實作指南

AWS WAF 的安全自動化

AWS WAF 的安全自動化: 實作指南

Table of Contents

解決方案概觀 1
功能和優勢 2
使用 AWS 受管規則規則群組保護您的 Web 應用程式 2
使用預先定義的 HTTP 洪水自訂規則提供第 7 層洪水保護 3
使用預先定義的掃描器和探查自訂規則封鎖漏洞入侵 3
使用預先定義的錯誤機器人自訂規則偵測和防禦入侵 3
封鎖具有預先定義 IP 評價的惡意 IP 地址會列出自訂規則 3
使用預先定義的允許和拒絕 IP 清單自訂規則提供手動 IP 組態 3
建置您自己的監控儀表板 4
使用案例 4
概念和定義 4
架構概觀 7
架構圖 7
AWS Well-Architected 設計考量事項 10
卓越營運 10
安全 10
可靠性 11
效能效率 11
成本最佳化 11
永續性 11
架構詳細資訊 12
此解決方案中的 AWS 服務 12
日誌剖析器選項 13
AWS WAF 速率型規則 13
Amazon Athena 日誌剖析器 13
AWS Lambda 日誌剖析器 14
元件詳細資訊 14
日誌剖析器 - 應用程式 14
日誌剖析器 - AWS WAF 16
日誌剖析器 - 錯誤的機器人 17
IP 清單剖析器 18
規劃您的部署 19
支援的 AWS 區域 19
成本 20

CloudWatch 日誌的成本估算 22
Athena 的成本估算 22
安全 23
IAM 角色 23
資料 23
保護功能 24
配額 24
此解決方案中 AWS 服務的配額 25
AWS WAF 配額 25
部署考量 25
AWS WAF 規則 25
Web ACL 流量記錄 25
請求元件的超大處理 26
多個解決方案部署 26
部署的最低角色許可 （選用） 26
部署解決方案 34
部署程序概觀 34
AWS CloudFormation 範本 35
主要堆疊 35
WebACL 堆疊 35
Firehose Athena 堆疊 35
先決條件 36
設定 CloudFront 分佈 36
設定 ALB 36
步驟 1. 啟動 堆疊 36
步驟 2. 將 Web ACL 與您的 Web 應用程式建立關聯 62
步驟 3。設定 web 存取記錄 62
從 CloudFront 分佈存放 Web 存取日誌 62
從 Application Load Balancer 存放 Web 存取日誌 63
更新解決方案 64
更新考量事項 64
資源類型更新 65
WAFV2 升級 65
堆疊更新時的自訂 65
無效的機器人保護升級 65
CDK 升級 66

解除安裝解決方案 67
使用 解決方案 68
修改允許和拒絕的 IP 集 （選用） 68
在 Web 應用程式中嵌入 Honeypot 連結 （選用） 68
為 Honeypot 端點建立 CloudFront 原始伺服器 69
將 Honeypot 端點內嵌為外部連結 70
使用 Lambda 日誌剖析器 JSON 檔案 70
使用 Lambda 日誌剖析器 JSON 檔案進行 HTTP 洪水保護 70
使用 Lambda 日誌剖析器 JSON 檔案進行掃描器和探查保護 72
在 HTTP 洪水 Athena 日誌剖析器中使用國家/地區和 URI 73
檢視 Amazon Athena 查詢 73
檢視 WAF 日誌查詢 74
檢視應用程式存取日誌查詢 75
檢視新增 Athena 分割區查詢 75
在允許和拒絕的 AWS WAF IP 集上設定 IP 保留 76
運作方式 76
開啟 IP 保留 77
組建監控儀表板 78
處理 XSS 誤報 79
疑難排解 80
聯絡 支援 80
建立案例 80
如何提供協助？ 80
其他資訊 80
協助我們更快解決您的案例 80
立即解決或聯絡我們 81
開發人員指南 82
來源碼 82
參考資料 83
匿名資料收集 83
相關資源 84
關聯的 AWS 白皮書 84
關聯的 AWS 安全部落格文章 84
第三方 IP 評價清單 84
貢獻者 84
修訂 86

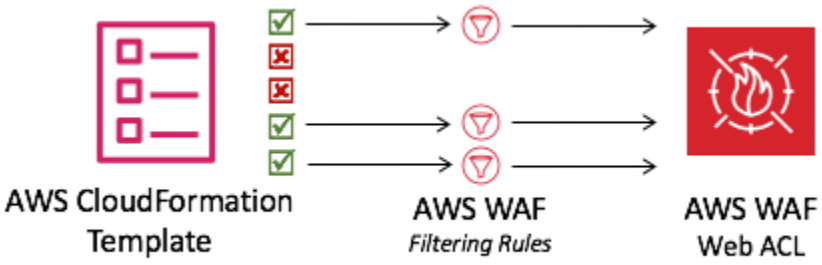
注意 87
..... lxxxviii

自動部署單一 Web 存取控制清單，透過 AWS WAF 上的安全自動化來篩選 Web 型攻擊

AWS WAF 安全自動化解決方案會部署一組預先設定的規則，協助您保護應用程式免於常見的 Web 入侵。此解決方案的核心服務 AWS WAF 可協助保護 Web 應用程式免受可能影響應用程式可用性、危及安全性或耗用過多資源的攻擊技術。您可以使用 AWS WAF 來定義可自訂的 Web 安全規則。這些規則控制哪些流量允許或封鎖部署在 Amazon CloudFront、Application Load Balancer (ALB) 等 AWS 資源上的 Web 應用程式和應用程式程式設計介面 (APIs)。如需更多支援的資源類型，請參閱AWS WAF、AWS Firewall Manager 和 AWS Shield 進階開發人員指南》中的 AWS WAF。

設定 AWS WAF 規則對大型和小型組織來說可能具有挑戰性和負擔，尤其是沒有專用安全團隊的組織。為了簡化此程序，AWS WAF 安全自動化解決方案會自動部署單一 Web 存取控制清單 (ACL)，其中包含一組專為篩選常見 Web 型攻擊所設計的 AWS WAF 規則。在此解決方案 AWS CloudFormation 範本的初始組態期間，您可以指定要包含哪些保護功能。部署此解決方案之後，AWS WAF 會檢查現有 CloudFront 分佈或 ALB(s) 的 Web 請求，並在適用時封鎖這些請求。

CloudFormation 範本會使用 AWS WAF 篩選規則部署 Web ACL。



本實作指南討論在 Amazon Web Services (AWS) 雲端中部署此解決方案的架構考量、組態步驟和操作最佳實務。它包含 CloudFormation 範本的連結，這些範本使用 AWS 最佳實務來啟動、設定和執行在 AWS 上部署此解決方案所需的 AWS 安全性、運算、儲存和其他服務。

本指南中的資訊假設 AWS WAF、CloudFront、ALBs和 AWS Lambda 等 AWS 服務的工作知識。它還需要常見 Web 型攻擊和緩解策略的基本知識。

> **Note**
>
> 從 3.0.0 版開始，此解決方案支援最新版本的 AWS WAF 服務 API (AWS WAFV2)。

本指南適用於 IT 管理員、安全工程師、DevOps 工程師、開發人員、解決方案架構師和網站管理員。

> **Note**
>
> 我們建議您使用此解決方案做為實作 AWS WAF 規則的起點。您可以自訂原始程式碼、新增新的自訂規則，並根據您的需求利用更多 AWS WAF 受管規則。

使用此導覽表快速找到這些問題的答案：

如果您想要 . . .	讀取 . . .
了解執行此解決方案的成本。執行此解決方案的總成本取決於啟用的保護，以及擷取、儲存和處理的資料量。	成本
了解此解決方案的安全考量。	安全性
了解此解決方案支援哪些 AWS 區域。	支援的 AWS 區域
檢視或下載此解決方案中包含的 CloudFormation 範本，以自動部署此解決方案的基礎設施資源 (「堆疊」)。	AWS CloudFormation 範本
使用 支援來協助您部署、使用或疑難排解解決方案。	支援
存取原始程式碼，並選擇性地使用 AWS 雲端開發套件 (AWS CDK) 來部署解決方案	GitHub 儲存庫

功能和優勢

適用於 AWS WAF 的 Security Automations 解決方案提供下列功能和優勢。

使用 AWS 受管規則規則群組保護您的 Web 應用程式

AWS WAF 受管規則可針對常見的應用程式漏洞或其他不需要的流量提供保護。此解決方案包括 AWS 受管 IP 評價規則群組、AWS 受管基準規則群組和 AWS 受管使用案例特定規則群組。您可以選擇為 Web ACL 選取一或多個規則群組，最高可達 Web ACL 容量單位 (WCU) 配額上限。

使用預先定義的 HTTP 洪水自訂規則提供第 7 層洪水保護

HTTP 洪水自訂規則可在客戶定義的期間內防止 Web 層分散式Denial-of-Service(DDoS) 攻擊。您可以選擇下列其中一個選項來啟用此規則：

- AWS WAF 速率型規則
- Lambda 日誌剖析器
- Amazon Athena 日誌剖析器

Lambda 日誌剖析器或 Athena 日誌剖析器選項可讓您定義小於 100 的請求配額。此方法可協助您不達到 AWS WAF 速率型規則所需的配額。如需詳細資訊，請參閱日誌剖析器選項。

您也可以新增國家/地區和統一資源識別符 (URI) 來篩選條件，以增強 Athena 日誌剖析器。此方法可識別並封鎖具有不可預測 URI 模式的 HTTP 洪水攻擊。如需詳細資訊，請參閱 HTTP Flood Athena 日誌剖析器中的使用國家/地區和 URI。

使用預先定義的掃描器和探查自訂規則封鎖漏洞入侵

掃描器和探查自訂規則會剖析搜尋可疑行為的應用程式存取日誌，例如原始伺服器產生的異常錯誤量。然後，它會在客戶定義的期間內封鎖這些可疑來源 IP 地址。您可以選擇其中一個選項來啟用此規則：Lambda 日誌剖析器或 Athena 日誌剖析器。如需詳細資訊，請參閱日誌剖析器選項。

使用預先定義的錯誤機器人自訂規則偵測和防禦入侵

錯誤的機器人自訂規則會設定 Honeypot 端點，這是一種安全機制，旨在引誘和防禦嘗試的攻擊。您可以在網站中插入端點，以偵測來自內容抓取器和不良機器人的傳入請求。一旦偵測到，來自相同原始伺服器的任何後續請求都會遭到封鎖。如需詳細資訊，請參閱在 Web 應用程式中內嵌 Honeypot 連結。

封鎖具有預先定義 IP 評價的惡意 IP 地址會列出自訂規則

IP 評價清單自訂規則會檢查要封鎖的新 IP 範圍的每小時第三方 IP 評價清單。這些清單包括 Spamhaus 不路由或對等 (DROP) 和延伸 DROP (EDROP) 清單、Proofpoint 潛在威脅 IP 清單，以及 Tor 結束節點清單。

使用預先定義的允許和拒絕 IP 清單自訂規則提供手動 IP 組態

允許和拒絕的 IP 列出自訂規則，可讓您手動插入要允許或拒絕的 IP 地址。您也可以在允許和拒絕的 IP 清單上設定 IP 保留，以在設定的時間使 IPs過期。

建置您自己的監控儀表板

此解決方案會發出 Amazon CloudWatch 指標，例如允許的請求、封鎖的請求和其他相關指標。您可以建置自訂儀表板，將這些指標視覺化，並深入了解 AWS WAF 提供的攻擊和保護模式。如需詳細資訊，請參閱建置監控儀表板。

使用案例

以下是使用此解決方案的範例使用案例。您可以使用不限於此清單的創新方式來自訂此解決方案。

自動化 AWS WAF 規則的設定

AWS WAF 可保護您的 Web 應用程式免受常見攻擊；不過，設定 AWS WAF 規則可能很複雜且耗時。為了協助您，此解決方案會使用 CloudFormation 範本，自動將一組 AWS WAF 規則部署到您的 帳戶。如此一來，您就不需要自行設定 AWS WAF 規則，而且可以更快地開始使用 AWS WAF。

自訂 layer 7 HTTP 洪水保護

此解決方案提供三種啟用 HTTP 洪水保護的選項。您可以選擇符合您需求的選項，以獲得 DDoS 攻擊的保護。如需詳細資訊，請參閱 功能和優點中的使用預先定義的 HTTP 洪水自訂規則提供第 7 層洪水保護。

利用原始程式碼來套用自訂或建置您自己的安全自動化

此解決方案提供如何使用 AWS WAF 和其他 服務在 AWS 雲端上建置安全自動化的範例。GitHub 中的開放原始碼可讓您輕鬆地套用自訂或建置符合您需求的安全自動化。

概念和定義

本節說明關鍵概念並定義此解決方案特有的術語。

ALB 日誌

此解決方案會使用 ALB 資源的日誌。此解決方案中的掃描器和探查保護規則會檢查這些日誌。

Athena 日誌剖析器

Amazon Athena 是一種無伺服器互動式分析服務，以開放原始碼架構為基礎，支援開放式資料表和檔案格式。如果使用者在啟用 HTTP 洪水防護規則或掃描器與探查防護規則yes - Amazon Athena

log parser時選擇，此解決方案會執行排程的 Athena 查詢來檢查 AWS WAF、CloudFront 或 ALB 日誌，並可透過透過透過結構化邏輯鏈操作的偵測來啟用錯誤機器人保護。

AWS WAF 規則

AWS WAF 規則定義：

- 如何檢查 HTTP(S) Web 請求
- 當請求符合檢查條件時，要對請求採取的動作

您只能在規則群組或 Web ACL 的內容中定義規則。

CloudFront 日誌

此解決方案會使用 CloudFront 資源的日誌。此解決方案中的掃描器和探查保護規則會檢查這些日誌。

IP 集

IP 集提供您要使用的 IP 地址和 IP 地址範圍的集合

規則陳述式中的 。IP 集合是 AWS 資源。

Lambda 日誌剖析器

此解決方案會執行由 Amazon Simple Storage Service (Amazon S3) 物件建立事件調用的 Lambda 函數。如果使用者在啟用 HTTP 洪水保護 、掃描器和探查保護yes - AWS Lambda log parser時選擇，Lambda 函數會啟動 AWS WAF、CloudFront 或 ALB 日誌的檢查，並可透過透過透過結構化邏輯鏈操作的偵測來用於錯誤的機器人保護規則。

受管規則群組

受管規則群組是 AWS 和 AWS Marketplace 賣方為您撰寫和維護的預先定義、ready-to-use規則集合。AWS WAF 定價適用於您對任何受管規則群組的使用。

資源/端點類型

您可以將 AWS 資源與 Web ACLs 建立關聯，以保護它們。這些資源包括 CloudFront、ALB、AWS AppSync、Amazon Cognito、AWS App Runner 和 AWS Verified Access 資源。目前此解決方案 Amazon 支援 CloudFront 和 ALB。

WAF 日誌

此解決方案會將 AWS WAF 產生的日誌用於與 Web ACL 相關聯的資源。此解決方案的 HTTP 洪水保護、掃描器和探查保護和啟用錯誤機器人保護規則會檢查這些日誌。

WCU

AWS WAF 使用 Web 存取控制清單 (ACL) 容量單位 (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。AWS WAF 會強制執行 WCU 配額。 ACLs WCUs 不會影響 AWS WAF 檢查 Web 流量的方式。

