aws

擁抱零信任：安全且敏捷的業務轉型策略

AWS 方案指引

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 擁抱零信任：安全且敏捷的業務轉型策略

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介 1
決策程序 1
目標業務成果 3
改善安全狀態 3
順暢採用雲端 3
合規性和法規一致性 3
加強資料保護 3
高效率事件回應 4
提高人力的生產力 5
達成數位轉型 5
章節摘要 5
零信任原則 6
驗證和身分驗證 6
最低權限存取 6
微分段 6
持續監控和分析 6
自動化和協同運作 7
Authorization 7
章節摘要 7
ZTA 的關鍵元件 8
身分識別和存取管理 8
安全存取服務邊緣 8
資料外洩防護 8
安全資訊和事件管理 8
企業資源擁有權目錄 9
統一端點管理 9
以政策為基礎的強制執行點 9
章節摘要 9
組織準備程度 10
領導階層的共識和溝通 10
技能發展和培訓 10
組織結構和角色 11
IT 基礎設施和架構 11
風險管理、治理和變更控制 11

監控和評估 12
章節摘要 12
零信任思維 13
零信任教育和培訓 13
協作和通訊 13
持續學習和改進 13
指標和責任 13
章節摘要 13
分階段方法 14
第 1 階段：評估和規劃 14
第 2 階段：試行和實作 14
第 3 階段：監測和持續改善 15
章節摘要 15
最佳實務 16
關鍵要點 18
後續步驟 19
常見問答集 20
什麼是零信任？ 20
什麼 AWS 服務 可以協助我實作零信任架構？ 20
如何使用 確保資料安全 AWS？ 20
可以在零信任環境中 AWS 協助滿足合規要求嗎？ 20
在零信任環境中，是否有任何用於自動化安全性 AWS 的工具或服務？ 20
如何透過 在零信任雲端環境中確保持續監控和事件回應 AWS 21
Resources 22
參考 22
工具 22
文件歷史紀錄 23
..... xxiv

擁抱零信任：安全且敏捷的業務轉型策略

Greg Goden，Amazon Web Services (AWS)

2023 年 12 月 (文件歷史記錄)

如今，組織比以往任何時候都更聚焦於將安全性作為關鍵要務。這會產生各式各樣的好處，例如維持客戶的信任、改善人力流動性，或解鎖全新數位商機。在他們這麼做的時候，就會持續問一個老問題：「什麼是能確保系統和資料安全性正確等級和可用性的最佳模式？」「零信任」一詞已越來越常用來說明此問題的現代答案。

零信任架構 (ZTA) 是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。透過實作 ZTA 模型，您便能隨著網路安全和深度防禦概念持續發展成熟的過程，實現有意義的下一次迭代。

決策程序

實作 ZTA 策略需要仔細的規劃和決策，其中包含評估各種因素，並將其與組織目標保持一致。展開 ZTA 之旅的關鍵決策程序包括：

1. 利害關係人的參與 – 務必與其他高階主管、副總和資深經理互動，以了解他們對組織安全狀態的優先順序、疑慮和願景。若從一開始就將關鍵利害關係人納入其中，您便能將 ZTA 實作與整體策略目標保持一致，並取得必要的支持和資源。
2. 風險評估 – 進行全面的風險評估有助於識別問題、過大的受攻擊面積和關鍵資產，以便讓您針對安全控制項和投資做出明智的決策。評估組織現有的安全狀態、找出潛在弱點，並根據您產業和營運環境的特定風險格局，排定改善領域的優先順序。
3. 技術評估 – 評估組織現有的技術全貌並識別缺口，有助於選擇符合 ZTA 原則的適當工具和解決方案。這項評估應包括對以下項目的徹底分析：
    - 網路架構
    - 身分識別和存取管理系統
    - 身分驗證和授權機制
    - 統一端點管理
    - 資源擁有權工具和程序
    - 加密技術

- 監控和日誌功能
- 選擇正確的技術堆疊，對於建置堅實的 ZTA 模型至關重要。

4. 變更管理 – 認知到採用 ZTA 模型的文化和組織影響至關重要。實作變更管理實務有助於確保整個組織順利進行轉換和接納。其中包含向員工說明 ZTA 的原則和好處、提供有關新安全實務的培訓，以及培養有關安全意識的文化，鼓勵問責制和持續學習。

本規範性指引旨在為高階主管、副總和資深經理提供實作 ZTA 的全方位策略。它會深入探討 ZTA 的關鍵面向，其中包括以下層面：

- 組織準備程度
- 分階段採用方法
- 利害關係人協作
- 實現安全和敏捷業務轉型的最佳實務

透過遵循本指南，您的組織可以在 Amazon Web Services (AWS) 雲端中瀏覽 ZTA 環境，並在安全旅程中取得成功。 AWS 提供各種服務，可用於實作 ZTA，例如 AWS Verified Access、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。這些服務可協助保護 AWS 資源免於未經授權的存取。

目標業務成果

本節會討論為整個組織定義和實作零信任架構的相關期望結果。

改善安全狀態

您的組織可以透過採用零信任原則，強化安全狀態、降低安全風險，以及保護雲端基礎設施和資料。零信任的基本原則是基於僅知原則授予存取權限，再搭配嚴格的控制項、大幅減少受攻擊面積，以及限制安全事件的潛在影響。這種主動的方法有助於組織勝過新興的安全風險，並協助確保資產的機密性、完整性和可用性。

