ONTAP Operationen und Lambda Verbindung (Kunden VPC Komponente)

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

ONTAP Operationen und Lambda Verbindung (Kunden VPC Komponente)

Informationen zur Lambda-Verbindung für NetApp Workload Factory

NetApp Workload Factory verwendet einen Link, eine in Ihrer VPC bereitgestellte AWS Lambda-Funktion, um ONTAP-native Operationen innerhalb Ihres AWS-Kontos zu belassen, wenn die Amazon FSx for NetApp ONTAP API diese Operationen nicht bereitstellt. Der Link läuft in Ihren Subnetzen und Sicherheitsgruppen, sodass die Ausführungskomponente innerhalb Ihrer AWS-Umgebung bleibt. Workload Factory nutzt den Link nur für Operationen, die direkten ONTAP Zugriff erfordern, anstatt eine verfügbare AWS Service API zu verwenden. Die Architektur des Links wird mit dem Sicherheits- und Betriebsprofil des NetApp Console Agenten verglichen.

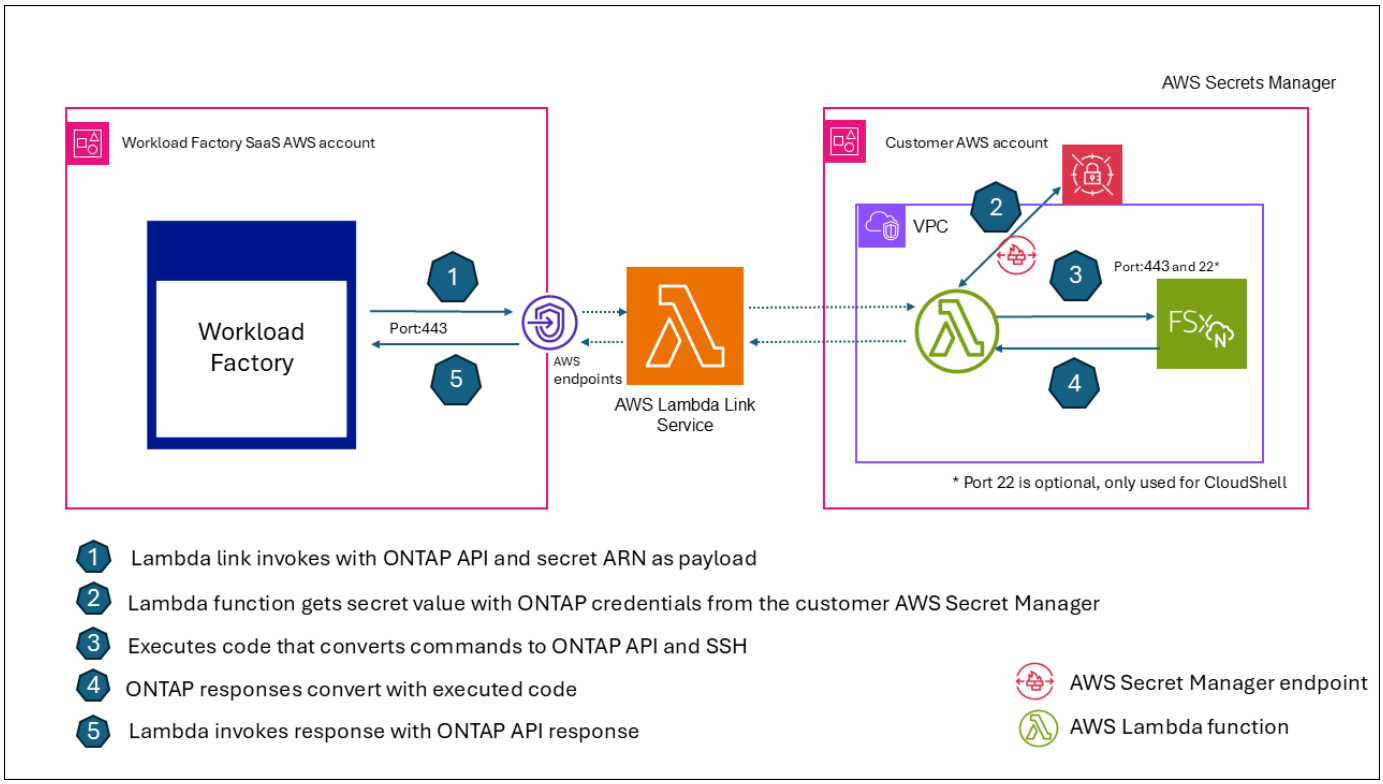
Sicherheitsarchitektur für Verbindungen

Ein Workload Factory Link erstellt eine Vertrauensbeziehung und eine indirekte Konnektivität zwischen einem Workload Factory Account und einem oder mehreren FSx for ONTAP File Systemen.

