



開發人員指南

AWS WAF、AWS Firewall Manager、AWS Shield Advanced和 AWS Shield 網路安全主管



AWS WAFAWS Firewall Manager、AWS Shield Advanced和 AWS Shield 網路安全主管: 開發人員指南

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，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

.....	xii
什麼是 AWS WAF Shield Advanced、AWS Shield 網路安全主管和 Firewall Manager ?	1
AWS WAF	1
Shield Advanced	3
AWS Shield 網路安全主管	3
AWS Firewall Manager	3
設定您的帳戶	4
註冊 AWS 帳戶	4
建立具有管理存取權的使用者	4
下載工具	5
AWS WAF	7
入門 AWS WAF	8
Set up AWS WAF (更新主控台)	9
Set up AWS WAF (標準主控台)	12
如何 AWS WAF 運作	18
您可以使用保護的資源 AWS WAF	19
使用更新的主控制台體驗	20
了解新的儀表板	22
設定保護	23
建立保護套件或 Web ACL	25
編輯保護套件或 Web ACL	33
管理規則群組行為	38
將保護與 AWS 資源建立關聯或取消關聯	41
將保護套件或 Web ACLs 與規則和規則群組搭配使用	44
設定保護套件或 Web ACL 預設動作	50
管理主體檢查大小限制	51
設定 CAPTCHA、挑戰和字符	52
檢視 Web 流量指標	52
刪除保護套件或 Web ACL	52
AWS WAF 規則	54
使用規則動作	55
使用規則陳述式	57
使用相符規則陳述式	79
使用邏輯規則陳述式	102

使用以速率為基礎的規則陳述式	109
使用規則群組規則陳述式	127
AWS WAF 規則群組	130
使用受管規則群組	131
管理您自己的規則群組	302
AWS Marketplace 規則群組	307
從其他 服務識別規則群組	310
Web ACL 容量單位 (WCUs)	311
判斷規則群組、保護套件或 Web ACL WCUs	312
超大 Web 請求元件	313
封鎖過大的元件	314
支援的規則表達式語法	315
IP 集合和規則運算式模式集	316
建立和管理 IP 集合	317
建立和管理規則運算式模式集	318
自訂的 Web 請求和回應	320
插入自訂請求標頭插入	322
傳送自訂回應	323
支援的回應狀態碼	326
Web 請求標籤	328
標籤的運作方式	329
標籤語法和命名需求	331
新增標籤的規則	333
符合標籤的規則	334
智慧威脅防禦	339
緩解選項	340
最佳實務	347
智慧型威脅緩解中的權杖	350
AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP)	362
AWS WAF 詐騙控制帳戶接管預防 (ATP)	382
AWS WAF 機器人控制	399
分散式阻斷服務 (DDoS) 預防	424
用戶端應用程式整合	433
CAPTCHA 和 Challenge	469
Web 流量的資料保護和記錄	480
日誌	481

資料保護	520
測試和調校您的保護	546
測試和調校高階步驟	547
準備進行測試	548
監控和調校您的 AWS WAF 保護	551
在生產環境中啟用您的保護	563
AWS WAF 搭配 Amazon CloudFront 使用	565
AWS WAF 如何使用不同的分佈類型	565
使用案例	567
您使用 AWS WAF 服務時的安全性	571
保護您的資料	572
搭配 使用 IAM AWS WAF	573
日誌記錄和監控	624
驗證合規	625
建置彈性	626
基礎設施安全性	626
AWS WAF 配額	626
將您的 AWS WAF Classic 資源遷移至 AWS WAF	630
為什麼要遷移至 AWS WAF ?	630
遷移警告	632
遷移的運作方式	633
遷移保護套件或 Web ACL	633
AWS WAF 傳統	639
設定 AWS WAF Classic	640
註冊 AWS 帳戶	4
建立具有管理存取權的使用者	4
下載工具	642
AWS WAF Classic 的運作方式	643
AWS WAF 傳統定價	647
.....	647
Classic 入門 AWS WAF	647
步驟 1：設定 AWS WAF Classic	649
步驟二：建立 Web ACL	649
步驟 3：建立 IP 比對條件	650
步驟 4：建立地理比對條件	650
步驟 5：建立字串比對條件	651

步驟 5A：建立 Regex 條件 (選用)	653
步驟 6：建立 SQL Injection 比對條件	655
步驟 7：(選用) 建立其他條件	656
步驟 8：建立規則並新增條件	656
步驟 9：新增規則至 Web ACL	658
步驟 10：清理您的資源	659
建立和設定 Web 存取控制清單 (Web ACL)	662
使用條件	663
使用規則	706
使用 Web ACL	716
使用 AWS WAF Classic 規則群組搭配 AWS Firewall Manager	730
建立 AWS WAF Classic 規則群組	731
從 AWS WAF Classic 規則群組新增和刪除規則	733
開始使用 AWS Firewall Manager 以啟用 AWS WAF Classic 規則	734
步驟 1：完成先決條件	735
步驟 2：建立規則	736
步驟 3：建立規則群組	736
步驟 4：建立和套用 AWS Firewall Manager AWS WAF Classic 政策	738
教學課程：使用階層規則建立 AWS Firewall Manager 政策	740
步驟 1：指定 Firewall Manager 管理員帳戶	741
步驟 2：使用 Firewall Manager 管理員帳戶建立規則群組	741
步驟 3：建立 Firewall Manager 政策並連接一般規則群組	741
步驟 4：新增帳戶專屬規則	742
結論	742
記錄 Web ACL 流量資訊	742
以速度為基礎的規則列出封鎖的 IP 地址	749
AWS WAF Classic 如何與 Amazon CloudFront 功能搭配使用	750
使用 AWS WAF Classic 搭配 CloudFront 自訂錯誤頁面	751
針對在您自己的 HTTP 伺服器上執行的應用程式，使用 AWS WAF Classic 搭配 CloudFront	751
選擇 CloudFront 回應的 HTTP 方法	752
安全	752
資料保護	754
身分與存取管理	755
日誌記錄和監控	777
法規遵循驗證	778

恢復能力	780
基礎架構安全	780
AWS WAF 傳統配額	781
AWS Shield	785
Shield 和 Shield Advanced 如何運作	786
AWS Shield Standard 概觀	787
AWS Shield Advanced 概觀	788
Shield Advanced 保護的資源	789
Shield Advanced 功能和選項	790
決定是否訂閱 AWS Shield Advanced	792
DDoS 攻擊的範例	794
Shield 如何偵測事件	795
Shield 如何緩解事件	798
建置 DDoS 彈性架構	804
Web 應用程式的 DDoS 彈性架構	805
TCP 和 UDP 應用程式的 DDoS 彈性架構	807
將 Shield Advanced 與其他結合 AWS 服務	809
設定 AWS Shield Advanced	809
訂閱 Shield Advanced	811
新增和設定資源保護	812
設定 SRT 支援	817
建立 DDoS 儀表板	819
SRT 支援	819
授予 SRT 的存取權	820
設定主動參與	823
聯絡 SRT	824
使用 SRT 設定自訂緩解措施	825
資源保護	825
受保護資源的清單	826
保護 Amazon EC2 執行個體和 Network Load Balancer	827
保護應用程式層 (第 7 層)	828
使用運作狀態檢查以運作狀態為基礎的偵測	842
將保護新增至資源	850
編輯保護	851
建立警示和通知	853
從資源移除保護	854

保護群組	855
追蹤保護變更	857
DDoS 事件的可見性	857
全域和帳戶活動	858
事件	861
帳戶之間的事件可見性	870
回應 DDoS 事件	872
聯絡應用程式層攻擊的支援	873
手動緩解應用程式層攻擊	874
在攻擊後請求點數	875
使用 Shield 服務的安全性	876
保護您的資料	877
搭配 Shield 使用 IAM	878
日誌記錄和監控	902
驗證合規	903
建置彈性	903
基礎設施安全性	904
AWS Shield Advanced 配額	904
AWS Shield 網路安全主管（預覽）	905
AWS Shield 網路安全主管定價	905
什麼是網路安全主管？	905
使用案例	905
重要概念	906
設定您的帳戶	909
註冊 AWS 帳戶	4
建立具有管理存取權的使用者	4
AWS Shield 網路安全主管入門	911
執行網路分析	911
識別具有安全問題的資源	912
使用網路拓撲映射	913
了解網路拓撲映射	913
導覽網路拓撲映射	913
分析拓撲映射中的資源	914
在拓撲映射中識別安全模式	914
尋找最高嚴重性資源的修復步驟	915
使用 Amazon Q Developer 分析網路安全	916

AWS Shield 網路安全主管配額	917
故障診斷 AWS Shield 網路安全主管	917
不支援的跨帳戶共用資源	917
調查結果和隱藏的可用性	918
資源掃描限制	918
其他資源	919
安全	919
身分和存取權管理	920
身分型政策範例	921
使用服務連結角色	924
使用 記錄 AWS Shield 網路安全主管 API 呼叫 AWS CloudTrail	931
CloudTrail 中的網路安全主管資訊	931
CloudTrail 記錄的網路安全主管 API 操作	931
了解網路安全主管日誌檔案項目	932
使用 Amazon CloudWatch 監控 CloudTrail 日誌	934
CloudTrail 與網路安全主管的最佳實務	934
AWS Firewall Manager	935
AWS Firewall Manager 先決條件	936
使用 Firewall Manager 加入和設定 AWS Organizations	936
建立 AWS Firewall Manager 預設管理員帳戶	937
啟用 AWS Config 以使用 Firewall Manager	938
在 Marketplace 中 AWS 訂閱並設定 Firewall Manager 第三方政策的第三方設定	939
使用 啟用 Network Firewall 和 DNS Firewall 政策的資源共用 AWS RAM	940
AWS Firewall Manager 在預設停用的區域中使用	940
使用 Firewall Manager 管理員	941
建立 Firewall Manager 管理員帳戶	942
更新 Firewall Manager 管理員帳戶	944
撤銷 Firewall Manager 管理員帳戶	944
變更預設管理員帳戶	945
取消管理員帳戶變更的資格	946
設定 AWS Firewall Manager 政策	947
設定 AWS WAF 政策	947
設定 AWS Shield Advanced 政策	950
設定 Amazon VPC 安全群組政策	955
設定 Amazon VPC 網路 ACL 政策	957
設定 AWS Network Firewall 政策	960

設定 DNS 防火牆政策	963
設定 Palo Alto Networks 雲端 NGFW 政策	965
設定 Fortigate CNF 政策	969
使用 AWS Firewall Manager 政策	972
一般設定	973
建立政策	973
刪除政策	1003
使用政策範圍	1004
AWS WAF 政策	1006
AWS Shield Advanced 政策	1018
安全群組政策	1022
網路 ACL 政策	1032
網路防火牆政策	1039
DNS 防火牆政策	1048
Palo Alto Networks 雲端 NGFW 政策	1050
Fortigate CNF 政策	1051
Network Firewall 和 DNS Firewall 政策的資源共用	1051
使用受管清單	1052
受管清單版本控制	1053
使用受管清單	1053
建立自訂受管清單	1053
檢視受管清單	1055
刪除自訂受管清單	1055
分組您的 資源	1057
在 Firewall Manager 中使用資源集時的考量事項	1057
建立資源集	1058
刪除資源集	1059
檢視政策的合規	1059
Firewall Manager 與 Security Hub 整合	1062
AWS WAF 政策調查結果	1064
AWS Shield Advanced 政策調查結果	1064
安全群組通用政策問題清單	1065
安全性群組內容稽核政策問題清單	1066
安全群組使用狀況稽核政策問題清單	1066
DNS 防火牆政策調查結果	1067
使用 Firewall Manager 服務的安全性	1067

資料保護	1068
身分和存取權管理	1069
日誌記錄和監控	1095
法規遵循驗證	1096
恢復能力	1096
基礎設施安全性	1097
AWS Firewall Manager 配額	1097
軟配額	1097
硬配額	1100
監控	1102
監控工具	1103
自動化監控工具	1103
手動工具	1104
使用 CloudWatch 進行監控	1105
檢視指標和維度	1105
AWS WAF 指標和維度	1106
AWS Shield Advanced 指標	1119
AWS Firewall Manager 通知	1124
使用 AWS CloudTrail 記錄 API 呼叫	1124
AWS WAF 中的資訊 AWS CloudTrail	1125
AWS Shield Advanced CloudTrail 中的資訊	1135
AWS Firewall Manager CloudTrail 中的資訊	1137
使用 AWS WAF 和 AWS Shield Advanced API	1140
使用 AWS SDKs	1140
向 AWS WAF 或 Shield Advanced 提出 HTTPS 請求	1140
請求 URI	1140
HTTP 標頭	1140
HTTP 請求內文	1142
HTTP 回應	1143
錯誤回應	1143
對請求進行身分驗證	1144
相關資訊	1146
文件歷史紀錄	1147
2018 年之前的更新	1185

推出 的新主控台體驗 AWS WAF

您現在可以使用更新後的體驗，在主控台的任何位置存取 AWS WAF 功能。如需詳細資訊，請參閱[使用更新的主控台體驗](#)。

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。

什麼是 AWS WAF、AWS Shield Advanced 和 AWS Shield 網路安全主管？

您可以使用 [AWS WAF](#)、[AWS Shield](#) 和 [AWS Firewall Manager](#) 一起建立全面的安全解決方案。AWS WAF 是一種 Web 應用程式防火牆，可用來監控最終使用者傳送到應用程式的 Web 請求，以及控制對內容的存取。Shield Advanced 可在網路和傳輸層（第 3 層和第 4 層）和應用程式層（第 7 層）上針對 AWS 資源的分散式拒絕服務 (DDoS) 攻擊提供保護。AWS Firewall Manager 提供跨帳戶和資源的 AWS WAF 和 Shield Advanced 等保護管理，即使新增了新的資源也一樣。

主題

- [什麼是 AWS WAF？](#)
- [什麼是 AWS Shield Advanced？](#)
- [什麼是 AWS Shield 網路安全主管？](#)
- [什麼是 AWS Firewall Manager？](#)

什麼是 AWS WAF？

AWS WAF 是一種 Web 應用程式防火牆，可讓您監控轉送至受保護 Web 應用程式資源的 HTTP 和 HTTPS 請求。您可以保護下列資源類型：

- Amazon CloudFront 分佈
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 已驗證的存取執行個體
- AWS Amplify

AWS WAF 可讓您控制對內容的存取。根據您指定的條件，例如請求的 IP 地址或查詢字串的值，您的受保護資源會使用請求的內容、HTTP 403 狀態碼（禁止）或自訂回應來回應請求。

在最簡單的層級，AWS WAF 讓您選擇下列其中一個行為：

- 允許除了您指定的請求之外的所有請求 – 當您希望 Amazon CloudFront、Amazon API Gateway、Application Load Balancer、AWS App Runner、AWS AppSync、Amazon Cognito 或 AWS Verified Access 為公有網站提供內容時，這非常有用，但您也想要封鎖來自攻擊者的請求。
- 封鎖您指定的請求以外的所有請求 – 當您想要為受限制網站提供內容，而其使用者可由 Web 請求中的屬性輕易識別，例如他們用來瀏覽網站的 IP 地址時，這會很有用。
- 計數符合您條件的請求 – 您可以使用 Count 動作來追蹤 Web 流量，而無需修改處理方式。您可以使用此功能進行一般監控，也可以測試新的 Web 請求處理規則。當您想要根據 Web 請求中的新屬性允許或封鎖請求時，您可以先設定 AWS WAF 來計算符合這些屬性的請求。這可讓您在切換規則以允許或封鎖相符請求之前，先確認新的組態設定。
- 針對符合您條件的請求執行 CAPTCHA 或挑戰檢查 – 您可以針對請求實作 CAPTCHA 和無提示挑戰控制，以協助減少對受保護資源的機器人流量。

使用 AWS WAF 有幾個優點：

- 使用您指定的條件防止 Web 攻擊的額外保護。您可以使用 Web 請求的特性來定義條件，如下所示：
 - 發出請求的 IP 地址。
 - 發出請求的國家/地區。
 - 請求標頭中的值。
 - 出現在請求中的字串，可以是符合規則表達式 (regex) 模式的特定字串或字串。
 - 請求的長度。
 - SQL 程式碼的存在很可能為惡意 (稱為 SQL injection)。
 - 指令碼的存在很可能為惡意 (稱為跨網站指令碼)。
- 可允許、封鎖或計數符合指定條件之 Web 請求的規則。或者，規則可以封鎖或計數不僅符合指定條件的 Web 請求，也可以超過一分鐘或五分鐘內指定的請求數。
- 規則，您可以重複在多個 web 應用程式上使用。
- 來自 AWS 和 AWS Marketplace 賣方的受管規則群組。
- 即時指標和採樣的 Web 請求。
- 使用 AWS WAF API 自動化管理。

如果您想要精細控制您新增至資源的保護，AWS WAF 單獨可能是正確的選擇。如需的詳細資訊 AWS WAF，請參閱 [AWS WAF](#)。

什麼是 AWS Shield Advanced？

您可以使用 AWS WAF Web 存取控制清單 (Web ACLs)，以協助將分散式阻斷服務 (DDoS) 攻擊的影響降至最低。為了針對 DDoS 攻擊提供額外保護，AWS 也會 AWS Shield Standard 自動包含 AWS Shield Standard 和 AWS Shield Advanced。除了您已支付的費用 AWS WAF 和其他 AWS 服務之外，無需額外付費。

Shield Advanced 為您的 Amazon EC2 執行個體、Elastic Load Balancing 負載平衡器、CloudFront 分佈、Route 53 託管區域和 AWS Global Accelerator 標準加速器提供擴展的 DDoS 攻擊保護。Shield Advanced 會產生額外費用。Shield Advanced 選項和功能包括自動應用程式層 DDoS 緩解、進階事件可見性，以及來自 Shield Response Team (SRT) 的專用支援。如果您擁有高可見性網站，或者容易受到頻繁的 DDoS 攻擊，請考慮購買 Shield Advanced 提供的額外保護。有關其他訊息，請參閱[AWS Shield Advanced 功能和選項](#)和[決定是否訂閱 AWS Shield Advanced 並套用其他保護](#)。

什麼是 AWS Shield 網路安全主管？

AWS Shield 網路安全主管透過探索您帳戶中的運算、聯網和網路安全資源，協助保護您的 AWS 環境。網路安全主管會根據 AWS 最佳實務和威脅情報分析網路拓撲和安全組態，來評估每個資源的安全組態。為了協助您強化安全性，網路安全主管會評估其調查結果的嚴重性從低到關鍵，並分享特定的修補步驟，您可以透過 Amazon Q Developer 使用自然語言查詢進行探索。

如需 AWS Shield 網路安全主管的詳細資訊，請參閱 [AWS Shield 網路安全主管（預覽）](#)。

什麼是 AWS Firewall Manager？

AWS Firewall Manager 簡化跨多個帳戶和資源的管理和維護任務，以實現各種保護 AWS WAF、AWS Shield Advanced，包括 Amazon VPC 安全群組和網路 ACLs、AWS Network Firewall，以及 Amazon Route 53 Resolver DNS Firewall。使用 Firewall Manager，您只需設定一次保護，服務會自動將保護套用至您的帳戶和資源，即使您新增新帳戶和資源也一樣。

如需防火牆管理員的詳細資訊，請參閱[AWS Firewall Manager](#)。

設定您的帳戶以使用 服務

本主題說明初步步驟，例如建立 帳戶、準備您使用 AWS WAF AWS Firewall Manager，以及 AWS Shield Advanced。您不需要支付這些初步項目的費用。您只需為所使用的 AWS 服務付費。

主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)
- [下載工具](#)

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，以及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權 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

1. 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](#)。

2. 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](#)。

下載工具

AWS Management Console 包含的主控台 AWS WAF AWS Shield Advanced，以及 AWS Firewall Manager，但如果您想要以程式設計方式存取服務，請參閱以下內容：

- API 指南會記錄服務支援的操作，並提供相關 SDK 和 CLI 文件的連結：
 - [AWS WAF API 參考](#)
 - [AWS Shield Advanced API 參考](#)
 - [AWS Firewall Manager API 參考](#)
- 若要呼叫 API，而無需處理低階詳細資訊，例如組合原始 HTTP 請求，您可以使用 AWS SDK。AWS SDKs 提供封裝 AWS 服務功能的函數和資料類型。若要下載 AWS SDK 並存取安裝指示，請參閱適用的頁面：
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)

如需完整的 AWS SDKs 清單，請參閱[適用於 Amazon Web Services 的工具](#)。

- 您可以使用 AWS Command Line Interface (AWS CLI) 從命令列控制多個 AWS 服務。您也可以使用指令碼自動執行命令。如需詳細資訊，請參閱[AWS Command Line Interface](#)。
- AWS Tools for Windows PowerShell 支援這些服務 AWS。如需詳細資訊，請參閱 [AWS Tools for PowerShell Cmdlet 參考](#)。

AWS WAF

AWS WAF 是一種 Web 應用程式防火牆，可讓您監控轉送至受保護 Web 應用程式資源的 HTTP(S) 請求。您可以保護下列資源類型：

- Amazon CloudFront 分佈
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 驗證存取執行個體
- AWS Amplify

AWS WAF 可讓您控制對內容的存取。根據您指定的條件，例如請求的 IP 地址或查詢字串的值，與受保護資源相關聯的服務會使用請求的內容、HTTP 403 狀態碼（禁止）或自訂回應來回應請求。

Note

您也可以使用 AWS WAF 來保護託管在 Amazon Elastic Container Service (Amazon ECS) 容器中的應用程式。Amazon ECS 是高度可擴展且快速的容器管理服務，可讓您在叢集上輕鬆執行、停止和管理 Docker 容器。若要使用此選項，請將 Amazon ECS 設定為使用 Application Load Balancer，該 Application Load Balancer 可讓 AWS WAF 路由和保護服務中任務的 HTTP(S) layer 7 流量。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 [Service Load Balancing](#)。

主題

- [開始使用 AWS WAF](#)
- [如何 AWS WAF 運作](#)
- [在 中設定保護 AWS WAF](#)
- [AWS WAF 規則](#)
- [AWS WAF 規則群組](#)
- [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)

- [在中過大 Web 請求元件 AWS WAF](#)
- [中支援的規則表達式語法 AWS WAF](#)
- [中的 IP 集和 regex 模式集 AWS WAF](#)
- [中的自訂 Web 請求和回應 AWS WAF](#)
- [中的 Web 請求標籤 AWS WAF](#)
- [中的智慧型威脅防禦 AWS WAF](#)
- [保護 AWS WAF 套件或 Web ACL 流量的資料保護和記錄](#)
- [測試和調校您的 AWS WAF 保護](#)
- [AWS WAF 搭配 Amazon CloudFront 使用](#)
- [您使用 AWS WAF 服務時的安全性](#)
- [AWS WAF 配額](#)
- [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)

開始使用 AWS WAF

開始使用 AWS WAF 取決於您使用的主控制台體驗。這兩種體驗都可以存取相同的核心 AWS WAF 功能，但它們在您設定和管理 Web 應用程式保護的方式上有所不同。

AWS WAF 提供兩種使用 主控台的選項：

更新的主控制台旨在簡化標準主控台工作流程所需的 Web ACL 組態程序。您可以使用引導式工作流程，透過保護套件簡化 Web ACL 建立和管理程序。保護套件可讓您更輕鬆地在主控制台中使用和管理 Web ACLs，但功能與 Web ACL 沒有差異。除了改善的保護組態程序之外，更新的主控制台還透過安全儀表板提供增強的防護可見性，讓您更輕鬆地在 AWS WAF 主控制台中監控您的安全狀態。

標準 AWS WAF 主控制台提供使用 Web ACLs 設定 Web 應用程式防火牆保護的傳統方法。它提供對個別規則和規則群組的精細控制，並熟悉現有 AWS WAF 使用者。使用此主控制台，您可以詳細控制保護組態，以便精確自訂您的安全設定。

Tip

選擇最符合您需求的主控制台體驗。如果您是初次使用，AWS WAF 或想要根據 AWS 建議開始設定保護，我們建議您從更新的主控制台體驗開始。不過，標準體驗一律可從主控台的導覽窗格開啟。

下列各節提供兩種主控台體驗的入門指引。檢閱每個方法，並選取最符合您安全需求和操作偏好設定的方法：

主題

- [AWS WAF 開始使用更新的主控台體驗](#)
- [AWS WAF 開始使用標準主控台體驗](#)

AWS WAF 開始使用更新的主控台體驗

本節將引導您使用更新 AWS WAF 後的主控台體驗進行設定，這可提供簡化的組態工作流程和增強的安全管理功能。

存取新的主控台體驗

若要存取新的 AWS WAF 主控台體驗：

登入 AWS Management Console 並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。

- 在導覽窗格中，尋找並選取嘗試新的體驗。

Note

您可以隨時使用導覽窗格中的連結在主控台體驗之間切換。

開始使用保護套件

本教學課程說明如何建立和設定保護套件來保護您的應用程式。保護套件提供針對特定工作負載類型量身打造的預先設定安全規則。

於本教學課程中，您會了解如何：

- 建立保護套件
- 設定應用程式特定的保護設定
- 新增要保護 AWS 的資源
- 選擇和自訂保護規則
- 設定記錄和監控

 Note

AWS 通常會針對您在本教學課程中建立的資源，向您收取每天不到 0.25 USD 的費用。當您完成時，我們建議您刪除資源以免產生不必要的費用。

步驟 1：設定 AWS WAF

如果您尚未遵循 中的一般設定步驟[設定您的帳戶以使用 服務](#)，請立即執行此操作。

步驟 2：建立保護套件

在此步驟中，您將建立保護套件，並設定其基本設定以符合您的應用程式類型。

1. 登入 AWS Management Console 並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇資源與保護。
3. 在資源與保護頁面上，選擇新增保護套件。
4. 在告訴我們您的應用程式，針對應用程式類別，選取一或多個最能描述您應用程式的應用程式類別。
5. 針對流量來源，選擇應用程式處理的流量類型：
 - API - 僅適用於 API 的應用程式
 - Web - 僅適用於 Web 的應用程式
 - API 和 Web - 適用於處理這兩種流量的應用程式

步驟 3：新增要保護的資源

現在，您將指定要使用保護套件來保護哪些 AWS 資源。

1. 在要保護的資源下，選擇新增資源。
2. 選擇要與此保護套件建立關聯的 AWS 資源類別：
 - Amazon CloudFront 分佈
 - 區域資源

如需資源類型的詳細資訊，請參閱 [將保護與 AWS 資源建立關聯](#)。

步驟 4：選擇保護規則

在此步驟中，您將選取保護套件的保護規則。對於第一次使用的使用者，我們建議您選擇建議選項。

AWS WAF 會根據您在告訴我們您的應用程式區段中的選擇，為您產生建議的保護套件。這些套件會為您的應用程式類型實作安全最佳實務。

- 選擇下一步以繼續執行保護套件設定。

Note

如果您有興趣建立自訂規則或使用您建置的選項，建議您先取得預先設定選項的體驗。如需建立自訂保護套件和規則的詳細資訊，請參閱 [在中建立保護套件或 Web ACL AWS WAF](#)。

步驟 5：自訂保護套件設定

現在，您將設定其他設定，例如預設動作、速率限制和記錄。

1. 在名稱和描述下，輸入保護套件的名稱。或者，輸入描述。

Note

您無法在建立保護套件之後變更名稱。

2. 在自訂保護套件下，設定下列設定：
 - a. 在預設規則動作下，選擇不符合任何規則之請求的預設動作。如需詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。
 - b. 在規則組態下，自訂這些設定：
 - 預設速率限制 - 設定限制以防止 DDoS 攻擊
 - IP 地址 - 設定 IP 允許/封鎖清單
 - 國家/地區特定原始伺服器 - 依國家/地區管理存取權
 - c. 針對記錄目的地，設定您要存放日誌的位置。如需詳細資訊，請參閱 [AWS WAF 記錄目的地](#)。
3. 檢閱您的設定，然後選擇新增保護套件。

步驟 6：清除您的資源

現在，您已成功完成教學課程。為了防止您的帳戶產生 AWS WAF 額外費用，您應該刪除您建立的保護套件，或修改它以符合您的生產需求。

刪除您的保護套件

1. 在導覽窗格中，選擇資源與保護。
2. 選取您建立的保護套件。
3. 選擇垃圾桶圖示，然後輸入「刪除」來確認刪除。

Note

如果您計劃在生產環境中使用此保護套件，而不是將其刪除，您應該檢閱和調整保護設定，以符合應用程式的安全需求。

AWS WAF 開始使用標準主控台體驗

AWS WAF 主控台會引導您完成設定程序 AWS WAF，以根據您指定的條件封鎖或允許 Web 請求，例如請求源自的 IP 地址或請求中的值。在此步驟中，您會建立保護套件或 Web ACL。如需 AWS WAF 保護套件或 Web ACLs 的詳細資訊，請參閱 [在中設定保護 AWS WAF](#)。

本教學課程說明如何使用 AWS WAF 來執行下列任務：

- 設定 AWS WAF。
- 使用 AWS WAF 主控台內的精靈建立 Web 存取控制清單 (Web ACL)。

建立 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在 AWS WAF 首頁中，選擇建立 Web ACL。
3. 對於 Name (名稱)，輸入您要用來識別此 Web ACL 的名稱。

Note

建立 Web ACL 後無法修改名稱。

4. (選擇性) 對於 Description - optional (描述 - 選用性)，如果需要，請為 Web ACL 輸入較長的描述。
5. 對於 CloudWatch 指標名稱，如果適用，請變更預設名稱。遵循主控台上的指引，以瞭解有效的字元。名稱不能包含特殊字元、空格或保留給 AWS WAF 使用的指標名稱，包括「All」和「Default_Action」。

 Note

您無法在建立 Web ACL 之後變更 CloudWatch 指標名稱。

6. 對於 Resource type (資源類型)，選擇 CloudFront distributions (CloudFront 分發)。Region (區域) 會自動填入 CloudFront 分發的 Global (CloudFront) (全域 (CloudFront))。
7. (選用) 對於關聯的 AWS 資源 - 選用，選擇新增 AWS 資源。在對話方塊中，選擇您要關聯的資源，然後選擇新增。AWS WAF 會返回描述 Web ACL 和關聯的 AWS 資源頁面。
8. 選擇下一步。

 Note

AWS 對於您在本教學課程中建立的資源，通常會向您收取每天不到 0.25 USD 的費用。當您完成此教學課程，我們建議您刪除資源以免產生不必要的費用。

步驟 1：設定 AWS WAF

如果您尚未遵循 中的一般設定步驟 [設定您的帳戶以使用 服務](#)，請立即執行此操作。

步驟 2：建立 Web ACL

AWS WAF 主控台會引導您完成設定程序 AWS WAF，以根據您指定的條件封鎖或允許 Web 請求，例如請求源自的 IP 地址或請求中的值。在此步驟中，建立 Web ACL。如需 AWS WAF Web ACLs 的詳細資訊，請參閱 [在 中設定保護 AWS WAF](#)。

建立 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在 AWS WAF 首頁中，選擇建立 Web ACL。

3. 對於 Name (名稱)，輸入您要用來識別此 Web ACL 的名稱。

 Note

建立 Web ACL 後無法修改名稱。

4. (選擇性) 對於 Description - optional (描述 - 選用性)，如果需要，請為 Web ACL 輸入較長的描述。
5. 對於 CloudWatch 指標名稱，如果適用，請變更預設名稱。遵循主控台上的指引，以瞭解有效的字元。名稱不能包含特殊字元、空格或保留給 AWS WAF 使用的指標名稱，包括「All」和「Default_Action」。

 Note

您無法在建立 Web ACL 之後變更 CloudWatch 指標名稱。

6. 對於 Resource type (資源類型)，選擇 CloudFront distributions (CloudFront 分發)。Region (區域) 會自動填入 CloudFront 分發的 Global (CloudFront) (全域 (CloudFront))。
7. (選用) 對於關聯的 AWS 資源 - 選用，選擇新增 AWS 資源。在對話方塊中，選擇您要關聯的資源，然後選擇新增。AWS WAF 會返回描述 Web ACL 和關聯的 AWS 資源頁面。
8. 選擇下一步。

步驟 3：新增字串比對規則

在此步驟中，您會建立使用字串比對陳述式的規則，並指出如何處理比對請求。字串比對規則陳述式可識別您要 AWS WAF 在請求中搜尋的字串。通常，字串包含可列印 ASCII 字元，但您可以指定十六字元範圍 0x00 到 0xFF 的任何字元 (小數點 0 到 255)。除了指定要搜尋的字串之外，您還可以指定要搜尋的 Web 請求元件，例如標頭、查詢字串或請求內文。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

 Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀有關 AWS WAF 可檢查多少內容的限制在 [中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

如需 AWS WAF 規則的其他資訊，請參閱 [AWS WAF 規則](#)。

建立字串比對規則陳述式

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)、Add my own rules and rule groups (新增我自己的規則和規則群組)、Rule builder (規則建置器) 及 Rule visual editor (規則視覺化編輯器)。

Note

主控台提供 Rule visual editor (規則視覺化編輯器) 和 Rule JSON editor (規則 JSON 編輯器)。JSON 編輯器可讓您在 Web ACL 之間輕鬆複製組態，並且是更複雜的規則集所需，例如具有多層巢狀的規則集。

此程序使用 Rule visual editor (規則視覺化編輯器)。

2. 對於 Name (名稱)，輸入您要用來識別此規則的名稱。
3. 對於 Type (類型)，選擇 Regular rule (一般規則)。
4. 對於 If a request (如果請求)，選擇 matches the statement (比對陳述式)。

其他選項適用於邏輯規則陳述式類型。您可以使用它們來合併或否定其他規則陳述式的結果。

5. 在陳述式上，針對檢查，開啟下拉式清單，然後選擇您要檢查的 Web AWS WAF 請求元件。在此範例中，選擇單一標頭。

選擇單一標頭時，您也可以指定要 AWS WAF 檢查的標頭。輸入 **User-Agent**。此值不會區分大小寫。

6. 對於 Match type (比對類型)，選擇指定的字串必須顯示在 User-Agent 標頭中的位置。

對於此範例，選擇 Exactly matches string (完全符合字串)。這表示會 AWS WAF 檢查每個 Web 請求中的使用者代理程式標頭是否有與您指定的字串相同的字串。

7. 對於 String to match (要比對的字串)，指定您要 AWS WAF 搜尋的字串。String to match (符合值) 的長度上限為 200 個字元。如果您想要指定 base64 編碼值，可在編碼前指定最多 200 個字元。

在此範例中，輸入 MyAgent。AWS WAF 會在 Web 請求中檢查 User-Agent 標頭的值 MyAgent。

8. 將 Text transformation (文字轉換) 保持設定為 None (無)。
9. 針對動作，選取您希望規則在符合 Web 請求時採取的動作。在此範例中，選擇計數並保留其他選項。計數動作會為符合規則的 Web 請求建立指標，但不會影響是否允許或封鎖請求。如需動作選擇的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#) 和 [設定規則優先順序](#)。
10. 選擇新增規則。

步驟 4：新增 AWS 受管規則規則群組

AWS 受管規則提供一組受管規則群組供您使用，其中大部分都是免費提供給 AWS WAF 客戶。如需規則群組的詳細資訊，請參閱 [AWS WAF 規則群組](#)。我們會將 AWS 受管規則規則群組新增至此 Web ACL。

新增 AWS 受管規則規則群組

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。
2. 在新增受管規則群組頁面上，展開 AWS 受管規則群組的清單。(您也會看到提供給 AWS Marketplace 賣方的清單。您可以訂閱其方案，然後以與 AWS 受管規則規則群組相同的方式使用它們。)
3. 對於您要新增的規則群組，請執行下列動作：
 - a. 在動作欄中，開啟新增至 Web ACL 切換。
 - b. 選取編輯，然後在規則群組的規則清單中，開啟覆寫所有規則動作下拉式清單，然後選取 Count。這會將規則群組中所有規則的動作設定為僅計數。這可讓您查看規則群組中的所有規則如何在 Web 請求中運作，然後再使用任何規則群組。
 - c. 選擇儲存規則。
4. 在新增受管規則群組頁面中，選擇新增規則。這會讓您返回新增規則和規則群組頁面。

步驟 5：完成 Web ACL 組態

完成將規則和規則群組新增至 Web ACL 組態時，請在 Web ACL 中管理規則的優先順序，以及進行指標、標記和記錄等設定來完成工作。

完成您的 Web ACL 組態

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Next (下一步)。
2. 在設定規則優先順序頁面上，您可以在 Web ACL 中查看規則和規則群組的處理順序。會從清單頂端開始 AWS WAF 處理它們。您可以透過上下移動規則來變更處理順序。若要這樣做，請在清單中選取一個，然後選擇 Move up (上移) 或 Move down (下移)。如需有關規則優先順序的詳細資訊，請參閱 [設定規則優先順序](#)。
3. 選擇下一步。
4. 在設定指標頁面上，對於 Amazon CloudWatch 指標，您可以查看規則和規則群組的計劃指標，也可以查看 Web 請求取樣選項。如需檢視取樣請求的詳細資訊，請參閱 [檢視 Web 請求的範例](#)。如需 Amazon CloudWatch 指標的相關資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。

您可以在 AWS WAF 主控台的 Web ACL 頁面上，流量概觀索引標籤下存取 Web 流量指標的摘要。主控台儀表板提供 Web ACL Amazon CloudWatch 指標的近乎即時摘要。如需詳細資訊，請參閱 [保護套件或 Web ACLs 流量概觀儀表板](#)。

5. 選擇下一步。
6. 在 Review and create web ACL (檢閱並建立 Web ACL) 頁面上，檢閱您的設定，然後選擇 Create web ACL (建立 Web ACL)。

精靈會將您返回列出新 Web ACL 的 Web ACL 頁面。

步驟 6：清除您的資源

現在，您已成功完成教學課程。若要防止您的帳戶產生 AWS WAF 額外費用，請清除您建立的 AWS WAF 物件。或者，您可以變更組態以符合您真正要使用的 Web 請求 AWS WAF。

Note

AWS 對於您在本教學課程中建立的資源，通常會向您收取每天不到 0.25 USD 的費用。當您完成時，我們建議您刪除資源以免產生不必要的費用。

刪除 AWS WAF 收費的物件

1. 在 Web ACL 頁面中，從清單中選擇您的 Web ACL，然後選擇編輯。
2. 在關聯的 AWS 資源索引標籤上，針對每個相關聯的資源，選取資源名稱旁的選項按鈕，然後選擇取消關聯。這會取消 Web ACL 與 AWS 資源的關聯。

3. 在下列每個畫面中，選擇下一步，直到您返回 Web ACL 頁面。

在 Web ACL 頁面中，從清單中選擇您的 Web ACL，然後選擇刪除。

規則和規則陳述式無法存在於規則群組和 Web ACL 定義之外。如果您刪除 Web ACL，這會刪除您在 Web ACL 中定義的所有個別規則。當您從 Web ACL 移除某個規則群組時，您只是移除對它的參考。

如何 AWS WAF 運作

您可以使用 AWS WAF 來控制受保護的資源如何回應 HTTP(S) Web 請求。您可以透過定義 Web 存取控制清單 (Web ACL) 或保護套件，然後將其與您要保護的一或多個 Web 應用程式資源建立關聯來執行此操作。相關聯的資源會將傳入的請求轉送至 AWS WAF，以供保護套件或 Web ACL 檢查。

在保護套件或 Web ACL 中，您可以建立規則來定義要在請求中尋找的流量模式，並指定要對相符請求採取的動作。動作選擇包括下列項目：

- 允許請求前往受保護的資源進行處理和回應。
- 封鎖請求。
- 計數請求。
- 針對請求執行 CAPTCHA 或挑戰檢查，以驗證人類使用者和標準瀏覽器的使用。

AWS WAF 元件

以下是的中央元件 AWS WAF：

- Web ACLs – 您可以使用 Web 存取控制清單 (Web ACL) 來保護一組 AWS 資源。您可以建立一個 Web ACL，並透過新增規則來定義其保護策略。規則會定義檢查 Web 請求的條件，並指定針對符合其條件的請求所要採取的動作。您也可以為 Web ACL 設定預設動作，指出是否透過規則尚未封鎖或允許的任何請求來封鎖或允許。如需 Web ACL 的詳細資訊，請參閱[在中設定保護 AWS WAF](#)。

Web ACL 是 AWS WAF 資源。

- 保護套件 – 您可以使用保護套件來保護一組 AWS 資源。保護套件在新主控台中執行的函數基本上與 Web ACLs 相同。您可以建立保護套件，並透過新增規則來定義其保護策略。規則會定義檢查 Web 請求的條件，並指定針對符合其條件的請求所要採取的動作。您也可以為保護套件設定預設動作，指出是否透過規則尚未封鎖或允許的任何請求來封鎖或允許。如需保護套件的詳細資訊，請參閱[在中設定保護 AWS WAF](#)。

保護套件是 AWS WAF 資源。

- 規則 – 每個規則都包含定義檢查條件的陳述式，以及在 Web 請求符合條件時要採取的動作。當 Web 請求符合準則時，這是一個相符。您可以設定規則來封鎖相符的請求、允許它們通過、計數它們，或對使用 CAPTCHA 拼圖或無提示用戶端瀏覽器挑戰的請求執行機器人控制。如需規則的詳細資訊，請參閱[AWS WAF 規則](#)。

規則不是 AWS WAF 資源。它只存在於保護套件或 Web ACL 或規則群組的內容中。

- 規則群組 – 您可以直接在保護套件或 Web ACL 內或在可重複使用的規則群組中定義規則。AWS 受管規則和 AWS Marketplace 賣方提供受管規則群組供您使用。您也可以定義自己的規則群組。如需規則群組的詳細資訊，請參閱[AWS WAF 規則群組](#)。

規則群組是 AWS WAF 資源。

- Web ACL 容量單位 (WCUs) – AWS WAF 使用 WCUs 計算和控制執行規則、規則群組、保護套件或 Web ACLs 所需的操作資源。

WCU 不是 AWS WAF 資源。它只存在於保護套件或 Web ACL、規則或規則群組的內容中。

您可以使用 保護的資源 AWS WAF

您可以使用 AWS WAF 保護套件或 Web ACL 來保護全域或區域資源類型。您可以透過將保護套件或 Web ACL 與您要保護的資源建立關聯來執行此操作。保護套件或 Web ACL 及其使用的任何 AWS WAF 資源都必須位於關聯資源所在的區域中。對於 Amazon CloudFront 分佈，這會設定為美國東部（維吉尼亞北部）。

Amazon CloudFront 分佈

您可以使用 AWS WAF 主控台或 APIs，將 AWS WAF 保護套件或 Web ACL 與 CloudFront 分佈建立關聯。您也可以在建立或更新分佈本身時，將保護套件或 Web ACL 與 CloudFront 分佈建立關聯。若要在中設定關聯 AWS CloudFormation，您必須使用 CloudFront 分佈組態。如需 Amazon CloudFront 的相關資訊，請參閱《Amazon CloudFront 開發人員指南》中的[使用 AWS WAF 控制對內容的存取](#)。

AWS WAF 可供 CloudFront 分發全域使用，但您必須使用美國東部區域（維吉尼亞北部）來建立保護套件或 Web ACL，以及保護套件或 Web ACL 中使用的任何資源，例如規則群組、IP 集和 regex 模式集。有些界面提供「全域 (CloudFront)」的區域選擇。選擇此選項與選擇美國東部（維吉尼亞北部）或「us-east-1」區域相同。

區域資源

您可以在 AWS WAF 可使用的所有區域中保護區域資源。您可以在的[AWS WAF 端點和配額](#)中查看清單 Amazon Web Services 一般參考。

您可以使用 AWS WAF 來保護下列區域資源類型：

- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 已驗證的存取執行個體
- AWS Amplify

您只能將保護套件或 Web ACL 與其中的 Application Load Balancer 建立關聯 AWS 區域。例如，您無法將保護套件或 Web ACL 與開啟的 Application Load Balancer 建立關聯 AWS Outposts。

您必須建立想要與 Global CloudFront 區域中的 Amplify 應用程式建立關聯的任何保護套件或 Web ACL。您的 中可能已有區域保護套件或 Web ACL AWS 帳戶，但它們與 Amplify 不相容。

保護套件或 Web ACL 及其使用的任何其他 AWS WAF 資源必須位於與受保護資源相同的區域中。監控和管理受保護區域資源的 Web 請求時，會將所有資料 AWS WAF 保留在與受保護資源相同的區域中。

多個資源關聯的限制

您可以使用下列限制，將單一保護套件或 Web ACL 與一或多個 AWS 資源建立關聯：

- 每個 AWS 資源只能與一個保護套件或 Web ACL 建立關聯。保護套件或 Web ACL 與 AWS 資源之間的關係是 one-to-many。
- 您可以將保護套件或 Web ACL 與一或多個 CloudFront 分佈建立關聯。您無法將與 CloudFront 分佈相關聯的保護套件或 Web ACL 與任何其他 AWS 資源類型建立關聯。

使用更新的主控制台體驗

AWS WAF 提供兩種使用 主控台的選項：

更新的主控制台旨在簡化標準主控台工作流程所需的 Web ACL 組態程序。您可以使用引導式工作流程，透過保護套件簡化 Web ACL 建立和管理程序。保護套件可讓您更輕鬆地在主控制台中使用和管理 Web ACLs，但功能與 Web ACL 沒有差異。除了改善的保護組態程序之外，更新的主控制台還透過安全儀表板提供增強的防護可見性，讓您更輕鬆地在 AWS WAF 主控制台中監控您的安全狀態。

標準 AWS WAF 主控台提供使用 Web ACLs 設定 Web 應用程式防火牆保護的傳統方法。它提供對個別規則和規則群組的精細控制，並熟悉現有 AWS WAF 使用者。使用此主控台，您可以詳細控制保護組態，以便精確自訂您的安全設定。

Tip

選擇最符合您的需求的主控台體驗。如果您是初次使用，AWS WAF 或想要根據 AWS 建議開始設定保護，我們建議您從更新的主控台體驗開始。不過，標準體驗一律可從主控台的導覽窗格開啟。

已更新和標準主控台體驗之間的功能同位

更新的主控台體驗可維持與現有主控台的完整功能同位，同時引進新功能：

- 所有現有 AWS WAF 功能仍然可用
- 透過統一儀表板增強可見性
- 簡化的組態工作流程
- 新的保護套件範本

Important

更新的主控台體驗使用與現有主控台相同的 WAFv2 APIs。這表示在更新主控台中建立的保護套件會在 API 層級實作為標準 WAFv2 Web ACLs。

主要差異

主控台體驗的比較

功能	先前的 AWS WAF 主控台體驗	更新的主控台體驗
組態程序	多頁工作流程	單頁界面
規則組態	建立個別規則	預先設定保護套件的選項
監控	個別儀表板	統一可見性

了解新的儀表板

可透過更新的儀表板透過這些視覺化提供統一的安全狀態可見性：

流量洞察建議 – AWS 威脅情報會監控您過去 2 週的允許流量、分析漏洞，並提供下列項目：

- 流量型規則建議
- 應用程式特定的安全建議
- 保護最佳化指引

摘要 – 顯示指定時間範圍內所有流量的請求計數。您可以使用下列條件來篩選流量資料：

- 規則 – 依保護套件中的個別規則篩選。
- 動作 – 顯示對 Allow、Block、Captcha 和 Challenge 等流量所採取特定動作的計數。
- 流量類型 – 僅顯示特定流量類型的計數，例如 anti-DDoS 或機器人。
- 時間範圍 – 從預先定義的時間範圍中選擇，或設定自訂範圍。
- 本機或 UTC 時間 – 您可以設定偏好的時間格式。

保護活動 – 視覺化您的保護規則及其順序對終止動作有何貢獻。

- 流量流經您的規則 – 顯示流量流經您的規則。從連續規則檢視切換到非連續規則檢視，以查看規則順序如何影響結果。
- 規則動作及其結果 – 顯示規則在指定期間內對流量採取的終止動作。

動作總計 – 視覺化在指定時間範圍內對請求所採取動作總數的圖表。使用 Overlay 過去 3 小時選項，將目前時間範圍與前 3 小時時間範圍進行比較。您可以依下列條件篩選資料：

- 允許動作
- 動作總數
- Captcha 動作
- 挑戰動作
- 封鎖動作

所有規則 – 視覺化保護套件中所有規則指標的圖表。

- 使用 Overlay 過去 3 小時選項，比較目前時間範圍與前 3 小時時間範圍。

概觀儀表板 – 提供安全狀態的完整圖形檢視，包括下列項目：

- 流量特性 – 請參閱依原始伺服器、攻擊類型或依傳送請求之用戶端裝置類型的流量概觀。
- 規則特性 – 10 個最常見規則和終止動作的攻擊明細。
- 機器人 – 視覺化機器人活動、偵測、類別和機器人相關訊號標籤。

- 反 DDoS – 偵測到和緩解的 layer 7 DDoS 活動的概觀。

在中設定保護 AWS WAF

此頁面說明什麼是保護套件和 Web 存取控制清單 (Web ACLs)，以及它們的運作方式。

保護套件或 Web ACL 基本上執行相同的函數。兩者都可讓您精細控制受保護資源回應的所有 HTTP(S) Web 請求。您可以保護 Amazon CloudFront、Amazon API Gateway、Application Load Balancer、AWS AppSync、Amazon Cognito、AWS App Runner、AWS Amplify 和 AWS Verified Access 資源。您可以在新的主控台體驗中使用保護套件，並在標準主控台中使用 Web ACLs。如需新主控台體驗的詳細資訊，請參閱 [使用更新的主控台體驗](#)。

您可以使用如下的準則來允許或封鎖請求：

- 請求的 IP 地址來源
- 請求的來源國家/地區
- 字串比對或規則運算式 (regex) 在請求的一部分比對
- 請求的特定部分的大小
- 偵測惡意 SQL 程式碼或指令碼

您也可以測試這些條件的任何組合。您可以封鎖或計數不僅符合指定條件的 Web 請求，也可以在一分鐘內超過指定的請求數量。您可以使用邏輯運算子結合條件。您也可以針對請求執行 CAPTCHA 拼圖和靜音用戶端工作階段挑戰。

您在 AWS WAF 規則陳述式中提供相符條件和要對相符項目採取的動作。您可以直接在保護套件或 Web ACL 內，以及您在保護套件或 Web ACL 中使用的可重複使用規則群組中定義規則陳述式。如需選項的完整清單，請參閱 [在中使用規則陳述式 AWS WAF](#) 和 [在中使用規則動作 AWS WAF](#)。

當您建立保護套件或 Web ACL 時，您可以指定要使用的資源類型。如需相關資訊，請參閱 [在中建立保護套件或 Web ACL AWS WAF](#)。定義保護套件或 Web ACL 之後，您可以將其與您的資源建立關聯，以開始為它們提供保護。如需詳細資訊，請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。

Note

在某些情況下，AWS WAF 可能會遇到內部錯誤，延遲回應有關是否允許或封鎖請求的相關聯 AWS 資源。在這些情況下，CloudFront 通常會允許請求或提供內容，而區域服務通常會拒絕請求且不提供內容。

⚠ 生產流量風險

在保護套件或 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

📘 Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱[中的 Web ACL 容量單位 \(WCUs\) AWS WAF](#) 和 [AWS WAF 定價](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新的地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

主題

- [在 中建立保護套件或 Web ACL AWS WAF](#)
- [在 中編輯保護套件或 Web ACL AWS WAF](#)
- [管理規則群組行為](#)
- [將保護與 AWS 資源建立關聯或取消關聯](#)
- [在 中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)

- [在 中設定保護套件或 Web ACL 預設動作 AWS WAF](#)
- [管理 的內文檢查大小限制 AWS WAF](#)
- [在 中設定 CAPTCHA、挑戰和字符 AWS WAF](#)
- [在 中檢視 Web 流量指標 AWS WAF](#)
- [刪除保護套件或 Web ACL](#)

在 中建立保護套件或 Web ACL AWS WAF

Creating a protection pack

本節提供透過 AWS 主控台建立保護套件的程序。

若要建立新的保護套件，請依照此頁面的程序使用保護套件建立精靈。

生產流量風險

在生產流量的保護套件中部署變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#) 和 [AWS WAF 定價](#)。

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇資源與保護。
3. 在資源與保護頁面上，選擇新增保護套件。
4. 在告訴我們您的應用程式，針對應用程式類別，選取一或多個應用程式類別。
5. 針對流量來源，選擇應用程式與 API、Web 或 API 和 Web 兩者互動的流量類型。
6. 在要保護的資源下，選擇新增資源。

7. 選擇您要與此保護套件建立關聯的資源類別 AWS，Amazon CloudFront 分佈或區域資源。如需詳細資訊，請參閱[將保護與 AWS 資源建立關聯或取消關聯](#)。
8. 在選擇規則保護下，選取您偏好的保護層級：建議、必要或您建置。
9. （選用）如果您選擇您建置它，請建置您的規則。
 - a. （選用）如果您想要新增自己的規則，請在新增規則頁面上，選擇自訂規則，然後選擇下一步。
 - i. 選擇規則類型。
 - ii. 對於 Action (動作)，選取規則在比對到 Web 請求時要採取的動作。如需有關您的選擇的相關資訊，請參閱[在 中使用規則動作 AWS WAF](#)和[在 中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

如果您使用 CAPTCHA 或 Challenge 動作，請視需要調整規則的抗擾性時間組態。如果您未指定設定，則規則會從保護套件繼承它。若要修改保護套件豁免時間設定，請在建立保護套件之後對其進行編輯。如需豁免時間的詳細資訊，請參閱[在 中設定時間戳記過期和字符豁免時間 AWS WAF](#)。

 Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

如果您想要自訂請求或回應，請選擇該請求的選項，並填寫自訂的詳細資訊。如需詳細資訊，請參閱[中的自訂 Web 請求和回應 AWS WAF](#)。

如果您想要讓規則將標籤新增至相符的 Web 請求，請選擇該請求的選項，然後填入標籤詳細資訊。如需詳細資訊，請參閱[中的 Web 請求標籤 AWS WAF](#)。

- iii. 對於 Name (名稱)，輸入您要用來識別此規則的名稱。請勿使用以 AWS、PreFM、Shield 或開頭的名稱 PostFM。這些字串是預留的，或可能導致與其他服務為您管理的規則群組混淆。
- iv. 根據您的需求輸入規則定義。您可以在邏輯 AND 和規則陳述式中結合 OR 規則。精靈會根據內容，引導您完成每個規則的選項。如需規則選項的相關資訊，請參閱[AWS WAF 規則](#)。
- v. 選擇建立規則。

 Note

如果您將多個規則新增至保護套件，會依照為保護套件列出的順序 AWS WAF 來評估規則。如需詳細資訊，請參閱[在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

- b. (選用) 如果您要新增受管規則群組，請在新增規則頁面上，選擇 AWS 受管規則群組或 AWS Marketplace 規則群組，然後選擇下一步。對於您要新增的每個受管規則群組執行下列動作：
 - i. 在新增規則頁面上，展開受管 AWS 規則群組或 AWS Marketplace 賣方的清單。
 - ii. 選擇規則群組的版本。
 - iii. 若要自訂保護套件如何使用規則群組，請選擇編輯。以下是常見的自訂設定：
 - 在檢查區段中新增縮小範圍陳述式，以減少規則群組檢查的 Web 請求範圍。如需此選項的詳細資訊，請參閱[在中使用縮小範圍陳述式 AWS WAF](#)。
 - 覆寫規則覆寫中部分或全部規則的規則動作。如果您未定義規則的覆寫動作，評估會使用規則群組內定義的規則動作。如需此選項的詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。
 - 有些受管規則群組會要求您提供額外的組態。請參閱受管規則群組提供者的文件。如需 AWS 受管規則規則群組的特定資訊，請參閱[AWS 的受管規則 AWS WAF](#)。
 - iv. 選擇下一步。
- c. (選用) 如果您要新增自己的規則群組，請在新增規則頁面上，選擇自訂規則群組，然後選擇下一步。對於您要新增的每個規則群組執行下列動作：
 - i. 針對名稱，在此保護套件中輸入您要用於規則群組規則的名稱。請勿使用以 AWS、PreFM、Shield 或開頭的名稱 PostFM。這些字串是預留的，或可能導致與其他服務為您管理的規則群組混淆。請參閱[辨識其他服務提供的規則群組](#)。
 - ii. 從清單中選擇您的規則群組。
 - iii. (選用) 在規則組態下，選擇規則覆寫。您可以將規則動作覆寫為任何有效的動作設定，就像對受管規則群組所做的一樣。
 - iv. (選用) 在新增標籤下，選擇新增標籤，然後輸入要新增至符合規則之請求的任何標籤。稍後在相同保護套件中評估的規則可以參考此規則新增的標籤。
 - v. 選擇建立規則。

10. 在名稱和描述下，輸入保護套件的名稱。或者，輸入描述。

 Note

您無法在建立保護套件之後變更名稱。

11. (選用) 在自訂保護套件下，設定預設規則動作、組態和記錄目的地：
 - a. (選用) 在預設規則動作下，選擇保護套件的預設動作。這是當保護套件中的規則未明確 AWS WAF 採取動作時，對請求採取的動作。如需詳細資訊，請參閱[中的自訂 Web 請求和回應 AWS WAF](#)。
 - b. (選用) 在規則組態下，自訂保護套件中規則的設定：
 - 預設速率限制 - 設定速率限制以封鎖可能影響可用性、危及安全性或耗用過多資源的阻斷服務 (DoS) 特性。此規則速率會封鎖每個 IP 地址超出應用程式允許速率的請求。如需詳細資訊，請參閱[在中使用以速率為基礎的規則陳述式 AWS WAF](#)
 - IP 地址 - 輸入要封鎖或允許的 IP 地址。此設定會覆寫其他保護規則。
 - 國家/地區特定原始伺服器 - 封鎖來自指定國家/地區的請求或計算所有流量。
 - c. 針對記錄目的地，設定記錄目的地類型和存放日誌的位置。如需詳細資訊，請參閱[AWS WAF 記錄目的地](#)。
12. 檢閱您的設定，然後選擇新增保護套件。

Creating a web ACL

本節提供透過 AWS 主控台建立 Web ACLs 的程序。

若要建立新的 Web ACL，請依照此頁面的程序使用 Web ACL 建立精靈。

 生產流量風險

在 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs](#)、[AWS WAF](#) 和 [AWS WAF 定價](#)。

建立 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中選擇 Web ACLs，然後選擇建立 Web ACL。
3. 對於 Name (名稱)，輸入您要用來識別此 Web ACL 的名稱。

Note

建立 Web ACL 後無法修改名稱。

4. (選擇性) 對於 Description - optional (描述 - 選用性)，如果需要，請為 Web ACL 輸入較長的描述。
5. 對於 CloudWatch 指標名稱，如果適用，請變更預設名稱。遵循主控台上的指引，以瞭解有效的字元。名稱不能包含特殊字元、空格或保留給的指標名稱 AWS WAF，包括 "All" 和 "Default_Action"。

Note

您無法在建立 Web ACL 之後變更 CloudWatch 指標名稱。

6. 在資源類型下，選擇要與此 Web ACL 建立關聯的資源類別 AWS，Amazon CloudFront 分佈或區域資源。如需詳細資訊，請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。
7. 對於區域，如果您已選擇區域資源類型，請選擇 AWS WAF 您要存放 Web ACL 的區域。

您只需為區域資源類型選擇此選項。對於 CloudFront 分佈，區域會硬式編碼至美國東部（維吉尼亞北部）區域 us-east-1，適用於全域 (CloudFront) 應用程式。

8. (CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access) 對於 Web 請求檢查大小限制 - 選用，如果您想要指定不同的內文檢查大小限制，請選取限制。在預設的 16

KB 上檢查內文大小可能會產生額外費用。如需此選項的詳細資訊，請參閱[管理的內文檢查大小限制 AWS WAF](#)。

9. (選用) 對於關聯的 AWS 資源 - 選用，如果您現在要指定資源，請選擇新增 AWS 資源。在對話方塊中，選擇您要關聯的資源，然後選擇 Add. AWS WAF returns you to the Describe Web ACL and associated AWS resources page。

 Note

當您選擇將 Application Load Balancer 與 Web ACL 建立關聯時，就會啟用資源層級 DDoS 保護。如需詳細資訊，請參閱[AWS WAF 分散式阻斷服務 \(DDoS\) 預防](#)。

10. 選擇下一步。
11. (選用) 如果您要新增受管規則群組，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。對於您要新增的每個受管規則群組執行下列動作：
- 在新增受管規則群組頁面上，展開受管 AWS 規則群組或您選擇的 AWS Marketplace 賣方的清單。
 - 對於您要新增的規則群組，請在動作欄中開啟新增至 Web ACL 切換。

若要自訂 Web ACL 使用規則群組的方式，請選擇編輯。以下是常見的自訂設定：

- 覆寫部分或全部規則的規則動作。如果您未定義規則的覆寫動作，評估會使用規則群組內定義的規則動作。如需此選項的詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。
- 新增縮小範圍陳述式，以減少規則群組檢查的 Web 請求範圍。如需此選項的詳細資訊，請參閱[在中使用縮小範圍陳述式 AWS WAF](#)。
- 有些受管規則群組會要求您提供額外的組態。請參閱受管規則群組提供者的文件。如需 AWS 受管規則規則群組的特定資訊，請參閱[AWS 的受管規則 AWS WAF](#)。

完成設定後，請選擇儲存規則。

選擇 Add rules (新增規則) 以完成新增受管規則，並回到 Add rules and rule group (新增規則和規則群組) 頁面。

Note

如果您將多個規則新增至 Web ACL，會依針對 Web ACL 列出的順序 AWS WAF 評估規則。如需詳細資訊，請參閱 [在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

12. (選用) 如果您要新增自己的規則群組，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add my own rules and rule groups (新增我自己的規則和規則群組)。對於您要新增的每個規則群組執行下列動作：
 - a. 在 Add my own rules and rule groups (新增我自己的規則和規則群組) 頁面上，選擇 Rule group (規則群組)。
 - b. 針對名稱，輸入您要在此 Web ACL 中用於規則群組規則的名稱。請勿使用以 AWS、PreFM、Shield 或開頭的名稱 PostFM。這些字串是預留的，或可能導致與其他服務為您管理的規則群組混淆。請參閱 [辨識其他服務提供的規則群組](#)。
 - c. 從清單中選擇您的規則群組。

Note

如果您想要覆寫自己的規則群組的規則動作，請先將其儲存至 Web ACL，然後在 Web ACL 的規則清單中編輯 Web ACL 和規則群組參考陳述式。您可以將規則動作覆寫為任何有效的動作設定，就像對受管規則群組所做的一樣。

- d. 選擇新增規則。
13. (選用) 如果您要新增自己的規則，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)、Add my own rules and rule groups (新增我自己的規則和規則群組)、Rule builder (規則建置器) 及 Rule visual editor (規則視覺化編輯器)。

Note

主控台 Rule visual editor (規則視覺化編輯器) 支援一個層級的巢狀化。例如，您可以使用單一邏輯 AND 或 OR 陳述式，並在其中巢狀一個層級的其他陳述式，但您無法在邏輯陳述式中巢狀化邏輯陳述式。若要管理更複雜的規則陳述式，請使用 Rule JSON editor (規則 JSON 編輯器)。如需有關規則的所有選項的資訊，請參閱 [AWS WAF 規則](#)。

此程序涵蓋 Rule visual editor (規則視覺化編輯器)。

- a. 對於 Name (名稱)，輸入您要用來識別此規則的名稱。請勿使用以 AWS、PreFM、Shield 或開頭的名稱 PostFM。這些字串是預留的，或可能導致與其他服務為您管理的規則群組混淆。
- b. 根據您的需求輸入規則定義。您可以在邏輯 AND 和規則陳述式中結合 OR 規則。精靈會根據內容，引導您完成每個規則的選項。如需規則選項的相關資訊，請參閱 [AWS WAF 規則](#)。
- c. 對於 Action (動作)，選取規則在比對到 Web 請求時要採取的動作。如需有關您的選擇的相關資訊，請參閱 [在中使用規則動作 AWS WAF](#) 和 [在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

如果您使用的是 CAPTCHA 或 Challenge 動作，請視需要調整規則的抗擾性時間組態。如果您未指定設定，則規則會從 Web ACL 繼承它。若要修改 Web ACL 豁免時間設定，請在建立 Web ACL 之後對其進行編輯。如需豁免時間的詳細資訊，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。

 Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

如果您想要自訂請求或回應，請選擇該請求的選項，並填寫自訂的詳細資訊。如需詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

如果您想要讓規則將標籤新增至相符的 Web 請求，請選擇該請求的選項，然後填入標籤詳細資訊。如需詳細資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#)。

- d. 選擇新增規則。
14. 選擇 Web ACL 的預設動作，Block 或 Allow。這是當 Web ACL 中的規則未明確允許或封鎖請求時，對請求 AWS WAF 採取的動作。如需詳細資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

如果您想要自訂預設動作，請選擇該動作的選項，然後填入自訂的詳細資訊。如需詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

15. 您可以定義權杖網域清單，以在受保護的應用程式之間啟用權杖共用。當您使用 AWS 受管規則規則群組進行 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP)、AWS WAF 詐騙控制帳戶接

管預防 (ATP) 和 AWS WAF 機器人控制時，CAPTCHA 和 Challenge 動作以及您實作的應用程式整合 SDKs 會使用字符。

不允許公有尾碼。例如，您無法使用 gov.au 或 co.uk 做為權杖網域。

根據預設，只 AWS WAF 接受受保護資源網域的權杖。如果您在此清單中新增權杖網域，會 AWS WAF 接受清單中所有網域的權杖，以及相關資源的網域的權杖。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

16. 選擇下一步。
17. 在設定規則優先順序頁面中，選取規則和規則群組，並將其移至您要 AWS WAF 處理的順序。從清單頂端 AWS WAF 開始處理規則。當您儲存 Web ACL 時，會依照您列出的順序，將數值優先順序設定 AWS WAF 指派給規則。如需詳細資訊，請參閱 [設定規則優先順序](#)。
18. 選擇下一步。
19. 在設定指標頁面中，檢閱選項並套用您需要的任何更新。您可以為多個來源提供相同的 CloudWatch 指標名稱，以結合多個來源的指標。
20. 選擇下一步。
21. 在 Review and create web ACL (檢閱並建立 Web ACL) 頁面中，檢查您的定義。如果您要變更任何區域，請針對區域選擇 Edit (編輯)。這會帶您回到 Web ACL 精靈中的頁面。進行任何變更，然後在頁面中選擇 Next (下一步)，直到您返回 Review and create web ACL (檢閱並建立 Web ACL) 頁面為止。
22. 選擇 建立 Web ACL。您的新 Web ACL 會列在 Web ACLs 頁面中。

在中編輯保護套件或 Web ACL AWS WAF

Editing a protection pack

本節提供透過 AWS 主控台編輯保護套件的程序。

若要從保護套件新增或移除規則或變更組態設定，請使用此頁面上的程序存取保護套件。更新保護套件時，會為您與保護套件相關聯的資源 AWS WAF 提供持續涵蓋。

生產流量風險

在生產流量的保護套件中部署變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱 [測試和調校您的 AWS WAF 保護](#)。

 Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs](#)、[AWS WAF](#) 和 [AWS WAF 定價](#)。

編輯保護套件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇資源與保護。
3. 選擇您要編輯的保護套件。主控台可讓主要保護套件卡可編輯，也會開啟附帶您可以編輯之詳細資訊的側邊窗格。
4. 視需要編輯保護套件。

以下列出可編輯的保護套件組態元件。

本節提供透過 AWS 主控台編輯 Web ACLs 的程序。

若要從 Web ACL 新增或移除規則或變更組態設定，請使用此頁面上的程序存取 Web ACL。更新 Web ACL 時，會為您與 Web ACL 相關聯的資源 AWS WAF 提供持續涵蓋。

 生產流量風險

在 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

 Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs](#)、[AWS WAF](#) 和 [AWS WAF 定價](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到資源存放的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

Editing a web ACL

本節提供透過 AWS 主控台編輯 Web ACLs 的程序。

若要從 Web ACL 新增或移除規則或變更組態設定，請使用此頁面上的程序存取 Web ACL。更新 Web ACL 時，會為您與 Web ACL 相關聯的資源 AWS WAF 提供持續涵蓋。

生產流量風險

在 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱[中的 Web ACL 容量單位 WCUs\) AWS WAF](#) 和 [AWS WAF 定價](#)。

編輯 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Web ACLs。
3. 選擇您要編輯的 Web ACL 名稱。主控台會帶您前往 Web ACL 的描述。
4. 視需要編輯 Web ACL。選取您感興趣的組態區域的標籤，然後編輯可變設定。對於您編輯的每個設定，當您選擇儲存並返回 Web ACL 的描述頁面時，主控台會將您的變更儲存到 Web ACL。

以下列出包含 Web ACL 組態元件的標籤。

- 規則索引標籤
 - Web ACL 中定義的規則 – 您可以編輯和管理您在 Web ACL 中定義的規則，類似於您在 Web ACL 建立期間所做的操作。

Note

請勿變更您未手動新增至 Web ACL 的任何規則名稱。如果您使用其他服務來管理規則，變更其名稱可能會移除或降低其提供預期保護的能力。AWS Shield Advanced 和 AWS Firewall Manager 都可以在您的 Web ACL 中建立規則。如需相關資訊，請參閱[辨識其他服務提供的規則群組](#)。

Note

如果您變更規則的名稱，並且希望規則的指標名稱反映變更，則也必須更新指標名稱。當您變更規則名稱時 AWS WAF，不會自動更新規則的指標名稱。您可以使用規則 JSON 編輯器，在主控台中編輯規則時變更指標名稱。您也可以透過 APIs 和用於定義保護套件或 Web ACL 或規則群組的任何 JSON 清單中變更這兩個名稱。

如需規則和規則群組設定的相關資訊，請參閱 [AWS WAF 規則](#) 和 [AWS WAF 規則群組](#)。

- 使用的 Web ACL 規則容量單位 – Web ACL 目前的容量使用量。這只是檢視。
- 不符合任何規則之請求的預設 Web ACL 動作 – 如需此設定的相關資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

- Web ACL CAPTCHA 和挑戰組態 – 這些豁免時間會決定 CAPTCHA 或挑戰字符在取得後保持有效的時間。建立 Web ACL 後，您只能在此處修改此設定。如需這些設定的資訊，請參閱 [在 中設定時間戳記過期和字符豁免時間 AWS WAF](#)。
- 字符網域清單 – AWS WAF 接受清單中所有網域的字符，以及相關聯資源的網域的字符。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。
- 關聯的 AWS 資源索引標籤
 - Web 請求檢查大小限制 – 僅包含保護 CloudFront 分佈 ACLs。內文檢查大小限制會決定要轉送多少內文元件 AWS WAF 以進行檢查。如需有關此設定的詳細資訊，請參閱 [管理的內文檢查大小限制 AWS WAF](#)。
 - 關聯的 AWS 資源 – Web ACL 目前與 建立關聯和保護的資源清單。您可以找到與 Web ACL 位於相同區域內的資源，並將其與 Web ACL 建立關聯。如需詳細資訊，請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。
- 自訂回應內文索引標籤
 - 自訂回應主體，可供動作設為 的 Web ACL 規則使用 Block。如需詳細資訊，請參閱 [傳送 Block 動作的自訂回應](#)。
- 記錄和指標索引標籤
 - 記錄 – 記錄 Web ACL 評估的流量。如需相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
 - Security Lake 整合 – 您在 Amazon Security Lake 中為 Web ACL 設定的任何資料收集的狀態。如需詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的 [從 AWS 服務收集資料](#)。
 - 範例請求 – 符合 Web 請求之規則的相關資訊。如需檢視取樣請求的詳細資訊，請參閱 [檢視 Web 請求的範例](#)。
 - 資料保護設定 – 您可以設定 Web 流量資料修訂和篩選可用於 Web ACL 的所有資料，以及僅針對 AWS WAF 傳送至已設定 Web ACL 記錄目的地的資料。如需資料保護的相關資訊，請參閱 [保護 AWS WAF 套件或 Web ACL 流量的資料保護和記錄](#)。
 - CloudWatch 指標 – Web ACL 中規則的指標。如需 Amazon CloudWatch 指標的相關資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到資源存放的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

管理規則群組行為

本節說明在保護套件或 Web ACL 中修改規則群組使用方式的選項。此資訊適用於所有規則群組類型。將規則群組新增至保護套件或 Web ACL 之後，您可以將規則群組中個別規則的動作覆寫為 `Count` 或覆寫為任何其他有效的規則動作設定。您也可以將規則群組產生的動作覆寫為 `Count`，這不會影響規則群組內評估規則的方式。

如需這些選項的資訊，請參閱 [在中覆寫規則群組動作 AWS WAF](#)。

覆寫規則群組中的規則動作

對於保護套件或 Web ACL 中的每個規則群組，您可以覆寫包含規則的部分或全部規則的動作。

最常見的使用案例是將規則動作覆寫為 `Count` 以測試新的或更新的規則。如果您已啟用指標，則會收到您覆寫之每個規則的指標。如需測試的詳細資訊，請參閱 [測試和調校您的 AWS WAF 保護](#)。

當您將受管規則群組新增至保護套件或 Web ACL 時，可以進行這些變更，也可以在編輯保護套件或 Web ACL 時將其新增至任何類型的規則群組。這些指示適用於已新增至保護套件或 Web ACL 的規則群組。如需此選項的詳細資訊，請參閱 [規則群組規則動作覆寫](#)。

protection pack

覆寫規則群組中的規則動作

1. 選擇您要編輯的保護套件。主控台可讓主要保護套件卡片可編輯，也會開啟側邊面板，其中包含您可以編輯的詳細資訊。
2. 在保護套件卡片中，選擇規則旁的編輯連結，以開啟管理規則面板。
3. 在規則群組的管理規則區段中，選擇受管規則以開啟其動作設定。

- 覆寫規則群組 – 將規則群組動作變更為計數模式，但所有個別規則動作保持不變。
 - 覆寫所有規則動作 – 將規則動作套用至所有規則，覆寫其目前狀態。
 - 單一規則覆寫 – 將規則動作套用至個別規則。
4. 完成變更後，請選擇儲存規則。

web ACL

覆寫規則群組中的規則動作

1. 編輯 Web ACL。
2. 在 Web ACL 頁面規則索引標籤中，選取規則群組，然後選擇編輯。
3. 在規則群組的規則區段中，視需要管理動作設定。
 - 所有規則 – 若要為規則群組中的所有規則設定覆寫動作，請開啟覆寫所有規則動作下拉式清單，然後選取覆寫動作。若要移除所有規則的覆寫，請選取移除所有覆寫。
 - 單一規則 – 若要設定單一規則的覆寫動作，請開啟規則的下拉式清單，然後選取覆寫動作。若要移除規則的覆寫，請開啟規則的下拉式清單，然後選取移除覆寫。
4. 完成變更後，請選擇儲存規則。規則動作和覆寫動作設定會列在規則群組頁面中。

下列範例 JSON 清單顯示保護套件或 Web ACL 內的規則群組宣告，覆寫規則 CategoryVerifiedSearchEngine 和 Count 的規則動作 CategoryVerifiedSocialMedia。在 JSON 中，您可以透過為每個個別規則提供 RuleActionOverrides 項目來覆寫所有規則動作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryVerifiedSearchEngine"
        }
      ]
    }
  }
}
```



```
{
  "ActionToUse": {
    "Count": {}
  },
  "Name": "CategoryVerifiedSocialMedia"
},
"ExcludedRules": []
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSBotControl-Example"
}
}
```

將規則群組的評估結果覆寫為 Count

您可以覆寫規則群組評估所產生的動作，而不會變更規則群組中的規則設定或評估方式。此選項不常用。如果規則群組中的任何規則產生相符項目，此覆寫會將規則群組的結果動作設為 Count。

Note

這是不常見的使用案例。大多數動作覆寫是在規則群組內的規則層級完成，如中所述[覆寫規則群組中的規則動作](#)。

當您新增或編輯規則群組時，可以在保護套件或 Web ACL 中覆寫規則群組產生的動作。在主控台中，開啟規則群組的覆寫規則群組動作 - 選用窗格，並啟用覆寫。在規則群組陳述OverrideAction式中的 JSON 集中，如下列範例清單所示：

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet"
    }
  },
  "OverrideAction": {
    "Count": {}
  }
}
```

```
    },  
    "VisibilityConfig": {  
        "SampledRequestsEnabled": true,  
        "CloudWatchMetricsEnabled": true,  
        "MetricName": "AWS-AWSBotControl-Example"  
    }  
}
```

將保護與 AWS 資源建立關聯或取消關聯

您可以使用 在保護套件或 Web ACLs 與資源之間 AWS WAF 建立下列關聯：

- 將區域保護套件或 Web ACL 與下列任何區域資源建立關聯。對於此選項，保護套件或 Web ACL 必須與資源位於相同的區域。
 - Amazon API Gateway REST API
 - Application Load Balancer
 - AWS AppSync GraphQL API
 - Amazon Cognito 使用者集區
 - AWS App Runner 服務
 - AWS 已驗證的存取執行個體
 - AWS Amplify
- 將全域保護套件或 Web ACL 與 Amazon CloudFront 分佈建立關聯。全域保護套件或 Web ACL 會有硬式編碼的美國東部（維吉尼亞北部）區域。

您也可以在建立或更新分佈本身時，將保護套件或 Web ACL 與 CloudFront 分佈建立關聯。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[使用 AWS WAF 控制對您的內容的存取](#)。

有關多個關聯的限制

您可以根據下列限制，將單一保護套件或 Web ACL 與一或多個 AWS 資源建立關聯：

- 每個 AWS 資源只能與一個保護套件或 Web ACL 建立關聯。保護套件或 Web ACL 與 AWS 資源之間的關係是 one-to-many。
- 您可以將保護套件或 Web ACL 與一或多個 CloudFront 分佈建立關聯。您無法將與 CloudFront 分佈相關聯的保護套件或 Web ACL 與任何其他 AWS 資源類型建立關聯。

其他限制

下列其他限制適用於保護套件或 Web ACL 關聯：

- 您只能將保護套件或 Web ACL 與其中的 Application Load Balancer 建立關聯 AWS 區域。例如，您無法將保護套件或 Web ACL 與開啟的 Application Load Balancer 建立關聯 AWS Outposts。
- 您無法將 Amazon Cognito 使用者集區與使用 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組 或 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組 的保護套件 `AWSManagedRulesACFPRuleSet` 或 Web ACL 建立關聯 `AWSManagedRulesATPRuleSet`。如需防止帳戶建立詐騙的資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)。如需防止帳戶接管的資訊，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)。

生產流量風險

在部署生產流量的保護套件或 Web ACL 之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整您的規則，然後再啟用它們。如需準則，請參閱 [測試和調校您的 AWS WAF 保護](#)。

將保護與 AWS 資源建立關聯

Associate a protection pack

1. 選擇您要編輯的保護套件。主控台可讓主要保護套件卡可編輯，也會開啟側邊面板，其中包含您可以編輯的詳細資訊。
2. 在保護套件卡片中，選擇資源旁的編輯連結，以開啟管理資源面板。
3. 在規則群組的管理資源區段中，選擇新增區域資源或新增全域資源。
4. 選擇資源，然後選擇新增。

Associate a web ACL

若要將 Web ACL 與 AWS 資源建立關聯，請執行下列程序。

將 Web ACL 與 AWS 資源建立關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Web ACLs。

3. 選擇您要與資源建立關聯的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。
4. 在關聯的 AWS 資源索引標籤上，選擇新增 AWS 資源。
5. 出現提示時，選擇資源類型，選取您要關聯的資源旁的選項按鈕，然後選擇新增。

取消保護與 AWS 資源的關聯

Disassociating a protection pack

1. 選擇您要編輯的保護套件。主控台可讓主要保護套件卡可編輯，也會開啟側邊面板，其中包含您可以編輯的詳細資訊。
2. 在保護套件卡片中，選擇資源旁的編輯連結，以開啟管理資源面板。
3. 在規則群組的管理資源區段中，選擇您要取消關聯的資源，然後選擇取消關聯。

Note

您必須一次取消一個資源的關聯。請勿選擇多個資源。

4. 在確認頁面中，輸入「取消關聯」，然後選擇取消關聯。

Disassociating a web ACL

若要取消 Web ACL 與 AWS 資源的關聯，請執行下列程序。

取消 Web ACL 與 AWS 資源的關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Web ACLs。
3. 選擇您要與資源取消關聯的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。
4. 在關聯的 AWS 資源索引標籤上，選取要取消與此 Web ACL 關聯的資源。

Note

您必須一次取消一個資源的關聯。請勿選擇多個資源。

 Note

當您選擇將 Application Load Balancer 與 webACL 建立關聯時，就會啟用資源層級 DDoS 保護。如需詳細資訊，請參閱[AWS WAF 分散式阻斷服務 \(DDoS\) 預防](#)。

5. 選擇取消關聯。主控台會開啟確認對話。確認您的選擇，以取消 Web ACL 與 AWS 資源的關聯。

在 中 使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF

本節介紹保護套件和 Web ACLs 如何與規則和規則群組搭配使用。

保護套件或 Web ACL 處理 Web 請求的方式取決於下列項目：

- 保護套件或 Web ACL 和規則群組內規則的數值優先順序設定
- 規則和保護套件或 Web ACL 上的動作設定
- 您在新增的規則群組中放置在規則上的任何覆寫

如需規則動作設定的清單，請參閱 [在 中使用規則動作 AWS WAF](#)。

您可以在規則動作設定和預設保護套件或 Web ACL 動作設定中自訂請求和回應處理。如需相關資訊，請參閱[中的自訂 Web 請求和回應 AWS WAF](#)。

主題

- [設定規則優先順序](#)
- [AWS WAF 如何處理規則和規則群組動作](#)
- [在 中覆寫規則群組動作 AWS WAF](#)

設定規則優先順序

本節說明如何 AWS WAF 使用數值優先順序設定來設定規則的評估順序。

在保護套件或 Web ACL 和任何規則群組中，您可以使用數值優先順序設定來判斷規則的評估順序。您必須為保護套件或 Web ACL 中的每個規則提供該保護套件或 Web ACL 內的唯一優先順序設定，並且必須為規則群組中的每個規則提供該規則群組內的唯一優先順序設定。

 Note

當您透過主控台管理規則群組、保護套件或 Web ACLs 時，會根據清單中的規則順序為您 AWS WAF 指派唯一的數值優先順序設定。AWS WAF 會將最低數值優先順序指派給清單頂端的規則，並將最高數值優先順序指派給底部的規則。

當針對 Web 請求 AWS WAF 評估任何規則群組、保護套件或 Web ACL 時，它會評估上最低數值優先順序設定的規則，直到找到終止評估或耗盡所有規則的相符項目為止。

例如，假設您的保護套件中有下列規則和規則群組，其優先順序如下所示：

- Rule1 – 優先順序 0
- RuleGroupA – 優先順序 100
 - RuleA1 – 優先順序 10,000
 - RuleA2 – 優先順序 20,000
- Rule2 – 優先順序 200
- RuleGroupB – 優先順序 300
 - RuleB1 – 優先順序 0
 - RuleB2 – 優先順序 1

AWS WAF 會依下列順序評估此保護套件的規則：

- Rule1
- RuleGroupA RuleA1
- RuleGroupA RuleA2
- Rule2
- RuleGroupB RuleB1
- RuleGroupB RuleB2

AWS WAF 如何處理規則和規則群組動作

本節說明 AWS WAF 如何使用規則和規則群組來處理動作。

當您設定規則和規則群組時，您可以選擇 AWS WAF 如何處理相符的 Web 請求：

- **Allow 和 Block 正在終止動作** – Allow 而 Block 動作會停止對相符 Web 請求進行保護套件或 Web ACL 的所有其他處理。如果保護套件或 Web ACL 中的規則找到請求的相符項目，且規則動作為 Allow 或 Block，則相符項目會決定保護套件或 Web ACL 之 Web 請求的最終處置。AWS WAF 不會處理在相符項目之後出現在保護套件或 Web ACL 中的任何其他規則。對於您直接新增至保護套件或 Web ACL 的規則，以及新增規則群組內的規則，這是如此。透過 Block 動作，受保護的資源不會接收或處理 Web 請求。
- **Count 是非終止動作** – 當具有 Count 動作的規則符合請求時，會 AWS WAF 計算請求，然後繼續處理保護套件或 Web ACL 規則集中遵循的規則。
- **CAPTCHA 和 Challenge 可以是非終止或終止動作** – 當具有這些動作之一的規則符合請求時，會 AWS WAF 檢查其字符狀態。如果請求具有有效的字符，會 AWS WAF 處理類似相符項目的 Count 相符項目，然後繼續處理保護套件或 Web ACL 規則集中遵循的規則。如果請求沒有有效的字符，會 AWS WAF 終止評估，並傳送 CAPTCHA 拼圖或無提示背景用戶端工作階段挑戰給用戶端來解決。

如果規則評估不會導致任何終止動作，則會將保護套件或 Web ACL 預設動作 AWS WAF 套用至請求。如需相關資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

在保護套件或 Web ACL 中，您可以覆寫規則群組內規則的動作設定，也可以覆寫規則群組傳回的動作。如需相關資訊，請參閱 [在中覆寫規則群組動作 AWS WAF](#)。

動作與優先順序設定之間的互動

AWS WAF 套用至 Web 請求的動作會受到保護套件或 Web ACL 中規則的數值優先順序設定影響。例如，假設您的保護套件或 Web ACL 具有 Allow 動作的規則和 50 的數值優先順序，以及另一個 Count 動作的規則和 100 的數值優先順序。會依其優先順序 AWS WAF 評估保護套件或 Web ACL 中的規則，從最低的設定開始，因此會在計數規則之前評估允許規則。符合兩個規則的 Web 請求會先符合允許規則。由於 Allow 是終止動作，AWS WAF 會停止此相符項目的評估，而不會針對計數規則評估請求。

- 如果您只想在計數規則指標中包含不符合允許規則的請求，則規則的優先順序設定會有效。
- 另一方面，如果您想要計數規則中的計數指標，即使請求符合允許規則，您也需要為計數規則提供比允許規則更低的數值優先順序設定，以便先執行。

如需優先順序設定的詳細資訊，請參閱 [設定規則優先順序](#)。

在中覆寫規則群組動作 AWS WAF

本節說明如何覆寫規則群組動作。

當您將規則群組新增至保護套件或 Web ACL 時，您可以覆寫在相符的 Web 請求上所採取的動作。覆寫保護套件或 Web ACL 組態內規則群組的動作並不會改變規則群組本身。它只會改變 AWS WAF 如何在保護套件或 Web ACL 的內容中使用規則群組。

規則群組規則動作覆寫

您可以將規則群組內規則的動作覆寫為任何有效的規則動作。當您執行此操作時，比對請求的處理方式與設定的規則動作為覆寫設定完全相同。

Note

規則動作可以終止或非終止。終止動作會停止請求的保護套件或 Web ACL 評估，並讓它繼續到您的受保護應用程式或封鎖它。

以下是規則動作選項：

- **Allow** – AWS WAF 允許將請求轉送至受保護 AWS 的資源以進行處理和回應。這是終止動作。在您定義的規則中，您可以將自訂標頭插入請求，然後再轉送到受保護的資源。
- **Block** – AWS WAF 封鎖請求。這是終止動作。根據預設，受保護 AWS 的資源會以 HTTP 403 (Forbidden) 狀態碼回應。在您定義的規則中，您可以自訂回應。當 AWS WAF 封鎖請求時，Block 動作設定會決定受保護資源傳回用戶端的回應。
- **Count** – AWS WAF 計算請求，但不決定允許或封鎖請求。這是非終止動作。會 AWS WAF 繼續處理保護套件或 Web ACL 中的其餘規則。在您定義的規則中，您可以將自訂標頭插入請求，也可以新增其他規則可比對的標籤。
- **CAPTCHA 和 Challenge** – AWS WAF 使用 CAPTCHA 拼圖和靜音挑戰來驗證請求不是來自機器人，並使用 AWS WAF 字符來追蹤最近成功的用戶端回應。

CAPTCHA 拼圖和無提示挑戰只能在瀏覽器存取 HTTPS 端點時執行。瀏覽器用戶端必須在安全的內容中執行，才能取得字符。

Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

這些規則動作可以終止或非終止，取決於請求中字符的狀態：

- 未終止有效、未過期的字符 – 如果字符根據設定的 CAPTCHA 或挑戰抗擾性時間有效且未過期，會 AWS WAF 處理類似於 Count 動作的請求。會根據保護套件或 Web ACL 中的其餘規則 AWS WAF 繼續檢查 Web 請求。與 Count 組態類似，在您定義的規則中，您可以選擇使用自訂標頭來設定這些動作以插入請求，也可以新增其他規則可比對的標籤。
- 終止無效或過期權杖的封鎖請求 – 如果權杖無效或指定的時間戳記已過期，會 AWS WAF 終止 Web 請求的檢查並封鎖請求，類似於 Block 動作。AWS WAF 然後以自訂回應碼回應用戶端。對於 CAPTCHA，如果請求內容指出用戶端瀏覽器可以處理它，AWS WAF 會在 JavaScript 問質中傳送 CAPTCHA 拼圖，其旨在區分人類用戶端和機器人。對於 Challenge 動作，AWS WAF 會傳送具有無提示挑戰的 JavaScript 問質，此挑戰旨在區分正常瀏覽器與由機器人執行的工作階段。

如需其他資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

如需如何使用此選項的詳細資訊，請參閱 [覆寫規則群組中的規則動作](#)。

將規則動作覆寫為 Count

規則動作覆寫的最常見使用案例是將部分或全部規則動作覆寫至 Count，以測試和監控規則群組的行為，然後再將其投入生產環境。

您也可以使用它來對產生誤報的規則群組進行故障診斷。當規則群組封鎖您預期不會封鎖的流量時，會發生誤報。如果您在規則群組中識別規則，該規則會封鎖您想要允許通過的請求，您可以保留該規則上的計數動作覆寫，以排除該規則對您的請求採取動作。

如需在測試中使用規則動作覆寫的詳細資訊，請參閱 [測試和調校您的 AWS WAF 保護](#)。

JSON 清單：RuleActionOverrides 取代 ExcludedRules

如果您在 2022 年 10 月 27 日之前將保護套件或 Web ACL 組態 Count 中的規則群組規則動作設為 `Count`，則會將保護套件或 Web ACL JSON 中的覆寫 AWS WAF 儲存為 `ExcludedRules`。現在，將規則覆寫為 `Count` 的 JSON 設定位於 `RuleActionOverrides` 設定中。

建議您將 JSON 清單中的所有 `ExcludedRules` 設定更新為動作設為 `RuleActionOverrides` 的設定 `Count`。如果您只使用新的設定，API 會接受任一 `RuleActionOverrides` 設定，但您會在主控台工作與 API 工作之間取得 JSON 清單中的一致性。

Note

在 AWS WAF 主控台中，保護套件或 Web ACL 取樣請求索引標籤不會顯示具有舊設定的規則範例。如需詳細資訊，請參閱 [檢視 Web 請求的範例](#)。

當您使用 AWS WAF 主控台編輯現有的規則群組設定時，主控台會自動將 JSON 中的任何 `ExcludedRules` 設定轉換為 `RuleActionOverrides` 設定，並將覆寫動作設定為 `Count`。

- 目前的設定範例：

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAdminProtectionRuleSet",
  "RuleActionOverrides": [
    {
      "Name": "AdminProtection_URI_PATH",
      "ActionToUse": {
        "Count": {}
      }
    }
  ]
}
```

- 舊設定範例：

```
OLD SETTING
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAdminProtectionRuleSet",
  "ExcludedRules": [
    {
      "Name": "AdminProtection_URI_PATH"
    }
  ]
}
OLD SETTING
```

規則群組傳回動作覆寫至 `Count`

您可以覆寫規則群組傳回的動作，將其設定為 `Count`。

Note

這不是在規則群組中測試規則的好選項，因為它不會改變規則群組本身 AWS WAF 的評估方式。它只會影響 AWS WAF 如何處理從規則群組評估傳回至保護套件或 Web ACL 的結果。如果您想要測試規則群組中的規則，請使用上一節中所述的選項 [規則群組規則動作覆寫](#)。

當您將規則群組動作覆寫為 `Count`，會正常 AWS WAF 處理規則群組評估。

如果規則群組中沒有相符的規則，或者所有相符的規則都具有 `Count` 動作，則此覆寫不會影響規則群組或保護套件或 Web ACL 的處理。

規則群組中符合 Web 請求且具有終止規則動作的第一個規則 AWS WAF 會導致 停止評估規則群組，並將終止動作結果傳回至保護套件或 Web ACL 評估層級。此時，在保護套件或 Web ACL 評估中，此覆寫會生效。會 AWS WAF 覆寫終止動作，使得規則群組評估的結果僅為 `Count` 動作。AWS WAF 然後繼續處理保護套件或 Web ACL 中的其餘規則。

如需如何使用此選項的詳細資訊，請參閱 [將規則群組的評估結果覆寫為 `Count`](#)。

在 中設定保護套件或 Web ACL 預設動作 AWS WAF

本節說明保護套件或 Web ACL 預設動作的運作方式。

當您建立和設定保護套件或 Web ACL 時，您必須設定保護套件或 Web ACL 預設動作。AWS WAF 會將此動作套用至任何 Web 請求，使其通過所有保護套件或 Web ACL 的規則評估，而不會套用終止動作。終止動作會停止請求的保護套件或 Web ACL 評估，並讓它繼續到您的受保護應用程式或封鎖它。如需規則動作的詳細資訊，請參閱 [在 中使用規則動作 AWS WAF](#)。

保護套件或 Web ACL 預設動作必須決定 Web 請求的最終處置，因此它是終止動作：

- **Allow** – 如果您想要允許大多數使用者存取您的網站，但想要封鎖對攻擊者的存取，其請求來自指定的 IP 地址，或其請求似乎包含惡意 SQL 程式碼或指定的值，請選擇 **Allow** 預設動作。然後，當您將規則新增至保護套件或 Web ACL 時，請新增規則來識別和封鎖您要封鎖的特定請求。透過此動作，您可以將自訂標頭插入請求，然後再將其轉送至受保護的資源。
- **Block** – 如果您想要防止大多數使用者存取您的網站，但您想要允許存取其請求來自指定 IP 地址的使用者，或是其請求包含指定值的使用者，請選擇 **Block** 預設動作。然後，當您將規則新增至保護套件或 Web ACL 時，請新增規則來識別並允許您想要允許的特定請求。根據預設，對於 **Block** 動作，AWS 資源會以 HTTP 403 (Forbidden) 狀態碼回應，但您可以自訂回應。

如需自訂請求和回應的詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

您自己的規則和規則群組的組態部分取決於您要允許還是封鎖多數的 Web 請求。例如，如果您想要允許大多數請求，您可以將保護套件或 Web ACL 預設動作設定為 **Allow**，然後新增規則來識別您要封鎖的 Web 請求，如下所示：

- 來自發出異常數量 IP 地址的請求
- 來自您不常交涉、或時常受到攻擊國家/地區的請求

- User-agent 標題中包含虛假值的請求
- 似乎含有惡意 SQL 程式碼的請求

受管規則群組規則通常使用 Block 動作，但並非全部都使用。例如，某些用於 Bot Control 的規則會使用 CAPTCHA 和 Challenge 動作設定。如需受管規則群組的相關資訊，請參閱 [在中使用受管規則群組 AWS WAF](#)。

管理 的內文檢查大小限制 AWS WAF

本節說明什麼是內文檢查大小限制及其運作方式。

內文檢查大小限制是 AWS WAF 可檢查的請求內文大小上限。當 Web 請求內文大於限制時，基礎主機服務只會將限制內的內容轉送至 AWS WAF 以供檢查。

- 對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB (8,192 位元組)。
- 對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB (16,384 位元組)，而且您可以將任何資源類型的限制以 16 KB 遞增，最多 64 KB。設定選項為 16 KB、32 KB、48 KB 和 64 KB。

過大主體處理

如果您的 Web 流量包含大於限制的內文，則會套用您設定的過大處理。如需處理過大選項的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

提高限制設定的定價考量

AWS WAF 會收取基本費率，以檢查資源類型預設限制內的流量。

對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access 資源，如果您增加限制設定，AWS WAF 可以檢查的流量包含不超過新限制的內文大小。只有在檢查內文大小大於預設 16 KB 的請求時，才會向您收取額外的費用。如需定價的詳細資訊，請參閱 [AWS WAF 定價](#)。

修改內文檢查大小限制的選項

您可以設定 CloudFront、API Gateway、Amazon Cognito、App Runner 或 Verified Access 資源的內文檢查大小限制。

當您建立或編輯保護套件或 Web ACL 時，您可以在資源關聯組態中修改內文檢查大小限制。如需 API，請參閱 [AssociationConfig](#) 中的保護套件或 Web ACL 的關聯組態。對於 主控台，請參閱您指定

保護套件或 Web ACL 相關聯資源之頁面上的組態。如需主控台組態的指引，請參閱 [在中檢視 Web 流量指標 AWS WAF](#)。

在中設定 CAPTCHA、挑戰和字符 AWS WAF

您可以為使用 CAPTCHA 或 Challenge 規則動作的規則設定保護套件或 Web ACL 中的選項，並為管理 AWS WAF 受管保護的無提示用戶端挑戰的應用程式整合 SDKs 設定選項。

這些功能透過使用 CAPTCHA 拼圖挑戰最終使用者，以及使用無提示的挑戰呈現用戶端工作階段，來緩解機器人活動。當用戶端成功回應時，AWS WAF 會提供權杖，供他們在 Web 請求中使用，並加上上次成功拼圖和挑戰回應的時間戳記。如需詳細資訊，請參閱 [中的智慧型威脅防禦 AWS WAF](#)。

在保護套件或 Web ACL 組態中，您可以設定如何 AWS WAF 管理這些字符：

- CAPTCHA 和挑戰豁免時間 – 這些會指定 CAPTCHA 或挑戰時間戳記的有效時間。保護套件或 Web ACL 設定會繼承到所有未設定其自身抗擾性時間設定的規則，以及應用程式整合 SDKs。如需詳細資訊，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。
- 權杖網域 – 根據預設，僅 AWS WAF 接受與保護套件或 Web ACL 相關聯之資源的網域權杖。如果您設定權杖網域清單，會 AWS WAF 接受清單中所有網域以及相關聯資源網域的權杖。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

在中檢視 Web 流量指標 AWS WAF

本節說明如何存取 Web 流量指標的摘要。

對於您使用的任何保護套件或 Web ACL，您可以在 AWS WAF 主控台的流量概觀索引標籤下，存取保護套件或 Web ACL 頁面上的 Web 流量指標摘要。主控台儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集。如需儀表板的詳細資訊，請參閱 [保護套件或 Web ACLs 流量概觀儀表板](#)。如需有關監控保護套件或 Web ACL 流量的其他資訊，請參閱 [監控和調校您的 AWS WAF 保護](#)。

刪除保護套件或 Web ACL

本節提供透過 AWS 主控台刪除保護套件或 Web ACLs 的程序。

若要刪除保護套件或 Web ACL，請先取消所有 AWS 資源與保護套件或 Web ACL 的關聯。請執行以下程序。

To delete a protection pack

1. 登入 AWS Management Console 並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇資源與保護。
3. 在保護套件卡片中，選擇資源旁的編輯連結，以開啟管理資源面板。
4. 在規則群組的管理資源區段中，選擇您要取消關聯的資源，然後選擇取消關聯。

Note

您必須一次取消一個資源的關聯。請勿選擇多個資源。

5. 在確認頁面中，輸入「取消關聯」，然後選擇取消關聯。重複以取消保護套件中每個資源的關聯。
6. 選擇您要刪除的保護套件。主控台可讓主要保護套件卡片可編輯，也會開啟側邊面板，其中包含您可以編輯的詳細資訊。
7. 在詳細資訊面板中，選擇垃圾桶圖示。
8. 在確認頁面中，輸入「刪除」，然後選擇刪除。

To delete a web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Web ACLs。
3. 選取您要刪除的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。

Note

如果您沒有看到要刪除的 Web ACL，請確定 Web ACLs 區段內的區域選擇正確無誤。保護 Amazon CloudFront 分佈的任何 Web ACLs 都位於全域 (CloudFront) 中。

4. 在關聯的 AWS 資源索引標籤上，針對每個相關聯的資源，選取資源名稱旁的選項按鈕，然後選擇取消關聯。這會將保護套件或 Web ACL 與您的 AWS 資源取消關聯。
5. 在導覽窗格中，選擇 Web ACLs。

6. 選取您要刪除的 Web ACL 旁邊的選項按鈕，然後選擇 Delete (刪除)。

AWS WAF 規則

本節說明什麼是 AWS WAF 規則及其運作方式。

AWS WAF 規則定義如何檢查 HTTP(S) Web 請求，以及在符合檢查條件時對請求採取的動作。您只能在規則群組或保護套件或 Web ACL 的內容中定義規則。

規則本身不存在於 AWS WAF 中。它們不是 AWS 資源，也沒有 Amazon Resource Name (ARNs)。您可以在定義規則群組或保護套件或 Web ACL 中依名稱存取規則。您可以使用規則群組的 JSON 檢視或包含規則的保護套件或 Web ACLs，來管理規則並將其複製到其他保護套件或 Web ACL。您也可以透過 AWS WAF 主控台規則建置器來管理它們，該建置器可用於保護套件或 Web ACLs 和規則群組。

規則名稱

每個規則都需要一個名稱。避免開頭為 `_` 的名稱，AWS 以及用於其他服務為您管理的規則群組或規則的名稱。請參閱 [辨識其他服務提供的規則群組](#)。

Note

如果您變更規則的名稱，且希望規則的指標名稱反映變更，則也必須更新指標名稱。AWS WAF 當您變更規則名稱時，不會自動更新規則的指標名稱。您可以使用規則 JSON 編輯器，在主控台中編輯規則時變更指標名稱。您也可以透過 APIs 和您用來定義保護套件或 Web ACL 或規則群組的任何 JSON 清單中變更這兩個名稱。

規則陳述式

每個規則還需要規則陳述式，以定義規則如何檢查 Web 請求。規則陳述式可能包含任何深度的其他巢狀陳述式，取決於規則和陳述式類型。有些規則陳述式採用一組條件。例如，您可以為 IP 集比對規則指定最多 10,000 個 IP 地址或 IP 地址範圍。

您可以定義規則來檢查條件，如下所示：

- 指令碼可能為惡意。攻擊者可以利用 web 應用程式的漏洞內嵌指令碼。這稱為跨網站指令碼 (XSS)。
- 發出請求的 IP 地址或地址範圍。

- 發出請求的國家/地區或地理位置。
- 請求指定部分的長度，例如查詢字串。
- SQL 程式碼可能為惡意。攻擊者會藉由內嵌惡意 SQL 程式碼於 web 請求中，嘗試從您的資料庫碼擷取資料。此稱為 SQL Injection。
- 字串會出現在請求，例如出現在 User-Agent 標頭的值或出現在查詢字串的文字字串。您也可以使用規則運算式 (regex) 指定這些字串。
- 保護套件或 Web ACL 中先前規則已新增至請求的標籤。

除了具有 Web 請求檢查條件的陳述式之外，也 AWS WAF 支援 AND、OR 和 的邏輯陳述式 NOT，您可用來在規則中結合陳述式。

例如，根據您最近從攻擊者看到的請求，您可以使用結合下列巢狀陳述式的邏輯 AND 陳述式來建立規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。
- 它們好像有包含類似 SQL 程式碼的查詢字串。

在此情況下，Web 請求需要符合所有陳述式，才能產生最上層 的相符項目 AND。

主題

- [在 中使用規則動作 AWS WAF](#)
- [在 中使用規則陳述式 AWS WAF](#)
- [在 中使用相符規則陳述式 AWS WAF](#)
- [在 中使用邏輯規則陳述式 AWS WAF](#)
- [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)
- [在 中使用規則群組規則陳述式 AWS WAF](#)

在 中使用規則動作 AWS WAF

本節說明規則動作的運作方式。

當 Web 請求符合規則中定義的條件時，規則動作會告知 AWS WAF 該如何處理。您可以選擇性地將自訂行為新增至每個規則動作。

Note

規則動作可以終止或非終止。終止動作會停止請求的保護套件或 Web ACL 評估，並讓它繼續到您的受保護應用程式或封鎖它。

以下是規則動作選項：

- **Allow** – AWS WAF 允許將請求轉送至受保護 AWS 的資源以進行處理和回應。這是終止動作。在您定義的規則中，您可以將自訂標頭插入請求，然後再轉送到受保護的資源。
- **Block** – AWS WAF 封鎖請求。這是終止動作。根據預設，受保護 AWS 的資源會以 HTTP 403 (Forbidden) 狀態碼回應。在您定義的規則中，您可以自訂回應。當 AWS WAF 封鎖請求時，Block 動作設定會決定受保護資源傳回用戶端的回應。
- **Count** – AWS WAF 計算請求，但不決定允許或封鎖請求。這是非終止動作。會 AWS WAF 繼續處理保護套件或 Web ACL 中的其餘規則。在您定義的規則中，您可以將自訂標頭插入請求，也可以新增其他規則可比對的標籤。
- **CAPTCHA 和 Challenge** – AWS WAF 使用 CAPTCHA 拼圖和靜音挑戰來驗證請求不是來自機器人，並使用 AWS WAF 字符來追蹤最近成功的用戶端回應。

CAPTCHA 拼圖和無提示挑戰只能在瀏覽器存取 HTTPS 端點時執行。瀏覽器用戶端必須在安全的内容中執行，才能取得字符。

Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

這些規則動作可以終止或非終止，取決於請求中字符的狀態：

- **未終止有效、未過期的字符** – 如果字符根據設定的 CAPTCHA 或挑戰抗擾性時間有效且未過期，會 AWS WAF 處理類似於 Count 動作的請求。會根據保護套件或 Web ACL 中的其餘規則 AWS WAF 繼續檢查 Web 請求。與 Count 組態類似，在您定義的規則中，您可以選擇使用自訂標頭來設定這些動作以插入請求，也可以新增其他規則可比對的標籤。
- **終止無效或過期權杖的封鎖請求** – 如果權杖無效或指定的時間戳記已過期，會 AWS WAF 終止 Web 請求的檢查並封鎖請求，類似於 Block 動作。AWS WAF 然後以自訂回應碼回應用戶端。對於 CAPTCHA，如果請求內容指出用戶端瀏覽器可以處理它，AWS WAF 會在 JavaScript 問質中

傳送 CAPTCHA 拼圖，其旨在區分人類用戶端和機器人。對於 Challenge 動作，AWS WAF 會傳送具有無提示挑戰的 JavaScript 間質，此挑戰旨在區分正常瀏覽器與由機器人執行的工作階段。

如需其他資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

如需自訂請求和回應的詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

如需將標籤新增至相符請求的詳細資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#)。

如需有關保護套件或 Web ACL 和規則設定如何互動的資訊，請參閱 [在 中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

在 中使用規則陳述式 AWS WAF

本節說明規則陳述式的運作方式。

規則陳述式是規則的一部分，AWS WAF 說明如何檢查 Web 請求。當 AWS WAF 在 Web 請求中找到檢查條件時，我們說 Web 請求符合 陳述式。視陳述式類型而定，每個規則陳述式會指定要尋找什麼以及如何尋找。

中的每個規則 AWS WAF 都有單一最上層規則陳述式，可包含其他陳述式。規則陳述式可以非常簡單。例如，您可以有一個陳述式，提供一組原始國家/地區來檢查的 Web 請求，或者您可以在保護套件或 Web ACL 中擁有僅參考規則群組的規則陳述式。規則陳述式也可以非常複雜。例如，您可以有一個陳述式，將許多其他陳述式與邏輯 AND、OR 和 NOT 陳述式結合。

對於大多數規則，您可以將自訂 AWS WAF 標籤新增至相符的請求。AWS 受管規則規則群組中的規則會將標籤新增至相符的請求。規則新增的標籤會將請求的相關資訊提供給稍後在保護套件或 Web ACL 以及 AWS WAF 日誌和指標中評估的規則。如需標籤的相關資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#) 和 [標籤比對規則陳述式](#)。

巢狀規則陳述式

AWS WAF 支援許多規則陳述式的巢狀化，但不支援所有規則陳述式。例如，您無法將規則群組陳述式巢狀在另一個陳述式內。您需要在某些案例中使用巢狀，例如縮小範圍陳述式和邏輯陳述式。以下規則陳述式列出和規則詳細資訊，說明每個類別和規則的巢狀功能和需求。

主控台中規則的視覺化編輯器僅支援規則陳述式的一個巢狀層級。例如，您可以在邏輯 AND 或 OR 規則內巢狀化許多類型的陳述式，但您無法巢狀另一個 AND 或 OR 規則，因為這需要第二層級的巢狀化。若要實作多個巢狀層級，請透過主控台 JSON 規則編輯器或透過 APIs 提供 JSON 中的規則定義。

主題

- [在 中調整規則陳述式設定 AWS WAF](#)
- [在 中使用縮小範圍陳述式 AWS WAF](#)
- [在 中參考可重複使用的實體 AWS WAF](#)

在 中調整規則陳述式設定 AWS WAF

本節說明您可以在檢查 Web 請求元件的規則陳述式中指定的設定。如需用量的相關資訊，請參閱 中的個別規則陳述式[在 中使用相符規則陳述式 AWS WAF](#)。

這些 Web 請求元件的子集也可用於以速率為基礎的規則，做為自訂請求彙總金鑰。如需相關資訊，請參閱 [在 中彙總以速率為基礎的規則 AWS WAF](#)。

對於請求元件設定，您可以指定元件類型本身，以及任何其他選項，具體取決於元件類型。例如，當您檢查包含文字的元件類型時，您可以在檢查之前套用文字轉換。

Note

除非另有說明，否則如果 Web 請求沒有規則陳述式中指定的請求元件，會將請求 AWS WAF 評估為不符合規則條件。

內容

- [在 中請求元件 AWS WAF](#)
 - [HTTP 方法](#)
 - [單一標頭](#)
 - [所有標頭](#)
 - [標頭順序](#)
 - [Cookie](#)
 - [URI 片段](#)
 - [URI 路徑](#)
 - [JA3 指紋](#)
 - [JA4 指紋](#)
 - [查詢字串](#)
 - [單一查詢參數](#)

- [所有查詢參數](#)
- [Body](#)
- [JSON 內文](#)
- [在 中使用轉送的 IP 地址 AWS WAF](#)
- [在 中檢查 HTTP/2 虛擬標頭 AWS WAF](#)
- [在 中使用文字轉換 AWS WAF](#)

在 中請求元件 AWS WAF

本節說明您可以指定用於檢查的 Web 請求元件。您可以為尋找 Web 請求內模式的比對規則陳述式指定請求元件。這些類型的陳述式包括字串比對、regex 比對、大小限制和 SQL Injection 攻擊陳述式。如需如何使用這些請求元件設定的詳細資訊，請參閱 中的個別規則陳述式 [在 中使用相符規則陳述式 AWS WAF](#)

除非另有說明，否則如果 Web 請求沒有規則陳述式中指定的請求元件，會將請求 AWS WAF 評估為不符合規則條件。

Note

您可以為每個需要它的規則陳述式指定單一請求元件。若要檢查請求的多個元件，請為每個元件建立規則陳述式。

AWS WAF 主控台和 API 文件為下列位置的請求元件設定提供指引：

- 主控台上的規則建置器 – 在一般規則類型的陳述式設定中，選擇您要在請求元件下的檢查對話中檢查的元件。
- API 陳述式內容 – FieldToMatch

本節的其餘部分說明 Web 請求要檢查的部分選項。

主題

- [HTTP 方法](#)
- [單一標頭](#)
- [所有標頭](#)

- [標頭順序](#)
- [Cookie](#)
- [URI 片段](#)
- [URI 路徑](#)
- [JA3 指紋](#)
- [JA4 指紋](#)
- [查詢字串](#)
- [單一查詢參數](#)
- [所有查詢參數](#)
- [Body](#)
- [JSON 內文](#)

HTTP 方法

檢查 HTTP 方法是否有請求。HTTP 方法表示 Web 請求要求受保護資源執行的操作類型，例如 POST 或 GET。

單一標頭

檢查請求中的單一具名標頭。

針對此選項，您可以指定標頭名稱，例如 User-Agent 或 Referer。名稱的字串比對不區分大小寫。

所有標頭

檢查所有請求標頭，包括 Cookie。您可以套用篩選條件來檢查所有標頭的子集。

針對此選項，您提供下列規格：

- 比對模式 – 用來取得用於 inspection. AWS WAF looks 標頭索引鍵中這些模式的標頭子集的篩選條件。

比對模式設定可以是下列其中一項：

- 全部 – 比對所有金鑰。評估所有標頭的規則檢查條件。
- 排除的標頭 – 僅檢查其金鑰不符合您在此處指定之任何字串的標頭。金鑰的字串比對不區分大小寫。

- 包含的標頭 – 僅檢查金鑰與您在此處指定的其中一個字串相符的標頭。金鑰的字串比對不區分大小寫。
- 比對範圍 – AWS WAF 應該使用規則檢查條件進行檢查的標頭部分。您可以指定金鑰、值或全部，以檢查金鑰和值是否相符。

全部不需要在索引鍵中找到相符項目，以及在值中找到相符項目。它需要在索引鍵或值或兩者中找到相符項目。若要在金鑰和值中要求比對，請使用邏輯AND陳述式來合併兩個比對規則，其中一個規則會檢查金鑰，另一個規則則會檢查值。

- 過大處理 – AWS WAF 應如何處理標頭資料大於 AWS WAF 可檢查的請求。最多 AWS WAF 可以檢查請求標頭的前 8 KB (8,192 位元組) 和前 200 個標頭。內容最多可在達到 AWS WAF 第一個限制之前進行檢查。您可以選擇繼續檢查，或略過檢查並將請求標記為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

標頭順序

檢查包含請求標頭名稱清單的字串，其順序如 AWS WAF 接收以供檢查的 Web 請求中所示。AWS WAF 會產生字串，然後使用該字串做為欄位來比對其檢查中的元件。會將字串中的標頭名稱與冒號 AWS WAF 分隔，且沒有新增空格，例如 `host:user-agent:accept:authorization:referer`。

針對此選項，您提供下列規格：

- 過大處理 – AWS WAF 應如何處理標頭資料數量或大於 AWS WAF 可以檢查的請求。最多 AWS WAF 可以檢查請求標頭的前 8 KB (8,192 個位元組) 和前 200 個標頭。內容最多可在達到 AWS WAF 第一個限制之前進行檢查。您可以選擇繼續檢查可用的標頭，或略過檢查並將請求標記為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

Cookie

檢查所有請求 Cookie。您可以套用篩選條件來檢查所有 Cookie 的子集。

針對此選項，您提供下列規格：

- 比對模式 – 用來取得一部分 Cookie 進行檢查的篩選條件。會在 Cookie 金鑰中 AWS WAF 尋找這些模式。

比對模式設定可以是下列其中一項：

- 全部 – 比對所有金鑰。評估所有 Cookie 的規則檢查條件。

- 排除的 Cookie – 僅檢查金鑰與您在此處指定的任何字串不相符的 Cookie。索引鍵的字串比對區分大小寫，而且必須完全正確。
- 包含的 Cookie – 僅檢查金鑰與您在此處指定的其中一個字串相符的 Cookie。索引鍵的字串比對區分大小寫，而且必須完全正確。
- 比對範圍 – AWS WAF 應使用規則檢查條件檢查的 Cookie 部分。您可以同時為金鑰和值指定金鑰、值或全部。

全部不需要在索引鍵中找到相符項目，以及在值中找到相符項目。它需要在索引鍵或值或兩者中找到相符項目。若要在金鑰和值中要求比對，請使用邏輯AND陳述式來合併兩個比對規則，其中一個規則會檢查金鑰，另一個規則則會檢查值。
- 過大處理 – AWS WAF 應如何處理 Cookie 資料大於 AWS WAF 可檢查的請求。最多 AWS WAF 可以檢查請求 Cookie 的前 8 KB (8,192 位元組) 和前 200 個 Cookie。內容最多可在達到 AWS WAF 第一個限制之前進行檢查。您可以選擇繼續檢查，或略過檢查並將請求標記為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

URI 片段

Note

Uri Fragment 檢查僅適用於 CloudFront 分佈和 Application Load Balancer。

檢查遵循 "#" 符號的 URL 部分，提供資源的其他資訊，例如 #section2。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

如果您不搭配此選項使用文字轉換，AWS WAF 不會正規化 URI 片段，並完全依照在請求中從用戶端接收到的 URI 片段進行檢查。如需文字轉換的資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

規則陳述式要求

您必須為此規則陳述式提供備用行為。如果 URI 缺少片段或相關聯的服務不是 Application Load Balancer 或 CloudFront，則備用行為是您想要 AWS WAF 指派給 Web 請求的比對狀態。如果您選擇比對，會將請求 AWS WAF 視為比對規則陳述式，並將規則動作套用至請求。如果您選擇不相符，會將請求 AWS WAF 視為不符合規則陳述式。

URI 路徑

檢查識別資源的 URL 部分，例如 /images/daily-ad.jpg。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

如果您不搭配此選項使用文字轉換，AWS WAF 不會正規化 URI，並完全依照在請求中從用戶端接收 URI 的方式進行檢查。如需文字轉換的資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

JA3 指紋

檢查請求的 JA3 指紋。

Note

JA3 指紋檢查僅適用於 Amazon CloudFront 分佈和 Application Load Balancer。

JA3 指紋是從傳入請求的 TLS Client Hello 衍生的 32 個字元雜湊。此指紋可做為用戶端 TLS 組態的唯一識別符。會針對具有足夠 TLS Client Hello 資訊以進行計算的每個請求 AWS WAF，計算並記錄此指紋。幾乎所有 Web 請求都包含此資訊。

如何取得用戶端的 JA3 指紋

您可以從保護套件或 Web ACL 日誌取得用戶端請求的 JA3 指紋。如果 AWS WAF 能夠計算指紋，它會將其包含在日誌中。如需記錄欄位的資訊，請參閱 [保護套件或 Web ACL 流量的日誌欄位](#)。

規則陳述式要求

您只能在設定為完全符合您提供的字串的字串比對陳述式內檢查 JA3 指紋。在字串比對陳述式規格中提供來自日誌的 JA3 指紋字串，以符合任何未來具有相同 TLS 組態的請求。如需字串比對陳述式的詳細資訊，請參閱 [字串比對規則陳述式](#)。

您必須為此規則陳述式提供備用行為。如果無法計算 JA3 指紋，則備用行為是您想要 AWS WAF 指派給 Web 請求 AWS WAF 的比對狀態。如果您選擇比對，AWS WAF 會將請求視為比對規則陳述式，並將規則動作套用至請求。如果您選擇不相符，會將請求 AWS WAF 視為不符合規則陳述式。

若要使用此比對選項，您必須記錄保護套件或 Web ACL 流量。如需相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

JA4 指紋

檢查請求的 JA4 指紋。

Note

JA4 指紋檢查僅適用於 Amazon CloudFront 分佈和 Application Load Balancer。

JA4 指紋是從傳入請求的 TLS Client Hello 衍生的 36 個字元雜湊。此指紋可做為用戶端 TLS 組態的唯一識別符。JA4 指紋是 JA3 指紋的延伸，可對某些瀏覽器產生較少的唯一指紋。會為每個具有足夠 TLS Client Hello 資訊的請求 AWS WAF 計算並記錄此指紋。幾乎所有 Web 請求都包含此資訊。

如何取得用戶端的 JA4 指紋

您可以從保護套件或 Web ACL 日誌取得用戶端請求的 JA4 指紋。如果 AWS WAF 能夠計算指紋，它會將其包含在日誌中。如需記錄欄位的資訊，請參閱 [保護套件或 Web ACL 流量的日誌欄位](#)。

規則陳述式要求

您只能在設定為完全符合您提供的字串的字串比對陳述式內檢查 JA4 指紋。在字串比對陳述式規格中提供來自日誌的 JA4 指紋字串，以符合任何未來具有相同 TLS 組態的請求。如需字串比對陳述式的詳細資訊，請參閱 [字串比對規則陳述式](#)。

您必須為此規則陳述式提供備用行為。如果無法計算 JA4 指紋，則備用行為是您想要 AWS WAF 指派給 Web 請求 AWS WAF 的比對狀態。如果您選擇比對，AWS WAF 會將請求視為比對規則陳述式，並將規則動作套用至請求。如果您選擇不相符，會將請求 AWS WAF 視為不符合規則陳述式。

若要使用此比對選項，您必須記錄保護套件或 Web ACL 流量。如需相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

查詢字串

檢查?字元後面出現的 URL 部分，如果有的話。

Note

對於跨網站指令碼比對陳述式，我們建議您選擇所有查詢參數，而不是查詢字串。選擇所有查詢參數會將 10 WCUs 新增至基本成本。

單一查詢參數

檢查您定義為查詢字串一部分的單一查詢參數。AWS WAF 檢查您指定的參數值。

針對此選項，您也可以指定查詢引數。例如，如果 URL 為 `www.xyz.com?`

`UserName=abc&SalesRegion=seattle`，您可以 `SalesRegion` 為查詢引數指定 `UserName` 或。引數名稱的長度上限為 30 個字元。名稱不區分大小寫，因此如果您指定 `UserName`，會 AWS WAF 比對的所有變化 `UserName`，包括 `username` 和 `UsERName`。

如果查詢字串包含您所指定查詢引數的多個執行個體，會使用 OR 邏輯 AWS WAF 檢查相符項目的所有值。例如，在 URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle` 中，AWS WAF 會評估您針對 `boston` 和 `seattle` 指定的名稱。如果其中一個相符，則檢查會是相符。

所有查詢參數

檢查請求中的所有查詢參數。這類似於單一查詢參數元件選擇，但會 AWS WAF 檢查查詢字串中所有引數的值。例如，如果 URL 為 `www.xyz.com?UserName=abc&SalesRegion=seattle`，則 AWS WAF 會在 `UserName` 或 `SalesRegion` 的值符合比對檢查準則時觸發比對。

選擇此選項會將 10 WCUs 新增至基本成本。

Body

檢查請求內文，評估為純文字。您也可以使用 JSON 內容類型將內文評估為 JSON。

請求內文是緊接請求標頭的請求部分。它包含 Web 請求所需的任何其他資料，例如來自表單的資料。

- 在主控台中，您可以透過選取內容類型選擇純文字，在請求選項選擇內文下選取此選項。
- 在 API 中，在規則的 `FieldToMatch` 規格中，您可以指定 `Body` 以純文字形式檢查請求內文。

對於 Application Load Balancer 和 AWS AppSync，AWS WAF 可以檢查請求內文的前 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設 AWS WAF 可以檢查前 16 KB，而且您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。如需詳細資訊，請參閱 [管理 的內文檢查大小限制 AWS WAF](#)。

您必須為此元件類型指定過大處理。過大處理定義 AWS WAF 如何處理內文資料大於 AWS WAF 可檢查的請求。您可以選擇繼續檢查，或略過檢查並將請求標記為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

您也可以將內文評估為剖析的 JSON。如需相關資訊，請參閱以下章節。

JSON 內文

檢查請求內文，評估為 JSON。您也可以將內文評估為純文字。

請求內文是緊接請求標頭的請求部分。它包含 Web 請求所需的任何其他資料，例如來自表單的資料。

- 在主控台中，您可以透過選取內容類型選擇 JSON，在請求選項選擇內文下選取此選項。
- 在 API 的規則 `FieldToMatch` 規格中，您可以指定 `JsonBody`。

對於 Application Load Balancer 和 AWS AppSync，AWS WAF 可以檢查請求內文的前 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設 AWS WAF 可以檢查前 16 KB，而且您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。如需詳細資訊，請參閱[管理的內文檢查大小限制 AWS WAF](#)。

您必須為此元件類型指定過大處理。過大處理定義 AWS WAF 如何處理內文資料大於 AWS WAF 可檢查的請求。您可以選擇繼續檢查，或略過檢查並將請求標記為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱[在中過大 Web 請求元件 AWS WAF](#)。

選擇此選項會將比對陳述式的基本成本 WCUs 加倍。例如，如果比對陳述式基本成本為 5 WCUs 而沒有 JSON 剖析，則使用 JSON 剖析會將成本加倍為 10 WCUs。

對於此選項，您可以提供其他規格，如下節所述。

AWS WAF 如何處理 JSON 內文檢查

當將 Web 請求內文 AWS WAF 檢查為 JSON 時，它會執行步驟來剖析內文，並擷取 JSON 元素以進行檢查。會根據您的組態選擇 AWS WAF 執行這些步驟。

下列列出 AWS WAF 執行的步驟。

1. 剖析內文內容 – AWS WAF 剖析 Web 請求內文的內容，以擷取 JSON 元素進行檢查。AWS WAF 會盡力剖析內文的整個內容，但剖析可能會因內容中的各種錯誤狀態而失敗。範例包括無效的字元、重複的金鑰、截斷，以及根節點不是物件或陣列的內容。

如果無法完整剖析 JSON 內文，內文剖析備用行為的選項會決定 AWS WAF 如何處理：

- None（預設行為） - 評估 AWS WAF 內容直到遇到剖析錯誤為止。
- 評估為字串 - 檢查內文為純文字。會將您為 JSON 檢查定義的文字轉換和檢查條件 AWS WAF 套用至內文文字字串。
- 相符 - 將 Web 請求視為符合規則陳述式。會將規則動作 AWS WAF 套用至請求。
- 不相符 - 將 Web 請求視為不符合規則陳述式。

Note

此備用行為只會在剖析 JSON 字串 AWS WAF 時發生錯誤時觸發。

剖析無法完全驗證 JSON

AWS WAF 剖析不會完全驗證輸入 JSON 字串，因此即使 JSON 無效，剖析也會成功。

例如，會 AWS WAF 剖析下列無錯誤的無效 JSON：

- 缺失逗號：`{"key1":"value1""key2":"value2"}`
- 缺失冒號：`{"key1":"value1", "key2""value2"}`
- 額外冒號：`{"key1"::"value1", "key2""value2"}`

對於剖析成功但結果不是完全有效 JSON 的這類案例，評估中後續步驟的結果可能會有所不同。擷取可能會遺漏一些元素，或者規則評估可能有非預期的結果。我們建議您驗證應用程式中收到的 JSON，並視需要處理無效的 JSON。

2. 擷取 JSON 元素 – 根據您的設定 AWS WAF 識別要檢查的 JSON 元素子集：

- 選項 JSON 比對範圍指定 JSON 中 AWS WAF 應檢查的元素類型。

您可以同時為金鑰和值指定金鑰、值或全部。

全部不需要在索引鍵中找到相符項目，以及在值中找到相符項目。它需要在索引鍵或值或兩者中找到相符項目。若要在金鑰和值中要求比對，請使用邏輯AND陳述式來合併兩個比對規則，一個規則會檢查金鑰，另一個規則則會檢查值。

- 要檢查的選項內容會指定如何篩選設定為您要 AWS WAF 檢查之子集的元素。

您必須指定下列其中一項：

- 完整 JSON 內容 - 評估所有元素。
- 僅包含的元素 - 僅評估路徑符合您提供的 JSON 指標條件的元素。請勿使用此選項來指示 JSON 中的所有路徑。請改用完整 JSON 內容。

如需 JSON 指標語法的相關資訊，請參閱網際網路工程任務小組 (IETF) 文件 [JavaScript 物件標記法 \(JSON\) 指標](#)。

例如，在 主控台中，您可以提供下列項目：

```
/dogs/0/name  
/dogs/1/name
```

在 API 或 CLI 中，您可以提供下列項目：

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

例如，假設要檢查設定的內容是僅包含的元素，而包含的元素設定是 `/a/b`。

對於下列範例 JSON 內文：

```
{
  "a": {
    "c": "d",
    "b": {
      "e": {
        "f": "g"
      }
    }
  }
}
```

AWS WAF 會檢查每個 JSON 比對範圍設定的元素集如下所示。請注意 b，金鑰 是包含元素路徑的一部分，因此不會進行評估。

- 全部：e、f，和 g。
- 金鑰：e 和 f。
- 值：g。

3. 檢查 JSON 元素集 – 將您指定的任何文字轉換 AWS WAF 套用至擷取的 JSON 元素，然後將產生的元素集與規則陳述式的比對條件相符。這與其他 Web 請求元件的轉換和評估行為相同。如果任何擷取的 JSON 元素相符，表示 Web 請求符合規則。

在 中使用轉送的 IP 地址 AWS WAF

本節適用於使用 Web 請求 IP 地址的規則陳述式。根據預設，AWS WAF 會使用 Web 請求原始伺服器的 IP 地址。不過，如果 Web 請求通過一或多個代理或負載平衡器，Web 請求原始伺服器將包含最後一個代理的地址，而不是用戶端的原始地址。在這種情況下，來源用戶端地址通常會在另一個 HTTP 標頭中轉送。此標頭通常是 X-Forwarded-For(XFF)，但可以是不同的標頭。

使用 IP 地址的規則陳述式

使用 IP 地址的規則陳述式如下：

- [IP 集合比對](#) - 檢查 IP 地址是否與 IP 集中定義的地址相符。
- [地理比對](#) - 使用 IP 地址來判斷原始國家/地區和區域，並將原始國家/地區與國家/地區清單比對。
- [ASN 比對](#) - 使用 IP 地址來判斷自治系統編號 (ASN)，並將 ASN 與 ASNs 清單比對。

- [使用以速率為基礎的規則陳述式](#) - 可以依其 IP 地址彙總請求，以確保沒有個別 IP 地址以過高的速率傳送請求。您可以單獨使用 IP 地址彙總，或與其他彙總金鑰結合使用。

您可以指示從 X-Forwarded-For 標頭或另一個 HTTP 標頭使用任何這些規則陳述式的 AWS WAF 轉送 IP 地址，而不是使用 Web 請求的原始伺服器。如需如何提供規格的詳細資訊，請參閱個別規則陳述式類型的指引。

Note

如果您指定的標頭不存在於請求中，AWS WAF 則不會將規則套用至 Web 請求。

備用行為

當您使用轉送的 IP 地址時，如果請求在指定位置沒有有效的 IP 地址，您會指出 AWS WAF 要指派給 Web 請求的比對狀態：

- MATCH - 將 Web 請求視為符合規則陳述式。會將規則動作 AWS WAF 套用至請求。
- NO MATCH - 將 Web 請求視為不符合規則陳述式。

機器人 AWS WAF 控制中使用的 IP 地址

Bot Control 受管規則群組會使用來自的 IP 地址來驗證機器人 AWS WAF。如果您使用 Bot Control，而且已驗證透過代理或負載平衡器路由的機器人，則需要使用自訂規則明確允許它們。例如，您可以設定自訂 IP 集比對規則，使用轉送的 IP 地址來偵測和允許已驗證的機器人。您可以使用規則，以多種方式自訂機器人管理。如需詳細資訊和範例，請參閱 [AWS WAF 機器人控制](#)。

使用轉送 IP 地址的一般考量

在使用轉送的 IP 地址之前，請注意下列一般注意事項：

- 代理可以沿途修改標頭，代理可能會以不同的方式處理標頭。
- 攻擊者可能會更改標頭的內容，嘗試繞過 AWS WAF 檢查。
- 標頭內的 IP 地址可能格式錯誤或無效。
- 您指定的標頭可能完全不存在於請求中。

搭配使用轉送 IP 地址的考量 AWS WAF

下列清單說明在 中使用轉送 IP 地址的要求和注意事項 AWS WAF：

- 對於任何單一規則，您可以為轉送的 IP 地址指定一個標頭。標頭規格不區分大小寫。
- 對於以速率為基礎的規則陳述式，任何巢狀範圍陳述式都不會繼承轉送的 IP 組態。為使用轉送 IP 地址的每個陳述式指定組態。
- 對於地理比對和以速率為基礎的規則，AWS WAF 會使用標頭中的第一個地址。例如，如果標頭包含 10.1.1.1, 127.0.0.0, 10.10.10.10 AWS WAF 使用 10.1.1.1
- 對於 ASN 比對，您可以指出要比對標頭中的第一個、最後一個或任何地址與指定的 ASN。如果您指定任何，會 AWS WAF 檢查標頭中的所有地址是否相符，最多 10 個地址。如果標頭包含超過 10 個地址，會 AWS WAF 檢查最後 10 個地址。
- 對於 IP 集比對，您可以指出要比對標頭中的第一個、最後一個或任何地址。如果您指定任何，會 AWS WAF 檢查標頭中的所有地址是否相符，最多 10 個地址。如果標頭包含超過 10 個地址，會 AWS WAF 檢查最後 10 個地址。
- 包含多個地址的標頭必須在地址之間使用逗號分隔符號。如果請求使用逗號以外的分隔符號，AWS WAF 會將標頭中的 IP 地址視為格式錯誤。
- 如果標頭中的 IP 地址格式錯誤或無效，AWS WAF 會根據您在轉送 IP 組態中指定的備用行為，將 Web 請求指定為符合規則或不相符。
- 如果您指定的標頭不存在於請求中，AWS WAF 則不會將規則套用至請求。這表示 AWS WAF 不會套用規則動作，也不會套用備用行為。
- 針對 IP 地址使用轉送 IP 標頭的規則陳述式不會使用 Web 請求來源報告的 IP 地址。

搭配使用轉送 IP 地址的最佳實務 AWS WAF

當您使用轉送的 IP 地址時，請使用下列最佳實務：

- 在啟用轉送 IP 組態之前，請仔細考慮請求標頭的所有可能狀態。您可能需要使用多個規則來取得您想要的行為。
- 若要檢查多個轉送 IP 標頭或檢查 Web 請求原始伺服器標頭和轉送 IP 標頭，請為每個 IP 地址來源使用一個規則。
- 若要封鎖具有無效標頭的 Web 請求，請設定規則動作來封鎖和設定要符合之轉送 IP 組態的備用行為。

轉送 IP 地址的範例 JSON

下列地理比對陳述式只有在 X-Forwarded-For 標頭包含的 IP 原始國家/地區為 時才會相符US：

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

下列以速率為基礎的規則會根據 X-Forwarded-For 標頭中的第一個 IP 彙總請求。規則只會計算符合巢狀地理比對陳述式的請求，而且只會封鎖符合地理比對陳述式的請求。巢狀地理比對陳述式也會使用 X-Forwarded-For 標頭來判斷 IP 地址是否指出 的原始國家/地區US。如果存在，或者如果標頭存在但格式不正確，則地理比對陳述式會傳回相符項目。

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
```

```
    "Limit": "100",
    "AggregateKeyType": "FORWARDED_IP",
    "ScopeDownStatement": {
      "GeoMatchStatement": {
        "CountryCodes": [
          "US"
        ],
        "ForwardedIPConfig": {
          "HeaderName": "x-forwarded-for",
          "FallbackBehavior": "MATCH"
        }
      }
    },
    "ForwardedIPConfig": {
      "HeaderName": "x-forwarded-for",
      "FallbackBehavior": "MATCH"
    }
  }
}
```

在 中檢查 HTTP/2 虛擬標頭 AWS WAF

本節說明如何使用 AWS WAF 來檢查 HTTP/2 虛擬標頭。

支援 HTTP/2 流量的受保護 AWS 資源不會將 HTTP/2 虛擬標頭轉送到 AWS WAF 進行檢查，但會在 AWS WAF 檢查的 Web 請求元件中提供虛擬標頭的內容。

您可以使用 僅 AWS WAF 檢查下表中列出的虛擬標頭。

HTTP/2 虛擬標頭內容對應至 Web 請求元件

HTTP/2 虛擬標頭	要檢查的 Web 請求元件	文件
:method	HTTP 方法	HTTP 方法
:authority	Host 標頭	單一標頭 所有標頭
:path	URI 路徑	URI 路徑

HTTP/2 虛擬標頭	要檢查的 Web 請求元件	文件
:path 查詢	查詢字串	查詢字串
		單一查詢參數
		所有查詢參數

在 中 使用文字轉換 AWS WAF

本節說明如何在檢查請求之前提供 AWS WAF 要套用的轉換。

在尋找模式或設定限制條件的陳述式中，您可以在檢查請求之前提供 AWS WAF 要套用的轉換。轉換會將 Web 請求重新格式化，以避免攻擊者用來試圖略過 AWS WAF 的某些異常格式。

當您搭配 JSON 內文請求元件選擇使用時，AWS WAF 會在剖析和擷取元素以從 JSON 檢查後套用轉換。如需詳細資訊，請參閱[JSON 內文](#)。

如果您提供多個轉換，您也可以設定讓 AWS WAF 套用它們的順序。

WCUs – 每個文字轉換都是 10 WCUs。

AWS WAF 主控台和 API 文件也為下列位置的這些設定提供指引：

- 主控台上的規則建置器 – 文字轉換。當您使用請求元件時，此選項可供使用。
- API 陳述式內容 – TextTransformations

文字轉換的選項

每個轉換清單會顯示主控台和 API 規格，後面接著描述。

Base64 decode – BASE64_DECODE

AWS WAF 解碼 Base64-encoded 字串。

Base64 decode extension – BASE64_DECODE_EXT

AWS WAF 會解碼 Base64-encoded 字串，但使用忽略無效字元的寬容實作。

Command line – CMD_LINE

此選項可緩解攻擊者可能注入作業系統命令列命令，並使用異常格式來掩飾部分或全部命令的情況。

使用此選項可執行下列轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將大寫字母 A-Z 轉換成小寫字母 a-z

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF 將多個空格取代為一個空格，並將下列字元取代為空格字元 (ASCII 32)，藉此壓縮空格：

- Formfeed (ASCII 12)
- Tab (ASCII 9)
- Newline (ASCII 10)
- 歸位運送 (ASCII 13)
- 垂直索引標籤 (ASCII 11)
- 非中斷空間 (ASCII 160)

CSS decode – CSS_DECODE

AWS WAF 解碼使用 CSS 2syndata.html#characters.x 逸出規則 編碼的字元。此函數在解碼過程中最多使用兩個位元組，因此它可以幫助您發現使用 CSS 編碼進行編碼的 ASCII 字元 (這些字元通常不會被編碼)。它在反擊逃脫方面也很有用，後者是反斜線和非十六進位字元的組合。例如，javascript 的 ja\vascript。

Escape sequences decode – ESCAPE_SEQ_DECODE

AWS WAF 解碼下列 ANSI C 逸出序列：\a、\b、\f、\n、\r\t、\v、\\?、\'、\"、\xHH (十六進位)、\0000 (八進位)。無效的編碼會保留在輸出中。

Hex decode – HEX_DECODE

AWS WAF 將一組十六進位字元解碼為二進位。

HTML entity decode – HTML_ENTITY_DECODE

AWS WAF &#nnnn; 會以對應的字元取代以十六進位格式 &#xhhhh; 或小數格式表示的字元。

AWS WAF 會以未編碼的字元取代下列 HTML 編碼的字元。此清單使用小寫 HTML 編碼，但處理方式不區分大小寫，例如 &Qu0t;，且處理 " 方式相同。

HTML 編碼字元	取代為...
"	"
&	&
<	<
>	>
 或 	非中斷空格，小數 160

	\n，十進位 10
		\t，小數 9
{ 或 {	{
|、| 或 |	
} 或 }	}
!	!
#	#
$	\$
&percent; 或 %	%
'	\
(	(
)	)
* 或 *	*
+	+
,	,

HTML 編碼字元	取代為...
.	.
/	/
:	:
;	;
=	=
?	?
˜ 或 ˜	~
−	-
[或 [	[
\	\\
] 或]	]
&hat;	^
_ 或 &underbar;	_
` 或 `	`

JS decode – JS_DECODE

AWS WAF 解碼 JavaScript 逸出序列。如果 \uHHHH 程式碼在 的完整寬度 ASCII 程式碼範圍內 FF01-FF5E，則會使用較高的位元組來偵測和調整較低的位元組。如果不是，則只會使用較低的位元組，並將較高的位元組歸零，而這可能導致資訊遺失。

Lowercase – LOWERCASE

AWS WAF 將大寫字母 (A-Z) 轉換為小寫 (a-z)。

MD5 – MD5

AWS WAF 從輸入中的資料計算 MD5 雜湊。計算出的雜湊是原始二進位形式。

None – NONE

AWS WAF 會檢查 Web 請求是否收到，而不會進行任何文字轉換。

Normalize path – NORMALIZE_PATH

AWS WAF 透過移除多個不在輸入開頭的斜線、目錄自我參考和目錄回溯參考來標準化輸入字串。

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF 會轉換反斜線字元以轉送斜線，然後使用NORMALIZE_PATH轉換處理產生的字串。

Remove nulls – REMOVE_NULLS

AWS WAF 會從輸入中移除所有NULL位元組。

Replace comments – REPLACE_COMMENTS

AWS WAF 會以單一空格取代每次出現的 C 樣式註解 (`/* ... */`)。它不會壓縮多個連續的出現。它以空格 (ASCII 0x20) 取代未終止的註解。它不會變更註解的獨立終止 (`*/`)。

Replace nulls – REPLACE_NULLS

AWS WAF 會以空格字元 (ASCII 0x20) NULL 取代輸入中的每個位元組。

SQL hex decode – SQL_HEX_DECODE

AWS WAF 解碼 SQL 十六進位資料。例如，將 (0x414243) AWS WAF 解碼為 (ABC)。

URL decode – URL_DECODE

AWS WAF 會解碼 URL 編碼的值。

URL decode Unicode – URL_DECODE_UNI

與 類似URL_DECODE，但支援 Microsoft 特定的%u編碼。如果代碼是在 FF01-FF5E 的全形 ASCII 碼範圍內，則使用較高的位元組來偵測和調整較低的位元組。否則，只會使用較低的位元組，而較高的位元組會歸零。

UTF8 to Unicode – UTF8_TO_UNICODE

AWS WAF 會將所有 UTF-8 字元序列轉換為 Unicode。這有助於正常化輸入，並將非英文語言的誤報和誤報降至最低。

在 中 使用縮小範圍陳述式 AWS WAF

本節說明縮小範圍陳述式及其運作方式。

縮小範圍陳述式是可巢狀規則陳述式，您可以在受管規則群組陳述式或速率型陳述式中新增，以縮小包含規則評估的一組請求。包含的規則只會評估最先符合範圍縮減陳述式的請求。

- 受管規則群組陳述式 – 如果您將範圍縮減陳述式新增至受管規則群組陳述式，會將不符合範圍縮減陳述式的任何請求 AWS WAF 評估為不符合規則群組。只有符合範圍縮減陳述式的請求才會針對規則群組進行評估。對於定價基於所評估請求數量的受管規則群組，範圍縮減陳述式有助於控制成本。

如需受管規則群組陳述式的詳細資訊，請參閱 [在 中使用受管規則群組陳述式 AWS WAF](#)。

- 速率型規則陳述式 – 沒有範圍縮減陳述式速率的速率型規則陳述式會限制規則評估的所有請求。如果您只想要控制特定類別請求的速率，請將範圍縮減陳述式新增至速率型規則。例如，若要僅追蹤和控制來自特定地理區域的請求率，您可以在地理比對陳述式中指定該地理區域，並將其新增至以速率為基礎的規則，做為縮小範圍陳述式。

如需速率型規則陳述式的詳細資訊，請參閱 [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)。

您可以在縮小範圍陳述式中使用任何可巢狀規則。如需可用的陳述式，請參閱 [在 中使用相符規則陳述式 AWS WAF](#) 和 [在 中使用邏輯規則陳述式 AWS WAF](#)。範圍縮減陳述式的 WCUs 是您定義規則陳述式所需的 WCUs。使用縮小範圍陳述式無需額外費用。

您可以在一般規則中使用陳述式時，以相同方式設定縮小範圍陳述式。例如，您可以將文字轉換套用至您正在檢查的 Web 請求元件，也可以指定轉送的 IP 地址做為 IP 地址。這些組態僅適用於範圍縮減陳述式，且不會繼承為包含受管規則群組或速率型規則陳述式的。

例如，如果您將文字轉換套用至範圍縮減陳述式中的查詢字串，範圍縮減陳述式會在套用轉換後檢查查詢字串。如果請求符合縮小範圍陳述式條件，AWS WAF 則會將 Web 請求傳遞至包含其原始狀態的規則，而不包含縮小範圍陳述式的轉換。包含範圍縮減陳述式的規則可能會套用自己的文字轉換，但不會繼承範圍縮減陳述式中的任何內容。

您不能使用縮小範圍陳述式來指定包含規則陳述式的任何請求檢查組態。您無法將範圍縮減陳述式用作包含規則陳述式的 Web 請求前置處理器。縮小範圍陳述式的唯一角色是判斷哪些請求會傳遞至包含規則陳述式以進行檢查。

在 中 參考可重複使用的實體 AWS WAF

本節說明可重複使用實體的運作方式 AWS WAF。

有些規則使用可重複使用且由您 AWS 或 AWS Marketplace 賣方在 Web ACLs 外部管理的實體。更新可重複使用的實體時，AWS WAF 會將更新傳播至您的規則。例如，如果您在保護套件或 Web ACL 中使用 AWS 受管規則規則群組，則在 AWS 更新規則群組時，會將變更 AWS 傳播到您的 Web ACL，以更新其行為。如果您在規則中使用 IP 集合陳述式，當您更新集合時，會將變更 AWS WAF 傳播到所有參考它的規則，因此任何使用這些規則的保護套件或 Web ACLs 都會隨著您的變更保持 up-to-date 狀態。

以下是您可以在規則陳述式中使用的可重複使用的實體。

- IP 集 – 您可以建立和管理自己的 IP 集。在主控台上，您可以從導覽窗格存取這些項目。如需管理 IP 集合的相關資訊，請參閱 [中的 IP 集和 regex 模式集 AWS WAF](#)。
- Regex 比對集 – 您可以建立和管理自己的 regex 比對集。在主控台上，您可以從導覽窗格存取這些項目。如需管理規則運算式模式集的相關資訊，請參閱 [中的 IP 集和 regex 模式集 AWS WAF](#)。
- AWS 受管規則規則群組 – AWS 管理這些規則群組。在主控台上，當您將受管規則群組新增至保護套件或 Web ACL 時，即可使用這些規則群組。如需這些項目的詳細資訊，請參閱 [AWS 受管規則規則群組清單](#)。
- AWS Marketplace 受管規則群組 – AWS Marketplace 賣方會管理這些規則群組，您可以訂閱這些規則群組以使用這些規則群組。若要管理您的訂閱，請在主控台的導覽窗格中選擇 AWS Marketplace。當您將 AWS Marketplace 受管規則群組新增至保護套件或 Web ACL 時，會列出受管規則群組。對於您尚未訂閱的規則群組，您也可以 AWS Marketplace 在該頁面上找到的連結。如需 AWS Marketplace 賣方受管規則群組的詳細資訊，請參閱 [AWS Marketplace 規則群組](#)。
- 您自己的規則群組 – 您可以管理自己的規則群組，通常是當您需要一些無法透過受管規則群組使用的行為時。在主控台上，您可以從導覽窗格存取這些項目。如需詳細資訊，請參閱 [管理您自己的規則群組](#)。

刪除參考集或規則群組

當您刪除參考的實體時，會 AWS WAF 檢查它目前是否在保護套件或 Web ACL 中使用。如果 AWS WAF 發現實體正在使用中，它會警告您。AWS WAF 幾乎總是能夠判斷實體是否被保護套件或 Web ACL 參考。但是在極少數的情況下，它也可能無法判斷。如果您需要確定要刪除的實體未在使用中，請在 Web ACL 中檢查它，然後再刪除它。

在中使用相符規則陳述式 AWS WAF

本節說明什麼是配對陳述式及其運作方式。

比對陳述式會將 Web 請求或其原始伺服器與您提供的條件進行比較。對於此類型的許多陳述式，AWS WAF 會比較符合內容請求的特定元件。

相符陳述式是可巢狀的。您可以在邏輯規則陳述式中巢狀化任何這些陳述式，也可以在縮小範圍陳述式中使用它們。如需邏輯規則陳述式的資訊，請參閱 [在中使用邏輯規則陳述式 AWS WAF](#)。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

此表格說明您可以新增至規則的一般比對陳述式，並提供一些準則來計算每個規則的保護套件或 Web ACL 容量單位 (WCU) 用量。如需 WCU 的相關資訊，請參閱 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

比對陳述式	描述	WCU
地理比對	檢查請求的來源國家/地區，並套用來源國家/地區和區域的標籤。	1
ASN 比對	檢查請求是否有與 IP 地址和地址範圍相關聯的 ASN。	1
IP 集同比對	針對一組 IP 地址和地址範圍檢查請求。	1 表示大多數情況。如果您將陳述式設定為使用具有轉送 IP 地址的標頭，並在標頭中指定位置 Any，則將 WCUs 增加 4。
標籤比對規則陳述式	檢查請求是否有由相同保護套件或 Web ACL 中其他規則新增的標籤。	1
Regex 比對規則陳述式	將 regex 模式與指定的請求元件進行比較。	3，作為基本成本。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。
規則運算式模式集		

比對陳述式	描述	WCU
	將規則運算式模式與指定的請求元件比較。	每個模式集 25 個，以基本成本表示。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。
大小約束	針對指定的請求元件檢查大小約束。	1，作為基本成本。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。
SQLi 攻擊	檢查指定請求元件中的惡意 SQL 程式碼。	20，作為基本成本。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。

比對陳述式	描述	WCU
字串比對	比較字串與指定的請求元件。	基本成本取決於字串比對的類型，且介於 1 到 10 之間。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。
XSS 指令碼攻擊	檢查指定請求元件中的跨網站指令碼攻擊。	40，作為基本成本。 如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。

地理比對規則陳述式

本節說明什麼是地理比對陳述式及其運作方式。

使用地理或地理比對陳述式，根據原始國家和區域來管理 Web 請求。地理比對陳述式會將標籤新增至 Web 請求，以指出來源國家和來源區域。無論陳述式條件是否符合請求，它都會新增這些標籤。地理比對陳述式也會執行與請求來源國的比對。

如何使用地理比對陳述式

您可以使用地理比對陳述式進行國家或地區比對，如下所示：

- **國家** - 您可以使用地理比對規則本身，僅根據請求的原始國家/地區來管理請求。規則陳述式符合國家/地區代碼。您也可以遵循地理比對規則，並在原始國家/地區標籤上遵循符合的標籤比對規則。
- **區域** — 使用地理比對規則，後面接著標籤比對規則，根據原始伺服器區域來管理請求。您無法單獨使用地理比對規則來比對區域代碼。

如需使用標籤比對規則的詳細資訊，請參閱 [標籤比對規則陳述式](#) 和 [中的 Web 請求標籤 AWS WAF](#)。

地理比對陳述式的運作方式

使用地理比對陳述式，AWS WAF 管理每個 Web 請求，如下所示：

1. 決定請求的國家和地區代碼 — 根據請求的 IP 地址 AWS WAF 來決定請求的國家和地區。根據預設，AWS WAF 會使用 Web 請求原始伺服器的 IP 地址。您可以在規則陳述式設定中啟用轉送的 IP 組態 X-Forwarded-For，AWS WAF 指示使用來自替代請求標頭的 IP 地址，例如。

AWS WAF 決定使用 MaxMind GeoIP 資料庫的請求位置。MaxMind 會在國家層級報告非常高的資料準確性，但準確性會根據國家/地區和 IP 類型等因素而有所不同。如需 MaxMind 的詳細資訊，請參閱 [MaxMind IP 地理位置](#)。如果您認為任何 GeoIP 資料不正確，您可以在 [MaxMind Correct GeoIP2 Data](#) 向 Maxmind 提交更正請求。

AWS WAF 使用國際標準化組織 (ISO) 3166 標準中的 alpha-2 國家和區域代碼。您可以在下列位置找到代碼：

- 在 ISO 網站上，您可以在 [ISO Online Browsing Platform \(OBP\)](#) 搜尋國家/地區代碼。
- 在 Wikipedia 上，國家/地區代碼列於 [ISO 3166-2](#)。

國家/地區的區域代碼列於 URL。https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code> 例如，美國的區域位於 [ISO 3166-2 : US](#)，烏克蘭則位於 [ISO 3166-2 : UA](#)。

2. 決定要新增至請求的國家/地區標籤和區域標籤 — 這些標籤指出地理比對陳述式是使用原始 IP 還是轉送 IP 組態。

- 原始 IP

國家/地區標籤為 `awsaf:clientip:geo:country:<ISO country code>`。美國的範例：`awsaf:clientip:geo:country:US`。

區域標籤為 `awsaf:clientip:geo:region:<ISO country code>-<ISO region code>`。美國奧勒岡州的範例：`awsaf:clientip:geo:region:US-OR`。

- 轉送的 IP

國家/地區標籤為 `awsaf:forwardedip:geo:country:<ISO country code>`。美國的範例：`awsaf:forwardedip:geo:country:US`。

區域標籤為 `awsaf:forwardedip:geo:region:<ISO country code>-<ISO region code>`。美國奧勒岡的範例：`awsaf:forwardedip:geo:region:US-OR`。

如果請求指定的 IP 地址無法使用國家或地區代碼，則 AWS WAF 會在 XX 標籤中使用 取代 值。例如，下列標籤適用於無法使用國家/地區的用戶端

IP : awswaf:clientip:geo:country:XX 而下列標籤適用於轉送 IP，其國家/地區為美國，但其區域碼無法使用：awswaf:forwardedip:geo:region:US-XX。

3. 根據規則條件評估請求的國家/地區代碼

地理比對陳述式會將國家和區域標籤新增至其檢查的所有請求，無論其是否找到比對。

Note

AWS WAF 在規則的 Web 請求評估結束時新增任何標籤。因此，您針對地理比對陳述式的標籤使用的任何標籤比對，都必須在包含地理比對陳述式的規則以外的個別規則中定義。

如果您想要只檢查區域值，您可以使用 Count 動作和單一國家/地區碼比對來撰寫地理比對規則，然後撰寫區域標籤的標籤比對規則。您必須為地理比對規則提供國家/地區代碼來評估，即使此方法也是如此。您可以指定不太可能成為網站流量來源的國家/地區，以減少記錄和計數指標。

CloudFront 分佈和 CloudFront 地理限制功能

對於 CloudFront 分佈，如果您使用 CloudFront 地理限制功能，請注意該功能不會將封鎖的請求轉送至 AWS WAF。它會將允許的請求轉送至 AWS WAF。如果您想要根據地理位置加上可在其中指定的其他條件來封鎖請求 AWS WAF，請使用 AWS WAF 地理比對陳述式，請勿使用 CloudFront 地理限制功能。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 1 個 WCU。

設定 – 此陳述式使用以下設定：

- 國家/地區代碼 – 要比較地理比對的國家/地區代碼陣列。這些必須是 ISO 3166 國際標準 alpha-2 國家 ISO 代碼的兩個字元國家代碼，例如 ["US", "CN"]。
- (選用) 轉送 IP 組態 – 預設情況下，AWS WAF 會使用 Web 請求原始伺服器中的 IP 地址來判斷原始國家/地區。或者，您可以改為將規則設定為在 HTTP 標頭中使用轉送的 IPX-Forwarded-For。AWS WAF 會使用標頭中的第一個 IP 地址。使用此組態，您也可以指定後援行為，以套用至

標頭中 IP 地址格式不正確的 Web 請求。備用行為會將請求的相符結果設定為相符或不相符。如需詳細資訊，請參閱[使用轉送的 IP 地址](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對請求選項，選擇來自 國家/地區的原始伺服器。
- API – [GeoMatchStatement](#)

範例

您可以使用地理比對陳述式來管理來自特定國家或地區的請求。例如，如果您想要封鎖來自某些國家/地區的請求，但仍允許來自這些國家/地區的一組特定 IP 地址的請求，您可以建立 動作設為 的規則，Block以及下列巢狀陳述式，如虛擬程式碼所示：

- AND 陳述式
 - 列出您要封鎖的國家/地區的地理比對陳述式
 - NOT 陳述式
 - IP 集合陳述式，指定您要允許通過的 IP 地址

或者，如果您想要封鎖某些國家/地區的某些區域，但仍允許這些國家/地區的其他區域的請求，您可以先定義地理比對規則，並將 動作設為 Count。然後，定義符合新增地理相符標籤的標籤相符規則，並根據需要處理請求。

下列虛擬程式碼說明此方法的範例：

1. Geo 比對陳述式列出具有您要封鎖之區域的國家，但動作設為 Count。無論相符狀態為何，這都會標記每個 Web 請求，也可讓您計算感興趣的國家/地區的指標。
2. AND 具有封鎖動作的 陳述式
 - 標籤比對陳述式，指定您要封鎖之國家/地區的標籤
 - NOT 陳述式
 - 標籤比對陳述式，指定您要允許透過之國家/地區的區域標籤

下列 JSON 清單顯示實作先前虛擬程式碼中所述的兩個規則。這些規則會封鎖來自美國的所有流量，但來自奧勒岡和華盛頓的流量除外。地理比對陳述式會將國家和區域標籤新增至其檢查的所有請求。標

籤比對規則會在地理比對規則之後執行，因此可以比對地理比對規則剛新增的國家和區域標籤。地理比對陳述式使用轉送的 IP 地址，因此標籤比對也會指定轉送的 IP 標籤。

```
{
  "Name": "geoMatchForLabels",
  "Priority": 10,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "X-Forwarded-For",
        "FallbackBehavior": "MATCH"
      }
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "blockUSButNotOR0rWA",
  "Priority": 11,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awsaf:forwardedip:geo:country:US"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "OrStatement": {
                "Statements": [
```



```

        "US"
    ]
}
},
"Action": {
    "Count": {}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
}
},
{
    "Name": "rateLimitOregon",
    "Priority": 195,
    "Statement": {
        "RateBasedStatement": {
            "Limit": 3000,
            "AggregateKeyType": "IP",
            "ScopeDownStatement": {
                "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awsfaf:clientip:geo:region:US-OR"
                }
            }
        }
    }
},
"Action": {
    "Block": {}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
}
},
{
    "Name": "rateLimitUSNotOR",
    "Priority": 200,
    "Statement": {
        "RateBasedStatement": {
            "Limit": 100,
            "AggregateKeyType": "IP",

```



```
    "ScopeDownStatement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "aws:waf:clientip:geo:country:US"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "LabelMatchStatement": {
                  "Scope": "LABEL",
                  "Key": "aws:waf:clientip:geo:region:US-OR"
                }
              }
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rateLimitUSNotOR"
    }
  }
}
```

IP 集合比對規則陳述式

本節說明什麼是 IP 集比對陳述式及其運作方式。

IP 集合比對陳述式會根據一組 IP 地址和地址範圍來檢查 Web 請求的 IP 地址。使用此選項以根據請求源自的 IP 地址來允許或封鎖 Web 請求。根據預設，AWS WAF 會使用來自 Web 請求原始伺服器的 IP 地址，但您可以將 X-Forwarded-For 改為將規則設定為使用 HTTP 標頭。

AWS WAF 支援除 以外的所有 IPv4 和 IPv6 CIDR 範圍/0。如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目 [無類別域間路由](#)。一個 IP 集合最多可容納 10,000 個 IP 地址或 IP 地址範圍進行檢查。

Note

每個 IP 集合比對規則都會參考一個 IP 集合，您可以獨立於規則而建立和維護。您可以在多個規則中使用單一 IP 集，當您更新參考集時，AWS WAF 會自動更新參考集的所有規則。如需建立和管理 IP 集的資訊，請參閱 [在 中建立和管理 IP 集 AWS WAF](#)。

當您在規則群組或保護套件或 Web ACL 中新增或更新規則時，請選擇選項 IP 集，然後選取您要使用的 IP 集名稱。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 大多數 1 個 WCU。如果您將陳述式設定為使用轉送的 IP 地址並指定 的位置 ANY，請將 WCU 用量增加 4。

此陳述式使用以下設定：

- IP 集規格 – 從清單中選擇您要使用的 IP 集，或建立新的 IP 集。
- (選用) 轉送 IP 組態 – 替代轉送 IP 標頭名稱，用於取代請求原始伺服器。您可以指定要比對標頭中的第一個、最後一個或任何地址。您也可以指定後援行為，以套用至指定標頭中 IP 地址格式不正確的 Web 請求。備用行為會將請求的相符結果設定為相符或不相符。如需詳細資訊，請參閱 [使用轉送的 IP 地址](#)。

尋找此規則陳述式的位置

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 在請求選項中，從 IP 地址選擇原始伺服器。
- 在主控台上新增我自己的規則和規則群組頁面 – 選擇 IP 集選項。
- API – [IPSetReferenceStatement](#)

自治系統編號 (ASN) 比對規則陳述式

中的 ASN 比對規則陳述式 AWS WAF 可讓您根據與請求 IP 地址相關聯的自治系統編號 (ASN) 來檢查 Web 流量。ASNs 是指派給大型網際網路網路的唯一識別符，由網際網路服務供應商、企業、大學或政府機構等組織管理。透過使用 ASN 比對陳述式，您可以允許或封鎖來自特定網路組織的流量，而無需管理個別 IP 地址。相較於以 IP 為基礎的規則，此方法提供更穩定且更有效率的方法來控制存取，因為 ASNs 變更的頻率低於 IP 範圍。

ASN 比對對於封鎖來自已知有問題網路的流量或僅允許來自信任合作夥伴網路的存取等案例特別有用。ASN 比對陳述式可讓您靈活地透過選用的轉送 IP 組態來判斷用戶端 IP 地址，使其與各種網路設定相容，包括使用內容交付網路 (CDNs) 或反向代理的網路設定。

Note

ASN 比對補充，但不取代標準身分驗證和授權控制。我們建議您實作身分驗證和授權機制，例如 IAM，以驗證應用程式中所有請求的身分。

ASN 比對陳述式的運作方式

AWS WAF 根據請求的 IP 地址決定請求的 ASN。根據預設，AWS WAF 會使用 Web 請求原始伺服器的 IP 地址。您可以透過在規則陳述式設定中啟用轉送的 IP 組態 X-Forwarded-For，AWS WAF 將設定為使用來自替代請求標頭的 IP 地址，例如。

ASN 比對陳述式會將請求的 ASN 與規則中指定的 ASNs 清單進行比較。如果 ASN 符合清單中的一個，則陳述式會評估為 true，並套用相關聯的規則動作。

處理未映射 ASNs

如果 AWS WAF 無法判斷有效 IP 地址的 ASN，則會指派 ASN 0。您可以在規則中包含 ASN 0，以明確處理這些案例。

無效的 IP 地址的備用行為

當您將 ASN 比對陳述式設定為使用轉送 IP 地址時，您可以為指定標頭中 IP 地址無效或遺失的請求指定相符或不相符的備用行為。

規則陳述式特性

可巢狀 – 您可以巢狀化此陳述式類型。

WCUs – 1 個 WCU

此陳述式使用以下設定：

- ASN 清單 – 要比較 ASN 比對的 ASN 編號陣列。有效值的範圍從 0 到 4294967295。您可以為每個規則指定最多 100 ASNs。
- (選用) 轉送 IP 組態 – 預設 AWS WAF 會使用 Web 請求原始伺服器中的 IP 地址來判斷 ASN。或者，您可以改為將規則設定為在 HTTP 標頭中使用轉送的 IPX-Forwarded-For。您可以指定是否使用標頭中的第一個、最後一個或任何地址。使用此組態，您也可以指定後援行為，以套用至標頭中 IP 地址格式不正確的 Web 請求。備用行為會將請求的相符結果設定為相符或不相符。如需詳細資訊，請參閱[使用轉送的 IP 地址](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對請求選項，選擇來自 ASN 的來源。
- API – [AsnMatchStatement](#)

範例

此範例會封鎖衍生自 X-Forwarded-For 標頭之兩個特定 ASNs 的請求。如果標頭中的 IP 地址格式不正確，則設定的備用行為為 NO_MATCH。

```
{
  "Action": {
    "Block": {}
  },
  "Name": "AsnMatchStatementRule",
  "Priority": 1,
  "Statement": {
    "AsnMatchStatement": {
      "AsnList": [64496, 64500]
    },
    "ForwardedIPConfig": {
      "FallbackBehavior": "NO_MATCH",
      "HeaderName": "X-Forwarded-For"
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AsnMatchRuleMetrics",
```

```
    "SampledRequestsEnabled": true
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "WebAclMetrics",
    "SampledRequestsEnabled": true
  }
}
```

標籤比對規則陳述式

本節說明什麼是標籤比對陳述式及其運作方式。

標籤比對陳述式會根據字串規格檢查 Web 請求上的標籤。可供規則檢查使用的標籤是已由相同保護套件或 Web ACL 評估中的其他規則新增至 Web 請求的標籤。

標籤不會保留在保護套件或 Web ACL 評估之外，但您可以在 CloudWatch 中存取標籤指標，而且您可以在主控台中 AWS WAF 查看任何保護套件或 Web ACL 的標籤資訊摘要。如需詳細資訊，請參閱[標籤指標和維度](#)及[監控和調校您的 AWS WAF 保護](#)。您也可以從日誌中查看標籤。如需相關資訊，請參閱[保護套件或 Web ACL 流量的日誌欄位](#)。

Note

標籤比對陳述式只能查看先前在保護套件或 Web ACL 中評估之規則的標籤。如需有關 如何 AWS WAF 評估保護套件或 Web ACL 中的規則和規則群組的資訊，請參閱[設定規則優先順序](#)。

如需新增和比對標籤的詳細資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#)。

規則陳述式特性

可巢狀 – 您可以巢狀化此陳述式類型。

WCUs – 1 個 WCU

此陳述式使用以下設定：

- 比對範圍 – 將此設定為標籤，以比對標籤名稱，並選擇性地比對先前的命名空間和字首。將此設定為命名空間，以比對部分或全部命名空間規格，並選擇性地比對前面的字首。

- 金鑰 – 您要比對的字串。如果您指定命名空間比對範圍，這應該只指定命名空間和選用的字首，加上結尾冒號。如果您指定標籤比對範圍，這必須包含標籤名稱，也可以選擇性地包含先前的命名空間和字首。

如需這些設定的詳細資訊，請參閱 [AWS WAF 符合標籤的 規則](#) 和 [AWS WAF 標籤比對範例](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對請求選項，選擇有標籤。
- API – [LabelMatchStatement](#)

Regex 比對規則陳述式

本節說明什麼是 regex 比對陳述式及其運作方式。

regex 比對陳述式會指示 AWS WAF 將請求元件與單一規則表達式 (regex) 比對。如果請求元件與您指定的 regex 相符，Web 請求就會符合陳述式。

對於您希望使用數學邏輯結合相符條件的情況 [規則運算式模式集比對規則陳述式](#)，此陳述式類型是 的絕佳替代方案。例如，如果您希望請求元件與某些規則運算式模式相符，並且不與其他規則運算式相符，您可以使用 [AND 規則陳述式](#) 和 [來結合規則運算式相符陳述式](#) [NOT 規則陳述式](#)。

AWS WAF 支援 PCRE 程式庫使用的模式語法 libpcre，但有一些例外狀況。程式庫記錄在 [PCRE - Perl 相容規則運算式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 3 WCUs，作為基本成本。如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

⚠ Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀 [中 AWS WAF 可檢查多少內容的限制](#) [在中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用的文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對相符類型，選擇相符規則表達式。
- API – [RegexMatchStatement](#)

規則運算式模式集比對規則陳述式

本節說明什麼是 regex 模式集比對陳述式及其運作方式。

規則表達式模式集比對會檢查您在規則表達式模式集內為規則表達式模式指定的 Web 請求部分。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外狀況。程式庫記錄在 [PCRE - Perl 相容規則運算式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

i Note

每個規則運算式模式集比對規則都會參考一個規則運算式模式集，您可以獨立於規則而建立和維護。您可以在多個規則中使用單一 regex 模式集，而且當您更新參考集時，AWS WAF 會自動更新所有參考規則。

如需建立和管理規則運算式模式集的相關資訊，請參閱 [在中建立和管理 regex 模式集 AWS WAF](#)。

regex 模式集比對陳述式 AWS WAF 會指示 搜尋您選擇的請求元件內集合中的任何模式。如果請求元件符合集合中的任何模式，則 Web 請求將比對模式集規則陳述式。

如果您想要使用邏輯合併您的 regex 模式比對，例如要比對某些規則表達式，但無法比對其他表達式，請考慮使用 [Regex 比對規則陳述式](#)。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 25 WCUs，作為基本成本。如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀 [中 AWS WAF 可檢查多少內容的限制](#) [在中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用的文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

此陳述式需要下列設定：

- Regex 模式集規格 – 從清單中選擇您要使用的 regex 模式集，或建立新的模式集。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對相符類型，選擇字串相符條件 > 從規則表達式集中比對模式。
- API – [RegexPatternSetReferenceStatement](#)

大小約束規則陳述式

本節說明什麼是大小限制陳述式及其運作方式。

大小限制陳述式會將 Web 請求元件 AWS WAF 接收的位元組數與您提供的數字進行比較，並根據您的比較條件進行比對。

Note

此陳述式使用 AWS WAF 接收用於檢查的元件大小。對於內文、標頭和 Cookie 元件，此大小可能小於傳送至受保護資源的原始大小。如需詳細資訊，請參閱[在中過大 Web 請求元件 AWS WAF](#)。

比較條件是大於 (>) 或小於 (<) 的運算子。例如，您可以比對大小大於 100 位元組的查詢字串請求。

如果您檢查 URI 路徑，路徑/中的任何 都會計為一個字元。例如，URI 路徑長度/logo.jpg 為九個字元。

Note

此陳述式只會檢查 Web 請求元件的大小。它不會檢查元件的內容。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 1 個 WCU，作為基本成本。如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。如需 Web 請求元件的詳細資訊，請參閱[在中調整規則陳述式設定 AWS WAF](#)。

套用任何轉換後，大小限制陳述式只會檢查元件的大小。它不會檢查元件的內容。

- 選用的文字轉換 – AWS WAF 您想要在檢查其大小之前，對請求元件執行的轉換。例如，您可以壓縮空格或解碼 HTML 實體。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱[在中使用文字轉換 AWS WAF](#)。

此外，此陳述式需要下列設定：

- 大小比對條件 – 這表示用來比較您提供的 大小與所選請求元件的數值比較運算子。從清單中選擇運算子。
- 大小 – 要在比較中使用的大小設定，以位元組為單位。

Note

對於內文、標頭和 Cookie 元件，請使用小於 AWS WAF 可檢查大小上限的大小。較大的數字永遠不會產生相符結果。如需詳細資訊，請參閱[在中過大 Web 請求元件 AWS WAF](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對相符類型，在大小相符條件下，選擇您要使用的條件。
- API – [SizeConstraintStatement](#)

SQL Injection 攻擊規則陳述式

本節說明什麼是 SQL Injection 規則陳述式及其運作方式。

SQL Injection 規則陳述式會檢查是否有惡意 SQL 程式碼。攻擊者會將惡意 SQL 程式碼插入 Web 請求，以執行修改資料庫或從中擷取資料等動作。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 基本成本取決於規則陳述式的敏感度等級設定：Low 成本 20 和 High 成本 30。

如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀有關 AWS WAF 可檢查多少內容的限制[在中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

此外，此陳述式需要下列設定：

- 敏感度層級 – 此設定會調整 SQL Injection 比對條件的敏感度。選項包括 LOW 和 HIGH。預設設定為 LOW。

HIGH 設定會偵測更多 SQL Injection 攻擊，而是建議設定。由於敏感度較高，此設定會產生更多誤報，特別是當您的 Web 請求通常包含不尋常的字串時。在保護套件或 Web ACL 測試和調校期間，您可能需要執行更多工作來緩解誤報。如需相關資訊，請參閱 [測試和調校您的 AWS WAF 保護](#)。

較低的設定提供較不嚴格的 SQL Injection 偵測，這也會減少誤報。對於具有其他 SQL Injection 攻擊保護或容錯能力較低的資源而言，LOW 是更好的選擇。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對比對類型，選擇攻擊比對條件 > 包含 SQL 注入攻擊。
- API – [SqliMatchStatement](#)

字串比對規則陳述式

本節說明字串比對陳述式是什麼及其運作方式。

字串比對陳述式指出 AWS WAF 您想要在請求中搜尋的字串、要搜尋的請求中的位置，以及如何搜尋。例如，您可以在請求中任何查詢字串的開頭尋找特定字串，或是在請求的 User-agent 標頭中尋找完全相符項目。通常，字串包含可列印 ASCII 字元，但您可以使用十六進位 0x00 到 0xFF 的任何字元 (小數 0 到 255)。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 基本成本取決於您使用的配對類型。

- 完全符合字串 – 2

- 以字串開頭 – 2
- 結尾為字串 – 2
- 包含字串 – 10
- 包含單字 – 10

如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs 加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀 [中 AWS WAF 可檢查多少內容的限制](#) [在中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用的文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

此外，此陳述式需要下列設定：

- 要比對的字串 – 這是您要與指定請求元件 AWS WAF 比較的字串。通常，字串包含可列印 ASCII 字元，但您可以使用十六進位 0x00 到 0xFF 的任何字元 (小數 0 到 255)。
- 字串比對條件 – 這表示您要 AWS WAF 執行的搜尋類型。
 - 完全符合字串 – 字串和請求元件的值相同。
 - 以字串開頭 – 字串會出現在請求元件的開頭。
 - 以字串結尾 – 字串會出現在請求元件的結尾。
 - 包含字串 – 字串會出現在請求元件的任何位置。
 - 包含單字 – 您指定的字串必須出現在請求元件中。

對於此選項，您指定的字串必須只包含英數字元或底線 (A-Z、a-z、0-9 或 `_`)。

下列其中一項必須為 true，才能比對請求：

- 該字串與請求元件的數值 (如標頭值) 完全相符。
- 該字串位於請求元件的開頭，後面加上非英數字元或底線 (_) 的字元，例如 BadBot;。
- 該字串位於請求元件的尾端，前面加上非英數字元或底線 (_) 的字元，例如 ;BadBot。
- 該字串位於請求元件的中間，前後加上非英數字元或底線 (_) 的字元，例如 -BadBot;。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對相符類型，選擇字串相符條件，然後填入您要比對的字串。
- API – [ByteMatchStatement](#)

跨網站指令碼攻擊規則陳述式

本節說明什麼是 XSS（跨網站指令碼）攻擊陳述式及其運作方式。

XSS 攻擊陳述式會檢查 Web 請求元件中是否有惡意指令碼。在 XSS 攻擊中，攻擊者會使用良性網站中的漏洞做為工具，將惡意用戶端網站指令碼注入其他合法的 Web 瀏覽器。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 40 WCUs，作為基本成本。如果您使用請求元件 所有查詢參數，請新增 10 WCUs。如果您使用請求元件 JSON 內文，請將基本成本 WCUs加倍。針對您套用的每個文字轉換，新增 10 WCUs。

此陳述式類型在 Web 請求元件上運作，且需要下列請求元件設定：

- 請求元件 – 要檢查的 Web 請求部分，例如查詢字串或內文。

Warning

如果您檢查請求元件內文、JSON 內文、標頭或 Cookie，請閱讀 [中 AWS WAF 可檢查多少內容的限制](#) [在中過大 Web 請求元件 AWS WAF](#)。

如需 Web 請求元件的詳細資訊，請參閱 [在中調整規則陳述式設定 AWS WAF](#)。

- 選用的文字轉換 – AWS WAF 您想要在檢查請求元件之前對請求元件執行的轉換。例如，您可以將轉換為小寫或標準化空格。如果您指定多個轉換，會依列出的順序 AWS WAF 處理它們。如需相關資訊，請參閱 [在中使用文字轉換 AWS WAF](#)。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 針對相符類型，選擇攻擊相符條件 > 包含 XSS 注入攻擊。
- API – [XssMatchStatement](#)

在中使用邏輯規則陳述式 AWS WAF

本節說明什麼是邏輯規則陳述式及其運作方式。

使用邏輯規則陳述式來合併其他陳述式或否定其結果。每個邏輯規則陳述式至少需要一個巢狀化的陳述式。

若要在邏輯上合併或否定規則陳述式結果，您可以在邏輯規則陳述式下巢狀化陳述式。

邏輯規則陳述式是可巢狀的。您可以將它們巢狀到其他邏輯規則陳述式中，並在縮小範圍陳述式中使用它們。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

Note

主控台上的視覺化編輯器支援一個層級的規則陳述式巢狀，這適用於許多需求。若要巢狀更多關卡，請在主控台上編輯規則的 JSON 表示法，或使用 APIs。

此表格說明邏輯規則陳述式，並提供計算每個保護套件或 Web ACL 容量單位 (WCU) 用量的指導方針。如需 WCU 的相關資訊，請參閱 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

邏輯陳述式	描述	WCU
AND 邏輯	結合巢狀陳述式與AND邏輯。	以巢狀化陳述式為基礎
NOT 邏輯	否定巢狀化陳述式的結果。	以巢狀化陳述式為基礎
OR 邏輯	結合巢狀陳述式與OR邏輯。	以巢狀化陳述式為基礎

AND 規則陳述式

AND 規則陳述式結合了巢狀陳述式與邏輯AND操作，因此所有巢狀陳述式都必須相符，陳述AND式才能相符。這至少需要兩個巢狀陳述式。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 取決於巢狀陳述式。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 如果請求，請選擇 符合所有陳述式 (AND)，然後填入巢狀陳述式。
- API – [AndStatement](#)

範例

下列清單顯示 AND和 NOT 邏輯規則陳述式的使用，以消除 SQL 注入攻擊陳述式相符項目的誤報。在此範例中，假設我們可以編寫單一位元組比對陳述式，以符合導致誤報的請求。

AND 陳述式會比對不符合位元組比對陳述式且符合 SQL 注入攻擊陳述式的請求。

```
{
  "Name": "SQLiExcludeFalsePositives",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "NotStatement": {
            "Statement": {
              "ByteMatchStatement": {
                "SearchString": "string identifying a false positive",
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                }
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ]
            }
          }
        }
      ]
    }
  }
}
```

```

        }
      ],
      "PositionalConstraint": "CONTAINS"
    }
  }
},
{
  "SqliMatchStatement": {
    "FieldToMatch": {
      "Body": {
        "OversizeHandling": "MATCH"
      }
    },
    "TextTransformations": [
      {
        "Priority": 0,
        "Type": "NONE"
      }
    ]
  }
}
],
}
},
{
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "SQLiExcludeFalsePositives"
  }
}
}

```

使用主控台規則視覺化編輯器，您可以在 或 陳述式下巢狀非邏輯陳述NOT式OR或AND陳述式。NOT陳述式的巢狀會顯示在先前的範例中。

使用主控台規則視覺化編輯器，您可以在邏輯規則陳述式下巢狀化最可巢狀的陳述式，例如先前範例所示的陳述式。您無法使用視覺化編輯器來巢狀OR或AND陳述式。若要設定此類型的巢狀，您需要在JSON 中提供規則陳述式。例如，下列 JSON 規則清單包含 OR陳述式巢狀在AND陳述式內。

```
{
```

```
"Name": "match_rule",
"Priority": 0,
"Statement": {
  "AndStatement": {
    "Statements": [
      {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
        }
      },
      {
        "NotStatement": {
          "Statement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
            }
          }
        }
      }
    ],
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "JM",
              "JP"
            ]
          }
        },
        {
          "ByteMatchStatement": {
            "SearchString": "JCountryString",
            "FieldToMatch": {
              "Body": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  }
}
```

```
        "PositionalConstraint": "CONTAINS"
      }
    }
  ]
}
}
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "match_rule"
}
}
```

NOT 規則陳述式

NOT 規則陳述式在邏輯上否定單一巢狀陳述式的結果，因此巢狀陳述式必須與要比對的NOT陳述式不相符，反之亦然。這需要一個巢狀化陳述式。

例如，如果您想要封鎖不是來自特定國家/地區的請求，請建立動作設為封鎖的NOT陳述式，並巢狀指定國家/地區的地理比對陳述式。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 取決於巢狀陳述式。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 如果請求，請選擇 與陳述式 (NOT) 不相符，然後填入巢狀陳述式。
- API – [NotStatement](#)

OR 規則陳述式

OR 規則陳述式結合了巢狀陳述式與OR邏輯，因此其中一個巢狀陳述式必須符合，陳述OR式才能相符。這至少需要兩個巢狀陳述式。

例如，如果您想要封鎖來自特定國家/地區的請求，或包含特定查詢字串的請求，您可以建立 OR 陳述式，並在其中巢狀化為該國家/地區的地理比對陳述式，以及查詢字串的字串比對陳述式。

如果您想要封鎖不是來自特定國家/地區的請求或包含特定查詢字串的請求，您可以修改先前的 OR 陳述式，將地理比對陳述式放在 NOT 陳述式內的一個層級。此巢狀層級需要您使用 JSON 格式，因為主控台僅支援一個巢狀層級。

規則陳述式特性

可巢狀 – 您可以巢狀此陳述式類型。

WCUs – 取決於巢狀陳述式。

尋找此規則陳述式的位置

- 主控台上的規則建置器 – 如果請求，請選擇至少符合其中一個陳述式 (OR)，然後填入巢狀陳述式。
- API – [OrStatement](#)

範例

下列清單顯示使用 OR 來結合其他兩個陳述式。如果其中一個巢狀 OR 陳述式相符，則陳述式是相符的。

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        }
      ]
    }
  }
}
```

```
    }
  },
  {
    "IPSetReferenceStatement": {
      "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
    }
  }
]
}
}
}
```

使用主控台規則視覺化編輯器，您可以在邏輯規則陳述式下巢狀化最可巢狀的陳述式，但無法使用視覺化編輯器來巢狀化OR或AND陳述式。若要設定此類型的巢狀，您需要在 JSON 中提供規則陳述式。例如，下列 JSON 規則清單包含 OR陳述式內巢狀的AND陳述式。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        }
      ]
    },
    {
      "OrStatement": {
        "Statements": [
          {
```

```
        "GeoMatchStatement": {
          "CountryCodes": [
            "JM",
            "JP"
          ]
        },
      ],
      {
        "ByteMatchStatement": {
          "SearchString": "JCountryString",
          "FieldToMatch": {
            "Body": {}
          },
          "TextTransformations": [
            {
              "Priority": 0,
              "Type": "NONE"
            }
          ],
          "PositionalConstraint": "CONTAINS"
        }
      ]
    ]
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

在 中使用以速率為基礎的規則陳述式 AWS WAF

本節說明什麼是以速率為基礎的規則陳述式及其運作方式。

以速率為基礎的規則會計數傳入的請求，並在以太快的速度到達時計算速率限制請求。此規則會根據您的條件彙總請求，並根據規則的評估時段、請求限制和動作設定，計數和速率會限制彙總分組。

Note

您也可以使用 Bot Control AWS 受管規則規則群組的目標保護層級來評分限制 Web 請求。使用此受管規則群組會產生額外費用。如需詳細資訊，請參閱[速率型規則和目標 Bot Control 規則中速率限制的選項](#)。

AWS WAF 會針對您使用的速率型規則的每個執行個體分別追蹤和管理 Web 請求。例如，如果您在兩個 Web ACLs 中提供相同的以速率為基礎的規則設定，則兩個規則陳述式中的每一個都代表以速率為基礎的規則的個別執行個體，並且每個都會取得自己的追蹤和管理 AWS WAF。如果您在規則群組內定義以速率為基礎的規則，然後在多個位置使用該規則群組，則每次使用都會建立以速率為基礎的規則的個別執行個體，以取得自己的追蹤和管理 AWS WAF。

不可巢狀化 – 您無法將此陳述式類型巢狀在其他陳述式中。您可以直接將其包含在保護套件或 Web ACL 或規則群組中。

縮小範圍陳述式 – 此規則類型可以採用縮小範圍陳述式，以縮小規則追蹤的請求範圍和速率限制。縮小範圍陳述式可以是選用或必要，視您的其他規則組態設定而定。本節涵蓋詳細資訊。如需縮小範圍陳述式的一般資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

WCUs 2，作為基本成本。針對您指定的每個自訂彙總金鑰，新增 30 WCUs。如果您在規則中使用縮小範圍陳述式，請計算並新增該陳述 WCUs。

尋找此規則陳述式的位置

- 保護套件或 Web ACL 中的規則建置器，在主控制台 – 在規則下，針對類型，選擇以速率為基礎的規則。
- API – [RateBasedStatement](#)

主題

- [中的以速率為基礎的規則高階設定 AWS WAF](#)
- [中的以速率為基礎的規則警告 AWS WAF](#)
- [在中彙總以速率為基礎的規則 AWS WAF](#)
- [以速率為基礎的規則彙總執行個體和計數](#)

- [將速率限制套用至 中的請求 AWS WAF](#)
- [中的以速率為基礎的規則範例 AWS WAF](#)
- [列出速率受到以速率為基礎的規則限制的 IP 地址](#)

中的以速率為基礎的規則高階設定 AWS WAF

以速率為基礎的規則陳述式使用以下高階設定：

- 評估時段 – 應包含在其請求計數中的時間 AWS WAF 量，以秒為單位，從目前時間回頭查看。例如，對於 120 的設定，當 AWS WAF 檢查速率時，它會計算目前時間前 2 分鐘的請求。有效設定為 60 (1 分鐘)、120 (2 分鐘)、300 (5 分鐘) 和 600 (10 分鐘)，以及 300 (5 分鐘)。

此設定不會決定 AWS WAF 檢查速率的頻率，但會在每次檢查時檢查速率的回溯程度。會經常 AWS WAF 檢查速率，且時間與評估時段設定無關。

- 速率限制 – 符合條件的請求數目上限，AWS WAF 應只追蹤指定的評估時段。允許的最低限制設定為 10。違反此限制時，會將規則動作設定 AWS WAF 套用至符合您條件的其他請求。

AWS WAF 會將速率限制套用至接近您設定的限制，但不保證完全符合限制。如需詳細資訊，請參閱[以速率為基礎的規則警告](#)。

- 請求彙總 – 在以速率為基礎的規則計數和速率限制的 Web 請求上使用的彙總條件。您設定的速率限制會套用至每個彙總執行個體。如需詳細資訊，請參閱[彙總以速率為基礎的規則](#) 和 [彙總執行個體和計數](#)。
- 動作 – 對規則速率限制的請求採取的動作。您可以使用 以外的任何規則動作 Allow。這在規則層級會照常設定，但有一些限制和行為是針對以速率為基礎的規則。如需規則動作的一般資訊，請參閱[在 中使用規則動作 AWS WAF](#)。如需速率限制的特定資訊，請參閱本節[將速率限制套用至 中的請求 AWS WAF](#)中的。
- 檢查範圍和速率限制 – 您可以新增範圍縮減陳述式，縮小以速率為基礎的陳述式追蹤的請求範圍和速率限制。如果您指定範圍縮減陳述式，則規則只會彙總、計數和速率限制符合範圍縮減陳述式的請求。如果您選擇請求彙總選項全部計數，則需要範圍縮減陳述式。如需縮小範圍陳述式的詳細資訊，請參閱[使用縮小範圍陳述式](#)。
- (選用) 轉送 IP 組態 – 只有在您在請求彙總的標頭中指定 IP 地址時，才會使用此組態，無論是單獨指定或做為自訂金鑰設定的一部分。AWS WAF 會擷取指定標頭中的第一個 IP 地址，並使用該地址做為彙總值。用於此目的的常見標頭是 X-Forwarded-For，但您可以指定任何標頭。如需詳細資訊，請參閱[使用轉送的 IP 地址](#)。

中的以速率為基礎的規則警告 AWS WAF

本節列出使用速率型規則的注意事項。

AWS WAF 速率限制旨在控制高請求率，並以最有效率且最有效的方式保護應用程式的可用性。它不適用於精確的請求速率限制。

- AWS WAF 使用演算法估計目前的請求率，該演算法更重視最近的請求。因此，AWS WAF 會將速率限制套用到接近您設定的限制，但不保證完全符合限制。
- 每次預估請求速率時，AWS WAF 都會回 AWS WAF 頭查看在設定的評估時段內傳入的請求數量。由於此情況和傳播延遲等其他因素，在 AWS WAF 偵測和速率限制請求之前，請求可能以太高的速率傳入最多幾分鐘。同樣地，請求率可以低於限制一段時間，之後 AWS WAF 才會偵測到降低並停止速率限制動作。通常，此延遲低於 30 秒。
- 如果您變更使用中規則中的任何速率限制設定，變更會重設規則的速率限制計數。這最多可暫停規則的速率限制活動一分鐘。速率限制設定是評估時段、速率限制、請求彙總設定、轉送 IP 組態和檢查範圍。

在中彙總以速率為基礎的規則 AWS WAF

本節說明彙總請求的選項。

根據預設，速率型規則會根據請求 IP 地址彙總和速率限制請求。您可以設定規則以使用各種其他彙總金鑰和金鑰組合。例如，您可以根據轉送的 IP 地址、HTTP 方法或查詢引數進行彙總。您也可以指定彙總金鑰組合，例如 IP 地址和 HTTP 方法，或兩個不同 Cookie 的值。

Note

您在彙總金鑰中指定的所有請求元件都必須存在於 Web 請求中，才能由規則評估請求或限制速率。

您可以使用下列彙總選項來設定速率型規則。

- 來源 IP 地址 – 僅使用來自 Web 請求來源的 IP 地址彙總。

來源 IP 地址可能不包含來源用戶端的地址。如果 Web 請求通過一或多個代理或負載平衡器，這將包含最後一個代理的地址。

- 標頭中的 IP 地址 – 僅使用 HTTP 標頭中的用戶端地址彙總。這也稱為轉送 IP 地址。

使用此組態，您也可以指定後援行為，以套用至標頭中 IP 地址格式不正確的 Web 請求。備用行為會將請求的相符結果設定為相符或不相符。對於不匹配，以速率為基礎的規則不計算請求或限制請求的速率。為了進行比對，以速率為基礎的規則會將請求與指定標頭中 IP 地址格式不正確的其他請求分組。

使用此選項時請小心，因為代理可能會以不一致的方式處理標頭，也可以修改標頭來繞過檢查。如需其他資訊和最佳實務，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。

- **ASN** – 使用與來源 IP 地址相關聯的自治系統編號 (ASN) 彙總做為彙總金鑰。這可能不是原始用戶端的地址。如果 Web 請求經過一或多個代理或負載平衡器，這會包含最後一個代理的地址。

如果 AWS WAF 無法從 IP 地址衍生 ASN，它會將 ASN 計為 ASN 0。如果您不想將速率限制套用至未映射 ASNs，您可以建立排除 ASN 0 請求的縮小範圍規則。

- **標頭中的 ASN** – 使用與 HTTP 標頭中的用戶端 IP 地址相關聯的 ASN 彙總。這也稱為轉送 IP 地址。使用此組態，您也可以指定後援行為，以套用至 IP 地址無效或格式不正確的 Web 請求。備用行為會將請求的相符結果設定為相符或不相符。如果您在轉送的 IP 組態中將備用行為設定為相符，AWS WAF 會將無效的 IP 地址視為相符值。這可讓 AWS WAF 繼續評估以速率為基礎的規則複合索引鍵的任何剩餘部分。對於不匹配，以速率為基礎的規則不計算請求或限制請求的速率。

使用此選項時請小心，因為代理可能會以不一致的方式處理標頭，並且可以修改標頭來繞過檢查。如需其他資訊和最佳實務，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。

- **全部計數** – 計數和速率會限制符合規則縮小範圍陳述式的所有請求。此選項需要縮小範圍陳述式。這通常用於限制一組特定請求，例如具有特定標籤的所有請求或來自特定地理區域的所有請求。
- **自訂金鑰** – 使用一或多個自訂彙總金鑰進行彙總。若要將任一 IP 地址選項與其他彙總金鑰合併，請在此處的自訂金鑰下定義它們。

自訂彙總金鑰是 中所述 Web 請求元件選項的子集 [在中請求元件 AWS WAF](#)。

金鑰選項如下。除非另有說明，否則您可以使用 選項多次，例如兩個標頭或三個標籤命名空間。

- **標籤命名空間** – 使用標籤命名空間做為彙總索引鍵。每個具有指定標籤命名空間的不同完整標籤名稱都有助於彙總執行個體。如果您只使用一個標籤命名空間做為自訂金鑰，則每個標籤名稱都會完整定義彙總執行個體。

速率型規則只會使用由保護套件或 Web ACL 中事先評估的規則新增至請求的標籤。

如需標籤命名空間和名稱的資訊，請參閱 [中的標籤語法和命名需求 AWS WAF](#)。

- **標頭** – 使用具名標頭做為彙總金鑰。標頭中的每個不同值都有助於彙總執行個體。

標頭會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- Cookie – 使用具名 Cookie 做為彙總金鑰。Cookie 中的每個不同值都有助於彙總執行個體。

Cookie 會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- 查詢引數 – 在請求中使用單一查詢引數做為彙總索引鍵。具名查詢引數的每個不同值都有助於彙總執行個體。

查詢引數會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- 查詢字串 – 使用請求中的整個查詢字串做為彙總索引鍵。每個不同的查詢字串都有助於彙總執行個體。您可以使用此金鑰類型一次。

查詢字串會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- URI 路徑 – 使用請求中的 URI 路徑做為彙總索引鍵。每個不同的 URI 路徑都有助於彙總執行個體。您可以使用此金鑰類型一次。

URI 路徑會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- URI 路徑 – 使用請求中的 URI 路徑做為彙總索引鍵。每個不同的 URI 路徑都有助於彙總執行個體。您可以使用此金鑰類型一次。

URI 路徑會進行選用的文字轉換。請參閱 [在中使用文字轉換 AWS WAF](#)。

- JA3 指紋 – 使用請求中的 JA3 指紋做為彙總金鑰。每個不同的 JA3 指紋都有助於彙總執行個體。您可以使用此金鑰類型一次。
- JA4 指紋 – 使用請求中的 JA4 指紋做為彙總金鑰。每個不同的 JA4 指紋都有助於彙總執行個體。您可以使用此金鑰類型一次。
- HTTP 方法 – 使用請求的 HTTP 方法做為彙總金鑰。每個不同的 HTTP 方法都有助於彙總執行個體。您可以使用此金鑰類型一次。
- IP 地址 – 使用來自 Web 請求原始伺服器的 IP 地址結合其他金鑰進行彙總。

這可能不會包含原始用戶端的地址。如果 Web 請求通過一或多個代理或負載平衡器，這將包含最後一個代理的地址。

- 標頭中的 IP 地址 – 使用 HTTP 標頭中的用戶端地址搭配其他金鑰進行彙總。這也稱為轉送 IP 地址。

使用此選項時請小心，因為代理可能會以不一致的方式處理標頭，並且可以修改標頭來繞過檢查。如需其他資訊和最佳實務，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。

以速率為基礎的規則彙總執行個體和計數

本節說明以速率為基礎的規則如何評估 Web 請求。

當以速率為基礎的規則使用您的彙總條件評估 Web 請求時，規則為指定的彙總金鑰尋找的每個唯一值集會定義唯一的彙總執行個體。

- 多個索引鍵 – 如果您已定義多個自訂索引鍵，則每個索引鍵的值都會有助於彙總執行個體定義。每個唯一的值組合都會定義彙總執行個體。
- 單一金鑰 – 如果您已在自訂金鑰中選擇單一金鑰，或是透過選取其中一個單一 IP 地址選項，則金鑰的每個唯一值都會定義彙總執行個體。
- 全部計數 - 無索引鍵 – 如果您已選取彙總選項全部計數，則規則評估的所有請求都屬於規則的單一彙總執行個體。此選擇需要縮小範圍的陳述式。

以速率為基礎的規則會針對其識別的每個彙總執行個體分別計算 Web 請求。

例如，假設以速率為基礎的規則評估具有下列 IP 地址和 HTTP 方法值的 Web 請求：

- IP 地址 10.1.1.1、HTTP 方法 POST
- IP 地址 10.1.1.1，HTTP 方法 GET
- IP 地址 127.0.0.0，HTTP 方法 POST
- IP 地址 10.1.1.1，HTTP 方法 GET

規則會根據您的彙總條件建立不同的彙總執行個體。

- 如果彙總條件只是 IP 地址，則每個 IP 地址都是彙總執行個體，並分別 AWS WAF 計算每個 IP 地址的請求。我們範例的彙總執行個體和請求計數如下：
 - IP 地址 10.1.1.1：計數 3
 - IP 地址 127.0.0.0：計數 1
- 如果彙總條件是 HTTP 方法，則每個個別 HTTP 方法都是彙總執行個體。我們範例的彙總執行個體和請求計數如下：
 - HTTP 方法 POST：計數 2
 - HTTP 方法 GET：計數 2
- 如果彙總條件是 IP 地址和 HTTP 方法，則每個 IP 地址和每個 HTTP 方法都有助於合併彙總執行個體。我們範例的彙總執行個體和請求計數如下：

- IP 地址 10.1.1.1，HTTP 方法 POST：計數 1
- IP 地址 10.1.1.1，HTTP 方法 GET：計數 2
- IP 地址 127.0.0.0，HTTP 方法 POST：計數 1

將速率限制套用至 中的請求 AWS WAF

本節說明速率限制行為如何適用於以速率為基礎的規則。

AWS WAF 用於對以速率為基礎的規則限制請求進行評分的条件與 AWS WAF 用於彙總規則請求的条件相同。如果您為規則定義縮小範圍陳述式，則 AWS WAF 只有符合縮小範圍陳述式的彙總、計數和速率限制請求。

導致以速率為基礎的規則將其規則動作設定套用至特定 Web 請求的比對條件如下：

- 如果已定義，則 Web 請求符合規則的範圍縮小陳述式。
- Web 請求屬於請求計數目前超過規則限制的彙總執行個體。

如何 AWS WAF 套用規則動作

當以速率為基礎的規則將速率限制套用至請求時，它會套用規則動作，如果您已在動作規格中定義任何自訂處理或標籤，則規則會套用這些動作。此請求處理與比對規則將其動作設定套用至比對 Web 請求的方式相同。速率型規則只會對其主動速率限制的請求套用標籤或執行其他動作。

您可以使用 以外的任何規則動作 Allow。如需規則動作的一般資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

下列清單說明速率限制如何針對每個動作運作。

- Block – AWS WAF 封鎖請求，並套用您定義的任何自訂封鎖行為。
- Count – AWS WAF 計算請求、套用您定義的任何自訂標頭或標籤，並繼續對請求進行保護套件或 Web ACL 評估。

此動作不會限制請求的速率。它只會計算超過限制的請求。

- CAPTCHA 或 Challenge – AWS WAF 根據請求字符的狀態 Count，以 Block 或 的形式處理請求。

此動作不會限制具有有效字符的請求速率。它會限制超出限制且也缺少有效字符的請求速率。

- 如果請求沒有有效、未過期的字符，動作會封鎖請求，並將 CAPTCHA 拼圖或瀏覽器挑戰傳回給用戶端。

如果最終使用者或用戶端瀏覽器成功回應，用戶端會收到有效的字符，並自動重新傳送原始請求。如果彙總執行個體的速率限制仍然有效，則具有有效、未過期字符的新請求將套用動作，如下一個項目符號所述。

- 如果請求具有有效、未過期的字符，CAPTCHA或 Challenge動作會驗證字符，並且不會對請求採取任何動作，類似於 Count動作。以速率為基礎的規則會將請求評估傳回至保護套件或 Web ACL，而不採取任何終止動作，且保護套件或 Web ACL 會繼續評估請求。

如需其他資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

如果您只對 IP 地址或轉送 IP 地址進行評分

當您將規則設定為僅對轉送 IP 地址的 IP 地址進行速率限制時，您可以擷取規則目前限制速率的 IP 地址清單。如果您使用的是縮小範圍陳述式，速率限制的請求只是 IP 清單中符合縮小範圍陳述式的請求。如需擷取 IP 地址清單的資訊，請參閱 [列出速率受到以速率為基礎的規則限制的 IP 地址](#)。

中的以速率為基礎的規則範例 AWS WAF

本節說明各種常見速率型規則使用案例的範例組態。

每個範例都會提供使用案例的描述，然後在自訂設定規則的 JSON 清單中顯示解決方案。

Note

這些範例中顯示的 JSON 清單是在主控台中建立，方法是設定規則，然後使用規則 JSON 編輯器進行編輯。

主題

- [速率限制對登入頁面的請求](#)
- [速率限制來自任何 IP 地址、使用者代理程式對的登入頁面請求](#)
- [速率限制缺少特定標頭的請求](#)
- [速率限制具有特定標籤的請求](#)
- [速率限制具有指定標籤命名空間之標籤的請求](#)
- [速率限制具有特定 ASNs請求](#)

速率限制對登入頁面的請求

若要限制對網站登入頁面的請求數量，而不影響對網站其他部分的流量，您可以建立速率型規則，其範圍縮減陳述式會將請求比對至您的登入頁面，並將請求彙總設為全部計數。

速率型規則會計算單一彙總執行個體中登入頁面的所有請求，並在請求超過限制時套用規則動作。

下列 JSON 清單顯示此規則組態的範例。計數所有彙總選項會在 JSON 中列為設定 CONSTANT。此範例符合以開頭的登入頁面/login。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

```
}
```

速率限制來自任何 IP 地址、使用者代理程式對的登入頁面請求

若要限制 IP 地址登入頁面的請求數量，超出限制的使用者代理程式對，請將請求彙總設定為自訂金鑰，並提供彙總條件。

下列 JSON 清單顯示此規則組態的範例。在此範例中，我們已將每個 IP 地址、使用者代理程式對的 5 分鐘內限制為 100 個請求。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    },
    {
      "IP": {}
    }
  ],
  "ScopeDownStatement": {
```

```
    "ByteMatchStatement": {
      "FieldToMatch": {
        "UriPath": {}
      },
      "PositionalConstraint": "STARTS_WITH",
      "SearchString": "/login",
      "TextTransformations": [
        {
          "Type": "NONE",
          "Priority": 0
        }
      ]
    }
  }
}
```

速率限制缺少特定標頭的請求

若要限制缺少特定標頭的請求數量，您可以使用計數所有彙總選項搭配範圍縮減陳述式。使用邏輯NOT陳述式來設定縮小範圍陳述式，其中包含僅在標頭存在且具有值時傳回 true 的陳述式。

下列 JSON 清單顯示此規則組態的範例。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
```

```

    "Statement": {
      "SizeConstraintStatement": {
        "FieldToMatch": {
          "SingleHeader": {
            "Name": "user-agent"
          }
        },
        "ComparisonOperator": "GT",
        "Size": 0,
        "TextTransformations": [
          {
            "Type": "NONE",
            "Priority": 0
          }
        ]
      }
    }
  }
}

```

速率限制具有特定標籤的請求

若要限制各種類別的請求數量，您可以將速率限制與將標籤新增至請求的任何規則或規則群組結合。若要這樣做，您可以設定保護套件或 Web ACL，如下所示：

- 新增新增標籤的規則或規則群組，並加以設定，使其不會封鎖或允許您要對限制進行評估的請求。如果您使用受管規則群組，您可能需要覆寫的一些規則群組規則動作Count，才能達成此行為。
- 將速率型規則新增至您的保護套件或 Web ACL，其優先順序數字設定高於標籤規則和規則群組。會以數字順序 AWS WAF 評估規則，從最低開始，因此您的速率型規則將在標籤規則之後執行。使用規則縮小範圍陳述式和標籤彙總中的標籤比對組合，在標籤上設定速率限制。

下列範例使用 Amazon IP 評價清單 AWS 受管規則規則群組。規則群組規則AWSManagedIPDDoSList會偵測和標記已知 IPs正主動參與 DDoS 活動的請求。規則的動作在規則群組定義Count中設定為。如需規則群組的詳細資訊，請參閱 [the section called “Amazon IP 評價清單”](#)。

下列保護套件或 Web ACL JSON 清單使用 IP 評價規則群組，後面接著標籤比對速率型規則。速率型規則使用縮小範圍陳述式來篩選規則群組規則已標記的請求。以速率為基礎的規則陳述式會彙總，並依其 IP 地址限制篩選的請求。

```
{
  "Name": "test-web-acl",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "aws:waf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      }
    }
  ]
}
```

```

        }
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "test-rbr"
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}

```

速率限制具有指定標籤命名空間之標籤的請求

Note

Bot Control 受管規則群組中的常見層級規則會為各種類別的機器人新增標籤，但只會封鎖來自未驗證機器人的請求。如需這些規則的詳細資訊，請參閱 [機器人控制規則清單](#)。

如果您使用 Bot Control 受管規則群組，則可以為來自個別已驗證機器人的請求新增速率限制。若要這樣做，您可以新增在 Bot Control 規則群組之後執行的速率型規則，並依其機器人名稱標籤彙總請求。您可以指定標籤命名空間彙總索引鍵，並將命名空間索引鍵設定為 `awswaf:managed:aws:bot-control:bot:name:`。具有指定命名空間的每個唯一標籤都會定義彙總執行個體。例如，標籤 `awswaf:managed:aws:bot-control:bot:name:axios` 和 `awswaf:managed:aws:bot-control:bot:name:curl` 每個標籤都會定義彙總執行個體。

下列保護套件或 Web ACL JSON 清單顯示此組態。此範例中的規則會將任何單一機器人彙總執行個體的請求限制在兩分鐘內 1,000 個。

```
{
  "Name": "test-web-acl",
  "Id": ...,
  "ARN": ...,
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
```



```

        {
            "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
            }
        }
    ],
    },
    "Action": {
        "Block": {}
    },
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
    }
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
},
"Capacity": 82,
"ManagedByFirewallManager": false,
"RetrofittedByFirewallManager": false,
"LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}

```

速率限制具有特定 ASNs 請求

若要根據請求的 IP 地址限制來自特定自治系統編號 (ASNs) 的請求數量，請將請求彙總設定為自訂金鑰並提供彙總條件。

下列 JSON 顯示彙總衍生自 X-Forwarded-For 標頭中轉送 IP 地址 ASNs 的規則範例。如果 AWS WAF 因為 IP 地址格式錯誤而無法衍生 ASN，則備用行為會設為 MATCH。

```

{
    "Name": "test-rbr",
    "Priority": 0,
    "Statement": {
        "RateBasedStatement": {
            "AggregateKeyType": "CUSTOM_KEYS",

```

```
    "CustomKeys": [
      {
        "ASN": {}
      },
      {
        "ForwardedIP": {}
      }
    ],
    "EvaluationWindowSec": 300,
    "ForwardedIPConfig": {
      "FallbackBehavior": "MATCH",
      "HeaderName": "X-Forwarded-For"
    },
    "Limit": 2000
  }
},
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "test-rbr",
  "SampledRequestsEnabled": true
}
}
```

列出速率受到以速率為基礎的規則限制的 IP 地址

本節說明如何使用 CLI、API 或任何軟體 SDKs，存取速率型規則目前限制速率的 IP 地址清單。

如果您的以速率為基礎的規則只會彙總 IP 地址或轉送 IP 地址，您可以擷取規則目前速率限制的 IP 地址清單。會將這些 IP 地址 AWS WAF 存放在規則的受管金鑰清單中。

Note

只有在您僅彙總 IP 地址或標頭中的 IP 地址時，才能使用此選項。如果您使用自訂金鑰請求彙總，則無法擷取速率有限的 IP 地址清單，即使您在自訂金鑰中使用其中一個 IP 地址規格。

速率型規則會將其規則動作套用至規則受管金鑰清單中符合規則縮小範圍陳述式的請求。當規則沒有縮小範圍陳述式時，它會將動作套用至清單中 IP 地址的所有請求。規則動作 Block 預設為，但除了之外，它可以是任何有效的規則動作 Allow。使用單一速率型規則執行個體 AWS WAF 可對限制進行評分的 IP 地址數目上限為 10,000。如果超過 10,000 個地址超過速率限制，會 AWS WAF 限制速率最高的地址。

您可以使用 CLI、API 或任何 SDKs 來存取速率型規則的受管金鑰清單。本主題涵蓋使用 CLI 和 API 進行存取。主控台目前不提供清單的存取權。

對於 AWS WAF API，命令為 [GetRateBasedStatementManagedKeys](#)。

對於 AWS WAF CLI，命令為 [get-rate-based-statement-managed-keys](#)。

以下顯示擷取 Amazon CloudFront 分佈上保護套件或 Web ACL 中使用的以速率為基礎的規則之速率限制 IP 地址清單的語法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
--web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

以下顯示區域應用程式、Amazon API Gateway REST API、Application Load Balancer、a AWS AppSync GraphQL API、Amazon Cognito 使用者集區 AWS Amplify、AWS App Runner 服務或 AWS Verified Access 執行個體的語法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF 會監控 Web 請求，並針對保護套件或 Web ACL、選用規則群組和速率型規則的每個唯一組合獨立管理金鑰。例如，如果您在規則群組內定義速率型規則，然後在保護套件或 Web ACL 中使用規則群組，AWS WAF 會監控 Web 請求並管理該保護套件或 Web ACL、規則群組參考陳述式和速率型規則執行個體的金鑰。如果您在第二個保護套件或 Web ACL 中使用相同的規則群組，AWS WAF 會監控 Web 請求並管理此第二個用途的金鑰，完全獨立於您的第一個。

對於您在規則群組中定義的以速率為基礎的規則，除了保護套件或 Web ACL 名稱，以及規則群組內以速率為基礎的規則名稱之外，還需要在請求中提供規則群組參考陳述式的名稱。以下顯示區域應用程式的語法，其中以速率為基礎的規則是在規則群組內定義，而規則群組用於保護套件或 Web ACL。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --
rule-name=RuleName
```

在 中使用規則群組規則陳述式 AWS WAF

Note

規則群組規則陳述式不可巢狀化。

本節說明您可以在保護套件或 Web ACL 中使用的規則群組規則陳述式。規則群組保護套件或 Web ACL 容量單位 (WCUs) 是在建立時由規則群組擁有者設定。如需 WCU 的相關資訊，請參閱 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

規則群組陳述式	描述	WCU
使用受管規則群組陳述式	執行指定的受管規則群組中定義的規則。 您可以新增縮小範圍陳述式，縮小規則群組評估的請求範圍。 您無法在任何其他陳述式類型內巢狀化受管規則群組陳述式。	由規則群組定義，加上範圍縮小陳述式的任何其他 WCUs。
使用規則群組陳述式	執行在您管理的規則群組中定義的規則。 您無法將縮小範圍陳述式新增至您自己的規則群組的規則群組參考陳述式。 您無法在任何其他陳述式類型內巢狀化規則群組陳述式	您可以在建立規則群組時定義規則群組的 WCU 限制。

在 中使用受管規則群組陳述式 AWS WAF

本節說明受管規則群組規則陳述式的運作方式。

受管規則群組規則陳述式會將保護套件或 Web ACL 規則清單中的參考新增至受管規則群組。您在主控台的規則陳述式下看不到此選項，但當您使用 Web ACL 的 JSON 格式時，您已新增的任何受管規則群組會在保護套件或 Web ACL 規則下顯示為此類型。

受管規則群組是 AWS 受管規則規則群組，其中大部分是免費提供給 AWS WAF 客戶，或是 AWS Marketplace 受管規則群組。當您將付費 AWS 的受管規則規則群組新增至保護套件或 Web ACL 時，

