AWS 白皮書

AWS DDoS 耐受力最佳實務

AWS DDoS 耐受力最佳實務: AWS 白皮書

Table of Contents

AWS DDoS 耐受力最佳實務

發佈日期：2021 年 9 月 21 日 (文件修訂)

摘要

保護您的企業免受分散式阻斷式服務 (DDoS) 攻擊以及其他網路攻擊的影響非常重要。透過保持應用程式的可用性和回應能力來保持客戶對服務的信任是首要之務。當基礎設施必須擴展以回應攻擊時，您還希望避免不必要的直接成本。Amazon Web Services (AWS) 致力於為您提供工具、最佳實務和服務，以防禦網際網路上的不良行為者。使用來自 AWS 的適當服務，可協助確保高可用性、安全性和耐受力。

在本白皮書中，AWS 會為您提供規範性的 DDoS 指導，以提高在 AWS 上執行的應用程式的耐受力。這包括具 DDoS 耐受力的參考架構，可用作指南，以協助保護應用程式可用性。本白皮書也會介紹不同的攻擊類型，例如，基礎設施層攻擊和應用程式層攻擊。AWS 會說明哪些最佳實務可最有效管控每個類型的攻擊。此外還概述適合 DDoS 緩解政策的服務和功能，並說明如何使用每項服務和功能來協助保護您的應用程式。

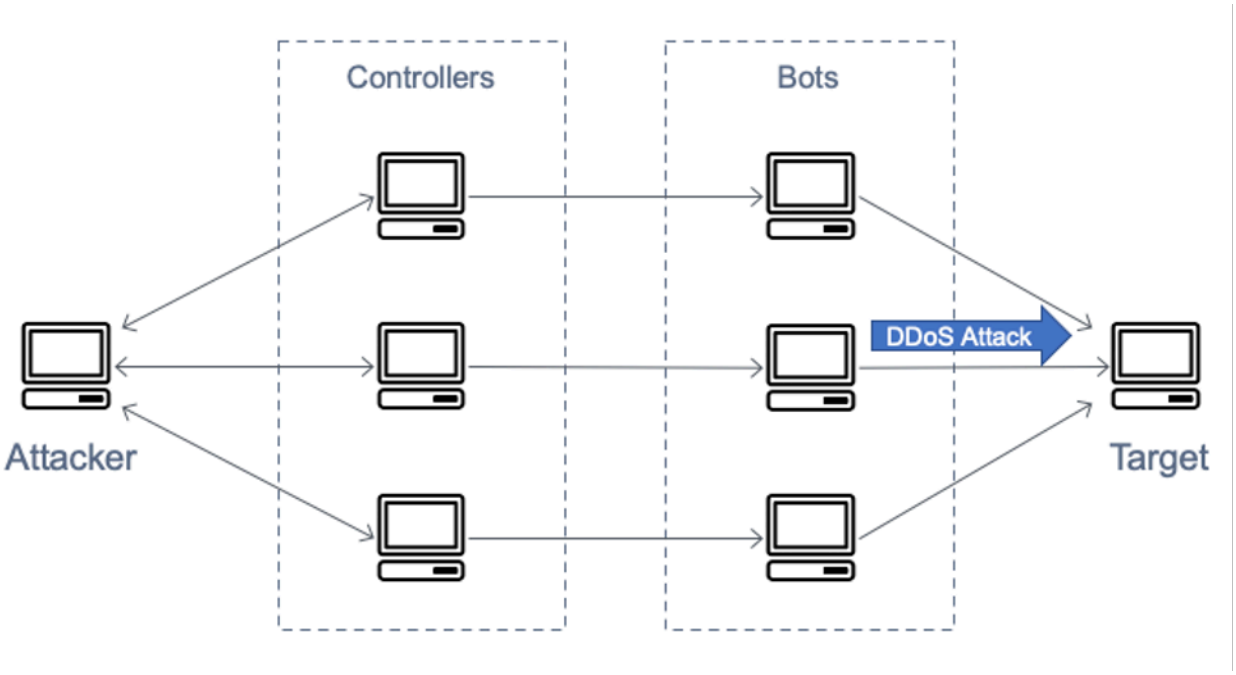
本白皮書的目標對象為熟悉聯網、安全和 AWS 基本概念的 IT 決策者和安全工程師。每個小節都有 AWS 文件的連結，它們提供有關最佳實務或功能的更多詳細資料。

簡介：阻斷式服務攻擊

阻斷式服務 (DoS) 攻擊是蓄意嘗試使網站或應用程式無法供使用者存取的行為，例如，用網路流量使其氾濫。攻擊者會使用各種技術，其會消耗大量網路頻寬或佔用其他系統資源，從而干擾合法使用者的存取。最簡單的形式是，單一攻擊者會使用單一來源對目標執行 DoS 攻擊，如下圖所示。

表 1：DoS 攻擊圖

在 DDoS 攻擊中，攻擊者會使用多個來源以協調對目標的攻擊。這些來源可以包括分散式群組，包括受到惡意軟體感染的電腦、路由器、IoT 裝置和其他端點。下圖顯示參與攻擊、產生大量封包或請求以將目標壓倒的受損主機網路。



DDoS 攻擊圖

開放式系統互連 (OSI) 模型中有七層，在開放式系統互連 (OSI) 模型表中對這些層進行說明。DDoS 攻擊最常見於第三層、第四層、第六層和第七層。第三層和第四層攻擊與 OSI 模型的網路層和傳輸層對應。在本白皮書內，AWS 將它們統稱為基礎設施層攻擊。第六層和第七層攻擊與 OSI 模型的展示層和應用程式層對應。AWS 會將這些項目共同處理為應用程式層攻擊。以下各節討論這些攻擊類型的範例。

開放式系統互聯 (OSI) 模型

#	層級	單位	描述	向量範例
7	應用程式	資料	網路程序到應用程式	HTTP 洪水、DNS 查詢洪水
6	展示	資料	資料展示和加密	TLS 濫用
5	工作階段	資料	中間主機通訊	不適用
4	傳輸	區段	端對端連線和可靠性	SYN 洪水
3	網路	封包	路徑判定與邏輯定址	UDP 反射攻擊
2	資料連結	影格	實體定址	不適用
1	實體	位元	媒體、訊號和二進位傳輸	不適用

主題

- 基礎設施層攻擊
- 應用程式層攻擊

基礎設施層攻擊

最常見的 DDoS 攻擊，即使用者資料包通訊協定 (UDP) 反射攻擊和同步 (SYN) 洪水，是基礎設施層攻擊。攻擊者可以使用這些方法中的其中一個來產生大量流量，這些流量可能會佔據網路容量，或佔用系統上的資源 (例如，伺服器、防火牆、入侵防禦系統 (IPS) 或負載平衡器)。雖然這些攻擊很容易識別，但為了有效地緩解它們，您必須擁有能比傳入流量洪水更快速擴充容量的網路或系統。此額外容量對於篩選掉或吸收攻擊流量，因而釋放系統和應用程式以回應合法客戶流量來說是必要的。

主題

- UDP 反射攻擊
- SYN 洪水攻擊

UDP 反射攻擊

使用者資料包通訊協定 (UDP) 反射攻擊會利用 UDP 是無狀態通訊協定的事實。攻擊者可以建立一個有效的 UDP 請求封包，將攻擊目標的 IP 地址列為 UDP 來源 IP 地址。攻擊者現在已偽造 (假冒) UDP 請求封包的來源 IP。UDP 封包包含假冒的來源 IP，並由攻擊者傳送至中繼伺服器。伺服器遭到欺騙將其 UDP 回應封包傳送到目標受害者 IP，而不是傳送回攻擊者的 IP 地址。使用中繼伺服器是因為它產生的回應比請求封包大數倍，可有效地放大傳送到目標 IP 地址的攻擊流量。

