AWS 安全簡介

2020 年 1 月

聲明

客戶有責任對本文件中的資訊進行獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品和實務，如有變更，恕不另行通知；及 (c) 並非 AWS 及其合作夥伴、供應商或許可方給予任何承諾或保證。AWS 產品或服務「按原樣」提供，不附帶任何明示或默示保證、陳述或條件。AWS 對客戶的責任和義務受 AWS 協議控制，並且本文件不構成 AWS 與其客戶之間的任何協議，也不會對其進行修改。

內容

摘要

Amazon Web Services (AWS) 提供了一個可擴展的雲端運算平台，旨在提供高可用性和高可靠性，以及讓您能夠執行各種應用程式的工具。AWS 將協助保護您的系統與資料的機密性、完整性和可用性視為是最重要的，一如我們竭力維持您對 AWS 的信任和信心。這份文件的用意是提供 AWS 的安全方法簡介，包含 AWS 環境中的各種控制方式，以及 AWS 為了滿足您的安全目標而提供給客戶的一些產品和功能。

AWS 基礎架構的安全性

AWS 基礎架構旨在建構現今最靈活且最安全的雲端運算環境。其旨在提供一個可擴展性極強、非常可靠的平台，允許客戶快速安全地部署應用程式和資料。

該基礎架構不僅根據安全最佳實務和標準進行建置和管理，而且考慮到雲端的獨特需求。AWS 使用冗餘和分層控制、連續驗證和測試以及大量自動化，以確保 24x7 全天候監控和保護基礎架構。AWS 確保在每個新的資料中心或服務中複寫這些控件。

所有 AWS 客戶都能從資料中心和網路架構的建置中獲益，以滿足客戶最為敏感的安全要求。這意味著您將獲得一個具有高安全性的彈性基礎架構，而沒有傳統資料中心的資本支出和營運開銷。

AWS 在共用的安全責任模型下執行，其中 AWS 負責基礎雲端基礎架構的安全，您負責保護在 (*圖 1*) 中部署的工作負載。這為您提供了所需的靈活性和敏捷性，以便在 AWS 環境中為業務功能實作最適用的安全控制。您可以嚴格限制對處理敏感資料環境的存取，也可以對要公開的資訊部署不太嚴格的控件。

圖 1：AWS 共用安全責任模型

安全產品和功能

AWS 和其合作夥伴提供各種工具和功能，可協助滿足您的安全目標。這些工具反映了您在內部部署環境中部署的熟悉控件。AWS 對於網路安全、設定管理、存取控制和資料安全性提供特有的安全工具和功能。此外，AWS 提供了監控和日誌記錄工具，可以提供對您的環境中發生情況的完全可視性。

基礎架構安全

AWS 提供數種安全功能與服務來加強隱私保護和控制網路存取。其中包括：

- 內建在 Amazon VPC 中的網路防火牆，能夠讓您建立私有網路以及控制對執行個體或應用程式的存取。在所有 AWS 服務之間的傳輸使用 TLS 客戶控制加密。
- 將您的辦公室或內部部署環境設定成私有或專用連線的連線選項。
- 適用於第 3 層或第 4 層以及第 7 層的 DDoS 緩解技術。這些可以用作應用程式和內容交付策略的一部分。
- 自動加密 AWS 全球和 AWS 安全設施的區域網路間的所有流量。

庫存和組態管理

AWS 提供下列各種工具讓您快速成長，同時仍能讓您確保雲端資源符合組織標準和最佳實務的規範。其中包括：

- 依據組織標準管理 AWS 資源的建立和解除委任的部署工具。
- 用來識別 AWS 資源，並於一段時間後追蹤和管理這些資源變更情況的詳細清單和組態管理工具。
- 用於為 Amazon EC2 執行個體建立標準、預先設定、強化虛擬機器的範本定義和管理工具。

資料加密

AWS 提供可擴展和有效的加密功能，讓您能夠為雲端中的靜態資料新增一層安全保護。其中包括：

- 大多數 AWS 服務中可用的靜態資料加密功能，例如 Amazon EBS、Amazon S3、Amazon RDS、Amazon Redshift、Amazon ElastiCache、AWS Lambda 和 Amazon SageMaker
- 彈性的金鑰管理選項，包括 AWS Key Management Service，可讓您選擇讓 AWS 管理加密金鑰或由您完全自行控管自己的金鑰
- 使用 AWS CloudHSM 的專屬硬體金鑰儲存，可讓您有助於滿足您的合規要求
- Amazon SQS 使用伺服器端加密 (SSE)，在傳輸敏感資料時加密訊息佇列

