Information security for NetApp Workload Factory

Information Security for Workload Factory

NetApp
October 09, 2026

This PDF was generated from https://docs.netapp.com/us-en/workload-infosec/index.html on October 09, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Learn about information security for NetApp Workload Factory . . . 1
- What Workload Factory is . . . 1
- Core security principles used in this guide . . . 1
- Types of information covered in this guide . . . 1
- Get started quickly . . . 2

Security model and responsibilities . . . 3
- Learn about the security model for NetApp Workload Factory . . . 3
  - High-level security model . . . 3
  - Key review questions . . . 3
  - What's next . . . 3
- Shared responsibility boundaries for NetApp Workload Factory . . . 3
  - NetApp responsibilities (service side) . . . 4
  - AWS responsibilities (cloud platform) . . . 4
  - Customer responsibilities (your configuration) . . . 4
  - Evidence to capture . . . 4
- NetApp Workload Factory onboarding security workflow . . . 4
  - Step 1: Decide your onboarding posture . . . 4
  - Step 2: Establish AWS trust and access . . . 5
  - Step 3: Apply least-privilege permissions . . . 5
  - Step 4: Configure connectivity and VPC boundaries (as needed) . . . 5
  - Step 5: Verify observability . . . 5
  - Step 6: Enable AI diagnostics (optional) . . . 5
- Compliance and security posture for NetApp Workload Factory . . . 6

Architecture and connectivity . . . 7
- Connectivity and trust paths for NetApp Workload Factory . . . 7
  - Connectivity paths . . . 7
  - Connection groups (protocols, ports, and auth) . . . 9
  - Summary: network requirements for your VPC . . . 11
- ONTAP execution options for NetApp Workload Factory . . . 11
  - Execution options . . . 11
  - Security considerations . . . 12
  - Related information . . . 12

Identity, credentials, and least privilege . . . 13
- AWS account integration for NetApp Workload Factory . . . 13
  - AWS account configuration . . . 13
  - Runtime . . . 13
- How AWS credentials flow through NetApp Workload Factory . . . 13
  - One-time setup . . . 14
  - Runtime (every API operation) . . . 14
  - Session policy . . . 14
  - Related information . . . 14
- AWS credential retention for NetApp Workload Factory . . . 14
  - Key behaviors . . . 15

Retention and storage summary . . . 15
Security controls . . . 16
Credential types for NetApp Workload Factory . . . 16
Credential types . . . 16
AWS credential-only operations . . . 16
ONTAP credentials-only operations . . . 17
Operations requiring both AWS and ONTAP credentials . . . 17
Related information . . . 17
Credential storage options for NetApp Workload Factory . . . 18
Read-only ONTAP access model . . . 18
Credential storage options comparison . . . 18
Additional considerations . . . 19
Least privilege permission tiers for NetApp Workload Factory . . . 19
Tiered permission model . . . 19
Granting permissions . . . 19
Security controls . . . 19
Permissions documentation . . . 19
Amazon CloudWatch monitoring permissions for NetApp Workload Factory . . . 20
Required CloudWatch monitoring permissions . . . 20
Data governance, privacy, and lifecycle . . . 21
Data handling and residency for NetApp Workload Factory . . . 21
Data classes handled by Workload Factory . . . 21
Data classes retained by Workload Factory . . . 21
Where information is kept . . . 21
How long information is kept . . . 22
What information leaves the VPC . . . 22
Configuration and metadata collection scope . . . 23
Encryption and key management for NetApp Workload Factory . . . 26
KMS encryption-at-rest scope for FSx . . . 27
Credential protection (service-side envelope encryption) . . . 27
NetApp Workload Factory account deletion . . . 28
Observability (logs, metrics, telemetry) . . . 29
Learn about observability in NetApp Workload Factory . . . 29
Telemetry and operational records . . . 29
Audit logging in Workload Factory . . . 29
Related information . . . 29
Metrics and telemetry for NetApp Workload Factory . . . 29
Metrics included . . . 29
About operational metrics . . . 30
About telemetry data collection . . . 30
Volume-level CloudWatch metrics (collected per volume) . . . 30
File system-level CloudWatch metrics . . . 30
Collection schedule and retention . . . 31
Generative AI security controls . . . 32
Learn about AI controls in NetApp Workload Factory . . . 32