放大係數是回應大小與請求大小的比率，它取決於攻擊者使用的通訊協定：
DNS、NTP、SSDP、CLDAP、Memcached、CharGen 或 QOTD。例如，DNS 的放大係數可以是原始位元組數的 28 到 54 倍。因此，如果攻擊者向 DNS 伺服器傳送 64 位元組的請求酬載，他們可能會向攻擊目標產生超過 3400 個位元組的不必要流量。與其他攻擊相比，UDP 反射攻擊更應對大量流量負責。UDP 反射攻擊圖說明反射策略和放大效果。

UDP 反射攻擊

SYN 洪水攻擊

當使用者連線到傳輸控制通訊協定 (TCP) 服務 (例如 Web 伺服器) 時，他們的用戶端會傳送 SYN 同步封包。伺服器會在確認中傳回 SYN-ACK 封包，最終用戶端會以確認 (ACK) 封包回應，進而完成預期的三向交握。下圖說明此典型的交握。

SYN 3 向交握

在 SYN 洪水攻擊中，惡意用戶端會傳送大量 SYN 封包，但永遠不會傳送最終 ACK 封包來完成交握。伺服器將等待對半開放 TCP 連線的回應，並最終用盡容量，無法接受新的 TCP 連線。這可防止新使用者連線到該伺服器。此攻擊會嘗試佔用可用的伺服器連線，使得資源無法供合法連線使用。儘管 SYN 洪水可達到數百 Gbps，但攻擊的目的不是要增加 SYN 流量。

應用程式層攻擊

攻擊者可以使用第 7 層或應用程式層攻擊，以應用程式本身為目標。在這些攻擊中，與 SYN 洪水基礎設施攻擊類似，攻擊者會嘗試使應用程式的特定功能過載，使得應用程式無法使用或無法對合法使用者回應。有時候，以只會產生少量網路流量的極低請求量也可以達成此目的。這會使得攻擊難以偵測和緩解。應用程式層攻擊的範例包括 HTTP 洪水、快取破壞攻擊和 WordPress XML-RPC 洪水。

在 HTTP 洪水攻擊中，攻擊者會傳送似乎來自 Web 應用程式有效使用者的 HTTP 請求。某些 HTTP 洪水會針對特定資源，而更複雜的 HTTP 洪水則會嘗試模擬與應用程式的人為互動。這會增加使用常見緩解技術 (例如請求率限制) 的困難度。

快取破壞攻擊是一種 HTTP 洪水，它會在查詢字串中使用變化來規避內容交付網路 (CDN) 快取。CDN 不需能夠傳回快取的結果，而是必須針對每個頁面請求與原始伺服器連絡，而這些來源擷取會為應用程式 Web 伺服器帶來額外的壓力。

使用 WordPress XML-RPC 洪水攻擊 (也稱為 WordPress pingback 洪水)，攻擊者即可針對託管於 WordPress 內容管理軟體的網站。攻擊者會濫用 XML-RPC API 函數來產生大量 HTTP 請求。pingback 功能會允許託管在 WordPress (網站 A) 的網站透過網站 A 建立連至網站 B 的連結，通知不同的 WordPress 網站 (網站 B)。然後網站 B 即可嘗試擷取網站 A 來驗證該連結存在。在 pingback 洪水中，攻擊者會誤用此功能來導致網站 B 攻擊網站 A。此類攻擊具有明確的簽章：WordPress 通常存在於 HTTP 請求標頭的 User-Agent 中。

還有其他形式的惡意流量可能會影響應用程式的可用性。網路爬蟲機器人可以自動嘗試存取 Web 應用程式，以竊取內容或記錄具競爭性資訊 (例如定價)。暴力破解和憑證填充攻擊程式的編寫是為了取得應用程式安全區域未經授權的存取權。這些不是嚴格的 DDoS 攻擊；但它們的自動化本質看起來類似 DDoS 攻擊，並且可以透過實作本白皮書中涵蓋的一些相同最佳實務來加以緩解。

應用程式層攻擊還可以針對網域名稱系統 (DNS) 服務。這些攻擊中最常見的是 DNS 查詢洪水，其中的攻擊者會使用許多格式良好的 DNS 查詢來耗盡 DNS 伺服器的資源。這些攻擊還可以包括一個快取破壞元件，其中攻擊者會將子網域字串隨機化，以略過任何指定解析程式的本機 DNS 快取。因此，解析程式無法利用快取網域查詢，而是必須重複連絡授權 DNS 伺服器，而這會將攻擊放大。

如果 Web 應用程式是透過 Transport Layer Security (TLS) 傳輸，攻擊者還可以選擇攻擊 TLS 交涉程序。TLS 的運算成本很高昂，因此會透過在伺服器上產生額外的工作負載來處理無法讀取的資料 (或無法理解 (密文)) 作為合法交握的攻擊者，可能會降低伺服器的可用性。在此攻擊的變化中，攻擊者會完成 TLS 交握，但永久重新交涉加密方法。攻擊者也可以透過開啟和關閉許多 TLS 工作階段來嘗試耗盡伺服器資源。

緩解技術

某些形式的 DDoS 緩解會自動隨著 AWS 服務包含。透過使用具有特定服務的 AWS 架構 (如以下各節所述)，以及透過為使用者與您的應用程式之間網路流程的每個部分實作其他最佳實務，即可以進一步提升 DDoS 耐受力。

所有 AWS 客戶都可受到 AWS Shield Standard 的自動保護，且不需額外付費。AWS Shield Standard 可防止以您的網站或應用程式做為目標的最常見和最常發生的網路和傳輸層 DDoS 攻擊。此保護一律會開啟、預先設定、靜態，且不會提供報告或分析。它會在所有 AWS 服務上並於每個 AWS 區域中提供。在 AWS 區域中，會偵測到 DDoS 攻擊，而 Shield Standard 系統會自動設定流量基準、識別異常情況，並視需要建立緩解措施。您可以使用 AWS Shield Standard 作為具 DDoS 耐受力架構的一部分，以同時保護 Web 和非 Web 應用程式。

您還可以利用從節點執行的 AWS 服務 (例如 Amazon CloudFront、Global Accelerator 和 Route 53) 來建置可抵禦所有已知基礎設施層攻擊的全面可用性保護。這些服務是 AWS 全球邊緣網路的一部分，在服務來自分散至世界各地的節點的任何類型的應用程式流量時，可以提高您的應用程式的 DDoS 耐受力。您可以在任何 AWS 區域中執行您的應用程式，並使用這些服務來保護您的應用程式可用性，並為合法最終使用者將應用程式的效能最佳化。

使用 Amazon CloudFront、Global Accelerator 和 Amazon Route 53 的優點包括：

- 存取整個 AWS 全球邊緣網路的網際網路和 DDoS 緩解容量。這對於緩解可達到 TB 規模的較大容量型攻擊非常有用。
- AWS Shield DDoS 緩解系統與 AWS 邊緣服務整合，將緩解時間從幾分鐘縮短到一秒內。
- 無狀態 SYN 洪水緩解技術會先代理並驗證傳入連線，然後再將它們傳遞到受保護的服務。這可確保只有有效的連線會連接到您的應用程式，同時保護合法的最終使用者免遭誤判的捨棄。
- 自動化流量工程系統，可分散或隔離大型容量型 DDoS 攻擊的影響。所有這些服務都會在攻擊到達您的原始伺服器之前，在來源位置隔離，這表示對受這些服務保護的系統的影響較小。
- 應用程式層防禦，與 AWS WAF 結合時不需要變更目前的應用程式架構 (例如，在 AWS 區域或內部部署資料中心)。