順暢採用雲端

制定明確定義的零信任架構 (ZTA) 採用計劃，可協助確保順利且成功地轉換至雲端環境。ZTA 原則與雲端安全最佳實務密切配合，為組織提供穩固的基礎，以便安全地獲得雲端運算的好處。若從一開始就整合 ZTA 原則，便有助於組織以安全性為核心元素來設計雲端架構。

合規性和法規一致性

實作 ZTA 實務有助於組織符合業界與法規要求和標準。ZTA 本身就會推動最低權限原則，以及強制執行嚴格的存取控制項。存取控制項通常受下列法規管理：

- 聯邦風險與授權管理計劃 (FedRAMP)
- 美國健康保險流通與責任法案 (HIPAA)
- 支付卡產業資料安全標準 (PCI DSS)。

您的組織可以透過採用零信任架構，表明自身對資料保護、隱私權和法規遵循的承諾，同時大幅降低受罰或聲譽受損的可能性。

加強資料保護

組織可以透過實作資料加密、存取控制項和定期安全評估來保護整個雲端採用程序中的敏感資料。您的組織可以採取下列特定步驟：

- 資料加密 – 資料加密 – 資料加密是透過需要金鑰才能將資料解密回原始純文字格式的方式，將純文字資料加密為密文的程序。這使得未經授權的人員更難以存取敏感資料，即使他們能夠取得資料副本亦然。
- 存取控制項 – 存取控制項會限制可存取敏感資料的人員，以及他們可以使用資料執行哪些事項。這項措施的執行方式可以是指派使用者角色和權限，以及使用多重因素身份驗證或其他方法來驗證使用者身份。
- 定期安全評估 – 定期進行安全評估，有助於組織識別和解決安全問題，並主動進行修復。此類評估可由內部安全團隊或外部安全公司進行。

零信任架構透過實作多種安全措施，對資料保護採取全方位的方法。此類措施包括高強度身分驗證、資料加密和精細的存取控制項。這種方法可大幅降低資料相關安全事件的風險，以及防止敏感資訊遭到未經授權的存取。

高效率事件回應

組織可以在雲端環境中建立監控和事件回應框架，以便更快速有效地偵測及回應安全事件。零信任架構強調持續監控、威脅情報整合，以及即時掌握使用者活動、網路流量和系統行為。安全團隊接著便能主動識別和緩解安全事件。這種方法可以縮短偵測和回應潛在問題的時間，並大幅降低對業務營運的影響。關鍵要點包括以下項目：

- 測試 – 無論組織採用何種事件回應框架或方式，都應該定期測試事件回應計劃。透過桌上演練、模擬和紅隊演練獲得練習機會，在實際的設定中練習事件回應、找出工具和能力的缺口，以及為事件回應人員建立經驗和信心。
- 監控 – 持續監控雲端環境是否出現異常活動的跡象。您可以使用各種工具和技術來完成這這項操作，例如日誌分析、網路監控和漏洞掃描。
- 威脅情報整合 – 將威脅情報整合至監控和事件回應框架。這有助於組織更快速有效地識別威脅並加以回應。
- 即時可見性 – 若要快速識別並回應安全事件，組織必須能即時掌握使用者活動、網路流量和系統行為。
- 主動識別和緩解 – 組織可透過主動識別和緩解安全事件，縮短偵測和回應潛在威脅的時間，大幅降低對業務營運的影響。

提高人力的生產力

現代的人力需要彈性，以便從日益增加的位置、裝置和時間完成工作。您可透過實作 ZTA 為這些需求提供支援，並改善人力流動性、生產力和滿意度，同時維持或改善組織的安全狀態。

達成數位轉型

作為數位轉型的一部分，組織越來越追求在傳統網路邊界之外的裝置、機器、設施、基礎設施和程序之間的互聯。物聯網 (IoT) 和營運技術 (OT，也稱為工業物聯網或 IIoT) 裝置通常會將遙測和預測性維護資訊直接傳輸到雲端。若要保護工作負載，就必須套用超出傳統邊界方法的安全控制項。

章節摘要

您的組織可透過聚焦於這些目標的業務成果，充分發揮 ZTA 的潛力，並強化雲端的安全狀態。務必使這類成果與特定的組織目標保持一致、根據獨特的業務要求量身制訂目標業務成果，以及定期評估有效性以推動持續的改善。

了解零信任原則

零信任架構 (ZTA) 奠基於構成其安全模型基礎的一系列核心原則。如果組織希望有效採用 ZTA 策略，就務必了解這些原則。本節會說明 ZTA 的核心原則。

驗證和身分驗證

驗證和身分驗證原則強調對所有類型的主體（包括使用者、機器和裝置）進行高強度識別和身份驗證的重要性。ZTA 要求在整個工作階段持續驗證身份和身份驗證狀態；理想狀態下，最好能針對每次請求執行。它不僅依賴傳統的網路位置或控制項運作。這包括實作現代高強度多重要素驗證 (MFA)，以及在身分驗證程序期間，評估額外的環境和背景資訊訊號。組織可採用此原則，協助確保以最完善的身份輸入資訊做出資源授權決策。

