架構與連線

Information Security for Workload Factory

NetApp
September 16, 2026

目錄

架構與連線

NetApp Workload Factory 的連線能力與信任路徑

NetApp Workload Factory 與 AWS API、客戶 AWS 帳戶資源、AWS Lambda 連結和 Amazon Bedrock 通訊，每個服務都有其自身的協定、連接埠和驗證方法。這些連線組織成不同的群組，分隔 AWS 管理平面、ONTAP 資料平面和 Lambda 連結流量，以便您可以獨立評估信任邊界。

連接路徑

Workload Factory 建立了多個不同的連線路徑，每條路徑都有特定的用途，用於探索、配置和管理您的 AWS 和 ONTAP 資源。部分路徑源自 Workload Factory 本身，使用假定的 AWS 認證資料，而其他路徑則透過 Lambda 連結執行，該連結在您的 VPC 內部運作，以連線至 ONTAP 管理端點，而無需將其公開。前往 Amazon Bedrock 的選用路徑支援 AI 輔助診斷，且只有在您的組織啟用該功能時才會作用中。

以下各節說明每條路徑，包括涉及的 AWS 或 ONTAP API、使用的認證資料或驗證，以及決定路徑是否為作用中的任何條件。了解這些路徑有助於您評估 Workload Factory 所需的網路存取和權限，以及資料跨越帳戶或 VPC 邊界的位置。

Workload Factory 到 **AWS API**

Workload Factory 使用 `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` 以及 EC2/VPC API 進行子網路和安全性群組探索。

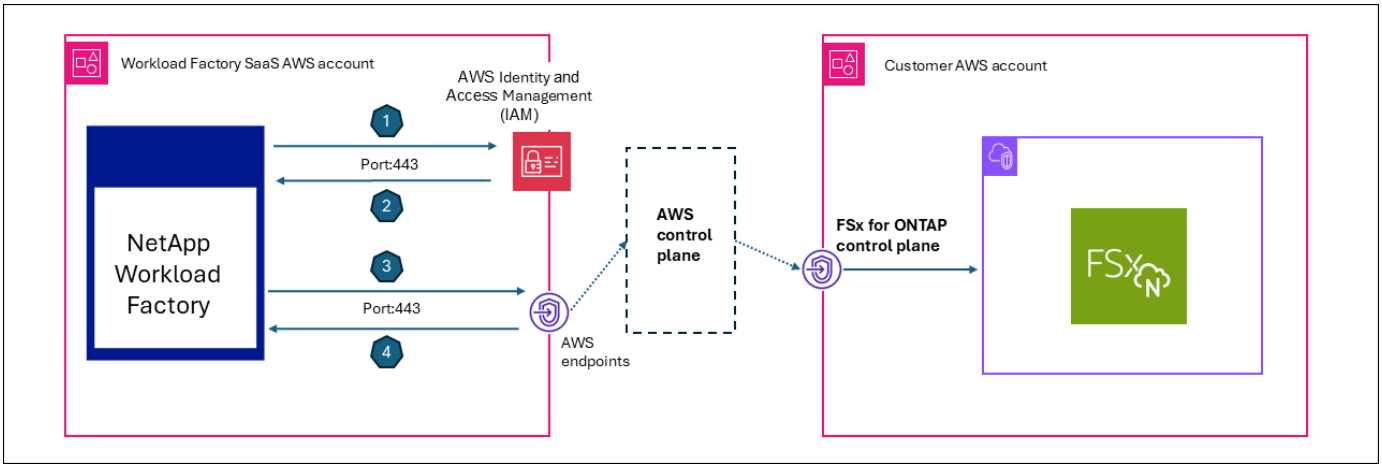
- 採集服務大約每五小時進行一次掃描。
- CRUD 操作隨需執行。
- 所有呼叫均使用具備外部 ID 的 STS 假設臨時認證資料。

Workload Factory 到客戶 **AWS** 帳戶資源（協調和自動化）

Workload Factory 與 AWS 互動，以進行通訊和建立資源。協調與自動化以多種方式進行。

- AWS CloudFormation 範本：Workload Factory 使用 AWS CloudFormation 範本建立角色和檔案系統等資源。例如，當您在使用者介面中建立檔案系統時，Workload Factory 會直接呼叫 CloudFormation 並將您重新導向至您的 AWS 帳戶。
- AWS API 呼叫：Workload Factory 使用 AWS API 呼叫（STS `AssumeRole`）來傳送 FSx for ONTAP 相關活動的 API 命令。
- AWS Lambda：Workload Factory 使用 CloudFormation 為與 ONTAP 通訊的連結部署 AWS Lambda 函數。