AWS 上的傳入資料傳輸不需付費，您也無需為 AWS Shield 緩解的 DDoS 攻擊流量付費。下面的架構圖包括 AWS 全球邊緣網路服務。

此架構包括數個 AWS 服務，可協助提高您的 Web 應用程式抵禦 DDoS 攻擊的耐受力。最佳實務摘要一表提供這些服務及其可提供功能的摘要。AWS 已為每項服務標示最佳實務指示 (BP1、BP2)，以

便在本文件內更易於參考。例如，下一節將討論 Amazon CloudFront 和 Global Accelerator 提供的功能，其包括最佳實務指示 BP1。

表 2 - 最佳實務的摘要

AWS 邊緣	AWS 區域					
	使用 Amazon CloudFront (BP1) 搭配 AWS WAF (BP2)	使用 Global Accelerator (BP1)	使用 Amazon Route 53 (BP3)	使用 Elastic Load Balancing (BP6) 搭配 AWS WAF (BP2)	在 Amazon VPC (BP5) 中使用安全群組和網路 ACL	使用 Amazon EC2 Auto Scaling (BP7)
第 3 層 (例如，UDP 反射) 攻擊緩解	✓	✓	✓	✓	✓	✓
第 4 層 (例如，SYN 洪水) 攻擊緩解	✓	✓	✓	✓		
第 6 層 (例如，TLS) 攻擊緩解	✓	✓	✓	✓		
減少受攻擊面	✓	✓	✓	✓	✓	
擴展以吸收應用程式層流量	✓	✓	✓	✓	✓	✓
第 7 層 (應用程式層) 攻擊緩解	✓	✓(*)	✓	✓	✓(*)	✓(*)

AWS 邊緣	AWS 區域					
過度流量和較大型 DDoS 攻擊的地理隔離和分散	✓	✓	✓			
✓ (*)：如果 AWS WAF 與 Application Load Balancer 一起使用						

另一種提高回應和緩解 DDoS 攻擊準備度的方式是訂閱 AWS Shield Advanced。

客戶可以根據以下獲得量身訂做的偵測：

- 應用程式的特定流量模式。
- 針對第 7 層 DDoS 攻擊的保護，包括 AWS WAF 而不需支付額外的費用。
- 存取 AWS SRT 提供的全天候專業支援。
- 透過 AWS Firewall Manager 集中管理安全政策。
- 成本保護，以防止由於 DDoS 相關的使用尖峰導致的擴展費用。

此選用的 DDoS 緩解服務有助於保護在任何 AWS 區域上託管的應用程式。該服務可在全球為 CloudFront、Route 53 和 Global Accelerator 提供。使用 Shield Advanced 搭配彈性 IP 地址，可讓您保護 Network Load Balancer (NLB) 或 Amazon EC2 執行個體。

使用 AWS Shield Advanced 的優點包括：

- 存取 AWS SRT 以獲得協助，以緩解會影響應用程式可用性的 DDoS 攻擊。
- 透過使用 AWS Management Console、API 和 Amazon CloudWatch 指標和警示，知悉 DDoS 攻擊。
- 存取過去 13 個月所有 DDoS 事件的歷程記錄。

- 存取 AWS Web 應用程式防火牆 (AWS WAF)，而無需針對緩解應用程式層 DDoS 攻擊支付額外的費用 (與 Amazon CloudFront 或 Application Load Balancer 搭配使用時)。
- 與 AWS WAF 搭配使用時，自動設定 Web 流量屬性的基準。
- 無需額外費用，即可存取 AWS Firewall Manager 以取得自動政策強制執行。
- 敏感偵測閾值，會及早將流量路由到 DDoS 緩解系統，並且在與彈性 IP 地址一起使用時，可縮短針對 Amazon EC2 或 Network Load Balancer 的攻擊的緩解時間。
- 成本保護，使您能夠針對 DDoS 攻擊導致的擴展相關成本請求有限的退款。
- AWS Shield Advanced 客戶特定的增強服務水準協議。
- 偵測到 Shield 事件時，AWS SRT 會主動參與。
- 可讓您捆綁資源的保護群組，透過將多個資源視為單一單元，提供一種自助服務方式來自訂應用程式的偵測和緩解範圍。資源分組可提高偵測的準確性，減少誤報，輕鬆實現新建立資源的自動保護，以及加速針對組成單一應用程式的許多資源的攻擊緩解時間。如需保護群組的相關資訊，請參閱 Shield Advanced 保護群組。

如需 AWS Shield Advanced 功能的完整清單以及如需 AWS Shield 的詳細資訊，請參閱 AWS Shield 的運作方式。

主題

DDoS 緩解的最佳實務

在以下各節中，將更深入地介紹 DDoS 緩解的建議最佳實務。如需為靜態或動態 Web 應用程式建置 DDoS 緩解層的快速且易於實作的指南，請參閱如何協助保護動態 Web 應用程式不受 DDoS 攻擊。

基礎設施層防禦 (BP1、BP3、BP6、BP7)

在傳統資料中心環境中，您可以透過使用過度佈建容量、部署 DDoS 緩解系統或借助 DDoS 緩解服務清理流量等技術來緩解基礎設施層 DDoS 攻擊。在 AWS 上，會自動提供 DDoS 緩解功能；但您可以透過選擇最能夠利用這些功能並還能讓您針對過度流量擴展的架構，將應用程式的 DDoS 耐受力最佳化。

協助緩解容量型 DDoS 攻擊的關鍵考量包括確保有足夠的傳輸容量和多樣性，以及保護 AWS 資源 (如 Amazon EC2 執行個體) 不受攻擊流量。

某些 Amazon EC2 執行個體類型支援可以更輕鬆地處理大量流量的功能，例如，高達 100 Gbps 的網路頻寬介面和增強型聯網。這有助於防止已到達 Amazon EC2 執行個體的流量介面壅塞。與傳統實作相比，支援增強型聯網的執行個體可提供更高的 I/O 效能、更高的頻寬和更低的 CPU 利用率。這可提高執行個體處理大量流量的能力，並最終使它們對每秒資料包 (pps) 負載具有高度耐受力。

為實現這種高層級的耐受力，AWS 建議使用 Amazon EC2 專用執行個體，或具有較高聯網輸送量的 Amazon EC2 執行個體，其具有 N 字尾並支援高達 100 Gbps 網路頻寬的增強型聯網 (例如 c6gn.16xlarge 和 c5n.18xlarge 或裸機執行個體 (例如 c5n.metal))。

如需支援 100 GB 網路介面和增強型聯網的 Amazon EC2 執行個體的詳細資訊，請參閱 Amazon EC2 執行個體類型。

增強型聯網所需的模組和必要的 enaSupport 屬性集隨附於 Amazon Linux 2 和最新版本的 Amazon Linux AMI。因此，如果您在支援的執行個體類型上使用 Amazon Linux 的 HVM 版本啟動執行個體，則您的執行個體已啟用增強型聯網。如需詳細資訊，請參閱測試是否已啟用增強型聯網。如需如何啟用增強型聯網的詳細資訊，請參閱 Linux 上的增強型聯網。

