NetApp Workload Factory 的資訊安全性

Information Security for Workload Factory

NetApp
September 16, 2026

目錄

了解 NetApp Workload Factory 的資訊安全性

資訊安全性是 NetApp Workload Factory 設計和營運的核心組成部分。資訊安全、雲端平台和儲存設備團隊可以利用這些詳細資訊來評估和就職 Workload Factory，以支援企業安全性需求。

什麼是 Workload Factory

Workload Factory 是一個 SaaS 生命週期管理平台，旨在協助您使用 Amazon FSx for NetApp ONTAP 最佳化和管理工作負載（例如儲存設備、VMware 遷移、EDA 專案和資料庫環境）。您的工作負載在 AWS 中運作。

Workload Factory 使用 AWS API 來執行所有可透過 AWS 原生提供的 FSx for ONTAP 操作，並使用 ONTAP REST API 來執行平台支援但無法透過 AWS API 原生提供的 Workload Factory 操作。

本指南中所使用的核心安全性原則

保密性

透過身分控制、最小權限原則、加密和網路邊界來保護資料免受未經授權的存取。

完整性

使用權限範圍、變更控制和可稽核性來保護系統和組態免受未經授權或意外變更的影響。

可用性

透過具有恢復能力的 AWS 設計和運作監控，確保授權使用者可以存取服務和工作負載。

本指南涵蓋的資訊類型

以下各節提供資訊，協助您評估與就職 Workload Factory，以支援企業安全性要求。

1. 安全性模型和職責
   - "安全性模型概覽"
   - "共同責任邊界"
2. 架構與連線
   - "連結性和信任路徑"
   - "ONTAP 執行選項"
3. 身分、憑證和最小權限
   - "AWS 帳戶整合"
   - "最小權限層級"
4. 資料治理、隱私和生命週期
   - "資料處理和駐留"
   - "帳戶刪除清單"

5. 可觀測性和監控
    - "指標和遙測"
6. AI 控制和 VPC 元件
    - "AI 控制總覽"
    - "Lambda 連結總覽"

快速入門

- 從_檢視、規劃和分析_（唯讀）權限開始，並僅在需要時擴充。
- 使用 AWS CloudTrail 驗證 `sts:AssumeRole`整合角色的活動。
- 事先決定您是否需要部署 Lambda 連結或 NetApp Console 代理程式的 ONTAP 原生作業。
- 事先決定是否允許生成式 AI，以及駐留限制是否需要單一區域推論設定檔。

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。

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。

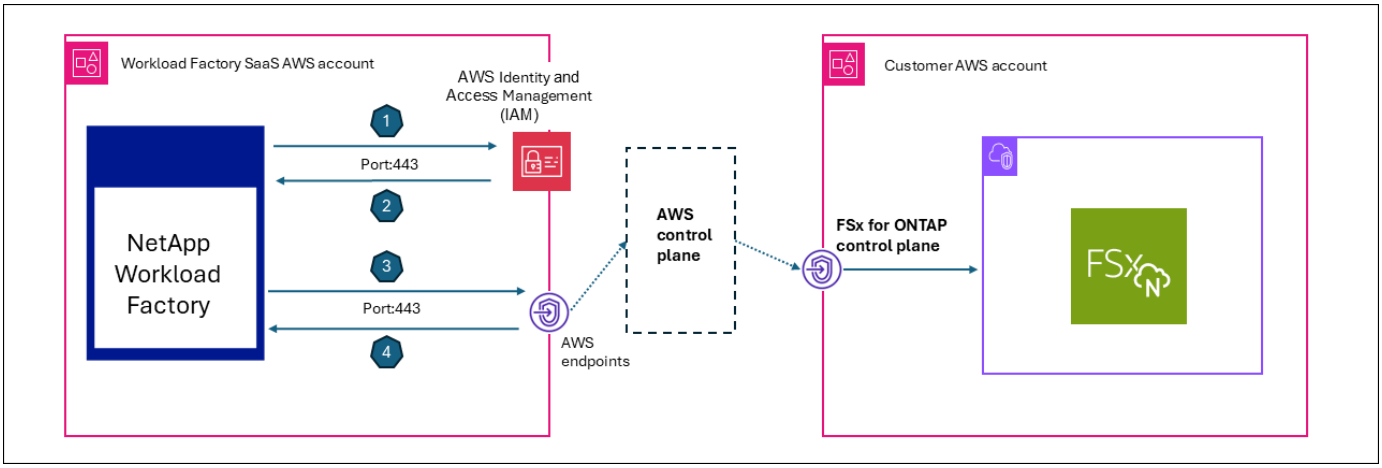
- 採集服務大約每五小時進行一次掃描。
- CRUD 操作隨需執行。
- 所有呼叫均使用具備外部 ID 的 STS 假設臨時認證資料。

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"

身分、憑證和最小權限

AWS 帳戶與 NetApp Workload Factory 整合

Workload Factory 使用 AWS `sts:AssumeRole` 取得您 AWS 帳戶的臨時認證資料，因此該服務不會儲存長期 AWS 存取金鑰。在上線期間，您設定一個 IAM 角色，Workload Factory 可以擔任該角色以進行核准的 AWS API 操作，並使用外部 ID 來協助防止未經授權的跨帳戶存取。Workload Factory 隨後會在執行階段使用產生的短期認證資料，AWS 會在每次工作階段後自動使其過期。

AWS 帳戶組態

若要讓 Workload Factory 存取您的 AWS 帳戶：

1. 在您的 AWS 帳戶中部署 IAM 角色（使用 CloudFormation 或手動）。
2. 確保角色信任原則允許 Workload Factory 的服務主體透過外部 ID 來承擔該角色。
3. 使用外部 ID 作為客戶與 Workload Factory 之間專屬共享的唯一秘密識別碼（UUID v4）。

   將其作為條件嵌入到您的 IAM 角色信任原則中 (`sts:ExternalId`)。

   外部 ID 可防止混淆代理人攻擊。在跨帳戶存取模型中，發現客戶角色 ARN 的攻擊者若沒有對應的外部 ID，就無法擔任該角色。AWS 建議將此模式用於第三方跨帳戶存取。如需詳細資訊，請參閱 AWS IAM 文件頁面 "存取第三方擁有的 AWS 帳戶"。

   外部 ID 在認證資料註冊期間產生一次，並與角色 ARN 一起加密儲存在 Workload Factory 資料庫中。

4. 在 Workload Factory 中註冊角色 ARN 和外部 ID。

執行階段

在執行階段，Workload Factory 會代入您的 IAM 角色，以便為每個 AWS API 操作取得短期認證資料：

1. Workload Factory 會使用您的角色 ARN 和外部 ID 來呼叫 `sts:AssumeRole`。
2. AWS 傳回臨時認證資料（存取金鑰、秘密金鑰和工作階段權杖）。
3. Workload Factory 會使用臨時認證資料來進行您帳戶中的 AWS API 操作。
4. 認證資料會自動過期（預設為一小時）。

AWS 認證資料如何流經 NetApp Workload Factory

AWS 認證資料流程描述了 NetApp Workload Factory 在部署和執行階段操作期間如何處理角色識別碼、外部 ID 和短期 AWS STS 認證資料。在一次性設定期間，您需要在 AWS 帳戶中建立 IAM 角色，並設定信任原則，該原則要求 Workload Factory 服務主體和正確的外部 ID。在執行階段，Workload Factory 會使用已儲存的角色 ARN 和外部 ID 來要求由每個要求的工作階段原則限定範圍的臨時認證資料，並會重複使用快取的認證資料，直到它

們過期為止。

一次性設定

對於一次性設定，流程如下：

步驟

1. 您產品發表 CloudFormation 堆疊或在您的 AWS 帳戶中手動建立 IAM 角色。
2. IAM 角色信任原則規定了兩個條件：
   a. 只有 Workload Factory 的服務主體才能承擔此責任。
   b. 呼叫者必須提供正確的外部識別碼。
3. Workload Factory 將角色 ARN 和外部 ID（加密）儲存在其資料庫中。

執行階段（每次 **API** 操作）

在執行階段，Workload Factory 使用儲存的角色 ARN 和外部 ID 來為每個 API 作業取得臨時的 AWS STS 認證資料。流程如下：

步驟

1. Workload Factory 從 MySQL 擷取儲存的角色 ARN 和外部 ID。
2. 它會檢查 Redis 中是否有此角色的一組快取臨時 AWS STS 認證資料。
3. 當快取未命中時，Workload Factory 會使用角色 ARN 和外部 ID 呼叫 `sts:AssumeRole`。此呼叫包含每個請求的即時工作階段原則，該原則將權限限制為僅該作業所需的特定 AWS 動作。
4. AWS STS 傳回帶有過期時間戳記的臨時認證資料（存取金鑰 ID、秘密存取金鑰、工作階段權杖）。
5. Workload Factory 將這些認證資料快取在 Redis 中，並使用它們來呼叫目標 AWS API。
6. 發生快取命中率時，Workload Factory 會略過 STS 呼叫，並直接使用快取的認證資料。

工作階段原則

每個 STS 呼叫都包含一個即時工作階段原則，其範圍限定為所需的最少 AWS 操作。

相關資訊

- "最小權限層級"

適用於 **NetApp Workload Factory** 的 **AWS** 認證資料保留

Workload Factory 透過短期有效的 AWS STS 認證資料、加密的角色中繼資料和限時保留機制來確保認證資料處理的安全性。此認證資料模型將保留的角色中繼資料與用於 API 操作的臨時 AWS 認證資料分隔。臨時認證資料僅在有限的時間內快取，並根據 AWS 的強制執行機制自動過期。刪除認證資料會阻止 Workload Factory 為該帳戶取得新的認證資料，而任何快取的認證資料也會在不久後過期。

關鍵行為

- Workload Factory 不儲存長期 AWS 存取金鑰。

  Workload Factory 僅儲存一個指標（角色 ARN）和一個共享的機密（外部 ID）。兩者本身均不授予 AWS 存取。

- 臨時 AWS STS 認證資料的壽命最長為一小時（AWS 強制執行）。

  Workload Factory 會將它們快取在 Redis 中最多 30 分鐘，然後強制執行新的 STS 呼叫。

- 如果快取的認證資料集剩餘時間少於 15 分鐘，Workload Factory 會將其捨棄並取得新的認證資料集。
- 客戶刪除認證資料將立即撤銷 Workload Factory 存取該帳戶的權限。

