{region}.api.aws`。如需詳細資訊，請參閱 [AWS Network Security Manager API 參考](#)。

若要開始使用 AWS Network Security Manager，請參閱 [設定 AWS Network Security Manager](#) 和 [教學課程：部署您的第一個網路安全保護](#)。

定價

您需為 AWS Network Security Manager 監控和保護的每個範圍內資源付費。您部署的基礎安全服務會收取額外費用，例如 AWS WAF 和 AWS Shield Advanced。如需詳細的定價資訊，請參閱 AWS 網站上的 [AWS Network Security Manager 定價](#)。

您是第一次使用 的新手嗎？

如果您是第一次使用 AWS Network Security Manager，我們建議您依序閱讀下列主題：

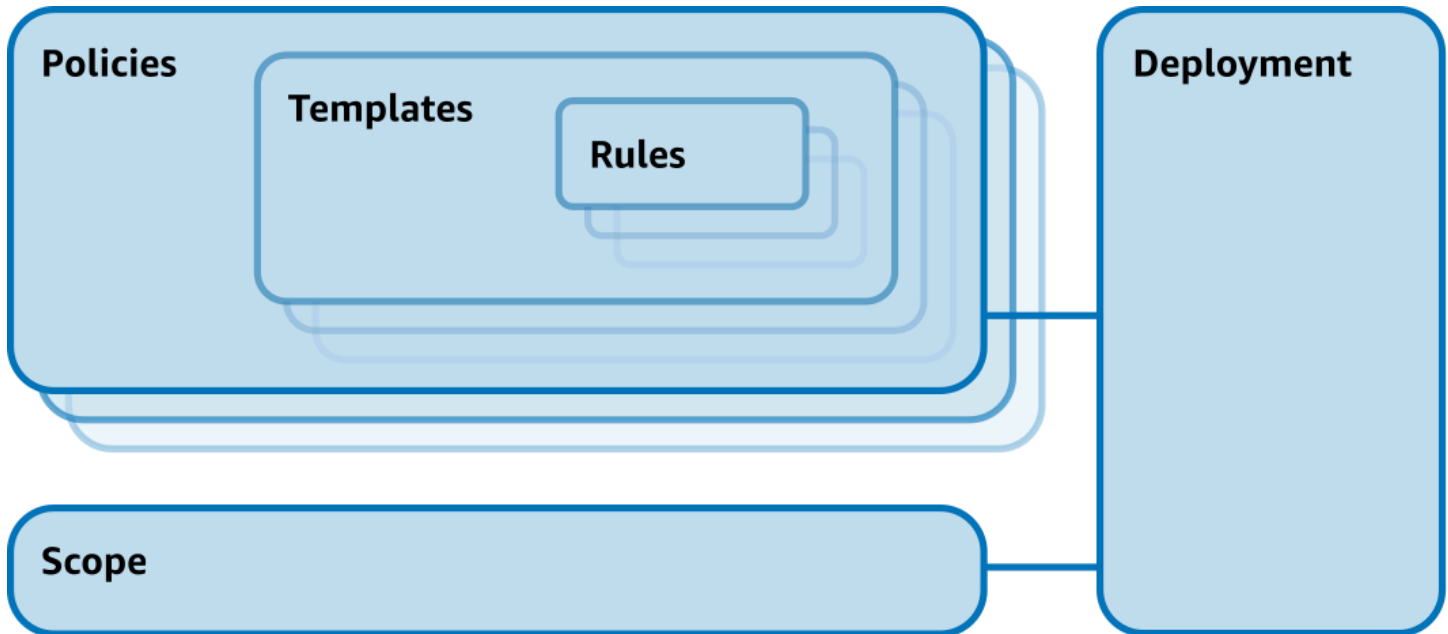
1. [AWS Network Security Manager 的運作方式](#) – 了解資源模型、生命週期狀態、政策合併和同步。
2. [設定 AWS Network Security Manager](#) – 完成使用 AWS Network Security Manager 的先決條件。
3. [教學課程：部署您的第一個網路安全保護](#) – 逐步解說建立您第一個部署的end-to-end教學課程。

AWS Network Security Manager 的運作方式

使用 AWS Network Security Manager 資源模型來設計和管理單一帳戶中或組織中多個帳戶中資源的網路安全保護。本章說明五種資源類型、它們如何形成階層，以及控管其行為的關鍵概念。

AWS Network Security Manager 資源模型

AWS Network Security Manager 使用在合成階層中配置的五種資源類型：



資源透過階層互相向上參考。規則用於範本和政策。範本、規則或兩者都在政策中使用。範圍參考政策在部署中保護的資源。

下列各節說明階層中的每個資源類型。

規則 – 網路安全組態的原子單位。規則有兩種類型：流量檢查規則和防火牆組態規則。流量檢查著重於安全服務如何處理流量。組態規則會指定流量檢查以外的系統操作。規則的結構因防火牆類型而異。

範本 – 單一防火牆類型的有序、可重複使用的規則群組。使用範本將相關規則封裝在一起，並在多個政策之間共用。範本是選用的。

政策 – 結合一組排序的範本和規則與防火牆類型的強制執行設定。每個政策都有優先順序（數字越小表示優先順序越高）。當多個政策保護相同的資源時，優先順序會決定衝突如何解決。對於流量檢查規則，優先順序會決定彙總規則的順序。對於防火牆組態規則，優先順序會決定適用於每個資源及其範圍內政策的組態。

範圍 – 套用保護的宣告性選擇。範圍會指定要保護的資源類型，而且您可以選擇依標籤或組態屬性篩選資源。在多帳戶模式中，範圍也會指定要包含或排除的帳戶或 OUs。在單一帳戶模式中，範圍適用於帳戶本身。範圍的模式會在您建立時修正。您無法在任一方向的多帳戶和單一帳戶模式之間切換範圍，因此多帳戶範圍永遠無法成為單一帳戶範圍，反之亦然。

部署 – 將一或多個政策繫結至範圍。發佈部署可啟用強制執行。AWS Network Security Manager 會探索範圍內的資源、計算預期的組態，並選擇性地修復out-of-sync的資源。

如需資源合成限制，請參閱 [配額](#)。

AWS Network Security Manager 資源生命週期、合併和同步

以下各節說明管理 AWS Network Security Manager 資源在建立後如何運作的行為和機制。

草稿和作用中生命週期

每個 AWS Network Security Manager 資源 - 包括規則、範本、政策、範圍和部署 - 的狀態為草稿或作用中：

- **作用中** – 預設狀態。資源已發佈並可供使用。其他資源可以參考它，以及包含它強制執行其組態的部署。
- **草稿** – 資源已儲存但尚未啟用。草稿資源不會強制執行，其他資源也無法參考。當您建立或更新資源時，請選擇儲存草稿以保持草稿狀態。

根據預設，AWS Network Security Manager 會將資源建立為作用中。若要使用 API 將資源建立為草稿，請在建立或更新操作false中將 isPublished 參數設定為 。

當您更新資源時，適用下列案例：

目前狀態	Action	結果
草稿	選擇儲存草稿	更新草稿（保留草稿）
草稿	選擇發佈	發佈草稿（變成作用中）
作用中	選擇發佈	更新並保持作用中（作用中）
作用中	選擇儲存草稿	建立草稿浮水印（變成下方具有作用中資源的草稿）

hasPublishedVersion 欄位會出現在清單中並取得回應。此欄位會告訴您發佈的作用中資源是否存在於草稿下方。當資源具有草稿狀態 和 時hasPublishedVersion: true，待定草稿位於即時發佈的作用中資源之上。

您無法刪除另一個作用中資源參考的作用中資源。

版本控制

每個 AWS Network Security Manager 資源，包括規則、範本、政策、範圍和部署，都可以進行版本控制。若要建立作用中資源的版本，請選取資源，選擇動作，然後選擇建立版本控制的快照。版本不會在每次更新時自動建立。

AWS CLI 替代方案

您也可以使用作用中資源上的 Create{Resource}Snapshot API 操作來建立版本。

金鑰版本屬性：

- 每個版本都有唯一的數字（循序整數）和符合版本資格的 ARN（例如 arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3）。
- 版本不可變。它們無法更新。
- 每個資源最多可以建立 10 個版本。
- 版本可標記。

使用 版本來保留所需的組態變體。若要轉返資源，請閱讀版本，然後使用版本所需的組態更新即時資源。

優先順序型政策合併

當多個政策保護相同的資源時，AWS Network Security Manager 會將其組態合併為單一結果。優先順序較低的數字表示優先順序較高（優先順序 1 優先於優先順序 2）。當 AWS Network Security Manager 合併包含流量檢查規則的政策時，優先順序會決定彙總規則的順序。對於防火牆組態規則，優先順序較高的政策會決定適用的組態。

AWS Network Security Manager 會以下列順序在兩個層級評估優先順序：

1. 管理員優先順序 – AWS Network Security Manager 會先評估管理員優先順序。每個組織管理員都會獲指派優先順序，如 中所述 [the section called “管理員和成員帳戶”](#)。當 AWS Network Security

Manager 合併政策時，它會將管理員政策排名為高於成員帳戶自己的單一帳戶政策。如果管理員政策和成員帳戶的單一帳戶政策都適用於資源和衝突，則管理員政策的組態會獲勝。成員帳戶無法選擇退出、覆寫或豁免管理員政策本身。

2. 政策優先順序：在每個帳戶中，AWS Network Security Manager 接著會使用政策優先順序來解決剩餘的衝突。政策優先順序值是從 1 開始的整數，且每個帳戶必須是唯一的。

您可以在 PutAdminAccount 操作上以必要 priority 欄位設定管理員優先順序，整數從 1 到 10。優先順序值是唯一的，因此兩個管理員永遠不會共用優先順序，也不需要中斷綁定。如需詳細資訊，請參閱 [AWS Network Security Manager API 參考](#)。

資源所有適用政策的合併結果是有效的防火牆組態。AWS Network Security Manager 會運算此組態、將其與資源的實際組態進行比較，並將任何差異報告為同步狀態。

當政策發生衝突時，AWS Network Security Manager 會比較每個屬性，並套用較高優先順序政策中的值。如果優先順序較高的政策未定義屬性，則會套用優先順序較低的政策值。符合有效組態的資源是 IN_SYNC。受到較低優先順序政策保護的資源，其設定被較高優先順序政策報告為低優先順序部署的 OUT_OF_SYNC。這是預期的行為，而不是失敗。

使用 Config AWS 進行資源探索

AWS Network Security Manager 會使用服務連結的 Config AWS 組態記錄器，探索您帳戶中的受保護資源。此記錄器會在該帳戶進入部署範圍時，在每個帳戶中自動建立。與 AWS Firewall Manager 不同，您不需要執行任何其他 setup。AWS Config 用量，AWS Network Security Manager 不會向 AWS Network Security Manager 客戶收費。

服務連結記錄器的主要特性：

- 它命名為 AWSConfigurationRecorderForNetworkSecurityManager。
- 它與帳戶中任何客戶管理的組態記錄器分開。
- 它只會記錄與作用中範圍和部署相關的資源類型。
- 您不需要設定 AWS Config 或建立組態記錄器。AWS Network Security Manager 會自動管理此項目。AWS Network Security Manager 的 AWS 組態用量不會向客戶收費。
- 您無法在使用時修改或刪除記錄器。AWS Network Security Manager 會自動管理其生命週期。

您不需要手動啟用或設定 AWS Config，AWS Network Security Manager 才能運作。服務會在您發佈部署後自動處理資源探索。

同步和修復

AWS Network Security Manager 中的強制執行是非同步且最終一致。發佈部署之後，或資源變更時，會發生下列階段：

1. 資源探索 – AWS Network Security Manager 會使用服務連結的 Config AWS 記錄器探索範圍內的資源。
2. 組態運算 – 對於每個探索的資源，AWS Network Security Manager 會依優先順序合併所有適用的政策，以計算有效的防火牆組態。
3. 同步評估 – AWS Network Security Manager 會將有效組態與資源的實際組態進行比較，並記錄同步狀態。
4. 修復（選用） – 如果您在政策 `remediationEnabled` 上設定，AWS Network Security Manager 會 `out-of-sync` 的資源，以符合有效的組態。

每個階段都是非同步的。工作流程的後果：

- 發佈部署與保護資源之間有延遲。
- 在範圍內建立新的資源和受保護的資源之間存在延遲。
- 同步狀態項目上的 `Last Checked` 時間戳記會告訴您 AWS Network Security Manager 上次評估資源的時間。

修補和資源清除是政策層級設定。您可以在 `policyConfiguration` 物件中為每個政策設定每個政策。

`remediationEnabled`

指定 AWS Network Security Manager 是否自動修復不合規的資源。當您啟用此設定時，AWS Network Security Manager 會 `out-of-sync` 的資源，以符合有效的組態。

`resourcesCleanUp`

指定 AWS Network Security Manager 是否在不再需要資源時自動移除它建立的資源。AWS Network Security Manager 會刪除它在您移除部署時建立的防火牆，或當帳戶或資源超出範圍時。