您會自動訂閱這些規則群組。您可以透過 訂閱 AWS Marketplace 受管規則群組 AWS Marketplace。如需詳細資訊，請參閱[在中使用受管規則群組 AWS WAF](#)。

當您將規則群組新增至保護套件或 Web ACL 時，您可以將群組中規則的動作覆寫為 Count 或另一個規則動作。如需詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。

您可以縮小使用規則群組 AWS WAF 評估的請求範圍。若要這樣做，請在規則群組陳述式中新增縮小範圍陳述式。如需縮小範圍陳述式的資訊，請參閱[在中使用縮小範圍陳述式 AWS WAF](#)。這可協助您管理規則群組如何影響流量，並協助您在使用規則群組時控制與流量相關聯的成本。如需搭配 AWS WAF Bot Control 受管規則群組使用縮小範圍陳述式的資訊和範例，請參閱[AWS WAF 機器人控制](#)。

規則陳述式特性

不可巢狀化 – 您無法將此陳述式類型巢狀在其他陳述式中，也無法將其包含在規則群組中。您可以直接將其包含在保護套件或 Web ACL 中。

(選用) 縮小範圍陳述式 – 此規則類型需要選用縮小範圍陳述式，以縮小規則群組評估的請求範圍。如需詳細資訊，請參閱[在中使用縮小範圍陳述式 AWS WAF](#)。

WCUs – 在建立時為規則群組設定。

尋找此規則陳述式的位置

- 主控台 – 在建立保護套件或 Web ACL 的過程中，在新增規則和規則群組頁面上，選擇新增受管規則群組，然後尋找並選取您要使用的規則群組。
- API – [ManagedRuleGroupStatement](#)

在中使用規則群組陳述式 AWS WAF

本節說明規則群組規則陳述式的運作方式。

規則群組規則陳述式會將保護套件或 Web ACL 規則清單的參考新增至您管理的規則群組。您在 主控台的規則陳述式下看不到此選項，但當您使用保護套件或 Web ACL 的 JSON 格式時，您已新增的任何規則群組都會顯示在此類型的保護套件或 Web ACL 規則下。如需有關使用您自己的規則群組的資訊，請參閱[管理您自己的規則群組](#)。

當您將規則群組新增至保護套件或 Web ACL 時，您可以將群組中規則的動作覆寫為 Count 或另一個規則動作。如需詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。

規則陳述式特性

不可巢狀化 – 您無法將此陳述式類型巢狀在其他陳述式中，也無法將其包含在規則群組中。您可以直接將其包含在保護套件或 Web ACL 中。

WCUs – 在建立時為規則群組設定。

尋找此規則陳述式的位置

- 主控台 – 在建立保護套件或 Web ACL 的過程中，在新增規則和規則群組頁面上，選擇新增我自己的規則和規則群組、規則群組，然後新增您要使用的規則群組。
- API – [RuleGroupReferenceStatement](#)

AWS WAF 規則群組

本節說明什麼是規則群組及其運作方式。

規則群組是一組可重複使用的規則，您可以新增至保護套件或 Web ACL。如需保護套件或 Web ACLs 的詳細資訊，請參閱 [在中設定保護 AWS WAF](#)。

規則群組分為下列主要類別：

- 您自己的規則群組，由您建立和維護。
- 受管規則團隊為您建立和維護的 AWS 受管規則群組。
- AWS Marketplace 賣方為您建立和維護的受管規則群組。
- 由 和 Shield Advanced 等其他服務擁有 AWS Firewall Manager 和管理的規則群組。

規則群組與保護套件或 Web ACLs之間的差異

規則群組和保護套件或 Web ACLs 都包含規則，這些規則在這兩個位置以相同的方式定義。規則群組與保護套件或 Web ACLs 有下列不同：

- 規則群組不能包含規則群組參考陳述式。
- 您可以在多個保護套件或 Web ACLs 中重複使用單一規則群組，方法是將規則群組參考陳述式新增至每個保護套件或 Web ACL。您無法重複使用保護套件或 Web ACL。
- 規則群組沒有預設動作。在保護套件或 Web ACL 中，您可以為包含的每個規則或規則群組設定預設動作。規則群組或保護套件或 Web ACL 內的每個個別規則都已定義動作。

- 您不會直接將規則群組與 AWS 資源建立關聯。若要使用規則群組保護資源，您可以在保護套件或 Web ACL 中使用規則群組。
- 系統會為每個保護套件或 Web ACL 定義最大容量 5,000 個保護套件或 Web ACL 容量單位 (WCUs)。每個規則群組都有一個 WCU 設定，必須在建立時設定。您可以使用此設定來計算使用規則群組將新增至保護套件或 Web ACL 的額外容量需求。如需 WCUs 的詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

如需規則的詳細資訊，請參閱 [AWS WAF 規則](#)。

本節提供建立和管理自有規則群組的指引、說明可供您使用的受管規則群組，並提供使用受管規則群組的指引。

主題

- [在 中使用受管規則群組 AWS WAF](#)
- [管理您自己的規則群組](#)
- [AWS Marketplace 規則群組](#)
- [辨識其他服務提供的規則群組](#)

在 中使用受管規則群組 AWS WAF

本節說明什麼是受管規則群組及其運作方式。

受管規則群組是預先定義、ready-to-use 規則的集合，AWS 和 AWS Marketplace 賣方會為您撰寫和維護這些規則。基本 AWS WAF 定價適用於您對任何受管規則群組的使用。如需 AWS WAF 定價資訊，請參閱 [AWS WAF 定價](#)。

- 除了基本費用之外，適用於 AWS WAF Bot Control、AWS WAF Fraud Control 帳戶接管預防 (ATP) 和 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 的 AWS 受管規則規則群組需額外付費。AWS WAF 如需定價詳細資訊，請參閱 [AWS WAF 定價](#)。
- 所有其他 AWS 受管規則規則群組可供 AWS WAF 客戶免費使用。
- AWS Marketplace 規則群組可透過 訂閱 AWS Marketplace。每個規則群組都由 AWS Marketplace 賣方擁有和管理。如需使用 AWS Marketplace 規則群組的定價資訊，請聯絡 AWS Marketplace 賣方。

有些受管規則群組主要用於協助保護特定類型的 Web 應用程式，像是 WordPress、Joomla 或 PHP。其他則針對已知威脅或常見的 Web 應用程式漏洞提供廣泛的保護，包括 [OWASP 前 10 名](#) 所列的部分

漏洞。如果您受限於法規合規，例如 PCI 或 HIPAA，您可以使用受管規則群組以達到 Web 應用程式防火牆的需求。

自動更新

為了保持在最新狀態以了解不斷變化的威脅趨勢，不僅費時而且耗錢。受管規則群組可以節省您實作和使用的時間 AWS WAF。許多 AWS 和 AWS Marketplace 賣方會自動更新受管規則群組，並在出現新的漏洞和威脅時提供新版本的規則群組。

在某些情況下，AWS 會在公開揭露之前收到新漏洞的通知，因為其參與了許多私有揭露社群。在這些情況下，AWS 可以更新 AWS 受管規則群組，並在新的威脅廣為人知之前為您部署這些規則群組。

受管規則群組中規則的有限存取

每個受管規則群組都會提供攻擊類型和漏洞的完整說明，這些攻擊和漏洞旨在防範。為了保護規則群組提供者的智慧財產權，您無法檢視規則群組中個別規則的所有詳細資訊。此限制也有助於防止惡意使用者利用規避發佈的規則設計攻擊威脅。

主題

- [在 中 使用版本控制的受管規則群組 AWS WAF](#)
- [使用受管規則群組](#)
- [AWS 的受管規則 AWS WAF](#)

在 中 使用版本控制的受管規則群組 AWS WAF

本節說明如何處理受管規則群組的版本控制。

許多受管規則群組提供者會使用版本控制來更新規則群組的選項和功能。通常，受管規則群組的特定版本是靜態的。有時候，供應商可能需要更新部分或全部受管規則群組的靜態版本，例如，以回應新興的安全威脅。

當您在保護套件或 Web ACL 中使用版本控制的受管規則群組時，您可以選取預設版本，並讓提供者管理您使用的靜態版本，也可以選取特定的靜態版本。

找不到您想要的版本？

如果您在規則群組的版本清單中沒有看到版本，則版本可能已排程為過期或已過期。版本排定過期後，AWS WAF 就無法再讓您為規則群組選擇該版本。

AWS 受管規則群組的 SNS 通知

AWS 受管規則規則群組都提供版本控制和 SNS 更新通知，但 IP 評價規則群組除外。提供通知的 AWS 受管規則規則群組都使用相同的 SNS 主題 Amazon Resource Name (ARN)。若要註冊 SNS 通知，請參閱 [收到新版本和更新的通知](#)。

主題

- [受管規則群組的版本生命週期](#)
- [受管規則群組的版本過期](#)
- [處理受管規則群組版本的最佳實務](#)

受管規則群組的版本生命週期

供應商會處理受管規則群組靜態版本的下列生命週期階段：

- 發行和更新 – 受管規則群組提供者會透過 Amazon Simple Notification Service (Amazon SNS) 主題的通知，宣布其受管規則群組即將推出和新的靜態版本。供應商也可能使用 主題來傳達有關其規則群組的其他重要資訊，例如緊急必要更新。

您可以訂閱規則群組的主題，並設定接收通知的方式。如需更多資訊，請參閱[收到新版本和更新的通知](#)。

- 過期排程 – 受管規則群組提供者會為過期排程規則群組的較舊版本。排程過期的版本無法新增至您的保護套件或 Web ACL 規則。排程版本過期後，會使用 Amazon CloudWatch 中的倒數指標 AWS WAF 追蹤過期。
- 版本過期 – 如果您的保護套件或 Web ACL 設定為使用受管規則群組的過期版本，則在保護套件或 Web ACL 評估期間，AWS WAF 會使用規則群組的預設版本。此外，會 AWS WAF 封鎖未移除規則群組或將其版本變更為未過期的保護套件或 Web ACL 的任何更新。

如果您使用 AWS Marketplace 受管規則群組，請向提供者詢問有關版本生命週期的任何其他資訊。

受管規則群組的版本過期

本節說明版本過期如何適用於版本控制的受管規則群組。

如果您使用特定版本的規則群組，請確定您未繼續使用超過過期日期的版本。您可以透過規則群組的 SNS 通知和 Amazon CloudWatch 指標來監控版本過期。

如果您在保護套件或 Web ACL 中使用的版本已過期，會 AWS WAF 封鎖保護套件或 Web ACL 的任何更新，而不包含將規則群組移至未過期的版本。您可以將規則群組更新為可用的版本，或從保護套件或 Web ACL 中移除。

受管規則群組的過期處理取決於規則群組提供者。對於 AWS 受管規則群組，過期版本會自動變更為規則群組的預設版本。對於 AWS Marketplace 規則群組，詢問提供者如何處理過期。

當提供者建立新版本的規則群組時，它會設定版本的預測生命週期。雖然版本未排定過期，但 Amazon CloudWatch 指標值會設定為預測的生命週期設定，而在 CloudWatch 中，您會看到指標的固定值。在提供者排定指標過期後，指標值會每天減少，直到過期當天達到零為止。如需監控過期的資訊，請參閱[追蹤版本過期](#)。

處理受管規則群組版本的最佳實務

當您使用版本控制的受管規則群組時，請遵循此最佳實務指南來處理版本控制。

當您在保護套件或 Web ACL 中使用受管規則群組時，您可以選擇使用規則群組的特定靜態版本，也可以選擇使用預設版本：

- 預設版本 – AWS WAF 一律將預設版本設定為供應商目前建議的靜態版本。當提供者更新其建議的靜態版本時，AWS WAF 會自動更新保護套件或 Web ACL 中規則群組的預設版本設定。

當您使用受管規則群組的預設版本時，請執行下列最佳實務：

- 訂閱通知 – 訂閱通知以取得規則群組的變更，並留意這些變更。大多數供應商會傳送新靜態版本和預設版本變更的進階通知。這些可讓您先檢查新靜態版本的效果，再 AWS 切換預設版本。如需更多資訊，請參閱[收到新版本和更新的通知](#)。
- 檢閱靜態版本設定的效果，並視需要在預設設定之前進行調整 – 在預設設定為新的靜態版本之前，請檢閱靜態版本對 Web 請求監控和管理的效果。新的靜態版本可能有要檢閱的新規則。尋找誤報或其他未預期的行為，以防您需要修改規則群組的使用方式。您可以設定規則來計算，例如，在您了解要如何處理新行為時，阻止它們封鎖流量。如需詳細資訊，請參閱[測試和調校您的 AWS WAF 保護](#)。
- 靜態版本 – 如果您選擇使用靜態版本，您必須在準備好採用新版本的規則群組時手動更新版本設定。

當您使用受管規則群組的靜態版本時，請執行下列最佳實務：

- 將您的版本保持在最新狀態 – 讓您的受管規則群組盡可能靠近最新版本。發行新版本時，請進行測試、視需要調整設定，並及時實作。如需測試的相關資訊，請參閱[測試和調校您的 AWS WAF 保護](#)。
- 訂閱通知 – 訂閱規則群組變更的通知，讓您知道提供者何時發佈新的靜態版本。大多數供應商會提供版本變更的進階通知。此外，您的提供者可能需要更新您用來關閉安全漏洞或其他緊急原因的靜態版本。如果您訂閱供應商的通知，就會知道發生了什麼情況。如需詳細資訊，請參閱[收到新版本和更新的通知](#)。

- 避免版本過期 – 不允許靜態版本在您使用時過期。處理過期版本的供應商可能會有所不同，可能包括強制升級至可用的版本或其他可能產生意外後果的變更。追蹤 AWS WAF 過期指標並設定警示，讓您有足夠的天數成功升級至支援的版本。如需詳細資訊，請參閱[追蹤版本過期](#)。

使用受管規則群組

本節提供存取和管理受管規則群組的指引。

當您將受管規則群組新增至保護套件或 Web ACL 時，您可以選擇與您自己的規則群組相同的組態選項，以及其他設定。

透過 主控台，您可以在新增和編輯保護套件或 Web ACLs 中的規則的過程中存取受管規則群組資訊。透過 APIs 和命令列界面 (CLI)，您可以直接請求受管規則群組資訊。

當您在保護套件或 Web ACL 中使用受管規則群組時，您可以編輯下列設定：

- 版本 – 只有在規則群組進行版本控制時，才能使用此功能。如需詳細資訊，請參閱[在 中使用版本控制的受管規則群組 AWS WAF](#)。
- 覆寫規則動作 – 您可以將規則群組中規則的動作覆寫為任何動作。將它們設定為 Count 有助於在使用規則群組來管理您的 Web 請求之前測試規則群組。如需詳細資訊，請參閱[規則群組規則動作覆寫](#)。
- 縮小範圍陳述式 – 您可以新增縮小範圍陳述式，以篩選出您不想使用規則群組評估的 Web 請求。如需詳細資訊，請參閱[在 中使用縮小範圍陳述式 AWS WAF](#)。
- 覆寫規則群組動作 – 您可以覆寫規則群組評估所產生的動作，並 Count 只將其設定為 。此選項不常用。它不會改變 如何 AWS WAF 評估規則群組中的規則。如需詳細資訊，請參閱[規則群組傳回動作覆寫至 Count](#)。

編輯保護套件或 Web ACL 中的受管規則群組設定

- 主控台
 - (選項) 當您將受管規則群組新增至保護套件或 Web ACL 時，您可以選擇編輯以檢視和編輯設定。
 - (選項) 將受管規則群組新增至保護套件或 Web ACL 後，從保護套件或 Web ACLs 頁面選擇您剛建立的保護套件或 Web ACL。這會帶您前往保護套件或 Web ACL 編輯頁面。
 - 選擇 Rules (規則)。
 - 選取規則群組，然後選擇編輯以檢視和編輯設定。

- APIs和 CLI – 在主控制台之外，您可以在建立和更新保護套件或 Web ACL 時管理受管規則群組設定。

擷取受管規則群組的清單

您可以擷取可在保護套件或 Web ACLs 中使用的受管規則群組清單。此清單包含下列項目：

- 所有 AWS 受管規則規則群組。
- 您已訂閱的 AWS Marketplace 規則群組。

Note

如需訂閱 AWS Marketplace 規則群組的資訊，請參閱 [AWS Marketplace 規則群組](#)。

當您擷取受管規則群組的清單時，您取得的清單取決於您使用的介面：

- 主控台 – 透過主控台，您可以看到所有受管規則群組，包括您尚未訂閱的 AWS Marketplace 規則群組。對於您尚未訂閱的介面，介面會提供您可以遵循的連結來訂閱。
- APIs和 CLI – 在主控制台之外，您的請求只會傳回可供您使用的規則群組。

擷取受管規則群組的清單

- 主控台 – 在建立 Web ACL 的過程中，在新增規則和規則群組頁面上，選擇新增受管規則群組。在最上層，會列出提供者名稱。展開每個提供者清單，以查看受管規則群組的清單。對於版本控制規則群組，此層級顯示的資訊適用於預設版本。當您將受管規則群組新增至保護套件或 Web ACL 時，主控台會根據命名方案 列出規則群組<Vendor Name>-<Managed Rule Group Name>。
- API –
 - ListAvailableManagedRuleGroups
- CLI –
 - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT | REGIONAL>`

擷取受管規則群組中的規則

您可以擷取受管規則群組中的規則清單。API 和 CLI 呼叫會傳回您可以在 JSON 模型中或透過其參考的規則規格 AWS CloudFormation。

擷取受管規則群組中的規則清單

- 主控台
 - (選項) 當您將受管規則群組新增至保護套件或 Web ACL 時，您可以選擇編輯以檢視規則。
 - (選項) 將受管規則群組新增至保護套件或 Web ACL 後，從保護套件或 Web ACLs 頁面選擇您剛建立的保護套件或 Web ACL。這會帶您前往保護套件或 Web ACL 編輯頁面。
 - 選擇 Rules (規則)。
 - 選取您要查看規則清單的規則群組，然後選擇編輯。AWS WAF 顯示規則群組中的規則清單。
- API – DescribeManagedRuleGroup
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

擷取受管規則群組的可用版本

受管規則群組的可用版本是尚未排定過期的版本。清單指出哪個版本是規則群組的目前預設版本。

擷取受管規則群組可用版本的清單

- 主控台
 - (選項) 當您將受管規則群組新增至保護套件或 Web ACL 時，請選擇編輯以查看規則群組的資訊。展開版本下拉式清單以查看可用版本的清單。
 - (選項) 將受管規則群組新增至保護套件或 Web ACL 之後，請在保護套件或 Web ACL 上選擇編輯，然後選取並編輯規則群組規則。展開版本下拉式清單以查看可用版本的清單。
- API –
 - ListAvailableManagedRuleGroupVersions
- CLI –
 - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

透過主控台將受管規則群組新增至保護套件或 Web ACL

本節說明如何透過主控台將受管規則群組新增至保護套件或 Web ACL。本指南適用於所有 AWS 受管規則群組和您訂閱的 AWS Marketplace 規則群組。

⚠ 生產流量風險

在保護套件或 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

📘 Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱[中的 Web ACL 容量單位 \(WCUs\) AWS WAF](#) 和 [AWS WAF 定價](#)。

透過主控台將受管規則群組新增至保護套件或 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中選擇保護套件或 Web ACLs。
3. 在保護套件或 Web ACLs 頁面的保護套件或 Web ACLs 清單中，選取您要新增規則群組的目標。這會帶您前往單一保護套件或 Web ACL 的頁面。
4. 在保護套件或 Web ACL 的頁面中，選擇規則索引標籤。
5. 在規則窗格中，選擇新增規則，然後選擇新增受管規則群組。
6. 在新增受管規則群組頁面中，展開規則群組廠商的選擇，以查看可用的規則群組清單。
7. 針對您要新增的每個規則群組，選擇新增至保護套件或 Web ACL。如果您想要變更規則群組的保護套件或 Web ACL 組態，請選擇編輯、進行變更，然後選擇儲存規則。如需選項的相關資訊，請參閱的版本控制指南，在[中使用版本控制的受管規則群組 AWS WAF](#)以及的保護套件或 Web ACL 中使用受管規則群組的指南在[中使用受管規則群組陳述式 AWS WAF](#)。
8. 在新增受管規則群組頁面底部，選擇新增規則。
9. 在設定規則優先順序頁面中，視需要調整規則執行的順序，然後選擇儲存。如需詳細資訊，請參閱[設定規則優先順序](#)。

在您的保護套件或 Web ACL 頁面中，您已新增的受管規則群組會列在規則索引標籤下。

在將 AWS WAF 保護用於生產流量之前，測試和調校保護的任何變更。如需相關資訊，請參閱[測試和調校您的 AWS WAF 保護](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新的地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

收到受管規則群組新版本和更新的通知

本節說明如何接收新版本和更新的 Amazon SNS 通知。

受管規則群組提供者會使用 SNS 通知來宣告規則群組變更，例如即將推出的新版本和緊急安全性更新。

如何訂閱 SNS 通知

若要訂閱規則群組的通知，請在美國東部（維吉尼亞北部）us-east-1 區域中為規則群組的 Amazon SNS 主題 ARN 建立 Amazon SNS 訂閱。

如需如何訂閱的資訊，請參閱 [Amazon Simple Notification Service 開發人員指南](#)。

Note

僅在 us-east-1 區域中建立 SNS 主題的訂閱。

版本控制的 AWS 受管規則規則群組都使用相同的 SNS 主題 Amazon Resource Name (ARN)。如需 AWS 受管規則規則群組通知的詳細資訊，請參閱 [部署通知](#)。

在何處尋找受管規則群組的 Amazon SNS 主題 ARN

AWS 受管規則規則群組使用單一 SNS 主題 ARN，因此您可以從其中一個規則群組擷取主題 ARN，並訂閱該 ARN，以取得所有提供 SNS 通知的 AWS 受管規則規則群組的通知。

- 主控台
 - (選項) 當您將受管規則群組新增至保護套件或 Web ACL 時，請選擇編輯以查看規則群組的資訊，其中包含規則群組的 Amazon SNS 主題 ARN。
 - (選項) 將受管規則群組新增至保護套件或 Web ACL 之後，請在保護套件或 Web ACL 上選擇編輯，然後選取並編輯規則群組規則，以查看規則群組的 Amazon SNS 主題 ARN。
- API – DescribeManagedRuleGroup
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

如需 Amazon SNS 通知格式和如何篩選所收到通知的一般資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的[剖析訊息格式](#)和[Amazon SNS 訂閱篩選條件政策 Amazon SNS](#)。

追蹤規則群組的版本過期

本節說明如何透過 Amazon CloudWatch 監控受管規則群組的過期排程。

如果您使用特定版本的規則群組，請確定您未繼續使用超過過期日期的版本。

Tip

註冊受管規則群組的 Amazon SNS 通知，並保持受管規則群組版本的最新狀態。您將受益於來自規則群組 up-to-date 保護，並保持在過期前。如需相關資訊，請參閱[收到新版本和更新的通知](#)。

透過 Amazon CloudWatch 監控受管規則群組的過期排程

1. 在 CloudWatch 中，尋找受管規則群組 AWS WAF 的過期指標。這些指標具有下列指標名稱和維度：
 - 指標名稱：DaysToExpiry
 - 指標維度：Region、Vendor、ManagedRuleGroup 和 Version

如果您的保護套件或 Web ACL 中有評估流量的受管規則群組，您會取得其指標。指標不適用於您未使用的規則群組。

2. 針對您感興趣的指標設定警示，以便及時通知您切換到規則群組的較新版本。

如需有關使用 Amazon CloudWatch 指標和設定警示的資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

JSON 和 YAML 中的受管規則群組組態範例

本節提供範例受管規則群組組態。

API 和 CLI 呼叫會傳回受管規則群組中所有規則的清單，您可以在 JSON 模型中或透過這些規則群組參考 AWS CloudFormation。

JSON

您可以使用 JSON 在規則陳述式中參考和修改受管規則群組。下列清單會以 JSON 格式顯示 AWS Managed Rules 規則群組 AWSManagedRulesCommonRuleSet。RuleActionOverrides 規格會列出已覆寫其動作至 的規則Count。

```
{
  "Name": "AWS-AWSManagedRulesCommonRuleSet",
  "Priority": 0,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesCommonRuleSet",
      "RuleActionOverrides": [

        {

          "ActionToUse": {

            "Count": {}

          },

          "Name": "NoUserAgent_HEADER"

        }

      ],
      "ExcludedRules": []
    }
  },
  "OverrideAction": {
    "None": {}
  }
}
```

```
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
  }
}
```

YAML

您可以使用 YAML 範本，在規則陳述 AWS CloudFormation 式中參考和修改受管規則群組。下列清單顯示 AWS CloudFormation 範本中的 AWS Managed Rules 規則群組 `AWSManagedRulesCommonRuleSet`。RuleActionOverrides 規格會列出已覆寫其動作至的規則 Count。

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
      - ActionToUse:
          Count: {}
          Name: NoUserAgent_HEADER
        ExcludedRules: []
  OverrideAction:
    None: {}
  VisibilityConfig:
    SampledRequestsEnabled: true
    CloudWatchMetricsEnabled: true
    MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS 的受管規則 AWS WAF

本節說明什麼 AWS WAF 是的 AWS 受管規則。

AWS 的受管規則 AWS WAF 是一項受管服務，可針對應用程式漏洞或其他不需要的流量提供保護。您可以選擇從每個 Web ACL 的 AWS 受管規則中選取一或多個規則群組，直到最大保護套件或 Web ACL 容量單位 (WCU) 限制為止。

緩解誤報和測試規則群組變更

在生產環境中使用任何受管規則群組之前，請先根據 [中的指引](#)，在非生產環境中進行測試 [測試和調校您的 AWS WAF 保護](#)。當您將規則群組新增至保護套件或 Web ACL、測試規則群組的新版本，以及每當規則群組未視需要處理您的 Web 流量時，請遵循測試和調校指引。

共同的安全責任

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，這取決於您選擇的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在 [中的資源](#) AWS 受到適當保護。

Important

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，這取決於您選擇的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在 [中的資源](#) AWS 受到適當保護。

AWS 受管規則規則群組清單

本節提供可用的 AWS 受管規則規則群組清單。

本節說明 AWS 受管規則規則群組的最新版本。當您將受管規則群組新增至保護套件或 Web ACL 時，您會在主控台上看到這些內容。透過 API，您可以透過呼叫 `DescribeManagedRuleGroup` 來擷取此清單以及您訂閱的 AWS Marketplace 規則群組 `ListAvailableManagedRuleGroups`。

Note

如需擷取 AWS 受管規則規則群組版本的資訊，請參閱 [擷取受管規則群組的可用版本](#)。

所有 AWS 受管規則規則群組都支援標記，本節中的規則清單包含標籤規格。您可以透過 API 呼叫 `DescribeManagedRuleGroup` 來擷取受管規則群組的標籤。這些標籤會列在回應的 `AvailableLabels` 屬性中。如需標籤的詳細資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#)。

在將 AWS WAF 保護用於生產流量之前，測試和調校保護的任何變更。如需相關資訊，請參閱 [測試和調校您的 AWS WAF 保護](#)。

AWS 受管規則規則群組

- [基準規則群組](#)

- [核心規則集 \(CRS\) 受管規則群組](#)
- [管理員保護受管規則群組](#)
- [已知錯誤輸入受管規則群組](#)
- [使用案例特定的規則群組](#)
 - [SQL 資料庫受管規則群組](#)
 - [Linux 作業系統受管規則群組](#)
 - [POSIX 作業系統受管規則群組](#)
 - [Windows 作業系統受管規則群組](#)
 - [PHP 應用程式受管規則群組](#)
 - [WordPress 應用程式受管規則群組](#)
- [IP 評價規則群組](#)
 - [Amazon IP 評價清單受管規則群組](#)
 - [匿名 IP 清單受管規則群組](#)
- [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)
 - [使用此規則群組的考量事項](#)
 - [此規則群組新增的標籤](#)
 - [字符標籤](#)
 - [ACFP 標籤](#)
 - [帳戶建立詐騙預防規則清單](#)
- [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)
 - [使用此規則群組的考量事項](#)
 - [此規則群組新增的標籤](#)
 - [字符標籤](#)
 - [ATP 標籤](#)
 - [帳戶接管預防規則清單](#)
- [AWS WAF 機器人控制規則群組](#)
 - [保護層級](#)
 - [使用此規則群組的考量事項](#)
 - [此規則群組新增的標籤](#)
 - [字符標籤](#)

- [機器人控制標籤](#)
- [機器人控制規則清單](#)
- [AWS WAF 分散式阻斷服務 \(DDoS\) 預防規則群組](#)
 - [使用此規則群組的考量事項](#)
 - [此規則群組新增的標籤](#)
 - [字符標籤](#)
 - [反 DDoS 標籤](#)
 - [反 DDoS 規則清單](#)

基準規則群組

基準管理的規則群組可針對各種常見威脅提供一般防護。選擇這些規則群組中的一或多個，以建立資源的基準保護。

核心規則集 (CRS) 受管規則群組

VendorName : AWS、Name : AWSManagedRulesCommonRuleSet、WCU : 700

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

核心規則集 (CRS) 規則群組包含通常適用於 Web 應用程式的規則。這可以防止各種漏洞遭到利用，包括 OWASP 出版品中所述的一些高風險和常見漏洞，例如 [OWASP 前 10 名](#)。考慮將此規則群組用於任何 AWS WAF 使用案例。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
NoUserAgent_HEADER	檢查是否有缺少 HTTP User-Agent 標頭的請求。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:NoUserAgent_Header
UserAgent_BadBots_HEADER	檢查指出請求是錯誤機器人的常見 User-Agent 標頭值。範例模式包括 <code>nessus</code> 和 <code>nmap</code>。如需機器人管理，另請參閱 AWS WAF 機器人控制規則群組。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:BadBots_Header
SizeRestrictions_QUERYSTRING	檢查是否有超過 2,048 個位元組的 URI 查詢字串。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:SizeRestrictions_QueryString
SizeRestrictions_Cookie_HEADER	檢查是否有超過 10,240 個位元組的 Cookie 標頭。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header

規則名稱	描述和標籤
SizeRestrictions_BODY	檢查請求內文是否超過 8 KB (8 , 192 位元組)。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:SizeRestrictions_Body
SizeRestrictions_URI_PATH	檢查是否有超過 1 , 024 個位元組的 URI 路徑。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:SizeRestrictions_URIPath

規則名稱	描述和標籤
EC2MetaDataSSRF_BODY	檢查是否有嘗試從請求內文滲透 Amazon EC2 中繼資料。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body
EC2MetaDataSSRF_COOKIE	檢查 是否嘗試從請求 Cookie 滲透 Amazon EC2 中繼資料。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie

規則名稱	描述和標籤
EC2MetaDataSSRF_URI_PATH	檢查 是否嘗試從請求 URI 路徑滲透 Amazon EC2 中繼資料。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath
EC2MetaDataSSRF_QUERY_ARGUMENTS	檢查是否有嘗試從請求查詢引數滲透 Amazon EC2 中繼資料。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments
GenericLFI_QUERY_ARGUMENTS	檢查查詢引數中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericLFI_QueryArguments
GenericLFI_URI_PATH	檢查 URI 路徑中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericLFI_URIPath

規則名稱	描述和標籤
GenericLFI_BODY	檢查要求主體中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericLFI_Body
RestrictedExtensions_URI_PATH	檢查 URI 路徑是否包含不安全讀取或執行之系統副檔名的請求。範例模式包括 .log 和 .ini 之類的副檔名。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:RestrictedExtensions_URIPath

規則名稱	描述和標籤
RestrictedExtensions_QUERYARGUMENTS	檢查查詢引數是否包含不安全讀取或執行之系統副檔名的請求。範例模式包括 .log 和 .ini 之類的副檔名。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	透過嵌入包含 IPv4 地址的 URLs (遠端檔案包含)。範例包括 http://、https://、ftp://、ftp://和等模式file://，在入侵嘗試中具有 IPv4 主機標頭。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericRFI_QueryArguments

規則名稱	描述和標籤
GenericRFI_BODY	透過嵌入包含 IPv4 地址URLs，檢查請求內文是否嘗試在 Web 應用程式中利用 RFI（遠端檔案包含）。範例包括 http://、https://、ftp://、ftp://和等模式file://，在入侵嘗試中具有 IPv4 主機標頭。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericRFI_Body

規則名稱	描述和標籤
GenericRFI_URI_PATH	透過嵌入包含 IPv4 地址URLs，檢查 URI 路徑是否嘗試在 Web 應用程式中利用 RFI（遠端檔案包含）。範例包括 http://、https://、ftp://、ftp://和等模式file://，在入侵嘗試中具有 IPv4 主機標頭。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:GenericRFI_URI_Path
CrossSiteScripting_COOKIE	使用內建 檢查 Cookie 標頭的值是否有常見的跨網站指令碼 (XSS) 模式 AWS WAF 跨網站指令碼攻擊規則陳述式。範例模式包括 <script>alert("hello")</script> 之類的指令碼。  Note AWS WAF 日誌中的規則比對詳細資訊不會填入此規則群組的 2.0 版。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_Cookie

規則名稱	描述和標籤
CrossSiteScripting_QUERYARGUMENTS	使用內建 檢查查詢引數的值是否有常見的跨網站指令碼 (XSS) 模式 AWS WAF 跨網站指令碼攻擊規則陳述式。範例模式包括 <code><script>alert("hello")</script></code> 之類的指令碼。  Note AWS WAF 日誌中的規則比對詳細資訊不會填入此規則群組的 2.0 版。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments

規則名稱	描述和標籤
CrossSiteScripting_BODY	使用內建 檢查請求內文是否有常見的跨網站指令碼 (XSS) 模式 AWS WAF 跨網站指令碼攻擊規則陳述式。範例模式包括 <code><script>alert("hello")</script></code> 之類的指令碼。  Note AWS WAF 日誌中的規則比對詳細資訊不會填入此規則群組的 2.0 版。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_Body

規則名稱	描述和標籤
CrossSiteScripting_URI_PATH	使用內建 檢查 URI 路徑的值是否有常見的跨網站指令碼 (XSS) 模式 AWS WAF 跨網站指令碼攻擊規則陳述式。範例模式包括 <code><script>alert("hello")</script></code> 之類的指令碼。  Note AWS WAF 日誌中的規則比對詳細資訊不會填入此規則群組的 2.0 版。 規則動作：Block 標籤：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_URI_Path

管理員保護受管規則群組

VendorName : AWS、Name : AWSManagedRulesAdminProtectionRuleSet、WCU : 100

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

管理員保護規則群組包含的規則可讓您封鎖對公開的管理頁面的外部存取。如果您執行第三方軟體，或想要降低惡意行為者取得應用程式系統管理存取權的風險，這可能會很有用。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
AdminProtection_URI_PATH	檢查通常保留用於管理 Web 伺服器或應用程式的 URI 路徑。範例模式包括 <code>sqlmanager</code>。 規則動作：Block 標籤：aws:waf:managed:aws:admin-protection:AdminProtection_URI_Path

已知錯誤輸入受管規則群組

VendorName : AWS , 名稱 : AWSManagedRulesKnownBadInputsRuleSet , WCU : 200

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

已知錯誤輸入規則群組包含的規則可封鎖已知無效且與利用或發現的漏洞相關的請求模式。這有助於降低惡意行為者發現易受攻擊應用程式的風險。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
JavaDeserializationRCE_HEADER	檢查 HTTP 請求標頭的金鑰和值是否有表示 Java 還原序列化遠端命令執行 (RCE) 嘗試的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。範例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。  Warning 此規則只會檢查請求標頭的前 8 KB 或前 200 個標頭，以先達到限制為準，並使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header
JavaDeserializationRCE_BODY	檢查請求內文是否有表示 Java 還原序列化遠端命令執行 (RCE) 嘗試的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。範例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文

規則名稱	描述和標籤
	大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制增加到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body
JavaDeserializationRCE_URI_PATH	檢查請求 URI 是否有表示 Java 還原序列化遠端命令執行 (RCE) 嘗試的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。範例模式包括 <code>(java.lang.Runtime).getRuntime().exec("whoami")</code>。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath

規則名稱	描述和標籤
JavaDeserializationRCE_QUERYSTRING	檢查請求查詢字串是否有表示 Java 還原序列化遠端命令執行 (RCE) 嘗試的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。範例模式包括 <code>(java.lang.Runtime).getRuntime().exec("whoami")</code> 。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString
Host_localhost_HEADER	檢查要求中的主機標頭是否有模式指出 localhost。範例模式包括 localhost 。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Host_Localhost_Header
PROPFIND_METHOD	檢查要求中的 HTTP 方法是否有 PROPFIND，這是類似 HEAD 的方法，但有滲透 XML 物件的額外意圖。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Propfind_Method

規則名稱	描述和標籤
ExploitablePaths_URI_PATH	檢查 URI 路徑是否有存取可利用 Web 應用程式路徑的嘗試。範例模式包括 web-inf 之類的路徑。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:ExploitablePaths_URI_Path
Log4JRCE_HEADER	檢查請求標頭的金鑰和值是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 <code>\${jndi:ldap://example.com/}</code>。  Warning 此規則只會檢查請求標頭的前 8 KB 或前 200 個標頭，以先達到限制為準，並使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_Header

規則名稱	描述和標籤
Log4JRCE_QUERYSTRING	檢查查詢字串是否有 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 <code>\${jndi:ldap://example.com/}</code> 。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_QueryString

規則名稱	描述和標籤
Log4JRCE_BODY	檢查內文是否有 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 <code>\${jndi:ldap://example.com/}</code>。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制增加到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_Body

規則名稱	描述和標籤
Log4JRCE_URI_PATH	檢查 URI 路徑是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 <code>\${jndi:ldap://example.com/}</code>。 規則動作：Block 標籤：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_URI_Path

使用案例特定的規則群組

使用案例特定的規則群組可為許多不同的 AWS WAF 使用案例提供增量保護。選擇套用至應用程式的規則群組。

SQL 資料庫受管規則群組

VendorName : AWS、Name : AWSManagedRulesSQLiRuleSet、WCU : 200

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

SQL 資料庫規則群組包含的規則，可封鎖與 SQL 資料庫利用相關的請求模式，例如 SQL Injection 攻擊。這有助於防止未經授權查詢的遠端注入。如果您的應用程式會與 SQL 資料庫互動，請評估此規則群組以供使用。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
SQLi_QUERYARGUMENTS	使用內建的 AWS WAF SQL Injection 攻擊規則陳述式，並將敏感度等級設為 Low，以檢查所有查詢參數的值是否有符合惡意 SQL 程式碼的模式。 規則動作：Block 標籤：aws:waf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	檢查所有查詢參數的值是否有符合惡意 SQL 程式碼的模式。此規則檢查的模式未涵蓋在規則內 SQLi_QUERYARGUMENTS 。 規則動作：Block 標籤：aws:waf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
SQLi_BODY	使用內建的 AWS WAF SQL Injection 攻擊規則陳述式，並將敏感度等級設為 Low，以檢查請求內文是否有符合惡意 SQL 程式碼的模式。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API

規則名稱	描述和標籤
	Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:sql-data base:SQLi_Body

規則名稱	描述和標籤
SQLiExtendedPatterns_BODY	檢查請求內文是否有符合惡意 SQL 程式碼的模式。此規則檢查的模式未涵蓋在規則內SQLi_BODY。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:sql-data-base:SQLiExtendedPatterns_Body
SQLi_COOKIE	使用內建的 AWS WAF SQL Injection 攻擊規則陳述式，並將敏感度等級設為 Low，以檢查請求 Cookie 標頭是否有符合惡意 SQL 程式碼的模式。 規則動作：Block 標籤：aws:waf:managed:aws:sql-data-base:SQLi_Cookie

Linux 作業系統受管規則群組

VendorName : AWS、Name : AWSManagedRulesLinuxRuleSet、WCU : 200

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

Linux 作業系統規則群組包含的規則會封鎖與利用 Linux 特定漏洞攻擊相關的請求模式，包括 Linux 特定本機檔案包含 (LFI) 攻擊。這有助於防止公開檔案內容的攻擊，或執行攻擊者不應存取的程式碼。如果應用程式的任何部分在 Linux 上執行，則應該評估此規則群組。您應該使用此規則群組結合 [POSIX 作業系統](#) 規則群組。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
LFI_URIPATH	檢查要求路徑是否有入侵 Web 應用程式中的本機檔案包含 (LFI) 弱點的嘗試。範例模式包括 /proc/version 之類的檔案，其可以對攻擊者提供作業系統訊息。 規則動作：Block 標籤：aws:waf:managed:aws:linux-os:LFI_URIPath
LFI_QUERYSTRING	檢查 querystring 的值是否有嘗試利用 Web 應用程式中的本機檔案包含 (LFI) 漏洞。範例模式包

規則名稱	描述和標籤
	括 <code>/proc/version</code> 之類的檔案，其可以對攻擊者提供作業系統訊息。 規則動作：Block 標籤：aws:waf:managed:aws:linux-os:LFI_QueryString
LFI_HEADER	檢查請求標頭是否有嘗試利用 Web 應用程式中的本機檔案包含 (LFI) 漏洞。範例模式包括 <code>/proc/version</code> 之類的檔案，其可以對攻擊者提供作業系統訊息。  Warning 此規則只會檢查請求標頭的前 8 KB 或前 200 個標頭，以先達到限制為準，並使用 Continue 選項處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:linux-os:LFI_Header

POSIX 作業系統受管規則群組

VendorName : AWS、Name : AWSManagedRulesUnixRuleSet、WCU : 100

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

POSIX 作業系統規則群組包含的規則會封鎖與利用 POSIX 和類似 POSIX 作業系統特定漏洞相關的請求模式，包括本機檔案包含 (LFI) 攻擊。這有助於防止公開檔案內容的攻擊，或執行攻擊者不應存取的程式碼。如果應用程式的任何部分在類似 POSIX 或類似 POSIX 的作業系統，包括 Linux、AIX、HP-UX、macOS、Solaris、FreeBSD 和 OpenBSD 上執行，則應該評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
UNIXShellCommandsVariables_QUERYSTRING	檢查查詢字串的值是否有嘗試利用在 Unix 系統上執行的 Web 應用程式中的命令注入、LFI 和路徑周遊漏洞。範例包括 <code>echo \$HOME</code> 和 <code>echo \$PATH</code> 之類的模式。 規則動作：Block 標籤：aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString
UNIXShellCommandsVariables_BODY	檢查要求主體是否有入侵在 Unix 系統上執行之 Web 應用程式中的命令注入、LFI 和路徑遍訪弱點的嘗試。範例包括 <code>echo \$HOME</code> 和 <code>echo \$PATH</code> 之類的模式。

規則名稱	描述和標籤
	 Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_Body

規則名稱	描述和標籤
UNIXShellCommandsVariables_HEADER	檢查所有請求標頭是否嘗試利用在 Unix 系統上執行的 Web 應用程式中的命令注入、LFI 和路徑周遊漏洞。範例包括 <code>echo \$HOME</code> 和 <code>echo \$PATH</code> 之類的模式。  Warning 此規則只會檢查請求標頭的前 8 KB 或前 200 個標頭，以先達到限制為準，並使用 Continue 選項處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_Header

Windows 作業系統受管規則群組

VendorName : AWS、Name : AWSManagedRulesWindowsRuleSet、WCU : 200

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

Windows 作業系統規則群組包含的規則會封鎖與利用 Windows 特定漏洞相關的請求模式，例如 PowerShell 命令的遠端執行。這有助於防止利用允許攻擊者執行未經授權的命令或執行惡意程式碼的漏洞。如果應用程式的任何部分在 Windows 作業系統上執行，請評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
WindowsShellCommands_COOKIE	在 Web 應用程式中檢查 WindowsShell 命令注入嘗試的請求 Cookie 標頭。比對模式代表 WindowsShell 命令。範例模式包括 <code> nslookup</code> 和 <code>;cmd</code>。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:WindowsShellCommands_Cookie
WindowsShellCommands_QUERY_ARGUMENTS	檢查 Web 應用程式中 WindowsShell 命令注入嘗試的所有查詢參數的值。比對模式代表 WindowsShell 命令。範例模式包括 <code> nslookup</code> 和 <code>;cmd</code>。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:WindowsShellCommands_QueryArguments
WindowsShellCommands_BODY	在 Web 應用程式中檢查 WindowsShell 命令注入嘗試的請求內文。比對模式代表 WindowsShell 命令。範例模式包括 <code> nslookup</code> 和 <code>;cmd</code>。

規則名稱	描述和標籤
	 Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:WindowsShellCommands_Body
PowerShellCommands_COOKIE	在 Web 應用程式中檢查 PowerShell 命令注入嘗試的請求 Cookie 標頭。比對模式代表 PowerShell 命令。例如 Invoke-Expression。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:PowerShellCommands_Cookie

規則名稱	描述和標籤
PowerShellCommands_QUERYARGUMENTS	檢查 Web 應用程式中 PowerShell 命令注入嘗試的所有查詢參數的值。比對模式代表 PowerShell 命令。例如 Invoke-Expression 。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:PowerShellCommands_QueryArguments

規則名稱	描述和標籤
PowerShellCommands_BODY	在 Web 應用程式中檢查 PowerShell 命令注入嘗試的請求內文。比對模式代表 PowerShell 命令。例如 Invoke-Expression 。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:windows-os:PowerShellCommands_Body

PHP 應用程式受管規則群組

VendorName : AWS、Name : AWSManagedRulesPHPRuleSet、WCU : 100

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援 中心](#)。

PHP 應用程式規則群組包含的規則會封鎖與利用 PHP 程式設計語言特定漏洞相關的請求模式，包括注入不安全的 PHP 函數。這有助於防止利用允許攻擊者遠端執行程式碼或命令未授權的漏洞。如果您的應用程式與其互動的任何伺服器上安裝 PHP，請評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
PHPHighRiskMethodsVariables_HEADER	檢查所有標頭是否有 PHP 指令碼程式碼注入嘗試。範例模式包括 <code>fsockopen</code> 之類的函數和 <code>\$_GET</code> 超全域變數。  Warning 此規則只會檢查請求標頭的前 8 KB 或前 200 個標頭，以先達到限制為準，並使用 Continue 選項處理過大的內容。如需詳細資訊，請參閱 在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header
PHPHighRiskMethodsVariables_QUERYSTRING	檢查請求 URL 中第一個 之後的所有項目，尋找 PHP 指令碼程式碼注入嘗試。範例模式包括

規則名稱	描述和標籤
	fsockopen 之類的函數和 \$_GET 超全域變數。 規則動作：Block 標籤：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString
PHPHighRiskMethodsVariables_BODY	檢查要求主體是否有 PHP 指令碼程式碼注入嘗試。範例模式包括 fsockopen 之類的函數和 \$_GET 超全域變數。  Warning 此規則只會檢查請求內文，直到保護套件或 Web ACL 和資源類型的內文大小限制為止。對於 Application Load Balancer 和 AWS AppSync，限制固定為 8 KB。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，預設限制為 16 KB，您可以在保護套件或 Web ACL 組態中將限制提高到 64 KB。此規則使用 Continue 選項來處理過大的內容。如需詳細資訊，請參閱在中過大 Web 請求元件 AWS WAF。 規則動作：Block 標籤：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

WordPress 應用程式受管規則群組

VendorName : AWS、Name : AWSManagedRulesWordPressRuleSet、WCU : 100

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

WordPress 應用程式群組包含的規則會封鎖與利用 WordPress 網站特定漏洞相關的請求模式。如果您正在執行 WordPress，您應該評估此規則群組。此規則群組應結合 [SQL 資料庫](#) 和 [PHP 應用程式](#) 規則群組使用。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
WordPressExploitableCommands_QUERYSTRING	檢查請求查詢字串是否有可能在有弱點的安裝或外掛程式中遭入侵的高風險 WordPress 命令。範例模式包括 do-reset-wordpress 之類的命令。 規則動作：Block 標籤：aws:waf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING
WordPressExploitablePaths_URI_PATH	檢查要求 URI 路徑是否有 WordPress 檔案，如 xmlrpc.php，其已知具有易於入侵的漏洞。

規則名稱	描述和標籤
	規則動作：Block
	標籤：aws:waf:managed:aws:wordpress-app:WordPressExploitablePaths_URI_PATH

IP 評價規則群組

IP 評價規則群組會根據其來源 IP 地址封鎖請求。

Note

這些規則使用來自 Web 請求原始伺服器的來源 IP 地址。如果您有流經一或多個代理或負載平衡器的流量，Web 請求原始伺服器將包含最後一個代理的地址，而不是用戶端的原始地址。

如果您要減少暴露於機器人流量、利用嘗試，或是對內容強制執行地理限制，請選擇一或多個這些規則群組。如需機器人管理，另請參閱 [AWS WAF 機器人控制規則群組](#)。

此類別中的規則群組不提供版本控制或 SNS 更新通知。

Amazon IP 評價清單受管規則群組

VendorName : AWS、Name : AWSManagedRulesAmazonIpReputationList、WCU : 25

Note

我們為 AWS 受管規則規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

Amazon IP 評價清單規則群組包含以 Amazon 內部威脅情報為基礎的規則。如果您要封鎖通常與 Bot 或其他威脅相關聯的 IP 地址，這會很有用。封鎖這些 IP 地址有助於減輕 Bot，並降低惡意行為者發現易受攻擊應用程式的風險。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
AWSManagedIPReputationList	檢查已識別為主動參與惡意活動的 IP 地址。AWS WAF 會從各種來源收集 IP 地址清單，包括 MadPot，這是 Amazon 用來保護客戶免受網路攻擊的威脅情報工具。如需 MadPot 的詳細資訊，請參閱 https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime。 規則動作：Block 標籤：aws:waf:managed:aws:amazon-ip-list:AWSManagedIPReputationList
AWSManagedReconnaissanceList	檢查來自對資源執行偵察之 IP AWS 地址的連線。 規則動作：Block 標籤：aws:waf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList
AWSManagedIPDDoSList	檢查已識別為主動參與 DDoS 活動的 IP 地址。 規則動作：Count 標籤：aws:waf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList

匿名 IP 清單受管規則群組

VendorName : AWS、Name : AWSManagedRulesAnonymousIpList、WCU : 50

Note

我們為 AWS 受管規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

匿名 IP 清單規則群組包含規則，可封鎖來自允許混淆檢視器身分之服務的請求。其中包括來自 VPNs、代理、Tor 節點和 Web 託管供應商的請求。如果您要篩除可能會嘗試從您應用程式隱藏自身身分的檢視器，則此規則群組相當有用。封鎖這些服務的 IP 地址能協助降低機器人，以及迴避地理區域限制的問題。

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

規則名稱	描述和標籤
AnonymousIpList	檢查 IP 位址清單是否有已知會使用戶端資訊匿名化的來源，例如 TOR 節點、暫時代理伺服器和其他遮罩服務。 規則動作：Block 標籤：aws:waf:managed:aws:anonymous-ip-list:AnonymousIpList
HostingProviderIpList	檢查來自 Web 託管和雲端提供者的 IP 地址清單，這些地址較不可能來源最終使用者流量。IP 清單不包含 AWS IP 地址。 規則動作：Block 標籤：aws:waf:managed:aws:anonymous-ip-list:HostingProviderIpList

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 規則群組

本節說明 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組的功能。

VendorName : AWS、Name : AWSManagedRulesACFPRuleSet、WCU : 50

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組標籤和管理可能是詐騙帳戶建立嘗試一部分的請求。規則群組會透過檢查用戶端傳送到應用程式註冊和帳戶建立端點的帳戶建立請求來執行此操作。

ACFP 規則群組會以各種方式檢查帳戶建立嘗試，為您提供潛在惡意互動的可見性和控制。規則群組使用請求字符來收集有關用戶端瀏覽器和建立帳戶請求時人類互動程度的資訊。規則群組透過依 IP 地址和用戶端工作階段彙總請求，以及依提供的帳戶資訊彙總，例如實體地址和電話號碼，來偵測和管理大量帳戶建立嘗試。此外，規則群組會使用已遭入侵的登入資料來偵測和封鎖新帳戶的建立，這有助於保護應用程式和新使用者的安全狀態。

使用此規則群組的考量事項

此規則群組需要自訂組態，其中包含應用程式帳戶註冊和帳戶建立路徑的規格。除非另有說明，否則此規則群組中的規則會檢查用戶端傳送至這兩個端點的所有請求。若要設定和實作此規則群組，請參閱中的指引[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

此規則群組是 中智慧型威脅緩解保護的一部分 AWS WAF。如需相關資訊，請參閱[中的智慧型威脅防禦 AWS WAF](#)。

若要降低您的成本，並確保您視需要管理 Web 流量，請根據 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

此規則群組不適用於 Amazon Cognito 使用者集區。您無法將使用此規則群組的保護套件或 Web ACL 與使用者集區建立關聯，也無法將此規則群組新增至已與使用者集區建立關聯的保護套件或 Web ACL。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

字符標籤

此規則群組使用 AWS WAF 字符管理，根據其 AWS WAF 字符的狀態來檢查和標記 Web 請求。AWS WAF 使用字符進行用戶端工作階段追蹤和驗證。

如需權杖和權杖管理的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

如需此處所述標籤元件的詳細資訊，請參閱 [中的標籤語法和命名需求 AWS WAF](#)。

用戶端工作階段標籤

標籤 `awswaf:managed:token:id:identifier` 包含 AWS WAF 字符管理用來識別用戶端工作階段的唯一識別符。如果用戶端取得新的字符，例如在捨棄正在使用的字符之後，識別符可能會變更。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

瀏覽器指紋標籤

標籤 `awswaf:managed:token:fingerprint:fingerprint-identifier` 包含強大的瀏覽器指紋識別符，權 AWS WAF 杖管理會從各種用戶端瀏覽器訊號運算。此識別符在多次字符擷取嘗試中保持不變。指紋識別符對單一用戶端來說不是唯一的。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

字符狀態標籤：標籤命名空間字首

字符狀態標籤會報告字符的狀態，以及其中包含的挑戰和 CAPTCHA 資訊。

每個字符狀態標籤都以下列其中一個命名空間字首開頭：

- `awsaf:managed:token:` – 用來報告字符的一般狀態，以及報告字符挑戰資訊的狀態。
- `awsaf:managed:captcha:` – 用來報告字符 CAPTCHA 資訊的狀態。

字符狀態標籤：標籤名稱

在字首後面，標籤的其餘部分提供詳細的字符狀態資訊：

- `accepted` – 請求字符存在且包含下列項目：
 - 有效的挑戰或 CAPTCHA 解決方案。
 - 未過期的挑戰或 CAPTCHA 時間戳記。
 - 適用於保護套件或 Web ACL 的網域規格。

範例：標籤 `awsaf:managed:token:accepted` 指出 Web 請求的權杖具有有效的挑戰解決方案、未過期的挑戰時間戳記，以及有效的網域。

- `rejected` – 請求字符存在，但不符合接受條件。

除了拒絕的標籤之外，字符管理還會新增自訂標籤命名空間和名稱，以指出原因。

- `rejected:not_solved` – 字符缺少挑戰或 CAPTCHA 解決方案。
- `rejected:expired` – 權杖的挑戰或 CAPTCHA 時間戳記已過期，根據您的保護套件或 Web ACL 設定的權杖抗擾性時間而定。
- `rejected:domain_mismatch` – 字符的網域不符合您的保護套件或 Web ACL 的字符網域組態。
- `rejected:invalid` – AWS WAF 無法讀取指定的字符。

範例：標籤 `awsaf:managed:captcha:rejected` 和

`awsaf:managed:captcha:rejected:expired` 一起指出請求沒有有效的 CAPTCHA 解決方法，因為字符中的 CAPTCHA 時間戳記已超過保護套件或 Web ACL 中設定的 CAPTCHA 字符豁免時間。

- `absent` – 請求沒有字符或字符管理器無法讀取。

範例：標籤 `awsaf:managed:captcha:absent` 指出請求沒有字符。

ACFP 標籤

此規則群組會產生具有命名空間字首的標籤，aws:waf:managed:aws:acfp:後面接著自訂命名空間和標籤名稱。規則群組可能會將多個標籤新增至請求。

您可以透過 API 呼叫 來擷取規則群組的所有標籤 `DescribeManagedRuleGroup`。這些標籤會列在回應的 `AvailableLabels` 屬性中。

帳戶建立詐騙預防規則清單

本節列出 中的 ACFP 規則，`AWSMangedRulesACFPRuleSet` 以及規則群組規則新增至 Web 請求的標籤。

此規則群組中的所有規則都需要 Web 請求字符，前兩個 `UnsupportedCognitoIDP` 和 除外 `AllRequests`。如需字符提供的資訊說明，請參閱 [AWS WAF 字符特性](#)。

除非另有說明，否則此規則群組中的規則會檢查用戶端傳送至您在規則群組組態中提供的帳戶註冊和帳戶建立頁面路徑的所有請求。如需設定此規則群組的資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)。

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在 的 changelog 日誌中報告版本變更 [AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援 中心](#)。

規則名稱	描述和標籤
UnsupportedCognitoIDP	檢查傳送至 Amazon Cognito 使用者集區的 Web 流量。ACFP 不適用於 Amazon Cognito 使用者集區，此規則有助於確保不會使用其他 ACFP 規則群組規則來評估使用者集區流量。 規則動作：Block

規則名稱	描述和標籤
	標籤：aws:waf:managed:aws:acfp:unsupported:cognito_idp 和 aws:waf:managed:aws:acfp:UnsupportedCognitoIDP
AllRequests	將規則動作套用至存取註冊頁面路徑的請求。您可以在設定規則群組時設定註冊頁面路徑。 根據預設，此規則會將 Challenge 套用至 請求。透過套用此動作，規則可確保用戶端在規則群組中的其餘規則評估任何請求之前，先取得挑戰字符。 確保您的最終使用者在提交帳戶建立請求之前載入註冊頁面路徑。 權杖會由用戶端應用程式整合 SDKs 和規則動作 CAPTCHA和 新增至請求Challenge。為了取得最有效率的權杖，我們強烈建議您使用應用程式整合 SDKs。如需詳細資訊，請參閱中的用戶端應用程式整合 AWS WAF。 規則動作：Challenge 標籤：無

規則名稱	描述和標籤
RiskScoreHigh	檢查具有 IP 地址或其他被視為高度可疑因素的帳戶建立請求。此評估通常基於多個促成因素，您可以在規則群組新增至請求的<code>risk_score</code> 標籤中看到這些因素。 規則動作：Block 標籤：<code>aws:waf:managed:aws:acfp:risk_score:high</code> 和 <code>aws:waf:managed:aws:acfp:RiskScoreHigh</code> 規則也可能套用 <code>medium</code>或<code>low</code>風險分數標籤到請求。 如果 AWS WAF 無法成功評估 Web 請求的風險分數，則規則會新增標籤 <code>aws:waf:managed:aws:acfp:risk_score:evaluation_failed</code> 此外，規則會新增包含風險分數評估狀態 <code>aws:waf:managed:aws:acfp:risk_score:contributor:</code> 的命名空間標籤，以及特定風險分數貢獻者的結果，例如 IP 評價和遭竊的登入資料評估。

規則名稱	描述和標籤
SignalCredentialCompromised	搜尋遭竊的登入資料資料庫，尋找在帳戶建立請求中提交的登入資料。 此規則可確保新用戶端以正面的安全狀態初始化其帳戶。  Note 您可以新增自訂封鎖回應，向最終使用者描述問題，並告訴他們如何繼續。如需相關資訊，請參閱ACFP 範例：針對遭到入侵的登入資料的自訂回應。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:signal:credential_compromised 和 aws:waf:managed:aws:acfp:SignalCredentialCompromised 規則群組會套用下列相關標籤，但不對其採取任何動作，因為並非所有建立帳戶的請求都會有登入資料：aws:waf:managed:aws:acfp:signal:missing_credential

規則名稱	描述和標籤
SignalClientHumanInteractivityAbsentLow	檢查帳戶建立請求的字符是否有資料指出與應用程式有異常的人類互動。透過滑鼠移動和按鍵等互動來偵測人類互動。如果頁面具有 HTML 表單，則人工互動包括與表單的互動。  Note 此規則只會檢查帳戶建立路徑的請求，而且只有在您已實作應用程式整合 SDKs 時才會進行評估。SDK 實作會被動擷取人類互動性，並將資訊存放在請求字符中。如需詳細資訊，請參閱AWS WAF 字符特性及中的用戶端應用程式整合 AWS WAF。
規則動作：CAPTCHA 標籤：無。規則會根據不同的因素來決定配對，因此沒有適用於每個可能配對案例的個別標籤。 規則群組可以將下列一或多個標籤套用至請求： <pre>awswaf:managed:aws:acfp:signal:client:human_interactivity: <i>low/medium/high</i></pre> <pre>awswaf:managed:aws:acfp:SignalClientHumanInteractivityAbsent <i>Low/Medium/High</i></pre> <pre>awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data</pre>	

規則名稱	描述和標籤
	<code>awswaf:managed:aws:acfp:signal:form_detected</code> .
AutomatedBrowser	檢查用戶端瀏覽器是否可能自動化的指標。 規則動作：Block 標籤： <code>awswaf:managed:aws:acfp:signal:automated_browser</code> 和 <code>awswaf:managed:aws:acfp:AutomatedBrowser</code>
BrowserInconsistency	檢查請求的字符是否有不一致的瀏覽器查詢資料。如需詳細資訊，請參閱AWS WAF 字符特性。 規則動作：CAPTCHA 標籤： <code>awswaf:managed:aws:acfp:signal:browser_inconsistency</code> 和 <code>awswaf:managed:aws:acfp:BrowserInconsistency</code>

規則名稱	描述和標籤
VolumetricIpHigh	檢查從個別 IP 地址傳送的大量帳戶建立請求。在 10 分鐘的時段內，大量超過 20 個請求。  Note 此規則套用的閾值可能因延遲而略有不同。對於高磁碟區，在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:high 和 aws:waf:managed:aws:acfp:VolumetricIpHigh 規則會將下列標籤套用至具有中等磁碟區（每 10 分鐘超過 15 個請求）和低磁碟區（每 10 分鐘超過 10 個請求）的請求，但不會對這些請求採取任何動作：aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium 和 aws:waf:managed:aws:acfp:aggregate:volumetric:ip:creation:low 。

規則名稱	描述和標籤
VolumetricSessionHigh	檢查從個別用戶端工作階段傳送的大量帳戶建立請求。在 30 分鐘的時段內，大量超過 10 個請求。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:session:creation:high 和 aws:waf:managed:aws:acfp:VolumetricSessionHigh 規則群組會將下列標籤套用至具有中等磁碟區（超過每 30 分鐘 5 個請求）和低磁碟區（超過每 30 分鐘 1 個請求）的請求，但不對其採取任何動作：aws:waf:managed:aws:acfp:aggregate:volumetric:session:creation:medium 和 aws:waf:managed:aws:acfp:aggregate:volumetric:session:creation:low 。

規則名稱	描述和標籤
AttributeUsernameTraversalHigh	檢查使用不同使用者名稱的單一用戶端工作階段是否有高速率的帳戶建立請求。高評估的閾值是在 30 分鐘內超過 10 個請求。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high 和 aws:waf:managed:aws:acfp:AttributeUsernameTraversalHigh 規則群組會將下列標籤套用至使用者名稱周遊請求的中等磁碟區（超過每 30 分鐘 5 個請求）和低磁碟區（超過每 30 分鐘 1 個請求）的請求，但不對其採取任何動作：aws:waf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium 和 aws:waf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low 。

規則名稱	描述和標籤
VolumetricPhoneNumberHigh	檢查是否有大量使用相同電話號碼的帳戶建立請求。高評估的閾值是在 30 分鐘內超過 10 個請求。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:high 和 aws:waf:managed:aws:acfp:VolumetricPhoneNumberHigh 規則群組會將下列標籤套用至具有中等磁碟區（每 30 分鐘超過 5 個請求）和低磁碟區（每 30 分鐘超過 1 個請求）的請求，但不對其採取任何動作：aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:medium 和 aws:waf:managed:aws:acfp:aggregate:volumetric:phone_number:low 。

規則名稱	描述和標籤
VolumetricAddressHigh	檢查是否有大量使用相同實體地址的帳戶建立請求。高評估的閾值為每個 30 分鐘時段超過 100 個請求。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:address:high 和 aws:waf:managed:aws:acfp:VolumetricAddressHigh

規則名稱	描述和標籤
VolumetricAddressLow	檢查使用相同實體地址的低和中等數量的帳戶建立請求。中型評估的閾值是每 30 分鐘時段超過 50 個請求，而低度評估則是每 30 分鐘時段超過 10 個請求。 此規則會套用中或低磁碟區的動作。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:address: <i>low/medium</i> 和 aws:waf:managed:aws:acfp:VolumetricAddress <i>Low/Medium</i>

規則名稱	描述和標籤
VolumetricIPSuccessfulResponse	檢查單一 IP 地址是否有大量的成功帳戶建立請求。此規則會將受保護資源的成功回應彙總到帳戶建立請求。高評估的閾值為每個 10 分鐘時段超過 10 個請求。 此規則有助於防止大量帳戶建立嘗試。其閾值低於規則 VolumetricIpHigh，僅計算請求。 如果您已設定規則群組來檢查回應內文或 JSON 元件，AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB) 是否有成功或失敗指標。 此規則會根據來自受保護資源的成功和失敗回應，以及來自相同 IP 地址的最近登入嘗試，將規則動作和標籤套用至來自 IP 地址的新 Web 請求。您可以在設定規則群組時，定義如何計算成功和失敗。  Note AWS WAF 只會在保護 Amazon CloudFront 分佈的保護套件或 Web ACLs 中評估此規則。  Note 此規則套用的閾值可能因延遲而略有不同。用戶端可能會傳送比規則在後續嘗試中開始比對之前允許的更成功的帳戶建立嘗試。

規則名稱	描述和標籤
	規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high 和 aws:waf:managed:aws:acfp:VolumetricIPSuccessfulResponse 規則群組也會將下列相關標籤套用至請求，而沒有任何相關聯的動作。所有計數都適用於 10 分鐘的時段。aws:waf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium 對於 5 個以上的成功請求，aws:waf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low 對於 1 個以上的成功請求，aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high 對於 10 個以上的失敗請求，aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium 對於 5 個以上的失敗請求，以及對於 1 個aws:waf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low 以上的失敗請求。

規則名稱	描述和標籤
VolumetricSessionSuccessfulResponse	檢查從受保護資源到從單一用戶端工作階段傳送的帳戶建立請求的成功回應數量是否很低。這有助於防止大量帳戶建立嘗試。低評估的閾值是每 30 分鐘時段 1 個以上的請求。 這有助於防止大量帳戶建立嘗試。此規則使用的閾值低於只 <code>VolumetricSessionHigh</code> 追蹤請求的規則。 如果您已設定規則群組來檢查回應內文或 JSON 元件，AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB) 是否有成功或失敗指標。 此規則會根據來自受保護資源的成功和失敗回應，以及來自相同用戶端工作階段的最近登入嘗試，將規則動作和標籤套用至來自用戶端工作階段的新 Web 請求。您可以在設定規則群組時，定義如何計算成功和失敗。  Note AWS WAF 只會在保護 Amazon CloudFront 分佈的保護套件或 Web ACLs 中評估此規則。  Note 此規則套用的閾值可能因延遲而略有不同。用戶端傳送失敗的帳戶建立嘗試次數可能超過規則在後續嘗試中開始比對之前允許的次數。

規則名稱	描述和標籤
	規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low 和 aws:waf:managed:aws:acfp:VolumetricSessionSuccessfulResponse 規則群組也會將下列相關標籤套用至請求。所有計數都適用於 30 分鐘的時段。aws:waf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high 對於 10 個以上的成功請求，aws:waf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:medium 對於 5 個以上的成功請求，aws:waf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high 對於 10 個以上的失敗請求，aws:waf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium 對於 5 個以上的失敗請求，以及對於 1 個aws:waf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low 以上的失敗請求。

規則名稱	描述和標籤
VolumetricSessionTokenReuseIp	檢查帳戶建立請求是否在超過 5 個不同的 IP 地址中使用單一字符。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip 和 aws:waf:managed:aws:acfp:VolumetricSessionTokenReuseIp

AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組

本節說明 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組的功能。

VendorName : AWS、Name : AWSManagedRulesATPRuleSet、WCU : 50

Note

本文件涵蓋此受管規則群組的最新版本。我們會在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。我們為 AWS 受管規則規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組標籤和管理可能屬於惡意帳戶接管嘗試一部分的請求。規則群組會透過檢查用戶端傳送到應用程式登入端點的登入嘗試來執行此操作。

- 請求檢查 – ATP 可讓您查看和控制使用遭竊登入資料的異常登入嘗試和登入嘗試，以防止可能導致詐騙活動的帳戶接管。ATP 會針對其遭竊的登入資料資料庫檢查電子郵件和密碼組合，因為在黑暗的 Web 上發現新的洩漏登入資料時，會定期更新。ATP 會依 IP 地址和用戶端工作階段彙總資料，以偵測和封鎖傳送過多可疑請求的用戶端。
- 回應檢查 – 對於 CloudFront 分佈，除了檢查傳入的登入請求之外，ATP 規則群組還會檢查應用程式的登入嘗試回應，以追蹤成功和失敗率。使用此資訊，ATP 可以暫時封鎖登入失敗次數過多的用戶端工作階段或 IP 地址。會以非同步方式 AWS WAF 執行回應檢查，因此這不會增加 Web 流量的延遲。

使用此規則群組的考量事項

此規則群組需要特定組態。若要設定和實作此規則群組，請參閱 [中的指引 AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)。

此規則群組是 中智慧型威脅防禦保護的一部分 AWS WAF。如需相關資訊，請參閱 [中的智慧型威脅防禦 AWS WAF](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

若要降低您的成本，並確保您視需要管理 Web 流量，請根據 [中的指引](#) 使用此規則群組 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

此規則群組不適用於 Amazon Cognito 使用者集區。您無法將使用此規則群組的保護套件或 Web ACL 與使用者集區建立關聯，也無法將此規則群組新增至已與使用者集區建立關聯的保護套件或 Web ACL。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

字符標籤

此規則群組使用 AWS WAF 字符管理，根據其 AWS WAF 字符的狀態來檢查和標記 Web 請求。AWS WAF 使用字符進行用戶端工作階段追蹤和驗證。

如需字符和字符管理的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

如需此處所述標籤元件的詳細資訊，請參閱 [中的標籤語法和命名需求 AWS WAF](#)。

用戶端工作階段標籤

標籤 `aws:waf:managed:token:id:identifier` 包含 AWS WAF 字符管理用來識別用戶端工作階段的唯一識別符。如果用戶端取得新的字符，例如在捨棄正在使用的字符之後，識別符可能會變更。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

瀏覽器指紋標籤

標籤 `aws:waf:managed:token:fingerprint:fingerprint-identifier` 包含強大的瀏覽器指紋識別符，權 AWS WAF 杖管理會從各種用戶端瀏覽器訊號運算。此識別符在多個字符擷取嘗試中保持不變。指紋識別符對單一用戶端來說不是唯一的。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

字符狀態標籤：標籤命名空間字首

字符狀態標籤會報告字符的狀態，以及其中包含的挑戰和 CAPTCHA 資訊。

每個字符狀態標籤都以下列其中一個命名空間字首開頭：

- `aws:waf:managed:token:` – 用來報告字符的一般狀態，以及報告字符挑戰資訊的狀態。
- `aws:waf:managed:captcha:` – 用來報告字符 CAPTCHA 資訊的狀態。

字符狀態標籤：標籤名稱

在字首後面，標籤的其餘部分提供詳細的字符狀態資訊：

- `accepted` – 請求字符存在且包含下列項目：
 - 有效的挑戰或 CAPTCHA 解決方案。
 - 未過期的挑戰或 CAPTCHA 時間戳記。

- 適用於保護套件或 Web ACL 的網域規格。

範例：標籤 `aws:waf:managed:token:accepted` 指出 Web 請求的權杖具有有效的挑戰解決方案、未過期的挑戰時間戳記，以及有效的網域。

- `rejected` – 請求字符存在，但不符合接受條件。

除了拒絕的標籤之外，字符管理還會新增自訂標籤命名空間和名稱，以指出原因。

- `rejected:not_solved` – 字符缺少挑戰或 CAPTCHA 解決方案。
- `rejected:expired` – 權杖的挑戰或 CAPTCHA 時間戳記已過期，根據您的保護套件或 Web ACL 設定的權杖抗擾性時間而定。
- `rejected:domain_mismatch` – 字符的網域不符合您的保護套件或 Web ACL 的字符網域組態。
- `rejected:invalid` – AWS WAF 無法讀取指定的字符。

範例：標籤 `aws:waf:managed:captcha:rejected` 和 `aws:waf:managed:captcha:rejected:expired` 一起指出請求沒有有效的 CAPTCHA 解決方法，因為字符中的 CAPTCHA 時間戳記已超過保護套件或 Web ACL 中設定的 CAPTCHA 字符豁免時間。

- `absent` – 請求沒有字符或字符管理器無法讀取。

範例：標籤 `aws:waf:managed:captcha:absent` 指出請求沒有字符。

ATP 標籤

ATP 受管規則群組會產生具有命名空間字首的標籤，`aws:waf:managed:aws:atp:` 後面接著自訂命名空間和標籤名稱。

除了規則清單中記下的標籤之外，規則群組還可能會新增下列任何標籤：

- `aws:waf:managed:aws:atp:signal:credential_compromised` – 表示在請求中提交的登入資料位於遭竊的登入資料資料庫中。
- `aws:waf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint` – 僅適用於受保護的 Amazon CloudFront 分佈。表示用戶端工作階段已傳送多個使用可疑 TLS 指紋的請求。
- `aws:waf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip` – 表示在超過 5 個不同的 IP 地址中使用單一字符。此規則套用的閾值可能因延遲而略有不同。在套用標籤之前，有些請求可能會使其超過限制。

您可以透過 API 呼叫 來擷取規則群組的所有標籤DescribeManagedRuleGroup。這些標籤會列在回應的 AvailableLabels 屬性中。

帳戶接管預防規則清單

本節列出 中的 ATP 規則，AWSManagedRulesATPRuleSet以及規則群組規則新增至 Web 請求的標籤。

Note

本文件涵蓋此受管規則群組的最新版本。我們會在 的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。我們為 AWS 受管規則規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。如果您需要比此處更多的資訊，請聯絡 [AWS 支援 中心](#)。

規則名稱	描述和標籤
UnsupportedCognitoIDP	檢查傳送至 Amazon Cognito 使用者集區的 Web 流量。ATP 不適用於 Amazon Cognito 使用者集區，此規則有助於確保不會使用其他 ATP 規則群組規則來評估使用者集區流量。 規則動作：Block 標籤：aws:waf:managed:aws:atp:unsupported:cognito_idp 和 aws:waf:managed:aws:atp:UnsupportedCognitoIDP
VolumetricIpHigh	檢查從個別 IP 地址傳送的大量請求。在 10 分鐘的時段內，大量超過 20 個請求。

規則名稱	描述和標籤
	 Note 此規則套用的閾值可能因延遲而略有不同。對於高磁碟區，在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:volumetric:ip:high 和 aws:waf:managed:aws:atp:VolumetricIpHigh 規則群組會將下列標籤套用至具有中等磁碟區（超過每 10 分鐘 15 個請求）和低磁碟區（超過每 10 分鐘 10 個請求）的請求，但不對其採取任何動作：aws:waf:managed:aws:atp:aggregate:volumetric:ip:medium 和 aws:waf:managed:aws:atp:aggregate:volumetric:ip:low 。

規則名稱	描述和標籤
VolumetricSession	檢查從個別用戶端工作階段傳送的大量請求。閾值為每個 30 分鐘時段超過 20 個請求。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。  Note 此規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:volumetric:session 和 aws:waf:managed:aws:atp:VolumetricSession
AttributeCompromisedCredentials	檢查來自使用遭竊憑證之相同用戶端工作階段的多個請求。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:attribute:compromised_credentials 和 aws:waf:managed:aws:atp:AttributeCompromisedCredentials

規則名稱	描述和標籤
AttributeUsernameTraversal	檢查來自使用使用者名稱周遊之相同用戶端工作階段的多個請求。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:attribute:username_traversal 和 aws:waf:managed:aws:atp:AttributeUsernameTraversal
AttributePasswordTraversal	檢查是否有多個請求具有使用密碼周遊的相同使用者名稱。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:attribute:password_traversal 和 aws:waf:managed:aws:atp:AttributePasswordTraversal

規則名稱	描述和標籤
AttributeLongSession	檢查來自使用長期工作階段之相同用戶端工作階段的多個請求。閾值是超過 6 小時的流量，每 30 分鐘至少有一個登入請求。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:attribute:long_session 和 aws:waf:managed:aws:atp:AttributeLongSession
TokenRejected	使用字符管理拒絕的 AWS WAF 字符檢查請求。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：Block 標籤：無。若要檢查權杖是否遭拒，請使用標籤比對規則來比對標籤：aws:waf:managed:token:rejected。

規則名稱	描述和標籤
SignalMissingCredential	檢查是否有憑證缺少使用者名稱或密碼的請求。 規則動作：Block 標籤：aws:waf:managed:aws:atp:signal:missing_credential 和 aws:waf:managed:aws:atp:SignalMissingCredential

規則名稱	描述和標籤
VolumetricIpFailedLoginResponseHigh	檢查最近登入嘗試失敗率太高的 IP 地址。在 10 分鐘內，來自 IP 地址的高磁碟區超過 10 個失敗的登入請求。 如果您已設定規則群組來檢查回應內文或 JSON 元件，AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB) 是否有成功或失敗指標。 此規則會根據來自受保護資源的成功和失敗回應，以及來自相同 IP 地址的最近登入嘗試，將規則動作和標籤套用至來自 IP 地址的新 Web 請求。您可以在設定規則群組時，定義如何計算成功和失敗。  Note AWS WAF 只會在保護 Amazon CloudFront 分佈的保護套件或 Web ACLs 中評估此規則。  Note 此規則套用的閾值可能因延遲而略有不同。用戶端傳送失敗的登入嘗試次數可能超過規則在後續嘗試時開始比對之前允許的次數。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_

規則名稱	描述和標籤
	<code>login_response:high</code> 和 <code>aws:waf:managed:aws:atp:VolumetricIpFailedLoginResponseHigh</code> 規則群組也會將下列相關標籤套用至請求，而沒有任何相關聯的動作。所有計數都適用於 10 分鐘的時段。<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium</code> 對於超過 5 個失敗的請求，<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low</code> 對於超過 1 個失敗的請求，<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low</code> 的請求，<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high</code> 對於超過 10 個成功的請求，<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium</code> 對於超過 5 個成功的請求，以及對於超過 1 個成功的請求。

規則名稱	描述和標籤
VolumetricSessionFailedLoginResponseHigh	檢查最近登入嘗試失敗率太高的用戶端工作階段。在 30 分鐘內，來自用戶端工作階段的高磁碟區超過 10 個失敗的登入請求。 如果您已設定規則群組來檢查回應內文或 JSON 元件，AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB) 是否有成功或失敗指標。 此規則會根據來自受保護資源的成功和失敗回應，以及來自相同用戶端工作階段的最近登入嘗試，將規則動作和標籤套用至來自用戶端工作階段的新 Web 請求。您可以在設定規則群組時，定義如何計算成功和失敗。  Note AWS WAF 只會在保護 Amazon CloudFront 分佈的保護套件或 Web ACLs 中評估此規則。  Note 此規則套用的閾值可能因延遲而略有不同。用戶端傳送失敗的登入嘗試次數可能超過規則在後續嘗試時開始比對之前允許的次數。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細

規則名稱	描述和標籤
	資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：Block 標籤：aws:waf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high 和 aws:waf:managed:aws:atp:VolumetricSessionFailedLoginResponseHigh 規則群組也會將下列相關標籤套用至請求，而沒有任何相關聯的動作。所有計數都適用於 30 分鐘的時段。aws:waf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium 對於超過 5 個失敗的請求，aws:waf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low 對於超過 1 個失敗aws:waf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low 的請求，aws:waf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high 對於超過 10 個成功的請求，aws:waf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium 對於超過 5 個成功的請求，以及對於超過 1 個成功的請求。

AWS WAF 機器人控制規則群組

本節說明 Bot Control 受管規則群組的功能。

VendorName : AWS、Name : AWSManagedRulesBotControlRuleSet、WCU : 50

Note

本文件涵蓋此受管規則群組的最新版本。我們會在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。我們為 AWS 受管規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

Bot Control 受管規則群組提供規則來管理來自機器人的請求。機器人可能會消耗過多的資源、扭曲業務指標、造成停機時間，以及執行惡意活動。

保護層級

Bot Control 受管規則群組提供兩種層級的保護，您可以從中選擇：

- 常見 – 偵測各種自我識別機器人，例如 Web 抓取架構、搜尋引擎和自動化瀏覽器。此層級的機器人控制保護會使用傳統機器人偵測技術來識別常見的機器人，例如靜態請求資料分析。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的流量。
- 目標型 – 包含共同層級的保護，並為無法自我識別的複雜機器人新增目標型偵測。針對性保護會使用速率限制和 CAPTCHA 和背景瀏覽器挑戰的組合來緩解機器人活動。
- **TGT_** – 提供目標保護的規則具有以開頭的名稱 TGT_。所有目標防護都使用瀏覽器查詢、指紋和行為啟發式等偵測技術來識別錯誤的機器人流量。
- **TGT_ML_** – 使用機器學習的目標保護規則具有以開頭的名稱 TGT_ML_。這些規則使用網站流量統計資料的自動化機器學習分析來偵測指示分散式、協調機器人活動的異常行為。AWS WAF 會分析網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。預設會啟用機器學習功能，但您可以在規則群組組態中停用這些功能。停用機器學習時，AWS WAF 不會評估這些規則。

目標保護層級和速率 AWS WAF 型規則陳述式都提供速率限制。如需兩個選項的比較，請參閱 [速率型規則和目標 Bot Control 規則中速率限制的選項](#)。

使用此規則群組的考量事項

此規則群組是 中智慧型威脅防禦保護的一部分 AWS WAF。如需相關資訊，請參閱[中的智慧型威脅防禦 AWS WAF](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

若要降低成本，並確保您視需要管理 Web 流量，請根據 中的指引使用此規則群組[中的智慧型威脅防禦最佳實務 AWS WAF](#)。

我們會定期更新目標防護層級 ML 型規則的機器學習 (ML) 模型，以改善機器人預測。ML 型規則的名稱開頭為 TGT_ML_。如果您注意到這些規則所做的機器人預測突然發生重大變更，請透過您的客戶經理聯絡我們，或在 [AWS 支援 Center](#) 開立案例。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

字符標籤

此規則群組使用 AWS WAF 字符管理，根據其 AWS WAF 字符的狀態來檢查和標記 Web 請求。AWS WAF 使用字符進行用戶端工作階段追蹤和驗證。

如需字符和字符管理的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

如需此處所述的標籤元件資訊，請參閱 [中的標籤語法和命名需求 AWS WAF](#)。

用戶端工作階段標籤

標籤 `awswaf:managed:token:id:identifier` 包含 AWS WAF 字符管理用來識別用戶端工作階段的唯一識別符。如果用戶端取得新的字符，例如在捨棄正在使用的字符之後，識別符可能會變更。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

瀏覽器指紋標籤

標籤 `aws:waf:managed:token:fingerprint:`*fingerprint-identifier* 包含強大的瀏覽器指紋識別符，權 AWS WAF 杖管理會從各種用戶端瀏覽器訊號運算。此識別符在多個字符擷取嘗試中保持不變。指紋識別符對單一用戶端來說不是唯一的。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

字符狀態標籤：標籤命名空間字首

字符狀態標籤會報告字符的狀態，以及其中包含的挑戰和 CAPTCHA 資訊。

每個字符狀態標籤都以下列其中一個命名空間字首開頭：

- `aws:waf:managed:token:` – 用來報告字符的一般狀態，以及報告字符挑戰資訊的狀態。
- `aws:waf:managed:captcha:` – 用來報告字符 CAPTCHA 資訊的狀態。

字符狀態標籤：標籤名稱

在字首後面，標籤的其餘部分提供詳細的字符狀態資訊：

- `accepted` – 請求字符存在並包含下列項目：
 - 有效的挑戰或 CAPTCHA 解決方案。
 - 未過期的挑戰或 CAPTCHA 時間戳記。
 - 適用於保護套件或 Web ACL 的網域規格。

範例：標籤 `aws:waf:managed:token:accepted` 指出 Web 請求的權杖具有有效的挑戰解決方案、未過期的挑戰時間戳記，以及有效的網域。

- `rejected` – 請求字符存在，但不符合接受條件。

除了拒絕的標籤之外，字符管理還會新增自訂標籤命名空間和名稱，以指出原因。

- `rejected:not_solved` – 字符缺少挑戰或 CAPTCHA 解決方案。
- `rejected:expired` – 權杖的挑戰或 CAPTCHA 時間戳記已過期，取決於您的保護套件或 Web ACL 設定的權杖抗擾性時間。

- `rejected:domain_mismatch` – 字符的網域不符合您的保護套件或 Web ACL 的字符網域組態。
- `rejected:invalid` – AWS WAF 無法讀取指定的字符。

範例：標籤 `aws:waf:managed:captcha:rejected` 和 `aws:waf:managed:captcha:rejected:expired` 一起指出請求沒有有效的 CAPTCHA 解決方法，因為字符中的 CAPTCHA 時間戳記已超過保護套件或 Web ACL 中設定的 CAPTCHA 字符豁免時間。

- `absent` – 請求沒有字符或字符管理器無法讀取。

範例：標籤 `aws:waf:managed:captcha:absent` 表示請求沒有字符。

機器人控制標籤

Bot Control 受管規則群組會產生具有命名空間字首的標籤，`aws:waf:managed:aws:bot-control:`後面接著自訂命名空間和標籤名稱。規則群組可能會將多個標籤新增至請求。

每個標籤都會反映 Bot Control 規則調查結果：

- `aws:waf:managed:aws:bot-control:bot:` – 與請求相關聯之機器人的相關資訊。
 - `aws:waf:managed:aws:bot-control:bot:name:<name>` – 機器人名稱，如果有的話，例如，自訂命名空間 `bot:name:slurp`、`bot:name:googlebot` 和 `bot:name:pocket_parser`。
 - `aws:waf:managed:aws:bot-control:bot:category:<category>` – 機器人的類別，如和 AWS WAF `bot:category:search_engine` 所定義 `bot:category:content_fetcher`。
 - `aws:waf:managed:aws:bot-control:bot:organization:<organization>` – 機器人的發佈者，例如 `bot:organization:google`。
 - `aws:waf:managed:aws:bot-control:bot:verified` – 用來指示識別自己且 Bot Control 能夠驗證的機器人。這用於常見的所需機器人，當與類別標籤如 `bot:category:search_engine` 或名稱標籤如 `bot:name:googlebot` 結合使用時非常有用。

Note

Bot Control 會使用來自 Web 請求原始伺服器的 IP 地址，協助判斷機器人是否已驗證。您無法將其設定為使用 AWS WAF 轉送的 IP 組態，以檢查不同的 IP 地址來源。如果您已驗證透過代理或負載平衡器路由的機器人，您可以新增在 Bot Control 規則群組之前執行的規則，以協助處理此問題。設定您的新規則以使用轉送的 IP 地址，並明確允許來自已驗證

機器人的請求。如需使用轉送 IP 地址的詳細資訊，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。

- `aws:waf:managed:aws:bot-control:bot:user_triggered:verified` – 用來表示類似於已驗證機器人的機器人，但最終使用者可能會直接叫用。機器人控制規則會將此類別的機器人視為未驗證的機器人。
- `aws:waf:managed:aws:bot-control:bot:developer_platform:verified` – 用來表示與已驗證的機器人類似的機器人，但開發人員平台用來編寫指令碼，例如 Google Apps Script。機器人控制規則會將此類別的機器人視為未驗證的機器人。
- `aws:waf:managed:aws:bot-control:bot:unverified` – 用來指示識別自己的機器人，因此可以命名和分類，但不會發佈可用來獨立驗證其身分的資訊。這些類型的機器人簽章可能是偽造的，因此會被視為未驗證。
- `aws:waf:managed:aws:bot-control:targeted:<additional-details>` – 用於 Bot Control 目標保護特有的標籤。
- `aws:waf:managed:aws:bot-control:signal:<signal-details>` 和 `aws:waf:managed:aws:bot-control:targeted:signal:<signal-details>` – 用於在某些情況下提供有關請求的其他資訊。

以下是訊號標籤的範例。這不是詳盡的清單：

- `aws:waf:managed:aws:bot-control:signal:cloud_service_provider:<CSP>` – 表示請求的雲端服務提供者 (CSP)。CSPs 的範例包括 `aws` Amazon Web Services 基礎設施、`gcp` Google Cloud Platform (GCP) 基礎設施、`azure` Microsoft Azure 雲端服務和 `oracle` Oracle Cloud 服務。
- `aws:waf:managed:aws:bot-control:targeted:signal:browser_automation_extension` – 指出協助自動化的瀏覽器延伸模組偵測，例如 Selenium IDE。

每當使用者安裝了這種類型的延伸模組時，就會新增此標籤，即使使用者未主動使用也一樣。如果您為此實作標籤比對規則，請注意在規則邏輯和動作設定中出現誤報的可能性。例如，您可以使用 CAPTCHA 動作，而不是 Block，或者您可以將此標籤比對與其他標籤比對結合，以提高您使用自動化的信心。

- `aws:waf:managed:aws:bot-control:signal:automated_browser` – 表示請求包含用戶端瀏覽器可能已自動化的指標。
- `aws:waf:managed:aws:bot-control:targeted:signal:automated_browser` – 表示請求的 AWS WAF 字符合包含用戶端瀏覽器可能已自動化的指標。

您可以透過 API 呼叫 來擷取規則群組的所有標籤DescribeManagedRuleGroup。這些標籤會列在回應的 AvailableLabels 屬性中。

Bot Control 受管規則群組會將標籤套用至一組通常允許的可驗證機器人。規則群組不會封鎖這些已驗證的機器人。如果需要，您可以編寫使用 Bot Control 受管規則群組所套用標籤的自訂規則來封鎖它們或其中一部分。如需此 和範例的詳細資訊，請參閱 [AWS WAF 機器人控制](#)。

機器人控制規則清單

本節列出機器人控制規則。

Note

本文件涵蓋此受管規則群組的最新版本。我們會在 的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。我們為 AWS 受管規則規則群組中的規則發佈的資訊，旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

規則名稱	描述
CategoryAdvertising	檢查用於廣告目的的機器人。例如，您可以使用需要以程式設計方式存取網站的第三方廣告服務。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:advertising 和 aws:waf:managed:aws:bot-control:CategoryAdvertising 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryArchiver	檢查用於封存目的的機器人。這些機器人會爬取 Web 並擷取內容，以建立封存。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:archiver 和 aws:waf:managed:aws:bot-control:CategoryArchiver 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategoryContentFetcher	檢查代表使用者造訪應用程式網站的機器人、擷取 RSS 摘要等內容，或驗證或驗證您的內容。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:content_fetcher 和 aws:waf:managed:aws:bot-control:CategoryContentFetcher 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryEmailClient	檢查機器人是否檢查指向應用程式網站的電子郵件中的連結。這可能包括由企業和電子郵件供應商執行的機器人，以驗證電子郵件中的連結並標記可疑的電子郵件。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:email_client 和 aws:waf:managed:aws:bot-control:CategoryEmailClient 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategoryHttpLibrary	檢查機器人從各種程式設計語言的 HTTP 程式庫產生的請求。這些可能包括您選擇允許或監控的 API 請求。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:http_library 和 aws:waf:managed:aws:bot-control:CategoryHttpLibrary 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryLinkChecker	檢查檢查檢查連結是否損壞的機器人。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:link_checker 和 aws:waf:managed:aws:bot-control:CategoryLinkChecker 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategoryMiscellaneous	檢查其他不符合其他類別的機器人。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:miscellaneous 和 aws:waf:managed:aws:bot-control:CategoryMiscellaneous 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryMonitoring	檢查用於監控目的的機器人。例如，您可以使用機器人監控服務來定期 ping 應用程式網站，以監控效能和運作時間等項目。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:monitoring 和 aws:waf:managed:aws:bot-control:CategoryMonitoring 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategoryScrapingFramework	檢查來自 Web 抓取架構的機器人，這些架構用於自動從網站爬取和擷取內容。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:scraping_framework 和 aws:waf:managed:aws:bot-control:CategoryScrapingFramework 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategorySearchEngine	檢查搜尋引擎機器人，哪些網路爬取網站編製內容索引，並使資訊可用於搜尋引擎結果。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:search_engine 和 aws:waf:managed:aws:bot-control:CategorySearchEngine 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategorySecurity	檢查掃描 Web 應用程式是否有漏洞或執行安全稽核的機器人。例如，您可以使用第三方安全廠商來掃描、監控或稽核 Web 應用程式的安全性。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:security 和 aws:waf:managed:aws:bot-control:CategorySecurity 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategorySeo	檢查用於搜尋引擎最佳化的機器人。例如，您可以使用搜尋引擎工具來編目您的網站，以協助您改善搜尋引擎排名。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:seo 和 aws:waf:managed:aws:bot-control:CategorySeo 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。
CategorySocialMedia	檢查社交媒體平台所使用的機器人，以便在使用者共用您的內容時提供內容摘要。 規則動作，僅適用於未驗證的機器人：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:social_media 和 aws:waf:managed:aws:bot-control:CategorySocialMedia 對於已驗證的機器人，規則群組不符合此規則，且不採取任何動作，但會新增機器人名稱和類別標籤加上標籤 aws:waf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryAI	檢查人工智慧 (AI) 機器人。  Note 此規則會將 動作套用至所有相符項目，無論機器人是否經過驗證。 規則動作：Block 標籤：aws:waf:managed:aws:bot-control:bot:category:ai 和 aws:waf:managed:aws:bot-control:CategoryAI 對於已驗證的機器人，規則群組符合此規則並採取 動作。它還會新增機器人名稱和類別標籤、規則標籤，以及標籤 aws:waf:managed:aws:bot-control:bot:verified 。
SignalAutomatedBrowser	檢查未來自己驗證機器人的請求，是否有可能自動化用戶端瀏覽器的指標。自動化瀏覽器可用於測試或抓取。例如，您可以使用這些類型的瀏覽器來監控或驗證您的應用程式網站。 規則動作：Block 標籤：aws:waf:managed:aws:bot-control:signal:automated_browser 和 aws:waf:managed:aws:bot-control:SignalAutomatedBrowser 對於已驗證的機器人，規則群組不符合此規則，且不會套用任何訊號或規則標籤。

規則名稱	描述
SignalKnownBotDataCenter	檢查未來自己驗證機器人的請求，是否有通常由機器人使用的資料中心指標。 規則動作：Block 標籤：aws:waf:managed:aws:bot-control:signal:known_bot_data_center 和 aws:waf:managed:aws:bot-control:SignalKnownBotDataCenter 對於已驗證的機器人，規則群組不符合此規則，且不會套用任何訊號或規則標籤。
SignalNonBrowserUserAgent	檢查不是來自自己驗證機器人的請求，是否有似乎不是來自 Web 瀏覽器的使用者代理程式字串。此類別可以包含 API 請求。 規則動作：Block 標籤：aws:waf:managed:aws:bot-control:signal:non_browser_user_agent 和 aws:waf:managed:aws:bot-control:SignalNonBrowserUserAgent 對於已驗證的機器人，規則群組不符合此規則，且不會套用任何訊號或規則標籤。

規則名稱	描述
TGT_VolumetricIpTokenAbsent	檢查過去 5 分鐘內未來自己驗證機器人的請求，其中包含來自單一用戶端的 5 個或更多請求，而該請求不包含有效的挑戰字符。如需字符的資訊，請參閱 用於 AWS WAF 智慧型威脅緩解的字符。  Note 如果來自相同用戶端的請求最近缺少字符，則此規則可能符合具有字符的請求。 此規則套用的閾值可能因延遲而略有不同。 此規則處理遺失字符的方式與字符標籤不同：<code>aws:waf:managed:token:absent</code>。字符標籤會標記沒有字符的個別請求。此規則會維護每個用戶端 IP 缺少字符的請求計數，並與超過限制的用戶端相符。 規則動作：Challenge 標籤：<code>aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent</code> 和 <code>aws:waf:managed:aws:bot-control:TGT_VolumetricIpTokenAbsent</code>

規則名稱	描述
TGT-TokenAbsent	檢查未來自未包含有效挑戰字符之已驗證機器人的請求。如需字符的資訊，請參閱 用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：Count 標籤：aws:waf:managed:aws:bot-control:TGT-TokenAbsent

規則名稱	描述
TGT_VolumetricSession	檢查是否有異常大量的請求，這些請求不是來自 5 分鐘內來自單一用戶端工作階段的已驗證機器人。評估是根據與使用歷史流量模式 AWS WAF 維護之標準容積基準的比較。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。  Note 此規則在您啟用後可能需要 5 分鐘才會生效。Bot Control 透過比較目前的流量與 AWS WAF 運算的流量基準，來識別 Web 流量中的異常行為。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high 和 aws:waf:managed:aws:bot-control:TGT_VolumetricSession 規則群組會將下列標籤套用至高於最低閾值的中等磁碟區和較低磁碟區請求。對於這些層級，無論用戶端是否已驗證：aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium 和 ，規則都不會採取任何動作aws:waf:managed:aws:bot-cont

規則名稱	描述
TGT_VolumetricSessionMaximum	<code>rol:targeted:aggregate:volumetric:session:low</code> 。 檢查是否有異常大量的請求，這些請求不是來自 5 分鐘內來自單一用戶端工作階段的已驗證機器人。評估是根據與使用歷史流量模式 AWS WAF 維護之標準容積基準的比較。 此規則表示評估的最大可信度。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。  Note 此規則在您啟用後可能需要 5 分鐘才會生效。Bot Control 透過比較目前的流量與 AWS WAF 運算的流量基準，來識別 Web 流量中的異常行為。 規則動作：Block 標籤：<code>aws:waf:managed:aws:bot-control:targeted:aggregate:volumetric:session:maximum</code> 和 <code>aws:waf:managed:aws:bot-control:TGT_VolumetricSessionMaximum</code>

規則名稱	描述
TGT_SignalAutomatedBrowser	檢查未來自己驗證機器人之請求的字符，是否有可能自動化用戶端瀏覽器的指標。如需詳細資訊，請參閱AWS WAF 字符特性。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:bot-control:targeted:signal:automated_browser 和 aws:waf:managed:aws:bot-control:TGT_SignalAutomatedBrowser
TGT_SignalBrowserAutomationExtension	檢查不是來自自己驗證機器人的請求，指出存在協助自動化的瀏覽器延伸模組，例如 Selenium IDE。每當使用者安裝這種類型的延伸模組時，即使他們沒有主動使用，此規則都會相符。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA 和 新增至請求 Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:bot-control:targeted:signal:browser_automation_extension 和 aws:waf:managed:aws:bot-control:TGT_SignalBrowserAutomationExtension

規則名稱	描述
TGT_SignalBrowserInconsistency	檢查來自已驗證機器人的請求是否有不一致的瀏覽器查詢資料。如需詳細資訊，請參閱AWS WAF 字符特性。 此檢查僅適用於 Web 請求具有字符的情況。權杖會由應用程式整合 SDKs 和規則動作 CAPTCHA和 新增至請求Challenge。如需詳細資訊，請參閱用於 AWS WAF 智慧型威脅緩解的字符。 規則動作：CAPTCHA 標籤：aws:waf:managed:aws:bot-control:targeted:signal:browser_inconsistency 和 aws:waf:managed:aws:bot-control:TGT_SignalBrowserInconsistency

規則名稱	描述
TGT_ML_CoordinatedActivityLow, TGT_ML_CoordinatedActivityMedium, TGT_ML_CoordinatedActivityHigh	檢查來自已驗證機器人的請求是否有與分散式、協調機器人活動一致的異常行為。規則層級表示一組請求是協同攻擊參與者的可信度層級。  Note 只有在規則群組設定為使用機器學習 (ML) 時，才會執行這些規則。如需設定此選項的詳細資訊，請參閱 將 AWS WAF Bot Control 受管規則群組新增至 Web ACL。  Note 這些規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 AWS WAF 透過網站流量統計資料的機器學習分析來執行此檢查。會每幾分鐘 AWS WAF 分析一次 Web 流量，並最佳化分析，以偵測分散在許多 IP 地址的低強度、長時間機器人。 這些規則在判斷協調式攻擊尚未進行之前，可能會在非常少量的請求上相符。因此，如果您只看到一兩個相符項目，則結果可能是誤報。不過，如果您看到這些規則出現許多相符項目，則可能正經歷協同攻擊。

規則名稱	描述
	 Note 在您使用 ML 選項啟用 Bot Control 目標規則後，這些規則最多可能需要 24 小時才會生效。Bot Control 會將目前的流量與已計算的 AWS WAF 流量基準進行比較，藉此識別 Web 流量中的異常行為。當您使用 Bot Control 目標規則搭配 ML 選項時，AWS WAF 只會計算基準，而且最多可能需要 24 小時才能建立有意義的基準。 我們會定期更新這些規則的機器學習模型，以改善機器人預測。如果您注意到這些規則所做的機器人預測突然發生重大變更，請聯絡您的客戶經理或在 AWS 支援 Center 開立案例。 規則動作： • 低：Challenge • 中型：CAPTCHA • 高：CAPTCHA 標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:coordinated_activity: <i>low/medium/high</i> 和 aws:waf:managed:aws:bot-control:TGT_ML_CoordinatedActivity <i>Low/Medium/High</i>

規則名稱	描述
TGT-TokenReuseIpLow ,TGT-TokenReuseIpMedium ,TGT-TokenReuseIpHigh	檢查未來自己驗證機器人的請求，以在過去 5 分鐘內在多個 IPs 中使用單一字符。每個層級都有不同 IPs 的數量限制： • 低：超過 3 • 中：超過 4 • 高：超過 8  Note 這些規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作： • 低：Count • 中型: CAPTCHA • 高: Block 標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:volume:metric:session:token_reuse:ip: <i>low/medium/high</i> 和 aws:waf:managed:aws:bot-control:TGT-TokenReuseIp <i>Low/Medium/High</i>

規則名稱	描述
TGT_TokenReuseCountryLow , TGT_TokenReuseCountryMedium , TGT_TokenReuseCountryHigh	檢查未來自己驗證機器人的請求，是否在過去 5 分鐘內跨多個國家使用單一字符。每個層級都有不同國家/地區的數量限制： • 低：超過 1 • 中：超過 2 • 高：超過 3  Note 這些規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作： • 低：Count • 中型: CAPTCHA • 高: Block 標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:volume:metric:session:token_reuse:country: <i>low/medium/high</i> 和 aws:waf:managed:aws:bot-control:TGT_TokenReuseCountry <i>Low/Medium/High</i>

規則名稱	描述
TGT-TokenReuseAsnLow , TGT-TokenReuseAsnMedium , TGT-TokenReuseAsnHigh	檢查未來自己驗證機器人的請求，是否在過去 5 分鐘內跨多個聯網自動系統編號 (ASNs) 使用單一字符。每個層級都有不同 ASNs 的數量限制： • 低：超過 1 • 中：超過 2 • 高：超過 3  Note 這些規則套用的閾值可能因延遲而略有不同。在套用規則動作之前，有些請求可能會使其超過限制。 規則動作： • 低：Count • 中型：CAPTCHA • 高：Block 標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:volume:metric:session:token_reuse:asn: <i>low/medium/high</i> 和 aws:waf:managed:aws:bot-control:TGT-TokenReuseAsn <i>Low/Medium/High</i>

AWS WAF 分散式阻斷服務 (DDoS) 預防規則群組

本節說明 AWS WAF 受管規則群組，用於防範分散式阻斷服務 (DDoS) 攻擊。

VendorName : AWS、Name : AWSManagedRulesAntiDDoSRuleSet、WCU : 50

Note

本文件涵蓋此受管規則群組的最新靜態版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

反 DDoS 受管規則群組提供規則，可偵測和管理正在參與或可能正在參與 DDoS 攻擊的請求。此外，規則群組會標記它在可能事件期間評估的所有請求。

使用此規則群組的考量事項

此規則群組為進入 DDoS 攻擊資源的 Web 請求提供軟式和硬式緩解。若要偵測不同的威脅層級，您可以將這兩種緩解類型的敏感度調整為高、中或低可疑層級。

- 軟性緩解 – 規則群組可以傳送靜音瀏覽器挑戰，以回應可處理挑戰間質的請求。如需執行挑戰需求的相關資訊，請參閱 [CAPTCHA 和 Challenge 動作行為](#)。
- 硬性緩解 – 規則群組可以完全封鎖請求。

如需規則群組運作方式及設定方式的詳細資訊，請參閱 [使用反 DDoS 受管規則群組的進階 AWS WAF 反 DDoS 保護](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

此規則群組是中智慧型威脅緩解保護的一部分 AWS WAF。如需相關資訊，請參閱[中的智慧型威脅防禦 AWS WAF](#)。

為了將成本降至最低並最佳化流量管理，請根據最佳實務準則使用此規則群組。請參閱 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 請求，這些請求可供保護套件或 Web ACL 中此規則群組之後執行的規則使用。AWS WAF 也會將標籤記錄到 Amazon CloudWatch 指標。如需標籤和標籤指標的一般資訊，請參閱 [Web 請求標籤](#) 和 [標籤指標和維度](#)。

字符標籤

此規則群組使用 AWS WAF 字符管理，根據其 AWS WAF 字符的狀態來檢查和標記 Web 請求。AWS WAF 使用字符進行用戶端工作階段追蹤和驗證。

如需權杖和權杖管理的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

如需此處所述標籤元件的詳細資訊，請參閱 [中的標籤語法和命名需求 AWS WAF](#)。

用戶端工作階段標籤

標籤 `aws:waf:managed:token:id:identifier` 包含 AWS WAF 字符管理用來識別用戶端工作階段的唯一識別符。如果用戶端取得新的字符，例如在捨棄正在使用的字符之後，識別符可能會變更。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

瀏覽器指紋標籤

標籤 `aws:waf:managed:token:fingerprint:fingerprint-identifier` 包含強大的瀏覽器指紋識別符，權 AWS WAF 杖管理會從各種用戶端瀏覽器訊號運算。此識別符在多次字符擷取嘗試中保持不變。指紋識別符對單一用戶端來說不是唯一的。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

字符狀態標籤：標籤命名空間字首

字符狀態標籤會報告字符的狀態，以及其中包含的挑戰和 CAPTCHA 資訊。

每個字符狀態標籤都以下列其中一個命名空間字首開頭：

- `aws:waf:managed:token:` – 用來報告字符的一般狀態，以及報告字符挑戰資訊的狀態。

- `aws:waf:managed:captcha:` – 用來報告字符 CAPTCHA 資訊的狀態。

字符狀態標籤：標籤名稱

在字首後面，標籤的其餘部分提供詳細的字符狀態資訊：

- `accepted` – 請求字符存在且包含下列項目：
 - 有效的挑戰或 CAPTCHA 解決方案。
 - 未過期的挑戰或 CAPTCHA 時間戳記。
 - 適用於保護套件或 Web ACL 的網域規格。

範例：標籤 `aws:waf:managed:token:accepted` 指出 Web 請求的權杖具有有效的挑戰解決方案、未過期的挑戰時間戳記，以及有效的網域。

- `rejected` – 請求字符存在，但不符合接受條件。

除了拒絕的標籤之外，字符管理還會新增自訂標籤命名空間和名稱，以指出原因。

- `rejected:not_solved` – 字符缺少挑戰或 CAPTCHA 解決方案。
- `rejected:expired` – 權杖的挑戰或 CAPTCHA 時間戳記已過期，根據您的保護套件或 Web ACL 設定的權杖抗擾性時間而定。
- `rejected:domain_mismatch` – 字符的網域不符合您的保護套件或 Web ACL 的字符網域組態。
- `rejected:invalid` – AWS WAF 無法讀取指定的字符。

範例：標籤 `aws:waf:managed:captcha:rejected` 和

`aws:waf:managed:captcha:rejected:expired` 一起指出請求沒有有效的 CAPTCHA 解決方法，因為字符中的 CAPTCHA 時間戳記已超過保護套件或 Web ACL 中設定的 CAPTCHA 字符豁免時間。

- `absent` – 請求沒有字符或字符管理器無法讀取。

範例：標籤 `aws:waf:managed:captcha:absent` 指出請求沒有字符。

反 DDoS 標籤

反 DDoS 受管規則群組會產生具有命名空間字首的標籤，`aws:waf:managed:aws:anti-ddos:` 後面接著任何自訂命名空間和標籤名稱。每個標籤都會反映反 DDoS 調查結果的某些層面。

除了個別規則新增的標籤之外，規則群組還可能將下列多個標籤新增至請求。

- `aws:waf:managed:aws:anti-ddos:event-detected` – 表示請求將傳送至受管規則群組偵測到 DDoS 事件的受保護資源。當資源的流量與資源的流量基準有顯著偏差時，受管規則群組會偵測事件。

當資源處於此狀態時，規則群組會將此標籤新增至資源的每個請求，因此合法流量和攻擊流量會取得此標籤。

- `aws:waf:managed:aws:anti-ddos:ddos-request` – 表示請求來自疑似參與事件的來源。

除了一般標籤之外，規則群組還會新增下列標籤，指出可信度層級。

`aws:waf:managed:aws:anti-ddos:low-suspicion-ddos-request` – 表示可能的 DDoS 攻擊請求。

`aws:waf:managed:aws:anti-ddos:medium-suspicion-ddos-request` – 表示非常可能的 DDoS 攻擊請求。

`aws:waf:managed:aws:anti-ddos:high-suspicion-ddos-request` – 表示非常可能的 DDoS 攻擊請求。

- `aws:waf:managed:aws:anti-ddos:challengeable-request` – 表示請求 URI 能夠處理 Challenge 動作。受管規則群組會將此套用至 URI 未豁免的任何請求。如果 URIs 符合規則群組的豁免 URI 規則表達式，則會豁免 URI。

如需可以接受無提示瀏覽器挑戰之請求需求的相關資訊，請參閱 [CAPTCHA 和 Challenge 動作行為](#)。

您可以透過 API 呼叫 來擷取規則群組的所有標籤 `DescribeManagedRuleGroup`。這些標籤會列在回應的 `AvailableLabels` 屬性中。

Anti-DDoS 受管規則群組會將標籤套用至請求，但不一定會對其採取行動。請求管理取決於規則群組判斷是否參與攻擊的可信度。如果需要，您可以新增在規則群組之後執行的標籤比對規則，來管理規則群組標籤的請求。如需此 和 範例的詳細資訊，請參閱 [AWS WAF 分散式阻斷服務 \(DDoS\) 預防](#)。

反 DDoS 規則清單

本節列出反 DDoS 規則。

Note

本文件涵蓋此受管規則群組的最新靜態版本版本。我們在的 changelog 日誌中報告版本變更[AWS 受管規則變更日誌](#)。如需其他版本的資訊，請使用 API 命令 [DescribeManagedRuleGroup](#)。

我們為 AWS 受管規則規則群組中的規則發佈的資訊旨在為您提供使用規則所需的內容，而不會給予不法份子規避規則所需的內容。

如果您需要比此處更多的資訊，請聯絡 [AWS 支援中心](#)。

規則名稱	描述
ChallengeAllDuringEvent	比對具有目前受到攻擊aws:waf:managed:aws:anti-ddos:challengeable-request 之任何受保護資源標籤的請求。 規則動作：Challenge 您只能將此規則動作覆寫為 Allow或 Count。Allow 不建議使用。對於任何規則動作設定，規則只會比對具有 challengeable-request 標籤的請求。 此規則的組態會影響下一個規則的評估，ChallengeDDoSRequests。AWS WAF only 只會在受管規則群組的 Web ACL 組態中 Count，此規則的動作覆寫設定為 時評估該規則。 如果您的工作負載容易受到未預期的請求量變更影響，我們建議您透過保留的預設動作設定來挑戰所有具有挑戰性的請求Challenge。對於較不敏感的應用程式，您可以將此規則的動作設定為，Count然後使用規則 調整Challenge回應的敏感度ChallengeDDoSRequests。

規則名稱	描述
	標籤：aws:waf:managed:aws:anti-ddos:ChallengeAllDuringEvent
ChallengeDDoSRequests	在資源受到攻擊的期間，比對符合或超過規則群組所設定之挑戰敏感度設定的受保護資源請求。 規則動作：Challenge 您只能將此規則動作覆寫為 Allow 或 Count。Allow 不建議使用。在任何情況下，規則只會比對具有 challengeable-request 標籤的請求。 AWS WAF 只有在您覆寫先前規則 Count 中的動作時，才會評估此規則 ChallengeAllDuringEvent。 標籤：aws:waf:managed:aws:anti-ddos:ChallengeDDoSRequests
DDoSRequests	在資源受到攻擊的期間，比對符合或超過規則群組所設定區塊敏感度設定的受保護資源請求。 規則動作：Block 標籤：aws:waf:managed:aws:anti-ddos:DDoSRequests

版本控制 AWS 受管規則規則群組的部署

本節介紹 AWS 如何將更新部署到 AWS 受管規則規則群組。

AWS 在三個標準部署中，將變更部署至其版本控制的 AWS 受管規則規則群組：發行候選版本、靜態版本和預設版本。此外，AWS 有時可能需要發佈例外狀況部署或復原預設版本部署。

 Note

本節僅適用於版本控制的 AWS 受管規則規則群組。唯一未進行版本控制的規則群組是 IP 評價規則群組。

主題

- [AWS 受管規則規則群組部署的通知](#)
- [AWS 受管規則的標準部署概觀](#)
- [AWS 受管規則的典型版本狀態](#)
- [發佈 AWS 受管規則的候選部署](#)
- [AWS 受管規則的靜態版本部署](#)
- [AWS 受管規則的預設版本部署](#)
- [AWS 受管規則的例外部署](#)
- [AWS 受管規則的預設部署復原](#)

AWS 受管規則規則群組部署的通知

本節說明 Amazon SNS 通知如何與 AWS 受管規則規則群組搭配使用。

版本控制的 AWS 受管規則規則群組都會為部署提供 SNS 更新通知，而且全部都使用相同的 SNS 主題 Amazon Resource Name (ARN)。唯一未進行版本控制的規則群組是 IP 評價規則群組。

對於影響您保護的部署，例如預設版本的變更，AWS 會提供 SNS 通知，通知您計劃的部署，並讓您知道部署何時開始。對於不影響您保護的部署，例如版本候選和靜態版本部署，AWS 可能會在部署開始後或甚至完成之後通知您。完成新靜態版本的部署時，會在變更日誌的 [AWS 受管規則變更日誌](#) 和文件歷史記錄頁面的 [AWS 更新本指南文件歷史紀錄](#)。

若要接收為 AWS 受管規則規則群組 AWS 提供的所有更新，請從本指南的任何 HTML 頁面訂閱 RSS 摘要，並訂閱 AWS 受管規則規則群組的 SNS 主題。如需訂閱 SNS 通知的資訊，請參閱 [收到受管規則群組新版本和更新的通知](#)。

SNS 通知的內容

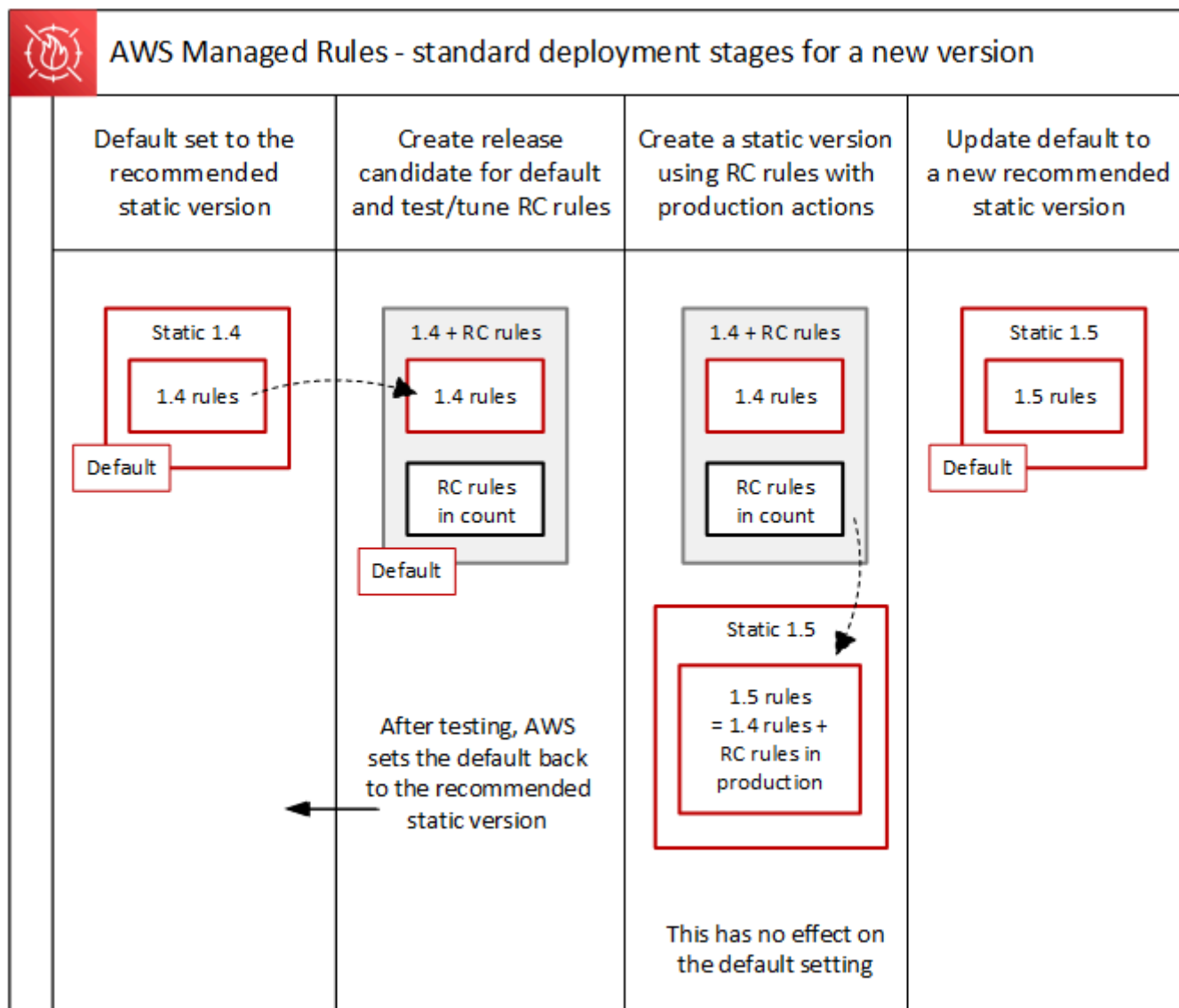
Amazon SNS 通知中的欄位一律包含主旨、訊息和 MessageAttributes。其他欄位取決於訊息的類型，以及通知的受管規則群組。以下顯示的範例通知清單AWSManagedRulesCommonRuleSet。

```
{
  "Type": "Notification",
  "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
  "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
  "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
  "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated the regex specification in this version to improve protection coverage, adding protections against insecure deserialization. For details about this change, see http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
  "Timestamp": "2021-08-24T11:12:19.810Z",
  "SignatureVersion": "1",
  "Signature": "EXAMPLEHXgJm...",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-f3ecfb7224c7233fe7bb5f59f96de52f.pem",
  "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-west-2:123456789012:MyTopic&Token=2336412f37...",
  "MessageAttributes": {
    "major_version": {
      "Type": "String",
      "Value": "v1"
    },
    "managed_rule_group": {
      "Type": "String",
      "Value": "AWSManagedRulesCommonRuleSet"
    }
  }
}
```

AWS 受管規則的標準部署概觀

AWS 使用三個標準部署階段推出新的 AWS 受管規則功能：版本候選、靜態版本和預設版本。

下圖說明這些標準部署。以下各節會更詳細地說明每個項目。

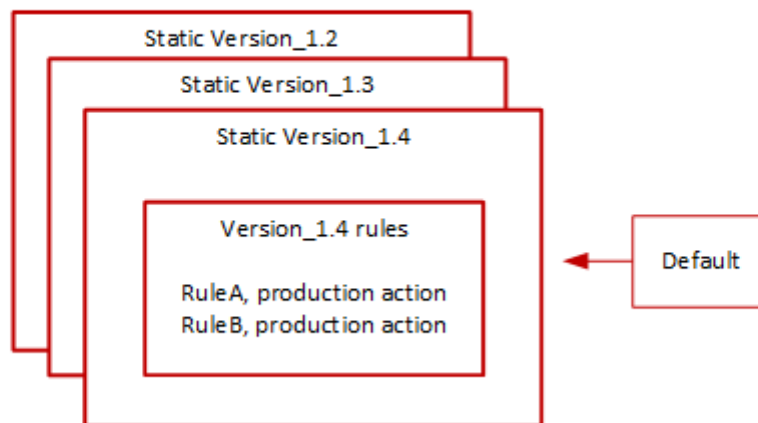


AWS 受管規則的典型版本狀態

一般而言，版本控制的受管規則群組有許多未過期的靜態版本，預設版本會指向 AWS 建議的靜態版本。下圖顯示典型靜態版本集和預設版本設定的範例。



Managed rule group: Version settings



靜態版本中大多數規則的生產動作是 Block，但可能設定為不同。如需規則動作設定的詳細資訊，請參閱 [中每個規則群組的規則清單](#)[AWS 受管規則規則群組清單](#)。

發佈 AWS 受管規則的候選部署

本節說明暫時版本候選部署的運作方式。

當 AWS 具有受管規則群組的候選規則變更集時，它會在暫時發行候選部署中對其進行測試。會根據生產流量 AWS 評估計數模式中的候選規則，並執行最終調校活動，包括緩解誤報。會針對使用規則群組預設版本的所有客戶，以這種方式 AWS 測試發行候選規則。版本候選部署不適用於使用靜態版本規則群組的客戶。

如果您使用預設版本，版本候選部署不會改變規則群組管理 Web 流量的方式。在測試候選規則時，您可能會注意到下列事項：

- 預設版本名稱從 變更為 Default (using Version_X.Y) Default (using Version_X.Y_PLUS_RC_COUNT)。
- Amazon CloudWatch 中的其他計數指標名稱RC_COUNT為 。這些是由版本候選規則產生。

AWS 會測試發行候選版本約一週，然後移除它，並將預設版本重設為目前建議的靜態版本。

AWS 會針對發行候選部署執行下列步驟：

1. 建立版本候選項目 – 根據目前建議的靜態版本 AWS 新增版本候選項目，這是預設值所指的版本。

版本候選名稱是附加 的靜態版本名稱_PLUS_RC_COUNT。例如，如果目前建議的靜態版本是 Version_2.1，則版本候選項目會命名為 Version_2.1_PLUS_RC_COUNT。

版本候選項目包含下列規則：

- 完全從目前建議的靜態版本複製的規則，規則組態不會變更。
- 使用規則動作設定為 Count，並使用以 結尾的名稱來候選新規則_RC_COUNT。

大多數候選規則為規則群組中已存在的規則提供建議的改進。每個規則的名稱都是以 附加的現有規則名稱_RC_COUNT。

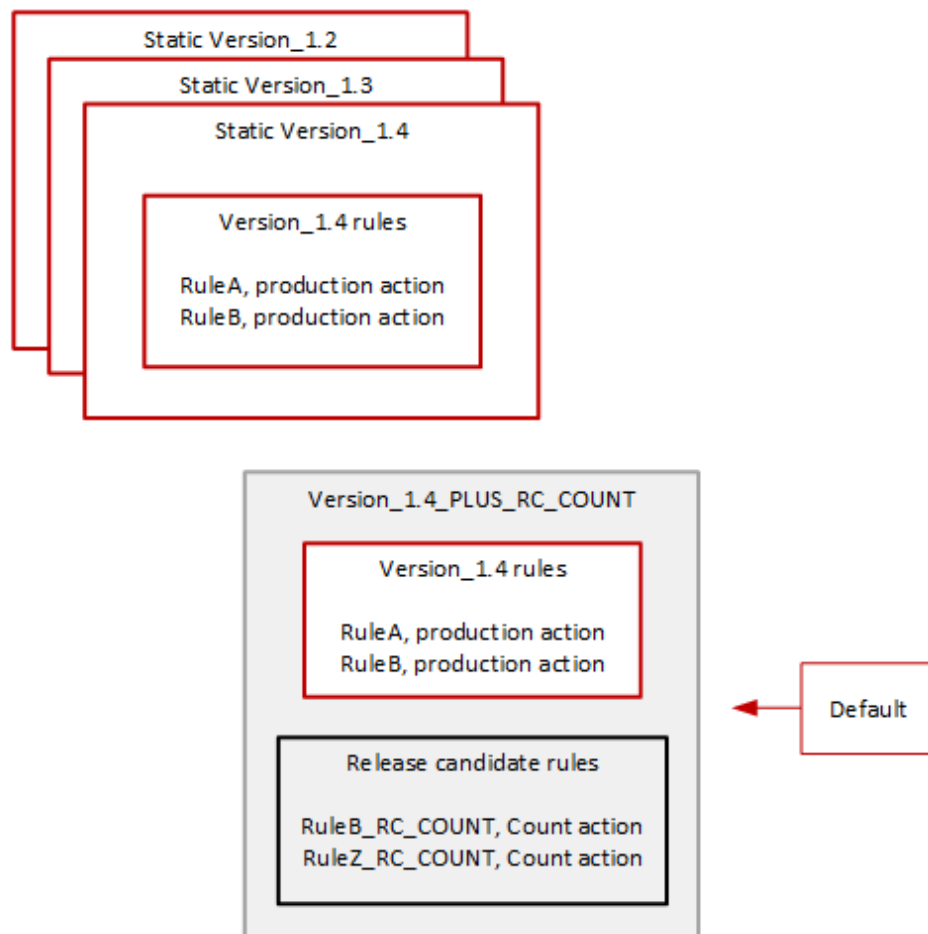
2. 將預設版本設定為發行候選版本，然後測試 – 將預設版本 AWS 設定為指向新的發行候選版本，以針對您的生產流量執行測試。測試通常需要一週的時間。

您會看到預設版本的名稱，從僅指示靜態版本的 變更為指示靜態版本加上發行候選規則Default (using Version_1.4)的 Default (using Version_1.4_PLUS_RC_COUNT)。此命名機制可讓您識別您用來管理 Web 流量的靜態版本。

下圖顯示目前範例規則群組版本的狀態。



Managed rule group: Versions with added release candidate



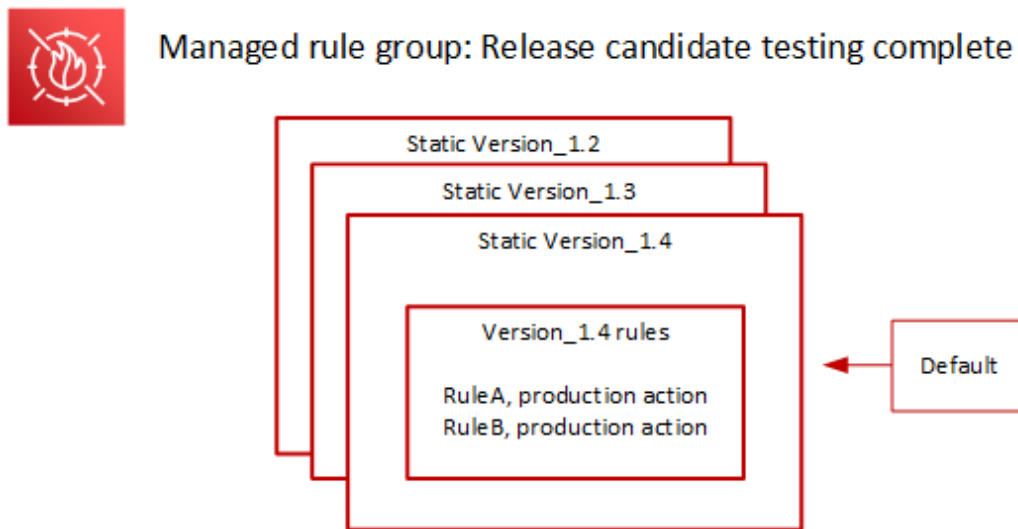
發行候選規則一律使用 Count動作設定，因此不會變更規則群組管理 Web 流量的方式。

發行候選規則會產生 Amazon CloudWatch 計數指標，AWS 用於驗證行為並識別誤報。AWS 會視需要進行調整，以調整發行候選計數規則的行為。

版本候選版本不是靜態版本，您無法從靜態規則群組版本清單中選擇。您只能在預設版本規格中看到版本候選版本的名稱。

3. 將預設版本傳回建議的靜態版本 – 測試版本候選規則之後，會將預設版本 AWS 設回目前的建議靜態版本。預設版本名稱設定會捨棄_PLUS_RC_COUNT結尾，而規則群組會停止為版本候選規則產生 CloudWatch 計數指標。這是無提示的變更，與預設版本復原的部署不同。

下圖顯示範例規則群組版本在版本候選項目測試完成後的狀態。



時間和通知

AWS 會視需要部署版本候選版本，以測試規則群組的改進。

- SNS – 在部署開始時 AWS 傳送 SNS 通知。通知指出測試版本候選項目的預估時間。測試完成時，會以 AWS 無提示方式將預設值傳回靜態版本設定，而不需要第二次通知。
- 變更日誌 – AWS 不會更新此部署類型的變更日誌或本指南的其他部分。

AWS 受管規則的靜態版本部署

當 AWS 判斷版本候選項目為規則群組提供寶貴的變更時，會根據版本候選項目為規則群組 AWS 部署新的靜態版本。此部署不會變更規則群組的預設版本。

新的靜態版本包含來自 版本候選項目的下列規則：

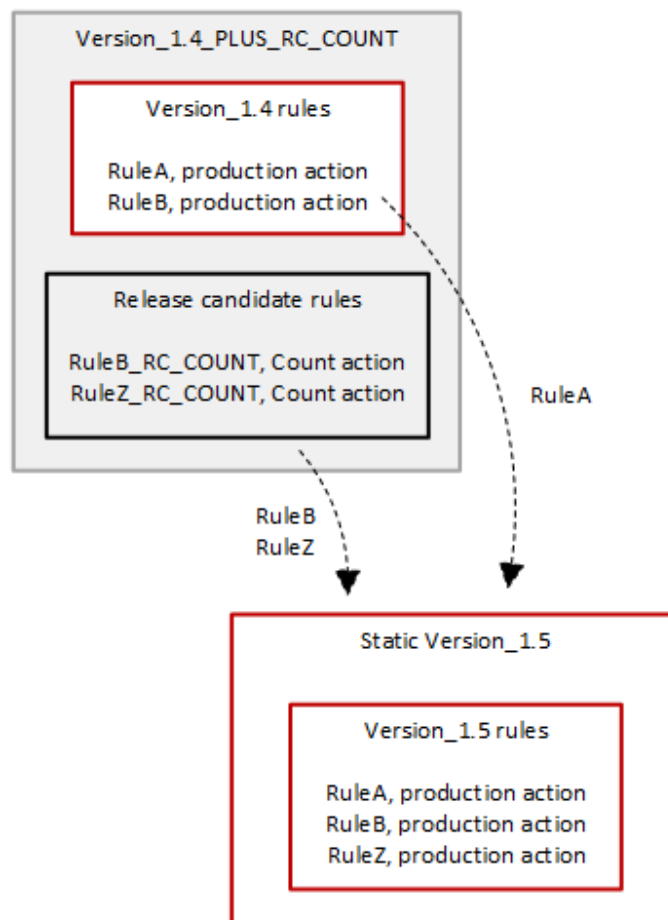
- 來自先前靜態版本的規則，在發行候選規則之間沒有替代候選項目。
- 發行候選規則，變更如下：
 - AWS 會移除版本候選詞尾碼 來變更規則名稱_RC_COUNT。
 - AWS 會將規則動作從 Count 變更為其生產規則動作。

對於取代先前現有規則的版本候選規則，這會取代新靜態版本中先前規則的功能。

下圖描述從 版本候選項目建立新的靜態版本。



Managed rule group: Create a new static version with tested release candidate rules



部署之後，新的靜態版本可供您測試，並在需要時用於您的保護。您可以在 的規則群組規則清單中檢閱新的和更新的規則動作和描述[AWS 受管規則規則群組清單](#)。

部署之後，靜態版本是不可變的，而且只會在 AWS 過期時變更。如需版本生命週期的相關資訊，請參閱 [在中使用版本控制的受管規則群組 AWS WAF](#)。

時間和通知

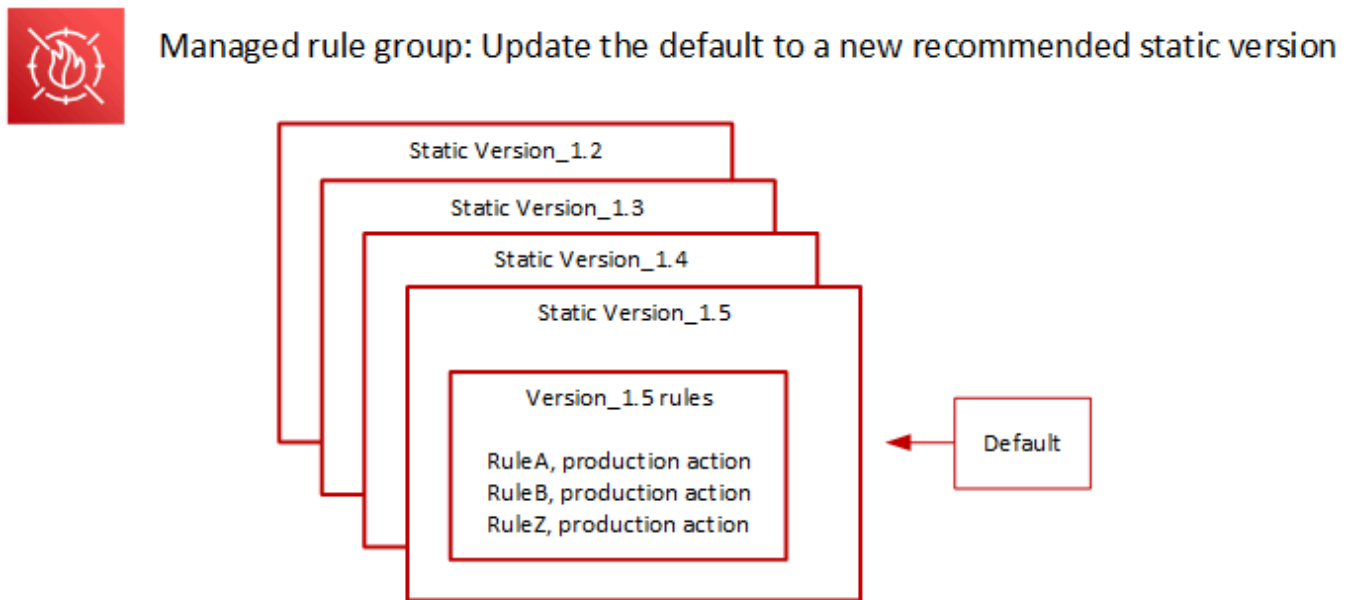
AWS 會視需要部署新的靜態版本，以部署規則群組功能的改善。部署靜態版本不會影響預設版本設定。

- SNS – 在部署完成時 AWS 傳送 SNS 通知。
- 變更日誌 – 部署在 AWS WAF 可用的地方完成後，會視需要 AWS 更新本指南中的規則群組定義，然後在 AWS 受管規則群組變更日誌和文件歷史記錄頁面中宣告版本。

AWS 受管規則的預設版本部署

當 AWS 判斷新的靜態版本相較於目前的預設值，為規則群組提供更好的保護時，會將預設版本 AWS 更新為新的靜態版本。在將多個靜態版本提升為規則群組的預設版本之前，AWS 可能會發行多個靜態版本。

下圖顯示將預設版本設定 AWS 移至新的靜態版本之後，範例規則群組版本的狀態。



在將此變更部署到預設版本之前，AWS 會提供通知，以便您可以測試和準備即將進行的變更。如果您使用預設版本，則無法採取任何動作，並在更新期間保留在其中。如果您想要延遲切換到新版本，您可以在預設版本部署的計劃開始之前，明確設定規則群組，以使用預設值設為的靜態版本。

時間和通知

AWS 當 為規則群組建議與目前使用中的 不同的靜態版本時， 會更新預設版本。

- SNS – 在目標部署日至少一週前 AWS 傳送 SNS 通知，然後在部署日當天的部署開始時傳送 SNS 通知。每個通知都包含規則群組名稱、預設版本要更新的靜態版本、部署日期，以及執行更新之每個 AWS 區域的部署排程時間。
- 變更日誌 – AWS 不會更新此部署類型的變更日誌或本指南的其他部分。

AWS 受管規則的例外部署

AWS 可能會略過標準部署階段，以快速部署可解決重大安全風險的更新。例外狀況部署可能涉及任何標準部署類型，而且可能會快速跨 AWS 區域推出。

AWS 會盡可能為例外狀況部署提供提前通知。

時間和通知

AWS 只會在需要時執行例外狀況部署。

- SNS – 盡可能在目標部署日期之前 AWS 傳送 SNS 通知，然後在部署開始時傳送另一個 SNS 通知。每個通知都包含規則群組名稱、正在進行的變更，以及部署日期。
- 變更日誌 – 如果部署適用於靜態版本，則在部署完成之後，視需要 AWS WAF AWS 更新本指南中的規則群組定義，然後在 AWS 受管規則群組變更日誌和文件歷史記錄頁面中宣告版本。

AWS 受管規則的預設部署復原

在特定情況下，AWS 可能會將預設版本復原為先前的設定。所有 AWS 區域的復原通常需要不到 10 分鐘的時間。

AWS 只會執行復原來緩解靜態版本中的重大問題，例如無法接受的高誤報層級。

在復原預設版本設定之後，會 AWS 加快具有問題的靜態版本的過期時間，以及發行新的靜態版本來解決問題。

時間和通知

AWS 只會在需要時執行預設版本復原。

- SNS – 在復原時 AWS 傳送單一 SNS 通知。通知包含規則群組名稱、預設版本所設定的版本，以及部署日期。此部署類型非常快速，因此通知不會提供 區域的計時資訊。

- 變更日誌 – AWS 不會更新此部署類型的變更日誌或本指南的其他部分。

AWS 受管規則變更日誌

本節列出自 2019 年 11 月發行 AWS WAF 以來的 AWS 受管規則變更。

Note

此變更日誌會報告 AWS 受管規則中規則和規則群組的變更 AWS WAF。

對於 [IP 評價規則群組](#)，此變更日誌會報告規則和規則群組的變更，並報告規則使用的 IP 地址清單來源的重大變更。由於這些清單的動態性質，它不會報告 IP 地址清單本身的變更。如果您對 IP 地址清單有任何疑問，請聯絡您的客戶經理或在 [AWS 支援 Center](#) 開立案例。

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組	此規則群組已發行靜態版本 1.18。	2025-06-18
- CrossSiteScripting_BODY - CrossSiteScripting_COOKIE - CrossSiteScripting_QUERYARGUMENTS - CrossSiteScripting_URI_PATH	改善跨網站指令碼規則的偵測簽章。	
AWS WAF 機器人控制規則群組	此規則群組已發行靜態 3.2 版。	2025-05-29
新標籤： 搜尋引擎機器人：	新增列出的新標籤。	

規則群組和規則	描述	日期
- aws-waf:managed:aws-bot-control:bot:name:evening - aws-waf:managed:aws-bot-control:bot:name:youspider - AI 機器人： - aws-waf:managed:aws-bot-control:bot:name:searchbot - aws-waf:managed:aws-bot-control:bot:name:nova_act - AI 機器人的組織標籤： - aws-waf:managed:aws-bot-control:bot:organization:openai - aws-waf:managed:aws-bot-control:bot:organization:marfeel		

規則群組和規則	描述	日期
- aws-waf:managed:aws-bot-control:bot:organization:facebook - aws-waf:managed:aws-bot-control:bot:organization:metaexternalagent - aws-waf:managed:aws-bot-control:bot:organization:amazon - 內容擷取器機器人： - aws-waf:managed:aws-bot-control:bot:name:google_cloud_vertex_bot - 雲端服務供應商訊號： - aws-waf:managed:aws-bot-control:signal:cloud_s		

規則群組和規則	描述	日期
ervice_provider:alibaba		
核心規則集 (CRS) 受管規則群組 - CrossSiteScripting_BODY - CrossSiteScripting_COOKIE - CrossSiteScripting_QUERYARGUMENTS - CrossSiteScripting_URI_PATH	已發行此規則群組的靜態版本 1.17。 改善跨網站指令碼規則的偵測簽章。	2025-03-03

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 新標籤： - 搜尋引擎機器人： - aws-waf:managed:aws-bot-control:bot:name:evensearchbot - aws-waf:managed:aws-bot-control:bot:name:yisouspider - AI 機器人： - aws-waf:managed:aws-bot-control:bot:name:searchbot - aws-waf:managed:aws-bot-control:bot:name:nova_act - AI 機器人的組織標籤： - aws-waf:managed:aws-bot-control:bot:org:	此規則群組已發行靜態 3.2 版。 新增列出的新標籤。	2025-05-29

規則群組和規則	描述	日期
- organization:openai - aws:waf:managed:aws:bot-control:bot:organization:marfeel - aws:waf:managed:aws:bot-control:bot:organization:facebook - aws:waf:managed:aws:bot-control:bot:organization:metaexternalagent - aws:waf:managed:aws:bot-control:bot:organization:amazon - 內容擷取器機器人： - aws:waf:managed:aws:bot-control:bot:name:google		

規則群組和規則	描述	日期
e_cloud_v ertex_bot - 雲端服務供應商訊號： - awsmaf:managed:aws:bot-control:signal:cloud_service_provider:alibaba		
核心規則集 (CRS) 受管規則群組 - CrossSiteScripting_BODY - CrossSiteScripting_COOKIE - CrossSiteScripting_QUERYARGUMENTS - CrossSiteScripting_URI_PATH	已發行此規則群組的靜態版本 1.17。 改善跨網站指令碼規則的偵測簽章。	2025-03-03

規則群組和規則	描述	日期
SQL 資料庫受管規則群組 - SQLi_COOKIE - SQLi_URIPATH - SQLi_QUERYARGUMENTS - SQLi_BODY	此規則群組已發行靜態版本 1.3。 已將雙URL_DECODE_UNI 文字轉換新增至列出的規則。	2025-01-24
Linux 作業系統受管規則群組 - LFI_HEADER - LFI_URIPATH - LFI_QUERYSTRING	此規則群組已發行靜態 2.6 版。 新增簽章以改善偵測。	2025-01-24
AWS WAF 機器人控制規則群組 機器人控制標籤中的新機器人名稱標籤：aws:waf:managed:aws:bot-control:bot::name:nyt:imes	此規則群組已發行靜態 3.1 版。 已將 New York Times 標籤新增至機器人名稱標籤清單。	2024-11-07

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_URI_PATH	此規則群組已發行靜態版本 1.16。 改善跨網站指令碼規則的偵測簽章。	2024-10-16

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 新規則： - TGT_TokenAbsent - TGT_VolumetricSessionMaximum - TGT_SignalBrowserAutomationExtension - TGT_ML_CoordinatedActivityLow、TGT_ML_CoordinatedActivityMedium 與 TGT_ML_CoordinatedActivityHigh - TGT_TokenReuseIpLow、TGT_TokenReuseIpMedium 與 TGT_TokenReuseIpHigh - TGT_TokenReuseAsnLow、TGT_TokenReuseAsnMedium 與 TGT_TokenReuseAsnHigh - TGT_TokenReuseCountryLow、TGT_TokenReuseCountryMedium 與 TGT_TokenReuseCountryHigh	此規則群組的發行靜態版本 2.0 和 3.0。2.0 版與 3.0 版相同，但所有新規則的規則動作都設為 Count。本指南會記錄每個規則群組的最新版本。 新增列出的新規則。 已更新標籤，以便所有規則套用模式為 的標籤aws:waf:managed:aws:bot-control: <i><RuleName></i>。 已將雲端服務供應商標籤新增至 Bot Control 訊號標籤。 新增由機器人類別規則檢查的新機器人名稱標籤。	2024-09-13

規則群組和規則	描述	日期
已刪除的規則： • TGT_TokenReuseIp 。以對應的新低、中和高規則取代。 新標籤： • HTTP 程式庫機器人： • awswaf:managed:aws:bot-control:bot:name:fasthttp • AI 機器人： • awswaf:managed:aws:bot-control:bot:name:bedrockbot • awswaf:managed:aws:bot-control:bot:name:claudebot • awswaf:managed:aws:bot-control:bot:name:anthropic • awswaf:managed:aws:bot-control:bot:name:metaxternalagent • awswaf:managed:aws:bot-		

規則群組和規則	描述	日期
control:bot:n ame:bytespider - awsmaf:ma naged:aws:bot- control:bot:n ame:omgili - awsmaf:ma naged:aws:bot- control:bot:n ame:diffbot - awsmaf:ma naged:aws:bot- control:bot:n ame:perplexitybot - awsmaf:ma naged:aws:bot- control:bot:n ame:timpibot - awsmaf:ma naged:aws:bot- control:bot:n ame:cohere - 搜尋引擎機器人： - awsmaf:ma naged:aws:bot- control:bot:n ame:naver - 廣告機器人： - awsmaf:ma naged:aws:bot- control:bot:n ame:naver_ads - 社交媒體機器人：		

規則群組和規則	描述	日期
• awswaf:managed:aws:bot-control:bot:name:snapchat • 內容擷取器機器人 : • awswaf:managed:aws:bot-control:bot:name:naver_preview • awswaf:managed:aws:bot-control:bot:name:censys • awswaf:managed:aws:bot-control:bot:name:imessage_preview • awswaf:managed:aws:bot-control:bot:name:imagesift • 雲端服務供應商訊號 : • awswaf:managed:aws:bot-control:signal:cloud_service_provider:aws • awswaf:managed:aws:bot-control:signal:cloud_s		

規則群組和規則	描述	日期
ervice_pr ovider:azure • awswaf:managed:aws:bot-control:signal:cloud_service_provider:gcp • awswaf:managed:aws:bot-control:signal:cloud_service_provider:oracle • awswaf:managed:aws:bot-control:signal:cloud_service_provider:digital_ocean • awswaf:managed:aws:bot-control:signal:cloud_service_provider:akamai • awswaf:managed:aws:bot-control:signal:cloud_service_provider:cloudflare		

規則群組和規則	描述	日期
aws:waf:managed:aws:bot-control:signal:cloud_service_provider:ibm_cloud 現有規則中的其他標籤。		
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 所有規則	此規則群組已發行靜態版本 1.1。 已更新標籤，以便所有規則套用模式為 的標籤aws:waf:managed:aws:atp: <i><RuleName></i> 。	2024-09-13
AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 規則群組 所有規則	此規則群組已發行靜態版本 1.1。 已更新標籤，以便所有規則套用模式為 的標籤aws:waf:managed:aws:acfp: <i><RuleName></i> 。	2024-09-13
Linux 作業系統受管規則群組 所有規則	此規則群組已發行靜態 2.5 版。 新增簽章以改善偵測。	2024-09-02

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 - GenericLFI_QUERYARGUMENTS - GenericLFI_URI_PATH - GenericLFI_BODY	此規則群組的發行靜態版本 1.15。 已改善一般 LFI 規則的偵測簽章。	2024-08-30
Windows 作業系統受管規則群組 - WindowsShellCommands_QUERYARGUMENTS - WindowsShellCommands_BODY - WindowsShellCommands_COOKIE	此規則群組已發行靜態 2.3 版。 已調整所列規則中的偵測簽章，以減少誤報。	2024-08-28
WordPress 應用程式受管規則群組 WordPressExploitableCommands_QUERYSTRING	此規則群組已發行靜態版本 1.3。 已將 JS_DECODE 文字轉換新增至列出的規則。	2024-07-15
Linux 作業系統受管規則群組 LFI_QUERYSTRING	此規則群組已發行靜態 2.4 版。 已將 JS_DECODE 文字轉換新增至列出的規則。	2024-07-12

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_QUERYARGUMENTS • GenericLFI_QUERYARGUMENTS • GenericLFI_BODY • RestrictedExtensions_QUERYARGUMENTS • GenericRFI_QUERYARGUMENTS • GenericRFI_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_URI_PATH	此規則群組已發行靜態版本 1.14。 已將 JS_DECODE 文字轉換新增至列出的規則。	2024-07-09
PHP 應用程式受管規則群組 • PHPHighRiskMethodsVariables_BODY • PHPHighRiskMethodsVariables_QUERYSTRING	此規則群組的發行靜態版本 2.1。 已將 JS_DECODE 文字轉換新增至列出的規則。	2024-07-03

規則群組和規則	描述	日期
Windows 作業系統受管規則群組 - WindowsShellCommands_QUERYARGUMENTS - WindowsShellCommands_BODY - PowerShellCommands_QUERYARGUMENTS - PowerShellCommands_BODY	此規則群組已發行靜態 2.2 版。 已將 JS_DECODE 文字轉換新增至列出的規則。	2024-07-03
Linux 作業系統受管規則群組 所有規則	此規則群組已發行靜態 2.3 版。 新增簽章以改善偵測。	2024-06-06

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 規則群組	機器人和詐騙規則群組現在已進行版本控制。如果您使用這些規則群組，則此更新不會變更它們處理 Web 流量的方式。 此更新會將目前的規則群組版本設定為靜態版本 1.0，並將預設版本設定為指向該版本。 如需版本控制受管規則的詳細資訊，請參閱下列內容： • 在 中 使用版本控制的受管規則群組 AWS WAF • 版本控制 AWS 受管規則規則群組的部署 • 收到受管規則群組新版本和更新的通知	2024-05-29

規則群組和規則	描述	日期
POSIX 作業系統受管規則群組	此規則群組已發行靜態版本 3.0。 • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY 已移除並將其UNIXShellCommandsVariables_QUERYARGUMENTS 取代為 UNIXShellCommandsVariables_QUERYSTRING 。如果您在 的標籤上有相符的規則UNIXShellCommandsVariables_QUERYARGUMENTS ，當您使用此版本時，請將它們切換為在 的標籤上相符UNIXShellCommandsVariables_QUERYSTRING 。新標籤為 awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString 。 新增規則 UNIXShellCommandsVariables_HEADER ，符合所有標頭。 以改善的偵測邏輯更新受管規則群組中的所有規則。 更正 標籤的記錄大小寫UNIXShellCommandsVariables_BODY 。	2024-05-28

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 CrossSiteScripting*	此規則群組已發行靜態版本 1.12。 新增所有跨網站指令碼規則的簽章，以改善偵測並減少誤判。	2024-05-21
SQL 資料庫受管規則群組 - SQLi_BODY - SQLi_QUERYARGUMENTS - SQLiExtendedPatterns_QUERYARGUMENTS	此規則群組已發行靜態版本 1.2。 已將JS_DECODE 文字轉換新增至列出的規則。	2024-05-14
已知錯誤輸入受管規則群組 - JavaDeserializationRCE_BODY - JavaDeserializationRCE_QUERYSTRING - Log4JRCE_QUERYSTRING - Log4JRCE_BODY - Log4JRCE_HEADER	此規則群組已發行靜態版本 1.22。 已將JS_DECODE 文字轉換新增至列出的規則。	2024-05-08
POSIX 作業系統受管規則群組	此規則群組已發行靜態 2.2 版。 將JS_DECODE 文字轉換新增至這兩個規則。	2024-05-08

規則群組和規則	描述	日期
Windows 作業系統受管規則群組 PowerShellCommands_BODY	此規則群組的發行靜態版本 2.1。 新增簽章至 PowerShellCommands_BODY 以改善偵測。	2024-05-03
Amazon IP 評價清單受管規則群組 AWSManagedIPReputationList	更新 IP 評價清單的來源，以改善主動從事惡意活動的地址識別，並減少誤報。 此更新不涉及新版本，因為此規則群組未進行版本控制。	2024-03-13
已知錯誤輸入受管規則群組	此規則群組已發行靜態版本 1.21。 新增簽章以改善偵測並減少誤報。	2023-12-16
已知錯誤輸入受管規則群組 ExploitablePaths_URI_PATH	此規則群組的發行靜態版本 1.20。 更新ExploitablePaths_URI_PATH 規則，為符合 Atlassian Confluence CVE-2023-22518 不當授權漏洞的請求新增偵測。此漏洞會影響 Confluence 資料中心和伺服器的所有版本。如需詳細資訊，請參閱 NIST：國家漏洞資料庫：CVE-2023-22518 詳細資訊。	2023-12-14

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 CrossSiteScripting*	此規則群組已發行靜態版本 1.11。 新增所有跨網站指令碼規則的簽章，以改善偵測並減少誤判。	2023-12-06
AWS WAF 機器人控制規則群組 新標籤：aws:waf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low	將協調活動低標籤新增至規則群組的目標保護層級標籤。此標籤未與任何規則相關聯。此標籤是中、高階規則和標籤的補充。	2023-12-05
機器人控制標籤 標籤：aws:waf:managed:aws:bot-control:targeted:signal:browser_automation_extension	已將訊號標籤新增至規則群組，指出協助自動化的瀏覽器延伸模組偵測。此標籤並非專屬於個別規則。	2023-11-14
核心規則集 (CRS) 受管規則群組 EC2MetaDataSSRF_QUERYARGUMENTS	此規則群組已發行靜態版本 1.10。 更新了一項規則，以改善偵測並減少誤報。	2023-11-02

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 - EC2MetaDataSSRF_BODY - EC2MetaDataSSRF_COOKIE - EC2MetaDataSSRF_URI_PATH - EC2MetaDataSSRF_QUERY_ARGUMENTS	此規則群組已發行靜態版本 1.9。 更新規則以改善偵測並減少誤報。	2023-10-30
POSIX 作業系統受管規則群組 UNIXShellCommandsVariables_QUERY_ARGUMENTS	此規則群組已發行靜態 2.1 版。 更新查詢引數規則以改善偵測。	2023-10-12
核心規則集 (CRS) 受管規則群組 - GenericLFI_QUERY_ARGUMENTS - GenericLFI_URI_PATH - RestrictedExtensions_URI_PATH - RestrictedExtensions_QUERY_ARGUMENTS	此規則群組已發行靜態版本 1.8。 更新規則以改善偵測。	2023-10-11

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 ExploitablePaths_U RIPATH	例外狀況部署：已發行此規則群組的靜態版本 1.19。更新預設版本以使用 1.19 版。 更新ExploitablePaths_U RIPATH 規則，為符合 Atlassian Confluence CVE-2023-22515 權限提升漏洞的請求新增偵測。此漏洞會影響部分版本的 Atlassian Confluence。如需詳細資訊，請參閱 NIST：國家漏洞資料庫：CVE-2023-22515 詳細資訊和 Atlassian Support：CVE-2023-22515 常見問答集。 如需此部署類型的詳細資訊，請參閱 AWS 受管規則的例外部署。	2023-10-04
已知錯誤輸入受管規則群組 - Host_localhost_HEADER - Log4J* - JavaDeserializatio n*	例外狀況部署：已發行此規則群組的靜態 1.18 版。這是此靜態版本的快速推出，以適應 1.19 版的建立和推出。 更新Host_localhost_HEADER 規則和所有 Log4J 和 Java 還原序列化規則，以改善偵測。 如需此部署類型的詳細資訊，請參閱 AWS 受管規則的例外部署。	2023-10-04

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 - TGT_TokenReuseIp - TGT_ML_CoordinatedActivityMedium - TGT_ML_CoordinatedActivityHigh	使用 Count動作將規則新增至規則群組。 字符重複使用 IP 規則會偵測和計數跨 IP 地址的字符共用。 協調活動規則使用網站流量的自動化機器學習 (ML) 分析來偵測機器人相關活動。在您的規則群組組態中，您可以選擇不使用 ML。在此版本中，目前使用目標保護層級的客戶可以選擇使用 ML。選擇退出會停用協調活動規則。	2023-09-06
AWS WAF 機器人控制規則群組 CategoryAI	已將規則CategoryAI 新增至規則群組。	2023-08-30

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 - RestrictedExtensions_URI_PATH - RestrictedExtensions_QUERY_ARGUMENTS - EC2MetadataSSRF_COOKIE - EC2MetadataSSRF_QUERY_ARGUMENTS - EC2MetadataSSRF_BODY - EC2MetadataSSRF_URI_PATH	此規則群組的發行靜態版本 1.7。 更新限制延伸模組和 EC2 中繼資料 SSRF 規則，以改善偵測並減少誤判。	2023-07-26
AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 規則群組 新規則群組中的所有規則	新增規則群組 AWSManagedRulesACFPRuleSet 。	2023-06-13
Linux 作業系統受管規則群組 - LFI_HEADER - LFI_URI_PATH - LFI_QUERY_STRING	此規則群組已發行靜態 2.2 版。 新增簽章以改善偵測。	2023-05-22

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 - RestrictedExtensions_URI_PATH - RestrictedExtensions_QUERY_ARGUMENTS - CrossSiteScripting_COOKIE - CrossSiteScripting_QUERY_ARGUMENTS - CrossSiteScripting_BODY - CrossSiteScripting_URI_PATH	此規則群組已發行靜態版本 1.6。 更新跨網站指令碼 (XSS) 和限制延伸規則，以改善偵測並減少誤判。	2023-04-28

規則群組和規則	描述	日期
PHP 應用程式受管規則群組	此規則群組已發行靜態 2.0 版。 - 已更新 PHPHighRiskMethodsVariables_BODY - 已移除 PHPHighRiskMethodsVariables_QUERYARGUMENTS - 已新增 PHPHighRiskMethodsVariables_QUERYSTRING - 已新增 PHPHighRiskMethodsVariables_HEADER 新增簽章以改善所有規則中的偵測。 將規則取代 PHPHighRiskMethodsVariables_QUERYARGUMENTS 為 PHPHighRiskMethodsVariables_QUERYSTRING，它會檢查整個查詢字串，而不只是查詢引數。 新增規則 PHPHighRiskMethodsVariables_HEADER，以擴展涵蓋範圍以包含所有標頭。 更新下列標籤，以符合標準 AWS 受管規則標籤： - 舊名稱：PHPHighRiskMethodsVariables_BODY 新名稱：PHPHighRiskMethodsVariables_Body - 舊名稱：PHPHighRiskMethodsVariables_QUERYARGUMENTS 新名稱：PHPHighRiskMethodsVariables_QueryString	2023-02-27

規則群組和規則	描述	日期
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 - VolumetricIpFailedLoginResponseHigh - VolumetricSessionFailedLoginResponseHigh	新增登入回應檢查規則，以搭配受保護的 Amazon CloudFront 分佈使用。這些規則可以封鎖最近成為太多失敗登入嘗試來源的 IP 地址和用戶端工作階段的新登入嘗試。	2023-02-15
核心規則集 (CRS) 受管規則群組 - NoUserAgent_HEADER - CrossSiteScripting_COOKIE - CrossSiteScripting_QUERYARGUMENTS - CrossSiteScripting_BODY - CrossSiteScripting_URI_PATH	此規則群組已發行靜態版本 1.5。 更新了跨網站指令碼 (XSS) 篩選條件，以改善偵測。	2023-01-25

規則群組和規則	描述	日期
Linux 作業系統受管規則群組 • LFI_COOKIE - 已移除 • LFI_HEADER - 已新增 • LFI_URIPATH • LFI_QUERYSTRING	此規則群組已發行靜態 2.1 版。 已移除規則LFI_COOKIE 及其標籤 awswaf:managed:aws:linux-os:LFI_Cookie，並將它們取代為新規則LFI_HEADER 及其標籤 awswaf:managed:aws:linux-os:LFI_Header。此變更會將檢查擴展到多個標頭。 新增文字轉換和簽章至所有規則，以改善偵測。	2022-12-15
核心規則集 (CRS) 受管規則群組 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	此規則群組已發行靜態 1.4 版。 新增文字轉換至 NoUserAgent_HEADER 以移除所有 null 位元組。更新了跨網站指令碼規則中的篩選條件，以改善偵測。	2022-12-05

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 - JavaDeserializatio nRCE_BODY - JavaDeserializatio nRCE_URI_PATH - JavaDeserializatio nRCE_HEADER - JavaDeserializatio nRCE_QUERYSTRING - Host_localhost_HEA DER	此規則群組的發行靜態版本 1.17。 更新 Java 還原序列化規則，為符合 Apache CVE-2022-42889 的請求新增偵測，這是 Apache Commons Text 1.10.0 之前的 Apache Commons Text 版本中的遠端程式碼執行 (RCE) 漏洞。如需詳細資訊，請參閱 NIST：國家漏洞資料庫：CVE-2022-42889 詳細資訊和 CVE-2022-42889：1.10.0 之前的 Apache Commons Text 允許 RCE 因不安全的插補預設值而套用至不受信任的輸入。 改善 中的偵測Host_loca lhost_HEADER 。	2022-10-20
已知錯誤輸入受管規則群組 - Log4JRCE_HEADER - Log4JRCE_QUERYSTR ING - Log4JRCE_URI_PATH - Log4JRCE_BODY	此規則群組已發行靜態版本 1.16。 移除 1.15 版中 AWS 識別的誤報。	2022-10-05

規則群組和規則	描述	日期
POSIX 作業系統受管規則群組 PHP 應用程式受管規則群組 WordPress 應用程式受管規則群組	更正記錄的標籤名稱。	2022-09-19
IP 評價規則群組 AWSManagedIPDDoSList	此變更不會改變規則群組處理 Web 流量的方式。 根據 Amazon 威脅情報，新增了具有 Count動作的新規則，以檢查是否有正在參與 DDoS 活動的 IP 地址。	2022-08-30

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 - Log4JRCE - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI_PATH - Log4JRCE_BODY - JavaDeserializationRCE_HEADER - JavaDeserializationRCE_BODY - JavaDeserializationRCE_URI_PATH - JavaDeserializationRCE_QUERYSTRING - Host_localhost_HEADER - PROPFIND_METHOD	此規則群組已發行靜態版本 1.15。 移除它Log4JRCE並將其取代為 Log4JRCE_HEADER 、 Log4JRCE_URI 、 Log4JRCE_QUERYSTRING 和 Log4JRCE_BODY ，以更精細地監控和管理誤報。 新增簽章，以改善對所有 和 JavaDeserializationRCE* Log4JRCE* 規則的偵測PROPFIND_METHOD 和封鎖。 更新標籤以更正所有 JavaDeserializationRCE* 規則中的 Host_localhost_HEADER 和 中的大寫。 已更正 的描述JavaDeserializationRCE_HEADER 。	2022-08-22
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 UnsupportedCognitoIDP	新增規則，以防止 Amazon Cognito 使用者集區 Web 流量使用帳戶接管預防受管規則群組。	2022-08-11

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組	AWS 已排定版本 Version_1.2 和規則群組 Version_2.0 的過期時間。版本將於 2022 年 9 月 9 日過期。如需版本過期的資訊，請參閱 在中使用版本控制的受管規則群組 AWS WAF 。	2022-06-09
核心規則集 (CRS) 受管規則群組 - GenericLFI_URI_PATH - GenericRFI_URI_PATH	已發行此規則群組的 1.3 版。此版本會更新規則 GenericLFI_URI_PATH 和 中的配對簽章 GenericRFI_URI_PATH，以改善偵測。	2022-05-24
AWS WAF 機器人控制規則群組 CategoryEmailClient	已將規則 CategoryEmailClient 新增至規則群組。	2022-04-06
已知錯誤輸入受管規則群組 - JavaDeserializationRCE_HEADER - JavaDeserializationRCE_BODY - JavaDeserializationRCE_URI - JavaDeserializationRCE_QUERYSTRING	已發行此規則群組的 1.14 版。四個 JavaDeserializationRCE 規則會移至 Block 模式。	2022-03-31

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 - JavaDeserializationRCE_HEADER_RC_COUNT - JavaDeserializationRCE_BODY_RC_COUNT - JavaDeserializationRCE_URI_RC_COUNT - JavaDeserializationRCE_QUERYSTRING_RC_COUNT	已發行此規則群組的 1.13 版。更新 Spring Core 和 Cloud Function RCE 漏洞的文字轉換。這些規則處於計數模式，以收集指標並評估相符的模式。標籤可用於封鎖自訂規則中的請求。後續版本將以區塊模式使用這些規則進行部署。	2022-03-31

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 - JavaDeserializationRCE_HEADER_RC_COUNT - JavaDeserializationRCE_BODY_RC_COUNT - JavaDeserializationRCE_URI_RC_COUNT - JavaDeserializationRCE_QUERYSTRING_RC_COUNT - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI - Log4JRCE_BODY - Log4JRCE	已發行此規則群組的 1.12 版。新增 Spring Core 和 Cloud Function RCE 漏洞的簽章。這些規則處於計數模式，以收集指標並評估相符的模式。標籤可用於封鎖自訂規則中的請求。後續版本將以區塊模式使用這些規則進行部署。 移除規則 Log4JRCE_HEADER 、 Log4JRCE_QUERYSTRING 、 和 Log4JRCE_URI ， Log4JRCE_BODY 並將它們取代為規則 Log4JRCE。	2022-03-30
IP 評價規則群組 AWSManagedReconnaissanceList	更新AWSManagedReconnaissanceList 規則，將動作從計數變更為區塊。	2022-02-15
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 新規則群組中的所有規則	新增規則群組 AWSManagedRulesATPRuleSet 。	2022-02-11

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 - Log4JRCE - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI - Log4JRCE_BODY	已發行此規則群組的 1.9 版。移除規則並將其Log4JRCE取代為規則 Log4JRCE_HEADER 、Log4JRCE_URI 、Log4JRCE_QUERYSTRING 和 Log4JRCE_BODY ，以彈性使用此功能。新增簽章以改善偵測和封鎖。	2022-01-28
核心規則集 (CRS) - CrossSiteScripting_URI_PATH - CrossSiteScripting_BODY - CrossSiteScripting_QUERY_ARGUMENTS - CrossSiteScripting_COOKIE	已發行此規則群組的 2.0 版。針對這些規則，調校偵測簽章以減少誤判。將URL_DECODE 文字轉換取代為雙URL_DECODE_UNI 文字轉換。新增HTML_ENTITY_DECODE 文字轉換。	2022-01-10
核心規則集 (CRS) - RestrictedExtensions_URI_PATH - RestrictedExtensions_QUERY_ARGUMENTS	作為此規則群組 2.0 版發行的一部分，新增URL_DECODE_UNI 了文字轉換。從 移除URL_DECODE 文字轉換RestrictedExtensions_URI_PATH 。	2022-01-10

規則群組和規則	描述	日期
SQL 資料庫 - SQLi_BODY - SQLi_QUERYARGUMENTS - SQLi_COOKIE - SQLi_URI_PATH - SQLiExtendedPatterns_BODY - SQLiExtendedPatterns_QUERYARGUMENTS	已發行此規則群組的 2.0 版。以雙URL_DECODE 文字轉換取代URL_DECODE_UNI 文字轉換，並新增COMPRESS_WHITE_SPACE 文字轉換。 已將更多偵測簽章新增至SQLiExtendedPatterns_QUERYARGUMENTS 。 已將 JSON 檢查新增至SQLi_BODY 。 新增規則 SQLiExtendedPatterns_BODY 。 已移除規則 SQLi_URI_PATH 。	2022-01-10
已知錯誤輸入 Log4JRCE	發佈規則的 1.8 版Log4JRCE，以改善標頭檢查和相符條件。	2021-12-17
已知錯誤輸入 Log4JRCE	發佈規則的 1.4 版Log4JRCE，以調整相符條件並檢查其他標頭。發行 1.5 版來調整相符條件。	2021-12-11

規則群組和規則	描述	日期
已知錯誤輸入 - Log4JRCE - BadAuthToken_COOKIE_AUTHORIZATION	新增規則 1.2 Log4JRCE 版，以回應 Log4j 中最近揭露的安全問題。如需詳細資訊，請參閱 CVE-2021-44228。此規則會檢查常見 URI 路徑、查詢字串、請求內文的前 8KB，以及常見標頭。規則使用雙URL_DECODE_UNI 文字轉換。發行 1.3 版Log4JRCE，以調整相符條件並檢查其他標頭。 已移除規則 BadAuthTo ken_COOKIE_AUTHORI ZATION 。	2021-12-10

下表列出 2021 年 12 月之前的變更。

規則群組和規則	描述	日期	
Amazon IP 評價清單	AWSManagedReconnaissanceList	在監控/計數模式中新增AWSManagedReconnaissanceList 規則。此規則包含正在對 AWS 資源執行偵察的 IP 地址。	2021-11-23
Windows 作業系統	WindowsShellCommands PowerShellCommands	為 WindowsShell 命令新增了三個新規則：WindowsShellCommands_COOKIE、WindowsSh	2021-11-23

規則群組和規則	描述	日期	
		ellComman ds_QUERYA RGUMENTS 和 WindowsSh ellComman ds_BODY 。 新增新的 PowerShell 規則：PowerShel lCommands _COOKIE 。 透過移除字串 _Set1 和 _Set2 來 重組PowerShel lComands 規則命 名。 已將更全面的偵測簽 章新增至 PowerShel lRules 。 已將URL_DECOD E_UNI 文字轉換新增 至所有 Windows 作業 系統規則。	

規則群組和規則	描述	日期	
Linux 作業系統	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	將雙URL_DECODE 文字轉換取代為雙 URL_DECODE_UNI 。 新增NORMALIZE_PATH_WIN 為第二個文字轉換。 將LFI_BODY規則取代為LFI_COOKIE 規則。 為所有LFI規則新增了更全面的偵測簽章。	2021-11-23
核心規則集 (CRS)	SizeRestrictions_BODY	減少大小限制，以封鎖內文承載大於 8 KB 的 Web 請求。先前，限制為 10 KB。	2021-10-27
核心規則集 (CRS)	EC2MetaDataSSRF_BODY EC2MetaDataSSRF_COOKIE EC2MetaDataSSRF_URIPATH EC2MetaDataSSRF_QUERYARGUMENTS	新增更多偵測簽章。 新增雙重 Unicode URL 解碼以改善封鎖。	2021-10-27

規則群組和規則	描述	日期	
核心規則集 (CRS)	GenericLFI_QUERYARGUMENTS GenericLFI_URI_PATH RestrictExtensions_URI_PATH RestrictExtensions_QUERYARGUMENTS	新增雙重 Unicode URL 解碼以改善封鎖。	2021-10-27
核心規則集 (CRS)	GenericRFI_QUERYARGUMENTS GenericRFI_BODY GenericRFI_URI_PATH	根據客戶意見回饋，更新規則簽章以減少誤判。新增雙重 Unicode URL 解碼以改善封鎖。	2021-10-27
全部	所有規則	已將 AWS WAF 標籤的支援新增至尚未支援標籤的所有規則。	2021-10-25
Amazon IP 評價清單	AWSManagedIPReputationList_xxxx	重組 IP 評價清單、從規則名稱中移除尾碼，以及新增對 AWS WAF 標籤的支援。	2021-05-04

規則群組和規則	描述	日期	
匿名 IP 清單	AnonymousIPList HostingProviderList	新增對 AWS WAF 標籤的支援。	2021-05-04
機器人控制	全部	新增 Bot Control 規則集。	2021-04-01
核心規則集 (CRS)	GenericRFI_QUERYARGUMENTS	新增雙重 URL 解碼。	2021-03-03
核心規則集 (CRS)	RestrictedExtensions_URI_PATH	已改善規則的組態，並新增額外的 URL 解碼。	2021-03-03
管理員保護	AdminProtection_URI_PATH	新增雙重 URL 解碼。	2021-03-03
已知錯誤輸入	ExploitablePaths_URI_PATH	已改善規則的組態，並新增額外的 URL 解碼。	2021-03-03
Linux 作業系統	LFI_QUERYARGUMENTS	已改善規則的組態，並新增額外的 URL 解碼。	2021-03-03
Windows 作業系統	全部	已改善規則的組態。	2020-09-23

規則群組和規則	描述	日期	
PHP 應用程式	PHPHighRiskMethods Variables_QUERYARGUMENTS PHPHighRiskMethods Variables_BODY	將文字轉換從 HTML 解碼變更為 URL 解碼，以改善封鎖。	2020-09-16
POSIX 作業系統	UNIXShell CommandsVariables_QUERYARGUMENTS UNIXShell CommandsVariables_BODY	將文字轉換從 HTML 解碼變更為 URL 解碼，以改善封鎖。	2020-09-16
核心規則集	GenericLFI_QUERYARGUMENTS GenericLFI_URI_PATH GenericLFI_BODY	將文字轉換從 HTML 解碼變更為 URL 解碼，以改善封鎖。	2020-08-07
Linux 作業系統	LFI_URI_PATH LFI_QUERYARGUMENTS LFI_BODY	將文字轉換從 HTML 實體解碼變更為 URL 解碼，以改善偵測和封鎖。	2020-05-19

規則群組和規則	描述	日期	
匿名 IP 清單	全部	中的新規則群組 IP 評價規則群組 可封鎖來自允許混淆檢視器身分之服務的請求，以協助緩解機器人和逃避地理限制。	2020-03-06
WordPress 應用程式	WordPress ExploitableCommand s_QUERYSTRING	能檢查查詢字串中可入侵字串的新規則	2020-03-03
核心規則集 (CRS)	SizeRestrictions_QUERYSTRING SizeRestrictions_Cookie_HEADER SizeRestrictions_BODY SizeRestrictions_URI_PATH	調整大小值限制條件以改善準確性。	2020-03-03
SQL 資料庫	SQLi_URI_PATH	規則現在會檢查訊息 URI。	2020-01-23
SQL 資料庫	SQLi_BODY SQLi_QUERY_ARGUMENTS SQLi_COOKIE	更新的文字轉換。	2019-12-20

規則群組和規則	描述	日期	
核心規則集 (CRS)	CrossSite Scripting _URIPATH CrossSite Scripting_BODY CrossSite Scripting _QUERYARGUMENTS CrossSite Scripting _COOKIE	更新的文字轉換。	2019-12-20

管理您自己的規則群組

您可以建立自己的規則群組，以重複使用在受管規則群組提供項目中找不到或您偏好自行處理的規則集合。

您建立保留規則的規則群組就像保護套件或 Web ACL 一樣，而且您以與保護套件或 Web ACL 相同的方式將規則新增至規則群組。建立自己的規則群組時，必須為其設定不可變的容量上限。

主題

- [建立規則群組](#)
- [編輯規則群組](#)
- [在保護套件或 Web ACL 中使用您的規則群組](#)
- [刪除規則群組](#)
- [共用規則群組](#)

建立規則群組

若要建立新的規則群組，請遵循此頁面上的程序。

建立規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Rule groups (規則群組)，然後選擇 Create rule group (建立規則群組)。
3. 輸入規則的名稱和描述。您將使用這些來識別規則集來管理它並使用它。

請勿使用以 AWS、PreFM、Shield 或開頭的名稱 PostFM。這些字串是預留的，或可能導致與其他服務為您管理的規則群組混淆。請參閱 [辨識其他服務提供的規則群組](#)。

Note

建立規則群組後無法修改名稱。

4. 對於 Region (區域)，選擇您要儲存規則群組的區域。若要在保護套件或保護 Amazon CloudFront 分佈 ACLs 中使用規則群組，您必須使用全域設定。您也可以對區域應用程式使用全域設定。
5. 選擇下一步。
6. 使用規則建置器精靈將規則新增至規則群組，就像您在保護套件或 Web ACL 管理中一樣。唯一的差異是您無法將規則群組新增到另一個規則群組。
7. 針對容量，設定規則群組使用保護套件或 Web ACL 容量單位 (WCUs 的最大值。這是一個不可變的設定。如需 WCU 的相關資訊，請參閱 [中的 Web ACL 容量單位 WCUs](#) AWS WAF。

當您將規則新增至規則群組時，Add rules and set capacity (新增規則和設定容量) 窗格會顯示所需的最小容量，這是根據您已新增的規則而定。您可以使用此項目和對於規則群組的未來計劃，協助評估規則群組將需要的容量。

8. 檢閱規則群組的設定，然後選擇 Create (建立)。

編輯規則群組

若要從規則群組新增或移除規則或變更組態設定，請使用此頁面上的程序存取規則群組。

⚠ 生產流量風險

如果您變更目前在保護套件或 Web ACL 中使用的規則群組，這些變更將影響您使用的保護套件或 Web ACL 行為。請務必在預備或測試環境中測試和調校所有變更，直到您熟悉對流量的

潛在影響為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

編輯規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 選擇您要編輯的規則群組名稱。主控台會帶您前往規則群組的頁面。

Note

如果您沒有看到要編輯的規則群組，請檢查規則群組區段中的區域選擇。對於用於保護 Amazon CloudFront 分佈的規則群組，請使用全域 (CloudFront) 設定。

4. 視需要編輯規則群組。您可以編輯規則群組的可變屬性，類似於您在建立期間所做的操作。主控台會隨心所欲儲存您的變更。

Note

如果您變更規則的名稱，且希望規則的指標名稱反映變更，則也必須更新指標名稱。AWS WAF 當您變更規則名稱時，不會自動更新規則的指標名稱。您可以使用規則 JSON 編輯器，在主控台中編輯規則時變更指標名稱。您也可以透過 APIs 和您用來定義保護套件或 Web ACL 或規則群組的任何 JSON 清單中變更這兩個名稱。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的一個區域中生效，而不會在另一個區域中生效。

- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新的地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

在保護套件或 Web ACL 中使用您的規則群組

若要在保護套件或 Web ACL 中使用規則群組，請在規則群組參考陳述式中將其新增至保護套件或 Web ACL。

生產流量風險

在保護套件或 Web ACL 中部署生產流量的變更之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整更新的規則，然後再啟用它們。如需準則，請參閱[測試和調校您的 AWS WAF 保護](#)。

Note

在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱[中的 Web ACL 容量單位 \(WCUs\)](#)、[AWS WAF](#) 和 [AWS WAF 定價](#)。

使用規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 選擇您要使用的規則群組名稱。
4. 選擇新增規則，然後選擇新增我自己的規則和規則群組。
5. 選擇規則群組，然後從清單中選擇您的規則群組。

在您的保護套件或 Web ACL 中，您可以將個別規則動作設定為 Count 或任何其他動作，以變更規則群組及其規則的行為。這可協助您執行像是測試規則群組、識別規則群組中規則的誤報，以及自訂受管規則群組如何處理您的請求。如需詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。

如果您的規則群組包含以速率為基礎的陳述式，則您使用規則群組的每個保護套件或 Web ACL 都有自己的個別速率追蹤和管理以速率為基礎的規則，與您使用規則群組的任何其他保護套件或 Web ACL 無關。如需詳細資訊，請參閱[在中使用以速率為基礎的規則陳述式 AWS WAF](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到資源存放的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

刪除規則群組

遵循本節中的指引來刪除規則群組。

刪除參考的集合和規則群組

當您刪除可在保護套件或 Web ACL 中使用的實體，例如 IP 集、regex 模式集或規則群組時，會 AWS WAF 檢查實體目前是否在保護套件或 Web ACL 中使用。如果發現正在使用中，會 AWS WAF 警告您。AWS WAF 幾乎總是能夠判斷保護套件或 Web ACL 是否參考實體。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有實體正在使用，請在刪除保護套件或 Web ACLs 之前檢查它。如果實體是參考集合，也請檢查沒有規則群組正在使用它。

刪除規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 選擇您要刪除的規則群組，然後選擇 Delete (刪除)。

 Note

如果您沒有看到要刪除的規則群組，請檢查規則群組區段中的區域選擇。對於用於保護 Amazon CloudFront 分佈的規則群組，請使用全域 (CloudFront) 設定。

共用規則群組

您可以與其他帳戶共用規則群組，以供這些帳戶使用。

共用規則群組

您可以與一或多個特定帳戶共用，也可以與組織中的所有帳戶共用。

若要共用規則群組，您可以使用 AWS WAF API 為您想要的規則群組共用建立政策。如需詳細資訊，請參閱《AWS WAF API 參考》中的 [PutPermissionPolicy](#)。

使用已與您共用的規則群組

如果規則群組已與您的帳戶共用，您可以透過 API 存取它，而且您可以在透過 API 建立或更新保護套件或 Web ACLs 時參考它。如需詳細資訊，請參閱 AWS WAF API 參考中的 [GetRuleGroup](#)、[CreateWebACL](#) 和 [UpdateWebACL](#)。與您共用的規則群組不會出現在 AWS WAF 主控台規則群組清單中。

AWS Marketplace 規則群組

本節說明如何使用 AWS Marketplace 規則群組。

AWS Marketplace 規則群組可透過 AWS Marketplace 主控台的訂閱取得 [AWS Marketplace](#)。訂閱 AWS Marketplace 規則群組後，您可以在其中使用它 AWS WAF。若要在 AWS Firewall Manager AWS WAF 政策中使用 AWS Marketplace 規則群組，組織中的每個帳戶都必須訂閱該群組。

您可以透過下列方式訂閱不同類型的規則群組 AWS Marketplace：

- AWS WAF 合作夥伴管理的規則群組
- 用戶端保護

在將 AWS WAF 保護用於生產流量之前，測試和調校保護的任何變更。如需相關資訊，請參閱 [測試和調校您的 AWS WAF 保護](#)。

AWS Marketplace 規則群組定價

AWS Marketplace 規則群組沒有長期合約，也沒有最低承諾。訂閱規則群組時，您必須按月支付費用 (依小時按比例分配)，以及基於用量的持續請求費用。如需詳細資訊，請參閱 [中每個 AWS Marketplace 規則群組的 AWS WAF 定價](#) 和描述 [AWS Marketplace](#)。

對 AWS Marketplace 規則群組有任何疑問？

有關賣方管理的規則群組 AWS Marketplace 以及請求功能變更的問題，請聯絡供應商的客戶支援團隊。若要尋找聯絡資訊，請參閱位於 [的提供者清單 AWS Marketplace](#)。

AWS Marketplace 規則群組提供者會決定如何管理規則群組，例如如何更新規則群組，以及規則群組是否已進行版本控制。供應商也會決定規則群組的詳細資訊，包括規則、規則動作，以及規則新增至相符 Web 請求的任何標籤。

訂閱 AWS Marketplace 規則群組

您可以在 AWS WAF 主控台上訂閱和取消訂閱 AWS Marketplace 規則群組。

Important

若要在 AWS Firewall Manager 政策中使用 AWS Marketplace 規則群組，組織中的每個帳戶必須先訂閱該規則群組。

訂閱 AWS Marketplace 規則群組

1. 登入 AWS Management Console 並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇附加元件保護。
3. 在 AWS Marketplace 區段中，選擇規則群組的名稱以檢視詳細資訊和定價資訊。

Tip

使用篩選條件快速排序您最感興趣的規則。例如，您可以使用類別篩選條件來僅檢視用戶端保護。

4. 若要訂閱 AWS Marketplace 規則群組：
 - a. 導覽至規則群組，然後選擇透過 Marketplace 訂閱。

- b. 在開啟的 Marketplace 頁面中，選擇檢視購買選項，然後選擇訂閱。

Note

如果您決定不訂閱規則群組，只要關閉快顯視窗即可。

訂閱 AWS Marketplace 規則群組後，您可以在保護套件或 Web ACLs 中使用它，就像使用其他受管規則群組一樣。如需相關資訊，請參閱[在中建立保護套件或 Web ACL AWS WAF](#)。

將規則群組新增至保護套件或 Web ACL 時，您可以覆寫規則群組中規則的動作，以及規則群組結果的動作。如需詳細資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。

從 AWS Marketplace 規則群組取消訂閱

您可以在 AWS Marketplace 主控台上取消訂閱 AWS Marketplace 規則群組。

Important

若要停止 AWS Marketplace 規則群組的訂閱費用，除了取消訂閱外，您還必須將其從 AWS WAF 和任何 Firewall Manager AWS WAF 政策中的所有保護套件或 Web ACLs 中移除。如果您取消訂閱 AWS Marketplace 規則群組，但未將其從保護套件或 Web ACLs 中移除，則會繼續向您收取訂閱費用。

取消訂閱 AWS Marketplace 規則群組

1. 從所有保護套件或 Web ACLs 移除規則群組。如需詳細資訊，請參閱[在中編輯保護套件或 Web ACL AWS WAF](#)。
2. 在 <https://console.aws.amazon.com/marketplace> 開啟 AWS 主控台。

隨即顯示管理訂閱頁面。
3. 開啟交付方法清單，然後選擇 SaaS。
4. 在協議下，開啟動作清單，然後選擇您要取消訂閱的規則群組名稱旁的取消訂閱。
5. 在取消訂閱對話方塊中，輸入 **confirm**，然後選擇是，取消訂閱。

對 AWS Marketplace 規則群組進行故障診斷

如果您發現 AWS Marketplace 規則群組封鎖合法流量，您可以執行下列步驟來疑難排解問題。

AWS Marketplace 規則群組的故障診斷

1. 覆寫動作以計算封鎖合法流量的規則。您可以使用 AWS WAF 抽樣請求或 AWS WAF 日誌來識別哪些規則封鎖特定請求。您可以查看日誌中的 `ruleGroupId` 欄位或取樣請求中的 `RuleWithinRuleGroup` 來識別規則。您可以在 模式 中識別規則 `<Seller Name>#<RuleGroup Name>#<Rule Name>`。
2. 如果將特定規則設定為僅計數請求無法解決問題，您可以覆寫所有規則動作，或將 AWS Marketplace 規則群組本身的動作從無覆寫變更為覆寫以計數。這允許 web 請求通過，無視規則群組內的個別規則動作。
3. 在覆寫個別規則動作或整個 AWS Marketplace 規則群組動作之後，請聯絡規則群組提供者的客戶支援團隊，以進一步疑難排解問題。如需聯絡資訊，請參閱 AWS Marketplace 中產品列表頁面的規則群組清單。

聯絡 AWS 支援

對於 AWS WAF 或由 管理的規則群組的問題 AWS，請聯絡 AWS 支援。如果賣方管理的規則群組發生問題 AWS Marketplace，請聯絡供應商的客戶支援團隊。若要尋找聯絡資訊，請參閱供應商的清單 AWS Marketplace。

辨識其他服務提供的規則群組

如果您或組織中的管理員使用 AWS Firewall Manager 或 AWS Shield Advanced 來管理資源保護 AWS WAF，您可能會在帳戶中看到新增至保護套件或 Web ACLs 規則群組參考陳述式。

這些規則群組的名稱開頭為下列字串：

- **ShieldMitigationRuleGroup** – 這些規則群組由 管理，AWS Shield Advanced 並用於為受保護的應用程式層（第 7 層）資源提供自動應用程式層 DDoS 緩解。

當您為受保護的資源啟用自動應用程式層 DDoS 緩解時，Shield Advanced 會將其中一個規則群組新增至與資源相關聯的保護套件或 Web ACL。Shield Advanced 會將優先順序設定為 10,000,000 的規則群組參考陳述式指派給規則群組參考陳述式，以便在您在保護套件或 Web ACL 中設定的規則之後執行。如需這些規則群組的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

⚠ Warning

請勿嘗試在保護套件或 Web ACL 中手動管理此規則群組。特別是，請勿從保護套件或 Web ACL 手動刪除 `ShieldMitigationRuleGroup` 規則群組參考陳述式。這樣做可能會對與保護套件或 Web ACL 相關聯的所有資源產生意外後果。反之，請使用 Shield Advanced 來停用與保護套件或 Web ACL 相關聯之資源的自動緩解。當不需要自動緩解時，Shield Advanced 會為您移除規則群組。

- **PREFManaged** 和 **POSTFManaged** – 這些規則群組是由 AWS Firewall Manager 根據 Firewall Manager AWS WAF 政策組態管理。Firewall Manager 在 Firewall Manager 管理的保護套件或 Web ACLs 內提供這些規則群組。

Firewall Manager 會為您建立名稱開頭為 `FMManagedWebACL` 的保護套件或 Web ACLs。您也可以設定 Firewall Manager 來改善現有的保護套件或 Web ACLs。對於這些，保護套件或 Web ACL 名稱是您在建立時指定的名稱。在任何一種情況下，防火牆管理員都會將這些規則群組新增至保護套件或 Web ACL。如需詳細資訊，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。

中的 Web ACL 容量單位 WCUs) AWS WAF

本節說明什麼是 Web ACL 容量單位 WCUs)，以及它們的運作方式。

AWS WAF 使用 WCUs 來計算和控制執行規則、規則群組和 Web ACLs 所需的操作資源。當您設定規則群組和 Web ACLs 時，會 AWS WAF 強制執行 WCU 限制。WCUs 不會影響 AWS WAF 檢查 Web 流量的方式。

AWS WAF 管理規則、規則群組和 Web ACLs 容量。

規則 WCUs

AWS WAF 當您建立或更新規則時，會計算規則容量。會針對每個規則類型以不同的方式 AWS WAF 計算容量，以反映每個規則的相對成本。相較於使用更多處理能力的複雜規則，執行成本較少的簡單規則，會使用較少的 WCU。例如，大小限制規則陳述式使用的 WCUs 少於使用 regex 模式集檢查請求的陳述式。

規則容量需求通常以規則類型的基本成本開始，並隨著複雜性而增加，例如，當您在檢查之前新增文字轉換，或檢查 JSON 內文時。如需規則容量需求的相關資訊，請參閱 [中規則陳述式的清單](#) [在中使用規則陳述式 AWS WAF](#)。

規則群組 WCUs

規則群組的 WCU 需求取決於您在規則群組中定義的規則。規則群組的最大容量為 5,000 WCUs。

每個規則群組都有不可變的容量設定，擁有者會在建立時指派此設定。這適用於您透過建立的受管規則群組和規則群組 AWS WAF。當您修改規則群組時，變更必須將規則群組的 WCUs 保持在其容量內。這可確保使用規則群組的保護套件或 Web ACLs 保持在其容量需求內。

規則群組中使用的 WCUs 是規則的 WCUs 總和減去 AWS WAF 可透過結合規則行為取得的任何處理最佳化。例如，如果您定義兩個規則來檢查相同的 Web 請求元件，且每個規則都會在檢查元件之前套用特定轉換，AWS WAF 則可能只需針對套用轉換向您收取一次費用。在保護套件或 Web ACL 中使用規則群組的 WCU 成本，一律是您在規則群組建立時定義的固定 WCU 設定。

當您建立規則群組時，請小心設定足夠高的容量，以容納您要在整個規則群組生命週期中使用的規則。

保護套件或 Web ACL WCUs

保護套件或 Web ACL 的 WCU 需求取決於您在保護套件或 Web ACL 中使用的規則和規則群組。

- 在保護套件或 Web ACL 中使用規則群組的成本是規則群組的容量設定。
- 使用規則的成本是規則的計算 WCUs 減去 AWS WAF 可從保護套件或 Web ACL 規則組合取得的任何處理最佳化。例如，如果您定義兩個規則來檢查相同的 Web 請求元件，且每個規則都會在檢查元件之前套用特定轉換，AWS WAF 則可能只需針對套用轉換向您收取一次費用。

保護套件或 Web ACL 的基本價格最多包含 1,500 WCUs。根據分層定價模式，使用超過 1,500 WCUs 會產生額外費用。隨著保護套件或 Web ACL WCU 用量的變更 AWS WAF，會自動調整您的保護套件或 Web ACL 定價。如需定價詳細資訊，請參閱 [AWS WAF 定價](#)。

保護套件或 Web ACL 的最大容量為 5,000 WCUs。

判斷規則群組、保護套件或 Web ACL WCUs

如先前章節所述，規則群組、保護套件或 Web ACL 中使用的 WCUs 總數將等於或小於規則群組、保護套件或 Web ACL 中定義之所有規則的 WCUs 總和。

在 AWS WAF 主控台中，您可以查看將規則新增至保護套件、Web ACL 或規則群組時所使用的容量。主控台會顯示您新增規則時所使用的目前容量單位。

透過 API，您可以檢查要在保護套件、Web ACL 或規則群組中使用的規則的最大容量需求。若要這樣做，請將規則的 JSON 清單提供給檢查容量呼叫。如需詳細資訊，請參閱 AWS WAF V2 API 參考中的 [CheckCapacity](#)。

在中過大 Web 請求元件 AWS WAF

本節說明如何管理在中檢查 Web 請求內文、標頭和 Cookie 的大小限制 AWS WAF。

AWS WAF 不支援檢查 Web 請求元件內文、標頭或 Cookie 的超大型內容。基礎主機服務對其轉送到 AWS WAF 進行檢查的項目具有計數和大小限制。例如，主機服務不會傳送超過 200 個標頭給 AWS WAF，因此對於具有 205 個標頭的 Web 請求，AWS WAF 無法檢查最後 5 個標頭。

當 AWS WAF 允許 Web 請求繼續到您的受保護資源時，會傳送整個 Web 請求，包括 AWS WAF 超出可檢查之計數和大小限制的任何內容。

元件檢查大小限制

元件檢查大小限制如下：

- **Body** 和 **JSON Body** – 對於 Application Load Balancer 和 AWS AppSync，AWS WAF 可以檢查請求主體的前 8 KB。根據預設，對於 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access，AWS WAF 可以檢查前 16 KB，並且您可以將保護套件或 Web ACL 組態中的限制提高到 64 KB。如需詳細資訊，請參閱[管理的內文檢查大小限制 AWS WAF](#)。
- **Headers** – 最多 AWS WAF 可以檢查請求標頭的前 8 KB (8,192 個位元組) 和前 200 個標頭。內容最多可在達到第一個限制 AWS WAF 之前進行檢查。
- **Cookies** – 最多 AWS WAF 可以檢查請求 Cookie 的前 8 KB (8,192 位元組) 和前 200 個 Cookie。內容最多可在達到第一個限制 AWS WAF 之前進行檢查。

規則陳述式的超大處理選項

當您撰寫規則陳述式來檢查其中一個請求元件類型時，您可以指定如何處理過大元件。當規則檢查的請求元件超過大小限制時，超大處理 AWS WAF 會告知如何處理 Web 請求。

處理過大元件的選項如下所示：

- **Continue** – 根據規則檢查條件，正常檢查請求元件。AWS WAF 會檢查大小限制內的請求元件內容。
- **Match** – 將 Web 請求視為符合規則陳述式。會將規則動作 AWS WAF 套用至請求，而不根據規則的檢查條件進行評估。
- **No match** – 將 Web 請求視為不符合規則陳述式，而不根據規則的檢查標準進行評估。會使用保護套件或 Web ACL 中的其餘規則 AWS WAF 繼續檢查 Web 請求，就像對任何不相符規則所做的一樣。

在 AWS WAF 主控台中，您必須選擇其中一個處理選項。在主控台外，預設選項為 Continue。

如果您在其動作設為 的規則中使用 Match 選項 Block，則規則會封鎖已檢查元件過大的請求。使用任何其他組態時，請求的最終處置取決於各種因素，例如保護套件或 Web ACL 中其他規則的組態，以及保護套件或 Web ACL 的預設動作設定。

在非您擁有的規則群組中處理過大

元件大小和計數限制適用於您在保護套件或 Web ACL 中使用的所有規則。這包括您使用但未管理的任何規則，在受管規則群組中，以及在另一個帳戶與您共用的規則群組中。

當您使用未管理的規則群組時，規則群組可能會有規則來檢查有限的請求元件，但不會以您需要處理它們的方式處理過大的內容。如需有關 AWS 受管規則如何管理過大元件的資訊，請參閱 [AWS 受管規則規則群組清單](#)。如需其他規則群組的資訊，請洽詢您的規則群組提供者。

管理保護套件或 Web ACL 中過大元件的準則

您在保護套件或 Web ACL 中處理過大元件的方式，可能取決於多種因素，例如請求元件內容的預期大小、保護套件或 Web ACL 的預設請求處理，以及保護套件或 Web ACL 中的其他規則如何符合和處理請求。

管理過大 Web 請求元件的一般準則如下：

- 如果您需要允許一些具有過大元件內容的請求，請盡可能新增規則以明確允許這些請求。排定這些規則的優先順序，使其在檢查相同元件類型的保護套件或 Web ACL 中的任何其他規則之前執行。透過此方法，您將無法使用 AWS WAF 來檢查您允許傳遞至受保護資源的超大元件的完整內容。
- 對於所有其他請求，您可以透過封鎖超過限制的請求來防止任何額外的位元組通過：
 - 您的規則和規則群組 – 在檢查具有大小限制的元件的規則中，設定過大處理，以便封鎖超出限制的請求。例如，如果您的規則封鎖具有特定標頭內容的請求，請將超大處理設定為符合具有超大標頭內容的請求。或者，如果您的保護套件或 Web ACL 預設封鎖請求，且您的規則允許特定標頭內容，則請將規則的過大處理設定為與具有過大標頭內容的任何請求不相符。
 - 您未管理的規則群組 – 若要防止未管理的規則群組允許過大請求元件，您可以新增單獨的規則來檢查請求元件類型，並封鎖超過限制的請求。優先考慮保護套件或 Web ACL 中的規則，使其在規則群組之前執行。例如，您可以在任何內文檢查規則在保護套件或 Web ACL 中執行之前，使用過大內文內容封鎖請求。下列程序說明如何新增這種類型的規則。

封鎖過大的 Web 請求元件

您可以在保護套件或 Web ACL 中新增規則，以封鎖具有過大元件的請求。

新增封鎖過大內容的規則

1. 當您建立或編輯保護套件或 Web ACL 時，請在規則設定中選擇新增規則、新增我自己的規則和規則群組、規則建置器，然後選擇規則視覺化編輯器。如需建立或編輯保護套件或 Web ACL 的指引，請參閱 [在中檢視 Web 流量指標 AWS WAF](#)。
2. 輸入規則的名稱，並將類型設定保留為規則。
3. 從其預設值變更下列比對設定：
 - a. 在陳述式上，針對檢查，開啟下拉式清單並選擇您需要的 Web 請求元件，包括內文、標頭或 Cookie。
 - b. 針對相符類型，選擇大於的大小。
 - c. 針對大小，輸入至少為元件類型大小下限的數字。針對標頭和 Cookie，輸入 8192。在 Application Load Balancer 或 AWS AppSync 保護套件或 Web ACLs，針對內文，輸入 8192。對於 CloudFront、API Gateway、Amazon Cognito、App Runner 或 Verified Access 保護套件或 Web ACLs 中的主體，如果您使用預設的主體大小限制，請輸入 16384。否則，請輸入您為保護套件或 Web ACL 定義的體型大小限制。
 - d. 針對超大處理，選取相符。
4. 針對動作，選取封鎖。
5. 選擇新增規則。
6. 新增規則後，在設定規則優先順序頁面上，將其移至您保護套件或 Web ACL 中檢查相同元件類型的任何規則或規則群組上方。這為新規則提供了較低的數值優先順序設定，這會導致 AWS WAF 先對其進行評估。如需詳細資訊，請參閱 [設定規則優先順序](#)。

中支援的規則表達式語法 AWS WAF

AWS WAF 支援 PCRE 程式庫使用的規則表達式模式語法 `libpcre`。程式庫記錄在 [PCRE - Perl 相容規則運算式](#) 中。

AWS WAF 不支援程式庫的所有建構。例如，它支援一些零寬度聲明，但不是全部。我們沒有支援的建構的完整清單。不過，如果您提供的 regex 模式無效或使用不支援的建構，則 AWS WAF API 會報告失敗。

AWS WAF 不支援下列 PCRE 模式：

- Backreferences 和擷取子運算式
- 子程式參考和遞迴模式

- 條件式模式
- 恢復控制動詞
- \C 單一位元組指令
- \R 換行比對指令
- \K 開頭比對重設指令
- 圖說文字和內嵌的程式碼
- 原子分組和所佔有的量詞

中的 IP 集和 regex 模式集 AWS WAF

本節介紹 IP 集和 regex 模式集的主題。

AWS WAF 會將一些更複雜的資訊儲存在您在規則中參考它們所使用的集合中。這些集合中的每一個都有一個名稱，並在建立時獲指派一個 Amazon Resource Name (ARN)。您可以從規則陳述式內管理這些集合，而且可以透過主控台導覽窗格存取和管理這些集合。

您可以在規則群組或保護套件或 Web ACL 中使用受管集。

- 若要使用 IP 集，請參閱 [IP 集合比對規則陳述式](#)。
- 若要使用 regex 模式集，請參閱 [規則運算式模式集比對規則陳述式](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到資源存放的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

主題

- [在 中建立和管理 IP 集 AWS WAF](#)
- [在 中建立和管理 regex 模式集 AWS WAF](#)

在 中建立和管理 IP 集 AWS WAF

IP 集合提供您要在規則陳述式中一起使用的 IP 地址和 IP 地址範圍的集合。IP 集是 AWS 資源。

若要在保護套件或 Web ACL 或規則群組中使用 IP 組，請先建立 IPSet 具有地址規格 AWS 的資源。然後在將 IP 集合規則陳述式新增至保護套件或 Web ACL 或規則群組時參考集合。

建立 IP 集合

遵循本節中的程序來建立新的 IP 集合。

Note

除了本節中的程序之外，您還可以在將 IP 比對規則新增至保護套件或 Web ACL 或規則群組時，選擇新增新的 IP 組。選擇該選項需要您提供與此程序所需的相同設定。

建立 IP 集合

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 IP sets (IP 集合)，然後選擇 Create IP set (建立 IP 集合)。
3. 輸入 IP 集合的名稱和描述。當您要使用它們時，您將使用它們來識別該集合。

Note

建立 IP 集合後無法修改名稱。

4. 針對區域，選擇全域 (CloudFront) 或選擇要存放 IP 集的區域。您只能在保護區域資源的保護套件或 Web ACLs 中使用區域 IP 集。若要使用保護套件中的 IP 集或保護 Amazon CloudFront 分佈 ACLs，您必須使用全域 (CloudFront)。
5. 針對 IP version (IP 版本)，選取您要使用的版本。

- 在 IP 地址文字方塊中，在 CIDR 表示法中輸入每行一個 IP 地址或 IP 地址範圍。AWS WAF 支援除以外的所有 IPv4 和 IPv6 CIDR 範圍/0。如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 文章 [無類別網域間路由](#)。

以下是一些範例：

- 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
- 若要指定 IPv6 地址 2620 : 0 : 2d0 : 200 : 0 : 0 : 0，請輸入 2620 : 0 : 2d0 : 200 : 0 : 0 : 0 : 0/128。
- 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
- 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。

- 檢閱 IP 集合的設定，然後選擇 Create IP set (建立 IP 集合)。

刪除 IP 集合

遵循本節中的指引來刪除參考集。

刪除參考的集合和規則群組

當您刪除可在保護套件或 Web ACL 中使用的實體，例如 IP 集、regex 模式集或規則群組時，會 AWS WAF 檢查實體目前是否在保護套件或 Web ACL 中使用。如果發現正在使用中，會 AWS WAF 警告您。AWS WAF 幾乎總是能夠判斷保護套件或 Web ACL 是否參考實體。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有實體正在使用，請在刪除保護套件或 Web ACLs 之前檢查它。如果實體是參考集合，也請檢查沒有規則群組正在使用它。

刪除 IP 集合

- 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
- 在導覽窗格中，選擇 IP sets (IP 集合)。
- 選取您要刪除的 IP 集合，然後選擇 Delete (刪除)。

在中建立和管理 regex 模式集 AWS WAF

規則運算式模式集提供您要在規則陳述式中一起使用的規則運算式的集合。Regex 模式集是 AWS 資源。

若要在保護套件或 Web ACL 或規則群組中使用 regex 模式集，請先 `RegexPatternSet` 建立具有 regex 模式規格 AWS 的資源。然後在將 regex 模式集規則陳述式新增至保護套件或 Web ACL 或規則群組時參考集合。規則運算式模式集必須至少包含一個規則運算式模式。

如果您的 regex 模式集包含多個 regex 模式，則在規則中使用它時，模式比對會與 OR 邏輯結合。也就是說，如果請求元件符合集合中的任何模式，則 Web 請求將比對模式集規則陳述式。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外。程式庫記錄在 [PCRE - Perl 相容規則表達式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

建立規則運算式模式集

遵循本節中的程序來建立新的規則運算式模式集。

建立規則運算式模式集

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 `Regex pattern sets` (規則運算式模式集)，然後選擇 `Create regex pattern set` (建立規則運算式模式集)。
3. 輸入規則運算式模式集的名稱和描述。當您要使用該集合時，您將使用這些項目來加以識別。

Note

建立規則運算式模式集後無法變更名稱。

4. 針對區域，選擇全域 (CloudFront) 或選擇要存放 regex 模式集的區域。您只能在保護區域資源的保護套件或 Web ACLs 中使用區域 regex 模式集。若要使用保護套件中的 regex 模式集或保護 Amazon CloudFront 分佈 ACLs，您必須使用全域 (CloudFront)。
5. 在 `Regular expressions` (規則運算式) 文字方塊中，每行輸入一個規則運算式模式。

例如，規則運算式 `I[a@]mAB[a@]dRequest` 符合下列字

串：`IamABadRequest`、`IamAB@dRequest`、`I@mABadRequest` 和 `I@mAB@dRequest`。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外。程式庫記錄在 [PCRE - Perl 相容規則表達式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

6. 檢閱規則運算式模式集的設定，然後選擇 `Create regex pattern set` (建立規則運算式模式集)。

刪除規則運算式模式集

遵循本節中的指引來刪除參考集。

刪除參考的集合和規則群組

當您刪除可在保護套件或 Web ACL 中使用的實體，例如 IP 集、regex 模式集或規則群組時，會 AWS WAF 檢查實體目前是否在保護套件或 Web ACL 中使用。如果發現正在使用中，會 AWS WAF 警告您。AWS WAF 幾乎總是能夠判斷保護套件或 Web ACL 是否參考實體。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有實體正在使用，請在刪除保護套件或 Web ACLs 之前檢查它。如果實體是參考集合，也請檢查沒有規則群組正在使用它。

刪除規則運算式模式集

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Regex pattern sets (規則運算式模式集)。
3. 選取您要刪除的規則運算式模式集，然後選擇 Delete (刪除)。

中的自訂 Web 請求和回應 AWS WAF

本節說明如何將自訂 Web 請求和回應處理行為新增至 AWS WAF 規則動作和預設保護套件或 Web ACL 動作。您的自訂設定會在附加至的動作套用時套用。

您可以透過下列方式自訂 Web 請求和回應：

- 透過 Allow、CAPTCHA、Count 和 Challenge 動作，您可以將自訂標頭插入 Web 請求。當 AWS WAF 轉送 Web 請求到受保護的資源時，請求會包含整個原始請求，以及您已插入的自訂標頭。對於 CAPTCHA 和 Challenge 動作，只有在請求通過 CAPTCHA 或挑戰字符檢查時，AWS WAF 才會套用自訂。
- 透過 Block 動作，您可以使用回應程式碼、標頭和內文來定義完整的自訂回應。受保護的資源會使用提供的自訂回應來回應請求 AWS WAF。您的自訂回應會取代的預設 Block 動作回應 403 (Forbidden)。

您可以自訂的動作設定

您可以在定義下列動作設定時指定自訂請求或回應：

- 規則動作。如需相關資訊，請參閱[在中使用規則動作 AWS WAF](#)。
- 保護套件或 Web ACL 的預設動作。如需相關資訊，請參閱[在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

您無法自訂的動作設定

對於您在保護套件或 Web ACL 中使用的規則群組，您無法在覆寫動作中指定自訂請求處理。請參閱[在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。另請參閱[在中使用受管規則群組陳述式 AWS WAF](#)和[在中使用規則群組陳述式 AWS WAF](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新的地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

自訂請求和回應的使用限制

AWS WAF 會為您使用自訂請求和回應定義最大設定。例如，每個保護套件或 Web ACL 或規則群組的請求標頭數目上限，以及單一自訂回應定義的自訂標頭數目上限。如需相關資訊，請參閱[AWS WAF 配額](#)。

主題

- [插入非封鎖動作的自訂請求標頭](#)
- [傳送Block動作的自訂回應](#)
- [自訂回應支援的狀態碼](#)

插入非封鎖動作的自訂請求標頭

本節說明如何在規則動作未封鎖請求時 AWS WAF，指示將自訂標頭插入原始 HTTP 請求。使用此選項，您只能將新增至請求。您無法修改或取代原始請求的任何部分。自訂標頭插入的使用案例包括發出下游應用程式的訊號，根據插入的標頭以不同方式處理請求，並標記分析請求。

此選項適用於規則動作 Allow、CAPTCHA、Count 和，Challenge 以及設定為 的保護套件或 Web ACL 預設動作 Allow。如需規則動作的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。如需預設保護套件或 Web ACL 動作的詳細資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

自訂請求標頭名稱

AWS WAF 會為其插入的所有請求標頭加上 的字首 x-amzn-waf-，以避免與已在請求中的標頭混淆。例如，如果您指定標頭名稱 sample，會 AWS WAF 插入標頭 x-amzn-waf-sample。

具有相同名稱的標頭

如果請求已有插入中相同名稱的標頭 AWS WAF，會 AWS WAF 覆寫標頭。因此，如果您在多個具有相同名稱的規則中定義標頭，則檢查請求並尋找相符項目的最後一個規則會新增其標頭，而任何先前的規則都不會新增。

具有非終止規則動作的自訂標頭

與 Allow 動作不同，Count 動作不會 AWS WAF 停止使用保護套件或 Web ACL 中的其餘規則來處理 Web 請求。同樣地，當 CAPTCHA 和 Challenge 判斷請求字符有效時，這些動作不會 AWS WAF 停止處理 Web 請求。因此，如果您使用規則搭配其中一個動作來插入自訂標頭，後續規則也可能插入自訂標頭。如需規則動作行為的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

例如，假設您有下列規則，依顯示的順序排定優先順序：

1. RuleA 具有 Count 動作和名為 的自訂標頭 RuleAHeader。
2. RuleB 具有 Allow 動作和名為 的自訂標頭 RuleBHeader。

如果請求同時符合 RuleA 和 RuleB，會 AWS WAF 插入標頭 x-amzn-waf-RuleAHeader 和 x-amzn-waf-RuleBHeader，然後將請求轉送至受保護的資源。

AWS WAF 在完成檢查請求時，會將自訂標頭插入 Web 請求。因此，如果您將自訂請求處理與 動作設定為 的規則搭配使用 Count，則您新增的自訂標頭不會受到後續規則的檢查。

