AWS 白皮書

AWS 雲端的 Web 應用程式託管

AWS 雲端的 Web 應用程式託管: AWS 白皮書

Table of Contents

AWS 雲端的 Web 應用程式託管

出版日期：2021 年 8 月 20 日 (文件修訂)

摘要

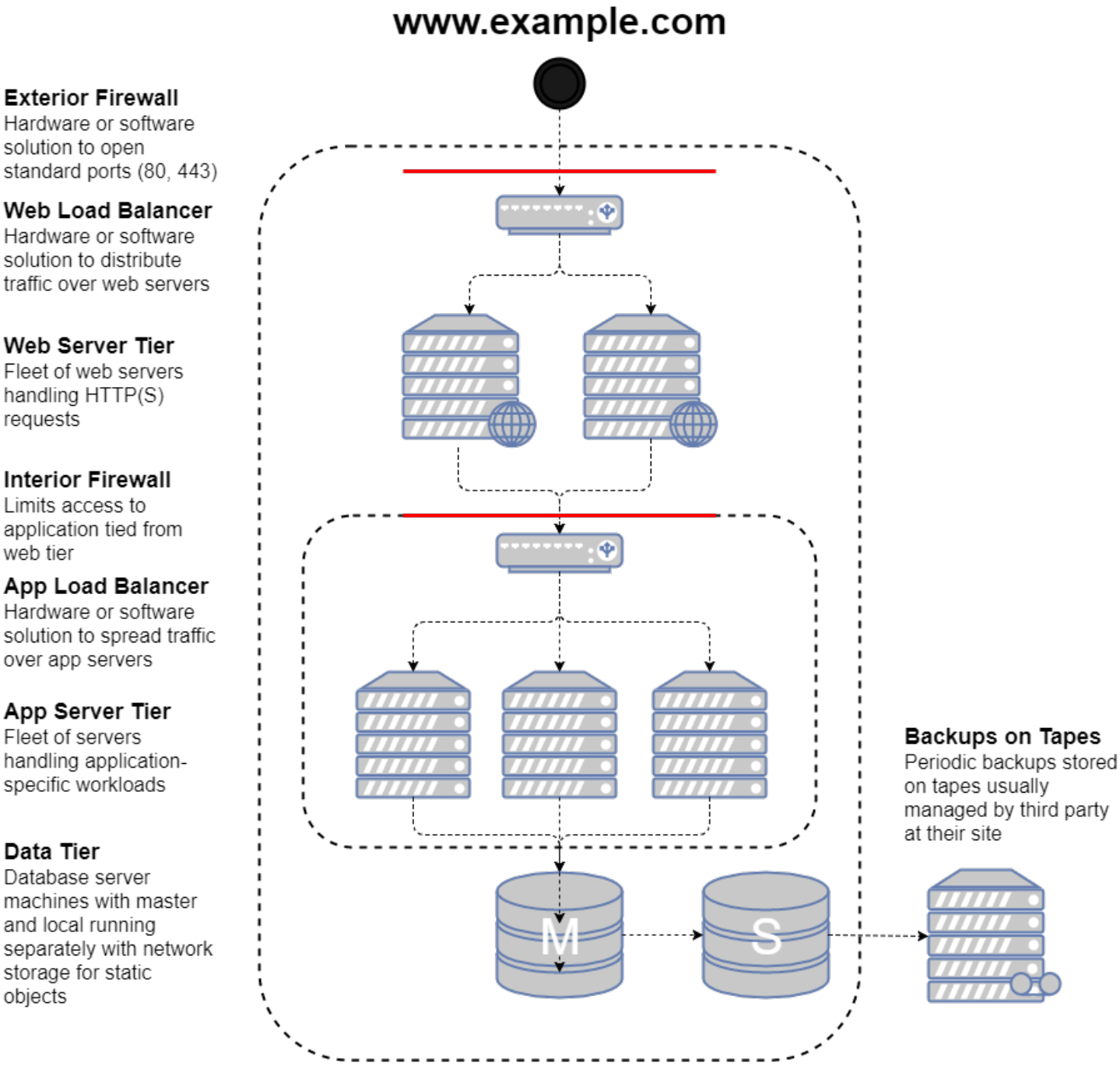
傳統的內部部署 Web 架構需要複雜的解決方案和準確的預留容量預測，以確保可靠性。密集的尖峰流量期間和流量模式的大幅波動會導致昂貴硬體的利用率低。這會導致維護閒置硬體的高營運成本，並且對未充分利用硬體的資本使用效率低。

Amazon Web Services (AWS) 為要求嚴苛的 Web 應用程式提供可靠、可擴展、安全、高效能的基礎設施。此基礎設施可幾乎即時將 IT 成本與客戶流量模式相符。

本白皮書的預期對象為希望瞭解如何在雲端中執行傳統 Web 架構以實現彈性、可擴展性和可靠性的 IT 經理和系統架構師。

傳統 Web 託管概觀

可擴展的 Web 託管是一個已知的問題空間。下圖描述的傳統 Web 託管架構會實作通用的三層 Web 應用程式模型。在此模型中，架構可分為表示層、應用程式層和持久層。可擴展性是透過在這些層增加主機來提供。該架構還有內建的效能、容錯移轉和可用性功能。傳統的 Web 託管架構只需進行少量修改，即可輕鬆地移植到 AWS 雲端。