Die folgende Tabelle bietet einen Überblick über die Lambda Link-Sicherheitsarchitektur. Diese Informationen geben Aufschluss darüber, wie die Lambda-Funktion in Ihrem AWS-Konto bereitgestellt und ausgeführt wird, einschließlich ihrer Netzwerkkonfiguration, Laufzeitumgebung und Betriebsgrenzen.

Eigenschaft	Detail
Compute	AWS Lambda (Container Image)
Laufzeit	Node.js 22
Bereitstellung	CloudFormation Stack in Ihrem AWS Account
VPC Platzierung	Ihre Subnetze, Ihre Sicherheitsgruppen
Zeitüberschreitung	10 Sekunden pro Aufruf
Aufruf	Synchron (RequestResponse)
Pakettyp	Container-Image (aus NetApp ECR)

Das folgende Diagramm zeigt die Sicherheitsarchitektur der Lambda-Verbindung.



Lambda link versus NetApp Console Agent

Die Lambda-Verbindung und der NetApp Console Agent dienen unterschiedlichen Zwecken und haben unterschiedliche Auswirkungen auf Sicherheit und Betrieb.

Dimension	Link (Lambda-basiert)	NetApp Console Agent (VM/Pods-basiert)
Laufzeitmodell	Serverless (AWS Lambda), kundenseitig bereitgestellt	Vom Kunden bereitgestellte VMs/Container; führt NetApp Console Service Pods aus
Primärer Umfang	Control plane ONTAP REST-Operationen (nur wenn AWS-APIs die Operation nicht unterstützen)	Orchestrierung plus Unterstützung für Datendienste
Unterstützung von Datendiensten	Bietet keine Datendienste an	Kann Datendienste hosten (führt NetApp Console Service Pods aus)
Betriebsaufwand	Keine ständig laufende VM	VM Lifecycle Management und Upgrades

Verwandte Informationen

Die vollständige Karte der systemübergreifenden Verbindungen ist unter "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory" zu finden.

Lambda-Link-Ports und Aufrufe für NetApp Workload Factory

NetApp Workload Factory verwendet Lambda-Link-Anfragen und Portgrenzen, um die

erforderliche ausgehende Konnektivität und die durch IAM autorisierte Ausführung zu definieren. Der Link unterstützt HTTPS-Anfragen an den ONTAP Management-Endpunkt, schreibgeschützte SSH-Befehle für Diagnose und Integritätsprüfungen. Die gesamte Konnektivität erfolgt ausgehend vom Link innerhalb Ihrer VPC, sodass keine eingehende Konnektivität oder freigelegte Endpunkte erforderlich sind. Workload Factory nutzt die AWS Lambda API mit IAM-basierter Autorisierung, um den Link aufzurufen.

Anfragetypen

- HTTPS (ONTAP REST API): Proxys HTTPS-Aufrufe an den ONTAP Management-Endpunkt (Port 443) für Volume-, Storage-VM- und Cluster-Operationen.
- SSH (ONTAP CLI): Führt schreibgeschützte ONTAP CLI-Befehle auf Port 22 für Diagnose- und Leistungsdaten aus.
- Gesundheitscheck: Gibt Status und unterstützte Funktionen zurück.

Ausgehende Netzwerkgrenzen

Richtung	Port	Ziel	Zweck
Ausgehend	443	ONTAP Management-IP (innerhalb Ihrer VPC)	REST API-Operationen
Ausgehend	22	ONTAP Management-IP (innerhalb Ihrer VPC)	SSH CLI-Befehle
Ausgehend	443	AWS Secrets Manager Endpoint (optional)	Abruf von Anmeldeinformationen bei Verwendung von Secrets Manager

Es ist keine eingehende Verbindung erforderlich. Der Link stellt keine Endpunkte bereit. Workload Factory ruft ihn mithilfe der AWS `lambda:InvokeFunction` API auf.