Amazon EC2 搭配 Auto Scaling (BP7)

緩解基礎架構和應用程式層攻擊的另一種方法是大規模執行。如果您有 Web 應用程式，則可以使用負載平衡器將流量分配給一些已過度佈建或設定為自動擴展的 Amazon EC2 執行個體。這些執行個體可以處理由於任何原因而發生的流量突增，包括快閃瀏覽或應用程式層 DDoS 攻擊。您可以將 Amazon CloudWatch 警示設定為啟動 Auto Scaling，以便自動擴展您的 Amazon EC2 機群的大小，以回應您所定義的事件 (例如 CPU、RAM、網路 I/O 和甚至自訂指標)。此方法可在請求量意外增加時保護應用程式的可用性。使用 Amazon CloudFront、Application Load Balancer、Classic Load Balancer 或 Network Load Balancer 搭配您的應用程式時，TLS 交涉會由分發 (Amazon CloudFront) 或負載平衡器處理。透過擴展以處理合法請求和 TLS 濫用攻擊，這些功能可協助保護您的執行個體不受基於 TLS 攻擊的影響。

如需使用 Amazon CloudWatch 叫用 Auto Scaling 的詳細資訊，請參閱監控您的 Auto Scaling 群組和執行個體的 Amazon CloudWatch 指標。

Amazon EC2 提供可調整大小的運算容量，以便您可以隨著需求的變更快速擴充或縮減規模。透過自動將執行個體新增至應用程式以擴展 Amazon EC2 Auto Scaling 群組的大小，您可以水平擴展，您還可以使用更大的 EC2 執行個體類型來垂直擴展。

Elastic Load Balancing (BP6)

大型 DDoS 攻擊可能會壓倒單一 Amazon EC2 執行個體的容量。使用 Elastic Load Balancing (ELB)，您可以透過將流量分配到許多後端執行個體，藉此降低應用程式過載的風險。Elastic Load Balancing 可以自動擴展，可讓您在出現非預期的額外流量時 (例如，由於快閃族或 DDoS 攻擊) 管理更大的量。對於在 Amazon VPC 內建置的應用程式，需考慮三個類型的 ELB，具體取決於您的應用程式類型：Application Load Balancer (ALB)、Classic Load Balancer (CLB) 和 Network Load Balancer (NLB)。

對於 Web 應用程式，您可以使用 Application Load Balancer 來根據內容路由流量，並僅接受格式良好的 Web 請求。Application Load Balancer 可封鎖許多常見的 DDoS 攻擊 (如 SYN 洪水或 UDP 反射攻擊)，從而保護您的應用程式不受攻擊。偵測到這些類型的攻擊時，Application Load Balancer 會自動擴展以吸收額外的流量。由於基礎設施層攻擊導致的擴展活動對 AWS 客戶來說是透明的，且不會影響您的帳單。

如需使用 Application Load Balancer 保護 Web 應用程式的詳細資訊，請參閱 Application Load Balancer 入門

對於基於 TCP 的應用程式，您可以使用 Network Load Balancer 以超低延遲將流量路由到目標 (例如 Amazon EC2 執行個體)。Network Load Balancer 的一個關鍵考量是，到達有效接聽程式上負載平衡器的任何流量，都將路由到您的目標，而不會被吸收。您可以使用 Shield Advanced 為彈性 IP 地址設定 DDoS 保護。針對每個可用區域將彈性 IP 地址指派至 Network Load Balancer 時，Shield Advanced 將對 Network Load Balancer 流量套用相關的 DDoS 保護。

如需使用 Network Load Balancer 保護 TCP 應用程式的詳細資訊，請參閱 Network Load Balancer 入門

利用 AWS 節點進行擴展 (BP1、BP3)

存取可高度擴展、多樣化的網際網路連線，可以顯著提高您最佳化延遲和使用者輸送量、吸收 DDoS 攻擊以及隔離故障的能力，同時最大限度地減少對應用程式可用性的影響。AWS 節點提供額外一層的網路基礎設施，可為使用 Amazon CloudFront、Global Accelerator 和 Amazon Route 53 的任何 Web 應用程式提供這些優點。利用這些服務，您可以在邊緣全面保護從 AWS 區域執行的應用程式。

Web 應用程式在邊緣交付 (BP1)

Amazon CloudFront 是一項服務，可用於交付您的整個網站，包括靜態、動態、串流和互動式內容。持續型連線和變動的存留時間 (TTL) 設定可用於從來源卸載流量，即使您未提供可快取的內容亦然。使用這些 CloudFront 功能可減少傳回您的來源的請求和 TCP 連線數，協助保護您的 Web 應用程式免

於遭受 HTTP 洪水。CloudFront 僅接受格式良好的連線，這可協助防範許多常見的 DDoS 攻擊 (例如 SYN 洪水和 UDP 反射攻擊) 到達您的來源。DDoS 攻擊在地理上也會隔離，但接近來源，這可防止影響其他位置的流量。這些功能可大幅提升您的能力，可在大型 DDoS 攻擊期間，仍繼續提供流量給使用者。您可以使用 CloudFront 以保護 AWS 上或網際網路上其他位置的來源。

如果您使用 Amazon S3 在網際網路上提供靜態內容，AWS 建議您使用 Amazon CloudFront 來保護您的儲存貯體。您可以使用來源存取識別 (OAI) 來確保使用者只能使用 CloudFront URL 來存取您的物件。

如需 OAI 的詳細資訊，請參閱使用原始存取身分限制對 Amazon S3 內容的存取。

如需使用 Amazon CloudFront 保護和最佳化 Web 應用程式效能的詳細資訊，請參閱 CloudFront 入門。

使用 AWS Global Accelerator 進一步保護來自來源的網路流量 (BP1)

Global Accelerator 是一項聯網服務，可將使用者流量的可用性和效能提高高達 60%。透過在離您的使用者最近的節點傳入流量並將流量透過 AWS 全球網路基礎設施路由到您的應用程式 (而無論應用程式在單一或多個 AWS 區域中執行)，即可實現此目標。

Global Accelerator 會根據與使用者最接近的 AWS 區域中的效能，將 TCP 和 UDP 流量路由到最佳端點。如果應用程式故障，Global Accelerator 將在 30 秒內提供容錯移轉到下一個最佳端點。Global Accelerator 利用 AWS 全球網路的巨大容量以及與 Shield 的整合 (例如可挑戰新連線嘗試的無狀態 SYN 代理功能)，並僅為合法最終使用者提供服務，以保護應用程式。

即使您的應用程式使用 CloudFront 不支援的通訊協定，或者您正在執行需要全球靜態 IP 地址的 Web 應用程式，您也可以實作具 DDoS 耐受力的架構，其提供與 Web 應用程式在邊緣交付最佳實務相同的許多優點。例如，您可能需要最終使用者可以將其新增到其防火牆允許清單，且不會被任何其他 AWS 客戶使用的 IP 地址。在這些情況下，您可以使用 Global Accelerator 來保護在 Application Load Balancer 上執行的 Web 應用程式，並結合 AWS WAF 以同時偵測和緩解 Web 應用程式層請求洪水。

如需使用 Global Accelerator 保護和最佳化網路流量效能的詳細資訊，請參閱 Global Accelerator 入門。

邊緣的網域名稱解析 (BP3)