傳統的 Web 託管架構

以下小節將說明為何應在 AWS 雲端中部署此類架構以及做法。

使用 AWS 在雲端託管 Web 應用程式

您應該問的第一個問題會涉及將託管解決方案的典型 Web 應用程式移至 AWS 雲端的價值。如果您認為雲端適合您，則將需要一個合適的架構。本小節將協助您評估 AWS 雲端解決方案。它會將在雲端部署您的 Web 應用程式與內部部署比較，呈現用於託管應用程式的 AWS 雲端架構，並討論 AWS 雲端架構解決方案的重要元件。

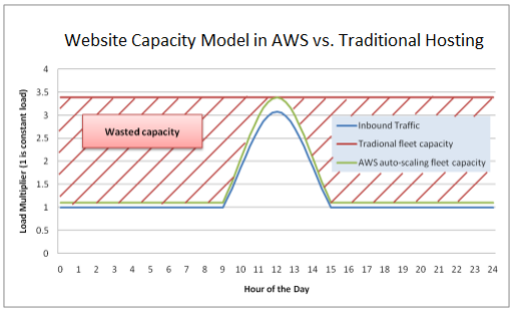
AWS 如何解決常見的 Web 應用程式託管問題

如果您負責執行 Web 應用程式，則可能會面臨各種基礎設施和架構的問題，AWS 可以為這些問題提供無縫且具成本效益的解決方案。以下是使用 AWS 相較於傳統託管模型的一些優點。

處理尖峰所需的大型機群具成本效益的替代方案

在傳統的託管模型中，您必須佈建伺服器來處理尖峰容量。未使用的週期會在尖峰期之外浪費。AWS 託管的 Web 應用程式可以利用額外伺服器的隨需佈建，因此您可以根據實際流量模式不斷調整容量和成本。

例如，下圖顯示的 Web 應用程式，其使用率尖峰從上午 9:00 到下午 3:00，且當天剩餘時間的使用率較少。基於實際流量趨勢的自動擴展方法 (僅在需要時佈建資源)，將減少容量浪費和成本降低 50% 以上。



典型託管模型中浪費容量的範例

用於處理未預期流量尖峰的可擴展解決方案

與傳統託管模型相關聯的佈建速度緩慢導致的更嚴重後果是，無法及時回應非預期的流量尖峰。在主流媒體中提及某網站之後，由於流量出現未預期的尖峰，使得 Web 應用程式變得無法使用有許多相關報導。在 AWS 雲端中，協助 Web 應用程式擴展以符合規律流量尖峰的相同隨需功能也可以處理非預期的負載。新主機可以啟動並在幾分鐘內提供使用，且當流量回到正常時，它們也可以同樣快速地離線。