`remediationEnabled` 和 `resourcesCleanUp` 設定都預設為 `false`。在您啟用這些設定之前，AWS Network Security Manager 不會修復或清除資源。`policyConfiguration` 物件也會保留

wafConfig，這適用於 AWS WAF 政策。如需詳細資訊，請參閱 [AWS Network Security Manager API 參考](#)。

當資源不同步時，同步狀態會包含out-of-sync的原因，其中包含每個設定的詳細資訊，顯示與實際值相比的預期值。原因分為下列類別：

- missingFirewall – 沒有與資源相關聯的防火牆保護。
- invalidFirewall – 防火牆存在，但其組態與有效組態不同。這包括六個詳細資訊儲存貯體：incorrectSingleValueConfigurations、missingAppendableConfigurationValues、missingUnexpectedAppendableConfigurationValues、incorrectAppendableConfigurationOrder和unexpectedMergeableConfigurationValues。

如果啟用修復，但 AWS Network Security Manager 無法修復資源，remediationIssues 欄位會提供 issueType、message描述問題的，以及correctiveAction建議如何解決問題。

AWS Network Security Manager 不會評估其未管理的設定。如果欄位未出現在任何貢獻規則中，AWS Network Security Manager 會在同步評估期間忽略該欄位。

管理員和成員帳戶

AWS Network Security Manager 使用以 AWS Organizations 為基礎的跨帳戶管理模型：

- 管理員帳戶 – 您建立和管理 AWS Network Security Manager 資源（規則、範本、政策、範圍和部署）的帳戶。您可以指定一或多個管理員帳戶，每個帳戶的優先順序為 1 到 10。
- 成員帳戶 – AWS Network Security Manager 探索資源、評估同步狀態，以及選擇性地修復out-of-sync組態的帳戶。AWS Network Security Manager 透過服務連結角色在成員帳戶中運作。如需詳細資訊，請參閱[the section called “服務連結角色”](#)。

您可以選擇將每個管理員範圍限定為帳戶、OUs 和防火牆類型的子集。使用此功能將特定區域的管理委派給不同的團隊。

AWS Network Security Manager 是一種區域服務。您可以為每個區域建立資源和部署，而不需要跨區域相依性。

服務連結角色

AWS Network Security Manager 使用名為 `AWSServiceRoleForNetworkSecurityManager` 的 IAM 服務連結角色，代表您在組織的成員帳戶中採取

行動。此角色信任 `network-security-manager.amazonaws.com` 服務委託人。它使用 `NetworkSecurityManagerServiceRolePolicy` AWS 受管政策。

AWS Network Security Manager 會在您啟用服務時自動建立此角色，因此不會手動設定。此角色可讓 AWS Network Security Manager 管理 AWS WAF 和 AWS Shield Advanced 保護、透過 AWS Config 探索受保護的資源，以及執行跨帳戶操作。如需詳細資訊，請參閱 [the section called “服務連結角色”](#)。

設定 AWS Network Security Manager

使用 AWS Network Security Manager，您可以在兩個組織模型中工作。直接在單一帳戶中使用它，或搭配 AWS Organizations 使用它來管理多個帳戶的保護。設定步驟取決於您選擇的模型。

主題

- [選擇您的組織模型](#)
- [設定 供單一帳戶使用](#)
- [設定 以搭配 AWS Organizations 使用多帳戶](#)
- [建立 AWS Network Security Manager 管理員帳戶](#)
- [使用 AWS Network Security Manager 許可建立 IAM 身分](#)
- [在預設停用的區域中使用 AWS Network Security Manager](#)

選擇您的組織模型

從下列組織模型中選擇：

- 單一帳戶 – 使用 AWS Network Security Manager 來保護一個帳戶中的資源。您不需要 AWS Organizations 或管理員帳戶。使用 AWS Network Security Manager 許可建立 IAM 身分，並直接開始使用服務。AWS Network Security Manager 會自動在您的帳戶中建立服務連結角色。
- 多帳戶 – 使用 AWS Network Security Manager 搭配 AWS Organizations 來保護多個帳戶的資源。此模式需要設定 AWS Organizations、啟用受信任的存取，以及建立管理員帳戶。

設定 供單一帳戶使用

若要在單一帳戶中使用 AWS Network Security Manager，請建立具有適當許可的 IAM 身分，並直接開始使用服務。您不需要建立管理員帳戶。AWS Network Security Manager 會在背景的帳戶中自動建立服務連結角色。跳至 [the section called “使用 AWS Network Security Manager 許可建立 IAM 身分”](#)。

設定 以搭配 AWS Organizations 使用多帳戶

若要管理多個帳戶的保護，請建立所需的 AWS Organizations 成員資格和組態。

1. 選擇要用作組織 AWS Network Security Manager 管理員的帳戶 – 這是您從中建立和管理 AWS Network Security Manager 資源的帳戶。

2. 驗證組織成員資格 – 如果您選擇的帳戶尚未成為組織的成員，請讓其加入。遵循 AWS Organizations 使用者指南中[邀請 AWS 帳戶加入組織](#)的指引。
3. 啟用組織中的所有功能 – AWS Organizations 有兩個可用的功能集：合併帳單功能和所有功能。若要使用 AWS Network Security Manager，您的組織必須啟用所有功能。如果您的組織僅針對合併帳單設定，請遵循 AWS Organizations 使用者指南中[啟用組織中所有功能](#)的指導。
4. 啟用 AWS Network Security Manager 的受信任存取 – 在 AWS Organizations 中啟用 AWS Network Security Manager 的受信任存取。啟用受信任存取後，AWS Network Security Manager 可以在成員帳戶中建立服務連結角色，並代其管理資源。
5. 註冊委派管理員帳戶 – 將您選擇的帳戶註冊為 AWS Organizations 中 AWS Network Security Manager 的委派管理員。使用 Organizations 管理帳戶來完成此步驟。

關閉受信任存取時停用多帳戶保護

如果您關閉 AWS Organizations 中 AWS Network Security Manager 的受信任存取權，或者取消註冊委派管理員帳戶，AWS Network Security Manager 會將多帳戶範圍和部署設定為 DISABLED 狀態，並清除其管理的保護。

建立 AWS Network Security Manager 管理員帳戶

此步驟僅適用於多帳戶模式。只有組織的管理帳戶可以建立 AWS Network Security Manager 管理員帳戶。

完成 Organizations 設定後，請將您的帳戶註冊為 AWS Network Security Manager 管理員。您可以從主控台或 AWS 命令列界面 (AWS CLI) 執行此操作。

當您建立管理員帳戶時，AWS Network Security Manager 會自動在您組織的所有帳戶中建立服務連結角色。透過此角色，AWS Network Security Manager 會探索資源並管理成員帳戶中的保護。

使用 AWS Network Security Manager，您可以有多個管理員來管理組織的防火牆資源。如果您想要在組織中使用多個管理員，您可以將管理範圍條件套用至每個管理員，以定義他們可以管理的資源。這可讓您彈性地在組織內擁有不同的管理員角色，並協助您維持最低權限存取的原則。例如，一個管理員可以管理一組組織單位 OUs)。另一個管理員只能管理特定的政策類型。

如需每個組織可擁有的管理員數量上限，請參閱 [配額](#)。

區域註冊

您可以在單一區域中註冊 AWS Network Security Manager 管理員帳戶 AWS。若要在其他區域中使用 AWS Network Security Manager，請在每個區域中重複此步驟。

使用主控台建立管理員帳戶

1. 開啟位於 <https://console.aws.amazon.com/network-security-manager/> 的 AWS Network Security Manager 主控台。
2. 在導覽窗格中，選擇設定。
3. 選擇新增管理員。
4. 選取帳戶，然後輸入優先順序值 (1 到 10)。
5. 選擇新增管理員以確認。

使用 CLI AWS 建立管理員帳戶

呼叫 PutAdminAccount 操作。您必須提供優先順序值 (1 到 10)。

下列 AWS CLI 範例會將帳戶註冊為優先順序為 1 的 AWS Network Security Manager 管理員：

```
aws network-security-manager put-admin-account \  
  --account-id 123456789012 \  
  --priority 1
```

您可以指定多個管理員帳戶，每個帳戶具有不同的優先順序。或者，您也可以提供 adminScope 參數，將每個管理員限制在特定帳戶、OUs 或防火牆類型。

使用主控台移除管理員帳戶

移除管理員時停用多帳戶保護

當您移除管理員帳戶時，AWS Network Security Manager 會將多帳戶範圍和部署設定為 DISABLED 狀態，並清除其管理的保護。

1. 在 <https://console.aws.amazon.com/network-security-manager/> 開啟 AWS Network Security Manager 主控台。
2. 在導覽窗格中，選擇設定。
3. 選取您要移除的管理員帳戶。
4. 選擇 Remove administrator (移除管理員)。
5. 若要確認，請選擇確認管理員刪除。

使用 AWS Network Security Manager 許可建立 IAM 身分

若要使用 AWS Network Security Manager，您需要具有呼叫 AWS Network Security Manager 操作許可的 IAM 身分（使用者或角色）。IAM 動作使用字首 `network-security-manager`。

下列範例 IAM 政策包含三個陳述式。第一個陳述式授予所有 AWS Network Security Manager 操作的完整存取權。第二個陳述式會授予 AWS Network Security Manager 所需的其他 AWS Organizations 和 AWS WAF 許可。AWS Network Security Manager 會使用這些許可來識別組織中的帳戶和組織單位 (OUs)，並列出可用的 WAF 規則群組和受管產品。這些許可也可讓 AWS Network Security Manager 啟用受信任存取，並在 Organizations 中 AWS 註冊委派管理員。第三個陳述式會授予 AWS Network Security Manager 建立其服務連結角色所需的 `iam:CreateServiceLinkedRole` 許可，該角色需要用於單一帳戶和多帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "network-security-manager:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "wafv2:ListRuleGroups",

```

```
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:DescribeAllManagedProducts"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*"
  }
]
```

針對生產用途，建議您僅授予所需的最低許可。如需詳細資訊，請參閱[the section called “身分與存取管理”](#)。

註冊 AWS 帳戶

若要開始使用 AWS，您需要 AWS 帳戶。如需建立的相關資訊 AWS 帳戶，請參閱《AWS 帳戶管理參考指南》中的[入門 AWS 帳戶](#)。

在預設停用的區域中使用 AWS Network Security Manager

若要在預設停用的區域中使用 AWS Network Security Manager，您必須為組織的管理帳戶和 AWS Network Security Manager 管理員帳戶啟用區域。如需預設停用的區域及其啟用方式的相關資訊，請參閱《AWS 一般參考》中的[管理 AWS 區域](#)。

啟用已停用的區域

對於 Organizations 管理帳戶和 AWS Network Security Manager 管理員帳戶，請遵循 AWS 一般參考中[啟用區域](#)的指導。

部署您的第一個網路安全保護

本教學課程將逐步引導您使用 AWS Network Security Manager 主控台部署 AWS WAF Web ACL。您完成下列步驟：

1. 建立規則
2. 建立範本
3. 建立政策
4. 建立範圍
5. 建立和發佈部署
6. 監控同步狀態

在本教學課程中，您會建立 AWS WAF Web ACL，以保護所選帳戶中的 Application Load Balancer。此程序與 AWS Network Security Manager 支援的所有安全服務和防火牆大致相同。

完成時間：約 10 分鐘

成本：本教學課程使用可能會產生費用 AWS 的服務。如需目前的定價，請參閱 AWS 網站上的 [AWS Network Security Manager 定價](#)。

先決條件

開始之前，請確認您符合下列要求：

- 已完成設定步驟，如 中所述[設定 AWS Network Security Manager](#)。
- 具有 AWS Network Security Manager 許可的 AWS Identity and Access Management (IAM) 身分。
- 已啟用所有功能的 AWS Organizations 組織，以及指定的 AWS Network Security Manager 管理員帳戶（多帳戶部署需要）。
- 存取 AWS Network Security Manager 主控台。

步驟 1：建立規則

規則是您安全組態的建置區塊。在此步驟中，您會建立兩個 AWS WAF 規則：一個用於設定預設動作，另一個用於設定可見性組態。預設動作和 VisibilityConfig 是 AWS WAF Web ACL 的必要欄位。

若要建立預設動作規則，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/network-security-manager/> 開啟 AWS Network Security Manager 主控台。
2. 在導覽窗格中，選擇概觀。
3. 在概觀頁面上，選擇建立規則。
4. 針對規則名稱，輸入描述性名稱，例如 my-default-action-rule。
5. 在規則定義區段中，針對防火牆類型選擇 AWS WAF。
6. 針對選取規則類型，選擇組態。
7. 選擇插入組態類型，然後選擇預設動作。JSON 編輯器會顯示預設組態。
8. 在 JSON 編輯器中，移除 Block 區段並僅保留 Allow 區段。
9. 選擇建立規則。

若要建立 VisibilityConfig 規則，請遵循下列步驟：

1. 在導覽窗格中，選擇概觀。
2. 在概觀頁面上，選擇建立規則。
3. 針對規則名稱，輸入描述性名稱，例如 my-visibility-config-rule。
4. 在規則定義區段中，針對防火牆類型選擇 AWS WAF。
5. 針對選取規則類型，選擇組態。
6. 選擇插入組態類型，然後選擇 VisibilityConfig。JSON 編輯器會顯示預設組態。
7. 選擇建立規則。

AWS CLI 替代方案

您也可以使用 CLI AWS 建立規則：