Web ACL

Web ACL 可讓您精細控制受保護資源回應的 HTTP(S) Web 請求。

> **Note**
>
> 如需 AWS 術語的一般參考，請參閱 AWS 詞彙表。

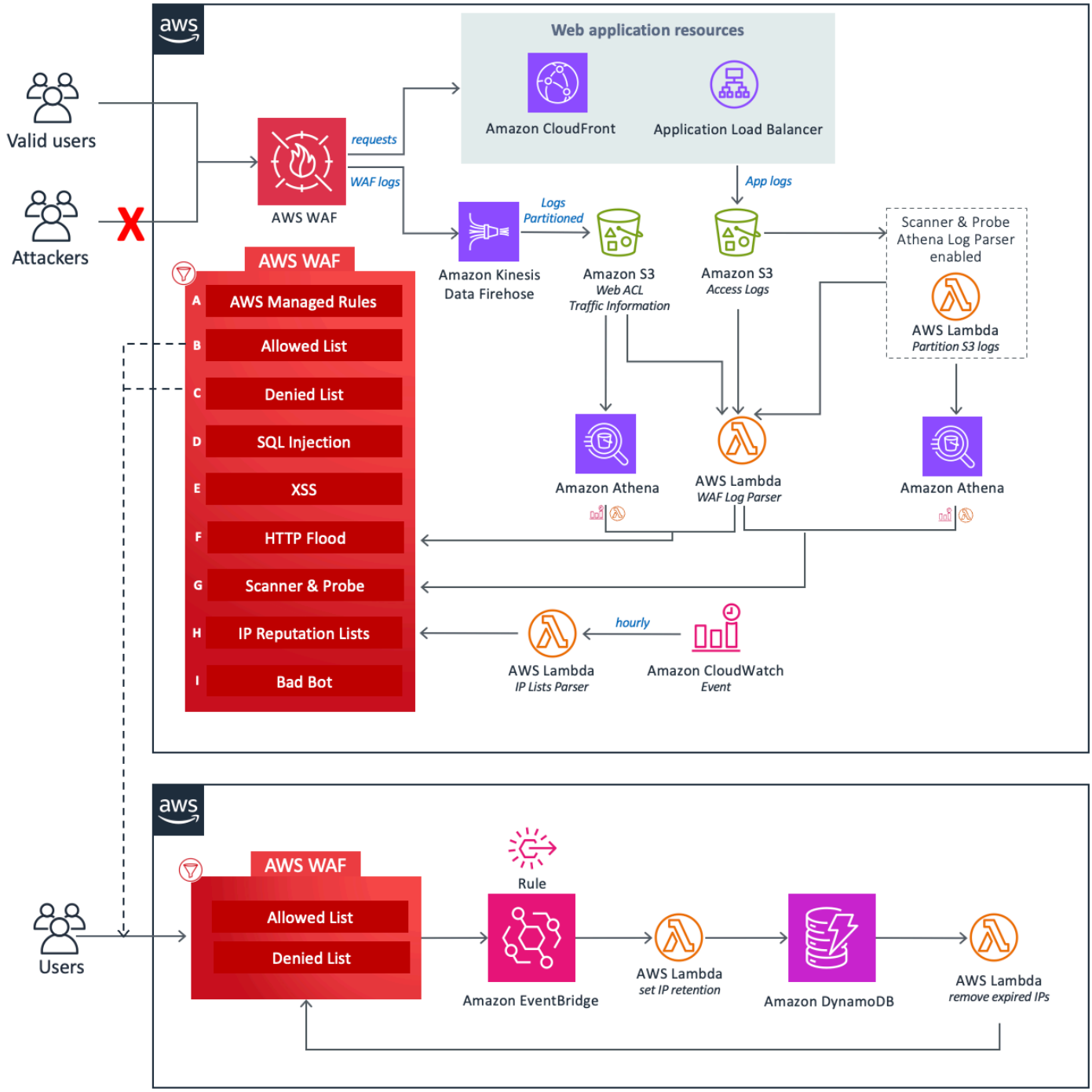
架構概觀

本節提供使用此解決方案所部署元件的參考實作架構圖。

架構圖

使用預設參數部署此解決方案會在您的 AWS 帳戶中部署下列元件。

CloudFormation 範本會部署 AWS WAF 和其他 AWS 資源，以保護 Web 應用程式免受常見攻擊。



設計的核心是 AWS WAF Web ACL，可做為 Web 應用程式所有傳入請求的中央檢查和決策點。在 CloudFormation 堆疊的初始組態期間，使用者定義要啟用哪些保護元件。每個元件都會獨立運作，並將不同的規則新增至 Web ACL。

此解決方案的元件可以分組到下列保護區域。

> **Note**
>
> 群組標籤不會反映 WAF 規則的優先順序層級。

- AWS 受管規則 (A) - 此元件包含 AWS 受管規則 IP 評價規則群組、基準規則群組和使用案例特定規則群組。這些規則群組可防止利用常見的應用程式漏洞或其他不需要的流量，包括 OWASP 出版物中所述的流量，而不必撰寫自己的規則。
- 手動 IP 清單 (B 和 C) - 這些元件會建立兩個 AWS WAF 規則。透過這些規則，您可以手動插入要允許或拒絕的 IP 地址。您可以使用 Amazon EventBridge 規則和 Amazon DynamoDB，在允許或拒絕的 IP 集上設定 IP 保留並移除過期的 IP 地址。如需詳細資訊，請參閱在允許和拒絕的 AWS WAF IP 集上設定 IP 保留。
- SQL Injection (D) 和 XSS (E) - 這些元件會設定兩個 AWS WAF 規則，這些規則旨在防止 URI、查詢字串或請求內文中的常見 SQL Injection 或跨網站指令碼 (XSS) 模式。
- HTTP 洪水 (F) - 此元件可防止來自特定 IP 地址的大量請求組成的攻擊，例如 Web 層 DDoS 攻擊或暴力登入嘗試。透過此規則，您可以設定配額，定義預設五分鐘期間內允許從單一 IP 地址傳入的請求數量上限（可使用 Athena Query Run Time Schedule 參數設定）。超過此閾值後，會暫時封鎖來自 IP 地址的其他請求。您可以使用 AWS WAF 速率型規則，或使用 Lambda 函數或 Athena 查詢處理 AWS WAF 日誌，來實作此規則。如需 HTTP 洪水緩解選項相關權衡的詳細資訊，請參閱日誌剖析器選項。
- 掃描器和探查 (G) - 此元件會剖析搜尋可疑行為的應用程式存取日誌，例如原始伺服器產生的異常錯誤量。然後，它會在客戶定義的期間內封鎖這些可疑來源 IP 地址。您可以使用 Lambda 函數或 Athena 查詢實作此規則。如需掃描器和探查緩解選項相關權衡的詳細資訊，請參閱日誌剖析器選項。
- IP 評價清單 (H) - 此元件是 `IP Lists Parser` Lambda 函數，可每小時檢查第三方 IP 評價清單，以封鎖新範圍。這些清單包括 Spamhaus 不路由或對等 (DROP) 和延伸 DROP (EDROP) 清單、Proofpoint 潛在威脅 IP 清單，以及 Tor 結束節點清單。
- 錯誤機器人 (I) - 除了 Honeypot 機制之外，此元件還可以監控 Application Load Balancer (ALB) 或 Amazon CloudFront 的直接連線，藉此增強錯誤的機器人偵測。如果機器人繞過 Honeypot 並嘗試與 ALB 或 CloudFront 互動，系統會分析請求模式和日誌，以識別惡意活動。偵測到錯誤的機器人時，會擷取其 IP 地址並新增至 AWS WAF 封鎖清單，以防止進一步存取。錯誤的機器人偵測會透過結構化邏輯鏈運作，以確保全面的威脅涵蓋範圍：
  - HTTP 洪水防護 Lambda 日誌剖析器 – 在洪水分析期間從日誌項目收集錯誤的機器人 IPs。
  - 掃描器和探查保護 Lambda 日誌剖析器 – 從掃描器相關的日誌項目識別錯誤的機器人 IPs。

- HTTP 洪水防護 Athena 日誌剖析器 – 使用跨查詢執行的分割區，從 Athena 日誌擷取錯誤的機器人 IPs。
- 掃描器和探查保護 Athena 日誌剖析器 – 使用相同的分割策略，從掃描器相關的 Athena 日誌擷取錯誤的機器人 IPs。
- 備用偵測 – 如果同時停用 HTTP 洪水防護和掃描器與探查防護，系統會依賴 Log Lambda 剖析器，該剖析器會根據 WAF 標籤篩選條件記錄機器人活動。

此解決方案中的三個自訂 Lambda 函數都會將執行時間指標發佈至 CloudWatch。如需這些 Lambda 函數的詳細資訊，請參閱元件詳細資訊。

AWS Well-Architected 設計考量事項

此解決方案使用 AWS Well-Architected Framework 的最佳實務，協助客戶在雲端設計和操作可靠、安全、有效率且符合成本效益的工作負載。

本節說明 Well-Architected Framework 的設計原則和最佳實務如何讓此解決方案受益。

卓越營運

本節說明如何使用卓越營運支柱的原則和最佳實務來建構此解決方案。

- 解決方案會將指標推送至 CloudWatch，以提供可觀測性的基礎設施、Lambda 函數、Amazon Data Firehose、Amazon S3 儲存貯體和其餘解決方案元件。
- 我們透過 AWS 持續整合和持續交付 (CI/CD) 管道來開發、測試和發佈解決方案。這有助於開發人員一致地達到高品質的結果。
- 您可以使用 CloudFormation 範本安裝解決方案，該範本會佈建您帳戶中所有必要的資源。若要更新或刪除解決方案，您只需要更新或刪除範本。

安全

本節說明如何使用安全支柱的原則和最佳實務來建構此解決方案。

- 所有服務間通訊都使用 AWS Identity and Access Management (IAM) 角色。
- 解決方案使用的所有角色都遵循最低權限存取。換句話說，它們只包含所需的最低許可，以便服務可以正常運作。
- 所有資料儲存，包括 Amazon S3 儲存貯體和 DynamoDB，都會進行靜態加密。

可靠性

本節說明如何使用可靠性支柱的原則和最佳實務來建構此解決方案。

- 解決方案會盡可能使用 AWS 無伺服器服務 （例如 Lambda、Firehose、Amazon S3 和 Athena），以確保高可用性並從服務故障中復原。
- 我們會對解決方案執行自動化測試，以快速偵測和修正錯誤。
- 解決方案使用 Lambda 函數進行資料處理。解決方案會將資料存放在 Amazon S3 和 DynamoDB 中，而且預設會保留在多個 Avaialbility 區域中。

效能效率

本節說明如何使用效能效率支柱的原則和最佳實務來建構此解決方案。

- 解決方案使用無伺服器架構，以降低成本來確保高可擴展性和可用性。
- 該解決方案透過剖析資料和最佳化查詢來增強資料庫效能，以減少資料掃描量並實現更快的結果。
- 每天都會自動測試和部署解決方案。我們的解決方案架構師和主題專家會審查要實驗和改進的領域解決方案。

成本最佳化

本節說明如何使用成本最佳化支柱的原則和最佳實務來建構此解決方案。

- 解決方案使用無伺服器架構，客戶只需為其使用量付費。
- 解決方案的運算層預設為使用pay-per-use模型的 Lambda。
- Athena 資料庫和查詢經過最佳化，可減少資料掃描量，進而降低成本。

永續性

本節說明如何使用永續性支柱的原則和最佳實務來建構此解決方案。

- 解決方案使用 受管和無伺服器服務，將後端服務對環境的影響降至最低。
- 解決方案的無伺服器設計旨在減少與持續操作現場部署伺服器的碳足跡相比的碳足跡。

架構詳細資訊

本節說明構成此解決方案的元件和 AWS 服務，以及這些元件如何一起運作的架構詳細資訊。

此解決方案中的 AWS 服務

AWS 服務	描述
AWS WAF	核心。部署 AWS WAF Web ACL、AWS 受管規則規則群組、自訂規則和 IP 集。進行 AWS WAF API 呼叫，以封鎖常見的攻擊和安全的 Web 應用程式。
Amazon Data Firehose	核心。將 AWS WAF 日誌交付至 Amazon S3 儲存貯體。
Amazon Simple Storage Service (Amazon S3)	核心。存放 AWS WAF、CloudFront 和 ALB 日誌。
AWS Lambda	核心。部署多個 Lambda 函數以支援自訂規則。
Amazon EventBridge	核心。建立事件規則以叫用 Lambda。
Amazon Athena	支援。建立 Athena 查詢和工作群組以支援 Athena 日誌剖析器。
AWS Glue	支援。建立資料庫和資料表以支援 Athena 日誌剖析器。
Amazon SNS	支援。傳送 Amazon Simple Notification Service (Amazon SNS) 電子郵件通知，以支援允許和拒絕清單上的 IP 保留。
AWS Systems Manager	支援。提供資源操作和成本資料的應用程式層級資源監控和視覺化。

日誌剖析器選項

如架構概觀中所述，有三個選項可處理 HTTP 洪水、掃描器和探查保護。以下各節會更詳細地說明這些選項。

AWS WAF 速率型規則

速率型規則可用於 HTTP 洪水防護。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。此解決方案可讓您指定用戶端 IP 在五分鐘期間內允許的 Web 請求數量，此請求會持續更新。如果 IP 地址違反設定的配額，AWS WAF 會封鎖封鎖的新請求，直到請求率低於設定的配額為止。

如果請求配額超過每五分鐘 2，000 個請求，而且您不需要實作自訂，建議您選取以速率為基礎的規則選項。例如，計數請求時，您不考慮靜態資源存取。

您可以進一步設定規則，以使用各種其他彙總金鑰和金鑰組合。如需詳細資訊，請參閱彙總選項和金鑰。

Amazon Athena 日誌剖析器

HTTP 洪水防護和掃描器和探查防護範本參數都提供 Athena 日誌剖析器選項。啟用時，CloudFormation 會佈建 Athena 查詢和排程 Lambda 函數，負責協調 Athena 執行、處理結果輸出和更新 AWS WAF。設定為每五分鐘執行一次的 CloudWatch 事件會叫用此 Lambda 函數。您可以使用 Athena Query Run Time Schedule 參數來設定。

當您無法使用 AWS WAF 速率型規則且熟悉 SQL 來實作自訂時，建議您選取此選項。如需如何變更預設查詢的詳細資訊，請參閱檢視 Amazon Athena 查詢。

HTTP 洪水防護是以 AWS WAF 存取日誌處理為基礎，並使用 WAF 日誌檔案。WAF 存取日誌類型具有較低的延遲時間，相較於 CloudFront 或 ALB 日誌交付時間，您可以使用它更快地識別 HTTP 洪水來源。不過，您必須在啟動掃描器和探查保護範本參數中選取 CloudFront 或 ALB 日誌類型，才能接收回應狀態碼。

> **Note**
>
> 如果惡意機器人繞過 Honeypot 並直接與 ALB 或 CloudFront 互動，則系統會透過日誌分析偵測惡意行為，除非 HTTP 洪水防護和掃描器和探查保護都未使用 Lambda 日誌剖析器。

AWS Lambda 日誌剖析器

HTTP 洪水防護和掃描器與探查防護範本參數提供 AWS Lambda Log Parser 選項。只有在無法使用 AWS WAF 速率型規則和 Amazon Athena 日誌剖析器選項時，才能使用 Lambda 日誌剖析器。此選項的已知限制是在正在處理的檔案內容中處理資訊。例如，IP 可能會產生比定義配額更多的請求或錯誤，但由於此資訊會分割成不同的檔案，因此每個檔案不會儲存足夠的資料來超過配額。

> **Note**
>
> 此外，如果惡意機器人繞過 Honeypot 並直接與 ALB 或 CloudFront 互動，偵測會依賴所選的日誌剖析器選項來有效識別和封鎖惡意活動。