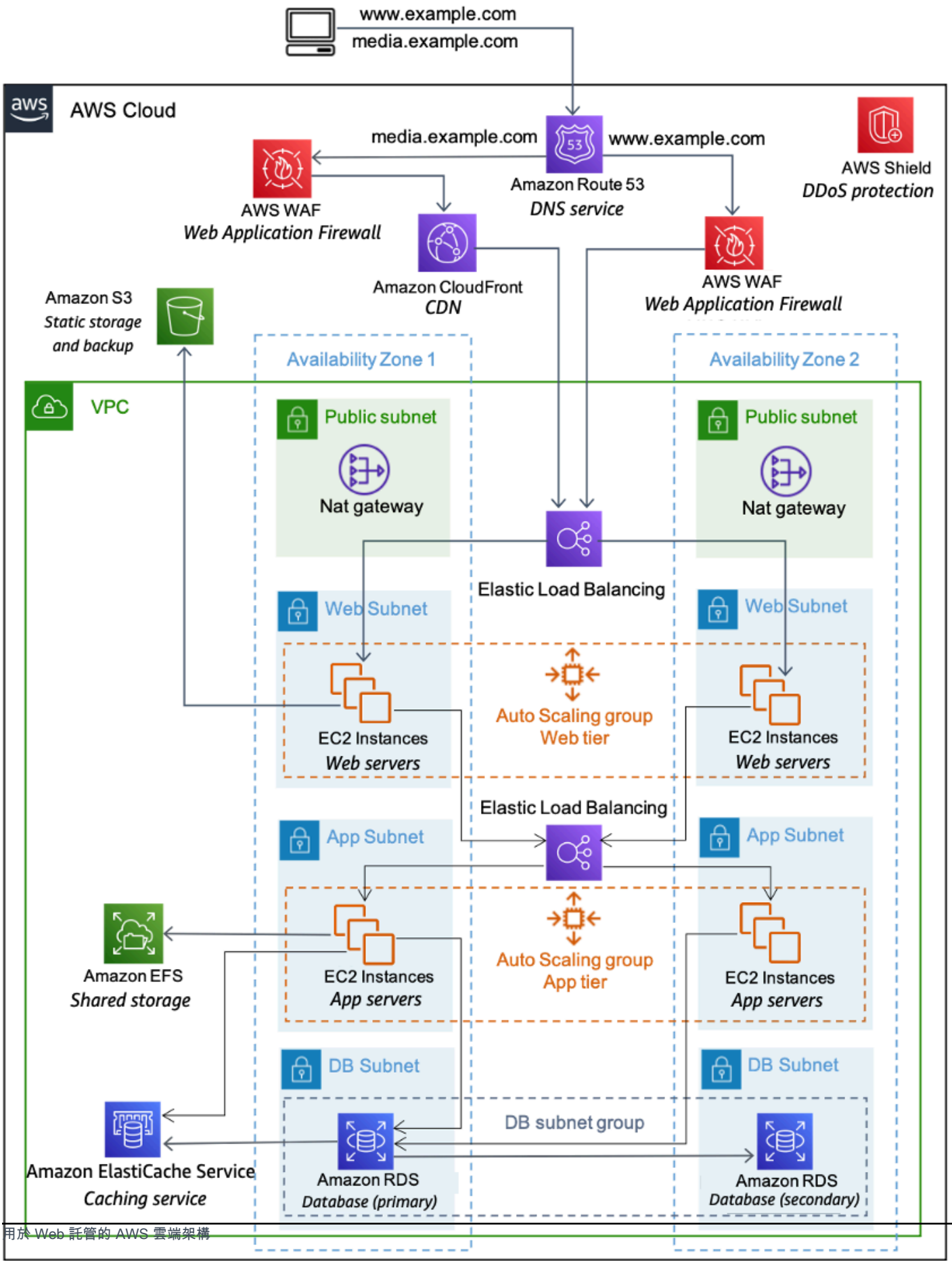
用於測試、負載、測試和再製環境的隨需解決方案

為生產 Web 應用程式建置和維護傳統託管環境的硬體成本不會隨著生產機群而停止。通常，您需要建立生產前、測試和測試機群，以確保 Web 應用程式在開發生命週期的每個階段的品量。雖然您可以進行各種最佳化，以確保盡可能使用此測試硬體，但這些並行機群並不總是能以最佳方式使用，而且許多昂貴的硬體會長時間未使用。

在 AWS 雲端中，您可以隨需佈建測試機群。這不僅讓您不需在實際使用提早幾天或幾個月佈建資源，同時讓您可以在不需要時有靈活性可撤下基礎設施元件。此外，您還可以在負載測試期間模擬 AWS 雲端上的使用者流量。您還可以將這些並行機群用作新生產版本的臨時環境。這可讓您快速從目前的生產切換到新應用程式版本，而只有少量或幾乎沒有服務中斷。

用於 Web 託管的 AWS 雲端架構

下圖提供該典型 Web 應用程式架構的另一個觀點，以及它如何利用 AWS 雲端運算基礎設施。


www.example.com
media.example.com
AWS Cloud
media.example.com
www.example.com
AWS Shield
DDoS protection
AWS WAF
Web Application Firewall
Amazon Route 53
DNS service
Amazon CloudFront
CDN
AWS WAF
Web Application Firewall
Amazon S3
Static storage and backup
Availability Zone 1
Availability Zone 2
VPC
Public subnet
Nat gateway
Public subnet
Nat gateway
Elastic Load Balancing
Web Subnet
Web Subnet
EC2 Instances
Web servers
Auto Scaling group
Web tier
EC2 Instances
Web servers
Elastic Load Balancing
App Subnet
App Subnet
Amazon EFS
Shared storage
EC2 Instances
App servers
Auto Scaling group
App tier
EC2 Instances
App servers
DB Subnet
DB Subnet
DB subnet group
Amazon ElastiCache Service
Caching service
Amazon RDS
Database (primary)
Amazon RDS
Database (secondary)

AWS 上 Web 託管架構的範例

1. 使用 Amazon Route 53 的 DNS 服務 - 提供 DNS 服務以簡化網域管理。
2. 使用 Amazon CloudFront 的邊緣快取 - Edge 會快取大量內容，以減少對客戶的延遲。
3. 使用 AWS WAF 的 Amazon CloudFront 的邊緣安全性 - 透過客戶定義的規則篩選惡意流量，包括跨網站指令碼 (XSS) 和 SQL Injection。
4. 使用 Elastic Load Balancing (ELB) 的負載平衡 - 讓您能夠跨多個可用區域和 AWS Auto Scaling 群組分散負載，以實現服務的備援和解耦。
5. 使用 AWS Shield 的 DDoS 保護 - 自動保護您的基礎設施免受最常見的網路和傳輸層 DDoS 攻擊。
6. 安全群組的防火牆 - 將安全性移至執行個體，以便為 Web 伺服器和應用程式伺服器提供具狀態的主機層級防火牆。
7. 使用 Amazon ElastiCache 快取 - 使用 Redis 或 Memcached 提供快取服務，以去除應用程式和資料庫的負載，並降低頻繁請求的延遲。
8. 使用 Amazon Relational Database Service (Amazon RDS) 的受管資料庫 - 使用六個可能的資料庫引擎建立高可用性、多可用區域資料庫架構。
9. 使用 Amazon Simple Storage Service (Amazon S3) 的靜態儲存和備份 - 為備份和靜態資產 (如影像和影片) 實現簡單的基於 HTTP 的物件存放區。

AWS Web 託管架構的重要元件

以下小節概述部署在 AWS 雲端中的 Web 託管架構的一些重要元件，並說明它們與傳統的 Web 託管架構有何不同。

網路管理

在 AWS 雲端中，能夠將您的網路與其他客戶的網路劃分，可實現更安全和可擴展的架構。雖然安全群組提供主機層級的安全性 (請參閱主機安全小節)，但 Amazon Virtual Private Cloud (Amazon VPC) 能讓您在邏輯上隔離和您定義的虛擬網路中啟動資源。