Workload Factory ruft Lambda Link auf

Workload Factory ruft die Lambda-Verbindung über die AWS Lambda API (`lambda:InvokeFunction` unter Verwendung einer IAM-basierten Autorisierung auf.

Die Aufrufnutzlast enthält:

- Ziel ONTAP Management-Endpunkt (IP/Hostname)
- Auszuführender Vorgang (REST API-Pfad oder SSH-Befehl)
- Authentifizierungsinformationen (Inline-Anmeldeinformationen oder eine Secrets Manager ARN-Referenz)

Verwandte Informationen

Die vollständige Karte der systemübergreifenden Konnektivität befindet sich unter "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory".

Lambda Link IAM-Berechtigungen für NetApp Workload Factory

NetApp Workload Factory verwendet Lambda link permission boundaries, um den für die Lambda-Ausführung und den Workload Factory-Aufruf erforderlichen IAM-Zugriff zu definieren. Diese Berechtigungen sind optional, aber für ONTAP native Operationen erforderlich. Bei der Konfiguration der Secrets Manager-Unterstützung ruft der Link ONTAP-Anmeldeinformationen zur Laufzeit direkt aus Ihrem AWS Secrets Manager ab, und das Passwort wird ausschließlich innerhalb Ihrer VPC übertragen, vom Secrets Manager zur Lambda-Funktion und anschließend zum ONTAP Endpoint.

Informationen zu Anfragepfad und Portanforderungen sind unter "Lambda Link-Ports und -Aufrufe" zu finden.

Berechtigungen der Lambda-Ausführungsrolle

Die Lambda-Ausführungsrolle benötigt beim Bereitstellen eines Links in Ihrer VPC die folgenden Berechtigungen:

Berechtigung	Zweck
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	Standardmäßige VPC-gebundene Lambda-Netzwerke
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP Management
secretsmanager:GetSecretValue (beschränkt auf FSxSecret*)	ONTAP Anmeldeinformationen abrufen (nur wenn Secrets Manager aktiviert ist)
CloudWatch Logs (verwaltete Richtlinie)	Lambda-Ausführungsprotokollierung

Berechtigungen zum Aufruf der Workload Factory

Die ressourcenbasierte Richtlinie für Lambda link gewährt dem Serviceprinzipal der Workload Factory die folgenden Berechtigungen:

Berechtigung	Zweck
lambda:InvokeFunction	Die Lambda-Funktion ausführen
lambda:GetFunction	Gesundheits- und Statusprüfungen
lambda:UpdateFunctionCode	Versionsaktualisierungen (Image-Updates)
lambda:GetFunctionConfiguration	Konfigurationsprüfung

Lebenszyklus der Lambda-Verbindung für NetApp Workload Factory

NetApp Workload Factory nutzt Lambda-Link-Lebenszyklussteuerungen, um Bereitstellung, Zustandsüberwachung und kontrollierte Image-Updates mit minimalem

Betriebsaufwand zu verwalten. Das Container-Image des Lambda-Links kann aktualisiert werden, um Verbesserungen oder Sicherheitspatches bereitzustellen, ohne den Amazon CloudFormation Stack neu bereitzustellen, unter Verwendung der `lambda:UpdateFunctionCode` Berechtigung. Die Lebenszyklussteuerungen definieren außerdem, wie die Link-Gesundheit überwacht wird und wie der Lambda-Link sowie die zugehörigen Ressourcen entfernt werden, wenn sie nicht mehr benötigt werden.

Lebenszyklus-Kontrollpunkte

- Bereitstellung: automatisiert über Amazon CloudFormation oder Terraform Stack-Bereitstellung
- Überwachung: Systemprüfungen erkennen Verbindungsprobleme; Fehlerzähler verfolgen die Zuverlässigkeit
- Entfernung: Das Löschen des CloudFormation Stacks entfernt die Lambda-Funktion und die zugehörigen Ressourcen aus Ihrem AWS-Konto.