Architektur und Konnektivität

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

Architektur und Konnektivität

Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory

NetApp Workload Factory kommuniziert mit AWS-APIs, kundenspezifischen AWS-Kontoressourcen, AWS Lambda Link und Amazon Bedrock, jeweils mit eigenen Protokollen, Ports und Authentifizierungsmethoden. Diese Verbindungen sind in Gruppen organisiert, die die AWS Management-Ebene, die ONTAP Datenebene und den Lambda Link-Datenverkehr voneinander trennen, sodass Vertrauensgrenzen unabhängig bewertet werden können.

Verbindungspfade

Workload Factory richtet mehrere separate Verbindungspfade ein, die jeweils einem spezifischen Zweck bei der Erkennung, Bereitstellung und Verwaltung Ihrer AWS und ONTAP Ressourcen dienen. Einige Pfade gehen direkt von Workload Factory aus und verwenden angenommene AWS-Anmeldeinformationen, während andere über Lambda Link laufen, das innerhalb Ihrer VPC ausgeführt wird, um ONTAP Management-Endpunkte zu erreichen, ohne diese öffentlich zugänglich zu machen. Ein optionaler Pfad zu Amazon Bedrock unterstützt KI-gestützte Diagnose und ist nur aktiv, wenn Ihre Organisation diese Funktion aktiviert.

Die folgenden Abschnitte beschreiben jeden Pfad, einschließlich der beteiligten AWS- oder ONTAP-APIs, der verwendeten Anmeldeinformationen oder Authentifizierung sowie aller Bedingungen, die bestimmen, ob der Pfad aktiv ist. Das Verständnis dieser Pfade unterstützt die Bewertung, welcher Netzwerkzugriff und welche Berechtigungen von Workload Factory benötigt werden und wo Daten Konto- oder VPC-Grenzen überschreiten.

Workload Factory zu AWS APIs

Workload Factory verwendet `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` und EC2/VPC APIs zur Ermittlung von Subnetzen und Sicherheitsgruppen.

- Der Collector-Service scannt etwa alle fünf Stunden.
- CRUD-Operationen werden bei Bedarf ausgeführt.
- Alle Aufrufe verwenden von STS angenommene temporäre Anmeldeinformationen mit einer externen ID.

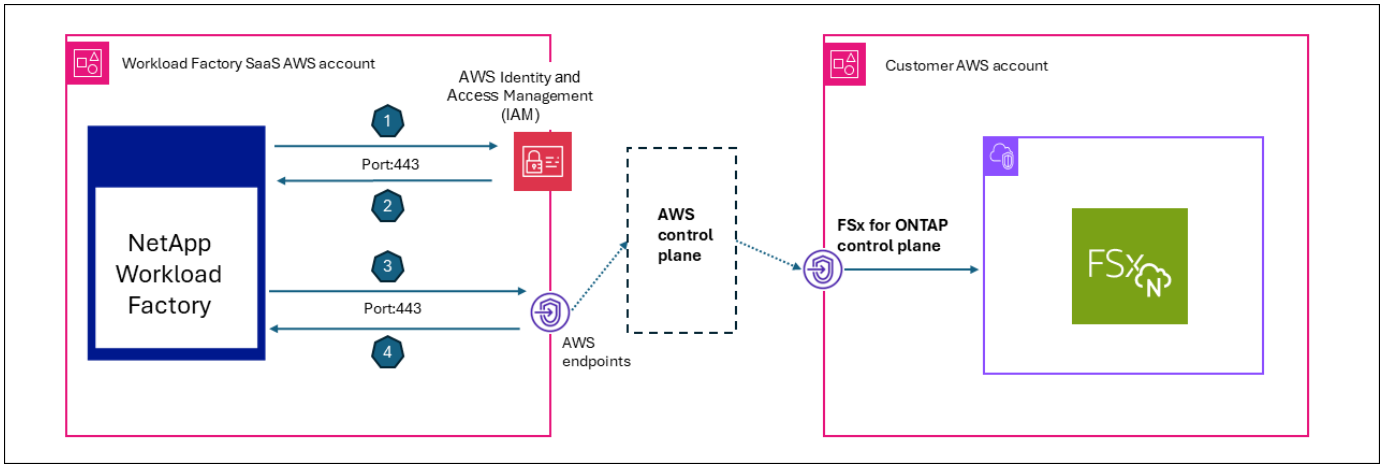
Workload Factory zu kundenspezifischen AWS-Kontoressourcen (Orchestrierung und Automatisierung)

Workload Factory interagiert mit AWS, um zu kommunizieren und Ressourcen zu erstellen. Orchestrierung und Automatisierung erfolgen auf verschiedene Weise.

