# Architettura e connettività

## Information Security for Workload Factory

NetApp
September 16, 2026

# Sommario

# Architettura e connettività

## Connettività e percorsi di fiducia per NetApp Workload Factory

NetApp Workload Factory comunica con le API AWS, le risorse dell'account AWS specifico del cliente, AWS Lambda link e Amazon Bedrock, ognuno con i propri protocolli, porte e metodi di autenticazione. Queste connessioni sono organizzate in gruppi che separano il piano di gestione AWS, il piano dati ONTAP e il traffico Lambda link, così puoi valutare i limiti di attendibilità in modo indipendente.

### Percorsi di connettività

Workload Factory stabilisce diversi percorsi di connettività distinti, ognuno con uno scopo specifico per individuare, predisporre e gestire le tue risorse AWS e ONTAP. Alcuni percorsi hanno origine da Workload Factory stessa utilizzando credenziali AWS assunte, mentre altri passano attraverso Lambda link, che opera all'interno della tua VPC per raggiungere gli endpoint di gestione ONTAP senza esporli pubblicamente. Un percorso opzionale verso Amazon Bedrock supporta la diagnostica assistita dall'AI ed è attivo solo quando la tua organizzazione abilita questa funzionalità.

Le sezioni seguenti descrivono ciascun percorso, incluse le API AWS o ONTAP coinvolte, le credenziali o l'autenticazione utilizzate e le eventuali condizioni che determinano se il percorso è attivo. Capire questi percorsi ti aiuta a valutare quali accessi di rete e autorizzazioni richiede Workload Factory e dove i dati attraversano i confini di account o VPC.

#### Workload Factory alle API AWS

Workload Factory utilizza `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` e le API EC2/VPC per il rilevamento di subnet e gruppi di sicurezza.

- Il servizio di raccolta dati effettua scansioni circa ogni cinque ore.
- Le operazioni CRUD vengono eseguite su richiesta.
- Tutte le chiamate utilizzano credenziali temporanee assunte da STS con un ID esterno.

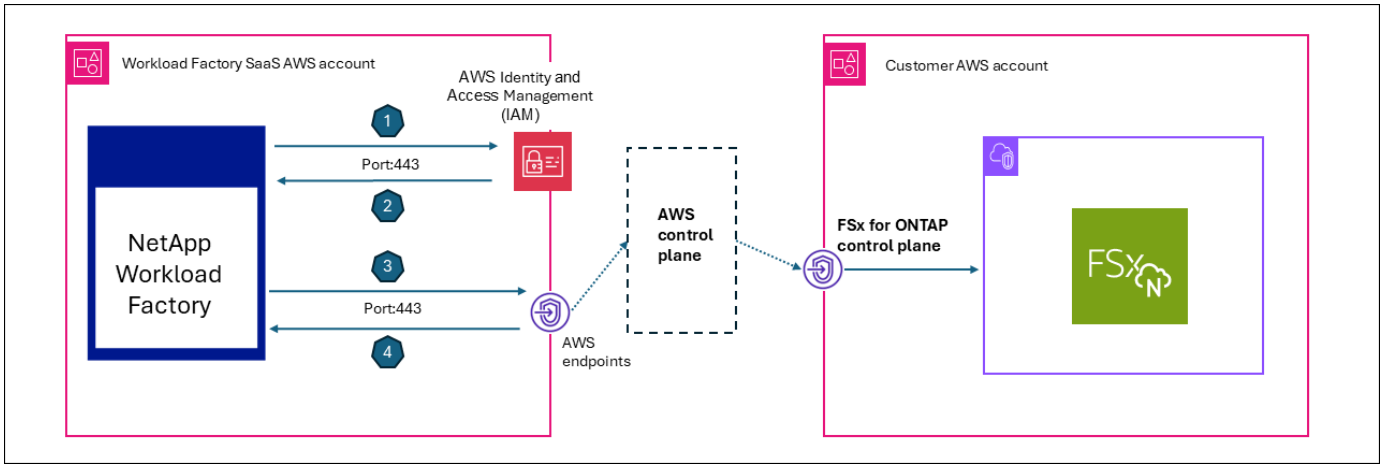
#### Workload Factory verso le risorse dell'account AWS del cliente (orchestrazione e automazione)

Workload Factory interagisce con AWS per comunicare e creare risorse. L'orchestrazione e l'automazione avvengono in diversi modi.

- Template AWS CloudFormation: Workload Factory utilizza template AWS CloudFormation per creare risorse come ruoli e file system. Ad esempio, quando crei un file system nell'interfaccia utente, Workload Factory chiama direttamente CloudFormation e ti reindirizza al tuo account AWS.
- Chiamate API AWS: Workload Factory utilizza le chiamate API AWS (STS `AssumeRole`) per inviare comandi API per attività correlate a FSx for ONTAP.
- AWS Lambda: Workload Factory utilizza CloudFormation per distribuire una funzione AWS Lambda per il collegamento che comunica con ONTAP.

Il diagramma seguente mostra come Workload Factory utilizza una relazione di fiducia tra un account AWS

NetApp e gli account AWS del cliente con file system FSx for ONTAP.