Security-scoped AI feature overview . . . 32
AWS Bedrock overview for AI diagnostics . . . 32
Related information . . . 32
Amazon Bedrock opt-in for NetApp Workload Factory AI diagnostics . . . 32
Before you begin . . . 32
Steps . . . 33
Disable AI diagnostics . . . 33
Region and cross-region inference profiles . . . 33
AI tool boundaries for NetApp Workload Factory . . . 33
Tool safety controls . . . 33
Data retention and model training boundaries . . . 34
AI model parameters and billing for NetApp Workload Factory . . . 34
Model and parameters . . . 34
Billing and usage limits . . . 34
Ask Me AI assistant . . . 34
Ask Me security architecture for NetApp Workload Factory . . . 34
Ask Me access control for NetApp Workload Factory . . . 35
Ask Me execution modes for NetApp Workload Factory . . . 36
Ask Me privacy and availability for NetApp Workload Factory . . . 37
ONTAP operations and Lambda link (customer VPC component) . . . 38
Learn about the Lambda link for NetApp Workload Factory . . . 38
Link security architecture . . . 38
Lambda link versus NetApp Console agent . . . 39
Related information . . . 39
Lambda link ports and calls for NetApp Workload Factory . . . 39
Request types . . . 40
Outbound network boundaries . . . 40
Workload Factory calls Lambda link . . . 40
Related information . . . 40
Lambda link IAM permissions for NetApp Workload Factory . . . 40
Lambda execution role permissions . . . 41
Workload Factory invocation permissions . . . 41
Lambda link lifecycle for NetApp Workload Factory . . . 41
Lifecycle control points . . . 41
Knowledge and support . . . 42
Register with NetApp support . . . 42
Support registration overview . . . 42
Register your account for NetApp support . . . 42
Get help with FSx for ONTAP for NetApp Workload Factory . . . 44
Get support for FSx for ONTAP . . . 44
Use self-support options . . . 44
Create a case with NetApp support . . . 44
Manage your support cases (Preview) . . . 47
Legal notices for NetApp Workload Factory . . . 50
Copyright . . . 50

Trademarks 50
Patents 50
Privacy policy 50
Open source 50

Learn about information security for NetApp Workload Factory

Information security is a core part of NetApp Workload Factory design and operation. Information Security, Cloud Platform, and Storage teams can use these details to evaluate and onboard Workload Factory in a way that supports enterprise security requirements.

What Workload Factory is

Workload Factory is a SaaS life-cycle management platform designed to help you optimize and manage workloads (for example, storage, VMware migrations, EDA projects, and database environments) using Amazon FSx for NetApp ONTAP. Your workloads run in AWS.

Workload Factory uses AWS APIs for all FSx for ONTAP operations that are natively available through AWS, and ONTAP REST APIs for Workload Factory operations that are supported by the platform but not natively available through AWS APIs.

Core security principles used in this guide

Confidentiality

Protect data from unauthorized access through identity controls, least privilege, encryption, and network boundaries.

Integrity

Protect systems and configurations from unauthorized or unintended change using permission scoping, change control, and auditability.

Availability

Ensure authorized users can access the service and workloads through resilient AWS designs and operational monitoring.

Types of information covered in this guide

The following sections provide information to help you evaluate and onboard Workload Factory in a way that supports enterprise security requirements.

1. Security model and responsibilities
   - Security model at a glance
   - Shared responsibility boundaries
2. Architecture and connectivity
   - Connectivity and trust paths
   - ONTAP execution options
3. Identity, credentials, and least privilege
   - AWS account integration
   - Least privilege permission tiers

4. Data governance, privacy, and lifecycle
    - Data handling and residency
    - Account deletion checklist
5. Observability and monitoring
    - Metrics and telemetry
6. AI controls and VPC components
    - AI controls overview
    - Lambda link overview

Get started quickly

- Start with *view, planning, and analysis* (read-only) permissions and expand only as required.
- Use AWS CloudTrail to validate `sts:AssumeRole` activity for the integration role.
- Decide upfront whether you need ONTAP-native operations that require deploying a Lambda link or NetApp Console agent.
- Decide upfront whether generative AI is permitted and whether residency constraints require single-region inference profiles.