最低權限存取

最低權限的原則包含授予主體執行任務所需的最低存取層級。組織可採用最低權限存取原則，強制執行精細的存取控制，讓主體只能存取履行其角色和責任的必要資源。其中包括實作即時存取佈建、角色型存取控制項 (RBAC) 以及定期審查存取權限，以大幅減少受攻擊面積和未經授權存取的風險。

微分段

微分段是一種網路安全策略，會將網路分割成較小的隔離區段，以授權特定的流量流程。您可以建立工作負載界限，並在不同區段之間強制執行嚴格的存取控制，以達成微分段。

微分段可以透過網路虛擬化、軟體定義聯網 (SDN)、主機型防火牆、網路存取控制清單 (NACLs) 以及 Amazon Elastic Compute Cloud (Amazon EC2) 安全群組或 等 AWS 特定功能來實作 AWS PrivateLink。分段閘道會控制區段之間的流量，以明確授予存取權限。微分段和分段閘道有助於組織限制網路中不必要的路徑，尤其是導向關鍵系統和資料的路徑。

持續監控和分析

持續監控和分析包含在組織環境中收集和分析與安全性相關的事件和資料，並且尋找關聯。您的組織能透過實作堅實的監視和分析工具，以融合的方式評估安全資料和遙測。

此原則強調掌握使用者行為、網路流量和系統活動的重要性，以辨識別異常和潛在的安全事件。安全資訊與事件管理 (SIEM)、使用者和實體行為分析 (UEBA)，以及威脅情報平台等進階技術，在達成持續監控和主動偵測威脅方面扮演要角。

自動化和協同運作

自動化和協同運作可協助組織簡化安全程序、減少人工干預，以及加強回應時間。透過自動執行例行的安全工作並使用協同運作功能，您的組織便能強制執行一致的安全政策，以及迅速回應安全事件。此原則也包括自動化存取佈建和取消佈建程序，以協助確保及時且準確地管理使用者權限。透過採用自動化和協同運作，您的組織便能提高營運效率、減少人為錯誤，同時將資源集中在更具策略性的安全措施上。

Authorization

在 ZTA 中，每項存取資源的請求都應由閘控強制執行點明確授權。除了驗證身分外，授權政策還必須考慮其他背景資訊，例如裝置健康狀態和安全狀態、行為模式、資源分類和網路因素。授權程序應根據與所存取資源相關的對應存取政策，來評估這項融合式背景資訊。最理想的情況下，機器學習模型可以為宣告式的政策提供動態補充。使用此類模型時，這些模型應僅聚焦於其他限制，且不應授予未明確指定的存取權限。

章節摘要

透過遵守 ZTA 的這些核心原則，組織便能建立符合現代企業環境多樣性的堅實安全模型。若要實作這些原則，必須採用結合技術、程序和人員的全方位方法，才能達成零信任思維，並建立具備恢復能力的安全狀態。

零信任架構的關鍵元件

若要有效地實作零信任架構 (ZTA) 策略，您的組織必須了解組成 ZTA 的關鍵元件。這些元件會共同運作，以便在符合零信任原則的全方位安全模型上持續改進。本節會說明 ZTA 的關鍵元件。

身分識別和存取管理

身分識別和存取管理提供堅實的使用者身分驗證和簡化的存取控制機制，構成 ZTA 的基礎。其中包括單一登入 (SSO)、多重要素驗證 (MFA) 以及身分治理和管理解決方案等技術。身分識別和存取管理會提供高等級的身分驗證保證和重要的背景資訊，這些項目是做出零信任授權決策時不可或缺的部分。同時，ZTA 是一種安全模型，會根據每位使用者、每部裝置和每個工作階段，授予應用程式和資源的存取權限。這有助於保護組織免受未經授權的存取，即便使用者的憑證洩漏亦然。

安全存取服務邊緣

安全存取服務邊緣 (SASE) 是新的網路安全方法，可將網路和安全功能虛擬化、互相結合並分派到以雲端為基礎的單一服務中。無論使用者身在何處，SASE 都能提供安全的應用程式和資源存取。

SASE 包括多種安全功能，例如安全網頁閘道、防火牆即服務，以及零信任網路存取 (ZTNA)。這些功能共同運作以保護組織免受各種威脅的侵害，其中包括惡意軟體、網路釣魚和勒索軟體。

資料外洩防護

資料外洩防護 (DLP) 技術可協助組織保護敏感資料，防止未經授權的披露。DLP 解決方案會監控和控制動態及靜態資料。這有助於組織定義政策並強制執行、預防資料相關的安全事件，以及確保敏感資訊在整個網路中都受到保護。

安全資訊和事件管理

安全資訊和事件管理 (SIEM) 解決方案會收集、彙總和分析來自組織基礎設施中各種來源的安全事件日誌。您可以使用此類資料偵測安全事件、促進事件回應，以及深入了解潛在威脅和漏洞。

對於 ZTA 而言，SIEM 解決方案能夠針對來自不同安全系統的相關遙測找出關聯並加以了解，對於改善偵測和回應異常模式的機制至關重要。

企業資源擁有權目錄

若要正確授予企業資源的存取權限，組織必須具備可靠的系統來分類這些資源，以及更重要的是，擁有這些資源的對象。這項事實來源必須提供工作流程，協助進行存取請求、相關核准決策以及其中的定期認證。隨著時間過去，這項事實來源就會包含「誰能存取哪些項目？」的答案，適用於組織內部。您可以將這些答案用於授權、稽核以及合規性。

