



ONTAP 操作和 Lambda 連結（客戶 VPC 元件）

Information Security for Workload Factory

NetApp
September 16, 2026

目錄

ONTAP 操作和 Lambda 連結（客戶 VPC 元件）	1
了解 NetApp Workload Factory 的 Lambda 連結	1
連結安全性架構	1
Lambda 連結與 NetApp Console 代理程式	2
相關資訊	2
NetApp Workload Factory 的 Lambda 連結埠和呼叫	2
請求類型	3
傳出網路邊界	3
Workload Factory 呼叫 Lambda 連結	3
相關資訊	3
適用於 NetApp Workload Factory 的 Lambda 連結 IAM 權限	3
Lambda 執行角色權限	3
Workload Factory 呼叫權限	4
NetApp Workload Factory 的 Lambda 連結生命週期	4
生命週期控制點	4

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。

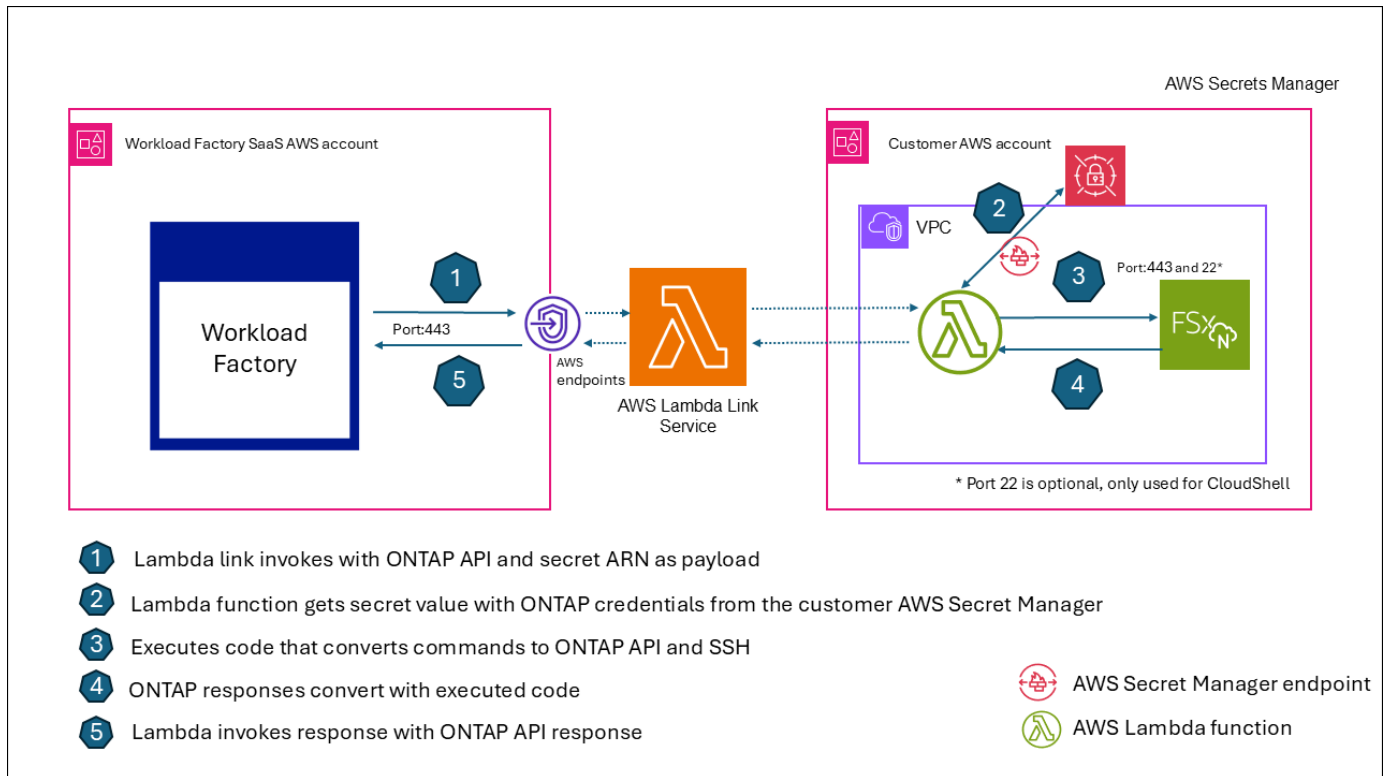
連結安全性架構

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

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。