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.

Architecture and connectivity

Connectivity and trust paths for NetApp Workload Factory

NetApp Workload Factory communicates with AWS APIs, customer AWS account resources, AWS Lambda link, and Amazon Bedrock, each with its own protocols, ports, and authentication methods. These connections are organized into groups that separate the AWS management plane, the ONTAP data plane, and Lambda link traffic so you can evaluate trust boundaries independently.

Connectivity paths

Workload Factory establishes several distinct connectivity paths, each serving a specific purpose in discovering, provisioning, and managing your AWS and ONTAP resources. Some paths originate from Workload Factory itself using assumed AWS credentials, while others run through Lambda link, which operates inside your VPC to reach ONTAP management endpoints without exposing them publicly. An optional path to Amazon Bedrock supports AI-assisted diagnostics and is active only when your organization enables that feature.

The following sections describe each path, including the AWS or ONTAP APIs involved, the credentials or authentication used, and any conditions that determine whether the path is active. Understanding these paths helps you evaluate what network access and permissions Workload Factory requires, and where data crosses account or VPC boundaries.

Workload Factory to AWS APIs

Workload Factory uses `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups`, and EC2/VPC APIs for subnet and security group discovery.

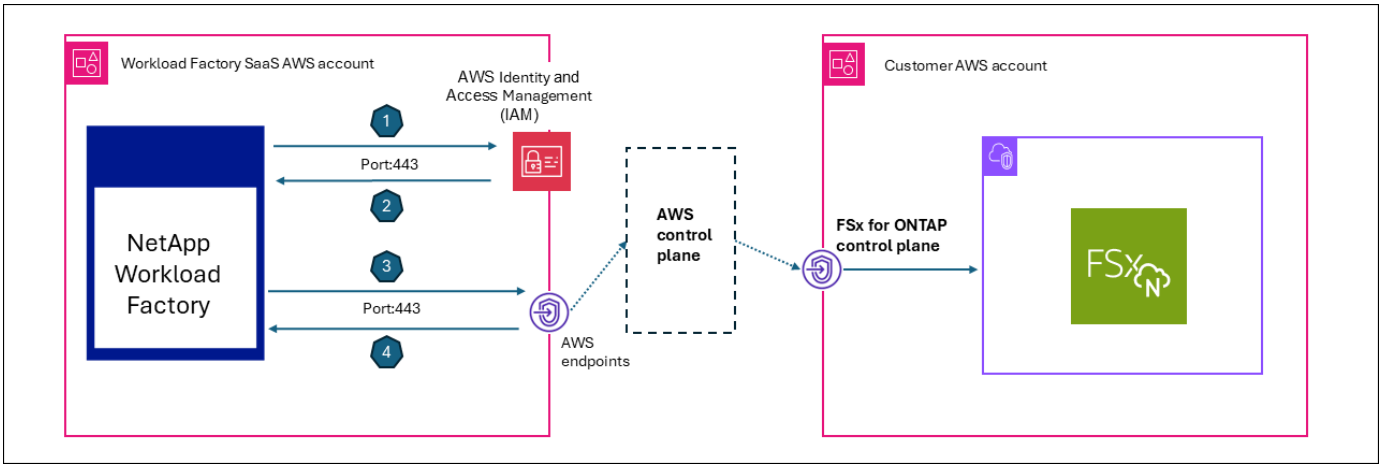
- Collector service scans about every five hours.
- CRUD operations run on demand.
- All calls use STS-assumed temporary credentials with an external ID.

Workload Factory to customer AWS account resources (orchestration and automation)

Workload Factory interacts with AWS to communicate and create resources. Orchestration and automation occurs in several ways.

- AWS CloudFormation templates: Workload Factory uses AWS CloudFormation templates to create resources like roles and file systems. For example, when you create a file system in the user interface, Workload Factory calls CloudFormation directly and redirects you to your AWS account.
- AWS API calls: Workload Factory uses AWS API calls (STS `AssumeRole`) to send API commands for FSx for ONTAP-related activities.
- AWS Lambda: Workload Factory uses CloudFormation to deploy an AWS Lambda function for the link that communicates with ONTAP.