Amazon VPC 是一項服務，可讓您完整控制 AWS 中聯網設定的詳細資訊。此控制項的範例包括為 Web 伺服器建立面向公眾的子網路，以及為資料庫建立無法存取網際網路的私有子網路。此外，Amazon VPC 可讓您使用硬體虛擬私有網路 (VPN) 建立混合架構，並將 AWS 雲端用作您自己資料中心的擴充。

除了對您的網路的傳統 IPv4 支援之外，Amazon VPC 還包括 IPv6 支援。

內容交付

若您的 Web 流量分散在各地，在全球範圍內複寫整個基礎設施並非總是可行，並且一定不具成本效益。內容交付網路 (CDN) 讓您能夠利用其節點的全域網路，將 Web 內容 (如影片、網頁、影像等) 的快取複本交付給客戶。為了減少回應時間，CDN 會利用離客戶最近的節點或原始請求位置來減少回應時間。由於 Web 資產從快取交付，因此輸送量會顯著提高。針對動態資料，可以將許多 CDN 設定為從原始伺服器擷取資料。

您可以使用 CloudFront 運用節點的全球網路交付您的網站，包括動態、靜態和串流內容。CloudFront 會自動將對內容的請求自動路由到最近的節點，因此能以最佳的效能發佈內容。CloudFront 經過最佳化，可與其他 AWS 服務，如 Amazon S3 和 Amazon Elastic Compute Cloud (Amazon EC2) 搭配使用。CloudFront 也可與存放您最新版本原始檔案的任何非 AWS 原始伺服器的原始伺服器完美搭配。

與其他 AWS 服務一樣，使用 CloudFront 沒有合約或每月承諾 - 您只需為您透過服務實際交付的內容多寡付費。

此外，Web 應用程式基礎設施中邊緣快取的任何現有解決方案，都應能在 AWS 雲端中正常運作。

管理公有 DNS

將 Web 應用程式移至 AWS 雲端需要進行一些網域名稱系統 (DNS) 的變更。為協助您管理 DNS 路由，AWS 提供 Amazon Route 53，這是一種高度可用且可擴展的雲端 DNS Web 服務。Route 53 旨在為開發人員和企業提供一種非常可靠且經濟實惠的方式，將名稱 (如 www.example.com) 轉換為電腦用於互相連接的數字 IP 地址 (如 192.0.2.1)，將最終使用者路由到網際網路應用程式。Route 53 也可與 IPv6 完全相容。

主機安全

除了在邊緣處進行入站網路流量篩選之外，AWS 還建議 Web 應用程式在主機層級套用網路流量篩選。Amazon EC2 提供名為安全群組的功能。安全群組類似於入站網路防火牆，您可以為其指定允許存取 EC2 執行個體的通訊協定、連接埠和來源 IP 範圍。

您可以為每個 EC2 執行個體指派一或多個安全群組。每個安全群組會允許適當的流量進入每個執行個體。可以設定安全群組，以便只有特定的子網路、IP 地址和資源才能存取 EC2 執行個體。或者，他們可以參考其他安全群組，來限制對特定群組中 EC2 執行個體的存取。

在圖 3 中的 AWS Web 託管架構中，Web 伺服器叢集的安全群組可能只會允許從 Web 層負載平衡器存取，並且只允許在連接埠 80 和 443 (HTTP 和 HTTPS) 上透過 TCP 存取。另一方面，應用程式伺服器安全群組可能僅會允許從應用程式層負載平衡器存取。在此模型中，您的支援工程師還需要存取

EC2 執行個體，而這可以使用 AWS Systems Manager Session Manager 來達成。如需有關安全性的更深入討論，請參閱 AWS 雲端安全，其中包含安全公告、認證資訊和說明 AWS 的安全功能的安全白皮書。

跨叢集負載平衡

硬體負載平衡器是傳統 Web 應用程式架構中使用的常見網路設備。AWS 透過 Elastic Load Balancing (ELB) 服務提供此功能。ELB 會自動將傳入的應用程式流量分配到多個目標，例如 EC2 執行個體、容器、IP 地址和 AWS Lambda 函數，以及虛擬設備。它可以在單一可用區域或跨多個可用區域處理您應用程式流量的各種負載。Elastic Load Balancing 提供四種負載平衡器，它們都具有下列特性：高可用性、自動擴展，以及讓您的應用程式具備容錯功能的強大安全防護。

尋找其他主機和服務

在傳統的 Web 託管架構中，您的大多數主機都會有靜態 IP 地址。在 AWS 雲端中，您的大多數主機都會有動態 IP 地址。儘管每個 EC2 執行個體都可以有公有和私有 DNS 項目，並且可以透過網際網路定址，但 DNS 項目和 IP 地址會在您啟動執行個體時動態指派。無法手動指派它們。靜態 IP 地址 (AWS 術語中的彈性 IP 地址) 可以在啟動後指派給執行中的執行個體。對於需要一致端點的執行個體和服務，例如主要資料庫、中央檔案伺服器和 EC2 受管的負載平衡器，您應該使用彈性 IP 地址。