Amazon Route 53 是一種高度可用且可擴展的網域名稱系統 (DNS) 服務，可用於將流量導向您的 Web 應用程式。它包括流量、運作狀態檢查和監控、以延遲為基礎的路由和 Geo DNS 等進階功能。這些進階功能可讓您控制服務如何回應 DNS 請求，以提高 Web 應用程式的效能並避免網站中斷。

Amazon Route 53 使用隨機分區和任一傳播分區之類的技術，可協助使用者存取您的應用程式，即使 DNS 服務是 DDoS 攻擊的目標亦然。

使用隨機分區，您委派組中的每個名稱伺服器都會與一組唯一的節點和網際網路路徑對應。這樣可提供更好的容錯能力，並最大限度地減少客戶間的重疊。如果委派組中的一個名稱伺服器無法可用，使用者可以重試並接收來自其他節點的另一個名稱伺服器的回應。

任一傳播分區允許每個 DNS 請求由最佳位置處理，從而分散網路負載並減少 DNS 延遲。這可為使用者提供更快的回應。此外，Amazon Route 53 可以偵測 DNS 查詢的來源和數量中的異常情況，並將來自已知可靠使用者的請求優先處理。

如需使用 Amazon Route 53 將使用者路由到您的應用程式的詳細資訊，請參閱 Amazon Route 53 入門。

應用程式層防禦 (BP1、BP2)

本白皮書目前討論的許多技術，都能有效地緩解基礎設施層 DDoS 攻擊對您的應用程式可用性的影響。為了同時防禦應用程式層攻擊，您需要實作一項架構，以便專門偵測、擴展以吸收和封鎖惡意請求。這是一項重要考量，因為基於網路的 DDoS 緩解系統通常無法有效緩解複雜的應用程式層攻擊。

偵測和篩選惡意 Web 請求 (BP1、BP2)

當您的應用程式在 AWS 上執行時，您可以同時利用 Amazon CloudFront 和 AWS WAF 來協助防禦應用程式層 DDoS 攻擊。

Amazon CloudFront 可讓您快取靜態內容並從 AWS 節點提供服務，這有助於降低來源上的負載。它還可以透過防止非 Web 流量到達您的原始伺服器來協助減少伺服器負載。此外，CloudFront 可以自動關閉來自緩慢讀取或緩慢寫入的攻擊者 (例如，Slowloris) 的連線。

透過使用 AWS WAF，您可以在 CloudFront 分發或 Application Load Balancer 上設定 Web 存取控制清單 (Web ACL)，以根據請求簽章篩選和封鎖請求。每個 Web ACL 都包含您可設定，以字串比對或規則運算式比對一或多個請求屬性的規則，例如，統一資源識別符 (URI)、查詢字串、HTTP 方法或標頭索引鍵。此外，透過使用 AWS WAF 速率型的規則，當符合規則的請求超過您定義的閾值時，您可以自動封鎖惡意人士的 IP 地址。

來自違規用戶端 IP 地址的請求將收到 403 禁止的錯誤回應，並且將保持封鎖，直到請求速率降低到閾值以下為止。這對於緩解偽裝成一般 Web 流量的 HTTP 洪水攻擊非常有用。若要根據 IP 地址信譽封鎖攻擊，您可以使用 IP 比對條件建立規則，或使用 AWS Marketplace 中的賣家為 AWS WAF 提供的受管規則。AWS WAF 直接提供 AWS 受管規則作為受管服務，您可以在其中選擇 IP 信譽規則群

組。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。匿名 IP 清單規則群組包含規則，能封鎖會允許檢視器身分模糊處理的服務請求。這些請求包括來自 VPN、代理、Tor 節點和雲端平台 (包括 AWS) 的請求。AWS WAF 和 CloudFront 還可讓您設定地理限制，以封鎖或允許來自選定國家/地區的請求。這可協助封鎖來自您不預期為使用者提供服務的地理位置的攻擊。

若要幫助識別惡意請求，請檢閱 Web 伺服器日誌或使用 AWS WAF 的記錄和取樣請求功能。透過啟用 AWS WAF 記錄，您可以獲得 Web ACL 分析的流量的詳細資訊。AWS WAF 支援日誌篩選，可讓您指定要記錄哪些 Web 請求以及在檢查後要從日誌中捨棄哪些請求。

日誌中記錄的資訊包括 AWS WAF 收到來自您的 AWS 資源請求的時間、請求的詳細資訊，以及所請求的每個規則的比對動作。取樣請求提供過去三小時內符合您的其中一個 AWS WAF 規則的請求的詳細資料。您可以使用此資訊識別潛在的惡意流量簽章，並建立新規則來拒絕這些請求。如果您看到許多具有隨機查詢字串的請求，請確保僅允許相關的查詢字串參數快取您的應用程式。此技術有助於緩解對來源的快取破壞攻擊。

如果您已訂閱 AWS Shield Advanced，則可以與 AWS Shield 回應團隊 (SRT) 連絡，以協助您建立規則，以緩解損害您的應用程式可用性的攻擊。您可以授與 AWS SRT 對您帳戶的 Shield Advanced 和 AWS WAF API 具有有限的存取權。AWS SRT 僅會在您的明確授權下存取這些 API，以便對您的帳戶進行緩解。如需詳細資訊，請參閱本文件的支援小節。

您可以使用 AWS Firewall Manager 以在整個組織集中設定和管理安全規則，例如 Shield Advanced 保護和 AWS WAF 規則。您的 AWS 組織管理帳戶可以指定一個管理員帳戶，該帳戶有權建立 Firewall Manager 政策。這些政策可讓您定義條件，例如，資源類型和標籤，這些條件會決定套用規則的位置。當您有多個帳戶並希望將防護標準化時，此功能非常有用。

如需以下的詳細資訊：

- AWS WAF 的 AWS 受管規則，請參閱 AWS WAF 的 AWS 受管規則。
- 使用地理限制來限制對 CloudFront 分發的存取，請參閱限制您的內容的地理分佈。
- 使用 AWS WAF，請參閱
  - AWS WAF 入門
  - 記錄 Web ACL 流量資訊
  - 檢視 Web 請求的範例
- 設定速率為基礎的規則，請參閱針對 AWS WAF 使用以速率為基礎的規則保護網站和服務
- 如何使用 Firewall Manager 跨您的 AWS 資源管理 AWS WAF 規則的部署，請參閱
  - Firewall Manager AWS WAF 政策入門。

- Firewall Manager Shield Advanced 政策入門。

受攻擊面減少

架構 AWS 解決方案時的另一個重要考量是限制攻擊者針對您的應用程式的機會。這個概念稱為受攻擊面減少。未暴露於網際網路的資源較難以攻擊，因而可限制攻擊者針對您的應用程式可用性的選項。

例如，如果您不希望使用者直接與某些資源互動，請確定您無法從網際網路存取這些資源。同樣地，請不要在不是通訊所必要的連接埠或通訊協定上接受來自使用者或外部應用程式的通訊。

在下一節，AWS 會提供最佳實務，以引導您減少您的受攻擊面和限制應用程式的網際網路暴露。

主題

將 AWS 資源模糊處理 (BP1、BP4、BP5)