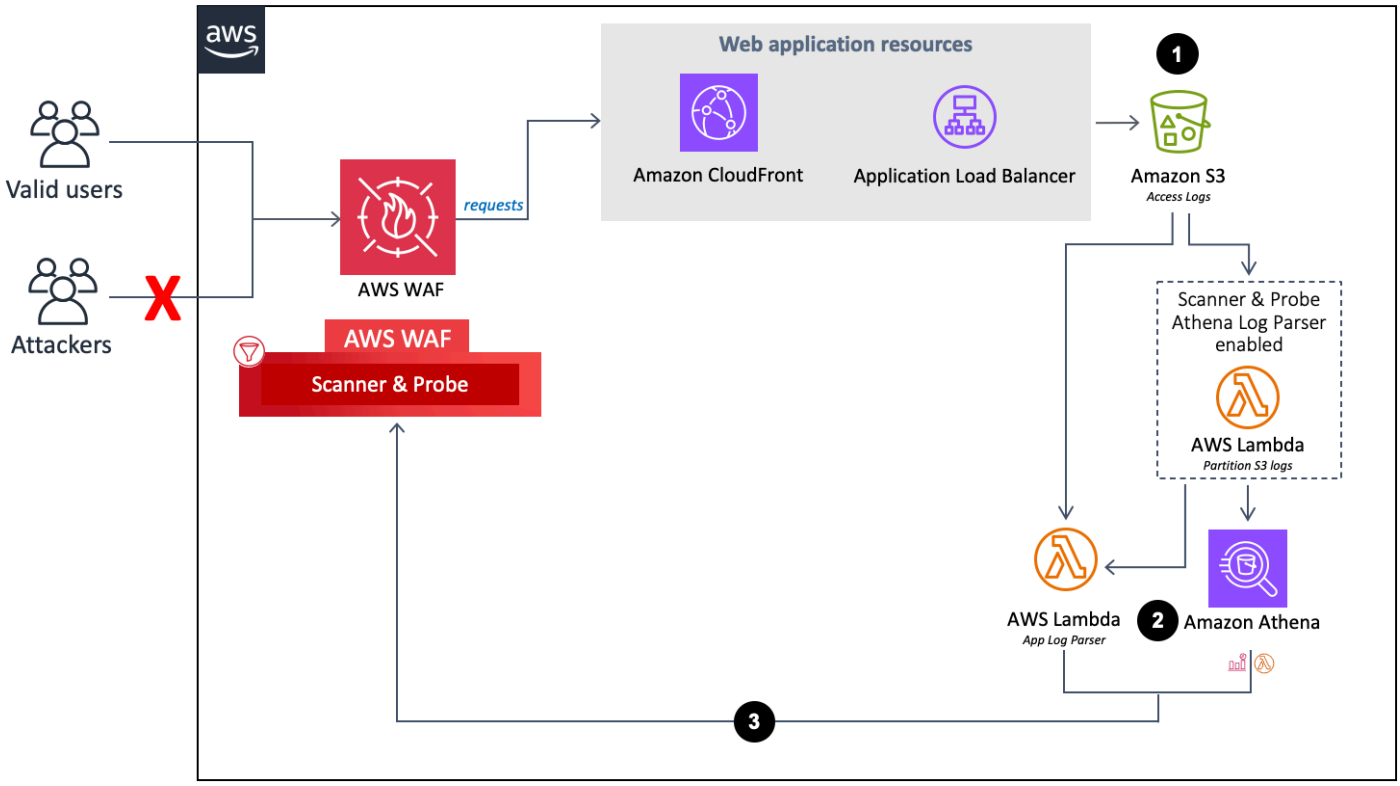
元件詳細資訊

如架構圖所述，此解決方案的四個元件會使用自動化來檢查 IP 地址，並將其新增至 AWS WAF 區塊清單。以下各節會更詳細地說明這些元件。

日誌剖析器 - 應用程式

應用程式日誌剖析器有助於防止掃描器和探查。

應用程式日誌剖析器流程。



1. 當 CloudFront 或 ALB 代表您的 Web 應用程式接收請求時，它會將存取日誌傳送至 Amazon S3 儲存貯體。

   a. （選用）如果您`Yes - Amazon Athena log parser`為範本參數選取 啟用 HTTP 洪水保護和啟用掃描器和探查保護，Lambda 函數會在存取日誌到達 Amazon S3 時，從其原始資料夾 *<customer-bucket>* /AWSLogs 移至新分割的資料夾 *<customer-bucket>* /AWSLogs-partitioned/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* /day= *<DD>* /hour= *<HH>*/。

   b. （選用）如果您`yes`選取在原始 S3 位置範本參數中保留資料，日誌會保留在其原始位置，並複製到其分割資料夾，複製您的日誌儲存體。

   > **Note**
   >
   > 對於 Athena 日誌剖析器，此解決方案只會在您部署此解決方案之後，分割抵達 Amazon S3 儲存貯體的新日誌。如果您有要分割的現有日誌，您必須在部署此解決方案之後，手動將這些日誌上傳至 Amazon S3。

2. 根據您對範本參數的選擇，啟用 HTTP 洪水防護和啟用掃描器與探查防護，此解決方案會使用下列其中一項處理日誌：

a. Lambda - 每次將新的存取日誌存放在 Amazon S3 儲存貯體時，就會啟動 Log Parser Lambda 函數。

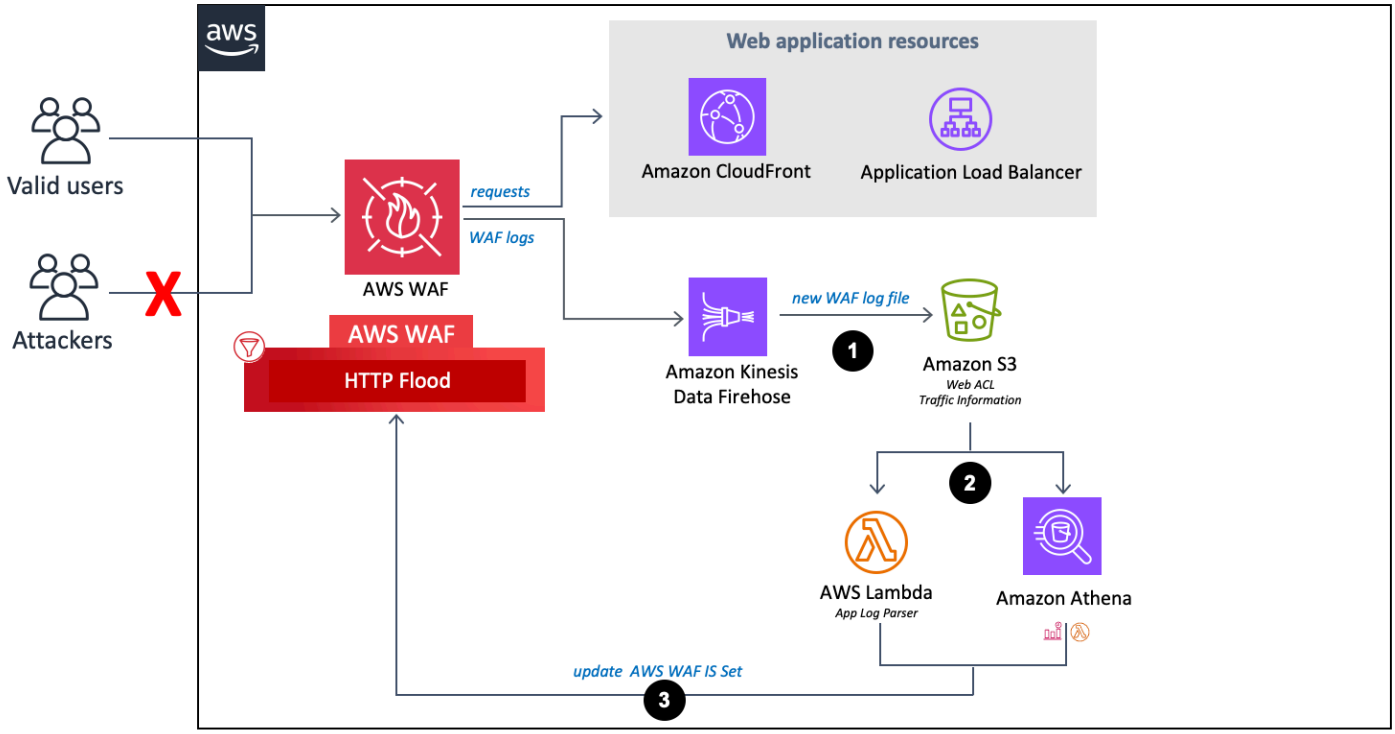
b. Athena - 根據預設，掃描器和探查保護 Athena 查詢每五分鐘執行一次，輸出會推送到 AWS WAF。此程序是由 CloudWatch 事件啟動，這會啟動負責執行 Athena 查詢的 Lambda 函數，並將結果推送至 AWS WAF。

3. 解決方案會分析日誌資料，以識別產生比定義配額更多錯誤的 IP 地址。解決方案接著會更新 AWS WAF IP 集合條件，在客戶定義的期間內封鎖這些 IP 地址。

日誌剖析器 - AWS WAF

如果您yes - Amazon Athena log parser為啟用 HTTP 洪水防護選取 yes - AWS Lambda log parser或 ，此解決方案會佈建下列元件，以剖析 AWS WAF 日誌來識別和封鎖以大於您定義配額的請求率洪水端點的原始伺服器。

AWS WAF 日誌剖析器流程。



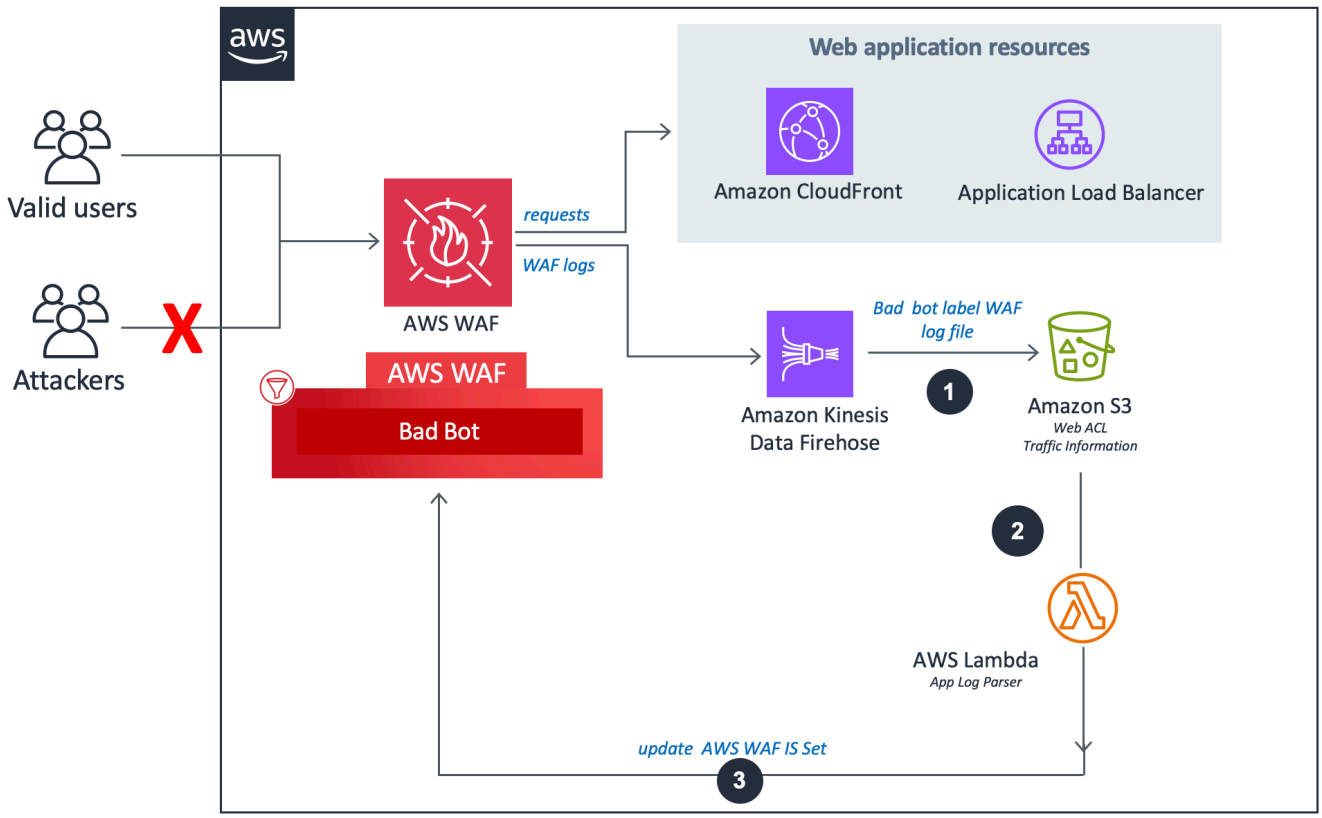
1. 當 AWS WAF 收到存取日誌時，會將日誌傳送至 Firehose 端點。接著 Firehose 會將日誌交付至 Amazon S3 中名為 *<customer-bucket>* /AWSLogs/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* /day= *<DD>* /hour= *<HH>* 的分割儲存貯體 /

2. 根據您對範本參數的選擇，啟用 HTTP 洪水防護和啟用掃描器與探查防護，此解決方案會使用下列其中一項處理日誌：
   a. Lambda：每次新的存取日誌存放在 Amazon S3 儲存貯體時，就會啟動 `Log Parser` Lambda 函數。
   b. Athena：根據預設，每五分鐘會執行掃描器和探查 Athena 查詢，並將輸出推送至 AWS WAF。此程序是由 Amazon CloudWatch 事件啟動，然後啟動負責執行 Amazon Athena 查詢的 Lambda 函數，並將結果推送到 AWS WAF。
3. 解決方案會分析日誌資料，以識別傳送的請求超過定義配額的 IP 地址。解決方案接著會更新 AWS WAF IP 集合條件，在客戶定義的期間內封鎖這些 IP 地址。

日誌剖析器 - 錯誤的機器人

錯誤的機器人日誌剖析器會檢查對 Honeypot 端點的請求，以擷取其來源 IP 地址。

錯誤的機器人日誌剖析器流程。



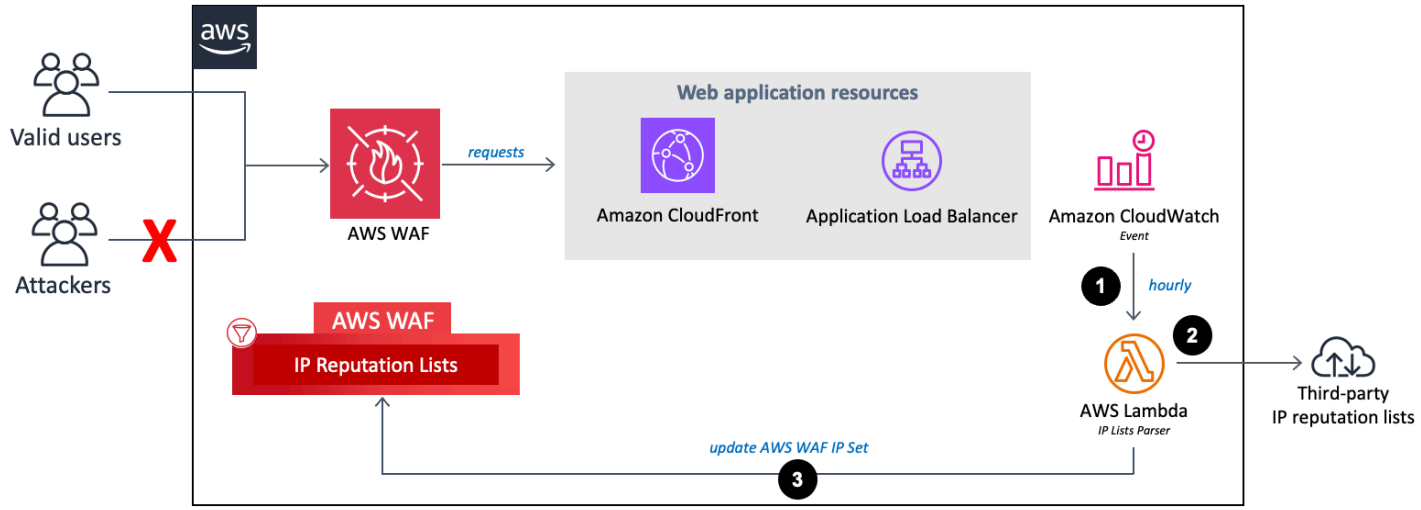
1. 如果 `Bad Bot Protection` 已啟用，且同時停用 HTTP 洪水防護和掃描器與探查防護功能：系統會使用 Log Lambda 剖析器，該剖析器只會根據 WAF 標籤篩選條件記錄錯誤的機器人請求。

