ONTAP operations and Lambda link (customer VPC component)

Information Security for Workload Factory

NetApp
September 16, 2026

Table of Contents

ONTAP operations and Lambda link (customer VPC component)

Learn about the Lambda link for NetApp Workload Factory

NetApp Workload Factory uses a *link*, an AWS Lambda function deployed in your VPC, to keep ONTAP-native operations inside your AWS account boundary when the Amazon FSx for NetApp ONTAP API doesn't expose those operations. The link runs in your subnets and security groups, so the execution component remains within your AWS environment. Workload Factory invokes the link only for operations that require direct ONTAP access rather than an available AWS service API. It compares the link's architecture with the security and operational profile of the NetApp Console agent.

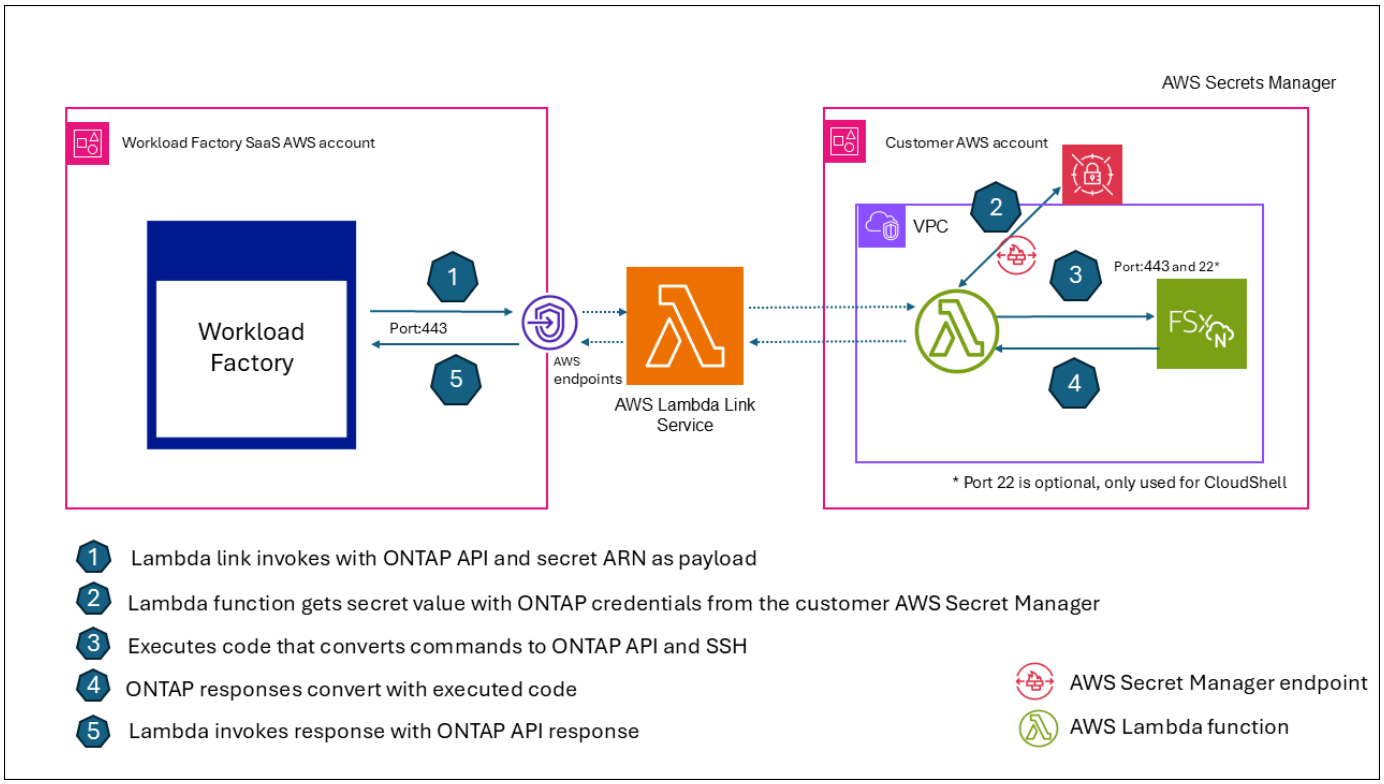
Link security architecture

A Workload Factory link creates a trust relationship and indirect connectivity between a Workload Factory account and one or more FSx for ONTAP file systems.

The following table provides an overview of the Lambda link security architecture. Use this information to understand how the Lambda function is deployed and executed in your AWS account, including its networking configuration, runtime environment, and operational limits.

