身分、憑證和最小權限

Information Security for Workload Factory

NetApp
September 16, 2026

目錄

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