下圖顯示 Workload Factory 如何使用 NetApp AWS 帳戶與具有 FSx for ONTAP 檔案系統的客戶 AWS 帳戶之間的信任關係。



1. Workload Factory 使用來自 AWS IAM 服務的客戶專屬外部 ID，向 AWS STS `AssumeRole` 提出要求。
2. AWS IAM 服務會擷取角色並建立工作階段。
3. Workload Factory 發出具有工作階段權限的 AWS API 請求。
4. Workload Factory 從 FSx for ONTAP 控制平面接收 AWS API 回應。

Lambda 連結到 **ONTAP** 管理端點

Lambda 連結在客戶 VPC 內部執行，用於私有子網路存取，而無需公開 ONTAP。從連結到 ONTAP 管理端點的所有連線僅限傳出，因此不需要傳入連線或公開的端點。此連結僅用於 Amazon FSx for NetApp ONTAP API 未公開的 ONTAP 原生作業。

Workload Factory 使用以下協定進行 Volume、儲存設備 VM 和叢集操作，以及唯讀診斷和效能資料：

- HTTPS/443（REST）
- SSH/22（CLI）

Lambda 連結到 **AWS Secrets Manager**（**ONTAP** 認證資料擷取）

僅當 ONTAP 管理員認證資料儲存在 AWS Secrets Manager 中時使用（替代方案：在 Workload Factory 中使用信封加密的認證資料）。

- 代理轉發器在標頭中傳遞 `x-aws-secret-arn`（Base64 編碼）。
- Lambda 連結會在執行時呼叫 `GetSecretValue`來擷取密碼。

這樣可以確保密碼在您的帳戶範圍內，並防止從 Workload Factory 傳輸出去。

Workload Factory 和客戶元件到 **Amazon Bedrock**（**AI** 診斷）

僅當啟用 AI 診斷時才會使用此路徑。

- Event Analyzer 使用此路徑進行 EMS 分析和延遲診斷。
- Bedrock 會使用您假定的認證資料和推論設定檔 ARN 執行，因此資料不會流向 NetApp 的帳戶。

傳送到 Bedrock 的資料可以包括 EMS 事件 JSON、QoS 統計資料、Volume 組態、彙總資料和節點資訊。只有為每個組織 (`ai_analyzer_config` 表格設定了推論設定檔時，此路徑才作用中）。

連線群組（協定、連接埠和驗證）

A 組 **— AWS** 管理平面信任路徑（假定認證資料）

連線	傳輸協定	連接埠	方向	驗證	理由
STS AssumeRole	HTTPS	443	WF → AWS STS（客戶帳戶）	IAM 認證資料 + ExternalId	取得臨時跨帳戶認證資料
FSx API（描述/建立/更新/刪除）	HTTPS	443	WF → AWS FSx 端點（客戶區域）	STS 臨時認證資料	檔案系統和 Volume 生命週期管理
EC2/VPC API	HTTPS	443	WF → AWS EC2 端點	STS 臨時認證資料	安全群組、子網路和 VPC 探索
CloudFormation API	HTTPS	443	WF → AWS CFN 端點	STS 臨時認證資料	IAM 角色和 FSx 配置的堆疊部署
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager 端點（客戶帳戶）	STS 臨時認證資料	擷取 ONTAP 管理員密碼（當儲存在 Secrets Manager 中時）
KMS 加密/解密	HTTPS	443	WF → AWS KMS 端點	STS 臨時認證資料	Volume 加密金鑰操作

所有 AWS API 呼叫均使用客戶的區域端點，如果已設定，則可透過 VPC 端點進行路由。

B 組 **— ONTAP** 資料平面

ONTAP 資料平面始終透過 Lambda 連結進行代理；Workload Factory 服務永遠不會直接連接到 ONTAP。

連線	傳輸協定	連接埠	方向	驗證	理由
ONTAP REST API	HTTPS	443	連結（客戶 VPC）→ ONTAP 管理 LIF	基本驗證（使用者名稱/密碼）或 Secrets Manager ARN	叢集、Volume 和儲存設備 VM 組態；QoS；EMS 事件；ARP 狀態
ONTAP SSH CLI	SSH	22	連結（客戶 VPC）→ ONTAP 管理 LIF	密碼驗證	診斷命令（QoS 統計資料、df、事件日誌、效率）

代理轉發器的路由策略（優先順序）：

1. 明確 `x-link-id`標頭：從資料庫中尋找 Lambda ARN
2. 目標 ID（FSx 檔案系統 ID）：尋找關聯連結
3. Console 代理程式 ID：透過訊息代理人路由至 Console 代理程式