2. Lambda 函數會攔截和檢查請求標頭，以擷取存取陷阱端點之來源的 IP 地址。
3. 解決方案會分析日誌資料，以識別傳送的請求超過定義配額的 IP 地址。解決方案接著會更新 AWS WAF IP 集合條件，在客戶定義的期間內封鎖這些 IP 地址。

IP 清單剖析器

`IP Lists Parser` Lambda 函數有助於防範第三方 IP 評價清單中識別的已知攻擊者。

IP 運算會列出剖析器流程。



1. 每小時 Amazon CloudWatch 事件會叫用 `IP Lists Parser` Lambda 函數。
2. Lambda 函數會從三個來源收集和剖析資料：
   - Spamhaus DROP 和 EDROP 清單
   - Proofpoint 新興威脅 IP 清單
   - Tor 結束節點清單
3. Lambda 函數會使用目前的 IP 地址更新 AWS WAF 封鎖清單。

規劃您的部署

本節說明部署解決方案之前的成本、安全性、配額和其他考量事項。

支援的 AWS 區域

根據您定義的範本輸入參數值，此解決方案需要不同的資源。這些資源（列於下表）可能無法在所有 AWS 區域使用。因此，您必須在提供這些服務的 AWS 區域中啟動此解決方案。如需各區域 AWS 服務的最新可用性，請參閱 AWS 區域服務清單。

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
端點類型				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
啟用 HTTP 洪水防護				
是 - AWS Lambda 日誌剖析器				✓
是 - Amazon Athena 日誌剖析器		✓	✓	✓
啟用掃描器和探查保護				
是 - Amazon Athena 日誌剖析器		✓	✓	

> **Note**
>
> 如果您選擇 CloudFront做為端點，則必須在美國東部 （維吉尼亞北部） 區域 () 部署解決方案us-east-1。

成本

您需負責支付執行 Security Automations for AWS WAF 解決方案時所使用的 AWS 服務成本。執行此解決方案的總成本取決於啟用的保護，以及擷取、儲存和處理的資料量。

我們建議您透過 AWS Cost Explorer 建立預算，以協助管理成本。如需完整詳細資訊，請參閱您在此解決方案中使用的每個 AWS 服務的定價網頁。

下表是在美國東部 （維吉尼亞北部） 區域 （不包括 AWS 免費方案） 執行此解決方案的成本明細範例。價格可能變動。

範例 1：啟用評價清單保護、無效的機器人保護、用於 HTTP 洪水保護的 AWS Lambda 日誌剖析器，以及掃描器和探查保護

AWS 服務	每月維度	成本 【美元】
Amazon Data Firehose	100 GB	~$2.90
Amazon S3	100 GB	~$2.30
AWS Lambda	128 MB：3 個函數、1M 調用，以及每個 Lambda 執行的平均 500 毫秒持續時間 512 MB：2 個函數、1M 調用，以及每個 Lambda 執行的平均 500 毫秒持續時間	~5.40 美元
AWS WAF Web ACL	1	5.00 美元
AWS WAF 規則	4	4.00 美元
AWS WAF 請求	1M	0.60 美元

AWS 服務	每月維度	成本 【美元】
總計		每月 ~20.60 美元

範例 2：啟用評價清單保護、錯誤機器人保護、用於 HTTP 洪水保護的 Amazon Athena 日誌剖析器，以及掃描器和探查保護

AWS 服務	每月維度	成本 【美元】
Amazon Data Firehose	100 GB	~$2.90
Amazon S3	100 GB	~$2.30
AWS Lambda	128 MB：3 個函數、1M 調用，以及每個 Lambda 執行的平均 500 毫秒持續時間 512 MB：2 個函數、7560 個叫用，以及每個 Lambda 執行的平均 500 毫秒持續時間	~1.26 美元
Amazon Athena	每天 120 萬個 CloudFront 物件命中或 120 萬個 ALB 請求，每個命中或請求產生約 500 個位元組的日誌記錄	~4.32 美元
AWS WAF Web ACL	1	5.00 美元
AWS WAF 規則	4	4.00 美元
AWS WAF 請求	1M	0.60 美元
總計		每月 ~20.38 美元

範例 3：為允許和拒絕的 IP 集啟用 IP 保留

AWS 服務	每月維度	成本 【美元】
Amazon DynamoDB	1K 寫入和 1 MB 資料儲存	~$0.00
AWS Lambda	128 MB：1 個函數、2K 調用，以及每個 Lambda 執行的平均 500 毫秒持續時間 512 MB：1 個函數、2K 調用，以及每個 Lambda 執行的平均 500 毫秒持續時間	~$0.01
Amazon CloudWatch	2K 事件	~$0.00
AWS WAF Web ACL	1	5.00 美元
AWS WAF 規則	2	2.00 美元
WAS WAF 請求	1M	0.60 美元
總計		每月 ~$7.61

CloudWatch 日誌的成本估算

此解決方案中使用的某些 AWS 服務，例如 Lambda，會產生 CloudWatch 日誌。這些日誌會產生費用。建議您刪除或封存日誌，以降低成本。如需日誌封存詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的將日誌資料匯出至 Amazon S3。 Amazon CloudWatch

如果您選擇在安裝時使用 Athena 日誌剖析器，此解決方案會排程查詢，以針對 Amazon S3 儲存貯體（如設定）中的 AWS WAF 或應用程式存取日誌執行。您需要根據每個查詢掃描的資料量付費。解決方案會將分割套用至日誌和查詢，以將成本降至最低。根據預設，解決方案會將應用程式存取日誌從原始 Amazon S3 位置移至分割的資料夾結構。您也可以保留原始日誌，但您需要支付重複日誌儲存的費用。此解決方案使用工作群組來分割工作負載，而且您可以同時設定 來管理查詢存取和成本。如需成本估算計算範例，請參閱 Athena 的成本估算。如需詳細資訊，請參閱 Amazon Athena 定價。

Athena 的成本估算

如果您在執行 HTTP 洪水保護、掃描器和探查保護或不良的機器人保護規則時使用 Athena 日誌剖析器選項，您將需要支付 Athena 用量的費用。根據預設，每個 Athena 查詢每五分鐘執行一次，並掃描

過去四小時的資料。解決方案會將分割套用至日誌和 Athena 查詢，以將成本降至最低。您可以變更 WAF Block Period 範本參數的值，以設定查詢掃描的資料時數。不過，增加掃描的資料量可能會增加 Athena 成本。

> **Tip**
>
> 以下是 CloudFront 記錄成本計算的範例：
> 平均而言，每個 CloudFront 命中項目可能會產生大約 500 個位元組的資料。
> 如果每天有 120 萬個 CloudFront 物件命中，則每四小時會有 200K (120 萬/6) 個命中，假設以一致速率擷取資料。計算成本時，請考慮您的實際流量模式。
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena 收取每掃描 TB 資料 5.00 USD 的費用。
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Athena 查詢每五分鐘執行一次，即每小時 12 次。
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> 實際成本取決於應用程式的流量模式。如需詳細資訊，請參閱 Amazon Athena 定價。

安全

當您在 AWS 基礎設施上建置系統時，安全責任將由您與 AWS 共同承擔。此共同責任模型可減少您的操作負擔，因為 AWS 會操作、管理和控制元件，包括主機作業系統、虛擬化層，以及服務操作所在設施的實體安全性。如需 AWS 安全性的詳細資訊，請造訪 AWS Cloud Security。

IAM 角色

使用 IAM 角色，您可以將精細存取、政策和許可指派給 AWS 雲端上的服務和使用者。此解決方案會建立具有最低權限的 IAM 角色，而這些角色會將所需的許可授予解決方案的資源。

資料

存放在 Amazon S3 儲存貯體和 DynamoDB 資料表中的所有資料都會進行靜態加密。使用 Firehose 傳輸中的資料也會加密。

保護功能

Web 應用程式容易遭受各種攻擊。這些攻擊包括專門製作的請求，旨在利用漏洞或控制伺服器；旨在截斷網站的容積攻擊；或設計成抓取和竊取 Web 內容的惡意機器人和抓取程式。

此解決方案使用 CloudFormation 設定 AWS WAF 規則，包括 AWS 受管規則規則群組和自訂規則，以封鎖下列常見攻擊：

- AWS 受管規則 - 此受管服務可針對常見的應用程式漏洞或其他不需要的流量提供保護。此解決方案包括 AWS 受管 IP 評價規則群組、AWS 受管基準規則群組和 AWS 受管使用案例特定規則群組。您可以選擇為 Web ACL 選取一或多個規則群組，最高可達 Web ACL 容量單位 (WCU) 配額上限。
- SQL Injection - 攻擊者將惡意 SQL 程式碼插入 Web 請求，以從您的資料庫擷取資料。我們設計此解決方案來封鎖包含潛在惡意 SQL 程式碼的 Web 請求。
- XSS - 攻擊者使用良性網站中的漏洞作為工具，將惡意用戶端網站指令碼注入合法使用者的 Web 瀏覽器。我們設計此項目來檢查傳入請求的常見探索元素，以識別和封鎖 XSS 攻擊。
- HTTP 洪水 - Web 伺服器和其他後端資源面臨 DDoS 攻擊的風險，例如 HTTP 洪水。當用戶端的 Web 請求超過可設定的配額時，此解決方案會自動叫用速率型規則。或者，您可以使用 Lambda 函數或 Athena 查詢處理 AWS WAF 日誌，以強制執行此配額。
- 掃描器和探查 - 透過傳送一系列產生 HTTP 4xx 錯誤碼的請求，惡意來源會掃描並探查面向網際網路的 Web 應用程式是否有漏洞。您可以使用此歷史記錄來協助識別和封鎖惡意來源 IP 地址。此解決方案會建立 Lambda 函數或 Athena 查詢，自動剖析 CloudFront 或 ALB 存取日誌、計算每分鐘來自唯一來源 IP 地址的錯誤請求數，以及更新 AWS WAF 以封鎖來自達到定義錯誤配額之地址的進一步掃描。
- 已知攻擊者來源 (IP 評價清單） – 許多組織會維護已知攻擊者操作的 IP 地址評價清單，例如垃圾郵件傳送者、惡意軟體發行者和殭屍網路。此解決方案會利用這些評價清單中的資訊，協助您封鎖來自惡意 IP 地址的請求。此外，此解決方案會根據 Amazon 內部威脅情報封鎖 IP 評價規則群組識別的攻擊者。
- 機器人和抓取器 - 可公開存取 Web 應用程式的運算子需要信任存取其內容的用戶端可以準確識別自己的身分，並按預期使用 服務。不過，某些自動化用戶端，例如內容抓取器或惡意機器人，會錯誤地表示自己繞過限制。此解決方案可協助您識別和封鎖惡意機器人和抓取器。

配額

服務配額 (也稱為限制) 是您 AWS 帳戶的服務資源或操作數目最大值。

此解決方案中 AWS 服務的配額

請確定您為此解決方案中實作的每個服務有足夠的配額。如需詳細資訊，請參閱 AWS 服務配額。若要在不切換頁面的情況下查看文件中所有 AWS 服務的服務配額，請改為在 PDF 的服務端點和配額頁面中檢視資訊。

AWS WAF 配額

每個 IP 比對條件的無類別網域間路由 (CIDR) 表示法中，AWS WAF 最多可封鎖 10，000 個 IP 地址範圍。此解決方案建立的每個清單都受限於此配額。如需詳細資訊，請參閱 AWS WAF 配額。從 3.0 版開始，此解決方案會建立兩個要連接到每個規則的 IP 集，一個用於 IPv4，另一個用於 IPv6。

AWS WAF 允許每個帳戶、每個 AWS 區域每秒最多一個請求，以對任何個別 `Create`、 `Put`或 `Update`動作進行 API 呼叫。如果您在解決方案之外進行這些 API 呼叫，您可能會遇到 API 限流問題。為了避免此問題，建議您避免在部署此解決方案的相同帳戶和區域中執行其他應用程式，以發出這些 API 呼叫。

部署考量

下列各節提供實作此解決方案的限制條件和考量事項。

AWS WAF 規則

此解決方案產生的 Web ACL 旨在為 Web 應用程式提供全面的保護。解決方案提供一組 AWS 受管規則和自訂規則，您可以將這些規則新增至 Web ACL。若要包含規則，請在啟動 CloudFormation 堆疊時`yes`為相關參數選擇 。請參閱步驟 1。啟動 堆疊以取得參數清單。

> **Note**
>
> out-of-box解決方案不支援 AWS Firewall Manager。如果您想要在 Firewall Manager 中使用規則，建議您將自訂套用至其原始程式碼。

Web ACL 流量記錄

如果您在美國東部 （維吉尼亞北部） 以外的 AWS 區域中建立堆疊，並將端點設定為 `CloudFront`，則必須將啟用 HTTP 洪水防護設定為 `no`或 `yes - AWS WAF rate based rule`。

其他兩個選項 (`yes - AWS Lambda log parser` 和 `yes - Amazon Athena log parser`) 需要在在所有 AWS 節點中執行的 Web ACL 上啟用 AWS WAF 日誌，而且在美國東部（維吉尼亞北部）以外不支援此功能。如需記錄 Web ACL 流量的詳細資訊，請參閱 AWS WAF 開發人員指南。

請求元件的超大處理

AWS WAF 不支援檢查 Web 請求元件內文、標頭或 Cookie 的過大內容。當您撰寫規則陳述式來檢查其中一個請求元件類型時，您可以選擇其中一個選項，告訴 AWS WAF 如何處理這些請求：

- `yes`（繼續）- 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。這是解決方案中使用的預設選項。
- `yes - MATCH` - 將 Web 請求視為與規則陳述式相符。AWS WAF 會將規則動作套用至請求，而不根據規則的檢查條件進行評估。對於具有 `Block`動作的規則，這會使用過大元件封鎖請求。
- `yes - 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條件進行評估。AWS WAF 會使用 Web ACL 中的其餘規則繼續檢查 Web 請求，就像使用任何不相符的規則一樣。

如需詳細資訊，請參閱在 AWS WAF 中處理過大 Web 請求元件。

多個解決方案部署

您可以在相同的帳戶和區域中多次部署解決方案。您必須為每個部署使用唯一的 CloudFormation 堆疊名稱和 Amazon S3 儲存貯體名稱。每個唯一部署都會產生額外費用，並受到每個區域每個帳戶的 AWS WAF 配額限制。

部署的最低角色許可（選用）

客戶可以手動建立具有部署所需最低許可的 IAM 角色：

- WAF 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:UpdateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:GetWebACL",
                "wafv2:ListWebACLs",
```

```
                "wafv2:CreateIPSet",
                "wafv2:UpdateIPSet",
                "wafv2:DeleteIPSet",
                "wafv2:GetIPSet",
                "wafv2:AssociateWebACL",
                "wafv2:DisassociateWebACL",
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration",
                "wafv2:ListWebACLs",
                "wafv2:ListIPSets",
                "wafv2:ListTagsForResource"
            ],
            "Resource": [
                "arn:aws:wafv2:*:*:regional/webacl/*",
                "arn:aws:wafv2:*:*:regional/ipset/*",
                "arn:aws:wafv2:*:*:global/webacl/*",
                "arn:aws:wafv2:*:*:global/ipset/*"
            ]
        }
```

- Lambda 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*"
        }
```

- Firehose 許可

```
        {
```

```
            "Effect": "Allow",
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- S3 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:PutBucketLogging",
                "s3:GetBucketLogging"
            ],
            "Resource": "arn:aws:s3:::*"
        }
```

- Athena 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "athena:CreateWorkGroup",
                "athena:DeleteWorkGroup",
                "athena:GetWorkGroup",
                "athena:UpdateWorkGroup",
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution"
            ],
            "Resource": "arn:aws:athena:*:*:workgroup/WAF*"
        }
```

- Glue 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch Logs 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream",
                "logs:PutRetentionPolicy",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/*",
                "arn:aws:logs:*:*:log-group:*",
                "arn:aws:logs:*:*:log-group:/aws/kinesisfirehose/*"
            ]
        }
```