  下一次 AssumeRole 呼叫失敗，快取的認證資料會在幾分鐘內過期。

保留和儲存設備總結

資料	儲存位置	保留時間	自動過期？	刪除方法
IAM 角色 ARN + 外部 ID	MySQL（靜態加密）	無限期保存（直至客戶明確刪除）	否	客戶在 UI 中點選「刪除認證資料」
暫時 AWS STS 認證資料（存取金鑰 + 機密 + 工作階段權杖）	Redis（記憶體快取）	最長 30 分鐘（快取 TTL）。底層 STS 認證資料的有效期限最長為一小時（AWS 預設值）。快取會在過期前五分鐘清除，作為安全利潤。	是的（Redis TTL 會自動驅逐；AWS 認證資料過期由 AWS 強制執行）	自動
ONTAP 管理員密碼	MySQL（使用 KMS 的 AES-256-CBC 信封加密）	無限期保存（直至客戶移除認證資料或刪除檔案系統）	否	客戶刪除認證資料，或檔案系統刪除觸發清理操作
已解密的 ONTAP 密碼（明文）	僅限記憶體（絕不寫入磁碟或快取）	單一請求持續時間（毫秒）	是的（請求完成後會被垃圾回收）	自動

安全性控制

- 外部 ID 可防止混淆代理攻擊。
- 工作階段原則強制執行每次請求的最小權限。
- Workload Factory 會在風險較高的過期視窗之前刷新短期的臨時 AWS STS 認證資料。
- 在標準、GovCloud 和中國環境中，區域和帳戶類型的處理方式有所不同。
- Workload Factory 從不儲存長期 AWS 存取金鑰。
- Workload Factory 絕對不會修改您的 IAM 角色權限。

- Workload Factory 的權限永遠不會超出您的角色原則所授予的權限。
- 工作階段原則只能減少權限；Workload Factory 永遠不會增加權限。

NetApp Workload Factory 的認證資料類型

NetAppWorkload Factory 使用分離認證資料模型，將 AWS 控制平面權限與直接的 ONTAP 管理存取分隔。AWS IAM 角色會驗證 Workload Factory 對 AWS API 的存取，以進行檔案系統管理、備份管理和資源探索等操作。ONTAP 認證資料會透過 Lambda 連結驗證對 ONTAP 管理端點的直接存取，以進行需要管理組態或診斷的操作。當某些工作流程結合 AWS API 操作與直接的 ONTAP 管理任務時，會需要同時使用這兩種認證資料。

認證資料類型

下表總結了 Workload Factory 中使用的兩種認證資料類型及其各自的驗證目標。

認證資料類型	驗證至	用於
AWS 認證資料（AssumeRole）	AWS API	所有透過 AWS FSx 服務 API 進行的操作
ONTAP 認證資料（管理員密碼）	ONTAP 管理端點	需要直接存取 ONTAP REST API 或 CLI 的操作

僅限 **AWS** 認證資料的操作

這些操作僅與 AWS API 互動，並且只需要 IAM 角色：

- 檔案系統的建立和刪除
- 檔案系統容量和處理量變化
- 備份建立和管理
- VPC、子網路和安全性群組探索
- KMS 金鑰列舉
- CloudWatch 計量擷取
- Cost Explorer 查詢
- 使用 FSx API 進行標籤管理

僅限 **ONTAP** 認證資料的操作

這些操作透過 Lambda 連結直接與 ONTAP 管理端點通訊，並且需要 ONTAP 管理員認證資料：

- Volume 層級 QoS 原則組態
- 匯出原則和規則管理
- 儲存設備 VM 協定組態（NFS、CIFS、iSCSI）
- igroup 和 LUN 管理

- SnapMirror（複寫）組態
- Snapshot 原則管理（ONTAP 等級）
- 效能診斷（QoS 統計資料、延遲細分）
- EMS 事件擷取與分析
- 反勒索軟體保護狀態監控
- FlexCache 管理
- 網路介面（LIF）查詢

需同時具備 **AWS** 和 **ONTAP** 認證資料的操作

工作流程	**AWS** 認證資料用於	**ONTAP** 認證資料用於
人工智慧驅動的事件分析	呼叫 Bedrock，描述檔案系統	使用 SSH 擷取 EMS 事件並執行診斷
建立檔案系統並設定儲存設備 VM	建立檔案系統（AWS API）	設定儲存設備虛擬機器協定（ONTAP REST）
使用匯出原則建立 Volume	建立 Volume（AWS API）	設定匯出原則規則（ONTAP REST）
儲存容量管理	更新檔案系統容量（AWS API）	檢查彙總使用率（ONTAP SSH）

相關資訊

- "ONTAP 執行選項"
- "Lambda 連結總覽"

NetApp Workload Factory 的認證資料儲存設備選項

NetApp Workload Factory 支援認證資料處理模式，以保留最低權限並減少 ONTAP 管理機密的暴露。AI 驅動的診斷功能在可用時會使用唯讀的 ONTAP 認證資料，以便診斷代理程式可以在不修改儲存環境的情況下進行觀察和診斷。您可以使用 Workload Factory 代管的加密儲存設備，或將 ONTAP 密碼儲存在 AWS Secrets Manager 中，並提供參考給 Workload Factory。此選擇會影響密碼的儲存位置、加密方式，以及您如何管理 GovCloud 支援和認證資料輪替等要求。

唯讀 **ONTAP** 存取模型

對於事件分析和延遲診斷等 AI 功能，Workload Factory 會在可用時使用唯讀 ONTAP 認證資料。唯讀認證資料模型可確保 AI 診斷代理程式無法修改您的儲存環境—它只能觀察和診斷。

認證資料儲存設備選項比較

AWS 憑證

AWS 認證資料始終透過 IAM 角色取得。Workload Factory 可以在內部管理角色資訊，或從 AWS Secrets

Manager 參照該資訊。

選項	**AWS** 憑證	儲存的內容	加密
Workload Factory 代管	IAM 角色 ARN + 外部 ID	IAM 角色 ARN + 外部 ID	角色 ARN 不是秘密（原樣儲存）

ONTAP 憑證

Workload Factory 既可以內部使用加密儲存設備管理 ONTAP 認證資料，也可以從 AWS Secrets Manager 引用這些認證資料。選擇哪種方式會影響密碼的儲存、加密和輪換方式。

Workload Factory 需要 ONTAP 認證資料，才能透過 "Lambda 連結" 與 ONTAP 檔案系統 API 互動。

選項	**ONTAP** 憑證	儲存的內容	加密
Workload Factory 代管	密碼（加密）	ONTAP 管理員密碼（已加密）	ONTAP 密碼使用 AES-256 信封加密
AWS Secrets Manager	Secrets Manager ARN 參考	Secrets Manager ARN	Secrets ARN 本身並非機密（原樣儲存）；AWS Secrets Manager 會對您帳戶中的機密進行加密

其他考量

GovCloud 要求

使用標準 IAM 角色；ONTAP 認證資料必須使用 Secrets Manager（不允許儲存密碼）。

輪替

角色原則已在您的帳戶中更新。在 Workload Factory（代管選項）中更新 ONTAP 密碼，或在 AWS Secrets Manager 中輪換密碼。

NetApp Workload Factory 的最小權限層級

您可以隨時限制 Workload Factory IAM 權限，以遵守最小權限要求，例如限制對特定資源（ARN）的存取，並套用 IAM 條件，例如標籤和 CIDR 範圍。

分層權限模型

Workload Factory 採用分層權限模型，遵循最小權限原則。新增 AWS 憑證時，您可以選擇要啟用的功能層級。您可以從唯讀探索開始，並根據需要擴充。

Workload Factory 透過您 AWS 帳戶中的 IAM 角色授予所有權限，該角色是透過 STS 使用外部 ID 來擔任。

Workload Factory 透過即時工作階段原則進一步限定每次 API 呼叫的範圍。

在 Workload Factory 主控台中，AI 聊天功能 *Ask Me* 可協助您安全地完善權限，它會建議限制選項並產生要在 AWS 中套用的更新原則。

授予權限

將 AWS 憑證新增至 Workload Factory 時，您可以選擇要啟用的權限分層。您可以隨時啟用或停用分層。

分層是累積的：啟用較高分層會自動啟用所有較低分層。

安全性控制

- 外部 ID（混淆代理保護）
- 按作業工作階段原則（每次請求最小權限）
- 基於標籤的條件（安全性群組修改僅限於 Workload Factory 建立的資源）
- 秘密 ARN 範圍（Secrets Manager 存取受限於 `FSxSecret*`）
- 執行階段權限驗證（回報缺少的行動/資源以進行針對性修復）

權限文件

Workload Factory 權限的主要參考資料是 Workload Factory 設定和管理文件中的 "權限參考"。您可以在此參考資料中找到有關從儲存設備 IAM 原則中移除權限之影響的資訊。

Amazon CloudWatch 針對 NetApp Workload Factory 的監控權限

Amazon CloudWatch 監控權限在 NetApp Workload Factory 中是選用的，且僅在您部署分隔的監控堆疊時才適用。監控堆疊透過收集檔案系統計量、發佈事件記錄、管理 CloudWatch 儀表板和警示，以及透過 Amazon SNS 發送警示通知，來提供營運可見度。該堆疊還需要存取權限，以便在監控需要時擷取 ONTAP 認證資料。

所需的 CloudWatch 監控權限

可選的監控堆疊需要以下權限：

權限	目的
fsx:Describe* / fsx:ListTagsForResource	收集檔案系統計量
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	管理儀表板和警報
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	發布事件記錄
sns:Publish	發送提醒通知
secretsmanager:GetSecretValue	擷取用於監控的 ONTAP 認證資料

資料治理、隱私和生命週期

NetApp Workload Factory 的資料處理與駐留

NetApp Workload Factory 將資料處理組織成不同的類別，這些類別描述了服務處理的運行資料、每類資料在安全性模型中的定位、資料儲存位置、保留期限以及是否會離開客戶環境。主要資料類別包括組態和中繼資料、運行日誌和事件以及遙測資料。保留的資料可能包括 FSx for ONTAP 組態快照、認證資料引用、AI 使用情況和成本資料、稽核記錄以及短期回應快取。儲存和處理位置因資料類型而異：某些資訊保留在客戶的 AWS 帳戶中，而其他運行資料則儲存在 NetApp 帳戶中。