The following diagram shows how Workload Factory uses a trust relationship between a NetApp AWS account and customer AWS accounts with FSx for ONTAP file systems.



1. Workload Factory requests AWS STS `AssumeRole`, using customer-specific external ID from the AWS IAM service.
2. AWS IAM service retrieves a role and creates a session.
3. Workload Factory issues an AWS API request with session permissions.
4. Workload Factory receives an AWS API response from the FSx for ONTAP control plane.

Lambda link to ONTAP management endpoint

Lambda links run inside the customer VPC for private subnet access without exposing ONTAP publicly. All connectivity from the link to the ONTAP management endpoint is outbound only, so no inbound connectivity or exposed endpoints are required. The link is used only for ONTAP-native operations that the Amazon FSx for NetApp ONTAP API doesn't expose.

Workload Factory uses the following protocols for volume, storage VM, and cluster operations, and for read-only diagnostics and performance data:

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

Lambda link to AWS Secrets Manager (ONTAP credential retrieval)

Used only when ONTAP admin credentials are stored in AWS Secrets Manager (alternative: credentials encrypted in Workload Factory using envelope encryption).

- The proxy-forwarder passes `x-aws-secret-arn` (Base64-encoded) in headers.
- Lambda link calls `GetSecretValue` at execution time to retrieve the password.

This keeps the password within your account boundary and prevents transmission from Workload Factory.

Workload Factory and customer components to Amazon Bedrock (AI diagnostics)

This path is used only when AI diagnostics are enabled.

- Event Analyzer uses this path for EMS analysis and latency diagnostics.
- Bedrock runs with your assumed credentials and inference profile ARN, so data does not flow to NetApp's account.

Data sent to Bedrock can include EMS event JSON, QoS statistics, volume configuration, aggregate data, and node information.
The path is active only when an inference profile is configured per organization (`ai_analyzer_config` table).

Connection groups (protocols, ports, and auth)

Group A — AWS management plane trust path (assumed credentials)

Connection	Protocol	Port	Direction	Auth	Justification
STS AssumeRole	HTTPS	443	WF → AWS STS (customer account)	IAM credentials + ExternalId	Obtain temporary cross-account credentials
FSx API (Describe/Create/Update/Delete)	HTTPS	443	WF → AWS FSx endpoint (customer region)	STS temporary credentials	File system and volume lifecycle management
EC2/VPC API	HTTPS	443	WF → AWS EC2 endpoint	STS temporary credentials	Security group, subnet, and VPC discovery
CloudFormation API	HTTPS	443	WF → AWS CFN endpoint	STS temporary credentials	Stack deployment for IAM roles and FSx provisioning
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager endpoint (customer account)	STS temporary credentials	Retrieve ONTAP admin password (when Secrets Manager-stored)
KMS Encrypt/Decrypt	HTTPS	443	WF → AWS KMS endpoint	STS temporary credentials	Volume encryption key operations

All AWS API calls use the customer's regional endpoint and can be routed through VPC endpoints if configured.

Group B — ONTAP data plane

The ONTAP data plane is always proxied through Lambda link; Workload Factory services never connect directly to ONTAP.

Connection	Protocol	Port	Direction	Auth	Justification
ONTAP REST API	HTTPS	443	Link (customer VPC) → ONTAP management LIF	Basic auth (username/password) or Secrets Manager ARN	Cluster, volume, and storage VM configuration; QoS; EMS events; ARP status
ONTAP SSH CLI	SSH	22	Link (customer VPC) → ONTAP management LIF	Password auth	Diagnostic commands (QoS stats, df, event logs, efficiency)

Routing strategy (priority order) for the proxy-forwarder:

1. Explicit `x-link-id` header: look up Lambda ARN from the database
2. Target ID (FSx file system ID): find the associated link
3. Console agent ID: route through the message broker to the Console agent

Group C — AWS Lambda link (deployed in your VPC)

Connection	Protocol	Port	Direction	Auth	Justification
Lambda Invoke	HTTPS (AWS SDK)	443	WF → AWS Lambda API (customer account)	IAM (`lambda:InvokeFunction`)	Execute ONTAP REST/SSH commands from within customer VPC
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (customer VPC) → ONTAP management LIF	Basic auth / password	Private subnet access to ONTAP without public exposure