自訂請求處理範例

您可以定義規則動作或保護套件或 Web ACL 預設動作的自訂請求處理。下列清單顯示新增至保護套件或 Web ACL 預設動作的自訂處理 JSON。

```
{
  "Name": "SampleWebACL",
  "Scope": "REGIONAL",
  "DefaultAction": {
    "Allow": {
      "CustomRequestHandling": {
        "InsertHeaders": [
          {
            "Name": "fruit",
            "Value": "watermelon"
          },
          {
            "Name": "pie",
            "Value": "apple"
          }
        ]
      }
    }
  },
  "Description": "Sample protection pack or web ACL with custom request handling configured for default action.",
  "Rules": [],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "SampleWebACL"
  }
}
```

傳送Block動作的自訂回應

本節說明如何指示 AWS WAF 將自訂 HTTP 回應傳回用戶端，以取得設定為 的規則動作或保護套件或 Web ACL 預設動作Block。如需規則動作的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。如需預設保護套件或 Web ACL 動作的詳細資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。

當您定義Block動作的自訂回應處理時，您可以定義狀態碼、標頭和回應內文。如需可與 搭配使用的狀態碼清單 AWS WAF，請參閱以下章節：[自訂回應支援的狀態碼](#)。

使用案例

自訂回應的使用案例包括下列項目：

- 將非預設狀態碼傳回用戶端。
- 將自訂回應標頭傳回用戶端。您可以指定 以外的任何標頭名稱 content-type。
- 傳送靜態錯誤頁面回用戶端。
- 將用戶端重新導向至不同的 URL。若要這樣做，您可以指定其中一個 3xx 重新導向狀態代碼，例如 301 (Moved Permanently) 或 302 (Found)，然後使用新的 URL 指定名為 Location 的新標頭。

與您在受保護資源中定義的回應互動

您為 AWS WAF Block 動作指定的自訂回應優先於您在受保護資源中定義的任何回應規格。

您使用 保護之 AWS 資源的主機服務 AWS WAF 可能會允許 Web 請求的自訂回應處理。範例如下：

- 使用 Amazon CloudFront，您可以根據狀態碼自訂錯誤頁面。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的 [產生自訂錯誤回應](#)。
- 透過 Amazon API Gateway，您可以定義閘道的回應和狀態碼。如需詳細資訊，請參閱《Amazon API Gateway [API Gateway 開發人員指南](#)》中的 [API Gateway 中的閘道回應](#)。

您無法在受保護 AWS 的資源中結合 AWS WAF 自訂回應設定與自訂回應設定。任何個別 Web 請求的回應規格完全 AWS WAF 來自或完全來自受保護的資源。

對於 AWS WAF 封鎖的 Web 請求，以下顯示優先順序。

1. AWS WAF 自訂回應 – 如果動作 AWS WAF Block 已啟用自訂回應，受保護的資源會將設定的自訂回應傳回給用戶端。您可能已在受保護資源本身中定義的任何回應設定都無效。
2. 受保護的資源中定義的自訂回應 – 否則，如果受保護的資源已指定自訂回應設定，則受保護的資源會使用這些設定來回應用戶端。
3. AWS WAF 預設 Block 回應 – 否則，受保護的資源會以 AWS WAF 預設回應 回應用戶端 Block 403 (Forbidden)。

對於 AWS WAF 允許的 Web 請求，受保護資源的組態會決定其傳回用戶端的回應。您無法 AWS WAF 在 中為允許的請求設定回應設定。您可以在 中 AWS WAF 為允許的請求設定的唯一自訂項目是

將自訂標頭插入原始請求，然後再將請求轉送至受保護的資源。此選項會在上一節中說明[插入非封鎖動作的自訂請求標頭](#)。

自訂回應標頭

您可以指定 以外的任何標頭名稱content-type。

自訂回應內文

您可以在要使用的保護套件、Web ACL 或規則群組的內容中定義自訂回應的內文。定義自訂回應內文之後，您可以在建立自訂回應內文的保護套件或 Web ACL 或規則群組中的任意位置參考。在個別 Block動作設定中，您會參考要使用的自訂內文，並定義自訂回應的狀態碼和標頭。

當您在主控台中建立自訂回應時，您可以從已定義的回應內文中進行選擇，也可以建立新的內文。在主控台外部，您可以在保護套件或 Web ACL 或規則群組層級定義自訂回應內文，然後從保護套件或 Web ACL 或規則群組內的動作設定參考它們。這會顯示在下一節的範例 JSON 中。

自訂回應範例

下列範例列出具有自訂回應設定的規則群組的 JSON。自訂回應內文是為整個規則群組定義，然後在規則動作中由索引鍵參考。

```
{
  "ARN": "test_rulegroup_arn",
  "Capacity": 1,

  "CustomResponseBodies": {
    "CustomResponseBodyKey1": {
      "Content": "This is a plain text response body.",
      "ContentType": "TEXT_PLAIN"
    }
  },

  "Description": "This is a test rule group.",
  "Id": "test_rulegroup_id",
  "Name": "TestRuleGroup",

  "Rules": [
    {
      "Action": {
        "Block": {
          "CustomResponse": {
            "CustomResponseBodyKey": "CustomResponseBodyKey1",
```

```
    "ResponseCode": 404,
    "ResponseHeaders": [
      {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
      }
    ]
  },
  {
    "Name": "GeoMatchRule",
    "Priority": 1,
    "Statement": {
      "GeoMatchStatement": {
        "CountryCodes": [
          "US"
        ]
      }
    },
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "TestRuleGroupReferenceMetric",
      "SampledRequestsEnabled": true
    }
  },
  {
    "Name": "GeoMatchRule",
    "Priority": 1,
    "Statement": {
      "GeoMatchStatement": {
        "CountryCodes": [
          "US"
        ]
      }
    },
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "TestRuleGroupMetric",
      "SampledRequestsEnabled": true
    }
  }
]
```

自訂回應支援的狀態碼

本節列出您可以在自訂回應中使用的狀態碼。如需 HTTP 狀態碼的詳細資訊，請參閱網際網路工程任務小組 (IETF) [的狀態碼](#) 和 Wikipedia [上的 HTTP 狀態碼清單](#)。

以下是 AWS WAF 支援自訂回應的 HTTP 狀態碼。

- 2xx Successful
 - 200 – OK

- 201 – Created
- 202 – Accepted
- 204 – No Content
- 206 – Partial Content
- 3xx Redirection
 - 300 – Multiple Choices
 - 301 – Moved Permanently
 - 302 – Found
 - 303 – See Other
 - 304 – Not Modified
 - 307 – Temporary Redirect
 - 308 – Permanent Redirect
- 4xx Client Error
 - 400 – Bad Request
 - 401 – Unauthorized
 - 403 – Forbidden
 - 404 – Not Found
 - 405 – Method Not Allowed
 - 408 – Request Timeout
 - 409 – Conflict
 - 411 – Length Required
 - 412 – Precondition Failed
 - 413 – Request Entity Too Large
 - 414 – Request-URI Too Long
 - 415 – Unsupported Media Type
 - 416 – Requested Range Not Satisfiable
 - 421 – Misdirected Request
 - 429 – Too Many Requests
- 5xx Server Error
 - 500 – Internal Server Error

- 501 – Not Implemented
- 502 – Bad Gateway
- 503 – Service Unavailable
- 504 – Gateway Timeout
- 505 – HTTP Version Not Supported

中的 Web 請求標籤 AWS WAF

本節說明什麼是 AWS WAF 標籤。

當規則符合請求時，標籤是規則新增至 Web 請求的中繼資料。新增後，標籤會保留在請求上，直到保護套件或 Web ACL 評估結束為止。您可以使用標籤比對陳述式，在稍後在保護套件或 Web ACL 評估中執行的規則中存取標籤。如需詳細資訊，請參閱[標籤比對規則陳述式](#)。

Web 請求上的標籤會產生 Amazon CloudWatch 標籤指標。如需指標和維度的清單，請參閱[標籤指標和維度](#)。如需透過 CloudWatch 和主控台存取指標和 AWS WAF 指標摘要的資訊，請參閱[監控和調校您的 AWS WAF 保護](#)。

標記使用案例

AWS WAF 標籤的常見使用案例包括下列項目：

- 在對請求採取動作之前，針對多個規則陳述式評估 Web 請求 – 在與保護套件或 Web ACL 中的規則找到相符項目之後，如果規則動作未終止保護套件或 Web ACL 評估，AWS WAF 則繼續針對保護套件或 Web ACL 評估請求。您可以在決定允許或封鎖請求之前，使用標籤來評估和收集來自多個規則的資訊。若要這樣做，請將現有規則的動作變更為 `Count` 並將它們設定為將標籤新增至相符的請求。然後，新增一或多個要在其他規則之後執行的新規則，並設定它們來評估標籤，並根據標籤比對組合管理請求。
- 依地理區域管理 Web 請求 – 您可以單獨使用地理比對規則，依來源國家/地區管理 Web 請求。若要將位置微調到區域層級，您可以使用地理比對規則搭配 `Count` 動作，後面接著標籤比對規則。如需地理比對規則的詳細資訊，請參閱[地理比對規則陳述式](#)。
- 跨多個規則重複使用邏輯 – 如果您需要跨多個規則重複使用相同的邏輯，您可以使用標籤來單一來源邏輯，並只測試結果。當您有多個複雜規則使用常見的巢狀規則陳述式子集時，跨複雜規則複製常見規則集可能會耗時且容易出錯。使用標籤，您可以建立一個具有常見規則子集的新規則，該規則子集會計數相符的請求，並將標籤新增至它們。您可以將新規則新增至保護套件或 Web ACL，使其在原始複雜規則之前執行。然後，在原始規則中，您可以將共用規則子集取代為檢查標籤的單一規則。

例如，假設您有多個規則，而您只想要套用至您的登入路徑。您可以實作包含該邏輯的單一新規則，而不是讓每個規則指定相同的邏輯以符合潛在的登入路徑。讓新規則將標籤新增至相符的請求，以指出請求位於登入路徑上。在保護套件或 Web ACL 中，將此新規則設為比原始規則更低的數值優先順序設定，以便先執行。然後，在您的原始規則中，將共用邏輯取代為檢查標籤是否存在。如需優先順序設定的資訊，請參閱 [設定規則優先順序](#)。

- 在規則群組中建立規則的例外狀況 – 此選項對於您無法檢視或修改的受管規則群組特別有用。許多受管規則群組規則會將標籤新增至相符的 Web 請求，以指出相符的規則，並可能提供有關相符項目的其他資訊。當您使用將標籤新增至請求的規則群組時，您可以覆寫規則群組規則來計算相符項目，然後在根據規則群組標籤處理 Web 請求的規則群組之後執行規則。所有 AWS 受管規則都會將標籤新增至相符的 Web 請求。如需詳細資訊，請參閱 [AWS 受管規則規則群組清單](#)。
- 使用標籤指標來監控流量模式 – 您可以存取透過規則新增標籤的指標，以及您在保護套件或 Web ACL 中使用的任何受管規則群組新增的指標。所有 AWS 受管規則規則群組都會將標籤新增至其評估的 Web 請求。如需標籤指標和維度的清單，請參閱 [標籤指標和維度](#)。您可以透過 CloudWatch 和 AWS WAF 主控台內的保護套件或 Web ACL 頁面來存取指標和指標摘要。如需相關資訊，請參閱 [監控和調校您的 AWS WAF 保護](#)。

標籤在 中的運作方式 AWS WAF

本節說明 AWS WAF 標籤的運作方式。

當規則符合 Web 請求時，如果規則已定義標籤，會在規則評估結束時將標籤 AWS WAF 新增至請求。在保護套件或 Web ACL 中比對規則之後評估的規則，可以比對規則新增的標籤。

誰會將標籤新增至請求

評估請求的保護套件或 Web ACL 元件可以將標籤新增至請求。

- 任何不是規則群組參考陳述式的規則，都可以將標籤新增至相符的 Web 請求。標記條件是規則定義的一部分，當 Web 請求符合規則時，會將規則的標籤 AWS WAF 新增至請求。如需相關資訊，請參閱 [the section called “新增標籤的規則”](#)。
- 地理比對規則陳述式會將國家和區域標籤新增至其檢查的任何請求，無論陳述式是否導致比對。如需相關資訊，請參閱 [the section called “地理比對”](#)。
- AWS WAF 所有的 AWS 受管規則會將標籤新增至其檢查的請求。它們會根據規則群組中的規則比對新增一些標籤，並根據受管規則群組使用的程序新增一些 AWS 標籤，例如當您使用智慧型威脅緩解規則群組時新增的字符標籤。如需每個受管規則群組新增之標籤的相關資訊，請參閱 [the section called “AWS 受管規則規則群組清單”](#)。

如何 AWS WAF 管理標籤

AWS WAF 在規則檢查請求結束時，會將規則的標籤新增至請求。標籤是規則比對活動的一部分，類似於動作。

保護套件或 Web ACL 評估結束後，標籤不會保留在 Web 請求中。為了讓其他規則與您的規則新增的標籤相符，您的規則動作不得終止保護套件或 Web ACL 對 Web 請求的評估。規則動作必須設定為 Count、CAPTCHA 或 Challenge。當保護套件或 Web ACL 評估未終止時，保護套件或 Web ACL 中的後續規則可以針對請求執行其標籤比對條件。如需規則動作的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

在保護套件或 Web ACL 評估期間存取標籤

新增後，只要針對保護套件或 Web ACL AWS WAF 評估請求，標籤仍可在請求上使用。保護套件或 Web ACL 中的任何規則都可以存取已在相同保護套件或 Web ACL 中執行的規則所新增的標籤。這包括直接在保護套件或 Web ACL 內定義的規則，以及在保護套件或 Web ACL 中使用的規則群組內定義的規則。

- 您可以使用標籤比對陳述式，比對規則請求檢查條件中的標籤。您可以比對連接到請求的任何標籤。如需陳述式詳細資訊，請參閱 [標籤比對規則陳述式](#)。
- 地理比對陳述式會新增有或沒有相符項目的標籤，但只有在包含保護套件或 Web ACL 規則的陳述式完成請求評估後才能使用。
 - 您無法使用單一規則，例如邏輯 AND 陳述式，針對地理標籤執行地理比對陳述式，後面接著標籤比對陳述式。您必須將標籤比對陳述式放在包含地理比對陳述式的規則之後執行的個別規則中。
 - 如果您使用地理比對陳述式做為以速率為基礎的規則陳述式或受管規則群組參考陳述式內的縮小範圍陳述式，則包含規則陳述式的陳述式無法檢查地理比對陳述式新增的標籤。如果您需要檢查以速率為基礎的規則陳述式或規則群組中的地理標籤，您必須在事先執行的單獨規則中執行地理比對陳述式。

存取保護套件或 Web ACL 評估以外的標籤資訊

在保護套件或 Web ACL 評估結束後，標籤不會保留在 Web 請求中，但會在日誌和指標中 AWS WAF 記錄標籤資訊。

- AWS WAF 會將前 100 個標籤的 Amazon CloudWatch 指標存放在任何單一請求上。如需存取標籤指標的資訊，請參閱 [使用 Amazon CloudWatch 監控](#) 和 [標籤指標和維度](#)。

- AWS WAF 摘要說明保護套件中的 CloudWatch 標籤指標或 AWS WAF 主控台中的 Web ACL 流量概觀儀表板。您可以在任何保護套件或 Web ACL 頁面上存取儀表板。如需詳細資訊，請參閱[保護套件或 Web ACLs 流量概觀儀表板](#)。
- AWS WAF 會在日誌中記錄請求前 100 個標籤的標籤。您可以使用標籤以及規則動作來篩選記錄的 AWS WAF 日誌。如需相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

您的保護套件或 Web ACL 評估可以將超過 100 個標籤套用至 Web 請求，並與超過 100 個標籤進行比對，但 AWS WAF 只會在日誌和指標中記錄前 100 個標籤。

中的標籤語法和命名需求 AWS WAF

本節說明如何建構和比對 AWS WAF 標籤。

標籤是由字首、選用命名空間和名稱組成的字串。標籤的元件以冒號分隔。標籤具有下列需求和特性：

- 標籤區分大小寫。
- 每個標籤命名空間或標籤名稱最多可有 128 個字元。
- 您可以在標籤中指定最多五個命名空間。
- 標籤的元件以冒號 () 分隔：。
- 您無法在為標籤指定的命名空間或名稱中使用下列預留字串：aws-waf、aws、waf、rulegroup-webacl、regex-pattern-set-ipset 和 managed。

標籤語法

完整標籤具有字首、選用命名空間和標籤名稱。字首識別新增標籤之規則的規則群組或保護套件或 Web ACL 內容。命名空間可用於為標籤新增更多內容。標籤名稱提供最低層級的標籤詳細資訊。它通常表示將標籤新增至請求的特定規則。

標籤字首會根據其原始伺服器而有所不同。

- 您的標籤 – 以下顯示您在保護套件或 Web ACL 和規則群組規則中建立的標籤的完整標籤語法。實體類型為 rulegroup 和 webacl。

```
aws-waf:<entity owner account id>:<entity type>:<entity name>:<custom namespace>:....:<label name>
```

- 標籤命名空間字首：aws-waf:<entity owner account id>:<entity type>:<entity name>:

- 自訂命名空間新增項目：<custom namespace>:...:

當您在規則群組或保護套件或 Web ACL 中定義規則的標籤時，您可以控制自訂命名空間字串和標籤名稱。其餘項目由 為您產生 AWS WAF。AWS WAF 會自動在所有標籤前面加上 awswaf，以及帳戶和保護套件或 Web ACL 或規則群組實體設定。

- 受管規則群組標籤 – 以下顯示受管規則群組中規則所建立標籤的完整標籤語法。

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

- 標籤命名空間字首：awswaf:managed:<vendor>:<rule group name>:
- 自訂命名空間新增項目：<custom namespace>:...:

所有 AWS 受管規則規則群組都會新增標籤。如需受管規則群組的相關資訊，請參閱 [在中使用受管規則群組 AWS WAF](#)。

- 來自其他 AWS 程序的標籤 – AWS 受管規則規則群組會使用這些程序，因此您會看到這些程序新增至您使用受管規則群組評估的 Web 請求。以下顯示由受管規則群組呼叫的程序所建立之標籤的完整標籤語法。

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

- 標籤命名空間字首：awswaf:managed:<process>:
- 自訂命名空間新增項目：<custom namespace>:...:

此類型的標籤會針對呼叫 程序 AWS 的受管規則群組列出。如需受管規則群組的相關資訊，請參閱 [在中使用受管規則群組 AWS WAF](#)。

規則的標籤範例

下列範例標籤由屬於帳戶 111122223333 testRules 的規則群組中的規則定義。

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

下列清單顯示 JSON 中的範例標籤規格。這些標籤名稱包含結尾標籤名稱之前的自訂命名空間字串。

```
Rule: {
  Name: "label_rule",
  Statement: {...}
  RuleLabels: [
    Name: "header:encoding:utf8",
    Name: "header:user_agent:firefox"
  ],
  Action: { Count: {} }
}
```

Note

您可以透過規則 JSON 編輯器在主控台中存取此類清單。

如果您在與上述標籤範例相同的規則群組和帳戶中執行上述規則，則產生的完整標籤如下：

```
awsaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awsaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

受管規則群組的標籤範例

以下顯示受 AWS 管規則規則群組的範例標籤，以及他們叫用的處理程序。

```
awsaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awsaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awsaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awsaf:managed:token:accepted
```

AWS WAF 新增標籤的規則

在幾乎所有規則中，您可以定義標籤 AWS WAF，並將其套用至任何相符的請求。

下列規則類型是唯一的例外狀況：

- 速率型規則標籤僅在速率限制時 – 速率型規則僅在該執行個體速率受到限制時，將標籤新增至特定彙總執行個體的 Web 請求 AWS WAF。如需速率型規則的相關資訊，請參閱 [在中使用以速率為基礎的規則陳述式 AWS WAF](#)。
- 規則群組參考陳述式中不允許標記 – 主控台不接受規則群組陳述式或受管規則群組陳述式的標籤。透過 API，指定任一陳述式類型的標籤會導致驗證例外狀況。如需這些陳述式類型的詳細資訊，請參閱 [在中使用受管規則群組陳述式 AWS WAF](#) 和 [在中使用規則群組陳述式 AWS WAF](#)。

WCUs – 您在保護套件或 Web ACL 或規則群組規則中定義的每 5 個標籤 1 個 WCU。

哪裡可以找到此項

- 主控台上的規則建置器 – 在規則的動作設定下，在標籤下。
- API 資料類型 – Rule RuleLabels

您可以在規則中定義標籤，方法是指定要附加到標籤命名空間字首的自訂命名空間字串和名稱。會從您定義規則的內容 AWS WAF 衍生字首。如需詳細資訊，請參閱 [下的標籤語法資訊中的標籤語法和命名需求 AWS WAF](#)。

AWS WAF 符合標籤的 規則

本節說明如何使用標籤比對陳述式來評估 Web 請求標籤。您可以比對需要標籤名稱的 Label，或是比對需要命名空間規格的 Namespace。對於標籤或命名空間，您可以選擇在規格中包含前面的命名空間和字首。如需此陳述式類型的一般資訊，請參閱 [標籤比對規則陳述式](#)。

標籤的字首定義了定義標籤規則的規則群組或保護套件或 Web ACL 的內容。在規則的標籤比對陳述式中，如果您的標籤或命名空間比對字串未指定字首，AWS WAF 會使用標籤比對規則的字首。

- 直接在保護套件或 Web ACL 內定義的規則標籤具有一個字首，可指定保護套件或 Web ACL 內容。
- 規則群組內規則的標籤具有指定規則群組內容的字首。這可以是您自己的規則群組或為您管理的規則群組。

如需詳細資訊，請參閱 [下的標籤語法中的標籤語法和命名需求 AWS WAF](#)。

Note

有些受管規則群組會新增標籤。您可以透過 API 呼叫 來擷取這些項目 DescribeManagedRuleGroup。這些標籤會列在回應的 AvailableLabels 屬性中。

如果您想要比對與規則內容不同的規則，則必須在比對字串中提供字首。例如，如果您想要比對受管規則群組中規則新增的標籤，您可以使用標籤比對陳述式在保護套件或 Web ACL 中新增規則，其比對字串會指定規則群組的字首，後面接著您的其他比對條件。

在標籤比對陳述式的比對字串中，您可以指定標籤或命名空間：

- 標籤 – 相符項目的標籤規格由標籤的結尾部分組成。您可以包含任意數量的連續命名空間，其緊接在標籤名稱前面，後面接著名稱。您也可以使用 字首啟動規格，以提供完整標籤。

範例規格：

- `testNS1:testNS2:LabelNameA`
- `aws:waf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- 命名空間 – 相符項目的命名空間規格由名稱以外的任何標籤規格連續子集組成。您可以包含 字首，也可以包含一或多個命名空間字串。

範例規格：

- `testNS1:testNS2:`
- `aws:waf:managed:aws:managed-rule-set:testNS1:`

AWS WAF 標籤比對範例

本節提供標籤比對規則陳述式的比對規格範例。

Note

這些 JSON 清單是在主控台中建立，方法是使用標籤比對規格將規則新增至保護套件或 Web ACL，然後編輯規則並切換到規則 JSON 編輯器。您也可以透過 APIs JSON。

主題

- [比對本機標籤](#)
- [比對其他內容中的標籤](#)
- [符合受管規則群組標籤](#)
- [比對本機命名空間](#)
- [符合受管規則群組命名空間](#)

比對本機標籤

下列 JSON 清單顯示已新增至本機 Web 請求之標籤的標籤比對陳述式，其內容與此規則相同。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

如果您在帳戶 111122223333 中使用此比對陳述式，在您為保護套件或 Web ACL 定義的規則中 testWebACL，它會符合下列標籤。

```
awsfaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awsfaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

它不符合下列標籤，因為標籤字串不是完全相符。

```
awsfaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

它不符合下列標籤，因為內容不同，因此字首不相符。即使您將規則群組新增至定義規則 productionRules 的保護套件或 Web ACL testWebACL，也是如此。

```
awsfaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

比對其他內容中的標籤

下列 JSON 清單顯示標籤比對規則，符合使用者建立的規則群組內規則的標籤。對於在保護套件或 Web ACL 中執行且不屬於具名規則群組的所有規則，規格中需要字首。此範例標籤規格僅符合確切的標籤。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "aws:waf:111122223333:rulegroup:testRules:header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

符合受管規則群組標籤

這是比對標籤的特殊案例，該標籤來自比對規則以外的其他內容。下列 JSON 清單顯示受管規則群組標籤的標籤比對陳述式。這只會比對標籤比對陳述式金鑰設定中指定的確切標籤。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "aws:waf:managed:aws:managed-rule-set:header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

比對本機命名空間

下列 JSON 清單顯示本機命名空間的標籤比對陳述式。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
```

```
        Key: "header:encoding:"
      }
    },
    Labels: [
      ...generate_more_labels...
    ],
    Action: { Block: {} }
  }
```

與本機Label比對類似，如果您在帳戶 111122223333 中使用此陳述式，在您為保護套件或 Web ACL 定義的規則中testWebACL，它會符合下列標籤。

```
aws:waf:111122223333:webacl:testWebACL:header:encoding:utf8
```

它不符合下列標籤，因為帳戶不同，因此字首不相符。

```
aws:waf:444455556666:webacl:testWebACL:header:encoding:utf8
```

字首也不符合受管規則群組套用的任何標籤，如下所示。

```
aws:waf:managed:aws:managed-rule-set:header:encoding:utf8
```

符合受管規則群組命名空間

下列 JSON 清單顯示受管規則群組命名空間的標籤比對陳述式。對於您擁有的規則群組，您也需要提供字首，才能比對規則內容以外的命名空間。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
      Key: "aws:waf:managed:aws:managed-rule-set:header:"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

此規格符合下列範例標籤。

```
aws:waf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
aws:waf:managed:aws:managed-rule-set:header:encoding:unicode
```

它不符合下列標籤。

```
aws:waf:managed:aws:managed-rule-set:query:badstring
```

中的智慧型威脅防禦 AWS WAF

本節涵蓋 提供的受管智慧型威脅緩解功能 AWS WAF。這些是進階的專門保護，您可以實作這些保護，以防止惡意機器人和帳戶接管嘗試等威脅。

Note

除了使用 的基本費用之外，此處所述的功能會產生額外費用 AWS WAF。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

本節中提供的指引適用於通常知道如何建立和管理 AWS WAF Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。

主題

- [中的智慧威脅緩解選項 AWS WAF](#)
- [中的智慧型威脅防禦最佳實務 AWS WAF](#)
- [用於 AWS WAF 智慧型威脅緩解的字符](#)
- [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)
- [AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)
- [AWS WAF 機器人控制](#)
- [AWS WAF 分散式阻斷服務 \(DDoS\) 預防](#)
- [中的用戶端應用程式整合 AWS WAF](#)
- [CAPTCHA 和 Challenge 中的 AWS WAF](#)

中的智慧威脅緩解選項 AWS WAF

本節提供實作智慧型威脅緩解選項的詳細比較。

AWS WAF 提供以下類型的智慧威脅緩解保護。

- AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) – 偵測和管理應用程式註冊頁面上的惡意帳戶建立嘗試。核心功能由 ACFP 受管規則群組提供。如需詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#) 和 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。
- AWS WAF 詐騙控制帳戶接管預防 (ATP) – 偵測和管理應用程式登入頁面上的惡意接管嘗試。核心功能由 ATP 受管規則群組提供。如需詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#) 和 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。
- AWS WAF 機器人控制 – 識別、標記和管理易記和惡意的機器人。此功能為具有跨應用程式唯一簽章的常見機器人，以及具有應用程式特定簽章的目標機器人提供管理。核心功能由 Bot Control 受管規則群組提供。如需詳細資訊，請參閱 [AWS WAF 機器人控制](#) 和 [AWS WAF 機器人控制規則群組](#)。
- 用戶端應用程式整合 SDKs – 驗證您網頁上的用戶端工作階段和最終使用者，並取得權杖供用戶端用於其 Web 請求。如果您使用 ACFP、ATP 或 Bot Control，請盡可能在用戶端應用程式中實作應用程式整合 SDKs，以充分利用所有規則群組功能。當關鍵資源需要快速保護，而且沒有足夠的時間進行 SDK 整合時，我們只建議使用這些規則群組，而沒有 SDK 整合做為臨時措施。如需有關實作 SDKs 的資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。
- Challenge 和 CAPTCHA 規則動作 – 驗證用戶端工作階段和最終使用者，並取得權杖，供用戶端用於其 Web 請求。您可以在指定規則動作的任何地方、在您的規則中，以及在您使用的規則群組中，將這些實作為覆寫。這些動作使用 AWS WAF JavaScript 中介來查詢用戶端或最終使用者，而且需要支援 JavaScript 的用戶端應用程式。如需詳細資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

智慧型威脅緩解 AWS 受管規則規則群組 ACFP、ATP 和 Bot Control 會使用權杖進行進階偵測。如需有關字符在規則群組中啟用的功能的資訊，請參閱 [搭配 ACFP 使用應用程式整合 SDKs](#)、[搭配 ATP 使用應用程式整合 SDKs](#) 和 [搭配 Bot Control 使用應用程式整合 SDKs](#)。

實作智慧型威脅緩解的選項，從基本使用規則動作來執行挑戰和強制執行權杖擷取，到智慧型威脅緩解 AWS 受管規則規則群組提供的進階功能。

下表提供基本和進階功能選項的詳細比較。

主題

- [挑戰和權杖取得的選項](#)

- [智慧威脅緩解受管規則群組的選項](#)
- [速率型規則和目標 Bot Control 規則中速率限制的選項](#)

挑戰和權杖取得的選項

本節會比較挑戰和字符管理選項。

您可以使用 AWS WAF 應用程式整合 SDKs 或規則動作 和 來提供挑戰Challenge並取得權杖CAPTCHA。廣義而言，規則動作較容易實作，但會產生額外的成本、深入了解您的客戶體驗，而且需要 JavaScript。SDKs需要在用戶端應用程式中進行程式設計，但可以提供更好的客戶體驗、免費使用，而且可以與 JavaScript 或 Android 或 iOS 應用程式搭配使用。您只能將應用程式整合 SDKs與使用其中一個付費智慧型威脅緩解受管規則群組的保護套件或 Web ACLs 搭配使用，如下節所述。

比較挑戰和權杖擷取的選項

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 挑戰	行動 SDK 挑戰
它是什麼	規則動作，透過向瀏覽器用戶端呈現無提示挑戰的間質性，強制執行對 AWS WAF 字符的取得	規則動作，透過向用戶端最終使用者提供視覺或音訊挑戰間質強制執行 AWS WAF 字符的取得	應用程式整合層，適用於用戶端瀏覽器和其他執行 JavaScript 的裝置。轉譯靜音挑戰並取得字符	應用程式整合層，適用於 Android 和 iOS 應用程式。原生轉譯靜音挑戰並取得字符
適合...	針對支援 JavaScript 之用戶端的機器人工作階段和字符擷取強制執行的無提示驗證	對於支援 JavaScript 的用戶端，針對機器人工作階段和強制執行字符獲取的最終使用者和靜音驗證	針對機器人工作階段的無提示驗證，以及針對支援 JavaScript 的用戶端強制執行權杖擷取。 SDKs提供最低延遲，並對挑戰指令碼在應用程式中執行的位置進行最佳控制。	針對 Android 和 iOS 上原生行動應用程式的機器人工作階段和字符擷取強制執行的靜音驗證。 SDKs提供最低延遲，並對挑戰指令碼在應用程式中執行的位置進行最佳控制。

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 挑戰	行動 SDK 挑戰
實作考量	實作為規則動作設定	實作為規則動作設定	需要保護套件或 Web ACL 中其中一個 ACFP、ATP 或 Bot Control 付費規則群組。 在用戶端應用程式中需要編碼。	需要保護套件或 Web ACL 中其中一個 ACFP、ATP 或 Bot Control 付費規則群組。 在用戶端應用程式中需要編碼。
執行時間考量	沒有有效字符之請求的侵入性流程。用戶端會重新導向至 AWS WAF 挑戰間質。新增網路往返，並需要 Web 請求的第二次評估。	沒有有效字符之請求的侵入性流程。用戶端會重新導向至 AWS WAF CAPTCHA 間質。新增網路往返，並需要 Web 請求的第二次評估。	可在幕後執行。讓您更能掌控挑戰體驗。	可在幕後執行。讓您更能掌控挑戰體驗。
需要 JavaScript	是	是	是	否
支援的用戶端	執行 Javascript 的瀏覽器和裝置	執行 Javascript 的瀏覽器和裝置	執行 Javascript 的瀏覽器和裝置	Android 和 iOS 裝置

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 挑戰	行動 SDK 挑戰
支援單頁應用程式 (SPA)	僅限強制執行。 您可以搭配 SDKs 使用 Challenge動作，以確保請求具有有效的挑戰字符。您無法使用規則動作將挑戰指令碼交付至頁面。	僅限強制執行。 您可以搭配 SDKs 使用 CAPTCHA動作，以確保請求具有有效的 CAPTCHA 字符。您無法使用規則動作將 CAPTCHA 指令碼交付至頁面。	是	N/A
額外費用	是，對於您明確指定的動作設定，可能是在您定義的規則中，或是在您使用的規則群組中做為規則動作覆寫。在所有其他情況下為否。	是，對於您明確指定的動作設定，可能是在您定義的規則中，或是在您使用的規則群組中做為規則動作覆寫。在所有其他情況下為否。	否，但需要其中一個付費規則群組 ACFP、ATP 或機器人控制。	否，但需要其中一個付費規則群組 ACFP、ATP 或機器人控制。

如需這些選項相關成本的詳細資訊，請參閱 [AWS WAF 定價](#) 中的智慧型威脅緩解資訊。

只需新增具有 Challenge或 CAPTCHA動作的規則，即可更輕鬆地執行挑戰並提供基本權杖強制執行。您可能需要使用規則動作，例如，如果您無法存取應用程式碼。

不過，如果您可以實作SDKs，相較於使用 Challenge動作，您可以節省保護套件的成本並減少用戶端 Web 請求的 Web ACL 評估延遲：

- 您可以在應用程式中的任何時間點撰寫 SDK 實作來執行挑戰。您可以在將 Web 請求傳送到受保護資源的任何客戶動作之前，在背景中取得字符。如此一來，字符即可與用戶端的第一個請求一起傳送。

- 如果您使用 Challenge 動作實作規則來取得字符，則當用戶端第一次傳送請求時以及字符過期時，規則和動作需要額外的 Web 請求評估和處理。Challenge 動作會封鎖沒有有效、未過期字符的請求，並將挑戰交還給用戶端。用戶端成功回應挑戰後，會使用有效的字符重新傳送原始 Web 請求，然後由保護套件或 Web ACL 再次評估。

智慧威脅緩解受管規則群組的選項

本節會比較受管規則群組選項。

智慧型威脅緩解 AWS 受管規則規則群組提供基本機器人的管理、複雜惡意機器人的偵測和緩解、帳戶接管嘗試的偵測和緩解，以及詐騙帳戶建立嘗試的偵測和緩解。這些規則群組結合上一節所述的應用程式整合 SDKs，可提供最先進的保護，並與用戶端應用程式進行安全耦合。

受管規則群組選項的比較

	ACFP	ATP	機器人控制共同層級	Bot Control 目標層級
它是什麼	在應用程式的註冊和註冊頁面上，管理可能屬於詐騙帳戶建立嘗試一部分的請求。 不管理機器人。 請參閱 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 規則群組。	管理可能屬於應用程式登入頁面上惡意接管嘗試一部分的請求。 不管理機器人。 請參閱 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。	使用應用程式間唯一的簽章，管理自我識別的常見機器人。 請參閱 AWS WAF 機器人控制規則群組。	使用應用程式特有的簽章，管理無法自我識別的目標機器人。 請參閱 AWS WAF 機器人控制規則群組。
適合...	使用使用者名稱周遊和從單一 IP 地址建立的許多新帳戶，檢查帳戶建立流量是否	檢查帳戶接管攻擊的登入流量，例如密碼周遊的登入嘗試，以及來自相同 IP 地址的許多登入嘗	一般自動化機器人流量的基本機器人保護和標籤。	針對複雜機器人的保護，包括用戶端工作階段層級的速率限制，以及偵測和緩解瀏覽器自

	ACFP	ATP	機器人控制共同層級	Bot Control 目標層級
	有詐騙性帳戶建立攻擊。	試。與字符搭配使用時，也會提供彙總保護，例如 IPs 和用戶端工作階段的速率限制，以處理大量失敗的登入嘗試。		動化工具，例如 Selenium 和 Puppeteer。
新增指示評估結果的標籤	是	是	是	是
新增字符標籤	是	是	是	是
封鎖沒有有效字符的請求	不包含。 請參閱 封鎖沒有有效 AWS WAF 字符的請求 。	不包含。 請參閱 封鎖沒有有效 AWS WAF 字符的請求 。	不包含。 請參閱 封鎖沒有有效 AWS WAF 字符的請求 。	封鎖在沒有字符的情況下傳送 5 個請求的用戶端工作階段。
需要權 AWS WAF 杖 aws-waf-token	所有規則皆必要。 請參閱 搭配 ACFP 使用應用程式整合 SDKs 。	許多規則都需要。 請參閱 搭配 ATP 使用應用程式整合 SDKs 。	否	是
取得 AWS WAF 權杖 aws-waf-token	是，由規則強制執行 AllRequests	否	否	有些規則會使用 Challenge或 CAPTCHA規則動作，以取得字符。

如需這些選項相關成本的詳細資訊，請參閱[AWS WAF 定價](#)中的智慧型威脅緩解資訊。

速率型規則和目標 Bot Control 規則中速率限制的選項

本節比較以速率為基礎的緩解選項。

AWS WAF Bot Control 規則群組的目標層級和速率 AWS WAF 型規則陳述式都提供 Web 請求速率限制。下表會比較這兩個選項。

速率型偵測和緩解選項的比較

	AWS WAF 以速率為基礎的規則	AWS WAF Bot Control 目標規則	
套用速率限制的方式	對速率太高的請求群組採取行動。您可以套用 以外的任何動作 Allow。	透過使用請求字符，強制執行類似人類的存取模式並套用動態速率限制。	
根據歷史流量基準？	否	是	
累積歷史流量基準所需的時間	N/A	動態閾值為五分鐘。缺少字符的 N/A。	
緩解延遲	通常為 30-50 秒。最長可達幾分鐘。	通常少於 10 秒。最長可達幾分鐘。	
緩解目標	可設定。您可以使用縮小範圍陳述式，以及使用一或多個彙總索引鍵來分組請求，例如 IP 地址、HTTP 方法和查詢字串。	IP 地址和用戶端工作階段	
觸發緩解所需的流量磁碟區層級	中 - 可在指定的時段內低至 10 個請求	低 - 用於偵測用戶端模式，例如慢速抓取器	
可自訂的閾值	是	否	
預設緩解動作	主控台預設為 Block。API 中沒有預設設定；需要設定。	規則群組規則動作設定 Challenge 適用於缺少字符，以及來自單一用戶端工作階段	

	AWS WAF 以速率為基礎的規則	AWS WAF Bot Control 目標規則	
	您可以將此設定為 以外的任何規則動作 Allow。	CAPTCHA 的大量流量。 您可以將這些規則之一設定為任何有效的規則動作。	
針對高度分散式攻擊的彈性	中 - 10,000 個 IP 地址上限，可自行限制 IP 地址	中 - IP 地址和權杖之間的總計限制為 50,000	
AWS WAF 定價	包含在 的標準費用中 AWS WAF。	包含在目標層級的 Bot Control 智慧威脅緩解費用中。	
如需詳細資訊	在 中使用以速率為基礎的規則陳述式 AWS WAF	AWS WAF 機器人控制規則群組	

中的智慧型威脅防禦最佳實務 AWS WAF

遵循本節中的最佳實務，以最有效率、最具成本效益的方式實作智慧型威脅緩解功能。

- 實作 JavaScript 和行動應用程式整合 SDKs – 實作應用程式整合，以最有效的方式啟用完整的 ACFP、ATP 或機器人控制功能。受管規則群組使用 SDKs 提供的字符，在工作階段層級將合法用戶端流量與不需要的流量分開。應用程式整合 SDKs 可確保這些字符隨時可用。如需詳細資訊，請參閱以下：
- [搭配 ACFP 使用應用程式整合 SDKs](#)
- [搭配 ATP 使用應用程式整合 SDKs](#)
- [搭配 Bot Control 使用應用程式整合 SDKs](#)

使用整合在您的用戶端中實作挑戰，並針對 JavaScript 自訂 CAPTCHA 拼圖如何呈現給最終使用者。如需詳細資訊，請參閱[中的用戶端應用程式整合 AWS WAF](#)。

如果您使用 JavaScript API 自訂 CAPTCHA 拼圖，並在保護套件或 Web ACL 的任何位置使用 CAPTCHA 規則動作，請遵循用戶端中處理 AWS WAF CAPTCHA 回應的指引 [從處理 CAPTCHA 回應 AWS WAF](#)。本指南適用於使用 CAPTCHA 動作的任何規則，包括 ACFP 受管規則群組中的規則，以及 Bot Control 受管規則群組的目標保護層級。

- 限制您傳送至 ACFP、ATP 和 Bot Control 規則群組的請求 – 使用智慧型威脅緩解 AWS 受管規則規則群組會產生額外費用。ACFP 規則群組會檢查您指定之帳戶註冊和建立端點的請求。ATP 規則群組會檢查您指定之登入端點的請求。Bot Control 規則群組會檢查保護套件或 Web ACL 評估中到達的每個請求。

請考慮以下方法來減少您對這些規則群組的使用：

- 在受管規則群組陳述式中使用縮小範圍陳述式排除來自檢查的請求。您可以使用任何可巢狀陳述式來執行此操作。如需相關資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。
- 在規則群組之前新增規則，從檢查中排除請求。對於您無法在縮小範圍陳述式中使用的規則，以及更複雜的情況，例如標記後接標籤比對，您可能想要新增在規則群組之前執行的規則。如需詳細資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#) 及 [在中使用規則陳述式 AWS WAF](#)。
- 在較便宜的規則之後執行規則群組。如果您有其他標準 AWS WAF 規則因任何原因封鎖請求，請在這些付費規則群組之前執行它們。如需規則和規則管理的詳細資訊，請參閱 [在中使用規則陳述式 AWS WAF](#)。
- 如果您使用的是多個智慧型威脅緩解受管規則群組，請依照下列順序執行它們，以降低成本：Bot Control、ATP、ACFP。

如需更多定價的詳細資訊，請參閱 [AWS WAF 定價](#)。

- 請勿限制您傳送至 Anti-DDoS 規則群組的請求 – 當您在 中設定規則群組以監控您未明確允許的所有 Web 流量時，此規則群組運作效果最佳。將其定位在您的 Web ACL 中，只在具有 Allow 規則動作的規則之後以及在所有其他規則之前進行評估。
- 對於分散式拒絕服務 (DDoS) 保護，請使用 Anti-DDoS 或 Shield Advanced 自動應用程式層 DDoS 緩解 – 其他智慧型威脅緩解規則群組不提供 DDoS 保護。ACFP 可防止對應用程式的註冊頁面進行詐騙帳戶建立嘗試。ATP 可防止帳戶接管嘗試您的登入頁面。Bot Control 著重於在用戶端工作階段上使用字符和動態速率限制強制執行類似人類的存取模式。

反 DDoS 可讓您監控和控制 DDoS 攻擊，以便快速回應和緩解威脅。Shield Advanced 搭配自動應用程式層 DDoS 緩解會自動回應偵測到的 DDoS 攻擊，方法是代表您建立、評估和部署自訂 AWS WAF 緩解措施。

如需 Shield Advanced 的詳細資訊，請參閱 [AWS Shield Advanced 概觀](#) 和 [使用 AWS Shield Advanced 和保護應用程式層（第 7 層）AWS WAF](#)。

如需分散式阻斷服務 (DDoS) 預防的詳細資訊，請參閱 [反 DDoS 規則群組](#) 和 [分散式阻斷服務 \(DDoS\) 預防](#)。

- 在正常 Web 流量期間啟用反 DDoS 規則群組和機器人控制規則群組的目標保護層級 – 這些規則類別需要時間來建立正常流量的基準。

在正常 Web 流量期間啟用 Bot Control 規則群組的目標保護層級 – 目標保護層級的某些規則需要時間建立正常流量模式的基準，才能識別和回應不規則或惡意流量模式。例如，TGT_ML_*規則最多需要 24 小時才能暖機。

當您沒有遭受攻擊時，請新增這些保護，並讓他們有時間建立基準，再預期他們做出適當的回應。如果您在攻擊期間新增這些規則，則需要在計數模式中啟用反 DDoS 規則群組。在攻擊消失後，建立基準的時間通常是正常所需時間的兩倍到三倍，因為攻擊流量增加的擺動。如需規則及其所需的任何暖機時間的詳細資訊，請參閱 [規則清單](#)。

- 對於分散式拒絕服務 (DDoS) 保護，請使用 Shield Advanced 自動應用程式層 DDoS 緩解 – 智慧型威脅緩解規則群組不提供 DDoS 保護。ACFP 可防止對應用程式的註冊頁面進行詐騙帳戶建立嘗試。ATP 可防止帳戶接管嘗試您的登入頁面。Bot Control 著重於在用戶端工作階段上使用字符和動態速率限制強制執行類似人類的存取模式。

當您在啟用自動應用程式層 DDoS 緩解措施的情況下使用 Shield Advanced 時，Shield Advanced 會透過代表您建立、評估和部署自訂 AWS WAF 緩解措施，自動回應偵測到的 DDoS 攻擊。如需 Shield Advanced 的詳細資訊，請參閱 [AWS Shield Advanced 概觀](#) 和 [使用 AWS Shield Advanced 和 保護應用程式層 \(第 7 層\) AWS WAF](#)。

- 當您為反 DDoS 規則群組建立基準時，請使用生產流量負載 – 使用人工測試流量來測試其他規則群組是常見的做法。不過，當您測試和建立 Anti-DDoS 規則群組的基準時，建議您使用反映生產環境中負載的流量流程。使用典型流量建立反 DDoS 基準是確保您的資源在生產環境中啟用規則群組時受到保護的最佳方式。
- 調校和設定字符處理 – 調整保護套件或 Web ACL 的字符處理，以獲得最佳使用者體驗。
 - 為了降低營運成本並改善最終使用者的體驗，請將權杖管理抗擾性時間調整為安全需求允許的最長時間。這可將 CAPTCHA 拼圖和靜音挑戰的使用降至最低。如需相關資訊，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。
 - 若要在受保護的應用程式之間啟用權杖共用，請為您的保護套件或 Web ACL 設定權杖網域清單。如需相關資訊，請參閱 [在中指定字符網域和網域清單 AWS WAF](#)。
- 使用任意主機規格拒絕請求 – 設定受保護的資源，要求 Web 請求中的 Host 標頭符合目標資源。您可以接受一個值或一組特定值，例如 myExampleHost.com 和 www.myExampleHost.com，但不接受主機的任意值。

- 對於屬於 CloudFront 分佈原始伺服器的 Application Load Balancer，請設定 CloudFront 和 AWS WAF 以進行適當的權杖處理 – 如果您將保護套件或 Web ACL 與 Application Load Balancer 建立關聯，並將 Application Load Balancer 部署為 CloudFront 分佈的原始伺服器，請參閱 [屬於 CloudFront 原始伺服器的 Application Load Balancer 所需的組態](#)。
- 部署前測試和調校 – 在您實作保護套件或 Web ACL 的任何變更之前，請遵循本指南中的測試和調校程序，以確保您獲得預期的行為。這對這些付費功能尤其重要。如需一般指引，請參閱 [測試和調校您的 AWS WAF 保護](#)。如需付費受管規則群組的特定資訊，請參閱 [測試和部署 ACFP](#)、[測試和部署 ATP](#) 和 [測試和部署 AWS WAF 機器人控制](#)。

用於 AWS WAF 智慧型威脅緩解的字符

本節說明權杖 AWS WAF 的功能。

AWS WAF 權杖是 AWS WAF 智慧型威脅緩解措施所提供增強型保護不可或缺的一部分。權杖，有時稱為指紋，是用戶端儲存的單一用戶端工作階段相關資訊集合，並提供用戶端傳送的每個 Web 請求。AWS WAF 會使用權杖來識別惡意用戶端工作階段，以及將其與合法工作階段分開，即使兩者都來自單一 IP 地址。權杖使用會對合法使用者施加可忽略的成本，但殭屍網路的成本會大規模增加。

AWS WAF 使用字符來支援其瀏覽器和最終使用者挑戰功能，該功能由應用程式整合 SDKs 和規則動作 Challenge 和 提供 CAPTCHA。此外，權杖會啟用 AWS WAF Bot Control 和帳戶接管預防受管規則群組的功能。

AWS WAF 會為成功回應沉默挑戰和 CAPTCHA 謎題的用戶端建立、更新和加密字符。當具有字符的用戶端傳送 Web 請求時，它會包含加密的字符，並 AWS WAF 解密字符並驗證其內容。

主題

- [AWS WAF 如何使用字符](#)
- [AWS WAF 字符特性](#)
- [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)
- [在中指定字符網域和網域清單 AWS WAF](#)
- [中的字符標籤類型 AWS WAF](#)
- [封鎖沒有有效 AWS WAF 字符的請求](#)
- [屬於 CloudFront 原始伺服器的 Application Load Balancer 所需的組態](#)

AWS WAF 如何使用字符

本節說明如何 AWS WAF 使用字符。

AWS WAF 使用字符來記錄和驗證下列類型的用戶端工作階段驗證：

- CAPTCHA – CAPTCHA 拼圖有助於區分機器人與人類使用者。CAPTCHA 僅由 CAPTCHA 規則動作執行。成功完成拼圖後，CAPTCHA 指令碼會更新字符的 CAPTCHA 時間戳記。如需詳細資訊，請參閱[CAPTCHA 和 Challenge 中的 AWS WAF](#)。
- 挑戰 – 挑戰會以無提示方式執行，以協助區分定期用戶端工作階段與機器人工作階段，並讓機器人運作成本更高。當挑戰成功完成時，挑戰指令碼 AWS WAF 會自動視需要從取得新的權杖，然後更新權杖的挑戰時間戳記。

AWS WAF 在下列情況中執行挑戰：

- 應用程式整合 SDKs – 應用程式整合 SDKs 會在您的用戶端應用程式工作階段中執行，並協助確保只有在用戶端成功回應挑戰之後，才允許嘗試登入。如需詳細資訊，請參閱[中的用戶端應用程式整合 AWS WAF](#)。
- Challenge 規則動作 – 如需詳細資訊，請參閱[CAPTCHA 和 Challenge 中的 AWS WAF](#)。
- CAPTCHA – 當 CAPTCHA 問卷執行時，如果用戶端還沒有權杖，則指令碼會自動先執行挑戰，以驗證用戶端工作階段並初始化權杖。

智慧型威脅 AWS 受管規則規則群組中的許多規則都需要權杖。這些規則使用字符來執行一些操作，例如區分工作階段層級的用戶端、判斷瀏覽器特性，以及了解應用程式網頁上的人類互動程度。這些規則群組會叫用 AWS WAF 權杖管理，這會套用權杖標籤，供規則群組檢查。

- AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) – ACFP 規則需要具有有效字符的 Web 請求。如需規則的詳細資訊，請參閱[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。
- AWS WAF 詐騙控制帳戶接管預防 (ATP) – 防止大量和長時間持續用戶端工作階段的 ATP 規則需要具有有效字符和未過期挑戰時間戳記的 Web 請求。如需詳細資訊，請參閱[AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。
- AWS WAF 機器人控制 – 此規則群組中的目標規則會限制用戶端在沒有有效字符的情況下可傳送的 Web 請求數量，並且使用字符工作階段追蹤進行工作階段層級監控和管理。視需要，規則會套用 Challenge 和 CAPTCHA 規則動作，以強制執行權杖擷取和有效的用戶端行為。如需詳細資訊，請參閱[AWS WAF 機器人控制規則群組](#)。

AWS WAF 字符特性

每個字符具有下列特性：

- 權杖存放在名為 `aws-waf-token` 的 Cookie 中。
- 字符已加密。
- 權杖會使用包含下列資訊的黏性精細識別符來指紋用戶端工作階段：
 - 用戶端最近成功回應無聲挑戰的時間戳記。
 - 最終使用者最近成功回應 CAPTCHA 的時間戳記。只有在保護中使用 CAPTCHA 時，才會出現這種情況。
 - 有關用戶端和用戶端行為的其他資訊，有助於將您的合法用戶端與不需要的流量分開。此資訊包含各種用戶端識別符和用戶端訊號，可用於偵測自動化活動。收集的資訊是非唯一的，無法映射到個別的人類。
 - 所有字符都包含來自用戶端瀏覽器查詢的資料，例如自動化和瀏覽器設定不一致的指示。此資訊是由 Challenge 動作和用戶端應用程式 SDKs 執行的指令碼擷取。指令碼會主動查詢瀏覽器，並將結果放入字符中。
 - 此外，當您實作用戶端應用程式整合 SDK 時，權杖包含被動收集的有關最終使用者與應用程式頁面互動的資訊。互動包括滑鼠移動、按鍵，以及與頁面上存在的任何 HTML 格式的互動。此資訊有助於 AWS WAF 偵測用戶端中的人類互動程度，以挑戰似乎不是人類的使用者。如需用戶端整合的相關資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。

基於安全考量，AWS 不提供 AWS WAF 字符內容的完整描述或字符加密程序的詳細資訊。

在 中設定時間戳記過期和字符豁免時間 AWS WAF

本節說明挑戰和 CAPTCHA 時間戳記如何過期。

AWS WAF 使用挑戰和 CAPTCHA 豁免時間來控制單一用戶端工作階段可呈現挑戰或 CAPTCHA 的頻率。在最終使用者成功回應 CAPTCHA 之後，CAPTCHA 親和性時間會決定最終使用者維持免受其他 CAPTCHA 影響的時間長度。同樣地，挑戰抗擾性時間會決定用戶端工作階段在成功回應挑戰後，仍能免於再次受到挑戰的時間。

AWS WAF 權杖抗擾性時間的運作方式

AWS WAF 透過更新字符內的對應時間戳記，記錄對挑戰或 CAPTCHA 的成功回應。當 AWS WAF 檢查字符是否有挑戰或 CAPTCHA 時，會從目前時間減去時間戳記。如果結果大於設定的抗擾性時間，則時間戳記已過期。

權 AWS WAF 杖抗擾性時間的可設定層面

您可以在保護套件或 Web ACL 以及使用 或 規則 CAPTCHA Challenge 動作的任何規則中設定挑戰和 CAPTCHA 豁免時間。

- 兩個抗擾性時間的預設保護套件或 Web ACL 設定為 300 秒。
- 您可以為使用 CAPTCHA 或 Challenge 動作的任何規則指定豁免時間。如果您未指定規則的豁免時間，則會繼承保護套件或 Web ACL 的設定。
- 對於使用 CAPTCHA 或 Challenge 動作的規則群組內的規則，如果您未指定規則的豁免時間，則會從您使用規則群組的每個保護套件或 Web ACL 繼承設定。
- 應用程式整合 SDKs 使用 保護套件或 Web ACL 的挑戰抗擾性時間。
- 挑戰抗擾性時間的最小值為 300 秒。CAPTCHA 抗擾性時間的最小值為 60 秒。兩個抗擾性時間的最大值為 259,200 秒或三天。

您可以使用保護套件或 Web ACL 和規則層級豁免時間設定來調整 CAPTCHA 動作 Challenge、或 SDK 挑戰管理行為。例如，您可以設定規則來控制存取具有低抗擾性時間的高敏感資料，然後在保護套件或 Web ACL 中為其他規則和要繼承 SDKs 設定更高的抗擾性時間。

特別是針對 CAPTCHA，解決拼圖可能會降低您的客戶網站體驗，因此調校 CAPTCHA 豁免時間可協助您減輕對客戶體驗的影響，同時仍然提供您想要的保護。

如需有關調校使用 Challenge 和 CAPTCHA 規則動作之抗擾性時間的其他資訊，請參閱 [使用 CAPTCHA 和 Challenge 動作的最佳實務](#)。

在何處設定 AWS WAF 字符豁免時間

您可以在保護套件或 Web ACL 以及使用 Challenge 和 CAPTCHA 規則動作的規則中設定豁免時間。

如需管理保護套件或 Web ACL 及其規則的一般資訊，請參閱 [在中檢視 Web 流量指標 AWS WAF](#)。

在何處設定保護套件或 Web ACL 的豁免時間

- 主控台 – 當您編輯保護套件或 Web ACL 時，請在規則索引標籤中編輯和變更保護套件或 Web ACL CAPTCHA 組態和保護套件或 Web ACL 挑戰組態窗格中的設定。在 主控台中，您只能在建立保護套件或 Web ACL 之後，設定保護套件或 Web ACL CAPTCHA 並挑戰抗擾性時間。
- 在主控台外部 – 保護套件或 Web ACL 資料類型具有 CAPTCHA 和挑戰組態參數，您可以在保護套件或 Web ACL 上設定和提供建立和更新操作。

在何處設定規則的豁免時間

- 主控台 – 當您建立或編輯規則並指定 CAPTCHA 或 Challenge 動作時，您可以修改規則的抗擾性時間設定。
- 在主控台外部 – 規則資料類型具有 CAPTCHA 和挑戰組態參數，您可以在定義規則時設定這些參數。

在 中指定字符網域和網域清單 AWS WAF

本節說明如何設定在字符 AWS WAF 中使用的網域，以及在字符中接受的網域。

當為用戶端 AWS WAF 建立權杖時，它會使用權杖網域來設定權杖。當 AWS WAF 檢查 Web 請求中的字符時，如果字符的網域不符合任何被視為對保護套件或 Web ACL 有效的網域，則會拒絕字符為無效。

根據預設，AWS WAF 僅接受網域設定完全符合與保護套件或 Web ACL 相關聯之資源的主機網域的權杖。這是 Web 請求中 Host 標頭的值。在瀏覽器中，您可以在 JavaScript `window.location.hostname` 屬性和使用者在地址列中看到的地址中找到此網域。

您也可以在接受保護套件或 Web ACL 組態中指定可接受的字符網域，如下節所述。在此情況下，AWS WAF 接受與主機標頭完全相符，且與字符網域清單中的網域相符。

您可以在設定網域和評估保護套件或 Web ACL 中的權杖時，指定 AWS WAF 要使用的權杖網域。您指定的網域不能是公有字尾，例如 `gov.au`。如需無法使用的網域，請參閱公有字尾清單 https://publicsuffix.org/list/public_suffix_list.dat 下的清單。 <https://publicsuffix.org/list/>

AWS WAF 保護套件或 Web ACL 字符網域清單組態

您可以設定保護套件或 Web ACL，在多個受保護的資源之間共用權杖，方法是提供權杖網域清單，其中包含 AWS WAF 您要接受的其他網域。使用字符網域清單，AWS WAF 仍然接受資源的主機網域。此外，它接受字符網域清單中的所有網域，包括其字首的子網域。

例如，`example.com` 字符網域清單中的網域規格符合 `example.com` (來自 `http://example.com/`)、`api.example.com` (來自 `http://api.example.com/`) 和 `www.example.com` (來自 `http://www.example.com/`)。它不符合 `example.api.com` (來自 `http://example.api.com/`) 或 `apiexample.com` (來自 `http://apiexample.com/`)。

您可以在建立或編輯權杖網域時，在接受保護套件或 Web ACL 中設定權杖網域清單。如需管理保護套件或 Web ACL 的一般資訊，請參閱 [在 中檢視 Web 流量指標 AWS WAF](#)。

AWS WAF 字域網域設定

AWS WAF 會在挑戰指令碼的要求下建立權杖，由應用程式整合 SDKs 和 Challenge 和 CAPTCHA 規則動作執行。

權杖中 AWS WAF 設定的網域取決於請求權杖的挑戰指令碼類型，以及您提供的任何其他權杖網域組態。AWS WAF 會將權杖中的網域設定為可在組態中找到的最短、最一般的設定。

- JavaScript 開發套件 – 您可以使用字域網域規格來設定 JavaScript 開發套件，該規格可包含一或多個網域。您設定的網域必須是 AWS WAF 根據受保護主機網域和保護套件或 Web ACL 權杖網域清單接受的網域。

當為用戶端 AWS WAF 發出權杖時，它會將權杖網域設定為與主機網域相符且最短的權杖網域，從已設定清單中的主機網域和網域之間。例如，如果主機網域是 `api.example.com` 且權杖網域清單具有 `example.com`，AWS WAF 會在權杖 `example.com` 中使用，因為它符合主機網域且較短。如果您未在 JavaScript API 組態中提供字域網域清單，會將網域 AWS WAF 設定為受保護資源的主機網域。

如需詳細資訊，請參閱 [提供用於字域網域](#)。

- 行動開發套件 – 在您的應用程式程式碼中，您必須使用字域網域屬性設定行動開發套件。此屬性必須是根據受保護主機網域 AWS WAF 和保護套件或 Web ACL 字域網域清單接受的網域。

當為用戶端 AWS WAF 發出權杖時，它會使用此屬性做為權杖網域。AWS WAF 不會在其為行動 SDK 用戶端發出的權杖中使用主機網域。

如需詳細資訊，請參閱 [中的 WAFConfigurationDomainName 設定](#) [AWS WAF 行動 SDK 規格](#)。

- Challenge 動作 – 如果您在保護套件或 Web ACL 中指定權杖網域清單，會將權杖網域 AWS WAF 設定為與主機網域相符且最短的網域，從主機網域和清單中的網域。例如，如果主機網域是 `api.example.com` 且權杖網域清單具有 `example.com`，會在權杖 AWS WAF `example.com` 中使用，因為它符合主機網域且較短。如果您未在保護套件或 Web ACL 中提供字域網域清單，會將網域 AWS WAF 設定為受保護資源的主機網域。

中的字域標籤類型 AWS WAF

本節說明 AWS WAF 權杖管理新增至 Web 請求的標籤。如需標籤的一般資訊，請參閱 [中的 Web 請求標籤 AWS WAF](#)。

當您使用任何 AWS WAF 機器人或詐騙控制受管規則群組時，規則群組會使用 AWS WAF 權杖管理來檢查 Web 請求權杖，並將權杖標籤套用至請求。如需受管規則群組的相關資訊，請參閱 [AWS WAF](#)

[詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)、[AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)和 [AWS WAF 機器人控制規則群組](#)。

Note

AWS WAF 只有在您使用其中一個智慧型威脅緩解受管規則群組時，才會套用權杖標籤。

權杖管理可以將下列標籤新增至 Web 請求。

用戶端工作階段標籤

標籤 `aws:waf:managed:token:id:identifier` 包含 AWS WAF 字串管理用來識別用戶端工作階段的唯一識別符。如果用戶端取得新的字串，例如在捨棄正在使用的字串之後，識別符可能會變更。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

瀏覽器指紋標籤

標籤 `aws:waf:managed:token:fingerprint:fingerprint-identifier` 包含強大的瀏覽器指紋識別符，權杖管理會從各種用戶端瀏覽器訊號運算。此識別符在多個字串擷取嘗試中保持不變。指紋識別符對單一用戶端來說不是唯一的。

Note

AWS WAF 不會報告此標籤的 Amazon CloudWatch 指標。

字串狀態標籤：標籤命名空間字首

字串狀態標籤會報告字串的狀態，以及其中包含的挑戰和 CAPTCHA 資訊。

每個字串狀態標籤都以下列其中一個命名空間字首開頭：

- `aws:waf:managed:token:` – 用來報告字串的一般狀態，以及報告字串挑戰資訊的狀態。
- `aws:waf:managed:captcha:` – 用來報告字串 CAPTCHA 資訊的狀態。

字符狀態標籤：標籤名稱

在字首後面，標籤的其餘部分提供詳細的字符狀態資訊：

- `accepted` – 請求字符存在且包含下列項目：
 - 有效的挑戰或 CAPTCHA 解決方案。
 - 未過期的挑戰或 CAPTCHA 時間戳記。
 - 適用於保護套件或 Web ACL 的網域規格。

範例：標籤 `aws:waf:managed:token:accepted` 指出 Web 請求的權杖具有有效的挑戰解決方案、未過期的挑戰時間戳記，以及有效的網域。

- `rejected` – 請求字符存在，但不符合接受條件。

除了拒絕的標籤之外，字符管理還會新增自訂標籤命名空間和名稱，以指出原因。

- `rejected:not_solved` – 字符缺少挑戰或 CAPTCHA 解決方案。
- `rejected:expired` – 權杖的挑戰或 CAPTCHA 時間戳記已過期，根據您的保護套件或 Web ACL 設定的權杖抗擾性時間而定。
- `rejected:domain_mismatch` – 字符的網域不符合您的保護套件或 Web ACL 的字符網域組態。
- `rejected:invalid` – AWS WAF 無法讀取指定的字符。

範例：標籤 `aws:waf:managed:captcha:rejected` 和 `aws:waf:managed:captcha:rejected:expired` 一起指出請求沒有有效的 CAPTCHA 解決方法，因為字符中的 CAPTCHA 時間戳記已超過保護套件或 Web ACL 中設定的 CAPTCHA 字符豁免時間。

- `absent` – 請求沒有字符或字符管理器無法讀取。

範例：標籤 `aws:waf:managed:captcha:absent` 指出請求沒有字符。

封鎖沒有有效 AWS WAF 字符的請求

本節說明如何封鎖在使用 AWS WAF 行動 SDK 時缺少字符的登入請求。

當您使用智慧型威脅 AWS 受管規則規則群組 `AWSMangedRulesACFPRuleSet`、`AWSMangedRulesATPRuleSet` 和 `AWSMangedRulesBotControlRuleSet`，規則群組會叫用 AWS WAF 權杖管理來評估 Web 請求權杖的狀態，並相應地標記請求。

Note

字符標籤只會套用到您使用其中一個受管規則群組評估的 Web 請求。

如需權杖管理套用之標籤的相關資訊，請參閱上一節：[中的字符標籤類型 AWS WAF](#)。

智慧型威脅緩解受管規則群組接著會處理字符需求，如下所示：

- `AWSManagedRulesACFPRuleSet AllRequests` 規則設定為針對所有請求執行 Challenge 動作，有效地封鎖任何沒有 `accepted` 字符標籤的。
- 會 `AWSManagedRulesATPRuleSet` 封鎖具有 `rejected` 字符標籤的請求，但不會封鎖具有 `absent` 字符標籤的請求。
- `AWSManagedRulesBotControlRuleSet` 目標保護層級會在用戶端傳送五個沒有 `accepted` 字符標籤的請求後，向用戶端提出挑戰。它不會封鎖沒有有效字符的個別請求。規則群組的常見保護層級不會管理字符需求。

如需智慧型威脅規則群組的其他詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)、[AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#) 和 [AWS WAF 機器人控制規則群組](#)。

使用 Bot Control 或 ATP 受管規則群組時，封鎖缺少字符的請求

使用 Bot Control 和 ATP 規則群組時，如果請求沒有有效的權杖，則可以結束規則群組評估，並繼續由保護套件或 Web ACL 進行評估。

若要封鎖缺少字符或字符遭到拒絕的所有請求，請在受管規則群組之後新增要立即執行的規則，以擷取和封鎖規則群組未為您處理的請求。

以下是使用 ATP 受管規則群組之保護套件或 Web ACL 的範例 JSON 清單。保護套件或 Web ACL 具有新增的規則，可擷取並處理 `aws:waf:managed:token:absent` 標籤。規則會將評估範圍縮小為前往登入端點的 Web 請求，以符合 ATP 規則群組的範圍。新增的規則會以粗體列出。

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Rules": [
    {
      "Name": "ExampleRule",
      "Id": "11111111-2222-3333-4444-555555555555",
      "Priority": 1,
      "Statement": {
        "And": [
          {
            "AWSManagedRulesManagedRuleSet": {
              "RuleSetName": "AWSManagedRulesBotControlRuleSet"
            }
          },
          {
            "ByteMatch": {
              "FieldToMatch": "URI",
              "Text": "example.com",
              "Position": 0,
              "PositionType": "EXACT"
            }
          }
        ]
      },
      "Action": {
        "Block": {}
      },
      "Enabled": true
    }
  ]
}
```

```
"Description": "",
"Rules": [
  {
    "Name": "AWS-AWSManagedRulesATPRuleSet",
    "Priority": 1,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesATPRuleSet",
        "ManagedRuleGroupConfigs": [
          {
            "AWSManagedRulesATPRuleSet": {
              "LoginPath": "/web/login",
              "RequestInspection": {
                "PayloadType": "JSON",
                "UsernameField": {
                  "Identifier": "/form/username"
                },
                "PasswordField": {
                  "Identifier": "/form/password"
                }
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,  
    "MetricName": "AWS-AWSManagedRulesATPRuleSet"  
  },  
{  
  "Name": "RequireTokenForLogins",  
  "Priority": 2,  
  "Statement": {  
    "AndStatement": {  
      "Statements": [  
        {  
          "Statement": {  
            "LabelMatchStatement": {  
              "Scope": "LABEL",  
              "Key": "awsaf:managed:token:absent"  
            }  
          },  
          {  
            "ByteMatchStatement": {  
              "SearchString": "/web/login",  
              "FieldToMatch": {  
                "UriPath": {}  
              },  
              "TextTransformations": [  
                {  
                  "Priority": 0,  
                  "Type": "NONE"  
                }  
              ],  
              "PositionalConstraint": "STARTS_WITH"  
            }  
          },  
          {  
            "ByteMatchStatement": {  
              "SearchString": "POST",  
              "FieldToMatch": {  
                "Method": {}  
              },  
              "TextTransformations": [  
                {  
                  "Priority": 0,  
                  "Type": "NONE"  
                }  
              ]  
            }  
          }  
        ]  
      }  
    }  
  }  
}
```

```

        ],
        "PositionalConstraint": "EXACTLY"
    }
}
]
}
},
"Action": {
    "Block": {}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "RequireTokenForLogins"
}
}
],
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"RetrofittedByFirewallManager": false,
"LabelNamespace": "aws-waf-111111111111:webacl:exampleWebACL:"
}

```

屬於 CloudFront 原始伺服器的 Application Load Balancer 所需的組態

如果您將保護套件或 Web ACL 與 Application Load Balancer 建立關聯，並將 Application Load Balancer 部署為 CloudFront 分佈的原始伺服器，請閱讀本節。

使用此架構時，您需要提供下列額外組態，才能正確處理字符資訊。

- 設定 CloudFront 將 `aws-waf-token` Cookie 轉送至 Application Load Balancer。根據預設，CloudFront 會從 Web 請求移除 Cookie，然後再將其轉送至原始伺服器。若要使用 Web 請求保留權杖 Cookie，請將 CloudFront 快取行為設定為僅包含權杖 Cookie 或所有 Cookie。如需如何執行此操作的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[根據 Cookie 快取內容](#)。
- 設定，AWS WAF 使其將 CloudFront 分佈的網域識別為有效的字符網域。根據預設，CloudFront 會將 Host 標頭設定為 Application Load Balancer 原始伺服器，AWS WAF 並使用該標頭做為受保護資源的網域。不過，用戶端瀏覽器會將 CloudFront 分佈視為主機網域，而為用戶端產生的字符會

使用 CloudFront 網域作為字網域。如果沒有任何其他組態，當 AWS WAF 檢查受保護的資源網域與權杖網域，就會得到不相符。若要修正此問題，請將 CloudFront 分佈網域名稱新增至保護套件或 Web ACL 組態中的字網域清單。如需如何進行該服務的詳細資訊，請參閱[AWS WAF 保護套件或 Web ACL 字網域清單組態](#)。

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP)

本節說明 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 的功能。

帳戶建立詐騙是一種線上非法活動，攻擊者會嘗試建立一或多個仿造帳戶。攻擊者使用偽造帳戶進行詐騙活動，例如濫用促銷和註冊獎金、冒充某人，以及網路釣魚等網路攻擊。存在仿造帳戶可能會損害您與客戶的評價並暴露在金融詐騙中，進而對您的業務造成負面影響。

您可以透過實作 ACFP 功能來監控和控制帳戶建立詐騙嘗試。AWS WAF 會在 AWS 受管規則規則群組中提供此功能，並 AWSManagedRulesACFPRuleSet 搭配應用程式整合 SDKs。

ACFP 受管規則群組會標記和管理可能屬於惡意帳戶建立嘗試一部分的請求。規則群組會透過檢查用戶端傳送到您應用程式帳戶註冊端點的帳戶建立嘗試來執行此操作。

ACFP 透過監控異常活動的帳戶註冊請求，以及自動封鎖可疑請求，來保護您的帳戶註冊頁面。規則群組使用請求識別符、行為分析和機器學習來偵測詐騙請求。

- 請求檢查 – ACFP 可讓您查看和控制使用遭竊登入資料的異常帳戶建立嘗試和嘗試，以防止建立詐騙帳戶。ACFP 會針對其遭竊的登入資料資料庫檢查電子郵件和密碼組合，該資料庫會在深色 Web 上發現新的洩漏登入資料時定期更新。ACFP 會評估電子郵件地址中使用的網域，並監控電話號碼和地址欄位的使用，以驗證項目並偵測詐騙行為。ACFP 會依 IP 地址和用戶端工作階段彙總資料，以偵測和封鎖傳送過多可疑請求的用戶端。
- 回應檢查 – 針對 CloudFront 分佈，除了檢查傳入的帳戶建立請求之外，ACFP 規則群組還會檢查應用程式對帳戶建立嘗試的回應，以追蹤成功和失敗率。使用此資訊，ACFP 可以暫時封鎖嘗試失敗次數過多的用戶端工作階段或 IP 地址。會以非同步方式 AWS WAF 執行回應檢查，因此這不會增加 Web 流量的延遲。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

 Note

ACFP 功能不適用於 Amazon Cognito 使用者集區。

主題

- [AWS WAF ACFP 元件](#)
- [搭配 ACFP 使用應用程式整合 SDKs](#)
- [將 ACFP 受管規則群組新增至 Web ACL](#)
- [測試和部署 ACFP](#)
- [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 範例](#)

AWS WAF ACFP 元件

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 的主要元件如下：

- **AWSManagedRulesACFPRuleSet** – 此 AWS 受管規則規則群組中的規則會偵測、標記和處理各種類型的詐騙帳戶建立活動。規則群組會檢查用戶端傳送至指定帳戶註冊端點的 HTTP GET text/html 請求，以及用戶端傳送至指定帳戶註冊端點的 POST Web 請求。對於受保護的 CloudFront 分佈，規則群組也會檢查分佈傳回至帳戶建立請求的回應。如需此規則群組規則的清單，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。您可以使用受管規則群組參考陳述式，將此規則群組包含在保護套件或 Web ACL 中。如需使用此規則群組的詳細資訊，請參閱 [將 ACFP 受管規則群組新增至 Web ACL](#)。

 Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

- 有關應用程式帳戶註冊和建立頁面的詳細資訊 – 當您將 AWSManagedRulesACFPRuleSet 規則群組新增至保護套件或 Web ACL 時，必須提供帳戶註冊和建立頁面的相關資訊。這可讓規則群組縮小其檢查的請求範圍，並正確驗證帳戶建立 Web 請求。註冊頁面必須接受 GET 文字/html 請求。帳戶建立路徑必須接受 POST 請求。ACFP 規則群組適用於電子郵件格式的使用者名稱。如需詳細資訊，請參閱 [將 ACFP 受管規則群組新增至 Web ACL](#)。
- 對於受保護的 CloudFront 分佈，有關應用程式如何回應帳戶建立嘗試的詳細資訊 – 您可以提供應用程式對帳戶建立嘗試回應的詳細資訊，而 ACFP 規則群組會從單一 IP 地址或單一用戶端工作階段

追蹤和管理大量帳戶建立嘗試。如需設定此選項的詳細資訊，請參閱 [將 ACFP 受管規則群組新增至 Web ACL](#)。

- JavaScript 和行動應用程式整合 SDKs – 使用 ACFP 實作實作 AWS WAF JavaScript 和行動 SDKs，以啟用規則群組提供的完整功能集。許多 ACFP 規則使用 SDKs 提供的資訊進行工作階段層級用戶端驗證和行為彙總，這是將合法用戶端流量與機器人流量分開的必要條件。如需 SDK 的詳細資訊，請參閱「[中的用戶端應用程式整合 AWS WAF](#)」。

您可以結合 ACFP 實作與下列項目，協助您監控、調整和自訂保護。

- 記錄和指標 – 您可以監控流量，並透過為保護套件或 Web ACL 設定和啟用日誌、Amazon Security Lake 資料收集和 Amazon CloudWatch 指標，了解 ACFP 受管規則群組如何影響流量。AWSManagedRulesACFPRuleSet 新增至 Web 請求的標籤會包含在資料中。如需選項的相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)、[使用 Amazon CloudWatch 監控](#) 和 [什麼是 Amazon Security Lake ?](#)。

根據您的需求和您看到的流量，您可能想要自訂 AWSManagedRulesACFPRuleSet 實作。例如，您可能想要從 ACFP 評估中排除一些流量，或者您可能想要使用縮小範圍陳述式或標籤比對規則等 AWS WAF 功能，改變它處理其識別的一些帳戶建立詐騙嘗試的方式。

- 標籤和標籤比對規則 – 對於 中的任何規則 AWSManagedRulesACFPRuleSet，您可以將封鎖行為切換為計數，然後比對規則新增的標籤。使用此方法來自訂如何處理由 ACFP 受管規則群組識別的 Web 請求。如需標記和使用標籤比對陳述式的詳細資訊，請參閱 [標籤比對規則陳述式](#) 和 [中的 Web 請求標籤 AWS WAF](#)。
- 自訂請求和回應 – 您可以將自訂標頭新增至您允許的請求，也可以為封鎖的請求傳送自訂回應。若要這樣做，請將標籤比對與 AWS WAF 自訂請求和回應功能配對。如需自訂請求和回應的詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

搭配 ACFP 使用應用程式整合 SDKs

我們強烈建議您實作應用程式整合 SDKs，以最有效地使用 ACFP 規則群組。

- 完整的規則群組功能 – ACFP 規則 SignalClientHumanInteractivityAbsentLow 僅適用於由應用程式整合填入的字符。此規則會偵測和管理與應用程式頁面的異常人類互動。應用程式整合 SDKs 可以透過滑鼠移動、按鍵和其他測量來偵測正常的人類互動。由規則動作傳送 CAPTCHA 且 Challenge 無法提供此資料類型的間質。
- 降低延遲 – 規則群組規則會將 Challenge 規則動作 AllRequests 套用至尚未具有挑戰字符的任何請求。發生這種情況時，規則群組會評估請求兩次：一次沒有字符，然後在透過 Challenge 動作間質取

得字符之後再評估一次。您只需使用 AllRequests 規則就不需要支付任何額外費用，但此方法會增加 Web 流量的負荷，並增加最終使用者體驗的延遲。如果您使用應用程式整合取得字符用戶端，在傳送帳戶建立請求之前，ACFP 規則群組會評估請求一次。

如需規則群組功能的詳細資訊，請參閱[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

如需 SDKs 的相關資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需 AWS WAF 權杖的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。如需規則動作的相關資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

將 ACFP 受管規則群組新增至 Web ACL

本節說明如何新增和設定 AWSManagedRulesACFPRuleSet 規則群組。

若要設定 ACFP 受管規則群組來辨識 Web 流量中的帳戶建立詐騙活動，您可以提供有關用戶端如何存取您的註冊頁面，並將帳戶建立請求傳送至應用程式的資訊。對於受保護的 Amazon CloudFront 分佈，您也可以提供應用程式如何回應帳戶建立請求的相關資訊。此組態是受管規則群組的一般組態以外的組態。

如需規則群組描述和規則清單，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

Note

ACFP 遭竊的登入資料資料庫僅包含電子郵件格式的使用者名稱。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。如需如何將受管規則群組新增至保護套件或 Web ACL 的基本資訊，請參閱 [透過主控台將受管規則群組新增至保護套件或 Web ACL](#)。

遵循最佳實務

根據的最佳實務使用 ACFP 規則群組 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

在保護套件或 Web ACL 中使用 AWSManagedRulesACFPRuleSet 規則群組

1. 將 AWS 受管規則群組 AWSManagedRulesACFPRuleSet 新增至您的保護套件或 Web ACL，並在儲存之前編輯規則群組設定。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

2. 在規則群組組態窗格中，提供 ACFP 規則群組用來檢查帳戶建立請求的資訊。
 - a. 對於在路徑中使用規則運算式，如果您 AWS WAF 想要為註冊和帳戶建立頁面路徑規格執行規則運算式比對，請開啟此選項。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外。程式庫記錄在 [PCRE - Perl 相容規則表達式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

- b. 針對註冊頁面路徑，提供應用程式的註冊頁面端點路徑。此頁面必須接受 GET 文字/html 請求。規則群組只會檢查對指定註冊頁面端點的 HTTP GET text/html 請求。

Note

端點比對不區分大小寫。Regex 規格不得包含旗標 `(?-i)`，這會停用不區分大小寫的比對。字串規格必須以正斜線 開頭/。

例如，對於 URL `https://example.com/web/registration`，您可以提供字串路徑規格 `/web/registration`。以您提供的路徑開頭的註冊頁面路徑會被視為相符項目。例如，`/web/registration` 符合註冊路徑 `/web/registration`、`/web/registrationPage`、`/web/registration/` 和 `/web/registration/thisPage`，但不符合路徑 `/home/web/registration` 或 `/website/registration`。

Note

確保您的最終使用者在提交帳戶建立請求之前載入註冊頁面。這有助於確保來自用戶端的帳戶建立請求包含有效的字符。

- c. 針對帳戶建立路徑，請在網站中提供接受已完成新使用者詳細資訊的 URI。此 URI 必須接受 POST 請求。

 Note

端點比對不區分大小寫。Regex 規格不得包含旗標 (?-i)，這會停用不區分大小寫的比對。字串規格必須以正斜線 開頭/。

例如，對於 URL `https://example.com/web/newaccount`，您可以提供字串路徑規格 `/web/newaccount`。以您提供的路徑開頭的帳戶建立路徑會被視為相符項目。例如，`/web/newaccount` 符合帳戶建立路徑 `/web/newaccount`、`/web/newaccountPage`、`/web/newaccount/` 和 `/web/newaccount/thisPage`，但不符合路徑 `/home/web/newaccount` 或 `/website/newaccount`。

- d. 針對請求檢查，提供請求承載類型，以及提供使用者名稱、密碼和其他帳戶建立詳細資訊之請求內文中的欄位名稱，以指定應用程式接受帳戶建立嘗試的方式。

 Note

對於主要地址和電話號碼欄位，請依欄位出現在請求承載中的順序提供欄位。

欄位名稱的規格取決於承載類型。

- JSON 承載類型 – 以 JSON 指標語法指定欄位名稱。如需有關 JSON Pointer 語法的資訊，請參閱 Internet Engineering Task Force (IETF) 文件 [JavaScript 物件標記法 \(JSON\) Pointer](#)。

例如，對於下列範例 JSON 承載，使用者名稱欄位規格為 `/signupform/username`，主要地址欄位規格為 `/signupform/addrp1`、`/signupform/addrp2` 和 `/signupform/addrp3`。

```
{
  "signupform": {
    "username": "THE_USERNAME",
    "password": "THE_PASSWORD",
    "addrp1": "PRIMARY_ADDRESS_LINE_1",
    "addrp2": "PRIMARY_ADDRESS_LINE_2",
    "addrp3": "PRIMARY_ADDRESS_LINE_3",
    "phonepcode": "PRIMARY_PHONE_CODE",
    "phonenumber": "PRIMARY_PHONE_NUMBER"
  }
}
```

```
}  
}
```

- FORM_ENCODED 承載類型 – 使用 HTML 表單名稱。

例如，對於具有名為 username1 和 之使用者和密碼輸入元素的 HTML 表單 password1，使用者名稱欄位規格為 username1，密碼欄位規格為 password1。

- e. 如果您要保護 Amazon CloudFront 分佈，請在回應檢查下指定應用程式在回應帳戶建立嘗試時如何表示成功或失敗。

Note

ACFP 回應檢查僅適用於保護 CloudFront 分佈的保護套件或 Web ACLs。

在您要 ACFP 檢查的帳戶建立回應中指定單一元件。對於內文和 JSON 元件類型，AWS WAF 可以檢查元件的前 65,536 個位元組 (64 KB)。

提供元件類型的檢查條件，如 界面所示。您必須同時提供成功和失敗條件，才能在元件中檢查。

例如，假設您的應用程式在回應的狀態碼中指出帳戶建立嘗試的狀態，並使用 200 OK 表示成功和 401 Unauthorized 或 403 Forbidden 表示失敗。您會將回應檢查元件類型設定為狀態碼，然後在成功文字方塊中輸入 200，然後在失敗文字方塊中輸入 401 在第一行和第二 403 行中輸入。

ACFP 規則群組只會計算符合您成功或失敗檢查條件的回應。規則群組規則在計算回應中的成功率過高時對用戶端採取行動，以減輕大量帳戶建立嘗試。如需規則群組規則的準確行為，請務必提供成功和失敗帳戶建立嘗試的完整資訊。

若要查看檢查帳戶建立回應的規則，請在 VolumetricSessionSuccessfulResponse 的規則清單中尋找 VolumetricIPSuccessfulResponse 和 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

3. 提供您想要用於規則群組的任何其他組態。

您可以將縮小範圍陳述式新增至受管規則群組陳述式，進一步限制規則群組檢查的請求範圍。例如，您只能檢查具有特定查詢引數或 Cookie 的請求。規則群組只會檢查符合您縮小範圍陳述式中條件，並傳送至您在規則群組組態中指定的帳戶註冊和帳戶建立路徑的請求。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

4. 將變更儲存至保護套件或 Web ACL。

在部署生產流量的 ACFP 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。如需指引，請參閱以下章節。

測試和部署 ACFP

本節提供為您的網站設定和測試 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作的一般指引。您選擇遵循的特定步驟將取決於您收到的需求、資源和 Web 請求。

此資訊是 所提供測試和調校的一般資訊之外的 [測試和調校您的 AWS WAF 保護](#)。

Note

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，這取決於您選擇的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在 中的資源 AWS 受到適當保護。

生產流量風險

在部署生產流量的 ACFP 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整規則，然後再啟用它們。

AWS WAF 提供測試登入資料，您可以用來驗證 ACFP 組態。在下列程序中，您將設定測試保護套件或 Web ACL 以使用 ACFP 受管規則群組、設定規則以擷取規則群組新增的標籤，然後使用這些測試憑證執行帳戶建立嘗試。您將檢查帳戶建立嘗試的 Amazon CloudWatch 指標，以確認您的保護套件或 Web ACL 已正確管理嘗試。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。

設定和測試 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 在計數模式中新增 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

將 AWS 受管規則規則群組 `AWSManagedRulesACFPRuleSet` 新增至新的或現有的保護套件或 Web ACL，並加以設定，使其不會變更目前的保護套件或 Web ACL 行為。如需此規則群組之規則和標籤的詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

- 當您新增受管規則群組時，請進行編輯並執行下列動作：
 - 在規則群組組態窗格中，提供應用程式帳戶註冊和建立頁面的詳細資訊。ACFP 規則群組會使用此資訊來監控登入活動。如需詳細資訊，請參閱[將 ACFP 受管規則群組新增至 Web ACL](#)。
 - 在規則窗格中，開啟覆寫所有規則動作下拉式清單，然後選擇 Count。使用此組態，會根據規則群組中的所有規則 AWS WAF 評估請求，並僅計算該結果的相符項目，同時仍將標籤新增至請求。如需詳細資訊，請參閱[覆寫規則群組中的規則動作](#)。

透過此覆寫，您可以監控 ACFP 受管規則的潛在影響，以判斷您是否要新增例外狀況，例如內部使用案例的例外狀況。

- 將規則群組放在保護套件或 Web ACL 中，以便在您現有的規則之後進行評估，其優先順序設定在數值上高於您已使用的任何規則或規則群組。如需詳細資訊，請參閱[設定規則優先順序](#)。

如此一來，您目前的流量處理不會中斷。例如，如果您有偵測惡意流量的規則，例如 SQL Injection 或跨網站指令碼，它們將繼續偵測並記錄。或者，如果您有允許已知非惡意流量的規則，它們可以繼續允許該流量，而不會被 ACFP 受管規則群組封鎖。您可以在測試和調校活動期間決定調整處理順序。

2. 實作應用程式整合 SDKs

將 AWS WAF JavaScript SDK 整合到瀏覽器的帳戶註冊和帳戶建立路徑。AWS WAF 也提供行動 SDKs 來整合 iOS 和 Android 裝置。如需整合 SDKs 的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需此建議的相關資訊，請參閱 [搭配 ACFP 使用應用程式整合 SDKs](#)。

Note

如果您無法使用應用程式整合 SDKs，則可以在保護套件或 Web ACL 中編輯 ACFP 規則群組，並移除您在規則上放置的覆寫，以測試 ACFP `AllRequests` 規則群組。這會啟用規則 Challenge 的動作設定，以確保請求包含有效的挑戰字符。

首先在測試環境中執行此操作，然後在生產環境中非常小心。這種方法可能會封鎖使用者。例如，如果您的註冊頁面路徑不接受GET文字/html 請求，則此規則組態可以有效地封鎖註冊頁面上的所有請求。

3. 啟用保護套件或 Web ACL 的記錄和指標

視需要設定 保護套件或 Web ACL 的記錄、Amazon Security Lake 資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見性工具來監控 ACFP 受管規則群組與流量的互動。

- 如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
- 如需 Amazon Security Lake 的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的什麼是 Amazon Security Lake？以及從 AWS 服務收集資料。
- 如需 Amazon CloudWatch 指標的相關資訊，請參閱[使用 Amazon CloudWatch 監控](#)。
- 如需 Web 請求取樣的詳細資訊，請參閱[檢視 Web 請求的範例](#)。

4. 將保護套件或 Web ACL 與資源建立關聯

如果保護套件或 Web ACL 尚未與測試資源建立關聯，請建立關聯。如需相關資訊，請參閱[將保護與 AWS 資源建立關聯或取消關聯](#)。

5. 監控流量和 ACFP 規則相符項目

請確定您的正常流量正在流動，而且 ACFP 受管規則群組規則正在將標籤新增至相符的 Web 請求。您可以在日誌中查看標籤，並在 Amazon CloudWatch 指標中查看 ACFP 和標籤指標。在日誌中，您已覆寫規則群組中計數的規則會顯示在 `ruleGroupList` 並將 `action` 設定為計數，並 `overriddenAction` 指出您覆寫的已設定規則動作。

6. 測試規則群組的登入資料檢查功能

使用測試洩露的登入資料執行帳戶建立嘗試，並檢查規則群組是否如預期相符。

- a. 存取受保護資源的帳戶註冊頁面，並嘗試新增新帳戶。使用下列 AWS WAF 測試登入資料對並輸入任何測試
 - 使用者：WAF_TEST_CREDENTIAL@wafexample.com
 - 密碼：WAF_TEST_CREDENTIAL_PASSWORD

這些測試登入資料會分類為遭到入侵的登入資料，而 ACFP 受管規則群組會將awsaf:managed:aws:acfp:signal:credential_compromised標籤新增至帳戶建立請求，您可以在日誌中看到。

- b. 在保護套件或 Web ACL 日誌中，在測試帳戶建立請求的日誌項目的 labels 欄位中尋找awsaf:managed:aws:acfp:signal:credential_compromised標籤。如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

驗證規則群組如預期擷取遭入侵的登入資料後，您可以採取步驟來設定其實作，以因應受保護資源的需求。

7. 針對 CloudFront 分佈，測試規則群組的大量帳戶建立嘗試管理

針對您為 ACFP 規則群組設定的每個成功回應條件執行此測試。在測試之間等待至少 30 分鐘。

- a. 針對您的每個成功條件，識別在回應中使用該成功條件成功的帳戶建立嘗試。然後，從單一用戶端工作階段，在 30 分鐘內執行至少 5 次成功的帳戶建立嘗試。使用者通常只會在您的網站上建立單一帳戶。

第一次成功建立帳戶後，VolumetricSessionSuccessfulResponse規則應該會根據您的規則動作覆寫，開始比對您帳戶建立回應的其餘部分，並加上標籤和計數。規則可能會因為延遲而遺漏前一或兩個。

- b. 在保護套件或 Web ACL 日誌中，在測試帳戶建立 Web 請求的日誌項目的 labels 欄位中尋找awsaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation標籤。如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

這些測試會檢查規則彙總的成功計數是否超過規則的閾值，以驗證您的成功條件是否符合您的回應。達到閾值後，如果您繼續從相同工作階段傳送帳戶建立請求，則規則將繼續相符，直到成功率低於閾值為止。超過閾值時，規則會同時符合工作階段地址中成功或失敗的帳戶建立嘗試。

8. 自訂 ACFP Web 請求處理

視需要新增您自己的規則，明確允許或封鎖請求，以變更 ACFP 規則處理它們的方式。

例如，您可以使用 ACFP 標籤來允許或封鎖請求，或自訂請求處理。您可以在 ACFP 受管規則群組之後新增標籤比對規則，以篩選要套用之處理方式的標記請求。測試之後，請將相關的 ACFP 規則保持在計數模式中，並在您的自訂規則中維護請求處理決策。如需範例，請參閱「[ACFP 範例：針對遭到入侵的登入資料的自訂回應](#)」。

9. 移除您的測試規則並啟用 ACFP 受管規則群組設定

根據您的情況，您可能已決定要將一些 ACFP 規則保留在計數模式中。對於您想要在規則群組中依設定執行的規則，請在保護套件或 Web ACL 規則群組組態中停用計數模式。完成測試後，您也可以移除測試標籤比對規則。

10. 監控和調校

為了確保 Web 請求可依您想要的方式處理，請在啟用您要使用的 ACFP 功能後密切監控流量。視需要使用規則群組上的規則計數覆寫和您自己的規則來調整行為。

完成測試 ACFP 規則群組實作後，如果您尚未將 AWS WAF JavaScript 開發套件整合至瀏覽器的帳戶註冊和帳戶建立頁面，我們強烈建議您這麼做。AWS WAF 也提供行動 SDKs，以整合 iOS 和 Android 裝置。如需整合 SDKs 的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需此建議的相關資訊，請參閱 [搭配 ACFP 使用應用程式整合 SDKs](#)。

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 範例

本節顯示滿足 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作常用案例的範例組態。

每個範例都會提供使用案例的描述，然後在自訂設定規則的 JSON 清單中顯示解決方案。

Note

您可以透過主控台保護套件或 Web ACL JSON 下載或規則 JSON 編輯器，或透過 APIs 和命令列界面中的 getWebACL 操作，擷取這些範例中顯示的 JSON 清單。

主題

- [ACFP 範例：簡易組態](#)
- [ACFP 範例：針對遭到入侵的登入資料的自訂回應](#)
- [ACFP 範例：回應檢查組態](#)

ACFP 範例：簡易組態

下列 JSON 清單顯示具有 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組的範例保護套件或 Web ACL。請注意額外的 CreationPath 和 RegistrationPagePath 組態，以及承載類型和在承載中尋找新帳戶資訊所需的資訊，以便進行驗證。規則群組會使用此資訊來監控和管理您的帳戶建

立請求。此 JSON 包含保護套件或 Web ACL 自動產生的設定，例如標籤命名空間和保護套件或 Web ACL 的應用程式整合 URL。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    }
                  ]
                }
              }
            }
          ]
        }
      }
    }
  ]
}
```

```
        "Identifier": "/form/phonenumber"
      }
    ],
    "AddressFields": [
      {
        "Identifier": "/form/name"
      },
      {
        "Identifier": "/form/street-address"
      },
      {
        "Identifier": "/form/city"
      },
      {
        "Identifier": "/form/state"
      },
      {
        "Identifier": "/form/zipcode"
      }
    ]
  },
  "EnableRegexInPath": false
}

]
}
},
"OverrideAction": {
  "None": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
}
},
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
"Capacity": 50,
"ManagedByFirewallManager": false,
```

```
"RetrofittedByFirewallManager": false,
"LabelNamespace": "aws:waf:111122223333:webacl:simpleACFP:"
}
```

ACFP 範例：針對遭到入侵的登入資料的自訂回應

根據預設，規則群組執行的登入資料檢查會透過標記請求並封鎖該請求，來處理AWSManagedRulesACFPRuleSet遭到入侵的登入資料。如需規則群組和規則行為的詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

若要通知使用者他們提供的帳戶登入資料已遭到入侵，您可以執行下列動作：

- 將**SignalCredentialCompromised**規則覆寫為 Count - 這會導致規則僅計數和標記相符請求。
- 使用自訂處理新增標籤比對規則 – 設定此規則以符合 ACFP 標籤，並執行您的自訂處理。

下列保護套件或 Web ACL 清單顯示先前範例中的 ACFP 受管規則群組，規則SignalCredentialCompromised動作會覆寫為計數。使用此組態時，當此規則群組評估任何使用遭入侵憑證的 Web 請求時，它會標記請求，但不會將其封鎖。

此外，保護套件或 Web ACL 現在具有名為的自訂回應aws-waf-credential-compromised和名為的新規則AccountSignupCompromisedCredentialsHandling。規則優先順序是高於規則群組的數值設定，因此會在保護套件或 Web ACL 評估中的規則群組之後執行。新規則會比對具有規則群組遭入侵憑證標籤的任何請求。當規則找到相符項目時，它會將Block動作套用至具有自訂回應內文的請求。自訂回應內文會向最終使用者提供其登入資料遭到入侵的資訊，並提議採取動作。

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
```

```
"ManagedRuleGroupConfigs": [
  {
    "AWSManagedRulesACFPRuleSet": {
      "CreationPath": "/web/signup/submit-registration",
      "RegistrationPagePath": "/web/signup/registration",
      "RequestInspection": {
        "PayloadType": "JSON",
        "UsernameField": {
          "Identifier": "/form/username"
        },
        "PasswordField": {
          "Identifier": "/form/password"
        },
        "EmailField": {
          "Identifier": "/form/email"
        },
        "PhoneNumberFields": [
          {
            "Identifier": "/form/country-code"
          },
          {
            "Identifier": "/form/region-code"
          },
          {
            "Identifier": "/form/phonenummer"
          }
        ],
        "AddressFields": [
          {
            "Identifier": "/form/name"
          },
          {
            "Identifier": "/form/street-address"
          },
          {
            "Identifier": "/form/city"
          },
          {
            "Identifier": "/form/state"
          },
          {
            "Identifier": "/form/zipcode"
          }
        ]
      }
    }
  }
]
```

```
        },
        "EnableRegexInPath": false
    }
},
],
"RuleActionOverrides": [
    {
        "Name": "SignalCredentialCompromised",
        "ActionToUse": {
            "Count": {}
        }
    }
]
}
},
"OverrideAction": {
    "None": {}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
}
},
{
    "Name": "AccountSignupCompromisedCredentialsHandling",
    "Priority": 1,
    "Statement": {
        "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "aws:waf:managed:aws:acfp:signal:credential_compromised"
        }
    },
    "Action": {
        "Block": {
            "CustomResponse": {
                "ResponseCode": 406,
                "CustomResponseBodyKey": "aws-waf-credential-compromised",
                "ResponseHeaders": [
                    {
                        "Name": "aws-waf-credential-compromised",
                        "Value": "true"
                    }
                ]
            }
        }
    }
}
```

```

    }
  }
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AccountSignupCompromisedCredentialsHandling"
}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "compromisedCreds"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"RetrofittedByFirewallManager": false,
"LabelNamespace": "aws-waf:111122223333:webacl:compromisedCreds:",
"CustomResponseBodies": {
  "aws-waf-credential-compromised": {
    "ContentType": "APPLICATION_JSON",
    "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have been found in a compromised credentials database.\\n\\nTry again with a different username, password pair.\\n\\n\"}"
  }
}
}
}

```

ACFP 範例：回應檢查組態

下列 JSON 清單顯示範例保護套件或 Web ACL，其中包含設定為檢查原始伺服器回應的 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組。請注意回應檢查組態，這會指定成功和回應狀態碼。您也可以根據標頭、內文和內文 JSON 相符項目來設定成功和回應設定。此 JSON 包含保護套件或 Web ACL 自動產生的設定，例如標籤命名空間和保護套件或 Web ACL 的應用程式整合 URL。

Note

ATP 回應檢查僅適用於保護 CloudFront 分佈的保護套件或 Web ACLs。

```
{
```



```
"Name": "simpleACFP",
"Id": "... ",
"ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
"DefaultAction": {
  "Allow": {}
},
"Description": "",
"Rules": [
  {
    "Name": "AWS-AWSManagedRulesACFPRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesACFPRuleSet",
        "ManagedRuleGroupConfigs": [
          {
            "AWSManagedRulesACFPRuleSet": {
              "CreationPath": "/web/signup/submit-registration",
              "RegistrationPagePath": "/web/signup/registration",
              "RequestInspection": {
                "PayloadType": "JSON",
                "UsernameField": {
                  "Identifier": "/form/username"
                },
                "PasswordField": {
                  "Identifier": "/form/password"
                },
                "EmailField": {
                  "Identifier": "/form/email"
                },
                "PhoneNumberFields": [
                  {
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenummer"
                  }
                ],
                "AddressFields": [
                  {
```

```
        "Identifier": "/form/name"
      },
      {
        "Identifier": "/form/street-address"
      },
      {
        "Identifier": "/form/city"
      },
      {
        "Identifier": "/form/state"
      },
      {
        "Identifier": "/form/zipcode"
      }
    ]
  },
  "ResponseInspection": {
    "StatusCode": {
      "SuccessCodes": [
        200
      ],
      "FailureCodes": [
        401
      ]
    }
  },
  "EnableRegexInPath": false
}
]
}
},
"OverrideAction": {
  "None": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
}
},
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
```

```
"CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
"Capacity": 50,
"ManagedByFirewallManager": false,
"RetrofittedByFirewallManager": false,
"LabelNamespace": "aws-waf-111122223333:webacl:simpleACFP:"
}
```

AWS WAF 詐騙控制帳戶接管預防 (ATP)

本節說明 AWS WAF 詐騙控制帳戶接管預防 (ATP) 的功能。

帳戶接管是一種線上非法活動，攻擊者可在其中未經授權存取個人帳戶。攻擊者可能會以多種方式執行此操作，例如使用遭竊的登入資料或透過一系列嘗試猜測受害者的密碼。當攻擊者取得存取權時，他們可能會從受害者竊取金錢、資訊或服務。攻擊者可能會偽裝成受害者，以存取受害者擁有的其他帳戶，或存取其他人或組織的帳戶。此外，他們可能會嘗試變更使用者的密碼，以封鎖受害者與自己的帳戶。

您可以實作 ATP 功能來監控和控制帳戶接管嘗試。AWS WAF 會在 AWS 受管規則規則群組 `AWSManagedRulesATPRuleSet` 和配套應用程式整合 SDKs 中提供此功能。

ATP 受管規則群組會標記和管理可能屬於惡意帳戶接管嘗試一部分的請求。規則群組會透過檢查用戶端傳送至您應用程式的登入端點的登入嘗試來達成此目的。

- 請求檢查 – ATP 可讓您查看和控制使用遭竊登入資料的異常登入嘗試和登入嘗試，以防止可能導致詐騙活動的帳戶接管。ATP 會針對其遭竊的登入資料資料庫檢查電子郵件和密碼組合，該資料庫會隨著在暗網中找到新的洩漏登入資料而定期更新。ATP 會依 IP 地址和用戶端工作階段彙總資料，以偵測和封鎖傳送過多可疑請求的用戶端。
- 回應檢查 – 對於 CloudFront 分佈，除了檢查傳入的登入請求之外，ATP 規則群組還會檢查應用程式的登入嘗試回應，以追蹤成功和失敗率。使用此資訊，ATP 可以暫時封鎖登入失敗次數過多的用戶端工作階段或 IP 地址。會以非同步方式 AWS WAF 執行回應檢查，因此這不會增加 Web 流量的延遲。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

Note

ATP 功能不適用於 Amazon Cognito 使用者集區。

主題

- [AWS WAF ATP 元件](#)
- [搭配 ATP 使用應用程式整合 SDKs](#)
- [將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)
- [測試和部署 ATP](#)
- [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 範例](#)

AWS WAF ATP 元件

AWS WAF 詐騙控制帳戶接管預防 (ATP) 的主要元件如下：

- **AWSManagedRulesATPRuleSet** – 此 AWS 受管規則群組中的規則會偵測、標記和處理各種類型的帳戶接管活動。規則群組會檢查用戶端傳送至指定登入端點的 HTTP POST Web 請求。對於受保護的 CloudFront 分佈，規則群組也會檢查分佈傳回這些請求的回應。如需規則群組規則的清單，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。您可以使用受管規則群組參考陳述式，將此規則群組包含在保護套件或 Web ACL 中。如需使用此規則群組的詳細資訊，請參閱 [將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

- 有關應用程式登入頁面的詳細資訊 – 當您將AWSManagedRulesATPRuleSet規則群組新增至保護套件或 Web ACL 時，必須提供登入頁面的相關資訊。這可讓規則群組縮小其檢查的請求範圍，並正確驗證 Web 請求中的登入資料用量。ATP 規則群組適用於電子郵件格式的使用者名稱。如需詳細資訊，請參閱[將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)。
- 對於受保護的 CloudFront 分佈，有關應用程式如何回應登入嘗試的詳細資訊 – 您可以提供有關應用程式對登入嘗試回應的詳細資訊，並且規則群組會追蹤和管理傳送太多失敗登入嘗試的用戶端。如需設定此選項的詳細資訊，請參閱 [將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)。
- JavaScript 和行動應用程式整合 SDKs – 使用 ATP 實作實作 AWS WAF JavaScript 和行動 SDKs，以啟用規則群組提供的完整功能集。許多 ATP 規則使用 SDKs 提供的資訊進行工作階段層級用戶端

驗證和行為彙總，這是將合法用戶端流量與機器人流量分開的必要條件。如需 SDK 的詳細資訊，請參閱「[中的用戶端應用程式整合 AWS WAF](#)」。

您可以結合 ATP 實作與下列項目，協助您監控、調校和自訂保護。

- 記錄和指標 – 您可以監控流量，並透過為保護套件或 Web ACL 設定和啟用日誌、Amazon Security Lake 資料收集和 Amazon CloudWatch 指標，了解 ACFP 受管規則群組如何影響流量。AWSManagedRulesATPRuleSet 新增至 Web 請求的標籤會包含在資料中。如需選項的相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)、[使用 Amazon CloudWatch 監控](#)和[什麼是 Amazon Security Lake ?](#)。

根據您的需求和您看到的流量，您可能想要自訂AWSManagedRulesATPRuleSet實作。例如，您可能想要從 ATP 評估中排除一些流量，或者您可能想要使用縮小範圍陳述式或標籤比對規則等 AWS WAF 功能，改變它處理其識別的一些帳戶接管嘗試的方式。

- 標籤和標籤比對規則 – 對於 中的任何規則AWSManagedRulesATPRuleSet，您可以將封鎖行為切換為計數，然後比對規則新增的標籤。使用此方法自訂如何處理 ATP 受管規則群組識別的 Web 請求。如需標記和使用標籤比對陳述式的詳細資訊，請參閱 [標籤比對規則陳述式](#)和 [中的 Web 請求標籤 AWS WAF](#)。
- 自訂請求和回應 – 您可以將自訂標頭新增至您允許的請求，也可以為封鎖的請求傳送自訂回應。若要這樣做，請將標籤比對與 AWS WAF 自訂請求和回應功能配對。如需自訂請求和回應的詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

搭配 ATP 使用應用程式整合 SDKs

本節說明如何搭配 ATP 使用應用程式整合 SDKs。

ATP 受管規則群組需要應用程式整合 SDKs 產生的挑戰字符。權杖會啟用規則群組提供的完整一組保護。

我們強烈建議您實作應用程式整合 SDKs，以最有效地使用 ATP 規則群組。挑戰指令碼必須在 ATP 規則群組之前執行，才能讓規則群組受益於指令碼取得的字符。應用程式整合 SDKs會自動發生這種情況。如果您無法使用 SDKs，您可以交替設定保護套件或 Web ACL，以便針對 ATP CAPTCHA規則群組將檢查的所有請求執行 Challenge或 規則動作。使用 Challenge或 CAPTCHA規則動作可能會產生額外費用。如需定價詳細資訊，請參閱 [AWS WAF 定價](#)。

不需要字符的 ATP 規則群組功能

當 Web 請求沒有字符時，ATP 受管規則群組能夠封鎖下列類型的流量：

- 發出大量登入請求的單一 IP 地址。
- 在短時間內發出大量失敗登入請求的單一 IP 地址。
- 使用相同的使用者名稱但變更密碼，以密碼周遊進行登入嘗試。

需要字符的 ATP 規則群組功能

挑戰字符中提供的資訊會擴展規則群組和整體用戶端應用程式安全性的功能。

字符會為每個 Web 請求提供用戶端資訊，讓 ATP 規則群組能夠將合法用戶端工作階段與行為不良的用戶端工作階段分開，即使兩者都來自單一 IP 地址。規則群組會使用字符中的資訊來彙總用戶端工作階段請求行為，以進行微調偵測和緩解。

當字符可用於 Web 請求時，ATP 規則群組可以在工作階段層級偵測和封鎖下列其他類別的用戶端：

- 軟體 SDKs 管理的無提示挑戰失敗的用戶端工作階段。
- 周遊使用者名稱或密碼的用戶端工作階段。這也稱為登入資料填充。
- 用戶端工作階段會重複使用遭竊的登入資料來登入。
- 長時間嘗試登入的用戶端工作階段。
- 發出大量登入請求的用戶端工作階段。ATP 規則群組提供比以 AWS WAF 速率為基礎的規則更好的用戶端隔離，這會依 IP 地址封鎖用戶端。ATP 規則群組也會使用較低的閾值。
- 在短時間內提出大量失敗登入請求的用戶端工作階段。此功能適用於受保護的 Amazon CloudFront 分佈。

如需規則群組功能的詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

如需 SDKs 的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需 AWS WAF 字符的資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。如需規則動作的相關資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

將 ATP 受管規則群組新增至您的保護套件或 Web ACL

本節說明如何新增和設定 `AWSManagedRulesATPRuleSet` 規則群組。

若要設定 ATP 受管規則群組來辨識 Web 流量中的帳戶接管活動，您可以提供有關用戶端如何將登入請求傳送到應用程式的資訊。對於受保護的 Amazon CloudFront 分佈，您也可以提供應用程式如何回應登入請求的相關資訊。此組態是受管規則群組的一般組態以外的組態。

如需規則群組描述和規則清單，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

Note

ATP 遭竊的登入資料資料庫僅包含電子郵件格式的使用者名稱。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。如需如何將受管規則群組新增至保護套件或 Web ACL 的基本資訊，請參閱 [透過主控台將受管規則群組新增至保護套件或 Web ACL](#)。

遵循最佳實務

根據的最佳實務使用 ATP 規則群組 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

在保護套件或 Web ACL 中使用 `AWSManagedRulesATPRuleSet` 規則群組

1. 將 AWS 受管規則群組 `AWSManagedRulesATPRuleSet` 新增至您的保護套件或 Web ACL，並在儲存之前編輯規則群組設定。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

2. 在規則群組組態窗格中，提供 ATP 規則群組用來檢查登入請求的資訊。
 - a. 對於在路徑中使用規則運算式，如果您 AWS WAF 想要針對登入頁面路徑規格執行規則運算式比對，請開啟此選項。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外。程式庫記錄在 [PCRE - Perl 相容規則表達式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

- b. 針對登入路徑，提供應用程式的登入端點路徑。規則群組只會檢查對指定登入端點的 HTTP POST 請求。

Note

端點比對不區分大小寫。Regex 規格不得包含旗標 `(?-i)`，這會停用不區分大小寫的比對。字串規格必須以正斜線開頭 `/`。

例如，對於 URL `https://example.com/web/login`，您可以提供字串路徑規格 `/web/login`。以您提供的路徑開頭的登入路徑會被視為相符項目。例如，`/web/login` 符合登入路徑 `/web/login`、`/web/login/`、`/web/loginPage` 和 `/web/login/thisPage`，但不符合登入路徑 `/home/web/login` 或 `/website/login`。

- c. 針對請求檢查，提供請求承載類型，以及提供使用者名稱和密碼之請求內文中的欄位名稱，以指定應用程式接受登入嘗試的方式。欄位名稱的規格取決於承載類型。
- JSON 承載類型 – 以 JSON 指標語法指定欄位名稱。如需有關 JSON Pointer 語法的資訊，請參閱 Internet Engineering Task Force (IETF) 文件 [JavaScript 物件標記法 \(JSON\) Pointer](#)。

例如，對於下列範例 JSON 承載，使用者名稱欄位規格為 `/login/username`，密碼欄位規格為 `/login/password`。

```
{
  "login": {
    "username": "THE_USERNAME",
    "password": "THE_PASSWORD"
  }
}
```

- FORM_ENCODED 承載類型 – 使用 HTML 表單名稱。

例如，對於具有名為 `username1` 和輸入元素的 HTML 表單 `password1`，使用者名稱欄位規格為 `username1`，密碼欄位規格為 `password1`。

- d. 如果您要保護 Amazon CloudFront 分佈，請在回應檢查下指定應用程式在對登入嘗試的回應中指出成功或失敗的方式。

 Note

ATP 回應檢查僅適用於保護 CloudFront 分佈的保護套件或 Web ACLs。

在您要 ATP 檢查的登入回應中指定單一元件。對於內文和 JSON 元件類型，AWS WAF 可以檢查元件的前 65,536 個位元組 (64 KB)。

提供元件類型的檢查條件，如界面所示。您必須同時提供成功和失敗條件，才能在元件中檢查。

例如，假設您的應用程式在回應的狀態碼中指出登入嘗試的狀態，並使用 200 OK 表示成功，和 401 Unauthorized 或 403 Forbidden 表示失敗。您會將回應檢查元件類型設定為狀態碼，然後在成功文字方塊中輸入 200，然後在失敗文字方塊中輸入 401 在第一行和第二行中輸入 403。

ATP 規則群組只會計算符合您成功或失敗檢查條件的回應。當用戶端在計數的回應中失敗率過高時，規則群組規則會對用戶端執行動作。如需規則群組規則的準確行為，請務必提供成功和失敗登入嘗試的完整資訊。

若要查看檢查登入回應的規則，請在 `VolumetricSessionFailedLoginResponseHigh` 的規則清單中尋找 `VolumetricIpFailedLoginResponseHigh` 和 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

3. 提供您想要用於規則群組的任何其他組態。

您可以將縮小範圍陳述式新增至受管規則群組陳述式，進一步限制規則群組檢查的請求範圍。例如，您只能檢查具有特定查詢引數或 Cookie 的請求。規則群組只會檢查對指定登入端點的 HTTP POST 請求，這些登入端點符合您縮小範圍陳述式中的條件。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

4. 將變更儲存至保護套件或 Web ACL。

在部署生產流量的 ATP 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。如需指引，請參閱以下章節。

測試和部署 ATP

本節提供為您的網站設定和測試 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作的一般指引。您選擇遵循的特定步驟將取決於您收到的需求、資源和 Web 請求。

此資訊是所提供測試和調校的一般資訊之外的。 [測試和調校您的 AWS WAF 保護](#)

Note

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，其取決於您選取的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在中的資源 AWS 受到適當保護。

生產流量風險

在部署生產流量的 ATP 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。

AWS WAF 提供測試登入資料，您可以用來驗證 ATP 組態。在下列程序中，您將設定測試保護套件或 Web ACL 以使用 ATP 受管規則群組、設定規則以擷取規則群組新增的標籤，然後使用這些測試憑證執行登入嘗試。您將透過檢查登入嘗試的 Amazon CloudWatch 指標，來驗證 Web ACL 是否已正確管理嘗試。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。

設定和測試 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 在計數模式中新增 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

將 AWS 受管規則規則群組 `AWSManagedRulesATPRuleSet` 新增至新的或現有的保護套件或 Web ACL，並加以設定，使其不會變更目前的保護套件或 Web ACL 行為。如需此規則群組之規則和標籤的詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

- 當您新增受管規則群組時，請進行編輯並執行下列動作：
 - 在規則群組組態窗格中，提供應用程式登入頁面的詳細資訊。ATP 規則群組會使用此資訊來監控登入活動。如需詳細資訊，請參閱[將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)。
 - 在規則窗格中，開啟覆寫所有規則動作下拉式清單，然後選擇 Count。使用此組態，會根據規則群組中的所有規則 AWS WAF 評估請求，並僅計算該結果的相符項目，同時仍將標籤新增至請求。如需詳細資訊，請參閱[覆寫規則群組中的規則動作](#)。

透過此覆寫，您可以監控 ATP 受管規則的潛在影響，以判斷您是否要新增例外狀況，例如內部使用案例的例外狀況。

- 將規則群組放在保護套件或 Web ACL 中，以便在您現有的規則之後進行評估，其優先順序設定在數值上高於您已使用的任何規則或規則群組。如需詳細資訊，請參閱[設定規則優先順序](#)。

如此一來，您目前的流量處理不會中斷。例如，如果您有偵測惡意流量的規則，例如 SQL Injection 或跨網站指令碼，它們將繼續偵測並記錄。或者，如果您有允許已知非惡意流量的規則，則可以繼續允許該流量，而不會被 ATP 受管規則群組封鎖。您可以在測試和調校活動期間決定調整處理順序。

2. 啟用保護套件或 Web ACL 的記錄和指標

視需要設定 保護套件或 Web ACL 的記錄、Amazon Security Lake 資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見性工具來監控 ATP 受管規則群組與流量的互動。

- 如需設定和使用記錄的相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
- 如需 Amazon Security Lake 的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的[什麼是 Amazon Security Lake ?](#) 以及[從 AWS 服務收集資料](#)。
- 如需 Amazon CloudWatch 指標的相關資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。
- 如需有關 Web 請求取樣的資訊，請參閱 [檢視 Web 請求的範例](#)。

3. 將保護套件或 Web ACL 與資源建立關聯

如果保護套件或 Web ACL 尚未與測試資源建立關聯，請建立關聯。如需相關資訊，請參閱[將保護與 AWS 資源建立關聯或取消關聯](#)。

4. 監控流量和 ATP 規則相符項目

請確定您的正常流量正在流動，且 ATP 受管規則群組規則正在將標籤新增至相符的 Web 請求。您可以在日誌中查看標籤，並在 Amazon CloudWatch 指標中查看 ATP 和標籤指標。在日誌中，您已覆寫規則群組中計數的規則會顯示在 `ruleGroupList` 並將 `action` 設定為計數，並 `overriddenAction` 指出您覆寫的已設定規則動作。

5. 測試規則群組的登入資料檢查功能

使用測試洩露的登入資料執行登入嘗試，並檢查規則群組是否如預期相符。

a. 使用以下 AWS WAF 測試登入資料對登入受保護資源的登入頁面：

- 使用者：WAF_TEST_CREDENTIAL@wafexample.com
- 密碼：WAF_TEST_CREDENTIAL_PASSWORD

這些測試登入資料會分類為遭到入侵的登入資料，而 ATP 受管規則群組會將 `aws:waf:managed:aws:atp:signal:credential_compromised` 標籤新增至登入請求，您可以在日誌中看到。

- b. 在保護套件或 Web ACL 日誌中，在測試登入 Web 請求的日誌項目的 `labels` 欄位中尋找 `aws:waf:managed:aws:atp:signal:credential_compromised` 標籤。如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

驗證規則群組如預期擷取遭入侵的登入資料後，您可以採取步驟來設定其實作，以因應受保護資源的需求。

6. 針對 CloudFront 分佈，測試規則群組的登入失敗管理

- a. 針對您為 ATP 規則群組設定的每個失敗回應條件執行測試。在測試之間等待至少 10 分鐘。

若要測試單一失敗條件，請在回應中識別失敗的登入嘗試。然後，從單一用戶端 IP 地址，在 10 分鐘內執行至少 10 次失敗的登入嘗試。

在前 6 次失敗之後，磁碟區失敗的登入規則應該會開始與您的其餘嘗試相符，並加上標籤和計數。規則可能會因為延遲而遺漏前一或兩個。

- b. 在保護套件或 Web ACL 日誌中，在測試登入 Web 請求的日誌項目的 `labels` 欄位中尋找 `aws:waf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` 標籤。如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

這些測試會檢查失敗的登入計數是否超過規則的閾值，以驗證您的失敗條件是否符合您的回應 `VolumetricIpFailedLoginResponseHigh`。達到閾值後，如果您繼續從相同的 IP 地址傳送登入請求，則規則會繼續比對，直到失敗率低於閾值為止。當超過閾值時，規則會同時符合來自 IP 地址的成功或失敗登入。

7. 自訂 ATP Web 請求處理

視需要新增您自己的規則，明確允許或封鎖請求，以變更 ATP 規則處理它們的方式。

例如，您可以使用 ATP 標籤來允許或封鎖請求，或自訂請求處理。您可以在 ATP 受管規則群組之後新增標籤比對規則，以篩選要套用之處理方式的標記請求。測試之後，請將相關的 ATP 規則保持在計數模式中，並在您的自訂規則中維護請求處理決策。如需範例，請參閱「[ATP 範例：針對遺失和遭入侵的登入資料進行自訂處理](#)」。

8. 移除您的測試規則並啟用 ATP 受管規則群組設定

根據您的情況，您可能已決定要將一些 ATP 規則保留在計數模式中。對於您想要在規則群組中依設定執行的規則，請在保護套件或 Web ACL 規則群組組態中停用計數模式。完成測試後，您也可以移除測試標籤比對規則。

9. 監控和調校

為了確保 Web 請求可依您想要的方式處理，請在啟用您要使用的 ATP 功能後密切監控流量。視需要使用規則群組上的規則計數覆寫和您自己的規則來調整行為。

完成測試 ATP 規則群組實作後，如果您尚未這麼做，強烈建議您將 AWS WAF JavaScript SDK 整合到瀏覽器登入頁面，以增強偵測功能。AWS WAF 也提供行動 SDKs 來整合 iOS 和 Android 裝置。如需整合 SDKs 的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需此建議的相關資訊，請參閱 [搭配 ATP 使用應用程式整合 SDKs](#)。

AWS WAF 詐騙控制帳戶接管預防 (ATP) 範例

本節顯示滿足 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作常用案例的範例組態。

每個範例都會提供使用案例的描述，然後在自訂設定規則的 JSON 清單中顯示解決方案。

Note

您可以透過主控台保護套件或 Web ACL JSON 下載或規則 JSON 編輯器，或透過 APIs 和命令列界面中的 `getWebACL` 操作，擷取這些範例中顯示的 JSON 清單。

主題

- [ATP 範例：簡易組態](#)
- [ATP 範例：針對遺失和遭入侵的登入資料進行自訂處理](#)
- [ATP 範例：回應檢查組態](#)

ATP 範例：簡易組態

下列 JSON 清單顯示具有 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組的保護套件或 Web ACL 範例。請注意額外的登入頁面組態，這會為規則群組提供監控和管理登入請求所需的資訊。此 JSON 包含保護套件或 Web ACL 自動產生的設定，例如標籤命名空間和保護套件或 Web ACL 的應用程式整合 URL。

```
{
  "WebACL": {
    "LabelNamespace": "aws:waf:111122223333:webacl:ATPModuleACL:",
    "Capacity": 50,
    "Description": "This is a test protection pack or web ACL for ATP.",
    "Rules": [
      {
        "Priority": 1,
        "OverrideAction": {
          "None": {}
        },
        "VisibilityConfig": {
          "SampledRequestsEnabled": true,
          "CloudWatchMetricsEnabled": true,
          "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
          "ManagedRuleGroupStatement": {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesATPRuleSet",
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesATPRuleSet": {
                  "LoginPath": "/web/login",
                  "RequestInspection": {
                    "PayloadType": "JSON",
                    "UsernameField": {
                      "Identifier": "/form/username"
                    },
                    "PasswordField": {
                      "Identifier": "/form/password"
                    }
                  },
                  "EnableRegexInPath": false
                }
              }
            ]
          }
        }
      }
    ]
  },
}
```

```

    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
      "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "RetrofittedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
    "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
    "Name": "ATPModuleACL"
  },
  "ApplicationIntegrationURL": "https://9z87abce34ea.us-east-1.sdk.aws.waf.com/9z87abce34ea/1234567a1b10/",
  "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}

```

ATP 範例：針對遺失和遭入侵的登入資料進行自訂處理

根據預設，規則群組執行的登入資料檢查會由 `AWSManagedRulesATPRuleSet` 處理 Web 請求，如下所示：

- 缺少登入資料 – 標籤和封鎖請求。
- 已遭入侵的登入資料 – 標記請求，但不要封鎖或計數。

如需規則群組和規則行為的詳細資訊，請參閱 [AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

您可以執行下列動作，為憑證遺失或遭到入侵的 Web 請求新增自訂處理：

- 覆寫 **MissingCredential** 規則至 Count - 此規則動作覆寫會導致規則僅計數和標記相符請求。
- 使用自訂處理新增標籤比對規則 – 將此規則設定為與兩個 ATP 標籤比對，並執行您的自訂處理。例如，您可以將客戶重新導向至註冊頁面。

下列規則顯示先前範例中的 ATP 受管規則群組，其中 **MissingCredential** 規則動作會覆寫為計數。這會導致規則將其標籤套用至相符的請求，然後只計算請求，而不是封鎖請求。

```

"Rules": [
  {

```



```
    "Priority": 1,
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AccountTakeOverValidationRule"
    },
    "Name": "DetectCompromisedUserCredentials",
    "Statement": {
      "ManagedRuleGroupStatement": {
        "ManagedRuleGroupConfigs": [
          {
            "AWSManagedRulesATPRuleSet": {
              "LoginPath": "/web/login",
              "RequestInspection": {
                "PayloadType": "JSON",
                "UsernameField": {
                  "Identifier": "/form/username"
                },
                "PasswordField": {
                  "Identifier": "/form/password"
                }
              },
              "EnableRegexInPath": false
            }
          }
        ]
      },
      "VendorName": "AWS",
      "Name": "AWSManagedRulesATPRuleSet",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "MissingCredential"
        }
      ],
      "ExcludedRules": []
    }
  }
}
```



```
],
```

透過此組態，當此規則群組評估任何缺少或洩露登入資料的 Web 請求時，它會標記請求，但不會封鎖請求。

下列規則的優先順序設定，其數值高於上述規則群組。會以數值順序 AWS WAF 評估規則，從最低開始，因此此規則將在規則群組評估後進行評估。規則設定為符合其中一個登入資料標籤，並傳送相符請求的自訂回應。

```
"Name": "redirectToSignup",
  "Priority": 10,
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:atp:signal:missing_credential"
          }
        },
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {
      "CustomResponse": {
        your custom response settings
      }
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "redirectToSignup"
  }
}
```

ATP 範例：回應檢查組態

下列 JSON 清單顯示範例保護套件或 Web ACL，其中包含設定為檢查原始伺服器回應的 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組。請注意回應檢查組態，這會指定成功和回應狀態碼。您也可以根據標頭、內文和內文 JSON 相符項目來設定成功和回應設定。此 JSON 包含保護套件或 Web ACL 自動產生的設定，例如標籤命名空間和保護套件或 Web ACL 的應用程式整合 URL。

Note

ATP 回應檢查僅適用於保護 CloudFront 分佈的保護套件或 Web ACLs。

```
{
  "WebACL": {
    "LabelNamespace": "aws:waf:111122223333:webacl:ATPModuleACL:",
    "Capacity": 50,
    "Description": "This is a test protection pack or web ACL for ATP.",
    "Rules": [
      {
        "Priority": 1,
        "OverrideAction": {
          "None": {}
        },
        "VisibilityConfig": {
          "SampledRequestsEnabled": true,
          "CloudWatchMetricsEnabled": true,
          "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
          "ManagedRuleGroupStatement": {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesATPRuleSet",
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesATPRuleSet": {
                  "LoginPath": "/web/login",
                  "RequestInspection": {
                    "PayloadType": "JSON",
                    "UsernameField": {
                      "Identifier": "/form/username"
                    }
                  }
                }
              ]
            }
          }
        }
      }
    ]
  }
}
```

```

        },
        "PasswordField": {
            "Identifier": "/form/password"
        }
    },
    "ResponseInspection": {
        "StatusCode": {
            "SuccessCodes": [
                200
            ],
            "FailureCodes": [
                401
            ]
        }
    },
    "EnableRegexInPath": false
}
]
}
}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "ATPValidationAcl"
},
"DefaultAction": {
    "Allow": {}
},
"ManagedByFirewallManager": false,
"RetrofittedByFirewallManager": false,
"Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
"ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
"Name": "ATPModuleACL"
},
"ApplicationIntegrationURL": "https://9z87abce34ea.us-east-1.sdk.aws.waf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}

```

AWS WAF 機器人控制

本節說明 Bot Control 執行的操作。

透過 Bot Control，您可以輕鬆監控、封鎖或限制速率的機器人，例如抓取器、掃描器、爬蟲程式、狀態監視器和搜尋引擎。如果您使用規則群組的目標檢查層級，也可以挑戰無法自我識別的機器人，讓惡意機器人對您的網站操作更困難且更昂貴。您可以單獨使用 Bot Control 受管規則群組，或結合其他 AWS 受管規則規則群組和您自己的自訂 AWS WAF 規則來保護應用程式。

Bot Control 包含主控台儀表板，可根據請求取樣，顯示目前有多少流量來自機器人。透過將 Bot Control 受管規則群組新增至您的保護套件或 Web ACL，您可以對機器人流量採取動作，並接收有關傳入應用程式的常見機器人流量的詳細即時資訊。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

Bot Control 受管規則群組提供基本的常見保護層級，可將標籤新增至自我識別機器人、驗證一般所需的機器人，並偵測高可信度的機器人簽章。這可讓您監控和控制常見的機器人流量類別。

Bot Control 規則群組也提供目標式保護層級，為無法自我識別的複雜機器人新增偵測。針對性保護使用偵測技術，例如瀏覽器查詢、指紋和行為啟發式，來識別錯誤的機器人流量。此外，針對性保護提供網站流量統計資料的選用自動化機器學習分析，以偵測機器人相關活動。當您啟用機器學習時，AWS WAF 會使用有關網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，來改善 Bot Control 機器學習模型。

如需 Bot Control 受管規則群組的詳細資訊，請參閱 [AWS WAF 機器人控制規則群組](#)。

當針對 Bot Control 受管規則群組 AWS WAF 評估 Web 請求時，規則群組會將標籤新增至偵測到與機器人相關的請求，例如機器人的類別和機器人名稱。您可以在自己的 AWS WAF 規則中比對這些標籤，以自訂處理。Bot Control 受管規則群組產生的標籤會包含在 Amazon CloudWatch 指標和您的保護套件或 Web ACL 日誌中。

您也可以使用 AWS Firewall Manager AWS WAF 政策，將 Bot Control 受管規則群組部署到組織中的多個帳戶中的應用程式 AWS Organizations。

AWS WAF 機器人控制元件

Bot Control 實作的主要元件如下：

- **AWSManagedRulesBotControlRuleSet** – Bot Control 受管規則群組，其規則會偵測和處理各種類別的機器人。此規則群組會將標籤新增至偵測到為機器人流量的 Web 請求。

 Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

Bot Control 受管規則群組提供兩種層級的保護，您可以從中選擇：

- 常見 – 偵測各種自我識別機器人，例如 Web 抓取架構、搜尋引擎和自動化瀏覽器。此層級的機器人控制保護會使用傳統機器人偵測技術來識別常見的機器人，例如靜態請求資料分析。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的流量。
- 目標型 – 包含共同層級的保護，並為無法自我識別的複雜機器人新增目標型偵測。針對性保護會使用速率限制和 CAPTCHA 和背景瀏覽器挑戰的組合來緩解機器人活動。
- **TGT_** – 提供目標保護的規則具有以 開頭的名稱TGT_。所有目標防護都使用瀏覽器查詢、指紋和行為啟發式等偵測技術來識別錯誤的機器人流量。
- **TGT_ML_** – 使用機器學習的目標保護規則具有以 開頭的名稱TGT_ML_。這些規則使用網站流量統計資料的自動化機器學習分析來偵測指示分散式、協調機器人活動的異常行為。AWS WAF 會分析網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。預設會啟用機器學習功能，但您可以在規則群組組態中停用這些功能。停用機器學習時，AWS WAF 不會評估這些規則。

如需包含規則群組規則相關資訊的詳細資訊，請參閱 [AWS WAF 機器人控制規則群組](#)。

您可以使用受管規則群組參考陳述式將此規則群組包含在保護套件或 Web ACL 中，並指出您要使用的檢查層級。針對目標層級，您也可以指出是否啟用機器學習。如需將此受管規則群組新增至保護套件或 Web ACL 的詳細資訊，請參閱 [將 AWS WAF Bot Control 受管規則群組新增至 Web ACL](#)。

- Bot Control 儀表板 – 適用於您保護套件或 Web ACL 的機器人監控儀表板，可透過保護套件或 Web ACL Bot Control 索引標籤取得。使用此儀表板來監控您的流量，並了解有多少流量來自各種類型的機器人。這可以是自訂機器人管理的起點，如本主題所述。您也可以使用它來驗證變更，並監控各種機器人和機器人類別的活動。
- JavaScript 和行動應用程式整合 SDKs – 如果您使用 Bot Control 規則群組的目標保護層級，則應實作 AWS WAF JavaScript 和行動 SDKs。目標規則使用用戶端字符中 SDKs 提供的資訊，以增強對惡意機器人的偵測。如需 SDK 的詳細資訊，請參閱「[中的用戶端應用程式整合 AWS WAF](#)」。
- 記錄和指標 – 您可以監控機器人流量，並了解 Bot Control 受管規則群組如何透過 AWS WAF 日誌、Amazon Security Lake 和 Amazon CloudWatch 研究為保護套件或 Web ACL 收集的資料，來

評估和處理您的流量。Bot Control 新增至 Web 請求的標籤會包含在資料中。如需這些選項的詳細資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)、[使用 Amazon CloudWatch 監控](#) 和 [什麼是 Amazon Security Lake ?](#)。

視您的需求和您看到的流量而定，您可能想要自訂 Bot Control 實作。以下是一些最常用的選項。

- 縮小範圍陳述式 – 您可以透過在 Bot Control 受管規則群組參考陳述式中新增縮小範圍陳述式，從 Bot Control 受管規則群組評估的 Web 請求中排除一些流量。縮小範圍陳述式可以是任何可巢狀規則陳述式。當請求不符合縮小範圍陳述式時，會將其 AWS WAF 評估為不符合規則群組參考陳述式，而不針對規則群組進行評估。如需縮小範圍陳述式的詳細資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。
- 使用 Bot Control 受管規則群組的成本會隨著 AWS WAF 評估的 Web 請求數量而增加。您可以使用縮小範圍陳述式來限制規則群組評估的請求，以協助降低這些成本。例如，您可能想要允許您的首頁載入每個人，包括機器人，然後將規則群組規則套用至前往應用程式 APIs 或包含特定類型內容的請求。
- 標籤和標籤比對規則 – 您可以自訂 Bot Control 規則群組如何處理使用 AWS WAF 標籤比對規則陳述式識別的一些機器人流量。Bot Control 規則群組會將標籤新增至您的 Web 請求。您可以在符合 Bot Control 標籤的 Bot Control 規則群組之後新增標籤比對規則，並套用您需要的處理。如需標記和使用標籤比對陳述式的詳細資訊，請參閱 [標籤比對規則陳述式](#) 和 [中的 Web 請求標籤 AWS WAF](#)。
- 自訂請求和回應 – 您可以將自訂標頭新增至您允許的請求，並透過將標籤比對與自訂請求和回應功能配對來傳送封鎖請求的 AWS WAF 自訂回應。如需自訂請求和回應的詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

搭配 Bot Control 使用應用程式整合 SDKs

本節說明如何搭配 Bot Control 使用應用程式整合 SDKs。

Bot Control 受管規則群組的大多數目標保護都需要應用程式整合 SDKs 產生的挑戰字符。在請求上不需要挑戰字符的規則是 Bot Control 常見層級保護和目標層級機器學習規則。如需規則群組中保護層級和規則的說明，請參閱 [AWS WAF 機器人控制規則群組](#)。

我們強烈建議您實作應用程式整合 SDKs，以最有效地使用 Bot Control 規則群組。挑戰指令碼必須在 Bot Control 規則群組之前執行，才能讓規則群組受益於指令碼取得的字符。

- 透過應用程式整合 SDKs，指令碼會自動執行。
- 如果您無法使用 SDKs，您可以設定保護套件或 Web ACL，以便針對 Bot Control CAPTCHA 規則群組將檢查的所有請求執行 Challenge 或 規則動作。使用 Challenge 或 CAPTCHA 規則動作可能會產生額外費用。如需定價詳細資訊，請參閱 [AWS WAF 定價](#)。

當您在用戶端中實作應用程式整合 SDKs 或使用執行挑戰指令碼的其中一個規則動作時，您可以擴展規則群組和整體用戶端應用程式安全性的功能。

字符提供每個 Web 請求的用戶端資訊。此額外資訊可讓 Bot Control 規則群組將合法用戶端工作階段與行為不良的用戶端工作階段分開，即使兩者都來自單一 IP 地址。規則群組會使用字符中的資訊來彙總用戶端工作階段請求行為，以進行針對性保護層級提供的微調偵測和緩解。

如需 SDKs 的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需 AWS WAF 字符的詳細資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。如需規則動作的相關資訊，請參閱 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

將 AWS WAF Bot Control 受管規則群組新增至 Web ACL

本節說明如何新增和設定 `AWSManagedRulesBotControlRuleSet` 規則群組。

Bot Control 受管規則群組 `AWSManagedRulesBotControlRuleSet` 需要額外的組態，以識別您要實作的保護層級。

如需規則群組描述和規則清單，請參閱 [AWS WAF 機器人控制規則群組](#)。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。如需如何將受管規則群組新增至保護套件或 Web ACL 的基本資訊，請參閱 [透過主控台將受管規則群組新增至保護套件或 Web ACL](#)。

遵循最佳實務

根據的最佳實務使用 Bot Control 規則群組 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

在保護套件或 Web ACL 中使用 `AWSManagedRulesBotControlRuleSet` 規則群組

1. 將 AWS 受管規則群組 `AWSManagedRulesBotControlRuleSet` 新增至您的保護套件或 Web ACL。如需完整的規則群組描述，請參閱 [the section called “機器人控制規則群組”](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

當您新增規則群組時，請進行編輯以開啟規則群組的組態頁面。

2. 在規則群組的組態頁面上的檢查層級窗格中，選取您要使用的檢查層級。

- 常見 – 偵測各種自我識別機器人，例如 Web 抓取架構、搜尋引擎和自動化瀏覽器。此層級的機器人控制保護會使用傳統機器人偵測技術來識別常見的機器人，例如靜態請求資料分析。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的流量。
 - 目標型 – 包含共同層級保護，並為無法自我識別的複雜機器人新增目標型偵測。針對性保護會使用速率限制和 CAPTCHA 和背景瀏覽器挑戰的組合來緩解機器人活動。
 - **TGT_** – 提供目標保護的規則具有以 **TGT_** 開頭的名稱。所有目標防護都使用偵測技術，例如瀏覽器查詢、指紋和行為啟發式，來識別錯誤的機器人流量。
 - **TGT_ML_** – 使用機器學習的目標保護規則具有以 **TGT_ML_** 開頭的名稱。這些規則使用網站流量統計資料的自動化機器學習分析來偵測指示分散式、協調機器人活動的異常行為。AWS WAF 分析網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。預設會啟用機器學習功能，但您可以在規則群組組態中停用這些功能。停用機器學習時，AWS WAF 不會評估這些規則。
3. 如果您使用目標保護層級，而且不想 AWS WAF 使用機器學習 (ML) 來分析分散式協調機器人活動的 Web 流量，請停用機器學習選項。名稱開頭為 **TGT_ML_** 的 Bot Control 規則需要機器學習。如需這些規則的詳細資訊，請參閱 [機器人控制規則清單](#)。
 4. 為規則群組新增縮小範圍陳述式，以包含使用規則群組的成本。縮小範圍陳述式會縮小規則群組檢查的一組請求。例如，使用案例，以 [Bot Control 範例：僅針對登入頁面使用 Bot Control](#) 和 [開頭機器人控制範例：僅將機器人控制用於動態內容](#)。
 5. 提供規則群組所需的任何其他組態。
 6. 將變更儲存至保護套件或 Web ACL。

為生產流量部署 Bot Control 實作之前，請先在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調整規則，然後再啟用它們。如需指引，請參閱以下各節。

使用 AWS WAF Bot Control 的誤判案例範例

本節提供使用 AWS WAF Bot Control 時可能遇到誤報的範例情況。

我們已仔細選取 AWS WAF Bot Control 受管規則群組中的規則，以將誤報降至最低。我們會針對全球流量測試規則，並監控其對測試保護套件或 Web ACLs 的影響。不過，由於流量模式的變更，仍然可能得到誤報。此外，已知某些使用案例會導致誤報，並且需要針對您的 Web 流量進行自訂。

您可能會遇到誤報的情況包括：

- 行動應用程式通常具有非瀏覽器使用者代理程式，規則預設會封鎖此 SignalNonBrowserUserAgent 代理程式。如果您預期來自行動應用程式的流量，或任何其他使用非瀏覽器使用者代理程式的合法流量，則需要新增例外狀況才能允許。
- 您可能會依賴某些特定的機器人流量來進行運作時間監控、整合測試或行銷工具。如果 Bot Control 識別並封鎖您想要允許的機器人流量，您需要新增自己的規則來改變處理方式。雖然這不是所有客戶的誤報案例，但如果是針對您，您將需要將其處理為與誤報相同的情況。
- Bot Control 受管規則群組會使用來自的 IP 地址來驗證機器人 AWS WAF。如果您使用 Bot Control，而且已驗證透過代理或負載平衡器路由的機器人，您可能需要使用自訂規則明確允許它們。如需如何建立此類型自訂規則的資訊，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。
- 全域誤報率較低的機器人控制規則可能會嚴重影響特定裝置或應用程式。例如，在測試和驗證中，我們可能不會觀察到來自低流量應用程式或較不常見瀏覽器或裝置的請求。
- 具有歷史低誤報率的機器人控制規則可能會增加有效流量的誤報。這可能是因為新的流量模式或請求屬性出現有效流量，導致它符合之前沒有的規則。這些變更可能是因為下列情況所造成：
 - 隨著流量流經網路設備而變更的流量詳細資訊，例如負載平衡器或內容分佈網路 (CDN)。
 - 流量資料的新興變更，例如新瀏覽器或現有瀏覽器的新版本。

如需有關如何處理您可能從 AWS WAF Bot Control 受管規則群組取得之誤報的資訊，請參閱以下章節中的指引：[測試和部署 AWS WAF 機器人控制](#)。

測試和部署 AWS WAF 機器人控制

本節提供設定和測試您網站之 AWS WAF Bot Control 實作的一般指引。您選擇遵循的特定步驟將取決於您的需求、資源和您收到的 Web 請求。

此資訊是所提供測試和調校的一般資訊之外的。[測試和調校您的 AWS WAF 保護](#)

Note

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，這取決於您選擇的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在中的資源 AWS 受到適當保護。

⚠ 生產流量風險

為生產流量部署 Bot Control 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。

設定和測試機器人控制實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 新增 Bot Control 受管規則群組

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

將受管 AWS 規則群組 `AWSManagedRulesBotControlRuleSet` 新增至新的或現有的保護套件或 Web ACL，並加以設定，使其不會變更目前的保護套件或 Web ACL 行為。

- 當您新增受管規則群組時，請進行編輯並執行下列動作：
 - 在檢查層級窗格中，選取您要使用的檢查層級。
 - 常見 – 偵測各種自我識別機器人，例如 Web 抓取架構、搜尋引擎和自動化瀏覽器。此層級的機器人控制保護會使用傳統機器人偵測技術來識別常見的機器人，例如靜態請求資料分析。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的流量。
 - 目標型 – 包含共同層級的保護，並為無法自我識別的複雜機器人新增目標型偵測。針對性保護會使用速率限制和 CAPTCHA 和背景瀏覽器挑戰的組合來緩解機器人活動。
 - **TGT_** – 提供目標保護的規則具有以 開頭的名稱 **TGT_**。所有目標防護都使用瀏覽器查詢、指紋和行為啟發式等偵測技術來識別錯誤的機器人流量。
 - **TGT_ML_** – 使用機器學習的目標保護規則具有以 開頭的名稱 **TGT_ML_**。這些規則使用網站流量統計資料的自動化機器學習分析來偵測指示分散式、協調機器人活動的異常行為。AWS WAF 會分析網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的

URL，以改善 Bot Control 機器學習模型。預設會啟用機器學習功能，但您可以在規則群組組態中停用這些功能。停用機器學習時，AWS WAF 不會評估這些規則。

如需此選項的詳細資訊，請參閱 [AWS WAF 機器人控制規則群組](#)。

- 在規則窗格中，開啟覆寫所有規則動作下拉式清單，然後選擇 Count。使用此組態，會根據規則群組中的所有規則 AWS WAF 評估請求，並僅計算該結果的相符項目，同時仍將標籤新增至請求。如需詳細資訊，請參閱 [覆寫規則群組中的規則動作](#)。

透過此覆寫，您可以監控機器人控制規則對流量的潛在影響，以判斷您是否要新增內部使用案例或所需機器人等物件的例外狀況。

- 將規則群組放置到最後在保護套件或 Web ACL 中進行評估，其優先順序設定在數值上高於您已使用的任何其他規則或規則群組。如需詳細資訊，請參閱 [設定規則優先順序](#)。

如此一來，您目前的流量處理不會中斷。例如，如果您有偵測惡意流量的規則，例如 SQL Injection 或跨網站指令碼，它們將繼續偵測並記錄這些請求。或者，如果您有允許已知非惡意流量的規則，則可以繼續允許該流量，而不會被 Bot Control 受管規則群組封鎖。您可以決定在測試和調校活動期間調整處理順序，但這是開始的好方法。

2. 啟用保護套件或 Web ACL 的記錄和指標

視需要設定 保護套件或 Web ACL 的記錄、Amazon Security Lake 資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見性工具來監控 Bot Control 受管規則群組與流量的互動。

- 如需日誌記錄的相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
- 如需 Amazon Security Lake 的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的[什麼是 Amazon Security Lake？](#)以及[從 AWS 服務收集資料](#)。
- 如需 Amazon CloudWatch 指標的相關資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。
- 如需有關 Web 請求取樣的資訊，請參閱 [檢視 Web 請求的範例](#)。

3. 將保護套件或 Web ACL 與資源建立關聯

如果保護套件或 Web ACL 尚未與資源建立關聯，請建立關聯。如需相關資訊，請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。

4. 監控流量和機器人控制規則相符項目

確定流量正在流動，且 Bot Control 受管規則群組規則正在將標籤新增至相符的 Web 請求。您可以在日誌中查看標籤，並在 Amazon CloudWatch 指標中查看機器人和標籤指標。在日誌中，

您已覆寫規則群組中計數的規則會顯示在 `ruleGroupList` 並將 `action` 設定為計數，並 `overriddenAction` 指出您覆寫的已設定規則動作。

Note

Bot Control 受管規則群組會使用來自的 IP 地址來驗證機器人 AWS WAF。如果您使用 Bot Control，而且已驗證透過代理或負載平衡器路由的機器人，您可能需要使用自訂規則明確允許它們。如需如何建立自訂規則的資訊，請參閱 [在中使用轉送的 IP 地址 AWS WAF](#)。如需有關如何使用規則自訂 Bot Control Web 請求處理的資訊，請參閱下一個步驟。

仔細檢閱 Web 請求處理，找出您可能需要透過自訂處理緩解的任何誤報。如需誤報的範例，請參閱 [使用 AWS WAF Bot Control 的誤判案例範例](#)。

5. 自訂 Bot Control Web 請求處理

視需要新增您自己的規則，明確允許或封鎖請求，以變更 Bot Control 規則處理它們的方式。

如何執行此操作取決於您的使用案例，但以下是常見的解決方案：

- 明確允許具有您在 Bot Control 受管規則群組之前新增之規則的請求。如此一來，允許的請求永遠不會到達規則群組進行評估。這有助於包含使用 Bot Control 受管規則群組的成本。
- 透過在 Bot Control 受管規則群組陳述式中新增縮小範圍陳述式，從 Bot Control 評估中排除請求。這的運作方式與上述選項相同。它有助於控制使用 Bot Control 受管規則群組的成本，因為不符合縮小範圍陳述式的請求永遠不會達到規則群組評估。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

如需範例，請參閱下方：

- [從機器人管理排除 IP 範圍](#)
- [允許來自您控制之機器人的流量](#)
- 在請求處理中使用機器人控制標籤來允許或封鎖請求。在 Bot Control 受管規則群組之後新增標籤比對規則，以從您要封鎖的請求中篩選出要允許的已標記請求。

測試之後，請將相關的機器人控制規則保持在計數模式中，並在您的自訂規則中維護請求處理決策。如需標籤比對陳述式的資訊，請參閱 [標籤比對規則陳述式](#)。

如需這類自訂的範例，請參閱下列內容：

- [為封鎖的使用者代理程式建立例外狀況](#)

- [允許特定封鎖的機器人](#)
- [封鎖已驗證的機器人](#)

如需額外的範例，請參閱[AWS WAF 機器人控制範例](#)。

6. 視需要啟用 Bot Control 受管規則群組設定

根據您的情況，您可能已決定要將部分機器人控制規則保留在計數模式，或使用不同的動作覆寫。對於您想要在規則群組內設定時執行的規則，請啟用規則組態。若要這樣做，請在保護套件或 Web ACL 中編輯規則群組陳述式，並在規則窗格中進行變更。

AWS WAF 機器人控制範例

本節顯示可滿足 AWS WAF 機器人控制實作各種常見使用案例的範例組態。

每個範例都會提供使用案例的描述，然後在自訂設定規則的 JSON 清單中顯示解決方案。

Note

這些範例中顯示的 JSON 清單是在主控台中建立，方法是設定規則，然後使用規則 JSON 編輯器進行編輯。

主題

- [機器人控制範例：簡易組態](#)
- [機器人控制範例：明確允許已驗證的機器人](#)
- [機器人控制範例：封鎖已驗證的機器人](#)
- [機器人控制範例：允許特定封鎖的機器人](#)
- [機器人控制範例：為封鎖的使用者代理程式建立例外狀況](#)
- [Bot Control 範例：僅針對登入頁面使用 Bot Control](#)
- [機器人控制範例：僅將機器人控制用於動態內容](#)
- [機器人控制範例：從機器人管理排除 IP 範圍](#)
- [Bot Control 範例：允許來自您控制之機器人的流量](#)
- [機器人控制範例：啟用目標檢查層級](#)
- [機器人控制範例：使用兩個陳述式來限制目標檢查層級的使用](#)

機器人控制範例：簡易組態

下列 JSON 清單顯示具有 AWS WAF Bot Control 受管規則群組的範例保護套件或 Web ACL。請注意可見性組態，這會導致 AWS WAF 存放請求範例和指標以供監控之用。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
    {
      ...
    },
    {
      "Name": "AWS-AWSBotControl-Example",
      "Priority": 5,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ],
          "RuleActionOverrides": [],
          "ExcludedRules": []
        },
        "VisibilityConfig": {
          "SampledRequestsEnabled": true,
          "CloudWatchMetricsEnabled": true,
          "MetricName": "AWS-AWSBotControl-Example"
        }
      }
    }
  ],
  "VisibilityConfig": {
    ...
  }
}
```

```
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false,
    "RetrofittedByFirewallManager": false
  }
```

機器人控制範例：明確允許已驗證的機器人

AWS WAF Bot Control 不會封鎖已知 AWS 為常見且可驗證的機器人。當 Bot Control 將 Web 請求識別為來自已驗證的機器人時，它會新增一個標籤，以命名機器人，並新增一個標籤，指出它是已驗證的機器人。Bot Control 不會新增任何其他標籤，例如訊號標籤，以防止封鎖已知的良好機器人。

您可能還有其他 AWS WAF 規則封鎖已驗證的機器人。如果您想要確保允許已驗證的機器人，請新增自訂規則，以根據機器人控制標籤來允許它們。您的新規則必須在 Bot Control 受管規則群組之後執行，才能比對標籤。

下列規則明確允許已驗證的機器人。

```
{
  "Name": "match_rule",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "aws:waf:managed:aws:bot-control:bot:verified"
    }
  },
  "RuleLabels": [],
  "Action": {
    "Allow": {}
  }
}
```

機器人控制範例：封鎖已驗證的機器人

若要封鎖已驗證的機器人，您必須新增規則來封鎖在 AWS WAF Bot Control 受管規則群組之後執行的機器人。若要執行此操作，請識別您要封鎖的機器人名稱，並使用標籤比對陳述式來識別和封鎖它們。如果您想要只封鎖所有已驗證的機器人，您可以省略與bot:name:標籤的比對。

下列規則只會封鎖bingbot已驗證的機器人。此規則必須在 Bot Control 受管規則群組之後執行。

```
{
  "Name": "match_rule",
```



```
"Statement": {
  "AndStatement": {
    "Statements": [
      {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
        }
      },
      {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:bot-control:bot:verified"
        }
      }
    ]
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  }
}
```

下列規則會封鎖所有已驗證的機器人。

```
{
  "Name": "match_rule",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "awswaf:managed:aws:bot-control:bot:verified"
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  }
}
```

機器人控制範例：允許特定封鎖的機器人

機器人可能會被多個 Bot Control 規則封鎖。針對每個封鎖規則執行下列程序。

如果 AWS WAF 機器人控制規則封鎖您不想封鎖的機器人，請執行下列動作：

1. 透過檢查日誌來識別封鎖機器人的機器人控制規則。封鎖規則將在名稱開頭為 `terminatingRule` 的欄位中的日誌中指定。如需保護套件或 Web ACL 日誌的相關資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。請注意，規則會新增至請求的標籤。
2. 在保護套件或 Web ACL 中，覆寫要計數的封鎖規則動作。若要在主控台中執行此操作，請在保護套件或 Web ACL 中編輯規則群組規則，並為規則選擇 `Count` 的規則動作覆寫。這可確保機器人不會被規則封鎖，但規則仍會將其標籤套用至相符的請求。
3. 在 Bot Control 受管規則群組之後，將標籤比對規則新增至您的保護套件或 Web ACL。設定規則以比對覆寫規則的標籤，並封鎖所有相符的請求，但您不想封鎖的機器人除外。

您的保護套件或 Web ACL 現在已設定完成，因此您透過日誌識別的封鎖規則不會再封鎖您要允許的機器人。

再次檢查流量和您的日誌，以確保透過 `Allow` 來允許機器人。如果沒有，請再次執行上述程序。

例如，假設您想要封鎖 `pingdom` 以外的所有監控機器人。在此情況下，您會覆寫 `CategoryMonitoring` 規則以計數，然後撰寫規則來封鎖所有監控機器人，但具有機器人名稱標籤的機器人除外 `pingdom`。

下列規則使用 Bot Control 受管規則群組，但會覆寫規則動作 `CategoryMonitoring` 讓計數。類別監控規則會照常將其標籤套用至相符的請求，但只會計算它們，而不是執行其一般的區塊動作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [
        {
          "ActionToUse": {
```

```
        "Count": {}
      },
      "Name": "CategoryMonitoring"
    }
  ],
  "ExcludedRules": []
}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSBotControl-Example"
}
}
```

下列規則會比對上述CategoryMonitoring規則新增至相符 Web 請求的類別監控標籤。在類別監控請求中，此規則會封鎖除了具有機器人名稱 標籤的所有 之外的所有 pingdom。

下列規則必須在保護套件或 Web ACL 處理順序中的上述 Bot Control 受管規則群組之後執行。

```
{
  "Name": "match_rule",
  "Priority": 10,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "aws:waf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "aws:waf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        }
      ]
    }
  }
}
```

```
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

機器人控制範例：為封鎖的使用者代理程式建立例外狀況

如果某些非瀏覽器使用者代理程式的流量遭到錯誤封鎖，您可以將違規的 AWS WAF Bot Control 規則設定為 `SignalNonBrowserUserAgent Count`，然後將規則的標籤與您的例外條件合併，以建立例外狀況。

 Note

行動應用程式通常具有非瀏覽器使用者代理程式，規則預設會封鎖該代理 `SignalNonBrowserUserAgent` 程式。

下列規則使用 Bot Control 受管規則群組，但會覆寫 `SignalNonBrowserUserAgent` 對計數的規則動作。訊號規則會像往常一樣將其標籤套用至相符的請求，但只會計算它們，而不是執行其一般的區塊動作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ]
    },
  },
}
```

```
"RuleActionOverrides": [
  {
    "ActionToUse": {
      "Count": {}
    },
    "Name": "SignalNonBrowserUserAgent"
  }
],
"ExcludedRules": []
}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSBotControl-Example"
}
}
```

下列規則會比對機器人控制SignalNonBrowserUserAgent規則新增至其相符 Web 請求的訊號標籤。在訊號請求中，此規則會封鎖除具有我們想要允許之使用者代理程式以外的所有。

下列規則必須在保護套件或 Web ACL 處理順序中的上述 Bot Control 受管規則群組之後執行。

```
{
  "Name": "match_rule",
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "ByteMatchStatement": {
                "FieldToMatch": {
                  "SingleHeader": {
                    "Name": "user-agent"
                  }
                }
              }
            }
          }
        }
      ]
    }
  }
}
```



```

    }
  ],
  "RuleActionOverrides": [],
  "ExcludedRules": []
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSBotControl-Example"
},
"ScopeDownStatement": {
  "ByteMatchStatement": {
    "SearchString": "login",
    "FieldToMatch": {
      "UriPath": {}
    }
  },
  "TextTransformations": [
    {
      "Priority": 0,
      "Type": "NONE"
    }
  ],
  "PositionalConstraint": "CONTAINS"
}
}
}
}

```

機器人控制範例：僅將機器人控制用於動態內容

此範例使用縮小範圍陳述式，僅將 AWS WAF 機器人控制套用至動態內容。

縮小範圍陳述式會否定 regex 模式集的相符結果，以排除靜態內容：

- regex 模式集已設定為符合靜態內容的延伸。例如，regex 模式集規格可能是 `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`。如需 regex 模式集和陳述式的相關資訊，請參閱 [規則運算式模式集比對規則陳述式](#)。
- 在縮小範圍陳述式中，我們透過將 regex 模式集陳述式巢狀化在 NOT 陳述式中，排除相符的靜態內容。如需 NOT 陳述式的詳細資訊，請參閱 [NOT 規則陳述式](#)。

```

{
  "Name": "AWS-AWSBotControl-Example",

```

```
"Priority": 5,
"Statement": {
  "ManagedRuleGroupStatement": {
    "VendorName": "AWS",
    "Name": "AWSManagedRulesBotControlRuleSet",
  "ManagedRuleGroupConfigs": [
    {
      "AWSManagedRulesBotControlRuleSet": {
        "InspectionLevel": "COMMON"
      }
    }
  ],
  "RuleActionOverrides": [],
  "ExcludedRules": []
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "AWS-AWSBotControl-Example"
},
"ScopeDownStatement": {
  "NotStatement": {
    "Statement": {
      "RegexPatternSetReferenceStatement": {
        "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/000000000-0000-0000-0000-000000000000",
        "FieldToMatch": {
          "UriPath": {}
        },
      },
      "TextTransformations": [
        {
          "Priority": 0,
          "Type": "NONE"
        }
      ]
    }
  }
}
}
```

機器人控制範例：從機器人管理排除 IP 範圍

如果您想要從 AWS WAF Bot Control 管理中排除一部分 Web 流量，並且可以使用規則陳述式來識別該子集，則透過將縮小範圍陳述式新增至 Bot Control 受管規則群組陳述式來排除它。

下列規則會在所有 Web 流量上執行正常的 Bot Control 機器人管理，但來自特定 IP 地址範圍的 Web 請求除外。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/000000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```


Bot Control 範例：允許來自您控制之機器人的流量

您可以設定一些網站監控機器人和自訂機器人來傳送自訂標頭。如果您想要允許來自這些類型機器人的流量，您可以將它們設定為在標頭中新增共用秘密。然後，您可以將範圍縮減陳述式新增至 AWS WAF Bot Control 受管規則群組陳述式，以排除具有 標頭的訊息。

下列範例規則會排除 Bot Control 檢查中具有秘密標頭的流量。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            }
          },
          "TextTransformations": [
            {
              "Priority": 0,
```

```
        "Type": "NONE"
      }
    ],
    "PositionalConstraint": "EXACTLY"
  }
}
}
```

機器人控制範例：啟用目標檢查層級

如需增強保護層級，您可以在 AWS WAF Bot Control 受管規則群組中啟用目標檢查層級。

在下列範例中，機器學習功能已啟用。您可以將 `EnableMachineLearning` 設定為 `false`，以選擇退出此行為。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

機器人控制範例：使用兩個陳述式來限制目標檢查層級的使用

作為成本最佳化，您可以在保護套件或 Web ACL 中使用兩個 AWS WAF Bot Control 受管規則群組陳述式，具有單獨的檢查層級和範圍。例如，您可以將目標檢查層級陳述式範圍限定為更敏感的應用程式端點。

下列範例中的兩個陳述式具有互斥範圍。如果沒有此組態，請求可能會導致兩次 Bot Control 評估計費。

Note

主控台的視覺化編輯器 `AWSManagedRulesBotControlRuleSet` 不支援參考多個陳述式。請改用 JSON 編輯器。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
    {
      ...
    },
    {
      "Name": "AWS-AWSBotControl-Common",
      "Priority": 5,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        },
        "RuleActionOverrides": [],
      }
    }
  ]
}
```

```
    "ExcludedRules": [],
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Common"
  },
  "ScopeDownStatement": {
    "NotStatement": {
      "Statement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/sensitive-endpoint",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
},
{
  "Name": "AWS-AWSBotControl-Targeted",
  "Priority": 6,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ]
    },
    "RuleActionOverrides": [],
  }
}
```

}

AWS WAF 分散式阻斷服務 (DDoS) 預防

AWS WAF 為您的 AWS 資源提供複雜且可自訂的 DDoS 攻擊防護。檢閱本節所述的選項，然後選取符合您安全和業務需求的反 DDoS 保護層級。

您可以在 中選擇兩個層級的 DDoS 保護 AWS WAF：

資源層級 DDoS 保護

標準層可在 Application Load Balancer 內運作，透過主機上篩選來防禦已知惡意來源。您可以設定保護行為，以對潛在的 DDoS 事件做出最佳反應。

資源層級 DDoS 保護：

- 自動監控您的流量模式。
- 即時更新威脅情報。
- 防範已知惡意來源。

AWS 受管規則群組 DDoS 保護

進階的 DDoS 保護層是透過提供 `AWSManagedRulesAntiDDoSRuleSet`。受管規則群組補充了資源層級的保護層，具有以下顯著差異：

- 保護延伸至 Application Load Balancer 和 CloudFront 分佈
- 流量基準是為您的受保護資源建立的，以改善新型攻擊模式的偵測。
- 保護行為會根據您選取的敏感度層級來啟用。
- 在可能的 DDoS 事件期間，管理和標記對受保護資源的請求。

如需包含的規則和功能的完整清單，請參閱 [AWS WAF 分散式阻斷服務 \(DDoS\) 預防規則群組](#)。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

主題

- [Application Load Balancer 的資源層級 DDoS 保護](#)
- [使用反 DDoS 受管規則群組的進階 AWS WAF 反 DDoS 保護](#)

Application Load Balancer 的資源層級 DDoS 保護

資源層級 DDoS 保護可為 Application Load Balancer 增加立即防禦，而不考慮 AWS WAF 受管規則群組的定價。此標準層的反 DDoS 保護使用 AWS 威脅情報和流量模式分析來保護 Application Load Balancer。為了識別已知的惡意來源，Anti-DDoS 保護會對直接用戶端 IP 地址和 X-Forwarded-For (XFF) 標頭執行主機上篩選。識別已知惡意來源後，會透過兩種模式之一來啟用保護：

在 DDoS 下作用中是預設保護模式，建議大多數使用案例使用。

此模式：

- 在偵測高負載條件或潛在的 DDoS 事件時自動啟用保護
- Rate-limits 僅在攻擊條件期間從已知惡意來源的流量
- 將正常操作期間對合法流量的影響降至最低
- 使用 Application Load Balancer 運作狀態指標和 AWS WAF 回應資料來判斷何時啟用保護

Always on 是選用模式，啟用後一律處於作用中狀態。

此模式：

- 持續防範已知惡意來源
- Rate-limiting 即時限制來自已知惡意來源的流量
- 對 XFF 標頭中具有惡意 IPs 直接連線和請求套用保護
- 對合法流量的影響可能較高，但可提供最大的安全性

在現有 webACL 上啟用標準 DDoS 保護

您可以在建立 Web ACL 時啟用 DDoS 保護，或更新與 Application Load Balancer 相關聯的現有 Web ACL。

 Note

如果您有與 Application Load Balancer 相關聯的現有 Web ACL，則預設會在 DDoS 模式下使用 Active 啟用反 DDoS 保護。

在 AWS WAF 主控台中啟用反 DDoS 保護

1. 登入 AWS Management Console 並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中選擇 Web ACLs，然後開啟與 Application Load Balancer 相關聯的任何 Web ACL。
3. 選擇關聯的 AWS 資源。
4. 在資源層級 DDoS 保護下，選擇編輯。

5. 選取下列其中一種保護模式：

- 在 DDoS 下作用中（建議）- 只有在高負載條件下才啟用保護
- Always on - 針對已知惡意來源的 Always-on 保護

6. 選擇儲存變更。

Note

如需建立 Web ACL 的詳細資訊，請參閱 [在中建立保護套件或 Web ACL AWS WAF](#)。

使用反 DDoS 受管規則群組的進階 AWS WAF 反 DDoS 保護

`AWSMangedRulesAntiDDoSRuleSet` 受管規則群組是 中可用的最進階的反 DDoS 保護層 AWS WAF。

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

AWS WAF 反 DDoS 保護元件

在 中實作進階反 DDoS 保護的主要元件 AWS WAF 包括下列項目：

`AWSMangedRulesAntiDDoSRuleSet` – 偵測、標記和挑戰可能參與 DDoS 攻擊的請求。它也會在事件期間標記對受保護資源的所有請求。如需規則群組規則和標籤的詳細資訊，請參閱 [AWS WAF 分散式阻斷服務 \(DDoS\) 預防規則群組](#)。若要使用此規則群組，請使用受管規則群組參考陳述式將其包含在保護套件或 Web ACL 中。如需相關資訊，請參閱 [將 Anti-DDoS 受管規則群組新增至您的保護套件或 Web ACL](#)。

- Web ACL 流量概觀儀表板 – 在主控台中提供 DDoS 活動和反 DDoS 回應的監控。如需詳細資訊，請參閱 [保護套件或 Web ACLs 流量概觀儀表板](#)。
- 記錄和指標 – 可讓您監控流量並了解反 DDoS 保護效果。為您的保護套件或 Web ACL 設定日誌、Amazon Security Lake 資料收集和 Amazon CloudWatch 指標。如需這些選項的詳細資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)、[使用 Amazon CloudWatch 監控](#) 和 [什麼是 Amazon Security Lake ?](#)。

- 標籤和標籤比對規則 – 可讓您自訂處理由 Anti-DDoS 受管規則群組識別的 Web 請求。對於 中的任何規則 `AWSManagedRulesAntiDDoSRuleSet`，您可以切換到計數模式並比對新增的標籤。如需詳細資訊，請參閱 [標籤比對規則陳述式及 中的 Web 請求標籤 AWS WAF](#)。
- 自訂請求和回應 – 可讓您將自訂標頭新增至允許的請求，並傳送封鎖請求的自訂回應。將標籤比對與 AWS WAF 自訂請求和回應功能配對。如需詳細資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。

將 Anti-DDoS 受管規則群組新增至您的保護套件或 Web ACL

本節說明如何新增和設定 `AWSManagedRulesAntiDDoSRuleSet` 規則群組。

若要設定 Anti-DDoS 受管規則群組，您可以提供設定，包括規則群組對 DDoS 攻擊的敏感度，以及對正在或可能正在參與攻擊的請求採取的動作。此組態是受管規則群組的一般組態以外的組態。

如需規則群組描述和規則和標籤清單，請參閱 [AWS WAF 分散式阻斷服務 \(DDoS\) 預防規則群組](#)。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。如需如何將受管規則群組新增至保護套件或 Web ACL 的基本資訊，請參閱 [透過主控台將受管規則群組新增至保護套件或 Web ACL](#)。

遵循最佳實務

根據 的最佳實務使用 Anti-DDoS 規則群組 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

在保護套件或 Web ACL 中使用 `AWSManagedRulesAntiDDoSRuleSet` 規則群組

1. 將 AWS 受管規則群組 `AWSManagedRulesAntiDDoSRuleSet` 新增至您的保護套件或 Web ACL，並在儲存之前編輯規則群組設定。

 Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

2. 在規則群組組態窗格中，為 `AWSManagedRulesAntiDDoSRuleSet` 規則群組提供任何自訂組態。
 - a. 針對區塊敏感度層級，指定您希望規則在規則群組的 DDoS 可疑標籤上相符 `DDoSRequests` 時的敏感度。敏感度越高，規則符合的標記層級就越低：
 - 低敏感度較不敏感，導致規則僅與攻擊中最明顯的參與者相符，且具有高度可疑標籤 `aws:waf:managed:aws:anti-ddos:high-suspicion-ddos-request`。

- 中等敏感度會導致規則在中等和高度懷疑標籤上相符。
- 高敏感度會導致規則在所有可疑標籤上相符：低、中和高。

此規則提供對疑似參與 DDoS 攻擊的 Web 請求的最嚴重處理方式。

- b. 針對啟用挑戰，選擇是否啟用規則 `ChallengeDDoSRequests` 和 `ChallengeAllDuringEvent`，預設會將 `Challenge` 動作套用至相符的請求。

這些規則提供請求處理，目的是允許合法使用者繼續處理其請求，同時封鎖 DDoS 攻擊的參與者。您可以將其動作設定覆寫為 `Allow` 或 `Count` 也可以完全停用其使用。

如果您啟用這些規則，請提供您想要的任何其他組態：

- 針對挑戰敏感度等級，指定您希望規則 `ChallengeDDoSRequests` 的敏感度。

敏感度越高，規則符合的標記層級就越低：

- 低敏感度較不敏感，導致規則僅與攻擊中最明顯的參與者相符，且具有高度可疑標籤 `aws:managed:aws:anti-ddos:high-suspicion-ddos-request`。
- 中等敏感度會導致規則在中等和高度懷疑標籤上相符。
- 高敏感度會導致規則在所有可疑標籤上相符：低、中和高。
- 對於豁免 URI 規則表達式，提供符合無法處理無提示瀏覽器挑戰之 Web 請求 URIs 的規則表達式。`Challenge` 動作會有效地封鎖來自缺少挑戰字元 URIs 的請求，除非它們可以處理靜音瀏覽器挑戰。

`Challenge` 動作只能由預期 HTML 內容的用戶端正確處理。如需動作運作方式的詳細資訊，請參閱 [CAPTCHA 和 Challenge 動作行為](#)。

檢閱預設規則表達式並視需要更新。這些規則使用指定的規則表達式來識別無法處理 `Challenge` 動作的請求 URIs，並防止規則傳送挑戰回去。您以這種方式排除的請求只能由規則群組使用規則 來封鎖 `DDoSRequests`。

主控台中提供的預設表達式涵蓋了大多數的使用案例，但您應該檢閱並根據您的應用程式進行調整。

AWS WAF 支援 PCRE 程式庫使用的模式語法 `libpcre`，但有一些例外。程式庫記錄在 [PCRE - Perl 相容規則表達式](#) 中。如需 AWS WAF 支援的相關資訊，請參閱 [中支援的規則表達式語法 AWS WAF](#)。

3. 提供您想要用於規則群組的任何其他組態，並儲存規則。

 Note

AWS 建議不要搭配此受管規則群組使用縮小範圍陳述式。縮小範圍陳述式會限制規則群組觀察到的請求，因此可能會導致流量基準不準確和 DDoS 事件偵測減少。縮小範圍陳述式選項適用於所有受管規則群組陳述式，但不應用於此陳述式。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。

4. 在設定規則優先順序頁面中，將新的反 DDoS 受管規則群組規則向上移動，使其僅在您擁有的任何 Allow 動作規則之後以及在任何其他規則之前執行。這可讓規則群組追蹤最多流量以進行反 DDoS 保護。
5. 將變更儲存至保護套件或 Web ACL。

在部署生產流量的反 DDoS 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。如需指引，請參閱以下章節。

測試和部署反 DDoS

在部署功能之前，您會想要設定和測試 AWS WAF 分散式阻斷服務 (DDoS) 預防。本節提供設定和測試的一般指引，但您選擇遵循的特定步驟將取決於您收到的需求、資源和 Web 請求。

此資訊是 所提供測試和調校的一般資訊之外的。 [測試和調校您的 AWS WAF 保護](#)

 Note

AWS 受管規則旨在保護您免受常見的 Web 威脅。根據文件使用時，AWS 受管規則規則群組會為您的應用程式新增另一層安全性。不過，AWS 受管規則規則群組並非旨在取代您的安全責任，這取決於您選擇的 AWS 資源。請參閱 [共同責任模型](#)，以確保您在 中的資源 AWS 受到適當保護。

 生產流量風險

在預備或測試環境中測試和調校您的反 DDoS 實作，直到您熟悉對流量的潛在影響為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。

本指南適用於通常知道如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組的使用者。這些主題涵蓋在本指南的先前章節中。

設定和測試 AWS WAF 分散式阻斷服務 (DDoS) 預防實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 在計數模式中新增 AWS WAF 分散式阻斷服務 (DDoS) 預防受管規則群組

Note

當您使用此受管規則群組時，需支付額外費用。如需詳細資訊，請參閱[AWS WAF 定價](#)。

將 AWS 受管規則群組 `AWSMangedRulesAntiDDoSRuleSet` 新增至新的或現有的保護套件或 Web ACL，並加以設定，使其不會變更目前的保護套件或 Web ACL 行為。如需此規則群組之規則和標籤的詳細資訊，請參閱 [AWS WAF 分散式阻斷服務 \(DDoS\) 預防規則群組](#)。

- 當您新增受管規則群組時，請進行編輯並執行下列動作：
 - 在規則群組組態窗格中，提供為您的 Web 流量執行反 DDoS 活動所需的詳細資訊。如需詳細資訊，請參閱[將 Anti-DDoS 受管規則群組新增至您的保護套件或 Web ACL](#)。
 - 在規則窗格中，開啟覆寫所有規則動作下拉式清單，然後選擇 Count。使用此組態，會根據規則群組中的所有規則 AWS WAF 評估請求，並僅計算該結果的相符項目，同時仍將標籤新增至請求。如需詳細資訊，請參閱[覆寫規則群組中的規則動作](#)。

透過此覆寫，您可以監控 Anti-DDoS 受管規則的潛在影響，以判斷您是否要進行修改，例如為無法處理無提示瀏覽器挑戰 URIs 擴展 regex。

- 放置規則群組，以便在允許流量的任何規則之後立即儘早進行評估。規則會以遞增的數值優先順序進行評估。主控台會為您設定順序，從規則清單頂端開始。如需詳細資訊，請參閱[設定規則優先順序](#)。

2. 啟用保護套件或 Web ACL 的記錄和指標

視需要設定 保護套件或 Web ACL 的記錄、Amazon Security Lake 資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見性工具來監控 Anti-DDoS 受管規則群組與流量的互動。

- 如需有關設定和使用記錄的資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

- 如需 Amazon Security Lake 的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的什麼是 Amazon Security Lake？以及[從 AWS 服務收集資料](#)。
- 如需 Amazon CloudWatch 指標的相關資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。
- 如需有關 Web 請求取樣的資訊，請參閱 [檢視 Web 請求的範例](#)。

3. 將保護套件或 Web ACL 與資源建立關聯

如果保護套件或 Web ACL 尚未與測試資源建立關聯，請建立關聯。如需相關資訊，請參閱[將保護與 AWS 資源建立關聯或取消關聯](#)。

4. 監控流量和反 DDoS 規則相符項目

請確定您的正常流量正在流動，且 Anti-DDoS 受管規則群組規則正在將標籤新增至相符的 Web 請求。您可以在日誌中查看標籤，並在 Amazon CloudWatch 指標中查看反 DDoS 和標籤指標。在日誌中，您已覆寫規則群組中計數的規則會顯示在 `ruleGroupList` 並將 `action` 設定為計數，並 `overriddenAction` 指出您覆寫的已設定規則動作。

5. 自訂反 DDoS Web 請求處理

視需要新增您自己的規則，明確允許或封鎖請求，以變更反 DDoS 規則處理它們的方式。

例如，您可以使用反 DDoS 標籤來允許或封鎖請求，或自訂請求處理。您可以在反 DDoS 受管規則群組之後新增標籤比對規則，以篩選要套用之處理方式的標記請求。測試之後，請將相關的 Anti-DDoS 規則保持在計數模式中，並在您的自訂規則中維護請求處理決策。

6. 移除測試規則並設定反 DDoS 設定

檢閱您的測試結果，以判斷您要在計數模式中保留哪些 Anti-DDoS 規則，只進行監控。對於您想要在主動保護下執行的任何規則，請在保護套件或 Web ACL 規則群組組態中停用計數模式，以允許他們執行其設定的動作。完成這些設定後，請移除任何臨時測試標籤比對規則，同時保留您為生產用途建立的任何自訂規則。如需其他反 DDoS 組態考量，請參閱 [中的智慧型威脅防禦最佳實務 AWS WAF](#)。

7. 監控和調校

為了確保 Web 請求可依您想要的方式處理，請在啟用您要使用的反 DDoS 功能後密切監控流量。視需要使用規則群組上的規則計數覆寫和您自己的規則來調整行為。

反 DDoS 的最佳實務

- 在正常流量期間啟用保護 – 這可讓保護在回應攻擊之前建立基準流量模式。當您沒有遭受攻擊時新增保護，並允許建立基準的時間。

- 定期監控指標 – 檢閱 CloudWatch 指標，以了解流量模式和保護有效性。
- 考慮關鍵應用程式的主動模式 – 雖然大多數使用案例都建議使用被動模式，但對於需要持續防護已知威脅的應用程式，請考慮使用主動模式。
- 在預備環境中測試 – 在生產環境中啟用保護之前，請在預備環境中測試和調校設定，以了解對合法流量的影響。

中的用戶端應用程式整合 AWS WAF

本節說明如何將智慧型威脅整合 APIs 和 JavaScript CAPTCHA 整合 API 與您的 AWS WAF 功能搭配使用。

使用 AWS WAF 用戶端應用程式整合 APIs 將用戶端保護與您的 AWS 伺服器端保護套件或 Web ACL 保護耦合，以協助驗證將 Web 請求傳送至受保護資源的用戶端應用程式是否為預期的用戶端，以及您的最終使用者是否為人類。

使用用戶端整合來管理無提示的瀏覽器挑戰和 CAPTCHA 拼圖、取得具有成功瀏覽器和最終使用者回應證明的字符，以及將這些字符包含在對受保護端點的請求中。如需 AWS WAF 字符的一般資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

將用戶端整合與需要有效字符才能存取資源的保護套件或 Web ACL 保護結合。您可以使用規則群組來檢查和監控挑戰字符，例如下一節列出的挑戰字符，網址為 [智慧型威脅整合和 AWS 受管規則](#)，而且您可以使用 CAPTCHA 和 Challenge 規則動作來檢查，如 [中所述 CAPTCHA 和 Challenge 中的 AWS WAF](#)。

AWS WAF 為 JavaScript 應用程式提供兩種整合層級，並為行動應用程式提供一種：

- 智慧威脅整合 – 驗證用戶端應用程式，並提供 AWS 權杖取得和管理。這類似於規則動作所提供的 AWS WAF Challenge 功能。此功能完全整合您的用戶端應用程式與 `AWSManagedRulesACFPRuleSet` 受管規則群組、`AWSManagedRulesATPRuleSet` 受管規則群組，以及 `AWSManagedRulesBotControlRuleSet` 受管規則群組的目標保護層級。

智慧型威脅整合 APIs 使用無 AWS WAF 提示瀏覽器挑戰，協助確保只有在用戶端取得有效的字符之後，才允許對您受保護資源的登入嘗試和其他呼叫。APIs 會管理用戶端應用程式工作階段的字符授權，並收集用戶端的相關資訊，以協助判斷其是否由機器人或人類操作。

Note

這適用於 JavaScript 和 Android 和 iOS 行動應用程式。

- CAPTCHA 整合 – 使用您在應用程式中管理的自訂 CAPTCHA 拼圖來驗證最終使用者。這類似於規則動作所提供的 AWS WAF CAPTCHA 功能，但增加了對拼圖放置和行為的控制。

此整合利用 JavaScript 智慧型威脅整合來執行無聲挑戰，並將 AWS WAF 權杖提供給客戶的頁面。

Note

這適用於 JavaScript 應用程式。

主題

- [智慧型威脅整合和 AWS 受管規則](#)
- [存取 AWS WAF 用戶端應用程式整合 APIs](#)
- [AWS WAF JavaScript 整合](#)
- [AWS WAF 行動應用程式整合](#)

智慧型威脅整合和 AWS 受管規則

本節說明智慧型威脅整合 APIs 如何與 AWS 受管規則規則群組搭配使用。

智慧型威脅整合 APIs 可與使用智慧型威脅規則群組的保護套件或 Web ACLs 搭配使用，以啟用這些進階受管規則群組的完整功能。

- AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組 `AWSMangedRulesACFPRuleSet`。

帳戶建立詐騙是一種線上非法活動，攻擊者會在您的應用程式中建立無效的帳戶，例如接收註冊獎金或冒充某人。ACFP 受管規則群組提供規則來封鎖、標記和管理可能屬於詐騙帳戶建立嘗試一部分的請求。APIs 可啟用經過微調的用戶端瀏覽器驗證和人類互動資訊，以供 ACFP 規則用來區隔有效的用戶端流量與惡意流量。

如需詳細資訊，請參閱[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)及[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)。

- AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組 `AWSMangedRulesATPRuleSet`。

帳戶接管是一種線上非法活動，攻擊者可在其中未經授權存取某人的帳戶。ATP 受管規則群組提供規則來封鎖、標記和管理可能屬於惡意帳戶接管嘗試一部分的請求。APIs 可啟用微調的用戶端驗證和行為彙總，讓 ATP 規則用來區隔有效的用戶端流量與惡意流量。

如需詳細資訊，請參閱[AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)及[AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)。

- AWS WAF Bot Control 受管規則群組 的目標保護層級 `AWSTManagedRulesBotControlRuleSet`。

機器人從自我識別和有用的機器人執行，例如大多數搜尋引擎和爬蟲程式，到針對您的網站操作且不自我識別的惡意機器人。Bot Control 受管規則群組提供規則來監控、標記和管理 Web 流量中的機器人活動。當您使用此規則群組的目標保護層級時，目標規則會使用 APIs 提供的用戶端工作階段資訊，以更好地偵測惡意機器人。

如需詳細資訊，請參閱[AWS WAF 機器人控制規則群組](#)及[AWS WAF 機器人控制](#)。

若要將其中一個受管規則群組新增至保護套件或 Web ACL，請參閱程序 [將 ACFP 受管規則群組新增至 Web ACL](#)、[將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#) 和 [將 AWS WAF Bot Control 受管規則群組新增至 Web ACL](#)。

Note

受管規則群組目前不會封鎖缺少字符的請求。為了封鎖缺少權杖的請求，在您實作應用程式整合 APIs 之後，請遵循 中的指引[封鎖沒有有效 AWS WAF 字符的請求](#)。

存取 AWS WAF 用戶端應用程式整合 APIs

本節說明在 AWS WAF 主控台中尋找應用程式整合 APIs 的位置。

JavaScript 整合 APIs 已全面推出，您可以將其用於您的瀏覽器和其他執行 JavaScript 的裝置。

AWS WAF 提供適用於 Android 和 iOS 行動應用程式的自訂智慧型威脅整合 SDKs。

- 對於 Android 行動和電視應用程式，SDKs 適用於 Android API 第 23 版 (Android 第 6 版) 和更新版本。如需 Android 版本的資訊，請參閱 [SDK 平台版本備註](#)。
- 對於 iOS 行動應用程式，SDKs 適用於 iOS 版本 13 和更新版本。如需 iOS 版本的資訊，請參閱 [iOS & iPadOS 版本備註](#)。
- 對於 Apple TV 應用程式，SDKs 適用於 tvOS 第 14 版或更新版本。如需 tvOS 版本的資訊，請參閱 [tvOS 版本備註](#)。

透過主控台存取整合 APIs

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中選擇應用程式整合，然後選擇您感興趣的索引標籤。
 - 智慧型威脅整合適用於 JavaScript 和行動應用程式。

標籤包含下列項目：

- 已啟用智慧型威脅應用程式整合的保護套件或 Web ACLs 清單。此清單包含每個使用 AWSManagedRulesACFPRuleSet 受管規則群組、AWSManagedRulesATPRuleSet 受管規則群組或 AWSManagedRulesBotControlRuleSet 受管規則群組的目標保護層級的保護套件或 Web ACL。當您實作智慧型威脅 APIs 時，您可以使用要與之整合的保護套件或 Web ACL 的整合 URL。
- 您可以存取 APIs。JavaScript APIs 一律可用。如需存取行動 SDKs，請聯絡 [Contact AWS](#) 的支援。
- CAPTCHA 整合適用於 JavaScript 應用程式。

標籤包含下列項目：

- 用於整合的整合 URL。
- 您為用戶端應用程式網域建立的 API 金鑰。您使用 CAPTCHA API 需要加密的 API 金鑰，讓用戶端有權從其網域存取 AWS WAF CAPTCHA。對於您整合的每個用戶端，請使用包含用戶端網域的 API 金鑰。如需這些要求以及管理這些金鑰的詳細資訊，請參閱 [管理 JS CAPTCHA API 的 API 金鑰](#)。

AWS WAF JavaScript 整合

本節說明如何使用 AWS WAF JavaScript 整合。

您可以使用 JavaScript 整合 APIs 在瀏覽器和其他執行 JavaScript 的裝置中實作 AWS WAF 應用程式整合。

CAPTCHA 拼圖和無提示挑戰只能在瀏覽器存取 HTTPS 端點時執行。瀏覽器用戶端必須在安全的內容中執行，才能取得字符。

- 智慧型威脅 APIs 可讓您透過無提示的用戶端瀏覽器挑戰來管理權杖授權，並在您傳送至受保護資源的請求中包含權杖。

- CAPTCHA 整合 API 會新增至智慧型威脅 APIs，並可讓您自訂用戶端應用程式中 CAPTCHA 拼圖的位置和特性。此 API 會利用智慧型威脅 APIs 來取得 AWS WAF 權杖，以便在最終使用者成功完成 CAPTCHA 拼圖後，於頁面中使用。

透過使用這些整合，您可以確保用戶端的遠端程序呼叫包含有效的字符。當您的應用程式頁面上有這些整合 APIs 時，您可以在保護套件或 Web ACL 中實作緩解規則，例如封鎖不包含有效字符的請求。您也可以實作規則，在規則中使用 Challenge 或 CAPTCHA 動作，強制使用用戶端應用程式取得的字符。

實作智慧型威脅 APIs 的範例

下列清單顯示 Web 應用程式頁面中智慧型威脅 APIs 典型實作的基本元件。

```
<head>
<script type="text/javascript" src="protection pack or web ACL integration URL/
challenge.js" defer></script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
</script>
```

CAPTCHA JavaScript API 的範例實作

CAPTCHA 整合 API 可讓您自訂最終使用者的 CAPTCHA 拼圖體驗。CAPTCHA 整合利用 JavaScript 智慧型威脅整合進行瀏覽器驗證和字符管理，並新增用於設定和轉譯 CAPTCHA 拼圖的函數。

下列清單顯示 CAPTCHA JavaScript API 在 Web 應用程式頁面中典型實作的基本元件。

```
<head>
  <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
  function showMyCaptcha() {
    var container = document.querySelector("#my-captcha-container");

    AwsWafCaptcha.renderCaptcha(container, {
```

```
        apiKey: "...API key goes here...",
        onSuccess: captchaExampleSuccessFunction,
        onError: captchaExampleErrorFunction,
        ...other configuration parameters as needed...
    });
}

function captchaExampleSuccessFunction(wafToken) {
    // Use WAF token to access protected resources
    AwsWafIntegration.fetch("...WAF-protected URL...", {
        method: "POST",
        ...
    });
}

function captchaExampleErrorFunction(error) {
    /* Do something with the error */
}
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

主題

- [提供用於字符的網域](#)
- [使用 JavaScript API 搭配內容安全政策](#)
- [使用智慧型威脅 JavaScript API](#)
- [使用 CAPTCHA JavaScript API](#)

提供用於字符的網域

本節說明如何提供字符的其他網域。

根據預設，當 AWS WAF 建立權杖時，它會使用與保護套件或 Web ACL 相關聯的資源的主機網域。您可以為 JavaScript APIs 在 AWS WAF 建立的字符提供額外的網域。若要這樣做，`window.awsWafCookieDomainList` 請使用一或多個字符網域來設定全域變數。

當 AWS WAF 建立字符時，它會使用來自中網域組合中最適當、最短的網域，`window.awsWafCookieDomainList` 以及與保護套件或 Web ACL 相關聯之資源的主機網域。

範例設定：

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

您無法在此清單中使用公有字尾。例如，您無法使用 gov.au 或 co.uk 做為清單中的字符網域。

您在此清單中指定的網域必須與其他網域和網域組態相容：

- 網域必須是 AWS WAF 將根據受保護主機網域和為保護套件或 Web ACL 設定的字符網域清單接受的網域。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。
- 如果您使用 JavaScript CAPTCHA API，CAPTCHA API 金鑰中至少有一個網域必須與 中的其中一個字符網域完全相符，window.awsWafCookieDomainList 或者必須是其中一個字符網域的頂點網域。

例如，對於字符網域 mySubdomain.myApex.com，API 金鑰 mySubdomain.myApex.com 是完全相符的，API 金鑰 myApex.com 是頂點網域。任一金鑰都符合字符網域。

如需 API 金鑰的詳細資訊，請參閱 [管理 JS CAPTCHA API 的 API 金鑰](#)。

如果您使用 AWSManagedRulesACFPRuleSet 受管規則群組，您可以設定符合您提供給規則群組組態之帳戶建立路徑的網域。如需此組態的詳細資訊，請參閱「[將 ACFP 受管規則群組新增至 Web ACL](#)」。

如果您使用 AWSManagedRulesATPRuleSet 受管規則群組，您可以在您提供給規則群組組態的登入路徑中，設定符合該網域的網域。如需此組態的詳細資訊，請參閱「[將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)」。

使用 JavaScript API 搭配內容安全政策

本節提供允許列出 AWS WAF 網域的範例組態。

如果您將內容安全政策 (CSP) 套用到您的資源，為了讓 JavaScript AWS WAF 實作運作，您需要允許列出頂點網域 aws.waf.com。JavaScript SDKs 會呼叫不同的 AWS WAF 端點，因此允許列出此網域可提供 SDKs 操作所需的許可。

以下顯示允許列出頂 AWS WAF 網域的範例組態：

```
connect-src 'self' https://*.aws.waf.com;
```

```
script-src 'self' https://*.aws.waf.com;  
script-src-elem 'self' https://*.aws.waf.com;
```

如果您嘗試將 JavaScript SDKs 與使用 CSP 的資源搭配使用，但您尚未允許列出 AWS WAF 網域，則會收到如下錯誤：

```
Refused to load the script ...aws.waf.com/<> because it violates the following Content Security Policy directive: "script-src 'self'"
```

使用智慧型威脅 JavaScript API

本節提供在用戶端應用程式中使用智慧型威脅 JavaScript API 的指示。

智慧型威脅 APIs 提供對使用者瀏覽器執行無提示挑戰的操作，以及處理提供成功挑戰證明和 CAPTCHA 回應的 AWS WAF 字符的操作。

先在測試環境中實作 JavaScript 整合，然後在生產環境中實作。如需其他編碼指引，請參閱以下各節。

使用智慧型威脅 APIs

1. 安裝 APIs

如果您使用 CAPTCHA API，則可以略過此步驟。安裝 CAPTCHA API 時，指令碼會自動安裝智慧型威脅 APIs。

- a. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
- b. 在導覽窗格中，選擇 Application integration (應用程式整合)。在應用程式整合頁面上，您可以看到標籤選項。
- c. 選取智慧型威脅整合
- d. 在索引標籤中，選取您要整合的保護套件或 Web ACL。保護套件或 Web ACL 清單僅包含使用 `AWSManagedRulesACFPRuleSet` 受管規則群組、`AWSManagedRulesATPRuleSet` 受管規則群組或 `AWSManagedRulesBotControlRuleSet` 受管規則群組的目標保護層級的保護套件或 Web ACLs。
- e. 開啟 JavaScript SDK 窗格，並複製指令碼標籤以用於整合。
- f. 在應用程式頁面程式碼的 `<head>` 區段中，插入您為保護套件或 Web ACL 複製的指令碼標籤。此包含項目會導致您的用戶端應用程式在頁面載入的背景中自動擷取字符。

```
<head>
  <script type="text/javascript" src="protection pack or web ACL integration
    URL/challenge.js" defer></script>
</head>
```

此 `<script>` 清單使用 `defer` 屬性設定，但如果 `async` 您想要為頁面採取不同的行為，您可以將設定變更為。

2. （選用）新增用戶端字符的網域組態 – 根據預設，當 AWS WAF 建立字符時，它會使用與保護套件或 Web ACL 相關聯之資源的主機網域。若要提供 JavaScript APIs 的其他網域，請遵循 [中的指引提供用於字符的網域](#)。
3. 為您的智慧型威脅整合編寫程式碼 – 撰寫程式碼，以確保字符擷取在用戶端將其請求傳送至受保護的端點之前完成。如果您已使用 `fetch` API 進行呼叫，則可以取代整合 `fetch` 包裝函式 AWS WAF。如果您不使用 `fetch` API，則可以改用 AWS WAF 整合 `getToken` 操作。如需編碼指引，請參閱下列各節。
4. 在保護套件或 Web ACL 中新增權杖驗證 – 將至少一個規則新增至保護套件或 Web ACL，以檢查用戶端傳送的 Web 請求中是否有有效的挑戰權杖。您可以使用規則群組來檢查和監控挑戰字符，例如 Bot Control 受管規則群組的目標層級，而且您可以使用 Challenge 規則動作來檢查，如中所述 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

保護套件或 Web ACL 新增項目會驗證對受保護端點的請求是否包含您在用戶端整合中取得的字符。包含有效、未過期字符的請求會通過 Challenge 檢查，並且不會向您的用戶端傳送另一個無提示挑戰。

5. （選用）封鎖缺少權杖的請求 – 如果您搭配 ACFP 受管規則群組、ATP 受管規則群組或 Bot Control 規則群組的目標規則使用 APIs，這些規則不會封鎖缺少權杖的請求。若要封鎖缺少字符的請求，請遵循 [中的指引封鎖沒有有效 AWS WAF 字符的請求](#)。

主題

- [智慧威脅 API 規格](#)
- [如何使用整合 `fetch` 包裝函式](#)
- [如何使用整合 `getToken`](#)

智慧威脅 API 規格

本節列出智慧型威脅緩解 JavaScript APIs 的方法和屬性規格。使用這些 APIs 進行智慧威脅和 CAPTCHA 整合。

AwsWafIntegration.fetch()

使用 AWS WAF 整合實作將 HTTP fetch請求傳送至伺服器。

AwsWafIntegration.getToken()

擷取儲存的 AWS WAF 字符，並將其存放在目前頁面上名為 aws-waf-token且值設定為字符值的 Cookie 中。

AwsWafIntegration.hasToken()

傳回布林值，指出 aws-waf-token Cookie 目前是否擁有未過期的字符。

如果您也使用 CAPTCHA 整合，請參閱 [中該整合的規格CAPTCHA JavaScript API 規格](#)。

如何使用整合fetch包裝函式

本節提供使用整合fetch包裝函式的說明。

您可以在AwsWafIntegration命名空間下變更對 fetch API 的正常fetch呼叫，以使用 AWS WAF fetch包裝函式。AWS WAF 包裝函式支援所有與標準 JavaScript fetch API 呼叫相同的選項，並新增整合的字符處理。此方法通常是整合您應用程式最簡單的方法。

包裝函式實作之前

下列範例清單顯示實作AwsWafIntegrationfetch包裝函式之前的標準程式碼。

```
const login_response = await fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
```

包裝函式實作之後

下列清單顯示與AwsWafIntegrationfetch包裝函式實作相同的程式碼。

```
const login_response = await AwsWafIntegration.fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
```

```
body: login_body
});
```

如何使用整合 `getToken`

本節說明如何使用 `getToken` 操作。

AWS WAF 需要您對受保護端點的請求，以包含名為 `aws-waf-token` 的 Cookie 與目前字符的值。

`getToken` 操作是一種非同步 API 呼叫，會擷取 AWS WAF 字符並將其存放在目前頁面上名為 `aws-waf-token` 且值設定為字符值的 Cookie 中。您可以在頁面中視需要使用此權杖 Cookie。

當您呼叫 `getToken`，它會執行下列動作：

- 如果已可使用未過期的字符，呼叫會立即傳回它。
- 否則，呼叫會從權杖提供者擷取新的權杖，在逾時之前等待最多 2 秒讓權杖擷取工作流程完成。如果操作逾時，它會擲回呼叫程式碼必須處理的錯誤。

`getToken` 操作具有隨附的 `hasToken` 操作，指出 `aws-waf-token` Cookie 目前是否擁有未過期的字符。

`AwsWafIntegration.getToken()` 會擷取有效的字符並將其儲存為 Cookie。大多數用戶端呼叫會自動連接此 Cookie，但有些則不會。例如，跨主機網域進行的呼叫不會連接 Cookie。在接下來的實作詳細資訊中，我們會示範如何使用這兩種類型的用戶端呼叫。

基本 `getToken` 實作，適用於連接 `aws-waf-token` Cookie 的呼叫

下列範例清單顯示使用登入請求實作 `getToken` 操作的標準程式碼。

```
const login_response = await AwsWafIntegration.getToken()
  .catch(e => {
    // Implement error handling logic for your use case
  })
// The getToken call returns the token, and doesn't typically require special
handling
.then(token => {
  return loginToMyPage()
})

async function loginToMyPage() {
  // Your existing login code
}
```


僅在字符可從 取得之後才提交表單 `getToken`

以下清單說明如何註冊事件接聽程式以攔截表單提交，直到可用的有效權杖為止。

```
<body>
  <h1>Login</h1>
  <p></p>
  <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
    <label for="input_username">USERNAME</label>
    <input type="text" name="input_username" id="input_username"><br>
    <label for="input_password">PASSWORD</label>
    <input type="password" name="input_password" id="input_password"><br>
    <button type="submit">Submit<button>
  </form>

<script>
  const form = document.querySelector("#login-form");

  // Register an event listener to intercept form submissions
  form.addEventListener("submit", (e) => {
    // Submit the form only after a token is available
    if (!AwsWafIntegration.hasToken()) {
      e.preventDefault();
      AwsWafIntegration.getToken().then(() => {
        e.target.submit();
      }, (reason) => { console.log("Error:"+reason) });
    }
  });
</script>
</body>
```

在用戶端預設不連接 **aws-waf-token** Cookie 時連接字符

`AwsWafIntegration.getToken()` 會擷取有效的字符並將其儲存為 Cookie，但並非所有用戶端呼叫預設會連接此 Cookie。例如，跨主機網域進行的呼叫不會連接 Cookie。

`fetch` 包裝函式會自動處理這些案例，但如果您無法使用 `fetch` 包裝函式，除了從 `aws-waf-token` Cookie 讀取權杖之外，您還可以使用自訂 `x-aws-waf-token` header. AWS WAF reads 權杖來處理。下列程式碼顯示設定 標頭的範例。

```
const token = await AwsWafIntegration.getToken();
```

```
const result = await fetch('/url', {
  headers: {
    'x-aws-waf-token': token,
  },
});
```

根據預設，AWS WAF 僅接受與請求的主機網域包含相同網域的字符。任何跨網域字符都需要保護套件或 Web ACL 字符網域清單中的對應項目。如需詳細資訊，請參閱[AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

如需跨網域字符使用的其他資訊，請參閱 [aws-samples/aws-waf-bot-control-api-protection-with-captcha](#)。

使用 CAPTCHA JavaScript API

本節提供使用 CAPTCHA 整合 API 的說明。

CAPTCHA JavaScript API 可讓您設定 CAPTCHA 拼圖，並將其放置在用戶端應用程式中您想要的位置。此 API 利用智慧型威脅 JavaScript APIs 的功能，在最終使用者成功完成 CAPTCHA 拼圖後取得和使用 AWS WAF 字符。

先在測試環境中實作 JavaScript 整合，然後在生產環境中實作。如需其他編碼指引，請參閱以下各節。

使用 CAPTCHA 整合 API

1. 安裝 API

- 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
- 在導覽窗格中，選擇 Application integration (應用程式整合)。在應用程式整合頁面上，您可以看到標籤選項。
- 選取 CAPTCHA 整合。
- 複製列出的 JavaScript 整合指令碼標籤，以用於您的整合。
- 在應用程式頁面程式碼的 <head> 區段中，插入您複製的指令碼標籤。此包含項目可讓 CAPTCHA 拼圖可供組態和使用。

```
<head>
  <script type="text/javascript" src="integrationURL/jsapi.js" defer></script>
```

</head>

此 `<script>` 清單是使用 `defer` 屬性設定，但如果 `async` 您希望頁面有不同的行為，您可以將設定變更為。

如果智慧型威脅整合指令碼尚未存在，CAPTCHA 指令碼也會自動載入。智慧型威脅整合指令碼可讓您的用戶端應用程式在頁面載入的背景中自動擷取字符，並提供您使用 CAPTCHA API 所需的其他字符管理功能。

2. （選用）新增用戶端字符的網域組態 – 根據預設，當 AWS WAF 建立字符時，它會使用與保護套件或 Web ACL 相關聯之資源的主機網域。若要提供 JavaScript APIs 的其他網域，請遵循 [中的指引提供用於字符的網域](#)。
3. 取得用戶端的加密 API 金鑰 – CAPTCHA API 需要加密的 API 金鑰，其中包含有效的用戶端網域清單。AWS WAF 使用此金鑰來驗證您搭配整合使用的用戶端網域是否已核准使用 AWS WAF CAPTCHA。若要產生您的 API 金鑰，請遵循 [中的指引管理 JS CAPTCHA API 的 API 金鑰](#)。
4. 為您的 CAPTCHA 小工具實作編寫程式碼：在您的頁面中您想要使用它的位置實作 `renderCaptcha()` API 呼叫。如需有關設定和使用此函數的資訊，請參閱下列各節 [CAPTCHA JavaScript API 規格](#) 和 [如何轉譯 CAPTCHA 拼圖](#)。

CAPTCHA 實作會與智慧威脅整合 APIs 整合，以進行權杖管理，並執行使用權 AWS WAF 杖的擷取呼叫。如需使用這些 APIs 的指引，請參閱 [使用智慧型威脅 JavaScript API](#)。

5. 在保護套件或 Web ACL 中新增權杖驗證 – 將至少一個規則新增至保護套件或 Web ACL，以檢查用戶端傳送的 Web 請求中是否有有效的 CAPTCHA 權杖。您可以使用 CAPTCHA 規則動作來檢查，如中所述 [CAPTCHA 和 Challenge 中的 AWS WAF](#)。

保護套件或 Web ACL 新增項目會驗證傳送至受保護端點的請求是否包含您在用戶端整合中取得的字符。包含有效、未過期 CAPTCHA 字符的請求會通過 CAPTCHA 規則動作檢查，而不會向最終使用者顯示另一個 CAPTCHA 拼圖。

實作 JavaScript API 之後，您可以檢閱 CAPTCHA 拼圖嘗試和解決方案的 CloudWatch 指標。如需指標和維度詳細資訊，請參閱 [帳戶指標和維度](#)。

主題

- [CAPTCHA JavaScript API 規格](#)
- [如何轉譯 CAPTCHA 拼圖](#)
- [從處理 CAPTCHA 回應 AWS WAF](#)
- [管理 JS CAPTCHA API 的 API 金鑰](#)

CAPTCHA JavaScript API 規格

本節列出 CAPTCHA JavaScript APIs 的方法和屬性規格。使用 CAPTCHA JavaScript APIs 在用戶端應用程式中執行自訂 CAPTCHA 拼圖。

此 API 建置在智慧型威脅 APIs 上，您可用來設定和管理 AWS WAF 權杖的取得和使用。請參閱 [智慧威脅 API 規格](#)。

AwsWafCaptcha.renderCaptcha(container, configuration)

向最終使用者展示 AWS WAF CAPTCHA 拼圖，並在成功時以 CAPTCHA 驗證更新用戶端字符。這僅適用於 CAPTCHA 整合。使用此呼叫搭配智慧型威脅 APIs 來管理權杖擷取，並在您的 fetch 呼叫中提供權杖。請參閱 中的智慧型威脅 APIs [智慧威脅 API 規格](#)。

與 AWS WAF 傳送的 CAPTCHA 問卷不同，此方法轉譯的 CAPTCHA 拼圖會立即顯示拼圖，無需初始標題畫面。

container

頁面上目標容器元素的 Element 物件。這通常是透過呼叫 `document.getElementById()` 或來擷取 `document.querySelector()`。

必要：是

類型：Element

組態

包含 CAPTCHA 組態設定的物件，如下所示：

apiKey

啟用用戶端網域許可的加密 API 金鑰。使用 AWS WAF 主控台為您的用戶端網域產生 API 金鑰。您最多可以將一個金鑰用於五個網域。如需相關資訊，請參閱 [管理 JS CAPTCHA API 的 API 金鑰](#)。

必要：是

類型：string

onSuccess: (wafToken: string) => void;

當最終使用者成功完成 CAPTCHA 拼圖時，使用有效的 AWS WAF 字符呼叫。在您傳送到使用 AWS WAF 保護套件或 Web ACL 保護之端點的請求中使用字符。字符提供最新成功拼圖完成的證明和時間戳記。

必要：是

onError?: (error: CaptchaError) => void;

在 CAPTCHA 操作期間發生錯誤時呼叫錯誤物件。

必要：否

CaptchaError 類別定義 – onError處理常式提供具有下列類別定義的錯誤類型。

```
CaptchaError extends Error {  
    kind: "internal_error" | "network_error" | "token_error" | "client_error";  
    statusCode?: number;  
}
```

- kind – 傳回的錯誤類型。
- statusCode – HTTP 狀態碼，如果有的話。network_error 如果錯誤是由於 HTTP 錯誤所造成，則會使用此功能。

onLoad?: () => void;

載入新的 CAPTCHA 拼圖時呼叫。

必要：否

onPuzzleTimeout?: () => void;

在 CAPTCHA 拼圖過期之前未完成時呼叫。

必要：否

onPuzzleCorrect?: () => void;

將正確答案提供給 CAPTCHA 拼圖時呼叫。

必要：否

onPuzzleIncorrect?: () => void;

當向 CAPTCHA 拼圖提供不正確的答案時呼叫。

必要：否

defaultLocale

用於 CAPTCHA 拼圖的預設地區設定。CAPTCHA 拼圖的書面說明提供阿拉伯文 (ar-SA)、簡體中文 (zh-CN)、荷蘭文 (nl-NL)、英文 (en-US)、法文 (fr-FR)、德文 (de-DE)、義大利文

(it-IT)、日文 (ja-JP)、巴西葡萄牙文 (pt-BR)、西班牙文 (es-ES) 和土耳其文 (tr-TR)。除了預設為英文的中文和日文以外，音訊指示適用於所有書面語言。若要變更預設語言，請提供國際語言和地區設定代碼，例如 ar-SA。

預設：目前在最終使用者的瀏覽器中使用的語言

必要：否

類型：string

disableLanguageSelector

如果設定為 true，CAPTCHA 拼圖會隱藏語言選擇器。

預設：false

必要：否

類型：boolean

dynamicWidth

如果設定為 true，CAPTCHA 拼圖會變更寬度，以與瀏覽器視窗寬度相容。

預設：false

必要：否

類型：boolean

skipTitle

如果設定為 true，CAPTCHA 拼圖不會顯示拼圖標題 解決拼圖。

預設：false

必要：否

類型：boolean

如何轉譯 CAPTCHA 拼圖

本節提供範例 `renderCaptcha` 實作。

您可以在 AWS WAF `renderCaptcha` 用戶端界面中使用您想要的 呼叫。呼叫會從 擷取 CAPTCHA 拼圖 AWS WAF、轉譯它，並將結果傳送至 AWS WAF 以進行驗證。當您進行呼叫時，您會提供

拼圖轉譯組態，以及在最終使用者完成拼圖時要執行的回呼。如需選項的詳細資訊，請參閱上一節：[CAPTCHA JavaScript API 規格](#)。

將此呼叫與智慧型威脅整合 APIs 的字符管理功能搭配使用。此呼叫會為您的用戶端提供權杖，以驗證 CAPTCHA 拼圖是否成功完成。使用智慧型威脅整合 APIs 來管理權杖，並在用戶端呼叫受 AWS WAF 保護套件或 Web ACLs 保護的端點時提供權杖。如需智慧型威脅 APIs 的詳細資訊，請參閱 [使用智慧型威脅 JavaScript API](#)。

實作範例

下列範例清單顯示標準 CAPTCHA 實作，包括在 <head> 區段中放置 AWS WAF 整合 URL。

此清單使用使用智慧型威脅整合 APIs `AwsWafIntegration.fetch` 包裝函式的成功回呼來設定 `renderCaptcha` 函數。如需此函數的詳細資訊，請參閱 [如何使用整合 `fetch` 包裝函式](#)。

```
<head>
  <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
  function showMyCaptcha() {
    var container = document.querySelector("#my-captcha-container");

    AwsWafCaptcha.renderCaptcha(container, {
      apiKey: "...API key goes here...",
      onSuccess: captchaExampleSuccessFunction,
      onError: captchaExampleErrorFunction,
      ...other configuration parameters as needed...
    });
  }

  function captchaExampleSuccessFunction(wafToken) {
    // Captcha completed. wafToken contains a valid WAF token. Store it for
    // use later or call AwsWafIntegration.fetch() to use it easily.
    // It will expire after a time, so calling AwsWafIntegration.getToken()
    // again is advised if the token is needed later on, outside of using the
    // fetch wrapper.