Workload Factory 處理的資料類別

Workload Factory 處理下列資料類別：

- 組態和中繼資料
- 操作日誌和事件
- 遙測

Workload Factory 保留的資料類別

Workload Factory 儲存以下資料：

- FSx 組態快照（每次掃描時刷新）
- ONTAP 認證資料參照，或使用 KMS 信封加密所加密的認證資料素材（取決於所選的認證資料模式）
- EDA 計量
- CloudFormation 範本（7 天 `Expires`標頭）
- AI 使用和成本資料
- 稽核記錄
- Redis 快取（FSx 回應），TTL 為 20 分鐘

資訊保存位置

AWS 帳戶

- ONTAP 管理員密碼儲存在您的 AWS Secrets Manager 中。
- Amazon Bedrock 透過您 AWS 帳戶中 STS 承擔的角色，使用您的推理設定檔 ARN 處理 AI 推理（EMS 分析）。

NetApp 帳戶

- FSx 組態、平衡計畫、ARP 組態和 AI 使用限制
- 臨時 AWS STS 認證資料（快取在 Redis 中）、回應快取、鎖定和部署狀態

- CloudFormation/Terraform 範本、WAD 組態描述元和壓縮報告
- AI 使用計量和收集器效能計量
- EDA 彙總計量
- 操作稽核追蹤
- OpenTelemetry 追蹤

區域考量

- 存放在 Amazon Bedrock 服務可用的地區。
- NetApp 內部在 `us-east-1`和 `us-west-2`中運作。

資訊保留時長

本節概述保留類別。有關詳細數值和原則行為，請參閱相關連結頁面。

- 認證資料和臨時 AWS STS 認證資料保留："NetApp Workload Factory 的認證資料保留"
- 營運計量和遙測保留："NetApp Workload Factory 的計量與遙測參考"
- 稽核記錄保留：受 NetApp Console 保留政策約束（不受 Workload Factory 控制）

哪些資訊會離開虛擬私人網路（**VPC**）

本節概述傳出資料類別。如需通訊協定層級與功能層級的詳細資訊，請參閱連結頁面。

至 **Workload Factory** 服務的管理平面流量

對於管理操作，FSx 組態、Volume 中繼資料、資源識別碼和操作指令會透過 HTTPS 流向 Workload Factory 服務分層。

稽核記錄至 **NetApp Console** 稽核服務

每個追蹤的作業都會傳送下列資訊：

- `accountId`
- `actionName`
- `status`
- `resourceId`
- `userId`
- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

AI 分析流量

提交給 AI 診斷的 FSx for ONTAP 緊急管理系統 (EMS) 事件、延遲資料與錯誤日誌，會透過您的 AWS 帳戶使用您設定的推論設定檔傳輸至 Amazon Bedrock，因此此流量會保留在您的環境中，而不會到達 NetApp 系統。

如需有關 AI 分析流量的詳細資訊，請參閱：

- "NetApp Workload Factory 的 AI 控制總覽"
- "Bedrock 選擇加入 NetApp Workload Factory AI 診斷"
- "NetApp Workload Factory 的人工智慧工具邊界"

AWS 服務 **API** 流量

請參閱"NetApp Workload Factory 的連結性和信任路徑"。

遙測和計量收集

請參閱 "計量和遙測參考"。

組態和中繼資料收集範圍

檔案系統層級

- 檔案系統組態（部署類型 Gen1/Gen2、處理量容量、儲存容量、儲存設備類型）
- 首選子網路、安全性群組、VPC 組態
- KMS 加密金鑰中繼資料
- 檔案系統標籤
- 檔案系統生命週期狀態
- 維護時段設定

Volume 層級（綜合）

- 識別與狀態：Volume 名稱、UUID、類型（rw/dp/ls）、樣式（FlexVol/FlexGroup）、狀態（線上/離線/受限）、建立時間
- 容量：總容量、已使用容量、可用容量、實體已使用容量、已使用百分比、SSD 實體佔用空間、容量資源池實體佔用空間、非活動資料位元組數/百分比
- 分級：原則（all/auto/none/snapshot_only），最短冷卻天數
- QoS：已指派的 QoS 原則名稱
- NAS 組態：交會路徑、匯出原則指派、UNIX 權限、安全樣式（unix/ntfs/混合）
- Snapshot 快照技術：Snapshot 快照技術保留大小/百分比/已用量，自動刪除設定
- 資料效率：壓縮類型/狀態、重複資料刪除、資料精簡、空間節約效益
- 自動調整大小：模式（grow/grow_shrink/off）、最小/最大大小、增大/縮小臨界值
- SnapLock：類型（法規遵循/企業/non_snaplock），保留期間（最短/最長/預設），自動提交期間

- 複製：父 Volume/Snapshot 快照技術/儲存設備 VM，是 FlexClone，分割狀態
- Inodes/檔案：最大可能數量、最大配置數量、已用數量
- 加密：已啟用/已停用狀態
- 存取時間：atime 更新已啟用/已停用和更新週期
- SnapMirror：保護狀態、目的地類型（雲端 / ONTAP）
- FlexGroup 再平衡：失衡百分比，最大臨界值
- Volume 移動：目的地 Aggregate，移動狀態
- FlexCache 端點類型：無/快取/來源
- 標籤：ONTAP 層級 Volume 標籤

Snapshot 快照技術資料

- Snapshot 快照技術名稱、UUID、建立時間、過期時間
- 大小（位元組）
- SnapMirror 標籤
- SnapLock 到期和鎖定狀態
- 狀態（有效/無效/部分有效）
- 使用者評論
- Snapshot 快照技術原則：名稱、啟用狀態、排程複本（數量、保留期間、排程名稱、前綴、SnapMirror 標籤）

匯出原則

- 原則名稱、ID、關聯的儲存設備 VM
- 規則：協定清單（NFS/CIFS/FlexCache）、用戶端比對模式、唯讀規則、讀寫規則、超級使用者規則、規則索引/優先權
- SUID、裝置建立、chown 模式、匿名使用者對映、NTFS UNIX 安全性設定

S3 存取點

- 生命週期狀態（可用/建立中/刪除中/失敗/配置錯誤）
- 建立時間、ARN、別名、名稱
- 檔案所有者使用者和類型（UNIX/WINDOWS）
- 網路組態（網際網路存取與 VPC 存取、VPC ID）
- AWS 標籤
- 中繼資料掃描能力開發、日誌記錄能力開發、CloudTrail ARN

反勒索軟體保護（**ARP**）

Workload Factory 會收集組態狀態和事件詳細資訊：

- 每個 Volume 的狀態（啟用/停用/試運行/暫停）
- 攻擊機率（無/低/中/高）
- 帶有時間戳記的攻擊報告
- 偵測參數：檔案副檔名臨界值、重新命名率激增百分比、熵率激增百分比、檔案建立/刪除率激增百分比
- 可疑檔案：檔案路徑、檔案名稱、檔案格式、可疑時間、關聯 Volume

複寫 **/ SnapMirror**

- 關係 UUID、狀態、健康狀態
- 來源和目的地（儲存設備虛擬機器、路徑、叢集）
- 傳輸統計資料（傳輸位元組數、持續時間、結束時間、狀態）
- 原則（名稱，類型：非同步/同步/連續）
- 節流設定
- 滯後時間
- 不健康的原因（訊息和代碼）
- 目前傳輸錯誤

iGroups

- 名稱、UUID、協定（FCP/iSCSI/混合）、作業系統類型
- 啟動器（IQN/WWPN）、連線狀態、最後出現時間
- LUN 對應（邏輯單元編號，LUN 詳細資料）

LUN

- 名稱、UUID、序號、作業系統類型、啟用狀態
- 大小、已使用空間、資源隨需配置設定
- 位置（Volume、節點、邏輯單元路徑）
- 自動刪除設定
- 容器狀態、映射狀態、唯讀狀態
- QoS 原則
- 效能計量（IOPS、延遲、每次讀寫/總處理量）
- 一致性群組成員資格

FlexCache

- 來源 Volume/儲存設備虛擬機器/叢集、快取大小、路徑
- 已啟用回寫功能，DR 快取狀態
- 相對規模組態
- 預先填入目錄路徑

- 快取與來源之間的連線狀態

儲存虛擬機器層級

- 名稱、UUID、狀態（執行中/停止）、子類型
- 已啟用/允許的協定（NFS、CIFS、iSCSI、FCP、NVMe、S3）
- DNS 伺服器和網域
- 名稱服務交換器組態（passwd、group、hosts 等）
- IP 介面（名稱、IP 位址、服務）
- 已指派的 Aggregate
- 反勒索軟體預設 Volume 狀態
- 空間強制執行設定
- 對等關係（應用程式、狀態、遠端叢集/儲存設備虛擬機器）

Aggregate / 儲存設備層級

- Aggregate 名稱、UUID、狀態、RAID 狀態
- 區塊儲存設備：磁碟數量、RAID 大小、可用/已使用/總空間、實體已使用
- 已使用的雲端儲存設備
- 效率：比率、邏輯已用、節省
- 加密、鏡射、SnapLock 設定
- 效能計量（IOPS、延遲、處理量）

利用率計量（**EDA**）

- 資料擷取頻率：容量/處理量每 12 小時擷取一次；延遲每 20 分鐘擷取一次
- 粒度：每個時間範圍內標準化至約 60 個資料點
- 保留和儲存設備詳情："計量與遙測參考"

NetApp Workload Factory 的加密與金鑰管理

NetApp Workload Factory 使用靜態加密，並在 Workload Factory 和 AWS 服務之間明確定義了金鑰管理職責。對於 Amazon FSx for NetApp ONTAP 檔案系統，您可以選擇自己的 AWS KMS 金鑰，也可以使用 AWS 代管的預設金鑰，而 FSx for ONTAP 會使用該金鑰執行加密作業。Workload Factory 也使用信封加密來保護儲存的 ONTAP 認證資料。

FSx 的 KMS 靜態加密範圍

透過 Workload Factory 建立 FSx for ONTAP 檔案系統時，您可以選擇指定自己的 AWS KMS 金鑰用於靜態資料加密。如果您未指定金鑰，Workload Factory 將使用 AWS 代管的預設 FSx 金鑰。