```
aws network-security-manager create-rule \  
  --rule-name "my-default-action-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"DefaultAction": {"Allow": {}}}' \  
  --is-published true  
  
aws network-security-manager create-rule \  
  --rule-name "my-visibility-config-rule" \  
  --firewall-type WAF \  
  --rule-type VISIBILITY_CONFIG
```

```
--rule-type CONFIGURATION \  
--configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true,  
"CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \  
--is-published true
```

步驟 2：建立範本

範本會將一或多個規則分組，以便跨政策重複使用。在此步驟中，您會建立範本，其中包含步驟 1 的規則：

1. 在導覽窗格中，選擇概觀。
2. 在概觀頁面上，選擇建立範本。
3. 針對範本名稱，輸入描述性名稱，例如 my-waf-template。
4. 針對防火牆類型，選擇 AWS WAF。
5. 在規則區段中，選擇新增規則，然後選取您在步驟 1 中建立的規則。
6. 選擇建立範本。

AWS CLI 替代方案

您也可以使用 CLI AWS 建立範本：

```
aws network-security-manager create-template \  
--template-name "my-waf-template" \  
--firewall-type WAF \  
--associated-rule-list '["ruleIdentifier": "rule-arn-from-step-1"]' \  
--is-published true
```

步驟 3：建立政策

政策結合 範本與強制執行設定。在此步驟中，您會建立參考範本並啟用自動修復的政策：

1. 在導覽窗格中，選擇概觀。
2. 在概觀頁面上，選擇建立政策。
3. 針對政策名稱，輸入描述性名稱，例如 my-waf-policy。

- 針對防火牆類型，選擇 AWS WAF。
- 在政策優先順序區段中，會顯示現有政策及其優先順序。檢閱新政策的優先順序。如果您需要調整，請選擇優先順序欄位，並將值變更為 1 或任何未使用的優先順序編號。
- 在範本和規則區段中，選擇新增範本，然後選取您在步驟 2 中建立的範本。
- 針對修復，選取已啟用。
- 針對現有客戶 Web ACL 解決方案，選擇無修補。
- 選擇建立政策。

AWS CLI 替代方案

您也可以使用 CLI AWS 建立政策：

```
aws network-security-manager create-policy \  
  --policy-name "my-waf-policy" \  
  --firewall-type WAF \  
  --priority 1 \  
  --associated-template-and-rule-list '["templateIdentifier": "template-arn-  
from-step-2"]]' \  
  --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":  
false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \  
  --is-published true
```

步驟 4：建立範圍

範圍會定義您的保護套用的位置。在此步驟中，您會建立以帳戶中 Application Load Balancer 為目標的範圍：

- 在導覽窗格中，選擇概觀。
- 在概觀頁面上，選擇建立範圍。
- 針對範圍名稱，輸入描述性名稱，例如 my-alb-scope。
- （選用）在帳戶和組織單位選取區段中，針對控制管理範圍的選取方法，選取範圍到整個 AWS 組織（所有 OUs 和帳戶）。略過此步驟以進行單一帳戶部署。
- 在資源區段中，針對資源類型，選取 Application Load Balancer。
- 選擇 Create scope (建立範圍)。

AWS CLI 替代方案

您也可以使用 CLI AWS 建立範圍：

```
aws network-security-manager create-scope \  
  --scope-name "my-alb-scope" \  
  --scope-configuration '{  
    "accountFilter": {"includeAll": {}},  
    "resourceScopes": {  
      "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {  
        "includeAll": true  
      }  
    }  
  }' \  
  --is-published true
```

步驟 5：建立和發佈部署

部署會將政策繫結至範圍，並啟用強制執行。若要建立和發佈部署：

1. 在導覽窗格中，選擇概觀。
2. 在概觀頁面上，選擇建立部署。
3. 針對部署名稱，輸入描述性名稱，例如 my-first-deployment。
4. 在政策區段中，選擇新增政策，然後選取您在步驟 3 中建立的政策。
5. 在範圍區段中，選擇新增範圍，然後選取您在步驟 4 中建立的範圍。
6. 選擇 Create deployment (建立部署)。

AWS Network Security Manager 會開始探索資源並套用保護。此程序是非同步的，可能需要幾分鐘的時間才能完成。

AWS CLI 替代方案

您也可以使用 CLI AWS 建立和發佈部署：

```
aws network-security-manager create-deployment \  
  --deployment-name "my-first-deployment" \  
  --policy-name "my-policy" \  
  --scope-name "my-alb-scope" \  
  --is-published true
```

```
--associated-policy-list ' [{"policyIdentifier": "policy-arn-from-step-3"}]' \
--associated-scope-list ' [{"scopeIdentifier": "scope-arn-from-step-4"}]' \
--deployment-configuration '{"enableCrossAccountVisibility": true}' \
--is-published true
```

步驟 6：監控同步狀態

發佈部署之後，AWS Network Security Manager 會探索資源並同步其組態。若要監控每個資源的狀態：

1. 在導覽窗格中，選擇概觀。
2. 選擇 Deployment (部署) 索引標籤。
3. 選擇您在步驟 5 中建立的部署。
4. 選擇同步索引標籤。
5. 檢閱每個資源的同步狀態：
 - IN_SYNC – 資源組態符合您預期的保護設定。
 - OUT_OF_SYNC – 資源組態不相符。啟用修復時，AWS Network Security Manager 會自動修復此問題。
 - NOT_APPLICABLE – 資源在範圍內，但無法由此部署評估。

AWS CLI 替代方案

您也可以使用 CLI AWS 檢查同步狀態：

```
aws network-security-manager list-resource-synchronization-statuses \
--deployment-identifier "deployment-arn-from-step-5"
```

步驟 7：清除

如果您不再需要您建立的資源，請以相反順序刪除它們，以停止強制執行並移除範圍內資源的保護：

相反的順序很重要，因為這些資源彼此參考。若要在刪除資源之前查看與資源相關聯的內容，請 `ListResourceAssociations` 呼叫該資源的 ARN。它會傳回每個相關聯資源的 ARN 和資源類型。如需詳細資訊，請參閱 [AWS Network Security Manager API 參考](#)。

1. 在導覽窗格中，選擇概觀。選擇 Deployment (部署) 索引標籤。選取您的部署，選擇動作，然後選擇刪除。
2. 選擇範圍索引標籤。選取您的範圍，選擇動作，然後選擇刪除。
3. 選擇 Policies (政策) 標籤。選取您的政策，選擇動作，然後選擇刪除。
4. 選擇範本索引標籤。選取您的範本，選擇動作，然後選擇刪除。
5. 選擇規則標籤。選取您的規則，選擇動作，然後選擇刪除。

AWS CLI 替代方案

在您刪除資源之前，請檢查其關聯以規劃刪除順序：

```
aws network-security-manager list-resource-associations \
  --resource-arn "resource-arn"
```

如果資源仍有關聯，請先移除或刪除相關聯的資源。

您可以使用 CLI AWS 以相反順序刪除資源：

```
aws network-security-manager delete-deployment \
  --deployment-identifier "deployment-arn"

aws network-security-manager delete-scope \
  --scope-identifier "scope-arn"

aws network-security-manager delete-policy \
  --policy-identifier "policy-arn"

aws network-security-manager delete-template \
  --template-identifier "template-arn"

aws network-security-manager delete-rule \
  --rule-identifier "rule-arn"
```

後續步驟

現在您已有可運作的部署，請探索下列方式來擴展網路安全保護：

- 了解 中的資源模型和生命週期 [AWS Network Security Manager 的運作方式](#)。
- 使用草稿/發佈工作流程在變更生效之前進行階段變更。如需詳細資訊，請參閱 [the section called “草稿和作用中生命週期”](#)。
- 建立快照以保留已知良好的組態。如需詳細資訊，請參閱 [the section called “版本控制”](#)。
- 使用 從自然語言描述GenerateRuleConfiguration建立規則。如需詳細資訊，請參閱 [AWS Network Security Manager API 參考](#)。
- 探索管理整個組織的 AWS WAF 和 AWS Shield Advanced 保護。如需詳細資訊，請參閱 [管理防火牆和安全服務](#)。

管理防火牆和安全服務

使用 AWS Network Security Manager，您可以定義和部署多個防火牆和安全服務的安全政策。雖然常見元素跨越 AWS 網路安全產品組合，但您需要在 AWS Network Security Manager 中解決的重要變化存在。

對於每個支援的網路安全服務，以下子節描述快速建立和標準詳細建立程序的唯一元素和步驟。

管理 AWS WAF ACLs

使用 AWS Network Security Manager，您可以集中設定和部署組織中帳戶和資源的 AWS WAF Web 存取控制清單 (Web ACLs)。您可以定義 AWS WAF 的 AWS Network Security Manager 規則，將其分組為保護範本，並透過 AWS Network Security Manager 政策和部署大規模強制執行這些規則。

AWS WAF 概念

下列概念專屬於搭配 AWS WAF 使用 AWS Network Security Manager。如需 AWS Network Security Manager 運作方式的詳細資訊，請參閱 [AWS Network Security Manager 的運作方式](#)。

AWS WAF 規則類型

對於 AWS WAF，規則是兩種類型之一：

- INSPECTION – 包含使用 PreProcessFirewallManagerRuleGroups (在客戶定義規則之前執行的規則) 或 PostProcessFirewallManagerRuleGroups (在之後執行的規則) 的規則群組定義。
- CONFIGURATION – 包含單一 Web ACL 組態設定。組態 JSON 必須僅包含符合支援設定的頂層金鑰 (例如 Description、DefaultAction、VisibilityConfig、LoggingConfiguration、CaptchaConfig、TokenDomains 或 MonetizationConfig)。

大多數 Web ACL 組態設定對應至 AWS WAF CreateWebACL 操作的參數。如需這些設定及其定義的詳細資訊，請參閱 AWS WAF API 參考中的 [CreateWebACL](#)。

例外是 LoggingConfiguration，您可以分別設定。如需詳細資訊，請參閱 [the section called “記錄”](#)。

AWS WAF 政策合併

對於 AWS WAF，每個組態設定使用下列其中一個合併策略：

SingleValue

只能有一個值的設定。最高優先順序政策獲勝。優先順序值是唯一的，因此兩個政策無法以相同的優先順序定義不同的值。如需 AWS Network Security Manager 如何解決優先順序的詳細資訊，請參閱 [the section called “優先順序型政策合併”](#)。下列設定使用 SingleValue：DefaultAction、VisibilityConfig、CaptchaConfig、ChallengeConfig、OnS MonetizationConfig 和 Description。

附加（和 AppendAndSort）

所有政策的項目會依優先順序附加至清單。TokenDomains 和 DataProtectionConfig.DataProtections 使用附加。PreProcessFirewallManagerRuleGroups 和 PostProcessFirewallManagerRuleGroups 使用 AppendAndSort，這會附加所有政策的規則群組，並依優先順序排序。排序很重要，因為 AWS WAF 會循序評估規則群組。

Merge

無論優先順序為何，所有政策的項目都會合併為單一集合。CustomResponseBodies 和 AssociationConfig.RequestBody 使用合併。

附加、AppendAndSort 和合併策略會移除重複的項目。當兩個政策提供相同的組態時，AWS Network Security Manager 會保留較高優先順序政策中的項目。因此，有效組態包含該項目的一個副本，而不是每個貢獻政策一個副本。

現有的 Web ACL 解析度

使用 AWS WAF 政策上的 existingCustomerWebACLResolution 設定，指定 AWS Network Security Manager 如何處理已有客戶受管 Web ACL 的資源：

- RETROFIT – 更新現有的 Web ACL，以符合有效的組態。
- OVERRIDE_ASSOCIATION – 改為將 AWS Network Security Manager 管理的 Web ACL 與資源建立關聯。
- NO_REMEDIATION – 如果您的 Web ACL 存在，請勿修復。

記錄 Web ACL 流量

您可以使用政策上的 `LoggingConfiguration` 設定來控制 Web ACL 記錄。AWS Network Security Manager 會使用 AWS WAF `PutLoggingConfiguration` 操作套用此設定。您可以為每個 Web ACL 定義一個記錄目的地。如需詳細資訊，請參閱 AWS WAF API 參考中的 [PutLoggingConfiguration](#)。

政策管理的每個範圍內 Web ACL 都會將其日誌傳送至政策指定的目的地。這可讓您集中記錄組織中的各個帳戶。使用它來取得 Web ACLs 分析整個組織之流量的詳細資訊。

若要跨多個帳戶集中記錄，您可以將日誌傳送至 Amazon S3 儲存貯體或 Amazon Data Firehose 交付串流。每個目的地類型都需要額外的組態，您必須先完成這些組態，AWS Network Security Manager 才能管理跨範圍內資源和帳戶的 AWS WAF 記錄。目的地名稱必須以開頭 `aws-waf-logs-`。

Amazon Data Firehose

建立具有下列特性的交付串流：

- 使用您的 AWS Network Security Manager 管理員帳戶建立
- 以開頭的名稱 `aws-waf-logs-`，例如 `aws-waf-logs-network-security-manager-central`
- PUT 來源
- 在您操作的區域中建立，或者如果您擷取 Amazon CloudFront 的日誌，則在美國東部（維吉尼亞北部）區域中建立

使用交付串流之前，請先進行測試，確認它有足夠的輸送量可供組織日誌使用。如需詳細資訊，請參閱 [《Amazon Data Firehose 開發人員指南》](#) 中的 [建立 Amazon Data Firehose 交付串流](#)。

Amazon S3

遵循 AWS WAF 開發人員指南中的 Amazon S3 指引建立儲存貯體。您也必須使用允許日誌交付寫入的許可來設定儲存貯體。下列儲存貯體政策會授予這些許可。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForNetworkSecurityManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3::aws-waf-logs-bucket-suffix"
},
{
    "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/
*\"",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
]
}