    // Use WAF token to access protected resources
    AwsWafIntegration.fetch("...WAF-protected URL...", {
      method: "POST",
      headers: {
        "Content-Type": "application/json",
```

```
        },
        body: "{ ... }" /* body content */
    });
}

function captchaExampleErrorFunction(error) {
    /* Do something with the error */
}
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

範例組態設定

下列範例清單顯示 `renderCaptcha` 具有寬度和標題選項非預設設定的。

```
AwsWafCaptcha.renderCaptcha(container, {
    apiKey: "...API key goes here...",
    onSuccess: captchaExampleSuccessFunction,
    onError: captchaExampleErrorFunction,
    dynamicWidth: true,
    skipTitle: true
});
```

如需組態選項的完整資訊，請參閱 [CAPTCHA JavaScript API 規格](#)。

從 處理 CAPTCHA 回應 AWS WAF

本節提供處理 CAPTCHA 回應的範例。

如果請求沒有具有有效 CAPTCHA 時間戳記的字符，則具有 CAPTCHA 動作的 AWS WAF 規則會終止對相符 Web 請求的評估。如果請求是 GET 文字/html 呼叫，則 CAPTCHA 動作會為用戶端提供具有 CAPTCHA 拼圖的間質。當您未整合 CAPTCHA JavaScript API 時，間質會執行拼圖，如果最終使用者成功解決，會自動重新提交請求。

當您整合 CAPTCHA JavaScript API 並自訂 CAPTCHA 處理時，您需要偵測終止的 CAPTCHA 回應、提供自訂 CAPTCHA，然後如果最終使用者成功解決拼圖，請重新提交用戶端的 Web 請求。

下列程式碼範例示範其做法：

 Note

AWS WAF CAPTCHA 動作回應的狀態碼為 HTTP 405，用於辨識此程式碼中的CAPTCHA回應。如果您的受保護端點使用 HTTP 405 狀態碼來通訊相同呼叫的任何其他類型回應，則此範例程式碼也會為這些回應轉譯 CAPTCHA 拼圖。

```
<!DOCTYPE html>
<html>
<head>
  <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
  <div id="my-captcha-box"></div>
  <div id="my-output-box"></div>

  <script type="text/javascript">
    async function loadData() {
      // Attempt to fetch a resource that's configured to trigger a CAPTCHA
      // action if the rule matches. The CAPTCHA response has status=HTTP 405.
      const result = await AwsWafIntegration.fetch("/protected-resource");

      // If the action was CAPTCHA, render the CAPTCHA and return

      // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
405
      // as an expected response status code, then this check won't be able to tell
the
      // difference between that and the CAPTCHA rule action response.

      if (result.status === 405) {
        const container = document.querySelector("#my-captcha-box");
        AwsWafCaptcha.renderCaptcha(container, {
          apiKey: "...API key goes here...",
          onSuccess() {
            // Try loading again, now that there is a valid CAPTCHA token
            loadData();
          },
        });
        return;
      }
    }
  </script>
</body>
</html>
```

```
const container = document.querySelector("#my-output-box");
const response = await result.text();
container.innerHTML = response;
}

window.addEventListener("load", () => {
  loadData();
});
</script>
</body>
</html>
```

管理 JS CAPTCHA API 的 API 金鑰

本節提供產生和刪除 API 金鑰的指示。

若要將 AWS WAF CAPTCHA 與 JavaScript API 整合到用戶端應用程式，您需要執行 CAPTCHA 拼圖之用戶端網域的 JavaScript API 整合標籤和加密的 API 金鑰。

JavaScript 的 CAPTCHA 應用程式整合 JavaScript 使用加密的 API 金鑰來驗證用戶端應用程式網域是否具有使用 AWS WAF CAPTCHA API 的許可。當您從 JavaScript 用戶端呼叫 CAPTCHA API 時，您會提供具有網域清單的 API 金鑰，其中包含目前用戶端的網域。您可以在單一加密金鑰中列出最多 5 個網域。

API 金鑰需求

您在 CAPTCHA 整合中使用的 API 金鑰必須包含套用至您使用金鑰之用戶端的網域。

- 如果您在用戶端的智慧型威脅整合 `window.awsWafCookieDomainList` 中指定，則 API 金鑰中至少有一個網域必須完全符合 中的其中一個字符網域，`window.awsWafCookieDomainList` 或者必須是其中一個字符網域的頂點網域。

例如，對於字符網域 `mySubdomain.myApex.com`，API 金鑰 `mySubdomain.myApex.com` 是完全相符的，API 金鑰 `myApex.com` 是頂點網域。任一金鑰都符合字符網域。

如需設定字符網域清單的相關資訊，請參閱 [提供用於字符的網域](#)。

- 否則，目前的網域必須包含在 API 金鑰中。目前的網域是您可以在瀏覽器地址列中看到的網域。

您使用的網域必須是 AWS WAF 根據受保護主機網域和為 Web ACL 設定的字符網域清單而接受的網域。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

如何選擇 API 金鑰的區域

AWS WAF 可以在可使用的任何區域中產生 CAPTCHA API AWS WAF 金鑰。

一般而言，您應該使用與保護套件或 Web ACL 相同的 CAPTCHA API 金鑰區域。不過，如果您預期全球受眾使用區域保護套件或 Web ACL，您可以取得範圍為 CloudFront 的 CAPTCHA JavaScript 整合標籤，以及範圍為 CloudFront 的 API 金鑰，並搭配區域保護套件或 Web ACL 使用。此方法可讓用戶端從最接近它們的區域載入 CAPTCHA 拼圖，從而減少延遲。

範圍限定在 CloudFront 以外區域的 CAPTCHA API 金鑰不支援跨多個區域使用。它們只能在其範圍範圍內的區域中使用。

為您的用戶端網域產生 API 金鑰

取得整合 URL，並透過主控台產生和擷取 API 金鑰。

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Application integration (應用程式整合)。
3. 在已啟用應用程式整合的窗格、保護套件或 Web ACLs 中，選取您要用於 API 金鑰的區域。您也可以在此 CAPTCHA 整合索引標籤的 API 金鑰窗格中選取區域。
4. 選擇 CAPTCHA 整合索引標籤。此索引標籤提供 CAPTCHA JavaScript 整合標籤，您可以在整合中使用，以及 API 金鑰清單。兩者都會範圍限定於選取的區域。
5. 在 API 金鑰窗格中，選擇產生金鑰。金鑰產生對話隨即出現。
6. 輸入您要包含在金鑰中的用戶端網域。您最多可以輸入 5 個。完成後，請選擇產生金鑰。界面會返回列出新金鑰的 CAPTCHA 整合索引標籤。

建立後，API 金鑰是不可變的。如果您需要變更金鑰，請產生新的金鑰並改用它。

7. (選用) 複製新產生的金鑰以用於您的整合。

您也可以為此工作使用 REST APIs 或其中一種特定語言 AWS SDKs。REST API 呼叫是 [CreateAPIKey](#) 和 [ListAPIKeys](#)。

刪除 API 金鑰

若要刪除 API 金鑰，您必須使用 REST API 或其中一種語言 AWS SDKs。REST API 呼叫是 [DeleteAPIKey](#)。您無法使用 主控台刪除金鑰。

刪除金鑰後，最多可能需要 24 小時 AWS WAF 才能禁止在所有區域中使用金鑰。

AWS WAF 行動應用程式整合

本節介紹使用 AWS WAF 行動 SDKs 實作適用於 Android 和 iOS 行動和電視應用程式的 AWS WAF 智慧型威脅整合 SDKs 的主題。對於電視應用程式，SDKs 與主要智慧型電視平台相容，包括 Android TV 和 Apple TV。

- 對於 Android 行動和電視應用程式，SDKs 適用於 Android API 第 23 版 (Android 第 6 版) 和更新版本。如需 Android 版本的資訊，請參閱 [SDK 平台版本備註](#)。
- 對於 iOS 行動應用程式，SDKs 適用於 iOS 版本 13 和更新版本。如需 iOS 版本的資訊，請參閱 [iOS & iPadOS 版本備註](#)。
- 對於 Apple TV 應用程式，SDKs 適用於 tvOS 第 14 版或更新版本。如需 tvOS 版本的資訊，請參閱 [tvOS 版本備註](#)。

透過行動 AWS WAF SDK，您可以管理權杖授權，並將權杖包含在傳送至受保護資源的請求中。透過使用 SDKs，您可以確保用戶端進行的這些遠端程序呼叫包含有效的字符。此外，當您的應用程式頁面上有此整合時，您可以在保護套件或 Web ACL 中實作緩解規則，例如封鎖不包含有效字符的請求。

如需存取行動 SDKs，請聯絡 [Contact AWS](#) 的支援。

Note

AWS WAF 行動 SDKs 不適用於 CAPTCHA 自訂。

使用 SDK 的基本方法是使用組態物件建立權杖提供者，然後使用權杖提供者從中擷取權杖 AWS WAF。根據預設，權杖提供者會在對受保護資源的 Web 請求中包含擷取的權杖。

以下是 SDK 實作的部分清單，其中顯示主要元件。如需更詳細的範例，請參閱 [AWS WAF 行動 SDK 的程式碼範例](#)。

iOS

```
let url: URL = URL(string: "protection pack or web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
"Domain name")
let tokenProvider = WAFTokenProvider(configuration)
let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("protection pack or web ACL integration URL");
String domainName = "Domain name";
WAFConfiguration configuration =
WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
configuration);
WAFToken token = tokenProvider.getToken();
```

安裝 AWS WAF 行動 SDK

本節提供安裝 AWS WAF 行動 SDK 的說明。

如需存取行動 SDKs，請聯絡 [Contact AWS](#) 的支援。

先在測試環境中實作行動 SDK，然後在生產環境中實作。

安裝 AWS WAF 行動 SDK

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇 Application integration (應用程式整合)。
3. 在智慧型威脅整合索引標籤中，執行下列動作：
 - a. 在啟用應用程式整合的窗格保護套件或 Web ACLs 中，找到您要整合的保護套件或 Web ACL。複製並儲存保護套件或 Web ACL 整合 URL，以用於您的實作。您也可以透過 API 呼叫取得此 URLGetWebACL。
 - b. 選擇行動裝置類型和版本，然後選擇下載。您可以選擇任何您喜歡的版本，但我們建議您使用最新版本。會將您裝置的 zip 檔案 AWS WAF 下載到您的標準下載位置。
4. 在您的應用程式開發環境中，將檔案解壓縮到您選擇的工作位置。在 zip 檔案的最上層目錄中，找到並開啟 README。遵循 README 檔案中的指示，安裝 AWS WAF 行動 SDK 以用於您的行動應用程式程式碼。
5. 根據以下章節中的指引來設定您的應用程式。

AWS WAF 行動 SDK 規格

本節列出 AWS WAF 行動 SDK 最新可用版本的 SDK 物件、操作和組態設定。如需字符提供者和操作如何針對各種組態設定組合運作的詳細資訊，請參閱 [AWS WAF 行動 SDK 的運作方式](#)。

WAFToken

保留 AWS WAF 權杖。

getValue()

擷取 的String表示法WAFToken。

WAFTokenProvider

管理行動應用程式中的字符。使用 WAFConfiguration 物件實作此項目。

getToken()

如果已啟用背景重新整理，這會傳回快取的字符。如果背景重新整理已停用，這會導致同步，封鎖呼叫 AWS WAF 以擷取新的字符。

loadTokenIntoProvider(WAFToken)

將指定的權杖載入 WAFTokenProvider，取代提供者管理的任何權杖。權杖提供者會取得新權杖的所有權，並在未來處理重新整理權杖。如果在 `setTokenCookie` 啟用，此操作也會更新 Cookie 存放區中的字符 WAFConfiguration。

onTokenReady(WAFTokenResultCallback)

指示權杖提供者重新整理權杖，並在作用中權杖就緒時叫用提供的回呼。當字符快取並就緒時，字符提供者會在背景執行緒中叫用您的回呼。當您的應用程式第一次載入時，以及它回到作用中狀態時，請呼叫此選項。如需返回作用中狀態的詳細資訊，請參閱 [the section called “在應用程式閒置後擷取字符”](#)。

對於 Android 或 iOS 應用程式，您可以將 WAFTokenResultCallback 設定為您希望權杖提供者在請求權杖就緒時叫用的操作。您的 實作WAFTokenResultCallback必須採用參數 WAFToken、SdkError。對於 iOS 應用程式，您可以交替建立內嵌函數。

storeTokenInCookieStorage(WAFToken)

指示 將指定的 AWS WAF 字符WAFTokenProvider存放到開發套件的 Cookie 管理員。根據預設，字符只會在第一次取得和重新整理時新增至 Cookie 存放區。如果應用程式因任何原因清除共用的 Cookie 存放區，軟體開發套件不會自動新增 AWS WAF 字符，直到下一次重新整理為止。

WAFConfiguration

保留實作的組態 `WAFTokenProvider`。當您實作此項目時，您會提供保護套件或 Web ACL 的整合 URL、要在字符中使用的網域名稱，以及您希望字符提供者使用的任何非預設設定。

下列清單指定您可以在 WAFConfiguration 物件中管理的組態設定。

`applicationIntegrationUrl`

應用程式整合 URL。從 AWS WAF 主控台或透過 `getWebACL` API 呼叫取得。

必要：是

類型：應用程式特定的 URL。對於 iOS，請參閱 [iOS URL](#)。對於 Android，請參閱 [java.net URL](#)。

`backgroundRefreshEnabled`

指出您是否希望權杖提供者在背景重新整理權杖。如果您設定此項目，權杖提供者會根據管理自動權杖重新整理活動的組態設定，在背景重新整理權杖。

必要：否

類型：Boolean

預設值：TRUE

`domainName`

要在字符中使用的網域，用於字符獲取和 Cookie 儲存。例如 `example.com` 或 `aws.amazon.com`。這通常是與保護套件或 Web ACL 相關聯的資源的主機網域，您將在其中傳送 Web 請求。對於 ACFP 受管規則群組 `AWSManagedRulesACFPRuleSet`，這通常是與您在規則群組組態中提供的帳戶建立路徑中的網域相符的單一網域。對於 ATP 受管規則群組 `AWSManagedRulesATPRuleSet`，這通常是與您在規則群組組態中提供的登入路徑中的網域相符的單一網域。

不允許公有尾碼。例如，您無法使用 `gov.au` 或 `co.uk` 做為字符網域。

網域必須是 AWS WAF 根據受保護主機網域和保護套件或 Web ACL 字符網域清單接受的網域。如需詳細資訊，請參閱 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

必要：是

類型：String

maxErrorTokenRefreshDelayMsec

嘗試失敗後重複權杖重新整理之前等待的時間上限，以毫秒為單位。對於失敗嘗試的每個自動重試，它會新增指數退避，直到指定的輸入延遲時間為止。此值會在字符擷取失敗並重試maxRetryCount時間後使用。

必要：否

類型：Integer

預設值：5000(5 秒)

允許的最小值：1(1 毫秒)

允許的值上限：30000(30 秒)

maxRetryCount

請求權杖時，以指數退避執行的重試次數上限。

必要：否

類型：Integer

預設值：Infinity

允許的最小值：0

允許的最大值：100

setTokenCookie

指出您是否希望開發套件的 Cookie 管理員將字符 Cookie 新增至請求和其他區域。

使用 TRUE值：

- Cookie 管理員會將權杖 Cookie 新增至路徑位於 中指定路徑下的所有請求tokenCookiePath。
- 除了將權杖載入權杖提供者之外，WAFTokenProvider操作還會loadTokenIntoProvider()更新 Cookie 存放區中的權杖。

必要：否

類型：Boolean

預設值：TRUE

tokenCookiePath

當 setTokenCookie 為 TRUE 時使用。指出您希望開發套件的 Cookie 管理員新增字符 Cookie 的頂層路徑。管理員會將權杖 Cookie 新增至您傳送至此路徑和所有子路徑的所有請求。

例如，如果您將此設定為 /web/login，則管理員會包含傳送至 的所有項目及其/web/login任何子路徑的字符 Cookie，例如 /web/login/help。它不包括傳送到其他路徑的請求字符，例如 /、/web或 /web/order。

必要：否

類型：String

預設值：/

tokenRefreshDelaySec

用於背景重新整理。背景權杖重新整理之間的秒數上限。

必要：否

類型：Integer

預設值：88

允許的最小值：88

允許的最大值：300(5 分鐘)

AWS WAF 行動 SDK 錯誤

本節列出目前 AWS WAF 行動 SDK 版本的可能錯誤。

SdkError

無法擷取字符時傳回的錯誤類型。Android 和 iOS 開發套件具有相同的錯誤類型。

AWS WAF 行動開發套件具有下列錯誤類型：

invalidChallenge

當字符伺服器傳回無效的挑戰資料，或攻擊者變更回應 Blob 時，會傳回此錯誤。

errorInvokingGetChallengeEndpoint

當字符伺服器傳送不成功的回應碼回用戶端或發生網路錯誤時，會傳回此錯誤。

invalidVerifyChallengeResponse

當aws-waf-token從 AWS WAF 伺服器的驗證回應擷取時發生錯誤，或伺服器回應遭到竄改時，就會傳回此錯誤。

errorInvokingVerifyEndpoint

驗證已解決的挑戰時，用戶端收到來自 AWS WAF 伺服器的錯誤回應或網路錯誤時，會傳回此錯誤。

internalError

此錯誤會在 SDK 本身可能發生的所有其他錯誤上傳回。

socketTimeoutException

在權杖擷取期間遇到網路錯誤時，通常會傳回此錯誤。

此錯誤可能由下列原因造成：

- 低網路頻寬：確認您的網路連線設定
- 變動的應用程式整合 URL：確認整合 URL 未從 AWS WAF 主控台上顯示的內容修改

AWS WAF 行動 SDK 的運作方式

本節說明 AWS WAF 行動 SDK 類別、屬性和操作如何一起運作。

行動SDKs為您提供可設定的權杖提供者，可用於權杖擷取和使用。字符提供者會驗證您允許的請求是否來自合法客戶。當您將請求傳送至 AWS 您保護的資源時 AWS WAF，您會在 Cookie 中包含權杖，以驗證請求。您可以手動處理權杖 Cookie，或讓權杖提供者為您處理權杖 Cookie。

本節涵蓋行動 SDK 中包含的類別、屬性和方法之間的互動。如需 SDK 規格，請參閱 [AWS WAF 行動 SDK 規格](#)。

權杖擷取和快取

當您在行動應用程式中建立權杖提供者執行個體時，您可以設定其管理權杖和權杖擷取的方式。您的主要選擇是如何維護有效的未過期字符，以便在應用程式的 Web 請求中使用：

- 已啟用背景重新整理 – 這是預設值。權杖提供者會在背景自動重新整理權杖並快取權杖。啟用背景重新整理後，當您呼叫 `getToken()`，操作會擷取快取的字符。

權杖提供者會以可設定的間隔執行權杖重新整理，以便在應用程式處於作用中狀態時，快取中一律可使用未過期的權杖。當您的應用程式處於非作用中狀態時，背景重新整理會暫停。如需詳細資訊，請參閱 [在應用程式閒置後擷取字符](#)。

- 背景重新整理已停用 – 您可以停用背景字符重新整理，然後僅隨需擷取字符。隨需擷取的權杖不會快取，您可以視需要擷取多個權杖。每個字符與您擷取的任何其他字符無關，每個字符都有自己的時間戳記，用於計算過期。

停用背景重新整理時，您有下列權杖擷取選項：

- **`getToken()`** – 當您呼叫 `getToken()` 時停用背景重新整理，呼叫會從中同步擷取新的字符 AWS WAF。如果您在主執行緒上調用應用程式回應能力，這可能會封鎖呼叫。
- **`onTokenReady(WAFTokenResultCallback)`** – 此呼叫會非同步擷取新的權杖，然後在權杖就緒時，在背景執行緒中調用提供的結果回呼。

權杖提供者如何重試失敗的權杖擷取

當擷取失敗時，字符提供者會自動重試字符擷取。一開始會使用指數退避執行重試，起始重試等待時間為 100 毫秒。如需指數重試的相關資訊，請參閱 [錯誤重試和指數退避 AWS](#)。

當重試次數達到設定的 `maxRetryCount`，字符提供者會停止嘗試或切換為每 `maxErrorTokenRefreshDelayMsec` 毫秒嘗試一次，取決於字符擷取的類型：

- **`onTokenReady()`** – 權杖提供者會在嘗試之間切換到等待 `maxErrorTokenRefreshDelayMsec` 毫秒，並繼續嘗試擷取權杖。
- 背景重新整理 – 權杖提供者會在嘗試之間切換到等待 `maxErrorTokenRefreshDelayMsec` 毫秒，並繼續嘗試擷取權杖。
- 停用背景重新整理時的隨需 **`getToken()`** 呼叫 – 權杖提供者會停止嘗試擷取權杖，並傳回先前的權杖值，如果沒有先前的權杖，則會傳回 `null` 值。

字符擷取重試案例

當字符提供者嘗試擷取字符時，根據字符擷取在字符擷取流程中失敗的位置，可能會導致自動重試。本節列出您可能會看到自動重試的可能位置。

- 透過 `/inputs` 或 `/verify` 取得或驗證 AWS WAF 挑戰：

- 當請求取得和驗證 AWS WAF 挑戰已提出且失敗時，可能會導致自動重試。
- 您可能會看到自動重試與 `socketTimeoutException` 錯誤一起發生。這可能有多個原因，包括：
 - 低網路頻寬：確認您的網路連線設定
 - 變動的應用程式整合 URL：確認整合 URL 未從 AWS WAF 主控台上顯示的內容修改
- 可使用 `maxRetryCount()` 函數設定自動重試計數
- 重新整理權杖：
 - 透過權杖處理常式提出重新整理權杖的請求時，可能會導致自動重試。
 - 此處的自動重試計數可透過 `maxRetryCount()` 函數設定。

設定 可進行沒有自動重試的組態 `maxRetryCount(0)`。

字符抑制時間和背景重新整理

您在 Web ACL 中設定的字符豁免時間與您在 AWS WAF 行動 SDK 中設定的字符重新整理間隔無關。當您啟用背景重新整理時，軟體開發套件會在您使用 指定的間隔重新整理字符 `tokenRefreshDelaySec()`。這可能會導致多個有效的字符同時存在，取決於您設定的抗擾性時間。

若要防止多個有效字符，您可以停用背景重新整理，並使用 `getToken()` 函數來管理行動應用程式中的字符生命週期。

在應用程式閒置後擷取字符

只有在您的應用程式視為應用程式類型的作用中時，才會執行背景重新整理：

- iOS – 背景重新整理會在應用程式位於前景時執行。
- Android – 背景重新整理會在應用程式未關閉時執行，無論是在前景或背景中。

如果您的應用程式保持在不支援背景重新整理的任何狀態超過設定的 `tokenRefreshDelaySec` 秒數，字符提供者會暫停背景重新整理。例如，對於 iOS 應用程式，如果 `tokenRefreshDelaySec` 是 300 且應用程式關閉或進入背景超過 300 秒，字符提供者會停止重新整理字符。當應用程式返回作用中狀態時，字符提供者會自動重新啟動背景重新整理。

當您的應用程式回到作用中狀態時，請呼叫 `onTokenReady()`，以便在權杖提供者擷取並快取新的權杖時收到通知。不要只呼叫 `getToken()`，因為快取可能尚未包含目前有效的字符。

應用程式整合 URL

AWS WAF 行動 SDK 應用程式整合 URL 指向您已啟用的應用程式整合的 Web ACL。此 URL 會將請求路由至正確的後端伺服器，並將其與您的客戶建立關聯。它不做為硬式安全控制，因此公開整合 URL 不會帶來安全風險。

您可以在技術上修改提供的整合 URL，但仍取得權杖。不過，我們不建議這麼做，因為您可能會失去對挑戰求解率的可見性，或遇到字符擷取失敗並 `socketTimeoutException` 發生錯誤。

相依性

每個可下載 AWS WAF 的行動 SDK 都包含一個 README 檔案，列出其特定版本 SDK 的相依性。如需行動 SDK 版本的相依性，請參閱 README。

Obfuscation/ProGuard（僅限 Android 開發套件）

如果您使用像 ProGuard 這樣的混淆或縮小產品，您可能需要排除某些命名空間，以確保行動 SDK 正常運作。檢查行動開發套件版本的 README，以尋找命名空間和排除規則的清單。

AWS WAF 行動 SDK 的程式碼範例

本節提供使用行動 SDK 的程式碼範例。

初始化權杖提供者並取得權杖

您可以使用組態物件啟動權杖提供者執行個體。然後，您可以使用可用的操作擷取字符。以下顯示必要程式碼的基本元件。

iOS

```
let url: URL = URL(string: "protection pack or web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
    "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
    if let token = token {
        //token available
    }

    if let error = error {
        //error occurred after exhausting all retries
    }
}
```

```
}  
}  
  
//getToken()  
let token = tokenProvider.getToken()
```

Android

Java 範例：

```
String applicationIntegrationURL = "protection pack or web ACL integration URL";  
//Or  
URL applicationIntegrationURL = new URL("protection pack or web ACL integration URL");  
  
String domainName = "Domain name";  
  
WAFConfiguration configuration =  
    WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(  
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,  
    configuration);  
  
// implement a token result callback  
WAFTokenResultCallback callback = (wafToken, error) -> {  
    if (wafToken != null) {  
        // token available  
    } else {  
        // error occurred in token refresh  
    }  
};  
  
// Add this callback to application creation or activity creation where token will  
    be used  
tokenProvider.onTokenReady(callback);  
  
// Once you have token in token result callback  
// if background refresh is enabled you can call getToken() from same tokenprovider  
    object  
// if background refresh is disabled you can directly call getToken()(blocking call)  
    for new token  
WAFToken token = tokenProvider.getToken();
```

Kotlin 範例：

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "protection pack or web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
    // Initialize the tokenprovider instance
    val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
    wafConfiguration =
        WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
            .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
    wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

    // getToken from tokenprovider object
    println("WAF: " + wafTokenProvider.token.value)

    // implement callback for where token will be used
    wafTokenProvider.onTokenReady {
        wafToken, sdkError ->
        run {
            println("WAF Token:" + wafToken.value)
        }
    }
}
```

允許 SDK 在 HTTP 請求中提供字符 Cookie

如果 `setTokenCookie` 是 `TRUE`，則權杖提供者會在 Web 請求中，將權杖 Cookie 包含到指定路徑下的所有位置 `tokenCookiePath`。根據預設，`setTokenCookie` 為 `TRUE`，而 `tokenCookiePath` 為 `/`。

您可以透過指定字符 Cookie 路徑來縮小包含字符 Cookie 的請求範圍，例如 `/web/login`。如果您這樣做，請檢查您的 AWS WAF 規則是否在您傳送到其他路徑的請求中檢查字符。使用 `AWSMangedRulesACFPRuleSet` 規則群組時，您可以設定帳戶註冊和建立路徑，而規則群組會檢查傳送至這些路徑之請求中的字符。如需詳細資訊，請參閱 [將 ACFP 受管規則群組新增至 Web ACL](#)。同樣地，當您使用 `AWSMangedRulesATPRuleSet` 規則群組時，您可以設定登入路徑，而規則群組會

檢查傳送至該路徑之請求中的字符。如需詳細資訊，請參閱[將 ATP 受管規則群組新增至您的保護套件或 Web ACL](#)。

iOS

當 `setTokenCookie` 為 `TRUE`，字符提供者會將 AWS WAF 字符存放在 `HTTPCookieStorage.shared` 並在您於 `CookieWAFConfiguration` 中指定的網域請求中自動包含 `CookieWAFConfiguration`。

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error in
}.resume()
```

Android

當 `setTokenCookie` 為 `TRUE`，字符提供者會將 AWS WAF 字符存放在整個共用應用程式的 `CookieHandler` 執行個體中。權杖提供者會自動將 `Cookie` 包含在對您在 `WAFConfiguration` 中指定之網域的請求中 `WAFConfiguration`。

Java 範例：

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Kotlin 範例：

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

如果您已初始化 `CookieHandler` 預設執行個體，字符提供者將使用它來管理 `Cookie`。如果沒有，字符提供者將使用 AWS WAF 字符初始化新的 `CookieManager` 執行個體，`CookiePolicy.ACCEPT_ORIGINAL_SERVER` 然後將此新執行個體設定為 `CookieHandler` 中的預設執行個體 `CookieHandler`。

下列程式碼顯示 SDK 如何在您的應用程式中無法使用 `Cookie` 管理員和 `Cookie` 處理常式時初始化 `Cookie` 管理員和 `Cookie` 處理常式。

Java 範例：

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
    // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
    cookieManager = new CookieManager();
    CookieHandler.setDefault(cookieManager);
}
```

Kotlin 範例：

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
    // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
    cookieManager = CookieManager()
    CookieHandler.setDefault(cookieManager)
}
```

在 HTTP 請求中手動提供字符 Cookie

如果您將 `setTokenCookie` 設定為 `FALSE`，則需要在對受保護端點的請求中，以 Cookie HTTP 請求標頭的形式手動提供字符 Cookie。下列程式碼示範如何執行此操作。

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
    "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Java 範例：

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Kotlin 範例：

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHA 和 Challenge 中的 AWS WAF

本節說明如何 Challenge 使用 CAPTCHA 和 AWS WAF。

您可以設定 AWS WAF 規則，針對符合規則檢查條件的 Web 請求執行 CAPTCHA 或 Challenge 動作。您也可以編寫 JavaScript 用戶端應用程式，以在本機執行 CAPTCHA 拼圖和瀏覽器挑戰。

CAPTCHA 拼圖和無提示挑戰只能在瀏覽器存取 HTTPS 端點時執行。瀏覽器用戶端必須在安全的內容中執行，才能取得字符。

- CAPTCHA – 要求最終使用者解決 CAPTCHA 拼圖，以證明人類正在傳送請求。CAPTCHA 拼圖旨在讓人類能夠輕鬆快速地順利完成，讓電腦能夠順利完成，或隨機地完成任何有意義的成功率。

在保護套件或 Web ACL 規則中，當 Block 動作停止太多合法請求時，通常會使用 CAPTCHA，但讓所有流量通過會導致無法接受的高度不需要的請求，例如來自機器人的請求。如需規則動作行為的資訊，請參閱 [和 AWS WAF CAPTCHA Challenge 規則動作的運作方式](#)。

您也可以用戶端應用程式整合 APIs 中編寫 CAPTCHA 拼圖實作的程式。執行此操作時，您可以自訂用戶端應用程式中拼圖的行為和位置。如需詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。

- Challenge – 執行靜音挑戰，要求用戶端工作階段驗證其是否為瀏覽器，而非機器人。驗證會在背景執行，而不涉及最終使用者。這是驗證您懷疑是無效的用戶端的好選項，而不會對 CAPTCHA 拼圖的最終使用者體驗產生負面影響。如需規則動作行為的資訊，請參閱 [和 AWS WAF CAPTCHA Challenge 規則動作的運作方式](#)。

Challenge 規則動作類似於用戶端智慧型威脅整合 APIs 執行的挑戰，如中所述 [中的用戶端應用程式整合 AWS WAF](#)。

Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

如需所有規則動作選項的說明，請參閱 [在 中使用規則動作 AWS WAF](#)。

主題

- [AWS WAF CAPTCHA 拼圖](#)
- [和 AWS WAF CAPTCHA Challenge 規則動作的運作方式](#)
- [使用 CAPTCHA 和 Challenge 動作的最佳實務](#)

AWS WAF CAPTCHA 拼圖

本節說明 AWS WAF CAPTCHA 拼圖的特徵和功能。

AWS WAF 提供標準 CAPTCHA 功能，可挑戰使用者確認他們是人類。CAPTCHA 代表完全自動化公有 Turing 測試，以告知電腦和人類。CAPTCHA 謎題旨在驗證人類是否正在傳送請求，並防止 Web 抓取、憑證填充和垃圾郵件等活動。CAPTCHA 拼圖無法除去所有不需要的請求。許多謎題已使用機器學習和人工智慧解決。為了避免 CAPTCHA，某些組織使用人工介入來補充自動化技術。儘管如此，CAPTCHA 仍然是防止較不複雜的機器人流量，並增加大規模操作所需的資源的有用工具。

AWS WAF 會隨機產生其 CAPTCHA 謎題並輪換它們，以確保使用者面臨獨特的挑戰。會 AWS WAF 定期新增新的謎題類型和樣式，以維持對自動化技術的有效。除了拼圖之外，AWS WAF CAPTCHA 指令碼還會收集有關用戶端的資料，以確保任務是由人類完成，並防止重播攻擊。

每個 CAPTCHA 拼圖都包含一組標準控制項，供最終使用者請求新的拼圖、切換音訊和視覺拼圖、存取其他指示，以及提交拼圖解決方案。所有拼圖都支援螢幕閱讀器、鍵盤控制和對比顏色。

AWS WAF CAPTCHA 謎題符合 Web Content Accessibility Guidelines (WCAG) 的要求。如需詳細資訊，請參閱 [全球資訊網協會 \(W3C\) 網站上的 Web 內容可存取性指南 \(WCAG\) 概觀](#)。

主題

- [CAPTCHA 拼圖語言支援](#)
- [CAPTCHA 拼圖範例](#)

CAPTCHA 拼圖語言支援

本節列出 AWS WAF CAPTCHA 拼圖支援的語言。

CAPTCHA 謎題以用戶端瀏覽器語言或不支援瀏覽器語言的英文撰寫說明開頭。拼圖透過下拉式選單提供替代語言選項。

使用者可以透過選取頁面底部的耳機圖示來切換到音訊指示。拼圖的音訊版本提供有關使用者應該在文字方塊中輸入的文字的口語說明，由背景雜訊覆蓋。

下表列出您可以在 CAPTCHA 拼圖中針對書面指示選擇的語言，以及每個選擇對音訊的支援。

AWS WAF CAPTCHA 拼圖支援的語言

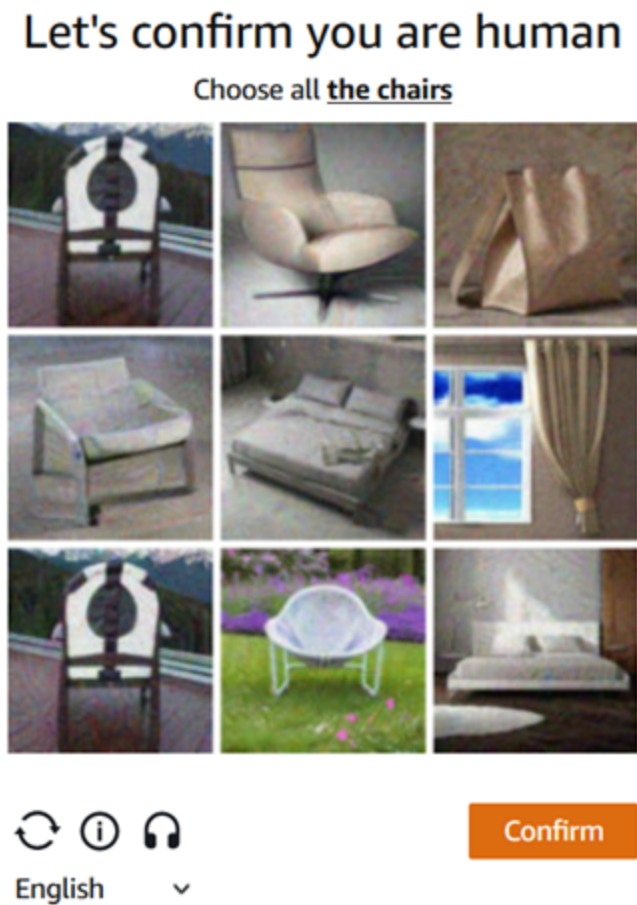
支援書面指示	地區設定程式碼	音訊指示支援
Arabic	ar-SA	Arabic
簡體中文	zh-CN	英文音訊
荷蘭文	nl-NL	荷蘭文
英文	zh-TW	英文
法文	fr-FR	法文
德文	de-DE	德文
義大利文	it-IT	義大利文
日文	ja-JP	英文音訊
巴西葡萄牙文	pt-BR	巴西葡萄牙文
西班牙文	es-ES	西班牙文

支援書面指示	地區設定程式碼	音訊指示支援
Turkish	tr-TR	Turkish

CAPTCHA 拼圖範例

典型的視覺效果 CAPTCHA 拼圖需要互動，以顯示使用者可以理解與一或多個影像互動。

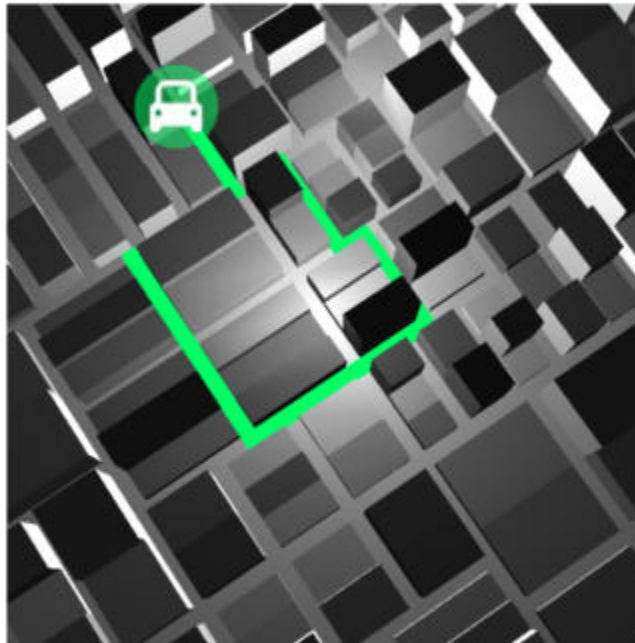
下列螢幕擷取畫面顯示圖片網格拼圖的範例。此拼圖要求您選取網格中包含特定類型物件的所有圖片。



下列螢幕擷取畫面顯示範例拼圖，要求您在繪圖中識別汽車路徑的端點。

Solve the puzzle

Place a dot at the end of the car's path



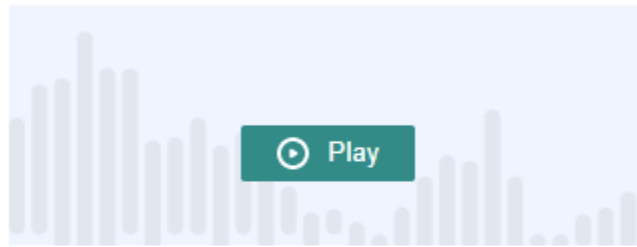
Submit

音訊拼圖提供背景噪音，與使用者應該在文字方塊中輸入的文字相關語音指示重疊。

下列螢幕擷取畫面顯示音訊拼圖選項的顯示。

Solve the puzzle

Click play to listen to instructions



Keyboard audio toggle: alt + space

Enter your response

Solve by listening to the recording and typing your answer into the text box.





和 AWS WAF CAPTCHA Challenge 規則動作的運作方式

本節說明 CAPTCHA 和 Challenge 的運作方式。

AWS WAF CAPTCHA 和 Challenge 是標準規則動作，因此相對容易實作。若要使用其中一項，請為規則建立檢查條件，以識別您要檢查的請求，然後指定兩個規則動作之一。如需規則動作選項的一般資訊，請參閱 [在 中使用規則動作 AWS WAF](#)。

除了從伺服器端實作無聲挑戰和 CAPTCHA 拼圖之外，您還可以在 JavaScript 和 iOS 和 Android 用戶端應用程式中整合無聲挑戰，並在 JavaScript 用戶端中呈現 CAPTCHA 拼圖。這些整合可讓您為最終使用者提供更好的效能和 CAPTCHA 拼圖體驗，而且他們可以降低使用規則動作和智慧型威脅緩解規則群組的相關成本。如需關於這些選項的詳細資訊，請參閱 [中的用戶端應用程式整合 AWS WAF](#)。如需定價資訊，請參閱 [AWS WAF 定價](#)。

主題

- [CAPTCHA 和 Challenge 動作行為](#)
- [CAPTCHA 日誌和指標中的 和 Challenge 動作](#)

CAPTCHA 和 Challenge 動作行為

本節說明 CAPTCHA 和 Challenge 動作的功能。

當 Web 請求符合具有 CAPTCHA 或 Challenge 動作之規則的檢查條件時，會根據其權杖和豁免時間組態的狀態，AWS WAF 決定如何處理請求。AWS WAF 也會考慮請求是否可以處理 CAPTCHA 拼圖或挑戰指令碼間質。指令碼設計成以 HTML 內容處理，而且只能由預期使用 HTML 內容的用戶端正確處理。

Note

當您在其中一個規則中使用 CAPTCHA 或 Challenge 規則動作，或做為規則群組中的規則動作覆寫時，需支付額外費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。

動作如何處理 Web 請求

AWS WAF 會將 CAPTCHA 或 Challenge 動作套用至 Web 請求，如下所示：

- 有效的字符 – AWS WAF 處理類似 Count 動作。AWS WAF 會套用您為規則動作設定的任何標籤和請求自訂，然後繼續使用保護套件或 Web ACL 中的其餘規則來評估請求。
- 權杖遺失、無效或過期 – AWS WAF 停止請求的保護套件或 Web ACL 評估，並封鎖它前往其預期目的地。

AWS WAF 會根據規則動作類型，產生傳回用戶端的回應：

- Challenge – AWS WAF 在回應中包含下列項目：
 - 具有 challenge 值的標頭 x-amzn-waf-action。

Note

對於在用戶端瀏覽器中執行的 Javascript 應用程式，此標頭僅適用於應用程式的網域。標頭不適用於跨網域擷取。如需詳細資訊，請參閱以下章節。

- HTTP 狀態碼 202 Request Accepted。
- 如果請求包含具有 text/html 值的 Accept 標頭，回應將包含 JavaScript 插入式頁面和挑戰指令碼。
- CAPTCHA – 在回應中 AWS WAF 包含下列項目：
 - 具有 captcha 值的標頭 x-amzn-waf-action。

Note

對於在用戶端瀏覽器中執行的 Javascript 應用程式，此標頭僅適用於應用程式的網域。標頭不適用於跨網域擷取。如需詳細資訊，請參閱以下章節。

- HTTP 狀態碼 405 Method Not Allowed。
- 如果請求包含值為 `Accept: text/html` 的 `Accept` 標頭，回應會包含 JavaScript 頁面與 CAPTCHA 指令碼的間質。

若要在保護套件或 Web ACL 或規則層級設定權杖過期的時間，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。

在用戶端瀏覽器中執行的 JavaScript 應用程式無法使用標頭

當使用 CAPTCHA 或挑戰 AWS WAF 回應回應用戶端請求時，它不包含跨來源資源共用 (CORS) 標頭。CORS 標頭是一組存取控制標頭，可告知用戶端 Web 瀏覽器哪些網域、HTTP 方法和 HTTP 標頭可供 JavaScript 應用程式使用。如果沒有 CORS 標頭，在用戶端瀏覽器中執行的 JavaScript 應用程式不會獲得 HTTP 標頭的存取權，因此無法讀取 CAPTCHA 和 Challenge 回應中提供的 `x-amzn-waf-action` 標頭。

挑戰和 CAPTCHA 中介裝置的作用

當挑戰間質執行時，在用戶端成功回應之後，如果它還沒有權杖，則間質會為其初始化一個權杖。然後，它會使用挑戰求解時間戳記來更新權杖。

當 CAPTCHA 間質執行時，如果用戶端還沒有權杖，CAPTCHA 間質會先叫用挑戰指令碼來挑戰瀏覽器並初始化權杖。然後，間質執行其 CAPTCHA 拼圖。當最終使用者成功完成拼圖時，間質會使用 CAPTCHA 求解時間戳記更新字符。

在這兩種情況下，在用戶端成功回應且指令碼更新字符之後，指令碼會使用更新的字符重新提交原始 Web 請求。

您可以設定 AWS WAF 如何處理字符。如需相關資訊，請參閱 [用於 AWS WAF 智慧型威脅緩解的字符](#)。

CAPTCHA 日誌和指標中的 和 Challenge 動作

本節說明如何 AWS WAF 處理 和 Challenge 動作的記錄 CAPTCHA 和指標。

CAPTCHA 和 Challenge 動作可以是非終止的，例如 Count，或是終止的，例如 Block。結果取決於請求是否具有動作類型的有效字符，以及未過期的時間戳記。

- 有效字符 – 當動作找到有效的字符且未封鎖請求時，會 AWS WAF 擷取指標和日誌，如下所示：
 - 增加 CaptchaRequests 和 RequestsWithValidCaptchaToken 或 ChallengeRequests 和 RequestsWithValidChallengeToken。
 - 使用 CAPTCHA 或 的動作將相符項目記錄為 nonTerminatingMatchingRules 項目 Challenge。下列清單顯示此類型 與 CAPTCHA 動作相符的日誌區段。

```
"nonTerminatingMatchingRules": [  
  {  
    "ruleId": "captcha-rule",  
    "action": "CAPTCHA",  
    "ruleMatchDetails": [],  
    "captchaResponse": {  
      "responseCode": 0,  
      "solveTimestamp": 1632420429  
    }  
  }  
]
```

- 缺少、無效或過期的字符 – 當動作因遺失或無效的字符而封鎖請求時，會 AWS WAF 擷取指標和日誌，如下所示：
 - 增加 CaptchaRequests 或 的指標 ChallengeRequests。
 - 將相符項目記錄為具有 HTTP 405 狀態碼 CaptchaResponse 的項目，或記錄為具有 HTTP 202 狀態碼 ChallengeResponse 的項目。日誌指出請求是否缺少字符或時間戳記已過期。日誌也會指出是 AWS WAF 將 CAPTCHA 問質頁面傳送到用戶端，還是將無訊息挑戰傳送到用戶端瀏覽器。下列清單顯示此類型 與 CAPTCHA 動作相符的日誌區段。

```
"terminatingRuleId": "captcha-rule",  
"terminatingRuleType": "REGULAR",  
"action": "CAPTCHA",  
"terminatingRuleMatchDetails": [],  
...  
"responseCodeSent": 405,  
...  
"captchaResponse": {  
  "responseCode": 405,  
  "solveTimestamp": 0,  
  "failureReason": "TOKEN_MISSING"
```

```
}
```

如需 AWS WAF 日誌的資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

如需 AWS WAF 指標的相關資訊，請參閱 [AWS WAF 指標和維度](#)。

如需規則動作選項的一般資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

沒有字符的請求似乎在日誌和指標中顯示兩次

根據本節所述的 [CAPTCHA 和 Challenge 動作行為](#) 和記錄和指標，沒有字符的請求通常會在日誌和指標中表示兩次。這是因為用戶端實際上傳送了兩次預期的請求。

- 第一個沒有字符的請求會收到上述記錄和指標處理，以處理遺漏、無效或過期的字符。CAPTCHA 或 Challenge 動作會終止此第一個請求，然後使用無提示挑戰或 CAPTCHA 拼圖來回應用戶端。
- 用戶端會評估挑戰或拼圖，如果用戶端瀏覽器或最終使用者成功回應，會使用新取得的字符再次傳送請求。第二個請求會收到上述記錄和指標處理，以處理具有有效字符的請求。

使用 CAPTCHA 和 Challenge 動作的最佳實務

遵循本節中的指引來規劃和實作 AWS WAF CAPTCHA 或挑戰。

規劃 CAPTCHA 和挑戰實作

根據您的網站使用情況、您要保護之資料的敏感度，以及請求類型，決定放置 CAPTCHA 拼圖或無提示挑戰的位置。選取您將套用 CAPTCHA 的請求，以便您視需要呈現拼圖，但避免在沒有用的地方呈現它們，並可能降低使用者體驗。使用 Challenge 動作來執行對最終使用者影響較小的無提示挑戰，但仍有助於驗證請求是否來自已啟用 JavaScript 的瀏覽器。

CAPTCHA 拼圖和無提示挑戰只能在瀏覽器存取 HTTPS 端點時執行。瀏覽器用戶端必須在安全的內容中執行，才能取得字符。

決定在用戶端上執行 CAPTCHA 拼圖和無提示挑戰的位置

識別您不想受到 CAPTCHA 影響的請求，例如 CSS 或映像的請求。僅在必要時使用 CAPTCHA。例如，如果您計劃在登入時進行 CAPTCHA 檢查，且使用者一律直接從登入另一個畫面取得，則可能不需要在第二個畫面中進行 CAPTCHA 檢查，而且可能會降低您的最終使用者體驗。

設定 Challenge 和 CAPTCHA 使用，以便 AWS WAF 只會傳送 CAPTCHA 拼圖和無提示挑戰以回應 GET text/html 請求。您無法執行拼圖或挑戰來回應 POST 請求、跨來源資源共享 (CORS) 預

檢 OPTIONS 請求或任何其他非 GET 請求類型。其他請求類型的瀏覽器行為可能會有所不同，且可能無法正確處理間質。

用戶端可以接受 HTML，但仍無法處理 CAPTCHA 或挑戰間質。例如，具有小型 iFrame 的網頁上的小工具可能接受 HTML，但無法顯示 CAPTCHA 或處理它。避免為這些類型的請求放置規則動作，與不接受 HTML 的請求相同。

使用 CAPTCHA 或 Challenge 來驗證先前的權杖取得

您只能在合法使用者應一律擁有有效權杖的位置，使用規則動作來驗證有效權杖是否存在。在這些情況下，請求是否可以處理間質並不重要。

例如，如果您實作 JavaScript 用戶端應用程式 CAPTCHA API，並在將第一個請求傳送到受保護的端點之前立即在用戶端上執行 CAPTCHA 拼圖，則您的第一個請求應一律包含同時適用於挑戰和 CAPTCHA 的字符。如需 JavaScript 用戶端應用程式整合的資訊，請參閱 [AWS WAF JavaScript 整合](#)。

在這種情況下，在您的保護套件或 Web ACL 中，您可以新增與此第一次呼叫相符的規則，並使用 Challenge 或 CAPTCHA 規則動作進行設定。當規則符合合法最終使用者和瀏覽器時，動作會尋找有效的字符，因此不會封鎖請求或傳送挑戰或 CAPTCHA 拼圖以回應。如需規則動作如何運作的詳細資訊，請參閱 [CAPTCHA 和 Challenge 動作行為](#)。

使用 CAPTCHA 和 保護您的敏感非 HTML 資料 Challenge

您可以使用 CAPTCHA 和 Challenge 保護來保護敏感的非 HTML 資料，例如 APIs，方法如下。

1. 識別接受 HTML 回應的請求，以及在您敏感、非 HTML 資料請求附近執行的請求。
2. 撰寫符合 HTML 請求的 CAPTCHA 或 Challenge 規則，以及符合敏感資料請求的 或 規則。
3. 調校您的 CAPTCHA 和 Challenge 抗擾性時間設定，以便對於一般使用者互動，用戶端從 HTML 請求取得的權杖可在其對敏感資料的請求中使用且未過期。如需調校資訊，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。

當您的敏感資料請求符合 CAPTCHA 或 Challenge 規則時，如果用戶端仍具有先前拼圖或挑戰中的有效字符，則不會封鎖該請求。如果字符不可用或時間戳記已過期，存取敏感資料的請求將會失敗。如需規則動作如何運作的詳細資訊，請參閱 [CAPTCHA 和 Challenge 動作行為](#)。

使用 CAPTCHA 和 Challenge 來調整現有的規則

檢閱您現有的規則，以查看您是否要更改或新增規則。以下是一些需要考慮的常見案例。

- 如果您有封鎖流量的速率型規則，但速率限制相對較高，以避免封鎖合法使用者，請考慮在封鎖規則之後新增第二個速率型規則。為第二個規則提供比封鎖規則更低的限制，並將規則動作設定為 CAPTCHA 或 Challenge。封鎖規則仍會封鎖速率太高的請求，而新規則會以更低的速率封鎖大多數自動化流量。如需速率型規則的相關資訊，請參閱 [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)。
- 如果您有封鎖請求的受管規則群組，您可以將部分或全部規則的行為從 切換Block為 CAPTCHA 或 Challenge。若要這樣做，請在受管規則群組組態中覆寫規則動作設定。如需覆寫規則動作的詳細資訊，請參閱 [規則群組規則動作覆寫](#)。

在部署 CAPTCHA 之前測試 CAPTCHA 並挑戰實作

至於所有新功能，請遵循 中的指引[the section called “測試和調校您的保護”](#)。

在測試期間，請檢閱您的字符時間戳記過期要求，並設定 Web ACL 和規則層級豁免時間組態，以便在控制網站存取和為客戶提供良好的體驗之間取得良好的平衡。如需相關資訊，請參閱[在 中設定時間戳記過期和字符豁免時間 AWS WAF](#)。

保護 AWS WAF 套件或 Web ACL 流量的資料保護和記錄

本節說明您可以搭配 使用的資料記錄、收集和保護選項 AWS WAF。以下為可用選項：

- 記錄 – 您可以設定保護套件或 Web ACL，將 Web 請求流量的日誌傳送至您選擇的記錄目的地。您可以為此選項設定欄位修訂和篩選。記錄會使用套用任何資料保護設定後可用的資料。

如需此選項的詳細資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

- 請求取樣 – 您可以設定保護套件或 Web ACL 來取樣其評估的 Web 請求，以了解應用程式正在接收的流量類型。請求取樣會使用套用任何資料保護設定後可用的資料。

如需此選項的詳細資訊，請參閱[檢視 Web 請求的範例](#)。

- Amazon Security Lake – 您可以設定 Security Lake 來收集保護套件或 Web ACL 資料。Security Lake 會從各種 AWS 來源收集日誌和事件資料，以進行標準化、分析和整合。Security Lake 從套用任何資料保護設定後可用的資料中收集。

如需此選項的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的[什麼是 Amazon Security Lake ?](#) 以及[從 AWS 服務收集資料](#)。

AWS WAF 不會向您收取使用此選項的費用。如需定價資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的[Security Lake 定價](#)和[Security Lake 定價的判斷方式](#)。

- **資料保護** – 您可以在兩個層級設定 Web 流量資料的資料保護：
 - **保護套件或 Web ACL 的資料保護** – 您可以為每個保護套件或 Web ACL 設定資料保護，這可讓您使用靜態字串或密碼編譯雜湊取代特定 Web 流量資料。此層級的資料保護可以集中設定，並套用於所有記錄和資料收集選項。

如需此選項的詳細資訊，請參閱[資料保護](#)。

- **記錄修訂和篩選** – 僅記錄時，您可以從日誌中設定一些 Web 流量資料進行修訂，也可以篩選您記錄的資料。除了您已設定的任何資料保護設定之外，此選項還會影響 AWS WAF 傳送到已設定記錄目的地的資料。

主題

- [記錄 AWS WAF 保護套件或 Web ACL 流量](#)
- [資料保護](#)

記錄 AWS WAF 保護套件或 Web ACL 流量

本節說明 AWS WAF 保護套件或 Web ACLs 的記錄選項。

您可以啟用日誌記錄取得您 Web ACL 分析流量的詳細資訊。記錄的資訊包括從您的 AWS 資源 AWS WAF 接收 Web 請求的時間、請求的詳細資訊，以及請求相符規則的詳細資訊。您可以將保護套件或 Web ACL 日誌傳送至 Amazon CloudWatch Logs 日誌群組、Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 交付串流。

除了您可以為保護套件或 Web ACLs 啟用的日誌之外，AWS 也會使用處理之網站或應用程式流量的服務日誌 AWS WAF，來支援和保護 AWS 客戶和服務的安全性。

Note

保護套件或 Web ACL 記錄組態只會影響 AWS WAF 日誌。特別是，用於記錄的修訂欄位組態不會影響請求抽樣或 Security Lake 資料收集。您可以設定保護套件或 Web ACL 資料保護，將欄位排除在收集或取樣之外。除了資料保護之外，Security Lake 資料收集是透過 Security Lake 服務完全設定。

主題

- [記錄保護套件或 Web ACL 流量資訊的定價](#)
- [AWS WAF 記錄目的地](#)

- [設定保護套件或 Web ACL 的記錄](#)
- [尋找您的保護套件或 Web ACL 記錄](#)
- [保護套件或 Web ACL 流量的日誌欄位](#)
- [保護套件或 Web ACL 流量的日誌範例](#)

其他資料收集和分析選項

除了記錄之外，您還可以為資料收集和分析啟用下列選項：

- Amazon Security Lake – 您可以設定 Security Lake 來收集保護套件或 Web ACL 資料。Security Lake 會從各種來源收集日誌和事件資料，以進行標準化、分析和管理的。如需此選項的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的什麼是 Amazon Security Lake？以及[從 AWS 服務收集資料](#)。

AWS WAF 不會向您收取使用此選項的費用。如需定價資訊，請參閱《Amazon [Security Lake 使用者指南](#)》中的 [Security Lake 定價](#)和 [Security Lake 定價的判斷方式](#)。

- 請求取樣 – 您可以設定保護套件或 Web ACL 來取樣其評估的 Web 請求，以了解應用程式正在接收的流量類型。如需此選項的詳細資訊，請參閱[檢視 Web 請求的範例](#)。

記錄保護套件或 Web ACL 流量資訊的定價

本節說明使用保護套件或 Web ACL 流量日誌的定價考量。

您需要根據與每個日誌目的地類型相關聯的成本，支付日誌保護套件或 Web ACL 流量資訊的費用。這些費用是使用的附加費用 AWS WAF。您的成本可能會因您選擇的目的地類型和記錄的資料量等因素而有所不同。

下列提供每個記錄目的地類型的定價資訊連結：

- CloudWatch Logs – 費用適用於付費日誌交付。請參閱 [Amazon CloudWatch Logs 定價](#)。在付費方案下，選擇日誌索引標籤，然後在已取代的日誌下，請參閱交付至 CloudWatch Logs 的資訊。
- Amazon S3 儲存貯體 – Amazon S3 費用是 CloudWatch Logs 將日誌交付至 Amazon S3 儲存貯體和使用 Amazon S3 的合併費用。
 - 對於 Amazon S3，請參閱 [Amazon S3 定價](#)。
 - 如需 CloudWatch Logs 將日誌交付至 Amazon S3，請參閱 [Amazon CloudWatch Logs 定價](#)。在付費方案下，選擇日誌索引標籤，然後在已取代的日誌下，查看交付至 S3 的資訊
- Firehose – 請參閱 [Amazon Data Firehose 定價](#)。

如需 AWS WAF 定價的資訊，請參閱 [AWS WAF 定價](#)。

AWS WAF 記錄目的地

本節說明您可以從日誌中選擇的記錄選項 AWS WAF。每個區段都提供設定記錄的指導，包括有關目的地類型特定之任何行為的資訊。設定記錄目的地之後，您可以將其規格提供給保護套件或 Web ACL 記錄組態，以開始記錄。

主題

- [將保護套件或 Web ACL 流量日誌傳送至 Amazon CloudWatch Logs 日誌群組](#)
- [將保護套件或 Web ACL 流量日誌傳送至 Amazon Simple Storage Service 儲存貯體](#)
- [將保護套件或 Web ACL 流量日誌傳送至 Amazon Data Firehose 交付串流](#)

將保護套件或 Web ACL 流量日誌傳送至 Amazon CloudWatch Logs 日誌群組

本主題提供將保護套件或 Web ACL 流量日誌傳送至 CloudWatch Logs 日誌群組的資訊。

Note

除了使用的費用之外，您還需要支付記錄費用 AWS WAF。如需相關資訊，請參閱[記錄保護套件或 Web ACL 流量資訊的定價](#)。

若要將日誌傳送至 Amazon CloudWatch Logs，您可以建立 CloudWatch Logs 日誌群組。當您啟用登入時 AWS WAF，請提供日誌群組 ARN。在您啟用保護套件或 Web ACL 的記錄後，會在日誌串流中 AWS WAF 將日誌傳遞至 CloudWatch Logs 日誌群組。

當您使用 CloudWatch Logs 時，您可以在主控台中探索保護套件或 Web ACL 的 AWS WAF 日誌。在保護套件或 Web ACL 頁面中，選取記錄洞見索引標籤。此選項是除了透過 CloudWatch 主控台為 CloudWatch Logs 提供的記錄洞見之外的。

在與 AWS WAF 保護套件或 Web ACL 相同的區域中設定保護套件或 Web ACL 日誌的日誌群組，並使用您用來管理保護套件或 Web ACL 的相同帳戶。如需有關設定 CloudWatch Logs 日誌群組的資訊，請參閱[使用日誌群組和日誌串流](#)。

CloudWatch Logs 日誌群組的配額

CloudWatch Logs 具有輸送量的預設最大配額，可在區域內所有日誌群組之間共用，您可以請求增加。如果您的記錄需求對於目前的輸送量設定而言太高，您會看到 PutLogEvents 帳戶的限流指標。

若要在 Service Quotas 主控台中檢視限制並請求增加，請參閱 [CloudWatch Logs PutLogEvents 配額](#)。

日誌群組命名

您的日誌群組名稱必須以 開頭aws-waf-logs-，並以您喜歡的任何尾碼結尾，例如 aws-waf-logs-testLogGroup2。

產生的 ARN 格式如下：

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

日誌串流具有下列命名格式：

```
Region_web-acl-name_log-stream-number
```

以下顯示區域 TestWebACL 中保護套件或 Web ACL 的日誌串流範例us-east-1。

```
us-east-1_TestWebACL_0
```

將日誌發佈至 CloudWatch Logs 所需的許可

為 CloudWatch Logs 日誌群組設定保護套件或 Web ACL 流量記錄需要本節所述的許可設定。當您使用其中一個 AWS WAF 完整存取受管政策 AWSWAFConsoleFullAccess或時，會為您設定許可AWSWAFFullAccess。如果您想要管理對記錄 AWS WAF 和資源的更精細存取，您可以自行設定許可。如需有關管理許可的資訊，請參閱《IAM 使用者指南》中的[存取 AWS 資源的管理](#)。如需 受管 AWS WAF 政策的相關資訊，請參閱 [AWS 的 受管政策 AWS WAF](#)。

這些許可可讓您變更保護套件或 Web ACL 記錄組態、設定 CloudWatch Logs 的日誌交付，以及擷取日誌群組的相關資訊。這些許可必須連接到您用來管理的使用者 AWS WAF。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2>DeleteLoggingConfiguration"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow",
    "Sid": "LoggingConfigurationAPI"
}
{
    "Sid": "WebACLLoggingCWL",
    "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]
```

允許對所有 AWS 資源執行動作時，政策中會指出動作，其 "Resource" 設定為 "*"。這表示每個動作支援的所有 AWS 資源都允許這些動作。例如，動作僅 `wafv2:PutLoggingConfiguration` 支援 `wafv2` 記錄組態資源。

將保護套件或 Web ACL 流量日誌傳送至 Amazon Simple Storage Service 儲存貯體

本主題提供將保護套件或 Web ACL 流量日誌傳送至 Amazon S3 儲存貯體的資訊。

Note

除了使用的費用之外，您還需要支付記錄費用 AWS WAF。如需相關資訊，請參閱[記錄保護套件或 Web ACL 流量資訊的定價](#)。

若要將保護套件或 Web ACL 流量日誌傳送至 Amazon S3，您可以從用來管理保護套件或 Web ACL 的相同帳戶設定 Amazon S3 儲存貯體，並從開始命名儲存貯體 `aws-waf-logs-`。當您啟用登入時 AWS WAF，請提供儲存貯體名稱。如需有關建立記錄儲存貯體的資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[建立儲存貯體](#)。

您可以使用 Amazon Athena 互動式查詢服務存取和分析 Amazon S3 日誌。Amazon Athena 可讓您使用標準 SQL 直接在 Amazon S3 中分析資料。透過中的幾個動作 AWS Management Console，您可以將 Athena 指向存放在 Amazon S3 中的資料，並快速開始使用標準 SQL 來執行臨機操作查詢並取得結果。如需詳細資訊，請參閱《Amazon Athena 使用者指南》中的[查詢 AWS WAF 日誌](#)。如需其他範例 Amazon Athena 查詢，請參閱 GitHub 網站上的[aws-samples/waf-log-sample-athena-queries](#)。

Note

AWS WAF 支援對 Amazon S3 金鑰類型 (SSE-S3) 和 for AWS Key Management Service (SSE-KMS) 使用 Amazon S3 儲存貯體進行加密 AWS KMS keys。AWS WAF 不支援對管理的 AWS Key Management Service 金鑰進行加密 AWS。

來自保護套件或 Web ACL 的日誌檔案會每隔 5 分鐘發佈至 Amazon S3 儲存貯體。每個日誌檔案都包含過去 5 分鐘內記錄之流量的日誌記錄。

日誌檔的大小上限為 75 MB。如果日誌檔案在 5 分鐘內達到檔案大小限制，日誌會停止新增記錄，將其發佈到 Amazon S3 儲存貯體，然後建立新的日誌檔案。

日誌檔案已壓縮。如果您使用 Amazon S3 主控台開啟檔案，Amazon S3 會解壓縮日誌記錄並顯示它們。如果您下載日誌檔案，則必須解壓縮它們才能檢視記錄。

單一日誌檔案包含具有多個記錄的交錯項目。若要查看保護套件或 Web ACL 的所有日誌檔案，請查看保護套件或 Web ACL 名稱、區域和您的帳戶 ID 彙總的項目。

命名要求和語法

用於 AWS WAF 記錄的儲存貯體名稱必須以開頭 `aws-waf-logs-`，並以您想要的任何尾碼結尾。例如 `aws-waf-logs-LOGGING-BUCKET-SUFFIX`。

儲存貯體位置

儲存貯體位置使用以下語法：

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/
```

儲存貯體 ARN

儲存貯體 Amazon Resource Name (ARN) 的格式如下：

```
arn:aws:s3:::aws-waf-logs-LOGGING-BUCKET-SUFFIX
```

具有字首的儲存貯體位置

如果您在物件金鑰名稱中使用字首來組織存放在儲存貯體中的資料，您可以在記錄儲存貯體名稱中提供字首。

Note

此選項無法透過主控台使用。使用 AWS WAF APIs、CLI 或 AWS CloudFormation。

如需在 Amazon S3 中使用字首的資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[使用字首組織物件](#)。

具有字首 的儲存貯體位置使用以下語法：

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/KEY-NAME-PREFIX/
```

儲存貯體資料夾和檔案名稱

在您的儲存貯體中，並遵循您提供的任何字首，您的 AWS WAF 日誌會以由您的帳戶 ID、區域、保護套件或 Web ACL 名稱，以及日期和時間決定的資料夾結構撰寫。

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

在資料夾中，日誌檔案名稱遵循類似的格式：

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

資料夾結構和日誌檔案名稱中使用的時間規格符合時間戳記格式規格 YYYYMMddTHH:mmZ。

以下顯示名為 *aws-waf-logs-LOGGING-BUCKET-SUFFIX* 之儲存貯體的 Amazon S3 儲存貯體中的範例日誌檔案。AWS 帳戶 為 111111111111。保護套件或 Web ACL 是 *TEST-WEBACL* 而區域是 *us-east-1*。

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/AWSLogs/111111111111/WAFLogs/us-east-1/TEST-WEBACL/2021/10/28/19/50/111111111111_waflogs_us-east-1_TEST-WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

Note

用於 AWS WAF 記錄的儲存貯體名稱必須以 開頭 `aws-waf-logs-`，並以您想要的任何尾碼結尾。

將日誌發佈至 Amazon S3 所需的許可

為 Amazon S3 儲存貯體設定保護套件或 Web ACL 流量記錄需要下列許可設定。當您使用其中一個 AWS WAF 完整存取受管政策 `AWSWAFConsoleFullAccess` 或 `AWSWAFFullAccess` 時，會為您設定這些許可。如果您想要進一步管理對日誌記錄 AWS WAF 和資源的存取，您可以自行設定這些許可。如需管理許可的資訊，請參閱《IAM 使用者指南》中的 [存取資源的 AWS 管理](#)。如需 AWS WAF 受管政策的相關資訊，請參閱 [AWS 的 受管政策 AWS WAF](#)。

下列許可可讓您變更保護套件或 Web ACL 記錄組態，以及設定 Amazon S3 儲存貯體的日誌交付。這些許可必須連接到您用來管理的使用者 AWS WAF。

Note

當您設定下列許可時，您可能會在 AWS CloudTrail 日誌中看到錯誤，指出存取遭拒，但許可適用於 AWS WAF 記錄。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "LoggingConfigurationAPI"
    },
    {
      "Sid": "WebACLLogDelivery",
```

```

    "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Sid": "WebACLLoggingS3",
    "Action": [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
    ],
    "Resource": [
        "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX"
    ],
    "Effect": "Allow"
}
]
}

```

允許對所有 AWS 資源執行動作時，政策中會指出動作，其 "Resource" 設定為 "*"。這表示每個動作支援的所有 AWS 資源都允許這些動作。例如，動作僅 wafv2:PutLoggingConfiguration 支援 wafv2 記錄組態資源。

根據預設，Amazon S3 儲存貯體及其包含的物件皆為私有。只有儲存貯體擁有者可存取儲存貯體及存放於其中的物件。不過，儲存貯體擁有者可以透過撰寫存取政策，將存取權授予其他資源和使用者。

如果建立日誌的使用者擁有 儲存貯體，服務會自動將下列政策連接至儲存貯體，以授予日誌將日誌發佈至其中的許可：

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",

```

```

    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX/AWSLogs/account-id/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceAccount": ["account-id"]
      },
      "ArnLike": {
        "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
      }
    }
  },
  {
    "Sid": "AWSLogDeliveryAclCheck",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": ["account-id"]
      },
      "ArnLike": {
        "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
      }
    }
  }
]
}

```

Note

用於 AWS WAF 記錄的儲存貯體名稱必須以 開頭aws-waf-logs-，並以您想要的任何尾碼結尾。

如果建立日誌的使用者沒有儲存貯體，或沒有儲存貯體的 GetBucketPolicy 和 PutBucketPolicy 許可，則日誌建立會失敗。在此情況下，儲存貯體擁有者必須手動將上述政策新增至儲存貯體，並指定日誌建立者的 AWS 帳戶 ID。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的 [我該如何新增 S3 儲存貯體政策？](#)。如果儲存貯體收到來自多個帳戶的日誌，請將 Resource 元素項目新增至每個帳戶 AWSLogDeliveryWrite 的政策陳述式。

例如，下列儲存貯體政策允許 AWS 帳戶 111122223333 將日誌發佈至名為 的儲存貯體 aws-waf-logs-*LOGGING-BUCKET-SUFFIX*：

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite20150319",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX/AWSLogs/111122223333/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["111122223333"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["111122223333"]
        }
      }
    }
  ]
}
```



```

    },
    "ArnLike": {
      "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
    }
  }
}
]
}

```

Note

在某些情況下，如果未將 `s3:ListBucket` 許可授予 `delivery.logs.amazonaws.com`，則可能會在 AWS CloudTrail 中看到 `AccessDenied` 錯誤。若要避免 CloudTrail 日誌中出現這些錯誤，您必須將 `s3:ListBucket` 許可授予 `delivery.logs.amazonaws.com`，且必須包含與先前儲存貯體政策中設定的 `s3:GetBucketAcl` 許可一起顯示的 `Condition` 參數。若要簡化此作業，您可以直接將 `更新AWSLogDeliveryAclCheck` 為 `Statement`，而不是建立新的 `"Action": ["s3:GetBucketAcl", "s3:ListBucket"]`。

AWS Key Management Service 搭配 KMS 金鑰使用的許可

如果您的記錄目的地使用伺服器端加密搭配存放在 AWS Key Management Service (SSE-KMS) 中的金鑰，而且您使用客戶受管金鑰 (KMS 金鑰)，您必須授予許可 AWS WAF 才能使用 KMS 金鑰。若要這樣做，請將金鑰政策新增至所選目的地的 KMS 金鑰。這允許 AWS WAF 記錄將日誌檔案寫入目的地。

將下列金鑰政策新增至您的 KMS 金鑰，AWS WAF 以允許記錄到您的 Amazon S3 儲存貯體。

```

{
  "Sid": "Allow AWS WAF to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*"
}

```

存取 Amazon S3 日誌檔案所需的許可

Amazon S3 使用存取控制清單 (ACLs) 來管理對日誌所建立日誌檔案的 AWS WAF 存取。根據預設，儲存貯體擁有者擁有各個日誌檔案的 FULL_CONTROL 許可。日誌交付擁有者與儲存貯體擁有者不同時，就沒有任何許可。日誌交付帳戶擁有 READ 與 WRITE 許可。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[存取控制清單 \(ACL\) 概觀](#)。

將保護套件或 Web ACL 流量日誌傳送至 Amazon Data Firehose 交付串流

本節提供將保護套件或 Web ACL 流量日誌傳送至 Amazon Data Firehose 交付串流的資訊。

Note

除了使用的費用之外，您還需要支付記錄費用 AWS WAF。如需相關資訊，請參閱[記錄保護套件或 Web ACL 流量資訊的定價](#)。

若要將日誌傳送至 Amazon Data Firehose，請將日誌從保護套件或 Web ACL 傳送至您在 Firehose 中設定的 Amazon Data Firehose 交付串流。啟用記錄後，會透過 Firehose 的 HTTPS 端點將日誌 AWS WAF 傳送至您的儲存目的地。

一個 AWS WAF 日誌等同於一個 Firehose 記錄。如果您通常每秒收到 10,000 個請求並啟用完整日誌，您應該在 Firehose 中每秒設定 10,000 個記錄。如果您未正確設定 Firehose，AWS WAF 則不會記錄所有日誌。如需詳細資訊，請參閱[Amazon Kinesis Data Firehose 配額](#)。

如需有關如何建立 Amazon Data Firehose 交付串流和檢閱儲存日誌的資訊，請參閱[什麼是 Amazon Data Firehose？](#)

如需建立交付串流的相關資訊，請參閱[建立 Amazon Data Firehose 交付串流](#)。

為您的保護套件或 Web ACL 設定 Amazon Data Firehose 交付串流

為您的保護套件或 Web ACL 設定 Amazon Data Firehose 交付串流，如下所示。

- 使用您用來管理保護套件或 Web ACL 的相同帳戶來建立它。
- 在與保護套件或 Web ACL 相同的區域中建立它。如果您要擷取 Amazon CloudFront 的日誌，請在美國東部（維吉尼亞北部）區域建立 firehoseus-east-1。
- 為資料提供開頭為字首的名稱aws-waf-logs-。例如 aws-waf-logs-us-east-2-analytics。

- 將其設定為直接放置，允許應用程式直接存取交付串流。在 [Amazon Data Firehose 主控台](#) 中，針對交付串流來源設定，選擇直接 PUT 或其他來源。透過 API，將交付串流屬性 `DeliveryStreamType` 設定為 `DirectPut`。

 Note

請勿使用 Kinesis stream 做為來源。

將日誌發佈至 Amazon Data Firehose 交付串流所需的許可

若要了解 Kinesis Data Firehose 組態所需的許可，請參閱 [使用 Amazon Kinesis Data Firehose 控制存取](#)。

您必須具有下列許可，才能使用 Amazon Data Firehose 交付串流成功啟用保護套件或 Web ACL 記錄。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

如需服務連結角色和 `iam:CreateServiceLinkedRole` 許可的相關資訊，請參閱 [使用的服務連結角色 AWS WAF](#)。

設定保護套件或 Web ACL 的記錄

本節提供設定保護套件或 Web ACL 資料保護的說明。

 Note

除了使用的費用之外，您還需要支付記錄費用 AWS WAF。如需相關資訊，請參閱 [記錄保護套件或 Web ACL 流量資訊的定價](#)。

若要啟用保護套件或 Web ACL 的記錄，您必須已設定要使用的記錄目的地。如需有關目的地選擇和每個目的地需求的資訊，請參閱 [AWS WAF 記錄目的地](#)。

設定保護套件或 Web ACL 的記錄

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇保護套件或 Web ACLs。
3. 選擇您要啟用記錄的保護套件或 Web ACL 名稱。主控台會帶您前往保護套件或 Web ACL 的描述，您可以在其中編輯它。
4. 在記錄和指標索引標籤上，選擇啟用記錄。
5. 選擇記錄目的地類型，然後選擇您設定的記錄目的地。您必須選擇名稱開頭為 `aws-waf-logs-` 的記錄目的地。
6. (選用) 如果您不希望日誌中包含一些欄位，請對其進行修訂。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。修改的欄位會在日誌中顯示為 `xxx`。

Note

此設定不會影響請求取樣。您可以透過設定保護套件或 Web ACL 資料保護，或停用保護套件或 Web ACL 的取樣，將欄位排除在請求取樣之外。

7. (選用) 如果您不想將所有請求傳送至日誌，請新增您的篩選條件和行為。在篩選日誌下，針對您要套用的每個篩選條件，選擇新增篩選條件，然後選擇篩選條件，並指定是否要保留或捨棄符合條件的請求。當您完成新增篩選條件時，如有需要，請修改預設記錄行為。
8. 選擇 Enable Logging (啟用記錄日誌)。

Note

當您成功啟用記錄時，AWS WAF 將建立一個服務連結角色，具有將日誌寫入記錄目的地的必要許可。如需詳細資訊，請參閱 [使用的服務連結角色 AWS WAF](#)。

尋找您的保護套件或 Web ACL 記錄

本節說明如何尋找您的保護套件或 Web ACL 記錄。

Note

除了使用的費用之外，您還需要支付記錄費用 AWS WAF。如需相關資訊，請參閱[記錄保護套件或 Web ACL 流量資訊的定價](#)。

如果您在日誌中找不到日誌記錄

在極少數情況下，AWS WAF 日誌交付可能會低於 100%，日誌會盡最大努力交付。AWS WAF 架構會將應用程式的安全性優先於所有其他考量。在某些情況下，例如記錄流程遇到流量調節時，這可能會導致記錄遭到捨棄。這不應影響多個記錄。如果您發現許多日誌項目遺失，請聯絡[AWS 支援中心](#)。

在保護套件或 Web ACL 的記錄組態中，您可以自訂 AWS WAF 傳送至日誌的內容。

- 欄位修訂 – 對於使用對應比對設定的規則，您可以從日誌記錄中修訂下列欄位：URI 路徑、查詢字串、單一標頭和 HTTP 方法。已修訂的欄位會在日誌 REDACTED 中顯示為 `REDACTED`。例如，如果您修訂查詢字串欄位，在日誌中，REDACTED 對於使用查詢字串比對元件設定的所有規則，它會列為 `REDACTED`。修訂僅適用於您在規則中指定用於比對的請求元件，因此單一標頭元件的修訂不適用於標頭上相符的規則。如需日誌欄位的清單，請參閱[保護套件或 Web ACL 流量的日誌欄位](#)。

Note

此設定不會影響請求取樣。您可以透過設定保護套件或 Web ACL 資料保護，或停用保護套件或 Web ACL 的取樣，將欄位排除在請求取樣之外。

- 日誌篩選 – 您可以新增篩選，以指定哪些 Web 請求保留在日誌中，以及哪些 Web 請求遭到捨棄。您可以篩選 Web 請求評估期間 AWS WAF 套用的設定。您可以依下列設定進行篩選：
 - 完整標籤 – 完整標籤具有字首、選用命名空間和標籤名稱。字首識別新增標籤之規則的規則群組或保護套件或 Web ACL 內容。如需標籤的資訊，請參閱[中的 Web 請求標籤 AWS WAF](#)。
 - 規則動作 – 您可以篩選任何正常規則動作設定，也可以篩選規則群組規則的舊版 EXCLUDED_AS_COUNT 覆寫選項。如需規則動作設定的資訊，請參閱[在中使用規則動作 AWS WAF](#)。如需規則群組規則目前和舊版規則動作覆寫的相關資訊，請參閱[在中覆寫規則群組動作 AWS WAF](#)。
 - 一般規則動作篩選條件適用於規則中設定的動作，也適用於使用目前選項來覆寫規則群組規則動作所設定的動作。
 - EXCLUDED_AS_COUNT 日誌篩選條件與 Count 動作日誌篩選條件重疊。會 EXCLUDED_AS_COUNT 同時篩選目前和舊版選項，以將規則群組規則動作覆寫至 Count。

保護套件或 Web ACL 流量的日誌欄位

下列清單說明可能的日誌欄位。

動作

AWS WAF 套用至請求的終止動作。這表示允許、封鎖、CAPTCHA 或挑戰。當 Web 請求不包含有效的字符時，CAPTCHA和 Challenge動作正在終止。

args

查詢字串。

captchaResponse

請求的 CAPTCHA 動作狀態，會在CAPTCHA動作套用至請求時填入。此欄位會填入任何 CAPTCHA動作，無論是否終止。如果請求多次套用CAPTCHA動作，此欄位會從上次套用動作之後填入。

當請求不包含字符或字符無效或過期時，CAPTCHA動作會終止 Web 請求檢查。如果CAPTCHA動作正在終止，此欄位會包含回應代碼和失敗原因。如果動作未終止，此欄位會包含求解時間戳記。若要區分終止和非終止動作，您可以在此欄位中篩選非空白failureReason屬性。

cfDistributionTenantId

與 Web 請求相關聯之 CloudFront 分佈租用戶的識別符。此欄位是選用的，僅適用於與 CloudFront 分發租用戶相關聯的保護套件或 Web ACLs。

challengeResponse

請求的挑戰動作狀態，Challenge會在動作套用至請求時填入。此欄位會填入任何Challenge動作，無論是否終止。如果請求多次套用Challenge動作，此欄位會從上次套用動作之後填入。

當請求不包含字符或字符無效或過期時，Challenge動作會終止 Web 請求檢查。如果Challenge動作正在終止，此欄位會包含回應代碼和失敗原因。如果動作未終止，此欄位會包含求解時間戳記。若要區分終止和非終止動作，您可以在此欄位中篩選非空白failureReason屬性。

clientIp

傳送請求的用戶端 IP 地址。

國家/地區

請求來源的國家/地區。如果 AWS WAF 無法判斷原始國家/地區，則會將此欄位設定為 -。

excludedRules

僅用於規則群組規則。規則群組中已排除的規則清單。這些規則的動作設定為 Count。

如果您使用覆寫規則動作選項覆寫規則以計數，則相符項目不會在此處列出。它們會列為動作對 action 和 overriddenAction。

exclusionType

表示排除規則具有動作 的類型Count。

ruleId

在規則群組中被排除的規則 ID。

formatVersion

日誌的格式版本。

標頭

標題清單。

httpMethod

請求的 HTTP 方法。

httpRequest

請求的中繼資料。

httpSourceId

相關聯資源的 ID：

- 對於 Amazon CloudFront 分佈，ID 是 ARN 語法 *distribution-id* 中的：

`arn:partition:cloudfront::account-id:distribution/distribution-id`

- 對於 Application Load Balancer，ID 是 ARN 語法 *load-balancer-id* 中的：

`arn:partition:elasticloadbalancing:region:account-id:loadbalancer/app/load-balancer-name/load-balancer-id`

- 對於 Amazon API Gateway REST API，ID 是 ARN 語法 *api-id* 中的：

`arn:partition:apigateway:region::/restapis/api-id/stages/stage-name`

- 對於 an AWS AppSync GraphQL API，ID 是 ARN 語法 *GraphQLApiId* 中的：

`arn:partition:appsync:region:account-id:apis/GraphQLApiId`

- 對於 Amazon Cognito 使用者集區，ID 是 ARN 語法 *user-pool-id* 中的：

arn:partition:cognito-idp:region:account-id:userpool/user-pool-id

- 對於 AWS App Runner 服務，ID 是 ARN 語法 *apprunner-service-id* 中的：

arn:partition:apprunner:region:account-id:service/apprunner-service-name/apprunner-service-id

httpSourceName

請求的來源。可能的值：CF 適用於 Amazon CloudFront、APIGW 適用於 Amazon API Gateway、ALB 適用於 Application Load Balancer、APPSYNC AWS AppSync、COGNITOIDP 適用於 Amazon Cognito、APPRUNNER 適用於 App Runner 和 VERIFIED_ACCESS 適用於 Verified Access。

httpVersion

HTTP 版本。

ja3Fingerprint

請求的 JA3 指紋。

Note

JA3 指紋檢查僅適用於 Amazon CloudFront 分佈和 Application Load Balancer。

JA3 指紋是從傳入請求的 TLS Client Hello 衍生的 32 個字元雜湊。此指紋可做為用戶端 TLS 組態的唯一識別符。會針對具有足夠 TLS Client Hello 資訊以進行計算的每個請求 AWS WAF，計算並記錄此指紋。

當您在保護套件或 Web ACL 規則中設定 JA3 指紋比對時，請提供此值。如需建立與 JA3 指紋相符項目的詳細資訊，請參閱 [JA3 指紋](#) 中的 [在中請求元件 AWS WAF](#) 以取得規則陳述式。

ja4Fingerprint

請求的 JA4 指紋。

Note

JA4 指紋檢查僅適用於 Amazon CloudFront 分佈和 Application Load Balancer。

JA4 指紋是從傳入請求的 TLS Client Hello 衍生的 36 個字元雜湊。此指紋可做為用戶端 TLS 組態的唯一識別符。會針對具有足夠 TLS Client Hello 資訊以進行計算的每個請求 AWS WAF，計算並記錄此指紋。

當您在保護套件或 Web ACL 規則中設定 JA4 指紋比對時，請提供此值。如需建立與 JA4 指紋相符項目的相關資訊，請參閱 [JA4 指紋](#) 中的 [在中請求元件 AWS WAF](#) 以取得規則陳述式。

labels

Web 請求上的標籤。這些標籤是由用來評估 request. AWS WAF logs 前 100 個標籤的規則所套用。

nonTerminatingMatchingRules

符合請求的非終止規則清單。清單中的每個項目都包含下列資訊。

動作

AWS WAF 套用至請求的動作。這表示計數、CAPTCHA 或挑戰。當 Web 請求包含有效的字符時，CAPTCHA 和 Challenge 不會終止。

ruleId

符合請求且未終止的規則 ID。

ruleMatchDetails

符合請求之規則的詳細資訊。此欄位只會填入 SQL Injection 和跨網站指令碼 (XSS) 比對規則陳述式。比對規則可能需要符合多個檢查條件，因此這些比對詳細資訊會以比對條件陣列的形式提供。

每個規則提供的任何其他資訊會根據規則組態、規則比對類型和比對的詳細資訊等因素而有所不同。例如，對於具有 CAPTCHA 或 Challenge 動作的規則，challengeResponse 將列出 captchaResponse 或。如果相符規則位於規則群組中，且您已覆寫其設定的規則動作，則設定的動作將在 中提供 overriddenAction。

oversizeFields

Web 請求中的欄位清單，由保護套件或 Web ACL 檢查，且超過 AWS WAF 檢查限制。如果欄位過大，但保護套件或 Web ACL 未檢查，則不會在此處列出。

此清單可包含下列零個或多個值：REQUEST_BODY、REQUEST_HEADERS、REQUEST_JSON_BODY 和 REQUEST_COOKIES。如需超大欄位的詳細資訊，請參閱 [在中過大 Web 請求元件 AWS WAF](#)。

rateBasedRuleList

處理請求的以速率為基礎的規則名單。如需速率型規則的相關資訊，請參閱 [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)。

rateBasedRuleId

處理請求的速率規則 ID。若此項目已終止請求，則 `rateBasedRuleId` 的 ID 將與 `terminatingRuleId` 的 ID 相同。

rateBasedRuleName

對請求採取動作的以速率為基礎的規則名稱。

limitKey

規則正在使用的彙總類型。可能的值 IP 適用於 Web 請求原始伺服器、請求中標頭轉送的 `FORWARDED_IP` IP、`CUSTOMKEYS` 自訂彙總金鑰設定。和 `CONSTANT` 用於將所有請求計數在一起，無需彙總。

limitValue

僅在單一 IP 地址類型的速率限制時使用。如果請求包含無效的 IP 地址，則 `limitvalue` 為 `INVALID`。

maxRateAllowed

特定彙總執行個體在指定時段內允許的請求數量上限。彙總執行個體是由 加上您在以速率為基礎的規則組態中提供 `limitKey` 的任何其他金鑰規格所定義。

evaluationWindowSec

AWS WAF 包含在請求中的時間，以秒為單位。

customValues

請求中以速率為基礎的規則識別的唯一值。對於字串值，日誌會列印字串值的前 32 個字元。根據金鑰類型，這些值可能僅適用於金鑰，例如 HTTP 方法或查詢字串，也可能適用於金鑰和名稱，例如標頭和標頭名稱。

requestHeadersInserted

插入以進行自訂請求處理的標頭清單。

requestId

請求的 ID，由基礎主機服務產生。對於 Application Load Balancer，這是追蹤 ID。對於所有其他，這是請求 ID。

responseCodeSent

隨自訂回應傳送的回應碼。

ruleGroupId

規則群組的 ID。若規則封鎖請求，則 ruleGroupId 的 ID 將與 terminatingRuleId 的 ID 相同。

ruleGroupList

對此請求採取動作的規則群組清單，其中包含相符資訊。

terminatingRule

終止請求的規則。如果存在，則會包含下列資訊。

動作

AWS WAF 套用至請求的終止動作。這表示允許、封鎖、CAPTCHA 或挑戰。當 Web 請求不包含有效的字符時，CAPTCHA 和 Challenge 動作正在終止。

ruleId

符合請求的規則 ID。

ruleMatchDetails

符合請求之規則的詳細資訊。此欄位只會填入 SQL Injection 和跨網站指令碼 (XSS) 比對規則陳述式。比對規則可能需要符合多個檢查條件，因此這些比對詳細資訊會以比對條件陣列的形式提供。

每個規則提供的任何其他資訊會根據規則組態、規則比對類型和比對的詳細資訊等因素而有所不同。例如，對於具有 CAPTCHA 或 Challenge 動作的規則，challengeResponse 將列出 captchaResponse 或。如果相符規則位於規則群組中，且您已覆寫其設定的規則動作，則設定的動作將在 overriddenAction 中提供。

terminatingRuleId

終止請求的規則 ID。如果無法終止請求，則值為 Default_Action。

terminatingRuleMatchDetails

符合請求之終止規則的詳細資訊。終止規則對 Web 請求具有結束檢查程序的動作。終止規則的可能動作包括 Allow、CAPTCHA、Block 和 Challenge。在檢查 Web 請求期間，在第一個符合請求且具有終止動作的規則中，會 AWS WAF 停止檢查並套用動作。除了日誌中針對相符終止規則所回報的威脅之外，Web 請求還可能包含其他威脅。

這只會為 SQL Injection 和跨網站指令碼 (XSS) 符合規則陳述式填入。比對規則可能需要符合多個檢查條件，因此這些比對詳細資訊會以比對條件陣列的形式提供。

terminatingRuleType

終止請求的規則類型。可能的值：RATE_BASED、REGULAR、GROUP 和 MANAGED_RULE_GROUP。

timestamp

時間戳記，以毫秒為單位。

uri

URI 請求。

fragment

遵循 "#" 符號的 URL 部分，提供有關資源的其他資訊，例如 #section2。

webaclId

保護套件或 Web ACL 的 GUID。

保護套件或 Web ACL 流量的日誌範例

本節提供記錄保護套件或 Web ACL 流量的範例。

Example 以速率為基礎的規則 1：使用一個索引鍵的規則組態，設定為 **Header:dogname**

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  }
}
```

```

    }
  ]
}
]
}
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "RateBasedRule"
}
}

```

Example 以速率為基礎的規則 1：以速率為基礎的規則封鎖請求的日誌項目

```

{
  "timestamp":1683355579981,
  "formatVersion":1,
  "webaclId": ...,
  "terminatingRuleId":"RateBasedRule",
  "terminatingRuleType":"RATE_BASED",
  "action":"BLOCK",
  "terminatingRuleMatchDetails":[

  ],
  "httpSourceName":"APIGW",
  "httpSourceId":"EXAMPLE11:rjveg5guh:CanaryTest",
  "ruleGroupList":[

  ],
  "rateBasedRuleList":[
    {
      "rateBasedRuleId": ...,
      "rateBasedRuleName":"RateBasedRule",
      "limitKey":"CUSTOMKEYS",
      "maxRateAllowed":100,
      "evaluationWindowSec":"120",
      "customValues":[

      ]
    }
  ]
}

```

```
        "key": "HEADER",
        "name": "dogname",
        "value": "ella"
      }
    ]
  },
  ],
  "nonTerminatingMatchingRules": [

  ],
  "requestHeadersInserted": null,
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "52.46.82.45",
    "country": "FR",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "52.46.82.45"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
      },
      {
        "name": "dogname",
        "value": "ella"
      },
      {
        "name": "User-Agent",
        "value": "RateBasedRuleTestKoipOneKeyModulePV2"
      }
    ]
  },
```

```
{
  "name": "Accept-Encoding",
  "value": "gzip, deflate"
},
{
  "uri": "/CanaryTest",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "Ed0AiHF_CGYF-DA="
}
}
```

Example 以速率為基礎的規則 2：具有兩個索引鍵的規則組態，設定為 **Header:dogname**和 **Header:catname**

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  {
    "Header": {
      "Name": "catname",
      "TextTransformations": [
        {
          "Priority": 0,
          "Type": "NONE"
        }
      ]
    }
  }
}
```

```

        ]
      }
    }
  ]
}
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "RateBasedRule"
}
}

```

Example 以速率為基礎的規則 2：以速率為基礎的規則封鎖請求的日誌項目

```

{
  "timestamp":1633322211194,
  "formatVersion":1,
  "webaclId":...,
  "terminatingRuleId":"RateBasedRule",
  "terminatingRuleType":"RATE_BASED",
  "action":"BLOCK",
  "terminatingRuleMatchDetails":[

  ],
  "httpSourceName":"APIGW",
  "httpSourceId":"EXAMPLE11:rjveg5guh:CanaryTest",
  "ruleGroupList":[

  ],
  "rateBasedRuleList":[
    {
      "rateBasedRuleId":...,
      "rateBasedRuleName":"RateBasedRule",
      "limitKey":"CUSTOMKEYS",
      "maxRateAllowed":100,
      "evaluationWindowSec":"120",
      "customValues":[
        {
          "key":"HEADER",

```



```
        "name": "dogname",
        "value": "ella"
      },
      {
        "key": "HEADER",
        "name": "catname",
        "value": "goofie"
      }
    ]
  }
],
"nonTerminatingMatchingRules": [

],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "52.46.82.35",
  "country": "FR",
  "headers": [
    {
      "name": "X-Forwarded-For",
      "value": "52.46.82.35"
    },
    {
      "name": "X-Forwarded-Proto",
      "value": "https"
    },
    {
      "name": "X-Forwarded-Port",
      "value": "443"
    },
    {
      "name": "Host",
      "value": "2311byn8v3.execute-api.eu-west-3.amazonaws.com"
    },
    {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
    },
    {
      "name": "catname",
      "value": "goofie"
    }
  ],
}
```

```

    {
      "name": "dogname",
      "value": "ella"
    },
    {
      "name": "User-Agent",
      "value": "Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
    },
    {
      "name": "Accept-Encoding",
      "value": "gzip, deflate"
    }
  ],
  "uri": "/CanaryTest",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "EdzmlH50CGYF1vQ="
}
}

```

Example SQLi 偵測時觸發之規則的日誌輸出 (終止)

```

{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/STMTTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
  "terminatingRuleId": "STMTTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "HIGH",
      "location": "HEADER",
      "matchedData": [
        "10",
        "AND",
        "1"
      ]
    }
  ],
}

```

```
"httpSourceName": "-",
"httpSourceId": "-",
"ruleGroupList": [],
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [],
"httpRequest": {
  "clientIp": "1.1.1.1",
  "country": "AU",
  "headers": [
    {
      "name": "Host",
      "value": "localhost:1989"
    },
    {
      "name": "User-Agent",
      "value": "curl/7.61.1"
    },
    {
      "name": "Accept",
      "value": "*/*"
    },
    {
      "name": "x-stm-test",
      "value": "10 AND 1=1"
    }
  ],
  "uri": "/myUri",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "rid"
},
"labels": [
  {
    "name": "value"
  }
]
}
```

Example SQLi 偵測時觸發之規則的日誌輸出（非終止中）

```
{
  "timestamp":1592357192516
```

```
, "formatVersion": 1
, "webaclId": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
, "terminatingRuleId": "Default_Action"
, "terminatingRuleType": "REGULAR"
, "action": "ALLOW"
, "terminatingRuleMatchDetails": []
, "httpSourceName": "-"
, "httpSourceId": "-"
, "ruleGroupList": []
, "rateBasedRuleList": []
, "nonTerminatingMatchingRules":
[
  {
    "ruleId": "TestRule"
    , "action": "COUNT"
    , "ruleMatchDetails":
      [
        {
          "conditionType": "SQL_INJECTION"
          , "sensitivityLevel": "HIGH"
          , "location": "HEADER"
          , "matchedData": [
              "10"
              , "and"
              , "1"
            ]
        }
      ]
    }
  ]
, "httpRequest": {
  "clientIp": "3.3.3.3"
  , "country": "US"
  , "headers": [
    { "name": "Host", "value": "localhost:1989" }
    , { "name": "User-Agent", "value": "curl/7.61.1" }
    , { "name": "Accept", "value": "*/*" }
    , { "name": "myHeader", "myValue": "10 AND 1=1" }
  ]
  , "uri": "/myUri", "args": ""
  , "httpVersion": "HTTP/1.1"
  , "httpMethod": "GET"
  , "requestId": "rid"
}
, "labels": [
  {
    "name": "value"
  }
]
```

```
]
}
```

Example 在規則群組內觸發的多個規則的日誌輸出 (RuleA-XSS 正在終止，而 Rule-B 正在非終止)

```
{
  "timestamp":1592361810888,
  "formatVersion":1,
  "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
  , "terminatingRuleId":"RG-Reference"
  , "terminatingRuleType":"GROUP"
  , "action":"BLOCK",
  "terminatingRuleMatchDetails":
  [{
    "conditionType":"XSS"
    , "location":"HEADER"
    , "matchedData":["<","frameset"]
  }]
  , "httpSourceName":"-"
  , "httpSourceId":"-"
  , "ruleGroupList":
  [{
    "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-world/c051b698-1f11-4m41-aef4-99a506d53f4b"
    , "terminatingRule":{
      "ruleId":"RuleA-XSS"
      , "action":"BLOCK"
      , "ruleMatchDetails":null
    }
    , "nonTerminatingMatchingRules":
    [{
      "ruleId":"RuleB-SQLi"
      , "action":"COUNT"
      , "ruleMatchDetails":
      [{
        "conditionType":"SQL_INJECTION"
        , "sensitivityLevel": "LOW"
        , "location":"HEADER"
        , "matchedData":[
          "10"
          , "and"
          , "1"]
      ]
    }
  ]
}
```

```
    ]
  ]
  , "excludedRules": null
}]
, "rateBasedRuleList": []
, "nonTerminatingMatchingRules": []
, "httpRequest": {
  "clientIp": "3.3.3.3"
  , "country": "US"
  , "headers":
  [
    { "name": "Host", "value": "localhost:1989" }
    , { "name": "User-Agent", "value": "curl/7.61.1" }
    , { "name": "Accept", "value": "*/*" }
    , { "name": "myHeader1", "value": "<frameset onload=alert(1)>" }
    , { "name": "myHeader2", "value": "10 AND 1=1" }
  ]
  , "uri": "/myUri"
  , "args": ""
  , "httpVersion": "HTTP/1.1"
  , "httpMethod": "GET"
  , "requestId": "rid"
},
"labels": [
  {
    "name": "value"
  }
]
}
```

Example 為檢查具有內容類型 JSON 的請求內文而觸發的規則的日誌輸出

AWS WAF 目前會將 JSON 內文檢查的位置報告為 UNKNOWN。

```
{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
  "terminatingRuleId": "STMTTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
```

```
        "sensitivityLevel": "LOW",
        "location": "UNKNOWN",
        "matchedData": [
            "10",
            "AND",
            "1"
        ]
    },
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 針對具有有效、未過期 CAPTCHA 字符之 Web 請求的 CAPTCHA 規則的日誌輸出

下列日誌清單適用於符合規則與 CAPTCHA 動作的 Web 請求。Web 請求具有有效和未過期的 CAPTCHA 字符，並且僅被標註為 CAPTCHA 比對者 AWS WAF，類似於 Count 動作的行為。此 CAPTCHA 比對會記錄在下 nonTerminatingMatchingRules。

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
```

```
"webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
"terminatingRuleId": "Default_Action",
"terminatingRuleType": "REGULAR",
"action": "ALLOW",
"terminatingRuleMatchDetails": [],
"httpSourceName": "APIGW",
"httpSourceId": "123456789012:b34myvfw0b:pen-test",
"ruleGroupList": [],
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [
  {
    "ruleId": "captcha-rule",
    "action": "CAPTCHA",
    "ruleMatchDetails": [],
    "captchaResponse": {
      "responseCode": 0,
      "solveTimestamp": 1632420429
    }
  }
],
"requestHeadersInserted": [
  {
    "name": "x-amzn-waf-test-header-name",
    "value": "test-header-value"
  }
],
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "72.21.198.65",
  "country": "US",
  "headers": [
    {
      "name": "X-Forwarded-For",
      "value": "72.21.198.65"
    },
    {
      "name": "X-Forwarded-Proto",
      "value": "https"
    },
    {
      "name": "X-Forwarded-Port",
      "value": "443"
    }
  ],
}
```



```
{
  "name": "Host",
  "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
},
{
  "name": "X-Amzn-Trace-Id",
  "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
},
{
  "name": "cache-control",
  "value": "max-age=0"
},
{
  "name": "sec-ch-ua",
  "value": "\"Chromium\";v=\"94\"\", \"Google Chrome\";v=\"94\"\", \";Not A Brand\";v=\"99\""
},
{
  "name": "sec-ch-ua-mobile",
  "value": "?0"
},
{
  "name": "sec-ch-ua-platform",
  "value": "\"Windows\""
},
{
  "name": "upgrade-insecure-requests",
  "value": "1"
},
{
  "name": "user-agent",
  "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
},
{
  "name": "accept",
  "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
},
{
  "name": "sec-fetch-site",
  "value": "same-origin"
},
{
```

```
    "name": "sec-fetch-mode",
    "value": "navigate"
  },
  {
    "name": "sec-fetch-user",
    "value": "?1"
  },
  {
    "name": "sec-fetch-dest",
    "value": "document"
  },
  {
    "name": "referrer",
    "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
  },
  {
    "name": "accept-encoding",
    "value": "gzip, deflate, br"
  },
  {
    "name": "accept-language",
    "value": "en-US,en;q=0.9"
  },
  {
    "name": "cookie",
    "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2081SkYDRqf1y0NcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
  }
],
"uri": "/pen-test/pets",
"args": "",
"httpVersion": "HTTP/1.1",
"httpMethod": "GET",
"requestId": "GINMHHUgoAMFxug="
}
```

Example 針對沒有 CAPTCHA 字符的 Web 請求記錄 CAPTCHA 規則的輸出

下列日誌清單適用於符合規則與 CAPTCHA 動作的 Web 請求。Web 請求沒有 CAPTCHA 權杖，且已被封鎖 AWS WAF。

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
```

```
    },
    {
      "name": "sec-ch-ua",
      "value": "\"Chromium\";v=\"94\"\", \"Google Chrome\";v=\"94\"\", \";Not A Brand  
\";v=\"99\"\"
    },
    {
      "name": "sec-ch-ua-mobile",
      "value": "?0"
    },
    {
      "name": "sec-ch-ua-platform",
      "value": "\"Windows\""
    },
    {
      "name": "upgrade-insecure-requests",
      "value": "1"
    },
    {
      "name": "user-agent",
      "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/94.0.4606.54 Safari/537.36"
    },
    {
      "name": "accept",
      "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/  
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
    },
    {
      "name": "sec-fetch-site",
      "value": "cross-site"
    },
    {
      "name": "sec-fetch-mode",
      "value": "navigate"
    },
    {
      "name": "sec-fetch-user",
      "value": "?1"
    },
    {
      "name": "sec-fetch-dest",
      "value": "document"
    },
  ],
```

```
{
  "name": "accept-encoding",
  "value": "gzip, deflate, br"
},
{
  "name": "accept-language",
  "value": "en-US,en;q=0.9"
}
],
"uri": "/pen-test/pets",
"args": "",
"httpVersion": "HTTP/1.1",
"httpMethod": "GET",
"requestId": "GINKHEssoAMFsrg="
},
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
}
```

資料保護

AWS WAF 資料保護設定可讓您在特定資料欄位實作自訂且精細的敏感資訊保護（密碼、API 金鑰、身分驗證字符和其他機密資料），例如標頭、參數和內文內容。

您可以在下列任一位置設定資料保護：

- 套用於所有輸出目的地的保護套件或 Web ACL 層級。
- 僅記錄，這只會影響 AWS WAF 傳送至已設定記錄目的地的資料。

資料保護可以指定為替代或雜湊。替代是指以文字取代內容 REDACTED。雜湊是指以取代內容 `sha256(account_number + content[:64])`。您應該檢閱 SHA-256 雜湊的特性，以判斷是否符合您的需求，再選取適當的資料保護方法。如果您想要達到相當於加密或字符化的結果，我們不建議依賴 SHA-256 雜湊。

主題

- [啟用資料保護](#)
- [資料保護例外狀況](#)

- [資料保護限制](#)
- [資料保護的範例](#)
- [設定保護套件或 Web ACL 的資料保護](#)

啟用資料保護

本節說明您可以從 主控台選取的資料保護和日誌組態選項。您可以啟用特定欄位的資料保護，以保護日誌中顯示的資料。資料保護可以套用來轉換各種輸出類型的敏感資訊，包括完整日誌、範例請求和 Security Lake。

在 AWS WAF 主控台中啟用資料保護

導覽至 主控台中的保護套件或 Web ACLs 頁面，以啟用保護設定。若要啟用日誌的資料保護，請選擇是否將其套用至所有日誌或特定日誌目的地。如需相關資訊，請參閱[保護套件或 Web ACL 流量的日誌欄位](#)。

Note

您不需要啟用記錄功能，即可在所有記錄上套用資料保護。無論是否啟用記錄，資料保護都會套用至所有輸出目的地。

在啟用保護設定頁面底部，選取資料保護欄位面板上的新增欄位按鈕。從下拉式選單中選取欄位類型。如需有關如何以資料保護保護每個欄位資料的資訊，請參閱下表。

欄位類型	詳細資訊
Single header	根據指定的選項（雜湊或子位置）永久轉換指定的標頭索引鍵值。轉換的值也會反映在完整的日誌中。
Body	永久轉換內文值。僅適用於 日誌RuleMatch Details 中的。
Query string	根據指定的選項（雜湊或子位置）永久轉換查詢字串。轉換的值也會反映在完整的日誌中。

欄位類型	詳細資訊
Single query argument	根據指定的選項（雜湊或子位置）永久轉換指定的查詢 arg 值。轉換的值也會反映在完整的日誌中。
Single cookie	根據指定的選項（雜湊或子位置）永久轉換 Cookie 值。轉換的值也會反映在完整的日誌中。

資料保護例外狀況

啟用時，資料保護將套用至其啟用的欄位，包括 RuleMatchDetails 和 rateBasedRuleList。不過，有些執行個體可能想要在 和 中包含受保護的資料 RuleMatchDetails 和 內容，rateBasedRuleList 以用於疑難排解和可見性目的。在這些情況下，您可以指定該欄位資料保護的例外狀況。

- **ExcludeRuleMatchDetails**：如果您為特定欄位指定此例外狀況，RuleMatchDetails 會顯示欄位的值，且不會在資料保護的範圍內。
- **ExcludeRateBasedDetails**：如果您為特定欄位指定此例外狀況，rateBasedRuleList 會顯示欄位的值，且不會在資料保護的範圍內。

範例：ExcludeRateBasedDetails 規則在 SINGLE_HEADER 和 "dogname" 的 HEADER_NAME 上啟用。

如果例外狀況未套用至規則，則 "dogname" 的值會顯示為 REDACTED。

```
"rateBasedRuleList": [ {"rateBasedRuleId": ...,
                        "rateBasedRuleName": "RateBasedRule", "limitKey": "CUSTOMKEYS",
                        "maxRateAllowed": 100, "evaluationWindowSec": "120",
                        "customValues": [
                            {"key": "HEADER", "name": "dogname", "value": "REDACTED" } ] } ]
```

如果規則已啟用例外狀況，則日誌中會顯示 "dogname" 值。

```
"rateBasedRuleList": [ {"rateBasedRuleId": ...,
                        "rateBasedRuleName": "RateBasedRule", "limitKey": "CUSTOMKEYS",
```

```
"maxRateAllowed":100, "evaluationWindowSec":"120",  
"customValues":[  
  {"key":"HEADER", "name":"dogname", "value":"ELLA" } ] } ]
```

Warning

資料保護功能可能會影響故障診斷 AWS WAF 功能。這些設定可能會導致非預期的偵測和緩解行為。將特定參數的資料保護限制為僅絕對必要的參數。

資料保護限制

以下是使用資料保護時應考慮的限制。

QueryString 和 SingleQueryArg

QueryString 保護

- 上的資料保護QueryString適用於所有查詢引數，並根據指定的設定替換/雜湊索引鍵和值。

RuleMatch詳細資訊和RateBased規則清單中的 QueryString

- 如果將資料保護套用至單一查詢引數，則會在完整日誌的 RuleMatchDetails和 RateBasedRule區段中取代/雜湊整個查詢字串。
- 如果在多個單一查詢引數中指定了不同的保護方法（替換和雜湊），則更嚴格的方法替換將套用至完整日誌中 RuleMatchDetails和 RateBasedRule區段中的整個查詢字串。

Cookie

Note

資料保護只有在單一標頭 Cookie 受到保護時，才會套用至 Cookie 的值。

RuleMatchDetails和 RateBasedRule 清單中的單一 Cookie

- 如果將資料保護套用至單一 Cookie，則完整日誌中 RuleMatchDetails和 RateBasedRule區段中的整個 Cookie 標頭將會取代/雜湊。

- 如果指定了不同的保護方法（替代和雜湊），更嚴格的方法、替代將套用至完整日誌中 RuleMatchDetails 和 RateBasedRule 區段中的整個 Cookie。

資料保護的範例

本節提供保護套件或 Web ACL 流量的資料保護記錄日誌範例。

DataProtection 雜湊

Webacl 組態

```
"data_protection_config": {
  "data_protections": [
    {
      "field": {
        "field_type": "SINGLE_QUERY_ARGUMENT",
        "field_keys": [
          "hoppy"
        ]
      },
      "action": "HASH",
      "exclude_rule_match_details": false,
      "exclude_rate_based_details": false
    }
  ]
}
```

範例 DataProtection 雜湊：受 SingleQuery 引數 "hoppy" 保護的日誌項目。

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
```

```
"nonTerminatingMatchingRules": [{
  "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
  "action": "COUNT",
  "ruleMatchDetails": [{
    "conditionType": "SQL_INJECTION",
    "sensitivityLevel": "HIGH",
    "location": "SINGLE_QUERY_ARG",
    "matchedData": [ "z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM=" ],
    "matchedFieldName": "hoppy"
  }]
}],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "54.239.98.137",
  "country": "US",
  "headers": [{
    "name": "X-Forwarded-For",
    "value": "54.239.98.137"
  }, {
    "name": "X-Forwarded-Proto",
    "value": "https"
  }, {
    "name": "X-Forwarded-Port",
    "value": "443"
  }, {
    "name": "Host",
    "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
  }, {
    "name": "X-Amzn-Trace-Id",
    "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
  }, {
    "name": "Accept-Encoding",
    "value": "gzip"
  }, {
    "name": "User-Agent",
    "value": "okhttp/3.12.1"
  }],
  "uri": "/CanaryTest",
  "args": "hoppy=z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM=&yellow=hello&x-hoppy-extra=generic-%3Cwords%3E-in-angle-brackets",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "Fep00F8fIAMEqoQ="
```

```
},
"labels": [{
  "name": "awsaf:forwardedip:geo:country:US"
}, {
  "name": "awsaf:forwardedip:geo:region:US-VA"
}]
}
```

DataProtection 替換

Webacl Config

```
"data_protection_config": {
  "data_protections": [
    {
      "field": {
        "field_type": "SINGLE_QUERY_ARGUMENT",
        "field_keys": [
          "hoppy"
        ]
      },
      "action": "SUBSTITUTION",
      "exclude_rule_match_details": false,
      "exclude_rate_based_details": false
    }
  ]
}
```

範例 DataProtection 替換：具有單一查詢引數的日誌項目「跳躍」受保護

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
```

```
"nonTerminatingMatchingRules": []
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "54.239.98.137",
  "country": "US",
  "headers": [{
    "name": "X-Forwarded-For",
    "value": "54.239.98.137"
  }, {
    "name": "X-Forwarded-Proto",
    "value": "https"
  }, {
    "name": "X-Forwarded-Port",
    "value": "443"
  }, {
    "name": "Host",
    "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
  }, {
    "name": "X-Amzn-Trace-Id",
    "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
  }, {
    "name": "Accept-Encoding",
    "value": "gzip"
  }, {
    "name": "User-Agent",
    "value": "okhttp/3.12.1"
  }],
  "uri": "/CanaryTest",
  "args": "hoppy=REDACTED&yellow=hello&x-hoppy-extra=generic-%3Cwords%3E-in-angle-brackets",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "Fep00F8fIAMEqoQ="
},
"labels": [{
  "name": "awsaf:forwardedip:geo:country:US"
}, {
  "name": "awsaf:forwardedip:geo:region:US-VA"
}]
}
```

在 RuleMatchDetails 中保留資料

Webacl 組態

```
"data_protection_config": {
  "data_protections": [
    {
      "field": {
        "field_type": "SINGLE_HEADER",
        "field_keys": [
          "hoppy"
        ]
      },
      "action": "HASH",
      "exclude_rule_match_details": true,
      "exclude_rate_based_details": false
    }
  ]
}
```

在 RuleMatchDetails 中保留資料的範例：具有單一Header「躍點」保護的日誌項目，但值只會保留在中RuleMatchDetails。

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [{
    "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
    "action": "COUNT",
    "ruleMatchDetails": [{
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "HIGH",
      "location": "HEADER",
```

```
        "matchedData": [ "10", "AND", "1" ],
        "matchedFieldName": "hoppy"
    }
  ]
},
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "54.239.98.137",
  "country": "US",
  "headers": [{
    "name": "X-Forwarded-For",
    "value": "54.239.98.137"
  }, {
    "name": "X-Forwarded-Proto",
    "value": "https"
  }, {
    "name": "X-Forwarded-Port",
    "value": "443"
  }, {
    "name": "Host",
    "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
  }, {
    "name": "X-Amzn-Trace-Id",
    "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
  }, {
    "name": "hoppy",
    "value": "zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="
  }, {
    "name": "Accept-Encoding",
    "value": "gzip"
  }, {
    "name": "User-Agent",
    "value": "okhttp/3.12.1"
  }, {
    "name": "hoppy",
    "value": "z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM="
  }
],
"uri": "/CanaryTest",
"args": "happy=true",
"httpVersion": "HTTP/1.1",
"httpMethod": "GET",
"requestId": "Fep00F8fIAMEqoQ="
},
"labels": [{
```

```
    "name": "awsaf:forwardedip:geo:country:US"
  }, {
    "name": "awsaf:forwardedip:geo:region:US-VA"
  }
]
```

在 rateBasedRule 中保留資料

```
"data_protection_config": {
  "data_protections": [
    {
      "field": {
        "field_type": "SINGLE_HEADER",
        "field_keys": [
          "hoppy"
        ]
      },
      "action": "HASH",
      "exclude_rule_match_details": false,
      "exclude_rate_based_details": true
    }
  ]
}
```

RateBasedRuleList 中的範例保留資料：受單一Header「躍點」保護的日誌項目，但值只會保留在 rateBasedRuleList

```
{
  "timestamp": 1683355579981,
  "formatVersion": 1,
  "webaclId": "...",
  "terminatingRuleId": "RateBasedRule",
  "terminatingRuleType": "RATE_BASED",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "EXAMPLE11:rjveg5guh:CanaryTest",
  "ruleGroupList": [],
  "rateBasedRuleList": [{
    "rateBasedRuleId": "...",
    "rateBasedRuleName": "RateBasedRule",
    "limitKey": "CUSTOMKEYS",
    "maxRateAllowed": 100,
```

```
    "evaluationWindowSec": "120",
    "customValues": [{
      "key": "HEADER",
      "name": "hoppy",
      "value": "ella"
    }]
  }],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "52.46.82.45",
    "country": "FR",
    "headers": [{
      "name": "X-Forwarded-For",
      "value": "52.46.82.45"
    }, {
      "name": "X-Forwarded-Proto",
      "value": "https"
    }, {
      "name": "X-Forwarded-Port",
      "value": "443"
    }, {
      "name": "Host",
      "value": "rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
    }, {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
    }, {
      "name": "hoppy",
      "value": "zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="
    }, {
      "name": "User-Agent",
      "value": "RateBasedRuleTestKoipOneKeyModulePV2"
    }, {
      "name": "Accept-Encoding",
      "value": "gzip,deflate"
    }
  ],
  "uri": "/CanaryTest",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "Ed0AiHF_CGYF-DA="
}
```



```
}
```

內文的資料保護

AWS WAF 只會記錄 中內文的子集RuleMatchDetails。

Webacl 組態

```
"data_protection_config": {
  "data_protections": [
    {
      "field": {
        "field_type": "BODY"
      },
      "action": "SUBSTITUTE",
      "exclude_rule_match_details": false,
      "exclude_rate_based_details": false
    }
  ]
}
```

內文DataProtection範例：內文位於 中的日誌項目ruleMatchDetails。

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [{
    "ruleId": "ProtectedSQLIBody",
    "action": "COUNT",
    "ruleMatchDetails": [{
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "HIGH",
      "location": "BODY",
```

```
        "matchedData": ["REDACTED"]
      ]
    },
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
      "clientIp": "54.239.98.137",
      "country": "US",
      "headers": [{
        "name": "X-Forwarded-For",
        "value": "54.239.98.137"
      }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
      }, {
        "name": "X-Forwarded-Port",
        "value": "443"
      }, {
        "name": "Host",
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
      }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
      }, {
        "name": "Accept-Encoding",
        "value": "gzip"
      }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
      }, {
        "name": "cookie",
        "value": "hoppy=dog;"
      }
    ],
    "uri": "/CanaryTest",
    "args": "baloo=abc&hoppy-query=xyz&x-hoppy-extra=generic-%3Cwords%3E-in-angle-
brackets",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "Fep00F8fIAMEqoQ="
  },
  "labels": [{
    "name": "awsaf:forwardedip:geo:country:US"
  }, {
    "name": "awsaf:forwardedip:geo:region:US-VA"
```

```
  ]]  
}
```

SINGLE_COOKIE 的資料保護

Webacl 組態

```
"data_protection_config": {  
  "data_protections": [  
    {  
      "field": {  
        "field_type": "SINGLE_COOKIE",  
        "field_keys": [  
          "MILO"  
        ]  
      },  
      "action": "HASH",  
      "exclude_rule_match_details": false,  
      "exclude_rate_based_details": false  
    }  
  ]  
}
```

的範例 DataProtection：具有SINGLE_COOKIE名為 "MILO" 保護的SINGLE_COOKIE日誌項目。

完整日誌顯示名為 MILO 的 Cookie 受到 ruleMatchDetails和 Cookie 標頭的保護。只會保護 Cookie 值，並排除金鑰名稱。

Note

所有受保護的欄位（單一標頭、Cookie、查詢 arg）不區分大小寫。因此，在此範例中，「MILO」符合「milo」。

```
{  
  "timestamp": 1738705092889,  
  "formatVersion": 1,  
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/  
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",  
  "terminatingRuleId": "Default_Action",  
  "terminatingRuleType": "REGULAR",  
  "action": "ALLOW",  
}
```

```
"terminatingRuleMatchDetails": [],
"httpSourceName": "APIGW",
"httpSourceId": "746533260405:xt7v59bhn7:ABC",
"ruleGroupList": [],
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [{
  "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
  "action": "COUNT",
  "ruleMatchDetails": [{
    "conditionType": "SQL_INJECTION",
    "sensitivityLevel": "HIGH",
    "location": "COOKIE",
    "matchedData": ["zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="],
    "matchedFieldName": "milo"
  }]
}],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "54.239.98.137",
  "country": "US",
  "headers": [{
    "name": "X-Forwarded-For",
    "value": "54.239.98.137"
  }, {
    "name": "X-Forwarded-Proto",
    "value": "https"
  }, {
    "name": "X-Forwarded-Port",
    "value": "443"
  }, {
    "name": "Host",
    "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
  }, {
    "name": "X-Amzn-Trace-Id",
    "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
  }, {
    "name": "Accept-Encoding",
    "value": "gzip"
  }, {
    "name": "User-Agent",
    "value": "okhttp/3.12.1"
  }, {
    "name": "cookie",
```

```

      "value": "hoppy=dog;milo=zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE=;aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/bS6YG0CJKAJqaRqDZ140ythKW0Zj9wKB2081SkYDRqf1y0NcVBfo5u0eYi0tvT4rtQCXsu+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
    }],
    "uri": "/CanaryTest",
    "args": "baloo=abc&hoppy-query=xyz&x-hoppy-extra=generic-%3Cwords%3E-in-angle-brackets",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "Fep00F8fIAMEqoQ="
  },
  "labels": [{
    "name": "aws-waf-forwardedip-geo-country:US"
  }, {
    "name": "aws-waf-forwardedip-geo-region:US-VA"
  }]
}

```

所有 Cookie 的資料保護

您可以使用 設定 Cookie 的資料保護SINGLE_HEADER。只會保護 Cookie 值，並排除金鑰名稱。

```

"DataProtectionConfig": {
  "DataProtections": [
    {
      "Field": {
        "FieldType": "SINGLE_HEADER",
        "FieldKeys": ["cookie"]
      },
      "Action": "SUBSTITUTION",
      "ExcludeRuleMatchDetails": false,
      "ExcludeRateBasedDetails": false
    }
  ]
}

```

header 「COOKIE」的範例 DataProtection：具有 Cookie 標頭保護的日誌項目。

Note

Cookie 名稱AWS-WAF-TOKEN超出資料保護的範圍。

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
      "name": "X-Forwarded-For",
      "value": "54.239.98.137"
    }, {
      "name": "X-Forwarded-Proto",
      "value": "https"
    }, {
      "name": "X-Forwarded-Port",
      "value": "443"
    }, {
      "name": "Host",
      "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
      "name": "Accept-Encoding",
      "value": "gzip"
    }, {
      "name": "User-Agent",
      "value": "okhttp/3.12.1"
    }, {
      "name": "cookie",
```

```

      "value": "hoppy=REDACTED;milo=REDACTED;aws-waf-
token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKAJqaRqDZ140ythKW0Zj9wKB2081SkYDRqf1y0NcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
    }],
    "uri": "/CanaryTest",
    "args": "baloo=xyz=&hoppy-query=abc&x-hoppy-extra=abc",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "Fep00F8fIAMEqoQ="
  },
  "labels": [{
    "name": "awswaf:forwardedip:geo:country:US"
  }, {
    "name": "awswaf:forwardedip:geo:region:US-VA"
  }]
}

```

單一查詢引數的資料保護

您可以使用 設定查詢字串的資料保護 `SINGLE_QUERY_ARGUMENT`。這會影響所有查詢引數的索引鍵和值。對於下列範例，原始查詢字串為 `baloo=10 AND 1=1&hoppy=10 AND 1=1&x-hoppy-extra=generic-%3Cwords`。

Webacl 組態

```

"DataProtectionConfig": {
  "DataProtections": [
    {
      "Field": {
        "FieldType": "SINGLE_QUERY_ARGUMENT",
        "FieldKeys": ["hoppy"]
      },
      "Action": "SUBSTITUTION",
      "ExcludeRuleMatchDetails": false,
      "ExcludeRateBasedDetails": false
    }
  ]
}

```

適用於 的範例 `DataProtectionSINGLE_QUERY_ARGUEMENT`：具有「跳躍」查詢字串的日誌項目，以替換保護。

```
{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "ProtectedHoppyQueryArg",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
          "conditionType": "SQL_INJECTION",
          "sensitivityLevel": "HIGH",
          "location": "SINGLE_QUERY_ARG",
          "matchedData": ["REDACTED"],
          "matchedFieldName": "hoppy"
        }
      ]
    },
    {
      "ruleId":
"FullQueryStringInspectionWhichDetectsTheFirstFieldWithSQLi_Baloo_IsAlsoMaskedMasked",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
          "conditionType": "SQL_INJECTION",
          "sensitivityLevel": "HIGH",
          "location": "QUERY_ARGS",
          "matchedData": ["REDACTED"],
        }
      ]
    },
    {
      "ruleId": "ProtectedBalooQueryArg",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
```



```
        "conditionType": "SQL_INJECTION",
        "sensitivityLevel": "HIGH",
        "location": "SINGLE_QUERY_ARG",
        "matchedData": [ "10", "AND", "1" ],
        "matchedFieldName": "baloo"
    ]}
],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
        "name": "X-Forwarded-For",
        "value": "54.239.98.137"
    }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
    }, {
        "name": "X-Forwarded-Port",
        "value": "443"
    }, {
        "name": "Host",
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
        "name": "Accept-Encoding",
        "value": "gzip"
    }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
    }],
    "uri": "/CanaryTest",
    "args": "baloo=10 AND 1=1&hoppy=REDACTED&x-hoppy-extra=generic-%3Cwords",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "Fep00F8fIAMEqoQ="
},
"labels": [{
    "name": "awsfaf:forwardedip:geo:country:US"
}, {
```

```

    "name": "awswaf:forwardedip:geo:region:US-VA"
  }]
}
```

查詢字串的資料保護

您可以使用 設定查詢字串的資料保護QUERY_STRING。這會影響所有查詢引數的索引鍵和值。針對下列範例，原始查詢字串為 baloo=10 AND 1=1&hoppy-query=10 AND 1=1&x-hoppy-extra=generic-%3Cwords。

Webacl 組態

```

"DataProtectionConfig": {
  "DataProtections": [
    {
      "Field": {
        "FieldType": "QUERY_STRING"
      },
      "Action": "SUBSTITUTION",
      "ExcludeRuleMatchDetails": false,
      "ExcludeRateBasedDetails": false
    }
  ]
}
```

的範例 DataProtection for QUERY_STRING：具有以替換保護之查詢字串的日誌項目。

```

{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "ProtectedHoppyQueryArg",
```

```
    "action": "COUNT",
    "ruleMatchDetails": [
      {
        "conditionType": "SQL_INJECTION",
        "sensitivityLevel": "HIGH",
        "location": "QUERY_STRING",
        "matchedData": ["REDACTED"]
      }
    ],
    {
      "ruleId": "ProtectedBalooQueryArg",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
          "conditionType": "SQL_INJECTION",
          "sensitivityLevel": "HIGH",
          "location": "SINGLE_QUERY_ARG",
          "matchedData": [ "REDACTED" ],
          "matchedFieldName": "REDACTED"
        }
      ]
    }
  ],
  "requestHeadersInserted": null,
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
      "name": "X-Forwarded-For",
      "value": "54.239.98.137"
    }, {
      "name": "X-Forwarded-Proto",
      "value": "https"
    }, {
      "name": "X-Forwarded-Port",
      "value": "443"
    }, {
      "name": "Host",
      "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
      "name": "Accept-Encoding",
```

```
        "value": "gzip"
      }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
      }],
      "uri": "/CanaryTest",
      "args": "REDACTED",
      "httpVersion": "HTTP/1.1",
      "httpMethod": "GET",
      "requestId": "Fep00F8fIAMEqoQ="
    },
    "labels": [{
      "name": "awsawaf:forwardedip:geo:country:US"
    }, {
      "name": "awsawaf:forwardedip:geo:region:US-VA"
    }]
  }
}
```

多個查詢引數的資料保護

您可以使用 設定個別查詢 args 的資料保護SINGLE_QUERY_ARGUMENT。報告本機資訊時，我們使用本機保護。不過，查詢字串和 Cookie 標頭中相符的字串有許多可以套用的保護組態。為了簡化，RuleMatchDetails會套用最嚴格的 保護，即使它未與符合的特定資料範圍重疊。

針對下列範例，原始查詢字串為 baloo=is_a_good_boy&hoppy=likes_to_sleep&x-hoppy-extra=10 AND 1=1。

```
"DataProtectionConfig": {
  "DataProtections": [
    {
      "Field": {
        "FieldType": "SINGLE_QUERY_ARGUMENT",
        "FieldKeys": ["hoppy"]
      },
      "Action": "SUBSTITUTION",
      "ExcludeRuleMatchDetails": false,
      "ExcludeRateBasedDetails": false
    },
    {
      "Field": {
        "FieldType": "SINGLE_QUERY_ARGUMENT",
        "FieldKeys": ["baloo"]
      },
    },
  ]
}
```

```

        "Action": "HASH",
        "ExcludeRuleMatchDetails": false,
        "ExcludeRateBasedDetails": false
    }
]
}

```

多個查詢引數的範例 DataProtection。

```

{
  "timestamp": 1738705092889,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "746533260405:xt7v59bhn7:ABC",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "ProtectedHoppyQueryArg",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
          "conditionType": "SQL_INJECTION",
          "sensitivityLevel": "HIGH",
          "location": "SINGLE_QUERY_ARG",
          "matchedData": ["REDACTED"],
          "matchedFieldName": "hoppy"
        }
      ]
    },
    {
      "ruleId": "ProtectedBalooQueryArg",
      "action": "COUNT",
      "ruleMatchDetails": [
        {
          "conditionType": "SQL_INJECTION",
          "sensitivityLevel": "HIGH",
          "location": "SINGLE_QUERY_ARG",

```

```
        "matchedData": ["zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="],
        "matchedFieldName": "baloo"
    }]
},
{
    "ruleId": "FullQueryStringDetects_x-hoppy-extra_IsSubstituted",
    "action": "COUNT",
    "ruleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "QUERY_ARGS",
            "matchedData": ["REDACTED"], // Harshet of Protection Config
        }
    ]
}
],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
        "name": "X-Forwarded-For",
        "value": "54.239.98.137"
    }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
    }, {
        "name": "X-Forwarded-Port",
        "value": "443"
    }, {
        "name": "Host",
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
        "name": "Accept-Encoding",
        "value": "gzip"
    }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
    }
    ],
    "uri": "/CanaryTest",
```

```
    "args": "baloo=zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE=&hoppy=REDACTED&x-hoppy-extra=10 AND 1=1",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "Fep00F8fIAMEqoQ="
  },
  "labels": [{
    "name": "awsaf:forwardedip:geo:country:US"
  }, {
    "name": "awsaf:forwardedip:geo:region:US-VA"
  }]
}
```

Note

您無法在相同的 webACL 中同時指定 QueryString 遮罩和單一查詢 Arg 遮罩。

設定保護套件或 Web ACL 的資料保護

本節提供設定保護套件或 Web ACL 資料保護的說明。

設定保護套件或 Web ACL 的資料保護

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇保護套件或 Web ACLs。
3. 選擇您要為其啟用資料保護的保護套件或 Web ACL 名稱。主控台會帶您前往保護套件或 Web ACL 的描述，您可以在其中編輯它。
4. 在記錄和指標索引標籤的資料保護設定窗格中，選擇啟用或停用。
5. 選擇範圍全域，然後進行欄位資料保護選擇。對於每個欄位資料保護組態，您也可以指定要從保護行為中排除的例外狀況。
6. 完成選擇後，請選擇儲存。界面會返回記錄和指標索引標籤，其中會摘要您的選擇。

測試和調校您的 AWS WAF 保護

本節提供測試和調校 AWS WAF 保護套件或 Web ACLs、規則、規則群組、IP 集和 regex 模式集的指引。

建議您在將 AWS WAF 保護套件或 Web ACL 的任何變更套用至網站或 Web 應用程式流量之前，先進行測試和調校。

生產流量風險

在部署生產流量的保護套件或 Web ACL 實作之前，請在預備或測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。然後，使用生產流量在計數模式中測試和調校規則，然後再啟用它們。

本節也提供一般指引，以測試您使用由其他人管理的規則群組。其中包括 AWS 受管規則規則群組、AWS Marketplace 受管規則群組，以及另一個帳戶與您共用的規則群組。對於這些規則群組，也請遵循您從規則群組提供者取得的任何指引。

- 如需 Bot Control AWS 受管規則規則群組，另請參閱 [測試和部署 AWS WAF 機器人控制](#)。
- 如需帳戶接管預防 AWS 受管規則規則群組，另請參閱 [測試和部署 ATP](#)。
- 如需帳戶建立詐騙預防 AWS 受管規則規則群組，另請參閱 [測試和部署 ACFP](#)。

更新期間的暫時性不一致

當您建立或變更保護套件或 Web ACL 或其他 AWS WAF 資源時，變更會花費少量的時間傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。

以下是您在變更傳播期間可能注意到的暫時不一致的範例：

- 建立保護套件或 Web ACL 之後，如果您嘗試將保護套件或 Web ACL 與資源建立關聯，您可能會收到例外狀況，指出保護套件或 Web ACL 無法使用。
- 將規則群組新增至保護套件或 Web ACL 之後，新的規則群組規則可能會在使用保護套件或 Web ACL 的一個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，在其他地方看到新動作。
- 將 IP 地址新增至封鎖規則中使用的 IP 集後，新的地址可能會在某個區域中遭到封鎖，同時仍允許在另一個區域中封鎖。

測試和調校高階步驟

本節提供測試 Web ACL 變更的步驟檢查清單，包括其使用的任何規則或規則群組。

 Note

若要遵循本節中的指引，您需要了解如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組等保護。本指南稍早章節會介紹該資訊。

測試和調校您的保護套件或 Web ACL

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 準備進行測試

準備您的監控環境，將新的 AWS WAF 保護切換到計數模式進行測試，並建立您需要的任何資源關聯。

請參閱 [準備測試您的 AWS WAF 保護](#)。

2. 在測試和生產環境中監控和調校

先在測試或預備環境中監控和調整您的 AWS WAF 保護，然後在生產環境中監控和調整保護，直到您對它們可以根據需要處理流量感到滿意為止。

請參閱 [監控和調校您的 AWS WAF 保護](#)。

3. 在生產環境中啟用您的保護

當您對測試保護感到滿意時，請將它們切換到生產模式、清除任何不必要的測試成品，然後繼續監控。

請參閱 [在生產環境中啟用您的保護](#)。

完成實作變更後，請繼續監控您的 Web 流量和生產環境中的保護，以確保它們如預期般運作。Web 流量模式可能會隨著時間而變更，因此您可能需要偶爾調整保護。

準備測試您的 AWS WAF 保護

本節說明如何設定來測試和調校您的 AWS WAF 保護。

 Note

若要遵循本節中的指引，您需要大致了解如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組等保護。本指南先前章節會介紹該資訊。

準備進行測試

1. 啟用保護套件或 Web ACL 記錄、Amazon CloudWatch 指標，以及保護套件或 Web ACL 的 Web 請求取樣

使用記錄、指標和抽樣來監控保護套件或 Web ACL 規則與 Web 流量的互動。

- 記錄 – 您可以設定 AWS WAF 來記錄保護套件或 Web ACL 評估的 Web 請求。您可以將日誌傳送至 CloudWatch 日誌、Amazon S3 儲存貯體或 Amazon Data Firehose 交付串流。您可以編輯欄位並套用篩選。如需詳細資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
- Amazon Security Lake – 您可以設定 Security Lake 來收集保護套件或 Web ACL 資料。Security Lake 會從各種來源收集日誌和事件資料，以進行標準化、分析和管理。如需此選項的相關資訊，請參閱《[Amazon Security Lake 使用者指南](#)》中的什麼是 Amazon Security Lake？以及[從 AWS 服務收集資料](#)。
- Amazon CloudWatch 指標 – 在保護套件或 Web ACL 組態中，為您要監控的所有項目提供指標規格。您可以透過 AWS WAF 和 CloudWatch 主控台檢視指標。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。
- Web 請求取樣 – 您可以檢視保護套件或 Web ACL 評估的所有 Web 請求範例。如需 Web 請求取樣的資訊，請參閱[檢視 Web 請求的範例](#)。

2. 將您的保護設定為 Count 模式

在保護套件或 Web ACL 組態中，將您要測試的任何項目切換為計數模式。這會導致測試保護針對 Web 請求記錄相符項目，而不會改變請求的處理方式。您將能夠在指標、日誌和抽樣請求中看到相符項目，以驗證相符條件並了解對 Web 流量的影響。將標籤新增至相符請求的規則，無論規則動作為何，都會新增標籤。

- 保護套件或 Web ACL 中定義的規則 – 編輯保護套件或 Web ACL 中的規則，並將其動作設定為 Count。
- 規則群組 – 在保護套件或 Web ACL 組態中，編輯規則群組的規則陳述式，然後在規則窗格中開啟覆寫所有規則動作下拉式清單，然後選擇 Count。如果您在 JSON 中管理保護套件或 Web ACL，請將規則新增至規則群組參考陳述式中的 RuleActionOverrides 設定，並將

ActionToUse 設定為 Count。下列範例清單顯示 AWSManagedRulesAnonymousIpList AWS 受管規則規則群組中兩個規則的覆寫。

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
  "RuleActionOverrides": [
    {
      "ActionToUse": {
        "Count": {}
      },
      "Name": "AnonymousIpList"
    },
    {
      "ActionToUse": {
        "Count": {}
      },
      "Name": "HostingProviderIpList"
    }
  ],
  "ExcludedRules": []
}
```

如需規則動作覆寫的詳細資訊，請參閱 [覆寫規則群組中的規則動作](#)。

對於您自己的規則群組，請勿修改規則群組本身中的規則動作。具有 Count 動作的規則群組規則不會產生測試所需的指標或其他成品。此外，變更規則群組會影響使用規則群組的所有保護套件或 Web ACLs，而保護套件或 Web ACL 組態內的變更只會影響單一保護套件或 Web ACL。

- 保護套件或 Web ACL – 如果您要測試新的保護套件或 Web ACL，請將保護套件或 Web ACL 的預設動作設定為允許請求。這可讓您試用 Web ACL，而不會以任何方式影響流量。

一般而言，計數模式會產生比生產更多的相符項目。這是因為計數請求的規則不會停止保護套件或 Web ACL 對請求的評估，因此稍後在保護套件或 Web ACL 中執行的規則也可能符合請求。當您將規則動作變更為其生產設定時，允許或封鎖請求的規則會終止其相符請求的評估。因此，相符的請求通常會由保護套件或 Web ACL 中的較少規則進行檢查。如需規則動作對 Web 請求整體評估之影響的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

使用這些設定，您的新保護不會改變 Web 流量，但會在指標、保護套件或 Web ACL 日誌中產生相符資訊，並請求範例。

3. 將保護套件或 Web ACL 與資源建立關聯

如果保護套件或 Web ACL 尚未與資源建立關聯，請建立關聯。

請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。

您現在可以監控和調整您的保護套件或 Web ACL。

監控和調校您的 AWS WAF 保護

監控和調整您的 AWS WAF 保護。

Note

若要遵循本節中的指引，您需要大致了解如何建立和管理 AWS WAF 保護套件或 Web ACLs、規則和規則群組等保護。本指南先前章節會介紹該資訊。

監控 Web 流量和規則相符項目，以驗證保護套件或 Web ACL 的行為。如果您發現問題，請調整您的規則以更正，然後監控以驗證調整。

重複下列程序，直到保護套件或 Web ACL 視需要管理您的 Web 流量為止。

監控和調校

1. 監控流量和規則相符項目

請確定流量正在流動，而且您的測試規則正在尋找相符的請求。

尋找以下資訊，了解您正在測試的保護：

- 日誌 – 存取符合 Web 請求之規則的相關資訊：
 - 您的規則 - 保護套件或 Web ACL 中具有 Count 動作的規則會列在 `nonTerminatingMatchingRules`。具有 Allow 或 Block 的規則會列為 `terminatingRule`。具有 CAPTCHA 或 Challenge 的規則可以終止或非終止，因此會根據規則比對的結果，列在兩個類別的其中之一。
 - 規則群組 - 在 `ruleGroupId` 欄位中識別規則群組，其規則比對的分類方式與獨立規則相同。
 - 標籤 - 規則已套用至請求的標籤會列在 `Labels` 欄位中。

如需詳細資訊，請參閱[保護套件或 Web ACL 流量的日誌欄位](#)。

- Amazon CloudWatch 指標 – 您可以存取以下用於保護套件或 Web ACL 請求評估的指標。
 - 您的規則 – 指標會依規則動作分組。例如，當您在 Count 模式下測試規則時，其相符項目會列為保護套件或 Web ACL 的 Count 指標。
 - 您的規則群組 – 規則群組的指標會列在規則群組指標下。
 - 另一個帳戶擁有的規則群組 – 規則群組指標通常只有規則群組擁有者可以看到。不過，如果您覆寫規則的規則動作，則該規則的指標會列在您的保護套件或 Web ACL 指標下。此外，任何規則群組新增的標籤都會列在您的保護套件或 Web ACL 指標中。

此類別中的規則群組是 [AWS 的受管規則 AWS WAF](#)、[辨識其他服務提供的規則群組](#)、[AWS Marketplace 規則群組](#) 和規則群組，這些群組由另一個帳戶與您共用。

- 標籤 – 在評估期間新增至 Web 請求的標籤會列在保護套件或 Web ACL 標籤指標中。您可以存取所有標籤的指標，無論它們是由您的規則和規則群組新增，還是由另一個帳戶擁有的規則群組中的規則新增。

如需詳細資訊，請參閱[檢視 Web ACL 的指標](#)。

- 保護套件或 Web ACL 流量概觀儀表板 – 存取保護套件或 Web ACL 已評估的 Web 流量摘要，方法是前往 AWS WAF 主控台內的保護套件或 Web ACL 頁面，並開啟流量概觀索引標籤。

流量概觀儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集。

如需詳細資訊，請參閱[保護套件或 Web ACLs 流量概觀儀表板](#)。

- 抽樣 Web 請求 – 存取符合 Web 請求抽樣之規則的資訊。範例資訊會依保護套件或 Web ACL 中規則的指標名稱來識別相符的規則。對於規則群組，指標會識別規則群組參考陳述式。對於規則群組內的規則，範例會列出相符的規則名稱 RuleWithinRuleGroup。

如需詳細資訊，請參閱[檢視 Web 請求的範例](#)。

2. 設定緩解措施以解決誤判

如果您判斷規則正在產生誤報，則透過比對不應該產生的 Web 請求，下列選項可協助您調整保護套件或 Web ACL 保護以緩解錯誤。

更正規則檢查條件

對於您自己的規則，您通常只需要調整您用來檢查 Web 請求的設定。範例包括變更規則運算式模式集中的規格、調整您在檢查之前套用至請求元件的文字轉換，或使用轉送的 IP 地址切換到。請參閱 [下導致問題的規則類型指引](#) [在中使用規則陳述式 AWS WAF](#)。

修正更複雜的問題

對於您無法控制的檢查條件和某些複雜的規則，您可能需要進行其他變更，例如新增明確允許或封鎖請求的規則，或消除有問題規則評估的請求。受管規則群組通常需要這種類型的緩解措施，但其他規則也可能需要。範例包括速率型規則陳述式和 SQL Injection 攻擊規則陳述式。

如何緩解誤報取決於您的使用案例。以下是常見的方法：

- 新增緩解規則 – 新增在新規則之前執行的規則，並明確允許導致誤報的請求。如需 Web ACL 中規則評估順序的資訊，請參閱 [設定規則優先順序](#)。

透過此方法，允許的請求會傳送至受保護的資源，因此永遠不會到達新規則進行評估。如果新規則就是付費的受管規則群組，此方法也可以協助包含使用規則群組的成本。

- 新增具有緩解規則的邏輯規則 – 使用邏輯規則陳述式將新規則與排除誤報的規則結合。如需相關資訊，請參閱 [在中使用邏輯規則陳述式 AWS WAF](#)。

例如，假設您正在新增 SQL Injection 攻擊比對陳述式，該陳述式會為某個類別的請求產生誤報。建立符合這些請求的規則，然後使用邏輯規則陳述式合併規則，以便僅在不符合誤報條件且確實符合 SQL Injection 攻擊條件的請求上進行比對。

- 新增縮小範圍陳述式 – 對於以速率為基礎的陳述式和受管規則群組參考陳述式，透過在主要陳述式中新增縮小範圍陳述式，排除導致誤報的請求。

不符合範圍縮小陳述式的請求絕不會達到規則群組或速率型評估。如需縮小範圍陳述式的資訊，請參閱 [在中使用縮小範圍陳述式 AWS WAF](#)。如需範例，請參閱「[從機器人管理排除 IP 範圍](#)」。

- 新增標籤比對規則 – 對於使用標籤的規則群組，請識別有問題規則套用至請求的標籤。如果您尚未這麼做，您可能需要先在計數模式中設定規則群組規則。新增標籤比對規則，定位為在規則群組之後執行，比對有問題的規則所新增的標籤。在標籤比對規則中，您可以從要封鎖的請求中篩選要允許的請求。

如果您使用此方法，在完成測試時，請將有問題的規則保留在規則群組中的計數模式中，並保留您的自訂標籤比對規則。如需標籤比對陳述式的詳細資訊，請參閱 [標籤比對規則陳述式](#)。如需範例，請參閱 [允許特定封鎖的機器人](#) 和 [ATP 範例：針對遺失和遭入侵的登入資料進行自訂處理](#)。

- 變更受管規則群組的版本 – 對於版本控制的受管規則群組，請變更您正在使用的版本。例如，您可以切換回您成功使用的最後一個靜態版本。

這通常是暫時修正。當您在測試或預備環境中繼續測試最新版本，或是等待供應商提供更相容的版本時，您可以變更生產流量的版本。如需受管規則群組版本的資訊，請參閱 [在中使用受管規則群組 AWS WAF](#)。

當您確定新規則符合所需的請求時，請移至測試的下一個階段並重複此程序。在生產環境中執行測試和調校的最後階段。

檢視 Web ACL 的指標

本節說明如何檢視保護套件或 Web ACL 的指標。

將保護套件或 Web ACL 與一或多個 AWS 資源建立關聯後，您可以在 Amazon CloudWatch 圖表中檢視關聯的產生指標。

如需 AWS WAF 指標的相關資訊，請參閱 [AWS WAF 指標和維度](#)。如需 CloudWatch 指標的相關資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》。

對於保護套件或 Web ACL 中的每個規則，以及關聯資源 AWS WAF 針對保護套件或 Web ACL 轉送的所有請求，CloudWatch 可讓您執行下列動作：

- 檢視前一小時或前三小時的資料。
- 變更資料點之間的間隔。
- 變更 CloudWatch 對資料執行的計算，例如最大值、最小值、平均值或總和。

Note

AWS WAF 使用 CloudFront 是一項全域服務，且指標只有在您於中選擇美國東部（維吉尼亞北部）區域時才能使用 AWS Management Console。如果您選擇其他區域，CloudWatch 主控台中不會顯示任何 AWS WAF 指標。

檢視保護套件或 Web ACL 中規則的資料

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。

2. 如有必要，請將區域變更為 AWS 資源所在的區域。針對 CloudFront，選擇美國東部（維吉尼亞北部）區域。
3. 在導覽窗格的指標下，選擇所有指標，然後在 的瀏覽索引標籤下搜尋AWS::WAFV2。
4. 選取您要檢視資料的保護套件或 Web ACL 的核取方塊。
5. 變更適用的設定：

統計數字

選擇 CloudWatch 對資料執行的計算。

時間範圍

選擇您想要檢視前一小時或前三個小時的資料。

期間

選擇圖形中資料點之間的間隔。

規則

選擇您要檢視資料的規則。

Note

如果您變更規則的名稱，並且希望規則的指標名稱反映變更，則也必須更新指標名稱。當您變更規則名稱時 AWS WAF，不會自動更新規則的指標名稱。您可以使用規則 JSON 編輯器，在主控台中編輯規則時變更指標名稱。您也可以透過 APIs 和用於定義保護套件或 Web ACL 或規則群組的任何 JSON 清單中變更這兩個名稱。

注意下列事項：

- 如果您最近將保護套件或 Web ACL 與 AWS 資源建立關聯，您可能需要等待幾分鐘，資料才會出現在圖形中，保護套件或 Web ACL 的指標才會出現在可用指標清單中。
- 如果您將多個資源與保護套件或 Web ACL 建立關聯，CloudWatch 資料將包含所有資源的請求。
- 您可以將游標暫留在資料點上，以取得詳細資訊。
- 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理



圖示。

如需 CloudWatch 指標的詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。

保護套件或 Web ACLs 流量概觀儀表板

本節說明 AWS WAF 主控台中的保護套件或 Web ACL 流量概觀儀表板。將保護套件或 Web ACL 與一個或多個 AWS 資源建立關聯並啟用保護套件或 Web ACL 的指標後，您可以前往 AWS WAF 主控台中的保護套件或 Web ACL 流量概觀索引標籤，存取保護套件或 Web ACL 評估的 Web 流量摘要。儀表板包含近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集。

Note

如果您在儀表板上看不到任何內容，請確定您已為保護套件或 Web ACL 啟用指標。

保護套件或 Web ACL 流量概觀索引標籤包含具有下列資訊類別的標籤式儀表板：

- 最佳安全洞見 – 透過直接查詢 Amazon CloudWatch logs 取得 AWS WAF 的 AWS WAF 保護洞見。儀表板的其餘部分使用 CloudWatch 指標。這些洞見提供更豐富的資訊，但查詢 CloudWatch 日誌會產生額外的成本。如需額外費用的詳細資訊，請參閱[Amazon CloudWatch Logs 定價](#)。
- 所有流量 – 保護套件或 Web ACL 評估的所有 Web 請求。

儀表板著重於終止動作，但您可以在下列位置檢視計數規則的相符項目：

- 此儀表板的前 10 個規則窗格。切換至計數動作以顯示計數規則相符項目。
- 保護套件或 Web ACL 頁面的範例請求索引標籤。此新標籤包含所有規則相符項目的圖形。如需相關資訊，請參閱[檢視 Web 請求的範例](#)。
- 反 DDoS – 保護套件或 Web ACL 使用 AntiDDoSRuleSet 反 DDoS 受管規則群組評估的 Web 請求。

只有在保護套件或 Web ACL 中使用此規則群組時，才能使用此標籤。

- 機器人控制 – 保護套件或 Web ACL 使用 Bot Control 受管規則群組評估的 Web 請求。
- 如果您在保護套件或 Web ACL 中未使用此規則群組，此標籤會顯示根據 Bot Control 規則評估 Web 流量取樣的結果。這可讓您了解應用程式接收的機器人流量，而且免費。

此規則群組是 AWS WAF 提供的智慧型威脅緩解選項的一部分。如需詳細資訊，請參閱[AWS WAF 機器人控制](#)及[AWS WAF 機器人控制規則群組](#)。

- 防止帳戶接管 – 保護套件或 Web ACL 使用 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組評估的 Web 請求。只有在保護套件或 Web ACL 中使用此規則群組時，才能使用此標籤。

ATP 規則群組是智慧型威脅緩解方案的一部分 AWS WAF。如需詳細資訊，請參閱[AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)及[AWS WAF 詐騙控制帳戶接管預防 \(ATP\) 規則群組](#)。

- 防止帳戶建立詐騙 – 保護套件或 Web ACL 使用 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組評估的 Web 請求。只有在保護套件或 Web ACL 中使用此規則群組時，才能使用此標籤。

ACFP 規則群組是智慧型威脅緩解產品的一部分 AWS WAF。如需詳細資訊，請參閱[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)及[AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\) 規則群組](#)。

儀表板是以保護套件或 Web ACL 的 CloudWatch 指標為基礎，而圖表提供 CloudWatch 中對應指標的存取權。對於智慧型威脅緩解儀表板，例如 Bot Control，使用的指標主要是標籤指標。

- 如需 AWS WAF 提供的指標清單，請參閱 [AWS WAF 指標和維度](#)。
- 如需 CloudWatch 指標的相關資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》。

儀表板會針對您選取的終止動作和日期範圍，提供流量模式的摘要。智慧型威脅緩解儀表板包含對應的受管規則群組評估的請求，無論受管規則群組本身是否套用終止動作。例如，如果選取 Block，帳戶接管預防儀表板會包含由 ATP 受管規則群組評估並在保護套件或 Web ACL 評估期間某個時間點封鎖的所有 Web 請求的資訊。ATP 受管規則群組、在保護套件或 Web ACL 中的規則群組之後執行的規則，或保護套件或 Web ACL 預設動作可以封鎖請求。

檢視保護套件或 Web ACL 的儀表板

遵循本節中的程序來存取保護套件或 Web ACL 儀表板，並設定資料篩選條件。如果您最近將保護套件或 Web ACL 與 AWS 資源建立關聯，您可能需要等待幾分鐘，才能在儀表板中使用資料。

儀表板包含您對與保護套件或 Web ACL 相關聯的所有資源的請求。

檢視保護套件或 Web ACL 的流量概觀儀表板

- 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
- 在導覽窗格中，選擇保護套件或 Web ACLs，然後搜尋您感興趣的 Web ACL。
- 選取保護套件或 Web ACL。主控台會帶您前往保護套件或 Web ACL 的頁面。預設會選取流量概觀索引標籤。
- 視需要變更資料篩選條件設定。

- 終止規則動作 – 選取要包含在儀表板中的終止動作。儀表板摘要說明具有保護套件或 Web ACL 評估所套用之所選動作之一的 Web 請求指標。如果您選取所有可用的動作，儀表板會包含所有評估的 Web 請求。如需動作的相關資訊，請參閱 [AWS WAF 如何處理規則和規則群組動作](#)。
- 時間範圍 – 選取要在儀表板中檢視的時間間隔。您可以選擇檢視相對於現在的時間範圍，例如過去 3 小時或上週，而且您可以從行事曆中選取絕對時間範圍。
- 時區 – 當您指定絕對時間範圍時，會套用此設定。您可以使用瀏覽器的本機時區或 UTC（國際標準時間）。

檢閱您感興趣的標籤中的資訊。資料篩選條件選擇會套用至所有儀表板。在圖形窗格中，您可以將游標暫留在資料點或區域上，以查看任何其他詳細資訊。

Count 動作規則

您可以在兩個位置之一檢視計數動作比對的資訊。

- 在此流量概觀索引標籤中，在所有流量儀表板上，尋找前 10 個規則窗格並切換切換切換以計數動作。開啟此切換後，窗格會顯示計數規則比對，而不是終止規則比對。
- 在保護套件或 Web ACL 的取樣請求索引標籤中，查看您在流量概觀索引標籤上設定的時間範圍之所有規則比對和動作的圖表。如需取樣請求索引標籤的相關資訊，請參閱 [檢視 Web 請求的範例](#)。

Amazon CloudWatch 指標

在儀表板圖形窗格中，您可以存取圖形資料的 CloudWatch 指標。選擇圖形窗格頂端的選項，或從窗格內的：（垂直省略號）下拉式選單中選擇。

重新整理儀表板

儀表板不會自動重新整理。若要更新顯示，請選擇重新整理



示。

圖

保護套件或 Web ACLs 的流量概觀儀表板範例

本節顯示保護套件或 Web ACLs 流量概觀儀表板的範例畫面。

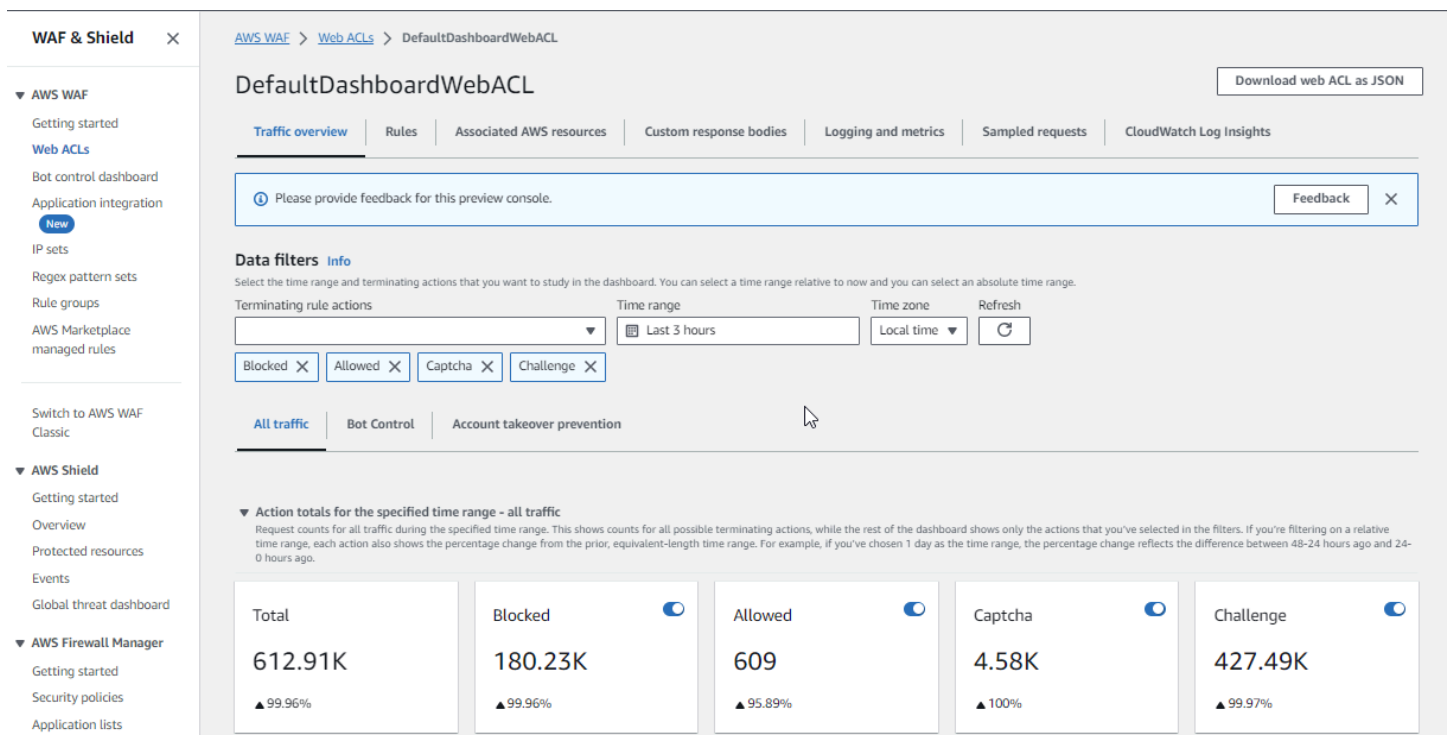
Note

如果您已使用 AWS WAF 來保護應用程式資源，您可以在 AWS WAF 主控台的頁面上查看任何保護套件或 Web ACLs 的儀表板。如需相關資訊，請參閱[檢視保護套件或 Web ACL 的儀表板](#)。

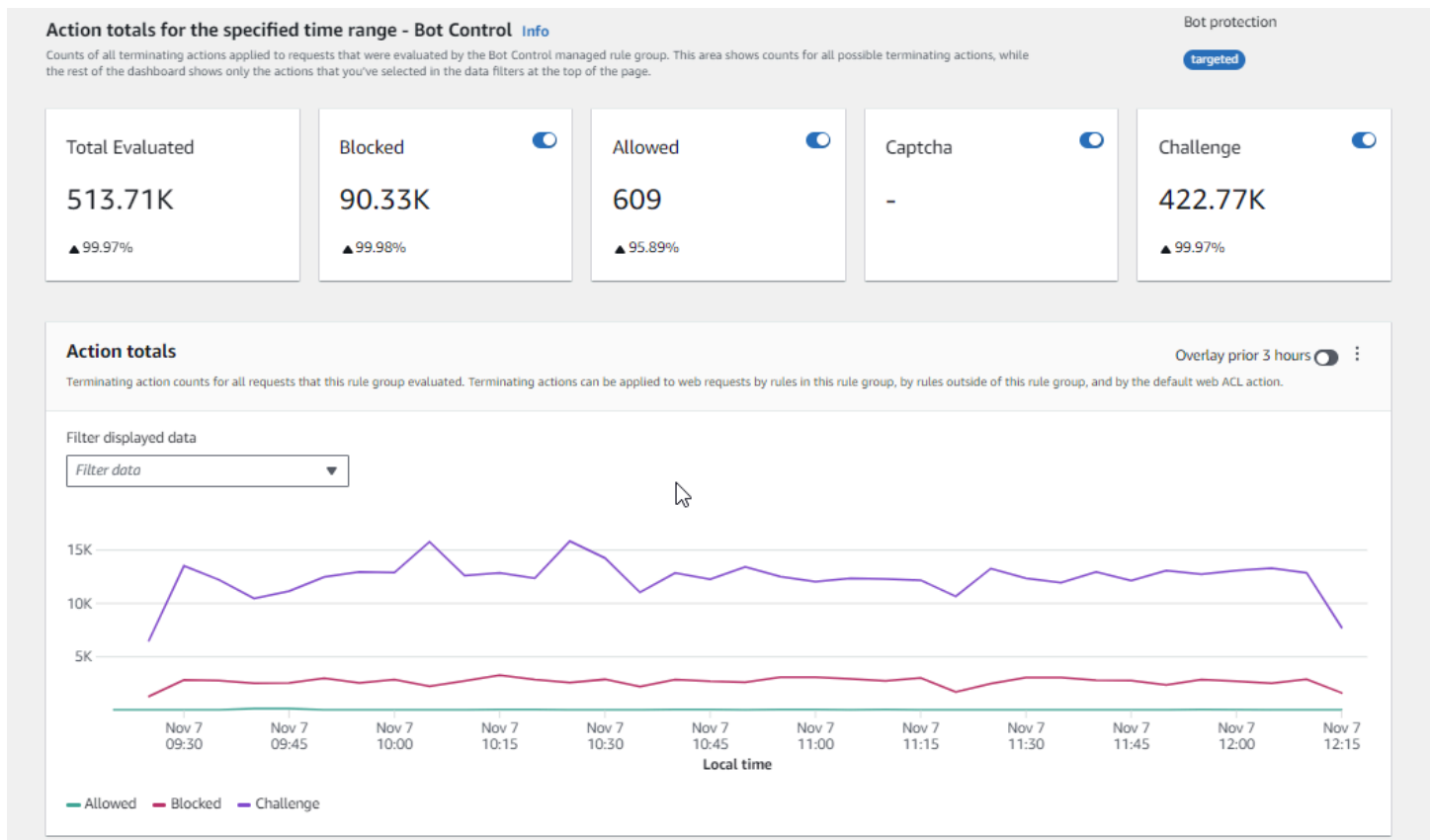
範例畫面：資料篩選條件和所有流量儀表板動作計數

下列螢幕擷取畫面說明已選取所有流量索引標籤的保護套件或 Web ACL 的流量概觀。資料篩選條件設定為預設值：過去三小時內的所有終止動作。

在所有流量儀表板中，是各種終止動作的動作總計。每個窗格都會列出請求計數，並顯示上/下箭頭，指出自前三個小時時間範圍以來的變更。

**範例畫面：Bot Control 儀表板動作計數**

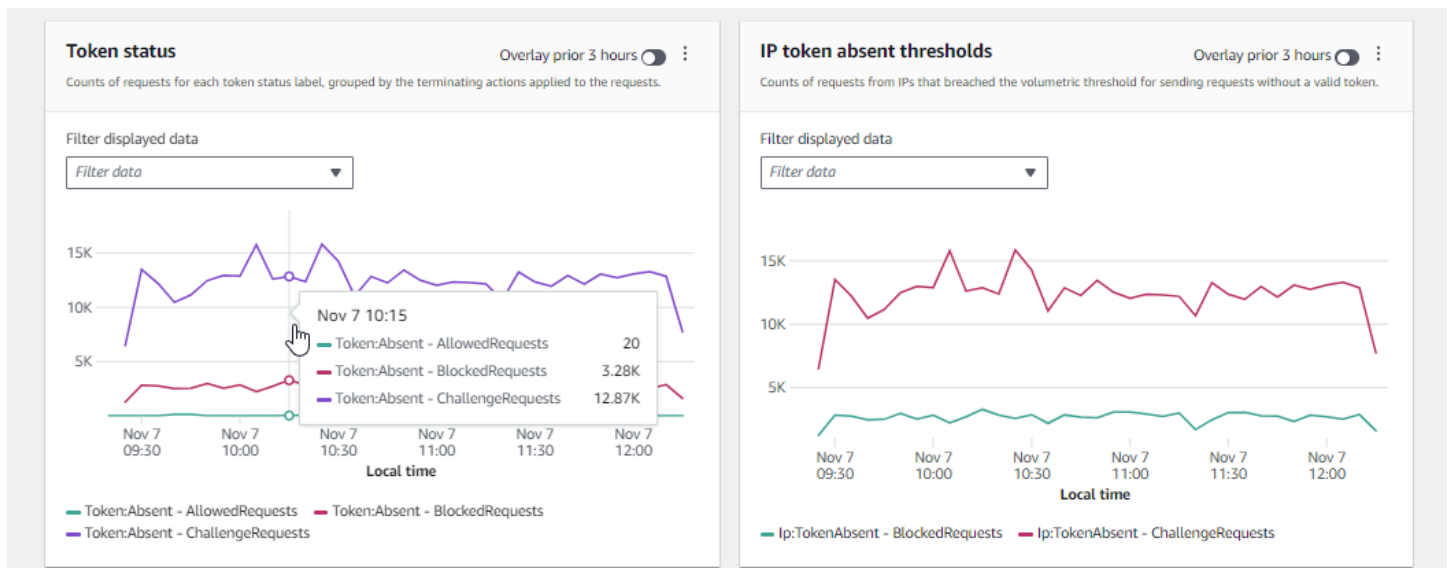
下列螢幕擷取畫面說明 Bot Control 儀表板的動作計數。這會顯示時間範圍的相同總計窗格，但計數僅適用於 Bot Control 規則群組評估的請求。進一步向下，在動作總計窗格中，您可以查看指定三小時時間範圍內的動作計數。在此時間範圍內，CAPTCHA動作不會套用至規則群組評估的任何請求。



範例畫面：Bot Control 儀表板字符狀態摘要圖表

下列螢幕擷取畫面說明 Bot Control 儀表板中提供的兩個摘要圖形。字符狀態窗格會顯示各種字符狀態標籤的計數，並搭配套用至請求的規則動作。IP 字符缺少閾值窗格會顯示來自 IP 的請求資料，這些 IPs 在沒有字符的情況下傳送太多請求。

將滑鼠游標暫留在圖形中的任何區域上，會顯示可用的資訊詳細資訊。在此螢幕擷取畫面中的字符狀態窗格中，滑鼠將游標暫留在某個時間點上，而不在任何圖形行上，因此主控台會顯示該時間點所有行的資料。



本節僅顯示保護套件或 Web ACL 流量概觀儀表板中提供的一些流量摘要。若要查看任何保護套件或 Web ACLs 儀表板，請在 主控台中開啟保護套件或 Web ACL 頁面。如需如何執行此操作的詳細資訊，請參閱 中的指引 [檢視保護套件或 Web ACL 的儀表板](#)。

檢視 Web 請求的範例

本節說明 AWS WAF 主控台內的保護套件或 Web ACL 取樣請求索引標籤。在此索引標籤中，您可以檢視 AWS WAF 已檢查之 Web 請求的所有規則相符項目的圖表。此外，如果您為保護套件或 Web ACL 啟用了請求取樣，您可以查看 AWS WAF 已檢查的 Web 請求範例的資料表檢視。您也可以透過 API 呼叫 擷取取樣的請求資訊 `GetSampledRequests`。

請求範例包含最多 100 個符合保護套件或 Web ACL 中規則條件的請求，以及另外 100 個不符合任何規則且已套用保護套件或 Web ACL 預設動作的請求。範例中的請求來自過去三小時內收到您內容請求的所有受保護資源。

當 Web 請求符合規則中的條件，且該規則的動作不會終止請求評估時，AWS WAF 會使用保護套件或 Web ACL 中的後續規則繼續檢查 Web 請求。因此，Web 請求可能會多次出現。如需規則動作行為的資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

檢視所有規則圖表和抽樣請求

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 在導覽窗格中，選擇保護套件或 Web ACLs。
3. 選擇您要檢視請求的保護套件或 Web ACL 名稱。主控台會帶您前往保護套件或 Web ACL 的描述，您可以在其中編輯它。

4. 在抽樣請求索引標籤中，您可以看到以下內容：

- 所有規則圖表 – 此圖表顯示指定時間範圍內執行的所有 Web 請求評估的相符規則和規則動作。

Note

此圖表的時間範圍是在保護套件或 Web ACL 流量概觀索引標籤的資料篩選條件區段中設定。如需相關資訊，請參閱[檢視保護套件或 Web ACL 的儀表板](#)。

- 取樣請求資料表 – 此資料表會顯示過去 3 小時的取樣請求資料。

Note

如果您沒有看到預期的受管規則群組範例，請參閱此程序下方的一節。

對於每個項目，資料表會顯示下列資料：

指標名稱

符合請求的保護套件或 Web ACL 中規則的 CloudWatch 指標名稱。如果 Web 請求不符合保護套件或 Web ACL 中的任何規則，則此值為預設值。

Note

如果您變更規則的名稱，且希望規則的指標名稱反映變更，則也必須更新指標名稱。AWS WAF 當您變更規則名稱時，不會自動更新規則的指標名稱。您可以使用規則 JSON 編輯器，在主控台中編輯規則時變更指標名稱。您也可以透過 APIs 和您用來定義保護套件或 Web ACL 或規則群組的任何 JSON 清單中變更這兩個名稱。

來源 IP

請求源自的 IP 地址，或者，如果檢視器使用 HTTP 代理或 Application Load Balancer 傳送請求，則為代理或 Application Load Balancer 的 IP 地址。

URI

URL 識別資源的一部分，例如 /images/daily-ad.jpg。

規則群組內的規則

如果指標名稱識別規則群組參考陳述式，這會識別符合請求之規則群組內的規則。

動作

指出對應規則的動作。如需可能規則動作的相關資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

時間

從受保護資源 AWS WAF 收到請求的時間。

若要顯示 Web 請求元件的其他資訊，請在請求資料列中選擇 URI 的名稱。

受管規則群組中規則的取樣請求

在主控台中，只有在沒有動作覆寫或動作覆寫使用最新的覆寫組態設定時，才會對受管規則群組規則提供取樣請求 `RuleActionOverrides`。無法使用主控台來覆寫使用較舊 `ExcludedRules` 設定的規則動作。如果您沒有看到所有預期的受管規則群組請求範例，請檢查您的保護套件或 Web ACL JSON 是否有使用舊版設定的覆寫。您可以從保護套件或 Web ACL 的主控台頁面下載 JSON。

如果您看到較舊的設定，請將它們取代為新的設定，以開始透過主控台提供取樣的請求。您可以透過主控台執行此操作，方法是編輯保護套件或 Web ACL 中的受管規則群組並加以儲存。AWS WAF 會自動將任何較舊的設定取代為 `RuleActionOverrides` 設定，並將規則動作覆寫設定為 `Count`。如需這兩個設定的詳細資訊，請參閱 [JSON 清單：RuleActionOverrides 取代 ExcludedRules](#)。

您可以透過 AWS WAF REST API、SDKs 或命令列，存取具有舊覆寫的規則的取樣請求。如需詳細資訊，請參閱《AWS WAF API 參考》中的 [GetSampledRequests](#)。

以下顯示命令列請求的語法：

```
aws wafv2 get-sampled-requests \
  --web-acl-arn webACL ARN \
  --rule-metric-name Metric name of the rule in the managed rule group \
  --scope=REGIONAL or CLOUDFRONT \
  --time-window StartTime=UTC timestamp,EndTime=UTC timestamp \
  --max-items 100
```

在生產環境中啟用您的保護

本節提供在生產環境中啟用調校保護的說明。

當您在生產環境中完成測試和調校的最後階段時，請在生產模式中啟用您的保護。

生產流量風險

在部署生產流量的保護套件或 Web ACL 實作之前，請在測試環境中進行測試和調校，直到您對流量的潛在影響感到滿意為止。在啟用生產流量的保護之前，也使用您的生產流量在計數模式中進行測試和調校。

Note

若要遵循本節中的指引，您需要大致了解如何建立和管理 AWS WAF 保護，例如保護套件或 Web ACLs、規則和規則群組。本指南稍早章節會介紹該資訊。

請先在測試環境中執行這些步驟，然後在生產環境中執行。

在生產環境中啟用您的 AWS WAF 保護

1. 切換到您的生產保護

更新您的保護套件或 Web ACL，並切換您的生產設定。

a. 移除您不需要的任何測試規則

如果您新增了生產環境中不需要的測試規則，請將其移除。如果您使用任何標籤比對規則來篩選受管規則群組規則的結果，請務必保留這些規則。

b. 切換到生產動作

將新規則的動作設定變更為其預期的生產設定。

- 保護套件或 Web ACL 中定義的規則 – 編輯保護套件或 Web ACL 中的規則，並將其動作從 Count 變更為生產動作。
- 規則群組 – 在規則群組的保護套件或 Web ACL 組態中，根據您的測試和調校活動的結果，切換規則以使用自己的動作或保留其 Count 動作覆寫。如果您使用標籤比對規則來篩選規則群組規則的結果，請務必保留該規則的覆寫。

若要使用規則的動作切換到 `Count`，請在保護套件或 Web ACL 組態中編輯規則群組的規則陳述式，並移除規則的 `Count` 覆寫。如果您在 JSON 中管理保護套件或 Web ACL，請在規則群組參考陳述式中，從 `RuleActionOverrides` 清單中移除規則的項目。

- 保護套件或 Web ACL – 如果您變更了測試的保護套件或 Web ACL 預設動作，請將其切換到其生產設定。

使用這些設定，您的新保護會如預期般管理 Web 流量。

當您儲存保護套件或 Web ACL 時，與之相關聯的資源將使用您的生產設定。

2. 監控和調校

為了確保 Web 請求可依您想要的方式處理，請在啟用新功能後密切監控流量。您將監控生產規則動作的指標和日誌，而不是您在調校工作中監控的計數動作。視需要持續監控和調整行為，以適應 Web 流量的變更。

AWS WAF 搭配 Amazon CloudFront 使用

了解如何 AWS WAF 搭配 Amazon CloudFront 功能使用。

當您建立保護套件或 Web ACL 時，您可以指定要檢查的 AWS WAF 一或多個 CloudFront 分佈。CloudFront 支援兩種分佈類型：保護個別租用戶的標準分佈，以及透過單一共用組態範本保護多個租用戶的多租用戶分佈。會根據您在保護套件或 Web ACLs 中定義的規則來 AWS WAF 檢查兩種分佈類型的 Web 請求，每種類型都有不同的實作模式。

主題

- [AWS WAF 如何使用不同的分佈類型](#)
- [使用 保護 CloudFront 分佈的常見使用案例 AWS WAF](#)

AWS WAF 如何使用不同的分佈類型

分佈類型

AWS WAF 為標準和多租用戶分佈 CloudFront 分佈提供 Web 應用程式防火牆功能。

標準分佈

對於標準分佈，會為每個分佈使用單一保護套件或 Web ACL AWS WAF 新增保護。您可以透過將現有的保護套件或 Web ACL 與 CloudFront 分佈建立關聯，或在 CloudFront 主控台中使用一鍵式保護來啟用此保護。這可讓您獨立管理每個分發的安全控制，因為保護套件或 Web ACL 的任何變更只會影響與其相關聯的分發。

這種保護 CloudFront 分佈的直接方法最適合為個別網域提供來自單一保護套件或 Web ACL 的特定保護。

標準分佈考量

- 保護套件或 Web ACL 的變更只會影響其關聯的分佈
- 每個分佈都需要獨立的保護套件或 Web ACL 組態
- 規則和規則群組會針對每個分佈分別管理

多租戶分佈

對於多租戶分佈，會使用單一保護套件或 Web ACL 在多個網域中 AWS WAF 新增保護。由多租用戶分佈管理的網域稱為分佈租用戶。您只能在多租用戶分佈建立程序期間或之後，在 CloudFront 主控台中啟用多租用戶分佈的 AWS WAF 保護。不過，保護套件或 Web ACL 的變更仍會透過 AWS WAF 主控台或 API 進行管理。

多租戶分佈提供在兩個層級啟用 AWS WAF 保護的彈性：

- 多租戶分佈層級 – 關聯的保護套件或 Web ACLs 提供基準安全控制，適用於共用該分佈的所有應用程式
- 分佈租用戶層級 – 多租用戶分佈中的個別租用戶可以擁有自己的保護套件或 Web ACLs 以實作額外的安全控制或覆寫多租用戶分佈設定

這兩個層使多租戶分佈最適合跨多個網域共用 AWS WAF 保護，而不會失去為個別分佈自訂安全性的能力。

多租戶分佈考量

- 個別分佈租用戶會繼承對與相關多租用戶分佈相關聯的保護套件或 Web ACLs 所做的變更
- 與特定分發租用戶相關聯的保護套件或 Web ACLs 可以覆寫在多租用戶保護套件或 Web ACL 層級設定的設定
- 受管規則群組可以在分佈和分佈租用戶層級實作

- 應用程式識別符可以位於日誌中，以依分佈追蹤安全事件

AWS WAF 依分佈類型的 功能

比較保護套件或 Web ACL 實作

AWS WAF 功能	標準分佈	多租戶分佈
關聯保護套件或 Web ACLs	每個分佈一個保護套件或 Web ACL	您可以使用選用的租用戶特定保護套件或 Web ACLs，跨租用戶共用保護套件或 Web ACLs
規則管理	規則會影響單一分佈	多租用戶分佈規則會影響所有相關租用戶；分佈租用戶特定規則只會影響該租用戶
受管規則群組	套用至個別分佈	可套用至所有租用戶的多租用戶分佈層級，或套用至特定應用程式的租用戶層級
日誌	標準 AWS WAF 日誌	日誌包含安全事件屬性的租用戶識別符

使用 保護 CloudFront 分佈的常見使用案例 AWS WAF

下列 AWS WAF 功能對所有 CloudFront 分佈的運作方式相同。多租戶分佈的考量事項會列在每個功能案例之後。

使用 AWS WAF 搭配 CloudFront 自訂錯誤頁面

根據預設，當根據您指定的條件 AWS WAF 封鎖 Web 請求時，它會將 HTTP 狀態碼傳回 403 (Forbidden) CloudFront，而 CloudFront 會將該狀態碼傳回給檢視器。然後，檢視器會顯示簡短且稀疏格式的預設訊息，如下所示：

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

您可以透過定義自訂回應來覆寫 AWS WAF 保護套件或 Web ACL 規則中的此行為。如需使用 AWS WAF 規則自訂回應行為的詳細資訊，請參閱 [傳送 Block 動作的自訂回應](#)。

Note

您使用 AWS WAF 規則自訂的回應優先於您在 CloudFront 自訂錯誤頁面中定義的任何回應規格。

如果您寧願透過 CloudFront 顯示自訂錯誤訊息，可能使用與網站其他部分相同的格式，您可以設定 CloudFront 將包含自訂錯誤訊息的物件（例如 HTML 檔案）傳回給檢視器。

Note

CloudFront 無法區分原始伺服器傳回的 HTTP 狀態碼 403，以及封鎖請求 AWS WAF 時傳回的狀態碼 403。這表示您無法根據不同原因導致 HTTP 狀態碼 403 而傳回不同的自訂錯誤頁面。

如需 CloudFront 自訂錯誤頁面的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[產生自訂錯誤回應](#)。

多租戶分佈中的自訂錯誤頁面

對於 CloudFront 多租用戶分佈，您可以透過下列方式設定自訂錯誤頁面：

- 在多租用戶層級 - 這些設定適用於使用多租用戶分佈範本的所有租用戶分佈
- 透過 AWS WAF 規則 - 保護套件或 Web ACLs 中定義的自訂回應優先於多租用戶分佈和租用戶層級自訂錯誤頁面

針對在您自己的 HTTP 伺服器上執行的應用程式，使用 AWS WAF 搭配 CloudFront

當您 AWS WAF 搭配 CloudFront 使用時，您可以保護在任何 HTTP Web 伺服器上執行的應用程式，無論是在 Amazon Elastic Compute Cloud (Amazon EC2) 中執行的 Web 伺服器，還是您私下管理的 Web 伺服器。您也可以將 CloudFront 設定為在 CloudFront 與您自己的 Web 伺服器之間，以及檢視器與 CloudFront 之間需要 HTTPS。

CloudFront 和您自己的 Web 伺服器之間需要 HTTPS

若要在 CloudFront 和您自己的 Web 伺服器之間要求 HTTPS，您可以使用 CloudFront 自訂原始伺服器功能，並為特定原始伺服器設定原始伺服器通訊協定政策和原始伺服器網域名稱設定。在 CloudFront 組態中，您可以指定伺服器的 DNS 名稱，以及您希望 CloudFront 從原始伺服器擷取物

件時使用的連接埠和通訊協定。您也應該確保自訂原始伺服器上的 SSL/TLS 憑證符合您設定的原始網域名稱。當您在外部使用自己的 HTTP Web 伺服器時 AWS，您必須使用由信任的第三方憑證授權機構 (CA) 簽署的憑證，例如 Comodo、DigiCert 或 Symantec。如需有關在 CloudFront 與您自己的 Web 伺服器之間需要 HTTPS 通訊的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[在 CloudFront 與自訂原始伺服器之間需要 HTTPS 通訊](#)的主題。

在檢視器和 CloudFront 之間需要 HTTPS

若要在檢視器和 CloudFront 之間要求 HTTPS，您可以變更 CloudFront 分佈中一或多個快取行為的檢視器通訊協定政策。如需在檢視器和 CloudFront 之間使用 HTTPS 的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的在[檢視器和 CloudFront 之間通訊需要 HTTPS](#)的主題。您也可以使用自己的 SSL 憑證，讓檢視器可以使用您自己的網域名稱透過 HTTPS 連線至 CloudFront 分佈，例如 <https://www.mysite.com>。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[設定替代網域名稱和 HTTPS](#) 主題。

對於多租戶分佈，HTTP 方法組態遵循以下階層：

- 範本層級設定會定義所有租用戶分佈允許的基準 HTTP 方法
- 租戶分佈可以覆寫這些設定以：
 - 允許比多租戶分佈更少的方法（使用 AWS WAF 規則來封鎖其他方法）
 - 如果多租用戶分佈設定為支援它們，則允許使用更多方法
- AWS WAF 無論 CloudFront 組態為何，多租戶分佈和租戶層級的規則都可以進一步限制 HTTP 方法

選擇 CloudFront 回應的 HTTP 方法

當您建立 Amazon CloudFront Web 分佈時，您可以選擇您希望 CloudFront 處理並轉送至原始伺服器的 HTTP 方法。您可以從下列選項來選擇：

- **GET，HEAD** – 您只能使用 CloudFront 從您的原始伺服器取得物件或取得物件標頭。
- **GET、HEAD、OPTIONS** – 您只能使用 CloudFront 從原始伺服器取得物件、取得物件標頭，或擷取原始伺服器支援的選項清單。
- **GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE** – 您可以使用 CloudFront 來取得、新增、更新和刪除物件，以及取得物件標頭。此外，您可以執行其他 POST 操作，例如從 Web 表單提交資料。

您也可以使用 AWS WAF 位元組比對規則陳述式，根據 HTTP 方法允許或封鎖請求，如中所述[字串比對規則陳述式](#)。如果您想要使用 CloudFront 支援的方法組合，例如 GET 和 HEAD，則不需要設定

AWS WAF 來封鎖使用其他方法的請求。如果您想要允許 CloudFront 不支援的方法組合，例如 GET、HEAD 和 POST，您可以設定 CloudFront 回應所有方法，然後使用 AWS WAF 封鎖使用其他方法的請求。

如需選擇 CloudFront 回應方法的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[您在建立或更新 Web 分佈時指定的主題值中允許的 HTTP 方法](#)。

多租戶分佈中允許的 HTTP 方法組態

對於多租戶分佈，在多租戶分佈層級設定的 HTTP 方法組態預設會套用至所有租戶分佈。租戶分佈可以視需要覆寫這些設定。

- 如果您想要使用 CloudFront 支援的方法組合，例如 GET 和 HEAD，您不需要設定 AWS WAF 來封鎖使用其他方法的請求。
- 如果您想要允許 CloudFront 預設不支援的方法組合，例如 GET、HEAD 和 POST，您可以設定 CloudFront 回應所有方法，然後使用 AWS WAF 封鎖使用其他方法的請求。

在多租用戶分佈中實作安全標頭時，請考慮下列事項：

- 範本層級安全標頭提供所有租用戶分佈的基準保護
- 租戶分佈可以：
 - 新增多租戶分佈中未定義的安全標頭
 - 修改租戶特定標頭的值
 - 無法移除或覆寫在多租戶分佈層級設定的安全標頭
- 考慮將多租用戶分佈層級標頭用於應適用於所有租用戶的關鍵安全控制

記錄注意事項

標準和多租用戶分佈都支援 AWS WAF 記錄，但日誌的結構和管理方式存在重要差異：

記錄比較

標準分佈	多租戶分佈
每個分佈一個日誌組態	範本和租戶層級記錄選項
標準日誌欄位	其他租戶識別符欄位

標準分佈	多租戶分佈
每個分佈的單一目的地	多租用戶分佈和租用戶日誌可能分開的目的地

其他資源

- 若要進一步了解多租戶分佈，請參閱《Amazon CloudFront 開發人員指南》中的[設定分佈](#)。
- 若要進一步了解如何 AWS WAF 搭配 CloudFront 使用，請參閱《Amazon CloudFront 開發人員指南》中的[使用 AWS WAF 保護](#)。
- 若要進一步了解 AWS WAF 日誌，請參閱[保護套件或 Web ACL 流量的日誌欄位](#)。

您使用 AWS WAF 服務時的安全性

本節說明如何套用共同責任模型 AWS WAF。

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，該架構專為滿足最安全敏感組織的需求而建置。

Note

本節提供使用 AWS WAF 服務及其 AWS 資源的標準 AWS 安全指導，例如 AWS WAF 保護套件或 Web ACLs 和規則群組。

如需有關使用 保護您的 AWS 資源的資訊 AWS WAF，請參閱 AWS WAF 本指南的其餘部分。

安全性是 AWS 與您之間共同責任。[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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用的合規計劃 AWS WAF，請參閱[AWS 合規計劃範圍內的服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您了解如何在使用 時套用共同責任模型 AWS WAF。下列主題說明如何設定 AWS WAF 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 WAF 資源。

主題

- [在 中保護您的資料 AWS WAF](#)
- [搭配 使用 IAM AWS WAF](#)
- [在 中記錄和監控 AWS WAF](#)
- [驗證 中的合規 AWS WAF](#)
- [在 中建置彈性 AWS WAF](#)
- [AWS WAF 中的基礎設施安全](#)

在 中保護您的資料 AWS WAF

AWS [共同責任模型](#)適用於 中的資料保護 AWS WAF。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](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 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 WAF 或使用主控台、API AWS CLI 或其他 AWS 服務 AWS SDKs 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。

AWS WAF 實體 - 例如保護套件或 Web ACLs、規則群組和 IP 集 - 會靜態加密，但無法使用加密的特定區域除外，包括中國（北京）和中國（寧夏）。每個區域都會採用唯一的加密金鑰。

刪除 AWS WAF 資源

您可以刪除您在其中建立的資源 AWS WAF。請參閱以下各節中每種資源類型的指導。

- [刪除保護套件或 Web ACL](#)
- [刪除規則群組](#)
- [刪除 IP 集合](#)
- [刪除規則運算式模式集](#)

搭配 使用 IAM AWS WAF

本節說明如何搭配 使用 IAM AWS WAF。

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驗證（登入）和授權（具有許可）來使用 AWS WAF 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 WAF 如何使用 IAM](#)
- [AWS WAF 的身分型政策範例](#)
- [AWS 的 受管政策 AWS WAF](#)
- [對 AWS WAF 身分和存取進行故障診斷](#)
- [使用的服務連結角色 AWS WAF](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在其中執行的工作 AWS WAF。

服務使用者 – 如果您使用 AWS WAF 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 AWS WAF 功能來執行工作時，您可能需要額外的許可。了解存取的管理方式可

協助您向管理員請求正確的許可。若您無法存取 AWS WAF 中的某項功能，請參閱 [對 AWS WAF 身分和存取進行故障診斷](#)。

服務管理員 – 如果您負責公司 AWS WAF 的資源，您可能可以完整存取 AWS WAF。您的任務是判斷服務使用者應存取哪些 AWS WAF 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搭配使用 IAM AWS WAF，請參閱 [AWS WAF 如何使用 IAM](#)。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS WAF 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的以 AWS WAF 身分為基礎的政策範例，請參閱 [AWS WAF 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 身分身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您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。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 登入《使用者指南》中的 [如何登入您的 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 AWS 服務是透過身分來源提供的登入資料存取的任何使用者。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 AWS 帳戶和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center？](#)。

IAM 使用者和群組

[IAM 使用者](#)是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 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。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](#)。委託人可以包含帳戶、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 WAF 如何使用 IAM

本節說明如何搭配使用 IAM 的功能 AWS WAF。

在您使用 IAM 管理對的存取之前 AWS WAF，請先了解哪些 IAM 功能可與搭配使用 AWS WAF。

您可以搭配使用的 IAM 功能 AWS WAF

IAM 功能	AWS WAF 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)	部分
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要全面了解 AWS WAF 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](#)。

的身分型政策 AWS WAF

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](#)。

若要檢視 AWS WAF 身分型政策的範例，請參閱 [AWS WAF 的身分型政策範例](#)。

中的資源型政策 AWS WAF

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](#)。

AWS WAF 使用資源型政策來支援跨帳戶共用規則群組。您可以將資源型政策設定提供給 AWS WAF API 呼叫 `PutPermissionPolicy` 或對等的 CLI 或 SDK 呼叫，以與其他 AWS 帳戶共用您擁有的規則群組。如需其他資訊，包括其他可用語言文件的範例和連結，請參閱 AWS WAF API 參考中的[PutPermissionPolicy](#)。此功能無法透過其他方式使用，例如 主控台或 AWS CloudFormation。

的政策動作 AWS WAF

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。

若要查看每個 AWS WAF 的動作和許可清單，請參閱服務授權參考中的[AWS WAF V2 定義的動作](#)。

中的政策動作在動作之前 AWS WAF 使用下列字首：

```
wafv2
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "wafv2:action1",  
    "wafv2:action2"  
]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要在 中指定以 AWS WAF 開頭的所有動作 List，請包含下列動作：

```
"Action": "wafv2:List*"
```

若要檢視 AWS WAF 身分型政策的範例，請參閱 [AWS WAF 的身分型政策範例](#)。

需要額外許可設定的動作

有些動作需要 服務授權參考中 [AWS WAF V2 定義的動作](#) 中無法完整描述的許可。本節提供額外的許可資訊。

主題

- [AssociateWebACL 的許可](#)
- [DisassociateWebACL 的許可](#)
- [GetWebACLForResource 的許可](#)
- [ListResourcesForWebACL 的許可](#)

AssociateWebACL 的許可

本節列出使用 AWS WAF 動作 將保護套件或 Web ACL 與資源建立關聯所需的許可 AssociateWebACL。

對於 Amazon CloudFront 分佈，請使用 CloudFront 動作，而不是此動作 UpdateDistribution。如需詳細資訊，請參閱《Amazon CloudFront API 參考》中的 [UpdateDistribution](#)。

Amazon API Gateway REST API

需要許可，才能在 REST API 資源類型 SetWebACL 上呼叫 API Gateway，以及在保護套件或 Web ACL 上呼叫 AWS WAF AssociateWebACL。

```
{  
    "Sid": "AssociateWebACL1",  
    "Effect": "Allow",
```

```

    "Action": [
      "wafv2:AssociateWebACL"
    ],
    "Resource": [
      "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
  },
  {
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
      "apigateway:SetWebACL"
    ],
    "Resource": [
      "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
  }
}

```

Application Load Balancer

需要許可才能呼叫 Application Load Balancer 資源類型的 `elasticloadbalancing:SetWebACL` 動作，以及在保護套件或 Web ACL `AssociateWebACL` 上呼叫 AWS WAF。

```

{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:SetWebACL"
  ],
  "Resource": [
    "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
  ]
}

```

AWS AppSync GraphQL API

需要許可，才能在 GraphQL API 資源類型上呼叫 AWS AppSync SetWebACL，以及在保護套件或 Web ACL 上呼叫 AWS WAF AssociateWebACL。

```
{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "appsync:SetWebACL"
  ],
  "Resource": [
    "arn:aws:appsync:*:account-id:apis/*"
  ]
}
```

Amazon Cognito 使用者集區

需要許可，才能在使用者集區資源類型上呼叫 Amazon Cognito AssociateWebACL 動作，以及在保護套件或 Web ACL 上呼叫 AWS WAF AssociateWebACL。

```
{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
```

```

    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}

```

AWS App Runner 服務

需要許可，才能在 App Runner 服務資源類型上呼叫 App Runner AssociateWebACL 動作，以及在 Web ACL 上呼叫 AWS WAF AssociateWebACL。

```

{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}

```

AWS 已驗證的存取執行個體

需要許可，才能在 Verified Access 執行個體資源類型上呼叫 ec2:AssociateVerifiedAccessInstanceWebAcl 動作，以及在 Web ACL 上呼叫 AWS WAF AssociateWebACL。

```

{

```

```
{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "ec2:AssociateVerifiedAccessInstanceWebAcl"
  ],
  "Resource": [
    "arn:aws:ec2:*:account-id:verified-access-instance/*"
  ]
}
```

DisassociateWebACL 的許可

本節列出使用 AWS WAF 動作 取消保護套件或 Web ACL 與資源的關聯所需的許可 DisassociateWebACL。

對於 Amazon CloudFront 分佈，請使用 CloudFront 動作 UpdateDistribution 搭配空的保護套件或 Web ACL ID。如需詳細資訊，請參閱《Amazon CloudFront API 參考》中的 [UpdateDistribution](#)。

Amazon API Gateway REST API

需要在 REST API 資源類型 SetWebACL 上呼叫 API Gateway 的許可。不需要呼叫 的許可 AWS WAF DisassociateWebACL。

```
{
  "Sid": "DisassociateWebACL",
  "Effect": "Allow",
  "Action": [
    "apigateway:SetWebACL"
  ],
  "Resource": [
    "arn:aws:apigateway:*::/restapis/*/stages/*"
  ]
}
```

Application Load Balancer

需要對 Application Load Balancer 資源類型呼叫 `elasticloadbalancing:SetWebACL` 動作的許可。不需要呼叫 的許可 `AWS WAF DisassociateWebACL`。

```
{
  "Sid": "DisassociateWebACL",
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:SetWebACL"
  ],
  "Resource": [
    "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
  ]
}
```

AWS AppSync GraphQL API

需要許可才能呼叫 AWS AppSync SetWebACL GraphQL API 資源類型。不需要呼叫 的許可 `AWS WAF DisassociateWebACL`。

```
{
  "Sid": "DisassociateWebACL",
  "Effect": "Allow",
  "Action": [
    "appsync:SetWebACL"
  ],
  "Resource": [
    "arn:aws:appsync:*:account-id:apis/*"
  ]
}
```

Amazon Cognito 使用者集區

需要許可，才能對使用者集區資源類型呼叫 `Amazon Cognito DisassociateWebACL` 動作並呼叫 `AWS WAF DisassociateWebACL`。

```
{
  "Sid": "DisassociateWebACL1",
  "Effect": "Allow",
  "Action": "wafv2:DisassociateWebACL",
  "Resource": "*"
}
```

```

},
{
  "Sid": "DisassociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "cognito-idp:DisassociateWebACL"
  ],
  "Resource": [
    "arn:aws:cognito-idp:*:account-id:userpool/*"
  ]
}

```

AWS App Runner 服務

需要對 App Runner 服務資源類型呼叫 App Runner DisassociateWebACL 動作和 呼叫的許可 AWS WAF DisassociateWebACL。

```

{
  "Sid": "DisassociateWebACL1",
  "Effect": "Allow",
  "Action": "wafv2:DisassociateWebACL",
  "Resource": "*"
},
{
  "Sid": "DisassociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "apprunner:DisassociateWebAcl"
  ],
  "Resource": [
    "arn:aws:apprunner:*:account-id:service/*/*"
  ]
}

```

AWS 已驗證的存取執行個體

需要對 Verified Access 執行個體資源類型呼叫

ec2:DisassociateVerifiedAccessInstanceWebAcl 動作和 呼叫的許可 AWS WAF DisassociateWebACL。

```

{
  "Sid": "DisassociateWebACL1",

```



```
"Effect": "Allow",
"Action": "wafv2:DisassociateWebACL",
"Resource": "*"
},
{
  "Sid": "DisassociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "ec2:DisassociateVerifiedAccessInstanceWebAcl"
  ],
  "Resource": [
    "arn:aws:ec2:*:account-id:verified-access-instance/*"
  ]
}
```

GetWebACLForResource 的許可

本節列出使用 AWS WAF 動作 取得受保護資源的保護套件或 Web ACL 所需的許可 GetWebACLForResource。

對於 Amazon CloudFront 分佈，請使用 CloudFront 動作，而不是此動作 GetDistributionConfig。如需詳細資訊，請參閱《Amazon CloudFront API 參考》中的 [GetDistributionConfig](#)。

Note

GetWebACLForResource 需要 許可才能呼叫 GetWebACL。在這種情況下，GetWebACL 只會 AWS WAF 使用 來驗證您的帳戶是否具有存取 GetWebACLForResource 傳回的保護套件或 Web ACL 所需的許可。當您呼叫 時 GetWebACLForResource，您可能會收到錯誤，指出您的帳戶未獲授權在 資源 wafv2:GetWebACL 上執行。AWS WAF 不會將此類型的錯誤新增至 AWS CloudTrail 事件歷史記錄。

Amazon API Gateway REST API、Application Load Balancer 和 AWS AppSync GraphQL API 需要呼叫 AWS WAF GetWebACLForResource 和 GetWebACL 的保護套件或 Web ACL 許可。

```
{
  "Sid": "GetWebACLForResource",
  "Effect": "Allow",
  "Action": [
    "wafv2:GetWebACLForResource",
```

```

        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}

```

Amazon Cognito 使用者集區

需要許可才能呼叫使用者集區資源類型的 Amazon Cognito `GetWebACLForResource` 動作，以及呼叫 AWS WAF `GetWebACLForResource` 和 `GetWebACL`。

```

{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}

```

AWS App Runner 服務

需要許可才能呼叫 App Runner 服務資源類型的 App Runner `DescribeWebAclForService` 動作，以及呼叫 AWS WAF `GetWebACLForResource` 和 `GetWebACL`。

```

{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [

```

```

        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}

```

AWS 已驗證的存取執行個體

需要許可才能呼叫 Verified Access 執行個體資源類型的 `ec2:GetVerifiedAccessInstanceWebAcl` 動作，以及呼叫 AWS WAF `GetWebACLForResource` 和 `GetWebACL`。

```

{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}

```

```
]
}
```

ListResourcesForWebACL 的許可

本節列出使用 AWS WAF 動作 擷取保護套件或 Web ACL 的受保護資源清單所需的許可 ListResourcesForWebACL。

對於 Amazon CloudFront 分佈，請使用 CloudFront 動作，而不是此動作 ListDistributionsByWebACLId。如需詳細資訊，請參閱《Amazon CloudFront API 參考》中的 [ListDistributionsByWebACLId](#)。

Amazon API Gateway REST API、Application Load Balancer 和 AWS AppSync GraphQL API 需要許可才能呼叫 AWS WAF ListResourcesForWebACL Web ACL。

```
{
  "Sid": "ListResourcesForWebACL",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
}
```

Amazon Cognito 使用者集區

需要對使用者集區資源類型呼叫 Amazon Cognito ListResourcesForWebACL 動作和呼叫 AWS WAF 的許可 ListResourcesForWebACL。

```
{
  "Sid": "ListResourcesForWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
```

```

    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}

```

AWS App Runner 服務

需要對 App Runner 服務資源類型呼叫 App Runner ListAssociatedServicesForWebAcl 動作和呼叫的許可 AWS WAF ListResourcesForWebACL。

```

{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}

```

AWS 已驗證的存取執行個體

需要許可才能呼叫 Verified Access 執行個體資源類型的 ec2:DescribeVerifiedAccessInstanceWebAclAssociations 動作，以及呼叫 AWS WAF ListResourcesForWebACL。

```

{

```

```
{
  "Sid": "ListResourcesForWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "ListResourcesForWebACL2",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
  ],
  "Resource": [
    "arn:aws:ec2:*:account-id:verified-access-instance/*"
  ]
}
```

的政策資源 AWS WAF

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 AWS WAF 資源類型及其 ARNs 的清單，請參閱服務授權參考中的 [AWS WAF V2 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 WAF V2 定義的動作](#)。若要允許或拒絕存取資源子集 AWS WAF，請在政策的 resource 元素中包含資源的 ARN。

資源 ARNs 格式如下：AWS WAF wafv2

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id

```

如需 ARN 規格的一般資訊，請參閱 中的 [Amazon Resource Name \(ARNs\)](#) Amazon Web Services 一般參考。

下列列出 wafv2 資源 ARNs 特有的要求：

- **region**：針對您用來保護 Amazon CloudFront 分佈 AWS WAF 的資源，將此設定為 `us-east-1`。否則，請將此設定為搭配受保護區域資源使用的 區域。
- **##**：將範圍設定為 `global`，以搭配 Amazon CloudFront 分佈使用 `regional`，或搭配 AWS WAF 支援的任何區域資源使用。區域資源是 Amazon API Gateway REST API、Application Load Balancer、a AWS AppSync GraphQL API、Amazon Cognito 使用者集區、AWS App Runner 服務和 AWS Verified Access 執行個體。
- **resource-type**：指定下列其中一個值：`webacl`、`rulegroup`、`regexpatternset`、`ipset` 或 `managedruleset`。
- **resource-name**：指定您提供 AWS WAF 資源的名稱，或指定萬用字元 (*) 來表示符合 ARN 中其他規格的所有資源。您必須指定資源名稱和資源 ID，或同時指定萬用字元。
- **resource-id**：指定資源的 AWS WAF ID，或指定萬用字元 (*)，以指出符合 ARN 中其他規格的所有資源。您必須指定資源名稱和資源 ID，或同時指定萬用字元。

例如，下列 ARN 會指定區域 `111122223333` 中帳戶區域範圍的所有保護套件或 Web ACLs `us-west-1`：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

下列 ARN 指定名為 `MyIPManagementRuleGroup` 的規則群組，其為區域 `111122223333` 中帳戶的全域範圍 `us-east-1`：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

若要檢視 AWS WAF 身分型政策的範例，請參閱 [AWS WAF 的身分型政策範例](#)。

的政策條件索引鍵 AWS WAF

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](#)。

此外，AWS WAF 支援下列條件索引鍵，您可以使用這些索引鍵為您的 IAM 政策提供精細篩選：

- wafv2 : LogDestinationResource

此條件金鑰會取得記錄目的地的 Amazon Resource Name (ARN) 規格。這是您在使用 REST API 呼叫時為記錄目的地提供的 ARNPutLoggingConfiguration。

您可以明確指定 ARN，也可以指定 ARN 的篩選。下列範例指定篩選具有特定位置和字首的 Amazon S3 儲存貯 ARNs。

```
"Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
```

- wafv2 : LogScope

此條件索引鍵定義字串中記錄組態的來源。目前，這一律設定為預設值 Customer，這表示記錄目的地由您擁有和管理。

若要查看 AWS WAF 條件索引鍵的清單，請參閱《服務授權參考》中的[AWS WAF V2 的條件索引鍵](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱[AWS WAF V2 定義的動作](#)。

若要檢視 AWS WAF 身分型政策的範例，請參閱[AWS WAF 的身分型政策範例](#)。

中的 ACLs AWS WAF

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 AWS WAF

支援 ABAC (政策中的標籤)：部分

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。您可以將標籤連接到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [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 \(ABAC\)](#)。

搭配使用暫時登入資料 AWS WAF

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。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](#)。

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](#)。

轉送服務的存取工作階段 AWS WAF

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 AWS 中執行動作時，您會被視為委託人。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，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](#)。

AWS WAF 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 AWS WAF 功能。只有在 AWS WAF 提供指引時，才能編輯服務角色。

的服務連結角色 AWS WAF

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。

如需建立或管理 AWS WAF 服務連結角色的詳細資訊，請參閱[使用的服務連結角色 AWS WAF](#)。

AWS WAF 的身分型政策範例

本節提供的身分型政策範例 AWS WAF。

根據預設，使用者和角色不具備建立或修改 AWS WAF 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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 \(主控台\)](#)。

如需定義的動作和資源類型的詳細資訊 AWS WAF，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 [AWS WAF V2 的動作、資源和條件索引鍵](#)。

主題

- [政策最佳實務](#)
- [使用 AWS WAF 主控台](#)
- [允許使用者檢視他們自己的許可](#)
- [授予對 AWS WAF CloudFront 和 CloudWatch 的唯讀存取權](#)
- [授予對 AWS WAF CloudFront 和 CloudWatch 的完整存取權](#)
- [授予對單一 的存取權 AWS 帳戶](#)
- [授予單一保護套件或 Web ACL 的存取權](#)
- [授予 CLI 對保護套件或 Web ACL 和規則群組的存取權](#)

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 WAF 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 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 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》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 AWS WAF 主控台

若要存取 AWS WAF 主控台，您必須擁有一組最低的許可。這些許可必須允許您列出和檢視中 AWS WAF 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。

為了確保使用者和角色可以使用 AWS WAF 主控台，請至少將 AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS 受管政策連接到實體。如需此受管政策的相關資訊，請參閱 [AWS 受管政策：AWSWAFConsoleReadOnlyAccess](#)。如需將受管政策連接至使用者的詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可給使用者](#)。

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: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": "*"
}
]
}
```

授予對 AWS WAF CloudFront 和 CloudWatch 的唯讀存取權

下列政策會授予使用者對 AWS WAF 資源、Amazon CloudFront Web 分佈和 Amazon CloudWatch 指標的唯讀存取權。需要許可來檢視 AWS WAF 條件、規則和保護套件或 Web ACLs 中的設定，以查看哪個分佈與保護套件或 Web ACL 相關聯，以及在 CloudWatch 中監控指標和請求範例的使用者非常有用。這些使用者無法建立、更新或刪除 AWS WAF 資源。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:Get*",
        "wafv2:List*",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributionTenantsByCustomization",
        "cloudfront:ListDistributionTenants",
        "cloudfront:GetDistributionTenant",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeRegions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
    }
  ]
}
```

授予對 AWS WAF CloudFront 和 CloudWatch 的完整存取權

下列政策可讓使用者執行任何 AWS WAF 操作、在 CloudFront Web 分佈上執行任何操作，以及在 CloudWatch 中監控指標和請求範例。這對身為 AWS WAF 管理員的使用者很有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:*",
        "cloudfront:CreateDistribution",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:DisassociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionWebACL",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:ListDistributionTenantsByCustomization",
        "cloudfront:ListDistributionTenants",
        "cloudfront>DeleteDistribution",
        "cloudfront:GetDistributionTenant",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeRegions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

我們強烈建議您為具有管理權限的使用者設定多重驗證 (MFA)。如需詳細資訊，請參閱《IAM 使用者指南》中的[搭配使用 Multi-Factor Authentication \(MFA\) 裝置 AWS](#)。

授予對單一 的存取權 AWS 帳戶

此政策會將下列許可授予帳戶 444455556666：

- 完整存取所有 AWS WAF 操作和資源。
- 讀取和更新所有 CloudFront 分發的存取權，這可讓您關聯保護套件或 Web ACLs 和 CloudFront 分發。
- 讀取所有 CloudWatch 指標和指標統計資料的存取權，讓您可以在 AWS WAF 主控台中檢視 CloudWatch 資料和請求範例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "wafv2:*"
      ],
      "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

授予單一保護套件或 Web ACL 的存取權

下列政策可讓使用者透過 主控台，對帳戶 中的特定保護套件或 Web ACL 執行任何 AWS WAF 操作444455556666。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "wafv2:*"
      ],
      "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/test123/112233d7c-86b2-458b-af83-51c51example",
      ]
    },
    {
      "Sid": "consoleAccess",
      "Effect": "Allow",
      "Action": [
        "wafv2:ListWebACLs",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

授予 CLI 對保護套件或 Web ACL 和規則群組的存取權

下列政策可讓使用者在帳戶 中的特定保護套件或 Web ACL 和特定規則群組上，透過 CLI 執行任何 AWS WAF 操作444455556666。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```