在 Web 應用程式內快取

記憶體內應用程式快取可以透過快取常用資訊來減少服務上的負載，並改善資料庫層的效能和可擴展性。Amazon ElastiCache 是一種 Web 服務，讓使用者能夠在雲端中輕鬆部署、操作和擴展記憶體內快取。您可以將建立的記憶體內快取設定為隨著負載自動擴展並自動取代失敗的節點。ElastiCache 與 Memcached 和 Redis 的通訊協定相容，可將從您目前的內部部署解決方案的遷移簡化。

資料庫組態、備份和容錯移轉

許多 Web 應用程式包含某種形式的持久性，通常採用關聯式資料庫或非關聯式資料庫的形式。AWS 同時提供關聯式和非關聯式資料庫服務。或者，您也可以在 EC2 執行個體上部署自己的資料庫軟體。下表摘要說明這些選項，本節中將對這些選項進行更詳細的討論。

表 1 - 關聯式和非關聯式資料庫解決方案

	關聯式資料庫解決方案	NoSQL 解決方案
受管資料庫服務	Amazon RDS for MySQL、Oracle、SQL	Amazon DynamoDB、Amazon

	關聯式資料庫解決方案	NoSQL 解決方案
	Server、MariaDB、PostgreSQL、Amazon Aurora	Keyspaces、Amazon Neptune、Amazon QLDB、Amazon Timestream
自我管理	在 Amazon EC2 執行個體上託管關聯式資料庫管理系統 (DBMS)	在 EC2 執行個體上託管非關聯式資料庫解決方案

Amazon RDS

Amazon Relational Database Service (Amazon RDS) 讓您可以存取熟悉的 MySQL、PostgreSQL、Oracle 和 Microsoft SQL Server 資料庫引擎的功能。您已在使用的程式碼、應用程式和工具，可與 Amazon RDS 搭配使用。Amazon RDS 可自動修補資料庫軟體和備份資料庫，並以使用者定義的保留時間存放備份。它還支援時間點復原。透過進行一次 API 呼叫，即可靈活地擴展與關聯式資料庫執行個體關聯的運算資源或儲存容量，讓您從中受益。

Amazon RDS 異地同步備份部署可提高資料庫的可用性，並保護您的資料庫免受意外停機的影響。Amazon RDS 僅供讀取複本提供資料庫的唯讀複本，因此針對讀取量較大的資料庫工作負載，您可以水平擴展，超出單一資料庫部署的容量。與所有 AWS 服務一樣，無需前期投資，只需為您所使用的資源付費。

在 Amazon EC2 執行個體上託管關聯式資料庫管理系統 (RDBMS)

除了受管 Amazon RDS 產品之外，您還可以在 EC2 執行個體上安裝您選擇的 RDBMS (如 MySQL、Oracle、SQL Server 或 DB2) 並自行管理。在 Amazon EC2 上託管資料庫的 AWS 客戶成功地使用各種主要/備用和複寫模型，包括唯讀副本的鏡像以及針對一律就緒的被動從屬節點的記錄傳送。

直接在 Amazon EC2 上管理您自己的資料庫軟體時，您還應考慮容錯和持久性儲存的可用性。為此，我們建議在 Amazon EC2 上執行的資料庫使用 Amazon Elastic Block Store (Amazon EBS) 磁碟區，其類似於網路連接儲存。

對於執行資料庫的 EC2 執行個體，您應將所有資料庫資料和記錄放在 EBS 磁碟區上。即使資料庫主機發生故障，這些資料庫仍然可用。此組態可實現簡單的容錯移轉案例，在其中，如果主機失敗，即可以啟動新的 EC2 執行個體，且現有的 EBS 磁碟區可以連接到新執行個體。然後，資料庫可以在其中斷的位置接著繼續。

EBS 磁碟區會自動在可用區域內提供備援。如果單一 EBS 磁碟區的效能不足以滿足您的資料庫需求，則可以對磁碟區進行條帶化以提高資料庫的每秒輸入/輸出作業 (IOPS) 效能。

對於要求苛刻的工作負載，您還可以使用 EBS 佈建 IOPS，在其中您可以指定所需的 IOPS。如果您使用 Amazon RDS，服務會管理其自己的儲存，使得您可以專注於管理資料。