一般來說，使用者可以快速且輕鬆地使用應用程式，而不需將 AWS 資源完全暴露在網際網路上。例如，當您在 Elastic Load Balancing 後面有 Amazon EC2 執行個體時，可能不需要公開存取執行個體本身。相反地，您可以為使用者提供對特定 TCP 連接埠上 Elastic Load Balancing 的存取權，並且只允許 Elastic Load Balancing 與執行個體通訊。您可以透過在 Amazon Virtual Private Cloud (Amazon VPC) 內設定安全群組和網路存取控制清單 (NACL) 來進行設定。Amazon VPC 可讓您在 AWS 雲端中佈建一個邏輯隔離的部分，在您定義的虛擬網路中啟動 AWS 資源。

安全群組和網路 ACL 類似，因為它們可讓您在您的 VPC 中控制對 AWS 資源的存取權。但是，安全群組可讓您在執行個體層級控制傳入和傳出流量，而網路 ACL 則在 VPC 子網路層級提供類似的功能。使用安全群組或網路 ACL 無需支付額外的費用。

安全群組和網路存取控制清單 (網路 ACL) (BP5)

您可以選擇在啟動執行個體時指定安全群組，還是稍後將執行個體與安全群組相關聯。通往安全群組的所有網際網路流量都會被隱含地拒絕，除非您建立一個允許規則以允許流量。例如，如果您有一個使用 Elastic Load Balancing 的 Web 應用程式和多個 Amazon EC2 執行個體，則可能會決定為 Elastic Load Balancing 建立一個安全群組 (Elastic Load Balancing 安全群組)，以及為執行個體建立一個安全群組 (Web 應用程式伺服器安全群組)。然後，您可以建立允許規則，以允許通往 ELB 安全群組的網際網路流量，以及另一個規則，以允許從 ELB 安全群組到 Web 應用程式伺服器安全群組的流量。這可確保網際網路流量無法直接與您的 Amazon EC2 執行個體通訊，使得攻擊者更難瞭解和影響您的應用程式。

建立網路 ACL 時，可以同時指定允許和拒絕規則。當您想要明確拒絕對您的應用程式的特定類型流量時，這會很有幫助。例如，您可以定義應拒絕存取整個子網路的 IP 地址 (CIDR 範圍形式)、通訊協定和目的地連接埠。如果您的應用程式僅用於 TCP 流量，則可以建立一個規則來拒絕所有 UDP 流量，反之亦然。此選項在回應 DDoS 攻擊時非常有用，因為當您知道來源 IP 或其他簽章時，它可讓您建立自己的規則來緩解攻擊。

如果已訂閱 AWS Shield Advanced，則可以將彈性 IP 地址註冊為受保護資源。對已註冊為受保護資源的彈性 IP 地址的 DDoS 攻擊可以更快速偵測到，從而縮短緩解時間。偵測到攻擊後，DDoS 緩解系統會讀取與目標彈性 IP 對應的網路 ACL，並在 AWS 網路邊界強制執行。這會顯著降低您受到多個基礎設施層 DDoS 攻擊影響的風險。

如需設定安全群組和網路 ACL，以針對 DDoS 耐受力最佳化的詳細資訊，請參閱如何透過減少受攻擊面協助為 DDoS 攻擊做好準備。

如需使用 Shield Advanced 搭配彈性 IP 地址作為受保護資源的詳細資訊，請參閱訂閱 AWS Shield Advanced 的步驟。

保護您的來源 (BP1、BP5)

如果您使用 Amazon CloudFront 搭配位於 VPC 內的來源，您可能希望確保只有您的 CloudFront 分發才能將請求轉送到您的來源。使用 Edge-to-Origin 請求標頭，當 CloudFront 將請求轉送到您的來源時，您可以新增或覆寫現有請求標頭的值。您可以使用來源自訂標頭 (例如 X-Shared-Secret 標頭)，以協助驗證對您的來源進行的請求是否從 CloudFront 傳送。

如需使用來源自訂標頭保護您的來源的詳細資訊，請參閱將自訂標頭新增到來源請求和限制對 Application Load Balancer 的存取。

如需實作範例解決方案以自動輪換來源存取限制的來源自訂標頭值的指南，請參閱如何使用 AWS WAF 和 Secrets Manager 增強 Amazon CloudFront 來源安全性。

或者，您可以使用 AWS Lambda 函數來自動更新安全群組規則，以便僅允許 CloudFront 流量。這可透過協助確保惡意使用者在存取 Web 應用程式時，無法略過 CloudFront 以及 AWS WAF，從而提高來源的安全性。

如需如何透過自動更新安全群組來保護您的來源的詳細資訊，請參閱 X-Shared-Secret 標題，請參閱如何使用 AWS Lambda 自動更新 Amazon CloudFront 和 AWS WAF 的安全群組。

保護 API 端點 (BP4)

通常，當您必須向公眾公開 API 時，可能會有 API 前端成為 DDoS 攻擊目標的風險。若要協助降低風險，您可以使用 Amazon API Gateway 作為 Amazon EC2、AWS Lambda 或其他位置上執行的應用程

式的入口通道。透過使用 Amazon API Gateway，您不需要自己的伺服器做為 API 前端，而您可以將應用程式的其他元件模糊處理。透過使偵測應用程式的元件更加困難，您可以協助防止這些 AWS 資源成為 DDoS 攻擊的目標。

當您使用 Amazon API Gateway 時，您可以從兩個類型的 API 端點選擇。第一個是預設選項：透過 Amazon CloudFront 分發存取的邊緣最佳化 API 端點。但是，該分發由 API Gateway 建立和管理，因此您無法控制它。第二個選項是使用從部署 REST API 所在的相同 AWS 區域存取的區域 API 端點。AWS 建議您使用第二個類型的端點，並將其與您自己的 Amazon CloudFront 分發相關聯。這使得您能夠控制 Amazon CloudFront 分發，並且能夠使用 AWS WAF 做為應用程式層保護。此模式可讓您存取在整個 AWS 全球邊緣網路擴展的 DDoS 緩解容量。

使用 Amazon CloudFront 和 AWS WAF 搭配 Amazon API Gateway 時，請設定以下選項：

- 設定分發的快取行為，將所有標頭轉送到 API Gateway 區域端點。透過這麼做，CloudFront 會將內容視為動態並略過快取內容。
- 透過在 API Gateway 中設定 API 金鑰值，將分發設定為包含來源自訂標頭 `x-api-key`，以保護 API Gateway 免遭直接存取。
- 透過為 REST API 中的每個方法設定標準或高載速率限制，保護後端免於遭受過度流量。

如需使用 Amazon API Gateway 建立 API 的詳細資訊，請參閱 Amazon API Gateway 入門。

作業技術

本白皮書中的緩解技術可協助您建置本質上對 DDoS 攻擊具耐受力的應用程式。在許多情況下，瞭解 DDoS 攻擊何時針對您的應用程式使得您可以採取緩解步驟也很有用。本節討論瞭解異常行為、警示和自動化、大規模管理保護以及與 AWS 交涉以取得其他支援的最佳實務。

主題

可見性

當關鍵作業指標實質上偏離預期值時，攻擊者可能會嘗試以您的應用程式可用性做為目標。熟悉應用程式的正常行為意味著您可以在偵測到異常時更快速地採取行動。Amazon CloudWatch 可以透過監控您在 AWS 上執行的應用程式幫助您。例如，您可以收集和追蹤指標、收集和監控日誌檔、設定警示，以及自動回應 AWS 資源中的變更。