加密的內容

所有儲存在支援 FSx for ONTAP 檔案系統的底層 EBS 磁碟區上的資料（AWS FSx 靜態加密）。

金鑰所有權

KMS 金鑰位於您的 AWS 帳戶中。

選擇和使用金鑰所需的權限

Workload Factory 需要：

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant`（允許 FSx for ONTAP 服務使用該金鑰）

金鑰存取模式

Workload Factory 從不直接使用您的 KMS 金鑰加密或解密資料。它會在檔案系統建立期間將金鑰 ID 傳遞給 Amazon FSx for NetApp ONTAP API；Amazon FSx for NetApp ONTAP 會執行加密作業。

認證資料保護（服務端信封加密）

當您透過 Workload Factory 儲存 ONTAP 認證資料（管理員密碼）時，它會在持久化之前使用信封加密來保護它們。

加密方法

使用唯一的資料加密金鑰（DEK）對每個認證資料記錄進行 AES-256-CBC 加密。

信封加密流程

1. 每個認證資料都會產生一個唯一的 256 位元 DEK。
2. DEK 對認證資料（密碼）進行加密。
3. DEK 本身使用根目錄金鑰進行加密，並與加密認證資料一起儲存。
4. 明文 DEK 永遠不會儲存。

加密內容

每個資料金鑰都透過加密方式與其特定的認證資料記錄綁定，防止金鑰在不同記錄之間重複使用。

替代方案：**AWS Secrets Manager**

您無需將加密密碼儲存在服務中，而是可以將 ONTAP 認證資料儲存在您自己帳戶的 AWS Secrets Manager 中。Workload Factory 從不檢視或儲存密碼；它會將 Secrets Manager ARN 傳遞給 Lambda 連結，該連結會在執行階段於您的 VPC 內擷取密碼。

GovCloud 帳戶需要 AWS Secrets Manager。

NetApp Workload Factory 帳戶刪除

帳戶刪除並非自助服務操作；這是一個退出工作流程，涉及 Workload Factory 服務和您

AWS 帳戶中的資源。清理過程包括安全地移除與 Workload Factory 帳戶、FSx for ONTAP 檔案系統、憑證、連結、通知通道，以及相關的 IAM、AWS Lambda 和 Amazon CloudWatch 資源相關聯的任何資料。此操作不可逆。

當您需要移除 Workload Factory 帳戶時，您必須"聯絡 NetApp 支援。"

可觀測性（日誌、計量、遙測）

了解 NetApp Workload Factory 中的可觀測性

可觀測性訊號有助於支援運行監控、疑難排解和調查。在 NetApp Workload Factory 中，可觀測性包括計量、遙測資料和運行記錄，這些指標和記錄能夠提供對服務行為、AI 使用情況以及透過 Workload Factory 執行的操作的可見度。遙測資料和運行記錄支援內部監控和客戶導向的稽核可見度，而 Tracker 則可協助您審查支援操作的進度、狀態和詳細資訊。

遙測與運作記錄

Workload Factory 使用下列遙測和作業記錄類型：

- OpenTelemetry 追蹤透過 OTLP HTTP 匯出至 SigNoz（內部可觀測性）
- AI 使用情況計量（權杖計數、模型成本）儲存在 AWS Timestream 中
- NetApp Console 稽核記錄（行動名稱、狀態、請求/回應中繼資料、時間戳記）

Workload Factory 中的稽核記錄

Workload Factory 提供 Tracker 監控功能，方便您監控正在執行的作業及其執行時間。透過 Tracker，您可以追蹤 FSx for ONTAP、認證資料和連結作業的進度和狀態，審查作業任務和子任務的詳細資料，並診斷任何問題或故障。

Tracker 提供多種操作。您可以按時間範圍（過去 24 小時、7 天、14 天或 30 天）、工作負載、狀態和使用者篩選工作；使用搜尋功能尋找工作；並將工作表下載為 CSV 檔案。

- "使用 Workload Factory 中的 Tracker 監控作業"

相關資訊

- "NetApp Workload Factory 的計量與遙測"

NetApp Workload Factory 的計量與遙測

NetApp Workload Factory 會在 AWS CloudWatch 中收集並儲存 Volume 級和檔案系統級計量，讓您對儲存效能和容量具有營運可見度。計算出的計量（例如處理量）是從這些收集的值衍生而來。了解計量定義、收集頻率、重新整理行為和保留詳細資訊。

包含的計量

NetApp Workload Factory 針對操作日誌和事件使用這些計量：

- Volume 層級 CloudWatch 計量（每個 Volume 收集）
- 檔案系統層級 CloudWatch 計量（按檔案系統收集）

- 計算計量
- 收集排程與保留

關於營運計量

計算計量使用以下公式：

- 處理量（位元組/秒）=（NetworkSentBytes + NetworkReceivedBytes）/ 週期

重新整理行為：

- Volume 和叢集計量每 12 小時重新整理一次。
- 延遲計量每 20 分鐘重新整理一次。
- DynamoDB 項目會在 14 天後自動過期。

關於遙測資料收集

- OpenTelemetry 追蹤透過 OTLP HTTP 匯出至 SigNoz（內部可觀測性）
- AI 使用情況計量（權杖計數、模型成本）儲存在 AWS Timestream 中
- NetApp Console 稽核記錄（行動名稱、狀態、請求/回應中繼資料、時間戳記）

Volume 層級 CloudWatch 計量（每個 Volume 收集）

指標	AWS CloudWatch 名稱	單元	它測量的內容
Volume 儲存容量	StorageCapacity	位元組	總配置容量
已使用的儲存設備	StorageUsed	位元組	實際儲存的資料
資料讀取位元組	DataReadBytes	位元組	讀取處理量
資料寫入位元組	DataWriteBytes	位元組	寫入處理量
資料讀取作業	DataReadOperations	計數	讀取 IOPS
資料寫入作業	DataWriteOperations	計數	寫入 IOPS
元資料操作	MetadataOperations	計數	中繼資料 IOPS
資料讀取作業時間	DataReadOperationTime	秒	讀取延遲
資料寫入作業時間	DataWriteOperationTime	秒	寫入延遲
中繼資料作業時間	MetadataOperationTime	秒	中繼資料延遲

檔案系統層級 CloudWatch 計量

指標	AWS CloudWatch 名稱	單元	它測量的內容
SSD 儲存容量	StorageCapacity	位元組	總 SSD 分層容量
已使用的 SSD 儲存設備	StorageUsed（SSD 分層）	位元組	SSD 分層消耗

指標	**AWS CloudWatch** 名稱	單元	它測量的內容
已使用的容量資源池	StorageUsed（容量資源池）	位元組	容量資源池消耗
CPU 使用率	CPU 使用率	百分比	檔案伺服器 CPU
SSD 容量使用率	StorageCapacityUtilization	百分比	SSD 分層使用率
網路處理量使用率	NetworkThroughputUtilization	百分比	網路使用率百分比
磁碟 IOPS 使用率	DiskIopsUtilization	百分比	磁碟 IOPS 使用率百分比
磁碟處理量使用率	FileServerDiskThroughputUtilization	百分比	磁碟處理量已使用百分比
磁碟 IOPS 使用率（伺服器）	FileServerDiskIopsUtilization	百分比	伺服器磁碟 IOPS 利用率
儲存設備效率節省	StorageEfficiencySavings	位元組	效率節省的空間
網路接收	NetworkReceivedBytes	位元組	傳入網路
網路傳送	NetworkSentBytes	位元組	傳出網路

收集排程與保留

時間範圍	收集期間	資料點	儲存	保留
1 天	24 分鐘	約 60	DynamoDB	14 天（TTL）
1 週	約 2.8 小時	約 60	DynamoDB	14 天（TTL）
1 個月	12 小時	約 60	DynamoDB	14 天（TTL）
3 個月	約 1.5 天	約 60	DynamoDB	14 天（TTL）
1 年	約 6 天	約 60	DynamoDB	14 天（TTL）

生成式 AI 安全性控制

了解 NetApp Workload Factory 中的 AI 控制

NetApp Workload Factory 包含生成式 AI 功能，可加快診斷速度，同時對模型存取、資料範圍和執行時間行為實施安全性控制。

Workload Factory 預設啟用 AI 診斷。您可以隨時透過 Workload Factory **Administration** 設定停用生成式 AI 功能。"了解更多關於管理 GenAI 功能的資訊。"

安全性範圍 AI 功能總覽

Workload Factory 目前將生成式 AI 套用至以下功能：

- Ask Me 助手（RAG，包含精選 NetApp 文件和有來源支援的回應）
- 延遲分析
- EMS 事件分析
- 錯誤日誌分析

適用於 AI 診斷的 AWS Bedrock 總覽

Workload Factory 使用 Amazon Bedrock 進行 AI 推論。推論在您的 AWS 帳戶中執行，使用您設定的憑證和推論設定檔。

相關資訊

- "Amazon 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 AI 模型參數與計費"

Amazon Bedrock 選擇加入 NetApp Workload Factory AI 診斷

NetApp Workload Factory AI 診斷使用 Amazon Bedrock 分析事件，此功能預設為啟用。在 Workload Factory 呼叫選定的 Bedrock 模型並收集診斷資料之前，您必須設定 IAM 權限、推論設定檔以及具有 SSH 功能的 Lambda 連結。如果缺少任何元件或 Bedrock 組態已移除，AI 診斷將無法使用。

AI 診斷功能預設為啟用。

開始之前

- 請確保您的帳戶包含 AWS Bedrock 推論設定檔。
- 擁有具備 SSH 功能的已連線 Lambda 連結，以進行診斷資料收集。

步驟

1. 在您的 IAM 角色中授予 Bedrock 權限：
   - `bedrock:InvokeModel`
   - `bedrock:InvokeModelWithResponseStream`
   - `bedrock:ListInferenceProfiles`
   - `bedrock:GetInferenceProfile`
2. 在 Workload Factory 設定中設定推論設定檔 ARN。

如果缺少任何先決條件，系統會報告特定缺少的元件，且 AI 功能將保持非作用中狀態。

停用 **AI** 診斷

若要停用 AI 診斷：

- 從您的 IAM 角色中移除 Bedrock 權限，或者
- 在 Workload Factory 設定中刪除 Bedrock 組態。

AI 診斷立即無法使用，且不會進行任何剩餘資料處理。

區域和跨區域推論設定檔

Bedrock 推理會在您推理設定檔指定的 AWS 區域中執行。如果您使用跨區域推理設定檔，根據 AWS Bedrock 的標準行為，AWS 可能會將請求路由到設定檔組態中的任何區域。資料不會離開 AWS 基礎架構。