```

        "wafv2:*"
      ],
      "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/test123rulegroup/55555555-6666-1234-abcd-00d11example"
      ]
    }
  ]
}

```

下列政策可讓使用者透過 主控台，對帳戶 中的特定保護套件或 Web ACL 執行任何 AWS WAF 操作 444455556666。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "wafv2:*"
      ],
      "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/test123/112233d7c-86b2-458b-af83-51c51example",
        "*"
      ]
    },
    {
      "Sid": "consoleAccess",
      "Effect": "Allow",
      "Action": [
        "wafv2:ListWebACLs",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

AWS 的 受管政策 AWS WAF

本節說明如何使用 的 AWS 受管政策 AWS WAF。

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 受管政策](#)。

AWS 受管政策：AWSWAFReadOnlyAccess

此政策授予唯讀許可，允許使用者存取整合服務 AWS WAF 的資源和資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito AWS App Runner AWS Amplify 和 AWS Verified Access。您可以將此政策連接到 IAM 身分。AWS WAF 也會將此政策連接到允許 代表您 AWS WAF 執行動作的服務角色。

如需此政策的詳細資訊，請參閱 IAM 主控台中的[AWSWAFReadOnlyAccess](#)。

AWS 受管政策：AWSWAFFullAccess

此政策授予整合服務 AWS WAF 的完整資源存取權，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito AWS App Runner AWS Amplify 和 AWS Verified Access。您可以將此政策連接到 IAM 身分。AWS WAF 也會將此政策連接到允許 代表您 AWS WAF 執行動作的服務角色。

如需此政策的詳細資訊，請參閱 IAM 主控台中的[AWSWAFFullAccess](#)。

AWS 受管政策：AWSWAFConsoleReadOnlyAccess

此政策會將唯讀許可授予 AWS WAF 主控台，其中包含 AWS WAF 和 整合服務的資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito AWS App Runner AWS Amplify 和 AWS Verified Access。您可以將此政策連接至 IAM 身分。

如需此政策的詳細資訊，請參閱 IAM 主控台中的[AWSWAFConsoleReadOnlyAccess](#)。

AWS 受管政策：AWSWAFConsoleFullAccess

此政策授予 AWS WAF 主控台的完整存取權，其中包括 AWS WAF 和 整合服務的資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito AWS App Runner AWS Amplify和 AWS Verified Access。您可以將此政策連接至 IAM 身分。AWS WAF 也會將此政策連接至允許 代表您 AWS WAF 執行動作的服務角色。

如需此政策的詳細資訊，請參閱 IAM 主控台中的 [AWSWAFConsoleFullAccess](#)。

AWS 受管政策：WAFV2LoggingServiceRolePolicy

此政策允許 AWS WAF 將日誌寫入 Amazon Data Firehose。只有在您啟用登入時，才會使用此政策 AWS WAF。此政策連接至 AWSServiceRoleForWAFV2Logging 服務連結角色。如需服務連結角色的詳細資訊，請參閱[使用的服務連結角色 AWS WAF](#)。

如需此政策的詳細資訊，請參閱 IAM 主控台中的 [WAFV2LoggingServiceRolePolicy](#)。

AWS WAFAWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS WAF 以來，AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱位於 AWS WAF 的文件歷史記錄頁面上的 RSS 摘要[文件歷史紀錄](#)。

政策	變更說明	日期
AWSWAFFullAccess 此政策允許 代表您 AWS WAF 在 AWS WAF 和整合服務中管理 AWS 資源。 IAM 主控台中的詳細資訊：AWSWAFFullAccess。	新增 所需的許可 AssociateWebACL、DisassociateWebACL、GetWebACLForResource 和 ListResourcesForWebACL AWS Amplify。	2025-05-05
AWSWAFReadOnlyAccess 此政策允許 代表您 AWS WAF 在 AWS WAF 和整合服務中管理 AWS 資源。	新增 所需的許可 GetWebACLForResource 和 ListResourcesForWebACL AWS Amplify。	2025-05-05

政策	變更說明	日期
如需此政策的詳細資訊，請參閱 IAM 主控台中的 AWSWAFReadOnlyAccess 。		

政策	變更說明	日期
AWSWAFConsoleReadOnlyAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleReadOnlyAccess。	新增下列許可： Amplify • <code>amplify:GetWebACLForResource</code> – 准許擷取與 Amplify 資源相關聯的 AWS WAF 保護套件或 Web ACL • <code>amplify:ListApps</code> – 准許擷取您 中的 Amplify 應用程式 AWS 帳戶 • <code>amplify:ListResourcesForWebACL</code> – 准許擷取與 AWS WAF 保護套件或 Web ACL 相關聯的 Amplify 應用程式 CloudFront • <code>cloudfront:GetDistributionConfig</code> – 准許取得 CloudFront 分佈的組態資訊 • <code>cloudfront:GetDistributionTenant</code> – 准許取得 CloudFront 分佈租用戶的相關資訊 • <code>cloudfront:ListDistributionsTenants</code> – 准許列出與您的 相關聯的 CloudFront 分佈租用戶 AWS 帳戶	2025-05-05

政策	變更說明	日期
	cloudfront:ListDistributionTenantsByCustomization – 允許列出與您的 相關聯的篩選 CloudFront 分佈租用戶 AWS 帳戶	

政策	變更說明	日期
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleFullAccess。	新增下列許可： Amplify • <code>amplify:AssociateWebACL</code> – 准許將 AWS WAF 保護套件或 Web ACL 與 Amplify 資源建立關聯 • <code>amplify:DisassociateWebACL</code> – 准許取消 AWS WAF 保護套件或 Web ACL 與 Amplify 資源的關聯 • <code>amplify:GetWebACLForResource</code> – 准許擷取與 Amplify 資源相關聯的 AWS WAF 保護套件或 Web ACL • <code>amplify:ListApps</code> – 准許擷取您 中的 Amplify 應用程式 AWS 帳戶 • <code>amplify:ListResourcesForWebACL</code> – 准許擷取與 AWS WAF 保護套件或 Web ACL 相關聯的 Amplify 應用程式 CloudFront • <code>cloudfront:AssociateDistributionTenantWebACL</code> – 准許將 AWS WAF 保護套件或 Web ACL 與 CloudFront 分佈租用戶建立關聯	2025-05-05

政策	變更說明	日期
	• <code>cloudfront:AssociateDistributionWebACL</code> – 准許將 AWS WAF 保護套件或 Web ACL 與 CloudFront 分佈建立關聯 • <code>cloudfront:DisassociateDistributionTenantWebACL</code> – 准許取消 AWS WAF 保護套件或 Web ACL 與 CloudFront 分佈租用戶的關聯 • <code>cloudfront:DisassociateDistributionWebACL</code> – 准許取消 AWS WAF 保護套件或 Web ACL 與 CloudFront 分佈的關聯 • <code>cloudfront:GetDistributionConfig</code> – 准許取得 CloudFront 分佈的組態資訊 • <code>cloudfront:GetDistributionTenant</code> – 准許取得 CloudFront 分佈租用戶的相關資訊 • <code>cloudfront:ListDistributionTenants</code> – 准許列出與您的 相關聯的 CloudFront 分佈租用戶 AWS 帳戶 • <code>cloudfront:ListDistributionTenantsByCustomization</code> – 准許列出與您的 相關聯的篩	

政策	變更說明	日期
	選 CloudFront 分佈租用戶 AWS 帳戶	
WAFV2LoggingServiceRolePolicy 此政策允許 AWS WAF 將日誌寫入 Amazon Data Firehose。只有在您啟用記錄時才會使用它。 IAM 主控台中的詳細資訊：WAFV2LoggingServiceRolePolicy。	在附加此政策的服務連結角色中，將陳述式 IDs (Sid) 新增至許可設定。	2024-06-03
AWSServiceRoleForWAFV2Logging 此服務連結角色提供許可政策，允許 AWS WAF 將日誌寫入 Amazon Data Firehose。 IAM 主控台中的詳細資訊：AWSServiceRoleForWAFV2Logging。	已將陳述式 IDs(Sid) 新增至許可設定。	2024-06-03
AWS WAF 新增變更追蹤	AWS WAF 已開始追蹤受管政策和WAFV2LoggingServiceRolePolicy 服務連結角色的變更AWSServiceRoleForWAFV2Logging 。	2024-06-03

政策	變更說明	日期
AWSWAFFullAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFFullAccess。	擴展許可，將 AWS Verified Access 執行個體新增至您可以使用的資源類型 AWS WAF。	2023-06-17
AWSWAFReadOnlyAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFReadOnlyAccess。	擴展許可，將 AWS Verified Access 執行個體新增至您可以使用的資源類型 AWS WAF。	2023-06-17
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleFullAccess。	擴展許可，將 AWS Verified Access 執行個體新增至您可以使用的資源類型 AWS WAF。	2023-06-17

政策	變更說明	日期
AWSWAFConsoleReadOnlyAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleReadOnlyAccess。	擴展許可，將 AWS Verified Access 執行個體新增至您可以使用的資源類型 AWS WAF。	2023-06-17
AWSWAFFullAccess 此政策允許代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFFullAccess。	擴展許可可以更正 AWS App Runner 服務的存取設定。	2023-06-06
AWSWAFReadOnlyAccess 此政策允許代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFReadOnlyAccess。	擴展許可可以更正 AWS App Runner 服務的存取設定。	2023-06-06

政策	變更說明	日期
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleFullAccess。	擴展許可可以更正 AWS App Runner 服務的存取設定。	2023-06-06
AWSWAFConsoleReadOnlyAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleReadOnlyAccess。	擴展許可可以更正 AWS App Runner 服務的存取設定。	2023-06-06
AWSWAFFullAccess 此政策允許代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFFullAccess。	擴展許可，將 AWS App Runner 服務新增至您可以使用的資源類型 AWS WAF。	2023-03-30

政策	變更說明	日期
AWSWAFReadOnlyAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFReadOnlyAccess。	擴展許可，將 AWS App Runner 服務新增至您可以使用的資源類型 AWS WAF。	2023-03-30
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleFullAccess。	擴展許可，將 AWS App Runner 服務新增至您可以使用的資源類型 AWS WAF。	2023-03-30
AWSWAFConsoleReadOnlyAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleReadOnlyAccess。	擴展許可，將 AWS App Runner 服務新增至您可以使用的資源類型 AWS WAF。	2023-03-30

政策	變更說明	日期
AWSWAFFullAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFFullAccess。	擴展許可，將 Amazon Cognito 使用者集區新增至您可以使用的資源類型 AWS WAF。	2022-08-25
AWSWAFReadOnlyAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFReadOnlyAccess。	擴展許可，將 Amazon Cognito 使用者集區新增至您可以使用的資源類型 AWS WAF。	2022-08-25
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleFullAccess。	擴展許可，將 Amazon Cognito 使用者集區新增至您可以使用的資源類型 AWS WAF。	2022-08-25

政策	變更說明	日期
AWSWAFConsoleReadOnlyAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleReadOnlyAccess。	擴展許可，將 Amazon Cognito 使用者集區新增至您可以使用的資源類型 AWS WAF。	2022-08-25
AWSWAFFullAccess 此政策允許代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFFullAccess。	更正 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs 的日誌交付許可設定。此變更可解決記錄組態期間發生的存取遭拒錯誤。如需有關記錄保護套件或 Web ACL 流量的資訊，請參閱 記錄 AWS WAF 保護套件或 Web ACL 流量。	2022-01-11
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊： AWSWAFConsoleFullAccess。	更正 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs 的日誌交付許可設定。此變更可解決記錄組態期間發生的存取錯誤。如需有關記錄保護套件或 Web ACL 流量的資訊，請參閱 記錄 AWS WAF 保護套件或 Web ACL 流量。	2022-01-11

政策	變更說明	日期
AWSWAFFullAccess 此政策允許 代表您 AWS WAF 管理整合服務中的 AWS WAF 和 中的 AWS 資源。 IAM 主控台中的詳細資訊：AWSWAFFullAccess。	新增了擴展記錄選項的新許可。 此變更可讓您 AWS WAF 存取其他記錄目的地 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs。如需有關記錄保護套件或 Web ACL 流量的資訊，請參閱 記錄 AWS WAF 保護套件或 Web ACL 流量。	2021-11-15
AWSWAFConsoleFullAccess 此政策允許 AWS WAF 代表您在 AWS WAF 和整合服務中管理 AWS 主控台資源和其他 AWS 資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleFullAccess。	新增了擴展記錄選項的新許可。 此變更可讓您 AWS WAF 存取其他記錄目的地 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs。如需有關記錄保護套件或 Web ACL 流量的資訊，請參閱 記錄 AWS WAF 保護套件或 Web ACL 流量。	2021-11-15
AWS WAF 開始追蹤變更	AWS WAF 已開始追蹤其 AWS 受管政策的變更。	2021-3-01

對 AWS WAF 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 AWS WAF 和 IAM 時可能遇到的常見問題。

主題

- [我無權在中執行動作 AWS WAF](#)

- [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 WAF 資源](#)

我無權在 中執行 動作 AWS WAF

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 wafv2: *GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
wafv2: 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 wafv2: *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，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 AWS WAF。

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。

名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS WAF 中執行動作時，發生下列範例錯誤。但是，動作要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 AWS WAF 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 是否 AWS WAF 支援這些功能，請參閱 [AWS WAF 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](#)。

使用的服務連結角色 AWS WAF

本節說明如何使用服務連結角色來 AWS WAF 存取您 AWS 帳戶中的資源。

AWS WAF use AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結的唯一 IAM 角色類型 AWS WAF。服務連結角色由 預先定義，AWS WAF 並包含服務 AWS 代表您呼叫其他服務所需的所有許可。

服務連結角色可讓您更 AWS WAF 輕鬆地設定，因為您不必手動新增必要的許可。AWS WAF 會定義其服務連結角色的許可，除非另有定義，否則 AWS WAF 只能擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

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

如需關於支援服務連結角色的其他服務的資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

的服務連結角色許可 AWS WAF

AWS WAF 使用服務連結角色AWSServiceRoleForWAFV2Logging將日誌寫入 Amazon Data Firehose。只有在您啟用登入時，才會使用此角色 AWS WAF。如需日誌記錄的相關資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

此服務連結角色會連接至 AWS 受管政策 WAFV2LoggingServiceRolePolicy。如需受管政策的更多相關資訊，請參閱[AWS 受管政策：WAFV2LoggingServiceRolePolicy](#)。

AWSServiceRoleForWAFV2Logging 服務連結角色信任 `wafv2.amazonaws.com` 服務來擔任該角色。

角色的許可政策 AWS WAF 允許 對指定的資源完成下列動作：

- Amazon Data Firehose 動作：PutRecord 和 PutRecordBatch 上的 Firehose 資料串流資源，名稱開頭為 `aws-waf-logs-`。例如：`aws-waf-logs-us-east-2-analytics`。
- AWS Organizations 動作：在 Organizations 組織資源 DescribeOrganization 上。

請參閱 IAM 主控台中的完整服務連結角色：[AWSServiceRoleForWAFV2Logging](#)。

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](#)。

為 AWS WAF 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 上啟用 AWS WAF 記錄 AWS Management Console，或您在 AWS WAF CLI 或 AWS WAF API 中提出 PutLoggingConfiguration 請求時，會為您 AWS WAF 建立服務連結角色。

您必須擁有 `iam:CreateServiceLinkedRole` 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 AWS WAF 記錄時，會再次為您 AWS WAF 建立服務連結角色。

為 AWS WAF 編輯服務連結角色

AWS WAF 不允許您編輯 AWSServiceRoleForWAFV2Logging 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

為 AWS WAF 刪除服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

Note

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

刪除使用 AWS WAF 的資源 `AWSServiceRoleForWAFV2Logging`

1. 在 AWS WAF 主控台上，從每個 Web ACL 移除記錄。如需詳細資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
2. 使用 API 或 CLI，為每個 Web ACL 提交 `DeleteLoggingConfiguration` 請求啟用記錄功能。如需詳細資訊，請參閱[AWS WAF API 參考](#)。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 `AWSServiceRoleForWAFV2Logging` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

AWS WAF 服務連結角色的支援區域

AWS WAF 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱[AWS WAF 端點和配額](#)。

在 中記錄和監控 AWS WAF

本節說明如何使用 AWS 工具來監控和回應 中的事件 AWS WAF。

監控是維護 和 AWS 解決方案的可靠性、可用性 AWS WAF 和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。AWS 提供數種工具來監控您的 AWS WAF 資源並回應潛在事件：

Amazon CloudWatch 警示

您可以使用 CloudWatch 警示觀察單一指標一段指定的時間。如果指標超過指定的閾值，CloudWatch 會傳送通知至 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。

AWS CloudTrail 日誌

CloudTrail 會提供使用者、角色或服務 AWS 在其中採取之動作的記錄 AWS WAF。您可以使用 CloudTrail 所收集的資訊來判斷提出的請求 AWS WAF、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。如需詳細資訊，請參閱[使用 AWS CloudTrail 記錄 API 呼叫](#)。

AWS WAF 保護套件或 Web ACL 流量記錄

AWS WAF 為您的保護套件或 Web ACLs 分析的流量提供記錄。日誌包含從受保護 AWS 資源 AWS WAF 接收請求的時間、請求的詳細資訊，以及請求相符規則的動作設定等資訊。如需詳細資訊，請參閱[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。

驗證 中的合規 AWS WAF

本節說明您在使用 時的合規責任 AWS WAF。

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](#)。

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的責任模型。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。

在中建置彈性 AWS WAF

本節說明 AWS 架構如何支援資料備援 AWS WAF。

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](#)。

AWS WAF 中的基礎設施安全

本節說明如何 AWS WAF 隔離服務流量。

作為受管服務，AWS WAF 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 發佈的 API 呼叫，AWS WAF 透過網路存取。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，您可以使用 [AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS WAF 配額

Note

這是 的最新版本 AWS WAF。如需 AWS WAF Classic，請參閱 [AWS WAF 傳統](#)。

AWS WAF 受下列配額限制（先前稱為限制）。這些配額與 AWS WAF 可使用的所有區域相同。每個區域分別受制於這些配額。配額不會跨區域累計。

AWS WAF 對每個帳戶可擁有的實體數量上限具有預設配額。您可以 [請求提高](#) 這些配額。

資源	每個區域每個帳戶的預設配額
保護套件或 Web ACLs 的數量上限	100
規則群組的數量上限	100
IP 集數量上限	100
每個保護套件或 Web ACL 每秒請求數上限	100,000
每個保護套件或 Web ACL 或規則群組的自訂請求標頭數量上限	100
每個保護套件或 Web ACL 或規則群組的自訂回應標頭數目上限	100
每個保護套件或 Web ACL 或規則群組的自訂回應內文數量上限	50
保護套件或 Web ACL 字符網域清單中字符網域的數量上限	10
regex 集的數量上限	10

在 CloudFront AWS WAF 上允許的每秒請求數上限 (RPS) 由 CloudFront 設定，如 [CloudFront 開發人員指南](#) 中所述。

AWS WAF 對每個區域每個帳戶的下列實體設定具有固定配額。這些配額無法變更。

資源	每個區域每個帳戶的配額
每個保護套件或 Web ACL* 的最大保護套件或 Web ACL 容量單位 WCUs)	5,000
每個規則群組 WCUs 上限	5,000
每個規則群組的參考陳述式數目上限。在規則群組中，參考陳述式可以參考 IP 集或 regex 模式集。	50
每個保護套件或 Web ACL 的參考陳述式數目上限。在保護套件或 Web ACL 中，參考陳述式可以參考規則群組、IP 集或 regex 模式集。	50

資源	每個區域每個帳戶的配額
每個 IP 集 CIDR 表示法中的 IP 地址數目上限	10,000
每個保護套件或 Web ACL 的速率型規則數目上限	10
每個規則群組的速率型規則數目上限	4
可針對速率型規則定義的最小請求速率	10
每個以速率為基礎的規則可以限制速率的唯一 IP 地址數目上限	10,000
字串比對陳述式中的字元數上限	200
每個規則運算式模式中的字元數上限	200
每個 regex 集的唯一 regex 模式數目上限	10
可檢查 Application Load Balancer 和 AWS AppSync 保護的 Web 請求內文大小上限	8 KB
可檢查 CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access 保護的 Web 請求內文大小上限**	64 KB
每個規則陳述式的文字轉換數目上限	10
單一自訂回應定義的自訂回應內文內容大小上限	4 KB
單一自訂回應定義的自訂標頭數目上限	10
單一自訂請求定義的自訂標頭數目上限	10
單一規則群組或單一保護套件或 Web ACL 所有回應內文內容的合併大小上限	50 KB

*在保護套件或 Web ACL 中使用超過 1,500 WCUs 會產生超出基本保護套件或 Web ACL 價格的成本。如需詳細資訊，請參閱 [中的 Web ACL 容量單位 WCUs](#)、[AWS WAF](#) 和 [AWS WAF 定價](#)。

**根據預設，CloudFront、API Gateway、Amazon Cognito、App Runner 和 Verified Access 資源的內文檢查限制設定為 16 KB，但您可以將保護套件或 Web ACL 組態中任何這些資源的檢查限制提高到列出的上限。如需詳細資訊，請參閱[管理的內文檢查大小限制 AWS WAF](#)。

AWS WAF 每個區域每個帳戶的呼叫具有下列固定配額。這些配額會套用至透過任何可用方式 (包括主控台、CLI、AWS CloudFormation、REST API 和 SDK) 對服務的呼叫總數。這些配額無法變更。

呼叫類型	每個區域每個帳戶的配額
AssociateWebACL 呼叫次數上限	每 2 秒一個請求
DisassociateWebACL 呼叫次數上限	每 2 秒一個請求
GetWebACLForResource 呼叫次數上限	每秒一個請求
ListResourcesForWebACL 呼叫次數上限	每秒一個請求
任何個別 Get 或 List 動作的呼叫次數上限 (若未定義其他配額)	每秒五個請求
任何個別 Create、Put 或 Update 動作的呼叫次數上限 (若未定義其他配額)	每秒一個請求

AWS WAF 對單一組織中所有帳戶的呼叫具有下列固定配額 AWS Organizations。這些配額會套用至透過任何可用方式 (包括主控台、CLI、AWS CloudFormation、REST API 和 SDK) 對服務的呼叫總數。這些配額無法變更。

呼叫類型	單一區域中每個組織的配額
在 區域美國東部 (維吉尼亞北部) (us-east-1)、ListResourcesForWebACL、美國西部 (奧勒岡) (us-west-2) 或歐洲 (愛爾蘭) (eu-west-1) 的任何單一區域中，組織中所有帳戶對的呼叫數量上限。	每秒 12 個請求
組織中所有帳戶對的呼叫數量上限 ListResourcesForWebACL，位於未在此資料表中列出不同配額的任何單一區域中。	每秒 6 個請求

將您的 AWS WAF Classic 資源遷移至 AWS WAF

本節提供將您的規則和保護套件或 Web ACLs 從 AWS WAF Classic 遷移至 的指引 AWS WAF。AWS WAF 已於 2019 年 11 月發行。如果您使用 AWS WAF Classic 建立規則和保護套件或 Web ACLs 等資源，則需要使用 AWS WAF Classic 使用這些資源，或將其遷移至此最新版本。

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

開始遷移工作之前，請先閱讀 AWS WAF，熟悉 [AWS WAF](#)。

主題

- [為什麼要遷移至 AWS WAF？](#)
- [遷移警告與限制](#)
- [遷移的運作方式](#)
- [將保護套件或 Web ACL 從 AWS WAF Classic 遷移至 AWS WAF](#)

為什麼要遷移至 AWS WAF？

最新版本的 AWS WAF 提供與先前版本相比的許多改善，同時維持您習慣的大多數概念和術語。

下列清單說明最新版 AWS WAF 中的主要變更。繼續遷移之前，請花一些時間檢閱此清單，並熟悉 AWS WAF 本指南的其餘部分。

- AWS WAF Classic 的支援將於 2025 年 9 月 30 日結束。
- 適用於 AWS 的受管規則 AWS WAF – 現在可透過 AWS 受管規則取得的規則群組可針對常見的 Web 威脅提供保護。這些規則群組大多免費包含在 中 AWS WAF。如需詳細資訊，請參閱 [AWS 受管規則規則群組清單](#) 和 部落格文章 [宣布的 AWS 受管規則 AWS WAF](#)。
- 新的 AWS WAF API – 新的 API 可讓您使用一組 APIs 來設定所有 AWS WAF 資源。為了區分區域和全域應用程式，全新的 API 包含一個 scope 設定。如需 API 的詳細資訊，請參閱 [AWS WAFV2 動作](#) 和 [AWS WAFV2 資料類型](#)。

在 APIs、SDKs、CLIs 和 中 AWS CloudFormation，AWS WAF Classic 會保留其命名機制，而此最新版本的 AWS WAF 會參考新增的 V2 或 v2，視內容而定。

- 簡化的服務配額（限制）– AWS WAF 現在允許每個保護套件或 Web ACL 有更多規則，並可讓您表達較長的規則運算式模式。如需詳細資訊，請參閱[AWS WAF 配額](#)。
- 運算需要決定容量限制 – 保護套件或 Web ACLs 的限制現在是以保護套件或 Web ACL 容量單位 (WCUs) 為基礎。會根據規則所需的操作容量來 AWS WAF 計算規則的 WCUs。保護套件或 Web ACL 的 WCUs 總數等於其所有規則和規則群組的 WCUs 總和。

如需 WCU 的一般資訊，請參閱 [如何 AWS WAF 運作](#)。如需每個規則 WCU 用量的資訊，請參閱 [在中使用規則陳述式 AWS WAF](#)。

- 以文件為基礎的規則寫入 – 您現在可以以 JSON 格式撰寫和表達規則、規則群組和保護套件或 Web ACLs。您不再需要使用個別 API 呼叫來建立不同的條件，然後將條件與規則產生關聯。這大幅簡化了編寫和維護程式碼的方式。當您檢視保護套件或 Web ACLs 時，您可以透過主控台存取保護套件或 Web ACL 的 JSON 格式，方法是選擇將保護套件或 Web ACL 下載為 JSON。當您建立自己的規則時，可以選擇 Rule JSON editor (規則 JSON 編輯器) 來存取其 JSON 表示。
- 規則巢狀化和完整的邏輯操作支援 – 您可以使用邏輯規則陳述式和巢狀化來撰寫複雜的合併規則。您可以建立如 [A AND NOT(B OR C)] 的陳述式。如需詳細資訊，請參閱[在中使用邏輯規則陳述式 AWS WAF](#)。
- 改善速率型規則 – 在最新版本的 中 AWS WAF，您可以自訂規則評估的時間範圍，以及規則如何彙總請求。您可以使用多種 Web 請求特性的組合來自訂彙總。此外，最新的速率型規則會更快地回應流量的變化。如需詳細資訊，請參閱[在中使用以速率為基礎的規則陳述式 AWS WAF](#)。
- IP 集的可變 CIDR 範圍支援 – IP 集規格現在在 IP 範圍內具有更大的靈活性。對於 IPv4，AWS WAF 支援 /1 /32。對於 IPv6，AWS WAF 支援 /1 /128。如需 IP 集合的詳細資訊，請參閱[IP 集合比對規則陳述式](#)。
- 可鏈結的文字轉換 – AWS WAF 可以在檢查之前針對 Web 請求內容執行多個文字轉換。如需詳細資訊，請參閱[在中使用文字轉換 AWS WAF](#)。
- 改善主控台體驗 – 新的 AWS WAF 主控台具有視覺化規則建置器和更使用者直覺式的主控台設計。
- Firewall Manager AWS WAF 政策的擴充選項 – 在 AWS WAF 保護套件或 Web ACLs 的 Firewall Manager 管理中，您現在可以建立一組規則群組，先 AWS WAF 處理，最後 AWS WAF 處理一組規則群組。套用 AWS WAF 政策後，本機帳戶擁有人可以新增自己的規則群組，在這兩個集之間 AWS WAF 處理。如需 Firewall Manager AWS WAF 政策的詳細資訊，請參閱[搭配 Firewall Manager 使用 AWS WAF 政策](#)。
- AWS CloudFormation 支援所有規則陳述式類型 – AWS WAF 中的 AWS CloudFormation 支援 AWS WAF 主控台和 API 支援的所有規則陳述式類型。此外，您可以輕鬆地將以 JSON 格式撰寫的規則轉換為 YAML 格式。

遷移警告與限制

遷移只會處理保護套件或 Web ACL 組態，而且保護套件或 Web ACL 遷移不會像您在 AWS WAF Classic 中一樣轉移所有設定。有些組態項目需要在 AWS WAF (v2) 中手動設定。有幾件事不完全在兩個版本之間映射，您需要決定如何設定 AWS WAF (v2) 中的功能。有些設定，例如保護套件或 Web ACL 與 AWS 資源的關聯，一開始會在新版本中停用，因此您可以在準備好時新增這些設定。

下列清單說明遷移的注意事項，並說明您可能想要採取的任何回應步驟。請使用此概觀來規劃遷移。稍後詳細的遷移步驟會帶您演練建議的緩解步驟。

- 單一帳戶遷移 – 您只能將任何帳戶的 AWS WAF Classic 資源遷移至相同帳戶 AWS WAF 的資源。
- 僅限保護套件或 Web ACL 組態 – 遷移只會遷移保護套件或 Web ACLs 以及保護套件或 Web ACLs 正在使用的資源。若要遷移任何已遷移 Web ACL 未使用的資源，例如規則群組或 IP 集，請在 AWS WAF (v2) 中手動建立資源。
- 無 AWS Marketplace 受管規則 – 遷移不會從 AWS Marketplace 賣方接管任何受管規則。有些 AWS Marketplace 賣方具有對等的受管規則 AWS WAF，您可以再次訂閱。執行此操作之前，請檢閱隨最新版本提供的 AWS 受管規則 AWS WAF。大多數使用者可免費使用。AWS WAF 如需受管規則的相關資訊，請參閱[在中使用受管規則群組 AWS WAF](#)。
- 無保護套件或 Web ACL 關聯 – 遷移不會帶來保護套件或 Web ACL 與受保護資源之間的任何關聯。這是經過設計的，以避免影響您的生產工作負載。確認一切已正確遷移後，請將新的保護套件或 Web ACL 與您的資源建立關聯。
- 已停用記錄 – 遷移保護套件或 Web ACL 的記錄預設為停用。這是設計本身所致。當您準備好從 AWS WAF Classic 切換到時，啟用記錄 AWS WAF。
- 無 AWS Firewall Manager 規則群組 – 遷移不會處理由 Firewall Manager 管理的規則群組。您可以遷移由 Firewall Manager 管理的保護套件或 Web ACL，但遷移不會帶來規則群組。不針對這些保護套件或 Web ACLs 使用遷移工具，而是在 Firewall Manager AWS WAF 中重新建立新的政策。

Note

Firewall Manager 為 AWS WAF Classic 管理的規則群組是 Firewall Manager 規則群組。使用新版本的時 AWS WAF，規則群組是 AWS WAF 規則群組。它們在功能上是一樣的。

- AWS WAF 安全自動化注意事項 – 請勿嘗試遷移任何 AWS WAF 安全自動化。遷移並不會轉換 Lambda 函數，這些函數可能正由自動化使用中。請考慮改為部署最新版本的自動化。如需詳細資訊，請參閱[AWS WAF 安全自動化](#)。

遷移的運作方式

自動化遷移會轉移您的大多數 AWS WAF Classic 保護套件或 Web ACL 組態，留下一些您需要手動處理的物件。

Note

某些保護組態無法自動遷移，且需要在 AWS WAF (v2) 中手動設定。請參閱的清單[遷移警告與限制](#)。

以下列出遷移保護套件或 Web ACL 的高階步驟。

1. 自動化遷移會讀取與現有保護套件或 Web ACL 相關的所有內容，而不會修改或刪除 AWS WAF Classic 中的任何內容。它建立與相容的 Web ACL 及其相關資源的表示 AWS WAF。它會為新的保護套件或 Web ACL 產生 AWS CloudFormation 範本，並將其存放在 Amazon S3 儲存貯體中。
2. 您可以將範本部署到 AWS CloudFormation，以便在 中重新建立保護套件或 Web ACL 和相關資源 AWS WAF。
3. 您可以檢閱保護套件或 Web ACL，並手動完成遷移，確保您的新保護套件或 Web ACL 充分利用最新的功能 AWS WAF。
4. 您手動將受保護的資源切換到新的保護套件或 Web ACL。

將保護套件或 Web ACL 從 AWS WAF Classic 遷移至 AWS WAF

若要遷移保護套件或 Web ACL 並切換到它，請執行自動遷移，然後完成一系列手動步驟。

主題

- [遷移保護套件或 Web ACL：自動遷移](#)
- [遷移保護套件或 Web ACL：手動追蹤](#)
- [遷移保護套件或 Web ACL：其他考量事項](#)
- [遷移保護套件或 Web ACL：切換](#)

遷移保護套件或 Web ACL：自動遷移

自動將保護套件或 Web ACL 組態從 AWS WAF Classic 遷移至 AWS WAF

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 選擇切換至 AWS WAF Classic，並檢閱保護套件或 Web ACL 的組態設定。請記下設定，並考慮前一節[遷移警告與限制](#)中所述的警告和限制。
3. 在頂端的資訊對話中，找到以遷移保護套件或 Web ACLs 開頭的句子，然後選擇遷移精靈的連結。這會啟動遷移精靈。

如果您沒有看到資訊性對話，則自啟動 AWS WAF Classic 主控台以來，您可能已經將其關閉。在導覽列中，選擇切換到新的 AWS WAF，然後選擇切換到 AWS WAF 傳統，而資訊性對話應該會重新出現。

4. 選取您要遷移的保護套件或 Web ACL。
5. 針對遷移組態，提供用於範本的 Amazon S3 儲存貯體。您需要已針對遷移 API 正確設定的 Amazon S3 儲存貯體，才能存放其產生的 AWS CloudFormation 範本。
 - 如果儲存貯體已加密，加密必須使用 Amazon S3 (SSE-S3) 金鑰。遷移不支援使用 AWS Key Management Service (SSE-KMS) 金鑰加密。
 - 儲存貯體名稱必須以 `aws-waf-migration-` 開頭。例如 `aws-waf-migration-my-web-acl`。
 - 儲存貯體必須位於您要部署範本的區域中。例如，對於 `us-west-2` 中的保護套件或 Web ACL，您必須在 `us-west-2` 中使用 Amazon S3 儲存貯體，而且必須將範本堆疊部署到 `us-west-2`。
6. 對於 S3 bucket policy (S3 儲存貯體政策)，建議您選擇 Auto apply the bucket policy required for migration (自動套用遷移所需的儲存貯體政策)。如果您選擇自行管理儲存貯體，則必須手動套用下列儲存貯體政策：
 - 對於全域 Amazon CloudFront 應用程式 (waf)：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "apiv2migration.waf.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
    * "
      }
    ]
  }

```

- 對於區域 Amazon API Gateway 或 Application Load Balancer 應用程式 (waf-regional) :

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "apiv2migration.waf-regional.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
    * "
      }
    ]
  }

```

7. 針對 Choose how to handle rules that cannot be migrated (選擇如何處理無法遷移的規則)，選擇排除無法遷移的規則，或停止遷移。如需無法遷移之規則的相關資訊，請參閱[遷移警告與限制](#)。
8. 選擇下一步。
9. 對於建立 AWS CloudFormation 範本，驗證您的設定，然後選擇開始建立 AWS CloudFormation 範本以開始遷移程序。這可能需要幾分鐘的時間，取決於保護套件或 Web ACL 的複雜性。
10. 在建立和執行 AWS CloudFormation 堆疊以完成遷移中，您可以選擇前往 AWS CloudFormation 主控台從範本建立堆疊，以建立新的保護套件或 Web ACL 及其資源。若要這樣做，請選擇建立 AWS CloudFormation 堆疊。

自動遷移程序完成後，您就可以繼續進行手動後續步驟。請參閱[遷移保護套件或 Web ACL：手動追蹤](#)。

遷移保護套件或 Web ACL：手動追蹤

自動化遷移完成後，請檢閱新建立的保護套件或 Web ACL，並填入遷移不會為您接管的元件。下列程序涵蓋遷移未處理的保護套件或 Web ACL 管理層面。如需清單，請參閱[遷移警告與限制](#)。

完成基本遷移 - 手動步驟

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/homev2> 開啟 AWS WAF 主控台。
2. 主控台應該自動使用最新版本的 AWS WAF。若要驗證這一點，請在導覽窗格中檢查您是否可以看到切換到 AWS WAF 傳統選項。如果您看到切換到新的 AWS WAF，請選擇該項目以切換到最新版本。
3. 在導覽窗格中，選擇保護套件或 Web ACLs。
4. 在保護套件或 Web ACLs 頁面中，在建立保護套件的區域清單中找到新的保護套件或 Web ACL。選擇保護套件或 Web ACL 的名稱，以顯示保護套件或 Web ACL 的設定。
5. 針對您先前的 AWS WAF Classic Web ACL，檢閱新保護套件或 Web ACL 的所有設定。根據預設，會停用記錄日誌和受保護的資源關聯。您可以在準備好切換時啟用這些功能。
6. 如果您的 AWS WAF Classic 保護套件或 Web ACL 具有受管規則群組，則不會在遷移中包含規則群組。您可以將受管規則群組新增至新的保護套件或 Web ACL。在檢閱受管規則群組的相關資訊，包括可與新版本搭配使用的 AWS 受管規則清單 AWS WAF [在中使用受管規則群組 AWS WAF](#)。若要新增受管規則群組，請執行下列動作：
 - a. 在保護套件或 Web ACL 設定頁面中，選擇保護套件或 Web ACL 規則索引標籤。
 - b. 選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。
 - c. 展開您所選廠商的清單，然後選取您要新增的規則群組。對於 AWS Marketplace 賣方，您可能需要訂閱規則群組。如需在保護套件或 Web ACL 中使用受管規則群組的詳細資訊，請參閱 [在中使用受管規則群組 AWS WAF](#) 和 [在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

完成基本遷移程序之後，我們建議您檢閱您的需求並考慮其他選項，以確保新的組態盡可能有效率，並且使用最新可用的安全選項。請參閱[遷移保護套件或 Web ACL：其他考量事項](#)。

遷移保護套件或 Web ACL：其他考量事項

檢閱您的新保護套件或 Web ACL，並考慮新中可用的選項，AWS WAF 以確保組態盡可能有效率，並且使用最新的可用安全選項。

其他 AWS 受管規則

請考慮在您的保護套件或 Web ACL 中實作其他 AWS 受管規則，以提高應用程式的安全狀態。這些包含在 AWS WAF 中，無需額外費用。AWS 受管規則具有下列類型的規則群組：

- 基準規則群組可針對各種常見威脅提供一般保護，例如停止已知的錯誤輸入進入您的應用程式，以及防止管理頁面存取。
- 使用案例特定的規則群組可為眾多不同的使用案例和環境提供增量式保護。
- IP 評價清單會根據用戶端的來源 IP 提供安全威脅情報。

如需詳細資訊，請參閱[AWS 的受管規則 AWS WAF](#)。

規則最佳化與清理

重新查看您的舊規則，並考慮進行重寫或刪除過時的規則將它們最佳化。例如，如果您過去從 OWASP 前 10 個 Web 應用程式漏洞的技術論文中部署 AWS CloudFormation 範本，[使用 AWS WAF 和我們的新白皮書準備 OWASP 前 10 個 Web 應用程式漏洞](#)，您應該考慮將其取代為 AWS 受管規則。雖然在文件中找到的概念仍然適用，並可協助您撰寫自己的規則，但由範本建立的規則大部分已由 AWS 受管規則取代。

Amazon CloudWatch 指標和警示

重新檢視您的 Amazon CloudWatch 指標，並視需要設定警示。遷移不會轉移 CloudWatch 警示，而且您的指標名稱可能不是您想要的名稱。

與您的應用程式團隊一起審核

與您的應用程式團隊合作，並檢查您的安全狀態。找出應用程式經常剖析的欄位，並相應地新增規則來清理輸入。檢查是否有任何邊緣案例，如果應用程式的商業邏輯無法處理，新增規則以找出這些案例。

規劃切換

與您的應用程式團隊一起規劃切換的時機。從舊的保護套件或 Web ACL 關聯切換到新的保護套件，可能需要一點時間才能傳播到儲存資源的所有區域。傳播時間可以是幾秒鐘到幾分鐘。在此期間，某些請求將由舊的保護套件或 Web ACL 處理，而其他請求將由新的保護套件或 Web ACL 處理。您的資源將在整個切換過程中受到保護，但您可能會在切換進行期間注意到請求處理不一致。

當您準備好切換時，請按照[遷移保護套件或 Web ACL：切換](#)中的程序進行操作。

遷移保護套件或 Web ACL：切換

驗證新的保護套件或 Web ACL 設定後，您可以開始使用它來取代 AWS WAF Classic 保護套件或 Web ACL。

開始使用新的 AWS WAF 保護套件或 Web ACL

1. 遵循 中的指引，將 AWS WAF 保護套件或 Web ACL 與您要保護的資源建立關聯[將保護與 AWS 資源建立關聯或取消關聯](#)。這會自動取消資源與舊保護套件或 Web ACL 的關聯。

轉換可能需要幾秒鐘到幾分鐘的時間才能傳播。在此期間，有些請求可能由舊的保護套件或 Web ACL 處理，有些則由新的保護套件或 Web ACL 處理。您的資源將在整個切換過程中受到保護，但您可能會注意到請求處理中的不一致，直到完成為止。

2. 遵循 中的指引，設定新保護套件或 Web ACL 的記錄[記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
3. （選用）如果您的 AWS WAF Classic 保護套件或 Web ACL 不再與任何資源相關聯，請考慮將其完全從 AWS WAF Classic 中移除。如需相關資訊，請參閱[刪除 Web ACL](#)。

AWS WAF 傳統

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS WAF Classic 是一種 Web 應用程式防火牆，可讓您監控轉送至 Amazon API Gateway API、Amazon CloudFront 或 Application Load Balancer 的 HTTP 和 HTTPS 請求。AWS WAF Classic 也可讓您控制對內容的存取。根據您指定的條件，例如請求的 IP 地址或查詢字串的值，API Gateway、CloudFront 或 Application Load Balancer 會使用請求的內容或 HTTP 403 狀態碼（禁止）回應請求。您也可以設定 CloudFront 在請求遭到封鎖時傳回自訂錯誤頁面。

主題

- [設定 AWS WAF Classic](#)
- [AWS WAF Classic 的運作方式](#)
- [AWS WAF 傳統定價](#)
- [Classic 入門 AWS WAF](#)
- [建立和設定 Web 存取控制清單 \(Web ACL\)](#)
- [使用 AWS WAF Classic 規則群組搭配 AWS Firewall Manager](#)
- [開始使用 AWS Firewall Manager 以啟用 AWS WAF Classic 規則](#)
- [教學課程：使用階層規則建立 AWS Firewall Manager 政策](#)
- [記錄 Web ACL 流量資訊](#)
- [以速度為基礎的規則列出封鎖的 IP 地址](#)
- [AWS WAF Classic 如何與 Amazon CloudFront 功能搭配使用](#)

- [AWS WAF Classic 中的安全性](#)
- [AWS WAF 傳統配額](#)

設定 AWS WAF Classic

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立了 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需的最新版本 AWS WAF，請參閱 [AWS WAF](#)。

本主題說明初步步驟，例如建立使用者帳戶，以準備使用 AWS WAF Classic。您不需要支付這些費用。您只需為所使用的 AWS 服務付費。

Note

如果您是新使用者 AWS WAF，請不要遵循 AWS WAF Classic 的這些設定步驟。相反地，請遵循 AWS WAF 中最新版本的步驟 [設定您的帳戶以使用服務](#)。

完成這些步驟後，請參閱 [Classic 入門 AWS WAF](#) 繼續開始使用 AWS WAF Classic。

Note

AWS Shield Standard 包含在 AWS WAF Classic 中，不需要額外的設定。如需詳細資訊，請參閱 [AWS Shield 和 Shield Advanced 如何運作](#)。

第一次使用 AWS WAF Classic 或 AWS Shield Advanced 之前，請完成本節中的步驟。

主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)
- [下載工具](#)

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

1. 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](#)。

2. 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](#)。

下載工具

AWS Management Console 包含 AWS WAF Classic 的主控台，但如果您想要以程式設計方式存取 AWS WAF Classic，請參閱以下內容：

- 如果您想要呼叫 AWS WAF Classic API，而不必處理低階詳細資訊，例如組合原始 HTTP 請求，您可以使用 AWS SDK。AWS SDKs 提供函數和資料類型，可封裝 AWS WAF Classic 和其他 AWS 服務的功能。若要下載 AWS SDK，請參閱適用的頁面，其中包含先決條件和安裝指示：
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)

- [Node.js](#)
- [PHP](#)
- [Python](#)
- [Ruby](#)

如需完整的 AWS SDKs 清單，請參閱[適用於 Amazon Web Services 的工具](#)。

- 如果您使用的程式設計語言 AWS 不提供 SDK，則 [AWS WAF API 參考](#) 會記錄 AWS WAF Classic 支援的操作。
- AWS Command Line Interface (AWS CLI) 支援 AWS WAF Classic。AWS CLI 可讓您從命令列控制多個 AWS 服務，並透過指令碼將其自動化。如需詳細資訊，請參閱[AWS Command Line Interface](#)。
- AWS Tools for Windows PowerShell 支援 AWS WAF Classic。如需詳細資訊，請參閱 [AWS Tools for PowerShell Cmdlet 參考](#)。

AWS WAF Classic 的運作方式

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

您可以使用 AWS WAF Classic 來控制 API Gateway、Amazon CloudFront 或 Application Load Balancer 如何回應 Web 請求。首先，建立條件、規則和 web 存取控制清單 (Web ACL)。定義您的條件，並將您的條件組合成規則，再組合這些規則到 Web ACL 中。

 Note

您也可以使用 AWS WAF Classic 來保護託管在 Amazon Elastic Container Service (Amazon ECS) 容器中的應用程式。Amazon ECS 是一種高度可擴展的快速容器管理服務，可讓您輕鬆地在叢集上執行、停止和管理 Docker 容器。若要使用此選項，請將 Amazon ECS 設定為使用啟用 AWS WAF Classic 的 Application Load Balancer，以路由和保護服務中任務之間的 HTTP/HTTPS（第 7 層）流量。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 [Service Load Balancing](#) 主題。

條件

條件定義您希望 AWS WAF Classic 在 Web 請求中監看的基本特性：

- 指令碼可能為惡意。攻擊者可以利用 web 應用程式的漏洞內嵌指令碼。此為跨網站指令碼。
- 發出請求的 IP 地址或地址範圍。
- 發出請求的國家/地區或地理位置。
- 指定請求的部分長度，例如：查詢字串。
- SQL 程式碼可能為惡意。攻擊者會藉由內嵌惡意 SQL 程式碼於 web 請求中，嘗試從您的資料庫碼擷取資料。此為 SQL injection。
- 字串會出現在請求，例如出現在 User-Agent 標頭的值或出現在查詢字串的文字字串。您也可以使用規則運算式 (regex) 指定這些字串。

某些條件採用多種數值 例如，您可以指定(最多) 10,000 個 IP 地址或在此 IP 條件下的 IP 地址範圍。

規則

您可以將條件結合到規則中，以精確鎖定您想要允許、封鎖或計數的請求。AWS WAF Classic 提供兩種類型的規則：

一般規則

一般規則只使用條件針對特定請求。例如，根據最近已知攻擊者的請求，您可建立包括以下條件的規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。
- 它們好像有包含類似 SQL 程式碼的查詢字串。

當規則包含多個條件時，如本範例所示，AWS WAF Classic 會尋找符合所有條件的請求，也就是一起尋找 AND 條件。

請至少新增一項條件至一般規則。沒有條件的一般規則無法符合任何請求，因此永遠不會觸發規則的動作（允許、計數或封鎖）。

以速率為基礎的規則

以速率為基礎的規則就像一般規則，但增加了速率限制。以速率為基礎的規則會計算從滿足規則條件的 IP 地址抵達的請求數。如果在五分鐘期間內，來自 IP 地址的請求超過速率限制，規則就會觸發動作。可能需要一兩分鐘的時間，動作才會觸發。

條件對以速率為基礎的規則來說是選用的。如果您未在以速率為基礎的規則中新增任何條件，速率限制會套用到所有 IP 地址。如果您結合條件與速率限制，速率限制會套用到符合條件的 IP 地址。

例如，根據最近已知攻擊者的請求，您可建立包括以下條件的以速率為基礎的規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。

在這以速率為基礎的規則中，您還可以定義的速率限制。在這個範例中，假設您建立的速率限制為 1,000。同時符合這兩種條件且每五分鐘超過 1,000 的請求，會觸發此規則在 Web ACL 定義的動作（封鎖或計數）。

未同時符合這兩個條件的請求不會計入速率限制，也不會受到此規則影響。

在第二個範例中，假設您想要限制對您網站的特定頁面所發出的請求。若要這麼做，您可以新增以下字串比對條件至以速率為基礎的規則中：

- 要篩選的請求部分是 URI。
- 請求類型是 Starts with。
- 符合值是 login。

更進一步，您需要指定 RateLimit 為 1,000。

將這個以速率為基礎的規則新增到 Web ACL，您就可以限制對您登入頁面的請求數量，但不影響網站的其他部分。

Web ACL

將您的條件組合成規則後，再組合這些規則到 Web ACL 中。在這裡，您可以為每個規則定義動作，例如允許、封鎖或計數，以及預設動作：

每個規則的動作

當 Web 請求符合規則中的所有條件時，AWS WAF Classic 可以封鎖請求或允許將請求轉送至 API Gateway API、CloudFront 分佈或 Application Load Balancer。您可以指定要 AWS WAF Classic 為每個規則執行的動作。

AWS WAF Classic 會根據您列出規則的順序，將請求與 Web ACL 中的規則進行比較。AWS WAF 然後，Classic 會採取與請求比對的第一個規則相關聯的動作。例如，如果 Web 請求符合允許請求的規則和封鎖請求的規則，AWS WAF Classic 會根據最先列出的規則來允許或封鎖請求。

如果您想要在開始使用新規則之前進行測試，您也可以設定 AWS WAF Classic 來計算符合規則中所有條件的請求。與允許或封鎖請求的規則一樣，計數請求的規則受其自身在 web ACL 清單上所列的順序影響。例如，如果 web 請求符合兩個規則，一個為允許請求，另一個為計數請求，如果該允許請求的規則先列於清單，則不會對此請求進行計數。

預設動作

預設動作會判斷 AWS WAF Classic 是否允許或封鎖不符合 Web ACL 中任何規則中所有條件的請求。例如，假設您建立 Web ACL，僅新增您之前定義過的規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。
- 它們好像有包含惡意 SQL 的查詢字串。

如果請求不符合規則中的所有三個條件，且預設動作為 ALLOW，AWS WAF Classic 會將請求轉送至 API Gateway、CloudFront 或 Application Load Balancer，且服務會以請求的物件回應。

如果您將兩個或多個規則新增至 Web ACL，只有在請求不符合任何規則中的所有條件時，AWS WAF Classic 才會執行預設動作。例如，假設您新增第二個規則，其中含有一項條件：

- 請求在 User-Agent 標頭有 BIGBadBot 值。

AWS WAF Classic 只有在請求不符合第一個規則中的所有三個條件，且不符合第二個規則中的一個條件時，才會執行預設動作。

在某些情況下，AWS WAF 可能會遇到內部錯誤，延遲回應 Amazon API Gateway、Amazon CloudFront 或 Application Load Balancer 是否允許或封鎖請求。在這些情況下，CloudFront 通常會允許請求或提供內容。API Gateway 和應用程式負載平衡器通常則會拒絕請求，而且不會處理內容。

AWS WAF 傳統定價

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

使用 AWS WAF Classic 時，您只需支付您建立 ACLs 和規則，以及 AWS WAF Classic 檢查的 HTTP 請求數量。如需詳細資訊，請參閱 [AWS WAF Classic Pricing](#)。

Classic 入門 AWS WAF

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

本教學課程說明如何使用 AWS WAF Classic 來執行下列任務：

- 設定 AWS WAF Classic。

- 使用 AWS WAF Classic 主控台建立 Web 存取控制清單 (Web ACL)，並指定您要用來篩選 Web 請求的條件。例如，您可以指定請求源於的 IP 地址和僅由攻擊者使用的請求數值。
- 新增條件至規則。規則可讓您定位要封鎖或允許的 web 請求。Web 請求必須符合 AWS WAF Classic 區塊之前規則中的所有條件，或根據您指定的條件允許請求。
- 新增規則至您的 Web ACL。可以在此處指定您是否想要根據所新增至每個規則的條件來允許或封鎖 web 請求。
- 指定預設動作 (封鎖或允許)。這是 AWS WAF Classic 在 Web 請求不符合您的任何規則時所採取的動作。
- 選擇您希望 AWS WAF Classic 檢查 Web 請求的 Amazon CloudFront 分佈。本教學課程僅涵蓋 CloudFront 的步驟，但 Application Load Balancer 和 Amazon API Gateway APIs 的程序基本上是相同的。AWS WAF Classic for CloudFront 適用於所有 AWS 區域。AWS WAF Classic 可與 API Gateway 搭配使用，或 Application Load Balancer 可用於[AWS 服務端點](#)列出的區域。

Note

AWS 通常針對您在本教學課程中建立的資源，每天收取不到 0.25 美元的費用。當您完成此教學課程，我們建議您刪除資源以免產生不必要的費用。

主題

- [步驟 1：設定 AWS WAF Classic](#)
- [步驟二：建立 Web ACL](#)
- [步驟 3：建立 IP 比對條件](#)
- [步驟 4：建立地理比對條件](#)
- [步驟 5：建立字串比對條件](#)
- [步驟 5A：建立 Regex 條件 \(選用\)](#)
- [步驟 6：建立 SQL Injection 比對條件](#)
- [步驟 7：\(選用\) 建立其他條件](#)
- [步驟 8：建立規則並新增條件](#)
- [步驟 9：新增規則至 Web ACL](#)
- [步驟 10：清理您的資源](#)

步驟 1：設定 AWS WAF Classic

如果您尚未遵循 中的一般設定步驟[設定 AWS WAF Classic](#)，請立即執行此操作。

步驟二：建立 Web ACL

AWS WAF Classic 主控台會引導您完成設定 AWS WAF Classic 的程序，以根據您指定的條件封鎖或允許 Web 請求，例如請求來源的 IP 地址或請求中的值。在此步驟中，建立 Web ACL。

建立 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 如果這是您第一次使用 AWS WAF Classic，請選擇移至 AWS WAF Classic，然後選擇設定 Web ACL。

如果您之前已使用 AWS WAF 過 Classic，請在導覽窗格中選擇 Web ACLs，然後選擇建立 Web ACL。

3. 在 Name web ACL (命名 Web ACL) 頁面的 Web ACL name (Web ACL 名稱) 中輸入名稱。

Note

建立 Web ACL 後無法修改名稱。

4. 針對 CloudWatch 指標名稱，輸入名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)。不能含有空格。

Note

建立 Web ACL 後無法修改名稱。

5. 對於 區域，選擇一個區域。如果您要將此 Web ACL 與 CloudFront 分佈建立關聯，請選擇全域 (CloudFront)。
6. 對於要關聯的 AWS 資源，選擇您想要將此 Web ACL 關聯的資源，然後選擇下一步。

步驟 3：建立 IP 比對條件

IP 比對條件可指定發出請求的 IP 地址或 IP 地址範圍。在此步驟中，建立 IP 比對條件。在後續步驟中，您指定是否要允許或封鎖來自指定 IP 地址的請求。

Note

如需 IP 比對條件的詳細資訊，請參閱[使用 IP 比對條件](#)。

建立 IP 比對條件

1. 在建立條件頁面，於 IP 符合條件，選擇建立條件。
2. 在 Create IP match condition (建立 IP 比對條件) 對話方塊中，於 Name (名稱)，輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_! " # ' + * } , . /。
3. 針對 Address (地址)，輸入 192.0.2.0/24。指定於 CIDR 符號的此 IP 地址範圍，包含 IP 地址，從 192.0.2.0 192.0.2.255。(例如，預留 192.0.2.0/24 IP 地址範圍，則沒有任何 web 請求會來自這些 IP 地址)。

AWS WAF Classic 支援 IPv4 地址範圍：/8 和 /16 到 /32 之間的任何範圍。AWS WAF Classic 支援 IPv6 地址範圍：/24、/32、/48、/56、/64 和 /128。(若要指定單一 IP 地址，例如 192.0.2.44，請輸入 192.0.2.44/32)。不支援其他範圍。

如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 文章 [無類別網域間路由](#)。

4. 選擇 Create (建立)。

步驟 4：建立地理比對條件

地理比對條件指定國家/地區為請求的發源地。在此步驟中，建立地理比對條件。在後續步驟中，您指定是否要允許或封鎖來自指定國家/地區的請求。

Note

如需地理比對條件的詳細資訊，請參閱[使用地理比對條件](#)。

建立地理比對條件

1. 在建立條件頁面，於地理符合條件，選擇建立條件。
2. 在 Create geo match condition (建立地理比對條件) 對話方塊中，於 Name (名稱)，輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_!"#`+*},./。
3. 選擇位置類型和國家/地區。目前，Location type (位置類型) 只能是 Country (國家/地區)。
4. 選擇新增位置。
5. 選擇 Create (建立)。

步驟 5：建立字串比對條件

字串比對條件可識別您希望 AWS WAF Classic 在請求中搜尋的字串，例如標頭或查詢字串中的指定值。通常，字串包含可列印 ASCII 字元，但您可以指定十六字元範圍 0x00 到 0xFF 的任何字元 (小數點 0 到 255)。在此步驟中，建立字串比對條件。在後續步驟中，您指定是否要允許或封鎖含有指定字串的請求。

Note

如需字串比對條件的詳細資訊，請參閱[使用字串比對條件](#)。

建立字串比對條件

1. 在 Create conditions (建立條件) 頁面，於 String and regex match conditions (字串和 regex 符合條件) 選擇 Create condition (建立條件)。
2. 在 Create string match condition (建立字串比對條件) 對話方塊中，輸入以下的值：

名稱

輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_!"#`+*},./。

Type

選擇 String match (字串比對)。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查指定字串的 Web 請求部分。

在此範例中，請選擇 Header (標頭)。

 Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)，因為 CloudFront 只會轉送前 8192 個位元組以進行檢查。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

標頭 (必要，如果「部分請求的篩選條件」為「標頭」時)

由於您為要篩選的部分請求選擇標頭，因此您必須指定要讓 AWS WAF Classic 檢查的標頭。輸入 User-Agent (使用者代理程式)。(此值不區分大小寫)。

符合類型

選擇指定字串必須顯示在 User-Agent (使用者代理程式) 標頭中的位置，例如，在開始時或在字串中。

在此範例中，選擇完全相符，這表示 AWS WAF Classic 會檢查 Web 請求的標頭值是否與您指定的值相同。

轉換

為了繞過 AWS WAF Classic，攻擊者會在 Web 請求中使用不尋常的格式，例如新增空格或 URL 編碼部分或全部請求。轉換藉由移除空格、URL 解碼、或執行其他操作可以降低攻擊常使用的不常見格式，將 web 請求轉換成更標準的格式。

您只能指定一種文字轉換類型。

在此範例中，請選擇 None (無)。

base64 編碼值

如果您於 Value to match (符合值) 輸入的值是 base64 編碼，請選取此核取方塊。

在此範例中，不需選取核取方塊。

符合值

指定您希望 AWS WAF Classic 在 Web 請求部分中搜尋的值，而您在要篩選的請求部分中表示。

在此範例中，輸入 `BadBot`。AWS WAF Classic 會檢查 Web 請求中的 `User-Agent` 標頭是否有 `BadBot` 值。

符合值的長度上限為 50 個字元。如果您想要指定 base64 編碼值，可在編碼前提供最多 50 個字元。

3. 如果您希望 AWS WAF Classic 檢查 Web 請求是否有多個值，例如包含的 `User-Agent` 標頭 `BadBot` 和包含的查詢字串 `BadParameter`，您有兩種選擇：
- 如果您想要當它們含有兩者得的值時 (AND) 才允許或封鎖 web 請求，您可以為每個值建立一個字串比對條件。
 - 如果您想要當它們含有其中一個值或兩者的值時 (OR) 才允許或封鎖 web 請求，您可以新增兩者的值至相同的字串比對條件中。

在本範例中，請選擇 `Create` (建立)。

步驟 5A：建立 Regex 條件 (選用)

規則表達式條件是一種字串比對條件，類似 `String match`，它識別您希望 AWS WAF Classic 在請求中搜尋的字串，例如標頭或查詢字串中的指定值。主要差別是您使用規則表達式 (regex) 來指定您要 AWS WAF Classic 搜尋的字串模式。在此步驟中，建立 regex 比對條件。在後續步驟中，您指定是否要允許或封鎖含有指定字串的請求。

Note

如需規則運算式比對條件的詳細資訊，請參閱[使用 Regex 比對條件](#)。

建立 regex 比對條件

1. 在 `Create conditions` (建立條件) 頁面，於 `String match and regex conditions` (字串符合和 regex 條件) 選擇 `Create condition` (建立條件)。
2. 在 `Create string match condition` (建立字串比對條件) 對話方塊中，輸入以下的值：

名稱

輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：`_!\"#'+*},./`。

Type

選擇 Regex match (Regex 比對)。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查指定字串的 Web 請求部分。

在此範例中，請選擇 Body (內容主體)。

Note

如果您選擇內文作為要篩選之請求部分的值，AWS WAF 則 Classic 只會檢查前 8192 個位元組 (8 KB)，因為 CloudFront 只會轉送前 8192 個位元組以進行檢查。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

轉換

為了繞過 AWS WAF Classic，攻擊者會在 Web 請求中使用不尋常的格式，例如新增空格或 URL 編碼部分或全部請求。轉換藉由移除空格、URL 解碼、或執行其他操作可以降低攻擊常使用的不常見格式，將 web 請求轉換成更標準的格式。

您只能指定一種文字轉換類型。

在此範例中，請選擇 None (無)。

比對請求的 Regex 模式

選擇 Create regex pattern set (建立 Regex 模式集)。

新模式集的名稱

輸入名稱，然後指定您要 AWS WAF Classic 搜尋的 regex 模式。

接著，輸入規則表達式 `!【a@】mAB【a@】dRequest`。AWS WAF Classic 將檢查 Web 請求中的 User-Agent 標頭是否有值：

- `!amABadRequest`
- `!amAB@dRequest`
- `!@mABadRequest`

- l@mAB@dRequest

3. 選擇 Create pattern set and add filter (建立模式集並新增篩選條件)。
4. 選擇 Create (建立)。

步驟 6：建立 SQL Injection 比對條件

SQL 注入比對條件可識別 Web 請求的部分，例如您要 AWS WAF Classic 檢查惡意 SQL 程式碼的標頭或查詢字串。攻擊者使用 SQL 查詢來擷取您資料庫的資料。在此步驟中，建立 SQL injection 比對條件。在後續步驟中，您指定是否要允許或封鎖貌似含有惡意 SQL 程式碼的請求。

Note

如需字串比對條件的詳細資訊，請參閱[使用 SQL Injection 比對條件](#)。

建立 SQL Injection 比對條件

1. 在 Create conditions (建立條件) 頁面，於 SQL injection match conditions (SQL injection 符合條件)，選擇 Create condition (建立條件)。
2. 在 Create SQL injection match condition (建立 SQL injection 比對條件) 對話方塊中，輸入以下的值：

名稱

輸入名稱。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查惡意 SQL 程式碼的 Web 請求部分。

在此範例中，選擇 Query string (查詢字串)。

Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)，因為 CloudFront 只會轉送前 8192 個位元組以進行檢查。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

轉換

在此範例中，請選擇 URL decode (URL 解碼)。

攻擊者會使用不尋常的格式，例如 URL 編碼，以嘗試繞過 AWS WAF Classic。在 AWS WAF Classic 檢查請求之前，URL 解碼選項會消除 Web 請求中的部分格式。

您只能指定一種文字轉換類型。

3. 選擇 Create (建立)。
4. 選擇 Next (下一步)。

步驟 7：(選用) 建立其他條件

AWS WAF Classic 包含其他條件，包括下列項目：

- 大小限制條件 – 識別 Web 請求的部分，例如您要 AWS WAF Classic 檢查長度的標頭或查詢字串。如需詳細資訊，請參閱[使用容量限制條件](#)。
- 跨網站指令碼比對條件 – 識別 AWS WAF 您要檢查惡意指令碼的 Web 請求部分，例如標頭或查詢字串。如需詳細資訊，請參閱[使用跨網站指令碼比對條件](#)。

您可以現在選擇性地建立這些條件，或者您可以略過此步驟，前往 [步驟 8：建立規則並新增條件](#)。

步驟 8：建立規則並新增條件

您可以建立規則來指定您希望 AWS WAF Classic 在 Web 請求中搜尋的條件。如果您將多個條件新增至規則，Web 請求必須符合 AWS WAF Classic 規則中的所有條件，才能根據該規則允許或封鎖請求。

Note

如需規則的詳細資訊，請參閱[使用規則](#)。

建立規則並新增條件

1. 在 Create rules (建立規則) 頁面上，選擇 Create rules (建立規則)。

2. 在 Create rules (建立規則) 對話方塊中，輸入以下的值：

名稱

輸入名稱。

CloudWatch 指標名稱

輸入 AWS WAF Classic 將建立並將與規則建立關聯的 CloudWatch 指標名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)。不能含有空格。

規則類型

選擇 Regular rule (一般規則) 或 Rate-based rule (以速率為基礎的規則)。以速率為基礎的規則與一般規則相同，但還會考慮每五分鐘，從已識別的 IP 地址所發出的請求數量。如需這些規則類型的詳細資訊，請參閱[AWS WAF Classic 的運作方式](#)。在此範例中，選擇 Regular rule。

速率限制

對於以速率為基礎的規則，輸入五分鐘期間內允許來自符合規則條件之 IP 地址的最大請求數量。

3. 對於您希望新增到規則的第一個條件，請指定以下設定：

- 根據 Web 請求是否符合條件中的設定，選擇是否要讓 AWS WAF Classic 允許或封鎖請求。

在此範例中，請選擇 does (有符合)。

- 選擇您想新增至規則的條件類型：IP 比對設定條件、字串比對設定條件、或是 SQL injection 比對設定條件。

在此範例中，選擇 originate from IP addresses in (源於的 IP 地址)。

- 選擇要新增到規則的條件。

在此範例中，選擇您在上一任務中所建立的 IP 比對條件。

4. 選擇新增條件。

5. 新增您之前建立的地理比對條件。指定下列值：

- When a request does (當請求有)
- 源於的地理位置
- 選擇您的地理比對條件。

6. 選擇新增其他條件。

7. 新增您之前建立的字串比對條件。指定下列值：

- When a request does (當請求有)
- 至少符合字串比對條件裡的一項篩選條件
- 選擇您的字串比對條件。

8. 選擇新增條件。

9. 新增您之前建立的 SQL injection 比對條件。指定下列值：

- When a request does (當請求有)
- 至少符合 SQL injection 比對條件裡的一項篩選條件
- 選擇您的 SQL injection 比對條件。

10. 選擇新增條件。

11. 新增您之前建立的容量限制條件。指定下列值：

- When a request does (當請求有)
- 至少符合容量限制條件裡的一項篩選條件
- 選擇您的容量限制條件。

12. 如果您建立任何其他的條件，例如 regex 條件，以相同方式新增。

13. 選擇 Create (建立)。

14. 對於 Default action (預設動作)，選擇 Allow all requests that don't match any rules (允許不符合任何規則的請求)。

15. 選擇 Review and create (檢閱和建立)。

步驟 9：新增規則至 Web ACL

當您新增規則至 Web ACL，您可以指定以下設定：

- 您希望 AWS WAF Classic 對符合規則中所有條件的 Web 請求採取的動作：允許、封鎖或計數請求。
- Web ACL 的預設動作。這是您希望 AWS WAF Classic 對不符合規則中所有條件的 Web 請求採取的動作：允許或封鎖請求。

AWS WAF Classic 會開始封鎖符合下列所有條件的 CloudFront Web 請求（以及您可能新增的任何其他請求）：

- User-Agent 標頭的值為 BadBot
- (如果您建立並新增 regex 條件) Body 的值為任何符合 `I[a@]mAB[a@]dRequest` 模式的四個字串 (four strings)。
- 發出請求的 IP 地址範圍為 192.0.2.0-192.0.2.255
- 您在地理比對條件中選取發出請求的國家/地區
- 請求貌似有包含惡意 SQL 的查詢字串。

AWS WAF Classic 可讓 CloudFront 回應不符合這三個條件的任何請求。

步驟 10：清理您的資源

現在，您已成功完成教學課程。為了防止您的帳戶產生額外的 AWS WAF Classic 費用，您應該清除您建立的 AWS WAF Classic 物件。或者，您可以變更設定，以確實比對要允許、封鎖和計數的 web 請求。

Note

AWS 通常針對您在本教學課程中建立的資源，每天收取不到 0.25 美元的費用。當您完成時，我們建議您刪除資源以免產生不必要的費用。

刪除 AWS WAF Classic 收取的物件

1. 取消 Web ACL 與 CloudFront 分佈的關聯：

- a. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

- b. 選擇您要刪除的 Web ACL 名稱。這會開啟頁面，並在右側窗格中顯示 Web ACL 的詳細資訊。
- c. 在右窗格中的規則索引標籤上，AWS 使用此 Web ACL 區段前往資源。對於您建立 Web ACL 關聯的 CloudFront 分佈，請在類型欄中選擇 x。

2. 從您的規則移除條件：

- a. 在導覽窗格中，選擇規則。
- b. 選擇在本教學課程中建立的規則。

- c. 選擇編輯規則。
 - d. 選擇每個條件標題右邊的 x。
 - e. 選擇更新。
3. 從您的 Web ACL 移除規則，以及刪除 Web ACL：
 - a. 在導覽窗格中，選擇 Web ACL。
 - b. 選擇您在教學課程中建立的 Web ACL 名稱。這會開啟頁面，並在右側窗格中顯示 Web ACL 的詳細資訊。
 - c. 在規則標籤上，選擇 Edit web ACL (編輯 Web ACL)。
 - d. 選擇每個規則標題右邊的 x。
 - e. 選擇 Actions (動作)，然後選擇 Delete web ACL (刪除 Web ACL)。
4. 刪除您的規則：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇在本教學課程中建立的規則。
 - c. 選擇 刪除。
 - d. 在刪除對話方塊中，再次選擇刪除確認。

AWS WAF Classic 不會針對條件收費，但如果您想要完成清除，請執行下列程序，從條件中移除篩選條件並刪除條件。

刪除篩選條件和條件

1. 刪除您的 IP 比對條件的 IP 地址範圍，以及刪除 IP 比對條件：
 - a. 在 AWS WAF Classic 主控台的導覽窗格中，選擇 IP 地址。
 - b. 選擇在本教學課程中建立的 IP 比對條件。
 - c. 選取您新增的 IP 地址範圍的核取方塊。
 - d. 選擇刪除 IP 地址或範圍。
 - e. 在 IP match conditions (IP 比對條件) 窗格中，選擇刪除。
 - f. 在刪除對話方塊中，再次選擇刪除確認。
2. 刪除您的 SQL injection 比對條件的篩選條件，以及刪除 SQL injection 比對條件：
 - a. 在導覽窗格中，選擇 SQL injection。

- b. 選擇在本教學課程中建立的 SQL injection 比對條件。
 - c. 選取您新增篩選條件的核取方塊。
 - d. 選擇刪除篩選條件。
 - e. 在 SQL injection match conditions (SQL injection 比對條件) 窗格中，選擇刪除。
 - f. 在刪除對話方塊中，再次選擇刪除確認。
3. 刪除您的字串比對條件的篩選條件，以及刪除字串比對條件：
 - a. 在導覽窗格中選擇字串和 regex 比對。
 - b. 選擇在本教學課程中建立的字串比對條件。
 - c. 選取您新增篩選條件的核取方塊。
 - d. 選擇刪除篩選條件。
 - e. 在 String match conditions (字串比對條件) 窗格中，選擇刪除。
 - f. 在刪除對話方塊中，再次選擇刪除確認。
4. 如果您有建立的話，請刪除您的 regex 比對條件的篩選條件，以及刪除 regex 比對條件：
 - a. 在導覽窗格中選擇字串和 regex 比對。
 - b. 選擇在本教學課程中建立的 regex 比對條件。
 - c. 選取您新增篩選條件的核取方塊。
 - d. 選擇刪除篩選條件。
 - e. 在 Regex match conditions (Regex 比對條件)窗格中，選擇刪除。
 - f. 在刪除對話方塊中，再次選擇刪除確認。
5. 刪除您的容量限制條件的篩選條件，以及刪除容量限制條件：
 - a. 在導覽窗格中，選擇容量限制。
 - b. 選擇在本教學課程中建立的容量限制條件。
 - c. 選取您新增篩選條件的核取方塊。
 - d. 選擇刪除篩選條件。
 - e. 在 Size constraint conditions (容量限制條件) 窗格中，選擇刪除。
 - f. 在刪除對話方塊中，再次選擇刪除確認。

建立和設定 Web 存取控制清單 (Web ACL)

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

Web 存取控制清單 (Web ACL) 可讓您精細控制 Amazon API Gateway API、Amazon CloudFront 分佈或 Application Load Balancer 回應的 Web 請求。您可以允許或封鎖以下類型的請求：

- 源自於 IP 地址或 IP 地址的範圍
- 源自於特定國家/地區
- 包含指定的字串或符合特定請求中的規則運算式 (regex) 模式
- 超過指定的長度
- 似乎含有惡意 SQL 程式碼 (稱為 SQL injection)
- 似乎含有惡意指令碼 (稱為跨網站指令碼)

您葛已操是這些條件的任意組合，封鎖或計數不僅只符合指定條件的 web 請求，還有在任五分鐘內超過指定數量的請求。

若要選擇您想允許的請求，以存取您的內容，或您想要封鎖的內容，請執行以下：

1. 選擇預設的動作，允許或封鎖不符合任何您所指定條件的 web 請求。如需詳細資訊，請參閱[決定 Web ACL 的預設動作](#)。
2. 指定您想要允許或封鎖請求的條件：
 - 若要根據請求是否有含有惡意指令碼，允許或封鎖請求，請建立跨網站指令碼比對條件。如需詳細資訊，請參閱[使用跨網站指令碼比對條件](#)。

- 若要根據他們源於的 IP 地址，允許或封鎖請求，請建立 IP 比對條件。如需詳細資訊，請參閱[使用 IP 比對條件](#)。
 - 若要根據他們源於的國家/地區執行，允許或封鎖請求，請建立地理比對條件。如需詳細資訊，請參閱[使用地理比對條件](#)。
 - 若要根據請求是否超過指定的長度，允許或封鎖請求，請建立容量的限制條件。如需詳細資訊，請參閱[使用容量限制條件](#)。
 - 若要根據請求是否有含有惡意 SQL 碼，允許或封鎖請求，請建立 SQL injection 比對條件。如需詳細資訊，請參閱[使用 SQL Injection 比對條件](#)。
 - 若要根據在請求中出現的字串，允許或封鎖請求，請建立字串比對條件。如需詳細資訊，請參閱[使用字串比對條件](#)。
 - 若要根據在請求中出現的 regex 模式，允許或封鎖請求，請建立 regex 比對條件。如需詳細資訊，請參閱[使用 Regex 比對條件](#)。
3. 將此條件新增至一個或多個規則。如果您將多個條件新增至相同的規則，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據規則允許或封鎖請求。如需詳細資訊，請參閱[使用規則](#)。或者，您可以使用以速率為基礎的規則來取代一般規則，限制來自任何 IP 地址且符合條件的請求數量。
 4. 新增規則至 Web ACL。針對每個規則，指定您要 AWS WAF Classic 根據您新增至規則的條件來允許或封鎖請求。如果您將多個規則新增至 Web ACL，AWS WAF Classic 會依在 Web ACL 中列出的順序評估規則。如需詳細資訊，請參閱[使用 Web ACL](#)。

當您新增新的規則或更新現有的規則，可能需要一分鐘左右讓所做的變更完成，才會出現在您的 Web ACL 和資源。

主題

- [使用條件](#)
- [使用規則](#)
- [使用 Web ACL](#)

使用條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

指定何時您想要允許或封鎖請求的條件。

- 若要根據請求是否有含有惡意指令碼，允許或封鎖請求，請建立跨網站指令碼比對條件。如需詳細資訊，請參閱[使用跨網站指令碼比對條件](#)。
- 若要根據他們源於的 IP 地址，允許或封鎖請求，請建立 IP 比對條件。如需詳細資訊，請參閱[使用 IP 比對條件](#)。
- 若要根據他們源於的國家/地區執行，允許或封鎖請求，請建立地理比對條件。如需詳細資訊，請參閱[使用地理比對條件](#)。
- 若要根據請求是否超過指定的長度，允許或封鎖請求，請建立容量的限制條件。如需詳細資訊，請參閱[使用容量限制條件](#)。
- 若要根據請求是否有含有惡意 SQL 碼，允許或封鎖請求，請建立 SQL injection 比對條件。如需詳細資訊，請參閱[使用 SQL Injection 比對條件](#)。
- 若要根據在請求中出現的字串，允許或封鎖請求，請建立字串比對條件。如需詳細資訊，請參閱[使用字串比對條件](#)。
- 若要根據在請求中出現的 regex 模式，允許或封鎖請求，請建立 regex 比對條件。如需詳細資訊，請參閱[使用 Regex 比對條件](#)。

主題

- [使用跨網站指令碼比對條件](#)
- [使用 IP 比對條件](#)
- [使用地理比對條件](#)
- [使用容量限制條件](#)
- [使用 SQL Injection 比對條件](#)
- [使用字串比對條件](#)
- [使用 Regex 比對條件](#)

使用跨網站指令碼比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

攻擊者有時會將指令碼插入到 web 請求中，利用 web 應用程式的漏洞。您可以建立一或多個跨網站指令碼比對條件，以識別您希望 AWS WAF Classic 檢查潛在惡意指令碼的 Web 請求部分，例如 URI 或查詢字串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖貌似含有惡意指令碼的請求。

主題

- [建立跨網站指令碼比對條件](#)
- [當您建立或編輯跨網站指令碼比對條件時所指定的值](#)
- [新增和刪除跨網站指令碼比對條件的篩選條件](#)
- [刪除跨網站指令碼比對條件](#)

建立跨網站指令碼比對條件

當您建立跨網站指令碼比對條件時，請您指定篩選條件。篩選條件指出您希望 AWS WAF Classic 檢查惡意指令碼的 Web 請求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至跨網站指令碼比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個組態如何影響 AWS WAF Classic 行為的方式：

- 每個跨網站指令碼比對條件超過一個篩選條件（建議） – 當您將包含多個篩選條件的跨網站指令碼比對條件新增至規則，並將規則新增至 Web ACL 時，Web 請求必須僅符合跨網站指令碼比對條件中的其中一個篩選條件，AWS WAF Classic 才能根據該條件允許或封鎖請求。

例如，假設您建立一個跨網站指令碼比對條件，此條件含有兩個篩選條件。一個篩選條件指示 AWS WAF Classic 檢查 URI 是否有惡意指令碼，另一個則指示 AWS WAF Classic 檢查查詢字串。AWS WAF 如果請求在 URI 或查詢字串中似乎包含惡意指令碼，則 Classic 允許或封鎖請求。

- 每個跨網站指令碼比對條件一個篩選條件 – 當您將個別的跨網站指令碼比對條件新增至規則並將規則新增至 Web ACL 時，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據條件允許或封鎖請求。

假設您建立兩個條件，每個條件含有前述範例中兩個篩選條件中的一個。當您將兩個條件新增至相同規則並將規則新增至 Web ACL 時，AWS WAF Classic 只會在 URI 和查詢字串都顯示包含惡意指令碼時，才允許或封鎖請求。

Note

當您將跨網站指令碼比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖看起來不包含惡意指令碼的 Web 請求。

建立跨網站指令碼比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱[當您建立或編輯跨網站指令碼比對條件時所指定的值](#)。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 完成新增篩選條件，請選擇建立。

當您建立或編輯跨網站指令碼比對條件時所指定的值

當您建立或更新跨網站指令碼比對條件時，您需指定的以下的值：

名稱

跨網站指令碼比對條件的篩選條件的名稱。

名稱僅能由 A-Z、a-z、0-9 和特殊字元：_! " # ' + * } , . / 組成。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查惡意指令碼的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，User-Agent 或 Referer 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出請求請求請求原始伺服器執行的操作類型。CloudFront 支援下列方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

Note

對於跨網站指令碼比對條件，建議您選擇所有查詢參數（僅限值），而不是針對要篩選的部分請求的查詢字串。

URI

請求的 URI 路徑，可識別資源，例如 /images/daily-ad.jpg。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

除非指定轉換，否則 URI 不會標準化，並會如同在請求中從用戶端 AWS 接收一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

 Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果 URL 為「www.xyz.com?UserName=abc&SalesRegion=seattle」，則您可以新增篩選條件至 UserName 或 SalesRegion 參數。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您將在查詢字串參數中檢查的項目，例如 UserName 或 SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區分大小寫。例如，您指定 UserName 為查詢參數名稱，此會比對所有 UserName 的異體，如 username 和 UsERName。

所有的查詢參數 (僅數值)

與單一查詢參數 (僅限值) 類似，但與其檢查單一參數的值，AWS WAF Classic 會檢查查詢字串內的所有參數值是否有可能的惡意指令碼。例如，如果 URL 為 "www.xyz.com?UserName=abc&SalesRegion=seattle"，且您選擇所有查詢參數 (僅限值)，則如果 UserName 或 SalesRegion 的值包含可能的惡意指令碼，AWS WAF Classic 將觸發相符項目。

標頭

如果您選擇了要篩選的部分請求的標頭，請從常見標頭清單中選擇標頭，或輸入您要 AWS WAF Classic 檢查惡意指令碼的標頭名稱。

轉換

轉換會在 AWS WAF Classic 檢查請求之前重新格式化 Web 請求。這可消除攻擊者在 Web 請求中使用的一些異常格式，以嘗試繞過 AWS WAF Classic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 不會在 Web 請求上執行任何文字轉換，然後再檢查值中的字串是否相符。

轉換成小寫

AWS WAF Classic 會將大寫字母 (A-Z) 轉換為小寫 (a-z)。

HTML 解碼

AWS WAF Classic 以未編碼的字元取代 HTML 編碼的字元：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF Classic 以空格字元取代下列字元 (十進位 32)：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除跨網站指令碼比對條件的篩選條件

您可以新增和刪除跨網站指令碼比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

若要新增和刪除跨網站指令碼比對條件的篩選條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
3. 選擇您想要在條件裡新增或刪除的篩選條件。
4. 若要新增篩選條件，請執行以下步驟：
 - a. 選擇新增篩選條件。
 - b. 指定適用的篩選條件設定。如需詳細資訊，請參閱[當您建立或編輯跨網站指令碼比對條件時所指定的值](#)。
 - c. 選擇新增。
5. 若要刪除篩選條件，請執行以下步驟：
 - a. 選取您要刪除的篩選條件。
 - b. 選擇刪除篩選條件。

刪除跨網站指令碼比對條件

如果您想要刪除跨網站指令碼比對條件，您必須先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除跨網站指令碼比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
3. 在跨網站指令碼比對條件窗格中，選擇您要刪除的跨網站指令碼比對條件。
4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

如果使用此跨網站指令碼比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該跨網站指令碼比對條件的規則中移除該條件，請執行以下步驟：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該跨網站指令碼比對條件的規則名稱。
 - c. 在右窗格中，選擇要刪除使用該跨網站指令碼比對條件的規則，然後選擇移除選取的條件。
 - d. 對所有剩下要刪除使用該跨網站指令碼比對條件的規則，重複步驟 b 和 c。
 - e. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
 - f. 在跨網站指令碼比對條件窗格中，選擇您要刪除的跨網站指令碼比對條件。
6. 選擇刪除以刪除選取的條件。

使用 IP 比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想根據請求源於的 IP 地址，允許或封鎖 web 請求，請建立一個或多個 IP 比對條件。IP 比對條件可列出 10,000 個您的請求源於的 IP 地址或 IP 地址範圍。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖自這些 IP 地址的請求。

主題

- [建立 IP 比對條件](#)
- [編輯 IP 比對條件](#)
- [刪除 IP 比對條件](#)

建立 IP 比對條件

如果您想根據請求源於的 IP 地址執行允許某些請求、封鎖某些請求的話，請建立您想允許請求 IP 地址的 IP 比對條件，和您想封鎖請求 IP 地址的 IP 比對條件。

Note

當您將 IP 比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖不是來自您在條件中指定的 IP 地址的 Web 請求。

建立 IP 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇 IP 地址。
3. 選擇 Create condition (建立條件)。
4. 在 Name (名稱) 欄位中輸入名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_! " # ` + * } , . /。條件的名稱在建立後無法變更。

5. 選擇正確的 IP 版本，並使用 CIDR 符號指定 IP 地址或 IP 地址範圍。以下是一些範例：
 - 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
 - 若要指定 IPv6 地址 0:0:0:0:ffff:c000:22c，請輸入 0:0:0:0:ffff:c000:22c/128。
 - 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
 - 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。

AWS WAF Classic 支援 IPv4 地址範圍：/8 和 /16 到 /32 之間的任何範圍。AWS WAF Classic 支援 IPv6 地址範圍：/24、/32、/48、/56、/64 和 /128。如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目 [無類別域間路由](#)。

6. 選擇新增另一個 IP 地址或範圍。
7. 如果您希望新增另一個 IP 地址或範圍，重複步驟五和六。

8. 當您完成新增後，請選擇建立 IP 比對條件。

編輯 IP 比對條件

您可以將 IP 地址範圍新增至 IP 比對條件中，也可刪除範圍。若要變更範圍、新增新的範圍、和刪除舊的範圍。

編輯 IP 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 IP 地址。
3. 在 IP 比對條件窗格中，選擇您要編輯的 IP 比對條件。
4. 若要新增 IP 地址或範圍：
 - a. 在右窗格中，選擇新增 IP 地址或範圍。
 - b. 選擇正確的 IP 版本，並使用 CIDR 符號輸入 IP 地址。以下是一些範例：
 - 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
 - 若要指定 IPv6 地址 0:0:0:0:ffff:c000:22c，請輸入 0:0:0:0:ffff:c000:22c/128。
 - 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
 - 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。

AWS WAF Classic 支援 IPv4 地址範圍：/8 和 /16 到 /32 之間的任何範圍。AWS WAF Classic 支援 IPv6 地址範圍：/24、/32、/48、/56、/64 和 /128。如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目 [無類別域間路由](#)。

- c. 若要新增更多 IP 地址，請選擇 Add another IP address (新增另一個 IP 地址) 並輸入值。
 - d. 選擇新增。
5. 若要刪除 IP 地址或範圍：
 - a. 在右窗格中，選取要刪除的數值。
 - b. 選擇刪除 IP 地址或範圍。

刪除 IP 比對條件

如果您想要刪除 IP 比對條件，您必須先刪除該條件內的所有 IP 地址和範圍，以及從所有使用它的規則中移除，請參閱下列程序。

刪除 IP 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 IP 地址。
3. 在 IP 比對條件窗格中，選擇您要刪除的 IP 比對條件。
4. 在右窗格中，選擇規則標籤。

如果使用此 IP 比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該 IP 比對條件的規則中移除該條件，請執行以下步驟：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該 IP 比對條件的規則名稱。
 - c. 在右窗格中，選擇要刪除 IP 比對條件的規則，然後選擇移除選取的條件。
 - d. 對所有剩下要刪除使用該 IP 比對條件的規則，重複步驟 b 和 c。
 - e. 在導覽窗格中，選擇 IP 比對條件。
 - f. 在 IP 比對條件窗格中，選擇您要刪除的 IP 比對條件。
6. 選擇刪除以刪除選取的條件。

使用地理比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想根據請求源於的國家/地區，允許或封鎖 web 請求，請建立一個或多個地理比對條件。地理比對條件列出的國家/地區為您請求的發源地。稍後，當您建立 Web ACL，您需要指定是否要允許或封來自這些國家/地區的請求。

您可以使用地理比對條件搭配其他 AWS WAF Classic 條件或規則來建置複雜的篩選。例如，如果您想要封鎖特定國家/地區，但仍想允許該國家/地區的特定 IP 地址，您可以建立地理比對條件和 IP 比對條件，將這兩個一起增至一項規則中。設定規則以封鎖來自該國家/地區的請求，和未受核准的 IP 地址。舉另一個例子，如果您想未特定國家/地區的使用者劃分資源優先使用順序，您可以在兩個不同以速率為基礎的規則中，放入相同的地理比對條件。為慣用的國家/地區的使用者這定高速率限制，對其他國家/地區的使用者設定低的速率限制。

Note

如果您使用 CloudFront 地理限制功能來封鎖國家/地區存取您的內容，則來自該國家/地區的任何請求都會遭到封鎖，且不會轉送至 AWS WAF Classic。因此，如果您想要根據地理位置加上其他 AWS WAF Classic 條件允許或封鎖請求，則不應使用 CloudFront 地理限制功能。反之，您應該使用 AWS WAF Classic 地理比對條件。

主題

- [建立地理比對條件](#)
- [編輯地理比對條件](#)
- [刪除地理比對條件](#)

建立地理比對條件

如果您想根據請求源於的國家/地區執行允許某些請求、封鎖某些請求的話，請建立您想允許請求國家/地區的地理比對條件，和您想封鎖請求國家/地區的地理比對條件。

Note

當您將地理比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖不是來自您在條件中指定國家/地區的 Web 請求。

建立地理比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇地理比對。
3. 選擇 Create condition (建立條件)。
4. 在 Name (名稱) 欄位中輸入名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_!@#%^&*},./。條件的名稱在建立後無法變更。

5. 選擇一個區域。
6. 選擇位置類型和國家/地區。Location type (位置類型) 目前只能是 Country (國家/地區)。
7. 選擇新增位置。
8. 選擇 Create (建立)。

編輯地理比對條件

您可以從地理比對條件新增或刪除國家/地區。

編輯地理比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇地理比對。
3. 在地理比對條件窗格中，選擇您要編輯的地理比對條件。
4. 新增國家/地區：

- a. 在右窗格中選擇新增篩選條件。
 - b. 選擇位置類型和國家/地區。Location type (位置類型) 目前只能是 Country (國家/地區)。
 - c. 選擇新增。
5. 若要刪除國家/地區：
- a. 在右窗格中，選取要刪除的數值。
 - b. 選擇刪除篩選條件。

刪除地理比對條件

如果您想要刪除地理比對條件，您必須先移除該條件內的所有國家/地區，以及從所有使用它的規則中移除，請參閱下列程序。

刪除地理比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 從使用該地理比對條件的規則中移除該條件：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該地理比對條件的規則名稱。
 - c. 在右窗格中選擇編輯規則。
 - d. 在您要刪除的條件旁，選擇 X。
 - e. 選擇更新。
 - f. 對所有剩下要刪除使用該地理比對條件的規則，重複步驟。
3. 從您想刪除的條件移除篩選條件：
 - a. 在導覽窗格中，選擇地理比對。
 - b. 選擇您要刪除的地理比對條件名稱。
 - c. 在右窗格中，選擇篩選條件旁的核取方塊，以選取所有篩選條件。
 - d. 選擇刪除篩選條件。
4. 在導覽窗格中，選擇地理比對。
5. 在地理比對條件窗格中，選擇您要刪除的地理比對條件。

6. 選擇刪除以刪除選取的條件。

使用容量限制條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想根據指定部分請求的長度，允許或封鎖 web 請求，請建立容量限制條件。大小限制條件會識別您希望 AWS WAF Classic 查看的 Web 請求部分、您希望 AWS WAF Classic 尋找的位元組數，以及運算子，例如大於 (>) 或小於 (<)。例如，您可以使用容量限制條件，以尋找超過 100 位元組的查詢字串。稍後，當您建立 Web ACL，您需要指定是否要根據這些設定允許或封鎖請求。

請注意，如果您設定 AWS WAF Classic 來檢查請求內文，例如，透過搜尋內文以取得指定的字串，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)。如果您的 Web 請求的請求主體永遠不會超過 8192 個位元組，您可以建立容量限制條件，封鎖大於 8192 位元組的請求。

主題

- [建立容量限制條件](#)
- [在您建立或編輯容量限制條件時所指定的值](#)
- [新增和刪除容量限制條件的篩選條件](#)
- [刪除容量限制條件](#)

建立容量限制條件

當您建立大小限制條件時，您可以指定篩選條件，以識別您希望 AWS WAF Classic 評估長度的 Web 請求部分。您可以將多個篩選條件增至容量限制條件，或您可以為每個篩選條件建立獨立的條件。以下是每個組態如何影響 AWS WAF Classic 行為的方式：

- 每個大小限制條件一個篩選條件 – 當您將個別大小限制條件新增至規則並將規則新增至 Web ACL 時，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據條件允許或封鎖請求。

例如，假設您建立兩個條件。一個符合 web 請求查詢字串大於 100 位元組。另一個符合 web 請求內文大於 1024 位元組。當您將兩個條件新增至相同的規則並將規則新增至 Web ACL 時，AWS WAF Classic 只會在兩個條件都為 true 時允許或封鎖請求。

- 每個大小限制條件都有多個篩選條件：當您將包含多個篩選條件的大小限制條件新增至規則，並將規則新增至 Web ACL 時，Web 請求只需要符合 AWS WAF Classic 大小限制條件中的其中一個篩選條件，即可根據該條件允許或封鎖請求。

假設您建立一個條件而不是兩個條件，而一個條件包含與上述範例中相同的兩個篩選條件。如果查詢字串大於 100 個位元組，或請求內文大於 1024 個位元組，AWS WAF Classic 允許或封鎖請求。

Note

當您將大小限制條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖不符合條件中值的 Web 請求。

建立容量限制條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇容量限制。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您建立或編輯容量限制條件時所指定的值](#)。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 當您完成新增篩選條件後，請選擇建立容量限制條件。

在您建立或編輯容量限制條件時所指定的值

在建立或更新容量限制條件時，請指定以下的值：

名稱

輸入容量限制條件的名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_!\"#`+*},./。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 評估其長度的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，User-Agent 或 Referer 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出請求請求請求原始伺服器執行的操作類型。CloudFront 支援下列方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

請求的 URI 路徑，可識別資源，例如 /images/daily-ad.jpg。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

除非指定轉換，否則 URI 不會標準化，並會如同在請求中從用戶端 AWS 接收一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果 URL 為「www.xyz.com?UserName=abc&SalesRegion=seattle」，則您可以新增篩選條件至 UserName 或 SalesRegion 參數。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您將在查詢字串參數中檢查的項目，例如 UserName。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區

分大小寫。例如，您指定 `UserName` 為查詢參數名稱，此會比對所有 `UserName` 的異體，如 `username` 和 `UsERName`。

所有的查詢參數 (僅數值)

類似於單一查詢參數 (僅限值)，但與其檢查單一參數的值，AWS WAF Classic 會檢查查詢字串內所有參數的值，以了解大小限制條件。例如，如果 URL 為 `"www.xyz.com?UserName=abc&SalesRegion=seattle"`，且您選擇所有查詢參數 (僅限值)，則如果 `UserName` 或 `SalesRegion` 超過指定的大小，AWS WAF Classic 會觸發的值。

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您選擇了要篩選的部分請求的標頭，請從常見標頭清單中選擇標頭，或輸入您要 AWS WAF Classic 評估長度的標頭名稱。

比較運算子

選擇您希望 AWS WAF Classic 如何針對您為大小指定的值，評估 Web 請求中查詢字串的長度。

例如，如果您選擇大於表示比較運算子，且輸入 100 表示大小，AWS WAF Classic 會評估超過 100 個位元組的查詢字串的 Web 請求。

大小

輸入您希望 AWS WAF Classic 在查詢字串中監看的長度，以位元組為單位。

Note

如果您選擇 URI 為部分請求的值來篩選，則會視 URI 的 `/` 為一個字元。例如，URI 路徑長度 `/logo.jpg` 為九個字元。

轉換

在 AWS WAF Classic 評估請求指定部分的長度之前，轉換會重新格式化 Web 請求。這可消除攻擊者在 Web 請求中使用的一些異常格式，以嘗試繞過 AWS WAF Classic。

Note

如果您選擇篩選部分請求的內文，則無法設定 AWS WAF Classic 來執行轉換，因為只有前 8192 個位元組會轉送以供檢查。不過，您仍然可以根據 HTTP 請求內文的大小來篩選流量，並指定無轉換。(AWS WAF Classic 會從請求標頭取得內文的長度。)

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF 在檢查長度之前，Classic 不會對 Web 請求執行任何文字轉換。

轉換成小寫

AWS WAF Classic 會將大寫字母 (A-Z) 轉換為小寫 (a-z)。

HTML 解碼

AWS WAF Classic 以未編碼的字元取代 HTML 編碼的字元：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF Classic 以空格字元取代下列字元（十進位 32）：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ ' ^

- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除容量限制條件的篩選條件

您可以新增和刪除容量限制條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除容量限制條件的篩選條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇容量限制。
3. 選擇您想要在條件裡新增或刪除的篩選條件。
4. 若要新增篩選條件，請執行以下步驟：
 - a. 選擇新增篩選條件。
 - b. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您的建立或編輯容量限制條件時所指定的值](#)。
 - c. 選擇新增。
5. 若要刪除篩選條件，請執行以下步驟：
 - a. 選取您要刪除的篩選條件。
 - b. 選擇刪除篩選條件。

刪除容量限制條件

如果您想要刪除容量限制條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除容量限制條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇容量限制。
3. 在容量限制條件窗格中，選擇您要刪除的容量限制條件。
4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

如果使用此容量限制條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該容量限制條件的規則中移除該條件，請執行以下步驟：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該容量限制條件的規則名稱。
 - c. 在右窗格中，選擇要刪除使用該容量限制條件的規則，然後選擇移除選取的條件。
 - d. 對所有剩下要刪除使用該容量限制條件的規則，重複步驟 b 和 c。
 - e. 在導覽窗格中，選擇容量限制。
 - f. 在容量限制條件窗格中，選擇您要刪除的容量限制條件。
6. 選擇刪除以刪除選取的條件。

使用 SQL Injection 比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

攻擊者有時插入惡意 SQL 程式碼到 web 請求中，以從您的資料庫擷取資料。若要根據請求是否有含有惡意 SQL 碼，允許或封鎖 web 請求，請建立一個或多個 SQL injection 比對條件。SQL 注入比對條件可識別您要 AWS WAF Classic 檢查的 Web 請求部分，例如 URI 路徑或查詢字串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖貌似含有惡意 SQL 程式碼的請求。

主題

- [使用 SQL Injection 比對條件](#)
- [在您建立或編輯 SQL Injection 比對條件時所指定的值](#)
- [新增和刪除 SQL Injection 比對條件的篩選條件](#)
- [刪除 SQL Injection 比對條件](#)

使用 SQL Injection 比對條件

當您建立 SQL 注入比對條件時，您可以指定篩選條件，指出您希望 AWS WAF Classic 檢查惡意 SQL 程式碼的 Web 請求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至 SQL injection 比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個組態如何影響 AWS WAF Classic 行為的方式：

- 每個 SQL 注入比對條件都有多個篩選條件（建議）：當您將包含多個篩選條件的 SQL 注入比對條件新增至規則，並將規則新增至 Web ACL 時，Web 請求只需要比對 AWS WAF Classic SQL 注入比對條件中的其中一個篩選條件，即可根據該條件允許或封鎖請求。

例如，假設您建立一個 SQL injection 比對條件，此條件含有兩個篩選條件。一個篩選條件指示 AWS WAF Classic 檢查 URI 是否有惡意 SQL 程式碼，另一個則指示 AWS WAF Classic 檢查查詢字串。AWS WAF 如果請求在 URI 或查詢字串中似乎包含惡意 SQL 程式碼，則 Classic 允許或封鎖請求。

- 每個 SQL 注入比對條件有一個篩選條件 – 當您將個別的 SQL 注入比對條件新增至規則並將規則新增至 Web ACL 時，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據條件允許或封鎖請求。

假設您建立兩個條件，每個條件含有前述範例中兩個篩選條件中的一個。當您將兩個條件新增至相同的規則並將規則新增至 Web ACL 時，AWS WAF Classic 只會在 URI 和查詢字串都顯示包含惡意 SQL 程式碼時，才允許或封鎖請求。

Note

當您將 SQL 注入比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖看起來不包含惡意 SQL 程式碼的 Web 請求。

建立 SQL Injection 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 SQL injection。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您建立或編輯 SQL Injection 比對條件時所指定的值](#)。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 完成篩選條件，請選擇建立。

在您建立或編輯 SQL Injection 比對條件時所指定的值

在建立或更新 SQL Injection 比對條件時，請指定以下的值：

名稱

SQL Injection 比對條件的名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_! " # ' + * } , . /。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查惡意 SQL 程式碼的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，User-Agent 或 Referer 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，表示請求請求請求原始伺服器執行的操作類型。CloudFront 支援下列方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查詢字串

出現在？字元後的 URL 部分 (如果有)。

Note

針對 SQL 注入比對條件，建議您選擇所有查詢參數（僅限值），而不是針對要篩選的部分請求的查詢字串。

URI

請求的 URI 路徑，可識別資源，例如 /images/daily-ad.jpg。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

除非指定轉換，否則 URI 不會標準化，並且會如同在請求中從用戶端 AWS 接收一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖內文超過 8192 個位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果 URL 為「www.xyz.com?UserName=abc&SalesRegion=seattle」，則您可以新增篩選條件至 UserName 或 SalesRegion 參數。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您將在查詢字串參數中檢查的項目，例如 `UserName` 或 `SalesRegion`。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區分大小寫。例如，您指定 `UserName` 為查詢參數名稱，此會比對所有 `UserName` 的異體，如 `username` 和 `UsERName`。

所有的查詢參數 (僅數值)

與單一查詢參數 (僅限值) 類似，但與其檢查單一參數的值，AWS WAF Classic 會檢查查詢字串內所有參數的值是否有可能的惡意 SQL 程式碼。例如，如果 URL 為 `"www.xyz.com?UserName=abc&SalesRegion=seattle"`，且您選擇所有查詢參數 (僅限值)，則如果 `UserName` 或 `SalesRegion` 的值包含可能的惡意 SQL 程式碼，AWS WAF Classic 將觸發相符項目。

標頭

如果您選擇了要篩選的部分請求的標頭，請從常見標頭清單中選擇標頭，或輸入您要 AWS WAF Classic 檢查惡意 SQL 程式碼的標頭名稱。

轉換

轉換會在 AWS WAF Classic 檢查請求之前重新格式化 Web 請求。這可消除攻擊者在 Web 請求中使用的一些異常格式，以試圖繞過 AWS WAF Classic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 不會在 Web 請求上執行任何文字轉換，然後再檢查值中的字串是否相符。

轉換成小寫

AWS WAF Classic 會將大寫字母 (A-Z) 轉換為小寫 (a-z)。

HTML 解碼

AWS WAF Classic 以未編碼的字元取代 HTML 編碼的字元：

- 將 `"` 換成 `&`
- 以非中斷空格取代 ` `;
- 將 `<` 換成 `<`
- 將 `>` 換成 `>`
- 將表示為十六進位格式的字元 `&#xhhhh`；以對應字元取代
- 將表示為十進位格式的字元 `&#nnnn`；以對應字元取代

標準化空格

AWS WAF Classic 以空格字元 (十進位 32) 取代下列字元：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除 SQL Injection 比對條件的篩選條件

您可以新增和刪除 SQL Injection 比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除 SQL Injection 比對條件的篩選條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 SQL injection。
3. 選擇您想要在條件裡新增或刪除的篩選條件。

4. 若要新增篩選條件，請執行以下步驟：

- a. 選擇新增篩選條件。
- b. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您的建立或編輯 SQL Injection 比對條件時所指定的值](#)。
- c. 選擇新增。

5. 若要刪除篩選條件，請執行以下步驟：

- a. 選取您要刪除的篩選條件。
- b. 選擇刪除篩選條件。

刪除 SQL Injection 比對條件

如果您想要刪除 SQL Injection 比對條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除 SQL Injection 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 SQL injection。
3. 在 SQL Injection 比對條件窗格中，選擇您要刪除的 SQL Injection 比對條件。
4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

如果使用此 SQL Injection 比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該 SQL Injection 比對條件的規則中移除該條件，請執行以下步驟：

- a. 在導覽窗格中，選擇規則。
- b. 選擇要刪除使用該 SQL Injection 比對條件的規則名稱。
- c. 在右窗格中，選擇要刪除 SQL Injection 比對條件的規則，然後選擇移除選取的條件。
- d. 對所有剩下要刪除使用該 SQL Injection 比對條件的規則，重複步驟 b 和 c。
- e. 在導覽窗格中，選擇 SQL injection。
- f. 在 SQL Injection 比對條件窗格中，選擇您要刪除的 SQL Injection 比對條件。

6. 選擇刪除以刪除選取的條件。

使用字串比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想根據請求裡出現的字串，允許或封鎖 web 請求，請建立一個或多個字串比對條件。字串比對條件可識別您要搜尋的字串，以及您希望 AWS WAF Classic 檢查字串的 Web 請求部分，例如指定的標頭或查詢字串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖含有這些字串的請求。

主題

- [建立字串比對條件](#)
- [在您建立或編輯字串比對條件時所指定的值](#)
- [新增和刪除字串比對條件的篩選條件](#)
- [刪除字串比對條件](#)

建立字串比對條件

當您建立字串比對條件時，您可以指定篩選條件，以識別您要搜尋的字串，以及您希望 AWS WAF Classic 檢查該字串的 Web 請求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至字串比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個組態如何影響 AWS WAF Classic 行為的方式：

- 每個字串比對條件一個篩選條件 – 當您將個別字串比對條件新增至規則並將規則新增至 Web ACL 時，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據條件允許或封鎖請求。

例如，假設您建立兩個條件。一個符合 web 請求，還有 User-Agent 標頭的 BadBot 值。另一個符合 web 請求，含有查詢字串的 BadParameter 值。當您將兩個條件新增至相同的規則並將規則新增至 Web ACL 時，AWS WAF Classic 只會允許或封鎖包含兩個值的請求。

- 每個字串比對條件超過一個篩選條件 – 當您將包含多個篩選條件的字串比對條件新增至規則並將規則新增至 Web ACL 時，Web 請求只需要比對 AWS WAF Classic 字串比對條件中的其中一個篩選條件，以允許或封鎖根據一個條件提出的請求。

假設您建立一個條件而不是兩個條件，而一個條件包含與上述範例中相同的兩個篩選條件。AWS WAF Classic 允許或封鎖在 BadBotUser-Agent 標頭或查詢字串 BadParameter 中包含的請求。

Note

當您將字串比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖不符合條件中值的 Web 請求。

建立字串比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您建立或編輯字串比對條件時所指定的值](#)。
5. 選擇新增篩選條件。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 完成篩選條件，請選擇建立。

在您建立或編輯字串比對條件時所指定的值

在建立或更新字串比對條件時，請指定以下的值：

名稱

輸入字串比對條件的名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_!"#\$%&'*,./。條件的名稱在建立後無法變更。

Type

選擇 String match (字串比對)。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查每個 Web 請求中您在值中指定的字串以符合的部分：

標頭

指定的請求標頭，例如，User-Agent 或 Referer 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出請求請求請求原始伺服器執行的操作類型。CloudFront 支援下列方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

請求的 URI 路徑，可識別資源，例如 /images/daily-ad.jpg。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

除非指定轉換，否則 URI 不會標準化，並且會如同在請求中從用戶端 AWS 接收一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果 URL 為「www.xyz.com?UserName=abc&SalesRegion=seattle」，則您可以新增篩選條件至 UserName 或 SalesRegion 參數。

如果重複的參數顯示在查詢字串上，則數值評估則為「OR」。也就是說，將會觸發符合的值。例如，在 URL「www.xyz.com?SalesRegion=boston&SalesRegion=seattle」，在符合值的「boston」或「seattle」將會觸發比對符合。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您將在查詢字串參數中檢查的項目，例如 UserName 或 SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區分大小寫。例如，您指定 UserName 為查詢參數名稱，此會比對所有 UserName 的異體，如 username 和 UsERName。

所有的查詢參數 (僅數值)

類似於單一查詢參數 (僅限值)，但與其檢查單一參數的值，AWS WAF Classic 會檢查查詢字串中所有參數的值，以便值相符。例如，如果 URL 為 "www.xyz.com?UserName=abc&SalesRegion=seattle"，且您選擇所有查詢參數 (僅限值)，則如果 UserName 或 SalesRegion 的值指定為要比對的值，則 AWS WAF Classic 將觸發相符項目。

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您從請求的 部分選擇標頭以在清單中篩選，請從常見標頭清單中選擇標頭，或輸入您要 AWS WAF Classic 檢查的標頭名稱。

符合類型

在您希望 AWS WAF Classic 檢查的請求部分中，選擇值中要比對的字串必須顯示為符合此篩選條件的位置：

包含

該字串出現在指定請求部分中的任何位置。

包含的字

指定的請求部分必須包含符合值，且符合值必須只能含有字母數字字元或底線 (A-Z, a-z, 0-9, or _)。此外，符合值必須為字，表示以下其中一項：

- 符合值完全符合指定的值，例如 web 請求部分的標頭的值。
- 符合值為指定的 Web 請求部分的開始，後面接的字元為一個字母數字字元或底線 (_)，例如 BadBot；。

- 符合值為指定的 Web 請求部分的結尾，前面接的字元為一個字母數字字元或底線 (_)，例如 ;BadBot。
- 符合值為指定的 Web 請求部分的中間，前後面接的字元為字母數字字元或底線 (_)，例如 -BadBot;。

完全符合

字串和指定的請求部分，值為相同的。

開頭為

該字串出現在指定請求部分中的起始位置。

結尾為

該字串出現在指定請求部分中的結束位置。

轉換

轉換會在 AWS WAF Classic 檢查請求之前重新格式化 Web 請求。這可消除攻擊者在 Web 請求中使用的一些異常格式，以嘗試繞過 AWS WAF Classic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 不會在 Web 請求上執行任何文字轉換，然後再檢查值中的字串是否相符。

轉換成小寫

AWS WAF Classic 會將大寫字母 (A-Z) 轉換為小寫 (a-z)。

HTML 解碼

AWS WAF Classic 以未編碼的字元取代 HTML 編碼的字元：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF Classic 以空格字元取代下列字元（十進位 32）：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

若您將擔心攻擊者插入作業命令列命令，或使用不尋常的格式偽裝某些或所有命令，請使用此選項執行下列轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

base64 編碼值

如果符合值的值是 base64 編碼，請選取此核取方塊。使用 base64 編碼指定攻擊者在其請求中使用的無法列印字元，例如標籤和換行。

符合值

指定您希望 AWS WAF Classic 在 Web 請求中搜尋的值。長度上限為 50 個位元組。如果您使用 base64 編碼此數值，50 個位元組的長度上限適用於之前編碼的值。

新增和刪除字串比對條件的篩選條件

您可以新增和刪除字串比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除字串比對條件的篩選條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇您想要在條件裡新增或刪除的篩選條件。
4. 若要新增篩選條件，請執行以下步驟：
 - a. 選擇新增篩選條件。
 - b. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您建立或編輯字串比對條件時所指定的值](#)。
 - c. 選擇新增。
5. 若要刪除篩選條件，請執行以下步驟：
 - a. 選取您要刪除的篩選條件。
 - b. 選擇刪除篩選條件。

刪除字串比對條件

如果您想要刪除字串條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除字串比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 從使用該字串比對條件的規則中移除該條件：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該字串比對條件的規則名稱。
 - c. 在右窗格中選擇編輯規則。
 - d. 在您要刪除的條件旁，選擇 X。
 - e. 選擇更新。

- f. 對所有剩下要刪除使用該字串比對條件的規則，重複步驟。
3. 從您想刪除的條件移除篩選條件：
 - a. 在導覽窗格中選擇字串和 regex 比對。
 - b. 選擇您要刪除的字串比對條件名稱。
 - c. 在右窗格中，選擇篩選條件旁的核取方塊，以選取所有篩選條件。
 - d. 選擇刪除篩選條件。
 4. 在導覽窗格中選擇字串和 regex 比對。
 5. 在字串比對條件窗格中，選擇您要刪除的字串比對條件。
 6. 選擇刪除以刪除選取的條件。

使用 Regex 比對條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想根據請求裡出現符合規則運算式 (regex) 模式的字串，允許或封鎖 web 請求，請建立一個或多個 Regex 比對條件。regex 比對條件是一種字串比對條件，可識別您要搜尋的模式，以及您希望 AWS WAF Classic 檢查模式的 Web 請求部分，例如指定的標頭或查詢字串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖含有這些模式的請求。

主題

- [建立 Regex 比對條件](#)
- [在您建立或編輯 RegEx 比對條件時所指定的值](#)
- [編輯 Regex 比對條件](#)

建立 Regex 比對條件

當您建立 Regex 比對條件，您需指定模式集以識別您想搜尋的字串 (使用規則運算式)。然後，將這些模式集新增至篩選條件，以指定您希望 AWS WAF Classic 檢查該模式集的 Web 請求部分，例如 URI 或查詢字串。

您可以將多個規則運算式增至單一模式集中。若您這麼做，這些運算式會與 OR 結合。如此，如果請求符合清單中的任一個運算式，web 請求將比對模式集。

當您將 regex 比對條件新增至規則時，您也可以設定 AWS WAF Classic 來允許或封鎖不符合條件中值的 Web 請求。

AWS WAF Classic 支援大多數[標準 Perl 相容規則表達式 \(PCRE\)](#)。然而，目前不支援下列各項：

- Backreferences 和擷取子運算式
- 任意零寬度宣告
- 子程式參考和遞迴模式
- 條件式模式
- 恢復控制動詞
- \C 單一位元組指令
- \R 換行比對指令
- \K 開頭比對重設指令
- 圖說文字和內嵌的程式碼
- 原子分組和所佔有的量詞

建立 regex 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱[在您的 AWS WAF 規則中指定 RegEx 比對條件時所指定的值](#)。

5. 選擇建立模式集和新增篩選條件 (如果您建立了新的模式集) 或新增篩選條件，如果您是使用現有的模式。
6. 選擇 Create (建立)。

在您建立或編輯 RegEx 比對條件時所指定的值

在建立或更新 Regex 比對條件時，請指定以下的值：

名稱

輸入 Regex 比對條件的名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_! " # ` + * } , . /。條件的名稱在建立後無法變更。

Type

選擇 Regex match (Regex 比對)。

要篩選的請求部分是

選擇您希望 AWS WAF Classic 檢查每個 Web 請求的部分，以檢查您在值中指定的模式，以符合：標頭

指定的請求標頭，例如，User-Agent 或 Referer 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，表示請求請求請求原始伺服器執行的操作類型。CloudFront 支援下列方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

請求的 URI 路徑，可識別資源，例如 /images/daily-ad.jpg。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

除非指定轉換，否則 URI 不會標準化，並且會如同在請求中從用戶端 AWS 接收一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

 Note

如果您選擇內文以取得要篩選之請求部分的值，AWS WAF Classic 只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖內文超過 8192 位元組的請求，您可以建立大小限制條件。(AWS WAF Classic 會從請求標頭取得內文的長度。) 如需詳細資訊，請參閱[使用容量限制條件](#)。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果 URL 為「www.xyz.com?UserName=abc&SalesRegion=seattle」，則您可以新增篩選條件至 UserName 或 SalesRegion 參數。

如果重複的參數顯示在查詢字串上，則數值評估則為「OR」。也就是說，將會觸發符合的值。例如，在 URL 「www.xyz.com?SalesRegion=boston&SalesRegion=seattle」，符合在符合值裡「boston」或「seattle」的模式，將會觸發比對符合。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您將在查詢字串參數中檢查的項目，例如 UserName 或 SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區分大小寫。例如，您指定 UserName 為查詢參數名稱，此會比對所有 UserName 的異體，如 username 和 UsERName。

所有的查詢參數 (僅數值)

與單一查詢參數 (僅限值) 類似，但與其檢查單一參數的值，AWS WAF Classic 會檢查查詢字串內所有參數的值，以找出值中指定的相符模式。例如，在 URL 「"www.xyz.com?UserName=abc&SalesRegion=seattle」，在符合值裡的模式，符合 UserName 或 SalesRegion，將會觸發比對符合。

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您從請求的部分中選擇標頭以在清單中篩選，請從常見標頭清單中選擇標頭，或輸入您要 AWS WAF Classic 檢查的標頭名稱。

轉換

轉換會在 AWS WAF Classic 檢查請求之前重新格式化 Web 請求。這可消除攻擊者在 Web 請求中使用的一些異常格式，以試圖繞過 AWS WAF Classic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 不會在 Web 請求上執行任何文字轉換，然後再檢查它是否有值中的字串相符。

轉換成小寫

AWS WAF Classic 會將大寫字母 (A-Z) 轉換為小寫 (a-z)。

HTML 解碼

AWS WAF Classic 以未編碼的字元取代 HTML 編碼的字元：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF Classic 以空格字元取代下列字元（十進位 32）：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

若您將擔心攻擊者插入作業命令列命令，或使用不尋常的格式偽裝某些或所有命令，請使用此選項執行下列轉換：

- 刪除以下字元：\ " ' ^

- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

比對請求的 Regex 模式

您可以選擇現有的模式集，或建立新的。如果您建立新的模式集指定以下：

新模式集的名稱

輸入名稱，然後指定您要 AWS WAF Classic 搜尋的 regex 模式。

如果您新增多個規則運算式至模式集，這些運算式會與 OR 結合。如此，如果請求符合清單中的任一個運算式，web 請求將比對模式集。

符合值 的長度上限為 70 個字元。

編輯 Regex 比對條件

您可以使用下列變更現有的 regex 比對條件：

- 刪除現有模式集裡的模式
- 新增模式至現有的模式集
- 從現有的 Regex 比對條件刪除篩選條件
- 將篩選條件新增至現有的 regex 比對條件（在 regex 比對條件中只能有一個篩選條件。因此，若要新增篩選條件，您必須先刪除現有的篩選條件。）
- 刪除現有的 Regex 比對條件

Note

您不能從現有篩選條件新增或刪除模式集。您必須編輯模式集、或刪除篩選條件並建立新的篩選條件與其新的模式集。

刪除現有模式集裡的模式

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇檢視 Regex 模式集。
4. 選擇您要編輯的模式集名稱。
5. 選擇編輯。
6. 在您要刪除的模式旁，選擇 X。
7. 選擇 Save (儲存)。

新增模式至現有的模式集

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇檢視 Regex 模式集。
4. 選擇要編輯的模式集名稱。
5. 選擇編輯。
6. 輸入新的 Regex 模式。
7. 選擇新的模式旁的 +。
8. 選擇 Save (儲存)。

從現有的 Regex 比對條件刪除篩選條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇您要刪除的篩選條件的比對條件名稱。

4. 選擇您要刪除篩選條件旁的方塊。
5. 選擇刪除篩選條件。

刪除 Regex 比對條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 從 Regex 比對條件刪除篩選條件。請參閱 [從現有的 Regex 比對條件刪除篩選條件](#) 以取得執行此動作的指示。)
3. 從使用該 Regex 比對條件的規則中移除該條件：
 - a. 在導覽窗格中，選擇規則。
 - b. 選擇要刪除使用該 Regex 比對條件的規則名稱。
 - c. 在右窗格中選擇編輯規則。
 - d. 在您要刪除的條件旁，選擇 X。
 - e. 選擇更新。
 - f. 對所有剩下要刪除使用該 Regex 比對條件的規則，重複步驟。
4. 在導覽窗格中選擇字串和 regex 比對。
5. 選擇您要刪除條件旁的按鈕。
6. 選擇 刪除。

從現有的 Regex 比對條件新增或變更篩選條件

Regex 比對條件只能擁有一個篩選條件。如果您想新增或變更篩選條件，您必須先刪除現有的篩選條件。

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 從您想變更的 Regex 條件刪除篩選條件：請參閱 [從現有的 Regex 比對條件刪除篩選條件](#) 以取得執行此動作的指示。)
3. 在導覽窗格中選擇字串和 regex 比對。

4. 選擇您要變更的條件名稱。
5. 選擇新增篩選條件。
6. 為新的篩選條件輸入適當的值，然後選擇新增。

使用規則

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

規則可讓您指定要讓 AWS WAF Classic 監控的確切條件，精確鎖定您希望 AWS WAF Classic 允許或封鎖的 Web 請求。例如，AWS WAF Classic 可以監控請求來源的 IP 地址、請求包含的字串以及字串出現的位置，以及請求是否包含惡意 SQL 程式碼。

主題

- [建立規則和新增條件](#)
- [建立和移除規則的條件](#)
- [刪除規則](#)
- [AWS Marketplace 規則群組](#)

建立規則和新增條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您將多個條件新增至規則，Web 請求必須符合 AWS WAF Classic 的所有條件，才能根據該規則允許或封鎖請求。

建立規則並新增條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入下列值：

名稱

輸入名稱。

CloudWatch 指標名稱

輸入 AWS WAF Classic 將建立並將與規則建立關聯的 CloudWatch 指標名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF Classic 預留的空格或指標名稱，包括「全部」和「預設_動作」。

規則類型

選擇 Regular rule 或 Rate-based rule。以速率為基礎的規則與一般規則相同，但也要考量在五分鐘內從 IP 地址抵達的請求數量。如需這些規則類型的詳細資訊，請參閱 [AWS WAF Classic 的運作方式](#)。

速率限制

對於以速率為基礎的規則，輸入五分鐘期間內允許來自符合規則條件之 IP 地址的最大請求數量。速率限制必須至少為 100。

您可以單獨指定速率限制，也可以同時指定速率限制和條件。如果您只指定速率限制，會將限制 AWS WAF 放在所有 IP 地址上。如果您指定速率限制和條件，會將限制 AWS WAF 放在符合條件的 IP 地址上。

當 IP 地址達到速率限制閾值時，會盡快 AWS WAF 套用指派的動作（封鎖或計數），通常在 30 秒內。動作到位後，如果經過五分鐘沒有 IP 地址的請求，會將計數器 AWS WAF 重設為零。

5. 若要新增條件至規則，請指定以下值：

請求為有 (does)/沒有 (does not) 的時機

如果您希望 AWS WAF Classic 根據條件中的篩選條件允許或封鎖請求，請選擇。例如，如果 IP 比對條件包含 IP 地址範圍 192.0.2.0/24，而您希望 AWS WAF Classic 允許或封鎖來自這些 IP 地址的請求，請選擇。

如果您希望 AWS WAF Classic 根據條件中的篩選條件反面允許或封鎖請求，請選擇不。例如，如果 IP 比對條件包含 IP 地址範圍 192.0.2.0/24，而您希望 AWS WAF Classic 允許或封鎖不是來自這些 IP 地址的請求，請選擇不。

符合/來自

選擇要新增到規則的條件類型。

- 跨網站指令碼比對條件 – 選擇比對跨網站指令碼比對條件中至少一個篩選條件
- IP 比對條件 – 選擇來自 中的 IP 地址
- 地理比對條件 – 選擇來自 中的地理位置
- 大小限制條件 – 選擇至少符合大小限制條件中的其中一個篩選條件
- SQL 注入比對條件 – 選擇至少符合 SQL 注入比對條件中的其中一個篩選條件
- 字串比對條件 – 選擇比對字串比對條件中至少一個篩選條件
- 規則表達式比對條件 – 選擇至少符合 regex 比對條件中的其中一個篩選條件

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述步驟中所選擇的條件類型。

6. 若要新增其他條件至規則，請選擇新增另一個條件，並重複步驟四和五。注意下列事項：

- 如果您新增多個條件，Web 請求必須至少符合每個條件中的一個篩選條件，AWS WAF Classic 才能根據該規則允許或封鎖請求

- 如果您將兩個 IP 比對條件新增至相同的規則，AWS WAF Classic 只會允許或封鎖來自兩個 IP 比對條件中出現之 IP 地址的請求

7. 完成新增條件，請選擇建立。

建立和移除規則的條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

您可以新增或移除條件來變更規則。

新增或移除規則裡的條件

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇規則。
3. 選擇要新增或移除條件的規則名稱。
4. 選擇新增規則。
5. 若要新增一個條件，請選擇新增條件 並指定以下值：

請求為有 (does)/沒有 (does not) 的時機

如果您希望 AWS WAF Classic 根據條件中的篩選條件允許或封鎖請求，例如，源自 IP 地址範圍 192.0.2.0/24 的 Web 請求，請選擇。

如果您希望 AWS WAF Classic 根據條件中的篩選條件反面允許或封鎖請求，請選擇不允許。例如，如果 IP 比對條件包含 IP 地址範圍 192.0.2.0/24，而您希望 AWS WAF Classic 允許或封鎖不是來自這些 IP 地址的請求，請選擇不。

符合/來自

選擇要新增到規則的條件類型。

- 跨網站指令碼比對條件 – 選擇比對跨網站指令碼比對條件中至少一個篩選條件
- IP 比對條件 – 選擇來自 中的 IP 地址
- 地理比對條件 – 選擇來自 中的地理位置
- 大小限制條件 – 選擇至少符合大小限制條件中的其中一個篩選條件
- SQL 注入比對條件 – 選擇至少符合 SQL 注入比對條件中的其中一個篩選條件
- 字串比對條件 – 選擇比對字串比對條件中至少一個篩選條件
- 規則表達式比對條件 – 選擇至少比對 regex 比對條件中的其中一個篩選條件

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述步驟中所選擇的條件類型。

6. 若要移除條件，選擇條件名稱右邊的 X。
7. 選擇更新。

刪除規則

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

如果您想要刪除規則，您必須先從 Web ACL 移除使用它的規則，並移除包含此條件的規則。

刪除規則

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 若要從正在使用規則 ACLs 中移除規則，請為每個 Web ACLs 執行下列步驟：
 - a. 在導覽窗格中，選擇 Web ACL。
 - b. 選擇要刪除使用該規則的 Web ACL。

Note

如果您沒有看到 Web ACL，請確定區域選擇正確。保護 Amazon CloudFront 分佈的 Web ACLs 位於全域 (CloudFront)。

- c. 選擇規則標籤。
 - d. 選擇編輯 Web ACL。
 - e. 選擇您要刪除之規則右側的 X，然後選擇更新。
3. 在導覽窗格中，選擇規則。
 4. 選擇您要刪除的規則名稱。

Note

如果您沒有看到規則，請確定區域選擇正確。保護 Amazon CloudFront 分佈的規則位於全域 (CloudFront)。

5. 選擇 Delete (刪除)。

AWS Marketplace 規則群組

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS WAF Classic 提供 AWS Marketplace 規則群組，可協助您保護資源。AWS Marketplace 規則群組是預先定義、ready-to-use 規則的集合，由 AWS 和 AWS 合作夥伴公司撰寫和更新。

某些 AWS Marketplace 規則群組旨在協助保護特定類型的 Web 應用程式，例如 WordPress、Joomla 或 PHP。其他 AWS Marketplace 規則群組可針對已知威脅或常見的 Web 應用程式漏洞提供廣泛的保護，例如 [OWASP 前 10 名](#) 中列出的漏洞。

您可以從偏好的 AWS 合作夥伴安裝單一 AWS Marketplace 規則群組，也可以新增自訂的 AWS WAF Classic 規則，以提高保護。如果您受到 PCI 或 HIPAA 等法規合規規範，您可能可以使用 AWS Marketplace 規則群組來滿足 Web 應用程式防火牆需求。

AWS Marketplace 規則群組可用，沒有長期合約，也沒有最低承諾。訂閱規則群組時，您必須按月支付費用 (依小時按比例分配)，以及基於用量的持續請求費用。如需詳細資訊，請參閱 [AWS WAF Classic Pricing](#) 和 上每個 AWS Marketplace 規則群組的描述 AWS Marketplace。

自動更新

掌握不斷變化的威脅態勢的最新情況可能很耗時且昂貴。AWS Marketplace 規則群組可以節省您實作和使用 AWS WAF Classic 的時間。另一個好處是，AWS 當新的漏洞和威脅出現時，AWS 我們的合作夥伴會自動更新 AWS Marketplace 規則群組。

許多公開這些漏洞前，我們的合作夥伴會先收到相關通知。他們可以更新規則群組並將它們部署給您，即使在新的威脅已廣泛為人熟知之前。很多合作夥伴也有威脅研究團隊調查和分析最新的威脅，以便寫入最相關的規則。

存取規則群組中的 AWS Marketplace 規則

每個 AWS Marketplace 規則群組都會提供攻擊類型的完整描述，以及其旨在防範的漏洞類型。為了保護規則群組供應商的智慧財產權，所以您無法在規則群組裡逐一查看規則。此限制也有助於防止惡意使用者利用規避發佈的規則設計攻擊威脅。

由於您無法檢視 AWS Marketplace 規則群組中的個別規則，因此您也無法編輯 AWS Marketplace 規則群組中的任何規則。然而，您可將特定規則自規則群組排除。這稱為「規則群組例外」。排除規則不

會移除這些規則，而是會將規則的動作變更為 COUNT。因此，符合排除規則的請求會納入計算，但不会被封鎖。您將接收每個已排除規則的 COUNT 指標。

針對意外封鎖流量 (誤報) 的規則群組進行故障排除時，排除規則十分實用。一個故障排除技巧就是去辨識規則群組內封鎖所需流量的特定規則，然後停用 (排除) 該條規則。

除了排除特定規則，您可啟用或停用整個規則群組，並選擇欲執行的規則群組動作，藉此強化保護。如需詳細資訊，請參閱[使用 AWS Marketplace 規則群組](#)。

配額

您只能啟用一個 AWS Marketplace 規則群組。您也可以啟用一個自訂規則群組，供您使用 建立 AWS Firewall Manager。這些規則群組會計入每 Web ACL 的 10 個規則限額。因此，您可以在單一 Web ACL 中有一個 AWS Marketplace 規則群組、一個自訂規則群組和最多八個自訂規則。

定價

如需 AWS Marketplace 規則群組定價，請參閱[AWS WAF Classic Pricing](#) 和每個 AWS Marketplace 規則群組上的描述 AWS Marketplace。

使用 AWS Marketplace 規則群組

您可以在 AWS WAF Classic 主控台上訂閱和取消訂閱 AWS Marketplace 規則群組。您亦可將特定規則自規則群組排除。

訂閱和使用 AWS Marketplace 規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇市集。
3. 在 Available marketplace products (提供市場產品)，選擇規則的名稱，檢視其詳細資訊和定價資訊。
4. 如果您想訂閱此規則群組，選擇繼續。

Note

如果您不想訂閱此規則群組，只需在您的瀏覽器關閉此頁面。

5. 選擇 Set up your account (建立您的帳戶)。

6. 新增規則群組至 Web ACL，就像您新增個別規則一樣。如需詳細資訊，請參閱 [建立 Web ACL](#) 或 [編輯 Web ACL](#)。

 Note

新增一個規則群組至 Web ACL 時，您為規則群組設定的動作 (No override (不覆寫) 或 Override to count (覆寫計數)) 稱為規則群組覆寫動作。如需詳細資訊，請參閱 [規則群組覆寫](#)。

取消訂閱 AWS Marketplace 規則群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 從所有 Web ACL 中移除規則群組。如需詳細資訊，請參閱 [編輯 Web ACL](#)。
3. 在導覽窗格中，選擇市集。
4. 選擇 Manage your subscriptions (管理我的訂閱)。
5. 在您想要取消訂閱的規則群組名稱旁，選擇取消訂閱。
6. 選擇是，取消訂閱。

自規則群組排除規則 (規則群組例外)

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 如果尚未啟用，請啟用 AWS WAF Classic 記錄。如需詳細資訊，請參閱 [記錄 Web ACL 流量資訊](#)。使用 AWS WAF Classic 日誌來識別您要排除 IDs。這些通常是封鎖正當請求的規則。
3. 在導覽窗格中，選擇 Web ACL。
4. 選擇您要編輯的 Web ACL 名稱。這會在右側窗格中開啟包含 Web ACL 詳細資訊的頁面。

 Note

您希望編輯的規則群組必須與 Web ACL 建立關聯，之後您才能自該規則群組排除規則。

5. 在規則標籤上，右側窗格中，選擇編輯 Web ACL。
6. 在 Rule group exceptions (規則群組例外) 的部分，請展開您想要編輯的規則群組。
7. 選擇欲排除規則旁的 X。您可以使用 AWS WAF Classic 日誌來識別正確的規則 ID。
8. 選擇更新。

排除規則不會將這些規則自規則群組中移除，而是會將規則的動作變更為 COUNT。因此，符合排除規則的請求會納入計算，但不會被封鎖。您將接收每個已排除規則的 COUNT 指標。

Note

您可使用相同程序從 AWS Firewall Manager 中所建立的自訂規則群組中排除規則。然而，若不想使用這些步驟來將規則從自訂規則群組中排除，您只要編輯自訂規則群組即可，步驟詳見 [從 AWS WAF Classic 規則群組新增和刪除規則](#)。

規則群組覆寫

AWS Marketplace 規則群組有兩個可能的動作：無覆寫和覆寫計數。如果您想要測試規則群組，設定動作為覆寫計數。這個規則群組動作會覆寫任何群組內個別規則所指定的封鎖動作。也就是說，如果規則群組的動作是設定為覆寫計數，部會封鎖這些符合群組規則的請求，而是將這些請求計數在內。反之，如果您設定規則群組的動作為不覆寫，則會使用該群組裡規則的動作。

針對 AWS Marketplace 規則群組進行故障診斷

如果您發現 AWS Marketplace 規則群組封鎖合法流量，請執行下列步驟。

AWS Marketplace 規則群組的故障診斷

1. 排除會封鎖正當流量的特定規則。您可以使用 AWS WAF Classic 日誌來識別哪些規則封鎖哪些請求。如需排除規則的詳細資訊，請參閱 [自規則群組排除規則 \(規則群組例外\)](#)。
2. 如果排除特定規則無法解決問題，您可以將 AWS Marketplace 規則群組的動作從無覆寫變更為覆寫以計算。這允許 web 請求通過，無視規則群組內的個別規則動作。這也為您提供規則群組的 Amazon CloudWatch 指標。
3. 將 AWS Marketplace 規則群組動作設定為覆寫計數之後，請聯絡規則群組提供者的客戶支援團隊，以進一步疑難排解問題。如需聯絡資訊，請參閱 AWS Marketplace 中產品列表頁面的規則群組清單。

聯絡客戶支援

對於 AWS WAF Classic 或 管理的規則群組的問題 AWS，請聯絡 AWS 支援。對於由 AWS 合作夥伴管理的規則群組問題，請聯絡該合作夥伴的客戶支援團隊。若要尋找合作夥伴聯絡資訊，請參閱合作夥伴的清單 AWS Marketplace。

建立和銷售 AWS Marketplace 規則群組

如果您想要在上銷售 AWS Marketplace 規則群組 AWS Marketplace，請參閱[如何銷售您的軟體 AWS Marketplace](#)。

使用 Web ACL

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱[將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱[AWS WAF](#)。

當您將規則新增至 Web ACL 時，您可以指定要 AWS WAF Classic 根據規則中的條件允許或封鎖請求。如果您將多個規則新增至 Web ACL，AWS WAF Classic 會根據您在 Web ACL 中列出規則的順序來評估每個請求。當 Web 請求符合規則中的所有條件時，AWS WAF Classic 會立即採取對應的動作 — 允許或封鎖 — 並且不會針對 Web ACL 中的其餘規則評估請求，如果有的話。

如果 Web 請求不符合 Web ACL 中的任何規則，AWS WAF Classic 會採取您為 Web ACL 指定的預設動作。如需詳細資訊，請參閱[決定 Web ACL 的預設動作](#)。

如果您想要在開始使用規則來允許或封鎖請求之前進行測試，您可以設定 AWS WAF Classic 來計算符合規則條件的 Web 請求。如需詳細資訊，請參閱[測試 Web ACL](#)。

主題

- [決定 Web ACL 的預設動作](#)

- [建立 Web ACL](#)
- [將 Web ACL 與 Amazon API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯或取消關聯](#)
- [編輯 Web ACL](#)
- [刪除 Web ACL](#)
- [測試 Web ACL](#)

決定 Web ACL 的預設動作

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

當您建立和設定 Web ACL 時，您首先必須做的最重要決定是預設動作是讓 AWS WAF Classic 允許 Web 請求或封鎖 Web 請求。預設動作會指出您希望 AWS WAF Classic 在檢查 Web 請求後執行的動作，以找出您指定的所有條件，而 Web 請求不符合下列任何條件：

- 允許 – 如果您想要允許大多數使用者存取您的網站，但您想要封鎖對請求來自指定 IP 地址，或請求似乎包含惡意 SQL 程式碼或指定值的攻擊者的存取，請選擇允許預設動作。
- 封鎖：如果您想要防止大多數可能使用者存取您的網站，但想要允許存取其請求來自指定 IP 地址的使用者，或是其請求包含指定值的使用者，請選擇封鎖進行預設動作。

在決定預設動作後，您做的許多決定會取決於您是要允許還是封鎖大多數 Web 請求。例如，如果您想要允許大多數的請求，您建立的比對條件通常應指定您想要封鎖的 web 請求，如下所示：

- 來自發出異常數量 IP 地址的請求
- 來自您不常交涉、或時常受到攻擊國家/地區的請求

- 請求包含仿造使用者代理程式標頭中的值
- 似乎含有惡意 SQL 程式碼的請求

建立 Web ACL

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

建立 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 如果這是您第一次使用 AWS WAF Classic，請選擇移至 AWS WAF Classic，然後選擇設定 Web ACL。如果您之前已使用 AWS WAF 過 Classic，請在導覽窗格中選擇 Web ACLs，然後選擇建立 Web ACL。
3. 針對 Web ACL 名稱，輸入名稱。

Note

建立 Web ACL 後無法修改名稱。

4. 針對 CloudWatch 指標名稱，請變更預設名稱，如適用。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF Classic 預留的空格或指標名稱，包括「全部」和「預設_動作」。

 Note

建立 Web ACL 後無法修改名稱。

5. 對於 區域，選擇一個區域。
6. 對於AWS 資源，請選擇您想要將此 Web ACL 關聯的資源，然後選擇下一步。
7. 如果您已建立您希望 AWS WAF Classic 用來檢查 Web 請求的條件，請選擇下一步，然後繼續下一個步驟。

若您尚未建立條件，請立即執行。如需詳細資訊，請參閱下列主題：

- [使用跨網站指令碼比對條件](#)
 - [使用 IP 比對條件](#)
 - [使用地理比對條件](#)
 - [使用容量限制條件](#)
 - [使用 SQL Injection 比對條件](#)
 - [使用字串比對條件](#)
 - [使用 Regex 比對條件](#)
8. 如果您已建立要新增至此 Web ACL 的規則或規則群組（或訂閱 AWS Marketplace 規則群組），請將規則新增至 Web ACL：
 - a. 在規則清單中選擇規則。
 - b. 選擇 Add rule to web ACL (新增規則至 Web ACL)。
 - c. 重複步驟 a 和 b，直到您已新增所有想要新增至 Web ACL 的規則。
 - d. 前往步驟 10。
 9. 如果您尚未建立規則，您可以現在新增規則：
 - a. 選擇建立規則。
 - b. 輸入下列值：

名稱

輸入名稱。

CloudWatch 指標名稱

輸入 AWS WAF Classic 將建立且將與規則建立關聯的 CloudWatch 指標名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF Classic 預留的空格或指標名稱，包括「全部」和「預設_動作」。

Note

建立規則後無法修改指標名稱。

- c. 若要新增條件至規則，請指定以下值：

請求為有 (does)/沒有 (does not) 的時機

如果您希望 AWS WAF Classic 根據條件中的篩選條件允許或封鎖請求，例如，源自 IP 地址範圍 192.0.2.0/24 的 Web 請求，請選擇。

如果您希望 AWS WAF Classic 根據條件中的篩選條件反面允許或封鎖請求，請選擇不。例如，如果 IP 比對條件包含 IP 地址範圍 192.0.2.0/24，而您希望 AWS WAF Classic 允許或封鎖不是來自這些 IP 地址的請求，請選擇不。

符合/來自

選擇要新增到規則的條件類型。

- 跨網站指令碼比對條件 – 選擇比對跨網站指令碼比對條件中至少一個篩選條件
- IP 比對條件 – 選擇來自 中的 IP 地址
- 地理比對條件 – 選擇來自 中的地理位置
- 大小限制條件 – 選擇至少符合大小限制條件中的其中一個篩選條件
- SQL 注入比對條件 – 選擇至少符合 SQL 注入比對條件中的其中一個篩選條件
- 字串比對條件 – 選擇比對字串比對條件中至少一個篩選條件
- Regex 比對條件 – 選擇比對至少一個 regex 比對條件中的篩選條件

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述名單中所選擇的條件類型。

- d. 若要新增其他條件至規則，請選擇 Add another condition (新增另一個條件)，並重複步驟 b 和 c。注意下列事項：

- 如果您新增多個條件，Web 請求必須至少符合每個條件中的一個篩選條件，AWS WAF Classic 才能根據該規則允許或封鎖請求。
 - 如果您將兩個 IP 比對條件新增至相同的規則，AWS WAF Classic 只會允許或封鎖來自兩個 IP 比對條件中出現之 IP 地址的請求。
- e. 重複步驟九，直到您已建立所有想要新增至 Web ACL 的規則。
 - f. 選擇 Create (建立)。
 - g. 繼續執行步驟 10。
10. 針對 Web ACL 中的每個規則或規則群組，選擇您希望 AWS WAF Classic 提供的管理類型，如下所示：
- 針對每個規則，選擇您是否希望 AWS WAF Classic 根據規則中的條件允許、封鎖或計數 Web 請求：
 - 允許 – API Gateway、CloudFront 或 Application Load Balancer 會回應請求的物件。在 CloudFront 的情況下，如果物件不在邊緣快取中，CloudFront 會將請求轉送到原始伺服器。
 - 封鎖 – API Gateway、CloudFront 或 Application Load Balancer 會使用 HTTP 403（禁止）狀態碼回應請求。CloudFront 也可以使用自訂錯誤頁面來回應。如需詳細資訊，請參閱[使用 AWS WAF Classic 搭配 CloudFront 自訂錯誤頁面](#)。
 - Count – AWS WAF Classic 會增加符合規則條件的請求計數器，然後繼續根據 Web ACL 中的其餘規則檢查 Web 請求。
- 如需先使用 Count (計數) 來測試 Web ACL，再開始用於允許或封鎖 Web 請求的詳細資訊，請參閱[計數在 Web ACL 中符合規則的 web 請求](#)。
- 對於每個規則群組，設定規則群組的覆寫動作：
 - 無覆寫 – 導致使用規則群組中個別規則的動作。
 - 覆寫以計數 – 覆寫群組中個別規則指定的任何區塊動作，以便僅計數所有相符的請求。
- 如需詳細資訊，請參閱[規則群組覆寫](#)。
11. 如果您想要變更 Web ACL 中規則的順序，請使用順序欄中的箭頭。AWS WAF Classic 會根據規則在 Web ACL 中出現的順序來檢查 Web 請求。
 12. 如果您想要移除新增到 Web ACL 的規則，在該規則列選擇 x。
 13. 選擇 Web ACL 的預設動作。這是 AWS WAF Classic 在 Web 請求不符合此 Web ACL 中任何規則的條件時所採取的動作。如需詳細資訊，請參閱[決定 Web ACL 的預設動作](#)。
 14. 選擇 Review and create (檢閱和建立)。
 15. 檢視 Web ACL 的設定，然後選擇確認並建立。

將 Web ACL 與 Amazon API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯或取消關聯

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

若要關聯或取消關聯 Web ACL，請執行適用的程序。請注意，您也可以在建​​立或更新分佈時，將 Web ACL 與 CloudFront 分佈建立關聯。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[使用 AWS WAF Classic 控制對您內容的存取](#)。

當與 Web ACL 關聯時，套用以下限制：

- 每個 API Gateway API、Application Load Balancer 和 CloudFront 分佈只能與一個 Web ACL 建立關聯。
- 與 CloudFront 分佈相關聯的 Web ACLs 無法與 Application Load Balancer 或 API Gateway API 建立關聯。不過，Web ACL 可以與其他 CloudFront 分佈建立關聯。

將 Web ACL 與 API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要與 API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯的 Web ACL 名稱。這會在右側窗格中開啟包含 Web ACL 詳細資訊的頁面。
4. 在規則索引標籤上，AWS 使用此 Web ACL 的資源下，選擇新增關聯。

5. 出現提示時，請使用資源清單來選擇您要與此 Web ACL 建立關聯的 API Gateway API、CloudFront 分佈或 Application Load Balancer。如果您選擇 Application Load Balancer，您也必須指定區域。
6. 選擇新增。
7. 若要將此 Web ACL 與其他 API Gateway API、CloudFront 分佈或其他 Application Load Balancer 建立關聯，請重複步驟 4 到 6。

取消 Web ACL 與 API Gateway API、CloudFront 分佈或 Application Load Balancer 的關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要與 API Gateway API、CloudFront 分佈或 Application Load Balancer 取消關聯的 Web ACL 名稱。這會在右側窗格中開啟包含 Web ACL 詳細資訊的頁面。
4. 在規則索引標籤上，AWS 使用此 Web ACL 的資源下，選擇您要取消此 Web ACL 關聯的每個 API Gateway API、CloudFront 分佈或 Application Load Balancer 的 x。

編輯 Web ACL

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

若要從 Web ACL 移除規則或變更預設動作，請執行下列程序。

編輯 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要編輯的 Web ACL 名稱。這會在右側窗格中開啟包含 Web ACL 詳細資訊的頁面。
4. 在規則標籤上，右側窗格中，選擇編輯 Web ACL。
5. 若要新增規則至 Web ACL，請執行以下步驟：
 - a. 在規則名單中，選擇您要新增的規則。
 - b. 選擇 Add rule to web ACL (新增規則至 Web ACL)。
 - c. 重複步驟 a 和 b，直到您已加入所有想新增的規則。
6. 如果您想要變更 Web ACL 中規則的順序，請使用順序欄中的箭頭。AWS WAF Classic 會根據規則在 Web ACL 中出現的順序來檢查 Web 請求。
7. 若要從 Web ACL 移除規則，在該規則行的右邊選擇 x。這不會從 AWS WAF Classic 刪除規則，只會從此 Web ACL 移除規則。
8. 若要變更規則的動作或 Web ACL 的預設動作，選擇慣用的選項。

Note

為規則群組或 AWS Marketplace 規則群組（而不是單一規則）設定動作時，您為規則群組設定的動作（無覆寫或覆寫計數）稱為覆寫動作。如需詳細資訊，請參閱 [規則群組覆寫](#)

9. 選擇 Save changes (儲存變更)。

刪除 Web ACL

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

若要刪除 Web ACL，您必須移除 Web ACL 中包含的規則，並取消所有 CloudFront 分佈和 Application Load Balancer 與 Web ACL 的關聯。請執行以下程序。

刪除 Web ACL

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要刪除的 Web ACL 名稱。這會在右側窗格中開啟包含 Web ACL 詳細資訊的頁面。

 Note

如果您沒有看到 Web ACL，請確定區域選擇正確。保護 Amazon CloudFront 分佈的 Web ACLs 位於全域 (CloudFront)。

4. 在規則標籤上，右側窗格中，選擇編輯 Web ACL。
5. 若要從 Web ACL 移除所有規則，在每個規則行的右邊選擇 x。這不會從 AWS WAF Classic 刪除規則，只會從此 Web ACL 移除規則。
6. 選擇更新。
7. 取消 Web ACL 與所有 CloudFront 分佈和 Application Load Balancer 的關聯。在規則索引標籤上，AWS 使用此 Web ACL 的資源下，為每個 API Gateway API、CloudFront 分佈或 Application Load Balancer 選擇 x。
8. 在 Web ACL 頁面上確認已選取您要刪除的 Web ACL，然後選擇 Delete (刪除)。

測試 Web ACL

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

為了確保您不意外地設定 AWS WAF Classic 來封鎖您想要允許或允許您想要封鎖的請求，建議您在網站或 Web 應用程式開始使用 Web ACL 之前，先徹底測試您的 Web ACL。

主題

- [計數在 Web ACL 中符合規則的 web 請求](#)
- [檢視 API Gateway CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 的 Web 請求範例](#)

計數在 Web ACL 中符合規則的 web 請求

當您將規則新增至 Web ACL 時，您可以指定是否要讓 AWS WAF Classic 允許、封鎖或計數符合該規則中所有條件的 Web 請求。建議您以下列組態開始動作：

- 設定 Web ACL 的所有規則，以計數 Web 請求
- 設定 Web ACL 的預設動作，以允許請求

在此組態中，AWS WAF Classic 會根據第一個規則中的條件檢查每個 Web 請求。如果 Web 請求符合該規則中的所有條件，AWS WAF Classic 會遞增該規則的計數器。然後，AWS WAF Classic 會根據下一個規則中的條件來檢查 Web 請求。如果請求符合該規則中的所有條件，AWS WAF Classic 會遞增規則的計數器。這會持續到 AWS WAF Classic 根據您的所有規則的條件檢查請求為止。

在 Web ACL 中設定所有規則以計算請求，並將 Web ACL 與 Amazon API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯之後，您可以在 Amazon CloudWatch 圖表中檢視產生的計數。對於 Web ACL 中的每個規則，以及 API Gateway、CloudFront 或 Application Load Balancer 轉送至 Web ACL 的 AWS WAF Classic 的所有請求，CloudWatch 可讓您：

- 檢視前一小時或前三小時的資料，
- 變更資料點之間的間隔。
- 變更 CloudWatch 對資料執行的計算，例如最大值、最小值、平均值或總和

Note

AWS WAF Classic with CloudFront 是一項全球服務，且指標只有在您選擇中的美國東部（維吉尼亞北部）區域時才能使用 AWS Management Console。如果您選擇其他區域，CloudWatch 主控台中不會顯示 AWS WAF Classic 指標。

若要在 Web ACL 查看規則資料

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中，於 Metrics (指標) 下選擇 WAF。
3. 選取要檢視資料的 Web ACL 的核取方塊。
4. 變更適用的設定：

統計數字

選擇 CloudWatch 對資料執行的計算。

時間範圍

選擇您想要檢視前一小時或前三個小時的資料。

期間

選擇圖形中資料點之間的間隔。

規則

選擇您要檢視資料的規則。

注意下列事項：

- 如果您剛將 Web ACL 與 API Gateway API、CloudFront 分佈或 Application Load Balancer 建立關聯，您可能需要等待幾分鐘，資料才會出現在圖形中，而 Web ACL 的指標才會出現在可用指標清單中。
- 如果您將多個 API Gateway API、CloudFront 分佈或 Application Load Balancer 與 Web ACL 建立關聯，CloudWatch 資料將包含與 Web ACL 關聯的所有分佈的所有請求。
- 您可以將滑鼠指標移至資料點以取得更多資訊。
- 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理



圖示。

5. (選用) 檢視 API Gateway CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 之個別請求的詳細資訊。如需詳細資訊，請參閱[檢視 API Gateway CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 的 Web 請求範例](#)。
6. 如果您認為規則正在攔截您不希望攔截的請求，請變更設定。如需詳細資訊，請參閱[建立和設定 Web 存取控制清單 \(Web ACL\)](#)。

當您對所有規則都能攔截到正確請求感到滿意時，請將每個規則的操作更改為允許或封鎖。如需詳細資訊，請參閱[編輯 Web ACL](#)。

檢視 API Gateway CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 的 Web 請求範例

在 AWS WAF Classic 主控台中，您可以檢視 API Gateway CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 進行檢查的請求範例。對於每個抽樣請求，您可以查看請求的詳細資料，例如源於的 IP 地址和包含在請求中的標頭。您也可以檢視請求符合的規則、規則是否有正確設定以用於允許或封鎖請求。

請求樣本最多含有 100 個請求符合所有條件中的每個規則中，以及另外 100 個預設動作的請求，這些請求適用於不符合所有條件中的任何規則。範例中的請求來自過去 15 分鐘內收到內容請求的所有 API Gateway APIs、CloudFront 節點或 Application Load Balancer。

檢視 API Gateway；CloudFront 或 Application Load Balancer 已轉送至 AWS WAF Classic 的 Web 請求範例

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇您要檢視的 Web ACL 請求。
3. 在右窗格中，選擇請求標籤。

抽樣請求 表為每個請求顯示以下的值：

來源 IP

請求來源的 IP 地址，或者，如果檢視器使用 HTTP 代理或 Application Load Balancer 傳送請求，則為代理或 Application Load Balancer 的 IP 地址。

URI

請求的 URI 路徑，可識別資源，例如 `/images/daily-ad.jpg`。這不包含 URI 的查詢字串或片段元件。如需詳細資訊，請參閱[統一資源識別符 \(URI\)：一般語法](#)。

比對規則

識別 web 請求中符合所有 Web ACL 條件的中第一個規則。如果 web 請求不符合和所有 Web ACL 條件的規則，則 Matches rule (比對規則) 為預設。

請注意，當 Web 請求符合規則中的所有條件，且該規則的動作為 Count 時，AWS WAF Classic 會根據 Web ACL 中的後續規則繼續檢查 Web 請求。在這種情況下，web 請求可能會在抽樣請求名單上出現兩次：一次因為規則操作 Count (計數) 的動作，並再次在後續規則或預設動作操作。

動作

指出動作對應的規則為允許、封鎖 或 Count (計數)。

時間

AWS WAF Classic 從 API Gateway、CloudFront 或 Application Load Balancer 收到請求的時間。

4. 若要顯示請求的其他資訊，請選擇該請求 IP 地址左側的箭頭。AWS WAF Classic 會顯示下列資訊：

來源 IP

相同的 IP 地址做為表格中來源 IP 欄的值。

Country

請求源自國家的雙字母國家/地區代碼。如果檢視器使用 HTTP 代理或 Application Load Balancer 來傳送請求，這是 HTTP 代理或 Application Load Balancer 所在的國家/地區的兩個字母國家/地區代碼。

如需雙字母國家/地區代碼對應的國家/地區名稱，請參閱 Wikipedia 項目 [ISO 3166-1 alpha-2](#)。

方法

HTTP 請求方法的請求：GET、HEAD、OPTIONS、PUT、POST、PATCH 或 DELETE。

URI

相同的 URI 做為表格中來源 IP 欄的值。

請求標頭

請求的標頭和請求的標頭值。

- 若要重新整理範例清單，選擇 Get new samples (取得新的範例)。

使用 AWS WAF Classic 規則群組搭配 AWS Firewall Manager

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。
如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS WAF Classic 規則群組是您新增至 AWS WAF Classic AWS Firewall Manager 政策的一組規則。您可以建立自己的規則群組，也可以從中購買受管規則群組 AWS Marketplace。

Important

如果您想要將 AWS Marketplace 規則群組新增至 Firewall Manager 政策，組織中的每個帳戶都必須首先訂閱該規則群組。所有帳戶都已完成訂閱後，您就可以將規則群組新增至政策。如需詳細資訊，請參閱[AWS Marketplace 規則群組](#)。

主題

- [建立 AWS WAF Classic 規則群組](#)
- [從 AWS WAF Classic 規則群組新增和刪除規則](#)

建立 AWS WAF Classic 規則群組

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

當您建立要搭配使用的 AWS WAF Classic 規則群組時 AWS Firewall Manager，您可以指定要新增至群組的規則。

建立規則群組 (主控台)

1. AWS Management Console 使用您在先決條件中設定的 AWS Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fms>。

 Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [建立 AWS Firewall Manager 預設管理員帳戶](#)。

2. 在導覽窗格中，選擇切換至 AWS WAF 傳統。
3. 在 AWS WAF 傳統導覽窗格中，選擇規則群組。
4. 選擇 建立規則群組。

 Note

您不能將以速率為基礎的規則新增至規則群組中。

5. 如果您已建立了希望新增至規則群組的規則，選擇 Use existing rules for this rule group (對此規則群組使用現有的規則)。如果您要建立新規則以新增到群組中，選擇 Create rules and conditions for this rule group (為此規則群組建立規則和條件)。
6. 選擇 Next (下一步)。
7. 如果您選擇建立規則，請遵循 [建立規則和新增條件](#) 的步驟來建立規則。

 Note

使用 AWS WAF Classic 主控台建立您的規則。

建立所有需要的規則後，請移至下一個步驟。

8. 輸入規則名稱。
9. 若要新增規則至規則群組，請選取規則，然後選擇 Add rule (新增規則)。選擇是否允許、封鎖或計數符合規則條件的請求。如需選項的詳細資訊，請參閱 [AWS WAF Classic 的運作方式](#)。
10. 完成規則新增作業時，選擇 Create (建立)。

您可以將規則群組新增至 AWS WAF WebACL，並將 WebACL 動作設定為覆寫為計數，以測試規則群組。此動作會覆寫您為群組中規則選擇的任何動作，且只會計數符合的請求。如需詳細資訊，請參閱 [建立 Web ACL](#)。

從 AWS WAF Classic 規則群組新增和刪除規則

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

您可以在 AWS WAF Classic 規則群組中新增或刪除規則。

刪除規則群組裡的規則，並不刪除規則本身。它只會移除規則群組裡的規則。

新增或刪除規則群組裡的規則 (主控台)。

1. AWS Management Console 使用您在先決條件中設定的 AWS Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fms>。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [建立 AWS Firewall Manager 預設管理員帳戶](#)。

2. 在導覽窗格中，選擇切換至 AWS WAF 傳統。
3. 在 AWS WAF 傳統導覽窗格中，選擇規則群組。
4. 選擇您要編輯的規則群組。

Note

如果您沒有看到要編輯的規則群組，請確定您已選取正確的區域。對於用於保護 Amazon CloudFront 分佈的規則群組，請使用全域 (CloudFront) 設定。

5. 選擇編輯規則群組。
6. 若要新增規則，請執行以下步驟：
 - a. 選取一個規則，然後選擇Add rule to rule group (新增規則至規則群組)。選擇是否允許、封鎖或計數符合規則條件的請求。如需選項的詳細資訊，請參閱[AWS WAF Classic 的運作方式](#)。重複，以新增更多規則至規則群組。

 Note

您不能將以速率為基礎的規則新增至規則群組中。

- b. 選擇更新。
7. 若要刪除規則，請執行以下步驟：
 - a. 在您要刪除的規則旁，選擇 X。重複，以刪除更多規則群組裡的規則。
 - b. 選擇更新。

開始使用 AWS Firewall Manager 以啟用 AWS WAF Classic 規則

 Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

您可以使用 AWS Firewall Manager 來啟用 AWS WAF 規則、AWS WAF 傳統規則 AWS Shield Advanced、保護和 Amazon VPC 安全群組。每個開始設定的步驟稍微不同。

- 若要使用 Firewall Manager 啟用使用最新版本的規則 AWS WAF，請勿使用此主題。反之，請依照 [設定 AWS Firewall Manager AWS WAF 政策](#) 中的步驟進行。

- 若要使用 Firewall Manager 啟用 AWS Shield Advanced 保護，請遵循中的步驟[設定 AWS Firewall Manager AWS Shield Advanced 政策](#)。
- 若要使用 Firewall Manager 啟用 Amazon VPC 安全群組，請遵循中的步驟[設定 AWS Firewall Manager Amazon VPC 安全群組政策](#)。

若要使用 Firewall Manager 啟用 AWS WAF Classic 規則，請依序執行下列步驟。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立規則](#)
- [步驟 3：建立規則群組](#)
- [步驟 4：建立和套用 AWS Firewall Manager AWS WAF Classic 政策](#)

步驟 1：完成先決條件

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。先完成所有的先決條件，再進行 [步驟 2：建立規則](#)。

步驟 2：建立規則

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

在此步驟中，您會使用 AWS WAF Classic 建立規則。如果您已有想要與搭配使用 AWS WAF 的 Classic 規則 AWS Firewall Manager，請略過此步驟，然後前往 [步驟 3：建立規則群組](#)。

Note

使用 AWS WAF Classic 主控台建立您的規則。

建立 AWS WAF Classic 規則（主控台）

- 建立您的規則，然後將您的條件新增至您的規則。如需詳細資訊，請參閱[建立規則和新增條件](#)。

您現在可以前往[步驟 3：建立規則群組](#)。

步驟 3：建立規則群組

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

規則群組是一組規則的集合，定義當滿足特定條件時該採取的動作。您可以從使用受管規則群組 AWS Marketplace，也可以建立自己的規則群組。如需受管規則群組的相關資訊，請參閱 [AWS Marketplace 規則群組](#)。

若要建立自己的安全群組，請執行下列程序。

建立規則群組 (主控台)

1. AWS Management Console 使用您在先決條件中設定的 AWS Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fms>。
2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循指示，然後再度開始此步驟 (建立規則群組)。如果您已滿足先決條件，選擇關閉。
4. 選擇 建立政策。

針對 Policy type (政策類型)，選擇 AWS WAF Classic。
5. 選擇建立 AWS Firewall Manager 政策並新增規則群組。
6. 選擇 AWS 區域，然後選擇下一步。
7. 由於您已建立的規則，所以您無需建立條件。選擇 Next (下一步)。
8. 由於您已建立的規則，所以您無需建立規則。選擇 Next (下一步)。
9. 選擇 建立規則群組。
10. 在 Name (名稱) 中，輸入易記的名稱。
11. 輸入 AWS WAF Classic 將建立且將與規則群組建立關聯的 CloudWatch 指標名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_! " # ' + * } , . / 。不能含有空格。
12. 選取一個規則，然後選擇新增規則。規則有動作設定，可讓您選擇是否允許、封鎖或計數符合規則條件的請求。在此教學課程，請選擇計數。重複新增規則，直到您已新增完所有想要新贈至規則群組的規則。
13. 選擇 Create (建立)。

您現在可以前往 [步驟 4：建立和套用 AWS Firewall Manager AWS WAF Classic 政策](#)。

步驟 4：建立和套用 AWS Firewall Manager AWS WAF Classic 政策

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

建立規則群組之後，您可以建立 AWS Firewall Manager AWS WAF 政策。Firewall Manager AWS WAF 政策包含您想要套用至資源的規則群組。

建立 Firewall Manager AWS WAF 政策（主控台）

1. 在您建立規則群組後（上一個程序的最後一個步驟，[步驟 3：建立規則群組](#)）主控台會顯示 Rule group summary（規則群組摘要）頁面。選擇 Next（下一步）。
2. 在 Name（名稱）中，輸入易記的名稱。
3. 針對政策類型，選擇 WAF。
4. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇全域。

若要保護多個區域中的資源（CloudFront 資源除外），您必須為每個區域建立個別的 Firewall Manager 政策。

5. 選取要新增得規則群組，然後選擇新增規則群組。
6. 政策有兩種動作：規則群組這定的動作和計數。如果您想要測試政策和規則群組，設定動作為計數。這個動作覆寫任何由政策裡規則群組所指定的封鎖動作。也就是說，如果政策的動作是設定為計數，只會計算請求，而不會封鎖請求。反之，如果您設定政策的動作為規則群組這定的動作，則會使用該政策裡規則群組的動作。在此教學課程，請選擇計數。
7. 選擇 Next（下一步）。

8. 如果您想要在政策中只包含特定帳戶、或在政策中排除特定帳戶，請選取 **Select accounts to include/exclude from this policy (optional)** (選擇此政策要包含/排除的帳戶選用)。選擇在此政策中只包含這些帳戶或在此政策中排除這些帳戶。您只可以選擇一個選項。選擇新增。選取要包含或排除的帳戶號碼，然後選擇 OK。

 Note

如果您未選取此選項，則 Firewall Manager 會將政策套用至組織中的所有帳戶 AWS Organizations。如果您將新帳戶新增至組織，防火牆管理員會自動將政策套用到該帳戶。

9. 選擇您要保護的資源類型。
10. 如果您只想保護具有特定標籤的資源，或排除具有特定標籤的資源，請選擇 **Use tags to include/exclude resources** (使用標籤包含/排除資源)，輸入標籤的類型，然後選擇包含或排除。您只可以選擇一個選項。

如果您輸入多個標籤 (以逗號分隔)，且如果資源擁有其中任一的標籤，都會被視為符合條件。

如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。

11. 選擇建立和套用此政策到現有的和新的資源。

此選項會在 組織中的每個適用帳戶中建立 Web ACL AWS Organizations，並將 Web ACL 與帳戶中指定的資源建立關聯。此選項還會將政策套用到與前述條件 (資源類型和標籤) 符合的所有新的資源。或者，如果您選擇建立，但不將此政策套用到現有或新的資源，則 Firewall Manager 會在組織內每個適用的帳戶中建立 Web ACL，但不套用 Web ACL 到任何資源。之後，您必須將政策套用到資源。

12. 在預設設定中保留 [取代現有關聯的 Web ACL] 的選擇。

選取此選項時，防火牆管理員會從範圍內資源移除所有現有的 Web ACL 關聯，然後再將新政策的 Web ACLs 與其建立關聯。

13. 選擇 Next (下一步)。
14. 檢視新政策。若要修改，選擇編輯。當您滿意時，選擇 建立政策。

教學課程：使用階層規則建立 AWS Firewall Manager 政策

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前在中建立 AWS WAF 規則和 Web ACLs 等資源，且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需的最新版本 AWS WAF，請參閱 [AWS WAF](#)。

使用 AWS Firewall Manager，您可以建立和套用包含階層規則的 AWS WAF Classic 保護政策。也就是，您可以集中建立並強制執行特定規則，但將帳戶專屬規則的建立和維護作業委派給其他個人。您可以監控集中套用 (通用) 的任何意外刪除或錯誤處理規則，因此可確保一致地套用這些規則。帳戶專屬規則可新增針對個別團隊需求自訂的進一步防護。

Note

在最新版本的 AWS WAF 中，此功能內建於中，不需要任何特殊處理。如果您尚未使用 AWS WAF Classic，請改用最新版本。請參閱 [為建立 AWS Firewall Manager 政策 AWS WAF](#)。

下列教學課程說明如何建立防護規則的階層組。

主題

- [步驟 1：指定 Firewall Manager 管理員帳戶](#)
- [步驟 2：使用 Firewall Manager 管理員帳戶建立規則群組](#)
- [步驟 3：建立 Firewall Manager 政策並連接一般規則群組](#)
- [步驟 4：新增帳戶專屬規則](#)
- [結論](#)

步驟 1：指定 Firewall Manager 管理員帳戶

若要使用 AWS Firewall Manager，您必須將組織中的帳戶指定為 Firewall Manager 管理員帳戶。此帳戶可以是管理帳戶或組織中的成員帳戶。

您可以使用 Firewall Manager 管理員帳戶來建立一組通用規則，這些規則會套用至組織中的其他帳戶。組織中的其他帳戶無法變更集中套用的規則。

若要將帳戶指定為 Firewall Manager 管理員帳戶，並完成使用 Firewall Manager 的其他先決條件，請參閱 [中的說明](#)[AWS Firewall Manager 先決條件](#)。如果您已完成先決條件，則可以跳至此教學課程中的步驟 2。

在本教學課程中，我們將管理員帳戶稱為 **Firewall-Administrator-Account**。

步驟 2：使用 Firewall Manager 管理員帳戶建立規則群組

接著，使用 **Firewall-Administrator-Account** 建立一個規則群組。此規則群組包含您將套用至所有成員帳戶的通用規則。這些成員帳戶是以您在下一步中建立的政策管理。僅 **Firewall-Administrator-Account** 可以變更這些規則和容器規則群組。

在本教學課程中，我們將此容器規則群組稱為 **Common-Rule-Group**。

若要建立規則群組，請參閱[建立 AWS WAF Classic 規則群組](#)中的說明。遵循這些指示時，請記得使用 Firewall Manager 管理員帳戶 (**Firewall-Administrator-Account**) 登入主控台。

步驟 3：建立 Firewall Manager 政策並連接一般規則群組

使用 **Firewall-Administrator-Account** 建立 Firewall Manager 政策。建立此政策時，您必須執行下列作業：

- 新增 **Common-Rule-Group** 至新政策。
- 將組織內您想要套用 **Common-Rule-Group** 的所有帳戶納入。
- 新增您想要套用 **Common-Rule-Group** 的所有資源。

如需建立政策的說明，請參閱[建立 AWS Firewall Manager 政策](#)。

此會在各指定的帳戶中建立 web ACL，並將 **Common-Rule-Group** 新增至各 web ACL。建立政策後，此 web ACL 和通用規則便會部署至所有指定的帳戶。

在本教學課程中，我們將此 web ACL 稱為 **Administrator-Created-ACL**。唯一的 **Administrator-Created-ACL** 現在存在於組織中各個指定成員帳戶內。

步驟 4：新增帳戶專屬規則

組織中的各成員帳戶現在可以將自己的帳戶專屬規則新增至存在於其帳戶中的 **Administrator-Created-ACL**。已經在 中的常見規則會 **Administrator-Created-ACL** 繼續套用，以及新的帳戶特定規則。會根據規則出現在 Web ACL 中的順序來 AWS WAF 檢查 Web 請求。這適用於 **Administrator-Created-ACL** 和帳戶專屬規則。

若要將規則新增至 **Administrator-Created-ACL**，請參閱 [在中編輯保護套件或 Web ACL AWS WAF](#)。

結論

您現在有一個 Web ACL，其中包含 Firewall Manager 管理員帳戶管理的常見規則，以及每個成員帳戶維護的帳戶特定規則。

各帳戶中的 **Administrator-Created-ACL** 參照單一 **Common-Rule-Group**。因此，防火牆管理員帳戶未來變更為 **Common-Rule-Group** 將立即在每個成員帳戶中生效。

會員帳戶無法變更或移除 **Common-Rule-Group** 中的通用規則。

帳戶專屬規則不會影響其他帳戶。

記錄 Web ACL 流量資訊

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

 Note

您無法使用 Amazon Security Lake 收集 AWS WAF Classic 資料。

您可以啟用日誌記錄取得您 Web ACL 分析流量的詳細資訊。日誌中包含的資訊包括 AWS WAF Classic 從您的 AWS 資源接收請求的時間、請求的詳細資訊，以及每個請求相符規則的動作。

開始請您先建立 Amazon Kinesis Data Firehose。您可以選擇存放日誌的目的地。然後，可以選擇要啟用記錄的 Web ACL。啟用記錄後，會透過 firehose 將日誌 AWS WAF 傳遞至您的儲存目的地。

如需有關如何建立 Amazon Kinesis Data Firehose 和檢閱儲存日誌的資訊，請參閱[什麼是 Amazon Data Firehose？](#) 若要了解 Kinesis Data Firehose 組態所需的許可，請參閱[使用 Amazon Kinesis Data Firehose 控制存取](#)。

您必須擁有以下權限，才能順利啟用記錄：

- iam:CreateServiceLinkedRole
- firehose:ListDeliveryStreams
- waf:PutLoggingConfiguration

如需服務連結角色和 iam:CreateServiceLinkedRole 許可的詳細資訊，請參閱[使用 AWS WAF Classic 的服務連結角色](#)。

啟用 Web ACL 記錄

1. 使用名稱開頭字首「aws-waf-logs-」建立 Amazon Kinesis Data Firehose，例如 aws-waf-logs-us-east-2-analytics。使用 PUT 來源以及您正在操作的區域建立資料 firehose。如果您要擷取 Amazon CloudFront 的日誌，請在美國東部（維吉尼亞北部）建立 firehose。如需詳細資訊，請參閱[建立 Amazon Data Firehose 交付串流](#)。

 Important

請勿選擇 Kinesis stream 做為您的來源。

一個 AWS WAF Classic 日誌相當於一個 Firehose 記錄。如果您通常每秒收到 10,000 個請求，並啟用完整日誌，您應該在 Firehose 中每秒有 10,000 個記錄設定。如果您未正確設定 Firehose，AWS WAF Classic 將不會記錄所有日誌。如需詳細資訊，請參閱[Amazon Kinesis Data Firehose 配額](#)。

2. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換到 AWS WAF 傳統，請選取它。

3. 在導覽窗格中，選擇 Web ACL。
4. 選擇您要為其啟用記錄的 Web ACL 名稱。這會開啟頁面，並在右側窗格中顯示 Web ACL 的詳細資訊。
5. 在記錄標籤中，選擇啟用記錄。
6. 選擇您在第一步驟建立的 Kinesis Data Firehose。您必須選擇開頭為「aws-waf-logs-」的 firehose。
7. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 REDACTED。例如，如果您編寫 Cookie 欄位，在日誌的 Cookie 欄位則會為 REDACTED。
8. 選擇 Enable Logging (啟用記錄日誌)。

Note

當您成功啟用日誌記錄時，AWS WAF Classic 將建立一個服務連結角色，具有將日誌寫入 Amazon Kinesis Data Firehose 的必要許可。如需詳細資訊，請參閱[使用 AWS WAF Classic 的服務連結角色](#)。

停用 Web ACL 記錄

1. 在導覽窗格中，選擇 Web ACL。
2. 選擇您要停用記錄的 Web ACL 名稱。這會開啟頁面，並在右側窗格中顯示 Web ACL 的詳細資訊。
3. 在記錄標籤中，選擇停用記錄。
4. 在對話方塊中，選擇停用記錄。

Example 範例日誌

```
{  
  
  "timestamp":1533689070589,
```

```
"formatVersion":1,
"webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
"terminatingRuleId":"Default_Action",
"terminatingRuleType":"REGULAR",
"action":"ALLOW",
"httpSourceName":"CF",
"httpSourceId":"i-123",
"ruleGroupList":[
    {
        "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
        "terminatingRule":null,
        "nonTerminatingMatchingRules":[
            {
                "action" : "COUNT",
                "ruleId" :
"4659b169-2083-4a91-bbd4-08851a9aaf74"}
        ],
        "excludedRules":
[
            {
                "exclusionType" :
"EXCLUDED_AS_COUNT",
                "ruleId" :
"5432a230-0113-5b83-bbb2-89375c5bfa98"}
        ]
    }
],

"rateBasedRuleList":[
    {
        "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

        "limitKey":"IP",
        "maxRateAllowed":100
    },
    {
        "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
        "limitKey":"IP",
        "maxRateAllowed":100
    }
],

"nonTerminatingMatchingRules":[
    {
        "action" : "COUNT",
```

```
        "ruleId" : "4659b181-2011-4a91-bbd4-08851a9aaf52"}
    ],

    "httpRequest":{
        "clientIp":"192.10.23.23",

        "country":"US",

        "headers":[
            {
                "name":"Host",
                "value":"127.0.0.1:1989"
            },
            {
                "name":"User-Agent",
                "value":"curl/7.51.2"
            },
            {
                "name":"Accept",
                "value":"*/*"
            }
        ],
        "uri":"REDACTED",
        "args":"username=abc",
        "httpVersion":"HTTP/1.1",
        "httpMethod":"GET",
        "requestId":"cloud front Request id"
    }
}
```

以下是這些日誌中所列項目的說明：

timestamp

時間戳記，以毫秒為單位。

formatVersion

日誌的格式版本。

webaclId

Web ACL 的 GUID。

terminatingRuleId

終止請求的規則 ID。如果無法終止請求，則值為 Default_Action。

terminatingRuleType

終止請求的規則類型。可能的值：RATE_BASED、REGULAR 及 GROUP。

動作

動作。終止規則可能的值：ALLOW 及 BLOCK。COUNT 並非終止規則的有效值。

terminatingRuleMatchDetails

符合請求之終止規則的詳細資訊。終止規則對 Web 請求具有結束檢查程序的動作。終止規則可能的動作是「允許」和「封鎖」。這只會為 SQL Injection 和跨網站指令碼 (XSS) 符合規則陳述式填入。與所有檢查多個項目的規則陳述式一樣，AWS WAF 會在第一個符合項目上套用動作，並停止檢查 Web 請求。具有終止動作的 Web 請求除了包含記錄中報告的威脅之外，還可能包含其他威脅。

httpSourceName

請求的來源。可能的值：CF (如果來源是 Amazon CloudFront)、APIGW (如果來源是 Amazon API Gateway) 和 ALB (如果來源是 Application Load Balancer)。

httpSourceId

來源 ID。此欄位會顯示關聯的 Amazon CloudFront 分佈 ID、適用於 API Gateway 的 REST API，或 Application Load Balancer 的名稱。

ruleGroupList

處理此請求的規則群組名單。前述程式碼範例僅有一個規則群組。

ruleGroupId

規則群組的 ID。若規則封鎖請求，則 ruleGroupId 的 ID 將與 terminatingRuleId 的 ID 相同。

terminatingRule

在規則群組中終止請求的規則。若此不是 null 值，則也包含 ruleid (ruleid) 和 action (動作)。在這種情況下，動作一律是 BLOCK。

nonTerminatingMatchingRules

規則群組中符合請求的規則名單。這些一律是 COUNT 規則 (符合的非終止規則)。

動作 (nonTerminatingMatchingRules 群組)

這一律是 COUNT (符合的非終止規則)。

ruleId (nonTerminatingMatchingRules 群組)

在規則群組符合請求的規則 ID 為非終止的。也就是 COUNT (計數) 規則。

excludedRules

規則群組中已排除的規則清單。這些規則的動作設定為 COUNT。

exclusionType (excludedRules 群組)

此類型表示已排除的規則均具備動作 COUNT。

ruleId (excludedRules 群組)

在規則群組中被排除的規則 ID。

rateBasedRuleList

處理請求的以速率為基礎的規則名單。

rateBasedRuleId

處理請求的速率規則 ID。若此項目已終止請求，則 rateBasedRuleId 的 ID 將與 terminatingRuleId 的 ID 相同。

limitKey

AWS WAF 用於判斷請求是否可能來自單一來源，因此受速率監控影響的欄位。可能的值：IP。

maxRateAllowed

五分鐘內允許的請求數量上限，此值與 limitKey 指定之欄位中的值相同。如果請求數量超過，maxRateAllowed 而且也符合規則中指定的其他述詞，AWS WAF 則會觸發為此規則指定的動作。

httpRequest

請求的中繼資料。

clientIp

傳送請求的用戶端 IP 地址。

國家/地區

請求來源的國家/地區。如果 AWS WAF 無法判斷原始國家/地區，則會將此欄位設定為 -。

標頭

標題清單。

uri

URI 請求。前述程式碼範例說明此欄位經修訂後可能的值。

args

查詢字串。

httpVersion

HTTP 版本。

httpMethod

請求的 HTTP 方法。

requestId

請求的 ID。

以速度為基礎的規則列出封鎖的 IP 地址

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS WAF Classic 提供速率型規則封鎖的 IP 地址清單。

檢視以速度為基礎的規則的地址

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF 主控台。

如果您在導覽窗格中看到切換至 AWS WAF Classic，請選取它。

2. 在導覽窗格中，選擇規則。
3. 在名稱欄，選擇以速率為基礎的規則。

此名單顯示規則目前封鎖的 IP 地址。

AWS WAF Classic 如何與 Amazon CloudFront 功能搭配使用

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

當您建立 Web ACL 時，您可以指定一或多個您希望 AWS WAF Classic 檢查的 CloudFront 分佈。AWS WAF Classic 會根據您在 Web ACL 中識別的條件開始允許、封鎖或計數這些分佈的 Web 請求。CloudFront 提供一些增強 AWS WAF Classic 功能的功能。本章說明您可以設定 CloudFront 讓 CloudFront 和 AWS WAF Classic 一起運作的幾種方式。

主題

- [使用 AWS WAF Classic 搭配 CloudFront 自訂錯誤頁面](#)
- [針對在您自己的 HTTP 伺服器上執行的應用程式，使用 AWS WAF Classic 搭配 CloudFront](#)
- [選擇 CloudFront 回應的 HTTP 方法](#)

使用 AWS WAF Classic 搭配 CloudFront 自訂錯誤頁面

當 AWS WAF Classic 根據您指定的條件封鎖 Web 請求時，它會將 HTTP 狀態碼 403（禁止）傳回 CloudFront。接下來，CloudFront 會將該狀態碼傳回給檢視器。檢視器然後會顯示與此相似的簡短且稀疏格式化的預設訊息：

```
Forbidden: You don't have permission to access /myfilename.html on this
server.
```

如果您寧願顯示自訂錯誤訊息，可能使用與網站其他部分相同的格式，您可以設定 CloudFront 將包含自訂錯誤訊息的物件（例如 HTML 檔案）傳回給檢視器。

Note

CloudFront 無法區分原始伺服器傳回的 HTTP 狀態碼 403，以及封鎖請求時 AWS WAF Classic 傳回的狀態碼 403。這表示您無法根據不同原因導致 HTTP 狀態碼 403 而傳回不同的自訂錯誤頁面。

如需 CloudFront 自訂錯誤頁面的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[自訂錯誤回應](#)。

針對在您自己的 HTTP 伺服器上執行的應用程式，使用 AWS WAF Classic 搭配 CloudFront

當您搭配 CloudFront 使用 AWS WAF Classic 時，您可以保護在任何 HTTP Web 伺服器上執行的應用程式，無論是在 Amazon Elastic Compute Cloud (Amazon EC2) 中執行的 Web 伺服器，還是私下管理的 Web 伺服器。您也可以將 CloudFront 設定為在 CloudFront 與您自己的 Web 伺服器之間，以及檢視器與 CloudFront 之間需要 HTTPS。

在 CloudFront 和您自己的 Web 伺服器之間需要 HTTPS

若要在 CloudFront 和您自己的 Web 伺服器之間要求 HTTPS，您可以使用 CloudFront 自訂原始伺服器功能，並設定特定原始伺服器的原始伺服器通訊協定政策和原始伺服器網域名稱設定。在 CloudFront 組態中，您可以指定伺服器的 DNS 名稱，以及連接埠和您希望 CloudFront 從原始伺服器擷取物件時使用的通訊協定。您也應確保您自訂原始伺服器上的 SSL/TLS 憑證符合您已設定的原始伺服器的網域名稱。當您在外部使用自己的 HTTP Web 伺服器時 AWS，您必須使用由信任的第三方憑證授權機構 (CA) 簽署的憑證，例如 Comodo、DigiCert 或 Symantec。如需在 CloudFront 和您自己的

Web 伺服器之間需要 HTTPS 通訊的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[在 CloudFront 和您的自訂原始伺服器之間需要 HTTPS 通訊](#)的主題。

在檢視器和 CloudFront 之間需要 HTTPS

若要在檢視器和 CloudFront 之間要求 HTTPS，您可以變更 CloudFront 分佈中一或多個快取行為的檢視器通訊協定政策。如需在檢視器和 CloudFront 之間使用 HTTPS 的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的在[檢視器和 CloudFront 之間通訊需要 HTTPS](#)的主題。Amazon CloudFront 您也可以攜帶自己的 SSL 憑證，讓檢視器可以透過 HTTPS 使用您自己的網域名稱連線至 CloudFront 分佈，例如 <https://www.mysite.com>。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[設定替代網域名稱和 HTTPS](#) 主題。

選擇 CloudFront 回應的 HTTP 方法

當您建立 Amazon CloudFront Web 分佈時，您可以選擇您希望 CloudFront 處理並轉送至原始伺服器的 HTTP 方法。您可以從下列選項來選擇：

- GET、HEAD – 您只能使用 CloudFront 從您的原始伺服器取得物件或取得物件標頭。
- GET、HEAD、OPONS – 您只能使用 CloudFront 從您的原始伺服器取得物件、取得物件標頭，或擷取原始伺服器支援的選項清單。
- GET、HEAD、OPONS、PUT、POST、PATCH、DELETE – 您可以使用 CloudFront 來取得、新增、更新和刪除物件，以及取得物件標頭。此外，您可以執行其他 POST 操作，例如從 Web 表單提交資料。

您也可以使用 AWS WAF Classic 字串比對條件，根據 HTTP 方法允許或封鎖請求，如中所述[使用字串比對條件](#)。如果您想要使用 CloudFront 支援的方法組合，例如 GET 和 HEAD，則不需要設定 AWS WAF Classic 來封鎖使用其他方法的請求。如果您想要允許 CloudFront 不支援的方法組合，例如 GET、HEAD 和 POST，您可以設定 CloudFront 回應所有方法，然後使用 AWS WAF Classic 封鎖使用其他方法的請求。

如需選擇 CloudFront 回應方法的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[您在建立或更新 Web 分佈時指定的主題值](#)中的[允許 HTTP 方法](#)。

AWS WAF Classic 中的安全性

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

 Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

的雲端安全 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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用於 AWS WAF Classic 的合規計劃，請參閱 [AWS 合規計劃範圍內的服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您了解如何在使用 AWS WAF Classic 時套用共同責任模型。下列主題說明如何設定 AWS WAF Classic 以符合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 AWS WAF Classic 資源。

主題

- [AWS WAF Classic 中的資料保護](#)
- [AWS WAF Classic 的身分和存取管理](#)
- [在 AWS WAF Classic 中記錄和監控](#)
- [AWS WAF Classic 的合規驗證](#)
- [AWS WAF Classic 中的彈性](#)
- [AWS WAF Classic 中的基礎設施安全性](#)

AWS WAF Classic 中的資料保護

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS [共同責任模型](#)適用於 AWS WAF Classic 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](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 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 透過命令列介面或 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 WAF Classic 或其他 AWS 服務主控台、API 或 AWS CLI 時。

AWS SDKs 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。

AWS WAF 傳統實體，例如 Web ACLs、規則和條件，都會靜態加密，但無法使用加密的特定區域除外，包括中國（北京）和中國（寧夏）。每個區域都會採用唯一的加密金鑰。

刪除 AWS WAF Classic 資源

您可以刪除您在 AWS WAF Classic 中建立的資源。請參閱以下各節中每種資源類型的指南。

- [刪除 Web ACL](#)
- [從 AWS WAF Classic 規則群組新增和刪除規則](#)
- [刪除規則](#)

AWS WAF Classic 的身分和存取管理

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

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驗證（登入）和授權（具有許可）來使用 AWS WAF Classic 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 WAF Classic 如何與 IAM 搭配使用](#)
- [AWS WAF Classic 的身分型政策範例](#)
- [對 AWS WAF Classic 身分和存取進行故障診斷](#)
- [使用 AWS WAF Classic 的服務連結角色](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 AWS WAF Classic 中執行的工作。

服務使用者 – 如果您使用 AWS WAF Classic 服務來執行您的任務，則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 AWS WAF Classic 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 AWS WAF Classic 中的功能，請參閱 [對 AWS WAF Classic 身分和存取進行故障診斷](#)。

服務管理員 – 如果您在公司負責 AWS WAF Classic 資源，您可能擁有 AWS WAF Classic 的完整存取權。您的任務是判斷您的服務使用者應存取哪些 AWS WAF Classic 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搭配 AWS WAF Classic 使用 IAM，請參閱 [AWS WAF Classic 如何與 IAM 搭配使用](#)。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 AWS WAF Classic 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 AWS WAF Classic 身分型政策範例，請參閱 [AWS WAF Classic 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 角色身分進行身分驗證（登入 AWS）。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 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 服務來使用與身分提供者的聯合來存取。

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，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，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 AWS 帳戶和群組，以用於所有和應用程式。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](#)是具有單一個人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到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源相關聯時，AWS 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](#)。委託人可以包含帳戶、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，可指定中組織或組織單位 (OU) 的最大許可 AWS Organizations。AWS Organizations 是用於分組和集中管理您企業擁有 AWS 帳戶之多個的服務。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 AWS 服務支援 RCPs 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 WAF Classic 如何與 IAM 搭配使用

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱[將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱[AWS WAF](#)。

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

您可以搭配 AWS WAF Classic 使用的 IAM 功能

IAM 功能	AWS WAF 傳統支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是

IAM 功能	AWS WAF 傳統支援
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC(政策中的標籤)	部分
暫時性憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要深入了解 AWS WAF Classic 和其他 AWS 服務如何搭配大多數 IAM 功能使用，請參閱 [《AWS IAM 使用者指南》中的搭配 IAM 使用的服務](#)。

AWS WAF Classic 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](#)。

若要檢視 AWS WAF Classic 身分型政策的範例，請參閱 [AWS WAF Classic 的身分型政策範例](#)。

AWS WAF Classic 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。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（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](#)。

AWS WAF Classic 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 AWS WAF 傳統動作清單，請參閱服務授權參考中的[由定義的動作 AWS WAF](#)和[由 AWS WAF 區域定義的動作](#)。

AWS WAF Classic 中的政策動作在動作之前使用下列字首：

```
waf
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "waf:action1",  
    "waf:action2"  
]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要在以開頭的 AWS WAF Classic 中指定所有動作List，請包含下列動作：


```
"Action": "waf:List"
```

若要檢視 AWS WAF Classic 身分型政策的範例，請參閱 [AWS WAF Classic 的身分型政策範例](#)。

AWS WAF Classic 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 AWS WAF Classic 資源類型及其 ARNs 的清單，請參閱服務授權參考中的 [區域定義的資源](#) [AWS WAF](#) 和 [AWS WAF 區域定義的資源](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [定義的動作 AWS WAF](#) 和 [AWS WAF 區域定義的動作](#)。若要允許或拒絕存取 Classic AWS WAF 資源的子集，請在政策的 resource 元素中包含資源的 ARN。

在 AWS WAF Classic 中，資源是 Web ACLs 和規則。AWS WAF Classic 也支援位元組比對、IP 比對和大小限制等條件。

這些資源和條件都有獨一無二的 Amazon Resource Name (ARN) 與其相關聯，如下表所示。

AWS WAF 主控台的名稱	AWS WAF SDK/CLI 中的名稱	ARN 格式	
Web ACL	WebACL	arn:aws:waf:: <i>account:webacl</i> / <i>ID</i>	
規則	Rule	arn:aws:waf:: <i>account:rule</i> / <i>ID</i>	
字串比對條件	ByteMatch Set	arn:aws:waf:: <i>account:bytematch set</i> / <i>ID</i>	

AWS WAF 主控台的名稱	AWS WAF SDK/CLI 中的名稱	ARN 格式	
SQL injection 符合條件	SqlInjectionMatchSet	arn:aws:waf:: <i>account:sqlinjectionset /ID</i>	
容量限制條件	SizeConstraintSet	arn:aws:waf:: <i>account:sizeconstraintset /ID</i>	
IP 符合條件	IPSet	arn:aws:waf:: <i>account:ipset /ID</i>	
跨網站指令碼比對條件	XssMatchSet	arn:aws:waf:: <i>account:xssmatchset /ID</i>	

若要允許或拒絕存取 Classic AWS WAF 資源的子集，請在政策的 `resource` 元素中包含資源的 ARN。AWS WAF Classic ARNs 格式如下：

```
arn:aws:waf::account:resource /ID
```

將 *##*、*##* 和 *ID* 變數取代為有效值。有效值如下：

- *##*：您的 ID AWS 帳戶。您必須指定一個數值。
- *##*：AWS WAF Classic 資源的類型。
- *ID*：AWS WAF Classic 資源的 ID 或萬用字元 (*)，以指出與指定相關聯的指定類型的所有資源 AWS 帳戶。

例如，以下 ARN 為帳戶 111122223333 指定所有的 Web ACL：

```
arn:aws:waf::111122223333:webacl/*
```

AWS WAF Classic 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 AWS WAF Classic 條件索引鍵的清單，請參閱服務授權參考中的[AWS WAF 區域定義的和資源的條件索引鍵 AWS WAF](#)。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 WAF](#)和[AWS WAF 區域定義的動作](#)。

若要檢視 AWS WAF Classic 身分型政策的範例，請參閱[AWS WAF Classic 的身分型政策範例](#)。

AWS WAF Classic 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。

具有 AWS WAF Classic 的 ABAC

支援 ABAC (政策中的標籤)：部分

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 AWS WAF Classic 使用臨時憑證

支援臨時憑證：是

當您使用臨時憑證登入時，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 AWS WAF Classic 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 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

AWS WAF Classic 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 AWS WAF Classic 功能。只有在 AWS WAF Classic 提供指引時，才能編輯服務角色。

AWS WAF Classic 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 AWS WAF Classic 服務連結角色的詳細資訊，請參閱[使用 AWS WAF Classic 的服務連結角色](#)。

AWS WAF Classic 的身分型政策範例

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱[將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱[AWS WAF](#)。

根據預設，使用者和角色沒有建立或修改 AWS WAF Classic 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 AWS WAF Classic 定義之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[適用於的動作、資源和條件索引鍵 AWS WAF](#)，以及適用於 [AWS WAF Regional 的動作、資源和條件索引鍵](#)。

主題

- [政策最佳實務](#)

- [使用 AWS WAF Classic 主控台](#)
- [允許使用者檢視他們自己的許可](#)

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 AWS WAF Classic 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 AWS 受管政策，將許可授予許多常見使用案例。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，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 AWS WAF Classic 主控台

若要存取 AWS WAF Classic 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 WAF Classic 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。