Group D — NetApp Console Agent (EC2 in your VPC, outbound-only)

Connection	Protocol	Port	Direction	Auth	Justification
Agent polling	HTTPS	443	Console agent (customer VPC) → WF message broker	Bearer token (occm-access scope)	Long-poll for pending ONTAP commands (7-second timeout; reconnects)
Agent response	HTTPS	443	Console agent (customer VPC) → WF message broker	Bearer token	Return ONTAP command results (optionally zlib-compressed)
Console agent → ONTAP	HTTPS + SSH	443, 22	Console agent (customer VPC) → ONTAP management LIF	Basic auth / password	Execute proxied ONTAP operations

Key design: Workload Factory never initiates inbound connections to the Console agent.
Work is queued in Redis streams; the Console agent polls `GET /messagebroker/v1/requests` and responds with `POST /messagebroker/v1/responses`.

Group E — CloudFormation custom resource callbacks

Connection	Protocol	Port	Direction	Auth	Justification
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (customer) → WF Lambda (NetApp)	JWT token + reference token	Report IAM role creation status and pass back role ARN

Connection	Protocol	Port	Direction	Auth	Justification
ONTAP CloudFormation Resource Provider → Link	HTTPS	443	CloudFormation resource Lambda (customer) → Link Lambda (customer)	IAM	Create/update/delete ONTAP resources during stack operations

Summary: network requirements for your VPC

Component	Inbound	Outbound
FSx for ONTAP	Port 443 and 22 from Link Lambda or Console agent security group	N/A
Link Lambda	None	Port 443 (ONTAP, AWS APIs) and port 22 (ONTAP SSH)
Console agent EC2	None	Port 443 (WF endpoints, ONTAP, AWS APIs) and port 22 (ONTAP SSH)
VPC endpoints (optional)	N/A	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

No inbound internet access is required for any component in the customer VPC.
All connections are either outbound-initiated (Console agent polling) or invoked through AWS service APIs (Lambda Invoke).

ONTAP execution options for NetApp Workload Factory

Some NetApp Workload Factory workflows require ONTAP-native operations that aren’t exposed through AWS APIs. Workload Factory offers two execution options that keep these operations inside your AWS account boundary: a Lambda link that runs ONTAP operations from within your VPC, and a NetApp Console Agent that uses outbound-only connectivity from an EC2 instance. Both options let you perform required ONTAP operations while keeping network, credential, and lifecycle decisions within your security model.

Execution options

Lambda link (AWS Lambda in your VPC)

Executes ONTAP REST and read-only ONTAP CLI diagnostics from within your VPC, without exposing ONTAP publicly.

NetApp Console Agent (EC2 in your VPC, outbound-only)

Executes proxied ONTAP operations where the agent initiates outbound connections and Workload Factory never initiates inbound connections to the agent.

Security considerations

- Network boundaries: confirm required outbound ports (443/22) and destinations.
- Credential boundaries: decide whether ONTAP credentials are stored in Workload Factory (envelope encrypted) or referenced from AWS Secrets Manager.
- Auditability: confirm operational records for component activity and failures.
- Lifecycle management: confirm how updates and removal occur.

Related information

- Lambda link overview for NetApp Workload Factory
- Connectivity and trust paths for NetApp Workload Factory
- Encryption and key management for NetApp Workload Factory

Identity, credentials, and least privilege

AWS account integration for NetApp Workload Factory

Workload Factory uses AWS `sts:AssumeRole` to obtain temporary credentials for your AWS account, so long-term AWS access keys are not stored by the service. During onboarding, you configure an IAM role that Workload Factory can assume for approved AWS API operations, using an external ID to help prevent unauthorized cross-account access. Workload Factory then uses the resulting short-lived credentials at runtime, which AWS automatically expires after each session.

AWS account configuration

To let Workload Factory access your AWS account:

1. Deploy an IAM role in your AWS account (using CloudFormation or manually).
2. Ensure the role trust policy allows the service principal for Workload Factory to assume it, gated by an external ID.
3. Use an external ID as a unique secret identifier (UUID v4) shared exclusively between the customer and Workload Factory.

   Embed it as a condition in your IAM role trust policy (`sts:ExternalId`).