```

將儲存####取代為您自己的儲存貯體名稱尾碼，並將 *policy-id* 取代為政策的 ID。

CloudWatch Logs 僅支援單一帳戶使用

如果您跨多個帳戶使用 AWS Network Security Manager，則無法使用 Amazon CloudWatch Logs 日誌群組做為記錄目的地。日誌群組必須位於與 Web ACL 相同的 AWS 帳戶和相同區域。對於多帳戶部署，請改用 Amazon S3 儲存貯體或 Amazon Data Firehose 交付串流。

快速建立 AWS WAF

使用快速建立，您可以在單一引導式工作流程中定義和部署 AWS WAF 保護。當您想要在單一工作階段中透過部署設定規則的完整 Web ACL 保護時，請使用 Quick Create。

若要使用 Quick Create 定義和部署 AWS WAF 保護，請依序完成下列程序。

建立政策並新增保護

1. 在 <https://console.aws.amazon.com/network-security-manager/> 開啟 AWS Network Security Manager 主控台。
2. 在導覽窗格中，選擇概觀。
3. 在概觀頁面的右上角，選擇快速建立和部署。快速建立和部署頁面會顯示多個窗格。
4. 在政策詳細資訊窗格中，針對名稱輸入政策名稱。在描述，請輸入描述。
5. 在定義保護窗格中，選擇您要使用的防火牆類型。選取 AWS WAF。範本和規則子窗格隨即出現，您可以在其中新增規則或範本。
6. 若要新增規則，請選擇新增或管理規則。在出現的視窗中，針對選取規則類型，選擇下列其中一項：
 - AWS 受管規則 – 資料表顯示 AWS WAF 支援的所有 AWS 受管規則。
 - 規則 – 此資料表顯示您擁有的 AWS WAF 規則群組，但 AWS 受管規則除外。

選取您要新增至政策之規則的核取方塊。然後選擇新增規則。

7. 若要新增範本，請選擇新增範本。在出現的新增範本視窗中，資料表會顯示任何可用的範本。選取您想要的範本，以及要包含在政策中的版本。然後選擇新增範本。

設定政策

1. 在範本和規則表格中檢閱您的選擇。Position 欄中的整數決定規則和範本的評估順序。若要變更評估順序，請在位置欄中選擇位置值。使用箭頭變更值。若要接受變更，請選擇確認。若要還原變更，請選擇取消。
2. 在定義保護窗格中的政策組態下，決定 AWS Network Security Manager 在目標範圍內採取的自動化動作：
 - 修復會將定義的政策套用至安全狀態未與 AWS Network Security Manager 中所述的所需狀態同步的任何資源。
 - 資源清除會在移除部署或帳戶或資源超出範圍時，刪除 AWS Network Security Manager 為資源建立的防火牆。
 - 現有的客戶 WebACL 解決方案會決定如何解決您正在定義的政策與可能已部署的政策之間的衝突。從功能表中，選擇下列其中一個選項：
 - 沒有任何補救措施會略過任何已擁有 Web ACL 資源的補救措施。
 - 覆寫關聯會將現有的 Web ACL 取代為 AWS Network Security Manager 建立的 Web ACL。
 - 改造會將其規則修改到每個現有的 Web ACL，並保持與資源相關聯的 Web ACL。

3. 在政策優先順序窗格中，設定優先順序。AWS Network Security Manager 會根據政策的優先順序來評估政策，以解決衝突。較低的位置（較低的整數）具有較高的優先順序。若要編輯優先順序，請選擇位置值。然後使用箭頭遞增，或直接輸入值。若要確認選擇，請選擇確認。若要捨棄變更，請選擇取消。

設定範圍

1. 在設定範圍窗格中，定義政策套用的資產集。針對範圍名稱，輸入名稱。在描述，請輸入描述。

2.

僅限多帳戶模式

此步驟僅適用於多帳戶模式。在多帳戶模式中，使用帳戶和組織單位選取子窗格來選擇要包含或排除的帳戶或 OUs。在單一帳戶模式中，此子窗格不會出現在主控台中，因此請略過此步驟。

在帳戶和組織單位選取子窗格中，選取下列其中一個選項：

- 整個 AWS 組織的範圍。不需要進一步定義。
 - 範圍涵蓋整個 AWS 組織，但排除特定 OUs 和帳戶。組織單位子窗格和帳戶子窗格隨即出現。若要排除組織單位，請選擇新增 OUs。選取組織樹狀目錄中的組織單位，然後選擇新增 OUs。若要排除個別帳戶，請選擇新增帳戶。選取組織樹狀目錄中的帳戶，然後選擇新增帳戶。
 - 請勿限制為整個 AWS 組織，且僅包含特定的 OUs 和帳戶。使用相同的新增 OUs 和新增帳戶機制來包含您想要的組織單位和帳戶。
3. 在資源子窗格中，針對資源類型，選取所有或特定 AWS WAF 資源類型。這些選項是下列一或多個項目：
- Application Load Balancer
 - Amazon API Gateway REST API
 - CloudFront 分佈

CloudFront 區域需求

若要保護 CloudFront 分佈資源，請使用美國東部（維吉尼亞北部）區域 (us-east-1)。

全域和區域資源類型

您可以選取全域資源類型 (CloudFront Distribution) 或區域資源類型 (Application Load Balancer 和 Amazon API Gateway REST API)，但不能同時選取兩者。選取資源類型後，您無法在更新組態時切換 CloudFront Distribution 和區域資源類型。

未受管 CloudFront 資源

AWS Network Security Manager 不會管理使用 CloudFront 固定費率定價計劃或 CloudFront 預備分佈的 CloudFront 分佈。這些資源出現不同步。

4. 針對每個選取的資源類型，選擇下列其中一個互斥選項：

- 包含所有資源
- 包含特定資源
- 排除特定資源

5. 如果您選擇包含特定資源，請選擇下列其中一種表達式類型，然後建置適當的標籤或 ARNs 組合：

- 單一條件
- 符合所有條件 (AND)
- 符合任何條件 (OR)
- NOT

所有資源類型都有標籤和 ARN 納入標準。如果您選擇標籤，請輸入金鑰和選用值。您可以識別多個標籤。如果您的資源類型是 Application Load Balancer，則會顯示額外的組態條件。在組態中，選擇具有面向網際網路或內部選項的結構描述。

檢閱和部署政策

1. 在檢閱和部署窗格中，針對部署名稱輸入名稱。在描述，請輸入描述。若要判斷您組織中的其他帳戶是否可看見部署的內容，請選取啟用此部署的跨帳戶可見性。
2. (選用) 若要將標籤新增至資源，請選擇新增標籤，然後輸入金鑰和選用值組合。
3. 若要執行您定義的內容，請選擇建立和部署。程序完成時，會顯示部署頁面，您可以在其中查看所建立項目的詳細資訊。

部署可能會產生費用

部署會建立網路安全服務，並將其連接到受保護的資源。AWS Network Security Manager 會收取受保護資源的費用。安全服務本身會保護資源，這會產生額外費用。部署之前，請檢閱 [AWS Network Security Manager 定價頁面](#) 和 [AWS WAF 定價頁面](#)。

AWS WAF 的標準建立程序

使用標準建立程序，您可以個別建立每個 AWS WAF 元件 - 規則、範本、政策、範圍和部署 - 以進行完全控制。當您想要建立可重複使用的元件並視需要結合它們時，請使用此方法。

AWS Network Security Manager AWS WAF 政策可以包含規則和範本。當您套用政策時，AWS Network Security Manager 會在每個範圍內帳戶中建立 Web ACL。

建立規則 (主控台)

1. 使用您的 AWS Network Security Manager 管理員帳戶登入 AWS 管理主控台，然後開啟位於 <https://console.aws.amazon.com/network-security-manager/> 的 AWS Network Security Manager 主控台。

管理員帳戶設定

如需設定 AWS Network Security Manager 管理員帳戶的資訊，請參閱 [設定 AWS Network Security Manager](#)。

2. 在導覽窗格中，選擇 AWS 網路安全管理員，然後選擇概觀。
3. 在概觀窗格中，選擇建立規則。輸入描述性名稱，然後輸入選用的描述。
4. 在規則定義窗格中，針對防火牆類型，選擇 AWS WAF。
5. 針對規則類型，選擇檢查或組態。

如果您選擇檢查，則會出現名為定義規則群組參考的 JSON 編輯器窗格，其中包含下列選項：

- 插入範本 – 為第一個（預處理）規則或最後一個（後處理）規則選取 JSON 範本。當您進行選擇時，AWS Network Security Manager 會將對應的 JSON 插入編輯器，如果需要輸入才能完成範本，則會一併插入警告圖示。
- 插入規則群組 – 顯示由三個選項驅動的選擇清單：

- AWS 受管規則 (AMR) 規則群組
- 現有的自訂規則群組
- AWS Marketplace 規則群組

AWS Network Security Manager 會顯示與您選擇相關聯的規則群組，而且您可以選擇單一執行個體來包含。進行選擇後，請選擇選取規則群組。AWS Network Security Manager 會將具有正確語法的檢查規則參考插入 JSON 編輯器。

- 使用 AI 插入 – 開啟名為 AI 組態產生器的浮水印視窗。使用此工具以純語言描述您的規則，AWS Network Security Manager 會在編輯器中產生相關聯的 JSON。然後，您可以檢閱產生的程式碼，並選擇接受、修改或刪除輸出。
6. (選用) JSON 規則定義完成後，您可以將標籤與規則建立關聯。選擇 Add new tag (新增標籤)，然後輸入 Key (索引鍵) 和選用的 Value (值)。
 7. 當您完成定義時，請選擇儲存草稿以儲存非作用中、可能不完整的物件，或建立規則。

Web ACL 名稱為永久性

您無法在建立 Web ACL 名稱之後對其進行變更。如果您更新政策的名稱，AWS Network Security Manager 不會更新相關聯的 Web ACL 名稱。若要讓 AWS Network Security Manager 建立不同名稱的 Web ACL，您必須建立新的政策。

建立範本 (主控台)

範本會依優先順序組合規則，以在政策中進行評估。您可以將規則類型組織成符合安全目標的群組。您也可以讓不同的團隊建置符合其責任和技能的安全控制陳述式。

1. 在概觀頁面上的概觀窗格中，選擇建立範本。在建立範本頁面上，輸入範本名稱，輸入選用的描述，然後選擇防火牆類型 (在此情況下為 AWS WAF)。
2. 當您選擇防火牆類型時，會顯示規則窗格。選擇兩個新增規則按鈕之一，以開啟可用規則的清單。選取規則名稱左側的核取方塊，將其新增至範本。若要選擇規則的特定版本，請選取規則的版本欄位。如果有多個版本可用，請選取您想要的版本，然後選擇確認。
3. (選用) 建立範本的標籤。完成後，請選擇儲存草稿或建立範本。若要繼續建立政策，請選擇建立範本。

建立 政策 (主控台)

這是政策定義和準備部署的最後一步。

1. 在概觀頁面上的概觀窗格中，選擇建立政策。在建立政策頁面上，輸入名稱和選用的描述，然後選擇防火牆類型（在此情況下為 AWS WAF）。
2. 在政策優先順序窗格中，設定優先順序。AWS Network Security Manager 會根據政策的優先順序來評估政策，以解決衝突。較低的位置（較低的整數）具有較高的優先順序。若要編輯優先順序，請選擇位置值。然後使用箭頭遞增，或直接輸入值。若要確認選擇，請選擇確認。若要捨棄變更，請選擇取消。
3. 在政策組態窗格中，決定 AWS Network Security Manager 在目標範圍內採取的自動化動作：
 - 修復會將定義的政策套用至安全狀態未與 AWS Network Security Manager 中所述的所需狀態同步的任何資源。
 - 資源清除會在移除部署或帳戶或資源超出範圍時，刪除 AWS Network Security Manager 為資源建立的防火牆。
 - 現有的客戶 WebACL 解決方案會決定如何解決您正在定義的政策與可能已部署的政策之間的衝突。從功能表中，選擇下列其中一個選項：
 - 沒有任何補救措施會略過任何已擁有 Web ACL 資源的補救措施。
 - 覆寫關聯會將現有的 Web ACL 取代為 AWS Network Security Manager 建立的 Web ACL。
 - 改造會將其規則修改到每個現有的 Web ACL，並保持與資源相關聯的 Web ACL。
4. 這些組態設定完成後，請選取您要新增至政策的規則和範本。在範本和規則窗格中，選擇新增規則或新增範本以填入政策。這兩個程序都會開啟一個視窗，其運作方式與本節先前所述的規則選擇程序相同。