如果在架構應用程式時遵循具 DDoS 耐受力的參考架構，常見的基礎設施層攻擊將在連接您的應用程式之前遭到封鎖。如果您已訂閱 AWS Shield Advanced，則可以存取許多 CloudWatch 指標，其會指出您的應用程式正成為目標。例如，您可以設定警示，以在發生 DDoS 攻擊時通知您，使得您可以檢查應用程式的運作狀態並決定是否要與 AWS SRT 交涉。您可以設定 `DDoSDetected` 指標以告知您是否偵測到攻擊。如果您希望根據攻擊量收到警示，還可以使用 `DDoSAttackBitsPerSecond`、`DDoSAttackPacketsPerSecond` 或 `DDoSAttackRequestsPerSecond` 指標。您可以透過將 CloudWatch 與您自己的工具整合，或使用第三方提供的工具 (如 Slack 或 PagerDuty) 來監控這些指標。

應用程式層攻擊可以提升許多 Amazon CloudWatch 指標。如果您使用 AWS WAF，則可以使用 CloudWatch 來監控並針對您在 AWS WAF 設定要允許、計數或封鎖的相關請求的增加啟動警示。這可讓您在流量層級超過應用程式可處理的層級時收到通知。您還可以使用在 CloudWatch 中追蹤的 Amazon CloudFront、Amazon Route 53、Application Load Balancer、Network Load Balancer、Amazon EC2 和 Auto Scaling 指標來偵測可能指出 DDoS 攻擊的變更。

建議的 CloudWatch 指標一表列出經常用於偵測和應對 DDoS 攻擊的 CloudWatch 指標的說明。

表 3 - 建議的 Amazon CloudWatch 指標

主題	指標	描述
AWS Shield Advanced	DDoSDetected	指出特定 Amazon 資源名稱 (ARN) 的 DDoS 事件。
AWS Shield Advanced	DDoSAttackBitsPerSecond	在特定 ARN 的 DDoS 事件期間觀察到的位元組數。本指標僅適用於第 3/4 層的 DDoS 事件。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	在特定 ARN 的 DDoS 事件期間觀察到的封包數。本指標僅適用於第 3/4 層的 DDoS 事件。
AWS Shield Advanced	DDoSAttackRequestsPerSecond	在特定 ARN 的 DDoS 事件期間觀察到的請求數。本指標僅適用於第 7 層的 DDoS 事件，並只會針對最重大的第 7 層事件回報。
AWS WAF	AllowedRequests	允許的 Web 請求數目。
AWS WAF	BlockedRequests	封鎖的 Web 請求數目。
AWS WAF	CountedRequests	計入的 Web 請求數目。
AWS WAF	PassedRequests	已傳遞的請求數。這僅用於經過規則群組評估而不未符合任何規則群組規則的請求。
Amazon CloudFront	請求	HTTP/S 請求數。
Amazon CloudFront	TotalErrorRate	HTTP 狀態碼為 4xx 或 5xx 的所有請求的百分比。
Amazon Route 53	HealthCheckStatus	運作狀態檢查端點的狀態。

主題	指標	描述
Application Load Balancer	ActiveConnectionCount	從用戶端到負載平衡器以及從負載平衡器到目標的並行作用中 TCP 連線總數。
Application Load Balancer	ConsumedLCUs	負載平衡器所使用的負載平衡器容量單位 (LCU) 數目。
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	負載平衡器產生的 HTTP 4xx 或 5xx 用戶端錯誤碼數目。
Application Load Balancer	NewConnectionCount	從用戶端到負載平衡器以及從負載平衡器到目標建立的新 TCP 連線總數。
Application Load Balancer	ProcessedBytes	負載平衡器處理的位元組總數。
Application Load Balancer	RejectedConnectionCount	因負載平衡器已達其連線數目上限而拒絕的連線數目。
Application Load Balancer	RequestCount	處理的請求數。
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之後到收到目標回應之前所經歷的時間 (秒)。
Application Load Balancer	UnHealthyHostCount	視為不健康的目標數目。
Network Load Balancer	ActiveFlowCount	從用戶端到目標的並行 TCP 流程 (或連線) 總數。
Network Load Balancer	ConsumedLCUs	負載平衡器所使用的負載平衡器容量單位 (LCU) 數目。

主題	指標	描述
Network Load Balancer	NewFlowCount	在期間內，從用戶端到目標建立的新 TCP 流程 (或連線) 總數。
Network Load Balancer	ProcessedBytes	負載平衡器所處理的位元組總數，包含 TCP/IP 標頭。
Global Accelerator	NewFlowCount	在期間內，從用戶端到端點建立的新 TCP 和 UDP 流程 (或連線) 總數。
Global Accelerator	ProcessedBytesIn	加速器所處理的傳入位元組總數，包括 TCP/IP 標頭。
Auto Scaling	GroupMaxSize	Auto Scaling 群組的最高大小。
Amazon EC2	CPUUtilization	目前正在使用的已配置 EC2 運算單位百分比。
Amazon EC2	NetworkIn	執行個體在所有網路介面上收到的位元組數目。

如需使用 Amazon CloudWatch 偵測您的應用程式上的 DDoS 攻擊的詳細資訊，請參閱 Amazon CloudWatch 入門。

若要探索使用上表中的部分指標建置的儀表板範例，請參閱自訂基準監控系統

AWS 包括幾個額外的指標和警示，以通知您相關的攻擊並協助您監控應用程式的資源。AWS Shield 主控台或 API 提供每個帳戶的事件摘要和偵測到的攻擊的詳細資料。

此外，全球威脅環境儀表板還提供 AWS 偵測到的所有 DDoS 攻擊的摘要資訊。此資訊可能有助於更好地瞭解更多應用程式母體中的 DDoS 威脅，以及攻擊趨勢，並將其與您可能觀察到的攻擊進行比較。

如果您已訂閱 AWS Shield Advanced，則服務儀表板將顯示在受保護資源上偵測到的事件的其他偵測和緩解指標及網路流量詳細資料。AWS Shield 會依多個維度評估通往您的受保護資源的流量。偵測到異常時，AWS Shield 會建立事件並報告觀察到異常情況的通訊維度。透過進行的緩解，這可以保護您的資源不會收到過度流量和符合已知 DDoS 事件簽章的流量。

當 Web ACL 與受保護的資源相關聯時，偵測指標會基於取樣的網路流程或 AWS WAF 日誌。緩解指標會基於 Shield 的 DDoS 緩解系統觀察到的流量。緩解指標是對傳入您的資源的流量的更精確衡量。

網路最高貢獻者量度可讓您瞭解在偵測到的事件期間流量來自何處。您可以檢視最大量的貢獻者，並依通訊協定、來源連接埠和 TCP 旗標等面向來排序。最高貢獻者度量包括在各種維度的資源上觀察到的所有流量的指標。它提供額外的指標維度，供您用來瞭解事件期間傳送到您的資源的網路流量。

服務儀表板還包括為緩解 DDoS 攻擊而自動採取的動作的詳細資料。這些資訊可以讓您更輕鬆調查異常、探索流量的維度，並更好地瞭解 Shield Advanced 為保護您的可用性而採取的行動。

可協助您瞭解針對您的應用程式流量的另一個工具是 VPC 流程日誌。在傳統網路上，您可以使用網路流程日誌來疑難排解連線和安全問題，並確保網路存取規則如預期般運作。透過使用 VPC 流程日誌，您可以擷取進入和來自 VPC 中網路介面的 IP 流量的相關資訊。