- AWS CloudFormation Vorlagen: Workload Factory verwendet AWS CloudFormation Vorlagen, um Ressourcen wie Rollen und Dateisysteme zu erstellen. Beispielsweise wird beim Erstellen eines Dateisystems über die Benutzeroberfläche Workload Factory CloudFormation direkt aufgerufen und eine Weiterleitung zu Ihrem AWS-Konto erfolgt.
- AWS API-Aufrufe: Workload Factory verwendet AWS API-Aufrufe (STS `AssumeRole`), um API-Befehle für FSx for ONTAP-bezogene Aktivitäten zu senden.

- AWS Lambda: Workload Factory verwendet CloudFormation, um eine AWS Lambda-Funktion für die Verbindung bereitzustellen, die mit ONTAP kommuniziert.

Das folgende Diagramm zeigt, wie Workload Factory eine Vertrauensbeziehung zwischen einem NetApp AWS-Konto und AWS-Kundenkonten mit FSx for ONTAP Dateisystemen nutzt.



1. Workload Factory fordert AWS STS `AssumeRole`an, wobei die kundenspezifische externe ID aus dem AWS IAM-Service verwendet wird.
2. Der AWS IAM Service ruft eine Rolle ab und erstellt eine Sitzung.
3. Workload Factory sendet eine AWS API-Anfrage mit Sitzungsberechtigungen.
4. Workload Factory empfängt eine AWS API-Antwort von der FSx for ONTAP Steuerungsebene.

Lambda-Verbindung zum ONTAP Management-Endpunkt

Lambda-Links laufen innerhalb der Kunden-VPC für den Zugriff auf das private Subnetz, ohne ONTAP öffentlich zugänglich zu machen. Die gesamte Verbindung vom Link zum ONTAP Management-Endpunkt ist ausschließlich ausgehend, sodass keine eingehende Konnektivität oder freigegebene Endpunkte erforderlich sind. Der Link wird nur für ONTAP native Operationen verwendet, die die Amazon FSx for NetApp ONTAP API nicht bereitstellt.

Workload Factory verwendet die folgenden Protokolle für Volume-, Storage-VM- und Clusteroperationen sowie für schreibgeschützte Diagnose- und Leistungsdaten:

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

Lambda-Verbindung zu AWS Secrets Manager (ONTAP-Anmeldeinformationen-Abruf)

Wird nur verwendet, wenn ONTAP Administratoranmeldeinformationen im AWS Secrets Manager gespeichert sind (Alternative: Anmeldeinformationen, die in der Workload Factory mit Envelope-Verschlüsselung verschlüsselt werden).

- Der Proxy-Forwarder übergibt `x-aws-secret-arn` (Base64-kodiert) in Headern.
- Lambda-Link-Aufrufe `GetSecretValue` zur Ausführungszeit zum Abrufen des Passworts.

Dadurch bleibt das Passwort innerhalb Ihres Kontobereichs und wird nicht von Workload Factory übertragen.

Workload Factory und kundenspezifische Komponenten zu Amazon Bedrock (KI-Diagnose)

Dieser Pfad wird nur verwendet, wenn die KI-Diagnose aktiviert ist.

- Event Analyzer nutzt diesen Pfad für EMS-Analysen und Latenzdiagnose.
- Bedrock wird mit Ihren angenommenen Anmeldeinformationen und dem ARN des Inferenzprofils ausgeführt, sodass keine Daten an das Konto von NetApp fließen.

