



安全性模型和職責 Information Security for Workload Factory

NetApp
September 16, 2026

目錄

安全性模型和職責	1
了解 NetApp Workload Factory 的安全性模型	1
高階安全性模型	1
關鍵審查問題	1
接下來	1
NetApp Workload Factory 的共享的責任邊界	1
NetApp 職責（服務方）	1
AWS 職責（雲端平台）	2
客戶責任（您的組態）	2
要收集的證據	2
NetApp Workload Factory 上線安全性工作流程	2
步驟 1：決定您的上線方式	2
步驟 2：建立 AWS 信任與存取	3
步驟 3：套用最小權限	3
步驟 4：設定連線與 VPC 邊界（視需要）	3
步驟 5：驗證可觀測性	3
步驟 6：啟用 AI 診斷（選用）	3
NetApp Workload Factory 的法規遵循與安全性狀態	4

安全性模型和職責

了解 NetApp Workload Factory 的安全性模型

NetApp Workload Factory 是一個 SaaS 控制平面，可協助您管理和最佳化在 AWS 環境中執行於 Amazon FSx for NetApp ONTAP 上的工作負載。安全性結果取決於 NetApp、AWS 和您的組織之間的共享的責任。

高階安全性模型

- Workload Factory 使用 IAM 角色承擔模型來取得臨時 AWS STS 認證資料，以便在您的帳戶中呼叫 AWS API。
- 有些工作流程需要 ONTAP 原生操作，這些操作沒有透過 AWS API 公開；您可以使用客戶部署的執行元件（例如 Lambda 連結）在 VPC 內執行這些操作。
- 可觀測性訊號（計量、遙測資料和運行記錄）支援運行監控和調查。

關鍵審查問題

- Workload Factory 需要對您的 AWS 帳戶擁有哪些存取（角色信任 + 權限）？
- 哪些執行路徑適用於您預期的工作流程（僅限 AWS API 或透過 VPC 元件執行 ONTAP 原生操作）？
- 處理哪些資料類別（組態/中繼資料、操作日誌/事件、遙測資料）？它們存放在哪裡？
- 存在哪些監控訊號？它們的保留特性是什麼？

接下來

- ["NetApp Workload Factory 的共享的責任邊界"](#)
- ["NetApp Workload Factory 的連線能力與信任路徑"](#)
- ["NetApp Workload Factory 的最小權限層級"](#)

NetApp Workload Factory 的共享的責任邊界

NetApp Workload Factory 安全性責任是由 NetApp（SaaS 營運）、AWS（雲端基礎架構與代管服務）以及您（客戶組態）共享的。了解各方責任的起訖範圍，有助於您正確設定 AWS 環境並避免安全性漏洞。這些界限釐清了 NetApp 營運的內容、AWS 保護的內容，以及您必須自行設定與維護的內容。

NetApp 職責（服務方）

NetApp 負責營運和保障 Workload Factory SaaS 平台的安全。這包括對儲存的組態參考和營運資料的服務端處理。

AWS 職責（雲端平台）

AWS 負責您的部署和工作流程使用的雲端基礎架構和代管服務的安全性（例如 IAM/STS、FSx for ONTAP、CloudWatch、KMS、Secrets Manager、CloudFormation、Lambda 和連網原語）。

客戶責任（您的組態）

您負責：

- AWS IAM 角色、信任原則和最小權限
- VPC 控制（子網路、安全性群組、路由、端點和出口）
- 認證資料治理（包括工作流程所需的 ONTAP 認證資料）
- 加密和金鑰管理決策（例如，FSx for ONTAP 的選用客戶代管 KMS 金鑰）
- 監控、警報、保留原則和事件回應流程

要收集的證據

- IAM 角色信任關係（包括外部 ID 條件）
- IAM 權限分層選擇與原則工件
- 網路邊界決策（僅限 AWS API 與 VPC 執行元件，例如 Lambda 連結）
- 可觀測性決策與保留預期
- AI 能力開發決策（除非明確停用，否則 AI 診斷預設為啟用）

NetApp Workload Factory 上線安全性工作流程

上線至 NetApp Workload Factory 可在您開始使用產品之前，建立對您 AWS 環境的安全的存取。此流程結合了 AWS 信任組態、權限界定、連線設定、可觀測性驗證，以及選用的 AI 診斷能力開發。

步驟 1：決定您的上線方式

- 確定 AWS 帳戶和環境邊界（例如，生產環境與非生產環境的分隔）。
- 識別所需的工作流程（唯讀探索、資源配置與 ONTAP 原生作業）。
- 根據工作流程需求決定是否部署 VPC 執行元件（例如 Lambda 連結）。
- 決定是否啟用 AI 診斷（預設啟用）。

相關資訊

- ["認證資料類型"](#)
- ["Lambda 連結總覽"](#)
- ["AI 控制總覽"](#)

步驟 2：建立 **AWS** 信任與存取

1. 在您的 AWS 帳戶中部署 IAM 角色。
2. 使用信任原則中的外部 ID 來控管角色代入。
3. 在 Workload Factory 中註冊角色 ARN 和外部 ID。

相關資訊

["AWS 帳戶整合"](#)

步驟 3：套用最小權限

1. 選擇支援您預期工作流程的最低權限分層。
2. 驗證每個請求的工作階段原則是否將動作限制為正在執行的作業。

相關資訊

["NetApp Workload Factory 的最小權限層級"](#)。

步驟 4：設定連線與 **VPC** 邊界（視需要）

1. 驗證到 AWS 端點的必要網路路徑。
2. 如果您需要 ONTAP 原生操作，請在您的 VPC 中部署並驗證適當的執行選項。

相關資訊

- ["NetApp Workload Factory 的連線能力與信任路徑"](#)
- ["NetApp Workload Factory 的 ONTAP 執行選項"](#)

步驟 5：驗證可觀測性

1. 確認計量和遙測資料已如預期收集和保留。
2. 請確認您可以存取所需的運作記錄，以便進行疑難排解和調查。

相關資訊

- ["NetApp Workload Factory 的可觀測性總覽"](#)
- ["NetApp Workload Factory 的計量與遙測"](#)

步驟 6：啟用 **AI** 診斷（選用）

AI 診斷預設為啟用。若啟用，請確認您符合所有先決條件，並將權限範圍限定在最低要求。

相關資訊

- ["Bedrock 選擇加入 NetApp Workload Factory AI 診斷"](#)
- ["NetApp Workload Factory 的人工智慧工具邊界"](#)

NetApp Workload Factory 的法規遵循與安全性狀態

NetApp Workload Factory 以法規遵循和安全性為核心優先順序進行建置。Workload Factory 中的所有工作負載均在 Amazon FSx for NetApp ONTAP 上執行。除了 "[AWS 安全功能](#)" 之外，NetApp Workload Factory 還具有 "[SOC2 Type 1](#)、[SOC2 Type 2](#) 和 [HIPAA 法規遵循](#)"。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory 是一個 "[用於部署企業應用程式的 AWS 解決方案](#)"，它遵循 AWS 架構完善的最佳實務。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。