建立範圍（主控台）

1. 您可以從概觀頁面或工具中的其他區域開始此步驟。在範圍詳細資訊窗格中，輸入範圍名稱和選用的描述。

2. 僅限多帳戶模式

此步驟僅適用於多帳戶模式。在多帳戶模式中，使用帳戶和組織單位選取子窗格來選擇要包含或排除的帳戶或 OUs。在單一帳戶模式中，此子窗格不會出現在主控制台中，因此請略過此步驟。

在帳戶和組織單位選取窗格中，選擇控制管理範圍的三種方法之一：

- 整個 AWS 組織的範圍（所有 OUs 和帳戶） – 不需要進一步定義。
 - 範圍涵蓋整個 AWS 組織，但排除特定 OUs 和帳戶 – 出現兩個子窗格，一個用於組織單位，另一個用於帳戶。選擇新增 OUs 以開啟新增 OUs 視窗，從組織樹狀目錄中選取您需要的組織單位，然後選擇新增 OUs。若要新增個別帳戶，請在帳戶子窗格中選擇新增帳戶、從組織樹狀目錄中選取帳戶，然後選擇新增帳戶。
 - 請勿限制為整個 AWS 組織，只包含特定 OUs 和帳戶 – 使用相同的子窗格來新增具有上述選項所述相同機制的 OUs 或帳戶。
3. 接著，在資源子窗格中選取資源。在資源類型選擇方塊中，選取所有或特定 AWS WAF 資源類型。對於 AWS WAF，選項包括下列任何或所有項目：
- Application Load Balancer
 - Amazon API Gateway REST API
 - CloudFront 分佈

CloudFront 區域需求

若要保護 CloudFront 分佈資源，請使用美國東部（維吉尼亞北部）區域 (us-east-1)。

全域和區域資源類型

您可以選取全域資源類型 (CloudFront Distribution) 或區域資源類型 (Application Load Balancer 和 Amazon API Gateway REST API)，但不能同時選取兩者。選取資源類型後，您無法在更新組態時切換 CloudFront Distribution 和區域資源類型。

未受管 CloudFront 資源

AWS Network Security Manager 不會管理使用 CloudFront 固定費率定價計劃或 CloudFront 預備分佈的 CloudFront 分佈。這些資源出現不同步。

4. 針對每個選取的資源類型，選擇下列其中一個互斥選項：
- 包含所有資源
 - 包含特定資源
 - 排除特定資源
5. 如果您選擇包含特定資源，請選取下列其中一個表達式類型：

- 單一條件
 - 符合所有條件 (AND)
 - 符合任何條件 (OR)
 - NOT
6. 每個表達式類型都支援單一或多個納入標準和 ARNs，因此您可以建置標籤或 ARNs 的組合。所有資源類型都支援標籤和 ARN 納入標準。如果您選擇標籤，請識別金鑰和選用值。您可以識別多個標籤。
 7. 對於 Application Load Balancer，會顯示額外的組態條件。在組態中，您可以使用面向網際網路或內部的選項來設定結構描述。

建立部署（主控台）

部署會將您的政策繫結至範圍，並啟用強制執行，這會導致 AWS Network Security Manager 將您的 AWS WAF 規則套用至範圍內資源。

1. 在概觀頁面上的概觀窗格中，選擇建立部署。您也可以從工具中的其他區域開始此步驟。
2. 選擇您要部署的政策。
3. 選擇定義 AWS Network Security Manager 套用政策之帳戶和資源的範圍。
4. 針對部署名稱，輸入名稱。在描述，請輸入描述。
5. （選用）若要讓組織中的其他帳戶可看見部署，請選取為此部署啟用跨帳戶可見性。
6. （選用）若要新增標籤，請選擇新增標籤，然後輸入金鑰和選用值組合。
7. 選擇 Create and deploy (建立和部署)。部署頁面隨即出現，您可以在其中查看 AWS Network Security Manager 建立項目的詳細資訊。

部署可能會產生費用

部署會建立網路安全服務，並將其連接到受保護的資源。AWS Network Security Manager 會收取受保護資源的費用。安全服務本身會保護資源，這會產生額外費用。部署之前，請檢閱 [AWS Network Security Manager 定價頁面](#) 和 [AWS WAF 定價頁面](#)。

管理 Shield Advanced AWS 的 DDoS 保護

使用 AWS Network Security Manager，您可以集中設定和部署組織中帳戶和資源的 AWS Shield Advanced 保護。您可以定義 DDoS 保護政策，並透過 AWS Network Security Manager 政策和部署大規模強制執行這些政策。

AWS Network Security Manager 會另外計費

AWS Network Security Manager 不屬於 AWS Shield Advanced 優惠的一部分。如需定價的詳細資訊，請參閱 [AWS Network Security Manager 定價](#) 和 [AWS Shield Advanced 定價](#)。

AWS Shield Advanced 訂閱

當作用中部署包含其範圍內的帳戶時，AWS Network Security Manager 會將該帳戶訂閱 AWS Shield Advanced。當帳戶離開範圍或移除部署時，AWS Network Security Manager 不會取消訂閱。若要取消 AWS Shield Advanced 訂閱，請參閱 AWS WAF 開發人員指南中的 [訂閱 AWS Shield Advanced](#)。

Shield Advanced AWS 的快速建立

使用 Quick Create，您可以在單一引導式工作流程中定義和部署 AWS Shield Advanced 保護。當您想要在單一工作階段中透過部署設定政策的 DDoS 保護時，請使用 Quick Create。

若要使用 Quick Create 定義和部署 AWS Shield Advanced 保護，請依序完成下列程序。

建立政策並設定保護

請完成下列步驟：

1. 開啟位於 <https://console.aws.amazon.com/network-security-manager/> 的 AWS Network Security Manager 主控台。
2. 在導覽窗格中，選擇概觀。
3. 在概觀頁面上，選擇快速建立和部署。快速建立和部署頁面會顯示多個窗格。
4. 在政策詳細資訊窗格中，針對名稱輸入政策名稱。在描述，請輸入描述。

5. 在定義保護窗格中，選擇您要使用的防火牆類型。選取 AWS Shield Advanced。
6. 在定義保護窗格中的政策組態下，決定 AWS Network Security Manager 在目標範圍內採取的自動化動作：
 - 修復會將定義的政策套用至安全狀態與 AWS Network Security Manager 描述的所需狀態不相符的任何資源。
 - 資源清除會在移除部署或帳戶或資源超出範圍時，刪除 AWS Network Security Manager 為資源建立的 DDoS 保護。
 - 現有的客戶 DDoS 解決方案會決定如何解決您正在定義的政策與可能已部署的政策之間的衝突。從功能表中，選擇下列其中一個選項：
 - 沒有任何補救措施會略過任何已具有 DDoS 保護之資源的補救措施。
 - 覆寫關聯會將現有的 DDoS 保護取代為 AWS Network Security Manager 建立的 DDoS 保護。
 - 改造會將其規則修改到每個現有的 DDoS 保護，並保持與資源相關聯的 DDoS 保護。
7. 在政策優先順序窗格中，設定優先順序。AWS Network Security Manager 會根據政策的優先順序來評估政策，以解決衝突。較低的位置（較低的整數）具有較高的優先順序。

若要編輯優先順序，請選擇位置值。然後使用箭頭遞增，或直接輸入值。若要確認選擇，請選擇確認。若要捨棄變更，請選擇取消。

設定範圍

請完成下列步驟：

1. 在設定範圍窗格中，定義政策套用的資產集。針對範圍名稱，輸入名稱。在描述，請輸入描述。

2.  僅限多帳戶模式

此步驟僅適用於多帳戶模式。在多帳戶模式中，使用帳戶和組織單位選取子窗格來選擇要包含或排除的帳戶或 OUs。在單一帳戶模式中，此子窗格不會出現在主控台中，因此請略過此步驟。

在帳戶和組織單位選取子窗格中，選取下列其中一個選項：

- 整個 AWS 組織的範圍。不需要進一步定義。
- 範圍涵蓋整個 AWS 組織，但排除特定 OUs 和帳戶。組織單位子窗格和帳戶子窗格隨即出現。若要排除組織單位，請選擇新增 OUs。選取組織樹狀目錄中的組織單位，然後選擇新增 OUs。若要排除個別帳戶，請選擇新增帳戶。選取組織樹狀目錄中的帳戶，然後選擇新增帳戶。

- 請勿範圍涵蓋整個 AWS 組織，只包含特定的 OUs 和帳戶。使用相同的新增 OUs 和新增帳戶機制來包含您想要的組織單位和帳戶。
3. 在資源子窗格中，針對資源類型，選取所有或特定 AWS Shield Advanced 資源類型。這些選項是下列一或多個項目：
 - Application Load Balancer
 - CloudFront 分佈
 - Classic Load Balancer
 - 彈性 IP 地址
 4. 針對每個選取的資源類型，選擇下列其中一個互斥選項：
 - 包含所有資源
 - 包含特定資源
 - 排除特定資源
 5. 如果您選擇包含特定資源，請選擇下列其中一種表達式類型，然後建置適當的標籤或 ARNs 組合：
 - 單一條件
 - 符合所有條件 (AND)
 - 符合任何條件 (OR)
 - NOT

所有資源類型都有標籤和 ARN 納入標準。如果您選擇標籤，請輸入金鑰和選用值。您可以識別多個標籤。

CloudFront 區域需求

若要保護 CloudFront 分佈資源，請使用美國東部（維吉尼亞北部）區域 (us-east-1)。

檢閱和部署政策

請完成下列步驟：

1. 在檢閱和部署窗格中，針對部署名稱輸入名稱。在描述，請輸入描述。若要判斷您組織中的其他帳戶是否可看見部署的內容，請選取啟用此部署的跨帳戶可見性。
2. （選用）若要將標籤新增至資源，請選擇新增標籤，然後輸入金鑰和選用值組合。

- 若要建立和部署政策和範圍，請選擇建立和部署。程序完成時，會顯示部署頁面，您可以在其中查看 AWS Network Security Manager 建立項目的詳細資訊。

部署可能會產生費用

部署會建立網路安全服務，並將其連接到受保護的資源。AWS Network Security Manager 會收取受保護資源的費用。安全服務本身會保護資源，這會產生額外費用。部署之前，請檢閱 [AWS Network Security Manager 定價頁面](#) 和 [AWS Shield Advanced 定價頁面](#)。

Shield Advanced AWS 的標準建立程序

使用標準建立程序，您可以個別設定每個 AWS Shield Advanced 元件 - 政策、範圍和部署，以獲得完全控制。當您想要建立可重複使用的元件並視需要結合它們時，請使用此方法。

Shield Advanced AWS 政策很簡單，不包含規則、規則群組或範本。當您套用政策時，AWS Network Security Manager 會在每個範圍內帳戶中建立 AWS Shield Advanced DDoS 保護。如需 AWS Network Security Manager 運作方式的相關資訊，請參閱 [AWS Network Security Manager 的運作方式](#)。

建立 政策 (主控台)

請完成下列步驟：

- 使用您的 AWS Network Security Manager 管理員帳戶登入 AWS 管理主控台，然後開啟位於 <https://console.aws.amazon.com/network-security-manager/> 的 AWS Network Security Manager 主控台。

管理員帳戶設定

如需設定 AWS Network Security Manager 管理員帳戶的資訊，請參閱 [設定 AWS Network Security Manager](#)。

- 在導覽窗格中，選擇 AWS 網路安全管理員，然後選擇概觀。
- 在概觀窗格中，選擇建立政策。輸入名稱和選用的描述，然後選擇防火牆類型（在此情況下為 AWS Shield Advanced）。
- 在政策優先順序窗格中，設定優先順序。AWS Network Security Manager 會根據政策的優先順序來評估政策，以解決衝突。較低的位置（較低的整數）具有較高的優先順序。

若要編輯優先順序，請選擇位置值。然後使用箭頭遞增，或直接輸入值。若要確認選擇，請選擇確認。若要捨棄變更，請選擇取消。

5. 在政策組態窗格中，決定 AWS Network Security Manager 在目標範圍內採取的自動化動作：

- 修復會將定義的政策套用至安全狀態與 AWS Network Security Manager 描述的所需狀態不相符的任何資源。
- 資源清除會在移除部署或帳戶或資源超出範圍時，刪除 AWS Network Security Manager 為資源建立的 DDoS 保護。
- 現有的客戶 DDoS 解決方案決定如何解決您正在定義的政策與可能已部署的政策之間的衝突。從功能表中，選擇下列其中一個選項：
 - 沒有任何補救措施會略過任何已具有 DDoS 保護之資源的補救措施。
 - 覆寫關聯會將現有的 DDoS 保護取代為 AWS Network Security Manager 建立的 DDoS 保護。
 - 改造會將其規則修改到每個現有的 DDoS 保護，並保持與資源相關聯的 DDoS 保護。

建立範圍（主控台）

請完成下列步驟：

1. 在範圍詳細資訊窗格中，輸入範圍名稱和選用的描述。

2.