- CloudWatch 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DeleteDashboards",
                "cloudwatch:GetDashboard",
                "cloudwatch:ListDashboards",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        }
```

- SNS 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:Subscribe",
```

```
                "sns:Unsubscribe",
                "sns:SetTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*"
        }
```

- DynamoDB 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeTable",
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/*"
        }
```

- CloudFormation 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "cloudformation:ListStacks"
            ],
            "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
        }
```

- Service Catalog 應用程式登錄檔許可

```
        {
```

```
            "Effect": "Allow",
            "Action": [
                "servicecatalog:CreateApplication",
                "servicecatalog:DeleteApplication",
                "servicecatalog:GetApplication",
                "servicecatalog:TagResource",
                "servicecatalog:CreateAttributeGroup",
                "servicecatalog:DeleteAttributeGroup",
                "servicecatalog:GetAttributeGroup",
                "servicecatalog:AssociateAttributeGroup",
                "servicecatalog:DisassociateAttributeGroup",
                "servicecatalog:AssociateResource",
                "servicecatalog:DisassociateResource"
            ],
            "Resource": "arn:aws:servicecatalog:*:*:*"
        }
```

- X-Ray 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords"
            ],
            "Resource": "*"
        }
```

- IAM 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
```

```
                "iam:GetRolePolicy",
                "iam:ListRoles",
                "iam:PassRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/*"
        }
```