統一端點管理

ZTA 除了對使用者進行高強度的身分驗證外，還必須考慮使用者裝置的健康狀態、安全狀態和情況，以便評估公司資料和資源存取是否安全。統一端點管理 (UEM) 平台提供下列功能：

- 裝置佈建
- 持續的組態和修補程式管理
- 安全性基準
- 遙測報告
- 裝置清潔和淘汰

以政策為基礎的強制執行點

在 ZTA 中，各項資源的存取權限應由以閘控政策為基礎的強制執行點明確授權。一開始，這類強制執行點可基於現有網路和身份系統中的現有強制執行點決定。只要將 ZTA 所提供更廣泛的背景資訊和訊號納入考量，便能讓強制執行點的功能逐漸增強。長期來看，您的組織應實作 ZTA 特定的強制執行點，以便在融合脈絡下運作、持續整合訊號提供者、維護全方位的政策集，以及透過結合遙測所收集的情報進行強化。

章節摘要

了解這些關鍵元件對於計劃採用 ZTA 的組織至關重要。透過實作這些元件並將它們整合到同一個緊密結合的安全模型中，您的組織便能根據零信任的原則建立強大的安全狀態。下列各節會探索組織準備程度、分階段採用方法以及最佳實務，協助您在組織內成功實作 ZTA。

評估組織對於採用零信任架構的準備程度

採用新的架構策略是極其重要的任務，因此必須進行仔細的規劃，並將組織因素皆納入考量。本節著重說明為整個企業採用零信任架構時的關鍵組織準備考量要素。處理這些考量要素後，您的組織便能做好準備，迎接更強大、更成功的安全狀態。

領導階層的共識和溝通

若要成功實作零信任架構，領導階層的共識和溝通不可或缺。領導階層必須了解零信任架構的優勢以及所需資源。領導者也必須願意改變組織的文化和程序。若要建立員工的信任並取得他們的贊同，請務必與員工溝通。員工需要了解組織實作零信任的理由、這項措施對他們的意義，以及他們能如何提供協助。溝通應該要保持開放、資訊透明且持續進行。

領導階層的支持和贊同

若要成功實作零信任架構 (ZTA)，請務必確保關鍵的利害關係人和高階主管在該架構的目標、優勢和成效衡量等方面達成共識。分享零信任原則對於強化安全性的重要性，以及若要捨棄傳統的邊界式安全措施，轉為使用更精細、以使用者為中心的方法來實現業務敏捷性，這些原則更是扮演要角。若改用這種方法，您的組織便能更迅速地適應變化和威脅。高階主管的共識會為組織建立基調，有助於克服阻擋變化的潛在阻力。

資訊透明的溝通

在實作零信任架構的過程中，請與員工維持開放且資訊透明的溝通。解釋採用該架構的理由、優勢和預期結果，並迅速解決疑慮。提供有關實作進度的定期更新資訊，這麼做能增加贊同的程度、減少阻力以及建立信任。

技能發展和培訓

在領導階層達成共識並且進行開放的溝通後，請務必協助即將實作零信任架構的員工發展相關技能和知識。其中包括了解零信任原則、如何在工作中實作這些原則，以及如何回應安全事件。請提供培訓和發展機會，協助員工掌握這些技能。

雲端知識和技能

評估組織在雲端技術和零信任原則方面的技能和知識缺口。提供培訓和發展計劃，以提高員工的技能並提供必要的專業知識，讓他們能在以雲端為中心的零信任環境中有效地工作。為了跟上不斷推陳出新的技術和安全實務，請培養持續學習的文化。

安全文化和意識

評估組織的安全文化。評估員工之間的安全意識程度、他們對安全最佳實務的理解，以及他們遵循政策和程序的程度。識別安全知識的任何缺口。不妨考慮進行安全意識培訓計劃，向員工說明零信任架構的重要性，以及他們在維護安全環境方面扮演的角色。

組織結構和角色

請建立有效的組織結構和角色，以便成功實作零信任架構。這包括建立雲端卓越中心 (CCoE)、檢閱和修改安全營運程序，以及針對漏洞管理、事件回應和安全監控等方面指派角色和相應的責任。

雲端卓越中心

建立 CCoE，為雲端營運提供指引、最佳實務和監督。CCoE 是由一個團隊或一組人員組成，負責建立和實作雲端相關的最佳實務、準則和治理政策。CCoE 應包括來自不同業務部門和 IT 團隊的代表，協助確保協作和共識。CCoE 在推動雲端託管工作負載採用零信任原則方面扮演要角。CCoE 也有利於整個組織的知識共享。

安全營運

若要符合零信任環境的需求，請檢閱並修改目前的安全營運組織。若要改善監控、事件回應和威脅情報功能，請考慮實作安全營運中心 (SOC) 或受管安全服務供應商 (MSSP)。針對漏洞管理、事件回應和安全監控建立角色和責任。若要確保能快速偵測輕微安全事件並加以修復，以便中斷一連串的事件，運作良好的事件回應程序至關重要。此程序有助於防止輕微事件發展成更具影響力的事件。