可以存取和使用 AWS 主控台的使用者也可以存取 AWS WAF Classic 主控台。不需要額外許可。

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上完成此動作的許可，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": "*"
    }
  ]
}
```

對 AWS WAF Classic 身分和存取進行故障診斷

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

使用下列資訊來協助您診斷和修正使用 AWS WAF Classic 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 AWS WAF Classic 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 WAF Classic 資源](#)

我無權在 AWS WAF Classic 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 waf:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
waf: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 waf:*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至 AWS WAF Classic。

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 WAF Classic 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 AWS WAF Classic 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 WAF Classic 是否支援這些功能，請參閱 [AWS WAF Classic 如何與 IAM 搭配使用](#)。
- 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 \(聯合身分\)](#)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 角色與資源型政策的差異](#)。

使用 AWS WAF Classic 的服務連結角色

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS WAF Classic 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 AWS WAF Classic 的唯一 IAM 角色類型。服務連結角色由 AWS WAF Classic 預先定義，並包含服務 AWS 代表您呼叫其他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 WAF Classic，因為您不必手動新增必要的許可。AWS WAF Classic 會定義其服務連結角色的許可，除非另有定義，否則只有 AWS WAF Classic 可以擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

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

如需關於支援服務連結角色的其他服務的資訊，請參閱 [可搭配 IAM 運作的 AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWS WAF Classic 的服務連結角色許可

AWS WAF Classic 使用以下服務連結角色：

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic 使用這些服務連結角色將日誌寫入 Amazon Data Firehose。只有在您啟用登入時，才會使用這些角色 AWS WAF。如需詳細資訊，請參閱 [記錄 Web ACL 流量資訊](#)。

AWSServiceRoleForWAFLogging AWSServiceRoleForWAFRegionalLogging 和服務連結角色信任下列 服務（分別）擔任該角色：

- waf.amazonaws.com
- waf-regional.amazonaws.com

角色的許可政策允許 AWS WAF Classic 對指定的資源完成下列動作：

- 動作：firehose:PutRecord在 Amazon Data Firehose 資料串流資源firehose:PutRecordBatch上，名稱開頭為「aws-waf-logs-」。例如：aws-waf-logs-us-east-2-analytics。

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](#)。

為 AWS WAF Classic 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 上啟用 AWS WAF Classic 記錄 AWS Management Console，或在 AWS WAF Classic CLI 或 AWS WAF Classic API 中提出PutLoggingConfiguration請求時，AWS WAF Classic 會為您建立服務連結角色。

您必須擁有 iam:CreateServiceLinkedRole 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 AWS WAF Classic 記錄時，AWS WAF Classic 會再次為您建立服務連結角色。

編輯 AWS WAF Classic 的服務連結角色

AWS WAF Classic 不允許您編輯

AWSServiceRoleForWAFLoggingAWSServiceRoleForWAFRegionalLogging和服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的[編輯服務連結角色](#)。

刪除 AWS WAF Classic 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

Note

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

刪除 `AWSServiceRoleForWAFLogging` 和所使用的 AWS WAF Classic 資源 `AWSServiceRoleForWAFRegionalLogging`

1. 在 AWS WAF Classic 主控台上，從每個 Web ACL 移除記錄。如需詳細資訊，請參閱[記錄 Web ACL 流量資訊](#)。
2. 使用 API 或 CLI，為每個 Web ACL 提交 `DeleteLoggingConfiguration` 請求啟用記錄功能。如需詳細資訊，請參閱[AWS WAF Classic API 參考](#)。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 來刪除

`AWSServiceRoleForWAFLogging`、`AWSServiceRoleForWAFRegionalLogging` 和服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

AWS WAF Classic 服務連結角色支援的區域

AWS WAF Classic 支援在下列中使用服務連結角色 AWS 區域。

區域名稱	區域身分	AWS WAF Classic 支援
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是

區域名稱	區域身分	AWS WAF Classic 支援
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (悉尼)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
Europe (Paris)	eu-west-3	是
南美洲 (聖保羅)	sa-east-1	是

在 AWS WAF Classic 中記錄和監控

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

監控是維護 AWS WAF Classic 和 AWS 解決方案可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。AWS 提供數種工具來監控您的 AWS WAF Classic 資源並回應潛在事件：

Amazon CloudWatch 警示

您可以使用 CloudWatch 警示觀察單一指標一段指定的時間。如果指標超過指定的閾值，CloudWatch 會傳送通知至 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。

AWS CloudTrail 日誌

CloudTrail 提供使用者、角色或 AWS WAF Classic 中的 AWS 服務所採取動作的記錄。使用 CloudTrail 收集的資訊，您可以判斷對 AWS WAF Classic 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。如需詳細資訊，請參閱 [使用 AWS CloudTrail 記錄 API 呼叫](#)。

AWS WAF Classic 的合規驗證

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。

如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

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](#)。

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的責任模型。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。

AWS WAF Classic 中的彈性

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎建置。AWS 區域提供多個實體分隔和隔離的可用區域，這些區域與低延遲、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](#)。

AWS WAF Classic 中的基礎設施安全性

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱 [將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱 [AWS WAF](#)。

作為受管服務，AWS WAF Classic 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 AWS WAF Classic。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，您可以使用[AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS WAF 傳統配額

Warning

AWS WAF 傳統支援將於 2025 年 9 月 30 日結束。

Note

這是 AWS WAF Classic 文件。只有在您在 2019 年 11 月 AWS WAF 之前建立 AWS WAF 規則和 Web ACLs 等資源，而且尚未將它們遷移到最新版本時，才應該使用此版本。若要遷移您的 Web ACLs，請參閱[將您的 AWS WAF Classic 資源遷移至 AWS WAF](#)。如需最新版本的 AWS WAF，請參閱[AWS WAF](#)。

AWS WAF Classic 受限於下列配額（先前稱為限制）。

AWS WAF Classic 在每個區域每個帳戶的實體數量上具有預設配額。您可以[請求增加](#)這些配額。

資源	每個區域每個帳戶的預設配額
Web ACL	50

資源	每個區域每個帳戶的預設配額
規則	100
Rate-based-rules	5
每個區域每個帳戶的條件數量	對於除 regex 比對和地理比對以外的所有條件，每個條件類型 100 個。例如，100 個大小限制條件和 100 個 IP 比對條件。如需 regex 和地理比對條件，請參閱下表。
每秒請求數	每個 Web ACL * 25,000 個

*此配額僅適用於 Application Load Balancer 上的 AWS WAF Classic。AWS WAF Classic on CloudFront 每秒請求數 (RPS) 配額與 CloudFront 提供的 RPS 配額支援相同，如 [CloudFront 開發人員指南](#) 所述。

Classic AWS WAF 實體上的下列配額無法變更。

資源	每個區域每個帳戶的配額
每個 web ACL 的規則群組	2 : 1 個客戶建立的規則群組和 1 個 AWS Marketplace 規則群組

資源	每個區域每個帳戶的配額
每個 Web ACL 的規則數	10
每個規則的條件數	10
每個 IP 比對條件的 IP 地址範圍 (採用 CIDR 表示法)	10,000 您一次最多可以更新 1,000 個地址。API 呼叫在單一請求中最多 UpdateIPSet 接受 1,000 個地址。
每個以速度為基礎的規則，受封鎖的 IP 地址	10,000
每 5 分鐘速率限制的最低以速率為基礎的規則	100
每個跨網站指令碼比對條件的篩選條件數	10
每個大小限制條件的篩選條件數	10
每個 SQL injection 比對條件的篩選條件數	10
每個字串比對條件的篩選條件數	10
在字串比對條件中，當您設定 AWS WAF Classic 來檢查 Web 請求中標頭是否有指定值時，HTTP 標頭名稱中的字元數	40
在字串比對條件中，您希望 AWS WAF Classic 搜尋的值中的字元數	50
Regex 比對條件	10
在 regex 比對條件下，您希望 AWS WAF Classic 搜尋的模式中的字元數	70
在 regex 符合條件的模式，每個模式設定的數量	10
在 regex 符合條件的模式，每個模式設定 regex 條件的數量	1

資源	每個區域每個帳戶的配額
模式集	5
地理比對條件	50
每個地理比對條件的位置	50

AWS WAF Classic 在每個區域每個帳戶的呼叫具有下列固定配額。這些配額適用於透過任何可用方式對服務進行的總呼叫，包括主控台、CLI AWS CloudFormation、REST API 和 SDKs。這些配額無法變更。

呼叫類型	每個區域每個帳戶的配額
AssociateWebACL 呼叫次數上限	每 2 秒 1 個請求
DisassociateWebACL 呼叫次數上限	每 2 秒 1 個請求
GetWebACLForResource 呼叫次數上限	每秒 1 個請求
ListResourcesForWebACL 呼叫次數上限	每秒 1 個請求
CreateWebACLMigrationStack 呼叫次數上限	每秒 1 個請求
GetChangeToken 呼叫次數上限	每秒 10 個請求
GetChangeTokenStatus 呼叫次數上限	每秒 1 個請求
任何個別 List 動作的呼叫數上限 (若未定義其他配額)	每秒 5 個請求
任何個別 Create、Put、Get 或 Update 動作的呼叫次數上限 (若未定義其他配額)	每秒 1 個請求

AWS Shield

防止分散式阻斷服務 (DDoS) 攻擊對您的面向網際網路的應用程式來說至關重要。當您在 上建置應用程式時 AWS，您可以使用 AWS 提供的保護，無需額外費用。此外，您可以使用 AWS Shield Advanced 受管威脅防護服務，透過額外的 DDoS 偵測、緩解和回應功能來改善您的安全狀態。

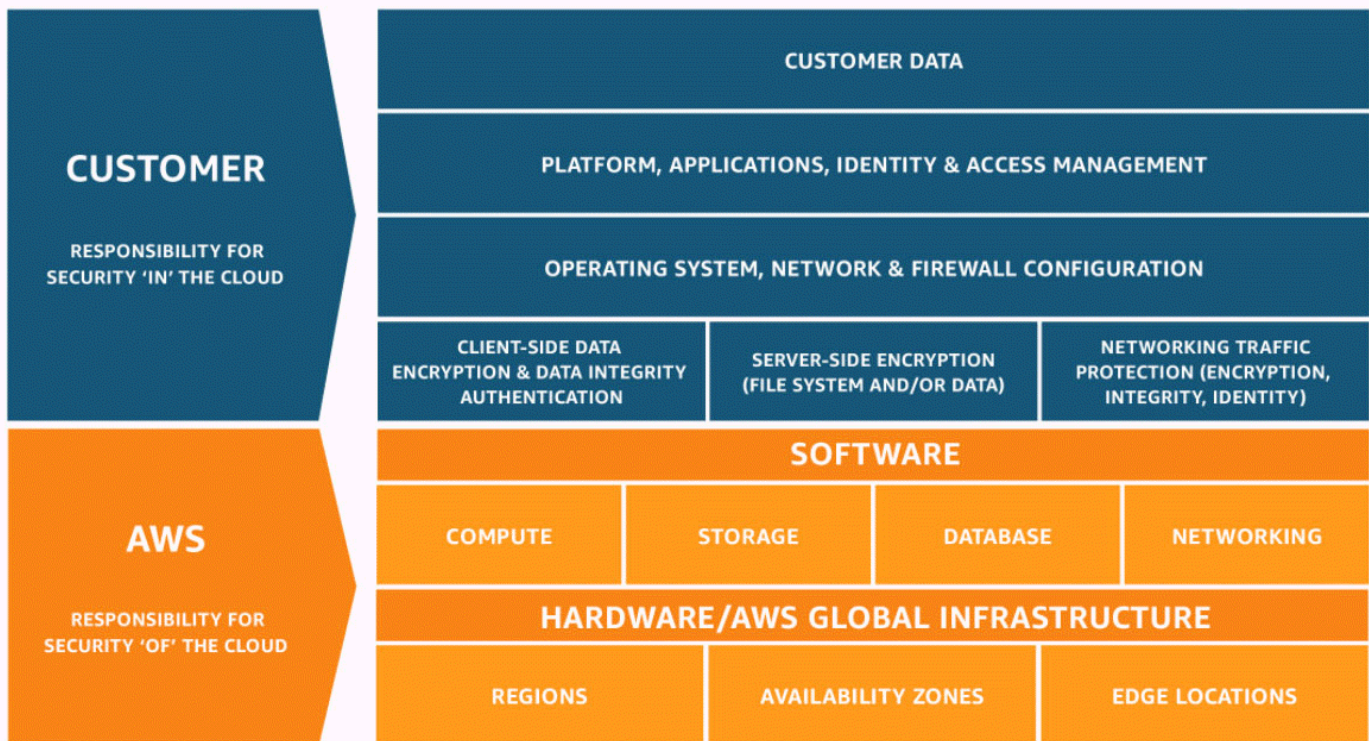
AWS 致力於為您提供工具、最佳實務和服務，以協助確保在防禦網際網路上的不良行為時具有高可用性、安全性和彈性。本指南旨在協助 IT 決策者和安全工程師了解如何使用 Shield 和 Shield Advanced 來更好地保護其應用程式免受 DDoS 攻擊和其他外部威脅。

當您在 上建置應用程式時 AWS，您會收到 自動保護 AWS，防範常見的容積 DDoS 攻擊向量，例如 UDP 反射攻擊和 TCP SYN 洪水。您可以利用這些保護，AWS 透過設計和設定 DDoS 彈性的架構，來確保您在 上執行的應用程式可用性。

本指南提供的建議可協助您設計、建立和設定應用程式架構，以實現 DDoS 彈性。遵守本指南所提供最佳實務的應用程式，當其被較大的 DDoS 攻擊和更廣泛的 DDoS 攻擊向量鎖定時，可以受益於可用性的改善持續性。此外，本指南說明如何使用 Shield Advanced 為您的關鍵應用程式實作最佳化的 DDoS 保護狀態。這些包括您已保證客戶在 DDoS 事件 AWS 期間需要 操作支援的應用程式。

安全性是 AWS 和 之間共同責任。[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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用於 Shield Advanced 的合規計劃，請參閱 [AWS 合規計劃範圍內的服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。



AWS Shield 和 Shield Advanced 如何運作

此頁面說明 AWS Shield Standard 和 之間的差異 AWS Shield Advanced。它還描述了 Shield 偵測到的攻擊類別。

AWS Shield Standard 和 為 AWS 網路和傳輸層（第 3 層和第 4 層）和應用程式層（第 7 層）上的資源 AWS Shield Advanced 提供防範分散式阻斷服務 (DDoS) 攻擊的保護。DDoS 攻擊是一種攻擊，其中多個遭入侵的系統嘗試讓目標充滿流量。DDoS 攻擊可防止合法最終使用者存取目標服務，並可能導致目標因流量過載而當機。

AWS Shield 提供針對各種已知 DDoS 攻擊向量和零日攻擊向量的保護。Shield 偵測和緩解旨在提供威脅的涵蓋範圍，即使服務在偵測時未明確知道。

Shield Standard 會在您使用時自動提供，且不收取額外費用 AWS。如需更高層級的攻擊防護，您可以訂閱 AWS Shield Advanced。

Shield 偵測到的攻擊類別包括下列項目：

- 網路容積攻擊（第 3 層）– 這是基礎設施層攻擊向量的子類別。這些向量會嘗試飽和目標網路或資源的容量，以拒絕向合法使用者提供服務。

- 網路通訊協定攻擊（第 4 層）– 這是基礎設施層攻擊向量的子類別。這些向量會濫用通訊協定來拒絕目標資源的服務。網路通訊協定攻擊的常見範例是 TCP SYN 洪水，這會耗盡伺服器、負載平衡器或防火牆等資源上的連線狀態。網路通訊協定攻擊也可以是容積。例如，較大的 TCP SYN 洪水可能打算使網路的容量飽和，同時耗盡目標資源或中繼資源的狀態。
- 應用程式層攻擊（第 7 層）– 此類型的攻擊向量會嘗試拒絕向合法使用者提供服務，方法是使用對目標有效的查詢來攻擊應用程式，例如 Web 請求洪水。

內容

- [AWS Shield Standard 概觀](#)
- [AWS Shield Advanced 概觀](#)
- [AWS Shield Advanced 保護 AWS 的資源清單](#)
- [AWS Shield Advanced 功能和選項](#)
- [決定是否訂閱 AWS Shield Advanced 並套用其他保護](#)
- [DDoS 攻擊的範例](#)
- [如何 AWS Shield 偵測事件](#)
 - [AWS Shield 基礎設施層威脅的偵測邏輯（第 3 層和第 4 層）](#)
 - [應用程式層威脅的 Shield Advanced 偵測邏輯（第 7 層）](#)
 - [適用於應用程式中多個資源的 Shield Advanced 偵測邏輯](#)
- [如何 AWS Shield 緩解事件](#)
 - [AWS Shield DDoS 緩解功能的清單](#)
 - [AWS Shield CloudFront 和 Route 53 的緩解邏輯](#)
 - [AWS Shield 區域的緩解邏輯 AWS](#)
 - [AWS Shield AWS Global Accelerator 標準加速器的緩解邏輯](#)
 - [AWS Shield Advanced 彈性 IPs 緩解邏輯](#)
 - [AWS Shield Advanced Web 應用程式的緩解邏輯](#)

AWS Shield Standard 概觀

AWS Shield 是一種受管威脅防護服務，可保護應用程式的周邊。周邊是來自 AWS 網路外部之應用程式流量的第一個進入點。

若要判斷您的應用程式周邊位於何處，請考慮使用者如何從網際網路存取您的應用程式。如果第一個進入點位於 AWS 區域，則應用程式周邊是您的 Amazon Virtual Private Cloud (VPC)。如果 Amazon

Route 53 將使用者導向您的應用程式，並先使用 Amazon CloudFront 或 存取應用程式 AWS Global Accelerator，則應用程式周邊會從 AWS 網路邊緣開始。

Shield 為執行 的所有應用程式提供 DDoS 偵測和緩解優勢 AWS，但您在設計應用程式架構時所做的決策會影響您的 DDoS 彈性水準。DDoS 彈性是應用程式在攻擊期間繼續在預期參數內操作的能力。

所有 AWS 客戶都能受益於 Shield Standard 的自動保護，無需額外費用。Shield Standard 可防禦以您的網站或應用程式為目標的最常見、經常發生的網路和傳輸層 DDoS 攻擊。雖然 Shield Standard 有助於保護所有 AWS 客戶，但您可以使用 Amazon Route 53 託管區域、Amazon CloudFront 分佈和 AWS Global Accelerator 標準加速器來獲得特定優勢。這些資源可針對所有已知的網路和傳輸層攻擊，提供全面的可用性保護。

AWS Shield Advanced 概觀

AWS Shield Advanced 是一項受管服務，可協助您保護應用程式免受外部威脅，例如 DDoS 攻擊、大量機器人和漏洞入侵嘗試。如需更高層級的攻擊防護，您可以訂閱 AWS Shield Advanced。

當您訂閱 Shield Advanced 並為您的資源新增保護時，Shield Advanced 會為這些資源提供擴展的 DDoS 攻擊保護。您從 Shield Advanced 收到的保護可能會因您的架構和組態選擇而有所不同。使用本指南中的資訊來建置和保護使用 Shield Advanced 的彈性應用程式，並在您需要專家協助時向上呈報。

Shield Advanced 訂閱和 AWS WAF 成本

Shield Advanced 訂閱涵蓋您使用 Shield Advanced 保護之資源的標準 AWS WAF 功能的成本。Shield Advanced 保護涵蓋的標準 AWS WAF 費用是每個保護套件或 Web ACL 的成本、每個規則的成本，以及 Web 請求檢查每百萬請求的基本價格、最多 1,500 WCUs，以及最多預設內文大小。

啟用 Shield Advanced 自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入您保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)、[使用 Shield Advanced 規則群組保護應用程式層及中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

您對 Shield Advanced 的訂閱不涵蓋對使用 Shield Advanced 時未保護之資源 AWS WAF 的使用。它也不會涵蓋受保護資源的任何其他非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括 Bot Control、CAPTCHA 規則動作、使用超過 1,500 個 WCUs ACLs，以及檢查超出預設內文大小的請求內文。AWS WAF 定價頁面上提供完整清單。您對 Shield Advanced 的訂閱包括對 Layer 7 Anti-DDoS Amazon Managed Rule 群組的存取。作為訂閱的一部分，您在一個日曆月內最多會收到 500 億個 Shield Advanced 受保護 AWS WAF 資源的請求。超過 500 億的請求將根據 AWS Shield Advanced 定價頁面計費。

如需完整資訊和定價範例，請參閱 [Shield 定價](#)和[AWS WAF 定價](#)。

Shield Advanced 訂閱帳單

如果您是 AWS 通路經銷商，請洽詢您的客戶團隊以取得資訊和指導。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他，適用下列訂閱和帳單準則：

- 對於屬於 AWS Organizations 組織成員的帳戶，會根據組織的付款人帳戶 AWS 計費 Shield Advanced 訂閱，無論付款人帳戶本身是否訂閱。
- 當您訂閱同一[AWS Organizations 合併帳單帳戶系列](#)中的多個帳戶時，一個訂閱價格會涵蓋系列中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶 及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費用，以為您提供所有這些帳戶。請聯絡您的客戶經理或 AWS 支援，並請求免除除其中一個組織以外的所有 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱 [AWS Shield 定價](#)。

AWS Shield Advanced 保護 AWS 的資源清單

Note

Shield Advanced 保護僅針對您在 Shield Advanced 中明確指定的資源，或是透過 Shield Advanced AWS Firewall Manager 政策保護的資源啟用。Shield Advanced 不會自動保護您的資源。

您可以使用 Shield Advanced 搭配下列資源類型進行進階監控和保護：

- Amazon CloudFront 分佈。對於 CloudFront 連續部署，Shield Advanced 會保護與受保護的主要分佈相關聯的任何預備分佈。
- Amazon Route 53 託管區域。
- AWS Global Accelerator 標準加速器。
- Amazon EC2 彈性 IP 地址。Shield Advanced 會保護與受保護彈性 IP 地址相關聯的資源。
- Amazon EC2 執行個體，透過與 Amazon EC2 彈性 IP 地址的關聯。

- 下列 Elastic Load Balancing (ELB) 負載平衡器：
 - Application Load Balancer。
 - Classic Load Balancer。
 - Network Load Balancer，透過與 Amazon EC2 彈性 IP 地址的關聯。

如需這些資源類型的保護的詳細資訊，請參閱 [AWS Shield Advanced 保護的資源清單](#)。

AWS Shield Advanced 功能和選項

AWS Shield Advanced 訂閱包含下列功能和選項。這些補充了您已使用的 DDoS 偵測和緩解功能 AWS。

- AWS WAF 整合 – Shield Advanced 使用 AWS WAF Web ACLs、規則和規則群組作為其應用程式層保護的一部分。如需的詳細資訊 AWS WAF，請參閱 [如何 AWS WAF 運作](#)。

Note

Shield Advanced 訂閱涵蓋您使用 Shield Advanced 保護之資源的標準 AWS WAF 功能的成本。Shield Advanced 保護涵蓋的標準 AWS WAF 費用是每個保護套件或 Web ACL 的成本、每個規則的成本，以及 Web 請求檢查每百萬請求的基本價格，最多可達 1,500 個 WCUs，最多可達預設內文大小。

啟用 Shield Advanced 自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)、[使用 Shield Advanced 規則群組保護應用程式層](#) 及 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

您對 Shield Advanced 的訂閱不涵蓋對使用 Shield Advanced 時未保護之資源 AWS WAF 的使用。它也不會涵蓋受保護資源的任何其他非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括 Bot Control、CAPTCHA 規則動作、使用超過 1,500 個 WCUs ACLs，以及檢查超出預設內文大小的請求內文。AWS WAF 定價頁面上提供完整清單。您對 Shield Advanced 的訂閱包括對 Layer 7 Anti-DDoS Amazon Managed Rule 群組的存取。作為訂閱的一部分，您會在一個日曆月收到最多 500 億個 Shield Advanced 受保護 AWS WAF 資源的請求。超過 500 億的請求將根據 AWS Shield Advanced 定價頁面計費。

如需完整資訊和定價範例，請參閱 [Shield 定價](#) 和 [AWS WAF 定價](#)。

- 自動應用程式層 DDoS 緩解 – 您可以設定 Shield Advanced 自動回應，以緩解針對受保護資源的應用程式層（第 7 層）攻擊。透過自動緩解，Shield Advanced 會對來自已知 DDoS 來源的請求強制

執行 AWS WAF 速率限制，並自動新增和管理自訂 AWS WAF 保護，以回應偵測到的 DDoS 攻擊。您可以設定自動緩解，以計算或封鎖屬於攻擊一部分的 Web 請求。

如需詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

- 以運作狀態為基礎的偵測 – 您可以使用 Amazon Route 53 運作狀態檢查搭配 Shield Advanced 來通知事件偵測和緩解。運作狀態檢查會根據您的規格監控您的應用程式，在符合規格時報告運作狀態良好，而在不符合規格時報告運作狀態不佳。搭配 Shield Advanced 使用運作狀態檢查有助於防止誤報，並在受保護的資源運作狀態不佳時提供更快的偵測和緩解。您可以針對 Route 53 託管區域以外的任何資源類型使用運作狀態型偵測。Shield Advanced 主動參與僅適用於已啟用運作狀態型偵測的資源。

如需詳細資訊，請參閱[透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。

- 保護群組 – 您可以使用保護群組來建立受保護資源的邏輯群組，以增強整體群組的偵測和緩解能力。您可以定義保護群組中的成員資格條件，以便自動包含新受保護的資源。受保護的資源可以屬於多個保護群組。

如需詳細資訊，請參閱[分組您的 AWS Shield Advanced 保護](#)。

- 增強對 DDoS 事件和攻擊的可見性 – Shield Advanced 可讓您存取進階的即時指標和報告，以全面了解受保護 AWS 資源的事件和攻擊。您可以透過 Shield Advanced API 和主控台，以及透過 Amazon CloudWatch 指標存取此資訊。

如需詳細資訊，請參閱[使用 Shield Advanced 的 DDoS 事件可見性](#)。

- 的 Shield Advanced 保護集中管理 AWS Firewall Manager – 您可以使用 Firewall Manager 自動將 Shield Advanced 保護套用至新帳戶和資源，並將規則部署 AWS WAF 到您的 Web ACLs。Shield Advanced 客戶可免費使用 Firewall Manager Shield Advanced 保護政策。您也可以使用 Firewall Manager 搭配 Amazon Simple Notification Service (SNS) 主題或 ，來集中您帳戶的 Shield Advanced 監控活動 AWS Security Hub。

如需使用 Firewall Manager 管理 Shield Advanced 保護的詳細資訊，請參閱 [AWS Firewall Manager](#)和 [在 Firewall Manager 中使用 AWS Shield Advanced 政策](#)。如需 Firewall Manager 定價的資訊，請參閱 [AWS Firewall Manager 定價](#)。

- AWS Shield Response Team (SRT) – SRT 在保護 AWS Amazon.com 及其附屬公司方面擁有豐富的經驗。身為 AWS Shield Advanced 客戶，您可以在 DDoS 攻擊期間隨時聯絡 SRT 尋求協助，這會影響應用程式的可用性。您也可以使用 SRT 來建立和管理資源的自訂緩解措施。若要使用 SRT 的服務，您還必須訂閱[商業支援計劃](#)或[企業支援計劃](#)。

如需詳細資訊，請參閱[使用 Shield Response Team \(SRT\) 支援的受管 DDoS 事件回應](#)。

- **主動參與** – 透過主動參與，如果與受保護資源相關聯的 Amazon Route 53 運作狀態檢查在 Shield Advanced 偵測到的事件期間變得運作狀態不佳，Shield 回應團隊 (SRT) 會直接與您聯絡。當您的應用程式可用性可能受到可疑攻擊的影響時，這可讓您更快地與專家互動。

如需詳細資訊，請參閱[設定 SRT 的主動參與，以直接與您聯絡](#)。

- **成本保護機會** – Shield Advanced 提供一些成本保護，以防止因對受保護資源的 DDoS 攻擊而導致的 AWS 帳單峰值。這可能包括 Shield Advanced 資料傳輸 (DTO) 使用費中峰值的涵蓋範圍。Shield Advanced 以 Shield Advanced 服務點數的形式提供任何成本保護。

如需詳細資訊，請參閱[在攻擊 AWS Shield Advanced 後請求 中的額度](#)。

決定是否訂閱 AWS Shield Advanced 並套用其他保護

檢閱本節中的案例，以協助決定要訂閱哪些帳戶 AWS Shield Advanced 以及在何處套用其他保護。使用 Shield Advanced，您需要為合併帳單帳戶下建立的所有帳戶支付每月訂閱費，以及根據傳輸之 GB 資料的使用費。如需 Shield Advanced 定價的詳細資訊，請參閱 [AWS Shield Advanced 定價](#)。

若要使用 Shield Advanced 保護應用程式及其資源，請將管理應用程式的帳戶訂閱至 Shield Advanced，然後將保護新增至應用程式的資源。如需訂閱帳戶和保護資源的資訊，請參閱 [設定 AWS Shield Advanced](#)。

Shield Advanced 訂閱和 AWS WAF 成本

Shield Advanced 訂閱涵蓋您使用 Shield Advanced 保護之資源使用標準 AWS WAF 功能的成本。Shield Advanced 保護涵蓋的標準 AWS WAF 費用是每個保護套件或 Web ACL 的成本、每個規則的成本，以及 Web 請求檢查每百萬請求的基本價格、最多 1,500 個 WCUs，以及最多預設內文大小。

啟用 Shield Advanced 自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入您保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)、[使用 Shield Advanced 規則群組保護應用程式層及中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

您對 Shield Advanced 的訂閱不涵蓋對使用 Shield Advanced 時未保護之資源 AWS WAF 的使用。它也不會涵蓋受保護資源的任何其他非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA 規則動作、使用超過 1,500 個 WCUs ACLs，以及檢查超出預設內文大小的請求內文。AWS WAF 定價頁面上提供完整清單。您對 Shield Advanced 的訂閱包括對 Layer 7 Anti-DDoS Amazon Managed Rule 群組的存取。作為訂閱的一部分，您在一個日曆月內最多會收到 500 億

個 Shield Advanced 受保護 AWS WAF 資源的請求。超過 500 億的請求將根據 AWS Shield Advanced 定價頁面計費。

如需完整資訊和定價範例，請參閱 [Shield 定價](#) 和 [AWS WAF 定價](#)。

Shield Advanced 訂閱帳單

如果您是 AWS 通路經銷商，請洽詢您的客戶團隊以取得資訊和指導。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他，適用下列訂閱和帳單準則：

- 對於屬於 AWS Organizations 組織成員的帳戶，會根據組織的付款人帳戶來 AWS 計費 Shield Advanced 訂閱，無論付款人帳戶本身是否訂閱。
- 當您訂閱同一 [AWS Organizations 合併帳單帳戶系列](#) 中的多個帳戶時，一個訂閱價格涵蓋該系列中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費用，以為您提供所有這些帳戶。請聯絡您的客戶經理或 AWS 支援，並請求免除除其中一個組織以外的所有 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱 [AWS Shield 定價](#)。

識別要保護的應用程式

考慮為需要下列任何一項的應用程式實作 Shield Advanced 保護：

- 應用程式使用者的保證可用性。
- 如果應用程式受到 DDoS 攻擊影響，可快速存取 DDoS 緩解專家。
- AWS 了解應用程式可能會受到 DDoS 攻擊的影響，以及來自 AWS 和 的攻擊通知，並呈報給您的安全或營運團隊。
- 雲端成本的可預測性，包括 DDoS 攻擊影響您使用 AWS 服務的情況。

如果應用程式或其資源需要上述任何項目，請考慮為相關帳戶建立訂閱。

識別要保護的資源

對於每個訂閱的帳戶，請考慮將 Shield Advanced 保護新增至具有下列任何特性的每個資源：

- 資源為網際網路上的外部使用者提供服務。
- 資源會公開至網際網路，也是關鍵應用程式的一部分。考慮每個公開的資源，無論您是否想要讓網際網路上的使用者存取它。
- 資源受到 AWS WAF Web ACL 的保護。

若要進一步了解如何建立和管理資源的保護，請參閱 [中的資源保護 AWS Shield Advanced](#)。

此外，請遵循本指南中的建議，以協助確保您建構應用程式的 DDoS 彈性，並已正確設定 Shield Advanced 的功能，以獲得最佳保護。

DDoS 攻擊的範例

AWS Shield Advanced 針對許多類型的攻擊提供擴充的保護。

下列清單說明一些常見的攻擊類型：

使用者資料包通訊協定 (UDP) 反射攻擊

在 UDP 反射攻擊中，攻擊者可以欺騙請求的來源，並使用 UDP 從伺服器引出大型回應。導向詐騙、攻擊 IP 地址的額外網路流量可能會減慢目標伺服器的速度，並防止合法最終使用者存取所需的資源。

TCP SYN 洪水

TCP SYN 洪水攻擊的目的是透過將連線保持半開放狀態，耗盡系統的可用資源。當使用者連線到像 Web 伺服器的 TCP 服務時，用戶端會傳送 TCP SYN 封包。伺服器會傳回確認，而用戶端會傳回自己的確認，完成三向交握。在 TCP SYN 洪水中，不會傳回第三個確認，且伺服器會保留等待回應。這可防止其他使用者連線到該伺服器上。

DNS 查詢泛洪

在 DNS 查詢洪水中，攻擊者會使用多個 DNS 查詢來耗盡 DNS 伺服器的資源。AWS Shield Advanced 可協助針對 Route 53 DNS 伺服器上的 DNS 查詢洪水攻擊提供保護。

HTTP 洪水/cache-busting (layer 7) 攻擊

使用 HTTP 洪水，包括 GET 和 POST 洪水，攻擊者會傳送多個似乎來自 Web 應用程式真實使用者的 HTTP 請求。Cache-busting 攻擊也是一種 HTTP 洪水的類型，使用 HTTP 請求的查詢字串的變體防止使用位置快取內容，和強制從原始 web 伺服器提供內容，導致其他及潛在損壞原始 web 伺服器的壓力。

如何 AWS Shield 偵測事件

AWS 會操作 AWS 網路和個別 AWS 服務的服務層級偵測系統，以確保它們在 DDoS 攻擊期間保持可用。此外，資源層級偵測系統會監控每個個別 AWS 資源，以確保流向資源的流量保持在預期的參數內。此組合會套用可捨棄已知錯誤封包的緩解措施、反白顯示潛在惡意流量，以及排定來自最終使用者的流量優先順序，藉此保護目標 AWS 資源 AWS 和服務。

偵測到的事件會顯示在您的 Shield Advanced 事件摘要、攻擊詳細資訊和 Amazon CloudWatch 指標中，做為 DDoS 攻擊向量的名稱，或 Volumetric 假設評估是以流量而非簽章為基礎。如需 DDoS Detected CloudWatch 指標中可用之攻擊向量維度的詳細資訊，請參閱 [AWS Shield Advanced 指標](#)。

主題

- [AWS Shield 基礎設施層威脅的偵測邏輯（第 3 層和第 4 層）](#)
- [應用程式層威脅的 Shield Advanced 偵測邏輯（第 7 層）](#)
- [適用於應用程式中多個資源的 Shield Advanced 偵測邏輯](#)

AWS Shield 基礎設施層威脅的偵測邏輯（第 3 層和第 4 層）

此頁面說明事件偵測如何適用於基礎設施（網路和傳輸）層。

用於保護目標 AWS 資源免受基礎設施層（第 3 層和第 4 層）中 DDoS 攻擊的偵測邏輯取決於資源類型以及資源是否受到保護 AWS Shield Advanced。

Amazon CloudFront 和 Amazon Route 53 的偵測

當您使用 CloudFront 和 Route 53 提供 Web 應用程式時，應用程式的所有封包都會由全內嵌 DDoS 緩解系統進行檢查，這不會造成任何可觀測的延遲。即時緩解針對 CloudFront 分佈和 Route 53 託管區域的 DDoS 攻擊。無論您是否使用，這些保護都適用 AWS Shield Advanced。

盡可能遵循使用 CloudFront 和 Route 53 作為 Web 應用程式進入點的最佳實務，以最快地偵測和緩解 DDoS 事件。

AWS Global Accelerator 和 區域服務的偵測

資源層級偵測可保護在 AWS 區域中啟動 AWS Global Accelerator 的標準加速器和資源，例如 Classic Load Balancer、Application Load Balancer 和彈性 IP 地址 EIPs)。這些資源類型會受到監控，查看流量是否升高，可能表示存在需要緩解的 DDoS 攻擊。每分鐘都會評估每個 AWS 資源的流量。如果對資源的流量增加，則會執行其他檢查來測量資源的容量。

Shield 會執行下列標準檢查：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、連接至 Amazon EC2 執行個體 EIPs – Shield 從受保護的資源擷取容量。容量取決於目標的執行個體類型、執行個體大小，以及其他因素，例如執行個體是否使用增強型聯網。
- Classic Load Balancer 和 Application Load Balancer – Shield 從目標負載平衡器節點擷取容量。
- 連接至 Network Load Balancer EIPs – Shield 從目標負載平衡器擷取容量。容量與目標負載平衡器的群組組態無關。
- AWS Global Accelerator 標準加速器 – Shield 會擷取以端點組態為基礎的容量。

這些評估跨多個維度的網路流量進行，例如連接埠和通訊協定。如果超過目標資源的容量，Shield 會放置 DDoS 緩解措施。Shield 放置的緩解措施將減少 DDoS 流量，但可能不會消除。如果流量維度上超過資源容量的一小部分，且與已知的 DDoS 攻擊向量一致，Shield 也可能會進行緩解。Shield 會將此緩解措施放在有限的存留時間 (TTL) 中，只要攻擊持續進行，它就會延伸。

Note

Shield 放置的緩解措施將減少 DDoS 流量，但可能無法消除。您可以使用 AWS Network Firewall 或之類的主機防火牆等解決方案來增強 Shield 保護，以防止應用程式處理對應用程式無效的流量，或由合法最終使用者產生的流量。

Shield Advanced 保護會將下列項目新增至現有的 Shield 偵測活動：

- 較低的偵測閾值 – Shield Advanced 會將緩解措施放在計算容量的一半。這可以為緩慢增加的攻擊提供更快的緩解措施，並緩解具有更模稜兩可容積簽章的攻擊。
- 間歇性攻擊保護 – Shield Advanced 會根據攻擊的頻率和持續時間，以指數增加存活時間 (TTL) 來放置緩解措施。當資源經常成為目標，以及當攻擊以短爆量發生時，這可讓緩解措施保持更久的時間。
- 以運作狀態為基礎的偵測 – 當您將 Route 53 運作狀態檢查與 Shield Advanced 受保護資源建立關聯時，運作狀態檢查的狀態會用於偵測邏輯。在偵測到的事件期間，如果運作狀態檢查良好，Shield Advanced 需要更大的可信度，即事件是攻擊，才能進行緩解。如果運作狀態檢查運作狀態不佳，Shield Advanced 可能會在建立可信度之前進行緩解。此功能有助於避免誤報，並針對影響您應用程式的攻擊提供更快速的反應。如需使用 Shield Advanced 進行運作狀態檢查的資訊，請參閱 [透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。

應用程式層威脅的 Shield Advanced 偵測邏輯 (第 7 層)

此頁面說明事件偵測如何用於應用程式層。

AWS Shield Advanced 為受保護的 Amazon CloudFront 分佈和 Application Load Balancer 提供 Web 應用程式層偵測。當您使用 Shield Advanced 保護這些資源類型時，您可以將 AWS WAF Web ACL 與您的保護建立關聯，以啟用 Web 應用程式層偵測。Shield Advanced 會使用相關聯 Web ACL 的請求資料，並為您的應用程式建置流量基準。Web 應用程式層偵測依賴 Shield Advanced 與之間的原生整合 AWS WAF。若要進一步了解應用程式層保護，包括將 AWS WAF Web ACL 與 Shield Advanced 受保護資源建立關聯，請參閱 [使用 AWS Shield Advanced 和 保護應用程式層 \(第 7 層\) AWS WAF](#)。

對於 Web 應用程式層偵測，Shield Advanced 會監控應用程式流量，並將其與尋找異常的歷史基準進行比較。此監控涵蓋總磁碟區和流量的組成。在 DDoS 攻擊期間，我們預期流量的磁碟區和組成都會變更，而 Shield Advanced 需要兩者的統計顯著偏差才能宣告事件。

Shield Advanced 會根據歷史時段執行其測量。此方法可減少來自流量的合法變更或來自符合預期模式之流量變更的誤報，例如每天在相同時間提供的銷售。

Note

給予 Shield Advanced 時間來建立代表正常、合法流量模式的基準，以避免 Shield Advanced 保護中的誤報。當您將 Web ACL 與受保護的資源建立關聯時，Shield Advanced 會開始收集其基準的資訊。在任何可能導致 Web 流量異常模式的計劃事件之前至少 24 小時，將 Web ACL 與您的受保護資源建立關聯。Shield Advanced Web 應用程式層偵測在觀察到 30 天的正常流量時最準確。

Shield Advanced 偵測事件所需的時間會受到其在流量中觀察到的變更量的影響。對於較低的磁碟區變更，Shield Advanced 會觀察較長期間的流量，以建立事件發生時的可信度。對於更高的磁碟區變更，Shield Advanced 會更快速地偵測和報告事件。

無論是由您新增或由 Shield Advanced 自動應用程式層緩解功能新增的以速率為基礎的規則，都可以在攻擊達到可偵測層級之前緩解攻擊。如需自動應用程式層 DDoS 緩解的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

Note

您可以建構您的應用程式來擴展，以回應流量增加或負載增加，以確保不受較小的請求洪水影響。使用 Shield Advanced，您的受保護資源會受到成本保護。這可協助您避免因 DDoS 攻擊

而可能發生的雲端帳單意外增加。若要進一步了解 Shield Advanced 成本保護，請參閱[在攻擊 AWS Shield Advanced 後請求 中的額度](#)。

適用於應用程式中多個資源的 Shield Advanced 偵測邏輯

此頁面說明事件偵測如何對應用程式中的多個資源運作。

您可以使用 AWS Shield Advanced 保護群組來建立屬於相同應用程式的受保護資源集合。您可以選擇要放置在群組中的哪些受保護資源，或指出應將相同類型的所有資源視為一個群組。例如，您可以建立所有 Application Load Balancer 的群組。當您建立保護群組時，Shield Advanced 偵測會彙總群組中受保護資源的所有流量。如果您有許多資源，而每個資源都具有少量流量，但具有大型彙總磁碟區，則此功能非常有用。對於在受保護資源之間傳輸流量的藍綠部署，您也可以使用保護群組來保留應用程式基準。

您可以選擇以下列其中一種方式彙總保護群組中的流量：

- 總和 – 此彙總會合併保護群組中跨資源的所有流量。您可以使用此彙總來確保新建立的資源具有現有的基準，並減少偵測敏感度，這有助於防止誤報。
- 平均值 – 此彙總會使用保護群組中所有流量的平均值。對於跨資源的流量統一的應用程式，例如負載平衡器，您可以使用此彙總。
- 最大值 – 此彙總會使用保護群組中任何資源的最高流量。當保護群組中有多個應用程式層時，您可以使用此彙總。例如，您可能有一個保護群組，其中包含 CloudFront 分佈、其 Application Load Balancer 原始伺服器，以及 Application Load Balancer 的 Amazon EC2 執行個體目標。

您也可以使用保護群組來改善 Shield Advanced 對多個面向網際網路IPs 或 AWS Global Accelerator 標準加速器進行攻擊時的緩解速度。當保護群組中的一個資源成為目標時，Shield Advanced 會為群組中的其他資源建立可信度。這會將 Shield Advanced 偵測置於提醒上，並可減少建立其他緩解措施所需的時間。

若要進一步了解保護群組，請參閱[分組您的 AWS Shield Advanced 保護](#)。

如何 AWS Shield 緩解事件

此頁面介紹 AWS Shield 事件緩解的運作方式。

保護應用程式的緩解邏輯可能會因應用程式架構而異。當您使用 Amazon CloudFront 和 Amazon Route 53 保護 Web 應用程式時，您會受益於 Web 和 DNS 使用案例特有的緩解措施，並保護服務的

所有流量。當您應用程式的進入點是在 AWS 區域中執行的資源時，緩解邏輯會根據服務、資源類型和您的使用而有所不同 AWS Shield Advanced。

AWS DDoS 緩解系統由 Shield 工程師開發，並與 AWS 服務緊密整合。工程師會考慮架構的各個層面，例如目標資源的容量和運作狀態。Shield 工程師會持續監控 DDoS 緩解系統的效能和效能，並在發現或預期新的威脅時能夠快速回應。

您可以建構您的應用程式來擴展，以因應流量或負載增加，以協助確保不受較小的請求洪水影響。如果您使用 Shield Advanced 來保護您的資源，您會收到因 DDoS 攻擊而可能發生的雲端帳單意外增加的涵蓋範圍。

基礎設施緩解措施

對於基礎設施層攻擊，AWS Shield DDoS 緩解系統存在於 AWS 網路邊界和 AWS 節點。在整個 AWS 基礎設施中放置多個層級的安全控制，為您的雲端應用程式提供 defense-in-depth。

Shield 會在從網際網路傳入的所有點維護 DDoS 緩解系統。當 Shield 偵測到 DDoS 攻擊時，它會針對每個傳入點，透過相同位置的 DDoS 緩解系統重新路由流量。這不會帶來任何可觀測的額外延遲，並提供跨所有 AWS 區域和所有節點每秒超過 100 TeraBits (Tbps) 的緩解容量。Shield 保護您的資源可用性，而不會將流量重新路由到外部或遠端清理中心，這可能會增加延遲。

- 在 AWS 網路邊界，對於任何 AWS 服務或資源，DDoS 緩解系統可緩解來自網際網路的基礎設施層攻擊。當 Shield 偵測或 Shield 回應團隊 (SRT) 上的工程師發出訊號時，系統會執行其緩解措施。
- 在 AWS 節點，DDoS 緩解系統會持續檢查轉送至 Amazon CloudFront 分佈和 Amazon Route 53 託管區域的每個封包，無論其來源為何。如有需要，系統會套用專為 Web 和 DNS 流量設計的緩解措施。使用 Amazon CloudFront 和 Amazon Route 53 保護您的 Web 應用程式的額外好處是，DDoS 攻擊會立即緩解，而不需要來自 Shield 偵測的訊號。

應用程式層緩解措施

Shield Advanced 為已啟用 Shield Advanced 保護的 Amazon CloudFront 分佈和 Application Load Balancer 提供 Web 應用程式層緩解措施。當您啟用保護時，您可以將 AWS WAF Web ACL 與資源建立關聯，以啟用 Web 應用程式層偵測。此外，您可以選擇啟用自動應用程式層緩解，指示 Shield Advanced 在 DDoS 攻擊期間為您管理保護。

Shield 僅針對您已啟用 Shield Advanced 和自動應用程式層緩解的資源，提供應用程式層攻擊的自訂緩解措施。透過自動緩解，Shield Advanced 會對來自已知 DDoS 來源的請求強制執行 AWS WAF 速率限制，並自動新增和管理自訂 AWS WAF 保護，以回應偵測到的 DDoS 攻擊。如需此類型之緩解措施的詳細資訊，請參閱 [Shield Advanced 如何管理自動緩解](#)。

無論是由您新增或由 Shield Advanced 自動應用程式層緩解功能新增的以速率為基礎的規則，都可以在攻擊達到可偵測層級之前緩解攻擊。如需偵測的詳細資訊，請參閱 [應用程式層威脅的 Shield Advanced 偵測邏輯 \(第 7 層\)](#)。

主題

- [AWS Shield DDoS 緩解功能的清單](#)
- [AWS Shield CloudFront 和 Route 53 的緩解邏輯](#)
- [AWS Shield 區域的緩解邏輯 AWS](#)
- [AWS Shield AWS Global Accelerator 標準加速器的緩解邏輯](#)
- [AWS Shield Advanced 彈性 IPs 緩解邏輯](#)
- [AWS Shield Advanced Web 應用程式的緩解邏輯](#)

AWS Shield DDoS 緩解功能的清單

AWS Shield DDoS 緩解的主要功能如下：

- 封包驗證 – 這可確保每個檢查的封包符合預期的結構，且對其通訊協定有效。支援的通訊協定驗證包括 IP、TCP（包括標頭和選項）、UDP、ICMP、DNS 和 NTP。
- 存取控制清單 (ACLs) 和形狀器 – ACL 會根據特定屬性評估流量，並捨棄相符的流量或將其映射至形狀器。形狀器會限制相符流量的封包速率，捨棄多餘的封包，以包含到達目的地的磁碟區。AWS Shield 偵測和 Shield Response Team (SRT) 工程師可以為預期流量提供專用速率分配，以及為具有符合已知 DDoS 攻擊向量屬性的流量提供更嚴格的速率分配。ACL 可以相符的屬性包括封包承載中的連接埠、通訊協定、TCP 旗標、目的地地址、來源國家/地區和任意模式。
- 可疑評分 – 這會利用 Shield 對預期流量的了解，將分數套用至每個封包。更緊密遵守已知良好流量模式的封包，會獲得較低的懷疑分數。觀察已知的不良流量屬性可能會增加封包的可疑分數。需要對限制封包進行評分時，Shield 會先捨棄可疑分數較高的封包。這有助於 Shield 緩解已知和零時差 DDoS 攻擊，同時避免誤報。
- TCP SYN 代理 — 這透過傳送 TCP SYN Cookie 來挑戰新連線，然後允許它們傳遞到受保護的服務，從而提供對 TCP SYN 洪水的保護。Shield DDoS 緩解提供的 TCP SYN 代理是無狀態的，這允許它緩解最大的已知 TCP SYN 洪水攻擊，而不會達到狀態耗盡。這可透過與 AWS 服務整合來傳遞連線狀態，而不是在用戶端和受保護的服務之間維持連續代理來實現。TCP SYN 代理目前可在 Amazon CloudFront 和 Amazon Route 53 上使用。
- 速率分佈 – 這會根據流量的輸入模式，持續調整每個位置的形狀器值，以提供給受保護的資源。這可防止客戶流量的速率限制，而這些流量可能無法平均地進入 AWS 網路。

AWS Shield CloudFront 和 Route 53 的緩解邏輯

此頁面說明 Shield DDoS 緩解如何持續檢查 CloudFront 和 Route 53 的流量。這些服務從全球分佈的 AWS 節點網路運作，可讓您廣泛存取 Shield 的 DDoS 緩解容量，並從更接近最終使用者的基礎設施交付您的應用程式。

Important

AWS Shield Advanced 不支援 CloudFront 租用戶。

- CloudFront – Shield DDoS 緩解措施僅允許對 Web 應用程式有效的流量傳遞至服務。這可自動保護許多常見的 DDoS 向量，例如 UDP 反射攻擊。

CloudFront 會維護與應用程式原始伺服器的持續連線、透過與 Shield TCP SYN 代理功能的整合自動緩解 TCP SYN 洪水，並在邊緣終止 Transport Layer Security (TLS)。這些合併功能可確保您的應用程式原始伺服器只會收到格式正確的 Web 請求，並且可以防止較低層級的 DDoS 攻擊、連線洪水和 TLS 濫用。

CloudFront 使用 DNS 流量方向和任意傳送路由的組合。這些技術透過緩解靠近來源的攻擊、提供故障隔離，以及確保存取容量以緩解最大的已知攻擊，來改善應用程式的彈性。

- Route 53 – Shield 緩解措施只允許有效的 DNS 請求到達服務。Shield 使用可疑評分來緩解 DNS 查詢洪水，該評分會優先考慮已知的良好查詢，並取消優先處理包含可疑或已知 DDoS 攻擊屬性的查詢。

Route 53 使用隨機碎片為每個託管區域提供一組獨特的四個解析器 IP 地址，用於 IPv4 和 IPv6。每個 IP 地址對應至不同 Route 53 位置子集。每個位置子集都包含授權 DNS 伺服器，僅部分與任何其他子集中的基礎設施重疊。這可確保如果使用者查詢因任何原因失敗，則會在重試時成功提供。

Route 53 使用任意傳送路由，根據網路鄰近度將 DNS 查詢導向最近的節點。Anycast 也會將 DDoS 流量散播到許多節點，以防止攻擊聚焦於單一位置。

除了緩解速度之外，CloudFront 和 Route 53 還提供對 Shield 全球分佈容量的廣泛存取。若要利用這些功能，請使用這些服務做為動態或靜態 Web 應用程式的進入點。

若要進一步了解如何使用 CloudFront 和 Route 53 保護 Web 應用程式，請參閱[如何使用 Amazon CloudFront 和 Amazon Route 53 協助保護動態 Web 應用程式免受 DDoS 攻擊](#)。若要進一步了解 Route 53 上的故障隔離，請參閱[全域故障隔離中的案例研究](#)。

AWS Shield 區域的緩解邏輯 AWS

此頁面說明 Shield 事件緩解邏輯如何在 AWS 區域中運作。

在 AWS 區域中啟動的資源受到 Shield 資源層級偵測放置的 AWS Shield DDoS 緩解系統保護。區域資源包括彈性 IPs (EIPs)、Classic Load Balancer 和 Application Load Balancer。

在放置緩解措施之前，Shield 會識別目標資源及其容量。Shield 使用容量來判斷其緩解應允許轉送至資源的最大總流量。緩解措施內的存取控制清單 (ACLs) 和其他形狀器可能會減少某些流量的允許磁碟區，例如符合已知 DDoS 攻擊向量或預期不會大量出現的流量。這進一步限制了緩解措施允許 UDP 反射攻擊或具有 TCP SYN 或 FIN 旗標的 TCP 流量的流量。

Shield 會針對每個資源類型，以不同的方式決定容量和位置緩解。

- 對於 Amazon EC2 執行個體或連接至 Amazon EC2 執行個體的 EIP，Shield 會根據執行個體類型和其他執行個體屬性計算容量，例如執行個體是否已啟用增強型聯網。
- 對於 Application Load Balancer 或 Classic Load Balancer，Shield 會個別計算負載平衡器每個目標節點的容量。這些資源的 DDoS 攻擊緩解措施是由 Shield DDoS 緩解措施和負載平衡器自動擴展的組合所提供。當 Shield Response Team (SRT) 參與針對 Application Load Balancer 或 Classic Load Balancer 資源的攻擊時，它們可能會加速擴展，作為額外的保護措施。
- Shield 會根據基礎 AWS 基礎設施的可用容量來計算某些 AWS 資源的容量。這些資源類型包括 Network Load Balancer (NLBs)，以及透過 Gateway Load Balancer 或路由流量的資源 AWS Network Firewall。

Note

連接受到 Shield Advanced 保護 EIPs，以保護您的 Network Load Balancer。您可以使用 SRT，根據基礎應用程式的預期流量和容量來建置自訂緩解措施。

當 Shield 放置緩解時，Shield 在緩解邏輯中定義的初始速率限制會平均套用至每個 Shield DDoS 緩解系統。例如，如果 Shield 放置了每秒 100,000 個封包 (pps) 限制的緩解，則它最初會在每個位置允許 100,000 pps。然後，Shield 會持續彙總緩解指標，以判斷實際的流量比率，並使用比率來調整每個位置的速率限制。這可以防止誤報，並確保緩解措施不會過於寬鬆。

AWS Shield AWS Global Accelerator 標準加速器的緩解邏輯

此頁面說明 Shield 事件緩解邏輯如何適用於 AWS Global Accelerator 標準加速器。Shield 緩解功能僅允許有效流量到達 Global Accelerator 標準加速器的接聽程式端點。

標準加速器部署於全球，並提供您 IP 地址，可用來將流量路由到任何 AWS 區域中 AWS 的資源。Shield 針對 Global Accelerator 緩解措施強制執行的速率限制，是以標準加速器路由流量的資源容量為基礎。Shield 會在總流量超過確定速率時，以及當已知 DDoS 向量超過該速率的一小部分時，放置緩解措施。

當您設定標準加速器時，您可以為要路由應用程式流量的每個 AWS 區域定義端點群組。當 Shield 放置緩解措施時，它會計算每個端點群組的容量，並相應地更新每個 Shield DDoS 緩解系統的速率限制。根據 Shield 對流量如何從網際網路路由到 AWS 資源所做的假設，每個位置的速率會有所不同。端點群組的容量計算方式為群組中的資源數量乘以群組中任何資源的最低容量。Shield 會定期重新計算應用程式的容量，並視需要更新速率限制。

Note

使用流量微調器來變更導向端點群組的流量百分比，不會變更 Shield 計算速率限制的方式，或將速率限制分散至其 DDoS 緩解系統。如果您使用流量撥號，請將端點群組設定為在資源類型和數量上互相鏡射。這有助於確保 Shield 計算的容量可代表為您的應用程式提供流量的資源。

如需 Global Accelerator 中端點群組和流量撥號的詳細資訊，請參閱[AWS Global Accelerator 標準加速器中的端點群組](#)。

AWS Shield Advanced 彈性 IPs 緩解邏輯

此頁面說明 Shield 事件緩解邏輯如何搭配彈性 IPs 運作 AWS Shield Advanced。當您使用保護彈性 IP (EIP) 時 AWS Shield Advanced，Shield Advanced 會增強 Shield 在 DDoS 事件期間放置的緩解措施。

Shield Advanced DDoS 緩解系統會複寫與 EIP 相關聯的公有子網路的網路 ACL (NACL) 組態。例如，如果您的 NACL 設定為封鎖所有 UDP 流量，Shield Advanced 會將該規則合併到 Shield 放置的緩解措施中。

此額外功能可協助您避免因流量對您的應用程式無效而導致的可用性風險。您也可以使用 NACLs 來封鎖個別來源 IP 地址或來源 IP 地址 CIDR 範圍。這對於未分佈的 DDoS 攻擊而言，可能是有用的緩解工具。它也可讓您輕鬆管理自己的允許清單，或封鎖不應與應用程式通訊的 IP 地址，而無需依賴 AWS 工程師的介入。

AWS Shield Advanced Web 應用程式的緩解邏輯

AWS Shield Advanced 使用 AWS WAF 來緩解 Web 應用程式層攻擊。AWS WAF 包含在 Shield Advanced 中，無需額外費用。

標準應用程式層保護

當您保護 Amazon CloudFront 分佈或 Application Load Balancer 與 Shield Advanced 時，如果您尚未關聯，可以使用 Shield Advanced 將 AWS WAF Web ACL 與受保護的資源建立關聯。如果您尚未設定 Web ACL，您可以使用 Shield Advanced 主控台精靈來建立一個，並新增以速率為基礎的規則。以速率為基礎的規則會限制每個 IP 地址每五分鐘的請求時段數量，提供基本的 Web 應用程式層請求洪水防護。您可以設定速率，從低至 10。如需詳細資訊，請參閱[使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層](#)。

您也可以使用 AWS WAF 服務來管理 Web ACL。透過 AWS WAF，您可以展開 Web ACL 組態來執行一些操作，例如檢查特定 Web 請求元件是否有字串比對或模式、新增自訂請求和回應處理，以及比對請求來源的地理位置。如需 AWS WAF 規則的詳細資訊，請參閱[AWS WAF 規則](#)。

自動應用程式層緩解

若要增強保護，請啟用 Shield Advanced 自動應用程式層緩解。使用此選項，Shield Advanced 會針對來自已知 DDoS 來源的請求維護 AWS WAF 速率限制規則，並為偵測到的 DDoS 攻擊提供自訂緩解措施。

當 Shield Advanced 偵測到受保護資源的攻擊時，它會嘗試識別攻擊簽章，以隔離攻擊流量與應用程式的一般流量。Shield Advanced 會根據受攻擊資源的歷史流量模式，以及與相同 Web ACL 相關聯的任何其他資源，來評估已識別的攻擊簽章。

如果 Shield Advanced 判斷攻擊簽章只會隔離 DDoS 攻擊中涉及的流量，則會在關聯的 Web ACL 內在 AWS WAF 規則中實作簽章。您可以指示 Shield Advanced 放置的緩解措施只會計算其相符的流量，或封鎖流量，而且您可以隨時變更設定。當 Shield Advanced 判斷不再需要其緩解規則時，它會將其從 Web ACL 中移除。如需應用程式層事件緩解的詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

如需 Shield Advanced 應用程式層緩解措施的詳細資訊，請參閱[使用 AWS Shield Advanced 和 保護應用程式層（第 7 層）AWS WAF](#)。

使用 Shield Advanced 建置基本 DDoS 彈性架構

此頁面說明分散式阻斷服務 (DDoS) 彈性，並引進兩個範例架構。

DDoS 彈性是您的應用程式架構能夠承受 DDoS 攻擊，同時繼續為合法的最終使用者提供服務。在攻擊期間，具有高度彈性的應用程式可以保持可用，對效能指標的影響最小，例如錯誤或延遲。本節顯示一些常見的範例架構，並說明如何使用 AWS 和 Shield Advanced 提供的 DDoS 偵測和緩解功能來提高其 DDoS 恢復能力。

本節中的範例架構重點介紹為已部署應用程式提供最大 DDoS 彈性優勢 AWS 的服務。反白服務的優點包括：

- 存取全球分散式網路容量 – Amazon CloudFront、AWS Global Accelerator 和 Amazon Route 53 服務可讓您存取 AWS 全球邊緣網路中的網際網路和 DDoS 緩解容量。這有助於緩解較大的容積攻擊，這些攻擊可以大規模達到 TB。您可以在任何 AWS 區域中執行應用程式，並使用這些服務來保護可用性，並最佳化合法使用者的效能。
- 針對 Web 應用程式層 DDoS 攻擊向量的保護 – Web 應用程式層 DDoS 攻擊最好使用應用程式擴展和 Web 應用程式防火牆 (WAF) 的組合來緩解。Shield Advanced 使用來自的 Web 請求檢查日誌 AWS WAF，來偵測可自動或透過與 Shield 回應團隊 (SRT) 互動來緩解的 AWS 異常。自動緩解可透過部署 AWS WAF 的速率型規則，以及透過 Shield Advanced 自動應用程式層 DDoS 緩解。

除了檢閱這些範例之外，請檢閱並遵循 [AWS DDoS 復原的最佳實務中的適用最佳實務](#)。

主題

- [常見 Web 應用程式的範例 Shield Advanced DDoS 彈性架構](#)
- [TCP 和 UDP 應用程式的 Shield 進階 DDoS 彈性架構範例](#)

常見 Web 應用程式的範例 Shield Advanced DDoS 彈性架構

此頁面提供使用 AWS Web 應用程式最大化 DDoS 攻擊彈性的範例架構。

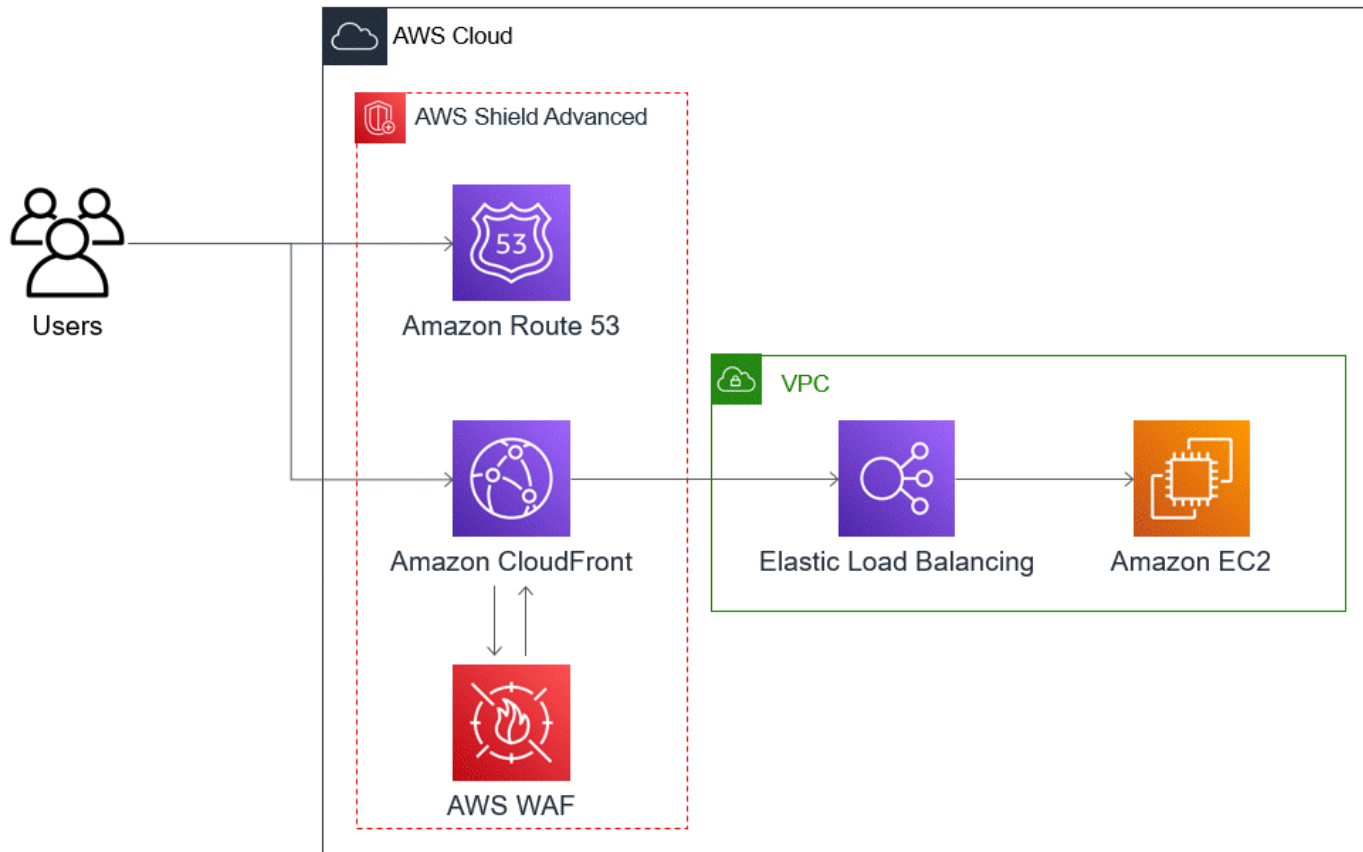
您可以在任何 AWS 區域中建置 Web 應用程式，並從區域中 AWS 提供的偵測和緩解功能接收自動 DDoS 保護。

此範例適用於使用 Classic Load Balancer、Application Load Balancer、Network Load Balancer、AWS Marketplace 解決方案或您自己的代理層等資源將使用者路由至 Web 應用程式的架構。您可以在這些 AWS WAF Web 應用程式資源與您的使用者之間插入 Amazon Route 53 託管區域、Amazon CloudFront 分佈和 Web ACLs，以改善 DDoS 彈性。這些插入會混淆應用程式原始伺服器、提供更接近最終使用者的請求，以及偵測和緩解應用程式層請求洪水。使用 CloudFront 和 Route 53 為使用者提供靜態或動態內容的應用程式，受到整合且全內嵌的 DDoS 緩解系統保護，可即時緩解基礎設施層攻擊。

有了這些架構改善，您就可以使用 Shield Advanced 來保護 Route 53 託管區域和 CloudFront 分佈。當您保護 CloudFront 分佈時，Shield Advanced 會提示您建立 AWS WAF Web ACLs 的關聯，並為它們建立以速率為基礎的規則，並提供啟用自動應用程式層 DDoS 緩解或主動參與的選項。主動參與和

自動應用程式層 DDoS 緩解會使用您與該資源相關聯的 Route 53 運作狀態檢查。若要進一步了解這些選項，請參閱[中的資源保護 AWS Shield Advanced](#)。

下列參考圖表說明 Web 應用程式的此 DDoS 彈性架構。



此方法為您的 Web 應用程式提供的優勢包括：

- 防範經常使用的基礎設施層（第 3 層和第 4 層）DDoS 攻擊，無需延遲偵測。此外，如果經常以資源為目標，Shield Advanced 會將緩解措施放置更長一段時間。Shield Advanced 也會使用從網路 ACLs(NACLs) 推斷的應用程式內容，進一步封鎖上游不需要的流量。這會隔離更接近其來源的故障，將對合法使用者的影響降至最低。
- 防範 TCP SYN 洪水。與 CloudFront、Route 53 整合的 DDoS 緩解系統，AWS Global Accelerator 並提供 TCP SYN 代理功能，可挑戰新的連線嘗試，且僅服務合法使用者。
- 防範 DNS 應用程式層攻擊，因為 Route 53 負責提供權威 DNS 回應。
- 防止 Web 應用程式層請求洪水。您在 AWS WAF Web ACL 中設定的以速率為基礎的規則，會在傳送的請求超過規則允許的數量時封鎖來源 IPs。

- 如果您選擇啟用此選項，則 CloudFront 分佈的自動應用程式層 DDoS 緩解措施。透過自動 DDoS 緩解，Shield Advanced 會在分佈的相關聯 AWS WAF Web ACL 中維護以速率為基礎的規則，以限制來自已知 DDoS 來源的請求量。此外，當 Shield Advanced 偵測到影響應用程式運作狀態的事件時，它會自動在 Web ACL 中建立、測試和管理緩解規則。
- 如果您選擇啟用此選項，則主動與 Shield Response Team (SRT) 互動。當 Shield Advanced 偵測到影響應用程式運作狀態的事件時，SRT 會使用您提供的聯絡資訊，回應並主動與您的安全或營運團隊互動。SRT 會分析流量中的模式，並可更新您的 AWS WAF 規則以封鎖攻擊。

TCP 和 UDP 應用程式的 Shield 進階 DDoS 彈性架構範例

此範例顯示使用 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或彈性 IP (EIP) 地址的 AWS 區域中 TCP 和 UDP 應用程式的 DDoS 彈性架構。

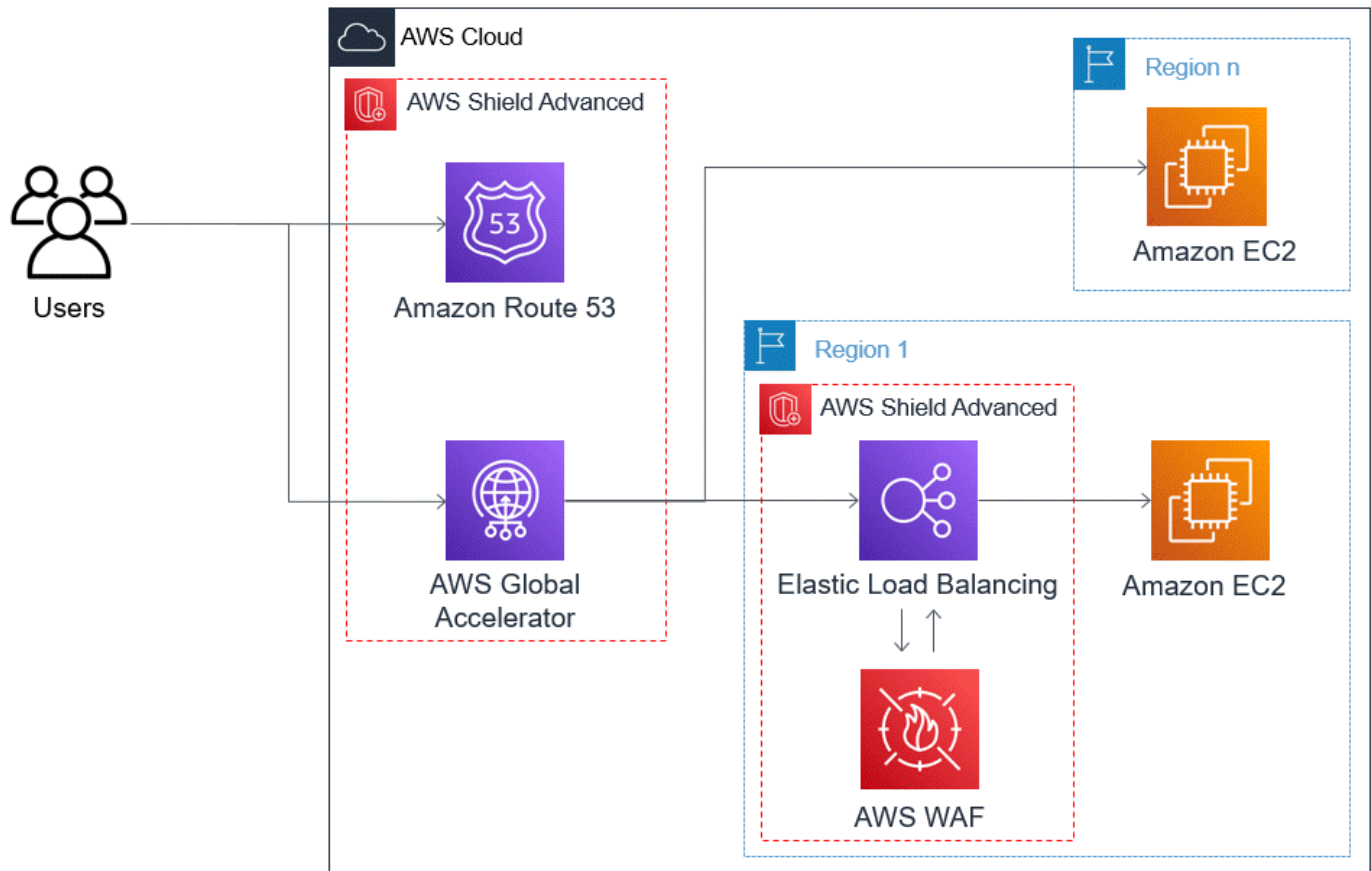
您可以遵循此一般範例來改善下列應用程式類型的 DDoS 彈性：

- TCP 或 UDP 應用程式。例如，用於遊戲、IoT 和 IP 語音的應用程式。
- 需要靜態 IP 地址或使用 Amazon CloudFront 不支援通訊協定的 Web 應用程式。例如，您的應用程式可能需要您的使用者可以新增到其防火牆允許清單的 IP 地址，而任何其他 AWS 客戶都不會使用。

您可以透過引入 Amazon Route 53 和 來改善這些應用程式類型的 DDoS 彈性 AWS Global Accelerator。這些服務可以將使用者路由到您的應用程式，並且可以為您的應用程式提供靜態 AWS IP 地址，這些 IP 地址會透過全球邊緣網路路由。Global Accelerator 標準加速器最多可將使用者延遲提高 60%。如果您有 Web 應用程式，您可以透過在 Application Load Balancer 上執行應用程式，然後使用 Web ACL 保護 Application Load Balancer，來偵測和緩解 AWS WAF Web 應用程式層請求洪水。

建置應用程式之後，請使用 Shield Advanced 來保護 Route 53 託管區域、Global Accelerator 標準加速器和任何 Application Load Balancer。當您保護 Application Load Balancer 時，您可以建立 AWS WAF Web ACLs 的關聯，並為其建立以速率為基礎的規則。您可以透過關聯新的或現有的 Route 53 運作狀態檢查，為 Global Accelerator 標準加速器和 Application Load Balancer 設定 SRT 主動參與。若要進一步了解選項，請參閱 [中的資源保護 AWS Shield Advanced](#)。

下列參考圖表說明 TCP 和 UDP 應用程式的範例 DDoS 彈性架構。



此方法為您的應用程式提供的優勢包括：

- 防範最大的已知基礎設施層（第 3 層和第 4 層）DDoS 攻擊。如果攻擊的量從上游造成擁塞 AWS，則故障會隔離到更接近其來源的位置，並將對合法使用者的影響降至最低。
- 防範 DNS 應用程式層攻擊，因為 Route 53 負責提供權威 DNS 回應。
- 如果您有 Web 應用程式，此方法可保護您免於 Web 應用程式層請求洪水。您在 AWS WAF Web ACL 中設定的速率型規則會在傳送的請求數量超過規則允許的數量時封鎖來源 IPs。
- 如果您選擇為合格資源啟用此選項，則主動與 Shield Response Team (SRT) 互動。當 Shield Advanced 偵測到影響應用程式運作狀態的事件時，SRT 會使用您提供的聯絡資訊，回應並主動與您的安全或營運團隊互動。

將 Shield Advanced 與其他 結合 AWS 服務

您可以使用 Shield Advanced 在許多類型的案例中保護您的資源。不過，在某些情況下，您應該使用其他 服務或將其他 服務與 Shield Advanced 結合，以提供最佳保護。以下是如何使用 Shield Advanced 或其他 AWS 服務協助保護 資源的範例。

目標	建議的服務	相關的服務文件
保護 web 應用程式和 RESTful API 對抗 DDoS 攻擊	Shield Advanced 保護 Amazon CloudFront 分佈和 Application Load Balancer	Elastic Load Balancing 文件 、 Amazon CloudFront 文件
保護 TCP 為基礎的應用程式對抗 DDoS 攻擊	Shield Advanced 保護 AWS Global Accelerator 標準加速器；連接至彈性 IP 地址	AWS Global Accelerator 文件 、 Elastic Load Balancing 文件
保護 UDP 為基礎的遊戲伺服器對抗 DDoS 攻擊	Shield Advanced 保護連接至彈性 IP 地址的 Amazon EC2 執行個體	Amazon Elastic Compute Cloud 文件

例如，如果您使用 Shield Advanced 來保護彈性 IP 地址，Shield Advanced 會保護與其相關聯的任何資源。在攻擊期間，Shield Advanced 會自動將您的網路 ACLs 部署到 AWS 網路邊界。當您的網路 ACLs 位於網路邊界時，Shield Advanced 可以提供對較大 DDoS 事件的保護。一般而言，網路 ACLs 會在 Amazon VPC 內的 Amazon EC2 執行個體附近套用。網路 ACL 只能減輕您的 Amazon VPC 和執行個體所能處理的攻擊。如果連接至 Amazon EC2 執行個體的網路介面最多可以處理 10 Gbps，則超過 10 Gbps 的磁碟區會減慢速度，並可能封鎖對該執行個體的流量。在攻擊期間，Shield Advanced 會將您的網路 ACL 提升為 AWS 邊界，以處理多個 TB 的流量。您的網路 ACL 能夠提供您的資源遠超過網路典型容量的保護。如需網路 ACL 的詳細資訊，請參閱 [網路 ACL](#)。

設定 AWS Shield Advanced

本教學課程會逐步引導您使用 Shield Advanced AWS Shield Advanced 主控台來開始使用。

Note

Shield Advanced 需要訂閱，但 AWS Shield Standard 不需要。Shield Standard 提供的保護為所有 AWS 客戶免費提供。

Shield Advanced 為網路層（第 3 層）、傳輸層（第 4 層）和應用程式層（第 7 層）攻擊提供進階 DDoS 偵測和緩解保護。如需 Shield Advanced 的詳細資訊，請參閱[AWS Shield Advanced 概觀](#)。

AWS 技術社群已發佈使用基礎設施做為程式碼 (IaC) 工具和 AWS CloudFormation Terraform 來設定 Shield Advanced 的自動化程序範例。如果您的帳戶是中組織的一部分，AWS Organizations 而且您要保護 Amazon Route 53 或以外的任何資源類型，則可以 AWS Firewall Manager 使用此解決方案 AWS Global Accelerator。若要探索此選項，請參閱 [aws-samples / aws-shield-advanced-one-click-deployment](#) 的程式碼儲存庫，以及 [Shield Advanced 一鍵式部署](#) 的教學課程。

Note

在分散式拒絕服務 (DDoS) 事件之前，請務必先完整設定 Shield Advanced。完成組態，以協助確保您的應用程式受到保護，而且如果您的應用程式受到 DDoS 攻擊的影響，您已準備好回應。

依序執行下列步驟以開始使用 Shield Advanced。

內容

- [訂閱 AWS Shield Advanced](#)
- [使用 Shield Advanced 新增和設定資源保護](#)
 - [使用 設定應用程式層（第 7 層）DDoS 保護 AWS WAF](#)
 - [使用 Shield Advanced 和 Route 53 為您的保護設定以運作狀態為基礎的偵測](#)
 - [使用 Shield Advanced 和 Amazon SNS 設定警示和通知](#)
 - [在 Shield Advanced 中檢閱並完成您的保護組態](#)
- [設定 DDoS AWS 事件回應的 Shield Response Team \(SRT\) 支援](#)
- [在 CloudWatch 中建立 DDoS 儀表板和設定 CloudWatch 警示](#)

訂閱 AWS Shield Advanced

此頁面說明如何訂閱 Shield Advanced，以開始使用 服務。

您必須為 AWS 帳戶 您要保護的每個訂閱 Shield Advanced。您不需要訂閱 Shield Standard。

Shield Advanced 訂閱計費

如果您是 AWS 通路經銷商，請洽詢您的客戶團隊以取得資訊和指導。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他，適用下列訂閱和帳單準則：

- 對於屬於 AWS Organizations 組織成員的帳戶，會根據組織的付款人帳戶來 AWS 計費 Shield Advanced 訂閱，無論付款人帳戶本身是否訂閱。
- 當您訂閱同一 [AWS Organizations 合併帳單帳戶系列](#) 中的多個帳戶時，一個訂閱價格會涵蓋系列中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶 及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費，以提供您擁有所有這些帳戶。請聯絡您的客戶經理或 AWS 支援，並請求免除除其中一個組織以外的所有 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱 [AWS Shield 定價](#)。

考慮使用 簡化訂閱 AWS Firewall Manager

如果您的帳戶是組織的一部分，我們建議您盡可能使用 AWS Firewall Manager 來自動化組織的訂閱和保護。Firewall Manager 支援 Amazon Route 53 和 以外的所有受保護資源類型 AWS Global Accelerator。若要使用 Firewall Manager，請參閱 [AWS Firewall Manager](#) 和 [設定 AWS Firewall Manager AWS Shield Advanced 政策](#)。

如果您不使用 Firewall Manager，請針對每個具有 資源的帳戶，使用下列程序來保護、訂閱和新增保護。

訂閱 帳戶 AWS Shield Advanced

- 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
- 在 AWS Shield 導覽列中，選擇開始使用。選擇訂閱 Shield Advanced。
- 在訂閱 Shield Advanced 頁面中，閱讀協議的每個條款，然後選取所有核取方塊，以表示您接受條款。對於合併帳單系列中的帳戶，您必須同意每個帳戶的條款。

Important

當您訂閱時，若要取消訂閱，您必須聯絡 [AWS 支援](#)。
若要停用訂閱的自動續約，您必須使用 Shield API 操作 [UpdateSubscription](#) 或 CLI 命令 [update-subscription](#)。

選擇訂閱 Shield Advanced。這會將您的帳戶訂閱 Shield Advanced 並啟用 服務。

您的帳戶已訂閱。繼續進行下列步驟，以使用 Shield Advanced 保護您帳戶的資源。

Note

Shield Advanced 不會在您訂閱後自動保護您的資源。您必須指定要 Shield Advanced 保護的資源。

使用 Shield Advanced 新增和設定資源保護

此頁面提供新增和設定 資源保護的說明。

Shield Advanced 僅保護您指定的資源，無論是透過 Shield Advanced 或在 Firewall Manager Shield Advanced 政策中。它不會自動保護已訂閱帳戶的資源。

Note

如果您使用 AWS Firewall Manager Shield Advanced 政策進行保護，則不需要執行此步驟。
您可以使用要保護的資源類型來設定政策，而 Firewall Manager 會自動為政策範圍內的資源新增保護。

如果您不使用 Firewall Manager，請針對每個具有要保護資源的帳戶執行下列程序。

使用 Shield Advanced 選擇要保護的資源

1. 從先前程序的訂閱確認頁面，或從受保護的資源或概觀頁面，選擇新增要保護的資源。
2. 在使用 Shield Advanced 選擇要保護的資源頁面中，在指定區域和資源類型中，為您要保護的資源提供區域和資源類型規格。您可以選取所有區域來保護多個區域中的資源，也可以選取全域，將

選取範圍縮小至全域資源。您可以取消選取您不想保護的任何資源類型。如需 資源類型保護的相關資訊，請參閱[AWS Shield Advanced 保護的資源清單](#)。

3. 選擇載入資源。Shield Advanced 會將符合您條件的資源填入選取資源區段 AWS。
4. 在選取資源區段中，您可以輸入要在資源清單中搜尋的字串來篩選資源清單。

選取您要保護的資源。

5. 在標籤區段中，如果您想要將標籤新增至您正在建立的 Shield Advanced 保護，請指定這些保護。如需標記 AWS 資源的相關資訊，請參閱[使用標籤編輯器](#)。
6. 選擇使用 Shield Advanced 保護。這會將 Shield Advanced 保護新增至 資源。

繼續執行主控台精靈畫面，以完成資源保護的組態。

主題

- [使用 設定應用程式層（第 7 層）DDoS 保護 AWS WAF](#)
- [使用 Shield Advanced 和 Route 53 為您的保護設定以運作狀態為基礎的偵測](#)
- [使用 Shield Advanced 和 Amazon SNS 設定警示和通知](#)
- [在 Shield Advanced 中檢閱並完成您的保護組態](#)

使用 設定應用程式層（第 7 層）DDoS 保護 AWS WAF

此頁面提供使用 AWS WAF Web ACLs 設定應用程式層保護的說明。

為了保護應用程式層資源，Shield Advanced 使用以速率為基礎的規則做為起點的 AWS WAF Web ACL。AWS WAF 是一種 Web 應用程式防火牆，可讓您監控轉送至應用程式層資源的 HTTP 和 HTTPS 請求，並可讓您根據請求的特性控制對內容的存取。速率型規則會根據您的請求彙總條件限制流量，為您的應用程式提供基本的 DDoS 保護。如需詳細資訊，請參閱[如何 AWS WAF 運作](#)及[在中使用以速率為基礎的規則陳述式 AWS WAF](#)。

您也可以選擇性地啟用 Shield Advanced 自動應用程式層 DDoS 緩解，讓來自已知 DDoS 來源的 Shield Advanced 速率限制請求，並自動為您提供事件特定的保護。

Important

如果您 AWS Firewall Manager 使用 Shield Advanced 政策來管理 Shield Advanced 保護，則無法在此處管理應用程式層保護。您必須在 Firewall Manager Shield Advanced 政策中管理它們。

Shield Advanced 訂閱和 AWS WAF 成本

Shield Advanced 訂閱涵蓋您使用 Shield Advanced 保護之資源的標準 AWS WAF 功能的成本。Shield Advanced 保護涵蓋的標準 AWS WAF 費用是每個保護套件或 Web ACL 的成本、每個規則的成本，以及 Web 請求檢查每百萬請求的基本價格、最多 1,500 WCUs，以及最多預設內文大小。

啟用 Shield Advanced 自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入您保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)、[使用 Shield Advanced 規則群組保護應用程式層及中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

您對 Shield Advanced 的訂閱不涵蓋對使用 Shield Advanced 時未保護之資源 AWS WAF 的使用。它也不會涵蓋受保護資源的任何其他非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括 Bot Control、CAPTCHA 規則動作、使用超過 1,500 個 WCUs ACLs，以及檢查超出預設內文大小的請求內文。AWS WAF 定價頁面上提供完整清單。您對 Shield Advanced 的訂閱包括對 Layer 7 Anti-DDoS Amazon Managed Rule 群組的存取。作為訂閱的一部分，您在一個日曆月內最多會收到 500 億個 Shield Advanced 受保護 AWS WAF 資源的請求。超過 500 億的請求將根據 AWS Shield Advanced 定價頁面計費。

如需完整資訊和定價範例，請參閱[Shield 定價](#)和[AWS WAF 定價](#)。

為區域設定第 7 層 DDoS 保護

Shield Advanced 可讓您選擇為所選資源所在的每個區域設定 layer 7 DDoS 緩解措施。如果您要在多個區域中新增保護，精靈會逐步引導您完成每個區域的下列程序。

1. 設定第 7 層 DDoS 保護頁面會列出尚未與 Web ACL 相關聯的每個資源。針對其中每一個，選擇現有的 Web ACL 或建立新的 Web ACL。對於已經有關聯 Web ACL 的任何資源，您可以先取消目前 ACL 的關聯，以變更 Web ACLs AWS WAF。如需詳細資訊，請參閱[將保護與 AWS 資源建立關聯或取消關聯](#)。

對於還沒有以速率為基礎的規則 ACLs，組態精靈會提示您新增規則。速率型規則會在傳送大量請求時限制來自 IP 地址的流量。速率型規則有助於保護您的應用程式免受 Web 請求洪水的影響，並且可以提供有關流量突然峰值的提醒，這可能表示潛在的 DDoS 攻擊。選擇新增速率限制規則，然後提供速率限制和規則動作，將速率型規則新增至 Web ACL。您可以在 Web ACL 中設定其他保護 AWS WAF。

如需有關在 Shield Advanced 保護中使用 Web ACLs 和速率型規則的資訊，包括速率型規則的其他組態選項，請參閱[使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層](#)。

2. 對於自動應用程式層 DDoS 緩解，如果您想要讓 Shield Advanced 自動緩解對應用程式層資源的 DDoS 攻擊，請選擇啟用，然後選取您希望 Shield Advanced 在其自訂 AWS WAF 規則中使用的規則動作。此設定適用於您在此精靈工作階段中管理之資源的所有 Web ACLs。

透過自動應用程式層 DDoS 緩解，Shield Advanced 會在資源的 AWS WAF Web ACL 中維護以速率為基礎的規則，以限制來自已知 DDoS 來源的請求量。此外，Shield Advanced 會將目前的流量模式與歷史流量基準進行比較，以偵測可能表示 DDoS 攻擊的偏差。當 Shield Advanced 偵測到 DDoS 攻擊時，它會透過建立、評估和部署自訂 AWS WAF 規則來回應。您可以指定自訂規則是否代表您計數或封鎖攻擊。

 Note

自動應用程式層 DDoS 緩解僅適用於使用最新版本 AWS WAF (v2) 建立的保護套件或 Web ACLs。

如需 Shield Advanced 自動應用程式層 DDoS 緩解措施的詳細資訊，包括使用此功能的注意事項和最佳實務，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

3. 選擇下一步。主控台精靈會進入以運作狀態為基礎的偵測頁面。

使用 Shield Advanced 和 Route 53 為您的保護設定以運作狀態為基礎的偵測

此頁面提供設定 Shield Advanced 以使用運作狀態型偵測的指示。這有助於改善攻擊偵測和緩解的回應能力和準確性。

設定良好的運作狀態檢查對於準確偵測事件至關重要。您可以為 Route 53 託管區域以外的任何資源類型設定運作狀態型偵測。

若要使用以運作狀態為基礎的偵測，請在 Route 53 中為您的資源定義運作狀態檢查，然後將運作狀態檢查與您的 Shield Advanced 保護建立關聯。您設定的運作狀態檢查必須準確反映資源的運作狀態。如需設定運作狀態檢查以搭配 Shield Advanced 使用的資訊和範例，請參閱 [透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。

Shield Response Team (SRT) 主動參與支援需要運作狀態檢查。如需主動參與的相關資訊，請參閱 [設定 SRT 的主動參與，以直接與您聯絡](#)。

 Note

當您將運作狀態檢查與 Shield Advanced 保護建立關聯時，必須報告運作狀態良好。

設定以運作狀態為基礎的偵測

1. 在 Associate Health Check (關聯運作狀態檢查) 下，選擇您要與保護產生關聯的運作狀態檢查 ID。

 Note

如果您沒有看到所需的運作狀態檢查，請前往 Route 53 主控台並驗證運作狀態檢查及其 ID。如需相關資訊，請參閱[建立和更新運作狀態檢查](#)。

2. 選擇 Next (下一步)。主控台精靈會進入警示和通知頁面。

使用 Shield Advanced 和 Amazon SNS 設定警示和通知

此頁面提供指示，可選擇性地設定 Amazon Simple Notification Service 通知，以偵測 Amazon CloudWatch 警示和以速率為基礎的規則活動。當 Shield 在受保護的資源上偵測到事件，或超過以速率為基礎的規則中設定的速率限制時，您可以使用這些來接收通知。

如需 Shield Advanced CloudWatch 指標的相關資訊，請參閱 [AWS Shield Advanced 指標](#)。如需 Amazon SNS 的相關資訊，請參閱 [Amazon Simple Notification Service 開發人員指南](#)。

設定警示和通知

1. 選取您要通知的 Amazon SNS 主題。您可以針對所有受保護的資源和速率型規則使用單一 Amazon SNS 主題，也可以選擇為您的組織自訂的不同主題。例如，您可以為負責特定資源集事件回應的每個團隊建立 SNS 主題。
2. 選擇 Next (下一步)。主控台精靈會進入資源保護檢閱頁面。

在 Shield Advanced 中檢閱並完成您的保護組態

若要檢閱並完成設定

1. 在檢閱和設定 DDoS 緩解和可見性頁面中，檢閱您的設定。若要進行修改，請在您要修改的區域中選擇編輯。這將帶您回到主控台精靈中的關聯頁面。進行變更，然後在後續頁面中選擇下一步，直到您返回檢閱並設定 DDoS 緩解和可見性頁面。
2. 選擇完成組態。受保護的資源頁面會列出新受保護的資源。

設定 DDoS AWS 事件回應的 Shield Response Team (SRT) 支援

此頁面提供設定 Shield Response Team (SRT) 支援的說明。

SRT 包含專精 DDoS 事件回應的安全工程師。您可以選擇性地新增許可，允許 SRT 在 DDoS 事件期間代表您管理資源。此外，如果您受保護資源的相關 Route 53 運作狀態檢查在偵測到的事件期間運作狀態不佳，您可以設定 SRT 主動與您互動。這兩種對您的保護的新增，都能更快速地回應 DDoS 事件。

Note

若要使用 Shield Response Team (SRT) 的服務，您必須訂閱 [Business Support 計劃](#)或 [Enterprise Support 計劃](#)。

SRT 可以在應用程式層事件期間監控 AWS WAF 請求資料和日誌，以識別異常流量。他們可以協助制定自訂 AWS WAF 規則，以緩解違規的流量來源。視需要，SRT 可能會提出架構建議，以協助您更好地調整資源與 AWS 建議。

如需 SRT 的詳細資訊，請參閱 [使用 Shield Response Team \(SRT\) 支援的受管 DDoS 事件回應](#)。

授予 SRT 許可

1. 在 AWS Shield 主控台概觀頁面的設定 AWS SRT 支援下，選擇編輯 SRT 存取。編輯 Shield 回應團隊 AWS (SRT) 存取頁面隨即開啟。
2. 針對 SRT 存取設定，選取其中一個選項：
 - 請勿授予 SRT 存取我的帳戶 – Shield 會移除您先前授予 SRT 存取您的帳戶和資源的任何許可。

- 為 SRT 建立新角色以存取我的帳戶 – Shield 會建立信任服務主體的角色 `drt.shield.amazonaws.com`，其代表 SRT，並將受管政策連接至 `AWSShieldDRTAccessPolicy` 該角色。受管政策允許 SRT 代表您進行 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 日誌。如需受管政策的更多相關資訊，請參閱 [AWS 受管政策：AWSShieldDRTAccessPolicy](#)。
- 選擇 SRT 的現有角色來存取我的帳戶 – 對於此選項，您必須在 AWS Identity and Access Management (IAM) 中修改角色組態，如下所示：
 - 將受管政策 `AWSShieldDRTAccessPolicy` 連接至角色。此受管政策允許 SRT 代表您進行 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 日誌。如需受管政策的更多相關資訊，請參閱 [AWS 受管政策：AWSShieldDRTAccessPolicy](#)。如需有關將受管政策連接至角色的資訊，請參閱 [連接和分離 IAM 政策](#)。
 - 修改角色以信任服務委託人 `drt.shield.amazonaws.com`。這是代表 SRT 的服務主體。如需詳細資訊，請參閱 [IAM JSON 政策元素：委託人](#)。

3. 選擇儲存，以儲存變更。

如需授予 SRT 存取您保護和資料的詳細資訊，請參閱 [授予 SRT 的存取權](#)。

啟用 SRT 主動參與

1. 在 AWS Shield 主控台概觀頁面的主動參與和聯絡下，於聯絡區域選擇編輯。

在編輯聯絡人頁面中，提供您希望 SRT 主動參與聯絡人的聯絡資訊。

如果您提供多個聯絡案例，請在備註中指出每個聯絡案例的使用情形。包含主要和次要聯絡人指定，並提供每個聯絡人的可用時間和時區。

聯絡備註範例：

- 這是 24x7x365 全年無休配置的熱線。請與回應分析師合作，他們會在通話中取得適當的人員。
- 如果熱線未在 5 分鐘內回應，請聯絡我。

2. 選擇 Save (儲存)。

概觀頁面反映更新的聯絡資訊。

3. 選擇編輯主動參與功能，選擇啟用，然後選擇儲存以啟用主動參與。

如需主動參與的詳細資訊，請參閱 [設定 SRT 的主動參與，以直接與您聯絡](#)。

在 CloudWatch 中建立 DDoS 儀表板和設定 CloudWatch 警示

此頁面提供在 CloudWatch 中建立 DDoS 儀表板和設定 CloudWatch 警示的指示。

您可以使用 Amazon CloudWatch 監控潛在的 DDoS 活動，該活動會從 Shield Advanced 收集原始資料，並將其處理為可讀且近乎即時的指標。您可以使用 CloudWatch 中的統計資料來深入了解 Web 應用程式或服務的運作方式。如需使用 CloudWatch 的詳細資訊，請參閱《Amazon [CloudWatch 使用者指南](#)》中的什麼是 CloudWatch。Amazon CloudWatch

- 如需建立 CloudWatch 儀表板的說明，請參閱 [使用 Amazon CloudWatch 監控](#)。
- 如需可新增至儀表板的 Shield Advanced 指標說明，請參閱[AWS Shield Advanced 指標](#)。

Shield Advanced 會在 DDoS 事件期間比沒有事件正在進行時更頻繁地向 CloudWatch 報告資源指標。Shield Advanced 會在事件期間每分鐘報告一次指標，然後在事件結束後立即報告一次指標。雖然沒有進行中的事件，但 Shield Advanced 每天在指派給資源的時間報告一次指標。此定期報告會保持指標作用中，並可用於自訂 CloudWatch 警示。

這完成了 Shield Advanced 入門的教學課程。若要充分利用您選擇的保護，請繼續探索 Shield Advanced 的功能和選項。若要開始，請熟悉您在 [使用 Shield Advanced 的 DDoS 事件可見性](#)和中檢視和回應事件的選項在 [中回應 DDoS 事件 AWS](#)。

使用 Shield Response Team (SRT) 支援的受管 DDoS 事件回應

此頁面說明 Shield Response Team (SRT) 的 函數。

SRT 為 Shield Advanced 客戶提供額外支援。SRT 是專精 DDoS 事件回應的安全工程師。作為您 AWS 支援 計劃的額外支援，您可以直接與 SRT 合作，利用他們的專業知識作為事件回應工作流程的一部分。如需 選項和組態指導的相關資訊，請參閱下列主題。

Note

若要使用 Shield Response Team (SRT) 的服務，您必須訂閱 [Business Support 計劃](#)或 [Enterprise Support 計劃](#)。

SRT 支援活動

與 SRT 互動的主要目標是保護應用程式的可用性和效能。根據 DDoS 事件的類型和應用程式的架構，SRT 可能會採取下列一或多個動作：

- **AWS WAF 日誌分析和規則** – 對於使用 AWS WAF Web ACL 的資源，SRT 可以分析您的 AWS WAF 日誌，以識別應用程式 Web 請求中的攻擊特性。在參與期間獲得您的核准後，SRT 可以將變更套用至您的 Web ACL，以封鎖他們已識別的攻擊。
- **建置自訂網路緩解措施** – SRT 可以為您撰寫基礎設施層攻擊的自訂緩解措施。SRT 可以與您一起了解應用程式預期的流量、封鎖非預期的流量，以及最佳化每秒封包速率限制。如需詳細資訊，請參閱 [使用 SRT 設定針對 DDoS 攻擊的自訂緩解措施](#)。
- **網路流量工程** – SRT 與 AWS 聯網團隊緊密合作，以保護 Shield Advanced 客戶。必要時，AWS 可以變更網際網路流量到達 AWS 網路的方式，以便為您的應用程式配置更多緩解容量。
- **架構建議** – SRT 可能會判斷攻擊的最佳緩解措施需要架構變更，才能更符合 AWS 最佳實務，且有助於支援您實作這些實務。如需詳細資訊，請參閱 [AWS DDoS 彈性的最佳實務](#)。

以下各節提供與 SRT 互動的說明

主題

- [授予 SRT 的存取權](#)
- [設定 SRT 的主動參與，以直接與您聯絡](#)
- [聯絡 SRT 以協助處理可疑的 DDoS 事件](#)
- [使用 SRT 設定針對 DDoS 攻擊的自訂緩解措施](#)

授予 SRT 的存取權

此頁面提供授予許可給 SRT 以代表您行事的說明，以便他們可以存取您的 AWS WAF 日誌並呼叫 AWS Shield Advanced 和 AWS WAF APIs 來管理保護。

在應用程式層 DDoS 事件期間，SRT 可以監控 AWS WAF 請求以識別異常流量，並協助制定自訂 AWS WAF 規則來緩解違規的流量來源。

此外，您可以授予 SRT 存取您在 Amazon S3 儲存貯體中存放的其他資料，例如 Application Load Balancer、Amazon CloudFront 或第三方來源的封包擷取或日誌。

Note

若要使用 Shield Response Team (SRT) 的服務，您必須訂閱 [Business Support 計劃](#) 或 [Enterprise Support 計劃](#)。

管理 SRT 的許可

1. 在 AWS Shield 主控台概觀頁面的設定 AWS SRT 支援下，選擇編輯 SRT 存取。編輯 Shield 回應團隊 AWS (SRT) 存取頁面隨即開啟。
2. 針對 SRT 存取設定，選取其中一個選項：
 - 請勿授予 SRT 存取我的帳戶 – Shield 會移除您先前授予 SRT 存取您的帳戶和資源的任何許可。
 - 為 SRT 建立新角色以存取我的帳戶 – Shield 會建立信任服務主體的角色 `drt.shield.amazonaws.com`，其代表 SRT，並將受管政策連接至 `AWSShieldDRTAccessPolicy` 該角色。受管政策允許 SRT 代表您進行 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 日誌。如需受管政策的更多相關資訊，請參閱 [AWS 受管政策：AWSShieldDRTAccessPolicy](#)。
 - 選擇 SRT 的現有角色來存取我的帳戶 – 對於此選項，您必須在 AWS Identity and Access Management (IAM) 中修改角色組態，如下所示：
 - 將受管政策 `AWSShieldDRTAccessPolicy` 連接至角色。此受管政策允許 SRT 代表您進行 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 日誌。如需受管政策的更多相關資訊，請參閱 [AWS 受管政策：AWSShieldDRTAccessPolicy](#)。如需有關將受管政策連接至角色的資訊，請參閱 [連接和分離 IAM 政策](#)。
 - 修改角色以信任服務委託人 `drt.shield.amazonaws.com`。這是代表 SRT 的服務主體。如需詳細資訊，請參閱 [IAM JSON 政策元素：委託人](#)。
3. 對於（選用）：授予 SRT 對 Amazon S3 儲存貯體的存取權，如果您需要共用不在 AWS WAF Web ACL 日誌中的資料，請設定此選項。例如，Application Load Balancer 存取日誌、Amazon CloudFront 日誌或第三方來源的日誌。

Note

您不需要為 AWS WAF Web ACL 日誌執行此操作。當您授予帳戶存取權時，SRT 即可存取這些項目。

- a. 根據下列準則設定 Amazon S3 儲存貯體：
 - 儲存貯體位置必須與您在上一個步驟 AWS Shield Response Team (SRT) 存取中授予 SRT 一般存取權的位置 AWS 帳戶 相同。

- 儲存貯體可以是純文字或 SSE-S3 加密。如需 Amazon S3 SSE-S3 加密的詳細資訊，請參閱《Amazon S3 使用者指南》中的[使用伺服器端加密搭配 Amazon S3-Managed 加密金鑰 \(SSE-S3\) 保護資料](#)。Amazon S3

SRT 無法檢視或處理存放在儲存貯體中的日誌，這些儲存貯體使用儲存在 AWS Key Management Service () 中的金鑰加密 AWS KMS。

- b. 在 Shield Advanced (選用)：授予 Amazon S3 儲存貯體的 SRT 存取權，針對儲存資料或日誌的每個 Amazon S3 儲存貯體，輸入儲存貯體的名稱，然後選擇新增儲存貯體。您最多可以新增 10 個儲存貯體。

這會授予 SRT 每個儲存貯體的下列許可：s3:GetObject、s3:GetBucketLocation 和 s3:ListBucket。

如果您想要授予 SRT 存取超過 10 個儲存貯體的許可，您可以編輯其他儲存貯體政策並手動授予此處列出的 SRT 許可。

以下顯示範例政策清單。

```
{
  "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
  "Effect": "Allow",
  "Principal": {
    "Service": "drt.shield.amazonaws.com"
  },
  "Action": [
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"
  ]
}
```

4. 選擇儲存，以儲存變更。

您也可以透過 API 授權 SRT，方法是建立 IAM 角色、將政策 AWSShieldDRTAccessPolicy 連接至該角色，然後將該角色傳遞至操作 [AssociateDRTRole](#)。

設定 SRT 的主動參與，以直接與您聯絡

此頁面提供設定 SRT 主動參與的說明。

透過主動參與，SRT 會在應用程式可用性或效能因可能的攻擊而受到影響時直接與您聯絡。我們建議使用此互動模型，因為它提供最快的 SRT 回應，並允許 SRT 即使在與您建立聯絡之前，也開始故障診斷。

主動參與適用於彈性 IP 地址和 AWS Global Accelerator 標準加速器上的網路層和傳輸層事件，以及 Amazon CloudFront 分佈和 Application Load Balancer 上的 Web 請求洪水。主動參與僅適用於具有相關聯 Amazon Route 53 運作狀態檢查的 Shield Advanced 資源保護。如需管理和使用運作狀態檢查的資訊，請參閱[透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。

在 Shield Advanced 偵測到的事件期間，SRT 會使用運作狀態檢查的狀態來判斷事件是否符合主動參與的資格。若是如此，SRT 會根據您在主動參與組態中提供的聯絡指引與您聯絡。

您最多可以設定 10 個聯絡人進行主動參與，並提供備註，以引導 SRT 與您聯絡。您的主動參與聯絡人應該可在事件期間與 SRT 互動。如果您沒有全年無休的營運中心，您可以提供呼叫器聯絡人，並在聯絡備註中指出此聯絡偏好設定。

主動參與需要您執行下列動作：

- 您必須訂閱[商業支援計劃](#)或[企業支援計劃](#)。
- 您必須將 Amazon Route 53 運作狀態檢查與您希望透過主動參與保護的任何資源建立關聯。SRT 會使用運作狀態檢查的狀態，協助判斷事件是否需要主動參與，因此運作狀態檢查必須準確反映受保護資源的狀態。如需詳細資訊和指引，請參閱[透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。
- 對於與 AWS WAF Web ACL 相關聯的資源，您必須使用 AWS WAF (v2) 建立 Web ACL，這是的最新版本 AWS WAF。
- 您必須提供至少一個聯絡人，SRT 才能在事件期間用於主動參與。保持您的聯絡資訊完整且為最新狀態。

啟用 SRT 主動參與

1. 在 AWS Shield 主控台概觀頁面的主動參與和聯絡下，於聯絡區域選擇編輯。

在編輯聯絡人頁面中，提供您希望 SRT 主動參與聯絡人的聯絡資訊。

如果您提供多個聯絡案例，請在備註中指出應該使用每個聯絡案例的情況。包含主要和次要聯絡人指定，並提供每個聯絡人的可用時間和時區。

聯絡備註範例：

- 這是 24 小時全年無休配置的熱線。請與回應分析師合作，他們會在通話中取得適當的人員。
- 如果熱線未在 5 分鐘內回應，請聯絡我。

2. 選擇 Save (儲存)。

概觀頁面反映更新的聯絡資訊。

3. 選擇編輯主動參與功能，選擇啟用，然後選擇儲存以啟用主動參與。

聯絡 SRT 以協助處理可疑的 DDoS 事件

您可以使用下列其中一種方式聯絡 SRT：

支援案例

您可以在 AWS Support Center 主控台AWS Shield的 下開啟案例。

如需建立支援案例的指引，請參閱 [AWS 支援中心](#)。

選取適合您情況的嚴重性，並提供您的聯絡詳細資訊。在描述中，盡可能提供詳細資訊。提供您認為可能受到影響的任何受保護資源，以及最終使用者體驗目前狀態的相關資訊。例如，如果您的使用者體驗降級或部分應用程式目前無法使用，請提供該資訊。

- 對於可疑的 DDoS 攻擊 – 如果應用程式可用性或效能目前受到可能的 DDoS 攻擊影響，請選擇下列嚴重性和聯絡選項：
 - 針對嚴重性，選擇您支援計劃可用的最高嚴重性：
 - 對於商業支援，這是生產系統關閉：< 1 小時。
 - 對於企業支援，這是業務關鍵系統關閉：< 15 分鐘。
 - 針對聯絡選項，選取電話或聊天，並提供您的詳細資訊。使用即時聯絡方法提供最快的回應。

主動參與

透過 AWS Shield Advanced 主動參與，如果與受保護資源相關聯的 Amazon Route 53 運作狀態檢查在偵測到事件期間變得運作狀態不佳，SRT 會直接與您聯絡。如需有關此選項的詳細資訊，請參閱 [設定 SRT 的主動參與，以直接與您聯絡](#)。

使用 SRT 設定針對 DDoS 攻擊的自訂緩解措施

此頁面提供使用 SRT 建置自訂 DDoS 攻擊緩解措施的說明。

對於彈性 IPs(EIPs) 和 AWS Global Accelerator 標準加速器，您可以使用 SRT 來設定自訂緩解措施。如果您知道在置放緩解措施時應強制執行的特定邏輯，這會很有用。例如，您可能只想要允許來自特定國家/地區的流量、強制執行特定速率限制、設定選用驗證、不允許片段，或只允許符合封包承載中特定模式的流量。

常見的自訂緩解措施範例包括：

- 模式比對 – 如果您操作與用戶端應用程式互動的服務，您可以選擇比對這些應用程式獨有的已知模式。例如，您可以操作遊戲或通訊服務，要求最終使用者安裝您分發的特定軟體。您可以在應用程式傳送至服務的每個封包中包含魔術數字。您可以比對非分段 TCP 或 UDP 封包承載和標頭的最多 128 個位元組（個別或連續）。相符項目可以十六進位表示法表示為封包承載開始時的特定位移，或已知值之後的動態位移。例如，緩解措施可以尋找位元組，0x01然後預期 0x12345678會是接下來的四個位元組。
- DNS 特定 – 如果您使用 Global Accelerator 或 Amazon Elastic Compute Cloud (Amazon EC2) 等服務來操作自己的權威 DNS 服務，您可以請求自訂緩解措施來驗證封包，以確保它們是有效的 DNS 查詢，並套用可疑評分來評估 DNS 流量特有的屬性。

若要查詢如何使用 SRT 建置自訂緩解措施，請在 下建立支援案例 AWS Shield。若要進一步了解如何建立 AWS 支援 案例，請參閱 [入門 AWS 支援](#)。

中的資源保護 AWS Shield Advanced

您可以新增和設定 資源的 AWS Shield Advanced 保護。您可以管理單一資源的保護，並將受保護的資源分組到邏輯集合中，以便更好地管理事件。您也可以使用 追蹤 Shield Advanced 保護的變更 AWS Config。

Note

Shield Advanced 僅保護您在 Shield Advanced 中或透過 Shield Advanced AWS Firewall Manager 政策指定的資源。它不會自動保護您的資源。

如果您使用的是 AWS Firewall Manager Shield Advanced 政策，則不需要管理政策範圍內資源的保護。Firewall Manager 會根據政策組態，自動管理政策範圍內的帳戶和資源保護。如需詳細資訊，請參閱在 [Firewall Manager 中使用 AWS Shield Advanced 政策](#)。

主題

- [AWS Shield Advanced 保護的資源清單](#)
- [使用 Shield Advanced 保護 Amazon EC2 執行個體和 Network Load Balancer](#)
- [使用 AWS Shield Advanced 和保護應用程式層（第 7 層）AWS WAF](#)
- [透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)
- [將 AWS Shield Advanced 保護新增至 AWS 資源](#)
- [編輯 AWS Shield Advanced 保護](#)
- [為 Shield Advanced 保護的資源建立警示和通知](#)
- [從 AWS 資源移除 AWS Shield Advanced 保護](#)
- [分組您的 AWS Shield Advanced 保護](#)
- [中的追蹤 Shield Advanced 資源保護變更 AWS Config](#)

AWS Shield Advanced 保護的資源清單

本節提供有關每個資源類型的 Shield Advanced 保護的資訊。

Shield Advanced 保護網路和傳輸層（第 3 層和第 4 層）和應用程式層（第 7 層）中的 AWS 資源。您可以透過與受保護的資源建立關聯，直接保護某些資源和其他資源。Shield Advanced 支援 IPv4，且不支援 IPv6。

Note

Shield Advanced 僅保護您在 Shield Advanced 中或透過 AWS Firewall Manager Shield Advanced 政策指定的資源。它不會自動保護您的資源。

您可以使用 Shield Advanced 搭配下列資源類型進行進階監控和保護：

- Amazon CloudFront 分佈。對於 CloudFront 連續部署，Shield Advanced 會保護與受保護的主要分佈相關聯的任何預備分佈。
- Amazon Route 53 託管區域。
- AWS Global Accelerator 標準加速器。

- Amazon EC2 彈性 IP 地址。Shield Advanced 會保護與受保護彈性 IP 地址相關聯的資源。
- Amazon EC2 執行個體，透過與 Amazon EC2 彈性 IP 地址的關聯。
- 下列 Elastic Load Balancing (ELB) 負載平衡器：
 - Application Load Balancer。
 - Classic Load Balancer。
 - Network Load Balancer，透過與 Amazon EC2 彈性 IP 地址的關聯。

Note

您無法使用 Shield Advanced 來保護任何其他資源類型。例如，您無法保護 AWS Global Accelerator 自訂路由加速器或 Gateway Load Balancer。

您可以監控和保護每個資源類型最多 1,000 個資源 AWS 帳戶。例如，在單一帳戶中，您可以保護 1,000 個 Amazon EC2 彈性 IP 地址、1,000 個 CloudFront 分佈和 1,000 個 Application Load Balancer。您可以透過 Service Quotas 主控台請求增加 Shield Advanced 可保護的資源數量，網址為 <https://console.aws.amazon.com/servicequotas/>。

使用 Shield Advanced 保護 Amazon EC2 執行個體和 Network Load Balancer

此頁面說明如何使用 Amazon EC2 執行個體和 Network Load Balancer 的 AWS Shield Advanced 保護。

您可以先將這些資源連接至彈性 IP 地址，然後在 Shield Advanced 中保護彈性 IP 地址，以保護 Amazon EC2 執行個體和 Network Load Balancer。

當您保護彈性 IP 地址時，Shield Advanced 會識別並保護其連接的資源。Shield Advanced 會自動識別連接到彈性 IP 地址的資源類型，並套用該資源的適當偵測和緩解措施。這包括設定彈性 IP 地址特有的網路 ACLs。如需搭配 AWS 資源使用彈性 IP 地址的詳細資訊，請參閱下列指南：[Amazon Elastic Compute Cloud 文件](#)或 [Elastic Load Balancing 文件](#)。

在攻擊期間，Shield Advanced 會自動將您的網路 ACLs 部署到 AWS 網路邊界。當您的網路 ACLs 位於網路邊界時，Shield Advanced 可以提供對較大 DDoS 事件的保護。一般而言，網路 ACLs 會在 Amazon VPC 內的 Amazon EC2 執行個體附近套用。網路 ACL 只能減輕您的 Amazon VPC 和執行個體所能處理的攻擊。例如，如果連接至 Amazon EC2 執行個體的網路介面最多可以處理 10 Gbps，則超過 10 Gbps 的磁碟區將減慢速度，並可能封鎖對該執行個體的流量。在攻擊期間，Shield Advanced

會將您的網路 ACL 提升為 AWS 邊界，以處理多個 TB 的流量。您的網路 ACL 能夠提供您的資源遠超過網路典型容量的保護。如需網路 ACL 的詳細資訊，請參閱 [網路 ACL](#)。

有些擴展工具 AWS Elastic Beanstalk，例如，不會讓您自動將彈性 IP 地址連接到 Network Load Balancer。在這些情況下，您需要手動連接彈性 IP 地址。

使用 AWS Shield Advanced 和 保護應用程式層（第 7 層）AWS WAF

此頁面說明 Shield Advanced 和 如何 AWS WAF 共同保護應用程式層（第 7 層）的資源。

若要使用 Shield Advanced 保護您的應用程式層資源，請先將 AWS WAF Web ACL 與資源建立關聯，並將一或多個速率型規則新增至其中。此外，您還可以啟用自動應用程式層 DDoS 緩解，這會導致 Shield Advanced 代表您自動建立和管理 Web ACL 規則，以回應 DDoS 攻擊。

當您使用 Shield Advanced 保護應用程式層資源時，Shield Advanced 會分析一段時間內的流量，以建立和維護基準。Shield Advanced 使用這些基準來偵測可能表示 DDoS 攻擊的流量模式異常。Shield Advanced 偵測到攻擊的時間點取決於 Shield Advanced 在攻擊之前能夠觀察到的流量，以及您用於 Web 應用程式的架構。可能影響 Shield Advanced 行為的架構變化包括您使用的執行個體類型、執行個體大小，以及執行個體類型是否支援增強型聯網。您也可以設定 Shield Advanced 來自動放置應用程式層攻擊的緩解措施。

Shield Advanced 訂閱和 AWS WAF 成本

Shield Advanced 訂閱涵蓋您使用 Shield Advanced 保護之資源的標準 AWS WAF 功能的成本。Shield Advanced 保護涵蓋的標準 AWS WAF 費用是每個保護套件或 Web ACL 的成本、每個規則的成本，以及 Web 請求檢查每百萬請求的基本價格、最多 1,500 WCUs，以及最多預設內文大小。

啟用 Shield Advanced 自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入您保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)、[使用 Shield Advanced 規則群組保護應用程式層](#) 及 [中的 Web ACL 容量單位 WCUs\) AWS WAF](#)。

您對 Shield Advanced 的訂閱不涵蓋對使用 Shield Advanced 時未保護之資源 AWS WAF 的使用。它也不會涵蓋受保護資源的任何其他非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括 Bot Control、CAPTCHA 規則動作、使用超過 1,500 個 WCUs ACLs，以及檢查超出預設內文大小的請求內文。AWS WAF 定價頁面上提供完整清單。您對 Shield Advanced 的訂閱包括對 Layer 7 Anti-DDoS Amazon Managed Rule 群組的存取。作為訂閱的一部分，您在一個日曆月內最多會收到 500 億個 Shield Advanced 受保護 AWS WAF 資源的請求。超過 500 億的請求將根據 AWS Shield Advanced 定價頁面計費。

如需完整資訊和定價範例，請參閱 [Shield 定價](#) 和 [AWS WAF 定價](#)。

主題

- [使用 Shield Advanced 影響應用程式層事件偵測和緩解的因素清單](#)
- [使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層](#)
- [使用以 AWS WAF 速率為基礎的規則和 Shield Advanced 保護應用程式層](#)
- [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)

使用 Shield Advanced 影響應用程式層事件偵測和緩解的因素清單

本節說明影響 Shield Advanced 偵測和緩解應用程式層事件的因素。

運作狀態檢查

準確報告應用程式整體運作狀態的運作狀態檢查，可提供 Shield Advanced 有關應用程式所經歷流量條件的資訊。當您的應用程式回報運作狀態不佳時，Shield Advanced 需要的資訊較少，而且如果您的應用程式回報狀況良好，則需要更多攻擊的證據。

請務必設定您的運作狀態檢查，以便正確報告應用程式運作狀態。如需詳細資訊和指引，請參閱 [透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。

流量基準

流量基準提供 Shield Advanced 有關應用程式正常流量特性的資訊。Shield Advanced 使用這些基準來識別您的應用程式未接收正常流量的時間，因此它可以通知您，並根據設定開始設計和測試緩解選項，以抵禦潛在的攻擊。如需 Shield Advanced 如何使用流量基準來偵測潛在事件的詳細資訊，請參閱概觀章節 [應用程式層威脅的 Shield Advanced 偵測邏輯（第 7 層）](#)。

Shield Advanced 會根據與受保護資源相關聯的 Web ACL 提供的資訊建立其基準。Web ACL 必須與該資源建立關聯至少 24 小時，最長 30 天，Shield Advanced 才能可靠地判斷應用程式的基準。當您透過 Shield Advanced 或透過 建立 Web ACL 關聯時，所需的時間就會開始 AWS WAF。

如需搭配 Shield Advanced 應用程式層保護使用 Web ACL 的詳細資訊，請參閱 [使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層](#)。

速率為基礎的規則

以速率為基礎的規則有助於緩解攻擊。他們也可以掩蓋攻擊，方法是在攻擊變成足夠大的問題之前加以緩解，以針對正常流量基準顯示或在運作狀態檢查狀態報告中顯示。

當您使用 Shield Advanced 保護應用程式資源時，我們建議您在 Web ACL 中使用以速率為基礎的規則。即使他們的緩解措施可能會掩蓋潛在的攻擊，但它們是寶貴的第一道防線，有助於確保您的應用程

式可供您的合法客戶使用。以速率為基礎的規則偵測的流量和速率限制會顯示在您的 AWS WAF 指標中。

除了您自己的速率型規則之外，如果您啟用自動應用程式層 DDoS 緩解，Shield Advanced 會將規則群組新增至 Web ACL，以用於緩解攻擊。在此規則群組中，Shield Advanced 一律具有以速率為基礎的規則，可限制來自已知為 DDoS 攻擊來源之 IP 地址的請求量。Shield Advanced 規則緩解的流量指標無法供您檢視。

如需速率型規則的詳細資訊，請參閱 [在中使用以速率為基礎的規則陳述式 AWS WAF](#)。如需有關 Shield Advanced 用於自動應用程式層 DDoS 緩解的速率型規則的資訊，請參閱 [使用 Shield Advanced 規則群組保護應用程式層](#)。

如需 Shield Advanced 和 AWS WAF 指標的詳細資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。

使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層

此頁面說明 AWS WAF Web ACLs 和 Shield Advanced 如何共同建立基本的應用程式層保護。

若要使用 Shield Advanced 保護應用程式層資源，請先將 AWS WAF Web ACL 與資源建立關聯。AWS WAF 是 Web 應用程式防火牆，可讓您監控轉送至應用程式層資源的 HTTP 和 HTTPS 請求，並可讓您根據請求的特性控制對內容的存取。您可以設定 Web ACL，根據請求的來源、查詢字串和 Cookie 的內容，以及來自單一 IP 地址的請求速率等因素來監控和管理請求。Shield Advanced 保護至少需要您將 Web ACL 與速率型規則建立關聯，這會限制每個 IP 地址的請求速率。

如果關聯的 Web ACL 未定義以速率為基礎的規則，Shield Advanced 會提示您定義至少一個規則。速率型規則會在來源 IPs 超過您定義的閾值時自動封鎖流量。它們有助於保護您的應用程式免受 Web 請求洪水的影響，並可提供有關流量突然峰值的提醒，這可能表示潛在的 DDoS 攻擊。

Note

以速率為基礎的規則會快速回應規則正在監控的流量尖峰。因此，以速率為基礎的規則不僅可以防止攻擊，還可以透過 Shield Advanced 偵測來偵測潛在的攻擊。這種權衡有利於防止完全掌握攻擊模式。我們建議您使用以速率為基礎的規則作為防禦攻擊的第一道防線。

在 Web ACL 就位的情況下，如果發生 DDoS 攻擊，您可以透過在 Web ACL 中新增和管理規則來套用緩解措施。您可以在 Shield Response Team (SRT) 的協助下直接執行此操作，或透過自動應用程式層 DDoS 緩解措施自動執行此操作。

 Important

如果您也使用自動應用程式層 DDoS 緩解，請參閱 [中管理 Web ACL 的最佳實務](#) [使用自動應用程式層 DDoS 緩解的最佳實務](#)。

如需使用 AWS WAF 來管理 Web 請求監控和管理規則的詳細資訊，請參閱 [在中建立保護套件或 Web ACL AWS WAF](#)。

使用以 AWS WAF 速率為基礎的規則和 Shield Advanced 保護應用程式層

此頁面說明以 AWS WAF 速率為基礎的規則和 Shield Advanced 如何一起運作，以建立基本的應用程式層保護。

當您使用速率型規則搭配其預設組態時，會 AWS WAF 定期評估過去 5 分鐘時段的流量。會 AWS WAF 封鎖來自任何超過規則閾值之 IP 地址的請求，直到請求速率下降到可接受的層級為止。當您透過 Shield Advanced 設定以速率為基礎的規則時，將其速率閾值設定為大於您在任何五分鐘時段內從任何一個來源 IP 預期之正常流量速率的值。

您可能想要在 Web ACL 中使用多個以速率為基礎的規則。例如，對於具有高閾值的所有流量，以及設定為符合 Web 應用程式特定部分且閾值較低的一或多個額外規則，您可以有一個速率型規則。例如，您可能會在閾值/login.html較低的 URI 上比對，以減少對登入頁面的濫用。

您可以設定以速率為基礎的規則，以使用不同的評估時段，並根據多個請求元件彙總請求，例如標頭值、標籤和查詢引數。如需詳細資訊，請參閱[在中使用以速率為基礎的規則陳述式 AWS WAF](#)。

如需詳細資訊和指導，請參閱安全部落格文章 [三個最重要的以 AWS WAF 速率為基礎的規則](#)。

透過 擴充組態選項 AWS WAF

Shield Advanced 主控台可讓您新增以速率為基礎的規則，並使用基本的預設設定進行設定。您可以透過管理以速率為基礎的規則來定義其他組態選項 AWS WAF。例如，您可以設定規則，根據轉送 IP 地址、查詢字串和標籤等金鑰來彙總請求。您也可以將縮小範圍陳述式新增至規則，以篩選來自評估和速率限制的一些請求。如需詳細資訊，請參閱[在中使用以速率為基礎的規則陳述式 AWS WAF](#)。

使用 Shield Advanced 自動化應用程式層 DDoS 緩解

此頁面介紹自動應用程式層 DDoS 緩解措施的主題，並列出相關聯的警告。

您可以設定 Shield Advanced 來自動回應，透過計算或封鎖屬於攻擊一部分的 Web 請求，來減輕對受保護應用程式層資源的應用程式層（第 7 層）攻擊。此選項是您透過 Shield Advanced 使用 AWS WAF Web ACL 和您自己的速率型規則新增的應用程式層保護的補充。

為資源啟用自動緩解時，Shield Advanced 會在資源相關聯的 Web ACL 中維護規則群組，以代表資源管理緩解規則。規則群組包含以速率為基礎的規則，可追蹤來自已知為 DDoS 攻擊來源之 IP 地址的請求量。

此外，Shield Advanced 會將目前的流量模式與歷史流量基準進行比較，以偵測可能表示 DDoS 攻擊的偏差。Shield Advanced 會透過在規則群組中建立、評估和部署其他自訂 AWS WAF 規則，來回應偵測到的 DDoS 攻擊。

使用自動應用程式層 DDoS 緩解措施的注意事項

以下清單說明 Shield Advanced 自動應用程式層 DDoS 緩解措施的注意事項，並說明您可能想要採取的步驟。

- 自動應用程式層 DDoS 緩解僅適用於使用最新版本 AWS WAF (v2) 建立的保護套件或 Web ACLs。
- Shield Advanced 需要時間來建立應用程式正常、歷史流量的基準，它利用它來偵測和隔離攻擊流量與正常流量，以緩解攻擊流量。建立基準的時間是從您將 Web ACL 與受保護的應用程式資源建立關聯起 24 小時到 30 天。如需流量基準的其他資訊，請參閱 [使用 Shield Advanced 影響應用程式層事件偵測和緩解的因素清單](#)。
- 啟用自動應用程式層 DDoS 緩解措施會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCUs) 的保護套件或 Web ACL。這些 WCUs 會計入保護套件或 Web ACL 中的 WCU 用量。如需詳細資訊，請參閱 [使用 Shield Advanced 規則群組保護應用程式層](#) 和 [中的 Web ACL 容量單位 WCUs](#) [AWS WAF](#)。
- Shield Advanced 規則群組會產生 AWS WAF 指標，但無法檢視。這與您在保護套件或 Web ACL 中使用的任何其他規則群組相同，但不擁有，例如 AWS 受管規則規則群組。如需 AWS WAF 指標的詳細資訊，請參閱 [AWS WAF 指標和維度](#)。如需此 Shield Advanced 保護選項的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。
- 對於保護多個資源 ACLs，自動緩解只會部署不會對任何受保護資源產生負面影響的自訂緩解措施。
- 從開始 DDoS 攻擊到 Shield Advanced 放置自訂自動緩解規則的時間會隨每個事件而異。有些 DDoS 攻擊可能會在部署自訂規則之前結束。當緩解措施已就緒時，可能會發生其他攻擊，因此從事件開始時，這些規則可能會緩解。此外，Web ACL 和 Shield Advanced 規則群組中的速率型規則可能會在偵測到為可能事件之前緩解攻擊流量。
- 對於透過內容交付網路 (CDN) 接收任何流量的 Application Load Balancer，例如 Amazon CloudFront，Shield Advanced 對這些 Application Load Balancer 資源的應用程式層自動緩解功能將

會減少。Shield Advanced 使用用戶端流量屬性來識別攻擊流量，並將攻擊流量從正常流量隔離到您的應用程式，而 CDNs 可能無法保留或轉送原始用戶端流量屬性。如果您使用 CloudFront，我們建議您在 CloudFront 分佈上啟用自動緩解。

- 自動應用程式層 DDoS 緩解措施不會與保護群組互動。您可以為保護群組中的資源啟用自動緩解，但 Shield Advanced 不會根據保護群組調查結果自動套用攻擊緩解。Shield Advanced 會針對個別資源套用自動攻擊緩解措施。

內容

- [使用自動應用程式層 DDoS 緩解的最佳實務](#)
- [啟用自動應用程式層 DDoS 緩解](#)
 - [當您啟用自動緩解時會發生什麼情況](#)
- [Shield Advanced 如何管理自動緩解](#)
 - [Shield Advanced 如何使用自動緩解來回應 DDoS 攻擊](#)
 - [Shield Advanced 如何管理規則動作設定](#)
 - [Shield Advanced 如何在攻擊消失時管理緩解措施](#)
 - [當您停用自動緩解時會發生什麼情況](#)
- [使用 Shield Advanced 規則群組保護應用程式層](#)
- [檢視資源的自動應用程式層 DDoS 緩解組態](#)
- [啟用和停用自動應用程式層 DDoS 緩解](#)
- [變更用於自動應用程式層 DDoS 緩解的動作](#)
- [使用 AWS CloudFormation 搭配自動應用程式層 DDoS 緩解](#)

使用自動應用程式層 DDoS 緩解的最佳實務

當您使用自動緩解時，請遵循本節中提供的指引。

一般保護管理

請遵循這些準則來規劃和實作您的自動緩解保護。

- 透過 Shield Advanced 管理所有自動緩解保護，或者，如果您使用 AWS Firewall Manager 來透過 Firewall Manager 管理 Shield Advanced 自動緩解設定。請勿混合使用 Shield Advanced 和 Firewall Manager 來管理這些保護。
- 使用相同的 Web ACLs 和保護設定管理類似的資源，並使用不同的 Web ACLs 管理不同的資源。當 Shield Advanced 緩解受保護資源的 DDoS 攻擊時，它會定義與資源相關聯的 Web ACL 規則，然

後針對與 Web ACL 相關聯的所有資源流量測試規則。Shield Advanced 只有在規則不會對任何相關聯的資源產生負面影響時，才會套用規則。如需詳細資訊，請參閱[Shield Advanced 如何管理自動緩解](#)。

- 對於透過 Amazon CloudFront 分佈代理其所有網際網路流量的 Application Load Balancer，只會在 CloudFront 分佈上啟用自動緩解。CloudFront 分佈將始終具有最多的原始流量屬性，Shield Advanced 會利用這些屬性來緩解攻擊。

偵測和緩解最佳化

請遵循這些準則，以最佳化自動緩解為受保護資源提供的保護。如需應用程式層偵測和緩解的概觀，請參閱[使用 Shield Advanced 影響應用程式層事件偵測和緩解的因素清單](#)。

- 設定受保護資源的運作狀態檢查，並在 Shield Advanced 保護中啟用運作狀態型偵測。如需準則，請參閱[透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測](#)。
- 在 Count 模式中啟用自動緩解，直到 Shield Advanced 建立正常、歷史流量的基準。Shield Advanced 需要 24 小時到 30 天的時間來建立基準。

建立正常流量模式的基準需要下列項目：

- Web ACL 與受保護資源的關聯。您可以 AWS WAF 直接使用 來建立 Web ACL 的關聯，也可以在啟用 Shield Advanced 應用程式層保護並指定要使用的 Web ACL 時讓 Shield Advanced 建立關聯。
- 正常流量流向受保護的應用程式。如果您的應用程式未遇到正常流量，例如在應用程式啟動之前，或長時間缺乏生產流量，則無法收集歷史資料。

Web ACL 管理

請遵循這些準則來管理您用於自動緩解 ACLs。

- 如果您需要取代與受保護資源相關聯的 Web ACL，請依序進行下列變更：
 - 在 Shield Advanced 中，停用自動緩解。
 - 在 AWS WAF 中，取消舊 Web ACL 的關聯，並關聯新的 Web ACL。
 - 在 Shield Advanced 中，啟用自動緩解。

Shield Advanced 不會自動將舊 Web ACL 的自動緩解措施轉移到新的 Web ACL。

- 請勿從名稱開頭為 ACLs 刪除任何規則群組規則 ShieldMitigationRuleGroup。如果您確實刪除此規則群組，您可以停用 Shield Advanced 自動緩解對與 Web ACL 相關聯的每個資源提供的保

護。此外，Shield Advanced 可能需要一些時間才能收到變更通知並更新其設定。在此期間，Shield Advanced 主控台頁面將提供不正確的資訊。

如需規則群組的詳細資訊，請參閱 [使用 Shield Advanced 規則群組保護應用程式層](#)。

- 請勿修改名稱開頭為 的規則群組規則的名稱ShieldMitigationRuleGroup。這樣做可能會干擾 Shield Advanced 透過 Web ACL 自動緩解提供的保護。
- 當您建立規則和規則群組時，請勿使用開頭為 的名稱ShieldMitigationRuleGroup。Shield Advanced 使用此字串來管理您的自動緩解措施。
- 在您的 Web ACL 規則管理中，請勿指派 10,000,000 的優先順序設定。Shield Advanced 會在新增時將此優先順序設定指派給其自動緩解規則群組規則。
- 將ShieldMitigationRuleGroup規則保持優先，以便在您希望它與 Web ACL 中的其他規則相關時執行。Shield Advanced 會將規則群組規則新增至優先順序為 10,000,000 的 Web ACL，以便在您的其他規則之後執行。如果您使用 AWS WAF 主控台精靈來管理您的 Web ACL，請在將規則新增至 Web ACL 之後視需要調整優先順序設定。
- 如果您使用 AWS CloudFormation 來管理 Web ACLs，則不需要管理ShieldMitigationRuleGroup規則群組規則。請遵循 中的指引[使用 AWS CloudFormation 搭配自動應用程式層 DDoS 緩解](#)。

啟用自動應用程式層 DDoS 緩解

此頁面說明如何設定 Shield Advanced 以自動回應應用程式層攻擊。

您可以啟用 Shield Advanced 自動緩解，做為資源的應用程式層 DDoS 保護的一部分。如需透過 主控台執行此操作的詳細資訊，請參閱 [設定應用程式層 DDoS 保護](#)。

自動緩解功能需要您執行下列動作：

- 將 Web ACL 與 資源建立關聯 – 這是任何 Shield Advanced 應用程式層保護的必要項目。您可以針對多個資源使用相同的 Web ACL。我們建議僅對具有類似流量的資源執行此操作。如需有關 Web ACLs 的資訊，包括搭配多個資源使用它們的要求，請參閱 [如何 AWS WAF 運作](#)。
- 啟用和設定 Shield Advanced 自動應用程式層 DDoS 緩解 – 當您啟用此功能時，您可以指定是否要 Shield Advanced 自動封鎖或計數其判定為 DDoS 攻擊一部分的 Web 請求。Shield Advanced 會將規則群組新增至相關聯的 Web ACL，並使用它動態管理其對資源上 DDoS 攻擊的回應。如需規則動作選項的相關資訊，請參閱 [在 中使用規則動作 AWS WAF](#)。
- （選用，但建議）將速率型規則新增至 Web ACL – 根據預設，速率型規則會防止任何個別 IP 地址在短時間內傳送太多請求，藉此為您的資源提供基本的 DDoS 攻擊防護。如需速率型規則的相關資訊，包括自訂請求彙總選項和範例，請參閱 [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)。

當您啟用自動緩解時會發生什麼情況

當您啟用自動緩解時，Shield Advanced 會執行下列動作：

- 視需要新增 Shield Advanced 使用的規則群組 – 如果您與資源相關聯的 AWS WAF Web ACL 尚未擁有專用於自動應用程式層 DDoS 緩解的 AWS WAF 規則群組規則，Shield Advanced 會新增規則群組規則。

規則群組規則的名稱開頭為 `ShieldMitigationRuleGroup`。規則群組一律包含名為 `的速率型規則` `ShieldKnownOffenderIPRateBasedRule`，這會限制來自已知為 DDoS 攻擊來源之 IP 地址的請求量。如需有關 Shield Advanced 規則群組和參考它的 Web ACL 規則的其他詳細資訊，請參閱 [使用 Shield Advanced 規則群組保護應用程式層](#)。

- 開始回應資源的 DDoS 攻擊 – Shield Advanced 會自動回應受保護資源的 DDoS 攻擊。除了一律存在的速率型規則之外，Shield Advanced 也會使用其規則群組來部署自訂 AWS WAF 規則，以緩解 DDoS 攻擊。Shield Advanced 會針對您的應用程式和應用程式遇到的攻擊量身打造這些規則，並在部署之前針對資源的歷史流量進行測試。

Shield Advanced 會在您用於自動緩解的任何 Web ACL 中使用單一規則群組規則。如果 Shield Advanced 已新增另一個受保護資源的規則群組，則不會將另一個規則群組新增至 Web ACL。

自動應用程式層 DDoS 緩解取決於規則群組是否存在，以緩解攻擊。如果規則群組因任何原因從 AWS WAF Web ACL 中移除，移除會停用與 Web ACL 相關聯的所有資源的自動緩解。

Shield Advanced 如何管理自動緩解

本節中的主題說明 Shield Advanced 如何處理自動應用程式層 DDoS 緩解的組態變更，以及啟用自動緩解時如何處理 DDoS 攻擊。

主題

- [Shield Advanced 如何使用自動緩解來回應 DDoS 攻擊](#)
- [Shield Advanced 如何管理規則動作設定](#)
- [Shield Advanced 如何在攻擊消失時管理緩解措施](#)
- [當您停用自動緩解時會發生什麼情況](#)

Shield Advanced 如何使用自動緩解來回應 DDoS 攻擊

當您在受保護的資源上啟用自動緩解時，Shield Advanced 規則群組 `ShieldKnownOffenderIPRateBasedRule` 中的速率型規則會自動回應來自已知 DDoS 來源的流量增加。此速率限制會快速套用，並做為對抗攻擊的前線防禦。

當 Shield Advanced 偵測到攻擊時，它會執行下列動作：

1. 嘗試識別攻擊簽章，該簽章會將攻擊流量與一般流量隔離到您的應用程式。目標是產生高品質的 DDoS 緩解規則，這些規則在放置時只會影響攻擊流量，而且不會影響應用程式的一般流量。
2. 針對受攻擊資源的歷史流量模式，以及與相同 Web ACL 相關聯的任何其他資源，評估已識別的攻擊簽章。Shield Advanced 會在部署任何規則以回應事件之前執行此操作。

根據評估結果，Shield Advanced 會執行下列其中一項：

- 如果 Shield Advanced 判斷攻擊簽章只會隔離 DDoS 攻擊中涉及的流量，則會在 Web ACL 中 Shield Advanced 緩解規則群組中的 AWS WAF 規則中實作簽章。Shield Advanced 會將您已為資源的自動緩解設定的動作設定提供給這些規則：Count 或 Block。
- 否則，Shield Advanced 不會放置緩解措施。

在整個攻擊過程中，Shield Advanced 會傳送相同的通知，並提供與基本 Shield Advanced 應用程式層保護相同的事件資訊。您可以在 Shield Advanced 事件主控台中查看事件和 DDoS 攻擊，以及攻擊的任何 Shield Advanced 緩解措施的相關資訊。如需相關資訊，請參閱 [使用 Shield Advanced 的 DDoS 事件可見性](#)。

如果您已將自動緩解設定為使用 Block 規則動作，且您遇到來自 Shield Advanced 部署之緩解規則的誤報，您可以將規則動作變更為 Count。如需如何執行此操作的詳細資訊，請參閱 [變更為自動應用程式層 DDoS 緩解的動作](#)。

Shield Advanced 如何管理規則動作設定

您可以將自動緩解的規則動作設定為 Block 或 Count。

當您變更受保護資源的自動緩解規則動作設定時，Shield Advanced 會更新資源的所有規則設定。它會更新 Shield Advanced 規則群組中資源目前採用的任何規則，並在建立新規則時使用新的動作設定。

對於使用相同 Web ACL 的資源，如果您指定不同的動作，Shield Advanced 會使用規則群組的速率型規則 Block 的動作設定 `ShieldKnownOffenderIPRateBasedRule`。Shield Advanced 會代表特定受保護資源在規則群組中建立和管理其他規則，並使用您為資源指定的動作設定。Web ACL 中 Shield Advanced 規則群組中的所有規則都會套用至所有相關聯資源的 Web 流量。

變更動作設定可能需要幾秒鐘的時間才能傳播。在此期間，您可能會在規則群組正在使用的某些位置看到舊設定，在其他位置看到新設定。

您可以在 主控台的事件頁面，以及透過應用程式層組態頁面，變更自動緩解組態的規則動作設定。如需事件頁面的詳細資訊，請參閱[在中回應 DDoS 事件 AWS](#)。如需組態頁面的詳細資訊，請參閱[設定應用程式層 DDoS 保護](#)。

Shield Advanced 如何在攻擊消失時管理緩解措施

當 Shield Advanced 判斷不再需要為特定攻擊部署的緩解規則時，它會將其從 Shield Advanced 緩解規則群組中移除。

移除緩解規則不一定會與攻擊的結束同時發生。Shield Advanced 會監控其在您的受保護資源上偵測到的攻擊模式。它會保留其已部署的規則，以防止該攻擊的初始發生，藉此主動防禦具有特定簽章的攻擊再次發生。視需要，Shield Advanced 會增加其保留規則的時間窗口。如此一來，Shield Advanced 可能會在影響受保護資源之前，使用特定簽章來緩解重複的攻擊。

Shield Advanced 永遠不會移除以速率為基礎的規則 `ShieldKnownOffenderIPRateBasedRule`，這會限制來自已知為 DDoS 攻擊來源之 IP 地址的請求量。

當您停用自動緩解時會發生什麼情況

當您停用資源的自動緩解時，Shield Advanced 會執行下列動作：

- 停止自動回應 DDoS 攻擊 – Shield Advanced 會停止其資源的自動回應活動。
- 從 Shield Advanced 規則群組中移除不需要的規則 – 如果 Shield Advanced 代表受保護的資源在其受管規則群組中維護任何規則，則會將其移除。
- 如果不再使用 Shield Advanced 規則群組，請將其移除 – 如果您與資源相關聯的 Web ACL 未與已啟用自動緩解的任何其他資源建立關聯，Shield Advanced 會從 Web ACL 中移除其規則群組規則。

使用 Shield Advanced 規則群組保護應用程式層

此頁面說明 Shield Advanced 規則群組如何在 Web ACL 中運作。

Shield Advanced 會使用規則群組中的規則來管理自動緩解活動，該規則群組會擁有並為您管理。Shield Advanced 參考規則群組，其中包含您已與受保護資源建立關聯的 Web ACL 中的規則。

Web ACL 中的規則群組規則

Web ACL 中的 Shield Advanced 規則群組規則具有下列屬性：

- 名稱 – `ShieldMitigationRuleGroup_account-id_web-acl-id_unique-identifier`
- Web ACL 容量單位 (WCU) – 150。這些 WCUs 會計入您 Web ACL 中的 WCU 用量。

Shield Advanced 會在您的 Web ACL 中建立此規則，優先順序設定為 10,000,000，因此它會在 Web ACL 中的其他規則和規則群組之後執行。會從啟動的最低數值優先順序設定 AWS WAF 執行 Web ACL 中的規則。在您管理 Web ACL 期間，此優先順序設定可能會變更。

除了 Web ACL 中規則群組使用的 WCUs 之外，自動緩解功能不會消耗您帳戶中的任何其他 AWS WAF 資源。例如，Shield Advanced 規則群組不會計入您帳戶的其中一個規則群組。如需中帳戶限制的相關資訊 AWS WAF，請參閱 [AWS WAF 配額](#)。

規則群組中的規則

在參考的 Shield Advanced 規則群組中，Shield Advanced 會維護以速率為基礎的規則 `ShieldKnownOffenderIPRateBasedRule`，這會限制來自已知為 DDoS 攻擊來源之 IP 地址的請求量。此規則可做為防禦任何攻擊的第一道防線，因為它一律存在於規則群組中，而且不依賴流量模式的分析來控制攻擊。此規則的動作會設定為您為自動緩解選擇的動作，就像規則群組中的其他規則一樣。如需速率型規則的相關資訊，請參閱 [在中使用以速率為基礎的規則陳述式 AWS WAF](#)。

Note

速率型規則 `ShieldKnownOffenderIPRateBasedRule` 的運作與 Shield Advanced 事件偵測無關。啟用自動緩解時，此規則速率會限制已知為 DDoS 攻擊來源的 IP 地址。對於這些 IP 地址，規則的速率限制可以防止攻擊，也可以防止攻擊出現在 Shield Advanced 偵測資訊中。這種權衡有利於防止對攻擊模式的完全可見性。

除了上述永久速率型規則之外，規則群組還包含 Shield Advanced 目前用來緩解 DDoS 攻擊的任何規則。Shield Advanced 會視需要新增、修改和移除這些規則。如需相關資訊，請參閱 [Shield Advanced 如何管理自動緩解](#)。

指標

規則群組會產生 AWS WAF 指標，但由於此規則群組由 Shield Advanced 擁有，因此這些指標無法檢視。如需詳細資訊，請參閱 [AWS WAF 指標和維度](#)。

檢視資源的自動應用程式層 DDoS 緩解組態

您可以在受保護資源頁面和個別保護頁面中檢視資源的自動應用程式層 DDoS 緩解組態。

檢視自動應用程式層 DDoS 緩解組態

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。在受保護資源清單中，資料欄自動應用程式層 DDoS 緩解指出是否啟用自動緩解，以及啟用時，Shield Advanced 要在其緩解中使用的動作。

您也可以選取任何應用程式層資源，以查看資源保護頁面上列出的相同資訊。

啟用和停用自動應用程式層 DDoS 緩解

下列程序說明如何啟用或停用受保護資源的自動回應。

啟用或停用單一資源的自動應用程式層 DDoS 緩解

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護索引標籤中，選取您要啟用自動緩解的應用程式層資源。資源的保護頁面隨即開啟。
4. 在資源的保護頁面中，選擇編輯。
5. 在頁面設定全域資源的第 7 層 DDoS 緩解 - 選用，針對自動應用程式層 DDoS 緩解，選擇您要用於自動緩解的選項。主控台內的選項如下：

- 保留目前的設定 – 不變更受保護資源的自動緩解設定。
- 啟用 – 啟用受保護資源的自動緩解。當您選擇此選項時，也請選取您希望自動緩解在 Web ACL 規則中使用的規則動作。如需規則動作設定的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。

如果您的受保護資源尚未擁有正常應用程式流量的歷史記錄，請在 Count 模式下啟用自動緩解，直到 Shield Advanced 可以建立基準。當您將 Web ACL 與受保護的資源建立關聯時，Shield Advanced 會開始收集其基準的資訊，而且建立正常流量的良好基準可能需要 24 小時到 30 天。

- 停用 – 停用受保護資源的自動緩解。
6. 逐步瀏覽其餘頁面，直到您完成並儲存組態為止。

在保護頁面中，會自動更新資源的緩解設定。

變更用於自動應用程式層 DDoS 緩解的動作

您可以在主控台的多個位置變更 Shield Advanced 用於其應用程式層自動回應的動作：

- 自動緩解組態 – 當您為資源設定自動緩解時，變更動作。如需此程序，請參閱上一節[啟用和停用自動應用程式層 DDoS 緩解](#)。
- 事件詳細資訊頁面 – 當您在主控台中檢視事件資訊時，變更事件詳細資訊頁面中的動作。如需相關資訊，請參閱[檢視 AWS Shield Advanced 事件詳細資訊](#)。

如果您有兩個共用 Web ACL 的受保護資源，且將一個 `Block` 和另一個 `Count` 的動作設為 `Block`，則 Shield Advanced 會將規則群組的速率型規則的動作 `ShieldKnownOffenderIPRateBasedRule` 設為 `Block`。

使用 AWS CloudFormation 搭配自動應用程式層 DDoS 緩解

此頁面說明如何使用 AWS CloudFormation 來管理您的保護和 AWS WAF Web ACLs。

啟用或停用自動應用程式層 DDoS 緩解

您可以使用 `AWS::Shield::Protection` 資源 AWS CloudFormation，透過 啟用和停用自動應用程式層 DDoS 緩解。效果與透過主控台或任何其他界面啟用或停用功能時相同。如需 AWS CloudFormation 資源的相關資訊，請參閱 AWS CloudFormation 使用者指南中的[AWS::Shield::Protection](#)。

管理用於自動緩解 ACLs

Shield Advanced 會使用受保護資源的 AWS WAF Web ACL 中的規則群組規則來管理受保護資源的自動緩解。透過 AWS WAF 主控台和 APIs，您會看到 Web ACL 規則中列出的規則，其名稱開頭為 `ShieldMitigationRuleGroup`。此規則專用於您的自動應用程式層 DDoS 緩解，並由 Shield Advanced 和 為您管理 AWS WAF。如需詳細資訊，請參閱[使用 Shield Advanced 規則群組保護應用程式層](#) 和 [Shield Advanced 如何管理自動緩解](#)。

如果您使用 AWS CloudFormation 來管理您的 Web ACLs，請勿將 Shield Advanced 規則群組規則新增至您的 Web ACL 範本。當您更新與自動緩解保護搭配使用的 Web ACL 時，AWS WAF 會自動管理 Web ACL 中的規則群組規則。

與透過您管理的其他 Web ACLs 相比，您會看到以下差異 AWS CloudFormation：

- AWS CloudFormation 如果沒有規則，則不會報告 Web ACL 的實際組態、Shield Advanced 規則群組規則和 Web ACL 範本之間堆疊偏離狀態的任何偏離。Shield Advanced 規則不會出現在偏離詳細資訊中資源的實際清單中。

您將能夠在您擷取的 Web ACL 清單中看到 Shield Advanced 規則群組規則 AWS WAF，例如透過 AWS WAF 主控台或 AWS WAF APIs。

- 如果您修改堆疊中的 Web ACL 範本，AWS WAF 且 Shield Advanced 會自動在更新的 Web ACL 中維護 Shield Advanced 自動緩解規則。Shield Advanced 提供的自動緩解保護不會因您對 Web ACL 的更新而中斷。

請勿在 AWS CloudFormation Web ACL 範本中管理 Shield Advanced 規則。Web ACL 範本不應列出 Shield Advanced 規則。遵循 Web ACL 管理的最佳實務，網址為 [使用自動應用程式層 DDoS 緩解的最佳實務](#)。

透過 Shield Advanced 和 Route 53 使用運作狀態檢查進行運作狀態型偵測

您可以設定 Shield Advanced 以使用以運作狀態為基礎的偵測，以提高攻擊偵測和緩解的回應能力和準確性。除了 Route 53 託管區域之外，您可以將此選項用於任何資源類型。

若要設定運作狀態型偵測，請在 Route 53 中定義資源的運作狀態檢查，確認報告狀態良好，然後將其與您的 Shield Advanced 保護建立關聯。如需有關 Route 53 運作狀態檢查的資訊，請參閱 [《Amazon Route 53 開發人員指南》](#) 中的 [Amazon Route 53 如何檢查資源的運作狀態](#)，以及 [建立、更新和刪除運作狀態檢查](#)。

Note

Shield Response Team (SRT) 主動參與支援需要運作狀態檢查。如需主動參與的相關資訊，請參閱 [設定 SRT 的主動參與，以直接與您聯絡](#)。

運作狀態檢查會根據您定義的要求來測量資源的運作狀態。運作狀態檢查狀態為 Shield Advanced 偵測機制提供重要輸入，讓它們對特定應用程式的目前狀態更敏感。

您可以針對 Route 53 託管區域以外的任何資源類型啟用運作狀態型偵測。

- 網路和傳輸層（第 3 層/第 4 層）資源 – 運作狀態型偵測可改善 Network Load Balancer、Elastic IP 地址和 Global Accelerator 標準加速器的網路層和傳輸層事件偵測和緩解的準確性。當您使用 Shield Advanced 保護這些資源類型時，Shield Advanced 可以為較小的攻擊提供緩解措施，並更快地緩解攻擊，即使流量在應用程式的容量內。

當您新增以運作狀態為基礎的偵測時，在相關運作狀態檢查運作狀態不佳的期間，Shield Advanced 可以更快地放置緩解措施，甚至降低閾值。

- 應用程式層（第 7 層）資源 – 以運作狀態為基礎的偵測可改善 CloudFront 分佈和 Application Load Balancer 的 Web 請求洪水偵測準確性。當您使用 Shield Advanced 保護這些資源類型時，如果流量出現統計上顯著的偏差，並結合流量模式的重大變更，根據請求特性，您會收到 Web 請求洪水偵測提醒。

透過以運作狀態為基礎的偵測，當相關聯的 Route 53 運作狀態檢查運作狀態不佳時，Shield Advanced 需要較小的偏差來提醒，並更快速地報告事件。相反地，當相關聯的 Route 53 運作狀態檢查良好時，Shield Advanced 需要較大的偏差來提醒。

如果運作狀態檢查僅在您的應用程式在可接受的參數內執行時報告運作狀態良好，且僅在未執行時報告運作狀態不佳，則您將受益於使用 Shield Advanced 進行運作狀態檢查。使用本節中的指引，在 Shield Advanced 中管理運作狀態檢查關聯。

Note

Shield Advanced 不會自動管理運作狀態檢查。

使用 Shield Advanced 執行運作狀態檢查時需要下列項目：

- 當您將其與 Shield Advanced 保護建立關聯時，運作狀態檢查必須報告良好。
- 運作狀態檢查必須與受保護資源的運作狀態相關。您有責任根據應用程式的特定需求，定義和維護可準確報告應用程式運作狀態的運作狀態檢查。
- 運作狀態檢查必須可供 Shield Advanced 保護使用。請勿在 Route 53 中刪除您用於 Shield Advanced 保護的運作狀態檢查。

內容

- [搭配 Shield Advanced 使用運作狀態檢查的最佳實務](#)
- [CloudWatch 指標通常用於使用 Shield Advanced 進行運作狀態檢查](#)
 - [用於監控應用程式運作狀態的指標](#)
 - [每個資源類型的 Amazon CloudWatch 指標](#)
- [將運作狀態檢查與 Shield Advanced 保護的資源建立關聯](#)
- [取消運作狀態檢查與 Shield Advanced 保護之資源的關聯](#)
- [在 Shield Advanced 中檢視運作狀態檢查關聯狀態](#)
- [Shield Advanced 的運作狀態檢查範例](#)

- [Amazon CloudFront 分佈](#)
- [負載平衡器](#)
- [Amazon EC2 彈性 IP 地址 \(EIP\)](#)

搭配 Shield Advanced 使用運作狀態檢查的最佳實務

當您使用 Shield Advanced 建立和使用運作狀態檢查時，請遵循本節中的最佳實務。

- 透過識別您要監控的基礎設施元件，規劃您的運作狀態檢查。請考慮下列運作狀態檢查的資源類型：
 - 關鍵資源。
 - 在 Shield Advanced 偵測和緩解中，您希望更高敏感度的任何資源。
 - 您希望 Shield Advanced 主動與您聯絡的資源。您的運作狀態檢查狀態會通知主動參與。

您可能想要監控的資源範例包括 Amazon CloudFront 分佈、面向網際網路的負載平衡器和 Amazon EC2 執行個體。

- 定義運作狀態檢查，以盡可能少的通知準確反映應用程式原始伺服器的運作狀態。
 - 撰寫運作狀態檢查，讓應用程式只在無法使用或未在可接受的參數內執行時運作狀態不佳。您有責任根據應用程式的特定需求來定義和維護運作狀態檢查。
 - 盡可能使用最少的運作狀態檢查，同時仍準確報告應用程式的運作狀態。例如，來自您應用程式多個區域的多個警示，這些警示都會報告相同的問題，可能會為您的回應活動增加額外負荷，而不會新增資訊值。
 - 使用計算的運作狀態檢查，使用 Amazon CloudWatch 指標的組合來監控應用程式的運作狀態。例如，您可以根據應用程式伺服器的延遲及其 5xx 錯誤率計算合併運作狀態，這表示原始伺服器未滿足請求。
 - 視需要建立並發佈您自己的應用程式運作狀態指標至 CloudWatch 自訂指標，並在計算的運作狀態檢查中使用它們。
- 實作和管理運作狀態檢查，以改善偵測並減少不必要的維護活動。
 - 將運作狀態檢查與 Shield Advanced 保護建立關聯之前，請確定運作狀態良好。關聯報告運作狀態不佳的運作狀態檢查可能會扭曲受保護資源的 Shield Advanced 偵測機制。
 - 讓運作狀態檢查可供 Shield Advanced 使用。請勿在 Route 53 中刪除您用於 Shield Advanced 保護的運作狀態檢查。
 - 僅使用預備和測試環境來測試運作狀態檢查。僅針對需要生產層級效能和可用性的環境維護運作狀態檢查關聯。請勿在 Shield Advanced 中維護預備和測試環境的運作狀態檢查關聯。

CloudWatch 指標通常用於使用 Shield Advanced 進行運作狀態檢查

本節列出在運作狀態檢查中常用的 Amazon CloudWatch 指標，以在分散式拒絕服務 (DDoS) 事件期間測量應用程式運作狀態。如需每個資源類型的 CloudWatch 指標的完整資訊，請參閱 資料表後面的清單。

主題

- [用於監控應用程式運作狀態的指標](#)
- [每個資源類型的 Amazon CloudWatch 指標](#)

用於監控應用程式運作狀態的指標

資源	指標	描述
Route 53	HealthCheckStatus	運作狀態檢查端點的狀態。
CloudFront	5xxErrorRate	HTTP 狀態碼為 5xx 的所有請求的百分比。這表示攻擊會影響應用程式。
Application Load Balancer	HTTPCode_ELB_5XX_Count	負載平衡器產生的 HTTP 5xx 用戶端錯誤碼數目。
Application Load Balancer	RejectedConnectionCount	因為負載平衡器達到其連線數上限而被拒絕的連線數。
Application Load Balancer	TargetConnectionErrorCount	負載平衡器與目標之間未成功建立的連線數目。
Application Load Balancer	TargetResponseTime	請求離開負載平衡器後經過的秒數，以及收到目標回應的時間。
Application Load Balancer	UnHealthyHostCount	視為不健康的目標數目。
Amazon EC2	CPUUtilization	目前正在使用的已配置 EC2 運算單位百分比。

每個資源類型的 Amazon CloudWatch 指標

如需受保護資源可用指標的詳細資訊，請參閱資源指南中的下列章節：

- Amazon Route 53 – Amazon [Route 53 開發人員指南中的使用 Amazon Route 53 運作狀態檢查和 Amazon CloudWatch 監控您的資源](#)。
- Amazon CloudFront – [Amazon CloudFront 開發人員指南中的使用 Amazon CloudWatch 監控 Amazon CloudFront](#)。
- Application Load Balancer – [Application Load Balancer 使用者指南中的 Application Load Balancer CloudWatch 指標](#)。
- Network Load Balancer – Network [Load Balancer 使用者指南中的 Network Load Balancer CloudWatch 指標](#)。
- AWS Global Accelerator – [在 開發人員指南中使用 Amazon CloudWatch 搭配 AWS Global Accelerator](#)。AWS Global Accelerator
- Amazon Elastic Compute Cloud – [在 `https://` 中列出執行個體可用的 CloudWatch 指標](#)。 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/>
- Amazon EC2 Auto Scaling – Amazon EC2 Auto Scaling 使用者指南中的[監控 Auto Scaling 群組和執行個體的 CloudWatch 指標](#)。

將運作狀態檢查與 Shield Advanced 保護的資源建立關聯

下列程序說明如何將 Amazon Route 53 運作狀態檢查與受保護的資源建立關聯。

Note

將運作狀態檢查與 Shield Advanced 保護建立關聯之前，請確定其處於運作狀態。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[監控運作狀態檢查狀態和取得通知](#)。

建立運作狀態檢查的關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護索引標籤上，選取要與運作狀態檢查建立關聯的資源。

4. 選擇設定保護。
5. 選擇下一步，直到您前往頁面 設定運作狀態檢查型 DDoS 偵測 - 選用。
6. 在 Associate Health Check (關聯運作狀態檢查) 下，選擇您要與保護產生關聯的運作狀態檢查 ID。

 Note

如果您沒有看到所需的運作狀態檢查，請前往 Route 53 主控台並驗證運作狀態檢查及其 ID。如需相關資訊，請參閱[建立和更新運作狀態檢查](#)。

7. 逐步瀏覽其餘頁面，直到您完成組態為止。在保護頁面上，會列出資源的更新運作狀態檢查關聯。
8. 在保護頁面上，檢查新關聯的運作狀態檢查報告是否正常運作。

當運作狀態檢查回報運作狀態不佳時，您無法在 Shield Advanced 中成功開始使用運作狀態檢查。這樣做會導致 Shield Advanced 在非常低的閾值下偵測誤報，並且也可能對 Shield Response Team (SRT) 為資源提供主動參與的能力產生負面影響。

如果新關聯的運作狀態檢查報告運作狀態不佳，請執行下列動作：

- a. 在 Shield Advanced 中取消運作狀態檢查與保護的關聯。
- b. 在 Amazon Route 53 中重新檢視運作狀態檢查規格，並驗證您的整體應用程式效能和可用性。
- c. 當您的應用程式在參數中執行以保持良好運作狀態，且運作狀態檢查報告良好時，請再試一次，將運作狀態檢查與 Shield Advanced 中的運作狀態檢查建立關聯。

當您建立新的運作狀態檢查關聯，並在 Shield Advanced 中報告運作狀態良好時，運作狀態檢查關聯程序即告完成。

取消運作狀態檢查與 Shield Advanced 保護之資源的關聯

下列程序說明如何取消 Amazon Route 53 運作狀態檢查與受保護資源的關聯。

取消與運作狀態檢查的關聯

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護索引標籤上，選取要與運作狀態檢查取消關聯的資源。

4. 選擇設定保護。
5. 選擇下一步，直到您前往頁面 設定運作狀態檢查型 DDoS 偵測 - 選用。
6. 在關聯的運作狀態檢查下，選擇空選項，列為 -。
7. 逐步瀏覽其餘頁面，直到您完成組態為止。

在保護頁面上，資源的運作狀態檢查欄位設定為 -，表示沒有運作狀態檢查關聯。

在 Shield Advanced 中檢視運作狀態檢查關聯狀態

您可以在 & Shield 主控台受保護資源頁面和每個資源的詳細資訊頁面上，查看與保護 AWS WAF 相關聯的運作狀態檢查狀態。

- 正常運作 – 運作狀態檢查已推出，且報告運作狀態良好。
- 運作狀態不佳 – 運作狀態檢查可用，且報告運作狀態不佳。
- 無法使用 – 運作狀態檢查不適用於 Shield Advanced。

解決無法使用的運作狀態檢查

建立和使用新的運作狀態檢查。在 Shield Advanced 中狀態為無法使用之後，請勿嘗試再次建立運作狀態檢查的關聯。

如需遵循這些步驟的詳細指引，請參閱上述主題。

1. 在 Shield Advanced 中，取消運作狀態檢查與資源的關聯。
2. 在 Route 53 中，為資源建立新的運作狀態檢查，並記下其 ID。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[建立和更新運作狀態檢查](#)。
3. 在 Shield Advanced 中，將新的運作狀態檢查與資源建立關聯。

Shield Advanced 的運作狀態檢查範例

本節顯示您可以在計算的運作狀態檢查中使用的運作狀態檢查範例。計算的運作狀態檢查會使用多個個別的運作狀態檢查來判斷合併狀態。每個個別運作狀態檢查的狀態取決於端點的運作狀態或 Amazon CloudWatch 指標的狀態。您可以將運作狀態檢查合併為計算的運作狀態檢查，然後設定計算的運作狀態檢查，根據個別運作狀態檢查的合併運作狀態來報告運作狀態。根據您的應用程式效能和可用性需求，調整所計算運作狀態檢查的敏感度。

如需計算運作狀態檢查的相關資訊，請參閱《Amazon Route 53 開發人員指南》中的[監控其他運作狀態檢查（計算的運作狀態檢查）](#)。如需詳細資訊，請參閱部落格文章[Route 53 改進 – 計算的運作狀態檢查和延遲檢查](#)。

主題

- [Amazon CloudFront 分佈](#)
- [負載平衡器](#)
- [Amazon EC2 彈性 IP 地址 \(EIP\)](#)

Amazon CloudFront 分佈

下列範例說明可以合併為 CloudFront 分佈的計算運作狀態檢查的運作狀態檢查：

- 透過指定提供動態內容之分佈上的路徑網域名稱來監控端點。運作狀態良好的回應會包含 HTTP 回應代碼 2xx 和 3xx。
- 監控 CloudWatch 警示的狀態，該警示正在測量 CloudFront 原始伺服器的運作狀態。例如，您可以在 Application Load Balancer 指標上維護 CloudWatch 警示 TargetResponseTime，並建立反映警示狀態的運作狀態檢查。當回應時間、請求離開負載平衡器和負載平衡器收到目標的回應之間，超過警示中設定的閾值時，運作狀態檢查可能運作不良。
- 監控 CloudWatch 警示的狀態，以測量回應的 HTTP 狀態碼為 5xx 的請求百分比。如果 CloudFront 分佈的 5xx 錯誤率高於 CloudWatch 警示中定義的閾值，則此運作狀態檢查的狀態將切換為運作狀態不佳。

負載平衡器

下列範例說明可用於 Application Load Balancer、Network Load Balancer 或 Global Accelerator 標準加速器計算的運作狀態檢查的運作狀態檢查。

- 監控 CloudWatch 警示的狀態，以測量用戶端與負載平衡器建立的新連線數。您可以設定高於每日平均值之某種程度上新連線平均數的警示閾值。每種資源類型的指標如下：
 - Application Load Balancer：NewConnectionCount
 - Network Load Balancer：ActiveFlowCount
 - Global Accelerator：NewFlowCount
- 對於 Application Load Balancer 和 Network Load Balancer，監控 CloudWatch 警示的狀態，該警示會測量被視為運作狀態良好的負載平衡器數量。您可以在可用區域或負載平衡器所需的運作狀態良好的主機數量下限上設定警示閾值。負載平衡器資源的可用指標如下所示：

- Application Load Balancer : HealthyHostCount
- Network Load Balancer : HealthyHostCount
- 對於 Application Load Balancer，監控 CloudWatch 警示的狀態，該警示會測量負載平衡器目標產生的 HTTP 5xx 回應碼數目。對於 Application Load Balancer，您可以使用指標，HTTPCode_Target_5XX_Count並根據負載平衡器所有 5xx 錯誤的總和來建立警示閾值。

Amazon EC2 彈性 IP 地址 (EIP)

下列範例運作狀態檢查可以合併為 Amazon EC2 彈性 IP 地址的計算運作狀態檢查：

- 透過指定彈性 IP 地址來監控端點。只要可以使用 IP 地址後方的資源建立 TCP 連線，運作狀態檢查就會保持正常運作。
- 監控 CloudWatch 警示的狀態，該警示會測量目前執行個體上使用的已配置 Amazon EC2 運算單位百分比。您可以使用 Amazon EC2 指標，CPUUtilization並根據您認為應用程式具有高 CPU 使用率的警示閾值，例如 90%。

將 AWS Shield Advanced 保護新增至 AWS 資源

遵循本節中的指引，將 Shield Advanced 保護新增至一或多個資源。

新增 AWS 資源的保護

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在導覽窗格中，AWS Shield 選擇受保護的資源。
3. 選擇新增要保護的資源。
4. 在使用 Shield Advanced 選擇要保護的資源頁面中，在指定區域和資源類型中，為您要保護的資源提供區域和資源類型規格。您可以選取所有區域來保護多個區域中的資源，也可以選取全域，將選取範圍縮小至全域資源。您可以取消選取您不想保護的任何資源類型。如需資源類型的保護資訊，請參閱 [AWS Shield Advanced 保護的資源清單](#)。
5. 選擇載入資源。Shield Advanced 會將符合您條件的資源填入選取資源區段 AWS。
6. 在選取資源區段中，您可以輸入要在資源清單中搜尋的字串來篩選資源清單。

選取您要保護的資源。
7. 在標籤區段中，如果您想要將標籤新增至您正在建立的 Shield Advanced 保護，請指定這些保護。如需標記 AWS 資源的相關資訊，請參閱[使用標籤編輯器](#)。

8. 選擇使用 Shield Advanced 保護。這會將 Shield Advanced 保護新增至資源。

編輯 AWS Shield Advanced 保護

您可以隨時變更 AWS Shield Advanced 保護的設定。若要執行此操作，請逐步解說所選保護的選項，並修改您需要變更的設定。

管理受保護的資源

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護索引標籤中，選取您要保護的資源。
4. 選擇設定保護和資源規格選項。
5. 逐步解說每個資源保護選項，並視需要進行變更。

設定應用程式層 DDoS 保護

為了防止 Amazon CloudFront 和 Application Load Balancer 資源受到攻擊，您可以新增 AWS WAF Web ACLs 和以速率為基礎的規則。如需相關資訊，請參閱 [使用 AWS WAF Web ACLs 和 Shield Advanced 保護應用程式層](#)。

您也可以啟用 Shield Advanced 自動應用程式層 DDoS 緩解。如需如何 AWS WAF 運作的詳細資訊，請參閱 [AWS WAF](#)。如需自動緩解功能的資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

Important

如果您 AWS Firewall Manager 使用 Shield Advanced 政策來管理 Shield Advanced 保護，則無法在此處管理應用程式層保護。對於所有其他資源，我們建議您至少將 Web ACL 連接到每個資源，即使 Web ACL 不包含任何規則。

 Note

當您為資源啟用自動應用程式層 DDoS 緩解時，操作會自動將服務連結角色新增至您的帳戶，為 Shield Advanced 提供管理 Web ACL 保護所需的許可。如需相關資訊，請參閱 [使用 Shield Advanced 的服務連結角色](#)。

設定應用程式層 DDoS 保護

1. 在設定第 7 層 DDoS 保護頁面中，如果資源尚未與 Web ACL 建立關聯，您可以選擇現有的 Web ACL 或建立您自己的 ACL。

若要建立 Web ACL，請執行下列步驟：

- a. 選擇 建立 Web ACL。
- b. 輸入名稱。建立 Web ACL 後無法修改名稱。
- c. 選擇 Create (建立)。

 Note

如果資源已與 Web ACL 關聯，您無法變更為不同的 Web ACL。如果您想要變更 Web ACL，您必須先從資源移除關聯的 Web ACL。如需詳細資訊，請參閱 [將保護與 AWS 資源建立關聯或取消關聯](#)。

2. 如果 Web ACL 未定義以速率為基礎的規則，您可以選擇新增速率限制規則，然後執行下列步驟來新增規則：
 - a. 輸入名稱。
 - b. 輸入速率限制。這是套用以速率為基礎的規則動作到 IP 地址之前，任何 5 分鐘內從任何單一 IP 地址允許的請求數量上限。當來自 IP 地址的請求低於限制時，動作會停止。
 - c. 設定規則動作，在 IP 地址的請求計數超過限制時計數或封鎖請求。應用程式和移除規則動作可能會在 IP 地址請求率變更後一兩分鐘生效。
 - d. 選擇新增規則。
3. 對於自動應用程式層 DDoS 緩解，選擇您是否希望 Shield Advanced 代表您自動緩解 DDoS 攻擊，如下所示：

- 若要啟用自動緩解，請選擇啟用，然後選擇您希望 Shield Advanced 在其自訂 AWS WAF 規則中使用的規則動作。您的選擇是 Count 和 Block。如需這些 AWS WAF 規則動作的詳細資訊，請參閱 [在中使用規則動作 AWS WAF](#)。如需有關 Shield Advanced 如何管理此動作設定的資訊，請參閱 [Shield Advanced 如何管理規則動作設定](#)。
- 若要停用自動緩解，請選擇停用。
- 若要為您管理的資源保持自動緩解設定不變，請保留預設選擇保持目前的設定。

如需有關 Shield Advanced 自動應用程式層 DDoS 緩解的資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

4. 選擇 Next (下一步)。

為 Shield Advanced 保護的資源建立警示和通知

下列程序說明如何管理受保護資源的 CloudWatch 警示。

Note

CloudWatch 會產生額外費用。如需 CloudWatch 定價，請參閱 [Amazon CloudWatch 定價](#)。

建立警示和通知

1. 在保護頁面建立警示和通知 - 選用，為您要接收的警示和通知設定 SNS 主題。對於您不想收到通知的資源，請選擇 No topic (無主題)。您可以新增 Amazon SNS 主題或建立新的主題。
2. 若要建立 Amazon SNS 主題，請遵循下列步驟：
 - a. 在下拉式清單中，選擇建立 SNS 主題。
 - b. 輸入主題名稱。
 - c. 選擇性地輸入 Amazon SNS 訊息將傳送至的電子郵件地址，然後選擇新增電子郵件。您可以輸入多個。
 - d. 選擇 Create (建立)。
3. 選擇 Next (下一步)。

從 AWS 資源移除 AWS Shield Advanced 保護

您可以隨時移除任何 AWS 資源的 AWS Shield Advanced 保護。

Important

刪除 AWS 資源不會從中移除資源 AWS Shield Advanced。您也必須移除資源的保護 AWS Shield Advanced，如此程序所述。

從 AWS 資源移除 AWS Shield Advanced 保護

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護索引標籤中，選取您要移除其保護的資源。
4. 選擇刪除保護。
 - 如果您為保護設定 Amazon CloudWatch 警示，您可以選擇刪除警示以及保護。如果您選擇此時不刪除警示，則可以稍後使用 CloudWatch 主控台將其刪除。

Note

對於已設定 Amazon Route 53 運作狀態檢查的保護，如果您稍後再次新增保護，則保護仍然包含運作狀態檢查。

上述步驟會移除對特定 AWS 資源的 AWS Shield Advanced 保護。他們不會取消您的 AWS Shield Advanced 訂閱。您將繼續支付該服務的費用。如需 AWS Shield Advanced 訂閱的相關資訊，請聯絡 [AWS 支援中心](#)。

從 Shield Advanced 保護中移除 CloudWatch 警示

若要從 Shield Advanced 保護中移除 CloudWatch 警示，請執行下列其中一項操作：

- 刪除 [從 AWS 資源移除 AWS Shield Advanced 保護](#) 所述的保護。請確實選取 Also delete related DDoSDetection alarm (同時刪除相關 DDoSDetection 警示) 旁的核取方塊。
- 使用 CloudWatch 主控台刪除警示。要刪除的警示名稱開頭為 DDoSDetectedAlarmForProtection。

分組您的 AWS Shield Advanced 保護

使用保護群組來建立受保護資源的邏輯集合，並以群組的形式管理其保護。如需管理資源保護的資訊，請參閱 [編輯 AWS Shield Advanced 保護](#)。

Note

自動應用程式層 DDoS 緩解不會與保護群組互動。您可以為保護群組中的資源啟用自動緩解，但 Shield Advanced 不會根據保護群組調查結果自動套用攻擊緩解。Shield Advanced 會將自動攻擊緩解措施套用至個別資源。

AWS Shield Advanced 保護群組可讓您透過將多個受保護資源視為單一單位，以自助方式自訂偵測和緩解的範圍。資源分組可以提供許多好處。

- 改善偵測的準確性。
- 減少無法操作的事件通知。
- 增加緩解動作的涵蓋範圍，以包含也可能在事件期間受到影響的受保護資源。
- 加快緩解具有多個類似目標的攻擊的時間。
- 協助自動保護新建立的受保護資源。

保護群組有助於在藍/綠交換等情況下減少誤報，其中資源在接近零負載和完全載入之間交替。另一個範例是，當您經常建立和刪除資源，同時維護在群組成員之間共用的負載層級時。對於這類情況，監控個別資源可能會導致誤報，同時監控資源群組的運作狀態則不會。

您可以設定保護群組，以包含所有受保護的資源、特定資源類型的所有資源，或個別指定的資源。符合您保護群組條件的新受保護資源會自動包含在保護群組中。受保護的資源可以屬於多個保護群組。

建立 Shield Advanced 保護群組

建立保護群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 選擇保護群組索引標籤，然後選擇建立保護群組。

4. 在建立保護群組頁面中，為您的群組提供名稱。您將使用此名稱來識別受保護資源清單中的群組。您無法在建立保護群組之後變更保護群組的名稱。
5. 針對保護群組條件，選取您希望 Shield Advanced 用來識別要包含在群組中受保護資源的條件。根據您選擇的條件進行其他選擇。
6. 針對彙總，選取您希望 Shield Advanced 如何合併群組的資源資料，以偵測、緩解和報告事件。
 - 總和 – 使用跨群組的總流量。對於大多數案例來說，這是不錯的選擇。範例包括手動或自動擴展 Amazon EC2 執行個體的彈性 IP 地址。
 - 平均值 – 使用整個群組的流量平均值。對於統一共用流量的資源而言，這是很好的選擇。範例包括加速器和負載平衡器。
 - Max – 使用來自每個資源的最高流量。這對於不共用流量的資源，以及以不均勻的方式共用流量的資源非常有用。範例包括 Amazon CloudFront CloudFront 分佈和原始資源。
7. 選擇儲存以儲存您的保護群組，並返回受保護的資源頁面。

在 Shield Events 頁面中，您可以檢視保護群組的事件，並向下切入以查看群組中受保護資源的其他資訊。

更新 Shield Advanced 保護群組

更新保護群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。
3. 在保護群組索引標籤中，選取您要修改的保護群組旁的核取方塊。
4. 在保護群組的頁面中，選擇編輯。對保護群組設定進行變更。
5. 選擇儲存，以儲存變更。

刪除 Shield Advanced 保護群組

刪除保護群組

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇受保護的資源。

3. 在保護群組索引標籤中，選取您要移除的保護群組旁的核取方塊。
4. 在保護群組的頁面中，選擇刪除並確認動作。

中的追蹤 Shield Advanced 資源保護變更 AWS Config

此頁面說明如何記錄對使用 AWS Shield Advanced 保護資源的變更 AWS Config。然後，您可以使用這些資訊來維護組態變更歷史記錄，稽核和排除故障問題。

若要記錄保護變更，AWS Config 請針對您要追蹤的每個資源啟用。如需詳細資訊，請參閱《AWS Config 開發人員指南》中的[開始使用 AWS Config](#)。

您必須 AWS Config 針對每個包含追蹤資源 AWS 區域的啟用。您可以 AWS Config 手動啟用，也可以使用 AWS CloudFormation 使用者指南中的 StackSets 範本的 AWS CloudFormation 「啟用 AWS Config」範本。[AWS CloudFormation StackSets](#)

如果您啟用 AWS Config，則會按[AWS Config 定價](#)頁面中詳述的方式向您收費。

Note

如果您已針對必要的區域和資源 AWS Config 啟用，則不需要執行任何動作。有關資源保護變更的 AWS Config 日誌會自動開始填入。

啟用後 AWS Config，請在 AWS Config 主控台中使用美國東部（維吉尼亞北部）區域來檢視 AWS Shield Advanced 全域資源的組態變更歷史記錄。

透過美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（奧勒岡）、美國西部（加利福尼亞北部）、歐洲（愛爾蘭）、歐洲（法蘭克福）、亞太區域（東京）和亞太區域（雪梨）區域的 AWS Config 主控台檢視 AWS Shield Advanced 區域資源的變更歷史記錄。

使用 Shield Advanced 的 DDoS 事件可見性

AWS Shield 提供下列類別的事件和事件活動的可見性：

- 全域 – 所有客戶都可以存取過去兩週內全域威脅活動的彙總檢視。您可以在 AWS Shield 主控台的入門和全球威脅儀表板頁面下查看此資訊。如需詳細資訊，請參閱[檢視 AWS Shield 全域和帳戶活動](#)。
- 帳戶 – 所有客戶都可以存取其帳戶上一年的事件摘要。您可以在 AWS Shield 主控台的入門頁面下查看此資訊。如需詳細資訊，請參閱[檢視 AWS Shield 全域和帳戶活動](#)。

當您訂閱 Shield Advanced 並為您的資源新增保護時，您可以存取有關受保護資源的事件和 DDoS 攻擊的其他資訊：

- 受保護資源上的事件 – Shield Advanced 透過 AWS Shield 主控台的事件頁面提供每個事件的詳細資訊。如需詳細資訊，請參閱[檢視 AWS Shield Advanced 事件](#)。
- 受保護資源的事件指標 – Shield Advanced 會針對其保護的所有資源發佈偵測、緩解和最大貢獻者 Amazon CloudWatch 指標。您可以使用這些指標來設定 CloudWatch 儀表板和警示。如需詳細資訊，請參閱[AWS Shield Advanced 指標](#)。
- 受保護資源的跨帳戶事件可見性 – 如果您使用 AWS Firewall Manager 來管理 Shield Advanced 保護，您可以使用 Firewall Manager 與 結合，以啟用跨多個帳戶的保護可見性 AWS Security Hub。如需詳細資訊，請參閱[AWS 帳戶使用 AWS Firewall Manager 和 檢視多個的 Shield Advanced 事件 AWS Security Hub](#)。

如果您為應用程式層保護啟用自動應用程式層 DDoS 緩解，Shield Advanced 會將規則群組新增至您的保護套件或 Web ACL，以用於管理自動化保護。此規則群組會產生 AWS WAF 指標，但無法檢視。這與您在保護套件或 Web ACL 中使用的任何其他規則群組相同，但不擁有，例如 AWS 受管規則規則群組。如需 AWS WAF 指標的詳細資訊，請參閱[AWS WAF 指標和維度](#)。如需此 Shield Advanced 保護選項的詳細資訊，請參閱[使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

主題

- [檢視 AWS Shield 全域和帳戶活動](#)
- [檢視 AWS Shield Advanced 事件](#)
- [AWS 帳戶使用 AWS Firewall Manager 和 檢視多個的 Shield Advanced 事件 AWS Security Hub](#)

檢視 AWS Shield 全域和帳戶活動

此頁面提供在 AWS Shield 主控台入門和全球威脅儀表板頁面中存取全域威脅活動彙總檢視和每個帳戶事件摘要的說明。

下列螢幕擷取畫面顯示範例入門頁面。

Security, Identity, and Compliance

AWS Shield

Managed DDoS protection service.

AWS Shield provides continuous attack detection and automatic mitigations. AWS Shield offers two tiers of protection - Standard and Advanced.

Get started with Shield Advanced

Subscribe and add resources that you want to protect with Shield Advanced.

[Add resources to protect](#)

Pricing (US)

Monthly \$3000 / month

Additional data transfer fees apply

[View pricing](#)

More resources

[Documentation](#)

[API reference](#)

[FAQs](#)

[Support forums](#)

Global activity detected by AWS Shield

The following is a summary of events detected by AWS Shield across all applications running on AWS. With AWS Shield Advanced, you also receive a dashboard that's specific to your applications.



Last two weeks summary

Largest packet attack	188 Mpps
Largest bit rate	428 Gbps
Most common vector	Volumetric
Threat level	Normal
Total number of attacks	41,990

Account activity detected by AWS Shield

Events summary in past year

Values are for interval 2019-10-27T00:00 UTC to 2020-10-27T00:00 UTC. The statistics refer to all of your resources that are supported by AWS Shield, both protected and unprotected.

8	45.2 Gbps	15.5 Mpps	1.2 krps
Total events	Largest bit rate	Largest packet rate	Largest request rate

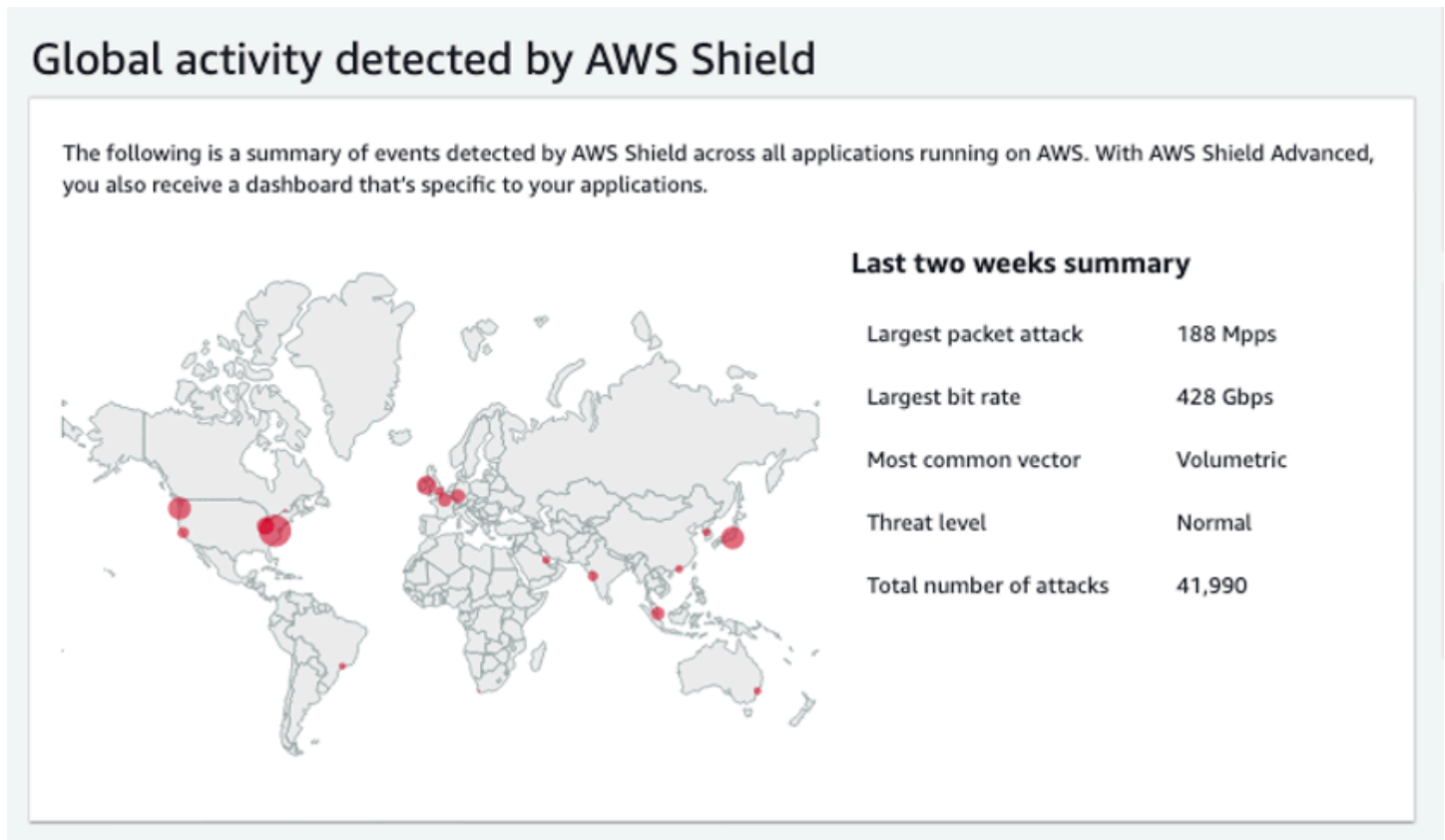
存取 AWS Shield 主控台

- 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。

您不需要訂閱 Shield Advanced 即可存取全域活動和帳戶事件摘要資訊。

全域活動

此資訊可透過 AWS Shield 主控台全域威脅儀表板和入門頁面取得。下列螢幕擷取畫面顯示全域活動窗格的範例。



全域活動描述所有 AWS 客戶觀察到的 DDoS 事件。每小時更新一次前兩週 AWS 的資訊。在主控台窗格中，您可以看到結果，依 AWS 區域分割，並顯示在世界熱度圖上。在地圖旁邊，Shield 會顯示摘要資訊，例如最大封包攻擊、最大位元速率、最常見的向量、攻擊總數和威脅層級。威脅層級是與一般觀察相比 AWS，目前全域活動的評估。預設的威脅層級值為「正常」。AWS 會自動將值更新為「高」，以增加 DDoS 活動。

全球威脅儀表板也提供時間序列指標，並可讓您在時間持續時間之間進行變更。若要檢視重大 DDoS 攻擊的歷史記錄，您可以自訂儀表板以取得從最後一天到過去兩週的檢視。時間序列指標可讓您檢視所選時段 AWS 內在 上執行之 AWS Shield 應用程式偵測到的所有事件的最大位元速率、封包速率或請求速率。

帳戶活動

此資訊可在 AWS Shield 主控台入門頁面取得。

下列螢幕擷取畫面顯示帳戶活動窗格的範例。

Account activity detected by AWS Shield

Events summary in past year

Values are for interval 2019-10-27T00:00 UTC to 2020-10-27T00:00 UTC. The statistics refer to all of your resources that are supported by AWS Shield, both protected and unprotected.

8

Total events

45.2 Gbps

Largest bit rate

15.5 Mpps

Largest packet rate

1.2 krps

Largest request rate

帳戶活動描述 Shield 偵測到的資源符合 Shield Advanced 保護資格的 DDoS 事件。每天，Shield 都會建立前一天 UTC 00:00 結束之年份的摘要指標，然後顯示總事件、最大位元速率、最大封包速率和最大請求速率。

- 總事件指標會在每次 Shield 在目的地為應用程式的流量中觀察到可疑屬性時反映。可疑屬性可以包括高於正常磁碟區的流量、不符合應用程式歷史描述檔的流量，或不符合 Shield 為有效應用程式流量定義的啟發式的流量。
- 每個資源都有可用的最大位元速率和最大封包速率統計資料。
- 最大的請求率統計資料僅適用於具有相關聯 AWS WAF Web ACL 的 Amazon CloudFront 分佈和 Application Load Balancer。

Note

您也可以透過 AWS Shield API 操作 [DescribeAttackStatistics](#) 存取帳戶層級事件摘要。

檢視 AWS Shield Advanced 事件

此頁面提供存取 Shield Advanced 中事件相關資訊的說明。

當您訂閱 Shield Advanced 並保護您的資源時，您可以存取資源的其他可見性功能。這包括 Shield Advanced 偵測到的事件近乎即時的通知，以及偵測到的事件和緩解措施的其他資訊。

Note

Shield Advanced 主控台的事件資訊是以 Shield Advanced 指標為基礎。如需 Shield Advanced 指標的詳細資訊，請參閱 [AWS Shield Advanced 指標](#)

AWS Shield 會沿著多個維度評估到受保護資源的流量。偵測到異常時，Shield Advanced 會為每個受影響的資源建立個別的事件。

您可以透過 Shield 主控台的事件頁面存取事件摘要和詳細資訊。最上層事件頁面提供目前和過去事件的概觀。

下列螢幕擷取畫面顯示具有單一進行中事件的範例事件頁面。此作用中事件也會在左側導覽窗格中標記。

The screenshot shows the AWS Shield console interface. On the left is a navigation pane with 'WAF & Shield' selected. Under 'AWS Shield', the 'Events' link is highlighted with a red notification badge showing '1'. The main content area is titled 'Shield > Events'. It contains a section 'Events' with a message: 'The following are the events detected by AWS Shield Advanced. For assistance mitigating current events [contact the AWS DDoS Response Team](#).' Below this is a table with one event.

AWS resource	Current status	Attack vectors	Start time	Duration
E1 - Cloudfront distribution	Mitigation in-progress	UDP traffic	Sep 16th 2020, 2:43:00 pm SAST	6 minutes

Shield Advanced 也可能自動根據流量類型和您設定的保護，對攻擊進行緩解。這些緩解措施可以保護您的資源免於接收過多流量或符合已知 DDoS 攻擊簽章的流量。

下列螢幕擷取畫面顯示範例事件清單，其中所有事件都已由 Shield Advanced 緩解或自行消除。

The screenshot shows the AWS Shield console 'Events' page. It includes a search bar and a table listing several past events. All events are marked as 'Identified (subsided)' or 'Mitigated'.

AWS resource	Current status	Attack vectors	Start time	Duration
- Application load balancer	Identified (subsided)	Request flood	Apr 12th 2022, 8:17:00 am PDT	11 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 11th 2022, 9:58:00 pm PDT	8 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 11th 2022, 7:11:00 pm PDT	12 minutes
- Application load balancer	Identified (subsided)	Request flood	Apr 8th 2022, 11:04:00 am PDT	43 minutes
- Protection group	Identified (subsided)	Request flood	Nov 29th 2021, 5:27:00 pm PST	an hour
Cloudfront distribution	Identified (subsided)	Request flood	Nov 29th 2021, 5:26:00 pm PST	an hour
Protection group	Identified (subsided)	Request flood	Nov 29th 2021, 10:38:00 am PST	33 minutes
Cloudfront distribution	Identified (subsided)	Request flood	Nov 29th 2021, 10:37:00 am PST	33 minutes
- Cloudfront distribution	Mitigated	SYN flood	Sep 15th 2021, 3:00:00 am PDT	13 hours

在事件發生之前保護您的資源

在 Shield Advanced 接收到正常預期流量時，在受到 DDoS 攻擊之前，透過保護資源來提高事件偵測的準確性。

為了準確報告受保護資源的事件，Shield Advanced 必須先為其建立預期的流量模式基準。

- Shield Advanced 會在資源受到保護至少 15 分鐘後報告資源的基礎設施層事件。
- Shield Advanced 會在資源受到保護至少 24 小時後報告資源的 Web 應用程式層事件。在 Shield Advanced 觀察到預期的流量 30 天後，偵測應用程式層事件的準確性是最佳的。

在 AWS Shield 主控台中存取事件資訊

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/wafv2/> 開啟 AWS WAF & Shield 主控台。
2. 在 AWS Shield 導覽窗格中，選擇事件。主控台會顯示事件頁面。
3. 從事件頁面，您可以選取清單中的任何事件，以查看事件的其他摘要資訊和詳細資訊。

主題

- [AWS Shield Advanced 事件摘要中的欄位清單](#)
- [檢視 AWS Shield Advanced 事件詳細資訊](#)

AWS Shield Advanced 事件摘要中的欄位清單

此頁面列出並定義 Shield Advanced 事件摘要中的欄位。

您可以在事件主控台頁面中檢視事件的摘要和詳細資訊。若要開啟事件的頁面，請從事件頁面清單中選取其 AWS 資源名稱。

下列螢幕擷取畫面顯示網路層事件的範例事件摘要。

Shield > Events > [redacted]

Event summary

AWS resource arn:aws:cloudfront::[redacted]:distribution/[redacted] [redacted]	Protection FMManagedShieldProtection [redacted]
Attack vectors UDP traffic	Automatic application layer DDoS mitigation Not applicable
Start time Jan 13th 2022, 2:06:00 am PST	Network layer automatic mitigation ✔ Enabled
End time Jan 13th 2022, 2:11:00 am PST	Status ✔ Mitigated

事件頁面摘要資訊包括下列項目。

- **目前狀態** – 指出事件狀態的值，以及 Shield Advanced 已對事件採取的動作。狀態值適用於基礎設施層（第 3 層或第 4 層）和應用程式層（第 7 層）事件。
- **已識別（進行中）和已識別（下尾）** – 這表示 Shield Advanced 偵測到事件，但目前為止尚未對其採取任何動作。已識別（底）表示 Shield 偵測到的可疑流量已停止，無需介入。
- **緩解進行中和緩解中** – 這些指示 Shield Advanced 偵測到事件並對其採取動作。當目標資源是 Amazon CloudFront 分佈或 Amazon Route 53 託管區域時，也會使用緩解，這些區域具有自己的自動內嵌緩解措施。
- **攻擊向量** – TCP SYN 洪水和請求洪水等 Shield Advanced 偵測啟發式等 DDoS 攻擊向量。這些可能是 DDoS 攻擊的指標。
- **開始時間** – 偵測到第一個異常流量資料點的日期和時間。
- **持續時間或結束時間** – 指示事件開始時間與 Shield Advanced 觀察到的上次觀察到的異常資料點之間經過的時間。當事件持續進行時，這些值會繼續增加。
- **保護** – 命名與資源相關聯的 Shield Advanced 保護，並提供其保護頁面的連結。這可在個別事件的頁面中使用。
- **自動應用程式層 DDoS 緩解** – 用於應用程式層保護，以指出是否針對資源啟用 Shield Advanced 自動應用程式層 DDoS 緩解。如果已啟用，這會提供存取和管理組態的連結。這可在個別事件的頁面中使用。

- 網路層自動緩解 – 指出資源是否在網路層具有自動緩解。如果資源具有網路層元件，則會啟用此功能。此資訊可在個別事件的頁面取得。

對於經常成為目標的資源，Shield 可能會在減少過多流量後保留緩解措施，以防止進一步的重複事件。

Note

您也可以透過 AWS Shield API 操作 [ListAttacks](#) 存取受保護資源的事件摘要。

檢視 AWS Shield Advanced 事件詳細資訊

您可以在 主控台頁面底部區段中，查看事件偵測、緩解和最大參與者的詳細資訊。本節可以包含合法和可能不需要的流量，並可能同時代表傳送到受保護資源的流量，以及 Shield 緩解機制封鎖的流量。

- 偵測和緩解 – 提供有關觀察到的事件和對其套用的任何緩解的資訊。如需事件緩解的資訊，請參閱 [在中回應 DDoS 事件 AWS](#)。
- 最大貢獻者 – 將事件中涉及的流量分類，並列出 Shield 已為每個類別識別的主要流量來源。對於應用程式層事件，請使用主要參與者資訊來取得事件性質的一般概念，但請使用 AWS WAF 日誌進行安全決策。如需詳細資訊，請參閱以下各節。

Shield Advanced 主控台的事件資訊是以 Shield Advanced 指標為基礎。如需 Shield Advanced 指標的相關資訊，請參閱 [AWS Shield Advanced 指標](#)

Amazon CloudFront 或 Amazon Route 53 資源不包含緩解指標，因為這些服務受到一律啟用的緩解系統保護，且個別資源不需要緩解。

詳細資訊區段會根據資訊是用於基礎設施層或應用程式層事件而有所不同。

主題

- [在 Shield Advanced 中檢視應用程式層（第 7 層）事件詳細資訊](#)
- [在 Shield Advanced 中檢視基礎設施層（第 3 層或第 4 層）事件詳細資訊](#)

在 Shield Advanced 中檢視應用程式層（第 7 層）事件詳細資訊

您可以在主控台頁面底部查看應用程式層事件偵測、緩解和最大貢獻者的詳細資訊。本節可以包含合法和可能不需要的流量組合，並可能代表傳送到受保護資源的流量，以及 Shield Advanced 緩解措施封鎖的流量。

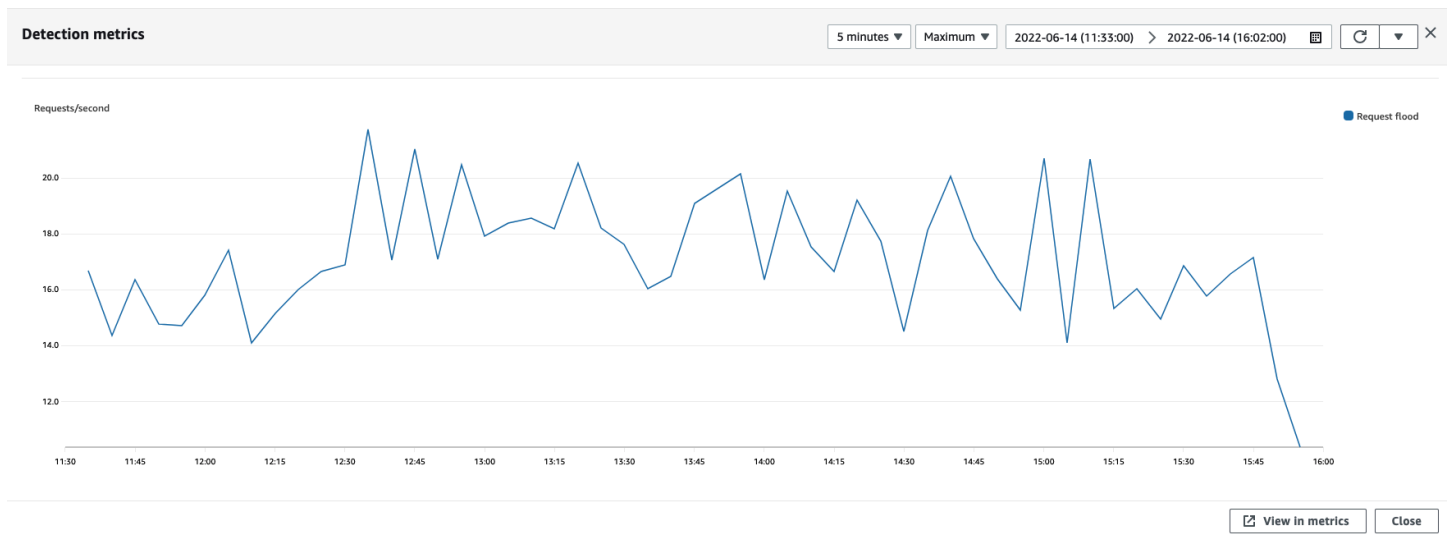
緩解詳細資訊適用於 Web ACL 中與資源相關聯的任何規則，包括專門為回應攻擊而部署的規則，以及 Web ACL 中定義的以速率為基礎的規則。如果您為應用程式啟用自動應用程式層 DDoS 緩解，緩解指標會包含這些額外規則的指標。如需這些應用程式層保護的相關資訊，請參閱[使用 AWS Shield Advanced 和 保護應用程式層（第 7 層）AWS WAF](#)。

偵測和緩解

對於應用程式層（第 7 層）事件，偵測和緩解索引標籤會顯示以從 AWS WAF 日誌取得的資訊為基礎的偵測指標。緩解指標是根據相關聯 Web ACL 中的 AWS WAF 規則，這些規則設定為封鎖不需要的流量。

對於 Amazon CloudFront 分佈，您可以設定 Shield Advanced 來為您套用自動緩解。透過任何應用程式層資源，您可以選擇在 Web ACL 中定義自己的緩解規則，也可以向 Shield Response Team (SRT) 請求協助。如需這些選項的資訊，請參閱[在中回應 DDoS 事件 AWS](#)。

下列螢幕擷取畫面顯示應用程式層事件的偵測指標範例，這些事件會在數小時後消失。



緩解規則生效之前所隱藏的事件流量不會在緩解指標中表示。這可能會導致偵測圖表中顯示的 Web 請求流量與緩解圖表中顯示的允許和封鎖指標之間的差異。

排名前茅的貢獻者

應用程式層事件的前 5 個貢獻者索引標籤會根據 Shield 擷取的 AWS WAF 日誌，顯示 Shield 為事件識別的前 5 個貢獻者。Shield 會依來源 IP、來源國家/地區和目的地 URL 等維度來分類主要參與者資訊。

Note

如需導致應用程式層事件之流量的最準確資訊，請使用 AWS WAF 日誌。

使用 Shield 應用程式層最大參與者資訊，只是為了取得攻擊性質的一般概念，而不是根據其做出的安全決策。對於應用程式層事件，AWS WAF 日誌是了解攻擊參與者和制定緩解策略的最佳資訊來源。

Shield 最大參與者資訊不一定完全反映 AWS WAF 日誌中的資料。擷取日誌時，Shield 會優先減少對系統效能的影響，而不是從日誌擷取完整的資料集。這可能會導致 Shield 可用於分析的資料中失去精細度。在大多數情況下，大多數資訊都是可用的，但最主要貢獻者資料可能會因為任何攻擊而偏移到某種程度。

下列螢幕擷取畫面顯示應用程式層事件的 Top contributors 索引標籤範例。

Detection and mitigation			Top contributors		
Application			Network		
Top 5 source IP addresses			Top 5 source countries		
Source IP	Total requests	Percentage of traffic	Source country	Total requests	Percentage of traffic
34.203.230.194	4392300	65.42%	US	6714171	100.00%
23.22.196.86	1282506	19.10%			
3.83.54.134	1039365	15.48%			
Top 5 destination URLs			Top 5 user agents		
Destination URL	Total requests	Percentage of traffic	Source user agent		
/	4425825	65.92%	Mozilla/5.0 (Macintosh; Intel Mac OS X 12_0_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15		
/[REDACTED].js	397737	5.92%	python/gevent-http-client-1.5.3		
/styles.css	381830	5.69%			
/runtime/[REDACTED].js	378136	5.63%			
/assets/public/images/[REDACTED].jpg	202612	3.02%			

貢獻者資訊是根據對合法和可能不需要的流量的請求。較大的磁碟區事件，以及請求來源未高度分佈的事件，更有可能具有可識別的首要參與者。顯著分佈的攻擊可能具有任意數量的來源，因此很難識別攻擊的主要原因。如果 Shield Advanced 無法識別特定類別的重要參與者，則會將資料顯示為無法使用。

在 Shield Advanced 中檢視基礎設施層（第 3 層或第 4 層）事件詳細資訊

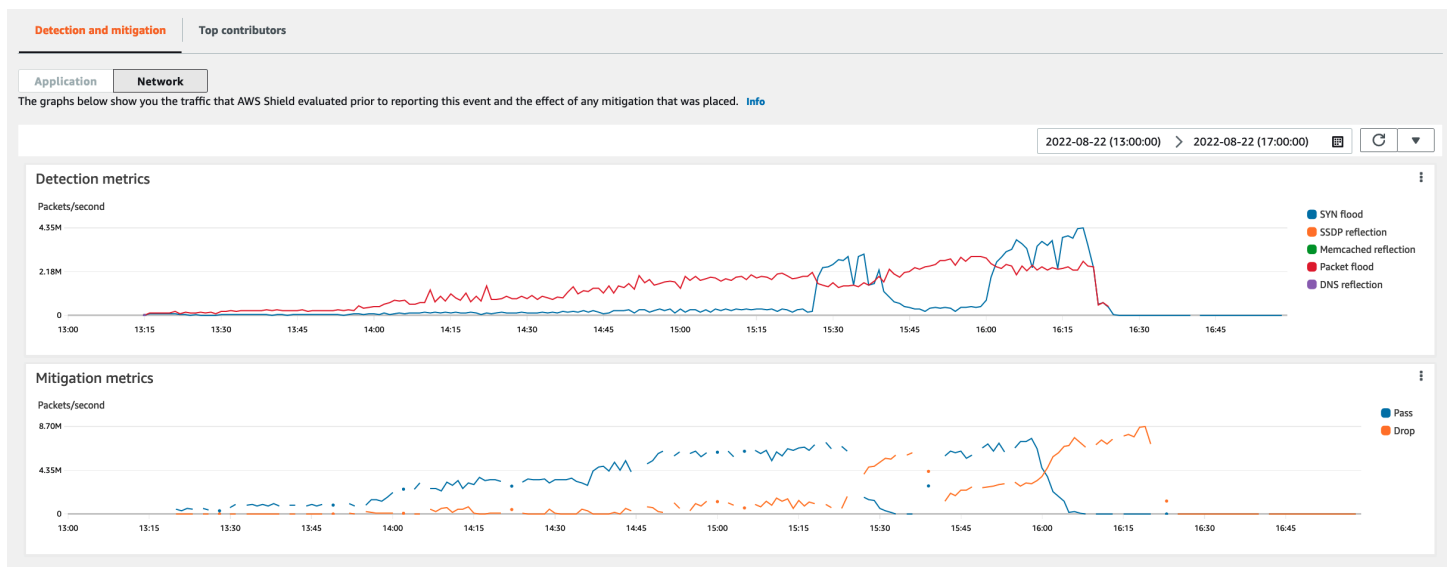
您可以在 主控台頁面底部區段中，查看有關基礎設施層事件偵測、緩解和最大貢獻者的詳細資訊。本節可以包含合法和可能不需要的流量組合，並可能代表傳送到受保護資源的流量，以及 Shield 緩解機制封鎖的流量。

偵測和緩解

對於基礎設施層（第 3 層或第 4 層）事件，偵測和緩解索引標籤會顯示以抽樣網路流程為基礎的偵測指標，以及以緩解系統觀察到的流量為基礎的緩解指標。緩解指標是更精確地測量傳入資源的流量。

Shield 會自動為受保護的資源類型 Elastic IP (EIP)、Classic Load Balancer (CLB)、Application Load Balancer (ALB) 和 AWS Global Accelerator 標準加速器建立緩解措施。EIP 地址和 AWS Global Accelerator 標準加速器的緩解指標表示傳遞和捨棄的封包數量。

下列螢幕擷取畫面顯示基礎設施層事件的範例偵測和緩解索引標籤。

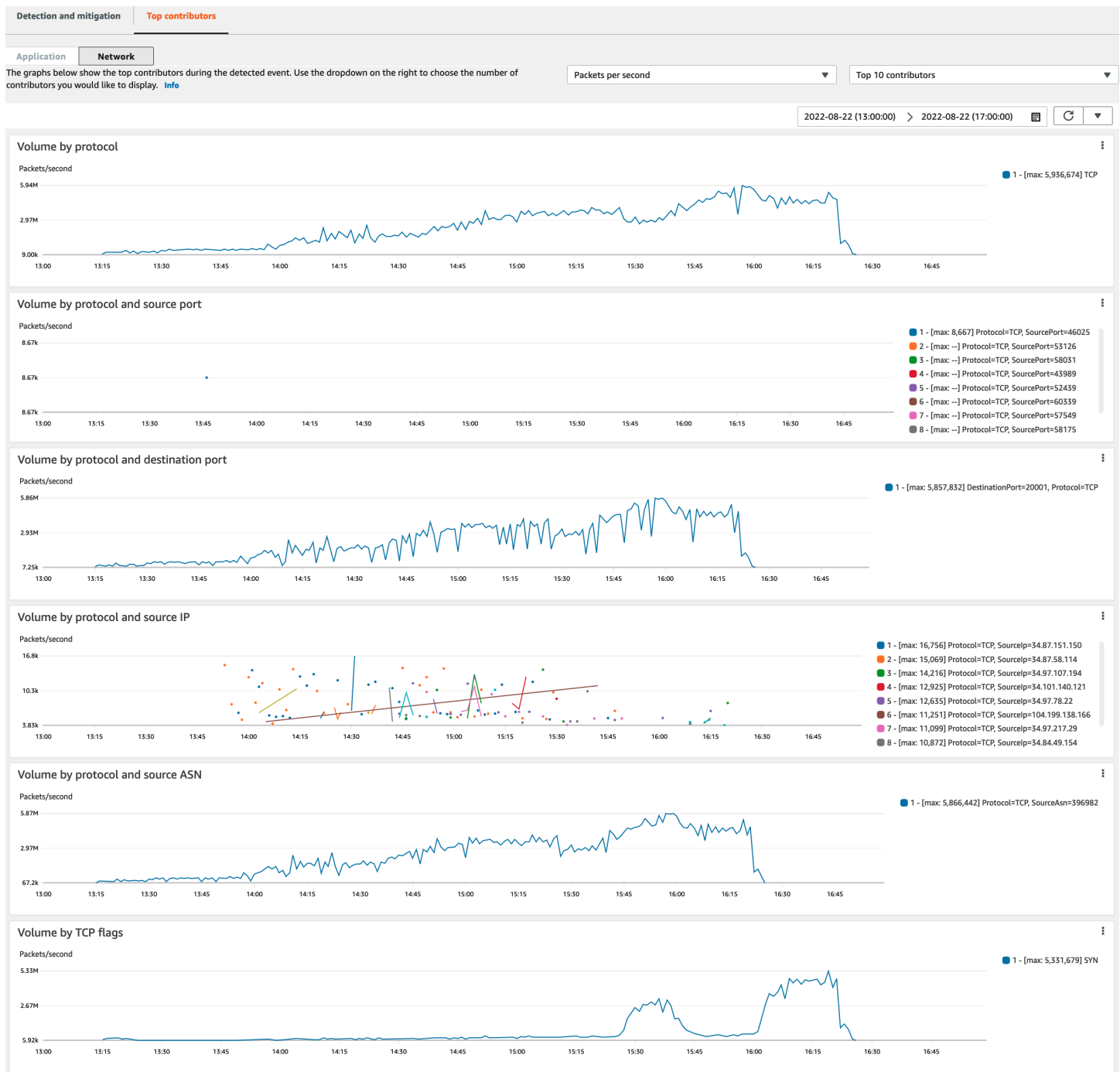


在 Shield 放置緩解之前所隱藏的事件流量不會在緩解指標中表示。這可能會導致偵測圖表中顯示的流量與緩解圖表中顯示的傳遞和捨棄指標之間的差異。

前幾名貢獻者

基礎設施層事件的前貢獻者索引標籤列出多個流量維度上最多 100 名前貢獻者的指標。詳細資訊包括任何維度的網路層屬性，其中至少可以識別五個重要的流量來源。流量來源的範例為來源 IP 和來源 ASN。

下列螢幕擷取畫面顯示基礎設施層事件的 Top contributors 索引標籤範例。



貢獻者指標是根據合法和潛在不需要流量的抽樣網路流程。較大的磁碟區事件，以及流量來源未高度分佈的事件，更有可能具有可識別的主要參與者。顯著分佈的攻擊可能具有任意數量的來源，因此很難識別攻擊的主要原因。如果 Shield 未識別特定指標或類別的任何重要參與者，則會將資料顯示為無法使用。

在基礎設施層 DDoS 攻擊中，流量來源可能會遭到欺騙或反射。詐騙來源是由攻擊者故意偽造的。反射來源是偵測到流量的真實來源，但不是攻擊的願意參與者。例如，攻擊者可能會透過反映網際網路上

通常合法的服務攻擊，產生大量擴增流量到目標。在此情況下，來源資訊可能有效，但不是攻擊的實際來源。這些因素可能會限制緩解技術根據封包標頭封鎖來源的可行性。

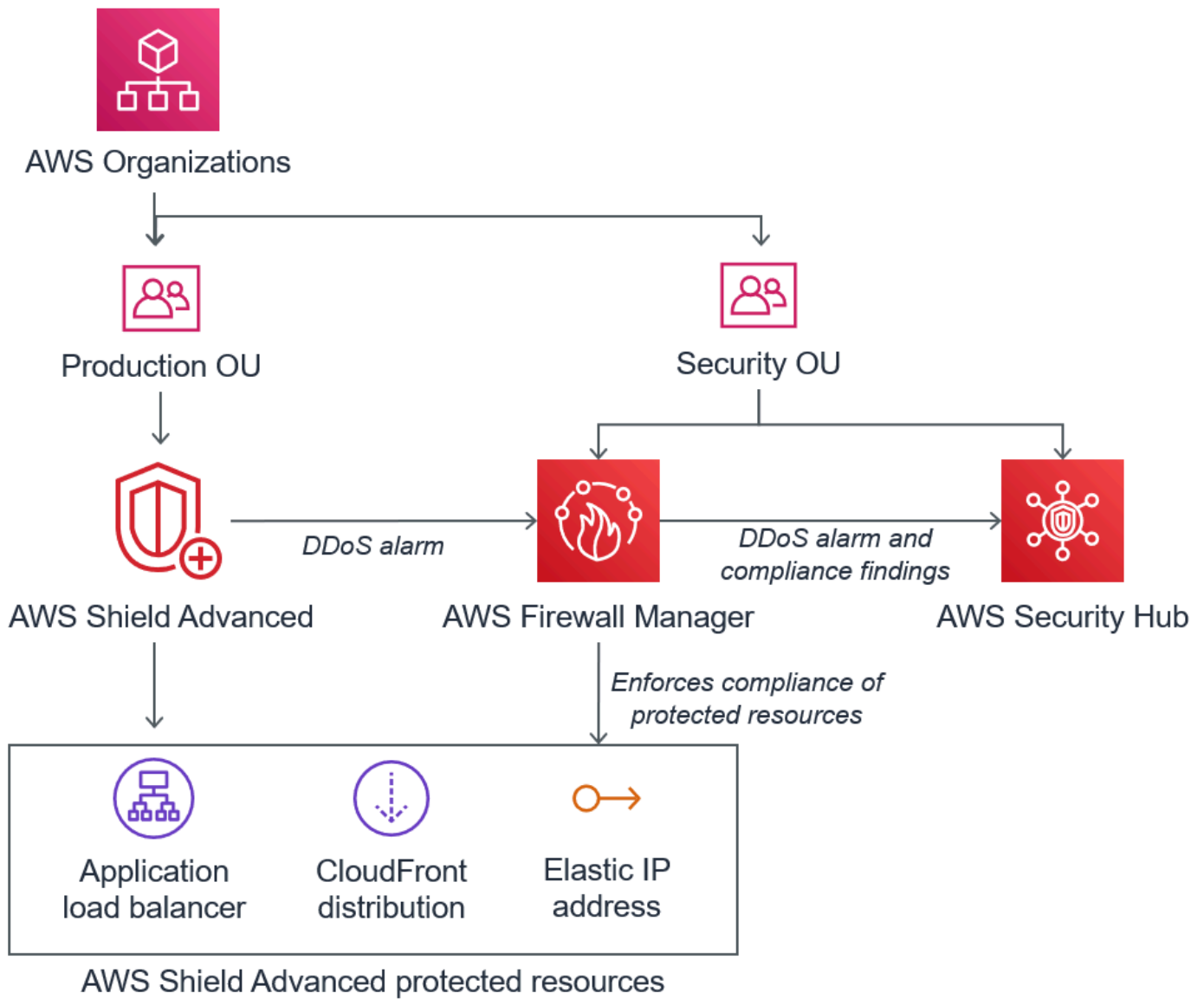
AWS 帳戶 使用 AWS Firewall Manager 和 檢視多個的 Shield Advanced 事件 AWS Security Hub

您可以使用 AWS Firewall Manager 和 AWS Security Hub 來管理和監控多個帳戶的 AWS Shield Advanced 受保護資源。

使用 Firewall Manager，您可以建立 Shield Advanced 安全政策，報告和強制執行所有帳戶的 DDoS 保護合規。Firewall Manager 會監控您的受保護資源，包括將保護新增至 Shield Advanced 政策範圍內的新資源。

您可以整合 Firewall Manager 與 AWS Security Hub，以取得單一儀表板，報告 Shield Advanced 和 Firewall Manager 合規調查結果偵測到的 DDoS 事件，當 Firewall Manager 識別不符合 Shield Advanced 安全政策的資源時。

下圖說明使用 Firewall Manager 和 Security Hub 監控 Shield Advanced 受保護資源的典型架構。



當您將 Firewall Manager 與 Security Hub 整合時，您可以在單一位置檢視安全問題清單，以及您所執行應用程式的其他提醒和合規狀態資訊 AWS。

下列螢幕擷取畫面會反白顯示您在整合此類型時，可在 Security Hub 主控台中看到的 Shield Advanced 事件資訊。

The screenshot displays the AWS Security Hub console. At the top, there's a 'Findings' section with filters for 'Title', 'Product name', 'Workflow status', and 'Record state'. A finding is listed with the title 'Shield Advanced detected attack against monitored resource'. The finding details on the right show it is 'INFORMATIONAL' and 'NEW', with the product 'Firewall Manager'. The resource ID is 'arn:aws:elasticloadbalancing:us-east-1:3502:49:loadbalancer/app/loadbalancer-3/dca87d7482d89b7f'. The finding details on the right indicate that Shield Advanced detected an attack on the protected resource.

若要了解如何將 Firewall Manager 和 Security Hub 與 Shield Advanced 整合，以集中監控受保護帳戶的事件和合規，請參閱 AWS 安全部落格[設定 DDoS 事件的集中監控和自動修復不合規資源](#)。

在中回應 DDoS 事件 AWS

此頁面說明 如何 AWS 回應 DDoS 攻擊，並提供如何進一步回應的選項。

AWS 會自動緩解網路和傳輸層（第 3 層和第 4 層）DDoS 攻擊。如果您使用 Shield Advanced 來保護 Amazon EC2 執行個體，在攻擊期間，Shield Advanced 會自動將您的 Amazon VPC 網路 ACLs 部署到網路邊界 AWS。這可讓 Shield Advanced 提供對較大 DDoS 事件的保護。如需網路 ACL 的詳細資訊，請參閱[網路 ACL](#)。

對於應用程式層（第 7 層）DDoS 攻擊，會 AWS 嘗試透過 CloudWatch 警示來偵測和通知 AWS Shield Advanced 客戶。根據預設，它不會自動套用緩解措施，以避免意外封鎖有效的使用者流量。

對於應用程式層（第 7 層）資源，您有下列選項可用於回應攻擊。

- 提供您自己的緩解措施 – 您可以自行調查和緩解攻擊。如需相關資訊，請參閱[手動緩解應用程式層 DDoS 攻擊](#)。
- 聯絡支援 – 如果您是 Shield Advanced 客戶，您可以聯絡[AWS 支援中心](#)以取得緩解措施的協助。重大和緊急案例會直接路由發送給 DDoS 專家。如需相關資訊，請參閱[在應用程式層 DDoS 攻擊期間聯絡支援中心](#)。

此外，在攻擊發生之前，您可以主動啟用下列緩解選項：

- Amazon CloudFront 分佈上的自動緩解 – 使用此選項，Shield Advanced 會在 Web ACL 中為您定義和管理緩解規則。如需自動應用程式層緩解的資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。
- 主動參與 – 當 AWS Shield Advanced 偵測到您的其中一個應用程式遭受大型應用程式層攻擊時，SRT 可以主動與您聯絡。SRT 會分類 DDoS 事件並建立 AWS WAF 緩解措施。SRT 會與您聯絡，並取得您的同意後，即可套用 AWS WAF 規則。如需有關此選項的詳細資訊，請參閱 [設定 SRT 的主動參與，以直接與您聯絡](#)。

在應用程式層 DDoS 攻擊期間聯絡支援中心

此頁面提供在應用程式層 DDoS 攻擊期間聯絡支援中心的指示。

如果您是 AWS Shield Advanced 客戶，您可以聯絡 [AWS 支援中心](#) 以取得緩解措施的協助。重大和緊急案例會直接路由發送給 DDoS 專家。使用時 AWS Shield Advanced，複雜案例可以呈報至 AWS Shield Response Team (SRT)，該團隊在保護 AWS Amazon.com 及其子公司方面擁有豐富的經驗。如需 SRT 的詳細資訊，請參閱 [使用 Shield Response Team \(SRT\) 支援的受管 DDoS 事件回應](#)。

若要取得 Shield Response Team (SRT) 支援，請聯絡 [AWS 支援中心](#)。您案例的回應時間取決於您選取的嚴重性和回應時間，這些時間會記錄在 [AWS 支援 Plans](#) 頁面上。

選取下列選項：

- 案例類型：技術支援
- 服務：分散式阻斷服務 (DDoS)
- 類別：傳入至 AWS
- 嚴重等級：選擇適當選項

與我們的代表討論時，請解釋您是可能遭受 DDoS 攻擊 AWS Shield Advanced 的客戶。我們的代表會引導您呼叫適當的 DDoS 專家。如果您使用分散式拒絕服務 (DDoS) 服務類型向 [AWS 支援中心](#) 開啟案例，您可以透過聊天或電話直接與 DDoS 專家交談。DDoS 支援工程師可協助您識別攻擊、建議改善 AWS 架構，並提供使用 AWS 服務進行 DDoS 攻擊緩解的指導。

對於應用程式層攻擊，SRT 可協助您分析可疑活動。如果您為資源啟用了自動緩解，SRT 可以檢閱 Shield Advanced 自動針對攻擊放置的緩解措施。在任何情況下，SRT 都可以協助您檢閱和緩解問題。SRT 建議的緩解措施通常需要 SRT 在您的帳戶中建立或更新 AWS WAF Web 存取控制清單 (Web ACLs)。SRT 將需要您的許可才能執行此工作。

Important

我們建議您遵循 中的步驟 AWS Shield Advanced 來[授予 SRT 的存取權](#)主動提供 SRT 在攻擊期間協助您所需的許可，以做為啟用的一部分。提前提供許可有助於防止在發生實際攻擊時所造成的事件延遲。

SRT 可協助您分類 DDoS 攻擊，以識別攻擊簽章和模式。在您同意的情況下，SRT 會建立和部署 AWS WAF 規則以緩解攻擊。

您也可以可能的攻擊之前或期間聯絡 SRT，以檢閱緩解措施，以及開發和部署自訂緩解措施。例如，如果您正在執行 Web 應用程式，且只需要開啟連接埠 80 和 443，則可以使用 SRT 來預先設定 Web ACL 以「僅允許」連接埠 80 和 443。

您授權並聯絡帳戶層級的 SRT。也就是說，如果您在 Firewall Manager Shield Advanced 政策中使用 Shield Advanced，帳戶擁有者，而不是 Firewall Manager 管理員，必須聯絡 SRT 以取得支援。Firewall Manager 管理員只能針對他們擁有的帳戶聯絡 SRT。

手動緩解應用程式層 DDoS 攻擊

此頁面提供手動緩解應用程式層 DDoS 攻擊的指示。

如果您判斷資源的事件頁面中的活動代表 DDoS 攻擊，您可以在 Web ACL 中建立自己的 AWS WAF 規則來緩解攻擊。如果您不是 Shield Advanced 客戶，這是唯一的選項。AWS WAF 包含在 AWS Shield Advanced 中，無需額外費用。如需有關在 Web ACL 中建立規則的資訊，請參閱 [在中設定保護 AWS WAF](#)。

如果您使用 AWS Firewall Manager，您可以將 AWS WAF 規則新增至 Firewall Manager AWS WAF 政策。

手動緩解潛在的應用程式層 DDoS 攻擊

1. 在 Web ACL 中建立符合異常行為條件的規則陳述式。若要從 開始，請將它們設定為計算相符的請求。如需設定 Web ACL 和規則陳述式的相關資訊，請參閱 [在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#) 和 [測試和調校您的 AWS WAF 保護](#)。

Note

一開始一律使用規則動作 Count 而非 Block 來測試您的規則。當您確定新規則識別正確的請求後，您可以修改它們以封鎖請求。

2. 監控請求計數，以判斷您是否要封鎖相符的請求。如果請求量持續異常高，且您確信您的規則正在擷取造成高容量的請求，請變更 Web ACL 中的規則以封鎖請求。
3. 繼續監控事件頁面，以確保您的流量依您希望的方式處理。

AWS 提供預先設定的範本，讓您快速開始使用。範本包含一組 AWS WAF 規則，您可以自訂和用來封鎖常見的 Web 型攻擊。如需詳細資訊，請參閱 [AWS WAF 安全自動化](#)。

在攻擊 AWS Shield Advanced 後請求 中的額度

如果您訂閱 AWS Shield Advanced 且遇到 DDoS 攻擊，增加 Shield Advanced 受保護資源的利用率，您可以在 Shield Advanced 未緩解的情況下，請求與使用率增加相關的費用的 Shield Advanced 服務額度。

Note

您只能將透過此程序收到的任何額度套用至 Shield Advanced 用量。Shield Advanced 點數不可與其他服務搭配使用。

點數僅適用於下列類型的費用：

- Shield Advanced 資料傳輸輸出
- Amazon CloudFront HTTP/HTTPS 請求
- CloudFront 資料傳輸輸出
- Amazon Route 53 查詢
- AWS Global Accelerator 標準加速器資料傳輸
- Application Load Balancer 的負載平衡器容量單位
- 由自動擴展政策建立以回應攻擊的受保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的執行個體成本

請求額度的先決條件

若要符合獲得點數的資格，您必須在攻擊開始之前完成下列動作：

- 您必須已將 Shield Advanced 保護新增至您要請求額度的資源。在攻擊期間新增的受保護資源不符合成本保護資格。

Note

在 上啟用 Shield Advanced AWS 帳戶 不會自動為個別資源啟用 Shield Advanced 保護。

如需如何使用 Shield Advanced 保護 AWS 資源的詳細資訊，請參閱 [將 AWS Shield Advanced 保護新增至 AWS 資源](#)。

- 對於適用的 CloudFront 和 Application Load Balancer 受保護的資源，您必須與 AWS WAF Web ACL 建立關聯，並在 Web ACL 中在 Block 模式中實作以速率為基礎的規則。如需速率型規則的相關資訊 AWS WAF，請參閱 [在 中使用以速率為基礎的規則陳述式 AWS WAF](#)。如需如何將 Web ACLs 與 AWS 資源建立關聯的詳細資訊，請參閱 [在 中設定保護 AWS WAF](#)。
- 您必須已在 [AWS DDoS 復原的最佳實務](#) 中實作適當的最佳實務，以將 DDoS 攻擊期間的成本降至最低的方式設定您的應用程式。

如何申請點數

若要符合抵用金的資格，您必須在發生攻擊的計費月份之後的 15 天內提交抵用金請求。

若要申請點數，請透過 [AWS 支援 中心](#) 提交帳單案例。在您的請求中包含下列項目：

- 主旨行中的「DDoS 優惠」
- 您請求額度的每個事件或可用性中斷的日期和時間
- 受影響的 AWS 服務和特定資源

在您提交請求後，Shield Response Team AWS (SRT) 將驗證 DDoS 攻擊是否發生，如果發生，則會驗證是否有任何受保護的資源擴展以吸收 DDoS 攻擊。如果 AWS 確定受保護的資源擴展以吸收 DDoS 攻擊，AWS 將為 AWS 判定為 DDoS 攻擊所導致的該部分流量發出額度。積分有效期限為 12 個月。

您使用 AWS Shield 服務的安全性

本節說明如何套用共同責任模型 AWS Shield。

的雲端安全 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。

Note

本節提供您使用 AWS Shield 服務及其 AWS 資源的標準 AWS 安全指導，例如 Shield Advanced 保護。

如需使用 Shield 和 Shield Advanced 保護您的 AWS 資源的資訊，請參閱 AWS Shield 本指南的其餘部分。

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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用於 Shield 的合規計劃，請參閱[AWS 合規計劃範圍內的服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您了解如何在使用 Shield 時套用共同的責任模型。下列主題說明如何設定 Shield 以符合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 Shield 資源。

主題

- [在 Shield 中保護您的資料](#)
- [搭配 使用 IAM AWS Shield](#)
- [在 Shield 中記錄和監控](#)
- [驗證 Shield 中的合規](#)
- [在 Shield 中建置彈性](#)
- [AWS Shield中的基礎設施安全](#)

在 Shield 中保護您的資料

本節說明 AWS 共同責任模型如何套用至 Shield 中的資料保護。

AWS [共同責任模型](#)適用於 中的資料保護 AWS Shield。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](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 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 Shield 或其他 AWS 服務主控台、API、AWS CLI 或 AWS SDKs 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。

Shield 實體 - 例如保護 - 靜態加密，但某些區域無法使用加密，包括中國（北京）和中國（寧夏）。每個區域都會採用唯一的加密金鑰。

搭配使用 IAM 和 AWS Shield

本節說明如何搭配使用 IAM 和 AWS Shield。

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）來使用 Shield 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 Shield 如何使用 IAM](#)
- [AWS Shield 的身分型政策範例](#)
- [AWS 的 受管政策 AWS Shield](#)
- [對 AWS Shield 身分和存取進行故障診斷](#)
- [使用 Shield Advanced 的服務連結角色](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Shield 中執行的工作。

服務使用者 – 如果您使用 Shield 服務來執行您的任務，則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 Shield 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 Shield 中的功能，請參閱 [對 AWS Shield 身分和存取進行故障診斷](#)。

服務管理員 – 如果您在公司負責 Shield 資源，您可能擁有 Shield 的完整存取權。您的任務是判斷服務使用者應存取的 Shield 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搭配 Shield 使用 IAM，請參閱 [AWS Shield 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 Shield 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Shield 身分型政策範例，請參閱 [AWS Shield 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 AWS 使用聯合身分存取時，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 AWS 服務是透過身分來源提供的登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，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 AWS 帳戶和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center？](#)。

IAM 使用者和群組

[IAM 使用者](#)是 中具有單一個人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 – 服務連結角色是一種連結至的服務角色。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 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到 AWS 身分或資源 AWS 來控制 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](#)。委託人可以包含帳戶、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 的 AWS 服務清單，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 Shield 如何使用 IAM

本節說明如何搭配使用 IAM 的功能 AWS Shield。

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

您可以搭配使用的 IAM 功能 AWS Shield

IAM 功能	Shield 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 (服務特定)	是
ACL	否
ABAC(政策中的標籤)	部分
暫時性憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要深入了解 Shield 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](#)。

Shield 的身分型政策

本節提供的身分型政策範例 AWS Shield。

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](#)。

若要檢視 Shield 身分型政策的範例，請參閱 [AWS Shield 的身分型政策範例](#)。

Shield 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。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（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](#)。

Shield 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 Shield 動作清單，請參閱服務授權參考中的 [定義的動作 AWS Shield](#)。

Shield 中的政策動作在動作之前使用下列字首：