非關聯式資料庫

除了支援關聯式資料庫之外，AWS 還提供了許多受管非關聯式資料庫：

- Amazon DynamoDB 是一項完全受管的 NoSQL 資料庫服務，可提供快速且可預期的效能及無縫的可擴展性。使用 AWS Management Console 或 DynamoDB API，您可以在無停機或效能下降的情況下將容量向上擴展或縮小。因為 DynamoDB 會處理操作及擴展分散式資料庫至 AWS 的管理負擔，您不再需要煩惱硬體佈建、設定和組態、複寫、軟體修補或叢集擴展。
- Amazon DocumentDB (與 MongoDB 相容) 是特別為大規模 JSON 資料管理建置的資料庫服務，完全受管且在 AWS 上執行，具備高耐用性非常適合企業使用。
- Amazon Keyspaces (適用於 Apache Cassandra) 是一種具可擴展性、高可用性且受管的 Apache Cassandra 相容資料庫服務。透過 Amazon Keyspaces，您可以在 AWS 上使用與今天相同的 Cassandra 應用程式程式碼和開發人員工具執行 Cassandra 工作負載。
- Amazon Neptune 是快速、可靠的全受管圖形資料庫服務，可讓您輕鬆建置及執行搭配高度連線資料集運作的應用程式。Amazon Neptune 的核心專為高效能圖形資料庫引擎而打造，並進行最佳化以存放數十億個關聯資訊並以數毫秒的延遲查詢圖片。
- Amazon Quantum Ledger Database (Amazon QLDB) (QLDB) 是全受管總帳資料庫，可針對集中信任單位所有的交易日誌提供透明、不可變及採用密碼演算法的可驗證交易日誌。QLDB 可用於追蹤所有應用程式資料變更，並維護一段時間內完整且可驗證的變更歷史記錄。
- Amazon Timestream 是一種適用於 IoT 和操作應用程式的快速、可擴展、無伺服器時間序列資料庫服務，可輕鬆存放和分析每天數兆個事件，速度是關聯式資料庫的 1,000 倍，但成本只有十分之一。

此外，您還可以使用 Amazon EC2 來託管您可能正在使用的其他非關聯式資料庫技術。

資料和資產的儲存和備份

AWS 雲端中有許多用於儲存、存取和備份 Web 應用程式資料和資產的選項。Amazon S3 提供高度可用且備援的物件存放區。對有些靜態或變化緩慢的物件，如影像、影片和其他靜態媒體來說，Amazon S3 是良好的儲存解決方案。Amazon S3 還透過與 CloudFront 互動支援這些資產的邊緣快取和串流。

對於類似連接檔案系統的儲存，EC2 執行個體可以連接 EBS 磁碟區。其作用類似於執行 EC2 執行個體的可掛載磁碟。Amazon EBS 非常適合需要作為區塊儲存存取並且需要的持久性超出執行中執行個體生命週期的資料，例如資料庫分割區和應用程式記錄。

除了擁有獨立於 EC2 執行個體的生命週期之外，您還可以取得 EBS 磁碟區的快照並將其存放在 Amazon S3 中。由於 EBS 快照僅會備份自上一個快照以來的變更，因此更頻繁的快照可以減少快照時間。您還可以將 EBS 快照用作跨多個 EBS 磁碟區複寫資料的基準，並將這些磁碟區連接到其他執行中執行個體。

EBS 磁碟區的大小可達 16 TB，而多個 EBS 磁碟區可以經過條帶化，以獲得更大的磁碟區或提高輸入/輸出 (I/O) 效能。若要將 I/O 密集型應用程式的效能最大化，您可以使用佈建 IOPS 磁碟區。佈建 IOPS 磁碟區的設計符合 I/O 密集工作負載的需求，特別是對隨機存取 I/O 輸送量中的儲存體效能和一致性敏感的資料庫工作負載。

您可以在建立磁碟區時指定 IOPS 速率，而 Amazon EBS 會為磁碟區的生命週期佈建該速率。Amazon EBS 目前支援的每一磁碟區 IOPS，範圍從最大 16000 個 (針對所有執行個體類型) 到 64,000 (針對以 Nitro System 為建置基礎的執行個體) 不等。您可以將多個磁碟區一起條帶化，為您的應用程式的每個執行個體提供數千個 IOPS。除此之外，對於需要低於一毫秒延遲的較高輸送量和任務關鍵型工作負載，您可以使用 io2 區塊快速磁碟區類型，其可以支援高達 256,000 IOPS，最大儲存容量為 64 TB。

自動擴展機群

AWS 雲端架構和傳統託管模型之間的重要差異之一是，AWS 可以隨需自動擴展 Web 應用程式機群，以處理流量的變化。在傳統的託管模型中，流量預測模型通常用於在預計流量之前佈建主機。在 AWS 中，您可以根據用於水平擴展和縮減機群的一組觸發程序快速佈建執行個體。

Auto Scaling 服務可以建立可隨需增加或縮小的伺服器容量群組。Auto Scaling 還可以直接與 CloudWatch 搭配以取得指標資料，以及與 Elastic Load Balancing 搭配以新增和移除主機以進行負載分發。例如，如果 Web 伺服器報告一段時間內的 CPU 利用率超過 80%，則可以快速部署額外的 Web 伺服器，然後自動將其新增到負載平衡器中，以便立即包含在負載平衡輪換中。

如 AWS Web 託管架構模型所示，您可以為架構的不同層建立多個 Auto Scaling 群組，使得每個層都可以獨立擴展。例如，Web 伺服器 Auto Scaling 群組可能會觸發縮減和水平擴展，以回應網路 I/O 的變更，而應用程式伺服器 Auto Scaling 群組可能會根據 CPU 利用率水平擴展和向內縮減。您可以設定最小值和最大值，以協助確保全天候的可用性，並將群組內的使用率設限。

Auto Scaling 觸發程序可以設定為增長和縮減指定層的總機群，以使資源利用率與實際需求相符。除了 Auto Scaling 服務之外，您還可以直接透過 Amazon EC2 API 擴展 Amazon EC2 機群，其可讓您啟動、終止和檢查執行個體。