IT 基礎設施和架構

檢查公司的 IT 架構和基礎設施，找出可能會對採用零信任方法造成影響的任何限制或相依性。判斷目前的應用程式和系統是否與必要的零信任架構元件相容。分析是否需要針對基礎設施進行任何改善或調整，以協助成功部署零信任原則。請針對每個應用程式或系統考慮是否最適合實作零信任架構，還是應透過規模更大的現代化工作來進行實作。

風險管理、治理和變更控制

請建立有效的風險管理、治理和變更控制程序，以便成功實作零信任架構。這包括使風險管理與零信任原則保持一致、制定事件回應計劃、與法律和合規部門合作，以及建立變更控制程序。

風險管理

檢查在您公司實施的風險管理策略，並判斷該策略遵守零信任原則的程度。分析現行事件回應系統的效率、安全措施和風險評估程序。判斷哪些區域需要改進，以符合零信任策略。開始開發自動化事件回應系統或持續監控和分析架構，以提高解決速度。

變更控制程序

為了確保所有與雲端相關的修改都遵守安全和合規要求，請建立有效的變更控制方法。建立系統化的變更管理程序，其中包括安全組態分析、風險評估、核准和記錄。經常檢閱和稽核更新內容，以保持零信任架構的完整性。

監控和評估

若要成功實作零信任架構，您的組織必須持續監控並評估其安全狀態。這包括建立關鍵績效指標（KPI）、監控和評估 KPI，以及培養持續改善的文化。組織可以透過遵循這些步驟確保成功實作零信任架構，也確保他們持續致力於提高安全性。

關鍵績效指標

建立相關的關鍵績效指標 (KPI)，以評估零信任部署的成效和效能。這類 KPI 可能會衡量使用者滿意度、裝備和推出進度、降低的成本、合規可觀測性，以及安全事件的數量。為了追蹤整體發展並找出改善的機會，請定期監控和評估這些 KPI。

持續改善

建立系統以吸引利害關係人提出意見和洞察，藉此培養持續改善的文化。鼓勵員工提供想法和建議，以改善雲端環境的安全性、有效性和使用者體驗。使用這些資訊來簡化程序、改善安全措施以及加速創新。

章節摘要

您的組織可透過解決這些組織和文化考量要素，為採用零信任安全模型的雲端建立能提供支援的環境。下節會探討分階段採用的方法，提供指引來說明如何以實用且可管理的方式逐步實作零信任原則。

培養零信任思維

實作零信任不僅止於技術實作。它需要組織中的文化轉移。培養零信任思維需要強調下列關鍵層面。

零信任教育和培訓

教育員工零信任架構 (ZTA) 的價值和優勢。透過培訓課程、研討會和其他資源，提供 ZTA 概念和方法的技術和非技術說明。鼓勵員工注意他們在建立和維護零信任安全範例方面的責任。

協作和通訊

促進參與 ZTA 實作的所有團隊和部門之間的協作和透明度。為了確保每個人都對計畫有徹底的了解，請促進跨職能的溝通、知識分享和資訊交換。建立共同責任的文化，其中每個人都認識到他們對業務整體安全所做的貢獻的重要性。

持續學習和改進

在零信任的環境中，優先考慮持續學習和改進。鼓勵員工隨時掌握最新的安全趨勢、技術和最佳實務。培養創新和實驗的文化，鼓勵員工探索新的解決方案和方法，以強化組織的安全狀態。

指標和責任

建立明確的指標和責任機制，以衡量零信任策略的有效性。定義符合組織安全目標的關鍵績效指標 (KPIs)，並定期追蹤進度。讓個人和團隊對其對零信任原則的實作和維護所做的貢獻負責。

章節摘要

透過解決這些層面並培養零信任思維，組織可以為成功採用和實作零信任奠定堅實的基礎。這種文化轉移對於協助組織中的每個人了解零信任的重要性，並積極為其成功做出貢獻至關重要。

下節會探討分階段採用的方法，提供指引來說明如何以實用且可管理的方式逐步實作零信任原則。

分階段採用零信任架構的方法

採用零信任架構 (ZTA) 需要進行仔細的規劃和實作。我們建議採用分階段採用方法以順利完成轉換，並將對業務營運的干擾降到最低。本節會針對採用 ZTA 包含的關鍵階段提供指引。

第 1 階段：評估和規劃

零信任實作的第一階段是評估和規劃。這個階段對於整體實作能否成功至關重要，因為此階段包含識別您組織目前安全狀態中的任何缺口，並加以解決。花時間評估目前的狀態並定義安全目標後，您便能為成功實作零信任架構奠定基礎。

同時，也不一定總是能獲得百分百完整且準確的評估結果。為了避免分析癱瘓導致您無法進行後續階段，請準備好透過區隔或其他方式，接受某種程度的不完美。

1. 評估目前的狀態 – 針對現有的安全基礎設施、政策和控制項進行評估。識別潛在漏洞、安全缺口，以及實作零信任原則後有助於改善的領域。
2. 定義安全目標 – 根據目前的狀態評估調查結果，定義符合零信任原則的安全目標。這些安全目標也應符合組織的整體安全策略，並解決已識別的漏洞和缺口。
3. 設計架構 – 開發有助於達成組織安全目標的 ZTA。此架構應包括必要的元件，例如身分識別和存取管理解決方案、網路分段機制，以及持續的監控系統。該架構也應具備可擴展性和適應性，並且能夠適應未來的成長和技術進展。理想情況下，此架構應該以負責實作該架構的團隊能輕易理解的格式來表示，例如 AWS CloudFormation 範本，而不只是文件或圖表。
4. 吸引利害關係人參與 – 納入業務單位、IT 團隊和安全團隊等所有利害關係人，以便取得洞察並使其目標與 ZTA 實作計劃保持一致。鼓勵進行協作和溝通，以便針對零信任方法的好處和要求建立共識。