1. Workload Factory effettua richieste ad AWS STS `AssumeRole`, utilizzando un ID esterno specifico del cliente dal servizio AWS IAM.
2. Il servizio AWS IAM recupera un ruolo e crea una sessione.
3. Workload Factory invia una richiesta API AWS con autorizzazioni di sessione.
4. Workload Factory riceve una risposta API AWS dal piano di controllo FSx for ONTAP.

### Collegamento Lambda all'endpoint di gestione ONTAP

I link Lambda vengono eseguiti all'interno della VPC del cliente per l'accesso alla sottorete privata senza esporre ONTAP pubblicamente. Tutta la connettività dal link all'endpoint di gestione di ONTAP è solo outbound, quindi non sono necessarie connettività in entrata o endpoint esposti. Il link viene utilizzato solo per operazioni native di ONTAP che l'API di Amazon FSx for NetApp ONTAP non espone.

Workload Factory utilizza i seguenti protocolli per le operazioni su volumi, storage VM e cluster, e per i dati di diagnostica e prestazioni in sola lettura:

- HTTPS/443 (REST)
- SSH/22 (CLI)

### Collegamento Lambda ad AWS Secrets Manager (recupero delle credenziali ONTAP)

Da utilizzare solo quando le credenziali di amministratore di ONTAP sono archiviate in AWS Secrets Manager (in alternativa: credenziali crittografate in Workload Factory tramite crittografia a busta).

- Il proxy-forwarder trasmette `x-aws-secret-arn` (codificate in Base64) nelle intestazioni.
- Le chiamate Lambda link `GetSecretValue` al momento dell'esecuzione recuperano la password.

In questo modo la password rimane all'interno del tuo account e ne viene impedita la trasmissione da Workload Factory.

### Workload Factory e componenti specifici del cliente su Amazon Bedrock (diagnostica AI)

Questo percorso viene utilizzato solo quando la diagnostica AI è abilitata.

- Event Analyzer utilizza questo percorso per l'analisi EMS e la diagnostica della latenza.

- Bedrock viene eseguito con le tue credenziali presunte e l'ARN del profilo di inferenza, quindi i dati non fluiscono verso l'account di NetApp.

I dati inviati a Bedrock possono includere JSON di eventi EMS, statistiche QoS, configurazione del volume, dati aggregati e informazioni sui nodi. Il percorso è attivo solo quando è configurato un profilo di inferenza per organizzazione (`ai_analyzer_config` table).

## Gruppi di connessione (protocolli, porte e autenticazione)

### Gruppo A — Percorso di attendibilità del piano di gestione AWS (credenziali presunte)

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| STS AssumeRole | HTTPS | 443 | WF → AWS STS (account cliente) | Credenziali IAM + ExternalId | Ottieni credenziali temporanee tra account |
| API FSx (Describe/Create/Update/Delete) | HTTPS | 443 | WF → Endpoint AWS FSx (regione del cliente) | Credenziali temporanee STS | Gestione del ciclo di vita del file system e dei volumi |
| API EC2/VPC | HTTPS | 443 | WF → endpoint AWS EC2 | Credenziali temporanee STS | Rilevamento di gruppi di sicurezza, subnet e VPC |
| API CloudFormation | HTTPS | 443 | WF → endpoint AWS CFN | Credenziali temporanee STS | Distribuzione dello stack per i ruoli IAM e il provisioning FSx |
| Secrets Manager GetSecretValue | HTTPS | 443 | WF → Endpoint di AWS Secrets Manager (account specifico del cliente) | Credenziali temporanee STS | Recupera la password di amministratore di ONTAP (quando memorizzata in Secrets Manager) |
| Crittografia/Decrittografia KMS | HTTPS | 443 | WF → endpoint AWS KMS | Credenziali temporanee STS | Operazioni della chiave di crittografia del volume |

Tutte le chiamate API di AWS utilizzano l'endpoint regionale del cliente e possono essere instradate tramite endpoint VPC se configurati.

### Gruppo B — piano dati ONTAP

Il piano dati di ONTAP è sempre instradato tramite Lambda link; i servizi di Workload Factory non si connettono mai direttamente a ONTAP.

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| API REST ONTAP | HTTPS | 443 | Collegamento (VPC del cliente) → LIF di gestione ONTAP | Autenticazione di base (nome utente/password) o ARN di Secrets Manager | Configurazione di cluster, volumi e storage VM; QoS; eventi EMS; stato ARP |

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| CLI SSH ONTAP | SSH | 22 | Collegamento (VPC del cliente) → LIF di gestione ONTAP | autenticazione tramite password | Comandi diagnostici (statistiche QoS, df, registri eventi, efficienza) |

Strategia di routing (ordine di priorità) per il proxy-forwarder:

1. Intestazione `x-link-id` esplicita: cerca l'ARN di Lambda nel database
2. ID di destinazione (ID del file system FSx): trova il collegamento associato
3. ID agente Console: instrada attraverso il broker all'agente Console