NetApp Workload Factory 的人工智慧工具邊界

NetApp Workload Factory 對其 AI 功能與您的 AWS 和 ONTAP 環境互動的方式實施嚴格的界線，因此您可以信賴 AI 輔助診斷，而不會有意外變更的風險。Amazon Bedrock 使用唯讀的 AWS CLI 和 ONTAP CLI 診斷工具，這些工具會區塊修改命令並依大小和執行限制輸出，且所使用的任何資料僅為暫時性，不會由 NetApp Workload Factory 或 AWS 保留。

工具安全控制

工具	功能	安全控制
AWS CLI（唯讀）	執行唯讀的 AWS CLI 指令（describe、list、get）	阻止所有修改動詞（建立、刪除、修改、更新、放置、移除）。每步最多 10 個命令。輸出大小截斷至 20 KB。
ONTAP CLI（唯讀）	使用 SSH 執行唯讀 ONTAP CLI 指令	封鎖所有變動動詞（刪除、毀損、建立、修改、移動）。輸出已截斷。

代理程式無法修改、建立或刪除資源。它只能觀察和診斷。

資料保留和模型訓練邊界

根據 AWS 原則，Amazon Bedrock 不會儲存或使用您的輸入和輸出來訓練或改進基礎模型。對於隨需推論（由 Workload Factory 使用），AWS 會暫時處理您的資料，並在回傳回應後不予保留。

NetApp Workload Factory 的 AI 模型參數與計費

NetApp Workload Factory 定義了與 AI 治理相關的模型組態、使用情況和計費邊界。設定的模型使用確定性參數並傳回結構化 JSON，以支援一致的分析結果。AWS 會將 Amazon Bedrock 推理費用計入您的帳戶，而 Workload Factory 則會追蹤 AI 使用情況並提供每個帳戶的每月成本可見度。這些小節說明了模型參數以及適用於 AI 消耗的限制。

模型和參數

參數	價值
模型	Anthropic Claude（使用跨區域推論設定檔）
溫度	0（確定性，無隨機性）
最大輸出 Token	2,048
最大推理步驟	每次分析 15
輸出格式	結構化 JSON（總結、嚴重程度、根目錄原因、糾正措施）

計費和使用限制

- AWS 會將 Bedrock 推論費用計入您的帳戶（您的推論設定檔、您的憑證）。
- Workload Factory 會在內部追蹤 AI 使用情況。
- Workload Factory 提供每個帳戶的每月成本可見度。

  "在 NetApp Workload Factory 中追蹤儲存設備成本"

Ask Me AI 助理

NetApp Workload Factory 的 Ask Me 安全性架構

Ask Me 是內建於 NetApp Workload Factory 的生成式 AI 助手。它為 Amazon FSx for NetApp ONTAP 和 Workload Factory 主題提供即時的對話式支援。回應均基於經過驗證的 NetApp 文件，且 Ask Me 無法存取公共網際網路或使用客戶資料來訓練模型。多層安全性機制有助於區塊惡意查詢，將回應限制在支援的網域內，並防止使用者輸入覆寫系統指令。當 Ask Me 使用工具時，授權邊界、唯讀查詢強制執行、臨時沙箱和稽核記錄有助於約束和監控執行。

您可以隨時透過 Workload Factory 管理 設定選擇退出 Ask Me，這將停用您使用者帳戶的助理。"了解更多關於管理 GenAI 功能的資訊。"

Ask Me 中的 **RAG** 架構

Ask Me 使用擷取增強生成（RAG）。

- 精心整理的知識庫：回覆基於經過驗證、已發佈的 NetApp 文件所組成的代管語料庫。
- 擷取評分與篩選：模型上下文中僅包含足夠相關的內容。
- 沒有網路存取：此模型無法取得、瀏覽或抓取外部內容。
- 來源標註：回覆包含所用來源文件的引用。

多層提示安全性

- 第 1 層：安全性分類器（LLM 作為評判者）封鎖惡意查詢（提示注入、權限提報、資料外洩、社交工程、原則違規）。

  系統會記錄被封鎖的查詢，生成式模型永遠不會看到它們。

- 第 2 層：系統提示強化可防止使用者輸入覆寫系統指令。
- 第 3 層：網域範圍限制對 FSx ONTAP 和 Workload Factory 主題的回應。
- 第 4 層：工具使用治理在加固的沙箱中驗證參數並執行查詢；此模型不能執行任意操作。

模型資料隔離和隱私

- 沒有使用客戶資料進行模型訓練
- 要求層級隔離（無跨租戶資料外洩）
- 工作階段範圍的對話上下文，具有有限的歷史記錄
- 無持久模型記憶體容量
- 代管推論基礎架構

工具使用和代理安全性

- 授權範圍工具（強制執行使用者權限邊界）
- 嚴格的工具執行逾時
- 用於擷取資料的臨時性、工作階段範圍沙箱
- 使用允許清單強制執行唯讀查詢
- 工具呼叫稽核及敏感參數清理

NetApp Workload Factory 的 Ask Me 存取控制

在 NetApp Workload Factory 中，Ask Me 存取安全性的核心在於經過驗證的工作階段、使用者層級的責任歸屬，以及在執行階段作業期間受保護的機密處理。驗證控制會驗證每個工作階段，並將互動與特定使用者建立關聯。敏感憑證會在執行階段從代管的機密保存庫中擷取，並從記錄中刪除。該服務也套用基礎架構控制，包括非根目錄 Container 執行和受限的 CORS 允許清單。

驗證

- 使用加密驗證進行簽署 JWT 驗證（包括對象、發行者和演算法檢查，例如 RS256）
- 服務邊界處的中介軟體強制驗證
- 使用者身分範圍限定，以便將互動歸因於特定使用者

憑證保護和機密處理

- 安全保存庫儲存設備：服務使用的敏感憑證儲存在代管的機密保存庫中，並在執行階段擷取。應用程式程式碼、組態檔案或 Container 映像檔中均不儲存任何機密。
- 日誌清理：在寫入日誌之前，會將敏感值（認證、權杖、密碼、存取金鑰、憑證）從日誌中遮蔽。

基礎架構安全性

- 非根目錄 Container 執行
- CORS 僅限於受信任 NetApp 網域的明確允許清單

NetApp Workload Factory 的 Ask Me 執行模式

NetApp Workload Factory 為 Ask Me 提供多種執行模式，每種模式都有不同的安全性和隱私特性。當 Ask Me 使用工具整合時（例如查詢客戶本身的 Workload Factory 資源），工具的執行會透過分層防護來控制。啟用工具的執行會在經過驗證的使用者權限範圍內運作，並對每次操作的持續時間和範圍套用限制。擷取到的資料會保留在短暫的工作階段沙箱中，該沙箱會封鎖外部存取，並在工作階段結束時毀損。獨立的提示與程式碼控制會強制執行唯讀查詢，而稽核記錄會擷取工具活動，並清除敏感值。

工具執行安全措施

- 授權範圍工具在已驗證使用者的權限範圍內運作。
- 工具執行逾時限制了長時間運行的操作。
- 臨時資料沙箱將工具檢索的資料儲存在工作階段範圍內，阻止外部存取、檔案 I/O、網路呼叫和引擎層級的擴充載入，並在工作階段結束時毀損。
- 唯讀查詢強制執行透過嚴格的允許清單來驗證產生的查詢。
- 提示強制執行與程式碼強制執行的安全性會獨立套用。
- 工具呼叫稽核會記錄工具名稱、參數、時間戳記和結果狀態，並進行敏感值清理。

輸出控制

- Token 限制執行
- 用於分類/安全性關鍵操作的確定性輸出（溫度 0）
- 具有提前終止與清理的串流

NetApp Workload Factory 的 Ask Me 隱私權與可用度

在 NetApp Workload Factory 中，Ask Me 隱私控制可限制資料暴露，讓工作階段處理保持隔離的，並維護使用者互動的隱私邊界。您的輸入由代管 AI 服務處理，該服務不會使用這些資料來訓練或改進基礎模型。擷取到的操作資料在工作階段期間保留在短暫的記憶體儲存設備中，不會持久化或是共享的。跨多個雲端區域的多模型後援鏈可在主要模型受限或無法使用時支援可用度，同時相同的安全性控制適用於所有後援模型。

資料處理和隱私

- 提示中的使用者資料：由代管 AI 服務處理，該服務不會使用您的輸入來訓練或改進基礎模型。
- 知識庫內容：僅包含精選、已發佈的 NetApp 文件；不包含您的資料。
- 操作資料：僅當使用者查詢自己的資源時才會擷取；在工作階段期間保存在短暫的記憶體容量儲存設備中，不會持續保留或共享的。
- 稽核記錄：已記錄查詢中繼資料（匿名使用者 ID、時間戳記、持續時間），並清理敏感欄位。
- 回饋資料：單獨儲存並與查詢 ID 關聯，不與匿名使用者 ID 以外的個人識別資訊關聯。

可用性和隔離控制

Ask Me 採用跨多個雲端區域的多模型回退鏈。

如果主模型受到限制或無法使用，系統可以容錯移轉至替代模型。

所有模型均受到相同的安全性控制、系統提示強化與隔離保證所規範。

ONTAP 操作和 Lambda 連結（客戶 VPC 元件）

了解 NetApp Workload Factory 的 Lambda 連結

NetApp Workload Factory 使用 *link*（部署在您 VPC 中的 AWS Lambda 函數），在 Amazon FSx for NetApp ONTAP API 未公開這些操作時，將 ONTAP 原生操作保留在您的 AWS 帳戶邊界內。該連結在您的子網路和安全性群組中執行，因此執行元件會保留在您的 AWS 環境中。Workload Factory 僅針對需要直接 ONTAP 存取而非可用 AWS 服務 API 的操作呼叫該連結。它會將連結的架構與 NetApp Console 代理程式的安全性和操作設定檔進行比較。