- EventBridge 許可

```
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:DescribeRule",
                "events:EnableRule",
                "events:ListRules",
                "events:PutRule",
                "events:DeleteRule",
                "events:ListEventSources",
                "events:DescribeEventSource",
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

部署解決方案

此解決方案使用 AWS CloudFormation 範本和堆疊來自動化其部署。CloudFormation 範本會指定此解決方案中包含的 AWS 資源及其屬性。CloudFormation 堆疊會佈建範本中所述的資源。

部署程序概觀

啟動 CloudFormation 範本之前，請檢閱本指南中討論的架構和組態考量事項。遵循本節中的step-by-step說明，設定解決方案並將其部署到您的帳戶。

部署時間：約 15 分鐘。

> **Note**
>
> 如果您先前已部署此解決方案，請參閱更新解決方案以取得更新指示。

先決條件

- 設定 CloudFront 分佈
- 設定 ALB

步驟 1. 啟動堆疊

- 在您的 AWS 帳戶中啟動 CloudFormation 範本。
- 輸入必要參數的值：堆疊名稱和應用程式存取日誌儲存貯體名稱。
- 檢閱其他範本參數，並視需要調整。

步驟 2. 將 Web ACL 與您的 Web 應用程式建立關聯

- 將您的 CloudFront Web 分佈 (s) 或 ALB (s) 與此解決方案產生的 Web ACL 建立關聯。您可以視需要建立任意數量的分佈或負載平衡器的關聯。

步驟 3. 設定 Web 存取記錄

- 開啟 CloudFront Web 分佈或 ALB (s) 的 Web 存取記錄，並將日誌檔案傳送至適當的 Amazon S3 儲存貯體。將日誌儲存在符合使用者定義字首的資料夾中。如果未使用使用者定義的字首，請將日

誌儲存至 AWSLogs（預設日誌字首 AWSLogs/)。請參閱步驟 1 中的應用程式存取日誌儲存貯體字首參數。 如需詳細資訊，請啟動 堆疊。

AWS CloudFormation 範本

此解決方案包含一個主要 AWS CloudFormation 範本和兩個巢狀範本。您可以在部署解決方案之前下載 CloudFormation 範本。

主要堆疊

View template

aws-waf-security-automations.template - 使用此範本作為在您帳戶中啟動解決方案的進入點。預設組態會使用預先設定的規則部署 AWS WAF Web ACL。您可以根據您的需求自訂範本。

WebACL 堆疊

View template

aws-waf-security-automations-webacl.template - 此巢狀範本佈建 AWS WAF 資源，包括 Web ACL、IP、集合和其他相關資源。

Firehose Athena 堆疊

View template

aws-waf-security-automations-firehose-athena.template - 此巢狀範本會佈建與 AWS Glue、Athena 和 Firehose 相關的資源。當您選擇掃描器和探查 Athena 日誌剖析器或 HTTP Flood Lambda 或 Athena 日誌剖析器時，就會建立它。

> **Note**
>
> AWS CloudFormation 資源是從 AWS 雲端開發套件 (AWS CDK) 建構模組建立。

此 AWS CloudFormation 範本會在 AWS 雲端中部署 AWS WAF 解決方案的安全自動化。

先決條件

此解決方案旨在與使用 CloudFront 或 ALB 部署的 Web 應用程式搭配使用。如果您尚未設定其中一個資源，請先完成適用的任務，再啟動此解決方案。

設定 CloudFront 分佈

完成下列步驟，為您的 Web 應用程式靜態和動態內容設定 CloudFront 分佈。如需詳細說明，請參閱 Amazon CloudFront 開發人員指南。

1. 建立 CloudFront Web 應用程式分佈。請參閱建立分佈。
2. 設定靜態和動態原始伺服器。請參閱搭配 CloudFront 分佈使用各種原始伺服器。
3. 指定分發的行為。請參閱您在建立或更新分佈時指定的值。

> **Note**
>
> 如果您選擇 `CloudFront`做為端點，則必須在美國東部（維吉尼亞北部）區域中建立 WAFV2 資源。

設定 ALB

若要設定 ALB 將傳入流量分配至 Web 應用程式，請參閱《Application Load Balancer 使用者指南》中的建立 Application Load Balancer。

步驟 1. 啟動 堆疊

此自動化 AWS CloudFormation 範本會在 AWS 雲端上部署解決方案。

1. 登入 AWS 管理主控台，然後選取啟動解決方案以啟動 `waf-automation-on-aws.template` CloudFormation 範本。

   Launch solution

2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同的 AWS 區域中啟動此解決方案，請使用主控台導覽列中的區域選擇器。如果您選擇 `CloudFront`做為端點，則必須在美國東部（維吉尼亞北部）(`us-east-1`) 區域部署解決方案。

> **Note**
>
> 根據您定義的輸入參數值，此解決方案需要不同的資源。這些資源目前僅適用於特定 AWS 區域。因此，您必須在提供這些服務的 AWS 區域中啟動此解決方案。如需詳細資訊，請參閱支援的 AWS 區域。

3. 在指定範本頁面上，確認您已選取正確的範本，然後選擇下一步。
4. 在指定堆疊詳細資訊頁面上，在堆疊名稱欄位中將名稱指派給您的 AWS WAF 組態。這也是範本建立的 Web ACL 名稱。
5. 在參數下，檢閱範本的參數並視需要修改。若要選擇退出特定功能，請no視需要選擇 none或 。此解決方案使用下列預設值。

參數	預設	描述
Stack name (堆疊名稱)	`[.red]# < 需要 input>``	堆疊名稱不能包含空格。此名稱在您的 AWS 帳戶中必須是唯一的，並且是範本建立的 Web ACL 名稱。
資源類型		
端點	`CloudFront`	選擇正在使用的資源類型。注意：如果您選擇 `CloudFront` 做為端點，則必須啟動解決方案，在美國東部（維吉尼亞北部）區域 () 建立 WAF 資源`us-east-1` 。
AWS 受管 IP 評價規則群組		
啟用 Amazon IP 評價清單受管規則群組保護	no	選擇`yes`開啟旨在將 Amazon IP 評價清單受管規則群組新增至 Web ACL 的元件。 此規則群組是以 Amazon 內部威脅情報為基礎。如果您想要封鎖通常與機器人或其他威

參數	預設	描述
		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。 所需的 WCU 為 25。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。
啟用匿名 IP 清單受管規則群組保護	no	選擇 yes以開啟旨在將匿名 IP 清單受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖來自允許混淆檢視器身分之服務的請求。這些包括來自 VPN，代理、Tor 節點和託管供應商的請求。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。 所需的 WCU 為 50。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
AWS 受管基準規則群組		
啟用核心規則集受管規則群組保護	no	選擇 yes 以開啟旨在將核心規則集受管規則群組新增至 Web ACL 的元件。 此規則群組提供保護，防止各種漏洞遭到利用，包括一些高風險和經常發生的漏洞。考慮將此規則群組用於任何 AWS WAF 使用案例。 所需的 WCU 為 700。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用管理員保護 受管規則群組保護	no	選擇 yes 以開啟旨在將 Admin Protection Managed Rule Group 新增至 Web ACL 的元件。 此規則群組會封鎖對公開管理頁面的外部存取權。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。 所需的 WCU 為 100。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用已知錯誤輸入受管規則群組保護	no	選擇 yes 以開啟旨在將已知錯誤輸入受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖對公開管理頁面的外部存取權。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。 所需的 WCU 為 100。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。
AWS 受管使用案例特定規則群組		

參數	預設	描述
啟用 SQL Database 受管規則群組保護	no	選擇 yes 以開啟旨在將 SQL 資料庫受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖與利用 SQL 資料庫相關聯的請求模式，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。如果您已啟用 AWS 受管 SQL 規則群組，則可選用 SQL Injection 自訂規則。 所需的 WCU 為 200。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用 Linux 作業系統受管規則群組保護	no	選擇 yes 以開啟旨在將 Linux 作業系統受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖與利用 Linux 特定漏洞相關聯的請求模式，包括 Linux 特定的本機檔案包含 (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。如果您的應用程式有任何部分在 Linux 上執行，請評估此規則群組。您應該將此規則群組與 POSIX 作業系統規則群組搭配使用。 所需的 WCU 為 200。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用 POSIX 作業系統受管規則群組保護	no	選擇 yes 以開啟旨在將核心規則集受管規則群組保護新增至 Web ACL 的元件。 此規則群組會封鎖與利用 POSIX 和類似 POSIX 作業系統特定漏洞相關的請求模式，包括 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 POSIX 或類似 POSIX 的作業系統上執行，請評估此規則群組。 所需的 WCU 為 100。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用 Windows 作業系統受管規則群組保護	no	選擇yes開啟旨在將 Windows 作業系統受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖與利用 Windows 特定漏洞相關聯的請求模式，例如遠端執行 PowerShell 命令。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。 所需的 WCU 為 200。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用 PHP 應用程式受管規則群組保護	no	選擇 yes以開啟旨在將 PHP Application Managed Rule Group 新增至 Web ACL 的元件。 此規則群組會封鎖與利用 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。這有助於防止漏洞遭到利用，允許攻擊者從遠端執行程式碼或未經授權的命令。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。 所需的 WCU 為 100。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。

參數	預設	描述
啟用 WordPress 應用程式受管規則群組保護	no	選擇 yes 以開啟旨在將 WordPress 應用程式受管規則群組新增至 Web ACL 的元件。 此規則群組會封鎖與利用 WordPress 網站特定漏洞相關聯的請求模式。如果您正在執行 WordPress，請評估此規則群組。此規則群組應與 SQL 資料庫和 PHP 應用程式規則群組搭配使用。 所需的 WCU 為 100。您的帳戶應有足夠的 WCU 容量，以避免 Web ACL 堆疊部署因超過容量限制而失敗。 如需詳細資訊，請參閱 AWS 受管規則規則群組清單。
自訂規則 - 掃描器和探查		
啟用掃描器和探查保護	yes - AWS Lambda log parser	選擇用於封鎖掃描器和探查的元件。如需與緩解選項相關的權衡詳細資訊，請參閱日誌剖析器選項。

參數	預設	描述
應用程式存取日誌儲存貯體名稱	[.red]<requires input>	如果您選擇yes啟用掃描器和探查保護參數，請輸入您要存放 CloudFront 分佈（多個）或 ALB（多個）存取日誌的 Amazon S3 儲存貯體名稱（新儲存貯體或現有儲存貯體）。如果您使用的是現有的 Amazon S3 儲存貯體，它必須位於部署 CloudFormation 範本的相同 AWS 區域。您應該為每個解決方案部署使用不同的儲存貯體。 若要停用此保護，請忽略此參數。注意：開啟 CloudFront Web 分佈或 ALB (s) 的 Web 存取記錄，將日誌檔案傳送到此 Amazon S3 儲存貯體。將日誌儲存在堆疊中定義的相同字首（預設字首 AWSLogs/)。如需詳細資訊，請參閱應用程式存取日誌儲存貯體字首參數。

參數	預設	描述
應用程式存取日誌儲存貯體字首	AWSLogs/	如果您選擇yes啟用掃描器和探查保護參數，您可以為上述應用程式存取日誌儲存貯體輸入選用的使用者定義字首。 如果您選擇 CloudFront 端點參數，您可以輸入任何字首，例如 yourprefix/ 。 如果您選擇 ALB端點參數，則必須將 附加AWSLogs/至字首，例如 yourprefix/AWSLogs/ 。 如果沒有使用者定義的字首，請使用 AWSLogs/（預設）。 若要停用此保護，請忽略此參數。
儲存貯體存取記錄是否已開啟？	no	yes 如果為應用程式存取日誌儲存貯體名稱參數輸入現有的 Amazon S3 儲存貯體名稱，且儲存貯體的伺服器存取記錄已開啟，請選擇此選項。 如果您選擇 no，解決方案會開啟儲存貯體的伺服器存取記錄。 如果您選擇no啟用掃描器和探查保護參數，請忽略此參數。

參數	預設	描述
錯誤閾值	50	如果您選擇yes啟用掃描器和探查保護參數，請輸入每個 IP 地址每分鐘可接受的錯誤請求上限。 如果您選擇no啟用掃描器和探查保護參數，請忽略此參數。
將資料保留在原始 S3 位置	no	如果您選擇yes - Amazon Athena log parser啟用掃描器和探查保護參數，解決方案會將分割套用至應用程式存取日誌檔案和 Athena 查詢。根據預設，解決方案會將日誌檔案從原始位置移至 Amazon S3 中的分割資料夾結構。 yes 如果也想要將日誌的副本保留在其原始位置，請選擇 。這將複製您的日誌儲存體。 如果您未yes - Amazon Athena log parser選擇 Activate Scanner & Probe Protection 參數，請忽略此參數。
自訂規則 - HTTP 洪水		
啟用 HTTP 洪水防護	yes - AWS WAF rate-based rule	選取用於封鎖 HTTP 洪水攻擊的元件。如需與緩解選項相關的權衡詳細資訊，請參閱日誌剖析器選項。

參數	預設	描述
預設請求閾值	100	如果您選擇yes啟用 HTTP 洪水防護參數，請輸入每個 IP 地址每五分鐘可接受的請求上限。 如果您選擇yes - AWS WAF rate-based rule 啟用 HTTP 洪水防護參數，則可接受的最小值為 10。 如果您yes - Amazon Athena log parser為啟用 HTTP 洪水防護參數選擇 yes - AWS Lambda log parser或 ，它可以是任何值。 若要停用此保護，請忽略此參數。

參數	預設	描述
依國家/地區請求閾值	< 選用輸入 >	如果您選擇yes - Amazon Athena log parser啟用 HTTP 洪水防護參數，您可以依照此 JSON 格式，依國家/地區輸入閾值{"TR":50, "ER":150} 。解決方案會將這些閾值用於來自指定國家/地區的請求。解決方案會針對剩餘的請求使用預設請求閾值參數。注意：如果您定義此參數，國家/地區將自動包含在 Athena 查詢群組中，以及您可以使用 HTTP 洪水 Athena 查詢參數中的依請求分組選取的 IP 和其他選用分組欄位。 + 如果您選擇停用此保護，請忽略此參數。
HTTP 洪水 Athena 查詢中的依請求分組	None	如果您選擇yes - Amazon Athena log parser啟用 HTTP 洪水防護參數，您可以選擇分組依據欄位來計算每個 IP 和所選分組依據欄位的請求。例如，如果您選擇 URI，解決方案會計算每個 IP 和 URI 的請求。 如果您選擇停用此保護，請忽略此參數。

參數	預設	描述
WAF 區塊期間	240	如果您選擇啟用掃描器和探查保護或啟用 HTTP 洪水保護參數yes - Amazon Athena log parser的 yes - AWS Lambda log parser或 ，請輸入封鎖適用 IP 地址的期間 （以分鐘為單位）。 若要停用日誌剖析，請忽略此參數。
Athena 查詢執行時間排程（分鐘）	5	如果您選擇yes - Amazon Athena log parser啟用掃描器和探查保護或啟用 HTTP 洪水保護參數，則可以輸入執行 Athena 查詢的時間間隔（以分鐘為單位）。根據預設，Athena 查詢每 5 分鐘執行一次。 如果您選擇停用這些保護，請忽略此參數。

參數	預設	描述
規則金鑰	IP	如果您選擇yes - AWS WAF rate-based rule 啟用 HTTP 洪水防護參數，請將此規則設定為使用各種其他彙總金鑰組合。可用選項： IP （預設） IP+自訂標頭 （如果選取此選項，Rule Keys Custom Header則為必要） IP+URI IP+HTTP 方法 如需詳細資訊，請參閱 WAF 規則率型彙總選項。
規則金鑰自訂標頭	no	如果您選擇IP+Custom Header使用 Rule Keys 參數，請輸入要用於請求彙總的自訂標頭名稱。 如需詳細資訊，請參閱 WAF 規則陳述式類型速率型彙總選項。

參數	預設	描述
時段閾值（分鐘）	5	HTTP 洪水防護的時間範圍閾值，以分鐘為單位。適用於以速率為基礎的規則和 lambda 日誌剖析器。可用的選項：【1、2、5、10】。 如果您選擇`yes - AWS WAF rate-based rule` 啟用 HTTP 洪水防護參數，則會用於評估時段。如需詳細資訊，請參閱 WAF Web ACL 速率型陳述式。 如果您選擇`yes - AWS Lambda log parser`啟用 HTTP 洪水防護參數，除了區塊期間之外，還會在評估期間使用 。
自訂規則 - 錯誤的機器人		
啟用無效的機器人保護	`yes`	選擇 `yes`以開啟設計用來封鎖不良機器人和內容抓取器的元件。
有權寫入您帳戶中 CloudWatch 日誌的 IAM 角色 ARN	< 選用輸入 >	提供 IAM 角色的選用 ARN，該角色可寫入您帳戶中的 CloudWatch 日誌。 例如：`ARN: arn:aws:iam::account_id:role/myrolename` 。 如果您將此參數保留空白（預設），解決方案會為您建立新的角色。

參數	預設	描述
自訂規則 - 第三方 IP 評價清單		
啟用評價清單保護	yes	選擇yes封鎖來自第三方評價清單（支援的清單包括 Spamhaus、Emerging Threats 和 Tor exit 節點）上 IP 地址的請求。
舊版自訂規則		

參數	預設	描述
啟用 SQL Injection Protection	yes	選擇 yes以開啟設計用來封鎖常見 SQL Injection 攻擊的元件。如果您未使用 AWS 受管核心規則集或 AWS 受管 SQL 資料庫規則群組，請考慮將其啟用。 您可以選擇其中一個選項 (yes （繼續）yes - MATCH、 或 yes - NO_MATCH)，讓 AWS WAF 處理超過 8 KB (8192 位元組） 的過大請求。根據預設，會根據規則yes檢查條件，檢查大小限制內的請求元件內容。如需詳細資訊，請參閱處理超大 Web 請求元件。 選擇 no以停用此功能。注意：CloudFormation 堆疊會將選取的超大處理選項新增至預設 SQL Injection 保護規則，並將其部署到您的 AWS 帳戶。如果您在 CloudFormation 之外自訂規則，您的變更會在堆疊更新後遭到覆寫。

參數	預設	描述
SQL Injection Protection 的敏感度等級	LOW	選擇您希望 AWS WAF 用來檢查 SQL Injection 攻擊的敏感度等級。 HIGH 偵測到更多攻擊，但可能會產生更多誤報。 對於已有其他 SQL 隱碼攻擊防護能力的資源，或誤判容錯能力較低的資源來說，LOW 通常是更好的選擇。 如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的 AWS WAF 新增 SQL Injection 規則陳述式的敏感度等級和 SensitivityLevel 屬性。 AWS CloudFormation 如果您選擇停用 SQL Injection 保護，請忽略此參數。注意：CloudFormation 堆疊會將選取的敏感度等級新增至預設 SQL Injection 保護規則，並將其部署到您的 AWS 帳戶。如果您在 CloudFormation 之外自訂規則，您的變更會在堆疊更新後遭到覆寫。

參數	預設	描述
啟用跨網站指令碼保護	yes	選擇 yes以開啟設計用來封鎖常見 XSS 攻擊的元件。如果您未使用 AWS 受管核心規則集，請考慮將其啟用。您也可以選取其中一個選項 (yes（繼續）yes - MATCH、 或 yes - NO_MATCH)，讓 AWS WAF 處理超過 8 KB (8192 位元組）的過大請求。根據預設， yes會使用 Continue選項，根據規則檢查條件檢查大小限制內的請求元件內容。如需詳細資訊，請參閱請求元件的超大處理。 選擇 no以停用此功能。注意：CloudFormation 堆疊會將選取的超大處理選項新增至預設的跨網站指令碼規則，並將其部署到您的 AWS 帳戶。如果您在 CloudFormation 之外自訂規則，您的變更會在堆疊更新後遭到覆寫。
允許和拒絕的 IP 保留設定		

參數	預設	描述
允許 IP 集的保留期間（分鐘）	-1	如果您想要啟用允許 IP 集合的 IP 保留，請輸入數字 (15 或更高）做為保留期間（分鐘）。到達保留期的 IP 地址會過期，而解決方案會從 IP 集中移除它們。解決方案支援最短 15 分鐘的保留期。如果您輸入 0和 之間的數字15，解決方案會將其視為 15。 將其保留為 -1（預設）以關閉 IP 保留。
遭拒 IP 集的保留期間（分鐘）	-1	如果您想要啟用已拒絕 IP 集的 IP 保留，請輸入數字 (15 或更高）做為保留期間（分鐘）。到達保留期的 IP 地址會過期，而解決方案會從 IP 集中移除它們。解決方案支援最短 15 分鐘的保留期。如果您輸入 0和 之間的數字15，解決方案會將其視為 15。 將其保留為 -1（預設）以關閉 IP 保留。
允許或拒絕 IP 集過期時接收通知的電子郵件	< 選用輸入 >	如果您啟用 IP 保留期參數（請參閱先前兩個參數），並想要在 IP 地址過期時收到電子郵件通知，請輸入有效的電子郵件地址。 如果您未啟用 IP 保留或想要關閉電子郵件通知，請保留空白（預設）。

參數	預設	描述
進階設定		
日誌群組的保留期間（天數）	365	如果您想要啟用 CloudWatch Log Groups 的保留，請輸入數字 (1 或更高）做為保留期間（天數）。您可以選擇一天 (1) 到十年 () 之間的保留期間3650。根據預設，日誌會在一年後過期。 將其設定為 -1以無限期保留日誌。

6. 選擇下一步。
7. 在設定堆疊選項頁面上，您可以為堆疊中的資源指定標籤（鍵/值對），並設定其他選項。選擇下一步。
8. 在檢閱和建立頁面上，檢閱並確認設定。選取確認範本將建立 IAM 資源和任何其他必要功能的方塊。
9. 選擇提交以部署堆疊。

   在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 15 分鐘內收到 CREATE_COMPLETE 狀態。

> **Note**
>
> 除了 `Log Parser`和 `IP Lists Parser` AWS Lambda 函數之外，此解決方案還包含 `helper`和 `custom-resource` Lambda 函數，這些函數只會在初始組態期間或資源更新或刪除時執行。
> 使用此解決方案時，您會在 AWS Lambda 主控台中看到所有函數，但只有三個主要解決方案函數會定期作用中。請勿刪除其他兩個函數；它們是管理相關聯資源的必要項目。

若要查看堆疊資源的詳細資訊，請選擇輸出索引標籤。這包括 BadBotHoneypotEndpoint 值。請記住此值，因為您會在 Web 應用程式的內嵌 Honeypot 連結中使用它。

步驟 2. 將 Web ACL 與您的 Web 應用程式建立關聯

更新您的 CloudFront 分佈或 ALB(s)，以使用您在步驟 1 中產生的資源來啟用 AWS WAF 和記錄。 啟動堆疊。

1. 登入 AWS WAF 主控台。
2. 選擇您要使用的 Web ACL。
3. 在 Associated AWS resources (關聯的 AWS 資源) 索引標籤上，選擇 Add AWS resources (新增 AWS 資源)。
4. 在資源類型下，選擇 CloudFront 分佈或 ALB。
5. 從清單中選擇資源，然後選擇新增以儲存變更。

步驟 3。設定 web 存取記錄

設定 CloudFront 或 ALB 將 Web 存取日誌傳送至適當的 Amazon S3 儲存貯體，以便此資料可供 Log Parser Lambda 函數使用。

從 CloudFront 分佈存放 Web 存取日誌

1. 登入 Amazon CloudFront 主控台。
2. 選取 Web 應用程式的分佈，然後選擇分佈設定。
3. 在 General (一般) 索引標籤上，選擇 Edit (編輯)。
4. 針對 AWS WAF Web ACL，選擇建立的 Web ACL 解決方案 (堆疊名稱參數）。
5. 對於 Logging (記錄)，選擇 On (開啟)。
6. 針對日誌儲存貯體，選擇您要用於儲存 Web 存取日誌的 S3 儲存貯體。這可以是用於主要堆疊的新或現有 S3 儲存貯體，並具有 CloudFront 寫入日誌的許可。下拉式清單會列舉與目前 AWS 帳戶相關聯的儲存貯體。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的基本 CloudFront 分佈入門。 Amazon CloudFront
7. 將日誌字首設定為用於部署解決方案的字首。您可以在主要堆疊、參數索引標籤、AppAccessLogBucketPrefixParam （預設 `AWSLogs/`) 中找到字首。
8. 選擇 Yes, edit (是，編輯)。

如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的設定和使用標準日誌（存取日誌）。

從 Application Load Balancer 存放 Web 存取日誌

1. 登入 Amazon Elastic Compute Cloud (Amazon EC2) 主控台。
2. 在導覽窗格中，選擇 Load Balancers (負載平衡器)。
3. 選取 Web 應用程式的 ALB。
4. 在 Description (描述) 標籤上，選擇 Edit attributes (編輯屬性)。
5. 選擇 Enable access logs (啟用存取日誌)。
6. 針對 S3 位置，輸入您要用來存放 Web 存取日誌的 S3 儲存貯體名稱。這可以是用於主要堆疊的新或現有 S3 儲存貯體，並具有 Application Load Balancer 寫入日誌的許可。
7. 將日誌字首設定為用於部署解決方案的字首。您可以在主要堆疊、參數索引標籤、AppAccessLogBucketPrefixParam （ 預設 `AWSLogs/`) 中找到字首。
8. 選擇儲存。

如需詳細資訊，請參閱《Elastic Load Balancing 使用者指南》中的 Application Load Balancer 的存取日誌。

更新解決方案

如果您先前已部署解決方案，請依照此程序更新解決方案的 CloudFormation 堆疊，以取得解決方案架構的最新版本。更新堆疊之前，請先仔細閱讀更新考量事項。

1. 登入 AWS CloudFormation 主控台。
2. 在左側導覽功能表中選取堆疊。
3. 選取您現有的 `aws-waf-security-automations` CloudFormation 堆疊。
4. 選擇更新。
5. 選取取代目前範本。
6. 在指定範本下：
   a. 選取 Amazon S3 URL。
   b. 複製 `aws-waf-security-automations.template` AWS CloudFormation 的連結。
   c. 將連結貼到 Amazon S3 URL 方塊中。
   d. 驗證 Amazon S3 URL 文字方塊中顯示的範本 URL 是否正確。
   e. 選擇下一步。
   f. 再次選擇 Next (下一步)。
7. 在參數下，檢閱範本的參數並視需要修改。請參閱步驟 1。如需參數的詳細資訊，請啟動 堆疊。
8. 選擇下一步。
9. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
10. 在檢視 頁面上，檢視和確認的設定。
11. 選取確認範本可能會建立 IAM 資源的方塊。
12. 選擇檢視變更集並驗證變更。
13. 選擇更新堆疊以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中查看堆疊的狀態。您應該會在大約 15 分鐘內看到 UPDATE_COMPLETE 狀態。

更新考量事項

下列各節提供更新此解決方案的限制條件和考量事項。

資源類型更新

您必須在建立堆疊後部署新的堆疊來更新端點參數。更新堆疊時，請勿變更端點參數。

WAFV2 升級

從 3.0 版開始，此解決方案支援 AWS WAFV2。我們將所有 AWS WAF Classic API 呼叫取代為 AWS WAFV2 API 呼叫。這會移除 Node.js 上的相依性，並使用up-to-date執行時間。若要繼續使用此解決方案搭配最新的功能和改進，您必須將 3.0 版或更新版本部署為新的堆疊。

堆疊更新時的自訂

out-of-box解決方案會使用 CloudFormation 堆疊，將一組具有預設組態的 AWS WAF 規則部署到您的 AWS 帳戶。我們不建議將自訂套用至解決方案部署的規則。堆疊更新會覆寫這些變更。如果您需要自訂規則，建議您在解決方案之外建立單獨的規則。

無效的機器人保護升級

在 4.1.0 版中，具有 API Gateway 的 Access Handler Lambda 已棄用，並取代為 `Log parser - Bad bot` 功能的增強型日誌功能。解決方案現在會重複使用日誌串流來偵測錯誤的機器人，而不是透過 API Gateway 使用直接請求。

先前的實作：

1. 必要的存取處理常式 Lambda 和 API Gateway。
2. 使用 Honeypot 端點直接處理請求。
3. 網站中必要的內嵌 Honeypot 端點。

新的實作 (4.1.0+)：錯誤的機器人保護日誌剖析器現在：

1. 透過 日誌檢查對 Honeypot 端點的請求。
2. 啟動錯誤機器人保護時處理請求。
3. 使用 WAF 篩選條件 BadBotRuleFilter 來識別錯誤的機器人請求。
4. 分析日誌資料以識別超過定義配額的 IP 地址。
5. 更新 AWS WAF IP 集合條件以封鎖已識別的地址。

此變更會消除重複的功能並利用現有的日誌處理功能，以簡化架構。

CDK 升級

從 4.1.0 版開始，CDK 支援此解決方案。如果從低於 v4.1.0 的版本遷移。在 Cloudformation 中使用新範本並更新解決方案。然後，您可以使用 cdk 部署開始透過終端機在本機更新解決方案 （ 如需詳細資訊，請參閱 README) 如果您嘗試直接使用 cdk 部署，您可能會看到此錯誤：流程集合中的縮排不足

另一種更新解決方案的方式是使用解決方案提供的範本，並前往 AWS 主控台的 Cloudformation 區段，然後按一下更新解決方案，然後將新範本貼到那裡。

> **Note**
>
> 如果您要從 3.0 版或 3.1 版升級至此解決方案的 3.2 版或更新版本，而且您已手動將 IP 地址插入允許或拒絕的 IP 集，則會有遺失這些 IP 地址的風險。若要防止這種情況發生，請在升級解決方案之前，在允許或拒絕的 IP 集中複製 IP 地址。然後，完成升級後，視需要將 IP 地址加回 IP 集。請參閱 get-ip-set 和 update-ip-set CLI 命令。如果您已使用 3.2 版或更新版本，請忽略此步驟。

解除安裝解決方案

若要解除安裝解決方案，請刪除 CloudFormation 堆疊：

1. 登入 AWS CloudFormation 主控台。
2. 選取解決方案的父堆疊。所有其他解決方案堆疊都會自動刪除。
3. 選擇 刪除。

> **Note**
>
> 解除安裝解決方案會刪除解決方案使用的所有 AWS 資源，但 Amazon S3 儲存貯體除外。如果某些 IP 集因為速率超過 AWA WAF API 配額引起的限流問題而無法刪除，請手動刪除這些 IP 集，然後刪除堆疊。

使用 解決方案

本節提供部署解決方案後使用解決方案的詳細說明。

修改允許和拒絕的 IP 集 （選用）

部署此解決方案的 CloudFormation 堆疊之後，您可以視需要手動修改允許和拒絕的 IP 集，以新增或移除 IP 地址。

1. 登入 AWS WAF 主控台。
2. 在左側導覽窗格中，選擇 IP 集。
3. 選擇允許清單的 IP 集，並從信任的來源新增 IP 地址。
4. 選擇拒絕清單的 IP 集，並新增您要封鎖的 IP 地址。

在 Web 應用程式中嵌入 Honeypot 連結 （選用）

如果您在步驟 `yes` 1 中選擇啟用無效的機器人保護參數。 啟動堆疊，CloudFormation 範本會建立低互動生產 Honeypot 的陷阱端點。此陷阱旨在偵測和轉移來自內容湊集器和不良機器人的傳入請求。有效使用者不會嘗試存取此端點。

除了 Honeypot 機制之外，此元件還會監控 Application Load Balancer (ALB) 或 Amazon CloudFront 的直接連線，藉此增強錯誤的機器人偵測。如果機器人繞過 Honeypot 並嘗試與 ALB 或 CloudFront 互動，系統會分析請求模式和日誌，以識別惡意活動。偵測到錯誤的機器人時，會擷取其 IP 地址並新增至 AWS WAF 封鎖清單，以防止進一步存取。錯誤的機器人偵測會透過結構化邏輯鏈運作，以確保全面的威脅涵蓋範圍：

- HTTP 洪水防護 Lambda 日誌剖析器 – 在洪水分析期間從日誌項目收集錯誤的機器人 IPs。
- 掃描器和探查保護 Lambda 日誌剖析器 – 從掃描器相關日誌項目識別錯誤的機器人 IPs。
- HTTP 洪水防護 Athena 日誌剖析器 – 使用跨查詢執行的分割區，從 Athena 日誌擷取錯誤的機器人 IPs。
- 掃描器和探查保護 Athena 日誌剖析器 – 使用相同的分割策略，從掃描器相關的 Athena 日誌擷取錯誤的機器人 IPs。
- 備用偵測 – 如果同時停用 HTTP 洪水防護和掃描器與探查防護，系統會依賴 Log Lambda 剖析器，該剖析器會根據 WAF 標籤篩選條件記錄機器人活動。

使用下列其中一個程序，為來自 CloudFront 分佈的請求嵌入 Honeypot 連結。

為 Honeypot 端點建立 CloudFront 原始伺服器

針對使用 CloudFront 分佈部署的 Web 應用程式，請使用此程序。使用 CloudFront，您可以包含 `robots.txt` 檔案，以協助識別忽略機器人排除標準的內容抓取器和機器人。請完成下列步驟，以嵌入隱藏的連結，然後明確地在您的 `robots.txt` 檔案中不允許該連結。

1. 登入 AWS CloudFormation 主控台。
2. 選擇您在步驟 1 中建置的堆疊。啟動堆疊
3. 選擇 Output (輸出) 索引標籤。
4. 從 BadBotHoneypotEndpoint 金鑰複製端點 URL。
   - 行為路徑 (`/ProdStage`)
5. 在指向 Honeypot 的內容中嵌入此端點連結。從您的人類使用者隱藏此連結。例如，請檢閱下列程式碼範例：`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`。
6. 修改網站根目錄中`robots.txt`的檔案，以明確禁止 Honeypot 連結，如下所示：