**Gruppo C — Collegamento AWS Lambda (distribuito nella tua VPC)**

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| Invocazione Lambda | HTTPS (AWS SDK) | 443 | WF → API AWS Lambda (account cliente) | IAM (`lambda:InvokeFunction`) | Esegui i comandi ONTAP REST/SSH dall'interno della VPC del cliente |
| Lambda → ONTAP | HTTPS + SSH | 443, 22 | Lambda (VPC del cliente) → LIF di gestione ONTAP | Autenticazione di base / password | Accesso a una sottorete privata a ONTAP senza esposizione pubblica |

**Gruppo D — NetApp Console Agent (EC2 nella tua VPC, solo outbound)**

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| Polling dell'agente | HTTPS | 443 | Agente console (VPC specifico del cliente) → broker di messaggi WF | Bearer token (ambito occm-access) | Long-poll per i comandi ONTAP in sospeso (timeout di 7 secondi; si riconnette) |
| Risposta dell'agente | HTTPS | 443 | Agente console (VPC specifico del cliente) → broker di messaggi WF | token Bearer | Restituisci i risultati dei comandi ONTAP (opzionalmente compressi con zlib) |
| Agente Console → ONTAP | HTTPS + SSH | 443, 22 | Agente console (VPC cliente) → LIF di gestione ONTAP | Autenticazione di base / password | Esegui operazioni ONTAP tramite proxy |

Progettazione chiave: Workload Factory non avvia mai connessioni in entrata all'agente Console. Il lavoro viene messo in coda nei flussi Redis; l'agente Console esegue il polling `GET /messagebroker/v1/requests` e risponde con `POST /messagebroker/v1/responses`.

**Gruppo E — callback di risorse personalizzate CloudFormation**

| Connessione | Protocollo | Porta | Direzione | Autenticazione | Giustificazione |
|---|---|---|---|---|---|
| CloudFormation → WF Lambda | HTTPS | 443 | CloudFormation (cliente) → WF Lambda (NetApp) | Token JWT + token di riferimento | Segnala lo stato di creazione del ruolo IAM e restituisci l'ARN del ruolo |
| ONTAP CloudFormation Resource Provider → Link | HTTPS | 443 | CloudFormation resource Lambda (cliente) → Link Lambda (cliente) | IAM | Crea/aggiorna/elimina risorse ONTAP durante le operazioni sullo stack |

### Riepilogo: requisiti di rete per la tua VPC

| Componente | In entrata | outbound |
|---|---|---|
| FSx for ONTAP | Porta 443 e 22 dal gruppo di sicurezza Link Lambda o Console agent | N/A |
| Collega Lambda | Nessuno | Porta 443 (ONTAP, AWS APIs) e porta 22 (ONTAP SSH) |
| Agente console EC2 | Nessuno | Porta 443 (endpoint WF, ONTAP, AWS API) e porta 22 (ONTAP SSH) |
| Endpoint VPC (opzionale) | N/A | STS, FSx, S3, Secrets Manager, Lambda, CloudFormation |

Nessun componente nella VPC del cliente richiede accesso a Internet in entrata. Tutte le connessioni sono avviate in uscita (polling dell'agente della Console) o vengono invocate tramite le API dei servizi AWS (Lambda Invoke).

# Opzioni di esecuzione ONTAP per NetApp Workload Factory

Alcuni flussi di lavoro di NetApp Workload Factory richiedono operazioni native di ONTAP che non sono esposte tramite le API di AWS. Workload Factory offre due opzioni di esecuzione che mantengono queste operazioni all'interno del perimetro del tuo account AWS: un collegamento Lambda che esegue operazioni ONTAP dall'interno della tua VPC e un NetApp Console Agent che utilizza solo la connettività outbound da un'istanza EC2. Entrambe le opzioni ti permettono di eseguire le operazioni ONTAP richieste mantenendo le decisioni su rete, credenziali e ciclo di vita all'interno del tuo modello di sicurezza.

## Opzioni di esecuzione

**Collegamento Lambda (AWS Lambda nella tua VPC)**

Esegue le diagnostiche ONTAP REST e ONTAP CLI in sola lettura all'interno della tua VPC, senza esporre ONTAP pubblicamente.

**NetApp Console Agent (EC2 nella tua VPC, solo outbound)**

Esegue operazioni ONTAP tramite proxy, in cui l'agente avvia connessioni outbound e Workload Factory

non avvia mai connessioni inbound verso l'agente.

## Considerazioni sulla sicurezza

- Confini di rete: conferma le porte outbound richieste (443/22) e le destinazioni.
- Limiti delle credenziali: decidi se le credenziali ONTAP vengono archiviate in Workload Factory (crittografate in busta) o se vengono richiamate da AWS Secrets Manager.
- Verificabilità: conferma le registrazioni operative per l'attività e i guasti dei componenti.
- Gestione del ciclo di vita: conferma come avvengono gli aggiornamenti e la rimozione.

## Informazioni correlate

- "Panoramica dei collegamenti Lambda per NetApp Workload Factory"
- "Connettività e percorsi di fiducia per NetApp Workload Factory"
- "Crittografia e gestione delle chiavi per NetApp Workload Factory"

## Informazioni sul copyright



## Informazioni sul marchio commerciale