```
shield
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "shield:action1",  
    "shield:action2"  
]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要在 Shield 中指定以開頭的所有動作 List，請包含下列動作：

```
"Action": "shield:List*"
```

若要檢視 Shield 身分型政策的範例，請參閱 [AWS Shield 的身分型政策範例](#)。

Shield 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 Shield 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 Shield](#)。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 Shield 定義的動作](#)。若要允許或拒絕存取一部分的 Shield 資源，請在政策的 `resource` 元素中包含資源的 ARN。

在中 AWS Shield，資源是保護和攻擊。這些資源都有與其相關的唯一 Amazon Resource Name (ARN)，如下表所示。

AWS Shield 主控台的名稱	AWS Shield SDK/CLI 中的名稱	ARN 格式
事件或攻擊	AttackDetail	arn:aws:shield:: <i>account</i> :attack/ <i>ID</i>
保護	Protection	arn:aws:shield:: <i>account</i> :protection/ <i>ID</i>

若要允許或拒絕對 Shield 資源子集的存取，請在政策的 `resource` 元素中包含資源的 ARN。Shield ARNs 格式如下：

```
arn:partition:shield::account:resource/ID
```

將 *##*、*##* 和 *ID* 變數取代為有效值。有效值如下：

- ##*：您的 ID AWS 帳戶。您必須指定一個數值。
- resource*：Shield 資源的類型，`attack` 或 `protection`。
- ID*：Shield 資源的 ID，或萬用字元 (*)，以指出與指定相關聯的指定類型的所有資源 AWS 帳戶。

例如，以下 ARN 為帳戶 111122223333 指定所有的保護：

```
arn:aws:shield::111122223333:protection/*
```

Shield 資源的 ARNs 格式如下：

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

如需 ARN 規格的一般資訊，請參閱 中的 [Amazon Resource Name \(ARNs\)](#) Amazon Web Services 一般參考。

下列列出 wafv2 資源 ARNs 特有的要求：

- **region**：針對您用來保護 Amazon CloudFront 分佈的 Shield 資源，請將此設為 us-east-1。否則，請將此設定為您搭配受保護區域資源使用的 區域。
- **##**：將範圍設定為 global，以搭配 Amazon CloudFront 分佈使用 regional，或搭配任何 AWS WAF 支援的區域資源使用。區域資源是 Amazon API Gateway REST API、Application Load Balancer、AWS AppSync GraphQL API、Amazon Cognito 使用者集區、AWS App Runner 服務和 AWS Verified Access 執行個體。
- **resource-type**：指定下列其中一個值：attack 用於事件或攻擊、protection 用於保護。
- **resource-name**：指定您提供 Shield 資源的名稱，或指定萬用字元 (*)，以指出符合 ARN 中其他規格的所有資源。您必須指定資源名稱和資源 ID，或同時指定萬用字元。
- **resource-id**：指定 Shield 資源的 ID，或指定萬用字元 (*)，以指出符合 ARN 中其他規格的所有資源。您必須指定資源名稱和資源 ID，或同時指定萬用字元。

例如，以下 ARN 為區域 us-west-1 中的帳戶 111122223333 指定所有的 Web ACL：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

下列 ARN 指定名為 的規則群組 MyIPManagementRuleGroup，其具有區域 111122223333 中帳戶的全域範圍 us-east-1：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

若要檢視 Shield 身分型政策的範例，請參閱 [AWS Shield 的身分型政策範例](#)。

Shield 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 支援全域條件索引鍵和服務特定條件索引鍵。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 Shield 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 Shield](#)。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 Shield](#)。

若要檢視 Shield 身分型政策的範例，請參閱 [AWS Shield的身分型政策範例](#)。

Shield 中的 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 Shield

支援 ABAC (政策中的標籤)：部分

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 Shield 使用臨時憑證

支援臨時憑證：是

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 Shield 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 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

Shield 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 Shield 功能。只有在 Shield 提供指引時，才能編輯服務角色。

Shield 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 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 Shield 服務連結角色的詳細資訊，請參閱 [使用 Shield Advanced 的服務連結角色](#)。

AWS Shield 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 Shield 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 Shield 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 Shield](#)。

主題

- [政策最佳實務](#)
- [使用 Shield 主控台](#)
- [允許使用者檢視他們自己的許可](#)
- [授予 Shield Advanced 保護的讀取存取權](#)
- [授予 Shield、CloudFront 和 CloudWatch 的唯讀存取權](#)
- [授予 Shield、CloudFront 和 CloudWatch 的完整存取權](#)

政策最佳實務

身分型政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Shield 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 AWS 受管政策，將許可授予許多常用案例。它們可在您的 AWS 帳戶中使用。我們建議您定義特定

於使用案例 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 Shield 主控台

若要存取 AWS Shield 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 Shield 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。

可以存取和使用 AWS 主控台的使用者也可以存取 AWS Shield 主控台。不需要額外許可。

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 主控台上完成此動作的許可，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": "*"
  }
]
}

```

授予 Shield Advanced 保護的讀取存取權

AWS Shield 允許跨帳戶資源存取，但不允許您建立跨帳戶資源保護。您只能從擁有這些資源的帳戶內建立資源保護。

以下為一個範例政策，該政策授與對所有資源進行 `shield:ListProtections` 動作的許可。Shield 不支援使用某些 API 動作的資源 ARNs (也稱為資源層級許可) 來識別特定資源，因此您可以指定萬用字元 (*)。這只允許存取您可以透過動作擷取的資源 `ListProtections`。

```

{
  "Version": "2016-06-02",

```

```

    "Statement": [
      {
        "Sid": "ListProtections",
        "Effect": "Allow",
        "Action": [
          "shield:ListProtections"
        ],
        "Resource": "*"
      }
    ]
  }

```

授予 Shield、CloudFront 和 CloudWatch 的唯讀存取權

下列政策會授予使用者對 Shield 和相關資源的唯讀存取權，包括 Amazon CloudFront 資源和 Amazon CloudWatch 指標。對於需要檢視 Shield 保護和攻擊中的設定，以及在 CloudWatch 中監控指標的許可的使用者來說，此功能非常有用。這些使用者無法建立、更新或刪除 Shield 資源。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ProtectedResourcesReadAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:List*",
        "elasticloadbalancing:List*",
        "route53:List*",
        "cloudfront:Describe*",
        "elasticloadbalancing:Describe*",
        "route53:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:*:*",
        "arn:aws:cloudfront:*:*:*",
        "arn:aws:route53:::hostedzone/*",
        "arn:aws:cloudwatch:*:*:*:*"
      ]
    }
  ]
}

```

```

        "arn:aws:globalaccelerator::*:*"
    ],
    },
    {
        "Sid": "ShieldReadOnly",
        "Effect": "Allow",
        "Action": [
            "shield:List*",
            "shield:Describe*",
            "shield:Get*"
        ],
        "Resource": "*"
    }
]
}

```

授予 Shield、CloudFront 和 CloudWatch 的完整存取權

下列政策可讓使用者執行任何 Shield 操作、在 CloudFront Web 分佈上執行任何操作，以及在 CloudWatch 中監控指標和請求範例。它適用於 Shield 管理員的使用者。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProtectedResourcesReadAccess",
            "Effect": "Allow",
            "Action": [
                "cloudfront:List*",
                "elasticloadbalancing:List*",
                "route53:List*",
                "cloudfront:Describe*",
                "elasticloadbalancing:Describe*",
                "route53:Describe*",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*",
                "cloudfront:GetDistribution*",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:DescribeAccelerator"
            ],
            "Resource": [
                "arn:aws:elasticloadbalancing::*:*",
            ]
        }
    ]
}

```

```
        "arn:aws:cloudfront::*:\"",
        "arn:aws:route53:::hostedzone/*",
        "arn:aws:cloudwatch:*:*:*:*\"",
        "arn:aws:globalaccelerator::*:\""
    ]
},
{
    "Sid": "ShieldFullAccess",
    "Effect": "Allow",
    "Action": [
        "shield:*"
    ],
    "Resource": "*"
}
]
```

我們強烈建議您為具有管理權限的使用者設定多重驗證 (MFA)。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 Multi-Factor Authentication \(MFA\) 裝置搭配 AWS](#)。

AWS 的 受管政策 AWS Shield

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有 服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 受管政策](#)。

AWS 受管政策：AWSShieldDRTAccessPolicy

本節說明如何使用 Shield 的 AWS 受管政策。

AWS Shield 當您授予 Shield Response Team (SRT) 代表您行事的許可時，會使用此受管政策。此政策可讓 SRT 有限地存取您的帳戶 AWS，以協助在高嚴重性事件期間緩解 DDoS 攻擊。此政策允許 SRT 管理您的 AWS WAF 規則和 Shield Advanced 保護，以及存取您的 AWS WAF 日誌。

如需授予許可給 SRT 以代表您操作的資訊，請參閱 [授予 SRT 的存取權](#)。

如需此政策的詳細資訊，請參閱 IAM 主控台中的 [AWSShieldDRTAccessPolicy](#)。

AWS 受管政策：AWSShieldServiceRolePolicy

Shield Advanced 會在您啟用自動應用程式層 DDoS 緩解時使用此受管政策，以設定其管理您帳戶資源所需的許可。此政策允許 Shield Advanced 在您已與受保護資源建立關聯的 Web ACLs 中建立和套用 AWS WAF 規則和規則群組，以自動回應 DDoS 攻擊。

您無法將 AWSShieldServiceRolePolicy 連接至 IAM 實體。Shield 將此政策連接至服務連結角色 AWSServiceRoleForAWSShield，以允許 Shield 代表您執行動作。

當您啟用自動應用程式層 DDoS 緩解時，Shield Advanced 會啟用此政策。如需此政策使用的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

如需使用此政策之服務連結角色 AWSServiceRoleForAWSShield 的相關資訊，請參閱 [使用 Shield Advanced 的服務連結角色](#)

如需此政策的詳細資訊，請參閱 IAM 主控台中的 [AWSShieldServiceRolePolicy](#)。

AWS 受管政策的 Shield 更新

檢視自此服務開始追蹤這些變更以來，Shield AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Shield 文件歷史記錄頁面上的 RSS 摘要 [文件歷史紀錄](#)。

政策	變更描述	日期
AWSShieldServiceRolePolicy 此政策允許 Shield 存取和管理 AWS 資源，以代表您自動回應應用程式層 DDoS 攻擊。 IAM 主控台中的詳細資訊： AWSShieldServiceRolePolicy	新增此政策，為 Shield Advanced 提供自動應用程式層 DDoS 緩解功能所需的許可。如需此功能的相關資訊，請參閱 使用 Shield Advanced 自動化應用程式層 DDoS 緩解 。	2021 年 12 月 1 日

政策	變更描述	日期
服務連結角色AWSServiceRoleForAWSShield 使用此政策。如需相關資訊，請參閱 使用 Shield Advanced 的服務連結角色 。		
Shield 已開始追蹤變更	Shield 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 3 日

對 AWS Shield 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 Shield 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 Shield 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 Shield 資源](#)

我無權在 Shield 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 shield:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
shield: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 shield:*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 Shield。

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 `marymajor` 的 IAM 使用者嘗試使用主控台在 Shield 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 Shield 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 Shield 是否支援這些功能，請參閱 [AWS Shield 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶在您的資源之間提供存取權，請參閱《[IAM 使用者指南](#)》中的在您的 AWS 帳戶的另一個資源中提供存取權給 IAM 使用者。
- 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 \(聯合身分\)](#)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《[IAM 使用者指南](#)》中的 [IAM 角色與資源型政策的差異](#)。

使用 Shield Advanced 的服務連結角色

本節說明如何使用服務連結角色，讓 Shield Advanced 存取您的 AWS 帳戶中的資源。

AWS Shield Advanced 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Shield Advanced 的唯一 IAM 角色類型。服務連結角色由 Shield Advanced 預先定義，並包含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 Shield Advanced，因為您不必手動新增必要的許可。Shield Advanced 會定義其服務連結角色的許可，除非另有定義，否則只有 Shield Advanced 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 Shield Advanced 資源，因為您不會意外移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Shield Advanced 的服務連結角色許可

Shield Advanced 使用名為 AWSServiceRoleForAWSShield 的服務連結角色。此角色允許 Shield Advanced 存取和管理 AWS 資源，以代表您自動回應應用程式層 DDoS 攻擊。如需此功能的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

AWSServiceRoleForAWSShield 服務連結角色信任下列服務擔任該角色：

- shield.amazonaws.com

名為 AWSShieldServiceRolePolicy 的角色許可政策可讓 Shield Advanced 在所有 AWS 資源上完成下列動作：

- wafv2:GetWebACL
- wafv2:UpdateWebACL
- wafv2:GetWebACLFForResource
- wafv2:ListResourcesForWebACL
- cloudfront:ListDistributions
- cloudfront:GetDistribution

當所有 AWS 資源上都允許動作時，政策中會將其表示為 "Resource": "*"。這僅表示服務連結角色可以對動作支援的所有 AWS 資源採取每個指定的動作。例如，動作僅wafv2:GetWebACL支援 wafv2 Web ACL 資源。

Shield Advanced 只會針對您已啟用應用程式層保護功能的受保護資源，以及與這些受保護資源相關聯的 Web ACLs，進行資源層級 API 呼叫。

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](#)。

為 Shield Advanced 建立服務連結角色

您不需要手動建立一個服務連結角色。當您為 AWS Management Console、AWS CLI 或 AWS API 中的資源啟用自動應用程式層 DDoS 緩解時，Shield Advanced 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您為資源啟用自動應用程式層 DDoS 緩解時，Shield Advanced 會再次為您建立服務連結角色。

編輯 Shield Advanced 的服務連結角色

Shield Advanced 不允許您編輯 AWSServiceRoleForAWSShield 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的[編輯服務連結角色](#)。

刪除 Shield Advanced 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

Note

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

刪除 AWSServiceRoleForAWSShield 使用的 Shield Advanced 資源

對於所有已設定應用程式層 DDoS 保護的資源，請停用自動應用程式層 DDoS 緩解。如需主控台說明，請參閱[設定應用程式層 DDoS 保護](#)。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、或 AWS API 來刪除 AWSServiceRoleForAWSShield 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

Shield 進階服務連結角色的支援區域

Shield Advanced 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱[Shield Advanced 端點和配額](#)。

在 Shield 中記錄和監控

本節說明如何使用 AWS 工具來監控和回應 中的事件 AWS Shield。

監控是維護 Shield 和 AWS 解決方案可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。AWS 提供數種工具來監控 Shield 資源並回應潛在事件：

Amazon CloudWatch 警示

您可以使用 CloudWatch 警示觀察單一指標一段指定的時間。如果指標超過指定的閾值，CloudWatch 會傳送通知至 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。

AWS CloudTrail 日誌

CloudTrail 提供 Shield AWS 中使用者、角色或服務所採取動作的記錄。使用 CloudTrail 收集的資訊，您可以判斷向 Shield 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。如需詳細資訊，請參閱[使用 AWS CloudTrail記錄 API 呼叫](#)。

驗證 Shield 中的合規

本節說明您在使用時的合規責任 AWS Shield。

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](#)。

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。

在 Shield 中建置彈性

本節說明 AWS 架構如何支援資料備援 AWS Shield。

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](#)。

AWS Shield中的基礎設施安全

本節說明如何 AWS Shield 隔離服務流量。

作為受管服務，AWS Shield 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 Shield。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，您可以使用 [AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS Shield Advanced 配額

AWS Shield Advanced 在每個區域的實體數量上具有預設配額。您可以[請求提高](#)這些配額。

資源	預設配額
每個帳戶每個 AWS Shield Advanced 資源類型提供保護的受保護資源數量上限。	1,000
每個帳戶的保護群組數目上限。	100
您可以特別包含在保護群組中的個別受保護資源數量上限。在 API 中，這適用於Members您在將保護群組設定為 時指定的 Pattern ARBITRARY 。在 主控台中，這適用於您為保護群組選擇的資源 從受保護的資源中選擇。	1,000

AWS Shield 網路安全主管（預覽）

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

AWS Shield 網路安全主管透過探索您帳戶中的運算、聯網和網路安全資源，協助保護您的 AWS 環境。網路安全主管會根據 AWS 最佳實務和威脅情報分析網路拓撲和安全組態，來評估每個資源的安全組態。為了協助您強化安全性，網路安全主管會評估其調查結果的嚴重性從低到關鍵，並分享特定的修補步驟，您可以透過 Amazon Q Developer 使用自然語言查詢進行探索。

AWS Shield 網路安全主管定價

AWS 目前不收取使用網路安全主管的費用。不過，您必須負責支付您所使用的基礎服務所產生的費用，例如 AWS WAF。當網路安全主管正式推出時，定價將與預覽版本不同。

什麼是 AWS Shield 網路安全主管？

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

AWS Shield 網路安全主管透過探索您帳戶中的運算、聯網和網路安全資源，協助保護您的 AWS 環境。網路安全主管會根據 AWS 最佳實務和威脅情報分析網路拓撲和安全組態，來評估每個資源的安全組態。為了協助您強化安全性，網路安全主管會評估其調查結果的嚴重性從低到關鍵，並分享特定的修補步驟，您可以透過 Amazon Q Developer 使用自然語言查詢進行探索。

主題

- [網路安全主管的常見使用案例](#)
- [網路安全主管中的關鍵概念](#)

網路安全主管的常見使用案例

網路安全主管可協助您透過下列使用案例識別和緩解網路安全問題：

對 Amazon EC2 執行個體的過度寬鬆存取

識別安全群組和網路 ACLs，允許無限制存取 VPCs 和 Amazon EC2 執行個體上的高風險連接埠（例如 22 和 3389）。取得 step-by-step 指引，以限制對這些連接埠的存取。

網際網路暴露的資源

識別可透過網際網路閘道從網際網路存取的資源。

AWS WAF 保護不足

識別面向網際網路的資源並評估其 AWS WAF 保護狀態。取得設定和部署的指引 AWS WAF，包括速率限制規則和 AWS 受管規則規則群組的建議。

已知威脅

識別暴露於已知威脅的資源，包括 DDoS 攻擊、SQL Injection 和跨網站指令碼 (XSS)。取得實作自訂規則或 AWS WAF AWS 受管規則規則群組以進行保護 step-by-step 說明。

未連接的安全服務

識別未保護任何資源的 AWS WAF Web ACL、安全群組和 NACLs。ACLs 取得移除或新增建議規則以供日後使用的指引。

網路安全主管中的關鍵概念

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

資源

處理應用程式流量的運算、聯網和安全資源：

- 運算 – Amazon Elastic Compute Cloud 執行個體
- 網路 – Application Load Balancer、Amazon API Gateways、Amazon CloudFront 分佈、VPC 子網路 and VPC 彈性網路介面 ENIs)
- 安全 – AWS WAF Web ACLs、VPC 安全群組和 VPC 網路存取控制清單 NACLs)

問題清單

有關缺少或設定錯誤網路安全服務的提醒，其嚴重性等級為 NONE、InformationAL、LOW、MEDIUM、HIGH 或 CRITICAL。網路安全主管會透過評估每個資源的組態設定和威脅情報來產生問題清單。

嚴重性

根據 AWS 最佳實務和威脅情報，測量資源對潛在安全事件的漏洞。嚴重性評估會同時考慮潛在的漏洞和現有的保護。資源的嚴重性層級符合其最嚴重的問題清單，如果沒有問題清單，則顯示為無。

網路拓撲

網路的視覺化呈現，顯示資源連線、網際網路暴露和標籤型關係。使用拓撲檢視來調查資源及其問題清單。

了解網路安全主管調查結果

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

網路安全主管會針對其分析的每種資源類型產生特定問題清單。這些調查結果可協助您識別安全問題並採取適當的動作。下表依資源類型列出所有可能的調查結果。

依資源類型分類的網路安全主管問題清單

資源類型	問題清單說明
Application Load Balancer	• 位於 CloudFront 分佈後方，但也會公開至網際網路 • 缺少對機器人的保護 • 具有 DDoS 活動 • 缺少防火牆保護 • 防火牆設定錯誤 • 具有未設定的防火牆 • 不受請求洪水影響 • 不受 Web 漏洞的保護

資源類型	問題清單說明
Amazon API Gateway	• 缺少對機器人的保護 • 缺少防火牆保護 • 防火牆設定錯誤 • 具有未設定的防火牆 • 不受請求洪水影響 • 不受 Web 漏洞的保護
Amazon CloudFront	• 缺少對機器人的保護 • 具有 DDoS 活動 • 缺少防火牆保護 • 防火牆設定錯誤 • 具有未設定的防火牆 • 不受請求洪水影響 • 不受 Web 漏洞的保護
Amazon Elastic Compute Cloud (EC2) 執行個體	• 允許來自所有連接埠上所有 IP 範圍的傳入存取 • 允許從遠端桌面通訊協定連接埠 (連接埠 3389) 上的所有 IP 範圍傳入存取 • 允許 SSH 連接埠 (連接埠 22) 上所有 IP 範圍的傳入存取 • 允許傳出存取所有連接埠上的所有 IP 範圍 • 位於沒有防火牆保護的 Application Load Balancer 後方 • 位於 CloudFront 分佈後方的 Application Load Balancer 後方，但也會公開至網際網路 • 位於沒有防火牆保護的 CloudFront 分發後方 • 缺少對機器人的保護 • 不受請求洪水影響 • 位於設定錯誤的防火牆後方 • 位於未設定的防火牆後方 • 位於未受 Web 漏洞保護的資源後方

資源類型	問題清單說明
VPC 安全群組	• 允許來自所有連接埠上所有 IP 範圍的傳入存取 • 允許從遠端桌面通訊協定連接埠 (連接埠 3389) 上的所有 IP 範圍傳入存取 • 允許 SSH 連接埠 (連接埠 22) 上所有 IP 範圍的傳入存取 • 允許傳出存取所有連接埠上的所有 IP 範圍
VPC 網路存取控制清單 (NACL)	• 允許來自所有連接埠上所有 IP 範圍的傳入存取 • 允許從遠端桌面通訊協定連接埠 (連接埠 3389) 上的所有 IP 範圍傳入存取 • 允許 SSH 連接埠 (連接埠 22) 上所有 IP 範圍的傳入存取 • 允許傳出存取所有連接埠上的所有 IP 範圍
AWS WAF Web ACL	• 具有機器人活動 • 缺少對機器人的保護 • 設定錯誤 • 未連接至任何資源 • 未設定為防止請求洪水 • 沒有規則 • 未設定為防止 Web 漏洞

設定您的帳戶以使用 AWS Shield 網路安全主管

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

本主題說明建立 帳戶等初步步驟，以準備您使用網路安全主管和相關服務，包括 Amazon Q Developer。您不需要支付這些初步項目的費用。您只需為所使用的 AWS 服務付費。

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](#)。

AWS Shield 網路安全主管入門

開始使用 網路安全主管之前，請確定您已完成中所述的設定步驟[設定您的帳戶以使用 AWS Shield 網路安全主管](#)。

下列工作流程會引導您分析和改善網路安全組態：

- [執行網路分析](#) - 執行您的第一個網路分析，以識別 AWS 環境中的潛在安全問題。
- [識別具有安全問題的資源](#) - 檢閱儀表板，以了解哪些資源具有需要注意的安全調查結果。
- [尋找最高嚴重性資源的修復步驟](#) - 取得改善資源安全組態的建議。
- [使用 Amazon Q Developer 分析網路安全](#) - 使用 Amazon Q Developer 以自然語言分析您的網路安全組態。

執行網路分析

Note

網路安全主管目前每個帳戶最多僅支援 300,000 個資源。請參閱[AWS Shield 網路安全主管配額](#)

若要開始使用網路安全主管，請執行網路分析。當您執行網路分析時，網路安全主管會識別並擷取與資源相關的安全資訊。

在網路安全主管中執行網路分析

1. 登入 AWS Management Console 並開啟 AWS Shield 網路安全主管主控台，網址為 <https://console.aws.amazon.com/wafv2/network-director/>。
2. 從網路安全主管首頁中，選擇開始使用。
3. 在網路安全主管入門頁面中，選擇啟動網路分析。

開始網路分析後，會出現網路安全主管儀表板。視您環境中的網路資源數量而定，可能需要幾分鐘的時間才能完成網路分析。

在網路分析期間，網路安全主管會分析您的運算和聯網資源是否有潛在的安全性問題清單。AWS Shield 網路安全主管會使用您最近網路分析的結果，將相關的安全性問題清單填入儀表板和主控台的其他部分。當您執行新的網路分析時，網路安全主管會在主控台中顯示最新的問題清單。

第一次網路分析完成後，請繼續[識別具有安全問題的資源](#)了解如何了解和解譯結果。

識別具有安全問題的資源

AWS Shield 網路安全主管會將嚴重性等級指派給最近網路分析中的每個問題清單。您可以指派 NONE、InformationAL、LOW、MEDIUM、HIGH 或 CRITICAL 資源。此嚴重性等級代表資源上所識別最嚴重問題清單的嚴重性等級。例如，如果您的最新網路分析判斷您的 Amazon EC2 執行個體有一個中等層級調查結果和兩個低嚴重性調查結果，則該資源會獲指派中等嚴重性層級。

您可以使用各種資料視覺化選項，在網路安全主管主控台中檢視網路分析的結果。

問題清單概觀小工具提供兩種方法來了解網路安全主管在您的資源中找到的問題清單：

- 從最高嚴重性資源，您可以快速了解哪些嚴重性等級在所有聯網資源中最為嚴重。您也可以查看清單，其中列出多少資源受到影響，以及網路安全主管為每個嚴重性等級指派的資源數量。
- 從嚴重性分佈中，您可以檢視每個資源類型具有特定嚴重性層級的資源數量，並將其與其他資源類型的資源進行比較。

識別哪些資源具有問題清單

1. 登入 AWS Management Console 並開啟 AWS Shield 網路安全主管主控台，網址為 <https://console.aws.amazon.com/wafv2/network-director/>。

2. 從網路安全主管儀表板中，導覽至調查結果概觀小工具。
3. 請注意顯示的嚴重性等級，以及指派該嚴重性等級的問題清單數量。
4. 從已識別的問題清單，選擇符合您在上一個步驟中記下的項目。

資源頁面隨即開啟，讓您開始進一步調查最高嚴重性的資源。

識別受影響的資源後，請繼續[尋找最高嚴重性資源的修復步驟](#)了解如何尋找受影響資源的特定修補建議。

使用網路拓撲映射

網路安全主管網路拓撲映射提供網路資源及其連線的視覺化呈現。此視覺化可協助您了解資源的連線方式，並識別網路架構中的潛在安全問題。最新網路分析完成後，網路拓撲映射可用於問題清單。

了解網路拓撲映射

網路拓撲映射使用節點和連線來代表您的網路資源及其關係：

- 節點代表個別資源，例如 Amazon EC2 執行個體、Application Load Balancer、AWS WAF 保護套件或 Web ACLs，以及其他網路元件。
- 連線代表資源之間的關係，例如流量或保護關係。
- 顏色表示資源的嚴重性等級，顏色較深表示較高的嚴重性等級。

拓撲貼圖可協助您視覺化：

- 哪些資源會公開至網際網路
- 流量如何在資源之間流動
- 有哪些安全保護
- 存在潛在安全問題的地方

導覽網路拓撲映射

您可以透過多種方式與網路拓撲映射互動：

- 縮放 - 使用縮放控制項或滑鼠滾輪來放大和縮小地圖。

- Pan - 按一下並拖曳以移動地圖。
- 選取 - 按一下節點以檢視該資源的詳細資訊。
- Filter - 使用篩選選項來專注於特定資源類型或問題清單嚴重性。

篩選網路拓撲映射

1. 在網路拓撲映射檢視中，找到右上角的篩選條件控制項。
2. 選取您要套用的篩選條件類型：
 - 資源類型 - 依特定資源類型篩選，例如 Amazon EC2 執行個體、Application Load Balancer 或 AWS WAF Web ACLs。
 - 嚴重性等級 - 依嚴重性等級篩選，以專注於具有特定嚴重性評分的資源。
 - 標籤 - 依資源標籤篩選，以專注於具有特定標籤的資源。
3. 套用您選取的篩選條件以更新地圖檢視。

分析拓撲映射中的資源

網路拓撲映射可讓您分析資源及其安全組態：

在拓撲映射中分析資源

1. 按一下拓撲映射中的資源節點。
2. 在出現的資源詳細資訊面板中，檢閱下列資訊：
 - 資源詳細資訊 - 資源的基本資訊，包括其 ID、類型和標籤。
 - 嚴重性等級 - 指派給資源的整體嚴重性等級。
 - 調查結果 - 與資源相關聯的安全調查結果。
 - 連線的資源 - 連接到此資源的其他資源。
3. 若要檢視問題清單的詳細修復建議，請展開問題清單並檢閱建議的步驟。

透過分析拓撲地圖中的資源，您可以識別安全調查結果，並了解它們與您的整體網路架構有何關聯。

在拓撲映射中識別安全模式

網路拓撲映射可協助您識別常見的安全模式和問題：

網際網路公開

拓撲映射中具有地球圖示的資源具有網際網路閘道的已識別通訊路徑。這些資源因為公有通訊路徑而增加威脅暴露。

缺少保護

應該有 AWS WAF 或 安全群組保護但不會顯示的資源與安全服務的連線較少。

過於寬鬆的存取

允許廣泛存取的安全群組或 NACLs 將以更高的嚴重性等級反白顯示。

未使用的安全資源

例如未連線至任何其他資源的 AWS WAF Web ACL 等安全資源可能未使用，而且可以移除。

ACLs

使用這些模式來識別您可以改善網路安全組態的區域。

探索網路拓撲之後，您可能想要更詳細地調查特定問題清單。繼續[尋找最高嚴重性資源的修復步驟](#)了解如何為您的 資源尋找詳細的修補建議。

尋找最高嚴重性資源的修復步驟

當網路分析完成時，網路安全主管會提供詳細建議，以修復資源調查結果中識別的漏洞。您可以根據資源 ID、嚴重性層級、資源類型或相關聯的調查結果來篩選任何易受攻擊的資源。根據預設，資源資料表會以最高到最低嚴重性的順序顯示資源。

尋找改善安全的建議

1. 登入 AWS Management Console 並開啟 AWS Shield 網路安全主管主控台，網址為 <https://console.aws.amazon.com/wafv2/network-director/>。
2. 在網路安全主管首頁中，選擇資源。
3. 從 資料表中，檢視並選擇性地篩選您的聯網資源。
4. 依嚴重性層級排序資源，從最高到最低的嚴重性。
5. 選擇指派給最高嚴重性等級的任何資源，以開啟其詳細檢視。
6. 在問題清單小工具中，找到任何嚴重性等級最高的問題清單。

資源可以由網路安全主管識別多個問題清單。每個調查結果代表在您最近一次網路分析期間發現的安全問題。

7. 展開問題清單的修復建議。
8. 請遵循網路安全主管建議的步驟，或選擇包含的文件連結以進一步了解。

檢閱並實作受影響資源的修補建議後，您可能想要取得有關整體安全組態的其他洞見。繼續[使用 Amazon Q Developer 分析網路安全](#)了解如何使用 Amazon Q Developer 進行進一步分析。

使用 Amazon Q Developer 分析網路安全

Amazon Q Developer 是採用生成式人工智慧（生成式 AI）技術的助理，可與網路安全主管合作，協助解答您的問題，並提供有關網路安全和修復選項的建議。

您可以在網路安全主管主控台中出現的任何位置選擇 Q 按鈕或使用 Amazon Q Developer 探索，以與 Amazon Q Developer 互動。本節會引導您完成從網路安全主管儀表板詢問 Q 問題的步驟。

與 Amazon Q Developer 互動

Note

您必須先完成網路分析，才能與 Amazon Q Developer 聊天。

1. 登入 AWS Management Console 並開啟 AWS Shield 網路安全主管主控台，網址為 <https://console.aws.amazon.com/wafv2/network-director/>。
2. 從網路安全主管首頁中，選擇儀表板。
3. 在詢問 Amazon Q 開發人員小工具中，選擇要在 Amazon Q 開發人員聊天介面中做為提示使用的問題。
4. 在 Amazon Q Developer 聊天介面中，提交您的請求。

以下是有關網路安全的範例問題，您可以詢問 Amazon Q Developer：

- 識別我的最佳網路安全問題清單
- 總結我環境的網路安全
- 我的系統是否有遭受 DDoS 攻擊的風險？
- 如何改善網路安全？
- 我是否有任何沒有 WAF 保護的資源？

- 哪些資源不受常見 Web 漏洞的保護？
- 我的 EC2 執行個體有哪些常見的網路安全問題？
- 我是否有任何 WAF Web ACLs 未保護任何內容？

資料保護考量

如需有關 Amazon Q Developer 如何存放對話的資訊，請參閱 [《Amazon Q Developer 使用者指南》中的 Amazon Q Developer 中的資料保護](#)。

如需有關 Amazon Q Developer 如何使用跨區域處理的資訊，請參閱 [《Amazon Q Developer 使用者指南》中的 Amazon Q Developer 中的跨區域處理](#)。

使用 Amazon Q Developer 取得其他洞見後，您可能想要執行另一個網路分析，以驗證安全組態中的任何改進。返回 [執行網路分析](#) 以開始新的分析。

AWS Shield 網路安全主管配額

AWS 帳戶具有每個 AWS 服務的預設配額，先前稱為限制。下表說明 網路安全主管的配額。如需可變更配額的詳細資訊，請參閱 [服務配額](#)。

資源	預設配額
每次掃描處理的 資源上限	300,000

當網路安全主管達到可在網路分析中處理的最大資源數量時，網路分析會失敗。您不需要為失敗的網路分析付費。

如果您的網路分析因為超過資源上限而失敗，請聯絡 AWS Support。

故障診斷 AWS Shield 網路安全主管

不支援的跨帳戶共用資源

AWS Shield 網路安全主管不支援某些跨帳戶共用資源。嘗試掃描這些資源時，您會收到錯誤訊息，指出無法分析資源。

不支援的共用資源和錯誤訊息

資源類型	錯誤訊息
Network Firewall FirewallPolicy	共用資源不支援 network-firewall : DescribeFirewallPolicy
Network Firewall 狀態規則群組	共用資源不支援 network-firewall : DescribeRuleGroup
Network Firewall 無狀態規則群組	共用資源不支援 network-firewall : DescribeRuleGroup
EC2 PrefixList	ec2 : GetManagedPrefixListEntries 不支援共用資源

調查結果和隱藏的可用性

網路安全主管會將網路掃描結果保留 60 天。在此期間之後，您必須執行新的掃描以檢視目前的問題清單。

只要您有作用中的網路掃描，抑制就會保留。如果因為超過 60 天而無法再使用網路掃描，您必須將禁止套用到下一次網路掃描。

資源掃描限制

掃描具有大量資源的帳戶時，您可能會遇到下列限制：

- 您可能會收到訊息，指出掃描已在進行中
- 服務無法提供掃描的預估完成時間
- 掃描持續時間會根據您帳戶中的資源數量而有所不同

Note

掃描持續時間取決於您帳戶中的資源總數，這在掃描程序本身期間決定。

其他資源

如果您遇到本故障診斷指南中未解決的問題，請聯絡 AWS Support 以取得其他協助。

使用 AWS Shield 網路安全主管的安全性

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

本節說明使用此網路安全主管預覽的主要安全考量事項。

資料來源

當您執行分析時，網路安全主管會使用公有 AWS API 端點擷取 [AWS 資源](#) 的相關資訊。擷取的資訊包括透過 AWS APIs 可供您帳戶使用的資源屬性。在您執行網路分析後 60 天內，來自掃描的資訊會通知網路安全主管提供的調查結果和修復建議。

AWS Shield 網路安全主管也會使用內部 AWS 資料來源和威脅情報來識別問題清單並建議補救措施。

資料加密

使用 網路安全主管時，請檢閱下列加密考量事項。

- 靜態加密 – 所有資料都會受到靜態保護。
- 傳輸中加密 – 所有資料都會使用 Transport Layer Security (TLS) 加密在傳輸中受到保護。所有通訊都會使用 Amazon Simple Storage Service AWS Signature 第 4 版 (SigV4) 進行驗證。如需 SigV4 的相關資訊，請參閱《Amazon S3 使用者指南》中的 [驗證請求 \(AWS 簽章版本 4\)](#)。
- 金鑰管理 – 目前不支援客戶受管金鑰。

主題

- [AWS Shield 網路安全主管的 Identity and Access Management](#)
- [AWS Shield 網路安全主管的身分型政策範例](#)
- [使用 AWS Shield 網路安全主管的服務連結角色](#)

AWS Shield 網路安全主管的 Identity and Access Management

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

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 Shield 網路安全主管資源。IAM 是您可以免費使用 AWS 服務的。

檢閱本節中的指引，了解如何使用 AWS Shield 網路安全主管支援的政策和角色。

AWS Shield 網路安全主管如何與 IAM 搭配使用

本節說明如何將 IAM 的功能與 AWS Shield 網路安全主管搭配使用。

在您使用 IAM 管理網路安全主管的存取權之前，請先了解哪些 IAM 功能可與網路安全主管搭配使用。

可與 AWS Shield 網路安全主管搭配使用的 IAM 功能

IAM 功能	AWS Shield 網路安全主管支援
身分型政策	是
服務連結角色	是

若要全面了解網路安全主管和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的[AWS 與 IAM 搭配使用的服務](#)。

網路安全主管的身分型政策

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](#)。

若要檢視 AWS Shield 網路安全主管身分型政策的範例，請參閱 [AWS Shield 網路安全主管的身分型政策範例](#)。

網路安全主管的服務連結角色

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。

如需建立或管理網路安全主管服務連結角色的詳細資訊，請參閱 [使用 AWS Shield 網路安全主管的服務連結角色](#)。

AWS Shield 網路安全主管的身分型政策範例

Note

當您開始使用 AWS Shield 網路安全主管時，我們會自動建立服務連結角色，以滿足所有最低許可要求。建立和管理您自己的身分型政策是選用的。

若要提供適當的網路安全主管存取權，您可以建立身分型政策，授予管理和唯讀存取權的必要許可。

如需建立和管理 IAM 政策的詳細資訊，請參閱《IAM 使用者指南》中的 [受管政策和內嵌政策](#)。

這些許可允許 AWS Shield 網路安全主管執行全面的安全分析，並提供準確的網路安全建議。本指南提供的範例政策是專為常見使用案例而設計。您可以使用這些政策做為起點，並視需要修改以符合您的特定需求。

本指南中的政策範例

- [管理存取身分型政策](#)
- [唯讀存取身分型政策](#)

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、存取或刪除網路安全主管資源。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 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》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](#)。

身分型政策的更新

將更新和功能新增至網路安全主管時，您可能需要更新身分型政策，以包含其他許可。監控本指南，以取得可能需要的新許可相關資訊。

與 AWS 受管政策不同，客戶受管政策不會自動更新。您有責任視需要維護和更新這些政策。

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](#)。

管理存取身分型政策

使用下列範例建立身分型政策，以提供網路安全主管操作的完整管理存取權，以及建立所需服務連結角色的能力。

政策名稱：NetworkSecurityDirectorAdminPolicy

政策描述：允許 AWS Shield 對網路安全主管操作的完整管理存取權，並提供為網路安全主管建立或刪除服務連結角色的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-secusrity-director:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/network-security-
director.amazonaws.com/AWSServiceRoleForNetworkSecurityDirector"
    }
  ]
}
```

唯讀存取身分型政策

使用下列政策範例建立身分型政策，以提供網路安全主管操作的唯讀存取權。

政策名稱：NetworkSecurityDirectorReadOnlyPolicy

政策描述：允許唯讀存取 AWS Shield 網路安全主管。


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

使用 AWS Shield 網路安全主管的服務連結角色

本節說明如何使用服務連結角色，讓 AWS Shield 網路安全主管存取您 AWS 帳戶中的資源。

AWS Shield 網路安全主管使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 AWS Shield 網路安全主管的唯一 IAM 角色類型。服務連結角色由 AWS Shield 網路安全主管預先定義，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 Shield 網路安全主管，因為您不必手動新增必要的許可。AWS Shield 網路安全主管會定義其服務連結角色的許可，除非另有定義，否則只有 AWS Shield 網路安全主管可以擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

請參閱 IAM 主控台中的完整服務連結角色：[NetworkSecurityDirectorServiceLinkedRolePolicy](#)。

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](#)。

如需關於支援服務連結角色的其他服務的資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWS Shield 網路安全主管的服務連結角色許可

NetworkSecurityDirectorServiceLinkedRolePolicy 服務連結角色信任下列服務以擔任角色：

- `network-director.amazonaws.com`

`NetworkSecurityDirectorServiceLinkedRolePolicy` 授予 AWS Shield 網路安全主管代表您存取和分析各種 AWS 資源和服務的許可。其中包含：

- 從 Amazon EC2 資源擷取網路組態和安全性設定
- 存取 CloudWatch 指標以分析網路流量模式
- 收集負載平衡器和目標群組的相關資訊
- 收集 AWS WAF 組態和規則
- 存取 AWS Direct Connect 閘道資訊
- 此外，如以下許可清單所述

下列清單適用於不支援縮小特定資源範圍的許可。其餘部分會針對指定的服務資源縮小範圍。

```
{
  "Sid": "ResourceLevelPermissionNotSupported",
  "Effect": "Allow",
  "Action": [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
```

```

    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:GetManagedPrefixListEntries",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "wafv2:ListWebACLs",
    "cloudfront:ListDistributions",
    "cloudfront:ListTagsForResource",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualInterfaces"
  ],
  "Resource": "*"
}
```

NetworkSecurityDirectorServiceLinkedRolePolicy 服務連結角色許可

下列清單涵蓋NetworkSecurityDirectorServiceLinkedRolePolicy服務連結角色啟用的所有許可。

Amazon CloudFront

```

{
  "Sid": "cloudfront",
  "Effect": "Allow",
  "Action": [
    "cloudfront:GetDistribution"
  ],
  "Resource": "arn:aws:cloudfront::*:distribution/*"
}
```

AWS WAF

```
{
  "Sid": "wafv2",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL",
    "wafv2:ListRuleGroups",
    "wafv2:ListAvailableManagedRuleGroups",
    "wafv2:GetRuleGroup",
    "wafv2:DescribeManagedRuleGroup",
    "wafv2:GetWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2::*:global/rulegroup/*",
    "arn:aws:wafv2::*:regional/rulegroup/*",
    "arn:aws:wafv2::*:global/managedruleset/*",
    "arn:aws:wafv2::*:regional/managedruleset/*",
    "arn:aws:wafv2::*:global/webacl/*/*",
    "arn:aws:wafv2::*:regional/webacl/*/*",
    "arn:aws:apprunner::*:service/*",
    "arn:aws:cognito-idp::*:userpool/*",
    "arn:aws:ec2::*:verified-access-instance/*"
  ]
}
```

AWS WAF 傳統

```
{
  "Sid": "classicWaf",
  "Effect": "Allow",
  "Action": [
    "waf:ListWebACLs",
    "waf:GetWebACL"
  ],
  "Resource": [
    "arn:aws:waf::*:webacl/*",
    "arn:aws:waf-regional::*:webacl/*"
  ]
}
```

AWS Direct Connect

```
{
  "Sid": "directconnect",
  "Effect": "Allow",
  "Action": [
    "directconnect:DescribeConnections",
    "directconnect:DescribeDirectConnectGatewayAssociations",
    "directconnect:DescribeDirectConnectGatewayAttachments",
    "directconnect:DescribeVirtualGateways"
  ],
  "Resource": [
    "arn:aws:directconnect::*:dx-gateway/*",
    "arn:aws:directconnect::*:dxcon/*",
    "arn:aws:directconnect::*:dxlag/*",
    "arn:aws:directconnect::*:dxvif/*"
  ]
}
```

AWS Transit Gateway 路由

```
{
  "Sid": "ec2Get",
  "Effect": "Allow",
  "Action": [
    "ec2:SearchTransitGatewayRoutes"
  ],
  "Resource": [
    "arn:aws:ec2::*:transit-gateway-route-table/*"
  ]
}
```

AWS Network Firewall

```
{
```

```
"Sid": "networkFirewall",
"Effect": "Allow",
"Action": [
    "network-firewall:ListFirewalls",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListRuleGroups",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeRuleGroup"
],
"Resource": [
    "arn:aws:network-firewall:*:*:*/*"
]
}
```

Amazon API Gateway

```
{
  "Sid": "apiGatewayGetAPI",
  "Effect": "Allow",
  "Action": [
    "apigateway:GET"
  ],
  "Resource": [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/apis",
    "arn:aws:apigateway:*::/apis/*",
    "arn:aws:apigateway:*::/tags/*",
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
}
```

為 AWS Shield 網路安全主管建立服務連結角色

您不需要手動建立一個服務連結角色。當您執行第一次網路分析時，AWS Shield 網路安全主管會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 AWS Shield 網路安全主管記錄時，AWS Shield 網路安全主管會再次為您建立服務連結角色。

編輯 AWS Shield 網路安全主管的服務連結角色

AWS Shield 網路安全主管不允許您編

輯 `NetworkSecurityDirectorServiceLinkedRolePolicy` 服務連結角色。因為可能有各種實體參考服務連結角色，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。如需更多資訊，請參閱 IAM 使用者指南中的 [編輯服務連結角色](#)。

刪除 AWS Shield 網路安全主管的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

這可保護您的 AWS Shield 網路安全主管資源，因為您不會不小心移除存取資源的許可。

Note

如果您嘗試刪除資源時 AWS Shield 網路安全主管服務正在使用角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除

`NetworkSecurityDirectorServiceLinkedRolePolicy` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

AWS Shield 網路安全主管服務連結角色支援的 區域

Note

AWS Shield 網路安全主管處於公開預覽版本，可能會有所變更。

AWS Shield 網路安全主管支援在以下區域中使用服務連結角色，並且只能擷取這些區域中資源的資料。

區域名稱	區域
US East (N. Virginia)	us-east-1
Europe (Stockholm)	eu-north-1

使用 記錄 AWS Shield 網路安全主管 API 呼叫 AWS CloudTrail

AWS Shield 網路安全主管與 整合 AWS CloudTrail，將所有 API 呼叫記錄為事件。此整合會擷取從網路安全主管主控台發出的呼叫、對網路安全主管 APIs 程式設計呼叫，以及從其他 AWS 服務發出的呼叫。

使用 CloudTrail，您可以在事件歷史記錄中檢視最近的事件，或建立追蹤，以將持續日誌交付至 Amazon Simple Storage Service 儲存貯體。這些日誌提供每個請求的詳細資訊，包括發起人的身分、時間、請求參數和回應。

若要進一步了解 CloudTrail，請參閱 [「AWS CloudTrail 使用者指南」](#)。

CloudTrail 中的網路安全主管資訊

AWS 您的帳戶會自動啟用 CloudTrail。當網路安全主管中發生活動時，它會在 CloudTrail 中記錄為事件。如需持續記錄事件，請建立將日誌檔案交付至 Amazon S3 儲存貯體的線索。

如需建立和管理追蹤的詳細資訊，請參閱：

- [為 AWS 您的帳戶建立線索](#)
- [AWS 服務與 CloudTrail Logs 的整合](#)
- [從多個區域和帳戶接收 CloudTrail 日誌檔案](#)

CloudTrail 記錄的網路安全主管 API 操作

CloudTrail 會記錄所有網路安全主管 API 操作，並記錄在 API 參考中。包含下列操作：

- StartNetworkSecurityScan：啟動網路安全掃描
- GetNetworkSecurityScan：擷取網路安全掃描的相關資訊
- ListResources：列出服務中可用的資源

- `GetResource`：擷取特定資源的詳細資訊
- `ListFindings`：列出安全性問題清單
- `GetFinding`：擷取特定調查結果的詳細資訊
- `UpdateFinding`：更新問題清單的狀態或其他屬性
- `ListRemediations`：列出問題清單的修復建議
- `ListInsights`：根據調查結果和資源列出洞見

了解網路安全主管日誌檔案項目

CloudTrail 日誌項目包含有關提出請求的人員、提出請求的時間，以及使用哪些參數的資訊。以下是 `StartNetworkSecurityScan` 動作的範例：

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/janedoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2023-11-28T22:02:58Z",
  "eventSource": "network-director.amazonaws.com",
  "eventName": "StartNetworkSecurityScan",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.9.19 Python/3.9.11 Linux/5.15.0-1031-aws botocore/2.4.5",
  "requestParameters": {},
  "responseElements": {
    "scan": {
      "state": "RESCANNING",
      "startTime": "2023-11-28T22:02:58Z"
    }
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "readOnly": false,
  "eventType": "AwsApiCall",
}
```

```
"managementEvent": true,  
"recipientAccountId": "111122223333",  
"eventCategory": "Management"  
}
```

以下是 GetNetworkSecurityScan 動作的範例：

```
{  
  "eventVersion": "1.08",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::111122223333:user/janedoe",  
    "accountId": "111122223333",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
    "userName": "janedoe"  
  },  
  "eventTime": "2023-11-28T22:03:15Z",  
  "eventSource": "network-director.amazonaws.com",  
  "eventName": "GetNetworkSecurityScan",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "192.0.2.0",  
  "userAgent": "aws-cli/2.9.19 Python/3.9.11 Linux/5.15.0-1031-aws botocore/2.4.5",  
  "requestParameters": {},  
  "responseElements": {  
    "scan": {  
      "state": "COMPLETE",  
      "startTime": "2023-11-28T22:02:58Z",  
      "completionTime": "2023-11-28T22:03:15Z"  
    }  
  },  
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",  
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",  
  "readOnly": true,  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "111122223333",  
  "eventCategory": "Management"  
}
```

使用 Amazon CloudWatch 監控 CloudTrail 日誌

您可以使用 Amazon CloudWatch 來監控和提醒 CloudTrail 日誌中的特定 API 活動。這可協助您偵測未經授權的存取嘗試、組態變更或異常活動模式。

若要設定 CloudWatch 監控：

1. 設定 CloudTrail 追蹤以將日誌傳送至 CloudWatch Logs
2. 建立指標篩選條件，從日誌事件擷取特定資訊
3. 根據這些指標建立警示

如需詳細說明，請參閱[使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案](#)。

CloudTrail 與網路安全主管的最佳實務

若要使用 CloudTrail 最大化安全性和可稽核性：

- 在所有區域中啟用 CloudTrail 以獲得全面涵蓋
- 啟用日誌檔案完整性驗證，以偵測未經授權的修改
- 使用 IAM 來控制遵循最低權限原則對 CloudTrail 日誌的存取
- 使用 CloudWatch 警示設定關鍵事件的警示
- 定期檢閱 CloudTrail 日誌以識別異常活動

AWS Firewall Manager

AWS Firewall Manager 可簡化跨多個帳戶和資源的管理和維護任務，以實現各種保護 AWS WAF、AWS Shield Advanced，包括 Amazon VPC 安全群組和網路 ACLs、AWS Network Firewall，以及 Amazon Route 53 Resolver DNS Firewall。使用 Firewall Manager，您只需設定一次保護，服務會自動將保護套用至您的帳戶和資源，即使您新增新帳戶和資源也一樣。

防火牆管理員有這些優點：

- 協助保護跨帳戶的資源
- 協助保護特定類型的所有資源，例如所有 Amazon CloudFront 分佈
- 協助保護有特定標籤的資源
- 自動新增保護到新增至帳戶中的資源
- 可讓您將 AWS Organizations 組織中的所有成員帳戶訂閱 AWS Shield Advanced，並自動訂閱加入組織的新範圍內帳戶
- 允許您將安全群組規則套用至所有會員帳戶或 AWS Organizations 組織中特定帳戶子集，並自動將規則套用至加入組織的範圍內新帳戶
- 可讓您使用自己的規則，或從 購買受管規則 AWS Marketplace

當您想要保護整個組織，而不是少量的特定帳戶和資源，或者您經常新增要保護的新資源時，防火牆管理員特別有用。Firewall Manager 也提供整個組織的 DDoS 攻擊集中監控。

Note

產生的費用 AWS Firewall Manager 適用於基礎服務，例如 AWS WAF 和 AWS Config。如需詳細資訊，請參閱 [AWS Firewall Manager 定價](#)。

主題

- [AWS Firewall Manager 先決條件](#)
- [使用 AWS Firewall Manager 管理員](#)
- [設定 AWS Firewall Manager 政策](#)
- [使用 AWS Firewall Manager 政策](#)
- [使用 Firewall Manager 受管清單](#)

- [在 Firewall Manager 中分組您的資源](#)
- [檢視 AWS Firewall Manager 政策的合規資訊](#)
- [AWS Firewall Manager 與 整合 AWS Security Hub](#)
- [您使用 AWS Firewall Manager 服務的安全性](#)
- [AWS Firewall Manager 配額](#)

AWS Firewall Manager 先決條件

本主題說明如何準備好進行管理 AWS Firewall Manager。您可以使用一個 Firewall Manager 管理員帳戶來管理組織的所有 Firewall Manager 安全政策 AWS Organizations。除非另有說明，否則請使用您將用作 Firewall Manager 管理員的帳戶來執行先決條件步驟。

第一次使用 Firewall Manager 之前，請依序執行下列步驟。

主題

- [使用 Firewall Manager 加入和設定 AWS Organizations](#)
- [建立 AWS Firewall Manager 預設管理員帳戶](#)
- [啟用 AWS Config 以使用 Firewall Manager](#)
- [在 Marketplace 中 AWS 訂閱並設定 Firewall Manager 第三方政策的第三方設定](#)
- [使用 啟用 Network Firewall 和 DNS Firewall 政策的資源共用 AWS RAM](#)
- [AWS Firewall Manager 在預設停用的區域中使用](#)

使用 Firewall Manager 加入和設定 AWS Organizations

若要使用 Firewall Manager，您的帳戶必須是您要使用 Firewall Manager 政策之 AWS Organizations 服務中的組織成員。

Note

如需 Organizations 的相關資訊，請參閱 [AWS Organizations 使用者指南](#)。

建立所需的 AWS Organizations 成員資格和組態

1. 選擇要在 Organizations 中做為組織 Firewall Manager 管理員的帳戶。

2. 如果您選擇的帳戶尚未成為組織的成員，請讓其加入。請遵循[邀請 AWS 帳戶以加入您的組織的指南](#)。
3. 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 Firewall 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[啟用組織中所有功能](#)的指示。

建立 AWS Firewall Manager 預設管理員帳戶

此頁面提供建立 AWS Firewall Manager 預設管理員帳戶的說明。

Note

此程序使用您在上述步驟中選擇和設定的帳戶和組織。

只有組織的管理帳戶可以建立 Firewall Manager 預設管理員帳戶。您建立的第一個管理員帳戶是預設管理員帳戶。預設管理員帳戶可以管理第三方防火牆，並具有完整的管理範圍。當您設定預設管理員帳戶時，防火牆管理員會自動將其設定為 Firewall Manager 的 AWS Organizations 委派管理員。這可讓 Firewall Manager 存取組織中組織單位 (OUs) 的相關資訊。您可以使用 OUs 來指定 Firewall Manager 政策的範圍。如需設定政策範圍的詳細資訊，請參閱下個別政策類型的指南[建立 AWS Firewall Manager 政策](#)。如需 Organizations 和管理帳戶的詳細資訊，請參閱[管理組織中 AWS 的帳戶](#)。

組織管理帳戶的必要設定

組織的管理帳戶必須具有下列設定，才能讓組織加入 Firewall Manager 並建立預設管理員：

- 它必須是您要在 AWS Organizations 其中套用 Firewall Manager 政策的組織成員。

設定預設管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager。
2. 開啟位於 <https://console.aws.amazon.com/wafv2/fmsv2> 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 輸入您選擇用作 Firewall Manager 管理員的帳戶的帳戶 AWS ID。

Note

預設管理員具有完整的管理範圍。完整的管理範圍表示此帳戶可以將政策套用至組織中的所有帳戶和組織單位 (OUs)、在所有區域中採取動作，以及管理所有 Firewall Manager 政策類型。

5. 選擇建立管理員帳戶以建立帳戶。

如需管理 Firewall Manager 管理員帳戶的詳細資訊，請參閱[使用 AWS Firewall Manager 管理員](#)。

啟用 AWS Config 以使用 Firewall Manager

若要使用 Firewall Manager，您必須啟用 AWS Config。

Note

您會根據 AWS Config 定價產生 AWS Config 設定的費用。如需詳細資訊，請參閱[入門 AWS Config](#)。

Note

為了讓 Firewall Manager 監控政策合規性，AWS Config 必須持續記錄受保護資源的組態變更。在您的 AWS Config 組態中，錄製頻率必須設定為連續，這是預設設定。

AWS Config 為 Firewall Manager 啟用

1. AWS Config 為每個 AWS Organizations 成員帳戶啟用，包括 Firewall Manager 管理員帳戶。如需詳細資訊，請參閱[入門 AWS Config](#)。
2. AWS Config 針對包含您要保護之資源 AWS 區域的每個啟用。您可以 AWS Config 手動啟用，也可以在[AWS CloudFormation StackSets 範本](#)中使用 AWS CloudFormation 範本「啟用 AWS Config」。

如果您不想 AWS Config 為所有資源啟用，則必須根據您使用的 Firewall Manager 政策類型啟用下列項目：

- WAF 政策 – 為 CloudFront Distribution、Application Load Balancer (從清單中選擇 ElasticLoadBalancingV2)、API Gateway、WAF WebACL、WAF Regional WebACL 和 WAFv2 WebACL 資源類型啟用 Config。若要啟用 AWS Config 來保護 CloudFront 分佈，您必須位於美國東部 (維吉尼亞北部) 區域。其他區域沒有 CloudFront 做為選項。
- Shield 政策 – 針對 Shield Protection、ShieldRegional Protection、Application Load Balancer、EC2 EIP、WAF WebACL、WAF Regional WebACL 和 WAFv2 WebACL 資源類型啟用 Config。
- 安全群組政策 – 為資源類型 EC2 SecurityGroup、EC2 執行個體和 EC2 NetworkInterface 啟用 Config。
- 網路 ACL 政策 – 為 Amazon EC2 子網路和 Amazon EC2 網路 ACL 資源類型啟用 Config。
- 網路防火牆政策 – 針對 NetworkFirewall FirewallPolicy、NetworkFirewall RuleGroup、EC2 VPC、EC2 InternetGateway、EC2 RouteTable 和 EC2 Subnet 資源類型啟用 Config。
- DNS 防火牆政策 – 為資源類型 EC2 VPC 啟用 Config。
- 第三方防火牆政策 – 為 Amazon EC2 VPC、Amazon EC2 InternetGateway、Amazon EC2 RouteTable、Amazon EC2 Subnet 和 Amazon EC2 VPCEndpoint 資源類型啟用 Config。

Note

如果您將 AWS Config 記錄器設定為使用自訂 IAM 角色，則需要確保 IAM 政策具有記錄 Firewall Manager 政策所需資源類型的適當許可。如果沒有適當的許可，可能不會記錄必要的資源，這會使 Firewall Manager 無法正確保護您的資源。Firewall Manager 無法查看這些許可設定錯誤。如需搭配使用 IAM 的詳細資訊 AWS Config，請參閱 [IAM for AWS Config](#)。

在 Marketplace 中 AWS 訂閱並設定 Firewall Manager 第三方政策的第三方設定

完成下列先決條件以設定 Firewall Manager 第三方防火牆政策。

Fortigate 雲端原生防火牆 (CNF) as a Service 政策先決條件

使用 Fortigate CNF for Firewall Manager

1. 在 AWS Marketplace 中訂閱 [Fortigate 雲端原生防火牆 \(CNF\) 即服務](#)。

2. 首先，在 Fortigate CNF 產品入口網站上註冊租戶。然後，在 Fortigate CNF 產品入口網站的租戶下新增您的 Firewall Manager 管理員帳戶。如需詳細資訊，請參閱 [Fortigate CNF 文件](#)。

如需使用 Fortigate CNF 政策的相關資訊，請參閱 [使用 Fortigate 雲端原生防火牆 \(CNF\) 做為 Firewall Manager 的服務政策](#)。

Palo Alto Networks 雲端新一代防火牆政策先決條件

使用適用於 Firewall Manager 的 Palo Alto Networks Cloud NGFW

1. 訂閱 AWS Marketplace 中的 [Palo Alto Networks 雲端新一代防火牆隨需 Pay-As-You-Go 服務](#)。
2. 完成部署 Palo Alto Networks Cloud NGFW for [中列出的 Palo Alto Networks Cloud NGFW 部署步驟 AWS](#)，並在 [AWS Firewall Manager](#) 部署指南的 Palo Alto Networks Cloud Next Generation Firewall AWS 中完成主題。

如需使用 Palo Alto Networks 雲端 NGFW 政策的相關資訊，請參閱 [使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策](#)。

使用 啟用 Network Firewall 和 DNS Firewall 政策的資源共用 AWS RAM

若要管理 Firewall Manager 網路防火牆和 DNS 防火牆政策，您必須在 AWS Organizations 中啟用與的共用 AWS Resource Access Manager。這可讓 Firewall Manager 在您建立這些政策類型時跨您的帳戶部署保護。

在 AWS Organizations 中啟用與 共享 AWS Resource Access Manager

- 請遵循 AWS Resource Access Manager 使用者指南中的 [啟用與 共享 AWS Organizations](#) 中的指引。

如果您遇到資源共用的問題，請參閱 中的指引 [Network Firewall 和 DNS Firewall 政策的資源共用](#)。

AWS Firewall Manager 在預設停用的區域中使用

若要在預設停用的區域中使用 Firewall Manager，您必須為 AWS 組織的管理帳戶和 Firewall Manager 預設管理員帳戶啟用 區域。如需預設停用的區域以及如何啟用它們的資訊，請參閱 AWS 一般參考中的 [管理 AWS 區域](#)。

啟用停用的區域

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

遵循這些步驟後，您可以設定 Firewall Manager 以開始保護您的資源。如需詳細資訊，請參閱 [設定 AWS Firewall Manager AWS WAF 政策](#)。

使用 AWS Firewall Manager 管理員

此頁面說明什麼是 Firewall Manager 管理員，並定義相關術語。

使用 AWS Firewall Manager，您可以擁有一或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 Firewall Manager 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。這可讓您靈活地在組織中擁有不同的管理員角色，並協助您維持最低權限存取的主體。例如，您可以讓一個管理員為您的組織管理一組組織單位 (OUs)，同時委派另一個管理員僅管理特定的 Firewall Manager 政策類型。如需 Organizations 和管理帳戶的詳細資訊，請參閱 [管理組織中 AWS 的帳戶](#)。

如需每個組織的管理員數量上限，請參閱 [AWS Firewall Manager 配額](#)

開始使用 Firewall Manager 管理員

開始使用 Firewall Manager 管理員之前，您必須完成 中列出的先決條件 [AWS Firewall Manager 先決條件](#)。在先決條件中，您將加入 AWS Organizations 組織至 Firewall Manager，並為 Firewall Manager 建立預設管理員帳戶。預設管理員帳戶能夠管理第三方防火牆，並具有完整的管理範圍。

管理範圍

管理範圍定義 Firewall Manager 管理員可以管理的資源。AWS Organizations 管理帳戶將組織加入 Firewall Manager 之後，管理帳戶可以建立具有不同管理範圍的其他 Firewall Manager 管理員。AWS Organizations 管理帳戶可以授予管理員完整或受限制的管理範圍。完整範圍可讓管理員完整存取上述所有資源類型。限制範圍是指僅將管理許可授予上述資源的子集。我們建議您只授予管理員執行其角色職責所需的許可。您可以將這些管理範圍條件的任意組合套用至管理員：

- 組織中的 帳戶或 OUs，管理員可以套用政策。
- 管理員可在其中執行動作的區域。
- 管理員可以管理的 Firewall Manager 政策類型。

管理員角色

Firewall Manager 中有兩種類型的管理員角色：預設管理員和 Firewall Manager 管理員。

- 預設管理員 - 組織的管理帳戶會在其組織加入 Firewall Manager 時建立 Firewall Manager 預設管理員帳戶，同時完成 [AWS Firewall Manager 先決條件](#)。如果您選擇擁有多個管理員，預設管理員可以管理第三方防火牆，並擁有完整的管理範圍，但其他管理員位於相同的對等層級。
- Firewall Manager 管理員 - Firewall Manager 管理員可以管理管理帳戶在其 AWS Organizations 管理範圍組態中為其指定的資源。如需每個組織可以擁有的管理員數量上限，請參閱 [AWS Firewall Manager 配額](#)。建立 Firewall Manager 管理員帳戶時，服務會使用 AWS Organizations 檢查帳戶是否已經是組織中 Firewall Manager 的委派管理員。如果沒有，則 Firewall Manager 會呼叫 Organizations，將帳戶設定為 Firewall Manager 的委派管理員。如需有關 Organizations 委派管理員的資訊，請參閱AWS Organizations 《使用者指南》中的[AWS Organizations 術語和概念](#)。

現有管理員

如果您是現有的 Firewall Manager 客戶，且已設定管理員，則此現有管理員將是 Firewall Manager 預設管理員。對現有的流程不應有任何影響。如果您想要新增更多管理員，您可以依照本章中的程序執行。

建立 Firewall Manager 管理員帳戶

下列程序說明如何使用 Firewall Manager 主控台建立 Firewall Manager 管理員帳戶。

Note

只有組織的管理帳戶可以建立 Firewall Manager 管理員帳戶。

建立 Firewall Manager 管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager。
2. 開啟位於 <https://console.aws.amazon.com/wafv2/fmsv2> 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 選擇建立管理員帳戶。
5. 在詳細資訊窗格中，針對AWS 帳戶 ID 輸入您要新增為 Firewall Manager 管理員的成員帳戶 AWS ID。
6. 針對管理範圍，選擇下列其中一個選項：

- 完整 – 這可讓管理員將政策套用至組織中的所有帳戶和組織單位 (OUs)、在所有區域中採取動作，以及套用所有 Firewall Manager 政策類型，但第三方防火牆除外。只有預設管理員可以建立和管理第三方防火牆。將此層級的許可授予管理員時，請小心。基於最低權限的精神，我們建議只授予管理員執行其角色職責所需的許可。
- 限制 – 如果套用限制範圍，則在設定管理範圍中設定帳戶和帳戶可管理的組織單位、區域和政策類型。

針對帳戶和組織單位，選擇選項，如下所示：

- 如果您想要將政策套用至組織中的所有帳戶或組織單位，請選擇包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至一組特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

對於區域，選擇選項，如下所示：

- 如果您想要允許管理員在所有可用區域中執行動作，請選擇包含所有區域。
- 如果您希望管理員僅在特定區域中執行動作，請選擇僅包含指定的區域，然後指定您要包含的區域。

 Note

若要包含預設停用的區域，您必須同時為 AWS Organizations 組織管理帳戶和預設管理帳戶啟用區域。如需為帳戶啟用區域的資訊，請參閱 [中的啟用區域](#) Amazon Web Services 一般參考。

針對政策類型，選擇選項，如下所示：

- 如果您想要允許管理員管理所有政策類型，請選擇包含所有政策類型。
- 如果您希望管理員僅管理特定政策類型，請選擇僅包含指定的政策類型，然後指定要包含的政策類型。

7. 選擇建立管理員帳戶以建立管理員帳戶。建立時，Firewall Manager 會呼叫 AWS Organizations 以查看管理員是否已是組織的委派管理員。如果沒有，防火牆管理員會將帳戶指定為委派管理

員。如需有關 Organizations 中委派管理員的資訊，請參閱AWS Organizations 《使用者指南》中的[AWS Organizations 術語和概念](#)。

如果您套用受限制的管理範圍，防火牆管理員會自動根據您的設定評估任何新資源。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將帳戶包含在管理範圍內。

更新 Firewall Manager 管理員帳戶

下列程序說明如何使用 Firewall Manager 主控台更新 Firewall Manager 管理員帳戶。

Note

若要更新管理員的範圍以包含預設停用的區域，您必須同時為 AWS Organizations 組織管理帳戶和預設管理帳戶啟用區域。如需為 帳戶啟用區域的資訊，請參閱 中的[啟用區域](#)Amazon Web Services 一般參考。

只有組織的管理帳戶可以更新 Firewall Manager 管理員帳戶。

更新管理員帳戶（主控台）

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager。
2. 開啟位於 <https://console.aws.amazon.com/wafv2/fmsv2> 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 在 Firewall Manager 管理員資料表中，選擇您要更新的帳戶。
5. 選取編輯以變更管理員帳戶的詳細資訊。您無法變更帳戶 ID。
6. 選擇儲存，以儲存變更。

撤銷 Firewall Manager 管理員帳戶

下列程序說明如何撤銷 Firewall Manager 管理員帳戶。如果您是預設管理員，則在您撤銷帳戶之前，組織中所有 Firewall Manager 管理員帳戶都必須先撤銷自己的帳戶。

Note

只有個別的 Firewall Manager 管理員可以撤銷自己的管理員帳戶。

撤銷管理員帳戶（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。
2. 在導覽窗格中，選擇設定。
3. 在管理員帳戶窗格中，選取撤銷管理員帳戶以撤銷您的帳戶。

Important

當您從管理員帳戶撤銷管理員權限時，該帳戶建立的所有 Firewall Manager 政策都會遭到刪除。

變更預設 Firewall Manager 管理員帳戶

下列程序說明如何變更預設 Firewall Manager 管理員帳戶。

您只能將組織中的一個帳戶指定為預設 Firewall Manager 管理員帳戶。預設管理員帳戶遵循先進先出的原則。若要指定不同的預設管理員帳戶，每個個別管理員帳戶必須先撤銷自己的帳戶。然後，現有的預設管理員可以撤銷自己的帳戶，這也會讓組織從 Firewall Manager 離職。當管理員撤銷其帳戶時，會刪除該帳戶建立的所有 Firewall Manager 政策。若要指定新的預設管理員帳戶，您必須使用 AWS Organizations 管理帳戶登入 Firewall Manager，以指定新的管理員帳戶。若要變更組織的預設管理員帳戶，請執行下列程序。

變更預設管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager。
2. 開啟位於 <https://console.aws.amazon.com/wafv2/fmsv2> 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 輸入您選擇用作 Firewall Manager 管理員的帳戶 ID。

Note

此帳戶獲得許可，可跨組織中的所有帳戶建立和管理 Firewall Manager 政策。

5. 選擇建立管理員帳戶。
6. 輸入您選擇用作 Firewall Manager 管理員的帳戶 AWS ID。

Note

此帳戶會獲得完整的管理範圍。完整的管理範圍表示此帳戶可以將政策套用至組織中的所有帳戶和組織單位 (OUs)、在所有區域中採取動作，以及管理所有 Firewall Manager 政策類型。

7. 選擇建立管理員帳戶以建立預設管理員帳戶。

取消對 Firewall Manager 管理員帳戶進行變更的資格

對管理員帳戶進行的某些變更，可能會使其不符合剩餘管理員帳戶的資格。

本節說明可能取消管理員帳戶資格的變更，以及 AWS 和 Firewall Manager 如何處理這些變更。

在 中從組織移除的帳戶 AWS Organizations

如果 AWS Firewall Manager 管理員帳戶已從 中的組織中移除 AWS Organizations，則無法再管理組織的政策。Firewall Manager 會採取下列其中一個動作：

- 沒有政策的帳戶 – 如果 Firewall Manager 管理員帳戶沒有 Firewall Manager 政策，則 Firewall Manager 會撤銷管理員帳戶。
- 具有 Firewall Manager 政策的帳戶 – 如果 Firewall Manager 管理員帳戶具有 Firewall Manager 政策，則 Firewall Manager 會傳送電子郵件，通知您情況，並在您的 AWS 銷售帳戶代表的協助下提供您可以採取的選項。

帳戶已關閉

如果您關閉用於 AWS Firewall Manager 管理員的帳戶，AWS 且 Firewall Manager 會處理關閉，如下所示：

- AWS 從 Firewall Manager 撤銷帳戶的管理員存取權，且 Firewall Manager 會停用任何由管理員帳戶管理的政策。這些政策提供的保護會在整個組織中停止。
- AWS 從管理員帳戶關閉的生效日期起，會保留帳戶的 Firewall Manager 政策資料 90 天。在此 90 天期間，您可以重新開啟已關閉的帳戶。
 - 如果您在 90 天期間內重新開啟已關閉的帳戶，會將該帳戶重新 AWS 指派為 Firewall Manager 管理員，並復原該帳戶的 Firewall Manager 政策資料。
 - 否則，在 90 天期間結束時，會 AWS 永久刪除帳戶的所有 Firewall Manager 政策資料。

設定 AWS Firewall Manager 政策

您可以使用 AWS Firewall Manager 來啟用多種不同類型的安全政策。每個開始設定的步驟稍微不同。

主題

- [設定 AWS Firewall Manager AWS WAF 政策](#)
- [設定 AWS Firewall Manager AWS Shield Advanced 政策](#)
- [設定 AWS Firewall Manager Amazon VPC 安全群組政策](#)
- [設定 AWS Firewall Manager Amazon VPC 網路 ACL 政策](#)
- [設定 AWS Firewall Manager AWS Network Firewall 政策](#)
- [設定 AWS Firewall Manager upDNS 防火牆政策](#)
- [設定 AWS Firewall Manager Palo Alto Networks 雲端新一代防火牆政策](#)
- [設定 AWS Firewall Manager 強制 CNF 政策](#)

設定 AWS Firewall Manager AWS WAF 政策

若要使用 AWS Firewall Manager 在整個組織中啟用 AWS WAF 規則，請依序執行下列步驟。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立和套用 AWS WAF 政策](#)
- [步驟 3：清除](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。先完成所有的先決條件，再進行[步驟 2：建立和套用 AWS WAF 政策](#)。

步驟 2：建立和套用 AWS WAF 政策

Firewall Manager AWS WAF 政策包含您要套用至資源的規則群組。Firewall Manager 會在您套用政策的每個帳戶中建立 Firewall Manager Web ACL。除了您已定義的規則群組之外，個別帳戶管理員還可以将規則和規則群組新增至產生的 Web ACL。如需 Firewall Manager AWS WAF 政策的詳細資訊，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。

建立 Firewall Manager AWS WAF 政策（主控台）

AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

1. 在導覽窗格中，選擇 Security policies (安全群組政策)。
2. 選擇建立政策。
3. 針對政策類型，選擇 AWS WAF。
4. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 分佈，請選擇全域。

若要保護多個區域中的資源 (CloudFront 分佈除外)，您必須為每個區域建立個別的 Firewall Manager 政策。

5. 選擇下一步。
6. 針對政策名稱，輸入描述性名稱。Firewall Manager 會在其管理的 Web ACLs 名稱中包含政策名稱。Web ACL 名稱 FManagedWebACLV2-後面接著您在此處輸入的政策名稱 - 和 Web ACL 建立時間戳記，以 UTC 毫秒為單位。例如 FManagedWebACLV2-MyWAFPolicyName-1621880374078。

Important

Web ACL 名稱無法在建立後變更。如果您更新政策的名稱，防火牆管理員不會更新相關的 Web ACL 名稱。若要讓 Firewall Manager 建立不同名稱的 Web ACL，您必須建立新的政策。

7. 在 Policy rules (政策規則) 下，針對 First rule groups (第一個規則群組)，選擇 Add rule groups (新增規則群組)。展開 AWS 受管規則群組。對於 Core rule set (核心規則集)，請切換 Add to web ACL (新增至 Web ACL)。對於 AWS 已知錯誤輸入，切換新增至 Web ACL。選擇 Add rules (新增規則)。

對於 Last rule groups (最後一個規則群組)，選擇 Add rule groups (新增規則群組)。展開 AWS 受管規則群組，並在 Amazon IP 評價清單中切換新增至 Web ACL。選擇 Add rules (新增規則)。

在第一個規則群組下，選取核心規則集，然後選擇下移。針對 AWS 已知的錯誤輸入規則群組 AWS WAF 評估 Web 請求，然後再針對核心規則集進行評估。

您也可以視需要使用 AWS WAF 主控台建立自己的 AWS WAF 規則群組。您建立的任何規則群組會顯示在描述政策：新增規則群組頁面的規則群組下。

您透過 Firewall Manager 管理的第一個和最後一個 AWS WAF 規則群組的名稱分別以 PREFMManaged- 或 開頭POSTFMMManaged-，後面接著 Firewall Manager 政策名稱，以及規則群組建立時間戳記，以 UTC 毫秒為單位。例如 PREFMManaged-MyWAFPolicyName-1621880555123。

8. 保留 Web ACL 的預設動作為 Allow (允許)。
9. 將 Policy action (政策動作) 保留為預設狀態，即不自動修補不合規的資源。您可於稍後變更此選項。
10. 選擇下一步。
11. 針對 Policy scope (政策範圍)，您可以提供帳戶的設定、資源類型和用以識別您要套用政策之資源的標記。在本教學課程中，請保留 AWS 帳戶和 資源設定，然後選擇一或多個資源類型。
12. 對於資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，但不能同時使用兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

13. 選擇下一步。
14. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
15. 選擇下一步。
16. 檢閱新的政策設定，並返回您需要進行任何調整的任何頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您檢閱政策在啟用變更之前所做的變更。

17. 當您滿意時，選擇 建立政策。

在AWS Firewall Manager 政策窗格中，應該列出您的政策。它可能會在帳戶標題下指出待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

步驟 3：清除

若要避免額外費用，請刪除任何不必要的政策和資源。

刪除政策 (主控台)

1. 在 AWS Firewall Manager 政策頁面上，選擇政策名稱旁的選項按鈕，然後選擇刪除。
2. 在 Delete (刪除) 確認方塊中，選取 Delete all policy resources (刪除所有政策資源)，然後再次選擇 Delete (刪除)。

AWS WAF 會移除在您的帳戶中建立的政策和任何相關資源，例如 Web ACLs。這些變更可能需要幾分鐘的時間才能傳播到所有帳戶。

設定 AWS Firewall Manager AWS Shield Advanced 政策

您可以使用 AWS Firewall Manager 在整個組織中啟用 AWS Shield Advanced 保護。

Important

Firewall Manager 不支援 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保護這些資源，則無法使用 Firewall Manager 政策。或者，請遵循[將 AWS Shield Advanced 保護新增至 AWS 資源](#)中的說明進行。

若要使用 Firewall Manager 啟用 Shield Advanced 保護，請依序執行下列步驟。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立和套用 Shield Advanced 政策](#)
- [步驟 3：\(選用\) 授權 Shield 回應團隊 \(SRT\)](#)
- [步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。先完成所有的先決條件，再進行 [步驟 2：建立和套用 Shield Advanced 政策](#)。

步驟 2：建立和套用 Shield Advanced 政策

完成先決條件後，您可以建立 AWS Firewall Manager Shield Advanced 政策。Firewall Manager Shield Advanced 政策包含您要使用 Shield Advanced 保護的帳戶和資源。

⚠ Important

Firewall Manager 不支援 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保護這些資源，則無法使用 Firewall Manager 政策。或者，請遵循[將 AWS Shield Advanced 保護新增至 AWS 資源](#)中的說明進行。

建立 Firewall Manager Shield 進階政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

i Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Shield Advanced。

若要建立 Shield Advanced 政策，您的 Firewall Manager 管理員帳戶必須訂閱 Shield Advanced。如果您未訂閱，系統會提示您訂閱。如需訂閱成本的相關資訊，請參閱 [AWS Shield Advanced 定價](#)。

i Note

您不需要手動訂閱每個成員帳戶給 Shield Advanced。Firewall Manager 會在建立政策時為您執行此操作。每個帳戶必須保持訂閱 Firewall Manager 和 Shield Advanced，才能繼續保護帳戶中的資源。

5. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇全域。

若要保護多個區域中的資源 (CloudFront 資源除外)，您必須為每個區域建立個別的 Firewall Manager 政策。

6. 選擇下一步。
7. 針對名稱，輸入描述性名稱。

8. (僅限全球區域) 對於全球區域政策，您可以選擇是否要管理 Shield Advanced 自動應用程式層 DDoS 緩解措施。在本教學課程中，請將此選項保留為忽略的預設設定。
9. 針對政策動作，選擇不會自動修復的選項。
10. 選擇下一步。
11. AWS 帳戶 此政策適用於 ，可讓您透過指定要包含或排除的帳戶來縮小政策的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。
12. 選擇您要保護的資源類型。

Firewall Manager 不支援 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保護這些資源，則無法使用 Firewall Manager 政策。相反地，請遵循的 Shield Advanced 指引[將 AWS Shield Advanced 保護新增至 AWS 資源](#)。

13. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，但不能同時使用兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 選擇下一步。
15. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
16. 選擇下一步。
17. 檢閱新的政策設定，並返回您需要進行任何調整的任何頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您檢閱政策在啟用變更之前所做的變更。

18. 當您滿意時，選擇 建立政策。

在AWS Firewall Manager 政策窗格中，應該列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

繼續進行[步驟 3：\(選用 \) 授權 Shield 回應團隊 \(SRT\)](#)。

步驟 3：(選用) 授權 Shield 回應團隊 (SRT)

的其中一個好處 AWS Shield Advanced 是 Shield 回應團隊 (SRT) 的支援。當您遇到潛在的 DDoS 攻擊時，您可以聯絡 [AWS 支援中心](#)。如有必要，支援中心會將您的問題呈報至 SRT。SRT 可協助您分析可疑活動，並協助您減輕問題。此緩解措施通常涉及在您的帳戶中建立或更新 AWS WAF 規則和 Web ACLs。SRT 可以檢查您的 AWS WAF 組態，並為您建立或更新 AWS WAF 規則和 Web ACLs，但團隊需要您的授權才能執行此操作。我們建議您主動提供 SRT 所需的授權 AWS Shield Advanced，做為設定的一部分。提前提供授權有助於防止在發生實際攻擊時所造成的問題緩解延遲。

您授權並聯絡帳戶層級的 SRT。也就是說，帳戶擁有者，而非 Firewall Manager 管理員，必須執行下列步驟來授權 SRT 以緩解潛在的攻擊。Firewall Manager 管理員只能為他們擁有的帳戶授權 SRT。同樣地，只有帳戶擁有者可以聯絡 SRT 以取得支援。

Note

若要使用 SRT 的服務，您必須訂閱[商業支援計劃](#)或[企業支援計劃](#)。

若要授權 SRT 代表您緩解潛在的攻擊，請遵循 中的指示[使用 Shield Response Team \(SRT\) 支援的受管 DDoS 事件回應](#)。您可以使用相同的步驟，隨時變更 SRT 存取和許可。

繼續進行[步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示](#)。

步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示

您可以繼續此步驟，而無需設定 Amazon SNS 通知或 CloudWatch 警示。不過，設定這些警示和通知可大幅提高您對可能 DDoS 事件的可見性。

您可以使用 Amazon SNS 監控受保護的資源是否有潛在的 DDoS 活動。若要接收可能的攻擊通知，請為每個區域建立 Amazon SNS 主題。

Important

潛在 DDoS 活動的 Amazon SNS 通知不會即時傳送，而且可能會延遲。DDoS 此外，如果您為每個帳戶的每個資源類型超過 Shield Advanced 配額 1,000 個受保護的資源，則 Firewall Manager 效能限制可能會阻止 DDoS 攻擊通知完全成功交付。如需詳細資訊，請參閱[AWS Shield Advanced 配額](#)。

若要啟用潛在 DDoS 活動的即時通知，您可以使用 CloudWatch 警示。您的警示必須根據來自受保護資源存在之帳戶的DDoSDetected指標。

在 Firewall Manager 中建立 Amazon SNS 主題（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中的 AWS FMS 下，選擇設定。
3. 請選擇 Create new topic (建立新主題)。
4. 輸入主題名稱。
5. 輸入 Amazon SNS 訊息將傳送到的電子郵件地址，然後選擇新增電子郵件地址。
6. 選擇更新 SNS 組態。

設定 Amazon CloudWatch 警示

Shield Advanced 會記錄 CloudWatch 中您可以監控的偵測、緩解和最大貢獻者指標。如需詳細資訊，請參閱[AWS Shield Advanced 指標](#)。CloudWatch 會產生額外費用。如需 CloudWatch 定價，請參閱[Amazon CloudWatch 定價](#)。

若要建立 CloudWatch 警示，請遵循[使用 Amazon CloudWatch 警示](#)中的指示。根據預設，Shield Advanced 會設定 CloudWatch，在只顯示一個潛在 DDoS 事件指標之後提醒您。如有需要，您可以使用 CloudWatch 主控台變更此設定，僅在偵測到多個指標時提醒您。

Note

除了警示之外，您也可以使用 CloudWatch 儀表板來監控潛在的 DDoS 活動。儀表板會收集來自 Shield Advanced 的原始資料，並將其處理為可讀且幾近即時的指標。您可以使用 Amazon CloudWatch 中的統計資料來深入了解 Web 應用程式或服務的效能。如需詳細資訊，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[什麼是 CloudWatch](#)。Amazon CloudWatch 如需建立 CloudWatch 儀表板的指示，請參閱 [使用 Amazon CloudWatch 監控](#)。如需可新增至儀表板的特定 Shield Advanced 指標資訊，請參閱 [AWS Shield Advanced 指標](#)。

當您完成 Shield Advanced 組態時，請熟悉您在檢視事件的選項[使用 Shield Advanced 的 DDoS 事件可見性](#)。

設定 AWS Firewall Manager Amazon VPC 安全群組政策

若要使用 AWS Firewall Manager 在整個組織中啟用 Amazon VPC 安全群組，請依序執行下列步驟。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立要在政策中使用的安全群組](#)
- [步驟 3：建立和套用常見的安全群組政策](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。先完成所有的先決條件，再進行 [步驟 2：建立要在政策中使用的安全群組](#)。

步驟 2：建立要在政策中使用的安全群組

在此步驟中，您會建立安全群組，您可以使用 Firewall Manager 在整個組織中套用。

Note

在本教學課程，您不會將自己的安全群組政策套用至組織中的資源。您只會建立政策，然後查看如果將政策的安全群組套用至資源，會發生什麼事？您可以停用政策上的自動修補，來執行此作業。

如果您已定義一般的安全群組，請略過此步驟並移至 [步驟 3：建立和套用常見的安全群組政策](#)。

建立安全群組以用於 Firewall Manager 一般安全群組政策

- 依照 [Amazon VPC 使用者指南](#) 中 [VPC 安全群組的指導](#)，建立您可以套用至組織中所有帳戶和資源的安全群組。

如需安全群組規則選項的資訊，請參閱[安全群組規則參考](#)。

您現在可以前往 [步驟 3：建立和套用常見的安全群組政策](#)。

步驟 3：建立和套用常見的安全群組政策

完成先決條件後，您可以建立 AWS Firewall Manager 常見的安全群組政策。通用安全群組政策為您的整個 AWS 組織提供集中控制的安全群組。它也會定義安全群組套用的 AWS 帳戶和資源。除了常見的安全群組政策之外，防火牆管理員還支援內容稽核安全群組政策、管理組織中正在使用的安全群組規則，以及管理未使用和備援安全群組的用量稽核安全群組政策。如需詳細資訊，請參閱[在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

在本教學課程，您會建立常見安全群組政策，並將其動作設為不要自動修補。這可讓您查看政策會有什麼影響，而不需要變更您的 AWS 組織。

建立 Firewall Manager 一般安全群組政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循說明進行，然後回到此步驟，以建立常見安全群組政策。
4. 選擇 建立政策。
5. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
6. 對於 Security group policy type (安全群組類型)，選擇 Common security groups (常見安全群組)。
7. 針對區域，選擇 AWS 區域。
8. 選擇 Next (下一步)。
9. 針對政策名稱，輸入描述性名稱。
10. Policy rules (政策規則)可讓您選擇如何套用和維護此政策中的安全群組。在本教學課程中，不要勾選選項。
11. 選擇 Add primary security group (新增主要安全群組)、選取您在本教學課程中建立的安全群組，然後選擇 Add security group (新增安全群組)。
12. 對於 Policy action (政策動作)，選擇 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)

13. 選擇 Next (下一步)。
14. AWS 帳戶 受此政策影響的 可讓您透過指定要包含或排除的帳戶來縮小政策的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。
15. 針對資源類型，根據您為 AWS 組織定義的資源，選擇一或多個類型。
16. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而不是兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

17. 選擇 Next (下一步)。
18. 針對政策標籤，新增任何您要新增至 Firewall Manager 政策資源的識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
19. 選擇 Next (下一步)。
20. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前，先檢閱政策所做的變更。

21. 當您滿意時，選擇 建立政策。

在AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

22. 完成探索後，如果不要保留本教學課程建立的政策，請選擇政策名稱、選擇 Delete (刪除)、選擇 Clean up resources created by this policy. (清理此政策建立的資源。)，最後選擇 Delete (刪除)。

如需 Firewall Manager 安全群組政策的詳細資訊，請參閱[在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

設定 AWS Firewall Manager Amazon VPC 網路 ACL 政策

若要使用 AWS Firewall Manager 在整個組織中啟用網路 ACLs，請依序執行本節中的步驟。

如需有關網路 ACLs 的資訊，請參閱《Amazon VPC 使用者指南》中的[使用網路 ACLs 控制子網路的流量](#)。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立網路 ACL 政策](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。先完成所有的先決條件，再進行 [步驟 2：建立網路 ACL 政策](#)。

步驟 2：建立網路 ACL 政策

完成先決條件後，您可以建立 Firewall Manager 網路 ACL 政策。網路 ACL 政策為您的整個 AWS 組織提供集中控制的網路 ACL 定義。它也定義網路 ACL 套用的 AWS 帳戶 和 子網路。

如需 Firewall Manager 網路 ACL 政策的相關資訊，請參閱 [網路 ACL 政策](#)。

如需 Firewall Manager 網路 ACL 政策的一般資訊，請參閱 [網路 ACL 政策](#)。

Note

在本教學課程中，您不會將網路 ACL 政策套用至組織中的子網路。您只需建立政策，並查看將政策的網路 ACL 套用至子網路時會發生什麼情況。您可以停用政策上的自動修補，來執行此作業。

建立 Firewall Manager 網路 ACL 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。

3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循指示，然後返回此步驟以建立網路 ACL 政策。
4. 選擇 建立政策。
5. 針對區域，選擇 AWS 區域。
6. 針對政策類型，選擇網路 ACL。
7. 選擇 Next (下一步)。
8. 針對政策名稱，輸入描述性名稱。
9. 針對網路 ACL 政策規則，定義傳入和傳出流量的第一個和最後一個規則。

您可以在 Firewall Manager 中定義網路 ACL 規則，類似於透過 Amazon VPC 定義規則的方式。唯一的差別在於，您不會自行指派規則編號，而是指派執行每組規則的順序，然後 Firewall Manager 會在儲存政策時為您指派編號。您最多可以定義 5 個傳入規則，以任何方式分割在第一個和最後一個規則之間，而且您最多可以定義 5 個傳出規則。

如需指定網路 ACL 規則的指引，請參閱《Amazon VPC 使用者指南》中的[新增和刪除網路 ACL 規則](#)。

您在 Firewall Manager 政策中定義的規則會指定網路 ACL 必須符合網路 ACL 政策的最低規則組態。例如，網路 ACL 的傳入規則無法符合政策，除非它們以 作為政策的傳入第一個規則，其順序與政策中指定的順序相同。如需詳細資訊，請參閱[網路 ACL 政策](#)。

10. 對於 Policy action (政策動作)，選擇 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)
11. 選擇 Next (下一步)。
12. AWS 帳戶 受此政策影響的 可讓您透過指定要包含或排除的帳戶來縮小政策的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)

網路 ACL 政策的資源類型一律為子網路。

13. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而不是兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 選擇 Next (下一步)。
15. 對於政策標籤，新增任何您要新增至 Firewall Manager 政策資源的識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。

16. 選擇 Next (下一步)。

17. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前，先檢閱政策所做的變更。

18. 當您滿意時，選擇 建立政策。

在 AWS Firewall Manager 政策窗格中，應該列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

19. 當您完成探索時，如果您不想保留為本教學課程建立的政策，請選擇政策名稱、選擇刪除、選擇清除此政策建立的資源，最後選擇刪除。

如需 Firewall Manager 網路 ACL 政策的詳細資訊，請參閱[網路 ACL 政策](#)。

設定 AWS Firewall Manager AWS Network Firewall 政策

若要使用 AWS Firewall Manager 在整個組織中啟用 AWS Network Firewall 防火牆，請依序執行下列步驟。如需 Firewall Manager 網路防火牆政策的詳細資訊，請參閱[在 Firewall Manager 中使用 AWS Network Firewall 政策](#)。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立要在政策中使用的網路防火牆規則群組](#)
- [步驟 3：建立和套用網路防火牆政策](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 2：建立要在政策中使用的網路防火牆規則群組

若要遵循本教學課程，您應該熟悉 AWS Network Firewall 並了解如何設定其規則群組和防火牆政策。

您必須在 Network Firewall 中至少有一個規則群組將用於您的 AWS Firewall Manager 政策。如果您尚未在 Network Firewall 中建立規則群組，請現在執行此操作。如需使用 Network Firewall 的相關資訊，請參閱 [AWS Network Firewall 開發人員指南](#)。

步驟 3：建立和套用網路防火牆政策

完成先決條件後，您可以建立 AWS Firewall Manager Network Firewall 政策。Network Firewall 政策為您的整個 AWS 組織提供集中控制的 AWS Network Firewall 防火牆。它還定義防火牆套用的 AWS 帳戶和資源。

如需 Firewall Manager 如何管理 Network Firewall 政策的詳細資訊，請參閱 [在 Firewall Manager 中使用 AWS Network Firewall 政策](#)。

建立 Firewall Manager 網路防火牆政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您尚未符合先決條件，主控台會顯示如何修正任何問題的指示。遵循指示，然後返回此步驟以建立網路防火牆政策。
4. 選擇建立安全政策。
5. 針對政策類型，選擇 AWS Network Firewall。
6. 針對區域，選擇 AWS 區域。
7. 選擇 Next (下一步)。
8. 針對政策名稱，輸入描述性名稱。
9. 政策組態可讓您定義防火牆政策。這與您在 AWS Network Firewall 主控台中使用的程序相同。您可以新增要在政策中使用的規則群組，並提供預設的無狀態動作。在本教學課程中，請以網路防火牆中防火牆政策的方式設定此政策。

 Note

AWS Firewall Manager Network Firewall 政策會自動進行自動修復，因此您不會在此處看到選擇不自動修復的選項。

10. 選擇 Next (下一步)。
11. 針對防火牆端點，選擇多個防火牆端點。此選項為您的防火牆提供高可用性。當您建立政策時，防火牆管理員會在每個可用區域中建立防火牆子網路，其中有要保護的公有子網路。
12. 針對AWS Network Firewall 路由組態，選擇監控，讓 Firewall Manager 監控 VPCs是否有路由組態違規，並提醒您修復建議，以協助您將路由符合規範。或者，如果您不想讓 Firewall Manager 監控您的路由組態並接收這些提醒，請選擇關閉。

 Note

監控可為您提供因路由組態故障而不合規資源的詳細資訊，並建議來自 Firewall Manager GetViolationDetails API 的修補動作。例如，如果流量未透過政策建立的防火牆端點路由，Network Firewall 會提醒您。

 Warning

如果您選擇監控，則無法在未來針對相同的政策將其變更為關閉。您必須建立新的政策。

13. 針對流量類型，選取新增至防火牆政策，以透過網際網路閘道路由流量。
14. AWS 帳戶 受此政策影響的 可讓您透過指定要包含或排除的帳戶來縮小政策的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)

Network Firewall 政策的資源類型一律為 VPC。

15. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而不是兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

16. 選擇 Next (下一步)。

17. 對於政策標籤，新增任何您要新增至 Firewall Manager 政策資源的識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
18. 選擇 Next (下一步)。
19. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前，先檢閱政策所做的變更。

20. 當您滿意時，選擇 建立政策。

在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

21. 當您完成探索時，如果您不想保留為本教學課程建立的政策，請選擇政策名稱、選擇刪除、選擇清除此政策建立的資源，最後選擇刪除。

如需 Firewall Manager 網路防火牆政策的詳細資訊，請參閱[在 Firewall Manager 中使用 AWS Network Firewall 政策](#)。

設定 AWS Firewall Manager upDNS 防火牆政策

若要使用 AWS Firewall Manager 在整個組織中啟用 Amazon Route 53 Resolver DNS Firewall，請依序執行下列步驟。如需 Firewall Manager DNS Firewall 政策的詳細資訊，請參閱[在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立要在政策中使用的 DNS 防火牆規則群組](#)
- [步驟 3：建立和套用 DNS 防火牆政策](#)

步驟 1：完成先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 2：建立要在政策中使用的 DNS 防火牆規則群組

若要遵循本教學課程，您應該熟悉 Amazon Route 53 Resolver DNS 防火牆，並了解如何設定其規則群組。

您必須在 DNS 防火牆中至少有一個規則群組，該群組將用於您的 AWS Firewall Manager 政策。如果您尚未在 DNS 防火牆中建立規則群組，請現在執行此操作。如需有關使用 DNS 防火牆的資訊，請參閱《[Amazon Route 53 開發人員指南](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html)》中的 [Amazon Route 53 Resolver DNS 防火牆](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html)。 <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

步驟 3：建立和套用 DNS 防火牆政策

完成先決條件後，您可以建立 AWS Firewall Manager DNS 防火牆政策。DNS 防火牆政策為您的整個 AWS 組織提供一組集中控制的 DNS 防火牆規則群組關聯。它還定義防火牆套用的 AWS 帳戶和資源。

如需 Firewall Manager 如何管理 DNS Firewall 規則群組關聯的詳細資訊，請參閱 [在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

建立 Firewall Manager DNS Firewall 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。
2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您尚未符合先決條件，主控台會顯示如何修正任何問題的指示。遵循指示，然後返回此步驟以建立 DNS 防火牆政策。
4. 選擇建立安全政策。
5. 針對政策類型，選擇 Amazon Route 53 Resolver DNS Firewall。
6. 針對區域，選擇 AWS 區域。
7. 選擇 Next (下一步)。
8. 針對政策名稱，輸入描述性名稱。
9. 政策組態可讓您定義要從 Firewall Manager 管理的 DNS 防火牆規則群組關聯。您可以新增要在政策中使用的規則群組。您可以定義關聯，先評估您的 VPCs 再定義一個關聯來評估最後。在此教學課程中，根據您的需求新增一或兩個規則群組關聯。
10. 選擇 Next (下一步)。

11. AWS 帳戶 受此政策影響的 可讓您透過指定要包含或排除的帳戶來縮小政策的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。

DNS 防火牆政策的資源類型一律為 VPC。

12. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而不是兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，Firewall Manager 會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

13. 選擇 Next (下一步)。
14. 針對政策標籤，新增任何您要新增至 Firewall Manager 政策資源的識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
15. 選擇 Next (下一步)。
16. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前，先檢閱政策所做的變更。

17. 當您滿意時，選擇 建立政策。

在AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

18. 當您完成探索時，如果您不想保留為本教學課程建立的政策，請選擇政策名稱、選擇刪除、選擇清除此政策建立的資源，最後選擇刪除。

如需 Firewall Manager DNS 防火牆政策的詳細資訊，請參閱[在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

設定 AWS Firewall Manager Palo Alto Networks 雲端新一代防火牆政策

若要使用 AWS Firewall Manager 啟用 Palo Alto Networks Cloud Next Generation Firewall (NGFW) 政策，請依序執行下列步驟。如需 Palo Alto Networks 雲端 NGFW 政策的詳細資訊，請參閱[使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策](#)。

主題

- [步驟 1：完成一般先決條件](#)
- [步驟 2：完成 Palo Alto Networks 雲端 NGFW 政策先決條件](#)
- [步驟 3：建立和套用 Palo Alto Networks 雲端 NGFW 政策](#)

步驟 1：完成一般先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 2：完成 Palo Alto Networks 雲端 NGFW 政策先決條件

您必須完成幾個額外的必要步驟，才能使用 Palo Alto Networks Cloud NGFW 政策。[Palo Alto Networks 雲端新一代防火牆政策先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 3：建立和套用 Palo Alto Networks 雲端 NGFW 政策

完成先決條件後，您可以建立 AWS Firewall Manager Palo Alto Networks 雲端 NGFW 政策。

如需 Palo Alto Networks Cloud NGFW 的 Firewall Manager 政策的詳細資訊，請參閱 [使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策](#)。

為 Palo Alto Networks Cloud NGFW 建立 Firewall Manager 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Palo Alto Networks Cloud NGFW。如果您尚未在 AWS Marketplace 中訂閱 Palo Alto Networks 雲端 NGFW 服務，您必須先執行此操作。若要在 AWS Marketplace 中訂閱，請選擇檢視 AWS Marketplace 詳細資訊。

5. 針對部署模型，選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 如何管理政策的端點。使用分散式模型時，防火牆管理員會在政策範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，防火牆管理員會在檢查 VPC 中維護單一端點。
6. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 針對政策名稱，輸入描述性名稱。
9. 在政策組態中，選擇要與此政策建立關聯的 Palo Alto Networks Cloud NGFW 防火牆政策。Palo Alto Networks 雲端 NGFW 防火牆政策清單包含與 Palo Alto Networks 雲端 NGFW 租用戶相關聯的所有 Palo Alto Networks 雲端 NGFW 防火牆政策。如需有關建立和管理 Palo Alto Networks Cloud NGFW 防火牆政策的資訊，請參閱部署指南中的[部署 Palo Alto Networks Cloud NGFW for AWS 搭配 AWS Firewall Manager](#) Palo Alto Networks Cloud NGFW 主題 AWS。
10. 對於 Palo Alto Networks 雲端 NGFW 記錄 - 選用，選擇性地選擇要為您的政策記錄的 Palo Alto Networks 雲端 NGFW 日誌類型(s)。如需 Palo Alto Networks 雲端 NGFW 日誌類型的相關資訊，請參閱《[Palo Alto Networks 雲端 NGFW](#)》中的在 上設定 Palo Alto Networks 雲端 NGFW 的日誌記錄 [AWS](#)以取得 AWS 部署指南。

針對日誌目的地，指定 Firewall Manager 應該寫入日誌的時間。

11. 選擇下一步。
12. 在設定第三方防火牆端點下執行下列其中一項操作，取決於您使用分散式或集中式部署模型來建立防火牆端點：
 - 如果您使用此政策的分散式部署模型，請在可用區域下選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
 - 如果您使用此政策的集中式部署模型，請在檢查 VPC AWS Firewall Manager 組態下的端點組態中，輸入檢查 VPC 擁有者 AWS 的帳戶 ID，以及檢查 VPC 的 VPC ID。
 - 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
13. 選擇下一步。
14. 對於政策範圍，AWS 帳戶 在此政策下適用於，選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

Network Firewall 政策的資源類型為 VPC。

15. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

16. 針對授予跨帳戶存取權，選擇下載 AWS CloudFormation 範本。這會下載範本 AWS CloudFormation，供您用來建立 AWS CloudFormation 堆疊。此堆疊會建立 AWS Identity and Access Management 角色，授予 Firewall Manager 跨帳戶許可來管理 Palo Alto Networks Cloud NGFW 資源。如需堆疊的相關資訊，請參閱AWS CloudFormation 《使用者指南》中的[使用堆疊](#)。
17. 選擇下一步。
18. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
19. 選擇下一步。
20. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱政策所做的變更。

21. 當您滿意時，選擇 建立政策。

在AWS Firewall Manager 政策窗格中，應列出您的政策。它可能表示帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取

代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

如需 Firewall Manager Palo Alto Networks 雲端 NGFW 政策的詳細資訊，請參閱[使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策](#)。

設定 AWS Firewall Manager 強制 CNF 政策

Fortigate Cloud Native Firewall (CNF) as a Service 是一種第三方防火牆服務，可用於您的 AWS Firewall Manager 政策。使用 Fortigate CNF for Firewall Manager，您可以建立並集中部署 Fortigate CNF 資源和政策集到所有 AWS 帳戶。若要使用 AWS Firewall Manager 啟用 Fortigate CNF 政策，請依序執行下列步驟。如需 Fortigate CNF 政策的詳細資訊，請參閱[使用 Fortigate 雲端原生防火牆 \(CNF\) 做為 Firewall Manager 的服務政策](#)。

主題

- [步驟 1：完成一般先決條件](#)
- [步驟 2：完成 Fortigate CNF 政策先決條件](#)
- [步驟 3：建立和套用 Fortigate CNF 政策](#)

步驟 1：完成一般先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 2：完成 Fortigate CNF 政策先決條件

您必須完成其他必要步驟，才能使用 Fortigate CNF 政策。[Fortigate 雲端原生防火牆 \(CNF\) as a Service 政策先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

步驟 3：建立和套用 Fortigate CNF 政策

完成先決條件後，您可以建立 AWS Firewall Manager Fortigate CNF 政策。

如需 Fortigate CNF 防火牆管理員政策的詳細資訊，請參閱[使用 Fortigate 雲端原生防火牆 \(CNF\) 做為 Firewall Manager 的服務政策](#)。

為 Fortigate CNF 建立 Firewall Manager 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Fortigate CNF。如果您尚未在 AWS Marketplace 中訂閱 Fortigate CNF 服務，則需要先執行此操作。若要在 AWS Marketplace 中訂閱，請選擇檢視 AWS Marketplace 詳細資訊。
5. 針對部署模型，選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 如何管理政策的端點。使用分散式模型時，防火牆管理員會在政策範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，防火牆管理員會在檢查 VPC 中維護單一端點。
6. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
- 8.
9. 在政策組態中，選擇要與此政策建立關聯的 Fortigate CNF 防火牆政策。Fortigate CNF 防火牆政策清單包含與您的 Fortigate CNF 租戶相關聯的所有 Fortigate CNF 防火牆政策。如需建立和管理 Fortigate CNF 防火牆政策的資訊，請參閱 [Fortigate CNF 文件](#)。
10. 選擇下一步。
11. 在設定第三方防火牆端點下執行下列其中一項操作，取決於您使用分散式或集中式部署模型來建立防火牆端點：
 - 如果您使用此政策的分散式部署模型，請在可用區域下選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
 - 如果您使用此政策的集中式部署模型，請在檢查 VPC AWS Firewall Manager 組態下的端點組態中，輸入檢查 VPC 擁有者 AWS 的帳戶 ID，以及檢查 VPC 的 VPC ID。
 - 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
12. 選擇下一步。

13. 對於政策範圍，AWS 帳戶 在此政策下適用於 ，選擇選項，如下所示：

- 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

Fortigate CNF 政策的資源類型為 VPC。

14. 對於 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

15. 針對授予跨帳戶存取權，選擇下載 AWS CloudFormation 範本。這會下載範本 AWS CloudFormation ，供您用來建立 AWS CloudFormation 堆疊。此堆疊會建立 AWS Identity and Access Management 角色，授予 Firewall Manager 跨帳戶許可來管理 Fortigate CNF 資源。如需堆疊的相關資訊，請參閱AWS CloudFormation 《使用者指南》中的[使用堆疊](#)。若要建立堆疊，您需要來自 Fortigate CNF 入口網站的帳戶 ID。

16. 選擇下一步。

17. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。

18. 選擇下一步。

19. 檢閱新的政策設定，並返回任何您需要調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱政策所做的變更。

20. 當您滿意時，選擇 建立政策。

在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能表示帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

如需 Firewall Manager Fortigate CNF 政策的詳細資訊，請參閱[使用 Fortigate 雲端原生防火牆 \(CNF\) 做為 Firewall Manager 的服務政策](#)。

使用 AWS Firewall Manager 政策

AWS Firewall Manager 提供下列類型的政策。對於每個政策類型，您可以定義：

- AWS WAF 政策 – Firewall Manager 支援 AWS WAF 和 AWS WAF Classic 政策。對於這兩個版本，您可以定義哪些資源受到政策保護。
 - AWS WAF 政策類型會先執行規則群組集，最後在 Web ACL 中執行。然後，在您套用 Web ACL 的帳戶中，帳戶擁有者可以新增規則和規則群組，以在兩組之間執行。
 - AWS WAF Classic 政策類型需要單一規則群組才能在 Web ACL 中執行。
- Shield Advanced 政策 – 此政策類型會針對您指定的資源類型，在整個組織中套用 Shield Advanced 保護。
- Amazon VPC 安全群組政策 – 此政策類型可讓您控制整個組織中正在使用的安全群組，並讓您在整個組織中強制執行一組基準規則。
- Amazon VPC 網路存取控制清單 (ACL) 政策 – 此政策類型可讓您控制整個組織中正在使用的網路 ACLs，並讓您在整個組織中強制執行一組基準網路 ACLs。
- 網路防火牆政策 – 此政策類型會將 AWS Network Firewall 保護套用至組織的 VPCs。
- Amazon Route 53 Resolver DNS 防火牆政策 – 此政策會將 DNS 防火牆保護套用至組織的 VPCs。
- 第三方防火牆政策 – 此政策類型會套用第三方防火牆保護。可透過 Marketplace 的 AWS Marketplace 主控台訂閱第三方防火牆[AWS](#)。
 - Palo Alto Networks 雲端 NGFW 政策 – 此政策類型會將 Palo Alto Networks 雲端新一代防火牆 (NGFW) 保護和 Palo Alto Networks 雲端 NGFW 規則堆疊套用至組織的 VPCs。

- Fortigate 雲端原生防火牆 (CNF) 即服務政策 – 此政策類型會將 Fortigate 雲端原生防火牆 (CNF) 即服務保護套用。Fortigate CNF 是一種以雲端為中心的解決方案，可透過業界領先的進階威脅預防、智慧型 Web 應用程式防火牆 (WAF) 和 API 保護來封鎖零時差威脅並保護雲端基礎設施。

Firewall Manager 政策專屬於個別政策類型。如果您想要跨帳戶強制執行多種政策類型，您可以建立多項政策。您可以為各種類型建立一個以上的政策。

如果您將新帳戶新增至使用建立的組織 AWS Organizations，防火牆管理員會自動將政策套用到該帳戶中在政策範圍內的資源。

AWS Firewall Manager 政策的一般設定

AWS Firewall Manager 受管政策有一些常見的設定和行為。對於所有，您可以指定名稱並定義政策的範圍，而且您可以使用資源標記來控制政策範圍。您可以選擇檢視不合規的帳戶和資源，但不採取修正動作或自動修補不合規的資源。

如需政策範圍的相關資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

建立 AWS Firewall Manager 政策

不同政策類型的政策建立步驟有所不同。務必根據您所需的政策類型使用程序。

Important

AWS Firewall Manager 不支援 Amazon Route 53 或 AWS Global Accelerator。如果您想要使用 Shield Advanced 保護這些資源，則無法使用 Firewall Manager 政策。或者，請遵循[將 AWS Shield Advanced 保護新增至 AWS 資源](#)中的說明進行。

主題

- [為建立 AWS Firewall Manager 政策 AWS WAF](#)
- [為 AWS WAF Classic 建立 AWS Firewall Manager 政策](#)
- [為建立 AWS Firewall Manager 政策 AWS Shield Advanced](#)
- [建立 AWS Firewall Manager 常見安全群組政策](#)
- [建立 AWS Firewall Manager 內容稽核安全群組政策](#)
- [建立 AWS Firewall Manager 用途稽核安全群組政策](#)

- [建立 AWS Firewall Manager 網路 ACL 政策](#)
- [為建立 AWS Firewall Manager 政策 AWS Network Firewall](#)
- [為 Amazon Route 53 Resolver DNS 防火牆建立 AWS Firewall Manager 政策](#)
- [為 Palo Alto Networks 雲端 NGFW 建立 AWS Firewall Manager 政策](#)
- [建立 Fortigate 雲端原生防火牆 \(CNF\) as a Service AWS Firewall Manager 的政策](#)

為建立 AWS Firewall Manager 政策 AWS WAF

在 Firewall Manager AWS WAF 政策中，您可以使用受管規則群組，AWS 和 AWS Marketplace 賣方會為您建立和維護。您也可以建立和使用自己的規則群組。如需規則群組的詳細資訊，請參閱[AWS WAF 規則群組](#)。

如果您想要使用自己的規則群組，請在建立 Firewall Manager AWS WAF 政策之前建立這些規則群組。如需準則，請參閱[管理您自己的規則群組](#)。若要使用個別的自訂規則，您必須定義自己的規則群組、在該群組中定義規則，然後在政策中使用規則群組。

如需 Firewall Manager AWS WAF 政策的詳細資訊，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。

為 AWS WAF（主控台）建立 Firewall Manager 政策

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 AWS WAF。
5. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 分佈，請選擇全域。

若要保護多個區域中的資源 (CloudFront 分佈除外)，您必須為每個區域建立個別的 Firewall Manager 政策。

6. 選擇下一步。

7. 針對政策名稱，輸入描述性名稱。Firewall Manager 會在其管理的 Web ACLs 名稱中包含政策名稱。Web ACL 名稱 FManagedWebACL V2-後面接著您在此處輸入的政策名稱 - 和 Web ACL 建立時間戳記，以 UTC 毫秒為單位。例如 FManagedWebACL V2-MyWAFPolicyName-1621880374078。
 8. 對於 Web 請求內文檢查，選擇性地變更內文大小限制。如需內文檢查大小限制的相關資訊，包括定價考量，請參閱《AWS WAF 開發人員指南》[管理的內文檢查大小限制 AWS WAF](#) 中的。
 9. 在政策規則下，新增 AWS WAF 您要在 Web ACL 中先評估和最後評估的規則群組。若要使用 AWS WAF 受管規則群組版本控制，請切換啟用版本控制。個別帳戶管理員可以在第一個規則群組和最後一個規則群組之間新增規則和規則群組。如需在 Firewall Manager 政策中使用 AWS WAF 規則群組的詳細資訊 AWS WAF，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。

(選用) 若要自訂 Web ACL 如何使用規則群組，請選擇編輯。以下是常見的自訂設定：
 - 對於受管規則群組，請覆寫部分或全部規則的規則動作。如果您未定義規則的覆寫動作，評估會使用規則群組內定義的規則動作。如需此選項的相關資訊，請參閱《AWS WAF 開發人員指南在 [中覆寫規則群組動作 AWS WAF](#)》中的。
 - 有些受管規則群組會要求您提供額外的組態。請參閱受管規則群組提供者的文件。如需 AWS 受管規則規則群組的特定資訊，請參閱《AWS WAF 開發人員指南 [AWS 的受管規則 AWS WAF](#)》中的。
- 完成設定後，請選擇儲存規則。
10. 設定 Web ACL 的預設動作。這是 AWS WAF 在 Web 請求不符合 Web ACL 中的任何規則時所採取的動作。您可以使用允許動作來新增自訂標頭，或新增封鎖動作的自訂回應。如需預設 Web ACL 動作的詳細資訊，請參閱 [在中設定保護套件或 Web ACL 預設動作 AWS WAF](#)。如需設定自訂 Web 請求和回應的資訊，請參閱 [中的自訂 Web 請求和回應 AWS WAF](#)。
 11. 針對記錄組態，選擇啟用記錄以開啟記錄。記錄提供有關 Web ACL 分析流量的詳細資訊。選擇記錄目的地，然後選擇您設定的記錄目的地。您必須選擇名稱開頭為 `aws-waf-logs-` 的記錄目的地。如需設定 AWS WAF 記錄目的地的資訊，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。
 12. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 REDACTED。例如，如果您修訂 URI 欄位，日誌中的 URI 欄位將為 REDACTED。
 13. (選用) 如果您不想將所有請求傳送到日誌，請新增您的篩選條件和行為。在篩選日誌下，針對您要套用的每個篩選條件，選擇新增篩選條件，然後選擇篩選條件，並指定是否要保留或捨棄符合

條件的請求。當您完成新增篩選條件時，如有需要，請修改預設記錄行為。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 [尋找您的保護套件或 Web ACL 記錄](#)。

14. 您可以定義權杖網域清單，以在受保護的應用程式之間啟用權杖共用。當您使用 AWS 受管規則規則群組進行 AWS WAF 詐騙控制帳戶接管預防 (ATP) 和 AWS WAF 機器人控制時，CAPTCHA 和 Challenge 動作以及您實作的應用程式整合 SDKs 會使用字符。

不允許公有字尾。例如，您無法使用 gov.au 或 co.uk 做為字符網域。

根據預設，僅 AWS WAF 接受受保護資源網域的字符。如果您在此清單中新增權杖網域，會 AWS WAF 接受清單中所有網域的權杖，以及相關聯資源的網域。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 [AWS WAF 保護套件或 Web ACL 字符網域清單組態](#)。

當您編輯現有的 Web ACL 時，您只能變更 Web ACL 的 CAPTCHA 和挑戰抗擾性時間。您可以在 Firewall Manager 政策詳細資訊頁面下找到這些設定。如需這些設定的資訊，請參閱 [在中設定時間戳記過期和字符豁免時間 AWS WAF](#)。如果您更新現有政策中的關聯組態、CAPTCHA、挑戰或權杖網域清單設定，防火牆管理員會使用新值覆寫本機 Web ACLs。不過，如果您未更新政策的關聯組態、CAPTCHA、挑戰或字符網域清單設定，則本機 Web ACLs 中的值將保持不變。如需此選項的相關資訊，請參閱《AWS WAF 開發人員指南 [CAPTCHA 和 Challenge 中的 AWS WAF](#)》中的。

15. 在 Web ACL 管理下，選擇 Firewall Manager 如何管理 Web ACL 建立和清除。
 - a. 針對管理未關聯的 Web ACLs，選擇 Firewall Manager 是否管理未關聯的 Web ACLs。使用此選項時，Firewall Manager 只會在至少一個資源將使用 Web ACLs 時，為政策範圍內的帳戶建立 Web ACLs。當帳戶進入政策範圍時，如果至少一個資源將使用它，防火牆管理員會自動在帳戶中建立 Web ACL。

當您啟用此選項時，防火牆管理員會在您的帳戶中執行一次性未關聯的 Web ACLs 清除。清除程序可能需要幾個小時。如果資源在 Firewall Manager 建立 Web ACL 之後離開政策範圍，則 Firewall Manager 會取消資源與 Web ACL 的關聯，但不會清除未關聯的 Web ACL。Firewall Manager 只會在您先在政策中啟用未關聯 Web ACLs 的管理時清除未關聯的 Web ACLs。

 - b. 針對 Web ACL 來源，指定要為範圍內資源建立所有新的 Web ACLs，還是盡可能修改現有的 Web ACLs。Firewall Manager 可以修改範圍內帳戶擁有 ACLs。

預設行為是建立所有新的 Web ACLs。如果您選擇這麼做，則所有由 Firewall Manager 管理 ACLs 都將具有以開頭的名稱 FMManagedWebACL V2。如果您選擇修改現有的 Web ACLs，則修改後的 Web ACLs 將具有以開頭的名稱 FMManagedWebACL V2。

16. 對於政策動作，如果您想要在組織內的每個適用帳戶中建立 Web ACL，但尚未將 Web ACL 套用到任何資源，請選擇識別不符合政策規則的資源，但不會自動修復，也不要選擇管理未關聯的 Web ACLs。您可以稍後變更這些選項。

如果您要改為自動將政策套用至現有的範圍內資源，請選擇 Auto remediate any noncompliant resources (自動修補任何不合規的資源)。如果停用管理未關聯的 Web ACLs，則自動修復任何不合規的資源選項會在組織的每個適用帳戶中建立 Web ACL，並將 Web ACL 與帳戶中的資源建立關聯。如果啟用管理未關聯的 Web ACLs，則自動修復任何不合規資源選項只會在具有資源資格可關聯至 Web ACL 的帳戶中建立並關聯 Web ACL。

當您選擇自動修復任何不合規的資源時，您也可以選擇從範圍內的資源中移除現有 Web ACL 關聯，以用於非由其他作用中 Firewall Manager 政策管理 ACLs。如果您選擇此選項，防火牆管理員會先將政策的 Web ACL 與資源建立關聯，然後移除先前的關聯。如果資源與另一個由不同作用中 Firewall Manager 政策管理的 Web ACL 有關聯，則此選項不會影響該關聯。

17. 選擇下一步。

18. 對於AWS 帳戶 此政策適用於，選擇 選項，如下所示：

- 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用到特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至特定帳戶或 AWS Organizations 組織單位 (OU) 以外的所有人，請選擇 Exclude the specified accounts and organizational units, and include all others (排除指定的帳戶和組織單位，並包含所有其他人)，然後新增您要排除的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

19. 針對 Resource type (資源類型)，請選擇您要保護的資源類型。
20. 對於 資源，您可以使用標記來縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

21. 選擇下一步。
22. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
23. 選擇下一步。
24. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 **建立政策**。在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

為 AWS WAF Classic 建立 AWS Firewall Manager 政策

建立 AWS WAF Classic 的 Firewall Manager 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對 Policy type (政策類型)，選擇 AWS WAF Classic。
5. 如果您已建立要新增至政策的 AWS WAF Classic 規則群組，請選擇建立 AWS Firewall Manager 政策並新增現有的規則群組。如果您想要建立新的規則群組，請選擇建立防火牆管理員政策並新增規則群組。
6. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇全域。

若要保護多個區域中的資源 (CloudFront 資源除外)，您必須為每個區域建立個別的 Firewall Manager 政策。

7. 選擇下一步。
8. 如果您要建立一個規則群組，則遵循[建立 AWS WAF Classic 規則群組](#)的指示。在您建立規則群組，請繼續執行以下步驟。
9. 輸入政策名稱。
10. 如果您要新增現有的規則群組，請使用下拉式功能表選取要新增的規則群組，然後選擇 [新增規則群組]。
11. 政策有兩種動作：規則群組這定的動作和計數。如果您想要測試政策和規則群組，設定動作為計數。這個動作覆寫任何由規則群組中的規則所指定的封鎖動作。也就是說，如果政策的動作是設定為計數，只會計算請求，而不會封鎖請求。反之，如果您設定政策的動作為規則群組設定的動作，則會使用該規則群組規則的動作。選擇適當動作。
12. 選擇下一步。
13. 對於AWS 帳戶 此政策適用於，選擇 選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
 - 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用到新帳戶。

14. 選擇您要保護的資源類型。
15. 對於 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

16. 如果您想自動套用政策到現有的資源，請選擇建立和套用此政策到現有的和新的資源。

此選項是在 AWS 組織內每個可用帳戶中，建立 Web ACL，並將 Web ACL 關聯至帳戶中的資源。此選項還會將政策套用到與前述條件 (資源類型和標籤) 符合的所有新的資源。或者，如果您選擇 Create policy but do not apply the policy to existing or new resources (建立政策，但不套用政策到現有或新的資源)，防火牆管理員在組織內每個可用帳戶內建立 Web ACL，但不套用 Web ACL 到任何資源。之後，您必須將政策套用到資源。選擇適當選項。

17. 對於 [取代現有相關聯的 Web ACL]，您可以選擇移除目前為範圍內資源定義的任何 Web ACL 關聯，然後使用以此政策建立的 Web ACL 關聯來取代它們。根據預設，防火牆管理員不會在新增 Web ACL 關聯之前移除現有的 Web ACL 關聯。如果您要移除現有的 Web ACL 關聯，請選擇此選項。
18. 選擇下一步。
19. 檢視新政策。若要修改，選擇編輯。當您滿意政策時，選擇 Create and apply policy (建立和套用政策)。

為 建立 AWS Firewall Manager 政策 AWS Shield Advanced

建立 Shield Advanced 的 Firewall Manager 政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Shield Advanced。

若要建立 Shield Advanced 政策，您必須訂閱 Shield Advanced。如果您未訂閱，系統會提示您訂閱。如需訂閱成本的相關資訊，請參閱 [AWS Shield Advanced 定價](#)。

5. 針對區域，選擇 AWS 區域。若要保護 Amazon CloudFront 分佈，請選擇全域。

對於全域以外的區域選擇，若要保護多個區域中的資源，您必須為每個區域建立個別的 Firewall Manager 政策。

6. 選擇下一步。

7. 在名稱中，輸入描述性名稱。
8. 僅針對全球區域政策，您可以選擇是否要管理 Shield Advanced 自動應用程式層 DDoS 緩解措施。如需此 Shield Advanced 功能的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

您可以選擇啟用或停用自動緩解，也可以選擇忽略它。如果您選擇忽略它，防火牆管理員完全不會管理 Shield Advanced 保護的自動緩解措施。如需這些政策選項的詳細資訊，請參閱 [搭配 Firewall Manager Shield Advanced 政策使用自動應用程式層 DDoS 緩解](#)。

9. 在 Web ACL 管理下，如果您希望 Firewall Manager 管理未關聯的 Web ACLs，請啟用管理未關聯的 Web ACLs。使用此選項時，Firewall Manager 僅在至少有一個資源將使用 Web ACLs 時，才會在政策範圍內的帳戶中建立 Web ACLs。如果帳戶在任何時候進入政策範圍，且至少一個資源將使用 Web ACL，則 Firewall Manager 會自動在帳戶中建立 Web ACL。啟用此選項後，防火牆管理員會在您的帳戶中執行一次性未關聯的 Web ACLs 清除。清除程序可能需要幾個小時。如果資源在 Firewall Manager 建立 Web ACL 之後離開政策範圍，則 Firewall Manager 不會取消資源與 Web ACL 的關聯。若要在一次性清除中包含 Web ACL，您必須先手動取消資源與 Web ACL 的關聯，然後啟用管理未關聯的 Web ACLs。
10. 針對政策動作，建議您使用 選項建立政策，該選項不會自動修復不合規的資源。當您停用自動修復時，您可以在套用新政策之前評估其效果。當您滿意變更是您想要的，請編輯政策並變更政策動作以啟用自動修復。

如果您要改為自動將政策套用至現有的範圍內資源，請選擇 Auto remediate any noncompliant resources (自動修補任何不合規的資源)。此選項會針對 AWS 組織內的每個適用帳戶和帳戶中的每個適用資源套用 Shield Advanced 保護。

僅適用於全球區域政策，如果您選擇自動修復任何不合規的資源，您也可以選擇讓 Firewall Manager 自動將任何現有的 AWS WAF Classic Web ACL 關聯取代為使用最新版本 AWS WAF (v2) 建立的 Web ACLs 的新關聯。如果您選擇這麼做，Firewall Manager 會移除與舊版 Web ACLs 關聯，並在任何尚未擁有政策的範圍內帳戶中建立新的空 Web ACLs 之後，建立與最新版本 Web ACLs 的新關聯。如需有關此選項的詳細資訊，請參閱 [將 AWS WAF Classic Web ACLs 取代為最新版本 ACLs](#)。

11. 選擇下一步。
12. 對於 AWS 帳戶 此政策適用於，選擇 選項，如下所示：
 - 如果您想要將政策套用至組織中的所有帳戶，請保留預設選擇：包含組織 AWS 下的所有帳戶。
 - 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

13. 選擇您要保護的資源類型。

Firewall Manager 不支援 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保護資源免受這些服務影響，則無法使用 Firewall Manager 政策。請改為遵循 Shield Advanced 指引[將 AWS Shield Advanced 保護新增至 AWS 資源](#)。

14. 對於 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

15. 選擇下一步。

16. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。

17. 選擇下一步。

18. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 建立政策。在AWS Firewall Manager 政策窗格中，應列出您的政策。它可能表示帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

建立 AWS Firewall Manager 常見安全群組政策

如需常見安全群組政策如何運作的資訊，請參閱 [搭配 Firewall Manager 使用常見的安全群組政策](#)。

若要建立常見的安全群組政策，您必須在 Firewall Manager 管理員帳戶中已建立安全群組，以便將其用作政策的主要群組。您可以透過 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全群組。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[使用安全群組](#)。

若要建立常見安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

 Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
5. 對於 Security group policy type (安全群組類型)，選擇 Common security groups (常見安全群組)。
6. 針對區域，選擇 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 對於 Policy rules (政策規則)，執行下列操作：
 - a. 從規則選項中，選擇您要套用至安全群組規則的限制，以及政策範圍內的資源。如果您選擇將標籤從主要安全群組分佈到此政策建立的安全群組，則您還必須選取識別並報告此政策建立的安全群組何時不合規。

 Important

Firewall Manager 不會將 AWS 服務新增的系統標籤分發至複本安全群組。系統標籤以 aws: 字首開頭。此外，如果政策具有與組織標籤政策衝突的標籤，則 Firewall Manager 不會更新現有安全群組的標籤或建立新的安全群組。如需標籤政策的相關資訊，請參閱 AWS Organizations 《使用者指南》中的[標籤政策](#)。

如果您選擇將安全群組參考從主要安全群組分佈到此政策建立的安全群組，則 Firewall Manager 只會在安全群組參考在 Amazon VPC 中具有作用中的對等連線時分佈。如需此選項的相關資訊，請參閱[政策規則設定](#)。

- b. 針對主要安全群組，選擇新增安全群組，然後選擇您要使用的安全群組。Firewall Manager 會填入 Firewall Manager 管理員帳戶中所有 Amazon VPC 執行個體的安全群組清單。

根據預設，每個政策的主要安全群組數量上限為 3。如需有關此設定的詳細資訊，請參閱[AWS Firewall Manager 配額](#)。

- c. 對於 Policy action (政策動作)，我們建議建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。

10. 選擇下一步。

11. 對於 AWS 帳戶 此政策適用於，請選擇 選項，如下所示：

- 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用到特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

12. 針對 Resource type (資源類型)，請選擇您要保護的資源類型。

對於資源類型 EC2 執行個體，您可以選擇修復所有 Amazon EC2 執行個體，或僅修復只有預設主要彈性網路界面 (ENI) 的執行個體。對於後者選項，防火牆管理員不會修復具有其他 ENI 連接的執行個體。相反地，啟用自動修復時，防火牆管理員只會標記這些 EC2 執行個體的合規狀態，而不會套用任何修復動作。請參閱 Amazon EC2 資源類型的其他注意事項和限制[安全群組政策警告和限制](#)。

13. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 對於共用的 VPC 資源，如果您想要在共用 VPC 中將政策套用至資源，除了帳戶擁有的 VPC 之外，請選取 Include resources from shared VPCs (包含來自共用 VPC 的資源)。
15. 選擇下一步。
16. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 會在範圍內帳戶內包含的每個 Amazon VPC 執行個體中建立主要安全群組的複本，每個帳戶最多可達支援的 Amazon VPC 最大配額。Firewall Manager 會將複本安全群組與每個範圍內帳戶的政策範圍內的資源建立關聯。如需此政策如何運作的詳細資訊，請參閱 [搭配 Firewall Manager 使用常見的安全群組政策](#)。

建立 AWS Firewall Manager 內容稽核安全群組政策

如需內容稽核安全群組政策如何運作的資訊，請參閱 [搭配 Firewall Manager 使用內容稽核安全群組政策](#)。

對於某些內容稽核政策設定，您必須為 Firewall Manager 提供稽核安全群組，以用作範本。例如，您可能有一個稽核安全群組，其中包含任何安全群組中不允許的所有規則。您必須使用 Firewall Manager 管理員帳戶建立這些稽核安全群組，才能在政策中使用它們。您可以透過 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全群組。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [使用安全群組](#)。

若要建立內容稽核安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。

3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
5. 對於 Security group policy type (安全群組政策類型)，選擇 Auditing and enforcement of security group rules (稽核和強制執行安全群組規則)。
6. 針對區域，選擇 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 針對政策規則，選擇您要使用的受管或自訂政策規則選項。

a. 對於設定受管稽核政策規則，請執行下列動作：

- i. 針對設定要稽核的安全群組規則，選取您希望稽核政策套用的安全群組規則類型。
- ii. 如果您想要根據安全群組中的通訊協定、連接埠和 CIDR 範圍設定來執行稽核規則等作業，請選擇稽核過度寬鬆的安全群組規則，然後選取您想要的選項。

對於選擇規則允許所有流量，您可以提供自訂應用程式清單來指定您要稽核的應用程式。如需自訂應用程式清單以及如何在政策中使用它們的詳細資訊，請參閱 [使用受管清單](#)和 [使用受管清單](#)。

對於使用通訊協定清單的選擇，您可以使用現有的清單，也可以建立新的清單。如需通訊協定清單以及如何在政策中使用它們的詳細資訊，請參閱 [使用受管清單](#)和 [使用受管清單](#)。

- iii. 如果您想要根據其對預留或非預留 CIDR 範圍的存取權來稽核高風險，請選擇稽核高風險應用程式，然後選取您想要的選項。

下列選項互斥：只能存取預留 CIDR 範圍的應用程式，以及允許存取非預留 CIDR 範圍的應用程式。您最多可以在任何政策中選取其中一個政策。

對於使用應用程式清單的選擇，您可以使用現有的清單，也可以建立新的清單。如需有關應用程式清單以及如何在政策中使用它們的資訊，請參閱 [使用受管清單](#)和 [使用受管清單](#)。

- iv. 使用覆寫設定明確覆寫政策中的其他設定。您可以選擇一律允許或拒絕特定安全群組規則，無論規則是否符合您為政策設定的其他選項。

針對此選項，您會提供稽核安全群組做為允許的規則或拒絕規則範本。針對稽核安全群組，選擇新增稽核安全群組，然後選擇您要使用的安全群組。Firewall Manager 會填入 Firewall Manager 管理員帳戶中所有 Amazon VPC 執行個體的稽核安全群組清單。政策

的稽核安全群組數目的預設限額為一個。如需增加配額的詳細資訊，請參閱[AWS Firewall Manager 配額](#)。

b. 對於設定自訂政策規則，請執行下列動作：

- i. 從規則選項中，選擇是否只允許在稽核安全群組中定義的規則，或拒絕所有規則。如需此選項的詳細資訊，請參閱[搭配 Firewall Manager 使用內容稽核安全群組政策](#)。
- ii. 針對稽核安全群組，選擇新增稽核安全群組，然後選擇您要使用的安全群組。Firewall Manager 會填入 Firewall Manager 管理員帳戶中所有 Amazon VPC 執行個體的稽核安全群組清單。政策的稽核安全群組數目的預設限額為一個。如需增加配額的詳細資訊，請參閱[AWS Firewall Manager 配額](#)。
- iii. 對於 Policy action (政策動作)，您必須建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。

10. 選擇下一步。

11. 對於AWS 帳戶 此政策適用於，選擇 選項，如下所示：

- 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用到特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

12. 對於 Resource type (資源類型)，請選擇您要保護的資源類型。

13. 針對 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 選擇下一步。

15. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 會根據您的政策規則設定，將稽核安全群組與組織中 AWS 的範圍內安全群組進行比較。您可以在政策主控台中檢閱 AWS Firewall Manager 政策狀態。建立政策後，您可以編輯該政策，並啟用自動修補，以使您的稽核安全群組政策生效。如需此政策如何運作的詳細資訊，請參閱 [搭配 Firewall Manager 使用內容稽核安全群組政策](#)。

建立 AWS Firewall Manager 用途稽核安全群組政策

如需用途稽核安全群組政策如何運作的資訊，請參閱 [搭配 Firewall Manager 使用用量稽核安全群組政策](#)。

建立用途稽核安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
5. 針對安全群組政策類型，選擇稽核和清除未關聯和備援的安全群組。
6. 針對區域，選擇 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 對於 Policy rules (政策規則)，選擇一個可用的選項或兩者都選擇。
 - 如果您選擇此政策範圍內的安全群組必須至少由一個資源使用，則 Firewall Manager 會移除其判斷為未使用的任何安全群組。啟用此規則時，防火牆管理員會在您儲存政策時執行它。

如需 Firewall Manager 如何判斷修復用量和時間的詳細資訊，請參閱 [搭配 Firewall Manager 使用用量稽核安全群組政策](#)。

 Note

當您使用此用量稽核安全群組政策類型時，請避免在短時間內對範圍內安全群組的關聯狀態進行多次變更。這樣做可能會導致 Firewall Manager 錯過對應的事件。

根據預設，防火牆管理員會在安全群組未使用時，將安全群組視為不符合此政策規則。您可以選擇性地指定安全群組在被視為不合規之前可以存在的未使用分鐘數，最長可達 525,600 分鐘 (365 天)。您可以使用此設定，讓自己有時間將新的安全群組與資源建立關聯。

 Important

如果您指定預設值為零以外的分鐘數，則必須在其中啟用間接關係 AWS Config。否則，您的用量稽核安全群組政策將無法如預期般運作。如需中間接關係的相關資訊 AWS Config，請參閱《AWS Config 開發人員指南》中的 [中的間接關係 AWS Config](#)。

- 如果您選擇此政策範圍內的安全群組必須是唯一的，則 Firewall Manager 會合併備援安全群組，以便只有一個與任何資源相關聯。如果您選擇這麼做，防火牆管理員會在您儲存政策時先執行它。
10. 對於 Policy action (政策動作)，我們建議建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。
 11. 選擇下一步。
 12. 對於AWS 帳戶 此政策適用於，請選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用到特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
 - 如果您想要將政策套用到除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

13. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 選擇下一步。
15. 如果您尚未從政策範圍中排除 Firewall Manager 管理員帳戶，防火牆管理員會提示您執行此操作。這樣做會在您的手動控制下，將您用於常見和稽核安全群組政策的 Firewall Manager 管理員帳戶中的安全群組保留。在此對話方塊中選擇您想要的選項。
16. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

如果您選擇要求唯一的安全群組，防火牆管理員會掃描每個範圍內 Amazon VPC 執行個體中的備援安全群組。然後，如果您選擇要求至少有一個資源使用每個安全群組，則 Firewall Manager 會掃描規則中指定分鐘內未使用的安全群組。您可以在政策主控台中檢閱 AWS Firewall Manager 政策狀態。如需此政策如何運作的詳細資訊，請參閱 [搭配 Firewall Manager 使用用量稽核安全群組政策](#)。

建立 AWS Firewall Manager 網路 ACL 政策

如需網路 ACL 政策運作方式的相關資訊，請參閱 [網路 ACL 政策](#)。

若要建立網路 ACL 政策，您必須知道如何定義網路 ACL 以搭配 Amazon VPC 子網路使用。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [使用網路 ACLs 控制子網路的流量和使用網路 ACLs](#)。

建立網路 ACL 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

 Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇網路 ACL。
5. 針對區域，選擇 AWS 區域。
6. 選擇下一步。
7. 針對政策名稱，輸入描述性名稱。
8. 針對政策規則，定義您要一律在 Firewall Manager 為您管理的網路 ACLs 中執行的規則。網路 ACLs 會監控和處理傳入和傳出流量，因此在政策中，您可以定義雙向的規則。

對於任一方向，您可以定義要一律先執行的規則，以及要一律最後執行的規則。在 Firewall Manager 管理的網路 ACLs 中，帳戶擁有者可以定義要在這些第一個和最後一個規則之間執行的自訂規則。

9. 針對政策動作，如果您想要識別不合規的子網路和網路 ACLs，但尚未採取任何修正動作，請選擇識別不符合政策規則但不會自動修復的資源。您可以稍後變更這些選項。

如果您想要自動將政策套用至現有的範圍內子網路，請選擇自動修復任何不合規的資源。使用此選項，您也可以指定是否在政策規則的流量處理行為與網路 ACL 中的自訂規則衝突時強制修復。無論您是否強制修復，防火牆管理員都會在其合規違規中報告衝突規則。

10. 選擇下一步。
11. 對於AWS 帳戶 此政策適用於，請選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
 - 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何不同的新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

12. 對於資源類型，設定在子網路中是固定的。
13. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

14. 選擇下一步。
15. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 會建立政策，並根據您的設定開始監控和管理範圍內的網路 ACLs。如需此政策如何運作的詳細資訊，請參閱 [網路 ACL 政策](#)。

為 建立 AWS Firewall Manager 政策 AWS Network Firewall

在 Firewall Manager Network Firewall 政策中，您可以使用您在 中管理的規則群組 AWS Network Firewall。如需有關管理規則群組的資訊，請參閱 Network Firewall 開發人員指南中的 [AWS Network Firewall 規則群組](#)。

如需 Firewall Manager Network Firewall 政策的詳細資訊，請參閱 [在 Firewall Manager 中使用 AWS Network Firewall 政策](#)。

為 AWS Network Firewall (主控台) 建立 Firewall Manager 政策

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
 3. 選擇建立政策。
 4. 針對政策類型，選擇 AWS Network Firewall。
 5. 在防火牆管理類型下，選擇您希望 Firewall Manager 管理政策防火牆的方式。您可以從以下選項中選擇：
 - 分散式 - Firewall Manager 會在政策範圍內的每個 VPC 中建立和維護防火牆端點。
 - 集中 - Firewall Manager 會在單一檢查 VPC 中建立和維護端點。
 - 匯入現有防火牆 - Firewall Manager 使用資源集從 Network Firewall 匯入現有防火牆。如需資源集的詳細資訊，請參閱 [在 Firewall Manager 中分組您的資源](#)。
 6. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
 7. 選擇下一步。
 8. 針對政策名稱，輸入描述性名稱。Firewall Manager 會在其建立的 Network Firewall 防火牆和防火牆政策的名稱中包含政策名稱。
 9. 在AWS Network Firewall 政策組態中，像在 Network Firewall 中一樣設定防火牆政策。新增無狀態和有狀態規則群組，並指定政策的預設動作。您可以選擇性地設定政策的狀態規則評估順序和預設動作，以及記錄組態。如需有關 Network Firewall 防火牆政策管理的資訊，請參閱《AWS Network Firewall 開發人員指南》中的[AWS Network Firewall 防火牆政策](#)。
- 當您建立 Firewall Manager 網路防火牆政策時，防火牆管理員會為範圍內的帳戶建立防火牆政策。個別帳戶管理員可以將規則群組新增至防火牆政策，但無法變更您在此處提供的組態。
10. 選擇下一步。
 11. 根據您在上一個步驟中選取的防火牆管理類型，執行下列其中一項操作：
 - 如果您使用的是分散式防火牆管理類型，請在防火牆端點位置下的端點AWS Firewall Manager 組態中，選擇下列其中一個選項：
 - 自訂端點組態 - Firewall Manager 會在您指定的可用區域中，為政策範圍內的每個 VPC 建立防火牆。每個防火牆至少包含一個防火牆端點。
 - 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
 - 如果您想要為 Firewall Manager 提供 CIDR 區塊，以用於 VPCs 中的防火牆子網路，則它們必須是 /28 CIDR 區塊。每行輸入一個區塊。如果您省略這些，防火牆管理員會從 VPCs 中可用的 IP 地址中為您選擇 IP 地址。

 Note

AWS Firewall Manager Network Firewall 政策會自動進行自動修復，因此您不會在此處看到選擇不自動修復的選項。

- 自動端點組態 - Firewall Manager 會自動在可用區域中建立防火牆端點，並在 VPC 中具有公有子網路。
- 針對防火牆端點組態，指定您希望防火牆端點如何由 Firewall Manager 管理。我們建議您使用多個端點以獲得高可用性。
- 如果您使用的是集中式防火牆管理類型，請在檢查 VPC AWS Firewall Manager 組態下的端點組態中，輸入檢查 VPC 擁有者 AWS 的帳戶 ID，以及檢查 VPC 的 VPC ID。
- 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
- 如果您想要為 Firewall Manager 提供 CIDR 區塊，以用於 VPCs 中的防火牆子網路，則它們必須是 /28 CIDR 區塊。每行輸入一個區塊。如果您省略這些，防火牆管理員會從 VPCs 中可用的 IP 地址中為您選擇 IP 地址。

 Note

AWS Firewall Manager Network Firewall 政策會自動進行自動修復，因此您不會在此處看到選擇不自動修復的選項。

- 如果您使用的是匯入現有的防火牆防火牆管理類型，請在資源集中新增一或多個資源集。資源集會定義組織帳戶擁有的現有 Network Firewall 防火牆，而您要在此政策中集中管理這些防火牆。若要將資源集新增至政策，您必須先使用主控台或 [PutResourceSet](#) API 建立資源集。如需資源集的詳細資訊，請參閱 [在 Firewall Manager 中分組您的資源](#)。如需從 Network Firewall 匯入現有防火牆的詳細資訊，請參閱 [匯入現有防火牆](#)。

12. 選擇下一步。

13. 如果您的政策使用分散式防火牆管理類型，請在路由管理下，選擇 Firewall Manager 是否會監控和提醒必須透過個別防火牆端點路由的流量。

 Note

如果選擇監控，您稍後就無法將設定變更為關閉。監控會持續進行，直到您刪除政策為止。

14. 對於流量類型，選擇性地新增您要透過 路由流量以進行防火牆檢查的流量端點。
15. 對於允許必要的跨可用區域流量，如果您啟用此選項，則 Firewall Manager 會將流量從可用區域傳送出來以檢查的合規路由視為沒有自己的防火牆端點的可用區域。具有端點的可用區域必須一律檢查自己的流量。
16. 選擇下一步。
17. 對於政策範圍，AWS 帳戶 在此政策下適用於 ，選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
 - 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

18. Network Firewall 政策的資源類型為 VPC。
 19. 對於 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。
- 資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。
20. 選擇下一步。
 21. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
 22. 選擇下一步。
 23. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 **建立政策**。在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能表示帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

為 Amazon Route 53 Resolver DNS 防火牆建立 AWS Firewall Manager 政策

在 Firewall Manager DNS Firewall 政策中，您可以使用您在 Amazon Route 53 Resolver DNS Firewall 中管理的規則群組。如需有關管理規則群組的資訊，請參閱《Amazon Route 53 開發人員指南》中的在[DNS 防火牆中管理規則群組和規則](#)。

如需 Firewall Manager DNS Firewall 政策的詳細資訊，請參閱[在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

為 Amazon Route 53 Resolver DNS Firewall 建立 Firewall Manager 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Amazon Route 53 Resolver DNS 防火牆。
5. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
6. 選擇下一步。
7. 針對政策名稱，輸入描述性名稱。
8. 在政策組態中，新增您希望 DNS 防火牆在 VPCs 的規則群組。您最多可以將兩個規則群組新增至政策。

當您建立 Firewall Manager DNS 防火牆政策時，防火牆管理員會使用您提供的關聯優先順序，為範圍內 VPCs 和帳戶建立規則群組關聯。個別帳戶管理員可以在您的第一個和最後一個關聯之間新增規則群組關聯，但無法變更您在此處定義的關聯。如需詳細資訊，請參閱[在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

9. 選擇下一步。

10. 對於AWS 帳戶 此政策適用於，選擇 選項，如下所示：

- 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
- 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

11. DNS 防火牆政策的資源類型為 VPC。

12. 對於 資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

13. 選擇下一步。

14. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。

15. 選擇下一步。

16. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 建立政策。在AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

為 Palo Alto Networks 雲端 NGFW 建立 AWS Firewall Manager 政策

使用 Palo Alto Networks Cloud 新一代防火牆 (Palo Alto Networks Cloud NGFW) 的 Firewall Manager 政策，您可以使用 Firewall Manager 部署 Palo Alto Networks Cloud NGFW 資源，並集中管理所有 AWS 帳戶的 NGFW 規則堆疊。

如需 Firewall Manager Palo Alto Networks 雲端 NGFW 政策的詳細資訊，請參閱 [使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策](#)。如需如何設定和管理適用於 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 的詳細資訊，請參閱文件 [上的 Palo Alto Networks Palo Alto Networks 雲端 NGFW AWS](#)。

先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

為 Palo Alto Networks Cloud NGFW 建立 Firewall Manager 政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Palo Alto Networks Cloud NGFW。如果您尚未在 AWS Marketplace 中訂閱 Palo Alto Networks 雲端 NGFW 服務，您必須先執行此操作。若要在 AWS Marketplace 中訂閱，請選擇檢視 AWS Marketplace 詳細資訊。
5. 針對部署模型，選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 如何管理政策的端點。使用分散式模型時，防火牆管理員會在政策範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，防火牆管理員會在檢查 VPC 中維護單一端點。
6. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 針對政策名稱，輸入描述性名稱。

9. 在政策組態中，選擇要與此政策建立關聯的 Palo Alto Networks Cloud NGFW 防火牆政策。Palo Alto Networks 雲端 NGFW 防火牆政策清單包含與 Palo Alto Networks 雲端 NGFW 租用戶相關聯的所有 Palo Alto Networks 雲端 NGFW 防火牆政策。如需有關建立和管理 Palo Alto Networks Cloud NGFW 防火牆政策的資訊，請參閱部署指南中的[部署 Palo Alto Networks Cloud NGFW for AWS 搭配 AWS Firewall Manager](#) Palo Alto Networks Cloud NGFW 主題 AWS。
10. 對於 Palo Alto Networks 雲端 NGFW 記錄 - 選用，選擇性地選擇要為您的政策記錄的 Palo Alto Networks 雲端 NGFW 日誌類型（哪些）。如需 Palo Alto Networks 雲端 NGFW 日誌類型的相關資訊，請參閱《[Palo Alto Networks 雲端 NGFW](#)》中的在 [上設定 Palo Alto Networks 雲端 NGFW 的日誌記錄 AWS](#) 以取得 AWS 部署指南。

針對日誌目的地，指定 Firewall Manager 應該寫入日誌的時間。

11. 選擇下一步。
12. 在設定第三方防火牆端點下執行下列其中一項操作，取決於您使用分散式或集中式部署模型來建立防火牆端點：
 - 如果您使用此政策的分散式部署模型，請在可用區域下選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
 - 如果您使用此政策的集中式部署模型，請在檢查 VPC AWS Firewall Manager 組態下的端點組態中，輸入檢查 VPC 擁有者 AWS 的帳戶 ID，以及檢查 VPC 的 VPC ID。
 - 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
13. 如果您想要為 Firewall Manager 提供 CIDR 區塊，以用於 VPCs 中的防火牆子網路，則它們必須是 /28 CIDR 區塊。每行輸入一個區塊。如果您省略這些，防火牆管理員會從 VPCs 中可用的 IP 地址中為您選擇 IP 地址。

 Note

AWS Firewall Manager Network Firewall 政策會自動進行自動修復，因此您不會在此處看到選擇不自動修復的選項。

14. 選擇下一步。
15. 對於政策範圍，AWS 帳戶 在此政策下適用於，選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。

- 如果您只想將政策套用至特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您想要將政策套用至除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用至新帳戶。

16. Network Firewall 政策的資源類型為 VPC。

17. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤來包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

18. 針對授予跨帳戶存取權，選擇下載 AWS CloudFormation 範本。這會下載範本 AWS CloudFormation，供您用來建立 AWS CloudFormation 堆疊。此堆疊會建立 AWS Identity and Access Management 角色，授予 Firewall Manager 跨帳戶許可來管理 Palo Alto Networks Cloud NGFW 資源。如需堆疊的相關資訊，請參閱 AWS CloudFormation 《使用者指南》中的 [使用堆疊](#)。

19. 選擇下一步。

20. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱 [使用標籤編輯器](#)。

21. 選擇下一步。

22. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 建立政策。在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能表示帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱 [檢視 AWS Firewall Manager 政策的合規資訊](#)。

建立 Fortigate 雲端原生防火牆 (CNF) as a Service AWS Firewall Manager 的政策

透過適用於 Fortigate CNF 的 Firewall Manager 政策，您可以使用 Firewall Manager 在所有 AWS 帳戶中部署和管理 Fortigate CNF 資源。

如需 Firewall Manager Fortigate CNF 政策的詳細資訊，請參閱 [使用 Fortigate 雲端原生防火牆 \(CNF\) 做為 Firewall Manager 的服務政策](#)。如需有關如何設定 Fortigate CNF 以搭配 Firewall Manager 使用的資訊，請參閱 [Fortinet 文件](#)。

先決條件

為 AWS Firewall Manager 準備您的帳戶有幾個必要的步驟。[AWS Firewall Manager 先決條件](#) 說明這些步驟。請先完成所有先決條件，再繼續進行下一個步驟。

為 Fortigate CNF 建立 Firewall Manager 政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 Fortigate Cloud Native Firewall (CNF) as a Service。如果您尚未在 [AWS Marketplace](#) 中訂閱 [Fortigate CNF 服務](#)，您必須先執行此操作。若要在 AWS Marketplace 中訂閱，請選擇檢視 AWS Marketplace 詳細資訊。
5. 針對部署模型，選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 如何管理政策的端點。使用分散式模型時，防火牆管理員會在政策範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，防火牆管理員會在檢查 VPC 中維護單一端點。
6. 針對區域，選擇 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 針對政策名稱，輸入描述性名稱。
9. 在政策組態中，選擇要與此政策建立關聯的 Fortigate CNF 防火牆政策。Fortigate CNF 防火牆政策清單包含與您的 Fortigate CNF 租戶相關聯的所有 Fortigate CNF 防火牆政策。如需建立和管理 Fortigate CNF 租用戶的資訊，請參閱 [Fortinet 文件](#)。

10. 選擇下一步。
11. 在設定第三方防火牆端點下執行下列其中一項操作，取決於您使用分散式或集中式部署模型來建立防火牆端點：
 - 如果您使用此政策的分散式部署模型，請在可用區域下選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
 - 如果您使用此政策的集中式部署模型，請在檢查 VPC AWS Firewall Manager 組態下的端點組態中，輸入檢查 VPC 擁有者 AWS 的帳戶 ID，以及檢查 VPC 的 VPC ID。
 - 在可用區域下，選取要建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 選取可用區域。
12. 如果您想要為 Firewall Manager 提供 CIDR 區塊，以用於 VPCs 中的防火牆子網路，則它們必須是 /28 CIDR 區塊。每行輸入一個區塊。如果您省略這些項目，防火牆管理員會從 VPCs 中可用的 IP 地址中為您選擇 IP 地址。

 Note

AWS Firewall Manager Network Firewall 政策會自動進行自動修復，因此您不會在此處看到選擇不自動修復的選項。

13. 選擇下一步。
14. 對於政策範圍，AWS 帳戶 在此政策下適用於 ，選擇選項，如下所示：
 - 如果您想要將政策套用到組織中的所有帳戶，請保留預設選擇：包含 AWS 組織下的所有帳戶。
 - 如果您只想將政策套用到特定帳戶或位於特定 AWS Organizations 組織單位 (OUs) 的帳戶，請選擇僅包含指定的帳戶和組織單位，然後新增您要包含的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
 - 如果您想要將政策套用到除特定帳戶或 AWS Organizations 組織單位 (OUs) 以外的所有帳戶或組織單位，請選擇排除指定的帳戶和組織單位，並包含所有其他帳戶，然後新增您要排除的帳戶和 OUs。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

您只能選擇一個選項。

套用政策後，防火牆管理員會自動根據您的設定評估任何新帳戶。例如，如果您只包含特定帳戶，則 Firewall Manager 不會將政策套用到任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子 OUs 時，防火牆管理員會自動將政策套用到新帳戶。

15. Network Firewall 政策的資源類型為 VPC。

16. 對於資源，您可以使用標記縮小政策的範圍，方法是使用您指定的標籤包含或排除資源。您可以使用包含或排除，而非兩者。如需定義政策範圍之標籤的詳細資訊，請參閱 [使用 AWS Firewall Manager 政策範圍](#)。

資源標籤只能有非空值。如果您省略標籤的值，防火牆管理員會以空字串值 "" 儲存標籤。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

17. 針對授予跨帳戶存取權，選擇下載 AWS CloudFormation 範本。這會下載範本 AWS CloudFormation，供您用來建立 AWS CloudFormation 堆疊。此堆疊會建立 AWS Identity and Access Management 角色，授予 Firewall Manager 跨帳戶許可來管理 Fortigate CNF 資源。如需堆疊的相關資訊，請參閱 AWS CloudFormation 《使用者指南》中的 [使用堆疊](#)。若要建立堆疊，您需要來自 Fortigate CNF 入口網站的帳戶 ID。

18. 選擇下一步。

19. 針對政策標籤，新增您要新增至 Firewall Manager 政策資源的任何識別標籤。如需標籤的詳細資訊，請參閱 [使用標籤編輯器](#)。

20. 選擇下一步。

21. 檢閱新的政策設定，並返回任何您需要調整的頁面。

當您滿意時，選擇 建立政策。在 AWS Firewall Manager 政策窗格中，應列出您的政策。它可能會指出帳戶標題下的待定，並指出自動修復設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱 [檢視 AWS Firewall Manager 政策的合規資訊](#)。

刪除 AWS Firewall Manager 政策

您可以執行以下步驟刪除防火牆管理員政策。

刪除政策 (主控台)

1. 在導覽窗格中，選擇 Security policies (安全群組政策)。
2. 選擇您要刪除的政策旁邊的選項。
3. 選擇 刪除。

Note

當您刪除 Firewall Manager 通用安全群組政策時，若要移除政策的複本安全群組，請選擇 選項以清除政策建立的資源。否則，刪除主要執行個體後，複本會保留，並在每個 Amazon VPC 執行個體中需要手動管理。

Important

當您刪除 Firewall Manager Shield Advanced 政策時，政策會遭到刪除，但您的帳戶仍會訂閱 Shield Advanced。

使用 AWS Firewall Manager 政策範圍

此頁面說明什麼是 Firewall Manager 政策範圍及其運作方式。

政策範圍會定義政策適用的位置。您可以將集中控制的政策套用至：

- 您組織內的所有帳戶和資源 AWS Organizations。
- 組織中您帳戶和資源的子集 AWS Organizations。

如需如何設定政策範圍的說明，請參閱 [建立 AWS Firewall Manager 政策](#)。

中的政策範圍選項 AWS Firewall Manager

當您將新帳戶或資源新增至組織時，防火牆管理員會自動針對每個政策的設定進行評估，並根據這些設定套用政策。例如，您可以選擇將政策套用至指定清單中的帳號以外的所有帳戶。資源標籤也可以用來定義政策範圍。您可以選擇套用政策，方法是排除或包含具有清單中所有標籤的資源。或者，您可以選擇僅將政策套用至清單中具有任何指定標籤的資源。

AWS 帳戶 範圍內

您為定義受政策 AWS 帳戶 影響的 所提供的設定，會決定 AWS 組織中要套用政策的帳戶。您可以透過下列方式之一套用政策：

- 套用至您組織中的所有帳戶
- 僅套用至特定包含帳戶號碼與 AWS Organizations 組織單位 (OU) 的清單

- 套用至特定排除帳戶號碼和 AWS Organizations 組織單位 (OU) 之外所有項目的清單

如需的詳細資訊 AWS Organizations，請參閱 [AWS Organizations 使用者指南](#)。

範圍內的資源

與範圍內帳戶的設定類似，您為資源提供的設定會決定要套用政策的範圍內資源類型。您可以選擇下列其中之一：

- 所有資源
- 具有您指定之所有標籤的資源
- 除了具有您指定之所有標籤的資源之外的所有資源
- 只有具有您指定之任何標籤的資源
- 除了只有具有您指定之任何標籤的資源之外的所有資源

您只能指定具有非空值的資源標籤。如果您未提供任何值，Firewall Manager 會儲存具有空字串值的標籤：""。資源標籤僅與具有相同索引鍵和相同值的標籤相符。

如需標記資源的詳細資訊，請參閱 [使用標籤編輯器](#)。

中的政策範圍管理 AWS Firewall Manager

政策到位時，防火牆管理員會持續管理它們，並根據政策範圍將它們套用到新增的新 AWS 帳戶和資源。

Firewall Manager 如何管理 AWS 帳戶和資源

如果帳戶或資源因任何原因超出範圍，AWS Firewall Manager 則不會自動移除保護或刪除 Firewall Manager 管理的資源，除非您選取自動移除離開政策範圍的資源保護核取方塊。

Note

選項 自動移除離開政策範圍的資源保護不適用於 AWS Shield Advanced 或 AWS WAF Classic 政策。

選取此核取方塊 AWS Firewall Manager 會指示自動清除 Firewall Manager 在帳戶離開政策範圍時為帳戶管理的資源。例如，當 Firewall Manager 離開政策範圍時，防火牆管理員會將 Firewall Manager 管理的 Web ACL 與受保護的客戶資源取消關聯。

若要判斷客戶資源離開政策範圍時應從保護中移除哪些資源，防火牆管理員會遵循下列準則：

- 預設行為：
 - 已刪除相關聯的 AWS Config 受管規則。此行為與核取方塊無關。
 - 任何不包含任何資源的相關聯 AWS WAF Web 存取控制清單 (Web ACLs) 都會遭到刪除。此行為與核取方塊無關。
 - 超出範圍的任何受保護資源都會保持關聯和受保護。例如，與 Web ACL 相關聯的 Application Load Balancer 或來自 API Gateway 的 API 會保持與 Web ACL 的關聯，且保護功能會維持在適當狀態。
- 在選取政策範圍核取方塊的情況下，自動移除資源的保護：
 - 已刪除相關聯的 AWS Config 受管規則。此行為與核取方塊無關。
 - 任何不包含任何資源的相關聯 AWS WAF Web 存取控制清單 (Web ACLs) 都會遭到刪除。此行為與核取方塊無關。
 - 超出範圍的任何受保護資源都會自動取消關聯，並在離開政策範圍時從 Firewall Manager 保護中移除。例如，對於安全群組政策，Elastic Inference 加速器或 Amazon EC2 執行個體會在離開政策範圍時自動與複寫的安全群組取消關聯。複寫的安全群組及其資源會自動從保護中移除。

搭配 Firewall Manager 使用 AWS WAF 政策

本節說明如何搭配 Firewall Manager 使用 AWS WAF 政策。在 Firewall Manager AWS WAF 政策中，您可以指定要用來保護政策範圍內所有資源的 AWS WAF 規則群組。當您套用政策時，防火牆管理員會開始使用指定的規則群組和其他政策組態來管理範圍內資源 ACLs。

您可以設定政策來建立和管理範圍內資源的所有新 Web ACLs，取代任何已在使用的 Web ACLs。或者，您可以設定政策以保留任何已與範圍內資源相關聯的 Web ACLs，並加以修改以供政策使用。使用第二個選項，防火牆管理員只會為尚未具有 Web ACLs 關聯的資源建立新的 Web ACL。

無論如何建立，在 Firewall Manager 管理 ACLs 中，除了您在 Firewall Manager 政策中定義的規則群組之外，個別帳戶還可以管理自己的規則和規則群組。

如需建立 Firewall Manager AWS WAF 政策的程序，請參閱 [為建立 AWS Firewall Manager 政策 AWS WAF](#)。

AWS WAF 政策的規則群組管理

由 Firewall Manager AWS WAF 政策管理 ACLs 包含三組規則。這些規則集為 Web ACL 中的規則和規則群組提供較高的優先順序：

- 您在 Firewall Manager AWS WAF 政策中定義的第一個規則群組。會先 AWS WAF 評估這些規則群組。
- Web ACL 中的帳戶管理員所定義的規則和規則群組。AWS WAF 接下來會評估所有帳戶管理的規則或規則群組。
- 您在 Firewall Manager AWS WAF 政策中定義的最後一個規則群組。最後 AWS WAF 評估這些規則群組。

在每組規則中，根據規則集內的優先順序設定，照常 AWS WAF 評估規則和規則群組。

在政策的第一個和最後一個規則群組集中，您只能新增規則群組，而不是個別規則。您可以使用受管規則群組，AWS 受管規則和 AWS Marketplace 賣方會為您建立和維護。您也可以管理和使用自己的規則群組。如需所有這些選項的詳細資訊，請參閱[AWS WAF 規則群組](#)。

如果您想要使用自己的規則群組，請在建立 Firewall Manager AWS WAF 政策之前建立這些規則群組。如需準則，請參閱[管理您自己的規則群組](#)。若要使用個別的自訂規則，您必須定義自己的規則群組、在該群組中定義規則，然後在政策中使用規則群組。

您透過 Firewall Manager 管理的第一個和最後一個 AWS WAF 規則群組的名稱分別以 PREFMManaged- 或 開頭POSTFManaged-，後面接著 Firewall Manager 政策名稱，以及規則群組建立時間戳記，以 UTC 毫秒為單位。例如：PREFMManaged-MyWAFPolicyName-1621880555123。

如需如何 AWS WAF 評估 Web 請求的資訊，請參閱[在中使用保護套件或 Web ACLs 搭配規則和規則群組 AWS WAF](#)。

Firewall Manager 會為您為 AWS WAF 政策定義的規則群組啟用取樣和 Amazon CloudWatch 指標。

個別帳戶擁有者可以完全控制其新增至政策受管 Web ACLs 的任何規則或規則群組的指標和抽樣組態。

AWS WAF 政策的 Web ACL 管理

Firewall Manager 會根據您的組態設定和一般政策管理，建立和管理範圍內資源ACLs。

Note

如果使用[進階自動應用程式層 DDoS 緩解](#)措施設定的資源進入 AWS WAF 政策的範圍，則 Firewall Manager 將無法將政策保護套用至資源，並將資源標記為不合規。

管理未關聯的 Web ACLs組態

當 Web ACLs 不會被任何資源使用時，指定 Firewall Manager 如何管理帳戶 Web ACLs 的政策組態設定。如果您啟用管理未關聯的 Web ACLs，Firewall Manager ACLs中建立 Web ACL，前提是至少有一個資源將使用 Web ACLs。如果您未啟用此選項，防火牆管理員會自動確保每個帳戶都有 Web ACL，無論是否將使用 Web ACL。

啟用此功能時，當帳戶進入政策範圍時，只有在至少一個資源將使用 Web ACL 時，防火牆管理員才會在帳戶中自動建立 Web ACL。

此外，當您啟用管理未關聯的 Web ACLs 時，在建立政策時，防火牆管理員會在您的帳戶中執行一次性未關聯的 Web ACLs 清除。在此清除期間，防火牆管理員會略過您在建立之後修改的任何 Web ACLs，例如，如果您將規則群組新增至 Web ACL 或修改其設定。清除程序可能需要幾個小時。如果資源在 Firewall Manager 建立 Web ACL 後離開政策範圍，則 Firewall Manager 會取消資源與 Web ACL 的關聯，但不會清除未關聯的 Web ACL。Firewall Manager 只有在您第一次在政策中啟用管理未關聯的 Web ACLs 時，才會清除未關聯的 Web ACLs。

在 API 中，此設定位於 [SecurityServicePolicyData](#) 資料類型optimizeUnassociatedWebACL中。

範例：`\\"optimizeUnassociatedWebACL\\":false`

Web ACL 來源組態：建立所有新的或改造現有的？

指定 Firewall Manager 如何處理與範圍內資源相關聯的現有 Web ACLs 的政策組態設定。

根據預設，防火牆管理員會建立範圍內資源的所有新 Web ACLs。透過新增，Firewall Manager 會使用任何已在使用中的現有 Web ACLs，而且只會為尚未建立關聯的資源建立新的 Web ACLs。

當政策設定為新增時，與範圍內資源相關聯的所有 Web ACLs 都會新增新增或標記為不合規。

Firewall Manager 只有在滿足下列需求時，才會修改 Web ACL：

- Web ACL 由客戶帳戶擁有。
- Web ACL 僅與範圍內的資源相關聯。

Tip

設定 AWS WAF 政策進行新增之前，請確定與政策範圍內資源相關聯的 Web ACLs 未與任何out-of-scope資源相關聯。

Tip

如果您想要刪除相關聯的資源，請先將其與 Web ACL 取消關聯。如果 Web ACL 因為與 out-of-scope 資源的關聯而不合規，則刪除 out-of-scope 資源而不先與 Web ACL 取消關聯可能會使 Web ACL 符合合規，然後 Firewall Manager 可以透過修復來修改 Web ACL，但在這種情況下的修復可能會延遲最多 24 小時。

如需存取合規違規詳細資訊的詳細資訊，請參閱 [檢視 AWS Firewall Manager 政策的合規資訊](#)。

如果可以修改 Web ACL，Firewall Manager 會修改它，如下所示：

- Firewall Manager 會將 AWS WAF 政策的第一個規則群組插入 Web ACL 現有規則的前面，並在最後附加 AWS WAF 政策的最後一個規則群組。如需規則群組管理的資訊，請參閱 [AWS WAF 政策的規則群組管理](#)。
- 如果政策具有記錄組態，則 Firewall Manager 只有在 Web ACL 尚未設定為記錄時，才會將其新增至 Web ACL。如果 Web ACL 已透過帳戶設定記錄，則 Firewall Manager 會在新增期間和政策記錄組態的任何後續更新期間將其保留。
- Firewall Manager 不會驗證或設定任何其他 Web ACL 屬性。例如，防火牆管理員不會修改 Web ACL 的預設動作、自訂請求標頭 CAPTCHA 或 Challenge 組態，或是字符網域清單。Firewall Manager 只會在 Firewall Manager 建立 ACLs 上設定這些其他屬性。

Firewall Manager 修改所有現有的相關聯 Web ACLs 之後，對於沒有 Web ACL 的任何範圍內資源，Firewall Manager 會按照預設政策行為處理資源。如果它是 AWS WAF 可以保護的資源，則 Firewall Manager 會建立 Firewall Manager Web ACL 並將其與該資源建立關聯。

在 API 中，Web ACL 來源設定位於 [SecurityServicePolicyData](#) 資料類型 webACLSource 中。範例：`"webACLSource": "RETROFIT_EXISTING"`

取樣和 CloudWatch 指標

AWS Firewall Manager 啟用 Web ACLs 的取樣和 Amazon CloudWatch 指標，以及其為 AWS WAF 政策建立的規則群組。

Web ACL 命名

Firewall Manager 建立的 Web ACL 是以 AWS WAF 政策命名，如下所

示：FMManagedWebACLV2-*policy name*-*timestamp*。時間戳記以 UTC 毫秒為單位。例如 FMManagedWebACLV2-MyWAFPolicyName-1621880374078。

Firewall Manager 新增的 Web ACL 具有客戶帳戶在建立時指定的名稱。Web ACL 名稱無法在建立後變更。

Note

如果設定 [進階自動應用程式層 DDoS 緩解](#) 措施的資源進入 AWS WAF 政策範圍，則 Firewall Manager 將無法將 AWS WAF 政策建立的 Web ACL 與資源建立關聯。

記錄 AWS WAF 政策

您可以為您的 AWS WAF 政策啟用集中式記錄，以取得由組織中的 Web ACL 分析流量的詳細資訊。AWS Firewall Manager 支援此選項 AWS WAFV2，而非 AWS WAF Classic。

日誌中的資訊包括從您的受保護 AWS 資源 AWS WAF 收到請求的時間、請求的詳細資訊，以及每個請求在所有範圍內帳戶比對的規則動作。如需 AWS WAF 記錄的資訊，請參閱《AWS WAF 開發人員指南 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)》中的。

您可以將日誌傳送至 Amazon Data Firehose 資料串流或 Amazon Simple Storage Service (S3) 儲存貯體。每個目的地類型都需要一些額外的組態，以便 Firewall Manager 能夠管理範圍內資源和帳戶的 AWS WAF 日誌記錄。以下各節提供詳細資訊。

如果政策已啟用 Web ACL 修訂，防火牆管理員不會覆寫現有 Web ACLs 中存在的任何記錄組態。如需有關新增的資訊，請參閱 Web ACL 來源組態資訊，網址為 [AWS WAF 政策的 Web ACL 管理](#)。

Note

只能透過 Firewall Manager 介面修改或停用 Firewall Manager 政策的記錄。如果您使用 AWS WAF 來更新或刪除由 Firewall Manager 管理的 Web ACL 記錄組態，則 Firewall Manager 不會自動偵測變更。如果您已使用 AWS WAF，您可以重新評估 AWS WAF 政策的規則，手動提示更新 Firewall Manager 政策 AWS Config。若要這樣做，請在 AWS Config 主控台中尋找 Firewall Manager 政策的 AWS Config 規則，然後選取重新評估動作。

主題

- [記錄目的地](#)
- [在 Firewall Manager 中啟用 AWS WAF 政策的記錄](#)
- [在 Firewall Manager 中停用 AWS WAF 政策的記錄](#)

記錄目的地

本節說明您可以選擇傳送 AWS WAF 政策日誌的記錄目的地。每節都會提供為目的地類型設定記錄的指引，以及目的地類型專屬行為的相關資訊。設定記錄目的地之後，您可以將其規格提供給 Firewall Manager AWS WAF 政策，以開始記錄。

建立記錄組態後，防火牆管理員無法查看日誌失敗。您有責任確認日誌交付是否如預期般運作。

Firewall Manager 不會修改組織成員帳戶中的任何現有記錄組態。

主題

- [Amazon Data Firehose 資料串流](#)
- [Amazon Simple Storage Service 儲存貯體](#)

Amazon Data Firehose 資料串流

本主題提供將 Web ACL 流量日誌傳送至 Amazon Data Firehose 資料串流的資訊。

當您啟用 Amazon Data Firehose 記錄時，防火牆管理員會將日誌從政策的 Web ACLs 傳送至您已設定儲存目的地的 Amazon Data Firehose。啟用記錄後，會透過 Kinesis Data Firehose 的 HTTPS 端點，將每個已設定 Web ACL 的日誌 AWS WAF 傳遞至已設定的儲存目的地。使用之前，請先測試您的交付串流，以確保其具有足夠的輸送量來容納組織的日誌。如需如何建立 Amazon Kinesis Data Firehose 和檢閱存放日誌的詳細資訊，請參閱[什麼是 Amazon Data Firehose？](#)

您必須具有下列許可，才能成功啟用 Kinesis 記錄：

- iam:CreateServiceLinkedRole
- firehose:ListDeliveryStreams
- wafv2:PutLoggingConfiguration

當您在 AWS WAF 政策上設定 Amazon Data Firehose 記錄目的地時，防火牆管理員會在 Firewall Manager 管理員帳戶中為政策建立 Web ACL，如下所示：

- Firewall Manager 在 Firewall Manager 管理員帳戶中建立 Web ACL，無論帳戶是否在政策範圍內。

- Web ACL 已啟用日誌名稱的記錄功能 `FMMangedWebACL` V2-Logging *policy name-timestamp*，其中時間戳記是為 Web ACL 啟用日誌的 UTC 時間，以毫秒為單位。例如：`FMMangedWebACL` V2-LoggingMyWAFPolicyName-1621880565180。Web ACL 沒有規則群組，也沒有相關聯的資源。
- 根據 AWS WAF 定價準則，您需要支付 Web ACL 的費用。如需詳細資訊，請參閱 [AWS WAF 定價](#)。
- Firewall Manager 會在您刪除政策時刪除 Web ACL。

如需服務連結角色和 `iam:CreateServiceLinkedRole` 許可的相關資訊，請參閱 [使用的服務連結角色 AWS WAF](#)。

如需建立交付串流的詳細資訊，請參閱 [建立 Amazon Data Firehose 交付串流](#)。

Amazon Simple Storage Service 儲存貯體

本主題提供將 Web ACL 流量日誌傳送至 Amazon S3 儲存貯體的資訊。

您選擇做為記錄目的地的儲存貯體必須由 Firewall Manager 管理員帳戶擁有。如需建立 Amazon S3 儲存貯體以進行記錄和儲存貯體命名需求的相關資訊，請參閱《AWS WAF 開發人員指南》中的 [Amazon Simple Storage Service](#)。

最終一致性

當您變更使用 Amazon S3 記錄目的地設定 AWS WAF 的政策時，Firewall Manager 會更新儲存貯體政策，以新增記錄所需的許可。執行此操作時，防火牆管理員會遵循 Amazon Simple Storage Service 遵循的 last-writer-wins 語意和資料一致性模型。如果您同時在 Firewall Manager 主控台或透過 [PutPolicy](#) API 對 Amazon S3 目的地進行多個政策更新，則可能不會儲存某些許可。如需 Amazon S3 資料一致性模型的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 [Amazon S3 資料一致性模型](#)。

將日誌發佈至 Amazon S3 儲存貯體的許可

在 AWS WAF 政策中為 Amazon S3 儲存貯體設定 Web ACL 流量記錄需要下列許可設定。當您將 Amazon S3 設定為您的記錄目的地，以授予服務將日誌發佈至儲存貯體的許可時，防火牆管理員會自動將這些許可連接到您的 Amazon S3 儲存貯體。如果您想要管理對日誌記錄和 Firewall Manager 資源的更精細存取，您可以自行設定這些許可。如需有關管理許可的資訊，請參閱《IAM 使用者指南》中的 [存取資源的 AWS 管理](#)。如需 AWS WAF 受管政策的相關資訊，請參閱 [AWS 的受管政策 AWS WAF](#)。

```
{
```

```

"Version": "2012-10-17",
"Id": "AWSLogDeliveryForFirewallManager",
"Statement": [
  {
    "Sid": "AWSLogDeliveryAclCheckFMS",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX"
  },
  {
    "Sid": "AWSLogDeliveryWriteFMS",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX/policy-id/
AWSLogs/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
      }
    }
  }
]
}

```

為了防止跨服務混淆代理問題，您可以將 [aws:SourceArn](#) 和 [aws:SourceAccount](#) 全域條件內容索引鍵新增至儲存貯體的政策。若要新增這些金鑰，您可以在設定記錄目的地時修改 Firewall Manager 為您建立的政策，或者如果您想要精細控制，您可以建立自己的政策。如果您將這些條件新增至記錄目的地政策，防火牆管理員不會驗證或監控混淆代理保護。如需混淆代理人問題的一般資訊，請參閱[混淆代理人問題](#)

IAM 使用者指南中的。

當您新增 `sourceAccounts` `sourceArn` 屬性時，它會增加儲存貯體政策大小。如果您要新增較長的 `sourceAccount` 新增 `sourceArn` 屬性清單，請小心不要超過 Amazon S3 儲存[貯體政策大小](#)配額。

下列範例示範如何在儲存貯體的政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵，以防止混淆代理人問題。將 *member-account-id* 取代為您組織中成員的帳戶 IDs。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForFirewallManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheckFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "member-account-id",
            "member-account-id"
          ]
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:logs:*:member-account-id:",
            "arn:aws:logs:*:member-account-id:"
          ]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryWriteFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::aws-waf-logs-LOGGING-BUCKET-SUFFIX/policy-id/AWSLogs/
*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": [
            "member-account-id",
            "member-account-id"
          ]
        }
      }
    }
  ]
}
```

```

    },
    "ArnLike": {
      "aws:SourceArn": [
        "arn:aws:logs:*:member-account-id-1:*",
        "arn:aws:logs:*:member-account-id-2:*"
      ]
    }
  }
}
]
}

```

Amazon S3 儲存貯體的伺服器端加密

您可以啟用 Amazon S3 伺服器端加密，或在 S3 儲存貯體上使用 AWS Key Management Service 客戶受管金鑰。如果您選擇在 Amazon S3 儲存貯體上使用預設的 Amazon S3 加密作為 AWS WAF 日誌，則不需要採取任何特殊動作。不過，如果您選擇使用客戶提供的加密金鑰來加密靜態 Amazon S3 資料，則必須將下列許可陳述式新增至 AWS Key Management Service 金鑰政策：

```

{
  "Sid": "Allow Logs Delivery to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}

```

如需搭配 Amazon S3 使用客戶提供的加密金鑰的資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[搭配客戶提供的金鑰 \(SSE-C\) 使用伺服器端加密](#)。

在 Firewall Manager 中啟用 AWS WAF 政策的記錄

下列程序說明如何在 Firewall Manager 主控台中啟用 AWS WAF 政策的記錄。

啟用 AWS WAF 政策的記錄

1. 您必須先將記錄目的地資源設定為下列內容，才能啟用記錄：
 - Amazon Kinesis Data Streams - 使用您的 Firewall Manager 管理員帳戶建立 Amazon Data Firehose。使用開頭為字首 的名稱aws-waf-logs-。例如：aws-waf-logs-firewall-manager-central。使用PUT來源和您正在操作的區域中建立資料 Firehose。如果您要擷取 Amazon CloudFront 的日誌，請在美國東部（維吉尼亞北部）建立 firehose。使用之前，請先測試您的交付串流，以確保其具有足夠的輸送量來容納組織的日誌。如需詳細資訊，請參閱[建立 Amazon Kinesis Data Firehose 交付串流](#)。
 - Amazon Simple Storage Service 儲存貯體 - 根據 AWS WAF 開發人員指南中的 Amazon Simple Storage Service 主題中的指導方針建立 Amazon S3 儲存貯體。<https://docs.aws.amazon.com/waf/latest/developerguide/logging-s3.html>您還必須使用 中列出的許可來設定 Amazon S3 儲存貯體將日誌發佈至 Amazon S3 儲存貯體的許可。
 2. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。
- 
- ### Note
- 如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。
3. 在導覽窗格中，選擇安全政策。
 4. 選擇您要啟用記錄 AWS WAF 的政策。如需有關 AWS WAF 記錄的詳細資訊，請參閱 [記錄 AWS WAF 保護套件或 Web ACL 流量](#)。
 5. 在政策詳細資訊索引標籤的政策規則區段中，選擇編輯。
 6. 針對記錄組態，選擇啟用記錄以開啟記錄。記錄提供有關 Web ACL 分析流量的詳細資訊。選擇記錄目的地，然後選擇您設定的記錄目的地。您必須選擇名稱開頭為 的記錄目的地aws-waf-logs-。如需設定 AWS WAF 記錄目的地的詳細資訊，請參閱 [搭配 Firewall Manager 使用 AWS WAF 政策](#)。
 7. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 REDACTED。例如，如果您編輯 URI 欄位，日誌中的 URI 欄位將為 REDACTED。
 8. (選用) 如果您不想將所有請求傳送至日誌，請新增您的篩選條件和行為。在篩選日誌下，針對您要套用的每個篩選條件，選擇新增篩選條件，然後選擇篩選條件，並指定是否要保留或捨棄符合

條件的請求。當您完成新增篩選條件時，如有需要，請修改預設記錄行為。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 [尋找您的保護套件或 Web ACL 記錄](#)。

9. 選擇 Next (下一步)。
10. 檢閱您的設定，然後選擇儲存以儲存對政策的變更。

在 Firewall Manager 中停用 AWS WAF 政策的記錄

下列程序說明如何在 Firewall Manager 主控台中停用 AWS WAF 政策的記錄。

停用 AWS WAF 政策的記錄

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

 Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇安全政策。
3. 選擇您要停用記錄 AWS WAF 的政策。
4. 在政策詳細資訊索引標籤的政策規則區段中，選擇編輯。
5. 針對記錄組態狀態，選擇停用。
6. 選擇 Next (下一步)。
7. 檢閱您的設定，然後選擇儲存以儲存對政策的變更。

 Note

只能透過 Firewall Manager 介面修改或停用 Firewall Manager 政策的記錄。如果您使用 AWS WAF 來更新或刪除由 Firewall Manager 管理的 Web ACL 記錄組態，則 Firewall Manager 不會自動偵測變更。如果您已使用 AWS WAF，您可以重新評估 AWS WAF 政策的規則，手動提示更新 Firewall Manager 政策 AWS Config。若要這樣做，請在 AWS Config 主控台中尋找 Firewall Manager 政策的 AWS Config 規則，然後選取重新評估動作。

在 Firewall Manager 中使用 AWS Shield Advanced 政策

此頁面說明如何搭配 Firewall Manager 使用 AWS Shield 政策。在 Firewall Manager AWS Shield 政策中，您可以選擇要保護的資源。當您在啟用自動修復的情況下套用政策時，對於尚未與 AWS WAF Web ACL 建立關聯的每個範圍內資源，防火牆管理員會將空的 AWS WAF Web ACL 建立關聯。空白 Web ACL 用於 Shield 監控目的。如果您接著將任何其他 Web ACL 與資源建立關聯，則 Firewall Manager 會移除空的 Web ACL 關聯。

Note

當 AWS WAF 政策範圍內的資源進入以[自動應用程式層 DDoS 緩解](#)設定的 Shield Advanced 政策範圍時，Firewall Manager 只會在關聯 AWS WAF 政策建立的 Web ACL 之後套用 Shield Advanced 保護。

如何在 Shield 政策中 AWS Firewall Manager 管理未關聯的 Web ACLs

您可以設定 Firewall Manager 透過政策中的管理未關聯的 Web ACLs 設定，或 API 中的 [SecurityServicePolicyData](#) 資料類型 `optimizeUnassociatedWebACLs` 設定，來為您管理未關聯的 Web ACLs。如果您啟用政策中未關聯的 Web ACLs 管理，則 Firewall Manager 僅在 Web ACLs 將由至少一個資源使用時，才會在政策範圍內的帳戶中建立 Web ACLs。如果帳戶在任何時候進入政策範圍，且至少一個資源將使用 Web ACL，則 Firewall Manager 會自動在帳戶中建立 Web ACL。

當您啟用管理未關聯的 Web ACLs 時，防火牆管理員會執行您帳戶中未關聯的 Web ACLs 的一次性清除。清除程序可能需要幾個小時的時間。如果資源在 Firewall Manager 建立 Web ACL 後離開政策範圍，則 Firewall Manager 不會取消資源與 Web ACL 的關聯。如果您希望 Firewall Manager 清除 Web ACL，您必須先手動取消資源與 Web ACL 的關聯，然後在政策中啟用管理未關聯的 Web ACLs 選項。

如果您未啟用此選項，則 Firewall Manager 不會管理未關聯的 Web ACLs，且 Firewall Manager 會在政策範圍內的每個帳戶中自動建立 Web ACL。

如何 AWS Firewall Manager 管理 Shield 政策中的範圍變更

帳戶和資源可能會因為許多變更而超出 AWS Firewall Manager Shield Advanced 政策的範圍，例如政策範圍設定的變更、資源上的標籤變更，以及從組織移除帳戶。如需政策範圍設定的一般資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

使用 AWS Firewall Manager Shield Advanced 政策，如果帳戶或資源超出範圍，Firewall Manager 會停止監控帳戶或資源。

如果帳戶因從組織中移除而超出範圍，則會繼續訂閱 Shield Advanced。由於帳戶不再是合併帳單系列的一部分，因此帳戶將產生按比例分配的 Shield Advanced 訂閱費用。另一方面，超出範圍但仍在組織中的帳戶不會產生額外費用。

如果資源超出範圍，它將繼續受到 Shield Advanced 保護，並繼續產生 Shield Advanced 資料傳輸費用。

搭配 Firewall Manager Shield Advanced 政策使用自動應用程式層 DDoS 緩解

此頁面說明自動應用程式層 DDoS 緩解如何與 Firewall Manager 搭配使用。

當您將 Shield Advanced 政策套用至 Amazon CloudFront 分佈或 Application Load Balancer 時，您可以選擇在政策中設定 Shield Advanced 自動應用程式層 DDoS 緩解措施。

如需有關 Shield Advanced 自動緩解的資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

Shield Advanced 自動應用程式層 DDoS 緩解有下列需求：

- 自動應用程式層 DDoS 緩解僅適用於 Amazon CloudFront 分佈和 Application Load Balancer。

如果將 Shield Advanced 政策套用至 Amazon CloudFront 分佈，您可以針對為全球區域建立的 Shield Advanced 政策選擇此選項。如果將保護套用至 Application Load Balancer，您可以將政策套用到 Firewall Manager 支援的任何區域。

- 自動應用程式層 DDoS 緩解僅適用於使用最新版本 AWS WAF (v2) 建立的保護套件或 Web ACLs。

因此，如果您的政策使用 AWS WAF Classic Web ACLs，您需要將政策取代為新的政策，這會自動使用最新版本的 AWS WAF，或讓 Firewall Manager 為您現有的政策建立新的 Web ACLs 版本，並切換到使用它們。如需選項的詳細資訊，請參閱 [將 AWS WAF Classic Web ACLs 取代為最新版本 ACLs](#)。

自動緩解組態

Firewall Manager Shield Advanced 政策的自動應用程式層 DDoS 緩解選項會將 Shield Advanced 自動緩解功能套用至政策的範圍內帳戶和資源。如需此 Shield Advanced 功能的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

您可以選擇讓 Firewall Manager 為政策範圍內的 CloudFront 分佈或 Application Load Balancer 啟用或停用自動緩解，也可以選擇讓政策忽略 Shield Advanced 自動緩解設定：

- 啟用 – 如果您選擇啟用自動緩解，您也可以指定緩解 Shield Advanced 規則是否應計數或封鎖相符的 Web 請求。如果範圍內的資源未啟用自動緩解，或者使用的規則動作與您為政策指定的規則動作不相符，則 Firewall Manager 會將這些資源標記為不合規。如果您設定政策進行自動修復，防火牆管理員會視需要更新不合規的資源。
- 停用 – 如果您選擇停用自動緩解，防火牆管理員會在啟用自動緩解時，將範圍內資源標記為不合規。如果您設定政策進行自動修復，防火牆管理員會視需要更新不合規的資源。
- 忽略 – 如果您選擇忽略自動緩解，則 Firewall Manager 在為政策執行修補活動時，不會考慮 Shield 政策中的任何自動緩解設定。此設定可讓您透過 Shield Advanced 控制自動緩解，而不需要 Firewall Manager 覆寫這些設定。此設定不適用於透過 Shield Advanced 管理的任何 Classic Load Balancer 或彈性 IPs 資源，因為 Shield Advanced 目前不支援這些資源的 L7 自動緩解。

將 AWS WAF Classic Web ACLs 取代為最新版本 ACLs

自動應用程式層 DDoS 緩解僅適用於使用最新版本 AWS WAF (v2) 建立的保護套件或 Web ACLs。

若要判斷 Shield Advanced 政策的 Web ACL 版本，請參閱 [判斷 Shield Advanced 政策 AWS WAF 使用的版本](#)。

如果您想要在 Shield Advanced 政策中使用自動緩解，且您的政策目前使用 AWS WAF Classic Web ACLs，您可以建立新的 Shield Advanced 政策來取代目前的政策，或者您可以使用本節所述的選項，將舊版 Web ACLs 取代為目前 Shield Advanced 政策中的新 (v2) Web ACLs。新政策一律使用最新版本的 建立 Web ACLs AWS WAF。如果您取代整個政策，當您刪除它時，也可以讓 Firewall Manager 刪除所有較早版本的 Web ACLs。本節的其餘部分說明取代現有政策內 Web ACLs 的選項。

當您修改 Amazon CloudFront 資源的現有 Shield Advanced 政策時，防火牆管理員可以在尚未擁有 v2 Web ACL 的任何範圍內帳戶中，自動為政策建立新的 empty AWS WAF (v2) Web ACL。當 Firewall Manager 建立新的 Web ACL 時，如果政策在相同帳戶中已有 AWS WAF Classic Web ACL，則 Firewall Manager 會使用與現有 Web ACL 相同的預設動作設定來設定新版本 Web ACL。如果沒有現有的 AWS WAF Classic Web ACL，防火牆管理員會在新的 Web ACL Allow 中將預設動作設為。Firewall Manager 建立新的 Web ACL 之後，您可以透過 主控台視需要 AWS WAF 加以自訂。

當您選擇下列任一政策組態選項時，防火牆管理員會為尚未擁有這些選項的範圍內帳戶建立新的 (v2) Web ACLs：

- 當您啟用或停用自動應用程式層 DDoS 緩解時。此選項只會導致 Firewall Manager 建立新的 Web ACLs，而不是取代政策範圍內資源上任何現有的 AWS WAF Classic Web ACL 關聯。

- 當您選擇自動修復的政策動作，並選擇將 AWS WAF Classic Web ACLs 取代為 AWS WAF (v2) Web ACLs 的選項。無論您的自動應用程式層 DDoS 緩解組態選擇為何，都可以選擇取代舊版 Web ACLs。

當您選擇取代選項時，防火牆管理員會視需要建立新的 Web ACLs 版本，然後針對政策的範圍內資源執行下列動作：

- 如果資源與任何其他作用中 Firewall Manager 政策的 Web ACL 相關聯，則 Firewall Manager 會單獨保留關聯。
- 對於任何其他情況，防火牆管理員會移除與 AWS WAF Classic Web ACL 的任何關聯，並將資源與政策的 AWS WAF (v2) Web ACL 建立關聯。

您可以選擇讓 Firewall Manager 在需要時將舊版 Web ACLs 取代為新版本的 Web ACLs。如果您先前已自訂政策的 AWS WAF Classic Web ACLs，您可以在選擇讓 Firewall Manager 執行取代步驟之前，將新版本的 Web ACLs 更新為類似的設定。

您可以透過適用於或 AWS WAF Classic 的相同版本主控台存取政策的任一 Web ACL 版本。

除非您刪除政策本身，否則 Firewall Manager 不會刪除任何已取代的 AWS WAF Classic Web ACLs。在政策不再使用 AWS WAF Classic Web ACLs 之後，您可以視需要將其刪除。

判斷 Shield Advanced 政策 AWS WAF 使用的 版本

此頁面說明如何判斷 Shield Advanced 政策使用的 AWS WAF Web ACL 版本。

您可以查看政策 AWS Config 的服務連結規則中的參數索引鍵，來判斷 AWS WAF Firewall Manager Shield Advanced 政策使用哪個版本。如果使用中的 AWS WAF 版本是最新的，則參數索引鍵包含 `policyId` 和 `webAclArn`。如果是舊版，AWS WAF Classic，參數索引鍵會包含 `webAclId` 和 `resourceTypes`。

此 AWS Config 規則只會列出政策目前搭配範圍內資源使用的 Web ACLs 金鑰。

若要判斷 AWS WAF Firewall Manager Shield Advanced 政策使用哪個版本

1. 擷取 Shield Advanced 政策的政策 ID：

- AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台 <https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

- b. 在導覽窗格中，選擇安全政策。
- c. 選擇政策的區域。對於 CloudFront 分佈，這是 Global。
- d. 尋找您想要的政策，並複製其政策 ID 的值。

範例政策 ID：1111111-2222-3333-4444-a55aa5aaa555。

2. 透過將政策 ID 附加至字串 來建立政策的 AWS Config 規則名稱 FMManagedShieldConfigRule。

範例 AWS Config 規則名稱：FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555。

3. 針對名為 policyId 和 的索引鍵，搜尋相關 AWS Config 規則的參數 webAclArn：
 - a. 在 <https://console.aws.amazon.com/config/home> 開啟 AWS Config 主控台。
 - b. 在導覽窗格中，選擇規則。
 - c. 在清單中尋找您 Firewall Manager 政策的 AWS Config 規則名稱，然後選取它。規則的頁面隨即開啟。
 - d. 在規則詳細資訊下，在參數區段中，查看金鑰。如果您找到名為 policyId 和 的金鑰 webAclArn，政策會使用使用最新版本 建立的 Web ACLs AWS WAF。如果您找到名為 webAclId 和 的金鑰 resourceTypes，政策會使用使用舊版 AWS WAF Classic 建立的 Web ACLs。

在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組

此頁面說明如何使用 AWS Firewall Manager 安全群組政策來管理組織的 Amazon Virtual Private Cloud 安全群組 AWS Organizations。您可以將集中控制的安全群組政策套用至整間組織，或選取您的帳戶和資源子集。您也可以監控並管理在您組織中使用的安全群組政策，以及監控稽核和用途安全群組政策。

Firewall Manager 會持續維護您的政策，並在在整個組織中新增或更新這些政策時將其套用至帳戶和資源。如需的詳細資訊 AWS Organizations，請參閱 [AWS Organizations 使用者指南](#)。

如需有關 Amazon Virtual Private Cloud 安全群組的資訊，請參閱《Amazon [VPC 使用者指南](#)》中的 [VPC 的安全群組](#)。

您可以使用 Firewall Manager 安全群組政策，在整個 AWS 組織中執行下列動作：

- 將常見安全群組套用至指定的帳戶和資源。

- 稽核安全群組規則，以尋找和修補不合規規則。
- 稽核安全群組的用途，以清理未使用的與備援安全群組。

本節涵蓋 Firewall Manager 安全群組政策的運作方式，並提供使用政策的指引。如需建立安全群組政策的程序，請參閱 [建立 AWS Firewall Manager 政策](#)。

安全群組政策的最佳實務

本節列出使用 AWS Firewall Manager 管理安全群組的建議。

排除 Firewall Manager 管理員帳戶

當您設定政策範圍時，請排除 Firewall Manager 管理員帳戶。當您透過主控台建立用途稽核安全群組政策時，這是預設選項。

從停用自動修補開始

對於內容或用途稽核安全群組政策，請先從停用自動修補開始。檢閱政策詳細資訊，以判定自動修補可能有的效用。當您確認這些變更正是您所需的時，請編輯政策，以啟用自動修補。

如果您也使用外部來源管理安全群組，請避免衝突

如果您使用 Firewall Manager 以外的工具或服務來管理安全群組，請小心避免 Firewall Manager 中的設定與外部來源中的設定之間發生衝突。如果您使用自動修補且設定有衝突，您可以建立消耗雙方資源的衝突修補循環。

例如，假設您設定另一個服務來維護一組 AWS 資源的安全群組，並設定 Firewall Manager 政策來維護部分或全部相同資源的不同安全群組。如果您設定任何其他安全群組與範圍內資源相關聯的任何一方，該方將會移除由另一方維護的安全群組關聯。如果雙方都以這種方式進行配置，則最終可能會產生衝突的分離和關聯循環。

此外，假設您建立 Firewall Manager 稽核政策，以強制執行與來自其他服務的安全群組組態衝突的安全群組組態。Firewall Manager 稽核政策套用的修補可以更新或刪除該安全群組，使其不符合其他服務的合規。如果其他服務設定為監控並自動修復發現的任何問題，它會重新建立或更新安全群組，使其再次不符合 Firewall Manager 稽核政策。如果 Firewall Manager 稽核政策設定為自動修復，它會再次更新或刪除外部安全群組，以此類推。

為了避免這類衝突，請在 Firewall Manager 與任何外部來源之間建立互斥的組態。

您可以使用標記從 Firewall Manager 政策的自動修復中排除外部安全群組。若要這樣做，請將一或多個標記新增至由外部來源管理的安全群組或其他資源。然後，當您定義 Firewall Manager 政策範圍時，請在資源規格中排除具有已新增標籤或標籤的資源。

同樣地，在您的外部工具或服務中，排除 Firewall Manager 從任何管理或稽核活動中管理的安全群組。請勿匯入 Firewall Manager 資源，或使用 Firewall Manager 特定的標記將其排除在外部管理之外。

用量稽核安全群組政策的最佳實務

當您使用用量稽核安全群組政策時，請遵循這些準則。

- 避免在短時間內對安全群組的關聯狀態進行多次變更，例如在 15 分鐘內。這樣做可能會導致 Firewall Manager 錯過部分或全部對應的事件。例如，請勿快速關聯和取消安全群組與彈性網路界面的關聯。

安全群組政策警告和限制

本節列出使用 Firewall Manager 安全群組政策的注意事項和限制。

資源類型：Amazon EC2 執行個體

本節列出使用 Firewall Manager 安全群組政策保護 Amazon EC2 執行個體的注意事項和限制。

- 使用保護 Amazon EC2 彈性網路介面 (ENIs) 的安全群組時，防火牆管理員不會立即看到安全群組的變更。Firewall Manager 通常會在幾個小時內偵測變更，但偵測最多可延遲六個小時。
- Firewall Manager 不支援由 Amazon Relational Database Service 建立的 Amazon EC2 ENIs 安全群組。Amazon Relational Database Service
- Firewall Manager 不支援更新使用 Fargate 服務類型建立之 Amazon EC2 ENIs 的安全群組。不過，您可以使用 Amazon EC2 服務類型更新 Amazon ECS ENIs 的安全群組。
- Firewall Manager 不支援更新請求者受管 Amazon EC2 ENIs 的安全群組，因為 Firewall Manager 沒有修改這些群組的許可。
- 對於常見的安全群組政策，這些注意事項涉及連接到 EC2 執行個體的彈性網路介面 (ENIs) 數量與指定是否僅修復沒有新增附件的 EC2 執行個體或修復所有執行個體的政策選項之間的互動。每個 EC2 執行個體都有預設的主要 ENI，您可以連接更多 ENIs。在 API 中，此選項的政策選項設定為 `ApplyToAllEC2InstanceENIs`。

如果範圍內的 EC2 執行個體已連接其他 ENIs，且政策設定為僅包含具有主要 ENI 的 EC2 執行個體，則 Firewall Manager 不會嘗試對 EC2 執行個體進行任何修復。此外，如果執行個體超出政策範圍，防火牆管理員不會嘗試取消其可能為執行個體建立的任何安全群組關聯的關聯。

對於下列邊緣案例，在資源清除期間，防火牆管理員可以保持複寫的安全群組關聯完整，無論政策的資源清除規格為何：

- 當具有其他 ENIs 執行個體先前已由設定為包含所有 EC2 執行個體的政策修復，然後執行個體超出政策範圍或政策設定變更為僅包含沒有其他 ENIs 執行個體。
- 當沒有其他 ENIs 執行個體被設定為僅包含沒有其他 ENIs 的執行個體的政策修復時，則另一個 ENI 連接到執行個體，然後執行個體超出政策範圍。

其他注意事項和限制

以下是 Firewall Manager 安全群組政策的其他注意事項和限制。

- Firewall Manager 安全群組政策不支援透過 共用的安全群組 AWS RAM。
- 只有使用滾動更新 (Amazon ECS) 部署控制器的 Amazon ECS 服務，才能更新 Amazon ECS ENIs。對於其他 Amazon ECS 部署控制器，例如 CODE_DEPLOY 或外部控制器，防火牆管理員目前無法更新 ENIs。
- Firewall Manager 不支援在 ENIs 中更新 Network Load Balancer 的安全群組。
- 在常見的安全群組政策中，如果稍後未與帳戶共用共用 VPC Firewall Manager，則不會刪除帳戶中的複本安全群組。
- 使用用量稽核安全群組政策時，如果您建立多個具有相同範圍之自訂延遲時間設定的政策，則第一個具有合規調查結果的政策將是報告調查結果的政策。

安全群組政策使用案例

您可以使用 AWS Firewall Manager 常見的安全群組政策來自動化主機防火牆組態，以便在 Amazon VPC 執行個體之間進行通訊。本節列出標準 Amazon VPC 架構，並說明如何使用 Firewall Manager 常見安全群組政策來保護每個架構。這些安全群組政策可協助您套用統一的規則集，以選取不同帳戶中的資源，並避免 Amazon Elastic Compute Cloud 和 Amazon VPC 中的每個帳戶組態。

使用 Firewall Manager 一般安全群組政策，您可以只標記與另一個 Amazon VPC 中的執行個體通訊所需的 EC2 彈性網路介面。然後，相同 Amazon VPC 中的其他執行個體會更安全且隔離。

使用案例：監控和控制對 Application Load Balancer 和 Classic Load Balancer 的請求

您可以使用 Firewall Manager 通用安全群組政策來定義您的範圍內負載平衡器應該提供哪些請求。您可以透過 Firewall Manager 主控台進行設定。只有符合安全群組傳入規則的請求才能到達負載平衡器，而且負載平衡器只會分發符合傳出規則的請求。

使用案例：可存取網際網路的公有 Amazon VPC

您可以使用 Firewall Manager 通用安全群組政策來保護公有 Amazon VPC，例如僅允許傳入連接埠 443。此做法與只允許公有 VPC 的傳入 HTTPS 流量相同。您可以標記 VPC 內的公有資源（例如，「PublicVPC」），然後將 Firewall Manager 政策範圍設定為僅具有該標籤的資源。Firewall Manager 會自動將政策套用至這些資源。

使用案例：公有和私有 Amazon VPC 執行個體

對於可存取網際網路的公有 Amazon VPC 執行個體，您可以對公有資源使用與先前使用案例中建議的相同常見安全群組政策。您可以使用第二個常見安全群組政策，限制公有資源與私有資源之間的通訊。將公有和私有 Amazon VPC 執行個體中的資源標記為「PublicPrivate」，以套用第二個政策。您可以使用第三個政策來定義私有資源與其他公司或私有 Amazon VPC 執行個體之間的允許通訊。對於此政策，您可以在私有資源上使用另一個識別標籤。

使用案例：中樞和發言的 Amazon VPC 執行個體

您可以使用常見的安全群組政策來定義中樞 Amazon VPC 執行個體與發言 Amazon VPC 執行個體之間的通訊。您可以使用第二個政策來定義從每個輪輻 Amazon VPC 執行個體到中樞 Amazon VPC 執行個體的通訊。

使用案例：Amazon EC2 執行個體的預設網路介面

您可以使用常見安全群組政策，只允許標準通訊，例如內部 SSH 和修補程式/作業系統更新服務，並不允許其他不安全通訊。

使用案例：識別具有開放許可的資源

您可以使用稽核安全群組政策，來識別您組織內擁有可與公有 IP 地址進行通訊之許可，或擁有屬於第三方廠商之 IP 地址的所有資源。

搭配 Firewall Manager 使用常見的安全群組政策

此頁面說明 Firewall Manager 常見安全群組政策的運作方式。

透過通用的安全群組政策，防火牆管理員提供安全群組與整個組織之帳戶和資源的集中控制關聯。您可以指定要在您組織中要套用政策的項目與如何套用。

您可以將常見的安全群組政策套用至下列資源類型：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體
- 彈性網路介面
- Application Load Balancer
- Classic Load Balancer

如需使用主控台建立常見安全群組政策的指引，請參閱 [建立常見安全群組政策](#)。

共用的 VPC

在通用安全性群組政策的政策範圍設定中，您可以選擇包含共用 VPC。此選項包括由另一個帳戶擁有且與範圍內帳戶共用的 VPC。一律包含範圍內帳戶擁有的 VPC。如需共用 VPCs 的相關資訊，請參閱《Amazon [VPCs 使用者指南](#)》中的[使用共用 VPC](#)。

下列注意事項適用於包含共用 VPCs 這些是 安全群組政策的一般注意事項。 [安全群組政策警告和限制](#)

- Firewall Manager 會將主要安全群組複寫到每個範圍內帳戶的 VPCs。對於共用的 VPC，防火牆管理員會針對共用 VPC 的每個範圍內帳戶複寫主要安全群組一次。這可能會導致單一共用 VPC 中的多個複本。
- 當您建立新的共用 VPC 時，在 VPC 中建立至少一項在政策範圍內的資源之前，您不會在 Firewall Manager 安全群組政策詳細資訊中看到它。
- 當您在已啟用共用 VPCs 的政策中停用共用 VPCs 時，在共用 VPCs 中，防火牆管理員會刪除未與任何資源相關聯的複本安全群組。Firewall Manager 會保留剩餘的複本安全群組，但會停止管理這些群組。移除這些剩餘的安全群組需要在每個共用 VPC 執行個體中進行手動管理。

主要安全群組

針對每個常見的安全群組政策，您 AWS Firewall Manager 提供一或多個主要安全群組：

- 主要安全群組必須由 Firewall Manager 管理員帳戶建立，並且可以位於帳戶中的任何 Amazon VPC 執行個體中。
- 您可以透過 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理主要安全群組。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[使用安全群組](#)。
- 您可以將一或多個安全群組命名為 Firewall Manager 安全群組政策的主要群組。政策中允許的安全群組數量預設為一個，但您可以提交增加數量的請求。如需相關資訊，請參閱 [AWS Firewall Manager 配額](#)。

政策規則設定

您可以為常見安全群組政策的安全群組和資源選擇下列一或多個變更控制行為：

- 識別並報告本機使用者對複本安全群組所做的任何變更。
- 取消任何其他安全群組與政策範圍內 AWS 資源的關聯。
- 將標籤從主要群組分佈到複本安全群組。

Important

Firewall Manager 不會將 AWS 服務新增的系統標籤分發至複本安全群組。系統標籤以 `aws:` 字首開頭。此外，如果政策的標籤與組織的標籤政策衝突，則 Firewall Manager 不會更新現有安全群組的標籤，也不會建立新的安全群組。如需標籤政策的相關資訊，請參閱 AWS Organizations 《使用者指南》中的[標籤政策](#)。

- 將安全群組參考從主要群組分發至複本安全群組。

這可讓您輕鬆地建立一般安全群組，將所有範圍內資源的規則參考到與指定安全群組的 VPC 相關聯的執行個體。當您啟用此選項時，防火牆管理員只會在安全群組參考 Amazon Virtual Private Cloud 中的對等安全群組時傳播安全群組參考。如果複本安全群組未正確參考對等安全群組，則 Firewall Manager 會將這些複寫的安全群組標記為不合規。如需有關如何在 Amazon VPC 中參考對等安全群組的資訊，請參閱《[Amazon VPC 對等指南](#)》中的[更新您的安全群組以參考對等安全群組](#)。

如果您未啟用此選項，防火牆管理員不會將安全群組參考傳播至複本安全群組。如需 Amazon VPC 中 VPC 對等互連的相關資訊，請參閱 [Amazon VPC 對等互連指南](#)。

政策建立與管理

當您建立常見的安全群組政策時，Fire Firewall Manager 會將主要安全群組複寫至政策範圍內的每個 Amazon VPC 執行個體，並將複寫的安全群組與政策範圍內的帳戶和資源建立關聯。當您修改主要安全群組時，防火牆管理員會將變更傳播到複本。

刪除常見安全群組政策時，您可以選擇是否要清理依此政策建立的資源。對於 Firewall Manager 通用安全群組，這些資源是複本安全群組。除非您想要在刪除政策後手動管理每個個別複本，否則請選擇清理選項。在大多數情況下，選擇清理是最簡單的方法。