C 組 **— AWS Lambda** 連結（部署在您的 **VPC** 中）

連線	傳輸協定	連接埠	方向	驗證	理由
Lambda 呼叫	HTTPS（AWS SDK）	443	WF → AWS Lambda API（客戶帳戶）	IAM (`lambda:InvokeFunction`)	從客戶 VPC 內部執行 ONTAP REST/SSH 命令
Lambda → ONTAP	HTTPS + SSH	443 、 22	Lambda（客戶 VPC）→ ONTAP 管理 LIF	基本驗證 / 密碼	無需公開暴露即可透過私有子網路存取 ONTAP

群組 **D — NetApp Console** 代理程式（您的 **VPC** 中的 **EC2**，僅限傳出）

連線	傳輸協定	連接埠	方向	驗證	理由
代理程式輪詢	HTTPS	443	控制台代理程式（客戶 VPC）→ WF 訊息代理人	持有者權杖（occm-access 範圍）	對待處理的 ONTAP 命令進行長輪詢（7 秒逾時；重新連線）
代理程式回應	HTTPS	443	控制台代理程式（客戶 VPC）→ WF 訊息代理人	Bearer 權杖	傳回 ONTAP 命令結果（可選擇 zlib 壓縮）
主控台代理程式 → ONTAP	HTTPS + SSH	443 、 22	控制台代理程式（客戶 VPC）→ ONTAP 管理 LIF	基本驗證 / 密碼	執行代理 ONTAP 作業

關鍵設計：Workload Factory 從不主動發起與 Console 代理程式的傳入連線。工作在 Redis 串流中佇列；Console 代理程式輪詢 `GET /messagebroker/v1/requests`並做出回應 `POST /messagebroker/v1/responses`。

E 組 **— CloudFormation** 自訂資源回呼

連線	傳輸協定	連接埠	方向	驗證	理由
CloudFormation → WF Lambda	HTTPS	443	CloudFormation（客戶）→ WF Lambda（NetApp）	JWT 權杖 + 參考權杖	報告 IAM 角色建立狀態並傳回角色 ARN
ONTAP CloudFormation 資源提供者 → 連結	HTTPS	443	CloudFormation 資源 Lambda（客戶）→ 連結 Lambda（客戶）	IAM	在堆疊操作期間建立/更新/刪除 ONTAP 資源

總結：**VPC** 的網路要求

元件	傳入	傳出
FSx for ONTAP	來自 Link Lambda 或控制台代理程式安全性群組的連接埠 443 和 22	N/A
連結 Lambda	無	連接埠 443（ONTAP、AWS API）和連接埠 22（ONTAP SSH）
主控台代理程式 EC2	無	連接埠 443（WF 端點、ONTAP、AWS API）和連接埠 22（ONTAP SSH）
VPC 端點（可選）	N/A	STS、FSx、S3、Secrets Manager、Lambda、CloudFormation

客戶 VPC 中的任何元件都不需要傳入網際網路存取。所有連線皆為傳出起始（Console 代理程式輪詢），或是透過 AWS 服務 API 呼叫（Lambda Invoke）。

NetApp Workload Factory 的 ONTAP 執行選項

某些 NetApp Workload Factory 工作流程需要執行 ONTAP 原生操作，而這些操作並未透過 AWS API 公開。Workload Factory 提供兩種執行選項，可將這些操作保留在您的 AWS 帳戶邊界內：一種是從您的 VPC 內執行 ONTAP 操作的 Lambda 連結，另一種是使用來自 EC2 執行個體僅傳出連線的 NetApp Console 代理程式。這兩種選項都允許您執行所需的 ONTAP 操作，同時將網路、認證資料和生命週期決策保留在您的安全性模型內。

執行選項

Lambda 連結（您 **VPC** 中的 **AWS Lambda**）

從您的 VPC 內部執行 ONTAP REST 和唯讀 ONTAP CLI 診斷，而無需公開 ONTAP。

NetApp Console 代理程式（您 **VPC** 中的 **EC2**，僅限傳出）

執行代理 ONTAP 操作，其中代理程式發起傳出連線，而 Workload Factory 從不發起與代理程式的傳入連線。

安全性考量

- 網路邊界：確認所需的傳出連接埠（443/22）和目的地。
- 認證資料邊界：決定 ONTAP 認證資料是儲存在 Workload Factory（信封加密）中，還是從 AWS Secrets Manager 中引用。
- 可稽核性：確認元件活動和故障的運作記錄。
- 生命週期管理：確認更新和移除如何發生。

相關資訊

- "NetApp Workload Factory 的 Lambda 連結總覽"

- "NetApp Workload Factory 的連線能力與信任路徑"
- "NetApp Workload Factory 的加密與金鑰管理"