第 2 階段：試行和實作

零信任實作的第二階段是試行和實作。這個階段包含在小規模且受到控制的環境中測試 ZTA，然後在整個組織中迭代部署。請務必向員工說明新的安全措施，以及他們在維護零信任環境中扮演的角色。

1. 試行部署 – 在小規模且受到控制的環境中測試 ZTA。實作架構設計階段所定義的必要元件和安全控制項。密切監控試行部署、收集意見回饋，並進行任何必要的調整。準備好在此過程的初期保持彈性，也就是當零信任架構從假設性演練轉變為您正在建置的實際體驗的時期。

2. 迭代部署 – 根據試行部署所汲取的經驗，開始在整個組織中迭代部署零信任架構。透過飛輪效應創造動力，無須透過廣泛的行銷活動即可達成關鍵的大規模部署。針對推出過程中較長尾的階段，保留可能需要的領導階層命令或上報機制。
3. 提供使用者培訓並提高意識 – 向員工說明新的安全措施，以及他們在維護零信任環境中扮演的角色。強調安全實務的重要性，例如高強度密碼、多重要素驗證以及定期的安全更新。
4. 管理變更 – 建立全方位的變更管理計劃，以便處理與採用零信任架構相關的組織和文化變更。向員工說明採用該架構的好處和理由，並解決任何疑慮或阻力。提供持續的支援和指引，促進順利轉換。

第 3 階段：監測和持續改善

零信任實作的第三和最終階段是監控和持續改進。這個階段包含建立全方位的監測和分析計劃、制定全面的事件回應計劃，以及定期徵求利害關係人和使用者的意見回饋。

1. 持續監控 – 建立全方位的監控和分析計劃，以持續評估安全狀態並偵測任何潛在的異常。使用進階安全工具和技術來監控使用者行為、網路流量和系統活動。
2. 規劃事件回應和修復 – 建立符合零信任原則的全方位事件回應計劃。建立明確的上報路徑、定義角色和責任，並在可能的情況下實作自動化事件回應機制。定期測試和更新事件回應計劃。
3. 取得意見回饋和評估 – 定期徵求利害關係人和使用者的意見回饋，以收集有關零信任架構 (ZTA) 有效性的洞察。進行定期評定和評估，以衡量對安全狀態、營運效率和使用者體驗的影響。使用意見回饋和評估結果來識別需要改善的領域。預期 ZTA 會隨著時間變化，並考慮開發團隊要如何以最少的努力或在盡量避免干擾的情況下，實作這些更新。

章節摘要

組織可以透過遵循這種分階段採用方法，有效地轉換到 ZTA，同時大幅降低風險和干擾。下節會討論透過零信任實作取得成功的最佳實務，範圍涵蓋高階主管、副總和資深經理的關鍵考量要素和建議。

透過零信任獲致成功的最佳實務

若要成功採用零信任架構 (ZTA)，就必須採用具策略性的方法並遵守最佳實務。本節會介紹一系列最佳實務，引導高階主管、副總和資深經理透過採用零信任獲致成功。您的組織可透過遵循這些建議，建立穩固的安全基礎，並實現零信任方法的好處：

- 定義明確的目標和業務成果 – 明確定義雲端營運的目標和期望的業務成果。將這些目標與零信任的原則保持一致，以建立堅實的安全基礎，同時促進業務成長和創新。
- 進行全面評估 – 針對目前的 IT 基礎設施、應用程式和資料資產執行全面的評估。識別相依性、技術負債和潛在的相容性問題。這項評估會為採用計劃提供資訊，並根據重要性、複雜性和業務影響來排定工作負載的優先順序。
- 制定採用計劃 – 整合詳細的採用計劃，概述將工作負載、應用程式和資料移至雲端的逐步方法。定義採用階段、時間表和相依性。吸引關鍵利害關係人參與其中，並據此分配資源。
- 儘早開始建置 - 只要您開始構建和部署零信任架構 (而不只是分析和談論該架構)，您就越來越能真實展現零信任架構在組織內的樣貌。
- 取得高階主管贊助 – 確保高階主管對於實作零信任架構的贊助和支持。吸引其他高階主管參與，以支持該計劃並分配必要資源。領導階層的承諾對於推動成功實作所需的文化和組織變更至關重要。
- 實作治理框架 – 建立治理框架，為零信任實作定義角色、責任和決策流程。清楚定義安全控制項、風險管理和合規的問責和擁有權。定期檢閱和更新治理框架，以適應持續演進的安全要求。
- 支援跨職能協作 – 鼓勵不同業務單位、IT 團隊和安全團隊之間進行協作和溝通。建立共同責任的文化，促進整個零信任實作程序的一致性和協作。鼓勵頻繁互動、共享知識以及共同解決問題。
- 保護資料和應用程式 – 零信任不僅關於最終使用者存取資源和應用程式的行為；零信任原則也應在工作負載內部和工作負載之間實作。也請一併使用資料中心內所有可用的背景資訊，以便套用相同的技術原則 (高強度身分識別、微分段和授權)。
- 提供深度防禦 – 使用多層安全控制項來實作深度防禦策略。結合多重要素驗證 (MFA)、網路分段、加密和異常偵測等各種安全技術，提供全方位的保護。確保每一層都與其他層相輔相成，以建立強大的防禦系統。
- 需要高強度的身分驗證 – 針對存取所有資源的所有使用者，強制執行 MFA 等高強度的身分驗證機制。理想情況下，請考慮 FIDO2 硬體支援的安全密鑰等現代化 MFA，它能為零信任架構提供高層級的身份驗證保證，且具備各種安全優點（例如，防止網路釣魚）。
- 集中並改善授權 – 特別是在每次嘗試存取時進行授權。根據協議的細節，這應該根據每次連線或每個請求執行。根據每個請求執行最為理想。使用身分識別、裝置、行為和網路資訊等所有可用的背景資訊，進行更精細、具適應性且完善的授權決策。