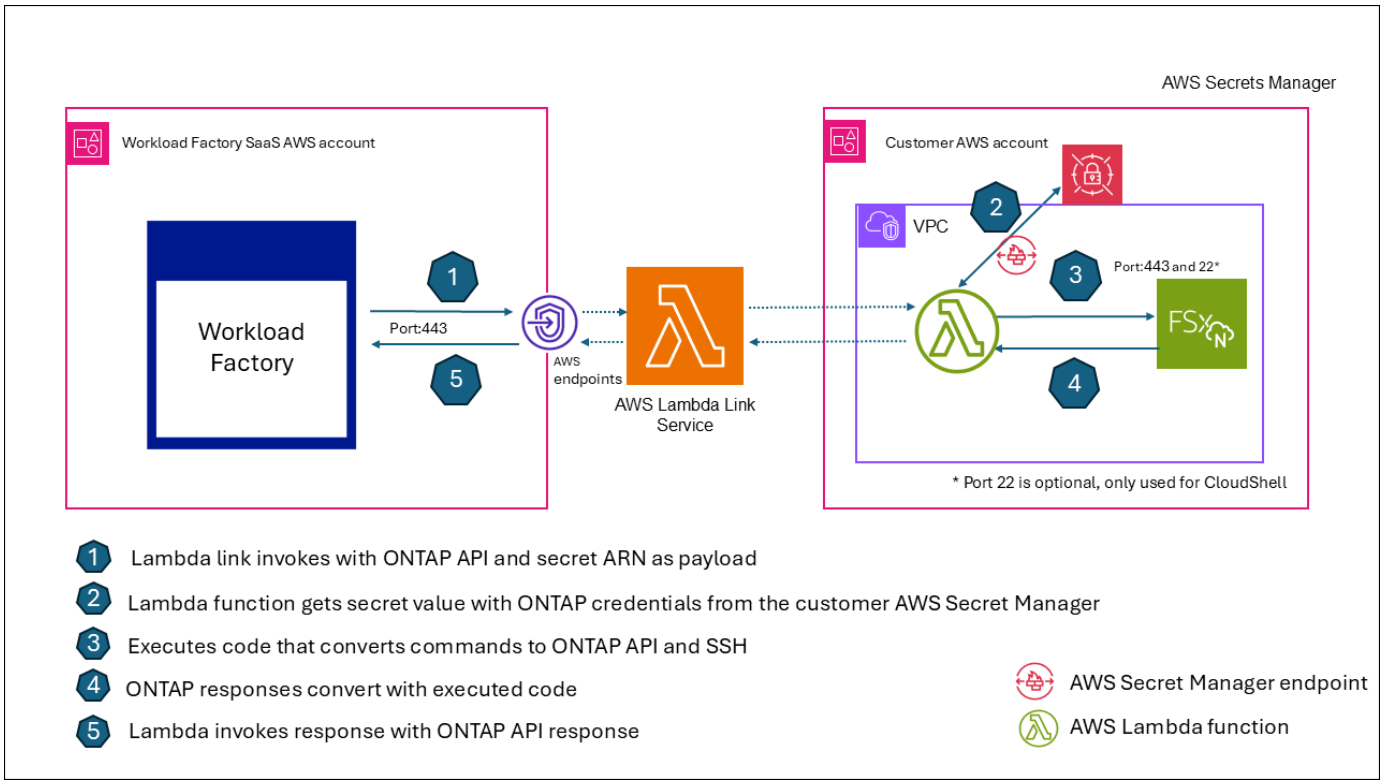
連結安全性架構

Workload Factory 連結在 Workload Factory 帳戶和一個或多個 FSx for ONTAP 檔案系統之間建立信任關係和間接連線。

下表提供 Lambda 連結安全性架構的總覽。使用此資訊來了解 Lambda 函數如何在您的 AWS 帳戶中部署和執行，包括其連網組態、執行環境和操作限制。

屬性	詳細資料
運算	AWS Lambda（Container 映像）
執行階段	Node.js 22
部署	您 AWS 帳戶中的 CloudFormation 堆疊
VPC 放置	您的子網路，您的安全性群組
逾時	每次調用 10 秒
呼叫	同步（RequestResponse）
套件類型	Container 映像（取自 NetApp ECR）

下圖顯示 Lambda 連結的安全性架構。



Lambda 連結與 NetApp Console 代理程式

Lambda 連結和 NetApp Console 代理程式用途不同，安全性和操作影響也不同。

維度	連結（基於 **Lambda**）	**NetApp Console** 代理程式（基於虛擬機器/**Pods**）
執行階段模型	無伺服器（AWS Lambda），客戶部署	客戶部署的虛擬機器/Container；執行 NetApp 控制台服務 pod
主要範圍	控制平面 ONTAP REST 操作（僅當 AWS API 不支援此操作時）	編排以及對資料服務的支援
資料服務支援	不代管資料服務	可作為資料服務主機（執行 NetApp 主控台服務 Pod）
營運例行成本	沒有全年無休的 VM	虛擬機器生命週期管理與升級

相關資訊

如需完整的跨系統連線圖，請參閱"NetApp Workload Factory 的連線能力與信任路徑"。

NetApp Workload Factory 的 Lambda 連結埠和呼叫

NetApp Workload Factory 使用 Lambda 連結請求和連接埠邊界來定義所需的傳出連線和 IAM 授權呼叫。此連結支援對 ONTAP 管理端點的 HTTPS 請求、用於診斷的唯讀 SSH 命令，以及健全狀況檢查。所有連線均從您的 VPC 內的連結傳出，因此不需要傳入連線或暴露的端點。Workload Factory 透過基於 IAM 的授權，經由 AWS Lambda API 呼叫該連結。

請求類型

- HTTPS（ONTAP REST API）：將 HTTPS 呼叫代理至 ONTAP 管理端點（連接埠 443），以進行 Volume、儲存設備 VM 和叢集操作。
- SSH（ONTAP CLI）：在連接埠 22 上執行唯讀 ONTAP CLI 命令，以取得診斷和效能資料。
- 健全狀況檢查：傳回狀態和支援的功能。

傳出網路邊界

方向	連接埠	目的地	目的
傳出	443	ONTAP 管理 IP（在您的 VPC 內）	REST API 操作
傳出	22	ONTAP 管理 IP（在您的 VPC 內）	SSH CLI 命令
傳出	443	AWS Secrets Manager 端點（選用）	使用 Secrets Manager 時擷取憑證

不需要傳入連線。該連結不會暴露任何端點。Workload Factory 使用 AWS `lambda:InvokeFunction` API 呼叫它。

Workload Factory 呼叫 Lambda 連結

Workload Factory 透過 AWS Lambda API (`lambda:InvokeFunction`）呼叫 Lambda 連結，使用基於 IAM 的授權。

呼叫有效負載包含：

- 目標 ONTAP 管理端點（IP/主機名稱）
- 要執行的操作（REST API 路徑或 SSH 命令）
- 驗證資訊（即時憑證或 Secrets Manager ARN 引用）

相關資訊

如需完整的跨系統連線圖，請參閱 "NetApp Workload Factory 的連結性和信任路徑"。

適用於 NetApp Workload Factory 的 Lambda 連結 IAM 權限

NetApp Workload Factory 使用 Lambda 連結權限邊界來定義 Lambda 執行和 Workload Factory 呼叫所需的 IAM 存取。這些權限是選用的，但對於 ONTAP 原生作業是必要的。設定 Secrets Manager 支援後，連結會在執行階段直接從您的 AWS Secrets Manager 取得 ONTAP 認證資料，且密碼僅在您的 VPC 內傳輸，從 Secrets Manager 到 Lambda 函數，然後再到 ONTAP 終端節點。

有關請求路徑和連接埠要求，請參閱"Lambda 連結埠和呼叫"。

Lambda 執行角色權限

在 VPC 中部署連結時，Lambda 執行角色需要以下權限：

權限	目的
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	標準 VPC 連接的 Lambda 連網
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP 管理
secretsmanager:GetSecretValue （作用域為 FSxSecret*）	擷取 ONTAP 認證資料（僅在啟用 Secrets Manager 時）
CloudWatch 日誌（代管原則）	Lambda 執行記錄

Workload Factory 呼叫權限

Lambda 連結資源型原則授予 Workload Factory 服務主體以下權限：

權限	目的
lambda:InvokeFunction	執行 Lambda
lambda:GetFunction	健全狀況與狀態檢查
lambda:UpdateFunctionCode	版本升級（映像更新）
lambda:GetFunctionConfiguration	設定驗證

NetApp Workload Factory 的 Lambda 連結生命週期

NetApp Workload Factory 使用 Lambda 連結生命週期控制來管理部署、健全狀況監控和受控映像更新，將維運風險降至最低。您可以使用 `lambda:UpdateFunctionCode`權限來更新 Lambda 連結 Container 映像，以部署改進或安全性修補程式，而無需重新部署 Amazon CloudFormation 堆疊。生命週期控制也定義如何監控連結健全狀況，以及在不再需要時如何移除 Lambda 連結及其關聯資源。

生命週期控制點

- 部署：透過 Amazon CloudFormation 或 Terraform 堆疊部署自動化
- 監控：健全狀況檢查偵測連線問題；故障計數器追蹤可靠性
- 移除：刪除 CloudFormation 堆疊會從您的 AWS 帳戶移除 Lambda 及相關資源

知識與支援

向 NetApp 支援註冊

在向 NetApp 技術支援開啟支援案例之前，您需要將 NetApp 支援網站帳戶新增至 Workload Factory，然後註冊以獲得支援。

必須註冊支援才能獲得專屬於 NetApp Workload Factory 及其儲存設備解決方案和服務的技術支援。您必須從 NetApp Console 註冊支援，這是一個與 Workload Factory 分隔的網路型主控台。

註冊支援並不會啟用雲端供應商檔案服務的 NetApp 支援。如需與雲端供應商檔案服務、其基礎架構或任何使用該服務的解決方案相關的技術支援，請參閱該產品 Workload Factory 文件中的「取得協助」。

"Amazon FSx for ONTAP"

支援註冊總覽

註冊您的帳戶 ID 支援訂閱（您的 20 位數 960xxxxxxxx 序號位於 NetApp Console 的「支援資源」頁面）即為您的單一支援訂閱 ID。每個 NetApp 帳戶層級的支援訂閱都必須註冊。

註冊後即可使用諸如開啟支援工單和自動產生案例等功能。註冊是透過將 NetApp 支援網站（NSS）帳戶新增至 NetApp Console 來完成，如下所述。

註冊您的帳戶以取得 **NetApp** 支援

若要註冊支援並啟動支援權限，您帳戶中的一位使用者必須將 NetApp 支援網站帳戶與其 NetApp Console 登入關聯。註冊 NetApp 支援的方式取決於您是否已擁有 NetApp 支援網站（NSS）帳戶。