Die an Bedrock gesendeten Daten können EMS-Ereignis-JSON, QoS-Statistiken, Volumenkonfiguration, aggregierte Daten und Knoteninformationen umfassen. Der Pfad ist nur aktiv, wenn ein Inferenzprofil pro Organisation (`ai_analyzer_config` Tabelle konfiguriert ist.

Verbindungsgruppen (Protokolle, Ports und Authentifizierung)

Gruppe A, AWS Management Plane Trust Path (angenommene Anmeldeinformationen)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
STS AssumeRole	HTTPS	443	WF → AWS STS (Kundenkonto)	IAM-Anmeldeinformationen + ExternalId	Temporäre kontoübergreifende Anmeldeinformationen erhalten
FSx API (Beschreiben/Erstellen/Aktualisieren/Löschen)	HTTPS	443	WF → AWS FSx Endpoint (Kundenregion)	STS temporäre Anmeldeinformationen	Dateisystem und Volume Lebenszyklusverwaltung
EC2/VPC API	HTTPS	443	WF → AWS EC2 Endpoint	STS temporäre Anmeldeinformationen	Erkennung von Sicherheitsgruppen, Subnetzen und VPCs
CloudFormation API	HTTPS	443	WF → AWS CFN Endpoint	STS temporäre Anmeldeinformationen	Stack-Bereitstellung für IAM-Rollen und FSx-Bereitstellung
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager Endpoint (Kundenkonto)	STS temporäre Anmeldeinformationen	ONTAP Administratorpasswort abrufen (wenn im Secrets Manager gespeichert)
KMS Verschlüsselung/Entschlüsselung	HTTPS	443	WF → AWS KMS Endpoint	STS temporäre Anmeldeinformationen	Verschlüsselungsschlüssel-Operationen für Volumes

Alle AWS-API-Aufrufe verwenden den regionalen Endpunkt des Kunden und können über VPC-Endpunkte geleitet werden, sofern diese konfiguriert sind.

Gruppe B, ONTAP Datenebene

Die ONTAP Datenebene wird immer über Lambda link weitergeleitet, Workload Factory Services stellen niemals eine direkte Verbindung zu ONTAP her.

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
ONTAP REST API	HTTPS	443	Link (Kunden VPC) → ONTAP Management LIF	Basisauthentifizierung (Benutzername/Passwort) oder Secrets Manager ARN	Cluster, Volume und Storage-VM-Konfiguration; QoS; EMS-Ereignisse; ARP-Status
ONTAP SSH CLI	SSH	22	Link (Kunden VPC) → ONTAP Management LIF	Passwortauthentifizierung	Diagnosebefehle (QoS Statistiken, df, Ereignisprotokolle, Effizienz)

Routingstrategie (Prioritätsreihenfolge) für den Proxy-Forwarder:

1. Expliziter `x-link-id`Header: Lambda-ARN aus der Datenbank abrufen
2. Ziel-ID (FSx-Dateisystem-ID): den zugehörigen Link finden
3. Konsolenagenten-ID: Weiterleitung über den Message Broker zum Konsolenagenten

Gruppe C, AWS Lambda Link (in Ihrer VPC bereitgestellt)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
Lambda Invoke	HTTPS (AWS SDK)	443	WF → AWS Lambda API (Kundenkonto)	IAM (`lambda:InvokeFunction`)	ONTAP REST/SSH-Befehle können innerhalb der Kunden-VPC ausgeführt werden.
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (Kunden-VPC) → ONTAP Management LIF	Basisauthentifizierung / Passwort	Privater Subnetzzugang zu ONTAP ohne öffentliche Zugänglichkeit

Gruppe D, NetApp Console Agent (EC2 in Ihrer VPC, nur ausgehend)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
Agentenabfrage	HTTPS	443	Konsolenagent (Kunden-VPC) → WF Message Broker	Bearer Token (occm-access scope)	Long-Polling für ausstehende ONTAP Befehle (7-Sekunden-Zeitüberschreitung; erneute Verbindungen)
Antwort des Agenten	HTTPS	443	Konsolenagent (Kunden-VPC) → WF Message Broker	Bearer Token	ONTAP-Befehlsausgaben zurückgeben (optional zlib-komprimiert)
Konsolenagent → ONTAP	HTTPS + SSH	443, 22	Konsolenagent (Kunden-VPC) → ONTAP Management LIF	Basisauthentifizierung / Passwort	Proxied ONTAP Vorgänge ausführen

Wesentliches Designmerkmal: Workload Factory initiiert niemals eingehende Verbindungen zum Console-Agenten. Die Arbeit wird in Redis-Streams in eine Warteschlange gestellt; der Console-Agent fragt `GET /messagebroker/v1/requests`ab und antwortet mit `POST /messagebroker/v1/responses`.