其他安全功能

分散式拒絕服務 (DDoS) 攻擊的數量和複雜程度不斷上升。傳統上，這些攻擊是難以抵擋的。它們往往在緩解時間和人力損耗方面的成本都很高昂，同時要付出在攻擊期間失去對網站的存取造成的機會成本。有許多 AWS 因素和服務可以協助您抵禦此類攻擊。其中之一是 AWS 網路的規模。AWS 基礎設施非常龐大，並能讓您利用我們的規模來最佳化您的防禦能力。有數項服務，包括 Elastic Load Balancing、Amazon CloudFront 和 Amazon Route 53，可以有效擴展您的 Web 應用程式，以因應流量的大幅增加。

基礎設施保護服務尤其有助於您的防禦策略：

- AWS Shield 是一項受管 DDoS 保護服務，可協助防範各種形式的 DDoS 攻擊向量。AWS Shield 的標準產品是免費的，並且會在您的整個帳戶中自動啟動。此標準產品有助於抵禦最常見的網路和傳輸層攻擊。除了此層級之外，進階產品還可以透過為您授與對進行中的攻擊近乎即時的可見性，以及在較高層級與前面提到的服務整合，從而為您的 Web 應用程式提供更高層級的保護。此外，您還可以連絡 AWS DDoS 回應團隊 (DRT)，以協助緩解針對您的資源的大規模和複雜攻擊。
- AWS WAF (Web 應用程式防火牆) 旨在保護您的 Web 應用程式免受可能損害可用性或安全性，或以其他方式消耗過多資源的攻擊。AWS WAF 會配合 CloudFront 或 Application Load Balancer 及您的自訂規則作業，以抵禦跨網站指令碼、SQL Injection 和 DDoS 等攻擊。與大多數 AWS 服務一樣，AWS WAF 隨附功能完整的 API，可以在您的安全需求變更時協助您將 AWS WAF 執行個體的規則的建立和編輯自動化。
- AWS Firewall Manager 是一種安全管理服務，可讓您在 AWS Organizations 中跨帳戶和應用程式集中設定和管理防火牆規則。隨著新應用程式的建立，AWS Firewall Manager 會透過強制執行一組通用的安全規則，輕鬆讓新應用程式和資源合規。

使用 AWS 容錯移轉

與傳統 Web 託管相比，AWS 的另一個重要優勢是可讓您輕鬆存取備援部署位置的可用區域。可用區域是實體上不同的位置，旨在與其他可用區域的故障隔離。它們提供同一 AWS 區域中其他可用區域的經濟實惠、低延遲網路連線能力。正如 AWS Web 託管架構圖所示，AWS 建議您跨多個可用區域部署 EC2 主機，以提高 Web 應用程式的容錯能力。

務必確保在出現故障時，可跨可用區域遷移單一存取點的佈建。例如，您應在第二個可用區域中設定備用資料庫待命，以便資料的持久性可保持一致且高可用，即使在不太可能出現的故障期間也是如此。在 Amazon EC2 或 Amazon RDS 上按一下按鈕即可執行此動作。

雖然在將現有 Web 應用程式遷移到 AWS 雲端時，通常需要進行一些架構變更，但使用 AWS 雲端對於可擴展性、可靠性和成本效益方面的顯著改進非常值得努力。下一節將討論這些改進項目。

使用 AWS 進行 Web 託管時的重要考量

AWS 雲端與傳統 Web 應用程式託管模型之間存在一些重要差異。上一節強調的是在將 Web 應用程式部署到雲端時應考慮的許多重要領域。本節指出在將任何應用程式引入雲端時需要考慮的一些重要架構轉變。

不再有實體網路設備

您無法在 AWS 中部署實體網路設備。例如，AWS 應用程式的防火牆、路由器和負載平衡器不能再置於實體裝置上，而必須以軟體解決方案取代。有各種企業級軟體解決方案，無論是負載平衡或建立 VPN 連接。這不是對 AWS 雲端上可以執行項目的限制，但如果您現今使用這些裝置，則會是對您的應用程式的架構變更。

防火牆無所不在

如果您曾經有一個簡單的非軍事區 (DMZ)，然後在傳統託管模型中開啟主機之間的通訊，AWS 會強制執行一種更安全的模型，其中的每個主機都被鎖定。規劃 AWS 部署的其中一個步驟是分析主機之間的流量。此分析將引導您進行需要開啟的確切連接埠的決策。您可以為架構中的每個類型主機建立安全群組。您還可以建立多種簡單和分層的安全模型，以實現架構內主機之間的最低存取權。Amazon VPC 內使用的網路存取控制清單可協助您在子網路層級鎖定您的網路。

考慮多個資料中心的可用性

將 AWS 區域內的可用區域視為多個資料中心。不同可用區域中的 EC2 執行個體在邏輯上和實體上都是分離的，而它們為跨資料中心部署應用程式提供一個易於使用的模型，以實現高可用性和可靠性。Amazon VPC 作為區域服務，使得您能夠利用可用區域，同時將所有資源保留在同一邏輯網路中。

將主機視為暫時性和動態

在建置 AWS 應用程式方面，最重要的轉變可能是應該將 Amazon EC2 主機視為暫時性和動態。為 AWS 雲端建置的任何應用程式都不應假設主機將一律可用，而且在設計時應瞭解，在 EC2 執行個體出現故障時，EC2 即時存放區中的任何資料都會遺失。

啟動新主機時，您不應假設主機的 IP 地址或在主機可用區域內的位置。您的組態模型必須靈活，而且自舉主機的方法必須將雲端的動態本質納入考量。這些技術對於建置和執行高度可擴展和容錯應用程式來說極為重要。