每個流程日誌記錄包括以下內容：來源和目的地 IP 地址、來源連接埠和目標連接埠、通訊協定，以及擷取時段期間傳輸的封包和位元組數。您可以使用此資訊來協助識別網路流量中的異常，並識別特定的攻擊向量。例如，大多數 UDP 反射攻擊都有特定的來源連接埠，如用於 DNS 反射的來源連接埠 53。這是一個清楚的攻擊簽章，您可以在流程日誌記錄中識別。作為回應，您可以選擇在執行個體層級封鎖特定來源連接埠，或者在應用程式不需要時建立網路 ACL 規則來封鎖整個通訊協定。

如需使用 VPC 流程日誌識別網路異常和 DDoS 攻擊向量的詳細資訊，請參閱 VPC 流程日誌和 VPC 流程日誌 - 記錄和檢視網路流量。

跨多個帳戶的可見性和保護管理

若您跨多個 AWS 帳戶操作並且需要保護多個元件，使用能讓您大規模操作並降低營運開銷的技術，可增加您的緩解能力。管理多個帳戶中受 AWS Shield Advanced 保護的資源時，可以使用 AWS Firewall Manager 和 AWS Security Hub 來設定集中式監控。使用 Firewall Manager，您可以建立一個安全政策，在所有帳戶中強制執行 DDoS 保護合規。您可以將這兩項服務一起使用，以跨多個帳戶管理受保護的資源，並集中監控這些資源。

Security Hub 會自動與 Firewall Manager 整合，允許 Shield Advanced 客戶在單一儀表板中檢視安全發現結果，以及其他高優先順序的安全警示和合規性狀態。例如，當 Shield Advanced 偵測到通往範圍內任何 AWS 帳戶中受保護資源的異常流量時，此發現結果將在 Security Hub 主控台中顯示。如果

設定，Firewall Manager 可以透過將資源建立為受 Shield Advanced 保護的資源來自動讓其合規，然後在資源處於合規狀態時更新 Security Hub。

如需集中監控 Shield 受保護的資源的詳細資訊，請參閱為 DDoS 事件設定集中監控和自動修復不合規的資源。

支援

如果您遇到攻擊，則還可以從評估威脅和檢閱應用程式架構獲得的 AWS 支援而受益，或者您可能想要請求其他協助。在發生實際事件之前，務必為 DDoS 攻擊建立回應計劃。本白皮書中概述的最佳實務旨在成為您在啟動應用程式之前實作的主動測量，但針對您的應用程式的 DDoS 攻擊仍可能會發生。請檢閱本節中的選項，以判斷最適合您的案例的支援資源。您的帳戶團隊可以評估您的使用案例和應用程式，並協助解決您遇到的特定問題或難題。

如果您 AWS 在上執行生產工作負載，請考慮訂閱 Business Support，其讓您可以全天候連絡能協助您解決 DDoS 攻擊問題的雲瑞支援工程師。如果您執行任務關鍵型工作負載，請考慮採用 Enterprise Support，其提供打開關鍵案例的能力，並可從資深雲端支援工程師獲得最快速的回應。

如果您已訂閱 AWS Shield Advanced 並同時訂閱 Business Support 或 Enterprise Support，則可以設定 Shield 主動參與。它可讓您設定運作狀態檢查、與您的資源相關聯，並提供全天候的作業連絡資訊。當 Shield 偵測到 DDoS 跡象並且您的應用程式運作狀態檢查顯示出降級跡象，AWS SRT 將主動與您連絡。這是我們建議的參與模式，因為它允許最快速的 AWS SRT 回應時間，並且能讓 AWS SRT 在與您建立連絡之前開始疑難排解。

主動參與功能需要您設定 Route 53 運作狀態檢查，以準確測量應用程式的運作狀態，並與 Shield Advanced 保護的資源相關聯。在 Shield 主控台中將 Route 53 運作狀態檢查相關聯後，Shield Advanced 偵測系統會使用運作狀態檢查狀態作為應用程式運作狀態的指示。Shield Advanced 基於運作狀態的偵測功能將確保您會收到通知，並且在應用程式運作狀態不佳時能更快地進行緩解。AWS SRT 將與您連絡，以疑難排解運作狀態不佳的應用程式是否成為 DDoS 攻擊的目標，並視需要進行其他緩解。

完成主動參與的組態包括在 Shield 主控台中新增連絡人詳細資料。AWS SRT 將使用此資訊與您連絡。如果您有任何特定連絡人需求或偏好設定，您最多可以設定 10 個連絡人，並提供其他備註。主動參與連絡人應擔任全天候的職務，例如，安全作業中心或可立即連絡的個人。

您可以為回應時間極為重要的所有資源或選定的重要生產資源啟用主動參與。這會透過僅為這些資源指派運作狀態檢查來實現。

如果您發生了影響應用程式可用性的 DDoS 相關事件，您還可以透過使用 AWS 支援主控台或支援 API 來建立 AWS Support 案例，以升級到 AWS SRT。

結論

本白皮書中概述的最佳實務會透過防範許多常見的基礎設施和應用程式層 DDoS 攻擊，協助您建置具 DDoS 耐受力的架構，來保護您的應用程式可用性。建置應用程式時遵循這些最佳實務的程度，將影響您可以緩解的 DDoS 攻擊的類型、向量和數量。您可以在不訂閱 DDoS 緩解服務的情況下納入耐受力。透過選擇訂閱 AWS Shield Advanced，您可以獲得額外的支援、可見性、緩解和成本保護功能，可進一步保護已具耐受力的應用程式架構。

作者群

此文件的作者包括：

- AWS 週邊防護 Jeffrey Lyon
- AWS 安全專家 TAM Rodrigo Ferroni
- AWS 解決方案架構師 Dmitriy Novikov
- AWS 解決方案架構師 Achraf Souk
- AWS 解決方案架構師 Yoshihisa Nakatani

資源

深入閱讀：

- AWS 上 DDoS 緩解的最佳實務
- 實作 AWS WAF 的指導方針
- SID324 - re:Invent 2017: Automating DDoS Response in the Cloud
- CTD304 - re:Invent 2017: Dow Jones & Wall Street Journal's Journey to Manage Traffic Spikes While Mitigating DDoS & Application Layer Threats
- CTD310 - re:Invent 2017: Living on the Edge, It's Safer Than You Think! 利用 Amazon CloudFront、AWS Shield 和 AWS WAF 打造強大功能
- SEC407 - re:Invent 2019: A defense-in-depth approach to building web applications
- SEC321 - re:Invent 2020: Get ahead of the curve with DDoS Response Team escalations
- William Hill：利用 AWS 實現高效能 DDoS 防護

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
白皮書更新	更新以包含最新的建議和功能。新增 AWS Global Accelerator 以做為邊緣全面保護的一部分。AWS Firewall Manager，用於集中監控 DDoS 事件和自動修復不合規的資源。	2021 年 9 月 21 日
白皮書更新	更新以澄清偵測和篩選惡意 Web 請求 (BP1、BP2) 小節的快取破壞情況，以及擴展以吸收 (BP6) 小節中的 ELB 和 ALB 使用量。更新圖表和表 2，將標記為「區域選擇」標示為 BP8。更新 BP7 小節，加上更多詳細資料。	2019 年 12 月 18 日
白皮書更新	更新以包含 AWS WAF 記錄作為最佳實務。	2018 年 12 月 1 日
白皮書更新	更新以包括 AWS Shield、AWS WAF 功能、AWS Firewall Manager 和相關的最佳實務。	2018 年 6 月 1 日
白皮書更新	新增規範性的架構指南，並更新以包括 AWS WAF。	2016 年 6 月 1 日
初次出版	發佈白皮書。	2015 年 6 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。