```
User-agent: <*>
        Disallow: /<behavior_path>
```

> **Important**
>
> CloudFront 中不需要任何路徑註冊，因為請求為：被 WAF BadBotRuleFilter 封鎖。自動在日誌中收集的解決方案。由日誌剖析器 lambda 處理。這種簡化的方法直接使用 WAF 日誌，而不是需要額外的端點組態，透過日誌分析讓錯誤的機器人偵測程序更有效率

> **Note**
>
> 您有責任驗證哪些標籤值適用於您的網站環境。`rel="nofollow"` 如果您的環境未觀察到，請勿使用 。如需機器人中繼標籤組態的詳細資訊，請參閱 Google 開發人員指南。修改網站根目錄中`robots.txt`的檔案，以明確禁止 Honeypot 連結，如下所示：

將 Honeypot 端點內嵌為外部連結

> **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。

針對 Web 應用程式使用此程序。

1. 登入 AWS CloudFormation 主控台。
2. 選擇您在步驟 1 中建置的堆疊。啟動堆疊。
3. 選擇 Output (輸出) 索引標籤。
4. 從 BadBotHoneypotEndpoint 金鑰複製端點 URL。

```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-hidden="true"><honeypot link></a>
```

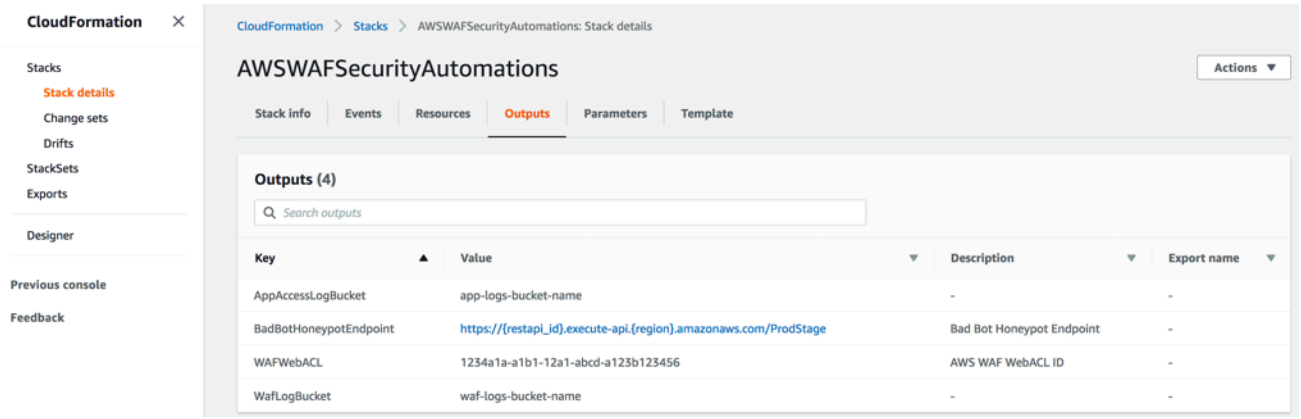
> **Note**
>
> 此程序使用 `rel=nofollow` 指示機器人不要存取 Honeypot URL。不過，由於連結是在外部內嵌，因此您無法包含明確不允許連結`robots.txt`的檔案。您有責任驗證哪些標籤可在您的網站環境中運作。`rel="nofollow"` 如果您的環境未觀察到，請勿使用 。

使用 Lambda 日誌剖析器 JSON 檔案

使用 Lambda 日誌剖析器 JSON 檔案進行 HTTP 洪水保護

如果您選擇`Yes - AWS Lambda log parser`啟用 HTTP 洪水防護範本參數，此解決方案會建立名為 的組態檔案，並將其 `<stack_name>-waf_log_conf.json`上傳至用於存放 AWS WAF 日誌檔案的 Amazon S3 儲存貯體。若要尋找儲存貯體名稱，請參閱 CloudFormation 輸出中的 WafLogBucket 變數。下圖顯示範例。

螢幕擷取畫面，描述標記為 AWSWAFSecurityAutomations 並列出四個輸出的螢幕



如果您在 Amazon S3 上編輯和覆寫 `<stack_name>-waf_log_conf.json`檔案，Log ParserLambda 函數會在處理新的 AWS WAF 日誌檔案時考慮新的值。以下是範例組態檔案：

範例組態檔案的螢幕擷取畫面