已擁有 **NSS** 帳戶的現有客戶

如果您是擁有 NSS 帳戶的 NetApp 客戶，您只需透過 NetApp Console 註冊以獲得支援。

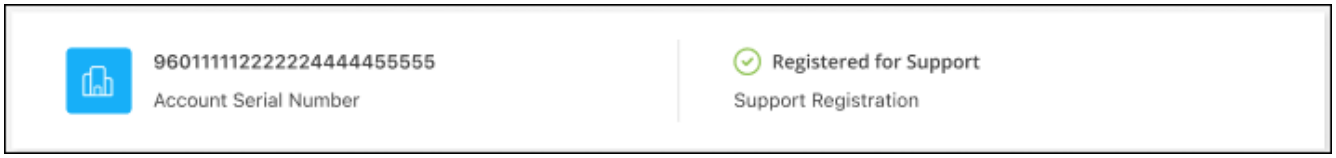
步驟

1. 在 Workload Factory 主控台的右上角，選取 說明 **>** 支援。

   選擇此選項會在新的瀏覽器索引標籤中開啟 NetApp Console，並載入支援儀表板。

2. 從 NetApp Console 選單中，選取 管理，然後選取 認證資料。
3. 選擇 **User Credentials**。
4. 選擇 新增 **NSS** 認證資料，然後按照 NetApp 支援網站（NSS）驗證提示進行操作。
5. 若要確認註冊程序是否成功，請選擇「說明」圖示，然後選擇 支援。

   「資源」頁面應顯示您的帳戶已註冊支援。



請注意，如果其他 NetApp Console 使用者尚未將 NetApp 支援網站帳戶與其 NetApp Console 登入建立關聯，他們將不會看到相同的支援註冊狀態。然而，這並不代表您的 NetApp 帳戶未註冊支援。只要帳戶中有一位使用者已依照這些步驟操作，您的帳戶即已註冊。

現有客戶但沒有 **NSS** 帳戶

如果您是現有 NetApp 客戶，擁有現有授權和序號，但沒有 NSS 帳戶，則需要建立 NSS 帳戶並將其與您的 NetApp Console 登入關聯。

步驟

1. 完成以下步驟即可建立 NetApp 支援網站帳戶 "NetApp 支援網站使用者註冊表"
   a. 請務必選擇適當的使用者層級，通常為 **NetApp** 客戶/終端使用者。
   b. 請務必複製上方使用的 NetApp 帳戶序號（960xxxx）至序號欄位。這將加快帳戶處理速度。
2. 請完成 已擁有 NSS 帳戶的現有客戶 下的步驟，將您的新 NSS 帳戶與您的 NetApp Console 登入關聯。

全新接觸 **NetApp**

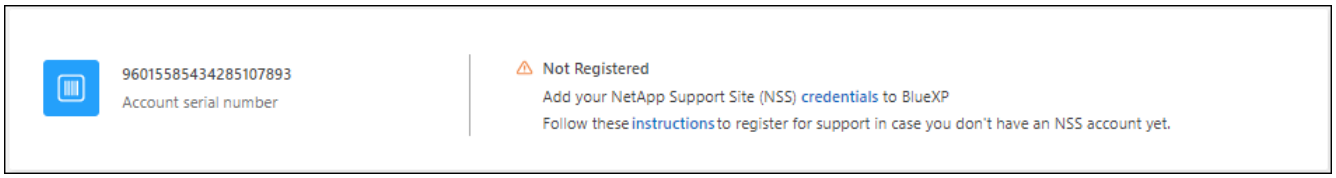
如果您是 NetApp 的全新使用者且還沒有 NSS 帳戶，請依照下列步驟操作。

步驟

1. 在 Workload Factory 主控台的右上角，選取 說明 **>** 支援。

   選擇此選項會在新的瀏覽器索引標籤中開啟 NetApp Console，並載入支援儀表板。

2. 請在支援資源頁面找到您的帳戶 ID 序號。



3. 導航至 "NetApp 的支援註冊網站" 並選取 我不是已註冊的 **NetApp** 客戶。
4. 請填寫必填項目（標有紅色星號的欄位）。
5. 在「產品線」欄位中，選擇「Cloud Manager」，然後選擇您適用的計費供應商。
6. 從上面的步驟 2 複製您的帳戶序號，完成安全性檢查，然後確認您已讀取 NetApp 的全球資料隱私政策。

   系統會立即傳送電子郵件至您提供的信箱，以完成此安全的交易。如果幾分鐘後您仍未收到驗證郵件，請務必檢查您的垃圾郵件資料夾。

7. 請在郵件中確認此行動。

   確認後，您的請求將提交至 NetApp，並建議您建立 NetApp 支援網站帳戶。

8. 完成以下步驟即可建立 NetApp 支援網站帳戶 "NetApp 支援網站使用者註冊表"
   a. 請務必選擇適當的使用者層級，通常為 **NetApp** 客戶/終端使用者。
   b. 請務必將上方使用的帳戶序號（960xxxx）複製到序號欄位。這將加快帳戶處理速度。

完成後

NetApp 將在此過程中與您聯繫。這是針對新使用者的一次性引導程序。

擁有 NetApp 支援網站帳戶後，請完成 已擁有 NSS 帳戶的現有客戶 下的步驟，將該帳戶與您的 NetApp Console 登入建立關聯。

取得適用於 NetApp Workload Factory 的 FSx for ONTAP 協助

NetApp 為 Workload Factory 及其雲端服務提供多種支援方式。提供 24x7 全天候的豐富免費自助支援選項，例如知識庫（KB）文章和社群論壇。您的支援註冊包含透過網路開立工單的遠端技術支援。

取得 FSx for ONTAP 的支援

如需與 FSx for ONTAP、其基礎架構或使用該服務的任何解決方案相關的技術支援，請參閱該產品的 Workload Factory 文件中的「取得協助」。

"Amazon FSx for ONTAP"

若要獲得針對 Workload Factory 及其儲存設備解決方案與服務的技術支援，請使用下列說明的支援選項。

使用自助選項

這些選項全天候 24 小時、每週 7 天免費提供：

- 文件

  您目前正在查看的 Workload Factory 文件。

- "知識庫"

  搜尋 Workload Factory 知識庫，尋找有助於解決問題的文章。

- "社群"

  加入 Workload Factory 社群，即可關注後續的討論或建立新的討論。

建立 NetApp 支援案例

除了上述自助支援選項外，您可以在啟動支援後與 NetApp 支援專家合作解決任何問題。

開始之前

若要使用 建立案例 功能，您必須先註冊支援。將您的 NetApp 支援網站認證資料與您的 Workload Factory 登入資訊建立關聯。"了解如何註冊以獲得支援"。

步驟

1. 在 Workload Factory 主控台的右上角，選取 說明 > 支援。

   選擇此選項會在新的瀏覽器索引標籤中開啟 NetApp Console，並載入支援儀表板。

2. 在「資源」頁面上，選擇「技術支援」下的可用選項之一：

   a. 如果您想透過電話與我們聯繫，請選擇「致電」。您將被引導至 netapp.com 上的頁面，該頁面列出您可以撥打的電話號碼。

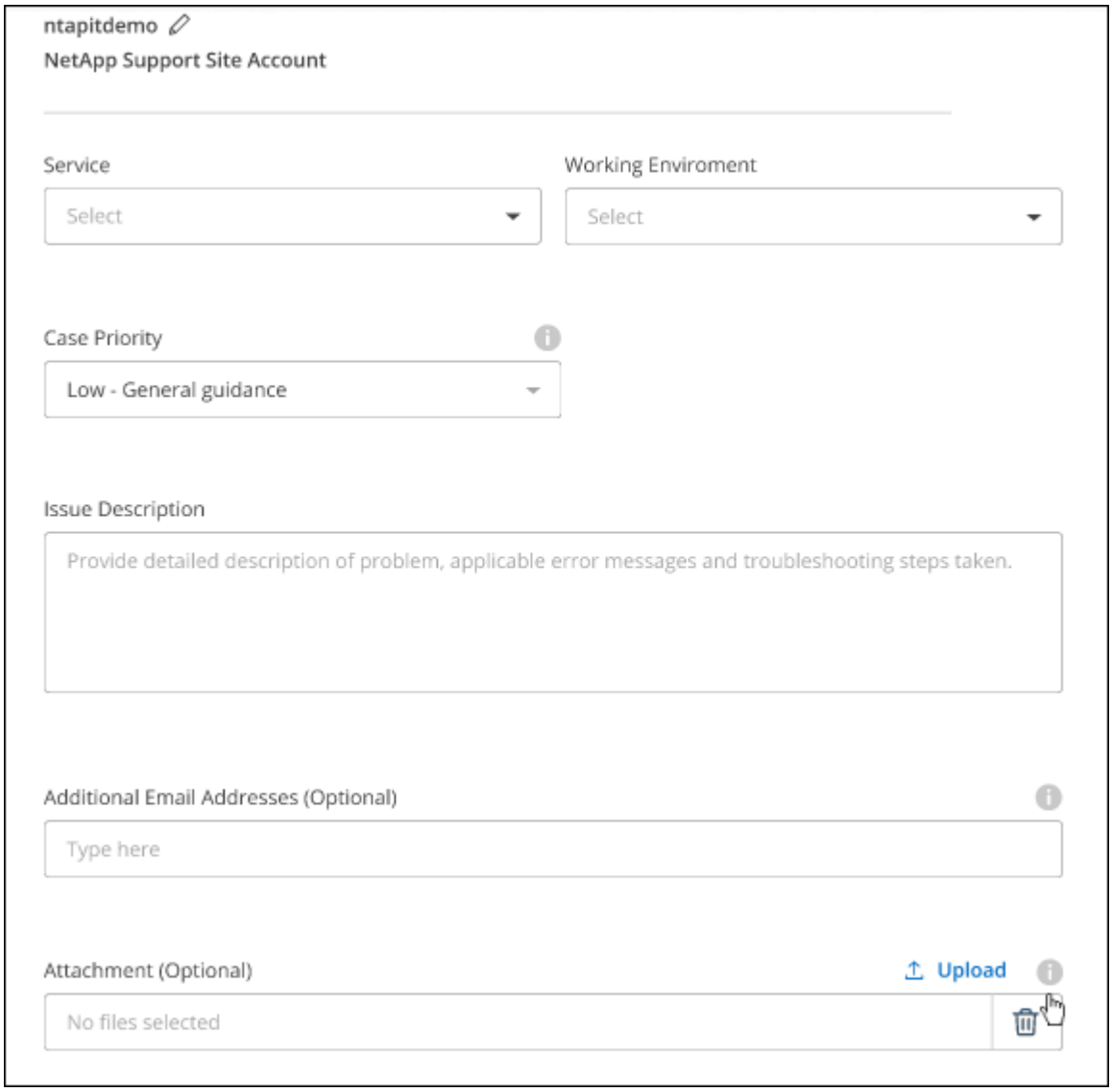
   b. 選擇「建立案例」以向 NetApp 支援專家開啟工單：

      - 服務：選擇 **Workload Factory**。
      - 案例優先順序：選擇案例的優先順序，可以是低、中、高或關鍵。

        若要深入瞭解這些優先順序的詳細資訊，請將滑鼠懸停在欄位名稱旁邊的資訊圖示上。

      - 問題執行摘要：請詳細描述您的問題，包括任何適用的錯誤訊息或您執行的疑難排解步驟。
      - 其他電子郵件地址：如果您想讓其他人知悉此問題，請輸入其他電子郵件地址。
      - 附件（選購）：一次最多可上傳五個附件。