- 使用最低權限原則 – 實作最低權限原則，授予使用者執行其工作職責所需的最低存取權限。根據工作角色、責任和業務需求，定期檢閱和更新存取權限。實作即時存取佈建。
- 使用特權存取管理 – 實作特權存取管理 (PAM) 解決方案，以保護特權帳戶的安全，以及降低未經授權存取關鍵系統的風險。PAM 解決方案可提供特權存取控制項、工作階段記錄和稽核功能，協助您的組織保護最敏感的資料和系統。
- 使用微分段 – 將網路分割成更小、隔離程度越高的區段。使用微分段功能，根據使用者角色、應用程式或資料敏感度，在區段之間強制執行嚴格的存取控制。努力清除所有不必要的網路路徑，特別是導向資料的路徑。
- 監控和回應安全警告 – 在雲端環境中實作全方位的安全監控和事件回應計劃。使用雲端原生安全工具和服務，即時偵測威脅、分析日誌，以及自動化事件回應。建立清楚的事件回應程序、定期執行安全評估，以及持續監控異常或可疑活動。
- 使用持續監控功能 – 若要快速有效地偵測和回應安全事件，請實作持續監控功能。使用進階安全分析工具來監控使用者行為、網路流量和系統活動。自動進行警告和通知，確保人員能即時回應事件。
- 推動安全和合規文化 – 在整個組織中推動安全和合規的文化。向員工說明安全最佳實務、遵守零信任原則的重要性，以及員工在維護安全雲端環境中所扮演的角色。定期進行安全意識培訓，協助確保員工對社交工程保持警惕，並且了解自己在資料保護和隱私權方面的責任。
- 使用社交工程模擬 – 進行社交工程模擬，以評估使用者對社交工程攻擊的敏感度。使用模擬結果來量身打造培訓計劃，以提高使用者的意識並改善對潛在威脅的因應方式。
- 推動持續教育 – 提供持續的安全培訓和資源，建立持續教育和學習的文化。讓使用者瞭解不斷推陳出新的安全最佳實務。鼓勵使用者保持警惕，以及迅速舉報任何可疑活動。
- 持續評估和最佳化 – 定期評估雲端環境以了解需要改善的領域。使用雲端原生工具監控資源用量和效能，並進行漏洞評估和滲透測試，以識別並解決任何弱點。
- 建立治理和合規性框架 – 制定治理和合規框架，協助確保您的組織符合業界標準和法規要求。在框架中定義政策、程序和控制項，以保護資料和系統免受未經授權的存取、使用、披露、干擾、修改或破壞。實作追蹤和回報合規指標的機制、定期進行稽核，以及迅速解決任何不合規的問題。
- 鼓勵合作和知識共享 – 鼓勵參與 ZTA 採用的團隊之間進行協作和知識共享。若要達成此目的，您可以促進 IT、安全性和業務單位之間的跨職能溝通和協作。您的組織也可以建立論壇、工作坊和知識分享會議，以促進理解、解決挑戰，並分享在整個採用過程中學到的經驗。