```
{
 "general": {
    "requestThreshold": 2000,
    "blockPeriod": 240,
    "ignoredSufixes": [".css", ".js", ".jpg", "png", ".gif"]
  },
 "uriList": {
    "/search": {
        "requestThreshold": 500,
        "blockPeriod": 600
    }
  }
}
```

參數包括下列項目：

- 一般：
  - 請求閾值 （必要） - 每個 IP 地址每五分鐘可接受的請求上限。此解決方案會使用您在佈建或更新 CloudFormation 堆疊時定義的值。
  - 封鎖期間 （必要） - 封鎖適用 IP 地址的期間 （分鐘）。此解決方案會使用您在佈建或更新 CloudFormation 堆疊時定義的值。
  - 忽略字尾 - 存取此類資源的請求不會計入請求閾值。根據預設，此清單為空白。
- URI 清單 - 使用此清單來定義特定 URLs的自訂請求閾值和封鎖期間。根據預設，此清單為空白。

當 WAF 日誌送達 WafLogBucket 時，Lambda 日誌剖析器函數將使用組態檔案中的組態來處理它們。解決方案會將結果寫入至相同儲存貯 <stack_name>-waf_log_out.json體中名為 的輸出檔案。如果輸出檔案包含識別為攻擊者的 IP 地址清單，解決方案會將它們新增至 HTTP 洪水的 WAF IP 集，而且會封鎖它們存取您的應用程式。如果輸出檔案沒有 IP 地址，請檢查您的組態檔案是否有效，或是否已根據組態檔案超過速率限制。

使用 Lambda 日誌剖析器 JSON 檔案進行掃描器和探查保護

如果您選擇Yes - AWS Lambda log parser啟用掃描器和探查保護範本參數，此解決方案會建立名為 的組態檔案，並將其 <stack_name>-app_log_conf.json上傳至用來存放 CloudFront 或 Application Load Balancer 日誌檔案的已定義 Amazon S3 儲存貯體。

如果您在 <stack_name>-app_log_conf.json Amazon S3 上編輯和覆寫 ，Log ParserLambda 函數會在處理新的 AWS WAF 日誌檔案時考慮新的值。以下是範例組態檔案：

組態檔案的螢幕擷取畫面

參數包括下列項目：

- 一般：
  - 錯誤閾值 （必要） - 每個 IP 地址每分鐘可接受的錯誤請求上限。此解決方案會使用您在佈建或更新 CloudFormation 堆疊時定義的值。
  - 封鎖期間 （必要） - 封鎖適用 IP 地址的期間 （分鐘）。此解決方案會使用您在佈建或更新 CloudFormation 堆疊時定義的值。
  - 錯誤碼 - 傳回狀態碼視為錯誤。根據預設，清單會將下列 HTTP 狀態碼視為錯誤：400 (Bad Request)、401 (Unauthorized)、403 (Forbidden)、 404 (Not Found)和 405 (Method Not Allowed)。
- URI 清單 - 用來定義特定 URLs的自訂請求閾值和封鎖期間。根據預設，此清單為空白。

當應用程式存取日誌送達 AppAccessLogBucket 時，Log ParserLambda 函數會使用組態檔案中的組態來處理它們。解決方案會將結果寫入相同儲存貯體中名為 <stack_name>`-app_log_out.json` 的輸出檔案。如果輸出檔案包含識別為攻擊者的 IP 地址清單，解決方案會將它們新增至掃描器和探查的 WAF IP 集，並封鎖它們存取您的應用程式。如果輸出檔案沒有 IP 地址，請檢查您的組態檔案是否有效，或是否已根據組態檔案超過速率限制。

在 HTTP 洪水 Athena 日誌剖析器中使用國家/地區和 URI

您可以在 Athena 查詢中依 IPs 以及國家/地區和 URI 分組，以偵測和封鎖具有不可預測 URI 模式的 HTTP 洪水攻擊。若要這樣做，請在啟動堆疊時，選取 HTTP 洪水 Athena 查詢參數中依請求分組的其中一個選項 (CountryURI、、Country and URI)。

您也可以使用依國家/地區請求閾值參數，依國家/地區輸入請求閾值。例如 {"TR": 50,"ER":150}。解決方案會將這些閾值用於來自這些指定國家/地區的請求。解決方案對來自其他國家的請求使用預設閾值。

> **Note**
>
> 如果您依國家/地區定義閾值，解決方案會自動在 Athena 查詢群組依子句中包含國家/地區。如需詳細資訊，請參閱步驟 1 中的參數表。啟動堆疊。

解決方案預設會在五分鐘期間內計算請求閾值。這可使用 Athena 查詢執行時間排程 （分鐘） 參數來設定。

> **Note**
>
> Athena 查詢透過將請求閾值除以時段來計算每分鐘閾值。例如：
> 請求閾值 （預設閾值或按國家/地區的閾值）：100
> Athena 查詢執行時間排程：5
> 每分鐘請求閾值：20 = 100 / 5

檢視 Amazon Athena 查詢

如果您選取Yes - Amazon Athena log parser啟用 HTTP 洪水防護或啟用掃描器和探查保護範本參數，此解決方案會建立並執行 CloudFront 或 ALB (ScannersProbesLogParser) 或 AWS WAF 日誌 (HTTPFloodLogParser) 的 Athena 查詢、剖析輸出，並相應地更新 AWS WAF。

為了改善效能並降低成本，解決方案會根據檔案名稱中的時間戳記來分割日誌。解決方案會動態產生 Athena 查詢以使用分割區索引鍵（年、月、日和小時）。根據預設，查詢會每五分鐘執行一次。您可以透過變更 Athena 查詢執行時間排程（分鐘）範本參數的值來設定其執行排程。根據預設，每個查詢執行會掃描最後四到五小時的資料。您可以變更 WAF Block Period 範本參數的值，來設定查詢掃描的資料量。解決方案也會將查詢放置在不同的工作群組中，以管理查詢存取和成本。

> **Note**
>
> 確認 Athena 已設定為存取 AWS Glue Data Catalog。此解決方案會在 AWS Glue 中建立存取日誌資料目錄，並設定 Athena 查詢來處理資料。如果未正確設定 Athena，則查詢不會執行。如需詳細資訊，請參閱step-by-step升級至最新的 AWSAWS Glue Data Catalog。

使用下列程序來檢視這些查詢：

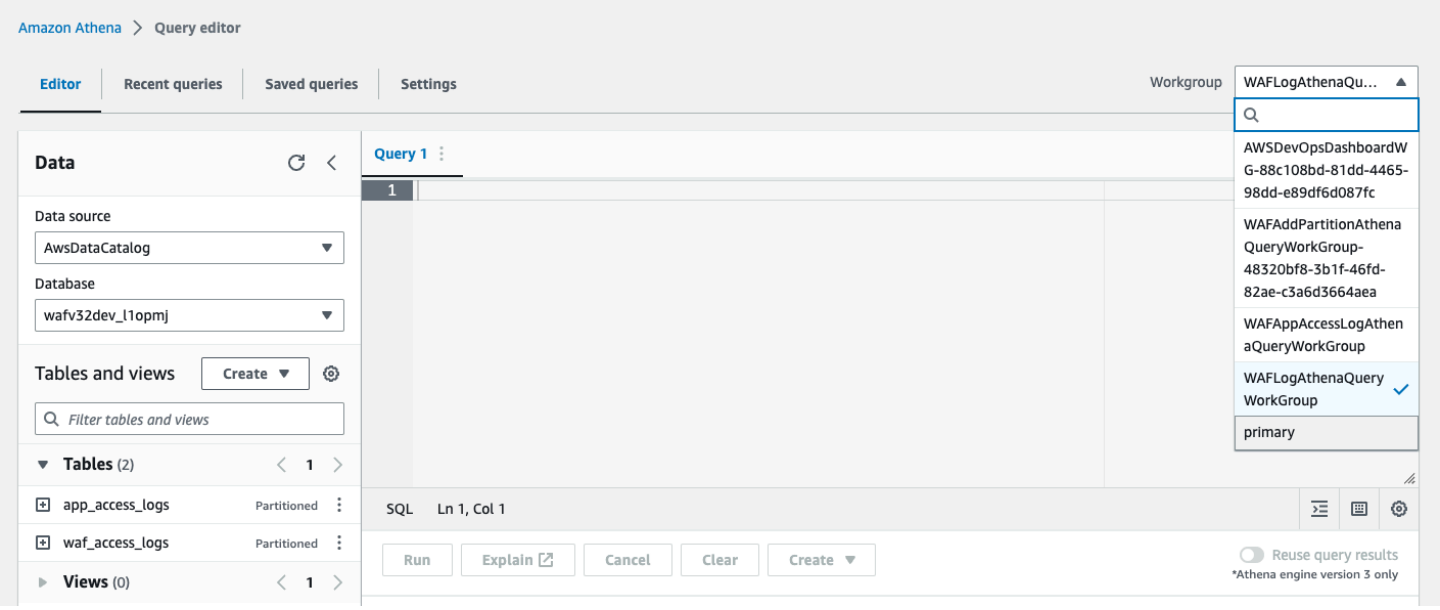
檢視 WAF 日誌查詢

1. 登入 Amazon Athena 主控台。
2. 選擇啟動查詢編輯器。
3. 選取此解決方案的資料庫。
4. 從下拉式清單中選取 WAFLogAthenaQueryWorkGroup。

> **Note**
>
> 只有在您`Yes - Amazon Athena log parser`選取啟用 HTTP 洪水防護範本參數時，此工作群組才會存在。

5. 選擇切換以切換工作群組。

Athena 查詢編輯器的螢幕擷取畫面，顯示沒有查詢



1. 選取歷史記錄索引標籤。
2. 從清單中選擇並開啟SELECT查詢。

檢視應用程式存取日誌查詢

1. 登入 Amazon Athena 主控台。
2. 選取工作群組索引標籤。
3. 從清單中選擇 WAFAppAccessLogAthenaQueryWorkGroup。

> **Note**
>
> 只有在您Yes - Amazon Athena log parser為啟動掃描器和探查保護範本參數選取時，此工作群組才會存在。

4. 選擇切換工作群組。
5. 選取最近查詢索引標籤。
6. 從清單中選擇並開啟SELECT查詢。

檢視新增 Athena 分割區查詢

1. 登入 Amazon Athena 主控台。

2. 選取工作群組索引標籤。
3. 從清單中選擇 WAFAddPartitionAthenaQueryWorkGroup。

> **Note**
>
> 只有在您`Yes - Amazon Athena log parser`選取啟用 HTTP 洪水防護和/或啟用掃描器和探查保護範本參數時，此工作群組才會存在。

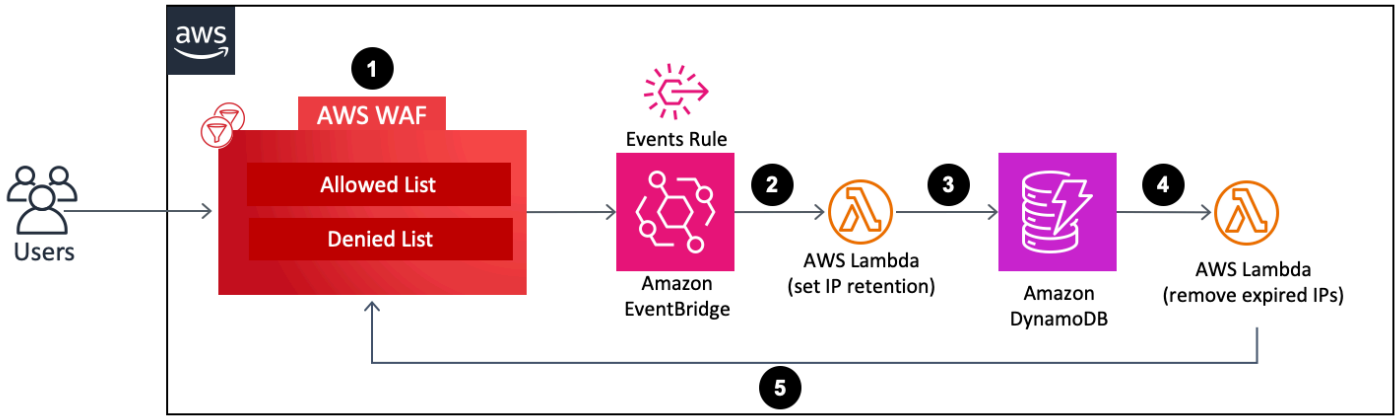
4. 選取切換工作群組。
5. 選取歷史記錄索引標籤。
6. 從清單中選擇並開啟`ALTER TABLE`查詢。這些查詢每小時執行一次，以將新的每小時分割區新增至 Athena 資料表。

在允許和拒絕的 AWS WAF IP 集上設定 IP 保留

您可以在解決方案建立的允許和拒絕 AWS WAF IP 集上設定 IP 保留。下列各節說明其運作方式，並提供設定步驟。

運作方式

描述 AWS WAF 允許和拒絕清單和其他 AWS 資源的架構圖



1. 當使用者更新（新增或刪除 IP 地址）允許或拒絕的 WAF IP 集時，此動作會叫用 AWS WAF `UpdateIPSet` API 呼叫並建立事件。
2. Amazon EventBridge 事件規則會根據預先定義的事件模式偵測事件，並叫用 Lambda 函數來設定更新後存在於 IP 集中所有 IP 地址的保留期間。

3. Lambda 函數會處理事件、將相關資料擷取至 IP 保留（例如 IP 集合名稱、ID、範圍、IP 地址），並將其插入 DynamoDB 資料表。它也會為每個 DynamoDB 項目插入`ExpirationTime`屬性。解決方案會將使用者定義的保留期新增至事件時間，以計算到期時間。資料表已開啟 DynamoDB 串流和存留時間 (TTL)。TTL 屬性為 `ExpirationTime`。
4. 當項目達到過期時間時，會叫用 TTL，且 DynamoDB 會在過期時間後從資料表中刪除項目。刪除項目時，已刪除的項目會新增至 DynamoDB 串流，以叫用 Lambda 函數進行下游處理。
5. Lambda 函數會從 DynamoDB 串流取得已刪除項目的相關資訊，並發出 AWS WAF API 呼叫，以從目標 AWS WAF IP 集中移除項目中包含的過期 IP 地址。

開啟 IP 保留

請依照下列步驟開啟 IP 保留：

1. 在您部署或更新的 Cloudformation 堆疊中，輸入允許 IP 集的 IP 保留期（分鐘）和遭拒 IP 集的 IP 保留期（分鐘）。最短保留期間為 15 分鐘。解決方案會將 `0`和 之間的任何數字`15`視為 15。如需部署組態的詳細資訊，請參閱步驟 1。啟動堆疊。
2. 如果您想要在從 AWS WAF IP 集移除過期 IP 地址時收到電子郵件通知，請輸入電子郵件地址。如果您選擇接收電子郵件通知，則必須使用解決方案成功部署後所收到電子郵件中的連結來確認訂閱。如需部署組態的詳細資訊，請參閱步驟 1。啟動堆疊。
3. 透過新增或刪除 IP 地址來更新 AWS WAF IP 集。這會啟動 IP 保留程序並建立 DynamoDB 項目，包括 IP 過期清單。此過期清單包含更新後存在於 AWS WAF IP 集合中的 IP 地址。
4. 一旦 DynamoDB 項目達到其過期時間並從資料表中刪除，解決方案會從 WAF IP 集刪除項目 IP 過期清單中包含的 IP 地址。

> **Note**
>
> 根據 DynamoDB 刪除 TTL 過期項目的時間，從 AWS WAF IP 集中過期 IP 地址的實際刪除操作可能會有所不同。DynamoDB TTL 刪除主要取決於資料表的大小和活動層級。由於 DynamoDB 刪除操作中AWS WAF 刪除操作中預期會有延遲。一般而言，解決方案會在 DynamoDB TTL 刪除後不久從 AWS WAF IP 集刪除過期的 IP 地址。如需詳細資訊，請參閱《Amazon DynamoDB 開發人員指南》中的 DynamoDB 存留時間 (TTL)。 DynamoDB

組建監控儀表板

AWS 建議您為每個關鍵端點設定自訂基準監控系統。如需有關建立和使用自訂指標檢視的資訊，請參閱 CloudWatch Dashboards - 建立和使用自訂指標檢視和使用 Amazon CloudWatch 儀表板。

下列儀表板螢幕擷取畫面顯示自訂基準監控系統的範例。

CloudFront 儀表板的螢幕擷取畫面

儀表板會顯示下列指標：

- 允許與封鎖請求 - 顯示您是否收到允許存取激增（正常尖峰存取的兩倍）或封鎖存取（識別超過 1K 封鎖請求的任何期間）。CloudWatch 會將警示傳送至 Slack 頻道。您可以使用此指標來追蹤已知的 DDoS 攻擊（當封鎖請求增加時）或攻擊的新版本（當允許請求存取系統時）。

  > **Note**
  >
  > 注意：解決方案提供此指標。

- BytesDownloaded 與 Uploaded - 協助識別 DDoS 攻擊的目標是通常不會接收大量耗盡資源的服務（例如，針對一個特定請求參數集傳送 MBs 資訊的搜尋引擎元件）。
- ELB 溢出和佇列長度 - 協助驗證 DDoS 攻擊是否造成基礎設施損壞，以及攻擊者是否繞過 CloudFront 或 AWS WAF layer，並直接攻擊未受保護的資源。

- ELB 請求計數 - 協助識別基礎設施的損壞。此指標顯示攻擊者是否繞過保護層，或者您是否應該檢閱 CloudFront 快取規則以提高快取命中率。
- ELB 運作狀態良好的主機 - 您可以使用此指標做為另一個系統運作狀態檢查指標。
- ASG CPU 使用率 - 協助識別攻擊者是否繞過 CloudFront、AWS WAF 和 Elastic Load Balancing。您也可以使用此指標來識別攻擊的損害。

處理 XSS 誤報

此解決方案會設定 AWS WAF 規則，檢查傳入請求的常見探索元素，以識別和封鎖 XSS 攻擊。如果您的工作負載允許合法使用者編寫和提交 HTML，例如，在內容管理系統中使用富文字編輯器，則此偵測模式效率較低。在此案例中，請考慮建立例外狀況規則，以略過接受富文字輸入的特定 URL 模式的預設 XSS 規則，並實作替代機制來保護這些排除URLs。

此外，某些影像或自訂資料格式可能會導致誤報，因為它們包含表示 HTML 內容中潛在 XSS 攻擊的模式。例如，SVG 檔案可能包含`<script>`標籤。如果您預期合法使用者提供這類內容，請嚴格調整 XSS 規則，以允許包含這些其他資料格式的 HTML 請求。

完成下列步驟以更新 XSS 規則，以排除接受 HTML 做為輸入的 URLs。如需詳細說明，請參閱 Amazon WAF 開發人員指南。

1. 登入 AWS WAF 主控台。
2. 建立字串比對或 regex 條件。
3. 設定篩選條件設定以檢查 URI，並列出您要針對 XSS 規則接受的值。
4. 編輯此解決方案的 XSS 規則，並新增您建立的新條件。

   例如，若要排除清單中的所有 URLs，請為當請求 時選擇以下項目：

   - 不會
   - 在字串比對條件中比對至少一個檔案器
   - XSS 允許清單

疑難排解

如果您需要此解決方案的協助，請聯絡 Support 以開啟此解決方案的支援案例。

聯絡 支援

如果您有 AWS 開發人員支援、AWS Business Support 或 AWS Enterprise Support，您可以使用 支援中心來取得此解決方案的專家協助。以下章節將提供說明。

建立案例

1. 開啟支援中心。
2. 選擇建立案例。

如何提供協助？

1. 選擇技術。
2. 針對服務，選取 WAF 或 AWS WAF。
3. 針對類別，選取 WAF 安全自動化或 AWS WAF 的安全自動化。
4. 對於嚴重性，最符合您使用案例的選項。
5. 當您輸入服務、類別和嚴重性時，界面會填入常見故障診斷問題的連結。如果您無法使用這些連結來解決問題，請選擇下一步：其他資訊。

其他資訊

1. 針對主旨，輸入摘要您的問題的文字。
2. 針對描述，請詳細說明問題。
3. 選擇連接檔案。
4. 連接 Support 處理請求所需的資訊。

協助我們更快解決您的案例

1. 輸入請求的資訊。

2. 選擇下一步驟：立即解決或聯絡我們。

立即解決或聯絡我們

1. 檢閱立即解決解決方案。
2. 如果您無法解決這些解決方案的問題，請選擇聯絡我們，輸入請求的資訊，然後選擇提交。

開發人員指南

本節提供解決方案的原始程式碼。

來源碼

請造訪我們的 GitHub 儲存庫，下載此解決方案的範本和指令碼，並與他人共用您的自訂項目。

此解決方案的範本是使用 AWS CDK 產生。如需其他資訊，請參閱 README.md 檔案。

參考資料

本節包含收集此解決方案唯一指標的選用功能、相關資源的指標，以及有助於此解決方案的建置器清單的相關資訊。

匿名資料收集

此解決方案包含將操作指標傳送至 AWS 的選項。我們使用這些資料更好地了解客戶使用此解決方案、相關服務和產品的方式。開啟時，解決方案會收集下列資訊，並在 CloudFormation 範本的初始部署期間將其傳送至 AWS：

- 解決方案 ID - AWS 解決方案識別符
- 唯一 ID (UUID) - 隨機產生此解決方案每次部署的唯一識別符
- 時間戳記 - 資料收集時間戳記
- 解決方案組態 - 在初始啟動期間開啟的功能和設定的參數
- 生命週期 - 客戶使用此解決方案的時間長度 （ 根據堆疊刪除 ）
- 日誌剖析器資料：
  - 掃描器和探查 IP 集、錯誤機器人 IP 集和要封鎖的 HTTP 洪水 IP 集中的 IP 地址數量
  - 處理和封鎖的請求數量
- IP 列出剖析器資料：
  - 評價清單 IP 集中的 IP 地址數量
  - 處理和封鎖的請求數量
- IP 保留資料 - 從允許或拒絕的 IP 集合中移除的過期 IP 地址數量

AWS 擁有透過此問卷收集的資料。資料收集受 AWS 隱私權政策約束。若要選擇退出此功能，請先完成下列步驟，再啟動 AWS CloudFormation 範本。

1. 下載 `aws-waf-security-automations.template` AWS CloudFormation 到您的本機硬碟。
2. 使用文字編輯器開啟 CloudFormation 範本。
3. 從以下位置修改 CloudFormation 範本映射區段：

```
Solution:
  Data:
```

```
    SendAnonymizedUsageData: "Yes"
```

至:

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. 在 AWS CloudFormation 主控台中登入。
5. 選取建立堆疊。
6. 在建立堆疊頁面指定範本區段中，選取上傳範本檔案。
7. 在上傳範本檔案下，選擇選擇檔案，然後從本機磁碟機中選取編輯的範本。
8. 選擇下一步，並遵循步驟 1 中的步驟。啟動堆疊。

相關資源

關聯的 AWS 白皮書

- DDoS 彈性的 AWS 最佳實務

關聯的 AWS 安全部落格文章

- 如何使用 AWS WAF、Amazon CloudFront 和 Referer Checking 預防熱連結

第三方 IP 評價清單

- Spamhaus DROP 清單網站
- Proofpoint 新興威脅 IP 清單
- Tor 結束節點清單

貢獻者

- Heitor Vital
- 李阿金森

- Ben Potter
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- Shu Jackson
- William Quan
- Mykhailo Markhain

修訂

請造訪 GitHub 儲存庫中的 CHANGELOG.md：//。

注意

此實作指南僅供參考。它代表截至本文件發行日期的目前 AWS 產品產品和實務，這些產品和實務可能會有所變更，恕不另行通知。客戶必須負責獨立評估本文件中的資訊，以及對 AWS 產品或服務的任何使用，每個產品或服務都「原樣」提供，無論明示或暗示，均不提供任何保證。本文件不會從 AWS、其附屬公司、供應商或授權方建立任何保證、聲明、合約承諾、條件或保證。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

AWS WAF 的安全自動化解決方案是根據 Apache License Version 2.0 的條款進行授權。

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。