        每個檔案的大小限制為 25 MB。支援的檔案副檔名有：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成後

螢幕上會彈出一個窗口，顯示您的支援案例編號。NetApp 支援專員將審查您的案例，並儘快與您聯繫。

若要查看您的支援案例歷史記錄，您可以選擇 **Settings > Timeline**，然後尋找名為「create support case」的行動。最右側的按鈕可讓您展開該行動以查看詳細資訊。

建立案例時，您可能會遇到以下錯誤訊息：

「您無權針對所選服務建立案例。」

此錯誤可能表示 NSS 帳戶及其關聯的註冊公司，與 NetApp Console 帳戶序號（例如960xxxx）或系統序號的註冊公司不同。您可以透過下列其中一種方式尋求協助：

- 使用產品內聊天功能
- 提交非技術性案例，請至 https://mysupport.netapp.com/site/help

管理您的支援案例（預覽版）

您可以直接從 NetApp Console 檢視和管理作用中和已解決的支援案例。您可以管理與您的 NSS 帳戶和公司關聯的案例。

案例管理目前以預覽版形式提供。我們計劃在後續版本中完善此體驗並新增增強功能。請透過產品內聊天功能向我們傳送回饋。

請注意下列事項：

- 頁面頂端的案例管理儀表板提供兩種檢視：
  - 左側檢視顯示您提供的使用者 NSS 帳戶在過去 3 個月內開啟的案例總數。
  - 右側檢視顯示過去 3 個月內，根據您的使用者 NSS 帳戶，您公司層級開立的案件總數。

  表格中的結果反映了與您選擇的檢視相關的案例。
- 您可以新增或移除感興趣的欄，也可以篩選諸如「優先順序」和「狀態」等欄的內容。其他欄位僅提供排序功能。

  請查看以下步驟以了解更多詳情。
- 在每個案件層級，我們提供更新案件備註或結案尚未處於「已結案」或「待結案」狀態的案件的功能。

步驟

1. 在 Workload Factory 主控台的右上角，選取 說明 **>** 支援。

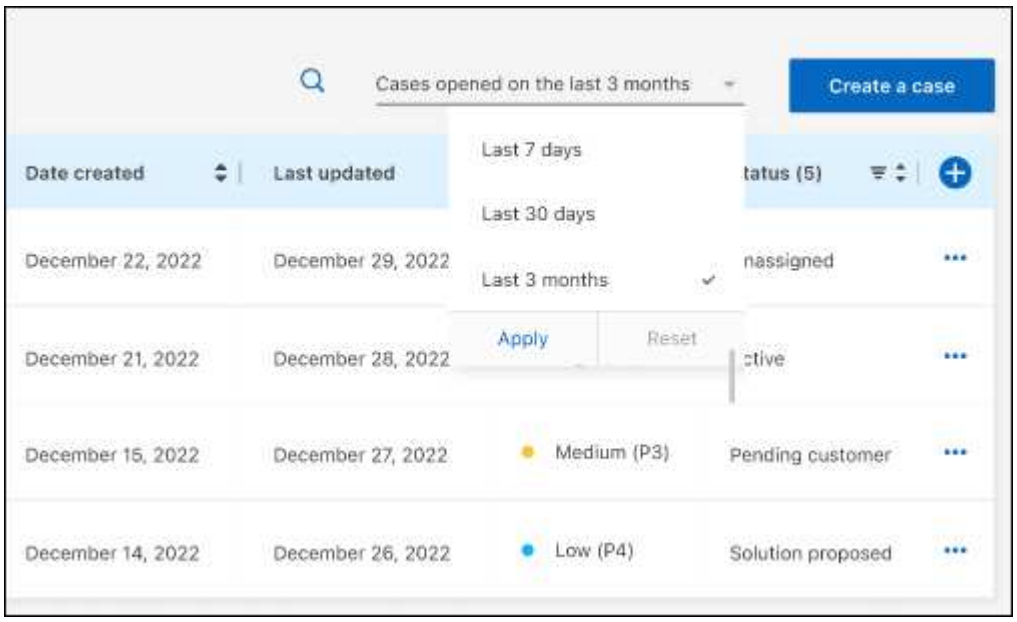
   選擇此選項會在新的瀏覽器標籤頁中開啟 NetApp Console 並載入支援儀表板。

2. 選擇 個案管理，如果系統提示，請將您的 NSS 帳戶新增至 NetApp Console。

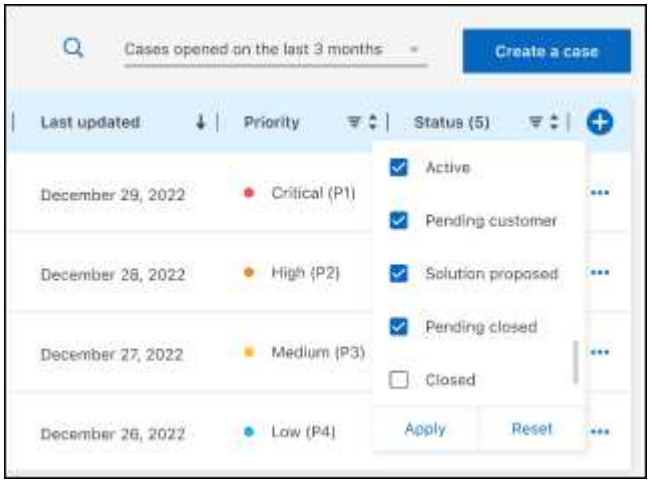
   *案例管理*頁面顯示與您的 NetApp Console 使用者帳戶相關聯之 NSS 帳戶相關的開啟案例。這與顯示在 *NSS 管理*頁面頂端的 NSS 帳戶相同。

3. 您可以選擇修改表格中顯示的資訊：
   - 在「組織案例」下，選擇「檢視」以檢視與貴公司相關的所有案例。

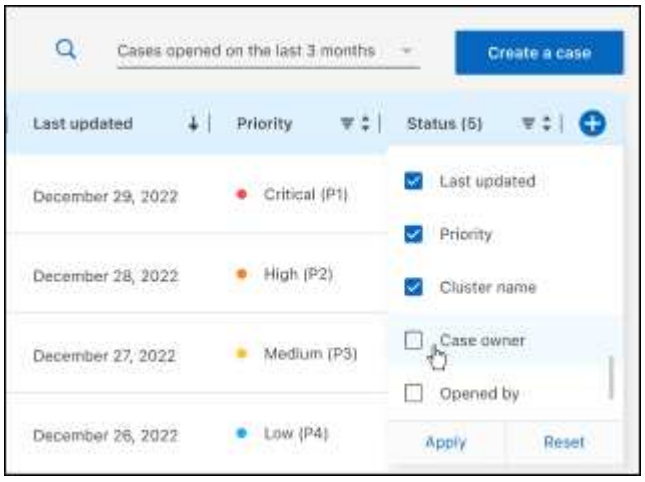
- 您可以選擇確切的日期範圍或選擇不同的時間範圍來修改日期範圍。



- 篩選各列的內容。



- 選取 ⊕，然後選擇要顯示的欄，即可變更表格中顯示的欄。

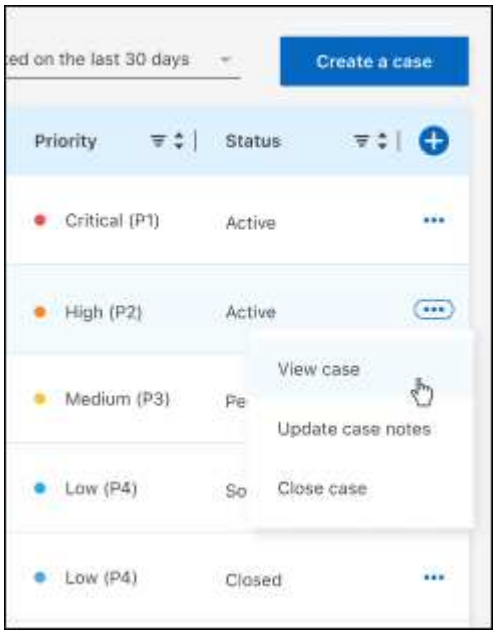


4. 透過選取 ••• 並選取其中一個可用選項來管理現有案例：

   - 檢視案例：檢視特定案例的完整詳細資訊。
   - 更新案例記錄：提供有關您問題的更多詳細資料，或選擇 **Upload files** 以附加最多五個檔案。

     每個檔案的大小限制為 25 MB。支援的檔案副檔名有：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

   - 結案：提供有關您結案原因的詳細資訊，然後選擇 結案。



NetApp Workload Factory 的法律聲明

法律聲明提供版權聲明、商標、專利等資訊的存取權限。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NETAPP、NETAPP 標誌以及 NetApp 商標頁面上所列的標記均為 NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

目前 NetApp 擁有的專利清單可在以下網址找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

開放原始碼

通知文件提供有關 NetApp 軟體中使用的第三方版權和授權的資訊。

"NetApp Workload Factory"