考慮容器和無伺服器

本白皮書主要聚焦於較傳統的 Web 架構。但是，請考慮透過移至容器和無伺服器技術來實現 Web 應用程式的現代化，利用 AWS Fargate 和 AWS Lambda 之類的服務，使您能夠將使用虛擬機器抽離來執行運算任務。利用無伺服器運算，基礎設施管理任務，如容量佈建和修補，會由 AWS 處理，因此您可以建置使您能夠更快速創新並回應變化的更敏捷應用程式。

考慮自動化部署

- Amazon Lightsail 是一種易於使用的虛擬私有伺服器 (VPS)，可為您提供建置應用程式或網站所需的一切內容，外加符合成本效益的每月計劃。Lightsail 非常適合較簡單的工作負載、快速部署以及在 AWS 上開始使用。設計用於協助您從小規模開始，然後隨增長擴展。
- AWS Elastic Beanstalk 是一項簡單易用的服務，可供您在常見的伺服器 (如 Apache、NGINX、Passenger 和 IIS) 上，針對使用 Java、.NET、PHP、Node.js、Python、Ruby、Go 與 Docker 開發的 Web 應用程式和服務進行部署及擴展作業。您只需上傳程式碼，Elastic Beanstalk 即可為您自動處理部署，包括容量佈建、負載平衡、自動擴展，以及應用程式運作狀態監控。同時，您也能完全控制支援應用程式的 AWS 資源，且可隨時存取基礎資源。
- AWS App Runner 是一項全受管服務，可讓開發人員輕鬆快速地大規模部署容器化 Web 應用程式和 API，而無需事先具備基礎設施經驗。從原始程式碼或容器映像開始。App Runner 會自動建置和部署 Web 應用程式，並透過加密來負載平衡流量。App Runner 還會自動擴展或縮減以滿足您的流量需求。
- AWS Amplify 是一套可以結合使用或單獨使用的工具和服務，用於協助前端 Web 和行動開發人員採用 AWS 技術建置可擴展的完整堆疊應用程式。藉助 Amplify，您可以在幾分鐘內設定應用程式後端並連接您的應用程式，按幾下即可部署靜態 Web 應用程式，以及在 AWS Management Console 外部輕鬆管理應用程式內容。

結論和貢獻者

結論

考慮將 Web 應用程式遷移到 AWS 雲端時，有許多架構性和概念性考量。擁有會隨著您的業務而成長，具成本效益、高度可擴展且容錯的基礎設施的優點，遠遠超過遷移到 AWS 雲端所耗費的工作量。

作者群

協力完成本文件的個人與組織如下：

- AWS 資深解決方案架構師 Amir Khairalomoum
- AWS 資深解決方案架構師 Dinesh Subramani
- AWS 資深解決方案架構師 Jack Hemion
- AWS 雲端支援工程師 Jatin Joshi
- AWS 資深解決方案架構師 Jorge Fonseca
- AWS 解決方案架構師 Shinduri K S

深入閱讀

- 部署以 Django 為基礎的應用程式至 Amazon LightSail
- 將高可用性 Drupal 網站部署到 Elastic Beanstalk
- 將高可用性 PHP 應用程式部署到 Elastic Beanstalk
- 將 Node.js 應用程式與 DynamoDB 部署到 Elastic Beanstalk
- AWS 雲端中的 Linux Web 應用程式入門
- 託管靜態網站
- 使用 Amazon S3 託管靜態網站
- 教學課程：使用 Elastic Beanstalk 部署 ASP.NET 核心應用程式
- 教學課程：如何使用 Elastic Beanstalk 部署 .NET 範例應用程式

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
白皮書已更新	更新多個小節和圖表，加上新服務、功能和更新的服務配額。	2021 年 8 月 20 日
白皮書已更新	更新圖 3 中「使用 ElastiCache 快取」的圖示標籤。	2019 年 9 月 29 日
白皮書已更新	針對新服務新增和更新多個小節。更新圖表以獲得額外的清晰度和服務。在「網路管理」中增加了 VPC 作為 AWS 中的標準聯網方法。 在「其他安全功能」中新增關於 DDoS 保護和緩解的小節。 新增關於 Web 託管的無伺服器架構的小節。	2017 年 7 月 1 日
白皮書已更新	更新多個小節以提升清晰度。更新圖表以使用 AWS 圖示。新增「管理公有 DNS」小節，說明有關 Amazon Route 53 的詳細資訊。針對清晰度更新「尋找其他主機和服務」小節。針對清晰度和 DynamoDB 更新「資料庫組態、備份和容錯移轉」小節。擴大「資料和資產的儲存和備份」小節，以涵蓋 EBS 佈建 IOPS 磁碟區。	2012 年 9 月 1 日
初次出版	發佈白皮書。	2010 年 5 月 1 日

聲明

本文件僅供提供資訊參考。其內容為文件發佈當日時，AWS 最新的產品內容及實務，如有變更，恕不另行通知。客戶需自行獨立評估本文件資訊，任何 AWS 產品或服務皆以「現狀」提供，不包含任何明示或暗示之保證。本文不提供任何來自 AWS、其附屬公司、供應商或授權人之任何保證、表示，契約承諾、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。