Gruppe E, CloudFormation kundenspezifische Ressourcen-Callbacks

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (Kunde) → WF Lambda (NetApp)	JWT-Token + Referenztoken	Status der IAM-Rollenerstellung melden und Rollen-ARN zurückgeben
ONTAP CloudFormation Ressourcenanbieter → Link	HTTPS	443	CloudFormation Ressource Lambda (Kunde) → Link Lambda (Kunde)	IAM	ONTAP Ressourcen während Stack-Operationen erstellen, aktualisieren oder löschen

Zusammenfassung: Netzwerkanforderungen für Ihre VPC

Komponente	Eingehend	Ausgehend
FSx for ONTAP	Port 443 und 22 von der Link Lambda oder Console Agent Sicherheitsgruppe	k. A.
Lambda verknüpfen	Keine	Port 443 (ONTAP, AWS APIs) und Port 22 (ONTAP SSH)
Konsolen-Agent EC2	Keine	Port 443 (WF Endpunkte, ONTAP, AWS APIs) und Port 22 (ONTAP SSH)
VPC Endpunkte (optional)	k. A.	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

Für keine Komponente in der Kunden-VPC ist ein eingehender Internetzugang erforderlich. Alle Verbindungen werden entweder ausgehend initiiert (Konsolenagent-Polling) oder über AWS-Service-APIs aufgerufen (Lambda Invoke).

ONTAP Ausführungsoptionen für NetApp Workload Factory

Einige NetApp Workload Factory Workflows erfordern ONTAP-native Operationen, die nicht über AWS APIs bereitgestellt werden. Workload Factory bietet zwei Ausführungsoptionen, die diese Operationen innerhalb Ihres AWS-Kontorahmens halten: einen Lambda-Link, der ONTAP Operationen innerhalb Ihrer VPC ausführt, und einen NetApp Console Agent, der ausschließlich ausgehende Verbindungen von einer EC2-Instanz nutzt. Beide Optionen ermöglichen die Durchführung der erforderlichen ONTAP Operationen, wobei Netzwerk-, Anmeldeinformations- und Lebenszyklusentscheidungen innerhalb Ihres Sicherheitsmodells verbleiben.

Ausführungsoptionen

Lambda-Verknüpfung (AWS Lambda in Ihrer VPC)

Führt ONTAP REST und schreibgeschützte ONTAP CLI Diagnose innerhalb Ihrer VPC aus, ohne ONTAP öffentlich zugänglich zu machen.

NetApp Console Agent (EC2 in Ihrer VPC, nur ausgehend)

Führt proxied ONTAP Operationen aus, bei denen der Agent ausgehende Verbindungen initiiert und Workload Factory niemals eingehende Verbindungen zum Agenten initiiert.

Sicherheitsüberlegungen

- Netzwerkgrenzen: Erforderliche ausgehende Ports (443/22) und Zieladressen prüfen.
- Grenzen der Anmeldeinformationen: Es kann festgelegt werden, ob ONTAP-Anmeldeinformationen in Workload Factory (umschlagverschlüsselt) gespeichert oder aus AWS Secrets Manager referenziert werden.
- Prüfbarkeit: Betriebsaufzeichnungen für Komponentenaktivitäten und -ausfälle werden bestätigt.
- Lebenszyklusmanagement: Es wird bestätigt, wie Aktualisierungen und Entfernung erfolgen.

Verwandte Informationen

- "Lambda-Link-Übersicht für NetApp Workload Factory"
- "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory"
- "Verschlüsselung und Schlüsselverwaltung für NetApp Workload Factory"