僅限多帳戶模式

此步驟僅適用於多帳戶模式。在多帳戶模式中，使用帳戶和組織單位選取子窗格來選擇要包含或排除的帳戶或 OUs。在單一帳戶模式中，此子窗格不會出現在主控制台中，因此請略過此步驟。

在帳戶和組織單位選取窗格中，選擇控制管理範圍的三種方法之一：

- 整個 AWS 組織的範圍（所有 OUs 和帳戶） – 不需要進一步定義。
 - 範圍涵蓋整個 AWS 組織，但排除特定 OUs 和帳戶 – 出現兩個子窗格，一個用於組織單位，另一個用於帳戶。選擇新增 OUs 以開啟新增 OUs 視窗，選取您需要的組織單位，然後選擇新增 OUs。若要新增個別帳戶，請在帳戶子窗格中選擇新增帳戶、選取帳戶，然後選擇新增帳戶。
 - 請勿限制為整個 AWS 組織，只包含特定 OUs 和帳戶 – 使用相同的子窗格來新增 OUs 或帳戶。
3. 接著，在資源子窗格中選取資源。在資源類型選擇方塊中，選取所有或特定 AWS Shield Advanced 資源類型。對於 AWS Shield Advanced，選項包括下列任何或所有項目：

- Application Load Balancer
 - CloudFront 分佈
 - Classic Load Balancer
 - 彈性 IP 地址
4. 針對每個選取的資源類型，選擇下列其中一個互斥選項：
- 包含所有資源
 - 包含特定資源
 - 排除特定資源
5. 如果您選擇包含特定資源，請選取下列其中一個表達式類型：
- 單一條件
 - 符合所有條件 (AND)
 - 符合任何條件 (OR)
 - NOT
6. 每個表達式類型都支援單一或多個納入標準和 ARNs，因此您可以建置標籤或 ARNs 的組合。所有資源類型都支援標籤和 ARN 納入標準。如果您選擇標籤，請識別金鑰和選用值。您可以識別多個標籤。

CloudFront 區域需求

若要保護 CloudFront 分佈資源，請使用美國東部（維吉尼亞北部）區域 (us-east-1)。

建立部署（主控台）

部署會將您的政策繫結至範圍並啟用強制執行。AWS Network Security Manager 接著會將您的 AWS Shield Advanced DDoS 保護套用至範圍內資源。

請完成下列步驟：

1. 在概觀頁面上的概觀窗格中，選擇建立部署。
2. 選擇您要部署的政策。
3. 選擇定義 AWS Network Security Manager 套用政策之帳戶和資源的範圍。
4. 針對部署名稱，輸入名稱。在描述，請輸入描述。

5. (選用) 若要讓組織中的其他帳戶可看見部署，請選取為此部署啟用跨帳戶可見性。
6. (選用) 若要新增標籤，請選擇新增標籤，然後輸入索引鍵和選用值組合。
7. 選擇 Create and deploy (建立和部署)。部署頁面隨即出現，您可以在其中查看 AWS Network Security Manager 建立項目的詳細資訊。

 部署可能會產生費用

部署會建立網路安全服務，並將其連接到受保護的資源。AWS Network Security Manager 會收取受保護資源的費用。安全服務本身會保護資源，這會產生額外費用。部署之前，請檢閱 [AWS Network Security Manager 定價頁面](#) 和 [AWS Shield Advanced 定價頁面](#)。

AWS Network Security Manager 和 AWS Firewall Manager

AWS Network Security Manager 是取代 AWS Firewall Manager 的服務。這兩個是完全獨立的服務，每個服務都有獨特的功能和不同的定價模式。如果您目前使用 AWS Firewall Manager，則不需要採取任何動作，您現有的防火牆和政策會繼續運作。本章說明這兩種服務如何共存、使用兩者時的優先順序如何運作，以及遷移在可用時如何運作。

AWS Network Security Manager 和 AWS Firewall Manager 會彼此並排運作，並獨立運作。在某個時間點，AWS Firewall Manager 將停止販售，然後停止操作。

與 AWS Firewall Manager 共存

AWS 除非您啟動動作來變更防火牆，否則 Network Security Manager 不會影響您使用 Firewall Manager 建立的 AWS 防火牆。除非您終止防火牆和政策 AWS，否則您使用 Firewall Manager 建立的防火牆和政策會繼續運作。即使 AWS 防火牆管理員已淘汰，也是如此。

修復期間的優先順序

當這兩個服務都運作時，您可以採取影響您使用 Firewall Manager 建立之 AWS 防火牆的動作。當您建立 AWS Network Security Manager 政策時，您可以將它們套用至範圍，這是一組目標資源。如果該範圍包含 AWS Firewall Manager 政策已處理的資源，AWS Network Security Manager 會在修復期間優先使用。在這種情況下，AWS Network Security Manager 政策和範圍會覆寫現有的 AWS Firewall Manager 防火牆和政策。特定行為取決於您選擇的解析度選項。

從 AWS Firewall Manager 的計劃遷移

從 AWS Firewall Manager 遷移至 AWS Network Security Manager 會將防火牆管理合併為單一服務，並可讓您使用其功能。遷移已規劃，但尚無法使用。當遷移可用時，您將能夠將 AWS Firewall Manager 政策移至 AWS Network Security Manager。遷移需要兩個服務中尚未就緒的新動作。

規劃的程序將從 AWS Firewall Manager 複製選取的政策，將其轉移至 AWS Network Security Manager，並將其翻譯為新的政策結構。此程序不會影響您在 AWS Firewall Manager 中的原始政策或其相關聯防火牆。

AWS Network Security Manager 中的安全

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模式](#)將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也提供您可以安全使用的服務。在[AWS 合規計劃](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS Network Security Manager 的合規計劃，請參閱[AWS 合規計劃的服務範圍](#)。
- 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。

本文件可協助您了解如何在使用 AWS Network Security Manager 時套用共同責任模型。下列主題說明如何設定 AWS Network Security Manager 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS Network Security Manager 資源。

主題

- [AWS Network Security Manager 中的資料保護](#)
- [AWS Network Security Manager 的身分和存取管理](#)
- [使用 AWS Network Security Manager 的服務連結角色](#)
- [AWS Network Security Manager 的合規驗證](#)
- [AWS Network Security Manager 中的彈性](#)
- [AWS Network Security Manager 中的基礎設施安全](#)
- [AWS Network Security Manager 的安全最佳實務](#)

AWS Network Security Manager 中的資料保護

[共同責任模型](#)適用於 AWS Network Security Manager AWS 中的資料保護。如此模型所述，AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需歐洲資料保護的詳細資訊，請參閱[一般資料保護規則 \(GDPR\) 中心](#)。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 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 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 AWS Network Security Manager 或使用主控台、API AWS CLI、AWS SDKs 的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

AWS Network Security Manager 會使用 AWS Key Management Service (AWS KMS) 金鑰加密所有靜態資料。服務受管 KMS 金鑰可保護您的資源組態、部署狀態和同步資料。您不需要設定或管理這些金鑰。

傳輸中加密

AWS Network Security Manager 會使用 Transport Layer Security (TLS) 加密傳輸中的所有資料。所有 API 請求都需要 TLS 1.2 或更新版本。Network AWS Security Manager API 端點的連線只會使用 HTTPS。

金鑰管理

AWS Network Security Manager 使用服務管理的 AWS KMS 金鑰進行靜態加密。您目前無法提供自己的 KMS 金鑰。

AWS Network Security Manager 的身分和存取管理

AWS Identity and Access Management (IAM) 是 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 AWS Network Security Manager 資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Network Security Manager 如何與 IAM 搭配使用](#)
- [AWS Network Security Manager 的身分型政策範例](#)
- [故障診斷 AWS Network Security Manager 身分和存取權](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會因您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [故障診斷 AWS Network Security Manager 身分和存取權](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [AWS Network Security Manager 如何與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [AWS Network Security Manager 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、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，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使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務憑證存取 Directory Service。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。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](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。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](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，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) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。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

當多種類型的政策套用到請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個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 Network Security Manager 如何與 IAM 搭配使用

在您使用 IAM 管理 AWS Network Security Manager 的存取權之前，請先了解哪些 IAM 功能可與 AWS Network Security Manager 搭配使用。

IAM 功能	AWS Network Security Manager 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要全面了解 AWS Network Security Manager 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](#)。

AWS Network Security Manager 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。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素參考](#)。

AWS Network Security Manager 中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包含帳戶、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，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。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](#)。

AWS Network Security Manager 不支援以資源為基礎的政策。

AWS Network Security Manager 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。政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Network Security Manager 動作清單，請參閱《服務授權參考》中的 [AWS Network Security Manager 定義的動作](#)。

AWS Network Security Manager 中的政策動作在動作之前使用下列字首：

```
network-security-manager
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "network-security-manager:action1",  
    "network-security-manager:action2"
```

]

AWS Network Security Manager 會跨其資源類型定義 IAM 動作。其中包括規則、範本、政策、範圍和部署的建立、讀取、更新和刪除 (CRUD) 操作，以及快照、標記、管理、同步狀態和資源關聯操作。

AWS Network Security Manager 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。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*" 
```

若要查看 AWS Network Security Manager 資源類型及其 ARNs 的清單，請參閱《服務授權參考》中的 [AWS Network Security Manager 定義的資源](#)。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 Network Security Manager 定義的動作](#)。

AWS Network Security Manager 會為其每個資源（規則、範本、政策、範圍和部署）定義 IAM 資源類型，以及每個資源的快照類型（例如 rule-snapshot）。ARN 格式為：

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

草稿 ARNs 會附加 :DRAFT，快照 ARNs 則會附加版本編號（例如 :3）。

草稿不是單獨的 IAM 資源類型。如需授權，草稿會被視為其作用中資源的子項，其為父項。:DRAFT 合格的 ARN 會針對作用中資源授權，因此對草稿採取動作的許可來自對該作用中資源採取動作的許可。

快照與草稿不同。每個快照都是自己的 IAM 資源類型，因此符合版本資格的 ARN 會直接針對該快照資源類型進行授權，而不是針對父作用中資源。

AWS Network Security Manager 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 元素會根據定義的條件，指定陳述式的執行時機。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 AWS Network Security Manager 條件金鑰清單，請參閱《服務授權參考》中的 [AWS Network Security Manager 的條件金鑰](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [AWS Network Security Manager 定義的動作](#)。

AWS Network Security Manager 支援下列屬性型存取控制 (ABAC) 的 AWS 全域標籤條件金鑰：

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

標籤型條件索引鍵適用於作用中的資源和快照。草稿資源無法標記，也不支援`aws:ResourceTag`條件。

AWS Network Security Manager 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。

AWS Network Security Manager 不支援存取控制清單 ACLs)。

ABAC 搭配 AWS Network Security Manager

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

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 \(ABAC\)](#)。

AWS Network Security Manager 支援使用全部三個 AWS 全域標籤條件索引鍵的屬性型存取控制。您可以根據連接到這些資源的標籤來限制 AWS 對 Network Security Manager 資源的存取。

搭配 AWS Network Security Manager 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。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 使用者指南》中的[IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務](#)。

AWS Network Security Manager 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (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。如需提出 FAS 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

AWS Network Security Manager 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給 AWS 服務](#)。

Warning

變更服務角色的許可可能會中斷 AWS Network Security Manager 功能。只有在 AWS Network Security Manager 提供指引時，才能編輯服務角色。

AWS Network Security Manager 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一種服務角色 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 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。

AWS Network Security Manager 會使用服務連結角色在組織的成員帳戶中操作。當您啟用服務時，AWS Network Security Manager 會自動建立服務連結角色。此角色授予 AWS Network Security

Manager 管理 AWS WAF 和 AWS Shield Advanced 資源的許可。此角色也會授予 Config AWS 的存取權，以進行資源探索，以及執行跨帳戶操作的許可。

如需建立和管理 AWS Network Security Manager 服務連結角色的詳細資訊，請參閱 [the section called “服務連結角色”](#)。

AWS Network Security Manager 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 AWS Network Security Manager 資源的許可。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。

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 \(主控台\)](#)。

如需有關 AWS Network Security Manager 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 [AWS Network Security Manager 的動作、資源和條件金鑰](#)。

主題

- [政策最佳實務](#)
- [使用 AWS Network Security Manager 主控台](#)
- [允許使用者檢視他們自己的許可](#)
- [Network AWS Security Manager 的唯讀存取權](#)
- [僅管理規則和範本](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS Network Security Manager 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管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 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 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 以提高安全性。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》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 AWS Network Security Manager 主控台

若要存取 AWS Network Security Manager 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 AWS Network Security Manager 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。

對於僅呼叫 AWS CLI 或 AWS API 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。

若要存取 AWS Network Security Manager 主控台，委託人至少需要 `network-security-manager:List*` 和 `network-security-manager:Get*` 動作的許可。

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 主控台或使用 或 AWS CLI 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:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Network AWS Security Manager 的唯讀存取權

下列政策會授予委託人對所有 AWS Network Security Manager 資源的唯讀存取權。這對於需要檢視組態和同步狀態而不進行變更的稽核人員或監控角色很有用。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}