如何管理複本

Amazon VPC 執行個體中的複本安全群組會與其他 Amazon VPC 安全群組一樣進行管理。如需詳細資訊，請參閱《[Amazon VPC 使用者指南](#)》中的[VPC 安全群組](#)。

搭配 Firewall Manager 使用內容稽核安全群組政策

此頁面說明 Firewall Manager 內容稽核安全群組政策的運作方式。

使用 AWS Firewall Manager 內容稽核安全群組政策來稽核政策動作，並將其套用至組織安全群組中使用的規則。根據您在政策中定義的範圍，內容稽核安全群組政策適用於 AWS 組織中使用的所有客戶建立的安全群組。

如需使用主控台建立內容稽核安全群組政策的指引，請參閱 [建立內容稽核安全群組政策](#)。

政策範圍資源類型

您可以將內容稽核安全群組政策套用至下列資源類型：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體
- 彈性網路界面
- Amazon VPC 安全群組

如果安全群組明確位於範圍內，或與範圍內的資源相關聯，則會將該安全群組視為在政策範圍內。

政策規則選項

您可以為每個內容稽核政策使用受管政策規則或自訂政策規則，但不能同時使用兩者。

- 受管政策規則 – 在具有受管規則的政策中，您可以使用應用程式和通訊協定清單來控制 Firewall Manager 稽核哪些規則，並將哪些規則標記為合規或不合規。您可以使用 Firewall Manager 管理的清單。您也可以建立和使用自己的應用程式和通訊協定清單。如需這些清單類型和自訂清單管理選項的相關資訊，請參閱 [使用 Firewall Manager 受管清單](#)。
- 自訂政策規則 – 在具有自訂政策規則的政策中，您將現有的安全群組指定為政策的稽核安全群組。您可以使用稽核安全群組規則做為範本，定義 Firewall Manager 稽核的規則，並標記為合規或不合規。

稽核安全群組

您必須使用 Firewall Manager 管理員帳戶建立稽核安全群組，才能在政策中使用它們。您可以透過 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全群組。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [使用安全群組](#)。

Firewall Manager 只會使用您用於內容稽核安全群組政策的安全群組，做為政策範圍內安全群組的比較參考。Firewall Manager 不會將其與組織中的任何資源建立關聯。

您在稽核安全群組中定義規則的方式取決於您在政策規則設定中的選擇：

- 受管政策規則 – 對於受管政策規則設定，您可以使用稽核安全群組來覆寫政策中的其他設定，以明確允許或拒絕可能具有其他合規結果的規則。
 - 如果您選擇一律允許稽核安全群組中定義的規則，則任何符合稽核安全群組中定義規則的規則都會視為符合政策，無論其他政策設定為何。
 - 如果您選擇一律拒絕稽核安全群組中定義的規則，則任何符合稽核安全群組中定義規則的規則都會視為不符合政策，無論其他政策設定為何。
- 自訂政策規則 – 針對自訂政策規則設定，稽核安全群組會提供範圍內安全群組規則中可接受或不接受的範例：
 - 如果您選擇允許使用規則，則所有範圍內的安全群組都必須擁有在政策稽核安全群組規則允許範圍內的規則。在這種情況下，政策的安全群組規則提供可接受的做法範例。
 - 如果您選擇拒絕使用規則，則所有範圍內的安全群組只能擁有不在政策稽核安全群組規則允許範圍內的規則。在此情況下，政策的安全群組會提供無法接受的行為範例。

政策建立與管理

建立稽核安全群組政策時，您必須停用自動修補。建議的實務為在啟用自動修補前檢閱政策建立的效用。檢閱預期的效用後，您可以編輯政策，並啟用自動修補。啟用自動修復時，防火牆管理員會更新或移除範圍內安全群組中不合規的規則。

受稽核安全群組政策影響的安全群組

您組織中由客戶建立的所有安全群組均有資格位於稽核安全群組政策中。

複本安全群組不是由客戶建立，因此沒有直接位於稽核安全群組政策範圍中的資格。不過它們可以隨著政策的自動修補活動而更新。常見安全群組政策的主要安全群組是由客戶建立，因此可以在稽核安全群組政策的範圍內。如果稽核安全群組政策對主要安全群組進行變更，防火牆管理員會自動將這些變更傳播到複本。

內容稽核安全群組政策的注意事項和限制

您無法在內容稽核安全群組政策中參考對等安全群組。

如需所有 Firewall Manager 安全群組中其他考量事項的資訊，請參閱 [安全群組政策警告和限制](#)。

搭配 Firewall Manager 使用用量稽核安全群組政策

此頁面說明 Firewall Manager 用量稽核安全群組政策的運作方式。

使用 AWS Firewall Manager 用量稽核安全群組政策來監控您的組織是否有未使用的和多餘的安全群組，並選擇性地執行清除。當您啟用此政策的自動修復時，防火牆管理員會執行下列動作：

1. 整合多餘的安全群組 (如果您已選擇該選項)。
2. 移除未使用的安全群組 (如果您已選擇該選項)。

您可以將用量稽核安全群組政策套用至下列資源類型：

- Amazon VPC 安全群組

如需使用 主控台 建立用量稽核安全群組政策的指引，請參閱 [建立用途稽核安全群組政策](#)。

Firewall Manager 如何偵測和修復備援安全群組

若要將安全群組視為備援，它們必須設定完全相同的規則，且位於相同的 Amazon VPC 執行個體中。

若要修復備援安全群組集，防火牆管理員會選取要保留的集合中的其中一個安全群組，然後將其與集合中與其他安全群組相關聯的所有資源建立關聯。然後，Firewall Manager 會取消其他安全群組與相關資源的關聯，讓這些群組變得未使用。

Note

如果您也選擇移除未使用的安全群組，則 Firewall Manager 會執行此操作。此動作會移除備援組中的安全群組。

Firewall Manager 如何偵測和修復未使用的安全群組

如果下列兩項都為 true，則 Firewall Manager 會將安全群組視為未使用：

- 任何 Amazon EC2 執行個體或 Amazon EC2 彈性網路介面都不會使用安全群組。
- Firewall Manager 未在政策規則期間指定的分鐘數內收到其組態項目。

政策規則時段的預設設定為零分鐘，但您可以將時間增加到 365 天 (525, 600 分鐘)，以便自己有時將新的安全群組與資源建立關聯。

⚠ Important

如果您指定預設值為零以外的分鐘數，則必須在其中啟用間接關係 AWS Config。否則，您的用量稽核安全群組政策將無法如預期般運作。如需有關 中的間接關係的資訊 AWS Config，請參閱《AWS Config 開發人員指南》中的 [中的間接關係 AWS Config](#)。

Firewall Manager 會盡可能根據規則設定從您的帳戶刪除未使用的安全群組，以修復未使用的安全群組。如果 Firewall Manager 無法刪除安全群組，它會將其標記為不合規政策。Firewall Manager 無法刪除另一個安全群組參考的安全群組。

修復的時間取決於您使用的是預設時段設定或自訂設定：

- 時間區段設定為零，預設值 – 使用此設定時，只要 Amazon EC2 執行個體或彈性網路介面未使用安全群組，就會被視為未使用。

對於此零時段設定，防火牆管理員會立即修復安全群組。

- 大於零的時段 – 在此設定中，當 Amazon EC2 執行個體或彈性網路介面未使用安全群組，且 Firewall Manager 未在指定的分鐘數內收到其組態項目時，安全群組即視為未使用。

對於非零時段設定，防火牆管理員會在安全群組保持未使用的狀態 24 小時後，對其進行修復。

預設帳戶規格

當您透過主控台建立用量稽核安全群組政策時，防火牆管理員會自動選擇排除指定的帳戶並包含所有其他帳戶。然後，服務會將 Firewall Manager 管理員帳戶放入清單中以排除。這是建議的方法，可讓您手動管理屬於 Firewall Manager 管理員帳戶的安全群組。

搭配 Firewall Manager 使用 Amazon VPC 網路存取控制清單 (ACL) 政策

本節涵蓋 AWS Firewall Manager 網路 ACL 政策的運作方式，並提供使用這些政策的指引。如需使用主控台建立網路 ACL 政策的指引，請參閱 [建立網路 ACL 政策](#)。

如需有關 Amazon VPC 網路存取控制清單 (ACLs) 的資訊，請參閱《Amazon VPC 使用者指南》中的 [使用網路 ACLs 控制子網路的流量](#)。

您可以使用 Firewall Manager 網路 ACL 政策來管理組織中的 Amazon Virtual Private Cloud (Amazon VPC) 網路存取控制清單 (ACLs) AWS Organizations。您可以定義政策的網路 ACL 規則設定，以及您想要強制執行設定的帳戶和子網路。Firewall Manager 會在您的組織中新增或更新帳戶和子網路時，持

續將您的政策設定套用至這些帳戶和子網路。如需政策範圍 和 的相關資訊 AWS Organizations，請參閱 [使用 AWS Firewall Manager 政策範圍](#)和 [AWS Organizations 使用者指南](#)。

當您定義 Firewall Manager 網路 ACL 政策時，除了標準 Firewall Manager 政策設定，例如名稱和範圍，您還會提供下列項目：

- 傳入和傳出流量處理的第一個和最後一個規則。Firewall Manager 會在政策範圍內的網路 ACLs 中強制執行這些項目的存在和排序，或報告不合規。您的個別帳戶可以建立自訂規則，以便在政策的第一個和最後一個規則之間執行。
- 是否在修復會導致網路 ACL 中規則之間的流量管理衝突時強制修復。這僅適用於針對政策啟用修復時。

使用 Firewall Manager 網路 ACL 政策的最佳實務

本節列出使用 Firewall Manager 網路 ACL 政策和受管網路 ACLs 的建議。

請參閱 **FManaged**標籤以識別由 Firewall Manager 管理的網路 ACLs

Firewall Manager 管理的網路 ACLs 會將FManaged標籤設定為 true。使用此標籤來協助區分您自己的自訂網路 ACLs 與您透過 Firewall Manager 管理的網路 ACL。

請勿修改網路 ACL 上**FManaged**標籤的值

Firewall Manager 使用此標籤來設定和判斷其管理狀態與網路 ACL。

請勿修改具有 Firewall Manager 受管網路 ACLs 之子網路的關聯

請勿手動變更子網路與 Firewall Manager 管理的任何網路 ACLs 之間的關聯。這樣做可以停用 Firewall Manager 管理這些子網路保護的能力。您可以尋找 的FManaged標籤設定，以識別由 Firewall Manager 管理的網路 ACLstrue。

若要從 Firewall Manager 政策管理中移除子網路，請使用 Firewall Manager 政策範圍設定來排除子網路。例如，您可以標記子網路，然後從政策範圍中排除該標籤。如需詳細資訊，請參閱[使用 AWS Firewall Manager 政策範圍](#)。

當您更新受管網路 ACL 時，請勿修改 Firewall Manager 管理的規則

在由 Firewall Manager 管理的網路 ACL 中，遵循 中所述的編號方案，將您的自訂規則與政策規則保持區隔在 [Firewall Manager 中使用網路 ACL 規則和標記](#)。僅新增或修改數字介於 5,000 到 32,000 之間的規則。

避免為您的帳戶限制新增太多規則

在修復網路 ACL 期間，防火牆管理員通常會暫時增加網路 ACL 規則計數。為了避免不合規問題，請確定您有足夠的空間來儲存正在使用的規則。如需詳細資訊，請參閱[Firewall Manager 如何修復不合規的受管網路 ACLs](#)。

從停用自動修補開始

從停用自動修復開始，然後檢閱政策詳細資訊，以判斷自動修復會帶來的影響。當您確認這些變更正是您所需的時，請編輯政策，以啟用自動修補。

Firewall Manager 網路 ACL 政策注意事項

本節列出使用 Firewall Manager 網路 ACL 政策的注意事項和限制。

- 更新時間比其他政策慢 – Firewall Manager 通常套用網路 ACL 政策和政策變更比其他 Firewall Manager 政策慢，因為 Amazon EC2 網路 ACL APIs 能夠處理請求的速率有限。您可能會注意到，政策變更需要比其他 Firewall Manager 政策的類似變更更長的時間，特別是當您第一次新增政策時。
- 對於初始子網路保護，防火牆管理員偏好較舊的政策 – 這僅適用於尚未受 Firewall Manager 網路 ACL 政策保護的子網路。如果子網路同時進入多個網路 ACL 政策的範圍，則 Firewall Manager 會使用最舊的政策來保護子網路。
- 政策停止保護子網路的原因 – 正在管理子網路網路 ACL 的政策會保留管理，直到發生下列其中一種情況：
 - 子網路超出政策的範圍。
 - 政策已刪除。
 - 您可以手動將子網路的關聯變更為由不同 Firewall Manager 政策管理且子網路在範圍內的網路 ACL。

主題

- [在 Firewall Manager 中使用網路 ACL 規則和標記](#)
- [Firewall Manager 如何啟動子網路的網路 ACL 管理](#)
- [Firewall Manager 如何修復不合規的受管網路 ACLs](#)
- [刪除 Firewall Manager 網路 ACL 政策](#)

在 Firewall Manager 中使用網路 ACL 規則和標記

本節說明由 Firewall Manager 管理的網路 ACL 政策規則規格和網路 ACLs。

受管網路 ACL 上的標記

Firewall Manager 會將受管網路 ACL 標籤為值為 `FMManged` 標籤 `true`。Firewall Manager 只會對具有此標籤設定的網路 ACLs 執行修復。

您在政策中定義的規則

在網路 ACL 政策規格中，您可以定義您要先執行和最後執行的傳入流量規則，以及您要先執行和最後執行的傳出流量規則。

根據預設，您最多可以定義 5 個傳入規則，以政策中第一個和最後一個規則的任意組合使用。同樣地，您最多可以定義 5 個傳出規則。如需這些限制的詳細資訊，請參閱 [軟配額](#)。如需有關網路 ACLs 一般限制的資訊，請參閱 [《Amazon VPC 使用者指南》中的網路 ACLs 上的 Amazon VPC 配額](#)。

您不會將規則編號指派給政策規則。反之，您可以按照您希望評估規則的順序指定規則，而 Firewall Manager 會使用該順序，在其管理的網路 ACLs 中指派規則編號。

除此之外，您可以管理政策的網路 ACL 規則規格，就像透過 Amazon VPC 管理網路 ACL 中的規則一樣。如需有關 Amazon VPC 中網路 ACL 管理的資訊，請參閱 [《Amazon VPC 使用者指南》中的使用網路 ACLs 控制子網路的流量和使用網路 ACLs](#)。

受管網路 ACL 中的規則

Firewall Manager 會在個別帳戶管理員定義的任何自訂規則之前和之後，將政策的第一個和最後一個規則放在其管理的網路 ACL 中，以設定規則。Firewall Manager 會保留自訂規則的順序。從最低編號的規則開始評估網路 ACLs。

Firewall Manager 第一次建立網路 ACL 時，會定義具有下列編號的規則：

- 第一個規則：1、2、... – 由您在 Firewall Manager 網路 ACL 政策中定義。

Firewall Manager 會指派從 1 開始的規則編號，以 1 為增量，並依照您在政策規格中訂購規則的順序排序。

- 自訂規則：5,000、5,100、... – 由個別帳戶管理員透過 Amazon VPC 管理。

Firewall Manager 會將數字指派給這些規則，從 5,000 開始，並為每個後續規則增加 100。

- 最後一個規則：... 32,765、32,766 – 由您在 Firewall Manager 網路 ACL 政策中定義。

Firewall Manager 會指派結尾為最高數字的規則編號 32766，增量為 1，並按照您在政策規格中訂購規則的順序排序。

網路 ACL 初始化後，防火牆管理員不會控制個別帳戶在其受管網路 ACLs 中所做的變更。個別帳戶可以變更網路 ACL，而不會使其不合規，只要任何自訂規則在政策的第一個和最後一個規則之間保持編號，而第一個和最後一個規則會維持其指定的順序。最佳實務是，在管理自訂規則時，請遵守本節所述的編號。

Firewall Manager 如何啟動子網路的網路 ACL 管理

本節說明 Firewall Manager 如何啟動子網路的網路 ACL 管理。

Firewall Manager 會將子網路與 Firewall Manager 建立並標記為 FManaged 的網路 ACL 建立關聯時，會開始管理子網路的網路 ACLtrue。

遵循網路 ACL 政策需要子網路的網路 ACL 先定位政策的第一個規則，依照政策中指定的順序、最後的規則，以及位於中間的任何其他自訂規則。這些需求可由未受管網路 ACL 滿足，而子網路已與受管網路 ACL 建立關聯或由受管網路 ACL 建立關聯。

當 Firewall Manager 將網路 ACL 政策套用到與未受管網路 ACL 相關聯的子網路時，防火牆管理員會依序檢查下列項目，並在識別可行選項時停止：

1. 關聯的網路 ACL 已合規 – 如果目前與子網路相關聯的網路 ACL 合規，則 Firewall Manager 會保留該關聯，而不會啟動子網路的網路 ACL 管理。

Firewall Manager 不會變更或以其他方式管理非其擁有的網路 ACL，但只要符合規定，防火牆管理員就會將其保留，並監控其是否符合政策。

2. 有合規的受管網路 ACL 可用 – 如果 Firewall Manager 已管理符合所需組態的網路 ACL，則這是選項。如果啟用修復，則 Firewall Manager 會將子網路與其建立關聯。如果停用修復，則 Firewall Manager 會將子網路標記為不合規，並提供取代網路 ACL 關聯做為修復選項。
3. 建立新的合規受管網路 ACL – 如果啟用修復，則 Firewall Manager 會建立新的網路 ACL，並將其與子網路建立關聯。否則，防火牆管理員會將子網路標記為不合規，並提供修復選項，以建立新的網路 ACL 和取代網路 ACL 關聯。

如果這些步驟失敗，防火牆管理員會報告子網路的不合規。

當子網路先進入範圍，以及子網路的未受管網路 ACL 不符合規範時，防火牆管理員會遵循這些步驟。

Firewall Manager 如何修復不合規的受管網路 ACLs

本節說明 Firewall Manager 如何在不符合政策時修復其受管網路 ACLs。Firewall Manager 只會修復受管網路 ACLs，並將FManaged標籤設定為 true。如需非由 Firewall Manager 管理的網路 ACLs，請參閱[初始網路 ACL 管理](#)。

修復會還原第一個、自訂和最後一個規則的相對位置，並還原第一個和最後一個規則的順序。在修復期間，防火牆管理員不一定會將規則移至網路 ACL 初始化中使用的規則號碼。如需這些規則類別的初始數字設定和說明，請參閱 [初始網路 ACL 管理](#)。

為了建立合規規則和規則順序，防火牆管理員可能需要在網路 ACL 內移動規則。Firewall Manager 會盡可能維持現有的合規規則順序，以保留網路 ACL 的保護。例如，它可能會暫時將規則複製到新位置，然後執行原始規則的有序移除，在過程中保留相對位置。

此方法可保護您的設定，但也需要網路 ACL 中臨時規則的空間。如果 Firewall Manager 達到網路 ACL 中規則的限制，則會停止修復。發生這種情況時，網路 ACL 會保持不合規，且 Firewall Manager 會報告原因。

如果帳戶將自訂規則新增至由 Firewall Manager 管理的網路 ACL，且這些規則干擾 Firewall Manager 修補，則 Firewall Manager 會停止網路 ACL 上的任何修補活動並報告衝突。

強制修復

如果您選擇政策的自動修復，您也可以指定要強制第一個規則或最後一個規則的修復。

當 Firewall Manager 在自訂規則和政策規則之間遇到流量處理衝突時，它是指對應的強制修補設定。如果啟用強制修復，則 Firewall Manager 會套用修復，即使發生衝突。如果未啟用此選項，則 Firewall Manager 會停止修復。在任何一種情況下，防火牆管理員都會報告規則衝突並提供修復選項。

規則計數需求和限制

在修復期間，防火牆管理員可能會暫時複製規則，以便在不變更其提供的保護的情況下移動規則。

對於傳入或傳出規則，防火牆管理員可能需要執行修復的最大規則數量如下：

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

網路 ACLs 和網路 ACL 政策受可變規則限制約束。如果 Firewall Manager 在修補工作中達到限制，則會停止嘗試修復和報告不合規。

若要讓 Firewall Manager 有空間執行其修補活動，您可以請求提高限制。或者，您可以變更政策或網路 ACL 中的組態，以減少使用的規則數量。

如需有關網路 ACL 限制的資訊，請參閱 [《Amazon VPC 使用者指南》中的網路 ACLs 上的 Amazon VPC 配額](#)。

當修復失敗時

更新網路 ACL 時，如果 Firewall Manager 因任何原因需要停止，則不會復原變更，而是讓網路 ACL 處於臨時狀態。如果您在將FMManaged標籤設為的網路 ACL 中看到重複的規則true，則 Firewall Manager 可能正在修復它。變更可能會部分完成一段時間，但由於 Firewall Manager 採取的修復方法，這不會中斷流量或減少相關子網路的保護。

當 Firewall Manager 未完全修復不合規的網路 ACLs 時，它會報告相關聯子網路的不合規情況，並建議可能的修復選項。

修復失敗後重試

在大多數情況下，如果 Firewall Manager 無法完成對網路 ACL 的修復變更，最終會重試變更。

修正達到網路 ACL 規則計數限制或 VPC 網路 ACL 計數限制時，就會發生這種情況。Firewall Manager 無法執行修復活動，將 AWS 資源超過其限制設定。在這些情況下，您需要減少計數或增加限制才能繼續。如需限制的相關資訊，請參閱 [《Amazon VPC 使用者指南》中的網路 ACLs 上的 Amazon VPC 配額](#)。

Firewall Manager 網路 ACL 合規報告

Firewall Manager 會監控並報告連接到範圍內子網路的所有網路 ACLs 的合規性。

一般而言，如果規則順序不正確或流量處理行為在政策規則和自訂規則之間發生衝突，就會發生不合規的情況。不合規報告包括合規違規和修補選項。

Firewall Manager 回報網路 ACL 政策的合規違規，方式與其他政策類型相同。如需合規報告的資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

政策更新期間不合規

修改網路 ACL 政策後，在 Firewall Manager 更新政策範圍內的網路 ACLs 之前，防火牆管理員會將這些網路 ACLs 標記為不合規。即使網路 ACLs 可能嚴格地說，防火牆管理員也會這樣做。

例如，如果您從政策規格中移除規則，雖然範圍內網路 ACLs 仍然有額外的規則，但其規則定義仍可能符合政策。不過，由於額外的規則是 Firewall Manager 管理規則的一部分，因此 Firewall Manager 會將它們視為違反目前政策設定的行為。這與 Firewall Manager 如何檢視您新增至 Firewall Manager 受管網路 ACLs自訂規則不同。

刪除 Firewall Manager 網路 ACL 政策

本節說明當您刪除 Firewall Manager 網路 ACL 政策時，防火牆管理員會發生什麼情況。

當您刪除 Firewall Manager 網路 ACL 政策時，防火牆管理員會在其為政策管理的所有網路 ACLs `false` 上將 `FMManged` 標籤值變更為。

此外，您可以選擇是否要清除政策建立的資源。如果您選擇清除，Firewall Manager 會依序嘗試下列步驟：

1. 將關聯放回原始 - Firewall Manager 會嘗試將子網路與防火牆管理員開始管理之前與其相關聯的網路 ACL 建立關聯。
2. 從網路 ACL 移除第一個和最後一個規則 – 如果無法變更關聯，則 Firewall Manager 會嘗試移除政策的第一個和最後一個規則，只將自訂規則保留在與子網路相關聯的網路 ACL 中。
3. 不對規則或關聯執行任何動作 – 如果無法執行上述任一動作，則 Firewall Manager 會離開網路 ACL 及其關聯。

如果您未選擇清除選項，則需要在刪除政策後手動管理每個網路 ACL。在大多數情況下，選擇清理是最簡單的方法。

在 Firewall Manager 中使用 AWS Network Firewall 政策

本節說明如何搭配 Firewall Manager 使用 AWS Network Firewall 政策。

您可以使用 AWS Firewall Manager Network Firewall 政策來管理整個組織中 Amazon Virtual Private Cloud VPCs AWS Network Firewall 的防火牆 AWS Organizations。您可以將集中控制的防火牆套用到整個組織，或套用到帳戶和 VPCs 的選取子集。

Network Firewall 為 VPCs 中的公有子網路提供網路流量篩選保護。Firewall Manager 會根據政策定義的防火牆管理類型來建立和管理防火牆。Firewall Manager 提供下列防火牆管理模型：

- 分散式 - 對於在政策範圍內的每個帳戶和 VPC，防火牆管理員會建立網路防火牆防火牆，並將防火牆端點部署到 VPC 子網路，以篩選網路流量。
- 集中 - Firewall Manager 在單一 Amazon VPC 中建立單一網路防火牆防火牆。
- 匯入現有防火牆 - Firewall Manager 會在單一 Firewall Manager 政策中匯入現有防火牆以進行管理。您可以將其他規則套用到政策管理的匯入防火牆，以確保您的防火牆符合您的安全標準。

Note

Firewall Manager Network Firewall 政策是您用來管理整個組織中 VPCs 網路防火牆保護的 Firewall Manager 政策。

Network Firewall 保護是在 Network Firewall 服務中稱為防火牆政策的資源中指定。

如需有關使用 Network Firewall 的資訊，請參閱 [AWS Network Firewall 開發人員指南](#)。

下列各節涵蓋使用 Firewall Manager 網路防火牆政策的要求，並說明政策的運作方式。如需建立政策的程序，請參閱 [為建立 AWS Firewall Manager 政策 AWS Network Firewall](#)。

Important

您必須啟用資源共用。Network Firewall 政策會與您組織中的帳戶共用 Network Firewall 規則群組。若要讓此項目正常運作，您必須啟用資源共用 AWS Organizations。如需如何啟用資源共用的資訊，請參閱 [Network Firewall 和 DNS Firewall 政策的資源共用](#)。

Important

您必須定義 Network Firewall 規則群組。當您指定新的 Network Firewall 政策時，您可以定義防火牆政策，就像 AWS Network Firewall 直接使用時一樣。您可以指定要新增的無狀態規則群組、預設無狀態動作和具狀態規則群組。您的規則群組必須已存在於 Firewall Manager 管理員帳戶中，您才能將規則群組包含在政策中。如需建立 Network Firewall 規則群組的詳細資訊，請參閱 [AWS Network Firewall 規則群組](#)。

主題

- [Firewall Manager 如何建立防火牆端點](#)
- [Firewall Manager 如何管理您的防火牆子網路](#)
- [Firewall Manager 如何管理您的 Network Firewall 資源](#)
- [Firewall Manager 如何管理和監控政策的 VPC 路由表](#)
- [設定 AWS Network Firewall 政策的記錄](#)

Firewall Manager 如何建立防火牆端點

本節說明 Firewall Manager 如何建立防火牆端點。

政策中的防火牆管理類型決定 Firewall Manager 如何建立防火牆。您的政策可以建立分散式防火牆、集中式防火牆，也可以匯入現有的防火牆：

- 分散式 - 使用分散式部署模型，Firewall Manager 會為政策範圍內的每個 VPC 建立端點。您可以透過指定要在其中建立防火牆端點的可用區域來自訂端點位置，或者 Firewall Manager 可以在具有公有子網路的可用區域中自動建立端點。如果您手動選擇可用區域，您可以選擇限制每個可用區域的允許 CIDRs 集。如果您決定讓 Firewall Manager 自動建立端點，您還必須指定服務是否將在 VPCs 中建立單一端點或多個防火牆端點。
- 對於多個防火牆端點，防火牆管理員會在每個可用區域中部署防火牆端點，其中您在路由表中具有具有網際網路閘道的子網路或防火牆管理員建立的防火牆端點路由。這是網路防火牆政策的預設選項。
- 對於單一防火牆端點，Firewall Manager 會在具有網際網路閘道路由的任何子網路中的單一可用區域中部署防火牆端點。使用此選項時，其他區域中的流量需要跨區域邊界，才能由防火牆篩選。

 Note

對於這兩個選項，必須有與路由表相關聯的子網路，該路由表中具有 IPv4/字首清單路由。Firewall Manager 不會檢查任何其他資源。

- 集中式 - 透過集中式部署模型，Firewall Manager 會在檢查 VPC 中建立一或多個防火牆端點。檢查 VPC 是 Firewall Manager 啟動端點的中央 VPC。當您使用集中式部署模型時，您也可以指定要在其中建立防火牆端點的可用區域。您無法在建立政策後變更檢查 VPC。若要使用不同的檢查 VPC，您必須建立新的政策。
- 匯入現有防火牆 - 當您匯入現有防火牆時，您可以透過將一或多個資源集新增至政策，來選擇要在政策中管理的防火牆。資源集是資源集合，在此情況下，網路防火牆中的現有防火牆是由組織中的帳戶管理。在政策中使用資源集之前，您必須先建立資源集。如需 Firewall Manager 資源集的詳細資訊，請參閱 [在 Firewall Manager 中分組您的資源](#)。

使用匯入的防火牆時，請記住下列考量事項：

- 如果匯入的防火牆不合規，防火牆管理員將嘗試自動解決違規，但下列情況除外：
 - 如果 Firewall Manager 與 Network Firewall 政策的狀態或無狀態預設動作不相符。
 - 如果匯入防火牆的防火牆政策中的規則群組具有與防火牆管理員政策中的規則群組相同的優先順序。
 - 如果匯入的防火牆使用與非政策資源集一部分的防火牆相關聯的防火牆政策。這可能是因為防火牆可以只有一個防火牆政策，但單一防火牆政策可以與多個防火牆相關聯。
 - 如果屬於匯入防火牆防火牆政策的預先存在規則群組，且防火牆管理員政策中也指定了不同的優先順序。

- 如果您在政策中啟用資源清除，防火牆管理員會從資源集範圍內的防火牆移除 FMS 匯入政策中的規則群組。
- 由 Firewall Manager 管理的防火牆匯入現有防火牆管理類型一次只能由一個政策管理。如果將相同的資源集新增至多個匯入網路防火牆政策，資源集中的防火牆將由資源集新增至的第一個政策管理，而第二個政策則會忽略。
- Firewall Manager 目前不會串流例外狀況政策組態。如需串流例外狀況政策的詳細資訊，請參閱《AWS Network Firewall 開發人員指南》中的[串流例外狀況政策](#)。

如果您使用分散式或集中式防火牆管理變更政策的可用區域清單，防火牆管理員會嘗試清除過去建立但目前不在政策範圍內的任何端點。只有在沒有參考超出範圍端點的路由表路由時，防火牆管理員才會移除端點。如果 Firewall Manager 發現無法刪除這些端點，它會將防火牆子網路標記為不合規，並繼續嘗試移除端點，直到可安全刪除為止。

Firewall Manager 如何管理您的防火牆子網路

本節說明 Firewall Manager 如何管理您的防火牆子網路。

防火牆子網路是 Firewall Manager 為篩選網路流量的防火牆端點建立的 VPC 子網路。每個防火牆端點都必須部署在專用 VPC 子網路中。Firewall Manager 會在政策範圍內的每個 VPC 中建立至少一個防火牆子網路。

對於使用分散式部署模型搭配自動端點組態的政策，防火牆管理員只會在可用區域中建立防火牆子網路，該區域具有具有網際網路閘道路由的子網路，或具有路由的子網路，而防火牆管理員會為其政策建立的防火牆端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[VPC 和子網路](#)。

對於使用分散式或集中式模型的政策，當您指定哪些可用區域 Firewall Manager 建立防火牆端點時，防火牆管理員會在這些特定可用區域中建立端點，無論可用區域中是否有其他資源。

當您第一次定義 Network Firewall 政策時，您可以指定 Firewall Manager 如何管理範圍內每個 VPCs 中的防火牆子網路。您稍後無法變更此選項。

對於使用分散式部署模型搭配自動端點組態的政策，您可以選擇下列選項：

- 為具有公有子網路的每個可用區域部署防火牆子網路。這是預設行為。這可提供高可用性的流量篩選保護。
- 在一個可用區域中部署單一防火牆子網路。使用此選項時，防火牆管理員會識別 VPC 中具有最多公有子網路的區域，並在其中建立防火牆子網路。單一防火牆端點會篩選 VPC 的所有網路流量。這可以降低防火牆成本，但它不是高度可用的，它需要來自其他區域的流量才能篩選出跨區域邊界。

對於使用具有自訂端點組態的分散式部署模型或集中式部署模型的政策，Firewall Manager 會在政策範圍內的指定可用區域中建立子網路。

您可以為 Firewall Manager 提供 VPC CIDR 區塊，以用於防火牆子網路，或者您可以將防火牆端點地址的選擇保留為 Firewall Manager 來決定。

- 如果您未提供 CIDR 區塊，Firewall Manager 會查詢您的 VPCs 以取得要使用的可用 IP 地址。
- 如果您提供 CIDR 區塊清單，防火牆管理員只會在您提供的 CIDR 區塊中搜尋新的子網路。您必須使用 /28 CIDR 區塊。對於 Firewall Manager 建立的每個防火牆子網路，它會逐步引導 CIDR 區塊清單，並使用第一個找到適用於可用區域和 VPC 且具有可用地址的子網路。如果 Firewall Manager 在 VPC 中找不到開放空間（有或沒有限制），則服務不會在 VPC 中建立防火牆。

如果 Firewall Manager 無法在可用區域中建立所需的防火牆子網路，則會將該子網路標記為不符合政策。當區域處於此狀態時，區域的流量必須跨越區域界限，才能由另一個區域中的端點篩選。這類似於單一防火牆子網路案例。

Firewall Manager 如何管理您的 Network Firewall 資源

本節說明如何在 Firewall Manager 中管理 Network Firewall 資源。

當您在 Firewall Manager 中定義政策時，您會提供標準 AWS Network Firewall 防火牆政策的網路流量篩選行為。您可以新增無狀態和具狀態網路防火牆規則群組，並為不符合任何無狀態規則的封包指定預設動作。如需在 中使用防火牆政策的資訊 AWS Network Firewall，請參閱[AWS Network Firewall 防火牆政策](#)。

對於分散式和集中式政策，當您儲存網路防火牆政策時，防火牆管理員會在政策範圍內的每個 VPC 中建立防火牆和防火牆政策。Firewall Manager 透過串連下列值來命名這些 Network Firewall 資源：

- 固定字串，FManagedNetworkFirewall 或 FManagedNetworkFirewallPolicy，取決於資源類型。
- Firewall Manager 政策名稱。這是您在建立政策時指派的名稱。
- Firewall Manager 政策 ID。這是 Firewall Manager 政策 AWS 的資源 ID。
- Amazon VPC ID。這是 Firewall Manager 建立防火牆和防火牆政策的 VPC AWS 資源 ID。

以下顯示由 Firewall Manager 管理之防火牆的範例名稱：

```
FManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```


以下顯示防火牆政策名稱範例：

```
FMMangedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

建立政策後，VPCs 中的成員帳戶無法覆寫防火牆政策設定或規則群組，但他們可以將規則群組新增至防火牆管理員建立的防火牆政策。

Firewall Manager 如何管理和監控政策的 VPC 路由表

本節說明 Firewall Manager 如何管理和監控 VPC 路由表。

Note

使用集中式部署模型的政策目前不支援路由表管理。

Firewall Manager 建立防火牆端點時，也會為其建立 VPC 路由表。不過，防火牆管理員不會管理您的 VPC 路由表。您必須設定 VPC 路由表，將網路流量導向 Firewall Manager 建立的防火牆端點。使用 Amazon VPC 傳入路由增強功能，變更路由表以透過新的防火牆端點路由流量。您的變更必須在您要保護的子網路和外部位置之間插入防火牆端點。您需要執行的確切路由取決於您的架構及其元件。

目前，防火牆管理員允許監控您的 VPC 路由表路由，以監控目的地為網際網路閘道的任何流量，而此流量會繞過防火牆。Firewall Manager 不支援其他目標閘道，例如 NAT 閘道。

如需有關管理 VPC 路由表的資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的[管理 VPC 路由表](#)。如需有關管理 Network Firewall 路由表的詳細資訊，請參閱《AWS Network Firewall 開發人員指南》中的[適用於的路由表組態 AWS Network Firewall](#)。

當您啟用政策監控時，防火牆管理員會持續監控 VPC 路由組態，並提醒您繞過該 VPC 防火牆檢查的流量。如果子網路有防火牆端點路由，則 Firewall Manager 會尋找下列路由：

- 將流量傳送至 Network Firewall 端點的路由。
- 將流量從 Network Firewall 端點轉送到網際網路閘道的路由。
- 從網際網路閘道到 Network Firewall 端點的傳入路由。
- 來自防火牆子網路的路由。

如果子網路具有網路防火牆路由，但網路防火牆和網際網路閘道路由表中有非對稱路由，則 Firewall Manager 會將子網路報告為不合規。Firewall Manager 也會偵測 Firewall Manager 建立的防火牆路由

表中網際網路閘道的路由，以及子網路的路由表，並將其回報為不合規。Network Firewall 子網路路由表和網際網路閘道路由表中的其他路由也會回報為不合規。視違規類型而定，防火牆管理員會建議修補動作，讓路由組態符合規範。Firewall Manager 不會在所有情況下提供建議。例如，如果您的客戶子網路具有在 Firewall Manager 外部建立的防火牆端點，則 Firewall Manager 不建議修補動作。

根據預設，防火牆管理員會將任何超過可用區域界限的流量標記為不合規。不過，如果您選擇自動在 VPC 中建立單一端點，防火牆管理員不會將跨越可用區域界限的流量標記為不合規。

對於使用具有自訂端點組態的分散式部署模型的政策，您可以選擇從沒有防火牆端點的可用區域跨越可用區域界限的流量是否標記為合規或不合規。

Note

- Firewall Manager 不建議 non-IPv4 路由的修補動作，例如 IPv6 和字首清單路由。
- 使用 DisassociateRouteTable API 呼叫進行的呼叫最多可能需要 12 小時才能偵測。
- Firewall Manager 會為包含防火牆端點的子網路建立 Network Firewall 路由表。Firewall Manager 假設此路由表僅包含有效的網際網路閘道和 VPC 預設路由。此路由表中的任何額外或無效路由都會被視為不合規。

當您設定 Firewall Manager 政策時，如果您選擇監控模式，則 Firewall Manager 會提供資源違規和資源修補的詳細資訊。您可以使用這些建議的修補動作來修正路由表中的路由問題。如果您選擇關閉模式，防火牆管理員不會為您監控路由表內容。使用此選項，您可以自行管理 VPC 路由表。如需這些資源違規的詳細資訊，請參閱[檢視 AWS Firewall Manager 政策的合規資訊](#)。

Warning

如果您在建立政策時選擇監控 AWS Network Firewall 低路由組態，則無法關閉該政策的組態。不過，如果您選擇關閉，您可以稍後再啟用它。

設定 AWS Network Firewall 政策的記錄

本節說明如何啟用網路防火牆政策的集中式記錄，以取得組織內流量的詳細資訊。您可以選擇流程記錄以擷取網路流量流程，或提醒記錄以報告符合規則且規則動作設為 DROP 或的流量 ALERT。如需記錄的詳細資訊 AWS Network Firewall，請參閱《AWS Network Firewall 開發人員指南》中的[從記錄網路流量 AWS Network Firewall](#)。

您可以將日誌從政策的網路防火牆防火牆傳送至 Amazon S3 儲存貯體。啟用記錄後，會透過更新防火牆設定，將日誌 AWS Network Firewall 傳遞至您選取的 Amazon S3 儲存貯體，並保留 AWS Firewall Manager 字首，來傳遞每個已設定之 Network Firewall 的日誌<policy-name>-<policy-id>。

Note

Firewall Manager 使用此字首來判斷 Firewall Manager 是否新增了記錄組態，或帳戶擁有者是否新增了記錄組態。如果帳戶擁有者嘗試使用保留字首進行自己的自訂記錄，則會由 Firewall Manager 政策中的記錄組態覆寫。

如需如何建立 Amazon S3 儲存貯體和檢閱儲存日誌的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[什麼是 Amazon S3 ?](#)。

若要啟用記錄，您必須符合下列要求：

- 您在 Firewall Manager 政策中指定的 Amazon S3 必須存在。
- 您必須具備下列許可：
 - logs:CreateLogDelivery
 - s3:GetBucketPolicy
 - s3:PutBucketPolicy
- 如果記錄目的地的 Amazon S3 儲存貯體使用伺服器端加密與存放於 中的金鑰 AWS Key Management Service，您必須將下列政策新增至 AWS KMS 客戶受管金鑰，以允許 Firewall Manager 登入您的 CloudWatch Logs 日誌群組：

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt*",
    "kms:Decrypt*",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:Describe*"
  ],
  "Resource": "*"
}
```

```
}
```

請注意，只有 Firewall Manager 管理員帳戶中的儲存貯體可用於 AWS Network Firewall 中央記錄。

當您在網路防火牆政策上啟用集中式記錄時，防火牆管理員會在您的帳戶上執行這些動作：

- Firewall Manager 會更新所選 S3 儲存貯體的許可，以允許日誌交付。
- Firewall Manager 會在 S3 儲存貯體中為政策範圍內的每個成員帳戶建立目錄。您可以在 `找到每個帳戶的日誌<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`。

啟用網路防火牆政策的記錄

1. 使用您的 Firewall Manager 管理員帳戶建立 Amazon S3 儲存貯體。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[建立儲存貯體](#)。
2. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱[AWS Firewall Manager 先決條件](#)。

3. 在導覽窗格中，選擇安全政策。
4. 選擇您要啟用記錄的網路防火牆政策。如需 AWS Network Firewall 記錄的詳細資訊，請參閱《AWS Network Firewall 開發人員指南》中的[從記錄網路流量 AWS Network Firewall](#)。
5. 在政策詳細資訊索引標籤的政策規則區段中，選擇編輯。
6. 若要啟用和彙總日誌，請在記錄組態下選擇一或多個選項：
 - 啟用和彙總流程日誌
 - 啟用和彙總警示日誌
7. 選擇您要交付日誌的 Amazon S3 儲存貯體。您必須為您啟用的每個日誌類型選擇一個儲存貯體。您可以針對這兩種日誌類型使用相同的儲存貯體。
8. （選用）如果您想要將自訂成員帳戶建立的記錄取代為政策的記錄組態，請選擇覆寫現有的記錄組態。
9. 選擇 Next (下一步)。

10. 檢閱您的設定，然後選擇儲存以儲存對政策的變更。

停用網路防火牆政策的記錄

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇安全政策。
3. 選擇您要停用記錄的網路防火牆政策。
4. 在政策詳細資訊索引標籤的政策規則區段中，選擇編輯。
5. 在記錄組態狀態下，取消選取啟用和彙總流量日誌，以及如果選取啟用和彙總提醒日誌。
6. 選擇 Next (下一步)。
7. 檢閱您的設定，然後選擇儲存以儲存對政策的變更。

在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策

此頁面說明如何使用 AWS Firewall Manager DNS 防火牆政策來管理 Amazon Route 53 Resolver DNS 防火牆規則群組與組織中 Amazon Virtual Private Cloud VPCs 之間的關聯 AWS Organizations。您可以將集中控制的規則群組套用到整個組織，或套用到帳戶和 VPCs 的選取子集。

DNS Firewall 為您的 VPCs 提供傳出 DNS 流量的篩選和調節。您可以在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合，並將規則群組與 VPCs 建立關聯。當您套用 Firewall Manager 政策時，針對政策範圍內的每個帳戶和 VPC，Firenet Manager 會使用您在 Firewall Manager 政策中指定的關聯優先順序設定，在政策中的每個 DNS 防火牆規則群組與政策範圍內的每個 VPC 之間建立關聯。

如需使用 DNS 防火牆的相關資訊，請參閱《[Amazon Route 53 開發人員指南](#)》中的 [Amazon Route 53 Resolver DNS 防火牆](#)。 <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

下列各節涵蓋使用 Firewall Manager DNS Firewall 政策的要求，並說明政策的運作方式。如需建立政策的程序，請參閱 [為 Amazon Route 53 Resolver DNS 防火牆建立 AWS Firewall Manager 政策](#)。

⚠ Important

您必須啟用資源共用。DNS 防火牆政策會與您組織中的帳戶共用 DNS 防火牆規則群組。若要讓此項目運作，您必須啟用 資源共用 AWS Organizations。如需如何啟用資源共用的資訊，請參閱[Network Firewall 和 DNS Firewall 政策的資源共用](#)。

⚠ Important

您必須定義 DNS 防火牆規則群組。當您指定新的 DNS 防火牆政策時，您可以定義規則群組，就像直接使用 Amazon Route 53 Resolver DNS 防火牆一樣。您的規則群組必須已存在於 Firewall Manager 管理員帳戶中，您才能將規則群組包含在政策中。如需建立 DNS 防火牆規則群組的詳細資訊，請參閱 [DNS 防火牆規則群組和規則](#)。

您可以定義最低和最高優先順序的規則群組關聯

您透過 Firewall Manager DNS Firewall 政策管理的 DNS 防火牆規則群組關聯包含 VPCs 的最低優先順序關聯和最高優先順序關聯。在您的政策組態中，這些顯示為第一個和最後一個規則群組。

DNS 防火牆會依下列順序篩選 VPC 的 DNS 流量：

1. 第一個規則群組，由您在 Firewall Manager DNS Firewall 政策中定義。有效值介於 1 到 99 之間。
2. 個別帳戶管理員透過 DNS 防火牆相關聯的 DNS 防火牆規則群組。
3. 最後一個規則群組，由您在 Firewall Manager DNS Firewall 政策中定義。有效值介於 9,901 和 10,000 之間。

Firewall Manager 如何為其建立的規則群組關聯命名

當您儲存 DNS 防火牆政策時，如果您啟用自動修復，則 Firewall Manager 會在政策中提供的規則群組與政策範圍內的 VPCs 之間建立 DNS 防火牆關聯。Firewall Manager 透過串連下列值來命名這些關聯：

- 固定字串 FMManaged_。
- Firewall Manager 政策 ID。這是 Firewall Manager 政策 AWS 的資源 ID。

以下顯示由 Firewall Manager 管理之防火牆的範例名稱：


```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

建立政策後，如果 VPCs 中的帳戶擁有者覆寫您的防火牆政策設定或規則群組關聯，則 Firewall Manager 會將政策標記為不合規，並嘗試提議補救動作。帳戶擁有者可以將其他 DNS 防火牆規則群組與 DNS 防火牆政策範圍內的 VPCs 建立關聯。由個別帳戶擁有者建立的任何關聯，都必須在第一個和最後一個規則群組關聯之間具有優先順序設定。

從 Firewall Manager DNS Firewall 政策刪除規則群組

刪除規則群組

若要從 Firewall Manager DNS Firewall 政策刪除規則群組，您必須執行下列步驟：

1. 從 Firewall Manager DNS Firewall 政策中移除規則群組。
2. 取消共用 中的規則群組 AWS Resource Access Manager。若要取消共用您擁有的規則群組，您必須將其從資源共用中移除。您可以使用 AWS RAM 主控台或 CLI AWS 來執行此操作。如需有關取消共用資源的資訊，請參閱AWS RAM 《使用者指南》中的[在 中更新資源共用 AWS RAM](#)。
3. 使用 DNS 防火牆主控台或 CLI AWS 刪除規則群組。

使用 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 政策

Palo Alto Networks 雲端新一代防火牆 (NGFW) 是一項第三方防火牆服務，可用於您的 AWS Firewall Manager 政策。使用適用於 Firewall Manager 的 Palo Alto Networks Cloud NGFW，您可以建立並集中部署您所有 AWS 帳戶的 Palo Alto Networks Cloud NGFW 資源和規則集。

若要搭配 Firewall Manager 使用 Palo Alto Networks 雲端 NGFW，請先在 AWS Marketplace 中訂閱 [Palo Alto Networks 雲端 NGFW Pay-As-You-Go](#) 服務。訂閱後，您會在 Palo Alto Networks 雲端 NGFW 服務中執行一系列步驟，以設定您的帳戶和雲端 NGFW 設定。然後，您可以建立 Firewall Manager Cloud FMS 政策，以集中部署和管理 AWS 組織中所有帳戶的 Palo Alto Networks Cloud NGFW 資源和規則。

如需建立 Firewall Manager 政策的程序，請參閱 [為 Palo Alto Networks 雲端 NGFW 建立 AWS Firewall Manager 政策](#)。如需有關如何設定和管理適用於 Firewall Manager 的 Palo Alto Networks 雲端 NGFW 的資訊，請參閱文件上的 [Palo Alto Networks Palo Alto Networks 雲端 NGFW AWS](#)。如需支援 AWS 的區域，請參閱[AWS 適用於支援區域和區域的雲端 NGFW](#)。

使用 Fortigate 雲端原生防火牆 (CNF) 做為 Firewall Manager 的服務政策

Fortigate Cloud Native Firewall (CNF) as a Service 是一種第三方防火牆服務，可用於您的 AWS Firewall Manager 政策。Fortigate CNF 是新一代防火牆服務，可讓您輕鬆保護雲端網路和管理安全政策。透過 Fortigate CNF for Firewall Manager，您可以在所有 AWS 帳戶中建立和集中部署 Fortigate CNF 資源和政策集。

若要將 Fortigate CNF 與 Firewall Manager 搭配使用，首先在 [AWS Marketplace 中訂閱 Fortigate 雲端原生防火牆 \(CNF\) 即服務](#)。訂閱後，您可以在 Fortigate CNF 服務中執行一系列步驟，以設定全域政策集和其他設定。然後，您可以建立 Firewall Manager 政策，在 AWS 組織中的所有帳戶中集中部署和管理 Fortigate CNF 資源。

如需建立 Fortigate CNF Firewall Manager 政策的程序，請參閱[建立 Fortigate 雲端原生防火牆 \(CNF\) as a Service AWS Firewall Manager 的政策](#)。如需有關如何設定和管理 Fortigate CNF 以搭配 Firewall Manager 使用的資訊，請參閱 [Fortigate CNF 文件](#)。

Network Firewall 和 DNS Firewall 政策的資源共用

若要管理 Firewall Manager 網路防火牆和 DNS 防火牆政策，您必須在 AWS Organizations 中啟用與的資源共用 AWS Resource Access Manager。這可讓 Firewall Manager 在您建立這些政策類型時跨您的帳戶部署保護。

若要啟用資源共用，請遵循 AWS Resource Access Manager 使用者指南中的[啟用與 共用 AWS Organizations](#)中的指示。

資源共用的問題

當您使用 AWS RAM 來啟用資源共用，或當您處理需要資源共用的 Firewall Manager 政策時，您可能會遇到問題。

這些問題的範例包括下列項目：

- 當您依照指示啟用共用時，在 AWS RAM 主控台中，啟用與 共用 AWS Organizations 的選項會顯示為灰色，且無法選取。
- 當您在 Firewall Manager 中處理需要資源共用的政策時，政策會標記為不合規，而且您會看到指出資源共用或未 AWS RAM 啟用的訊息。

如果您在資源共用時遇到問題，請使用下列程序來嘗試啟用它。

再試一次以啟用資源共用

- 請再試一次，以使用下列其中一個選項啟用共用：
 - (選項) 透過 AWS RAM 主控台，遵循 AWS Resource Access Manager 使用者指南中的[啟用與共用 AWS Organizations](#)中的指示。
 - (選項) 使用 AWS RAM API，呼叫 `EnableSharingWithAwsOrganization`。請參閱[EnableSharingWithAwsOrganization](#) 的文件。

使用 Firewall Manager 受管清單

本節說明什麼是受管清單，以及如何使用這些清單。

受管應用程式和通訊協定清單可簡化 AWS Firewall Manager 內容稽核安全群組政策的組態和管理。您可以使用受管清單來定義政策允許和不允許的通訊協定和應用程式。如需內容稽核安全群組政策的相關資訊，請參閱[搭配 Firewall Manager 使用內容稽核安全群組政策](#)。

您可以在內容稽核安全群組政策中使用下列類型的受管清單：

- Firewall Manager 應用程式清單和通訊協定清單 – Firewall Manager 會管理這些清單。
 - 應用程式清單包含 `FMS-Default-Public-Access-Apps-Allowed`和 `FMS-Default-Public-Access-Apps-Denied`，描述應允許或拒絕給一般大眾的常用應用程式。
 - 通訊協定清單包含 `FMS-Default-Protocols-Allowed`，即應允許一般大眾使用的常用通訊協定清單。您可以使用 Firewall Manager 管理的任何清單，但無法編輯或刪除。
- 自訂應用程式清單和通訊協定清單 – 您可以管理這些清單。您可以使用您需要的設定來建立任一類型的清單。您可以完全控制自己的自訂受管清單，也可以視需要建立、編輯和刪除這些清單。

Note

目前，當您刪除自訂受管清單時，防火牆管理員不會檢查其參考。這表示即使作用中的政策正在使用自訂受管應用程式清單或通訊協定清單，您也可以刪除。這可能會導致政策停止運作。只有在您確認任何作用中政策未參考應用程式清單或通訊協定清單之後，才能將其刪除。

受管清單是 AWS 資源。您可以標記自訂受管清單。您無法標記 Firewall Manager 受管清單。

受管清單版本控制

自訂受管清單沒有版本。當您編輯自訂清單時，參考清單的政策會自動使用更新的清單。

Firewall Manager 受管清單會進行版本控制。Firewall Manager 服務團隊會視需要發佈新版本，以將最佳安全實務套用至清單。

當您在政策中使用 Firewall Manager 受管清單時，您可以選擇版本控制策略，如下所示：

- 最新可用版本 – 如果您未指定清單的明確版本設定，則您的政策會自動使用最新版本。這是透過主控台提供的唯一選項。
- 明確版本 – 如果您為清單指定版本，則您的政策會使用該版本。在您修改版本設定之前，您的政策會維持鎖定至您指定的版本。若要指定版本，您必須在主控台外部定義政策，例如透過 CLI 或其中一個 SDKs。

如需選擇清單版本設定的詳細資訊，請參閱[在內容稽核安全群組政策中使用受管清單](#)。

在內容稽核安全群組政策中使用受管清單

當您建立內容稽核安全群組政策時，您可以選擇使用受管稽核政策規則。此選項的某些設定需要受管應用程式清單或通訊協定清單。這些設定的範例包括安全群組規則中允許的通訊協定，而應用程式可以存取網際網路。

下列限制適用於使用受管清單的每個政策設定：

- 您最多可以為任何設定指定一個 Firewall Manager 受管清單。根據預設，您最多可以指定一個自訂清單。自訂清單限制是軟配額，因此您可以請求增加配額。如需詳細資訊，請參閱[AWS Firewall Manager 配額](#)。
- 在 主控台中，如果您選取 Firewall Manager 受管清單，則無法指定版本。政策一律會使用最新版本的清單。若要指定版本，您必須在主控台外部定義政策，例如透過 CLI 或其中一個 SDKs。如需 Firewall Manager 受管清單版本控制的資訊，請參閱[受管清單版本控制](#)。

如需透過主控台建立內容稽核安全群組政策的相關資訊，請參閱[建立內容稽核安全群組政策](#)。

在 Firewall Manager 中建立自訂受管清單

請依照這些程序來建立自訂受管應用程式清單或自訂受管通訊協定清單。

主題

- [建立自訂受管應用程式清單](#)
- [建立自訂受管通訊協定清單](#)

建立自訂受管應用程式清單

建立自訂受管應用程式清單

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇應用程式清單。
3. 在應用程式清單頁面中，選擇建立應用程式清單。
4. 在建立應用程式清單頁面中，為您的清單命名。請勿使用 字首，fms- 因為此字首已保留給 Firewall Manager。
5. 透過提供通訊協定和連接埠號碼，或從類型下拉式清單中選取應用程式，來指定應用程式。為您的應用程式規格命名。
6. 選擇視需要新增另一個，並填寫應用程式資訊，直到您完成清單為止。
7. （選用）將標籤套用至您的清單。
8. 選擇儲存以儲存您的清單並返回應用程式清單頁面。

建立自訂受管通訊協定清單

建立自訂受管通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇通訊協定清單。
3. 在通訊協定清單頁面中，選擇建立通訊協定清單。
4. 在通訊協定清單建立頁面中，為您的清單命名。請勿使用字首 fms-，因為已保留給 Firewall Manager。
5. 指定通訊協定。
6. 選擇視需要新增另一個，並填寫通訊協定資訊，直到您完成清單為止。
7. （選用）將標籤套用至您的清單。
8. 選擇儲存以儲存您的清單並返回通訊協定清單頁面。

在 Firewall Manager 中檢視受管清單

檢視應用程式清單或通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇應用程式清單或通訊協定清單。

頁面會顯示所有可供您使用的所選類型清單。Firewall Manager 管理的清單在 ManagedList 欄中有 Y。

3. 若要查看清單的詳細資訊，請選擇其名稱。詳細資訊頁面會顯示清單的內容和任何標籤。

針對 Firewall Manager 受管清單，您也可以選取版本下拉式清單來查看可用的版本。

在 Firewall Manager 中刪除自訂受管清單

您可以刪除自訂受管清單。您無法編輯或刪除 Firewall Manager 管理的清單。

 Note

目前，當您刪除自訂受管清單時，防火牆管理員不會檢查其參考。這表示即使作用中的政策正在使用自訂受管應用程式清單或通訊協定清單，您也可以刪除。這可能會導致政策停止運作。只有在您確認任何作用中政策未參考應用程式清單或通訊協定清單之後，才能將其刪除。

刪除自訂受管應用程式或通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在 開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

 Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 執行下列動作，確定您要刪除的清單未用於任何稽核安全群組政策：
 - a. 在導覽窗格中，選擇 Security policies (安全群組政策)。
 - b. 在AWS Firewall Manager 政策頁面中，選取並編輯您的稽核安全群組，並移除您要刪除之自訂清單的任何參考。

如果您刪除在稽核安全群組政策中使用的自訂受管清單，則使用它的政策可能會停止運作。

3. 在導覽窗格中，根據要刪除的清單類型，選擇應用程式清單或通訊協定清單。
4. 在清單頁面中，選取您要刪除的自訂清單，然後選擇刪除。

在 Firewall Manager 中分組您的資源

本節說明什麼是資源集，並列出使用資源集的考量事項。

An AWS Firewall Manager resource set 是一組資源，例如防火牆，您可以在 Firewall Manager 政策中分組和管理這些資源。資源集可讓您組織中的成員精細控制政策中要管理的資源。若要使用資源集，請在 主控台 或使用 [PutResourceSet](#) API 建立資源集，然後將資源集新增至 Firewall Manager 政策。

您可以為下列資源和安全政策類型建立和管理資源集：

資源類型	Firewall Manager 安全政策類型
AWS Network Firewall - 防火牆	Network Firewall 政策 - 使用資源集從 Network Firewall 匯入現有的防火牆。如需有關在網路防火牆政策中使用資源集的資訊，請參閱 為建立 AWS Firewall Manager 政策 AWS Network Firewall 程序中的 匯入現有防火牆 步驟。

下列各節涵蓋建立和刪除資源集的需求。

主題

- [在 Firewall Manager 中使用資源集時的考量事項](#)
- [在 Firewall Manager 中建立資源集](#)
- [在 Firewall Manager 中刪除資源集](#)

在 Firewall Manager 中使用資源集時的考量事項

使用資源集時，請注意下列考量事項。

參考不存在的資源

當您將資源新增至資源集時，您可以使用 Amazon Resource Name (ARN) 建立資源的參考。Firewall Manager 會驗證 Amazon Resource Name (ARN) 是否為正確的格式，但 Firewall Manager 不會檢查參考的資源是否存在。如果資源不存在但尚未通過 ARN 驗證，則 Firewall Manager 會在資源集中包含資源參考。如果稍後建立具有相同 ARN 的新資源，則 Firewall Manager 會將資源集的關聯政策中的規則群組套用至新資源。

已刪除的資源

刪除資源集中的資源時，資源的參考會保留在資源集中，直到 Firewall Manager 管理員將其移除為止。

離開 AWS Organizations 組織的成員帳戶擁有的資源

如果成員帳戶離開組織，對該成員帳戶擁有的資源的任何參考都會保留在資源集中，但不再由資源集相關聯的任何政策進行管理。

與多個政策的關聯

資源集可以與多個政策相關聯，但並非所有政策類型都支援管理相同資源的多個政策。如需不支援案例的相關資訊，請參閱特定政策類型的文件。

在 Firewall Manager 中建立資源集

建立資源集（主控台）

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇資源集。
3. 選擇建立資源集。
4. 針對資源集名稱，輸入描述性名稱。
5. （選用）輸入資源集的描述。
6. 選擇 Next (下一步)。
7. 對於選擇資源，選取AWS 帳戶 ID，然後選取選擇資源，將此帳戶擁有和管理的資源新增至資源集。選取資源後，選取新增將資源新增至資源集。
8. 選擇 Next (下一步)。
9. 針對資源集標籤，新增您要用於資源集的任何識別標籤。如需標籤的詳細資訊，請參閱[使用標籤編輯器](#)。
10. 選擇 Next (下一步)。
11. 檢閱新的資源集。若要進行任何變更，請在您要變更的區域中選擇 Edit (編輯)。這會讓您返回建立精靈中的對應步驟。當您對資源集感到滿意時，請選擇建立資源集。

在 Firewall Manager 中刪除資源集

您必須先使用資源集取消資源集與所有政策的關聯，才能刪除資源集。您可以使用 主控台或 [PutPolicy API](#)，在政策詳細資訊頁面取消資源群組的關聯。

刪除資源集（主控台）

1. 在導覽窗格中，選擇資源集。
2. 選擇您要刪除的資源集旁的選項。
3. 選擇 Delete (刪除)。

檢視 AWS Firewall Manager 政策的合規資訊

本節提供檢視 AWS Firewall Manager 政策範圍內帳戶和資源合規狀態的指引。如需在 中設定控制項 AWS 以維護雲端安全性和合規性的相關資訊，請參閱 [Firewall Manager 的合規驗證](#)。

Note

為了讓 Firewall Manager 監控政策合規性，AWS Config 必須持續記錄受保護資源的組態變更。在您的 AWS Config 組態中，錄製頻率必須設定為連續，這是預設設定。

Note

若要在受保護的資源中維持適當的合規狀態，請避免重複變更 Firewall Manager 保護的狀態，無論是自動或手動。Firewall Manager 使用來自 的資訊 AWS Config 來偵測資源組態的變更。如果快速套用變更，AWS Config 可能會失去部分變更的追蹤，這可能會導致防火牆管理員中有關合規或修復狀態的資訊遺失。

如果您發現您使用 Firewall Manager 保護的資源具有不正確的合規或修復狀態，請先確定您沒有執行任何程序來變更或重設 Firewall Manager 保護，然後重新評估其中相關聯的組態規則，以重新整理資源的 AWS Config 追蹤 AWS Config。

如果您修改政策或範圍內資源，可能需要幾分鐘的時間，才能顯示合規狀態和詳細資訊的更新。

對於所有 AWS Firewall Manager 政策，您可以檢視政策範圍內帳戶和資源的合規狀態。如果政策中的設定反映在帳戶或資源的設定中，則帳戶或資源符合 Firewall Manager 政策。每個政策類型都有自己

的合規要求，您可以在定義政策時調整。對於某些政策，您也可以檢視範圍內資源的詳細違規資訊，以協助您進一步了解和管理安全風險。

檢視政策的合規資訊

1. AWS Management Console 使用您的 Firewall Manager 管理員帳戶登入，然後在開啟 Firewall Manager 主控台<https://console.aws.amazon.com/wafv2/fmsv2>。如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

Note

如需建立防火牆管理員帳戶的詳細資訊，請參閱 [AWS Firewall Manager 先決條件](#)。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇政策。在政策頁面的帳戶和資源索引標籤中，防火牆管理員會列出組織中的帳戶，並依政策範圍內的帳戶和範圍外的帳戶分組。

政策範圍窗格內的帳戶會列出每個帳戶的合規狀態。合規狀態表示政策已成功套用至帳戶的所有範圍內資源。不合規狀態表示政策尚未套用至帳戶的一或多個範圍內資源。

4. 選擇不合規的帳戶。在帳戶頁面中，防火牆管理員會列出每個不合規資源的 ID 和類型，以及資源違反政策的原因。

Note

針對資源類型 `AWS::EC2::NetworkInterface(ENI)` 和 `AWS::EC2::Instance`，防火牆管理員可能會顯示數量有限的不合規資源。若要列出其他不合規資源，請修正最初為帳戶顯示的資源。

5. 如果 Firewall Manager 政策類型是內容稽核安全群組政策，您可以存取資源的詳細違規資訊。

若要檢視違規詳細資訊，請選擇 資源。

Note

在新增詳細資源違規頁面之前，防火牆管理員發現不合規的資源可能沒有違規詳細資訊。

在資源頁面中，防火牆管理員會根據資源類型列出有關違規的特定詳細資訊。

- **AWS::EC2::NetworkInterface** (ENI) – Firewall Manager 會顯示資源未遵循的安全群組相關資訊。選擇安全群組以查看其詳細資訊。
- **AWS::EC2::Instance** – Firewall Manager 會顯示連接至 EC2 執行個體的 ENI，而該執行個體不合規。它也會顯示資源未遵守的安全群組相關資訊。選擇安全群組以查看其詳細資訊。
- **AWS::EC2::SecurityGroup** – Firewall Manager 會顯示下列違規詳細資訊：
 - 不合規的安全群組規則 – 違規的規則，包括其通訊協定、連接埠範圍、IP CIDR 範圍和描述。
 - 參考規則 – 不合規安全群組規則違反的稽核安全群組規則及其詳細資訊。
 - 違規原因 – 不合規問題清單的說明。
 - 修復動作 – 建議採取的動作。如果 Firewall Manager 無法判斷安全修補動作，則此欄位為空白。
- **AWS::EC2::Subnet** – 用於網路 ACL 和網路防火牆政策。

Firewall Manager 會顯示子網路 ID、VPC ID 和可用區域。如適用，Firewall Manager 會包含有關違規的其他資訊。違規描述元件包含資源預期狀態的描述、目前、不合規狀態，以及可用時造成差異的描述。

網路防火牆違規

- 路由管理違規 – 對於使用監控模式的網路防火牆政策，防火牆管理員會在子網路、網際網路閘道和網路防火牆子網路路由表中顯示基本子網路資訊，以及預期和實際路由。Firewall Manager 會提醒您，如果實際路由與路由表中的預期路由不相符，則會發生違規。
- 路由管理違規的修補動作 – 對於使用監控模式的網路防火牆政策，防火牆管理員建議對違規的路由組態採取可能的修補動作。

例如，假設子網路預期會透過防火牆端點傳送流量，但目前的子網路會直接將流量傳送至網際網路閘道。這是路由管理違規。在這種情況下，建議的補救措施可能是排序動作的清單。首先，建議將必要的路由新增至網路防火牆子網路的路由表，以將傳出流量導向網際網路閘道，並將 VPC 內目的地的傳入流量導向 `local`。第二個建議是取代網際網路閘道路由或子網路路由表中無效的網路防火牆路由，以將傳出流量導向防火牆端點。第三個建議是將必要的路由新增至網際網路閘道的路由表，以將傳入流量導向防火牆端點。

- **AWS::EC2::InternetGateway** – 用於已啟用監控模式的網路防火牆政策。
 - 路由管理違規 – 如果網際網路閘道未與路由表建立關聯，或網際網路閘道路由表中有無效的路由，表示網際網路閘道不合規。
 - 路由管理違規的修補動作 – Firewall Manager 建議可能的修補動作，以修補路由管理違規。

Example 1 – 路由管理違規和修復建議

網際網路閘道未與路由表建立關聯。建議的修補動作可能是排序動作的清單。第一個動作是建立路由表。第二個動作是將路由表與網際網路閘道建立關聯。第三個動作是將所需的路由新增至網際網路閘道路由表。

Example 2 – 路由管理違規和修復建議

網際網路閘道與有效的路由表相關聯，但路由設定不正確。建議的修補可能是排序動作的清單。第一個建議是移除無效的路由。第二個是將所需的路由新增至網際網路閘道路由表。

- **AWS::NetworkFirewall::FirewallPolicy** – 用於網路防火牆政策。Firewall Manager 會顯示有關網路防火牆政策的資訊，該政策已修改，使其不合規。此資訊提供預期的防火牆政策和在客戶帳戶中找到的政策，因此您可以比較無狀態和有狀態規則群組名稱和優先順序設定、自訂動作名稱和預設無狀態動作設定。違規描述元件包含資源預期狀態的描述、目前、不合規狀態，以及可用時造成差異的描述。
- **AWS::EC2::VPC** – 用於 DNS 防火牆政策。Firewall Manager 會顯示有關 VPC 的資訊，該 VPC 位於 Firewall Manager DNS 防火牆政策的範圍內，且不符合政策。提供的資訊包括預期與 VPC 相關聯的預期規則群組和實際規則群組。違規描述元件包含資源預期狀態的描述、目前、不合規狀態，以及可用時造成差異的描述。
- **AWS::WAFv2::WebACL** – 用於其組態指定修改現有 Web ACLs AWS WAF 的政策。Firewall Manager 會顯示與範圍內資源相關聯的 Web ACL 相關資訊，但無法完全相容於 Firewall Manager 的改造。例如，如果 Web ACL 也與不在政策範圍內的資源建立關聯，則 Firewall Manager 無法將其修改。

AWS Firewall Manager 與 整合 AWS Security Hub

此頁面說明如何同時使用 Firewall Manager 和 Security Hub。

AWS Firewall Manager 會為不符合合規的資源以及偵測到的攻擊建立問題清單，並將其傳送至其中 AWS Security Hub。如需 Security Hub 調查結果的資訊，請參閱 [中的調查結果 AWS Security Hub](#)。

當您使用 Security Hub 和 Firewall Manager 時，Firewall Manager 會自動將您的問題清單傳送到 Security Hub。如需有關開始使用 Security Hub 的資訊，請參閱 [AWS Security Hub 《使用者指南》](#) 中的 [設定 AWS Security Hub](#)。

Note

Firewall Manager 只會更新其管理的政策及其監控的資源的調查結果。
Firewall Manager 不會解析下列問題清單：

- 已刪除的政策。
- 已刪除的資源。
- 超出 Firewall Manager 政策範圍的資源，例如因為標籤變更或政策定義變更。

如何檢視 Firewall Manager 問題清單？

若要在 Security Hub 中檢視 Firewall Manager 問題清單，請遵循 [Security Hub 中的使用問題清單](#) 的指示，並使用下列設定建立篩選條件：

- 屬性設定為 Product Name (產品名稱)。
- 運算子設定為 EQUALS (等於)。
- 數值設定為 Firewall Manager。此設定會區分大小寫。

我可以停用此項目嗎？

您可以透過 Security Hub 主控台，停用與 Security Hub 的 AWS Firewall Manager 調查結果整合。在導覽列中選擇整合，然後在 Firewall Manager 窗格中選擇停用整合。如需詳細資訊，請參閱《AWS Security Hub 使用者指南》<https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html>。

AWS Firewall Manager 問題清單類型

- [AWS WAF 政策 Firewall Manager 調查結果](#)
- [AWS Shield Advanced 政策 Firewall Manager 調查結果](#)
- [安全群組常見政策 Firewall Manager 調查結果](#)
- [安全群組內容稽核政策 Firewall Manager 調查結果](#)
- [安全群組用量稽核政策 Firewall Manager 調查結果](#)
- [Amazon Route 53 Resolver DNS Firewall 政策 Firewall Manager 調查結果](#)

AWS WAF 政策 Firewall Manager 調查結果

此頁面說明 AWS WAF 政策的 Firewall Manager 調查結果。

您可以使用 Firewall Manager AWS WAF 政策將 AWS WAF 規則群組套用至您的 資源 AWS Organizations。如需詳細資訊，請參閱[使用 AWS Firewall Manager 政策](#)。

資源遺失 Firewall Manager 受管 Web ACL。

AWS 資源沒有符合 Firewall Manager 政策的 AWS Firewall Manager 受管 Web ACL 關聯。您可以在政策上啟用 Firewall Manager 修復來修正此問題。

- 嚴重性 – 80
- 狀態設定 – 通過/失敗
- 更新 – 如果 Firewall Manager 執行修復動作，則會更新問題清單，且嚴重性會從 降低HIGH為 INFORMATIONAL。如果您執行修復，防火牆管理員將不會更新問題清單。

Firewall Manager 受管 Web ACL 設定錯誤的規則群組。

這是 AWS WAF Classic 政策調查結果。Web ACL 中由 Firewall Manager 管理的規則群組未根據 Firewall Manager 政策正確設定。這表示 Web ACL 缺少政策所需的規則群組。您可以在政策上啟用 Firewall Manager 修復來修正此問題。

- 嚴重性 – 80
- 狀態設定 – 通過/失敗
- 更新 – 如果 Firewall Manager 執行修復動作，則會更新問題清單，且嚴重性會從 降低HIGH為 INFORMATIONAL。如果您執行修復，防火牆管理員將不會更新問題清單。

AWS Shield Advanced 政策 Firewall Manager 調查結果

此頁面說明 AWS Shield Advanced 政策的 Firewall Manager 調查結果。

如需 AWS Shield Advanced 政策的相關資訊，請參閱 [在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

資源缺乏 Shield Advanced 保護。

根據 Firewall Manager 政策，應該具有 Shield Advanced 保護 AWS 的資源沒有它。您可以在政策上啟用 Firewall Manager 修復，這將啟用 資源的保護。

- 嚴重性 – 60
- 狀態設定 – 通過/失敗
- 更新 – 如果 Firewall Manager 執行修補動作，則會更新問題清單，且嚴重性會從 降低HIGH為 INFORMATIONAL。如果您執行修復，防火牆管理員將不會更新問題清單。

Shield Advanced 偵測到對受監控資源的攻擊。

Shield Advanced 偵測到受保護 AWS 資源的攻擊。您可以在政策上啟用 Firewall Manager 修補。

- 嚴重性 – 70
- 狀態設定 – 無
- 更新 – Firewall Manager 不會更新此調查結果。

安全群組常見政策 Firewall Manager 調查結果

此頁面說明安全群組常見政策的 Firewall Manager 調查結果。

如需安全群組通用政策的資訊，請參閱[在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

資源具有設定錯誤的安全群組。

Firewall Manager 已根據 Firewall Manager 政策，識別缺少其應擁有之 Firewall Manager 受管安全群組關聯的資源。您可以在政策上啟用 Firewall Manager 修復，該政策會根據政策設定建立關聯。

- 嚴重性 – 70
- 狀態設定 – 通過/失敗
- 更新 – Firewall Manager 會更新此調查結果。

Firewall Manager 複本安全群組與主要安全群組不同步。

根據 Firewall Manager 複本安全群組的常見安全群組政策，與其主要安全群組不同步。您可以在政策上啟用 Firewall Manager 修復，該政策會將複本安全群組與主要群組同步。

- 嚴重性 – 80
- 狀態設定 – 通過/失敗
- 更新 – Firewall Manager 會更新此調查結果。

安全群組內容稽核政策 Firewall Manager 調查結果

此頁面說明安全群組內容稽核政策的 Firewall Manager 調查結果。

如需安全群組內容稽核政策的相關資訊，請參閱[在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

安全群組不符合內容稽核安全群組。

Firewall Manager 安全群組內容稽核政策已識別不合規的安全群組。這是客戶建立的安全群組，位於內容稽核政策的範圍內，且不符合政策及其稽核安全群組所定義的設定。您可以在政策上啟用 Firewall Manager 修復，這會修改不合規的安全群組，使其符合規範。

- 嚴重性 – 70
- 狀態設定 – 通過/失敗
- 更新 – Firewall Manager 會更新此調查結果。

安全群組用量稽核政策 Firewall Manager 調查結果

此頁面說明安全群組用量稽核政策的 Firewall Manager 調查結果。

如需安全群組使用狀況稽核政策的相關資訊，請參閱[在 Firewall Manager 中使用安全群組政策來管理 Amazon VPC 安全群組](#)。

Firewall Manager 找到備援安全群組。

Firewall Manager 安全群組用量稽核已識別備援安全群組。這是具有相同規則的安全群組，設定為相同 Amazon Virtual Private Cloud 執行個體中的另一個安全群組。您可以在用量稽核政策上啟用 Firewall Manager 自動修復，這會取代備援安全群組，並使用單一安全群組。

- 嚴重性 – 30
- 狀態設定 – 無
- 更新 – Firewall Manager 不會更新此調查結果。

Firewall Manager 找到未使用的安全群組。

Firewall Manager 安全群組用量稽核已識別未使用的安全群組。這是任何 Firewall Manager 常見安全群組政策未參考的安全群組。您可以在用量稽核政策上啟用 Firewall Manager 自動修復，這會移除未使用的安全群組。

- 嚴重性 – 30
- 狀態設定 – 無
- 更新 – Firewall Manager 不會更新此調查結果。

Amazon Route 53 Resolver DNS Firewall 政策 Firewall Manager 調查結果

此頁面說明 Amazon Route 53 Resolver DNS 防火牆政策的 Firewall Manager 調查結果。

如需 DNS 防火牆政策的資訊，請參閱 [在 Firewall Manager 中使用 Amazon Route 53 Resolver DNS 防火牆政策](#)。

資源缺少 DNS 防火牆保護

VPC 缺少 Firewall Manager DNS Firewall 政策中定義的 DNS Firewall 規則群組關聯。調查結果會列出政策指定的規則群組。

- 嚴重性 – 80

您使用 AWS Firewall Manager 服務的安全性

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，該架構旨在滿足最安全敏感組織的需求。

Note

本節提供您使用 AWS Firewall Manager 服務及其 AWS 資源的標準 AWS 安全指導，例如 Firewall Manager 網路防火牆政策和安全群組政策。

如需使用 Firewall Manager 保護 AWS 資源的相關資訊，請參閱 Firewall Manager 指南的其餘部分。

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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用於 Firewall Manager 的合規計劃，請參閱[AWS 合規計劃範圍內的服務](#)。
- 雲端安全 – 您的責任取決於您使用 AWS 的服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您了解如何在使用 Firewall Manager 時套用共同責任模型。下列主題說明如何設定 Firewall Manager 以符合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 Firewall Manager 資源。

主題

- [Firewall Manager 中的資料保護](#)
- [的身分和存取管理 AWS Firewall Manager](#)
- [在 Firewall Manager 中記錄和監控](#)
- [Firewall Manager 的合規驗證](#)
- [Firewall Manager 中的復原能力](#)
- [AWS Firewall Manager 中的基礎設施安全](#)

Firewall Manager 中的資料保護

AWS [共同責任模型](#) 適用於 中的資料保護 AWS Firewall Manager。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](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 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 Firewall Manager 或其他 AWS 服務 使用主控台、API 或 AWS CLI

或 AWS SDKs 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。

Firewall Manager 實體，例如政策，會靜態加密，但無法使用加密的特定區域除外，包括中國（北京）和中國（寧夏）。每個區域都會採用唯一的加密金鑰。

的身分和存取管理 AWS Firewall Manager

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驗證（登入）和授權（具有許可）來使用 Firewall Manager 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 Firewall Manager 如何使用 IAM](#)
- [的身分型政策範例 AWS Firewall Manager](#)
- [AWS 的 受管政策 AWS Firewall Manager](#)
- [對 AWS Firewall Manager 身分和存取進行故障診斷](#)
- [使用 Firewall Manager 的服務連結角色](#)
- [預防跨服務混淆代理人](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Firewall Manager 中執行的工作。

服務使用者 – 如果您使用 Firewall Manager 服務來執行您的任務，則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 Firewall Manager 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 Firewall Manager 中的功能，請參閱 [對 AWS Shield 身分和存取進行故障診斷](#)。

服務管理員 – 如果您在公司負責 Firewall Manager 資源，您可能可以完整存取 Firewall Manager。您的任務是判斷服務使用者應存取哪些 Firewall Manager 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搭配 Firewall Manager 使用 IAM，請參閱[AWS Shield 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 Firewall Manager 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Firewall Manager 身分型政策範例，請參閱[AWS Shield 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登入資料，以聯合身分 AWS 身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您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 服務來使用與身分提供者的聯合來存取。

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登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，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 AWS 帳戶 和群組，以用於所有 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 中具有單一個人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 –** 服務連結角色是一種連結至 的服務角色。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 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到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源相關聯時，AWS 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](#)。委託人可以包含帳戶、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 AWS 服務 支援 RCPs 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 Firewall Manager 如何使用 IAM

使用 IAM 管理 Firewall Manager 的存取權之前，請先了解哪些 IAM 功能可與 Firewall Manager 搭配使用。

您可以搭配 使用的 IAM 功能 AWS Firewall Manager

IAM 功能	Firewall Manager 支援
身分型政策	是
資源型政策	否
政策動作	是

IAM 功能	Firewall Manager 支援
政策資源	是
政策條件索引鍵 (服務特定)	否
ACL	否
ABAC (政策中的標籤)	是
暫時性憑證	是
轉送存取工作階段 (FAS)	是
服務角色	部分
服務連結角色	是

若要取得 Firewall Manager 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱《IAM 使用者指南》中的[AWS 與 IAM 搭配使用的 服務](#)。

Firewall 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。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](#)。

若要檢視 Firewall Manager 身分型政策的範例，請參閱[的身分型政策範例 AWS Firewall Manager](#)。

Firewall Manager 的身分型政策範例

若要檢視 Firewall Manager 身分型政策的範例，請參閱[的身分型政策範例 AWS Firewall Manager](#)。

Firewall 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。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（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](#)。

Firewall 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 Firewall Manager 動作清單，請參閱服務授權參考中的 [定義的動作 AWS Firewall Manager](#)。

Firewall Manager 中的政策動作在動作之前使用以下字首：

```
fms
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
    "fms:action1",  
    "fms:action2"  
]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "fms:Describe*"
```

若要檢視 Firewall Manager 身分型政策的範例，請參閱 [的身分型政策範例 AWS Firewall Manager](#)。

Firewall 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。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 Firewall Manager 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 Firewall Manager](#)。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 Firewall Manager 定義的動作](#)。

若要檢視 Firewall Manager 身分型政策的範例，請參閱 [的身分型政策範例 AWS Firewall Manager](#)。

Firewall Manager 的政策條件金鑰

支援服務特定的政策條件索引鍵：否

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 Firewall Manager 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 Firewall Manager](#)。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 Firewall Manager](#)。

若要檢視 Firewall Manager 身分型政策的範例，請參閱 [的身分型政策範例 AWS Firewall Manager](#)。

Firewall 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。

ABAC 搭配 Firewall Manager

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 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 Firewall Manager 使用臨時登入資料

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時登入資料，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](#)。

Firewall Manager 的轉送存取工作階段

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](#)。

Firewall Manager 的服務角色

支援服務角色：部分

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 Firewall Manager 功能。只有在 Firewall Manager 提供指引時，才能編輯服務角色。

在 Firewall Manager 中選擇 IAM 角色

若要在 Firewall Manager 中使用 *PutNotificationChannel* API 動作，您必須選擇一個角色，以允許 Firewall Manager 存取 Amazon SNS，以便服務可以代表您發佈 Amazon SNS 訊息。如需詳細資訊，請參閱 AWS Firewall Manager API 參考中的 [PutNotificationChannel](#)。

以下顯示 SNS 主題許可設定範例。若要將此政策與您自己的自訂角色搭配使用，請將 `SnsRoleName` ARN `AWSServiceRoleForFMS` 的 Amazon Resource Name (ARN)。


```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

如需 Firewall Manager 動作和資源的詳細資訊，請參閱 [定義的動作 AWS Firewall Manager](#) AWS Identity and Access Management 指南主題

Firewall 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 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。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 AWS Firewall Manager

根據預設，使用者和角色沒有建立或修改 Firewall Manager 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 Firewall Manager 定義的動作和資源類型的詳細資訊，包括每個資源類型的 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 Firewall Manager](#)。

主題

- [政策最佳實務](#)

- [使用 Firewall Manager 主控台](#)
- [允許使用者檢視他們自己的許可](#)
- [授予 Firewall Manager 安全群組的讀取存取權](#)

政策最佳實務

身分型政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Firewall 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 AWS 受管政策來授予許多常見使用案例的許可。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 Firewall Manager 主控台

若要存取 AWS Firewall 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 Firewall 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 Firewall Manager 主控台，也請將 Firewall Manager *ConsoleAccess*或*ReadOnly* 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的許可，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": "*"
    }
  ]
}
```

```
]
}
```

授予 Firewall Manager 安全群組的讀取存取權

Firewall Manager 允許跨帳戶資源存取，但不允許您建立跨帳戶資源保護。您只能從擁有這些資源的帳戶內建立資源保護。

以下是授予 `fms:Get`、`fms:List` 和所有資源 `ec2:DescribeSecurityGroups` 動作許可的範例政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "fms:Get*",
        "fms:List*",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS 的 受管政策 AWS Firewall Manager

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#)。

AWS 受管政策：**AWSFMAAdminFullAccess**

使用 AWSFMAAdminFullAccess AWS 受管政策來允許管理員存取 AWS Firewall Manager 資源，包括所有 Firewall Manager 政策類型。此政策不包含在 中設定 Amazon Simple Notification Service 通知的許可 AWS Firewall Manager。如需如何設定 Amazon Simple Notification Service 存取權的詳細資訊，請參閱[設定 Amazon Simple Notification Service 的存取權](#)。

如需政策清單和詳細資訊，請參閱 [AWSFMAAdminFullAccess](#) 中的 IAM 主控台。本節的其餘部分提供政策設定的概觀。

許可陳述式

此政策會根據一組許可分組為陳述式。

- AWS Firewall Manager 政策資源 - 允許 中資源的完整管理許可 AWS Firewall Manager，包括所有 Firewall Manager 政策類型。
- 將 AWS WAF 日誌寫入 Amazon Simple Storage Service - 允許 Firewall Manager 在 Amazon S3 中寫入和讀取 AWS WAF 日誌。
- 建立服務連結角色 – 允許管理員建立服務連結角色，讓 Firewall Manager 代表您存取其他服務中的資源。此許可僅允許建立僅供 Firewall Manager 使用的服務連結角色。如需 Firewall Manager 如何使用服務連結角色的資訊，請參閱 [使用 Firewall Manager 的服務連結角色](#)。
- AWS Organizations – 允許管理員將 Firewall Manager 用於 中的組織 AWS Organizations。在 中啟用 Firewall Manager 的受信任存取後 AWS Organizations，管理員帳戶的成員可以檢視整個組織的調查結果。如需 AWS Organizations 搭配 使用的詳細資訊 AWS Firewall Manager，請參閱 AWS Organizations 《使用者指南 [AWS](#) 》中的 [AWS Organizations 搭配其他服務使用](#)。

許可類別

以下列出政策中的許可類型及其提供的許可。

- fms – 使用 AWS Firewall Manager 資源。
- waf 和 waf-regional – 使用 AWS WAF Classic 政策。
- elasticloadbalancing – 將 AWS WAF Web ACLs 到 Elastic Load Balancer 建立關聯。
- firehose – 檢視 AWS WAF 日誌的相關資訊。
- organizations – 使用 AWS Organizations 資源。
- shield – 檢視政策的 AWS Shield 訂閱狀態。

- `route53resolver` – 在 Route 53 私有 DNS for VPCs政策中使用 Route 53 Private DNS for VPCs 規則群組。
- `wafv2` – 使用 AWS WAFV2 政策。
- `network-firewall` – 使用 AWS Network Firewall 政策。
- `ec2` – 檢視政策可用區域和區域。
- `s3` – 檢視 AWS WAF 日誌的相關資訊。

AWS 受管政策：**FMSServiceRolePolicy**

此政策允許在 Firewall Manager 和整合服務中代表您 AWS Firewall Manager 管理 AWS 資源。此政策連接至 `AWSServiceRoleForFMS` 服務連結角色。如需服務連結角色的詳細資訊，請參閱[使用 Firewall Manager 的服務連結角色](#)。

如需政策詳細資訊，請參閱 [FMSServiceRolePolicy](#) 的 IAM 主控台。

AWS 受管政策：**AWSFMAdminReadOnlyAccess**

授予所有 AWS Firewall Manager 資源的唯讀存取權。

如需政策清單和詳細資訊，請參閱 [AWSFMAdminReadOnlyAccess](#) 中的 IAM 主控台。本節的其餘部分提供政策設定的概觀。

許可類別

以下列出政策中的許可類型，以及許可允許唯讀存取的資訊。

- `fms` – AWS Firewall Manager 資源。
- `waf` 和 `waf-regional` – AWS WAF Classic 政策。
- `firehose` – AWS WAF logs。
- `organizations` – AWS 組織 資源。
- `shield` – AWS Shield 政策。
- `route53resolver` – Route 53 Private DNS for VPCs 政策中的 Route 53 Private DNS for VPCs 規則群組。
- `wafv2` – 可在 中使用的 AWS WAFV2 規則群組和 AWS 受管規則規則群組 AWS WAFV2。
- `network-firewall` – AWS Network Firewall 規則群組和規則群組中繼資料。
- `ec2` – AWS Network Firewall 政策可用區域 和區域 。
- `s3` – AWS WAF logs。

AWS 受管政策：AWSFMMemberReadOnlyAccess

授予 AWS Firewall Manager 成員資源的唯讀存取權。如需政策清單和詳細資訊，請參閱 [AWSFMMemberReadOnlyAccess](#) 中的 IAM 主控台。

AWS 受管政策的 Firewall Manager 更新

檢視自此服務開始追蹤這些變更以來，防火牆管理員 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請在 [Firewall Manager 文件歷史記錄](#) 頁面上訂閱 RSS 摘要 [文件歷史紀錄](#)。

變更	描述	日期
FMSServiceRolePolicy – 已更新政策	新增 Firewall Manager 服務政策的許可。 新增 Amazon CloudFront 所需的下列許可： • <code>cloudfront:AssociateDistributionWebACL</code> – 准許將 AWS WAF Web ACL 與 CloudFront 分佈建立關聯 • <code>cloudfront:DisassociateDistributionWebACL</code> – 准許取消 AWS WAF Web ACL 與 CloudFront 分佈的關聯	2025-05-21
FMSServiceRolePolicy – 已更新政策	新增 Firewall Manager 服務政策的許可。 新增以批次方式取得資源組態狀態的 <code>BatchGetResourceConfig</code> 許可。請	2025-02-10

變更	描述	日期
	參閱 IAM 主控台中的更新政策： FMSServiceRolePolicy 。	
FMSServiceRolePolicy – 已更新政策	新增 Firewall Manager 服務角色政策的許可。 新增讀取 Network Firewall TLS 組態資訊的功能。請參閱 IAM 主控台中的更新政策：FMSServiceRolePolicy。	2024-07-22
FMSServiceRolePolicy – 已更新政策	新增管理網路 ACLs許可。 請參閱 IAM 主控台中的更新政策：FMSServiceRolePolicy。	2024-04-22
FMSServiceRolePolicy – 已更新政策	新增允許 Firewall Manager 描述指定 AWS Config 規則是否合規的許可。 請參閱 IAM 主控台中的更新政策：FMSServiceRolePolicy。	2023-04-21
FMSServiceRolePolicy – 已更新政策	新增允許 Firewall Manager 描述 Amazon EC2 執行個體和網路介面屬性的許可。 請參閱 IAM 主控台中的更新政策：FMSServiceRolePolicy。	2022-11-15
AWSFMAdminReadOnlyAccess – 更新的政策	新增支援 AWS WAFV2、Shield、Network Firewall、DNS Firewall、Amazon VPC 安全群組、政策的許可。 請參閱 IAM 主控台中的更新政策：AWSFMAdminReadOnlyAccess。	2022-11-02

變更	描述	日期
AWSFMAdminFullAccess – 更新的政策	新增支援 AWS WAFV2、Shield、Network Firewall、DNS Firewall、Amazon VPC 安全群組、政策的許可。已移除 Amazon SNS 許可。 請參閱 IAM 主控台內的更新政策：AWSFMAdminFullAccess。	2022-10-21
FMSServiceRolePolicy – AWS Firewall Manager 第三方防火牆政策的新許可	此變更可讓 Firewall Manager 建立和刪除與第三方防火牆政策相關聯的 Amazon EC2 VPC 端點。	2022-03-30
FMSServiceRolePolicy – AWS Network Firewall 政策的新許可	新增支援部署 Network Firewall 政策防火牆的新許可。新的許可允許擷取政策範圍內帳戶的可用區域相關資訊。	2022-02-16
FMSServiceRolePolicy – AWS Shield 政策的新許可	新增擷取 AWS WAF 區域和 AWS WAF 全域資源標籤的新許可。新增使用資源 ACLs AWS WAF 的區域許可。新增支援 Shield 自動應用程式層 DDoS 緩解的許可。	2022-01-07
FMSServiceRolePolicy – AWS Shield 政策的新許可	新增擷取 Elastic Load Balancing 資源標籤的新許可。	2021-11-18

變更	描述	日期
FMSServiceRolePolicy – 安全群組和 AWS Network Firewall 政策的新許可	新增了新的許可，以啟用 AWS Network Firewall 政策的集中式記錄。此外，新增了唯讀 Amazon EC2 許可，以支援 Config 服務的變更，這些變更會影響如何 AWS Firewall Manager 查詢安全群組政策的資源。	2021-09-29
FMSServiceRolePolicy – AWS WAF 資源的 ARN 格式	更新 FMSServiceRolePolicy 以標準化 AWS WAF 資源的 ARN 格式。更新的 ARN 格式為 <code>arn:aws:waf:*:*:*</code> 和 <code>arn:aws:waf-regional:*:*:*</code> 。	2021-08-12
FMSServiceRolePolicy – 中國的其他區域	AWS Firewall Manager 已 FMSServiceRolePolicy 針對中國的 BJS 和 ZHY 區域啟用。	2021-08-12
FMSServiceRolePolicy – 更新現有政策	新增允許 AWS Firewall Manager 管理 Amazon Route 53 Resolver DNS 防火牆的新許可。 此變更允許 Firewall Manager 設定 Amazon Route 53 Resolver DNS 防火牆關聯。這可讓您使用 Firewall Manager 為整個組織中 VPCs 提供 DNS 防火牆保護 AWS Organizations。	2021-03-17
Firewall Manager 開始追蹤變更	Firewall Manager 開始追蹤其 AWS 受管政策的變更。	2021-03-02

對 AWS Firewall Manager 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 Firewall Manager 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 Firewall 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 Firewall Manager 資源](#)

我無權在 Firewall 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 `fms:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fms: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 `fms: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 Firewall 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 Firewall 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 Firewall 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 Firewall Manager 是否支援這些功能，請參閱 [AWS Shield 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《[IAM 使用者指南](#)》中的 [在您擁有 AWS 帳戶 的另一個資源中提供存取權給 IAM 使用者](#)。
- 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 \(聯合身分\)](#)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《[IAM 使用者指南](#)》中的 [IAM 角色與資源型政策的差異](#)。

使用 Firewall Manager 的服務連結角色

AWS Firewall Manager 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Firewall Manager 的唯一 IAM 角色類型。服務連結角色由 Firewall Manager 預先定義，並包含服務 AWS 代表您呼叫其他服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Firewall Manager，因為您不必手動新增必要的許可。Firewall Manager 會定義其服務連結角色的許可，除非另有定義，否則只有 Firewall 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。該許可政策無法連接至其他任何 IAM 實體。

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

如需關於支援服務連結角色的其他服務的資訊，請參閱 [可搭配 IAM 運作的 AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Firewall Manager 的服務連結角色許可

AWS Firewall Manager 使用服務連結角色名稱 `AWSServiceRoleForFMS`，讓 Firewall Manager 代表您呼叫 AWS 服務，以管理防火牆政策和 AWS Organizations 帳戶資源。此政策會連接至受

AWS 管角色 `AWSServiceRoleForFMS`。如需受管角色的詳細資訊，請參閱 [AWS 受管政策：
`FMSServiceRolePolicy`](#)。

`AWSServiceRoleForFMS` 服務連結角色信任服務擔任角色 `fms.amazonaws.com`。

角色許可政策允許 Firewall Manager 對指定的資源完成下列動作：

- `waf` - 管理您帳戶中 AWS WAF 的 Classic Web ACLs、規則群組許可和 Web ACLs 關聯。
- `ec2` - 在彈性網路介面和 Amazon EC2 執行個體上管理安全群組。管理 Amazon VPC 子網路上的網路 ACLs。
- `vpc` - 在 Amazon VPC 中管理子網路、路由表、標籤和端點。
- `wafv2` - 管理您帳戶中的 AWS WAF Web ACL、規則群組許可和 Web ACLs 關聯。ACLs
- `cloudfront` - 建立 Web ACLs 以保護 CloudFront 分佈。
- `config` - 在帳戶中管理 Firewall Manager 擁有的 AWS Config 規則。
- `iam` - 管理此服務連結角色，並在設定 AWS WAF 和 Shield 政策的記錄時建立必要的 AWS WAF 和 Shield 服務連結角色。
- `organization` - 建立 Firewall Manager 擁有的服務連結角色，以管理 Firewall Manager 使用 AWS Organizations 的資源。
- `shield` - 管理您帳戶中資源的 AWS Shield 保護和 L7 緩解組態。
- `ram` - 管理 DNS 防火牆規則群組和 Network Firewall 規則群組 AWS RAM 的資源共用。
- `network-firewall` - 管理 Firewall Manager 擁有 AWS Network Firewall 的資源和帳戶中相依的 Amazon VPC 資源。
- `route53resolver` - 在您的帳戶中管理 Firewall Manager 擁有的 DNS 防火牆關聯。

請參閱 IAM 主控台完整政策：[FMSServiceRolePolicy](#)。

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](#)。

為 Firewall Manager 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 上啟用 Firewall Manager 記錄 AWS Management Console，或您在 Firewall Manager CLI 或 Firewall Manager API 中提出 `PutLoggingConfiguration` 請求時，防火牆管理員會為您建立服務連結角色。

您必須擁有 `iam:CreateServiceLinkedRole` 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 Firewall Manager 記錄時，防火牆管理員會再次為您建立服務連結角色。

編輯 Firewall Manager 的服務連結角色

Firewall Manager 不允許您編輯 AWSServiceRoleForFMS 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的[編輯服務連結角色](#)。

刪除 Firewall Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

Note

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

使用 IAM 刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 來刪除 AWSServiceRoleForFMS 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

Firewall Manager 服務連結角色的支援區域

Firewall Manager 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 [Firewall Manager 端點和配額](#)。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況，AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源政策中使用 [aws:SourceArn](#) 和 [aws:SourceAccount](#) 全域條件內容索引鍵，以限制將另一個服務 AWS Firewall Manager 提供給資源的許可。如果您想要僅允許一個資源與跨服務存取

相關聯，則請使用 `aws:SourceArn`。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 `aws:SourceAccount`。

防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如：`arn:aws:fms:*:account-id:*`。

如果 `aws:SourceArn` 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

的值`aws:SourceArn`必須是 AWS Firewall Manager 管理員 AWS 的帳戶。

下列範例示範如何使用 Firewall Manager 中的`aws:SourceArn`全域條件內容索引鍵，以防止混淆代理人問題。

下列範例顯示如何使用 Firewall Manager 角色信任政策中的`aws:SourceArn`全域條件內容索引鍵，來防止混淆代理人問題。將`##`和`## ID` 取代為您自己的資訊。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"
        ]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

在 Firewall Manager 中記錄和監控

監控是維護 Firewall Manager 和 AWS 解決方案可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。AWS 提供數種工具來監控 Firewall Manager 資源並回應潛在事件：

Amazon CloudWatch 警示

您可以使用 CloudWatch 警示觀察單一指標一段指定的時間。如果指標超過指定的閾值，CloudWatch 會傳送通知至 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。

AWS CloudTrail 日誌

CloudTrail 提供由 Firewall Manager AWS 中的使用者、角色或服務所採取動作的記錄。使用 CloudTrail 收集的資訊，您可以判斷向 Firewall Manager 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。如需詳細資訊，請參閱[使用 AWS CloudTrail 記錄 API 呼叫](#)。

Firewall Manager 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](#)。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您的合規目標，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的責任模型。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。

Firewall Manager 中的復原能力

AWS 全域基礎設施是以 AWS 區域 和 可用區域為基礎建置。AWS 區域 提供多個實體分隔和隔離的可用區域，這些區域與低延遲、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](#)。

AWS Firewall Manager 中的基礎設施安全

作為受管服務，AWS Firewall Manager 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 發佈的 API 呼叫，透過網路存取 Firewall Manager。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用[AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS Firewall Manager 配額

AWS Firewall Manager 受下列配額限制（先前稱為限制）。

AWS Firewall Manager 具有預設配額，您可以提高和固定配額。

由 Firewall Manager 管理的安全群組政策和網路 ACL 政策受標準 Amazon VPC 配額約束。如需詳細資訊，請參閱《[Amazon VPC 使用者指南](#)》中的 [Amazon VPC Quotas](#)。 <https://docs.aws.amazon.com/vpc/latest/userguide/>

每個 Firewall Manager 網路防火牆政策都會建立具有相關聯防火牆政策及其規則群組的網路防火牆。這些 Network Firewall 資源受 Network Firewall 開發人員指南中配額列出的[AWS Network Firewall 配額](#)限制。

軟配額

AWS Firewall Manager 在每個區域的實體數量上具有預設配額。您可以[請求提高](#)這些配額。

所有政策類型

資源	每個區域的預設配額
中的每個組織的帳戶 AWS Organizations	各有不同。傳送給帳戶的邀請計入此配額。若受邀帳戶拒絕、

資源	每個區域的預設配額
	管理帳戶取消邀請或邀請到期，便會退回計數。
中的每個組織的 Firewall Manager 政策 AWS Organizations。	50。區域規格 Global 和 US East (N. Virginia) Region 參考相同的區域，因此此限制適用於其中兩個政策的總合併政策。
每個 Firewall Manager 政策範圍內的組織單位。	20
如果您明確包含和排除個別帳戶，則防火牆管理員政策範圍內的帳戶。	200
如果您未明確包含或排除個別帳戶，則防火牆管理員政策範圍內的帳戶。	2,500
中的組織 AWS Organizations 可以包含的帳戶，以便由 Firewall Manager 加入組織。計數包含 Firewall Manager 管理員帳戶。	10,000
每個 Firewall Manager 政策包含或排除資源的標籤。	8
每個帳戶的資源集數目。	20
每個資源集的資源數量。	100
每個 Firewall Manager 政策的資源集數目。	5

AWS WAF 政策

資源	每個區域的預設配額
AWS WAF 每個 Firewall Manager 管理員帳戶的規則群組。	100
AWS WAF 每個 Firewall Manager 管理員帳戶的傳統規則群組。	10

資源	每個區域的預設配額
每個 AWS WAF 政策的規則群組。	50
每個 AWS WAF 政策的合作夥伴規則群組。	1

常見安全群組政策

資源	每個區域的預設配額
每個政策的主要安全群組。	3
每個帳戶每個政策範圍內的 Amazon VPC 執行個體，包括共用 VPCs。	100

內容稽核安全群組政策

資源	每個區域的預設配額
每個政策稽核安全群組。	1
每個應用程式清單的應用程式。	50
允許所有流量的規則的自訂受管應用程式清單。	1
每個政策規則的自訂受管應用程式清單。	1
每個帳戶的自訂受管應用程式清單。	10
每個通訊協定清單的通訊協定。	5
政策中任何設定的自訂受管通訊協定清單。	1
每個帳戶的自訂受管通訊協定清單。	10

網路 ACL 政策

資源	每個區域的預設配額
每個網路 ACL 政策的傳入規則數量，用於第一個或最後一個規則。例如，您可以有 5 個第一個和 0 個最後一個傳入規則，或 2 個第一個和 3 個最後一個規則，但您不能有 4 個第一個和 2 個最後一個規則。	5
每個網路 ACL 政策的傳出規則數量，用於第一個或最後一個規則。例如，您可以有 5 個第一個和 0 個最後一個傳出規則，或 2 個第一個和 3 個最後一個，但您不能有 4 個第一個和 2 個最後一個。	5

網路防火牆政策

資源	每個區域的預設配額
您可以為單一政策提供的 IPV4 CIDRs 數量。	50
每個網路防火牆政策的狀態規則群組容量。	30,000

DNS 防火牆政策

資源	每個區域的預設配額
每個 DNS 防火牆政策的 DNS 防火牆規則群組。	2

硬配額

下列與 相關的每個區域配額 AWS Firewall Manager 無法變更。

所有政策類型

資源	每個區域的配額
您可以在 AWS Organizations 組織中擁有的 Firewall Manager 管理員數量上限。您必須擁有一個預設管理員，以及最多九個額外的 Firewall Manager 管理員。	10

AWS WAF 政策

資源	每個區域的配額
AWS WAF 政策中規則群組的 Web ACL 容量單位 (WCU) 總計。	5,000

AWS WAF 傳統政策

資源	每個區域的配額
AWS WAF 每個政策的傳統規則群組。	2 : 1 個客戶建立的規則群組和 1 個 AWS Marketplace 規則群組。
AWS WAF 每個 Firewall Manager AWS WAF Classic 規則群組的傳統規則。	10

網路防火牆政策

資源	每個區域的配額
可針對單一政策自動修復 VPCs 數量。	1,000
每個 Network Firewall 政策的無狀態規則群組。	20
每個網路防火牆政策的狀態規則群組。	20
每個網路防火牆政策的無狀態規則群組容量。	30,000

監控 AWS WAFAWS Firewall Manager，以及 AWS Shield Advanced

監控是維護服務可靠性、可用性和效能的重要部分。

Note

如需使用 Shield Advanced 監控 Shield Advanced 資源和識別可能 DDoS 事件的相關資訊，請參閱 [AWS Shield](#)。

在您開始監控這些服務時，應該先建立包含下列問題之回答的監控計劃：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

下一步是在各個時間點和不同的負載條件下測量效能，以在您的環境中確立 正常效能的基準。當您監控時 AWS WAF，防火牆管理員、Shield Advanced 和相關服務會儲存歷史監控資料，以便將其與目前的效能資料進行比較、識別正常效能模式和效能異常，並設計方法來解決問題。

對於 AWS WAF，您應該至少監控下列項目，以建立基準：

- 允許的 Web 要求數目
- 封鎖的 Web 要求數目

主題

- [監控工具](#)
- [使用 Amazon CloudWatch 監控](#)
- [使用 AWS CloudTrail記錄 API 呼叫](#)

監控工具

AWS 提供各種可用來監控 AWS WAF 和 的工具 AWS Shield Advanced。您可以設定其中一些工具為您監控，但其他工具則需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用下列自動化監控工具來監看 AWS WAF 和 AWS Shield Advanced，並在發生錯誤時回報：

- 保護套件或 Web ACL 流量概觀儀表板 – 透過前往 AWS WAF 主控台其中的 Web ACL 頁面並開啟流量概觀索引標籤，存取保護套件或 Web ACL 評估的 Web 流量摘要。

流量概觀儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集。您可以查看所有 Web 流量的摘要，以及智慧型威脅緩解規則群組評估的流量摘要。

如需詳細資訊，請參閱 [保護套件或 Web ACLs 流量概觀儀表板](#) 或前往 主控台 中的儀表板。

- Amazon CloudWatch 警示 – 在您指定的期間內監看單一指標，並根據相對於指定閾值的指標值，在多個期間內執行一或多個動作。此動作是傳送到 Amazon Simple Notification Service (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。警示僅會針對持續狀態變更呼叫動作。CloudWatch 警示不會只因處於特定狀態就叫用動作，狀態必須已變更並已維持一段指定的時間。如需詳細資訊，請參閱 [使用 CloudWatch 監控 CloudFront 活動 CloudWatch](#)。

Note

未啟用 CloudWatch 指標和警示 AWS Firewall Manager。

您不僅可以使用 CloudWatch 監控 AWS WAF 和 Shield Advanced 指標，如中所述 [使用 Amazon CloudWatch 監控](#)，還應該使用 CloudWatch 監控受保護資源的活動。如需詳細資訊，請參閱下列內容：

- 《Amazon [CloudFront 開發人員指南](#)》中的 [使用 CloudWatch 監控 CloudFront 活動](#) Amazon CloudFront
- 《[API Gateway 開發人員指南](#)》中的 [Amazon API Gateway 中的記錄和監控](#)
- 《Elastic Load Balancing 使用者指南》中的 [Application Load Balancer 的 CloudWatch 指標](#)
- 《AWS AppSync 開發人員指南》中的 [監控和記錄](#)

- 《[Amazon Cognito 開發人員指南](#)》中的在 [Amazon Cognito 中記錄和監控 Amazon Cognito](#)
- 《[AWS App Runner 開發人員指南](#)》中的[檢視串流至 CloudWatch Logs 的 App Runner 日誌，以及檢視回報至 CloudWatch 的 App Runner 服務指標](#)
- Amazon CloudWatch Logs – 監控、存放和存取來自 AWS CloudTrail 或其他來源的日誌檔案。如需詳細資訊，請參閱[什麼是 Amazon CloudWatch Logs？](#)。
- Amazon CloudWatch Events – 自動化您的 AWS 服務並自動回應系統事件。來自 AWS 服務的事件會以近乎即時的方式交付至 CloudWatch Events，而且您可以在事件符合您寫入的規則時指定要採取的自動化動作。如需詳細資訊，請參閱[什麼是 Amazon CloudWatch Events？](#)
- AWS CloudTrail 日誌監控 – 在帳戶之間共用日誌檔案、透過將日誌檔案傳送到 CloudWatch Logs 來即時監控 CloudTrail 日誌檔案、在 Java 中寫入日誌處理應用程式，以及驗證您的日誌檔案在 CloudTrail 交付後並未變更。如需詳細資訊，請參閱[使用 AWS CloudTrail 記錄 API 呼叫](#) 和《AWS CloudTrail 使用者指南》中的[使用 CloudTrail 記錄檔案](#)。
- AWS Config – 檢視您 AWS 帳戶中 AWS 資源的組態，包括資源彼此的關係，以及它們過去的設定方式，以便您可以查看組態和關係如何隨時間變化。

手動監控工具

監控 AWS WAF 和 AWS Shield Advanced 涉及手動監控 CloudWatch 警示未涵蓋的項目的另一個重要部分。您可以檢視 AWS WAF、Shield Advanced、CloudWatch 和其他 AWS Management Console 儀表板，以查看環境 AWS 的狀態。我們建議您也檢查 Web ACLs 和規則的日誌檔案。

- 例如，若要檢視 AWS WAF 儀表板：
 - 在 AWS WAF Web ACLs 頁面的請求索引標籤上，檢視符合您已建立之每個規則的請求總數和請求圖表。如需詳細資訊，請參閱[檢視 Web 請求的範例](#)。
- 檢視 CloudWatch 首頁以取得下列項目：
 - 目前警示與狀態
 - 警示與資源的圖表
 - 服務運作狀態

此外，您可以使用 CloudWatch 執行下列動作：

- 建立[自訂儀表板](#)以監控您注重的服務。
- 用於疑難排解問題以及探索趨勢的圖形指標資料。
- 搜尋和瀏覽您的所有 AWS 資源指標。
- 建立與編輯要通知發生問題的警示。

使用 Amazon CloudWatch 監控

您可以使用 Amazon CloudWatch 來監控 Web 請求和 Web ACLs 和規則，其會收集原始資料並將其處理 AWS WAF、AWS Shield Advanced 為可讀且近乎即時的指標。您可以使用 Amazon CloudWatch 中的統計資料，來深入了解 Web 應用程式或服務的效能。如需詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》中的[什麼是 CloudWatch](#)。Amazon CloudWatch

Note

Firewall Manager 未啟用 CloudWatch 指標和警示。

您可以建立 Amazon CloudWatch 警示，在警示變更狀態時傳送 Amazon SNS 訊息。警示會監看您指定時段的單個指標，然後根據幾個時間段內與指定閾值相關的指標值來執行一或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。警示僅會針對持續狀態變更呼叫動作。CloudWatch 警示不會只因處於特定狀態就調用動作，狀態必須已變更並已維持一段指定的時間。

主題

- [檢視指標和維度](#)
- [AWS WAF 指標和維度](#)
- [AWS Shield Advanced 指標](#)
- [AWS Firewall Manager 通知](#)

檢視指標和維度

指標會先依服務命名空間分組，然後依每個命名空間內的各種維度組合分組。AWS Firewall Manager 不會記錄指標。

- AWS WAF 命名空間是 AWS/WAFV2
- Shield Advanced 命名空間是 AWS/DDoSProtection

Note

AWS WAF 每分鐘報告一次指標。

Shield Advanced 會在事件期間每分鐘報告一次指標，其他時間則較少。

使用下列程序來檢視 AWS WAF 和 的指標 AWS Shield Advanced。

使用 CloudWatch 主控台檢視指標

1. 登入 AWS Management Console ，並在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 如有必要，請將區域變更為 AWS 資源所在的區域。針對 CloudFront，選擇美國東部（維吉尼亞北部）區域。
3. 在導覽窗格中的指標下，選擇所有指標，然後在服務的瀏覽索引標籤下搜尋。

使用 AWS CLI 檢視指標

- 對於 AWS/WAFV2，在命令提示字元中使用以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

對於 Shield Advanced，在命令提示字元中使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF 指標和維度

AWS WAF 每分鐘報告一次指標。AWS WAF 在 AWS/WAFV2 命名空間中提供指標和維度。

您可以在保護套件或 Web ACL 的流量概觀索引標籤中，透過 AWS WAF 主控台查看 AWS WAF 指標的摘要資訊。如需詳細資訊，請前往 主控台或參閱 [保護套件或 Web ACLs 流量概觀儀表板](#)。

您可以查看保護套件或 Web ACLs、規則、規則群組和標籤的下列指標。

- 您的規則 – 指標會依規則動作分組。例如，當您在 Count 模式下測試規則時，其相符項目會列為保護套件或 Web ACL 的 Count 指標。
- 您的規則群組 – 規則群組的指標會列在規則群組指標下。
- 另一個帳戶擁有的規則群組 – 規則群組指標通常只有規則群組擁有者可以看到。不過，如果您覆寫規則的規則動作，則該規則的指標會列在您的保護套件或 Web ACL 指標下。此外，任何規則群組新增的標籤都會列在您的保護套件或 Web ACL 指標中

此類別中的規則群組是 [AWS 的受管規則 AWS WAF](#)、[辨識其他服務提供的規則群組](#)、[AWS Marketplace 規則群組](#) 和規則群組，這些群組由另一個帳戶與您共用。

- 標籤 - 在評估期間新增至 Web 請求的標籤會列在保護套件或 Web ACL 標籤指標中。您可以存取所有標籤的指標，無論它們是由您的規則和規則群組新增，還是由另一個帳戶擁有的規則群組中的規則新增。

主題

- [AWS WAF 核心指標和維度](#)
- [標籤指標和維度](#)
- [免費機器人可見性指標和維度](#)
- [帳戶指標和維度](#)
- [AWS WAF 用量指標](#)

AWS WAF 核心指標和維度

AWS WAF 核心指標

指標	描述
AllowedRequests	允許的 Web 要求數目。 報告條件：有非零值。 有效的統計資訊：總和
BlockedRequests	封鎖的 Web 要求數目。 報告條件：有非零值。 有效的統計資訊：總和
CountedRequests	計入的 Web 要求數目。 報告條件：有非零值。 計算的 Web 請求是指至少符合其中一個規則的請求。 請求計數一般用於測試。

指標	描述
	有效的統計資訊：總和
CaptchaRequests	已套用 CAPTCHA 控制項的 Web 請求數目。 報告條件：有非零值。 CAPTCHA Web 請求符合具有 CAPTCHA 動作設定的規則。此指標會記錄所有相符的請求，無論 CAPTCHA 字符是否過期、無效、不存在或網域不相符。 有效的統計資訊：總和
RequestsWithValidCaptchaToken	已套用 CAPTCHA 控制項且具有有效 CAPTCHA 字符的 Web 請求數目。 報告條件：有非零值。 有效的統計資訊：總和
CaptchasAttempted	最終使用者為了回應 CAPTCHA 拼圖挑戰而提交的解決方案數量。 報告條件：有非零值。 有效的統計資訊：總和
CaptchasSolved	成功解決拼圖的已提交 CAPTCHA 拼圖解決方案數量。 報告條件：有非零值。 有效的統計資訊：總和

指標	描述
ChallengeRequests	套用挑戰控制項的 Web 請求數目。 報告條件：有非零值。 挑戰 Web 請求是符合具有Challenge動作設定的規則的請求。此指標會記錄所有相符的請求，無論挑戰字符是否過期、無效、不存在或網域不相符。 有效的統計資訊：總和
ChallengesAttempted	最終使用者為了回應Challenge規則提供的無提示挑戰而提交的嘗試次數。 報告條件：有非零值。 有效的統計資訊：總和
ChallengesSolved	成功通過Challenge規則所服務的無提示挑戰的無提示挑戰解決方案數量。 報告條件：有非零值。 有效的統計資訊：總和
PassedRequests	傳遞的請求數量。這僅用於經過規則群組評估，但未符合任何規則群組規則的請求。 報告條件：有非零值。 傳遞的請求是符合規則群組中任何規則的請求。 有效的統計資訊：總和
RequestsWithValidChallengeToken	套用了挑戰控制且具有有效挑戰字符的 Web 請求數量。 報告條件：有非零值。 有效的統計資訊：總和

指標	描述
LowReputationPacketsDropped	從已知惡意來源捨棄的封包數量。 報告條件：有非零值。 有效的統計資訊：總和 此指標會發佈至 AWS/ApplicationELB 命名空間。
LowReputationRequestsDenied	HTTP 403 回應拒絕的 HTTP 請求數目。 報告條件：有非零值。 有效的統計資訊：總和 此指標會發佈至 AWS/ApplicationELB 命名空間。

AWS WAF 核心維度

維度	描述
Region	除了 Amazon CloudFront 分佈之外，所有受保護的資源類型都需要。
Rule	下列其中一項： • Rule 的指標名稱。 • ALL，代表 WebACL 或 RuleGroup 內的所有規則。 • Default_Action（只有在與 WebACL 維度結合時），代表指派給任何請求的動作，其評估並未由保護套件或 Web ACL 中的規則動作終止。
RuleGroup	RuleGroup 的指標名稱。
WebACL	WebACL 的指標名稱。

維度	描述
WebACLArn	Web ACL 的 Amazon Resource Name (ARN)。此維度僅在啟用 AWS WAF 時可用。
ResourceType	受保護資源的類型，例如 CF、APIGW 或 ALB。
Resource	受保護資源的 Amazon Resource Name (ARN)。
Country	請求的來源國家/地區。這是國際標準化組織 (ISO) 3166 標準中的兩個字元指定。例如，美國為 US，烏克蘭為 UA。 如果請求有 X-Forwarded-For 標頭，AWS WAF 會使用 來判斷此設定。否則，AWS WAF 會使用用戶端 IP 的國家/地區。此判斷獨立於您在規則中用來判斷原始國家/地區的任何邏輯。會使用 MaxMind GeoIP 資料庫 AWS WAF 來判斷 IPs 的位置。
Attack	根據您在 Web ACL 中使用的規則和規則群組，在請求中 AWS WAF 識別的攻擊類型。 基準 AWS 受管規則群組中的規則和規則可以識別攻擊類型。例如，跨網站指令碼 (XSS) 規則符合識別 XSS 攻擊類型，以速率為基礎的規則則識別容積攻擊類型。攻擊類型通常表示終止 Web 請求評估的規則類型。
Device	傳送請求之用戶端的裝置類型，從 Web 請求的 user-agent 標頭取得。
LoadBalancerArn	負載平衡器的 Amazon Resource Name (ARN)。
LoadBalancerArnAvailabilityZone	負載平衡器 ARN 和可用區域的組合。
ManagedRuleGroup	ManagedRuleGroup 的指標名稱。
ManagedRuleGroupRule	內相符 ManagedRuleGroup 的規則。

標籤指標和維度

在規則和您在保護套件或 Web ACL 中使用的受管規則群組評估期間新增至請求的標籤指標。如需相關資訊，請參閱[Web 請求標籤](#)。

對於任何單一 Web 請求，最多可 AWS WAF 存放 100 個標籤的指標。您的保護套件或 Web ACL 評估可以套用超過 100 個標籤，並與超過 100 個標籤相符，但指標中只會反映前 100 個標籤。

標籤指標

指標	描述
AllowedRequests	Web 請求上Allow套用動作設定的標籤數量。標籤可在 Web 請求評估期間的任何時間點新增。 報告條件：有非零值。 有效的統計資訊：總和
BlockedRequests	已Block套用動作設定的 Web 請求標籤數量。標籤可在 Web 請求評估期間的任何時間點新增。 報告條件：有非零值。 有效的統計資訊：總和
CountedRequests	依具有Count動作設定的規則群組規則新增至 Web 請求的標籤數量。 此指標僅適用於規則群組內規則的擁有者。對於其他情況，計數標籤指標會彙總到套用至請求的終止動作中，例如 Allow或 Block。 報告條件：有非零值。 有效的統計資訊：總和
CaptchaRequests	Web 請求上已套用終止CAPTCHA動作的標籤數目。標籤可在 Web 請求評估期間的任何時間點新增。 報告條件：有非零值。

指標	描述
	有效的統計資訊：總和
ChallengeRequests	Web 請求上已套用終止Challenge動作的標籤數量。標籤可在 Web 請求評估期間的任何時間點新增。 報告條件：有非零值。 有效的統計資訊：總和
AllowRuleMatch	使用 Allow動作產生相關聯標籤和終止請求評估的相符規則數目。 報告條件：有非零值。 有效的統計資訊：總和
BlockRuleMatch	使用 Block動作產生相關聯標籤和終止請求評估的相符規則數目。 報告條件：有非零值。 有效的統計資訊：總和
CountRuleMatch	產生關聯標籤並套用Count動作的相符規則數目。 如果多個規則設定為相同的標籤和動作，則一個請求可能會導致此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和
CaptchaRuleMatch	使用 CAPTCHA動作產生相關聯標籤和終止請求評估的相符規則數目。 報告條件：有非零值。 有效的統計資訊：總和

指標	描述
ChallengeRuleMatch	使用 Challenge 動作產生相關聯標籤和終止請求評估的相符規則數目。 報告條件：有非零值。 有效的統計資訊：總和
CaptchaRuleMatchWithValidToken	產生關聯標籤並套用非終止CAPTCHA動作的相符規則數目。 如果多個規則設定為相同的標籤和動作，則一個請求可能會導致此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和
ChallengeRuleMatchWithValidToken	產生關聯標籤並套用非終止Challenge動作的相符規則數目。 如果多個規則設定為相同的標籤和動作，則一個請求可能會導致此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和

標籤維度

維度	描述
Region	除了 Amazon CloudFront 分佈之外，所有受保護的資源類型都需要。
RuleGroup	RuleGroup 的指標名稱。用於指標 CountedRequests。
WebACL	WebACL 的指標名稱。

維度	描述
ResourceType	受保護資源的類型，例如 CF、APIGW 或 ALB。
Resource	受保護資源的 Amazon Resource Name (ARN)。
LabelNamespace	新增至請求之標籤的命名空間字首。
Label	新增至請求的標籤名稱。
Context	做為標籤新增內容的受管規則群組。例如，等字符管理標籤的內容 <code>awswaf:managed:token:accepted</code> 是對請求使用字符管理的 AWS WAF 受管規則群組，例如 Bot Control 或 ATP 受管規則群組。此維度不適用於所有標籤。

免費機器人可見性指標和維度

當您未在保護套件或 Web ACL 中使用 Bot Control 時，會將 Bot Control 受管規則群組 AWS WAF 套用至 Web 請求的取樣，無需額外費用。這可以提供傳入受保護資源的機器人流量的概念。如需 Bot Control 的詳細資訊，請參閱 [AWS WAF 機器人控制規則群組](#)。

免費機器人可見性指標

指標	描述
SampleAllowedRequest	具有 Allow 動作的抽樣請求數量。 報告條件：有非零值。 有效的統計資訊：總和
SampleBlockedRequest	具有 Block 動作的抽樣請求數量。 報告條件：有非零值。 有效的統計資訊：總和
SampleCaptchaRequest	具有 CAPTCHA 動作的抽樣請求數量。 報告條件：有非零值。

指標	描述
	有效的統計資訊：總和
SampleChallengeRequest	具有 Challenge動作的抽樣請求數量。 報告條件：有非零值。 有效的統計資訊：總和
SampleCountRequest	具有 Count動作的抽樣請求數量。 報告條件：有非零值。 有效的統計資訊：總和

免費機器人可見度維度

維度	描述
Region	除了 Amazon CloudFront 分佈之外，所有受保護的資源類型都需要。
WebACL	WebACL 的指標名稱。
BotCategory	根據 Web 請求標籤，偵測到的機器人類別名稱。
VerificationStatus	根據 Web 請求標籤，偵測到的機器人驗證狀態的名稱。
Signal	根據 Web 請求標籤，偵測到的機器人訊號名稱。

帳戶指標和維度

帳戶指標提供透過 JavaScript API 服務之 CAPTCHA 拼圖和無提示Challenge規則動作的全帳戶資訊。

帳戶指標

指標	描述
CaptchasAttemptedSdk	最終使用者為回應 CAPTCHA 拼圖挑戰而提交的解決方案數量，適用於透過 CAPTCHA JavaScript API 提供的拼圖。 報告條件：有非零值。 有效的統計資訊：總和
CaptchasSolvedSdk	對於透過 CAPTCHA JavaScript API 提供的拼圖，成功解決拼圖的 CAPTCHA 拼圖解決方案數量。 報告條件：有非零值。 有效的統計資訊：總和
ChallengesAttemptedSdk	最終使用者為了回應 Challenge JavaScript API 提供的無提示挑戰而提交的嘗試次數。 報告條件：有非零值。 有效的統計資訊：總和
ChallengesSolvedSdk	提交的無提示挑戰解決方案數量，成功通過 Challenge JavaScript API 提供的無提示挑戰。 報告條件：有非零值。 有效的統計資訊：總和

帳戶維度

維度	描述
Region	除了 Amazon CloudFront 分佈之外，所有受保護的資源類型都需要。

AWS WAF 用量指標

您可以使用 CloudWatch 用量指標來提供您帳戶的資源用量可見度。使用這些指標，以 CloudWatch 圖表和儀表板視覺化目前的服務使用狀況。

AWS WAF 用量指標對應至 AWS 服務配額。您可以設定警示，在您的用量接近服務配額時發出警示。如需 CloudWatch 與 Service Quotas 整合的詳細資訊，請參閱「Amazon CloudWatch 使用者指南」中的 [AWS 用量指標](#)。

AWS WAF 在 AWS/Usage 命名空間中發佈下列指標。

用量指標

指標	描述
ResourceCount	您帳戶中指定的資源數量。資源由與指標相關聯的維度定義。 此指標最有用的統計資料是 MAXIMUM，它表示 1 分鐘內使用的最大資源數量。

以下維度用於精簡 發佈的用量指標 AWS WAF。

用量維度

維度	描述
Resource	報告用量的資源類型。

以下是 Resource 維度的支援值。

Resource 值

Value	描述
WebAclsPerAccountCloudFront	每個帳戶客戶在 CloudFront 中擁有的保護套件或 Web ACLs 數量。只有在 CloudFront 中至少有一個保護套件或 Web ACL 時，才能使用此指標。

Value	描述
WebAclsPerAccountRegional	每個帳戶在區域中客戶擁有的保護套件或 Web ACLs 數量。只有在該區域中至少有一個保護套件或 Web ACL 時，才能使用此指標。
RuleGroupsPerAccountCloudFront	客戶在每個帳戶 CloudFront 中擁有的規則群組數量。只有在 CloudFront 中至少有一個規則群組時，才能使用此指標。
RuleGroupsPerAccountRegional	每個帳戶客戶在一個區域中擁有的規則群組數量。只有在該區域中至少有一個規則群組時，才能使用此指標。
IpSetsPerAccountCloudFront	每個帳戶客戶在 CloudFront 中擁有的 IP 集數量。只有在 CloudFront 中至少設定一個 IP 時，才能使用此指標。
IpSetsPerAccountRegional	每個帳戶在區域中客戶擁有的 IP 集數量。只有在該區域中至少設定一個 IP 時，才能使用此指標。
RegexPatternSetsPerAccountCloudFront	每個帳戶客戶在 CloudFront 中設定的 regex 模式數目。只有在 CloudFront 中至少設定一個規則運算式模式時，才能使用此指標。
RegexPatternSetsPerAccountRegional	每個帳戶在區域中設定客戶的 regex 模式數目。只有在該區域中至少設定一個 regex 模式時，才能使用此指標。

AWS Shield Advanced 指標

Shield Advanced 會針對其保護的所有資源發佈 Amazon CloudWatch 偵測、緩解和最大貢獻者指標。這些指標可讓您為資源建立和設定 CloudWatch 儀表板和警示，藉此改善您監控資源的能力。

Shield Advanced 主控台提供其記錄的許多指標摘要。如需相關資訊，請參閱[使用 Shield Advanced 的 DDoS 事件可見性](#)。

如果您為應用程式層保護啟用自動應用程式層 DDoS 緩解，Shield Advanced 會將規則群組新增至您的保護套件或 Web ACL，以用於管理自動化保護。此規則群組會產生 AWS WAF 指標，但無法檢視。這

與您在保護套件或 Web ACL 中使用的任何其他規則群組相同，但不擁有，例如 AWS 受管規則規則群組。如需 AWS WAF 指標的詳細資訊，請參閱 [AWS WAF 指標和維度](#)。如需此 Shield Advanced 保護選項的詳細資訊，請參閱 [使用 Shield Advanced 自動化應用程式層 DDoS 緩解](#)。

指標報告位置

Shield Advanced 會報告美國東部（維吉尼亞北部）區域中的指標，us-east-1 包括下列項目：

- 全球服務 Amazon CloudFront 和 Amazon Route 53。
- 保護群組。如需保護群組的相關資訊，請參閱 [分組您的 AWS Shield Advanced 保護](#)。

對於其他資源類型，Shield Advanced 會報告資源區域中的指標。

指標報告的時機

Shield Advanced 會在 DDoS 事件期間比沒有事件正在進行時更頻繁地向 AWS 資源上的 Amazon CloudWatch 報告指標。Shield Advanced 會在事件期間每分鐘報告一次指標，然後在事件結束後立即報告一次指標。

雖然沒有進行中的事件，但 Shield Advanced 每天會在指派給資源的時間報告指標一次。此定期報告會保持指標作用中，並可用於自訂 CloudWatch 警示和儀表板。

警示建議

我們建議您建立警示，以通知您需要注意的情況。作為起點，您可以為每個受保護的資源建立警示，當 DDoS Detected 偵測指標為非零時報告。此指標中的非零值不一定表示 DDoS 攻擊正在進行中，但我們建議在指標處於此狀態時更仔細地查看資源狀態。

對於請求洪水，我們建議您為複合檢查建立警示，這些警示也會考慮應用程式運作狀態和 Web 請求磁碟區等因素。您可以選擇對報告各種攻擊向量維度流量的其他三個指標發出警示。透過考慮應用程式的容量，並在流量接近應用程式限制時發出警示，您可以建立一組規則，視需要通知您，而不會產生太多不必要的雜訊。

主題

- [偵測指標](#)
- [緩解指標](#)
- [最佳參與者指標](#)

偵測指標

Shield Advanced 提供AWS/DDoSProtection命名空間中的指標和維度。

偵測指標

指標	描述
DDoSDetected	指出特定 Amazon Resource Name (ARN) 是否正遭遇 DDoS 事件。 此指標在事件期間具有非零值。
DDoSAttackBitsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的位元組數。此指標僅適用於網路和傳輸層（第 3 層和第 4 層）DDoS 事件。 此指標在事件期間具有非零值。 單位：位元
DDoSAttackPacketsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的封包數量。此指標僅適用於網路和傳輸層（第 3 層和第 4 層）DDoS 事件。 此指標在事件期間具有非零值。 單位：封包數
DDoSAttackRequestsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的請求數量。本指標僅適用於 layer 3/4 的 DDoS 事件。本指標只會回報為最重大的 Layer 7 事件。 此指標在事件期間具有非零值。 單位：請求

Shield Advanced DDoSDetected 會在沒有其他維度的情況下發佈指標。剩餘的偵測指標包括對應於攻擊類型的AttackVector維度，從下列清單列出：

- ACKFlood
- CharginReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNflood
- UDPFragment
- UDPTraffic
- UDPReflection

緩解指標

Shield Advanced 在AWS/DDoSProtection命名空間中提供指標和維度。

緩解指標

指標	描述
VolumePacketsPerSecond	為回應偵測到的事件而部署的緩解措施所捨棄或傳遞的每秒封包數。 單位：封包數

緩解維度

維度	描述
ResourceArn	Amazon Resource Name (ARN)
MitigationAction	套用的緩解結果。可能的值為 Pass 或 Drop。

最佳參與者指標

Shield Advanced 在 `AWS/DDoSProtection` 命名空間中提供指標。

最佳參與者指標

指標	描述
VolumePacketsPerSecond	最大貢獻者的每秒封包數。 單位：封包數
VolumeBitsPerSecond	最大貢獻者的每秒位元數。 單位：位元

Shield Advanced 會依維度組合發佈主要參與者指標，以描述事件參與者的特性。您可以將下列任何維度組合用於任何主要參與者指標：

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

最佳參與者維度

維度	描述
ResourceArn	Amazon Resource Name (ARN)。
Protocol	IP 通訊協定名稱，TCP或 UDP。
SourcePort	來源 TCP 或 UDP 連接埠。
DestinationPort	目的地 TCP 或 UDP 連接埠。
SourceIp	來源 IP 地址。
SourceAsn	來源自主系統編號 (ASN)。
TcpFlags	TCP 封包中存在的旗標組合，以破折號 () 分隔-。監控的旗標為 ACK、FIN、RST、SYN。此維度值一律會依字母順序顯示。例如：ACK-FIN-RST-SYN、ACK-SYN 和 FIN-RST。

AWS Firewall Manager 通知

AWS Firewall Manager 不會記錄指標，因此您無法為 Firewall Manager 特別建立 Amazon CloudWatch 警示。不過，您可以設定 Amazon SNS 通知來提醒您可能的攻擊。若要在 Firewall Manager 中建立 Amazon SNS 通知，請參閱 [步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示](#)。

使用 AWS CloudTrail記錄 API 呼叫

AWS WAF AWS Shield Advanced、和 AWS Firewall Manager 已與服務整合 AWS CloudTrail，該服務提供使用者、角色或服務所採取動作的記錄 AWS。CloudTrail 會將這些服務的 API 呼叫子集擷取為事件，包括來自 AWS WAF、Shield Advanced 或 Firewall Manager 主控台的呼叫，以及對 AWS WAF、Shield Advanced 或 Firewall Manager APIs 程式碼呼叫。如果您建立追蹤，則可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AWS WAF、Shield Advanced 或 Firewall Manager 的事件。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 收集的資訊，您可以判斷對這些服務提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱 [《AWS CloudTrail 使用者指南》](#)。

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當 Shield Advanced AWS WAF 或 Firewall Manager 中發生支援的事件活動時，該活動會與事件歷史記錄中的其他服務 AWS 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》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html>。

若要持續記錄 中的事件 AWS 帳戶，包括 AWS WAF Shield Advanced 或 Firewall 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。在主控制台建立追蹤記錄時，該追蹤記錄預設會套用到所有區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。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](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)，以及 [從多個帳戶接收 CloudTrail 日誌檔案](#)

AWS WAF 中的資訊 AWS CloudTrail

所有 AWS WAF 動作都會由 記錄，AWS CloudTrail 並記錄在 [AWS WAF API 參考](#) 中。例如，呼叫 ListWebACL、UpdateWebACL 和 在 CloudTrail 日誌檔案中 DeleteWebACL 產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者登入資料提出請求
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 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](#)。

範例：AWS WAF 日誌檔案項目

線索是一種組態，可讓您將事件做為日誌檔案交付至您指定的 Amazon S3 儲存貯體。AWS CloudTrail 日誌檔案包含一或多個日誌項目。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 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下是 AWS WAF 保護套件或 Web ACL 操作的 CloudTrail 日誌項目範例。

範例：的 CloudTrail 日誌項目 CreateWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2019-11-06T03:43:07Z"
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    }
  },
  "description": "foo",
  "rules": [
    {
      "name": "foo",
```

```

    "priority": 1,
    "statement": {
      "geoMatchStatement": {
        "countryCodes": [
          "AF",
          "AF"
        ]
      }
    },
    "action": {
      "block": {}
    },
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "visibilityConfig": {
    "sampledRequestsEnabled": true,
    "cloudWatchMetricsEnabled": true,
    "metricName": "foo"
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}

```

範例：的 CloudTrail 日誌項目 GetWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


範例：的 CloudTrail 日誌項目 UpdateWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    }
  },
  "description": "foo",
  "rules": [
    {
      "name": "foo",
      "priority": 1,
```

```

    "statement": {
      "geoMatchStatement": {
        "countryCodes": [
          "AF"
        ]
      }
    },
    "action": {
      "block": {}
    },
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "visibilityConfig": {
    "sampledRequestsEnabled": true,
    "cloudWatchMetricsEnabled": true,
    "metricName": "foo"
  },
  "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
},
"responseElements": {
  "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
},
"requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
"eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
"eventType": "AwsApiCall",
"apiVersion": "2019-04-23",
"recipientAccountId": "112233445566"
}

```

範例：的 CloudTrail 日誌項目 DeleteWebACL

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",

```

```
{
  "accessKeyId": "accessKeyId",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "principalId",
      "arn": "arn:aws:iam::112233445566:role/Admin",
      "accountId": "112233445566",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2019-11-06T19:17:20Z"
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

範例：AWS WAF 傳統日誌檔案項目

AWS WAF Classic 是 的先前版本 AWS WAF。如需相關資訊，請參閱[AWS WAF 傳統](#)。

日誌項目會示範 CreateRule、GetRule、UpdateRule 和 DeleteRule 操作：

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "19434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "19434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
```

```
    "type": "IAMUser",
    "principalId": "AIDAIEP4IT4TPDEXAMPLE",
    "arn": "arn:aws:iam::777777777777:user/nate",
    "accountId": "777777777777",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "nate"
  },
  "eventTime": "2016-04-25T21:35:22Z",
  "eventSource": "waf.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
  },
  "responseElements": null,
  "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
  "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-08-24",
  "recipientAccountId": "777777777777"
},
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIEP4IT4TPDEXAMPLE",
    "arn": "arn:aws:iam::777777777777:user/nate",
    "accountId": "777777777777",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "nate"
  },
  "eventTime": "2016-04-25T21:35:13Z",
  "eventSource": "waf.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
    "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
    "updates": [
      {
```

```
        "predicate": {
          "type": "SizeConstraint",
          "dataId": "9239c032-bbbe-4b80-909b-782c0example",
          "negated": false
        },
        "action": "INSERT"
      }
    ],
    "responseElements": {
      "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
    },
    "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
    "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
      "accountId": "777777777777",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "nate"
    },
    "eventTime": "2016-04-25T21:35:28Z",
    "eventSource": "waf.amazonaws.com",
    "eventName": "DeleteRule",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "changeToken": "fd232003-62de-4ea3-853d-52932example",
      "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
    },
    "responseElements": {
      "changeToken": "fd232003-62de-4ea3-853d-52932example"
    },
    "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
    "eventID": "a3236565-1a1a-4475-978e-81c12example",
    "eventType": "AwsApiCall",
```

```
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  }
]
```

AWS Shield Advanced CloudTrail 中的資訊

AWS Shield Advanced 支援將下列動作記錄為 CloudTrail 日誌檔案中的事件：

- [列出堆疊](#)
- [DescribeAttack](#)
- [CreateProtection](#)
- [DescribeProtection](#)
- [DeleteProtection](#)
- [ListProtections](#)
- [CreateSubscription](#)
- [DescribeSubscription](#)
- [GetSubscriptionState](#)

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者登入資料提出請求
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 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](#)。

範例：Shield Advanced 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 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 DeleteProtection 和 ListProtections 動作的 CloudTrail 記錄項目。


```
[
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "1234567890987654321231",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:31:14Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": {
      "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789098765432123",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
```

```
{
  "sourceIPAddress": "AWS Internal",
  "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
  "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
  "eventType": "AwsApiCall",
  "apiVersion": "AWSShield_20160616",
  "recipientAccountId": "123456789012"
}
```

AWS Firewall Manager CloudTrail 中的資訊

AWS Firewall Manager 支援將下列動作記錄為 CloudTrail 日誌檔案中的事件：

- [AssociateAdminAccount](#)
- [DeleteNotificationChannel](#)
- [DeletePolicy](#)
- [DisassociateAdminAccount](#)
- [PutNotificationChannel](#)
- [PutPolicy](#)
- [GetAdminAccount](#)
- [GetComplianceDetail](#)
- [GetNotificationChannel](#)
- [GetPolicy](#)
- [ListComplianceStatus](#)
- [ListPolicies](#)

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者登入資料提出請求
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 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](#)。

範例：防火牆管理員日誌檔案項目

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 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

下列範例顯示示範 GetAdminAccount--> 動作的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890987654321231",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
    "accountId": "123456789012",
    "accessKeyId": "1AFGDT647FHU83JHFI81H",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated":
"false",
        "creationDate":
"2018-04-14T02:51:50Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId":
"1234567890987654321231",
        "arn":
"arn:aws:iam::123456789012:role/Admin",
        "accountId":
"123456789012",
        "userName": "Admin"
      }
    },
    "eventTime": "2018-04-14T03:12:35Z",
    "eventSource": "fms.amazonaws.com",
    "eventName": "GetAdminAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
```

```
    "userAgent": "console.amazonaws.com",  
    "requestParameters": null,  
    "responseElements": null,  
    "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",  
    "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",  
    "eventType": "AwsApiCall",  
    "apiVersion": "2018-01-01",  
    "recipientAccountId": "123456789012"  
}
```

使用 AWS WAF 和 AWS Shield Advanced API

本節說明如何向 AWS WAF 和 Shield Advanced API 提出請求，以在 中建立和管理配對集、規則和保護套件或 Web ACLs，AWS WAF 以及在 Shield Advanced 中建立和保護。本節可讓您熟悉請求元件、回應內容，以及如何驗證請求。

主題

- [使用 AWS SDKs](#)
- [向 AWS WAF 或 Shield Advanced 提出 HTTPS 請求](#)
- [HTTP 回應](#)
- [對請求進行身分驗證](#)

使用 AWS SDKs

如果您使用 AWS 提供 開發套件的語言，請使用 開發套件，而不是嘗試透過 APIs 進行操作。SDKs 可讓身分驗證更簡單、輕鬆與您的開發環境整合，並提供 AWS WAF 和 Shield Advanced 命令的輕鬆存取。如需 AWS SDKs 的詳細資訊，請參閱 主題[下載工具](#)中的 [設定您的帳戶以使用 服務](#)。

向 AWS WAF 或 Shield Advanced 提出 HTTPS 請求

AWS WAF 和 Shield Advanced 請求是 HTTPS 請求，如 [RFC 2616](#) 所定義。與任何 HTTP 請求一樣，對 AWS WAF 或 Shield Advanced 的請求包含請求方法、URI、請求標頭和請求內文。回應包含 HTTP 狀態碼、回應標題，有時還包括回應內文。

請求 URI

請求 URI 始終是一個單一斜線 /。

HTTP 標頭

AWS WAF 和 Shield Advanced 在 HTTP 請求的 標頭中需要以下資訊：

主機 (必要)

指定您資源所建立地點的端點。如需端點的相關資訊，請參閱 [AWS 服務端點](#)。例如，AWS WAF CloudFront 分佈的 Host 標頭值為 `waf.amazonaws.com:443`。

x-amz-date 或日期 (必要)

用來建立 Authorization 標頭中包含的簽章的日期。指定 ISO 8601 標準的格式，以 UTC 時間，如下所示：

```
x-amz-date: 20151007T174952Z
```

您必須包含 x-amz-date 或 Date。(有些 HTTP 用戶端程式庫不讓您設定 Date 標頭)。當 x-amz-date 標頭存在時，會在驗證請求時 AWS WAF 忽略任何 Date 標頭。

收到請求時，時間戳記必須在 AWS 系統時間的 15 分鐘內。若為非，請求失敗並發生 RequestExpired 錯誤碼，以防止其他人重播您的請求。

授權 (必要)

請求驗證所需的資訊。如需建構此標頭的詳細資訊，請參閱[對請求進行身分驗證](#)。

X-Amz-Target (必要)

AWSWAF_ 或 AWSShield_ 串接，API 版本無需標點符號、句點 (.) 和操作的名稱，例如：

```
AWSWAF_20150824.CreateWebACL
```

內容類型 (條件)

指定內容類型為 JSON 和 JSON 的版本，如下所示：

```
Content-Type: application/x-amz-json-1.1
```

條件：POST 請求為必要。

內容長度 (條件)

根據 RFC 2616 的訊息長度 (無標題)。

條件：如果請求內文本包含資訊 (大多數工具組將自動新增此標題)，則為必填項目。

以下是 HTTP 請求在 中建立保護套件或 Web ACL 的範例標頭 AWS WAF：

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
```

```
Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,  
SignedHeaders=host;x-amz-date;x-amz-target,
```

```
Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9  
X-Amz-Target: AWSWAF_20150824.CreateWebACL  
Accept: */*  
Content-Type: application/x-amz-json-1.1; charset=UTF-8  
Content-Length: 231  
Connection: Keep-Alive
```

HTTP 請求內文

許多 AWS WAF 和 Shield Advanced API 動作會要求您在請求內文中包含 JSON 格式的資料。

下列範例請求使用簡單的 JSON 陳述式來更新 IPSet，以包含 IP 地址 192.0.2.44（在 CIDR 表示法中表示為 192.0.2.44/32）：

```
POST / HTTP/1.1  
Host: waf.amazonaws.com:443  
X-Amz-Date: 20151007T174952Z  
Authorization: AWS4-HMAC-SHA256  
Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,  
SignedHeaders=host;x-amz-date;x-amz-target,  
  
Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9  
X-Amz-Target: AWSWAF_20150824.UpdateIPSet  
Accept: */*  
Content-Type: application/x-amz-json-1.1; charset=UTF-8  
Content-Length: 283  
Connection: Keep-Alive  
  
{  
  "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",  
  "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",  
  "Updates": [  
    {  
      "Action": "INSERT",  
      "IPSetDescriptor": {  
        "Type": "IPv4",  
        "Value": "192.0.2.44/32"  
      }  
    }  
  ]  
}
```

```
}
```

HTTP 回應

所有 AWS WAF 和 Shield Advanced API 動作在回應中都包含 JSON 格式的資料。

以下為 HTTP 回應中一些重要的標頭，以及在應用程式中如何應用他們，如果適用的話：

HTTP/1.1

此標頭後面有狀態碼。狀態碼 200 表示操作成功。

類型：字串

x-amzn-RequestId

由 AWS WAF 或 Shield Advanced 建立的值，可唯一識別您的請求，例如 K2QH8DN0U907N97FNA2GDLL80BVV4KQNS05AEMVJF66Q9ASUAAJG。如果您遇到問題 AWS WAF，AWS 可以使用此值來疑難排解問題。

類型：字串

內容長度

回應內文的長度，以位元組為單位。

類型：字串

日期

AWS WAF 或 Shield Advanced 回應的日期和時間，例如，2015 年 10 月 7 日星期三 12:00:00 GMT。

類型：字串

錯誤回應

如果請求的結果是錯誤，則 HTTP 回應會包含下列值：

- JSON 錯誤文件做為回應本文
- 內容類型
- 適用的 3xx、4xx 或 5xx HTTP 狀態碼

以下為 JSON 文件的範例：

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message": "1 validation error detected: Value null at 'TargetString' failed to satisfy constraint: Member must not be null"}
```

對請求進行身分驗證

如果您使用 AWS 提供 開發套件的語言，我們建議您使用 開發套件。與使用 AWS WAF 或 Shield Advanced API 相比，所有 AWS SDKs 都大幅簡化簽署請求的程序，並節省大量時間。此外，SDK 可與您的開發環境輕鬆整合，並可輕鬆存取相關命令。

AWS WAF 和 Shield Advanced 要求您透過簽署請求來驗證您傳送的每個請求。若要簽署請求，請您使用密碼編譯雜湊函數來計算數位簽章，其根據輸入傳回雜湊值。此輸入包含請求和私密存取金鑰的文字。雜湊函數會傳回一個雜湊值，您將此值包含在請求中做為簽章。該簽章是請求 Authorization 標頭中的一部分。

收到請求後，AWS WAF 或 Shield Advanced 會使用您用來簽署請求的相同雜湊函數和輸入來重新計算簽章。如果產生的簽章符合請求中的簽章，AWS WAF 或 Shield Advanced 會處理請求。如果不是，則會拒絕該請求。

AWS WAF 和 Shield Advanced 支援使用 [AWS Signature 第 4 版](#) 進行身分驗證。計算簽章的程序可以分成三個任務：

任務 1：建立正式請求

在正式格式中，如 <https://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html> 中的 Amazon Web Services 一般參考任務 1：建立簽章版本 4 的正式請求 所述，建立您的 HTTP 請求。

任務 2：建立登入字串

建立一個字串，您會使用此字串做為密碼編譯雜湊函數的其中一個輸入值。此字串稱為簽署字串，是下列值的串接：

- 雜湊演算法的名稱
- 要求日期
- 登入資料範圍字串
- 標準化請求之前的任務

登入資料範圍字串本身是日期、區域和服務資訊的串連。

針對 X-Amz-Credential 參數，請指定下列：

- 此端點的程式碼，為您正在傳送請求 us-east-2 的對象
- 使用於服務縮寫的 waf

例如：

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/  
aws4_request
```

任務 3：建立簽章

使用接受兩個輸入字串的密碼編譯雜湊函數來建立請求的簽章：

- 您的簽署字串，來自任務 2。
- 金鑰衍生。藉由從您的私密存取金鑰開始來計算此衍生金鑰和使用登入資料範圍字串，來建立一系列雜湊型訊息身分驗證代碼 (HMACs)。

相關資訊

以下相關資源可協助您使用此服務。

下列資源可供 AWS WAF、AWS Shield Advanced、和 使用 AWS Firewall Manager。

- [實作準則 AWS WAF](#) – 技術發佈，其中包含實作以保護 AWS WAF 現有和新 Web 應用程式的最新建議。
- [AWS 討論論壇](#) – 以社群為基礎的論壇，用於討論與此和其他 AWS 服務相關的技術問題。
- [AWS WAF 討論論壇](#) – 以社群為基礎的論壇，供開發人員討論相關的技術問題 AWS WAF。
- [Shield 進階討論論壇](#) – 以社群為基礎的論壇，供開發人員討論與 Shield 進階相關的技術問題。
- [AWS WAF 產品資訊](#) – 有關 的資訊的主要網頁 AWS WAF，包括功能、定價等。
- [Shield Advanced 產品資訊](#) – Shield Advanced 相關資訊的主要網頁，包括功能、定價等。

下列資源可供 Amazon Web Services 使用。

- [課程和研討會](#) – 連結至角色型和特殊課程，以及自定進度的實驗室，以協助強化您的 AWS 技能並取得實際經驗。
- [AWS 開發人員中心](#) – 探索教學課程、下載工具，並了解 AWS 開發人員事件。
- [AWS 開發人員工具](#) – 開發人員工具、SDKs、IDE 工具組和命令列工具的連結，用於開發和管理 AWS 應用程式。
- [入門資源中心](#) – 了解如何設定您的 AWS 帳戶、加入 AWS 社群，以及啟動您的第一個應用程式。
- [實用的教學課程](#) – 按照逐步教學課程在 AWS 上啟動第一個應用程式。
- [AWS 白皮書](#) – 技術 AWS 白皮書的完整清單連結，涵蓋架構、安全和經濟等主題，並由 AWS Solutions Architects 或其他技術專家撰寫。
- [AWS 支援 中心](#) – 建立和管理 AWS 支援 案例的中樞。也包含其他實用資源的連結，例如論壇、技術 FAQs、服務運作狀態和 AWS Trusted Advisor。
- [支援](#) – 有關 one-on-one、快速回應支援管道的資訊的主要網頁 支援，可協助您在雲端中建置和執行應用程式。
- [聯絡我們](#) – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- [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。

文件歷史紀錄

此頁面列出本文件的重大變更。

服務功能有時會逐步推出至提供服務 AWS 的區域。我們僅針對第一個版本更新此文件。我們不會提供有關區域可用性的資訊，也不會宣布後續區域的推展情況。如需服務功能的區域可用性和訂閱更新通知的相關資訊，請參閱[最新消息 AWS ?](#)。

變更	描述	日期
已更新的 AWS 受管規則 AWS WAF	更新了核心或通用規則集 (CRS)。	2025 年 6 月 18 日
網路安全主管的第一個預覽版本	AWS Shield 網路安全主管現已提供預覽版，可讓您深入了解 AWS 安全組態。	2025 年 6 月 17 日
新增 AWS Shield 網路安全主管的身分型客戶受管政策	您可以建立和管理自己的身分型政策，以授予 AWS Shield 網路安全主管適當的 AWS 資源存取權。	2025 年 6 月 17 日
AWS WAF 新增更新的主控台使用者體驗	AWS WAF 主控台現在具有簡化的加入工作流程，以及透過保護套件管理 Web ACLs 改善方式。	2025 年 6 月 17 日
更新 AWS WAF 指標和維度的新 Anti-DDoS 受管規則群組 AWS WAF	兩個新的分散式阻斷服務 (DDoS) 預防指標現在會發佈至 AWS/ApplicationELB 命名空間：LowReputationRequestsDenied 和 LowReputationPacketsDropped。	2025 年 6 月 11 日
	AWSManagedRulesAntiDDoSRuleSet 透過偵測、	2025 年 6 月 11 日

	標記和挑戰疑似參與 DDoS 攻擊的請求來保護您的資源。	
AWS WAF 新增資源層級 DDoS 保護	您現在可以使用反 DDoS 功能來偵測和防止 Application Load Balancer 中的 DDoS 攻擊。	2025 年 6 月 11 日
AWS WAF 新增 ASN 比對陳述式	您現在可以根據原始 IP 地址的自治系統編號 (ASN) 來比對 Web 請求。	2025 年 6 月 5 日
AWS WAF 新增 ASN 做為自訂金鑰彙總選項	您現在可以使用自訂金鑰彙總來限制來自特定自治系統編號 (ASNs) 的請求。	2025 年 6 月 5 日
已更新的 AWS 受管規則 AWS WAF	已更新 AWS WAF 機器人控制規則集。	2025 年 5 月 29 日
AWS Firewall Manager 安全政策更新	更新 FMSServiceRolePolicy 以新增 Amazon CloudFront 所需的許可。	2025 年 5 月 21 日
更新靜音的 AWS WAF 指標和維度 Challenge	已將 ChallengesAttempted 、 ChallengesAttemptedSdk 、 ChallengeSolved 和 ChallengeSolvedSdk 新增至 AWS WAF 指標和維度區段。	2025 年 5 月 16 日

AWS WAF 受管政策變更	新增 AWSWAFFullAccess、AWSWAFConsoleFullAccess、和 AWSWAFReadOnlyAccess。AWSWAFConsoleReadOnlyAccess 受管政策的 AWS Amplify 許可 AWSWAFConsoleFullAccess，以及和 AWSWAFConsoleReadOnlyAccess 受管政策的 Amazon CloudFront 許可。	2025 年 5 月 5 日
AWS WAF 新增對新 CloudFront 分佈的支援	您現在可以將 AWS WAF Web ACLs 與 CloudFront 多租用戶分佈和分佈租用戶建立關聯。	2025 年 4 月 28 日
日誌比對詳細資訊中的 URI 片段	日誌中的規則比對詳細資訊現在包含來自 Web 請求的 URI 片段。您可以將記錄設定為從日誌中修訂此欄位。	2025 年 3 月 17 日
新的 AWS WAF 請求元件	您現在可以檢查 URI fragment。	2025 年 3 月 17 日
已將用戶端保護新增至 AWS WAF	的用戶端保護 AWS Marketplace 現已可用。您可以透過 AWS Marketplace 主控台訂閱和取消訂閱用戶端保護。	2025 年 3 月 10 日
AWS WAF 支援新的 JA4 欄位比對	您可以根據進階 JavaScript 指紋 (JA4) 特性偵測和封鎖流量，並使用 JA4 指紋做為 WAF 速率型規則中支援的請求金鑰之一。	2025 年 3 月 4 日
已更新的 AWS 受管規則 AWS WAF	更新了核心或通用規則集 (CRS)。	2025 年 3 月 3 日

更新 AWS WAF 指標和維度	已將用量指標的相關資訊新增至 AWS WAF 指標和維度區段。	2025 年 2 月 21 日
AWS WAF 新增資料保護選項	AWS WAF 現在可讓您在保護套件或 Web ACL 層級或僅記錄層級設定資料保護。	2025 年 2 月 14 日
AWS Firewall Manager 安全政策更新	更新 FMSServiceRolePolicy 以新增許可，以批次取得資源組態狀態。	2025 年 2 月 10 日
AWS Firewall Manager 配額更新	更新 Firewall Manager 配額區段，以反映新的 AWS WAF 和 Network Firewall 政策。	2025 年 2 月 10 日
已更新的 AWS 受管規則 AWS WAF	已更新 SQLi 資料庫規則群組。	2025 年 1 月 24 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則群組。	2025 年 1 月 24 日
已更新的 AWS 受管規則 AWS WAF	已更新 SQLi 資料庫規則群組。	2025 年 1 月 24 日
AWS Firewall Manager 資源標籤的更新	Firewall Manager 現在可讓您使用邏輯 AND 運算子或邏輯 OR 運算子結合多個資源標籤。您也可以使用新的萬用字元運算子來比對任何索引鍵或值。	2025 年 1 月 9 日
AWS WAF Web ACL 儀表板新增了最佳安全洞見	AWS WAF 主控台 Web ACL 流量概觀儀表板具有新的熱門洞見索引標籤。	2025 年 1 月 2 日
JA3 和 JA4 指紋上的以速率為基礎的規則彙總	您現在可以在自訂彙總金鑰中指定速率型規則的 JA3 指紋和 JA4 指紋。	2024 年 12 月 20 日

AWS WAF 新增 JA4 指紋的檢查	您現在可以針對 Amazon CloudFront 分佈和 Application Load Balancer，對 Web 請求的 JA4 指紋執行完全相符。	2024 年 12 月 20 日
AWS WAF 行動 SDK 規格的更新	已將 loadTokenIntoProvider 操作新增至 WAFTokenProvider。	2024 年 11 月 19 日
應用程式整合 SDKs 新增電視應用程式	您可以使用適用於電視應用程式和行動應用程式的 Android 和 iOS 整合 SDKs。	2024 年 11 月 19 日
AWS WAF 權杖標記新增瀏覽器指紋	權杖管理現在會新增瀏覽器指紋的標籤。	2024 年 11 月 13 日
已更新的 AWS 受管規則 AWS WAF	已更新 Bot Control 規則群組。	2024 年 11 月 7 日
Firewall Manager AWS WAF 政策可以使用現有的 Web ACLs	Firewall Manager AWS WAF 政策現在可以修改現有的帳戶擁有 ACLs，並僅在需要時建立新的 Web ACLs。	2024 年 10 月 22 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024 年 10 月 16 日
已更新的 AWS 受管規則 AWS WAF	已更新機器人控制、ATP 和 ACFP 受管規則群組。	2024 年 9 月 13 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則群組。	2024 年 9 月 2 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024 年 8 月 30 日
較低的速率型規則閾值	速率型規則的最低請求率現在為 10。在此之前，它是 100。	2024 年 8 月 30 日

已更新的 AWS 受管規則 AWS WAF	已更新 Windows 作業系統規則群組。	2024 年 8 月 28 日
AWS WAF 指標新增了 CAPTCHA JavaScript API 的新指標	AWS WAF 新增兩個新的指標 CaptchasAttemptedSdk 和 CaptchasSolvedSdk，以顯示使用 CAPTCHA JavaScript API 的全帳戶 CAPTCHA 拼圖嘗試。	2024 年 8 月 28 日
為每個組織的呼叫新增配額 ListResourcesForWebACL	AWS WAF 現在會限制組織中任何單一區域的帳戶 ListResourcesForWebACL 對的呼叫數量。	2024 年 7 月 26 日
AWS Firewall Manager 安全政策更新	更新 FMSServiceRolePolicy 以新增讀取 Network Firewall TLS 組態資訊的許可。	2024 年 7 月 22 日
已更新的 AWS 受管規則 AWS WAF	已更新 WordPress 應用程式規則群組。	2024 年 7 月 15 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則群組。	2024 年 7 月 12 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024 年 7 月 9 日
已更新的 AWS 受管規則 AWS WAF	更新 PHP 應用程式和 Windows 作業系統規則群組。	2024 年 7 月 3 日
釐清 JSON 內文剖析的運作方式	更新 JSON 內文檢查的涵蓋範圍，以釐清 AWS WAF 如何處理剖析和內文剖析後援行為。	2024 年 6 月 25 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則群組。	2024 年 6 月 6 日

AWS WAF 受管政策變更	已更新 WAFV2LoggingServiceRolePolicy 和 AWSServiceRoleForWAFV2Logging，將陳述式 IDs (Sid) 新增至許可設定。	2024 年 6 月 3 日
AWS WAF 受管政策變更追蹤	AWS WAF 已開始追蹤受管政策和 WAFV2LoggingServiceRolePolicy 服務連結角色的變更 AWSServiceRoleForWAFV2Logging。	2024 年 6 月 3 日
已更新的 AWS 受管規則 AWS WAF	Bot Control、ATP 和 ACFP 受管規則群組現在已進行版本控制，並將提供版本更新的 SNS 通知，與其他版本控制的 AWS 受管規則相同。	2024 年 5 月 29 日
已更新的 AWS 受管規則 AWS WAF	已更新 POSIX 作業系統規則群組 AWSManagedRulesUnixRuleSet。	2024 年 5 月 28 日
CAPTCHA 和 Challenge 動作	新增說明瀏覽器用戶端需要 HTTPS 來執行 CAPTCHA 拼圖和無提示挑戰。	2024 年 5 月 24 日
與 Amazon Security Lake 整合	您現在可以使用 Security Lake 收集保護套件或 Web ACL 流量資料。如需詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的 從 AWS 服務收集資料 。	2024 年 5 月 22 日

與 Amazon Security Lake 整合	您現在可以使用 Security Lake 收集保護套件或 Web ACL 流量資料。如需詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的 從 AWS 服務收集資料 。	2024 年 5 月 22 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024 年 5 月 21 日
已更新的 AWS 受管規則 AWS WAF	已更新 SQLi 資料庫規則群組。	2024 年 5 月 14 日
已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入和 POSIX 作業系統規則群組。	2024 年 5 月 8 日
已更新的 AWS 受管規則 AWS WAF	已更新 Windows 作業系統規則群組。	2024 年 5 月 3 日
AWS WAF Mobile SDK Android Kotlin 程式碼範例	新增以 Kotlin 為基礎的 Android 整合的範例程式碼。	2024 年 5 月 2 日
AWS WAF 指標新增維度和新指標	AWS WAF 在規則指標 ManagedRuleSetRule 中為 新增了 維度，並為標籤指標的相符規則動作新增了新指標。	2024 年 5 月 2 日
AWS Firewall Manager 支援網路 ACL 政策	Firewall Manager 現在支援透過 Firewall Manager 網路 ACLs 政策管理 Amazon VPC 網路存取控制清單 (ACL)。	2024 年 4 月 25 日
AWS Firewall Manager 安全政策更新	更新 FMSServiceRolePolicy 以新增管理網路 ACLs 許可。	2024 年 4 月 22 日
更新運作狀態檢查指標清單	我們從常用於運作狀態檢查的指標清單中移除了一些指標。	2024 年 4 月 16 日

Firewall Manager 安全群組政策的更新	我們已更新用量稽核安全群組政策並改善文件。請參閱用量稽核政策一節，以及有關最佳實務和限制的章節。	2024 年 4 月 2 日
更新機器人控制範例	新增描述目標檢查層級的範例，並更新現有範例以反映最佳實務。	2024 年 3 月 27 日
更新的 ATP 範例	新增描述回應檢查組態的範例，並更新現有範例以反映最佳實務。	2024 年 3 月 27 日
更新的 ACFP 範例	新增描述回應檢查組態的範例。	2024 年 3 月 27 日
更新 Amazon CloudWatch Logs 日誌串流限制	AWS WAF 在將日誌發佈至 CloudWatch Logs 日誌串流時，不再具有每個保護套件或 Web ACL 限制。	2024 年 3 月 27 日
AWS Shield Advanced 應用程式層（第 7 層）保護	更新應用程式層偵測和緩解、Web ACL 使用、速率型規則和自動應用程式層 DDoS 緩解的一般和最佳實務指引。	2024 年 3 月 14 日
已更新的 AWS 受管規則 AWS WAF	已更新 IP 評價規則群組。	2024 年 3 月 13 日
內文檢查大小限制的變更	AWS WAF 現在支援某些區域資源更大的內文檢查大小限制。	2024 年 3 月 7 日
AWS WAF 速率型規則的可設定評估時段	您現在可以將速率型規則用來計算請求數的時間範圍設定為 1、2、5 或 10 分鐘。預設值為 5，這是此版本之前的唯一選項。	2024 年 2 月 28 日

擴展 CAPTCHA和 的記錄資訊 Challenge	最上層captchaResponse 和challengeResponse 欄位現在會填入要套用至請求的最後一個動作，無論終止或未終止。在此之前，僅針對終止動作填入這些欄位。	2024 年 2 月 22 日
JavaScript CAPTCHA API 金鑰管理	您現在可以透過 API 刪除 CAPTCHA JS AWS WAF APIs 金鑰。	2024 年 2 月 6 日
AWS WAF CAPTCHA 拼圖音訊	CAPTCHA 拼圖的音訊版本現在支援多種語言。	2024 年 2 月 6 日
AWS WAF 挑戰和 CAPTCHA 字符標籤	權杖管理現在會新增 CAPTCHA 權杖的標籤，並已增強挑戰權杖的權杖標籤。	2023 年 12 月 20 日
已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入規則群組。	2023 年 12 月 16 日
已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入規則群組。	2023 年 12 月 14 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 12 月 6 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：AWS WAF Bot Control。	2023 年 12 月 5 日
已更新 Firewall Manager AWS Config 先決條件	如果您使用自訂 IAM 角色，而不是的 Firewall Manager 受管角色 AWS Config，則必須確保您的許可政策允許 AWS Config 記錄器記錄 Firewall Manager 資源。	2023 年 11 月 17 日

AWS WAF 主控台儀表板	我們更正了在 AWS WAF 主控台中檢視保護套件或 Web ACL 的所有規則和取樣請求的指引。	2023 年 11 月 17 日
已更新的 AWS 受管規則 AWS WAF	已更新 Bot Control 規則群組。	2023 年 11 月 14 日
AWS WAF 主控台有新的 Web ACL 儀表板	AWS WAF 主控台內的 Web ACL 頁面具有新的 Web 流量概觀儀表板。	2023 年 11 月 14 日
已更新 ATP 受管規則群組	更正規則 VolumetricIpFailedLoginResponseHigh 和 的標籤資訊VolumetricSessionFailedLoginResponseHigh 。	2023 年 11 月 13 日
已更新 ACFP 受管規則群組	更正規則 VolumetricIPSuccessfulResponse 和 的標籤資訊VolumetricSessionSuccessfulResponse 。	2023 年 11 月 13 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 11 月 2 日
Shield Advanced 自動應用程式層 DDoS 緩解措施	Shield Advanced 現在會在自動緩解規則群組中維護以速率為基礎的規則，限制來自已知為 DDoS 攻擊來源之 IP 地址的請求量。	2023 年 10 月 31 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 10 月 30 日

Bot Control 受管規則群組已移除請求 CSP 的訊號標籤	Bot Control 受管規則群組已移除指示雲端服務提供者 (CSP) 的訊號標籤。	2023 年 10 月 28 日
請求 CSP 的機器人控制受管規則群組訊號標籤	Bot Control 受管規則群組訊號標籤包含指出雲端服務提供者 (CSP) 的標籤。	2023 年 10 月 27 日
已更新 AWS WAF IAM 許可資訊	對於管理保護套件或 Web ACL 關聯的 AWS WAF 動作，政策動作區段現在會列出每個 Web 應用程式資源類型的許可要求。	2023 年 10 月 25 日
修改 Web ACLs 的 Firewall Manager 管理	當您啟用管理未關聯的 Web ACLs 時，防火牆管理員不會在一次性清除未使用的資源中包含修改過的 Web ACLs。	2023 年 10 月 19 日
已更新的 AWS 受管規則 AWS WAF	已更新 POSIX 作業系統規則群組 AWSManagedRulesUnixRuleSet。	2023 年 10 月 12 日
AWS WAF 指標新增維度	AWS WAF 新增了檢視 Web ACL 指標的新維度。	2023 年 10 月 12 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 10 月 11 日
AWS WAF 行動 SDK 規格的新	已將 storeTokenInCookieStorage 操作新增至 WAFTokenProvider。	2023 年 10 月 11 日
的例外狀況部署 AWS 受管規則 AWS WAF	更新已知錯誤輸入規則群組的兩個靜態版本，並更新預設版本以指向最新的靜態版本。	2023 年 10 月 4 日
AWS WAF HTML 實體解碼文字轉換	擴充 HTML 實體解碼文字轉換的功能。	2023 年 10 月 4 日

已將新選項新增至 Firewall Manager 安全群組通用政策	Firewall Manager 現在可將安全群組參考分發至複本安全群組。	2023 年 10 月 3 日
AWS WAF 新增 JA3 指紋的檢查	您現在可以針對 Amazon CloudFront 分佈和 Application Load Balancer，對 Web 請求的 JA3 指紋執行完全相符。	2023 年 9 月 26 日
Firewall Manager 安全群組政策規則設定的更新	Firewall Manager 現在支援從主要安全群組參考到複本安全群組的安全群組。	2023 年 9 月 25 日
已更新 Shield Advanced 自動應用程式層 DDoS 緩解措施	Firewall Manager 現在支援使用自動應用程式層 DDoS 緩解設定的 Shield Advanced 政策的 Application Load Balancer 資源。	2023 年 9 月 14 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：AWS WAF Bot Control。	2023 年 9 月 6 日
AWS WAF 機器人控制	Bot Control 受管規則群組的目標保護層級現在會檢查 IP 地址之間的字符重複使用。它現在還提供可選的流量統計資料機器學習分析，以偵測一些機器人相關活動。	2023 年 9 月 6 日
AWS WAF 行動 SDK 規格的更新	將的最小值、最大值和預設值 tokenRefreshDelaySec 從最小值 300、最大值 600，以及預設值 300 降至最小值 88、最大值 300，以及預設值 88。	2023 年 9 月 5 日
已更新的 AWS 受管規則 AWS WAF	已更新 AWS WAF Bot Control 規則群組。	2023 年 8 月 30 日

Shield Advanced 自動應用程式層 DDoS 緩解措施	新增使用 AWS CloudFormation 來管理您用於自動應用程式層 DDoS 緩解 ACLs 的指引。	2023 年 8 月 30 日
新的 Firewall Manager 內容稽核安全群組政策選項	新增了稽核過度寬鬆規則群組的新選項，並改善了主控台程序描述。	2023 年 8 月 29 日
新的 Firewall Manager Shield 和 AWS WAF 政策選項	如果您在 AWS WAF 和 Shield 中啟用未關聯的 Web ACLs 管理，則 Firewall Manager 只有在 Web ACLs 將由至少一個資源使用時，才會在政策範圍內的帳戶中建立 Web ACLs。	2023 年 8 月 9 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 7 月 26 日
URI 路徑上的以速率為基礎的規則彙總	您現在可以在自訂彙總金鑰中指定速率型規則的 URI 路徑。	2023 年 7 月 19 日
中的新 AWS WAF 政策規則選項 AWS Firewall Manager	AWS Firewall Manager 新增設定 AWS WAF Web 請求內文檢查大小限制的支援。	2023 年 7 月 18 日
AWS WAF 受管政策變更	已更新 AWSWAFFullAccessPolicy、AWSWAFReadOnlyAccess、AWSWAFConsoleFullAccess 和 AWSWAFConsoleReadOnlyAccess，將 AWS Verified Access 新增至您可以使用的資源類型 AWS WAF。	2023 年 6 月 17 日

[已更新的 AWS 受管規則 AWS WAF](#)

已更新規則群組 `AWSMangedRulesACFPRuleSet` 。

2023 年 6 月 13 日

[更新 AWS WAF 詐騙控制帳戶接管預防 \(ATP\)](#)

您現在可以使用規則表達式指定 ATP 受管規則群組的登入端點。

2023 年 6 月 13 日

[CAPTCHA JavaScript API 的新資訊](#)

新章節說明如何在以 CAPTCHA AWS WAF 回應請求時提供自訂 CAPTCHA 拼圖。

2023 年 6 月 13 日

[新的 ACFP 受管規則群組](#)

使用新的規則群組 `AWSMangedRulesACFPRuleSet` 來偵測和封鎖詐騙帳戶建立嘗試。

2023 年 6 月 13 日

[新的 AWS WAF 詐騙控制帳戶建立詐騙預防 \(ACFP\)](#)

您可以使用新的 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組來偵測和封鎖詐騙帳戶建立嘗試 `AWSMangedRulesACFPRuleSet` 。透過受保護的 CloudFront 分佈，您也可以使用 ACFP 封鎖最近提交太多失敗帳戶建立嘗試的用戶端的新帳戶建立嘗試。

2023 年 6 月 13 日

[AWS WAF 受管政策變更](#)

更新 `AWSWAFFullAccessPolicy` 、 `AWSWAFReadOnlyAccess` 、 `AWSWAFConsoleFullAccess` 和 `AWSWAFConsoleReadOnlyAccess` 以更正 AWS App Runner 服務的存取設定。

2023 年 6 月 6 日

新增 Firewall Manager 安全群組政策的限制	如果稍後未共用共用的 VPC，防火牆管理員不會刪除關聯帳戶中的複本安全群組。	2023 年 6 月 2 日
新的 AWS WAF 請求元件：Header order	您現在可以比對請求中標頭名稱的排序清單。	2023 年 5 月 30 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則集。	2023 年 5 月 22 日
已更新 AWS WAF 規則區段的組織	規則陳述式清單現在會依陳述式類型分組。	2023 年 5 月 16 日
移動主題：列出速率受限的 IP 地址	列出受以速率為基礎的規則限制之 IP 地址的主題現在位於以速率為基礎的規則主題下。	2023 年 5 月 16 日
擴展速率型規則的選項	您現在可以根據 IP 地址以外的彙總金鑰對限制 Web 請求進行評分，也可以使用金鑰組合進行彙總。您也可以對符合縮小範圍陳述式的所有請求進行評分，而無需進一步彙總。	2023 年 5 月 16 日
Firewall Manager 配額增加	將中每個組織的 Firewall Manager 政策數目 AWS Organizations 從 20 增加到 50。將每個政策的主要安全群組數量上限從 1 增加到 3。將 WCUs 數目上限從軟式配額變更為硬式配額。	2023 年 5 月 5 日
增加每個規則群組 WCUs	您現在可以使用每個規則群組最多 5,000 個保護套件或 Web ACL 容量單位 WCUs)，而無需請求增加支援。此新限制無法增加。	2023 年 5 月 1 日

AWS WAF 字首為的 Amazon S3 日誌儲存貯體位置	AWS WAF 現在允許 Amazon S3 日誌儲存貯體名稱中的字首。	2023 年 5 月 1 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 4 月 28 日
新增對 AWS 的 Verified Access 執行個體支援 AWS WAF	您現在可以將 AWS WAF Web ACL 與 Verified Access 執行個體建立關聯。此變更僅適用於最新版本的 AWS WAF，不適用於 AWS WAF Classic。	2023 年 4 月 28 日
已修訂有關使用多個 Firewall Manager 管理員的章節	您現在可以指定多個 Firewall Manager 管理員來建立和管理組織的防火牆資源。	2023 年 4 月 24 日
AWS Firewall Manager 受管政策更新	已更新 FMSServiceRolePolicy。	2023 年 4 月 21 日
適用於 CAPTCHA 的新 JavaScript 用戶端應用程式整合	您現在可以自訂 JavaScript 用戶端應用程式中 CAPTCHA 拼圖的位置和特性。	2023 年 4 月 20 日
應用程式整合已重新命名為智慧型威脅整合	我們將用戶端應用程式整合的現有功能重新命名為智慧型威脅整合，以協助區分該功能和適用於 JavaScript 的新 CAPTCHA 應用程式整合。	2023 年 4 月 20 日
超過 1,500 個 Web ACL WCUs 的可變定價	在 Web ACL 中使用超過 1,500 個 Web ACL 容量單位 (WCUs) 會產生額外費用，這會隨著 Web ACL WCU 用量的增加和減少而自動調整。Web ACL 上限為 5,000 WCUs。	2023 年 4 月 11 日

[增加每個保護套件或 Web ACL WCUs](#)

您現在可以使用每個保護套件或 Web ACL 最多 5,000 個保護套件或 Web ACL 容量單位 (WCUs)，而無需請求增加支援。此新限制無法增加。

2023 年 4 月 11 日

[CloudFront 保護套件或 Web ACLs 的內文檢查大小限制](#)

對於保護 Amazon CloudFront 分佈的保護套件或 Web ACLs，您可以在保護套件或 Web ACL 組態中將內文檢查大小限制提高到 64 KB。

2023 年 4 月 11 日

[CloudFront 的內文檢查大小增 加](#)

Amazon CloudFront 分佈的 AWS WAF 內文檢查大小上限從 8 KB 增加到 64 KB。CloudFront 的預設檢查大小限制為 16 KB。

2023 年 4 月 11 日

[中的新 AWS WAF 政策規則選 項 AWS Firewall Manager](#)

AWS Firewall Manager 新增對 AWS WAF 詐騙控制帳戶接管預防 (ATP) 和 AWS WAF Bot Control AWS 受管規則規則群組、Amazon S3 記錄目的地、規則動作覆寫 CAPTCHA 和 Challenge 規則動作，以及字符網域清單的支援。

2023 年 4 月 7 日

AWS WAF 受管政策變更	已更新 AWSWAFFullAccessPolicy、AWSWAFReadOnlyAccess、AWSWAFConsoleFullAccess 和 AWSWAFConsoleReadOnlyAccess，將 AWS App Runner 服務新增至您可以使用的資源類型 AWS WAF。	2023 年 3 月 30 日
新增有關在安全群組政策內使用標籤的警告	如果政策的標籤與組織的標籤政策衝突，則 Firewall Manager 不會更新現有安全群組的標籤或建立新的安全群組。	2023 年 3 月 28 日
更新服務角色資訊	更新如何搭配 Firewall Manager 使用服務角色。	2023 年 3 月 8 日
更正以速率為基礎的規則如何執行速率限制的資訊	針對具有縮小範圍陳述式的規則，僅針對符合規則縮小範圍陳述式的速率限制請求進行評分。我們說明 限制套用至任何速率限制 IP 地址的所有請求。	2023 年 3 月 1 日
已更新的 AWS 受管規則 AWS WAF	已更新 PHP 應用程式規則群組。	2023 年 2 月 27 日
新增對的支援 AWS App Runner 至 AWS WAF	您現在可以將 AWS WAF Web ACL 與 AWS App Runner 服務建立關聯。此變更僅適用於最新版本的 AWS WAF，不適用於 AWS WAF Classic。	2023 年 2 月 23 日
更新的 IAM 指引 AWS Firewall Manager	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務 。	2023 年 2 月 16 日

已更新的 AWS 受管規則 AWS WAF	更新規則群組AWSManagedRulesATPRuleSet，在保護 Amazon CloudFront 分佈 ACLs 中新增登入回應檢查。	2023 年 2 月 15 日
AWS WAF 詐騙控制帳戶接管預防 (ATP) 登入回應檢查	對於受保護的 CloudFront 分佈，您現在可以使用 ATP 封鎖最近提交太多失敗登入嘗試的用戶端的新登入嘗試。	2023 年 2 月 15 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2023 年 1 月 25 日
智慧威脅防禦的最佳實務	已新增實作 Bot Control、ATP 和其他智慧型威脅緩解功能的最佳實務章節。	2023 年 1 月 22 日
如何檢查 HTTP/2 虛擬標頭	新增將 HTTP/2 虛擬標頭映射至其對應 Web 請求元件的區段。	2023 年 1 月 20 日
更新 AWS WAF Classic 的 IAM 指引	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務 。	2023 年 1 月 3 日
更新的 IAM 指引 AWS WAF	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務 。	2023 年 1 月 3 日
更新的 IAM 指引 AWS Shield	更新了指南以符合 IAM 最佳實務。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務 。	2023 年 1 月 3 日
更新 Amazon Route 53 Resolver DNS 防火牆政策	新增刪除 Amazon Route 53 Resolver DNS 防火牆規則群組的相關資訊。	2022 年 12 月 29 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則集。	2022 年 12 月 15 日

已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2022 年 12 月 5 日
Firewall Manager 新增對 Fortigate 雲端原生防火牆 (CNF) as a Service 政策的支援	Firewall Manager 現在支援 Fortigate CNF 政策。	2022 年 12 月 2 日
已移除 DNS 防火牆政策 AWS Config 的需求	對於 DNS 防火牆政策，您現在只需要為資源類型 EC2 VPC 啟用 Config。	2022 年 11 月 17 日
AWS Firewall Manager 受管政策更新	已更新 FMSServiceRolePolicy。	2022 年 11 月 15 日
擴展 AWS WAF CAPTCHA 拼圖的語言選項	CAPTCHA 拼圖現在以多種語言提供其書面指示。每個音訊拼圖內的指示仍僅以英文提供。	2022 年 11 月 11 日
資源集的新 Firewall Manager 配額	新增資源集的新配額。	2022 年 11 月 8 日
新增資源集的支援	您可以建立資源集，將要在 Firewall Manager 政策中管理的資源分組。	2022 年 11 月 8 日
新增從 Network Firewall 匯入防火牆的支援	您現在可以使用資源集在 Network Firewall 政策中匯入和管理現有的防火牆。	2022 年 11 月 8 日
AWS Firewall Manager 受管政策更新	已更新 AWSFMAdminReadOnlyAccess。	2022 年 11 月 2 日
地理比對陳述式現在會將標籤新增至國家和區域的請求	您現在可以將地理比對與標籤比對結合，在區域層級管理地理請求原始伺服器。	2022 年 10 月 31 日

重新命名最上層區段：受管保護	本節現在已命名為 AWS WAF 智慧型威脅防禦，符合我們的行銷頁面。	2022 年 10 月 27 日
Bot Control 受管規則群組中的新目標防護層級	Bot Control 受管規則群組現在提供額外的目標規則，用於偵測和緩解複雜的機器人。此保護層級需額外付費。	2022 年 10 月 27 日
AWS WAF 字符的新區段	了解 如何使用 AWS WAF 權杖進行智慧型威脅緩解。	2022 年 10 月 27 日
新增有關更新 Firewall Manager Network Firewall 政策的重要注意事項	當您更新 Firewall Manager 政策時，政策建立的所有 Network Firewall 政策都會更新為 Firewall Manager 政策的 Network Firewall 政策組態。	2022 年 10 月 27 日
規則群組中的動作覆寫	您現在可以將規則群組中規則的動作覆寫為任何規則動作設定。如同先前的 Count 動作覆寫，您可以將覆寫套用至規則群組中的所有規則和個別規則。	2022 年 10 月 27 日
AWS WAF 新 Challenge 規則動作選項	您可以設定規則來使用 Challenge，以確認瀏覽器正在傳送請求。	2022 年 10 月 27 日
AWS WAF 允許跨多個受保護應用程式共用字符	您可以透過為保護套件或 Web ACL 設定權杖網域清單，在多個受保護的應用程式間啟用權杖使用。	2022 年 10 月 27 日
所有標頭規格不區分大小寫	將所有標頭規格變更為不區分大小寫。這符合單一標頭行為。	2022 年 10 月 26 日

AWS Firewall Manager 受管政策變更	更正為 AWSFMAdminFullAccess 。	2022 年 10 月 21 日
已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入規則群組。	2022 年 10 月 20 日
已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入規則群組。	2022 年 10 月 5 日
AWS WAF 行動 SDK 規格的更新	將的預設值 tokenRefreshDelaySec 從 600 (10 分鐘) 降至 300 (5 分鐘) 。	2022 年 9 月 30 日
已更新的 AWS 受管規則 AWS WAF	更正本文中為下列規則群組提供的標籤名稱：POSIX 作業系統、PHP 應用程式、Word Press 應用程式。	2022 年 9 月 19 日
中的新 AWS WAF 政策規則選項 AWS Firewall Manager	AWS Firewall Manager 現在支援 AWS WAF 政策中預設 Web 動作的自訂 Web 請求和回應。	2022 年 9 月 9 日
更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：IP 評價。	2022 年 8 月 30 日
AWS WAF 受管政策變更	已更新 AWSWAFFullAccessPolicy、AWSWAFReadOnlyAccess、AWSWAFConsoleFullAccess 和 AWSWAFConsoleReadOnlyAccess，將 Amazon Cognito 使用者集區新增至您可以使用的資源類型 AWS WAF。	2022 年 8 月 25 日

AWS WAF 詐騙控制帳戶接管預防 (ATP)	您現在可以將 AWS WAF 詐騙控制帳戶接管預防 (ATP) 功能與 Amazon CloudFront 分佈搭配使用。	2022 年 8 月 24 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2022 年 8 月 22 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組： AWSManagedRulesATP RuleSet。	2022 年 8 月 11 日
新增對 Amazon Cognito 使用者集區的支援 AWS WAF	您現在可以將 AWS WAF Web ACL 與 Amazon Cognito 使用者集區建立關聯。此變更僅適用於最新版本的 AWS WAF，不適用於 AWS WAF Classic。	2022 年 8 月 11 日
新增了版本控制 AWS 受管規則規則群組部署的章節	新增章節，記錄版本控制的 AWS 受管規則規則群組的部署。本節包含如何在發行候選部署期間命名預設版本的相關資訊。	2022 年 7 月 29 日
更新設定 Network Firewall 政策記錄的需求	新增使用加密 Amazon S3 儲存貯體做為日誌目的地之 Network Firewall 政策的要求。	2022 年 7 月 26 日
SQLi 規則陳述式的敏感度層級選項	您現在可以提高 SQL Injection 規則陳述式的敏感度。這不會變更現有陳述式的行為，其敏感度層級預設為 LOW。	2022 年 7 月 15 日
新增 Network Firewall 政策組態選項	Firewall Manager 現在支援 Network Firewall 防火牆政策組態中的具狀態評估順序和預設動作。	2022 年 7 月 14 日

Firewall Manager 安全群組政策規則設定的更新	Firewall Manager 現在支援從主要安全群組到複本安全群組的標籤分佈。	2022 年 7 月 7 日
AWS Shield 指南的更新	展開 Shield 指南中的資訊，說明 Shield 如何執行事件緩解。	2022 年 6 月 24 日
更新測試和調校 AWS WAF 保護的指引	測試和調校的一般指引 AWS WAF 已更新，現在是頂層主題。	2022 年 6 月 20 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：核心規則集 (CRS)。	2022 年 6 月 9 日
新的 Firewall Manager 混淆代理人指引	新增有關如何防止 Firewall Manager 混淆代理人問題的指引。	2022 年 6 月 1 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：核心規則集 (CRS)。	2022 年 5 月 24 日
新的 AWS WAF 請求元件：Headers 和 Cookies	您現在可以檢查 Cookie，除了單一標頭之外，還可以檢查所有標頭。	2022 年 4 月 29 日
新的 AWS WAF 請求元件：Headers 和 Cookies	您現在可以檢查 Web 請求中的 Cookie，除了單一標頭之外，還可以檢查 Web 請求中的所有標頭。	2022 年 4 月 29 日
AWS WAF 處理過大的內文、標頭和 Cookie 請求元件	您現在可以在檢查這些元件的規則中指定 AWS WAF 應如何處理過大請求內文、標頭和 Cookie。您已建立用來檢查這些元件的規則，其行為符合處理過大的新 Continue 選項。	2022 年 4 月 29 日
AWS WAF Amazon S3 日誌政策變更	已更新 Amazon S3 日誌許可政策和範例。	2022 年 4 月 12 日

適用於 Application Load Balancer AWS Shield Advanced 的 現已提供自動應用程式層 DDoS 緩解選項	Shield Advanced 現在支援 Application Load Balancer 的自動應用程式層 DDoS 緩解措施，使其可用於所有應用程式層保護。您可以設定 Shield Advanced 自動計數或封鎖屬於受保護資源之應用程式層 DDoS 攻擊一部分的 Web 請求。	2022 年 4 月 8 日
新增受管規則群組目前預設版本設定的指標	受管規則群組版本清單現在指出哪個版本是目前的預設值。	2022 年 4 月 8 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：AWS WAF Bot Control。	2022 年 4 月 6 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2022 年 3 月 31 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2022 年 3 月 30 日
Firewall Manager 新增對 Palo Alto Networks 雲端新一代防火牆 (NGFW) 的支援	Firewall Manager 現在支援 Palo Alto Networks 雲端新一代防火牆 (NGFW)。	2022 年 3 月 30 日
將對 Palo Alto Networks Cloud NGFW 的支援新增至 AWS Firewall Manager	AWS Firewall Manager 現在支援 Palo Alto Networks 雲端新一代防火牆 (NGFW) 政策。	2022 年 3 月 30 日
AWS Shield 指南的更新	擴展 Shield 指南中的資訊，說明 Shield 如何執行事件偵測，並提供 DDoS 彈性架構的範例。	2022 年 3 月 16 日

AWS Shield 指南的更新	擴展了 Shield 指南中的資訊，並改善了各種章節的組織。主要變更位於下列 Shield 指南章節：Shield 回應團隊 (SRT) 支援、中的資源保護 AWS Shield Advanced，以及 DDoS 事件的可見性。	2022 年 2 月 28 日
Firewall Manager 現在支援 Network Firewall 集中式部署模型	新增了新程序，說明如何設定使用分散式和集中式部署模型的政策。	2022 年 2 月 24 日
Firewall Manager 新增對 AWS Network Firewall 集中式部署模型的支援	您現在可以將 AWS Network Firewall 政策設定為使用分散式或集中式部署模型。使用分散式部署模型，防火牆管理員會在政策範圍內的每個 VPC 中建立和維護防火牆端點。透過集中式部署模型，防火牆管理員會在單一檢查 VPC 中建立和維護防火牆端點。	2022 年 2 月 24 日
將 AWS WAF 受管規則群組版本控制的支援新增至 AWS Firewall Manager	AWS Firewall Manager 現在支援 Firewall Manager AWS WAF 政策中的 AWS WAF 受管規則群組版本控制。	2022 年 2 月 18 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy。	2022 年 2 月 16 日
更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：IP 評價清單。	2022 年 2 月 15 日
更新的 AWS 受管規則 AWS WAF	已更新 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 AWSManagedRulesATP RuleSet。	2022 年 2 月 11 日

AWS WAF 指南組織的變更	新增了受管保護的頂層區段。將 CAPTCHA 區段從規則下的移至新受管保護區段下的。將標籤區段從規則下移至自己的頂層區段。	2022 年 2 月 11 日
AWS WAF 用戶端應用程式整合	使用 AWS WAF JavaScript 和行動用戶端 APIs，將您的用戶端應用程式與智慧型威脅緩解 AWS 受管規則規則群組整合，以增強偵測。	2022 年 2 月 11 日
AWS WAF 詐騙控制帳戶接管預防 (ATP)	您可以使用新的 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組來偵測和封鎖帳戶接管嘗試。AWSManagedRulesATPRuleSet。	2022 年 2 月 11 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2022 年 1 月 28 日
AWS WAF 受管政策變更	已更新 AWSWAFFullAccessPolicy 和 AWSWAFConsoleFullAccess 以更正記錄許可。	2022 年 1 月 11 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：核心規則集 (CRS)、SQLi 資料庫。	2022 年 1 月 10 日
Firewall Manager 支援 Shield Advanced 自動應用程式層 DDoS 緩解措施	Amazon CloudFront 資源的 Firewall Manager Shield Advanced 政策現在包含對自動應用程式層 DDoS 緩解的支援。	2022 年 1 月 7 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy。	2022 年 1 月 7 日

更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2021 年 12 月 17 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2021 年 12 月 11 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：已知輸入錯誤。	2021 年 12 月 10 日
新的 AWS Shield Advanced 服務連結角色	新增AWSServiceRoleForAWSShield 以支援自動應用程式層 DDoS 緩解功能。	2021 年 12 月 1 日
新的 AWS Shield 受管政策	新增AWSShieldServiceRolePolicy 以支援自動應用程式層 DDoS 緩解功能。	2021 年 12 月 1 日
適用於 CloudFront AWS Shield Advanced 的 現已提供自動應用程式層 DDoS 緩解選項	Shield Advanced 現在支援 Amazon CloudFront 分佈的自動應用程式層 DDoS 緩解措施。您可以設定 Shield Advanced 自動計數或封鎖屬於 CloudFront 分佈上應用程式層 DDoS 攻擊一部分的 Web 請求。	2021 年 12 月 1 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：核心規則集 (CRS)、Windows 作業系統、Linux 作業系統和 IP 評價清單。	2021 年 11 月 23 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy 。	2021 年 11 月 18 日

擴展的記錄選項 AWS WAF	您現在可以記錄 Amazon CloudWatch Logs 日誌群組或 Amazon Simple Storage Service (Amazon S3) 儲存貯體的保護套件或 Web ACL 流量。這些選項是記錄到 Amazon Data Firehose 交付串流的現有選項以外的其他選項。	2021 年 11 月 15 日
AWS WAF 受管政策變更	已更新 AWSWAFFullAccessPolicy 和 AWSWAFConsoleFullAccess 以支援其他記錄目的地。	2021 年 11 月 15 日
AWS WAF 新CAPTCHA規則動作選項	您可以設定規則，針對 Web 請求執行 CAPTCHA，並視需要將 CAPTCHA 問題傳送至用戶端。	2021 年 11 月 8 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2021 年 10 月 27 日
已更新的 AWS 受管規則 AWS WAF	所有 AWS 受管規則規則群組現在都支援標記。規則描述包含標籤規格。	2021 年 10 月 25 日
Firewall Manager 支援 Network Firewall 日誌篩選	AWS Firewall Manager 現在支援 Network Firewall 政策的日誌篩選。	2021 年 10 月 4 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy。	2021 年 9 月 29 日
新增 regex 比對陳述式	您現在可以比對 Web 請求與單一規則表達式。	2021 年 9 月 22 日

規則群組內的速率型 AWS WAF 規則	您現在可以在規則群組中定義以速率為基礎的 AWS WAF 規則。在 中 AWS Firewall Manager，此功能完全支援 AWS WAF 政策。	2021 年 9 月 13 日
在 中自動移除out-of-scope的資源保護 AWS Firewall Manager	AWS Firewall Manager 可讓您自動移除離開政策範圍之資源的保護。	2021 年 8 月 25 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy 。	2021 年 8 月 12 日
已將版本控制新增至受管規則群組	受管規則群組提供者現在可以為其規則群組進行版本控制。	2021 年 8 月 9 日
修改 AWS Firewall Manager 管理員需求	您可以使用組織的管理帳戶做為 Firewall Manager 管理員帳戶。不允許這麼做。	2021 年 8 月 2 日
Firewall Manager 配額增加	您可以將 Firewall Manager 政策範圍內的 Amazon VPC 執行個體數量從 10 增加到 100。	2021 年 7 月 28 日
AWS Firewall Manager 支援 AWS Network Firewall 路由表監控	AWS Firewall Manager 現在支援路由表監控，並針對路由設定錯誤 AWS Network Firewall 的政策，向安全管理員提供修補動作建議。	2021 年 7 月 8 日
AWS WAF 其他文字轉換選項	文字轉換的擴充選項，您可以在檢查之前套用到 Web 請求元件。	2021 年 6 月 24 日
修改 Firewall Manager AWS WAF 政策資源的命名	Firewall Manager 為 AWS WAF 政策管理ACLs、規則群組和記錄的命名已變更。	2021 年 5 月 26 日

[更新的 AWS 受管規則 AWS WAF](#)

已更新對 IP 評價清單標籤的支援，並移除 Amazon IP 評價清單規則名稱的尾碼。

2021 年 5 月 4 日

[新增對 AWS Organizations 委派管理員的支援](#)

當您設定 AWS Firewall Manager 管理員帳戶時，防火牆管理員現在會將帳戶指定為 Firewall Manager 的 AWS Organizations 委派管理員。透過此變更，當您設定 Firewall Manager 管理員帳戶時，您必須提供組織管理帳戶以外的成員帳戶。此變更不會影響您現有的設定。

2021 年 4 月 30 日

[已更新的 AWS 受管規則 AWS WAF](#)

已更新 AWS WAF Bot Control 規則群組。

2021 年 4 月 1 日

[在規則群組Count中將個別規則動作設定為](#)

您現在可以將規則群組中的個別規則動作設定為 Count。已更正規則群組層級的現有覆寫資訊。

2021 年 4 月 1 日

[受管規則群組的範圍縮減陳述式](#)

您現在可以使用縮小範圍陳述式搭配受管規則群組，就像使用速率型陳述式一樣。

2021 年 4 月 1 日

[日誌篩選](#)

您現在可以根據規則動作和標籤，篩選您記錄的保護套件或 Web ACL 流量。

2021 年 4 月 1 日

[AWS WAF Web 請求上的標籤](#)

您可以設定規則，將標籤新增至相符的 Web 請求，並比對其他規則新增的標籤。

2021 年 4 月 1 日

AWS WAF 機器人控制	您可以使用新的 AWS WAF Bot Control 功能來監控和控制機器人流量，該功能結合了 Bot Control 受管規則群組與 Web 請求標籤、縮小範圍陳述式和日誌篩選。	2021 年 4 月 1 日
Firewall Manager 支援 Amazon Route 53 Resolver DNS Firewall 政策	AWS Firewall Manager 支援集中管理 VPCs 的 Amazon Route 53 Resolver DNS Firewall 傳出 DNS 流量篩選。	2021 年 3 月 31 日
自訂請求和回應處理	您可以為未封鎖的 AWS WAF Web 請求包含自訂標頭，也可以為封鎖的 AWS WAF Web 請求傳送自訂回應。這可用於保護套件或 Web ACL 預設動作和規則動作設定。	2021 年 3 月 29 日
AWS Firewall Manager 受管政策變更	更新至 FMSServiceRolePolicy 。	2021 年 3 月 17 日
已更新的 AWS 受管規則 AWS WAF	更新了下列規則群組：核心規則集 (CRS)、管理員保護、已知錯誤輸入和 Linux 作業系統。	2021 年 3 月 3 日
AWS Shield 受管政策變更追蹤	Shield 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 3 日
AWS Firewall Manager 受管政策變更追蹤	Firewall Manager 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 2 日
AWS WAF 受管政策變更追蹤	AWS WAF 已開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 1 日

檢查 Web 請求內文做為剖析的 JSON	新增將 Web 請求內文檢查為已剖析和篩選 JSON 的選項。這是現有選項以外的選項，可將 Web 請求內文檢查為純文字。	2021 年 2 月 12 日
Firewall Manager 支援 AWS Network Firewall 政策	AWS Firewall Manager 支援集中管理 VPCs AWS Network Firewall 的網路流量篩選。	2020 年 11 月 17 日
新增對 AWS Shield Advanced 保護群組的支援	您現在可以將受保護的資源分組為邏輯群組，並共同管理其保護。	2020 年 11 月 13 日
新增對的支援 AWS AppSync 至 AWS WAF	您現在可以將 AWS WAF Web ACL 與 AWS AppSync GraphQL API 建立關聯。此變更僅適用於最新版本的 AWS WAF，不適用於 AWS WAF Classic。	2020 年 10 月 1 日
已更新的 AWS 受管規則 AWS WAF	已更新 Windows 作業系統規則集。	2020 年 9 月 23 日
已更新的 AWS 受管規則 AWS WAF	已更新規則集 PHP 應用程式和 POSIX 作業系統。	2020 年 9 月 16 日
更新的 AWS Shield 主控台	AWS Shield 提供新的主控台選項，改善使用者體驗。文件中的主控台指引適用於新的主控台。	2020 年 9 月 1 日
一般安全群組政策的 Firewall Manager 更新	AWS Firewall Manager 常見的安全群組政策現在透過主控台實作支援 Application Load Balancer 和 Classic Load Balancer 資源類型。新選項可在常見政策的政策範圍設定中使用。	2020 年 8 月 11 日

已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2020 年 8 月 7 日
在 Web 請求中指定 IP 地址位置	新增從您指定的 HTTP 標頭使用 IP 地址的選項，而不是使用 Web 請求原始伺服器。替代標頭通常是 X-Forwarded-For(XFF)，但您可以指定任何標頭名稱。您可以使用此選項進行 IP 集比對、地理比對和以速率為基礎的規則計數彙總。	2020 年 7 月 9 日
Firewall Manager 更新內容稽核安全群組政策	AWS Firewall Manager 已擴展內容稽核安全群組政策的功能，包括使用受管應用程式和通訊協定清單的受管規則選項，以及資源違規的詳細資訊。	2020 年 7 月 7 日
Firewall Manager 受管清單	AWS Firewall Manager 現在支援受管應用程式和通訊協定清單。Firewall Manager 會管理一些清單，而且您可以建立和管理自己的清單。	2020 年 7 月 7 日
Firewall Manager 支援常見安全群組政策中的共用 VPCs	AWS Firewall Manager 現在支援在共用 VPCs 中使用通用安全群組政策。除了在範圍內帳戶擁有的 VPC 中使用它們之外，您還可以這樣做。	2020 年 5 月 26 日
已更新的 AWS 受管規則 AWS WAF	新增 AWS 受管規則中每個規則的文件 AWS WAF。	2020 年 5 月 20 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則群組。	2020 年 5 月 19 日

[新增將 AWS WAF Classic 資源遷移至 AWS WAF \(v2\) 的支援](#)

您現在可以使用 主控台或 API 匯出 AWS WAF Classic 資源，以遷移至最新版本的 AWS WAF。

2020 年 4 月 27 日

[在政策範圍內新增對 AWS Organizations 組織單位的支援](#)

AWS Firewall Manager 現在支援使用 AWS Organizations 組織單位 (OUs) 來指定政策範圍。除了包含或排除特定帳戶之外，您也可以使用 OU 來包含或排除範圍內的帳戶。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

2020 年 4 月 6 日

[將對 AWS WAF \(v2\) 的支援新增至 AWS Firewall Manager](#)

AWS Firewall Manager 除了舊版 Classic 之外 AWS WAF，現在還支援最新版本的 AWS WAF。

2020 年 3 月 31 日

[AWS Firewall Manager 一般安全群組政策的更新](#)

AWS Firewall Manager 通用安全群組政策現在可選擇將政策套用至範圍內 Amazon EC2 執行個體中的所有彈性網路介面。您仍然可以選擇只將原則套用至預設彈性網路介面。

2020 年 3 月 11 日

[已更新的 AWS 受管規則 AWS WAF](#)

AWS WAF 新增規則群組的 受管AWSManagedRulesAnonymousIpList 規則。

2020 年 3 月 6 日

[已更新的 AWS 受管規則 AWS WAF](#)

AWS 的受管規則 AWS WAF 更新了 WordPress 應用程式和AWSManagedRulesCommonRuleSet 規則群組。

2020 年 3 月 3 日

[將 Amazon Route 53 運作狀態檢查新增至 AWS Shield Advanced 保護選項](#)

Shield Advanced 現在支援使用 Amazon Route 53 運作狀態檢查關聯，以提高威脅偵測和緩解的準確性。

2020 年 2 月 14 日

[更新的 AWS 受管規則 AWS WAF](#)

AWS 的受管規則 AWS WAF 已更新 SQL 資料庫規則群組，以新增檢查訊息 URI。

2020 年 1 月 23 日

[安全群組用量稽核政策的 Firewall Manager 新選項](#)

Firewall Manager 有安全群組用量稽核政策的新選項。您現在可以設定安全群組在被視為不相容之前，必須保持未使用的最小分鐘數。根據預設，此分鐘設定為零。

2020 年 1 月 14 日

[AWS WAF 政策的 Firewall Manager 新選項](#)

Firewall Manager 有新的 AWS WAF 政策選項。您現在可以選擇從範圍內資源移除所有現有的 Web ACL 關聯，然後再將政策的新 Web ACL 與其建立關聯。

2020 年 1 月 14 日

[更新的 AWS 受管規則 AWS WAF](#)

AWS 的受管規則 AWS WAF 已更新核心規則集和 SQL 資料庫規則群組中規則的文字轉換。

2019 年 12 月 20 日

[AWS Firewall Manager 與整合 AWS Security Hub](#)

AWS Firewall Manager 現在會為不合規的資源和攻擊建立問題清單，並將其傳送到 AWS Security Hub。

2019 年 12 月 18 日

[AWS WAF 版本 2 的發行](#)

AWS WAF 開發人員指南的新版本。您可以管理 JSON 格式的 Web ACL 或規則群組。擴充的功能包括邏輯規則陳述式、規則陳述式巢狀化，以及對 IP 地址和地址範圍的完整 CIDR 支援。規則不再是 AWS 資源，但僅存在於 Web ACL 或規則群組的內容中。對於現有客戶，先前的服務版本現在稱為 AWS WAF Classic。在 APIs、SDKs 和 CLIs 中，AWS WAF Classic 會保留其命名機制，而此最新版本的 AWS WAF 會參考新增的「V2」或「v2」，視內容而定。AWS WAF 無法存取在 AWS WAF Classic 中建立 AWS 的資源。若要在 中使用這些資源 AWS WAF，您需要遷移這些資源。

2019 年 11 月 25 日

[AWS 的受管規則規則群組 AWS WAF](#)

新增 AWS 受管規則規則群組。這些都是免費提供給 AWS WAF 客戶。

2019 年 11 月 25 日

[AWS Firewall Manager 支援 Amazon Virtual Private Cloud 安全群組](#)

新增對 Firewall Manager 的 Amazon VPC 安全群組支援。

2019 年 10 月 10 日

[AWS Firewall Manager 的支援 AWS Shield Advanced](#)

新增對 Shield Advanced 的支援至 Firewall Manager。

2019 年 3 月 15 日

[教學課程：建立階層政策](#)

新增在 AWS Firewall Manager 中建立階層政策的教學課程。

2019 年 2 月 11 日

規則群組中的規則層級控制	您現在可以從 AWS Marketplace 規則群組以及您自己的規則群組中排除個別規則。	2018 年 12 月 12 日
AWS Shield Advanced 支援 AWS Global Accelerator 標準加速器	Shield Advanced 現在可以保護 AWS Global Accelerator 標準加速器。	2018 年 11 月 26 日
AWS WAF 支援 Amazon API Gateway	AWS WAF 現在可保護 Amazon API Gateway APIs。	2018 年 10 月 25 日
擴展的 AWS 遮罩進階入門精靈	新精靈提供建立速率型規則和 Amazon CloudWatch Events 的機會。	2018 年 8 月 31 日
AWS WAF logging	啟用日誌記錄取得您 web ACL 分析流量的詳細資訊。	2018 年 8 月 31 日
支援條件中的查詢參數	建立測試條件時，您現在可以搜尋請求的特定參數。	2018 年 6 月 5 日
Shield 進階入門精靈	推出訂閱 Shield Advanced AWS 的新簡化程序。	2018 年 6 月 5 日
展開允許的 CIDR 範圍	建立 IP 比對條件時，AWS WAF 現在支援 IPv4 地址範圍：/8 和 /16 到 /32 之間的任何範圍。	2018 年 6 月 5 日

2018 年之前的更新

下表說明 2018 年之前在 AWS WAF 開發人員指南的每個版本中所做的重要變更。

變更	API 版本	描述	版本日期
更新	2016-08-24	AWS Marketplace 規則群組	2017 年 11 月

變更	API 版本	描述	版本日期
更新	2016-08-24	Shield 進階支援彈性 IP 地址。	2017 年 11 月
更新	2016-08-24	全球威脅儀表板	2017 年 11 月
更新	2016-08-24	防 DDoS 網站教學課程	2017 年 10 月
更新	2016-08-24	Geo 和 regex 條件	2017 年 10 月
更新	2016-08-24	速率為基礎的規則	2017 年 6 月
更新	2016-08-24	重組	2017 年 4 月
更新	2016-08-24	新增 DDOS 保護和支援應用程式負載平衡器的資訊	2016 年 11 月
新功能	2015-08-24	您現在可以 AWS WAF 透過 記錄所有 API AWS CloudTrail 呼叫，該 AWS 服務會記錄您帳戶的 API 呼叫，並將日誌檔案傳送到您的 S3 儲存貯體。CloudTrail 日誌可用來啟用安全分析、追蹤 AWS 資源的變更，以及協助合規稽核。整合 AWS WAF 和 CloudTrail 可讓您判斷對 AWS WAF API 提出的請求、提出每個請求的來源 IP 地址、提出請求的人員、提出請求的時間等等。 如果您已經在使用 AWS CloudTrail，您會開始在 CloudTrail 日誌中看到 AWS WAF API 呼叫。如果您尚未為帳戶啟用 CloudTrail，您可以從 中在 CloudTrail 上啟用它 AWS Management Console。啟用 CloudTrail 無需額外費用，但適用 Amazon S3 和 Amazon SNS 用量的標準費率。	2016 年 4 月 28 日

變更	API 版本	描述	版本日期
新功能	2015-08-24	您現在可以使用 AWS WAF 來允許、封鎖或計數看似包含惡意指令碼的 Web 請求，稱為跨網站指令碼或 XSS。攻擊者有時會將惡意指令碼插入到 web 請求中，利用 web 應用程式的漏洞。如需詳細資訊，請參閱 跨網站指令碼攻擊規則陳述式 。	2016 年 3 月 29 日
新功能	2015-08-24	在此版本中，AWS WAF 新增下列功能： - 您可以設定 AWS WAF，根據請求的指定部分長度來允許、封鎖或計數 Web 請求，例如查詢字串或 URIs。如需詳細資訊，請參閱大小約束規則陳述式。 - 您可以設定根據請求內文中的內容 AWS WAF 來允許、封鎖或計數 Web 請求。這也是請求的一部分，其中包含您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。此功能適用於字串、SQL injection 符合條件，和在第一個項提及的新容量限制條件。如需詳細資訊，請參閱在中調整規則陳述式設定 AWS WAF。	2016 年 1 月 27 日
新功能	2015-08-24	您現在可以使用 AWS WAF 主控台來選擇要與 Web ACL 建立關聯的 CloudFront 分佈。如需詳細資訊，請參閱 關聯或取消關聯 Web ACL 和 CloudFront 分佈 。	2015 年 11 月 16 日
初始版本	2015-08-24	這是《AWS WAF 開發人員指南》的第一個版本。	2015 年 10 月 6 日