關鍵要點

本指南探討了制定成功零信任架構 (ZTA) 策略的重要層面。本節從會已呈現的規範性指引摘錄出關鍵要點：

- 了解零信任原則 – 零信任是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。熟悉零信任的核心原則，例如最低權限、微分段、持續的身分驗證以及適應性授權。
- 定義明確的目標 – 明確定義採用 ZTA 的目標和期望的業務成果。將這些目標與零信任的原則保持一致，協助確保穩固的安全基礎，同時促進業務成長和創新。
- 進行全面評估 – 對現有的 IT 基礎設施、應用程式和資料資產執行徹底的評估。識別相依性、技術負債和相容性問題，為您的採用策略提供參考資訊。
- 制定 ZTA 採用計劃 – 建立詳細計劃，列出逐步將工作負載、應用程式和資料移至雲端的方法。考慮合規需求和應用程式現代化等因素。
- 實作堅實的 ZTA – 設計並實作 ZTA，強制執行精細的存取控制項、高強度身分驗證機制以及持續監控。若要更有效率地採用 ZTA，請使用雲端原生零信任服務，例如 AWS Verified Access 和 Amazon VPC Lattice。
- 排定資料和應用程式安全性的優先順序 – 套用零信任原則 (高強度身分識別、微分段和授權)，以提供所有可用的背景資訊。將此背景資訊用於存取系統和資源的使用者，以及後端元件內部和之間的通訊和資料流程。
- 建立監控和事件回應框架 – 在雲端環境中實作堅實的安全監控和事件回應功能。使用雲端原生安全工具進行即時威脅偵測、日誌分析和事件回應自動化，例如 Amazon Inspector AWS Security Hub CSPM和 Amazon GuardDuty。
- 培養安全和合規的文化 – 在整個組織中推動安全意識和合規的文化。向員工說明安全最佳實務，以及他們在維護安全雲端環境中扮演的角色。
- 持續評估和最佳化 – 定期評估雲端環境、安全控制項和營運流程。若要收集洞察並針對資源使用率、成本管理和效能進行最佳化，請使用 Amazon CloudWatch 和 AWS Security Hub CSPM等雲端原生的分析和監控工具。
- 建立治理和合規框架 – 制定符合業界標準和法規要求的治理和合規框架。定義政策、程序和控制項，以協助確保遵守安全性、隱私權和合規性標準。

後續步驟

採用零信任架構 (ZTA) 是其中一項改善組織安全狀態並降低風險的最安全方法。本規範性指引為您提供實作零信任的全方位藍圖，包括了解原則、評估準備程度，以及實作必要元件。

此工作串流或網域中的後續步驟包含以下項目：

- 實作採用計劃
- 實作 ZTA
- 定期進行安全評估
- 持續最佳化雲端環境和安全控制項

ZTA 是一個持續進行的過程，需要持續的監控、評估和適應，以確保穩固的安全基礎。透過遵循本指南中概述的最佳實務，您的組織便能強化安全狀態、確保遵守法規，以及保護敏感資料。

常見問答集

本節提供有關設計和實作零信任架構 (ZTA) 的常見問題解答。

什麼是零信任？

零信任是一組概念模型和一系列相關聯的機制，著重於為數位資產提供安全控制項，且這些機制並非僅根據傳統的網路控制項或網路邊界運作，或完全不基於此類措施運作。而是透過身分識別、裝置、行為和其他豐富的背景資訊和訊號來增強網路控制，以做出更精細、更有智慧、更具適應性且持續的存取決策。

什麼 AWS 服務 可以協助我實作零信任架構？

AWS 提供數種服務，可協助實作零信任，例如 AWS Identity and Access Management (IAM) AWS Verified Access、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。

如何使用 確保資料安全 AWS？

AWS 提供靜態和傳輸中資料加密的服務，例如 AWS Key Management Service (AWS KMS)、用於網路隔離的 Amazon Virtual Private Cloud (Amazon VPC)，以及 AWS Secrets Manager 用於安全儲存和擷取登入資料的服務。

可以在零信任環境中 AWS 協助滿足合規要求嗎？

是， AWS 其合規計劃和服務可協助滿足各種法規要求。 AWS Artifact 提供 AWS 合規報告的存取權，並 AWS Config 支援持續監控和評估合規。

在零信任環境中，是否有任何用於自動化安全性 AWS 的工具或服務？

AWS 提供 等服務 AWS Security Hub CSPM，可集中和自動化安全調查結果，以及定義和強制執行安全政策的 AWS Config 規則。

如何透過 在零信任雲端環境中確保持續監控和事件回應 AWS

AWS 提供 Amazon CloudWatch 等服務，用於即時監控和 AWS CloudTrail 記錄和分析。如果需要事件回應的最佳實務，可以參考 AWS 《安全事件回應指南》。

Resources

參考

- 什麼是卓越雲端中心？您的組織為什麼必須建立該中心？ – 此部落格文章概述了 CCoE 以及如何建立有效 CCoE 的最佳實務等內容。
- 零信任 AWS- 此頁面提供 AWS 環境中零信任安全原則和最佳實務的概觀。
- 零信任架構： AWS 觀點 – 此部落格文章分享零信任實作方式的定義和指導方針 AWS。
- AWS Identity and Access Management (IAM) 使用者指南 – 本指南提供在零信任架構的關鍵元件 IAM 中管理使用者存取和許可的完整文件。
- AWS Security Hub CSPM – 了解 Security Hub CSPM，這項服務可讓您全面檢視整個 的安全提醒和合規狀態 AWS 帳戶。
- AWS Well-Architected Framework – 探索 Well-Architected Framework，該框架可針對在 AWS上建置安全、高效能、具恢復能力且有效率的架構提供指引。
- AWS 安全事件回應指南 – 本指南概述在組織 AWS 雲端 環境中回應安全事件的基本原則。它概述了雲端安全性和事件回應的概念，以及識別要回應安全問題的客戶可使用的雲端功能、服務和機制。

工具

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub CSPM
- AWS Verified Access

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
新增的更新	已新增資訊至「零信任架構的關鍵元件」一節、在「評估組織採用零信任的準備程度」一節中進行變更、已新增資訊至「最佳實務」一節，以及對「常見問答集」進行變更。	2023 年 12 月 4 日
初次出版	—	2023 年 6 月 19 日

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。