```

僅管理規則和範本

下列政策允許主體建立、更新和刪除規則和範本，而無需授予政策、範圍或部署的存取權。這對於撰寫安全組態但不控制強制執行的團隊很有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:CreateRule",
        "network-security-manager:GetRule",
        "network-security-manager:UpdateRule",
        "network-security-manager>DeleteRule",
        "network-security-manager:ListRules",
        "network-security-manager:CreateRuleSnapshot",
        "network-security-manager:ListRuleSnapshots",
        "network-security-manager:CreateTemplate",
        "network-security-manager:GetTemplate",
        "network-security-manager:UpdateTemplate",
        "network-security-manager>DeleteTemplate",
        "network-security-manager:ListTemplates",
        "network-security-manager:CreateTemplateSnapshot",
        "network-security-manager:ListTemplateSnapshots",
        "network-security-manager:TagResource",
        "network-security-manager:UntagResource",
        "network-security-manager:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

故障診斷 AWS Network Security Manager 身分和存取權

使用以下資訊來協助您診斷和修正使用 AWS Network Security Manager 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 AWS Network Security Manager 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 AWS Network Security Manager 資源](#)

我無權在 AWS Network Security Manager 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 `network-security-manager:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
network-security-manager: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 `network-security-manager: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，告知您無權執行 `iam:PassRole` 動作，您的政策必須更新，以允許您將角色傳遞給 AWS Network Security Manager。

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 AWS Network Security Manager 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 沒有將角色傳遞給服務的許可。

```
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 AWS Network Security Manager 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 AWS Network Security Manager 是否支援這些功能，請參閱 [AWS Network Security Manager 如何與 IAM 搭配使用](#)。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《[IAM 使用者指南](#)》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 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[將存取權提供給第三方 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](#)。

使用 AWS Network Security Manager 的服務連結角色

AWS Network Security Manager 使用 IAM [服務連結角色](#)。服務連結角色是直接連結至 AWS Network Security Manager 的唯一 IAM 角色類型。服務連結角色由 AWS Network Security Manager 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 AWS Network Security Manager，因為您不必手動新增必要的許可。AWS Network Security Manager 會定義其服務連結角色的許可。除非另有定義，否則只有 AWS Network Security Manager 可以擔任其角色。已定義的許可包括信任政策和許可政策。您無法將該許可政策連接至任何其他 IAM 實體。

您必須先刪除相關資源，才能刪除服務連結角色。這可保護您的 AWS Network Security Manager 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱[AWS 使用 IAM 的服務](#)，並在服務連結角色欄中尋找包含是的服務。選擇是連結，以檢視該服務的服務連結角色文件。

AWS Network Security Manager 的服務連結角色許可

AWS Network Security Manager 使用名為 的服務連結角色 `AWSServiceRoleForNetworkSecurityManager`。此服務連結角色信任 `network-security-manager.amazonaws.com` 服務主體擔任該角色。

名為 的角色許可政策 `NetworkSecurityManagerServiceRolePolicy` 是一種 AWS 受管政策，允許 AWS Network Security Manager 對指定的資源完成動作。

下列信任政策允許 `network-security-manager.amazonaws.com` 服務主體擔任該角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "network-security-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Note

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。

許可詳細資訊

AWS Network Security Manager 需要每組許可，才能保護和探索您帳戶和組織中的資源。NetworkSecurityManagerServiceRolePolicy 受管政策會授予下列許可，依服務分組：

- `wafv2` – 建立、讀取、更新和刪除 Web ACLs 和 Firewall Manager 規則群組。將 Web ACLs 與受保護的資源建立關聯和取消關聯。管理 Web ACL 記錄組態和規則群組許可政策。標記和取消標記資源。驗證 AWS Network Security Manager Web ACL 和規則組態。
- `shield` – 建立、描述、列出和刪除 AWS Shield Advanced 保護。建立和描述 AWS Shield Advanced 訂閱。
- `elasticloadbalancing` – 描述 Application Load Balancer 和標籤。在 Application Load Balancer 上建立、刪除和設定 Web ACL 關聯。
- `cloudfront` – 取得並列出 Amazon CloudFront 分佈、組態和標籤。關聯和取消關聯分佈 Web ACLs。讀取 VPC 原始伺服器。
- `apigateway` – 讀取 Amazon API Gateway REST APIs、階段和標籤。在 API 階段上設定 Web ACL。

- `ec2` – 讀取 Amazon EC2 驗證存取執行個體 Web ACLs 和關聯。描述 Shield Advanced AWS 保護的彈性 IP 地址。
- `cognito-idp`、`amplify`、`apprunner` `appsync` 和 `bedrock-agentcore` – 讀取 Amazon Cognito 使用者集區、AWS App Runner 服務、AWS AppSync GraphQL APIs、AWS Amplify 應用程式和 Amazon Bedrock AgentCore 開道的 Web ACL 關聯，以便 AWS Network Security Manager 可以探索受保護的資源。
- `config` – 選取資源組態，並管理 AWS Network Security Manager 用來探索範圍內資源的服務連結 AWS Config 組態記錄器。
- `organizations` – 讀取您的組織、帳戶、根目錄、組織單位和委派管理員，以便 AWS Network Security Manager 可以在整個組織中運作。
- `logs` – 建立、讀取、更新、刪除和列出 Web ACL 記錄的日誌交付。
- `s3` – 在名稱開頭為 `aws-waf-logs-` 的 Amazon S3 儲存貯體上取得和放置儲存貯體政策 `aws-waf-logs-`，以便交付 Web ACL 日誌。
- `iam` – 建立 AWS Shield Advanced AWS Config 和 AWS WAF 所需的服務連結角色，範圍依 `iam:AWSServiceName` 條件索引鍵而定。

下列 JSON 顯示完整的 `NetworkSecurityManagerServiceRolePolicy` 許可政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
```

```

        "s3:PutBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::aws-waf-logs-*"
},
{
    "Sid": "CloudfrontVpcOriginAccess",
    "Effect": "Allow",
    "Action": [
        "cloudfront:GetVpcOrigin"
    ],
    "Resource": "arn:aws:cloudfront::*:vpccorigin/*"
},
{
    "Sid": "ConfigUnscoped",
    "Effect": "Allow",
    "Action": [
        "config:SelectResourceConfig"
    ],
    "Resource": "*"
},
{
    "Sid": "DescribeOrganizationUnScoped",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
},
{
    "Sid": "DescribeAccountScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeAccount",
    "Resource": "arn:aws:organizations::*:account/o-*/*"
},
{
    "Sid": "DescribeOrganizationUnitScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeOrganizationalUnit",

```

```

    "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
  },
  {
    "Sid": "ListDelegatedAdministratorsScoped",
    "Effect": "Allow",
    "Action": "organizations:ListDelegatedAdministrators",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "network-security-manager.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "LoadBalancerNonMutationApiAccess",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeWebACLAssociation"
    ],
    "Resource": "*"
  },
  {
    "Sid": "LoadBalancerGetWebACLScoped",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
    "Resource": "arn:aws:elasticloadbalancing::*:loadbalancer/app/*/*"
  },
  {
    "Sid": "CloudFrontDistributionNonMutationApiAccess",
    "Effect": "Allow",
    "Action": [
      "cloudfront:GetDistribution",
      "cloudfront:GetDistributionConfig",
      "cloudfront:ListTagsForResource"
    ],
    "Resource": "arn:aws:cloudfront::*:distribution/*"
  },
  {
    "Sid": "ApiGatewayStageNonMutationApiAccess",
    "Effect": "Allow",

```

```

    "Action": "apigateway:GET",
    "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
    ]
},
{
    "Sid": "Wafv2General",
    "Effect": "Allow",
    "Action": [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2>DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
},
{
    "Sid": "Wafv2WebAclAndRuleGroupMutation",
    "Effect": "Allow",
    "Action": [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2>DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
    ],
    "Resource": [
        "arn:aws:wafv2:*:*:*/*webacl/*",
        "arn:aws:wafv2:*:*:*global/rulegroup/*",
        "arn:aws:wafv2:*:*:*regional/rulegroup/*",
        "arn:aws:wafv2:*:*:*global/managedruleset/*",
        "arn:aws:wafv2:*:*:*regional/managedruleset/*",
        "arn:aws:wafv2:*:*:*global/ipset/*",
        "arn:aws:wafv2:*:*:*regional/ipset/*",
        "arn:aws:wafv2:*:*:*global/regexpatternset/*",

```

```

        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
    ],
},
{
    "Sid": "Wafv2Logging",
    "Effect": "Allow",
    "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
},
{
    "Sid": "Wafv2ListLogging",
    "Effect": "Allow",
    "Action": "wafv2:ListLoggingConfigurations",
    "Resource": "*"
},
{
    "Sid": "Wafv2ListWebACLs",
    "Effect": "Allow",
    "Action": "wafv2:ListWebACLs",
    "Resource": "*"
},
{
    "Sid": "Wafv2PermissionPolicy",
    "Effect": "Allow",
    "Action": [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2>DeletePermissionPolicy"
    ],
    "Resource": [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
    ]
},
{
    "Sid": "Wafv2WebaclDescribe",
    "Effect": "Allow",
    "Action": "wafv2:GetWebACLForResource",
    "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
},

```

```
{
  "Sid": "CloudFrontListDistributions",
  "Effect": "Allow",
  "Action": [
    "cloudfront:ListDistributionsByWebACLId",
    "cloudfront:ListDistributions"
  ],
  "Resource": "*"
},
{
  "Sid": "CloudFrontDistributionMutation",
  "Effect": "Allow",
  "Action": [
    "cloudfront:AssociateDistributionWebACL",
    "cloudfront:DisassociateDistributionWebACL"
  ],
  "Resource": "arn:aws:cloudfront::*:distribution/*"
},
{
  "Sid": "ElbWebAclRemediationScoped",
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:CreateWebACLAssociation",
    "elasticloadbalancing>DeleteWebACLAssociation"
  ],
  "Resource": "arn:aws:elasticloadbalancing::*:loadbalancer/app/*/*"
},
{
  "Sid": "ElbSetWebAcl",
  "Effect": "Allow",
  "Action": "elasticloadbalancing:SetWebACL",
  "Resource": "*"
},
{
  "Sid": "ApiGatewayWebAclRemediation",
  "Effect": "Allow",
  "Action": "apigateway:SetWebACL",
  "Resource": "arn:aws:apigateway::*/restapis/*/stages/*"
},
{
  "Sid": "CognitoWebAclIntegration",
  "Effect": "Allow",
  "Action": [
    "cognito-idp:GetWebACLForResource",
```

```
    "cognito-idp:ListResourcesForWebACL"
  ],
  "Resource": "*"
},
{
  "Sid": "AppRunnerWebAclIntegration",
  "Effect": "Allow",
  "Action": [
    "apprunner:DescribeWebAclForService",
    "apprunner:ListAssociatedServicesForWebAcl"
  ],
  "Resource": "*"
},
{
  "Sid": "VerifiedAccessWebAclIntegration",
  "Effect": "Allow",
  "Action": [
    "ec2:GetVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
  ],
  "Resource": "*"
},
{
  "Sid": "AppSyncWebAclIntegration",
  "Effect": "Allow",
  "Action": [
    "appsync:GetWebACLForResource",
    "appsync:ListResourcesForWebACL"
  ],
  "Resource": "*"
},
{
  "Sid": "AmplifyWebAclIntegration",
  "Effect": "Allow",
  "Action": [
    "amplify:GetWebACLForResource",
    "amplify:ListResourcesForWebACL"
  ],
  "Resource": "*"
},
{
  "Sid": "ShieldGeneral",
  "Effect": "Allow",
  "Action": [
```

```

        "shield:CreateProtection",
        "shield>DeleteProtection",
        "shield:DescribeProtection",
        "shield>ListProtections",
        "shield>CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
    ],
    "Resource": "*"
},
{
    "Sid": "ShieldSlrCreation",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "shield.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowConfigRecorderList",
    "Effect": "Allow",
    "Action": "config:ListConfigurationRecorders",
    "Resource": "*"
},
{
    "Sid": "AllowPutServiceLinkedConfigRecorder",
    "Effect": "Allow",
    "Action": "config:PutServiceLinkedConfigurationRecorder",
    "Resource": "*"
},
{
    "Sid": "AllowConfigRecorderScopedAccess",
    "Effect": "Allow",
    "Action": [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config>DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
    ]
}