此外，AWS 還提供 API 讓您將加密和資料保護整合到您在 AWS 環境中開發或部署的任何服務。

身分和存取控制

AWS 讓您能夠定義、強制執行和管理 AWS 服務之間的使用者存取政策。其中包括：

- AWS Identity and Access Management (IAM) 讓您能夠使用特權帳戶的 AWS Multi-Factor Authentication 跨 AWS 資源許可，包括基於軟體和硬體身分驗證器的選項，來定義個別使用者帳戶。您可以使用現有的身份系統 (如 Microsoft Active Directory 或其他合作夥伴服務)，利用 IAM 授與員工和應用程式對 AWS 管理主控台和 AWS 服務 API 的聯合存取權。
- AWS Directory Service 可讓您整合公司目錄並與其聯合，以降低管理費用和改善最終使用者體驗。
- 有了 AWS Single Sign-On (AWS SSO)，您可以在 AWS Organizations 中集中管理所有帳戶的 SSO 存取及使用者許可，輕鬆便利。

AWS 在許多服務之間提供原生身分和存取管理整合，還提供與任何自有應用程式或服務的 API 整合。

監控和記錄

AWS 提供讓您查看 AWS 環境中發生情況的工具和功能。其中包括：

- 使用 AWS CloudTrail，您可以取得帳戶的 AWS API 呼叫歷史記錄，包括透過 AWS 管理主控台、AWS 開發套件、命令列工具和更高等級 AWS 服務發出的 API 呼叫，以便監控雲端的 AWS 部署。您也可以識別哪些使用者與帳戶呼叫 AWS API 以使用支援 CloudTrail 的服務、發出呼叫的來源 IP 地址以及發出呼叫的時間。
- Amazon CloudWatch 提供可靠、可擴展且靈活的監控解決方案，可讓您在短時間內就開始使用。您再也不需要設定、管理及擴展自己的監控系統和基礎設施。
- Amazon GuardDuty 是一種威脅偵測服務，可持續監控是否有惡意活動和未經授權的行為，以保護 AWS 帳戶和工作負載。Amazon GuardDuty 透過 Amazon CloudWatch 公佈通知，因此您可以觸發自動回應或通知人員。
- Amazon Detective 可自動從您的 AWS 資源中收集日誌資料，並使用機器學習、統計分析和圖論來建置關聯的資料集，讓您能夠輕鬆地進行更快、更有效的安全調查。

這些工具和功能可提供您找出問題的能力，以在問題衝擊到企業之前事先發現問題，並讓您改進環境的安全狀態和降低風險情形。

在 AWS Marketplace 中的安全產品

將生產工作負載移轉至 AWS 可以讓組織在確保安全環境的同時，提高敏捷性、可擴展性、創新性和成本節省。AWS Marketplace 提供領先業界的產品，這些產品與您內部部署環境中的現有產品在功能上相當、相同或者可以相互整合。這些產品可以補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境部署全方位的安全架構，還有提供更順暢的體驗。

安全指導

AWS 透過 AWS 及其合作夥伴提供的線上工具資源、支援以及專業服務，向客戶提供指導與專家意見。

AWS Trusted Advisor 是一個線上工具，其作用類似於自訂的雲端專家，可協助您設定資源以遵循最佳實務。Trusted Advisor 可檢查您的 AWS 環境以協助彌合安全漏洞，並找出可節省成本的機會、提升系統效能與可靠性。

AWS 客戶團隊提供了第一聯絡點，指導您進行部署和實作，並為您提供正確的資源以解決您可能遇到的安全問題。

AWS 企業支援提供 15 分鐘的回應時間，並透過電話、聊天或電子郵件提供 24×7 全天候服務；以及專門的技術客戶經理。這項服務台服務可確保盡快解決客戶的問題。

AWS 合作夥伴網路提供數百種領先業界的產品，這些產品與您內部部署環境中的現有產品在功能上相當、相同或者可以相互整合。這些產品可以補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境部署全方位的安全架構，提供更順暢的體驗，還有全球數百家經過認證的 AWS 諮詢合作夥伴，可協助您滿足安全性和合規性需求。

AWS 專業服務包含安全、風險和合規專業實務，可協助您在將最敏感的工作負載移轉至 AWS 雲端時建立信心和技術能力。AWS 專業服務可協助客戶根據久經驗證的設計制定安全政策和實務，並確保客戶的安全設計滿足內部和外部合規性要求。

AWS Marketplace 是包含獨立軟體開發廠商數千種軟體產品的數位型錄，可讓您輕鬆地尋找、測試、購買和部署在 AWS 上執行的軟體。AWS Marketplace 安全產品可以補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境部署全方位的安全架構，還有提供更順暢的體驗。

