Security model and responsibilities

Information Security for Workload Factory

NetApp
September 16, 2026

Table of Contents

Security model and responsibilities

Learn about the security model for NetApp Workload Factory

NetApp Workload Factory is a SaaS control plane that helps you manage and optimize workloads that run on Amazon FSx for NetApp ONTAP in your AWS environment. Security outcomes depend on shared responsibilities across NetApp, AWS, and your organization.

High-level security model

- Workload Factory uses an IAM assume-role model to obtain temporary AWS STS credentials to call AWS APIs in your account.
- Some workflows require ONTAP-native operations that are not exposed through AWS APIs; you can execute those operations inside your VPC using customer-deployed execution components (for example, Lambda link).
- Observability signals (metrics, telemetry, and operational records) support operational monitoring and investigations.

Key review questions

- What access does Workload Factory require to your AWS account (role trust + permissions)?
- Which execution paths apply to your intended workflows (AWS API-only or ONTAP-native operations via a VPC component)?
- What data categories are handled (configuration/metadata, operational logs/events, telemetry) and where are they stored?
- What monitoring signals exist and what are their retention characteristics?

What's next

- Shared responsibility boundaries for NetApp Workload Factory
- Connectivity and trust paths for NetApp Workload Factory
- Least privilege permission tiers for NetApp Workload Factory

Shared responsibility boundaries for NetApp Workload Factory

NetApp Workload Factory security responsibility is shared across NetApp (SaaS operation), AWS (cloud infrastructure and managed services), and you (customer configuration). Understanding where each party's responsibility begins and ends helps you configure your AWS environment correctly and avoid security gaps. These boundaries clarify what NetApp operates, what AWS secures, and what you must configure and maintain yourself.

NetApp responsibilities (service side)

NetApp is responsible for operating and securing the Workload Factory SaaS platform. This includes service-side handling of stored configuration references and operational data.

AWS responsibilities (cloud platform)

AWS is responsible for security of the cloud infrastructure and managed services used by your deployment and workflows (for example, IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda, and networking primitives).

Customer responsibilities (your configuration)

You are responsible for:

- AWS IAM roles, trust policies, and least-privilege permissions
- VPC controls (subnets, security groups, routing, endpoints, and egress)
- Credential governance (including ONTAP credentials if required by your workflows)
- Encryption and key management decisions (for example, optional customer-managed KMS keys for FSx for ONTAP)
- Monitoring, alerting, retention policies, and incident response processes

Evidence to capture

- IAM role trust relationship (including external ID condition)
- IAM permission tier selection and policy artifacts
- Network boundary decision (AWS API-only vs VPC execution component such as Lambda link)
- Observability decisions and retention expectations
- AI enablement decision (AI diagnostics are enabled by default unless explicitly disabled)

NetApp Workload Factory onboarding security workflow

Onboarding to NetApp Workload Factory establishes secure access to your AWS environment before you begin using the product. The process combines AWS trust configuration, permission scoping, connectivity setup, observability verification, and optional AI diagnostics enablement.

Step 1: Decide your onboarding posture

- Identify AWS accounts and environment boundaries (for example, prod vs non-prod separation).
- Identify required workflows (read-only discovery vs provisioning vs ONTAP-native operations).
- Decide whether to deploy VPC execution components (for example, Lambda link) based on workflow needs.
- Decide whether to enable AI diagnostics (enabled by default).

Related information

- Credential types
- Lambda link overview
- AI controls overview

Step 2: Establish AWS trust and access

1. Deploy an IAM role in your AWS account.
2. Gate role assumption using an external ID in the trust policy.
3. Register the role ARN and external ID in Workload Factory.

Related information

AWS account integration

Step 3: Apply least-privilege permissions

1. Select the minimum permission tier that supports your intended workflows.
2. Validate that per-request session policies restrict actions to the operation being performed.

Related information

Least privilege permission tiers for NetApp Workload Factory.

Step 4: Configure connectivity and VPC boundaries (as needed)

1. Validate required network paths to AWS endpoints.
2. If you require ONTAP-native operations, deploy and validate the appropriate execution option in your VPC.

Related information

- Connectivity and trust paths for NetApp Workload Factory
- ONTAP execution options for NetApp Workload Factory

Step 5: Verify observability

1. Confirm metrics and telemetry are collected and retained as expected.
2. Confirm you can access required operational records for troubleshooting and investigations.

Related information

- Observability overview for NetApp Workload Factory
- Metrics and telemetry for NetApp Workload Factory

Step 6: Enable AI diagnostics (optional)

AI diagnostics are enabled by default. If you enable them, verify that you meet the prerequisites and scope permissions to the minimum required.

Related information

- Bedrock opt-in for NetApp Workload Factory AI diagnostics
- AI tool boundaries for NetApp Workload Factory

Compliance and security posture for NetApp Workload Factory

NetApp Workload Factory is built with compliance and security as core priorities. All workloads in Workload Factory run on Amazon FSx for NetApp ONTAP. In addition to AWS security features, NetApp Workload Factory has SOC2 Type 1, SOC2 Type 2, and HIPAA compliance.

Amazon FSx for NetApp ONTAP for NetApp Workload Factory is an AWS solution for deploying enterprise apps, and it follows AWS Well-Architected best practices.

Copyright information

Trademark information