



資料治理、隱私和生命週期 Information Security for Workload Factory

NetApp
September 16, 2026

目錄

資料治理、隱私和生命週期	1
NetApp Workload Factory 的資料處理與駐留	1
Workload Factory 處理的資料類別	1
Workload Factory 保留的資料類別	1
資訊保存位置	1
資訊保留時長	2
哪些資訊會離開虛擬私人網路（VPC）	2
組態和中繼資料收集範圍	3
NetApp Workload Factory 的加密與金鑰管理	6
FSx 的 KMS 靜態加密範圍	6
認證資料保護（服務端信封加密）	7
NetApp Workload Factory 帳戶刪除	7

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](#)。"

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。