Property	Detail
Compute	AWS Lambda (container image)
Runtime	Node.js 22
Deployment	CloudFormation stack in your AWS account
VPC placement	Your subnets, your security groups
Timeout	10 seconds per invocation
Invocation	Synchronous (RequestResponse)
Package type	Container image (from NetApp ECR)

The following diagram shows the security architecture of the Lambda link.



Lambda link versus NetApp Console agent

The Lambda link and the NetApp Console agent serve different purposes and have different security and operational implications.

Dimension	Link (Lambda-based)	NetApp Console agent (VM/Pods-based)
Runtime model	Serverless (AWS Lambda), customer-deployed	Customer-deployed VM/containers; runs NetApp console service pods
Primary scope	Control-plane ONTAP REST operations (only when AWS APIs do not support the operation)	Orchestration plus support for data services
Data services support	Does not host data services	Can host data services (runs NetApp console service pods)
Operational overhead	No always-on VM	VM lifecycle management and upgrades

Related information

For the full cross-system connectivity map, refer to Connectivity and trust paths for NetApp Workload Factory.

Lambda link ports and calls for NetApp Workload Factory

NetApp Workload Factory uses Lambda link request and port boundaries to define required outbound connectivity and IAM-authorized invocation. The link supports HTTPS requests to the ONTAP management endpoint, read-only SSH commands for diagnostics, and health checks. All connectivity is outbound from the link within your VPC,

so no inbound connectivity or exposed endpoints are required. Workload Factory invokes the link through the AWS Lambda API using IAM-based authorization.

Request types

- HTTPS (ONTAP REST API): proxies HTTPS calls to the ONTAP management endpoint (port 443) for volume, storage VM, and cluster operations.
- SSH (ONTAP CLI): executes read-only ONTAP CLI commands on port 22 for diagnostics and performance data.
- Health check: returns status and supported features.

Outbound network boundaries

Direction	Port	Destination	Purpose
Outbound	443	ONTAP management IP (within your VPC)	REST API operations
Outbound	22	ONTAP management IP (within your VPC)	SSH CLI commands
Outbound	443	AWS Secrets Manager endpoint (optional)	Credential retrieval when using Secrets Manager

No inbound connectivity is required. The link does not expose any endpoints. Workload Factory invokes it using the AWS `lambda:InvokeFunction` API.

Workload Factory calls Lambda link

Workload Factory calls the Lambda link via the AWS Lambda API (`lambda:InvokeFunction`) using IAM-based authorization.

The invocation payload contains:

- target ONTAP management endpoint (IP/hostname)
- operation to perform (REST API path or SSH command)
- authentication information (inline credentials or a Secrets Manager ARN reference)

Related information

For the full cross-system connectivity map, refer to connectivity and trust paths for NetApp Workload Factory.

Lambda link IAM permissions for NetApp Workload Factory

NetApp Workload Factory uses Lambda link permission boundaries to define the IAM access required for Lambda execution and Workload Factory invocation. These permissions are optional, but they are required for ONTAP-native operations. When you configure Secrets Manager support, the link retrieves ONTAP credentials directly from your AWS Secrets Manager at runtime, and the password transits only within your VPC, from Secrets Manager to the Lambda function and then to the ONTAP endpoint.

For request-path and port requirements, refer to Lambda link ports and calls.

Lambda execution role permissions

The Lambda execution role requires the following permissions when deploying a link in your VPC:

Permission	Purpose
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	Standard VPC-attached Lambda networking
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP management
secretsmanager:GetSecretValue (scoped to FSxSecret*)	Retrieve ONTAP credentials (only when Secrets Manager is enabled)
CloudWatch Logs (managed policy)	Lambda execution logging

Workload Factory invocation permissions

The Lambda link resource-based policy grants the Workload Factory service principal the following permissions:

Permission	Purpose
lambda:InvokeFunction	Execute the Lambda
lambda:GetFunction	Health and status checks
lambda:UpdateFunctionCode	Version upgrades (image updates)
lambda:GetFunctionConfiguration	Configuration verification

Lambda link lifecycle for NetApp Workload Factory

NetApp Workload Factory uses Lambda link lifecycle controls to manage deployment, health monitoring, and controlled image updates with minimal operational exposure. You can update the Lambda link container image to deploy improvements or security patches without redeploying the Amazon CloudFormation stack, using the `lambda:UpdateFunctionCode` permission. The lifecycle controls also define how you monitor link health and remove the Lambda link and its associated resources when they are no longer needed.

Lifecycle control points

- Deployment: automated via Amazon CloudFormation or Terraform stack deployment
- Monitoring: health checks detect connectivity issues; failure counters track reliability
- Removal: deleting the CloudFormation stack removes the Lambda and associated resources from your AWS account

Copyright information

Trademark information