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

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

商標資訊