AWS 安全公告提供有關目前漏洞和威脅的安全公告，並讓客戶能夠與 AWS 安全專家一起解決報告濫用、漏洞和滲透測試等問題。我們還具有用於漏洞報告的線上資源。

AWS 安全文件顯示如何設定 AWS 服務，以滿足您的安全性和合規性目標。資料中心和網路架構都是依據安全性要求最高的組織需要所建立，因此 AWS 客戶能夠從中獲得不少好處。

AWS Well-Architected 架構協助雲端架構師建置安全、高效能、有彈性又有效率的應用程式基礎設施。The AWS Well-Architected 架構包括一個安全支柱，其著重於保護資訊和系統。重要主題包括資料機密性與完整性、透過權限管理識別和管理哪些人可以做哪些事、保護系統、建立控制機制以偵測安全事件。客戶可以從主控台使用精心設計的服務，也可以使用其中一位 APN 合作夥伴的服務來為他們提供協助。

AWS Well Architected Tool 可協助您審核工作負載的狀態，並將其與最新的 AWS 架構最佳實務進行比較。在回答一系列與卓越營運、安全性、可靠度、執行效率與成本最佳化相關的問題之後，即可在 AWS 管理主控台中使用此免費工具。AWS Well-Architected Tool 則可提供有關如何使用已經制定的最佳實務作法來架構雲端之方案。

合規

AWS 合規可讓客戶了解 AWS 在維護 AWS 雲端安全和保護資料方面所具備的強大控制能力。在 AWS 雲端中建置系統時，AWS 和客戶均應承擔合規責任。AWS 運算環境將持續進行稽核，並獲得跨地域和垂直領域的認證機構核發的認證，包括 SOC 1/SSAE 16/ISAE 3402 (前稱為 SAS 70)、SOC 2、SOC 3、ISO 9001 / ISO 27001、FedRAMP, DoD SRG 和 PCI DSS Level 1。此外，AWS 還制定有保證計劃，提供範本和控制映射以協助客戶建立其在 AWS 上執行的環境合規性，如需有關計劃的完整清單，請參閱 AWS 合規計劃。

我們可以確認所有 AWS 服務的使用均符合 GDPR 的要求。這表示除了受益於 AWS 為維護服務安全而採取的所有措施之外，客戶還可以將 AWS 服務做為其 GDPR 合規計劃部分進行部署。AWS 提供符合 GDPR 的資料處理增補合約 (GDPR DPA)，讓您能夠遵守 GDPR 合約義務。AWS GDPR DPA 已與 AWS 服務條款結合，且自動適用於需要符合 GDPR 要求的全球所有客戶。Amazon.com, Inc. 已獲得歐美隱私屏障的認證，且 AWS 涵蓋於此認證內。這有助於選擇將個人資料轉移至美國的客戶遵守其資料保護義務。Amazon.com Inc. 的認證可在歐美隱私屏障網站上找到：https://www.privacyshield.gov/list

透過在經過認證的環境中進行操作，客戶可以減少他們需要執行的稽核的範圍和成本。AWS 不斷對其基礎架構進行評定，包括其硬體和資料中心的物理和環境安全性，因此客戶可以利用這些認證，且只需這些固有的控制。

在傳統的資料中心中，常見的合規性活動通常是手動執行的定期活動。這些活動包括驗證資產組態和報告管理活動。此外，結果報告甚至在發佈之前就已過時。在 AWS 環境中進行操作讓客戶能夠利用內嵌式自動化工具，例如 AWS Security Hub、AWS Config 和 AWS CloudTrail) 來驗證合規性。由於這些任務變得日常、持續和自動化，因此這些工具減少了執行稽核所需的工作。透過減少在手動活動上的時間，可以協助您將公司中合規性角色從一種必要的管理負擔，發展為一種管理風險並改善安全狀況的負擔。

進一步閱讀

如需額外資訊，請參閱下列資源：

如需詳細資訊...	請參閱
AWS 上雲端安全的關鍵主題、研究領域和培訓機會	AWS 雲端安全學習
AWS 雲端採用框架將指南分為六個重點領域：業務、人員、管控、平台、安全和營運	AWS 雲端採用框架
AWS 的特定控制措施；如何將 AWS 整合至現有框架	Amazon Web Services：風險與合規
有關如何在 AWS 環境中部署安全控制的最佳實務指南	AWS 安全最佳實務
AWS Well-Architected 架構，安全性支柱	AWS Well-Architected 架構安全性支柱

文件修訂

日期	描述
2020 年 1 月	最新服務、資源和技術的更新資訊。
2015 年 7 月	首次出版。