```

```
    "config:DisassociateResourceTypes"
  ],
  "Resource": "arn:aws:config:*:*:configuration-recorder/*"
},
{
  "Sid": "AllowCreateConfigServiceLinkedRole",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "config.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowListActionsForAgentCoreGateway",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayListResourcesForWebACL"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowGetActionForAgentCoreGateway",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayGetWebACLForResource"
  ],
  "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
},
{
  "Sid": "WafV2LoggingSlrCreation",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam:*:*:role/aws-service-role/wafv2.amazonaws.com/*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "wafv2.amazonaws.com"
    }
  }
}
]
```

```
}
```

為 AWS Network Security Manager 建立服務連結角色

您不需要手動建立服務連結角色，當您啟用 AWS Network Security Manager 時，AWS Network Security Manager 會為您建立服務連結角色。沒有要執行的手動步驟。

如果您刪除此服務連結角色，然後需要再次建立該角色，AWS Network Security Manager 會在您下次使用服務時重新建立該角色。您不需要採取任何動作。

如需詳細資訊，請參閱《IAM 使用者指南》中的「[建立服務連結角色](#)」。

編輯 AWS Network Security Manager 的服務連結角色

您無法變更 `AWSServiceRoleForNetworkSecurityManager` 服務連結角色的許可。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。

如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

刪除 AWS Network Security Manager 的服務連結角色

如果您不再需要使用 AWS Network Security Manager，我們建議您刪除 `AWSServiceRoleForNetworkSecurityManager` 服務連結角色。

刪除服務連結角色之前，請先清除 AWS Network Security Manager 管理的資源。停用 AWS Network Security Manager 並移除政策和範圍，讓 AWS Network Security Manager 管理的資源不會保留在您的帳戶中。然後，您可以手動刪除角色。

Note

如果 AWS Network Security Manager 在您嘗試刪除資源時使用角色，刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

1. 在以下網址開啟 IAM 主控台：<https://console.aws.amazon.com/iam/>。
2. 在導覽窗格中，選擇角色。

3. 在搜尋方塊中，輸入 `AWSServiceRoleForNetworkSecurityManager`，然後選取角色。
4. 選擇 刪除。
5. 若要確認刪除，請輸入角色名稱，然後選擇刪除。

如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

AWS Network Security Manager 服務連結角色支援的 區域

AWS Network Security Manager 支援在所有可使用 AWS Network Security Manager 的 AWS 區域中使用服務連結角色。

AWS Network Security Manager 的合規驗證

我們的新 AWS 註冊體驗並非針對受管制的工作負載而設計。如果您正在使用我們新的 AWS 註冊體驗，但想要將 AWS 用於受管制的工作負載，您可以[註冊 AWS（進階）](#)或為您的 AWS 環境[啟用進階功能](#)。

若要了解 是否 AWS 服務 在特定合規計劃範圍內，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 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

AWS Network Security Manager 中的彈性

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，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施之外，AWS Network Security Manager 還提供數種功能，以協助支援您的資料彈性和備份需求。

AWS Network Security Manager 中的基礎設施安全

作為受管服務，AWS Network Security Manager 受到 [Amazon Web Services：安全程序概觀](#) 白皮書中所述的 AWS 全球網路安全程序的保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 AWS Network Security Manager。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。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。

AWS Network Security Manager 的安全最佳實務

下列最佳實務可協助您維護安全的 AWS Network Security Manager 組態。

預防性控制

- 使用 IAM 最低權限 -- 僅授予每個使用者或角色執行其 AWS Network Security Manager 任務所需的許可。盡可能使用 IAM 條件金鑰來限制對特定資源的存取。
- 使用服務連結角色 -- AWS Network Security Manager 使用服務連結角色代表您執行動作。這些角色具有範圍為最低必要存取的預先定義許可。
- 仔細設定範圍 -- 定義僅以需要保護的帳戶和資源類型為目標的範圍組態。範圍過大可能會導致意外強制執行。

偵測性控制

- 啟用 AWS CloudTrail 記錄 -- CloudTrail 會記錄所有 AWS Network Security Manager API 呼叫。檢閱這些日誌，以稽核誰對您的安全組態進行變更，以及變更時間。
- 監控同步狀態 -- 定期檢查部署的同步狀態，以識別與您預期安全狀態不同步的資源。

監控 AWS Network Security Manager

監控 AWS Network Security Manager 可協助您了解資源是否如預期般受到保護。AWS Network Security Manager 提供下列監控功能：

- 同步狀態 APIs -- 查詢部署中個別資源的保護狀態。
- AWS CloudTrail -- 記錄所有 AWS Network Security Manager API 呼叫以進行稽核、合規和操作故障診斷。

監控同步狀態

監控資源是否受到保護的主要方式是透過同步狀態 APIs。AWS Network Security Manager 會評估每個範圍內的資源，並記錄其實際防火牆組態是否符合預期的組態。

同步狀態操作

AWS Network Security Manager 提供兩種查詢同步狀態的操作：

`ListResourceSynchronizationStatuses`

傳回特定部署的每個資源狀態。需要 `deploymentIdentifier` 參數。選擇性地依 `synchronizationStatus`(`IN_SYNC`、`OUT_OF_SYNC` 或 `NOT_APPLICABLE`) 篩選。

`ListAggregateResourceSynchronizationStatuses`

傳回所有部署的每個資源彙總狀態。選擇性地依 `synchronizationStatus` 篩選。此操作會顯示套用至每個資源之所有政策的合併結果。

這兩個操作都支援使用 `maxResults`(1 到 100) 和 進行分頁 `nextToken`。

了解同步狀態值

`IN_SYNC`

資源的實際防火牆組態符合從所有適用政策計算的有效組態。

`OUT_OF_SYNC`

資源的實際組態與有效組態不同。`outOfSyncReasons` 欄位提供每個設定的詳細資訊，顯示預期值與實際值。

NOT_APPLICABLE

資源的帳戶和資源類型在範圍內，但資源本身不符合範圍篩選條件（例如，標籤篩選條件排除它）。不需採取任何動作。

如果資源完全沒有出現在結果中，則帳戶或資源類型不在部署範圍內。檢查您的範圍組態。

了解評估時間戳記

每個同步狀態項目包含兩個時間戳記：

- `evaluatedAt` -- 當 AWS Network Security Manager 上次評估資源的組態時。過時`evaluatedAt`值表示評估尚未針對最近的變更執行。
- `updatedAt` -- 同步狀態記錄本身上次變更時。如果 `updatedAt` 早於 `evaluatedAt`，則狀態自上次評估以來已穩定。

跨帳戶可見性

當多個管理員保護相同的資源時，彙總同步狀態的可見性取決於每個部署上的 `enableCrossAccountVisibility` 設定。

- 如果涵蓋資源的所有部署都已啟用跨帳戶可見性，則任何管理員都可以查看完整的彙總狀態和`out-of-sync`的原因。
- 如果任何部署已停用跨帳戶可見性，其他管理員會看到`NOT_VISIBLE`標記，而不是詳細的原因。這表示另一個管理員也會保護資源，但尚未共用可見性。

診斷out-of-sync的資源

當資源報告 `OUT_OF_SYNC` 時，`outOfSyncReasons` 欄位會識別特定的組態差異。最上層的原因如下：

- `missingFirewall` -- 沒有與資源相關聯的防火牆保護。
- `invalidFirewall` -- 防火牆存在，但其組態不符合預期。特定差異會列在分類的儲存貯體中。

如果啟用修復但無法修正資源，`remediationIssues` 欄位會提供如何手動解決問題`correctiveAction`的指引。修補是預設為關閉的政策層級設定。如需詳細資訊，請參閱[the section called “同步和修復”](#)。

具有不同組態的多個部署可以鎖定相同的資源。在此情況下，每次部署同步狀態可以是 OUT_OF_SYNC，而彙總同步狀態則是 IN_SYNC。這是預期的行為，而不是失敗。較高優先順序政策的設定在合併期間優先。因此，即使資源不符合低優先順序部署的組態，資源仍會符合有效的組態。

使用 記錄 AWS Network Security Manager API 呼叫 AWS CloudTrail

AWS Network Security Manager 已與 服務整合 AWS CloudTrail，此服務可提供使用者、角色或服務所採取動作的記錄 AWS。CloudTrail 會將 AWS Network Security Manager 的所有 API 呼叫擷取為管理事件。擷取的呼叫包括來自 AWS Network Security Manager 主控台的呼叫，以及對 AWS Network Security Manager API 操作的程式設計呼叫。

如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AWS Network Security Manager 的事件。如果您未設定追蹤，仍然可以在 CloudTrail 主控台的事件歷史記錄中檢視最新的事件。如需詳細資訊，請參閱 [「AWS CloudTrail 使用者指南」](#)。

AWS CloudTrail 中的 Network Security Manager 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 AWS Network Security Manager 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。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」](#)。

若要持續記錄 中的事件 AWS 帳戶，包括 AWS Network Security Manager 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。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會 AWS 記錄分割區中所有區域的事件。它會將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中收集的事件資料。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 Network Security Manager 操作。公有操作包括下列項目：

- 針對規則、範本、政策、範圍和部署建立、讀取、更新和刪除 (CRUD) 操作
- 快照操作

- 標記操作
- 管理員帳戶操作
- 同步狀態操作
- 資源關聯操作
- 規則產生操作

每個事件項目都包含下列資訊：

- 事件來源：network-security-manager.amazonaws.com
- 事件名稱，即 API 操作名稱（例如 CreatePolicy 或 ListDeployments）
- 受影響的資源，由 ARN 和資源類型識別

唯讀操作（例如 GetPolicy、ListRules 和 ListResourceSynchronizationStatuses）會以記錄 `readOnly: true`，且不包含回應元素。變動操作包括請求參數和回應元素。

Note

CloudTrail 會修訂事件記錄中的敏感欄位。例如，CloudTrail 會修訂 GenerateRuleConfiguration 操作中的 prompt 參數。

範例：CreatePolicy 事件

以下範例顯示 CreatePolicy 操作的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:my-session",
    "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/AdminRole",
```

```

        "accountId": "123456789012",
        "userName": "AdminRole"
    },
    "attributes": {
        "creationDate": "2026-08-10T18:22:41Z",
        "mfaAuthenticated": "false"
    }
},
{
    "eventTime": "2026-08-10T18:24:03Z",
    "eventSource": "network-security-manager.amazonaws.com",
    "eventName": "CreatePolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.44",
    "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
    "requestParameters": {
        "clientToken": "550e8400-e29b-41d4-a716-446655440001",
        "policyName": "production-web-acl-policy",
        "firewallType": "WAF",
        "priority": 1,
        "associatedTemplateAndRuleList": [
            {
                "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
            }
        ],
        "policyConfiguration": {
            "remediationEnabled": true,
            "resourcesCleanUp": false,
            "wafConfig": {
                "existingCustomerWebACLResolution": "RETROFIT",
                "conflictResolution": "MERGE_WHERE_APPLICABLE"
            }
        },
        "isPublished": true
    },
    "responseElements": {
        "policyId": "p9z8y7x6w5v4u3t2",
        "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
        "policyName": "production-web-acl-policy",
        "status": "ACTIVE",
        "version": "1"
    }
},

```

```
"requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
"eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
"readOnly": false,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::NetworkSecurityManager::Policy",
    "ARN": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

AWS Network Security Manager 配額

您的 AWS 帳戶 具有下列 AWS Network Security Manager 預設配額。除非另有說明，否則每個配額都是每個區域每個帳戶。

資源配額

下表列出您可以在每個區域中為每個帳戶建立 AWS 的 Network Security Manager 資源數量上限。

資源	預設配額	可調整
每個 帳戶的規則數	200	否
每個帳戶的範本	100	否
每個帳戶的政策數	100	否
每個帳戶的範圍	100	否
每個帳戶的部署	100	否
每個資源的快照	10	否

資源合成配額

下表列出 AWS Network Security Manager 資源如何在資源階層中互相參考的配額。

配額	Value
每個範本的規則	1 到 50
每個 AWS WAF 政策的範本	1 到 2
每個 AWS WAF 政策合併的規則和範本	1 到 100
每個 Shield Advanced AWS 政策的範本或規則	0 (必須為空白)

配額	Value
每個部署的政策	1 到 2
每個部署的範圍	1 (確切一個)

範圍組態配額

下表列出範圍組態表達式的配額。

配額	Value
每個範圍的資源類型範圍	20
範圍表達式深度 (巢狀層級)	2
範圍表達式廣度 (每個層級的條件)	20

管理員帳戶配額

下表列出 AWS Network Security Manager 管理員帳戶優先順序層級的配額。

配額	Value
管理員優先順序層級	1 到 10

API 分頁配額

下表列出清單操作的分頁限制。

配額	Value
每頁結果上限 (maxResults)	100
每頁結果下限 (maxResults)	1

配額調整性

前面各節中列出的配額是固定的，目前無法增加。

AWS Network Security Manager 開發人員指南的文件歷史記錄

下表說明 AWS Network Security Manager 的文件版本。

變更	描述	日期
初始版本	AWS Network Security Manager 開發人員指南的初始版本。	2026 年 8 月 1 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。