   The external ID prevents confused deputy attacks. In a cross-account access model, an attacker who discovers a customer's role ARN cannot assume that role without also possessing the corresponding external ID. AWS recommends this pattern for third-party cross-account access. For more information, refer to the AWS IAM documentation page "Access to AWS accounts owned by third parties".

   The external ID is generated once during credential onboarding and stored encrypted alongside the role ARN in a Workload Factory database.
4. Register the role ARN and external ID in Workload Factory.

Runtime

At runtime, Workload Factory assumes your IAM role to obtain short-lived credentials for each AWS API operation:

1. Workload Factory calls `sts:AssumeRole` with your role ARN and the external ID.
2. AWS returns temporary credentials (access key, secret key, and session token).
3. Workload Factory uses the temporary credentials for AWS API operations in your account.
4. Credentials expire automatically (by default, one hour).

How AWS credentials flow through NetApp Workload Factory

The AWS credential flow describes how NetApp Workload Factory handles role

identifiers, external IDs, and short-lived AWS STS credentials during onboarding and runtime operations. During one-time setup, you create an IAM role in your AWS account and configure a trust policy that requires the Workload Factory service principal and the correct external ID. At runtime, Workload Factory uses the stored role ARN and external ID to request temporary credentials scoped by a per-request session policy, and it reuses cached credentials until they expire.

One-time setup

For a one-time setup, the flow is as follows:

Steps

1. You launch a CloudFormation stack or manually create an IAM role in your AWS account.
2. The IAM role trust policy specifies two conditions:
   a. Only the service principal for Workload Factory can assume it.
   b. The caller must present the correct external ID.
3. Workload Factory stores the role ARN and external ID (encrypted) in its database.

Runtime (every API operation)

At runtime, Workload Factory uses the stored role ARN and external ID to obtain temporary AWS STS credentials for each API operation. The flow is as follows:

Steps

1. Workload Factory retrieves the stored role ARN and external ID from MySQL.
2. It checks Redis for a cached set of temporary AWS STS credentials for this role.
3. On a cache miss, Workload Factory calls `sts:AssumeRole` with the role ARN and external ID. The call includes a per-request inline session policy that restricts permissions to only the specific AWS actions needed for that operation.
4. AWS STS returns temporary credentials (access key ID, secret access key, session token) with an expiration timestamp.
5. Workload Factory caches these credentials in Redis and uses them to call the target AWS APIs.
6. On cache hit, Workload Factory skips the STS call and uses the cached credentials directly.

Session policy

Each STS call includes an inline session policy scoped to the minimum AWS actions required.

Related information

- Least privilege permission tiers

AWS credential retention for NetApp Workload Factory

Workload Factory secures credential handling through short-lived AWS STS credentials, encrypted role metadata, and bounded retention behavior. The credential model

separates retained role metadata from temporary AWS credentials used for API operations. Temporary credentials are cached only for a limited period and expire automatically under AWS enforcement. Removing a credential prevents Workload Factory from obtaining new credentials for the account, while any cached credentials expire shortly afterward.

Key behaviors

- Workload Factory does not store long-term AWS access keys.

  Workload Factory stores only a pointer (role ARN) and a shared secret (external ID). Neither grants AWS access on its own.

- Temporary AWS STS credentials have a hard maximum lifetime of one hour (AWS-enforced).

  Workload Factory caches them in Redis for at most 30 minutes before forcing a fresh STS call.

- If a cached credential set has fewer than 15 minutes remaining, Workload Factory discards it and obtains a new one.
- Credential deletion by the customer immediately revokes the ability for Workload Factory to access that account.

  The next AssumeRole call fails, and cached credentials expire within minutes.

Retention and storage summary

Data	Storage location	Retention duration	Autoexpires?	Deletion method
IAM role ARN + external ID	MySQL (encrypted at rest)	Indefinite (stored until customer explicitly removes)	No	Customer clicks "Delete credential" in the UI
Temporary AWS STS credentials (access key + secret + session token)	Redis (in-memory cache)	Maximum 30 minutes (cache TTL). Underlying STS credentials are valid for up to one hour (AWS default). Cache evicts five minutes before expiry as a safety margin.	Yes (Redis TTL auto-evicts; AWS credential expiry is enforced by AWS)	Automatic
ONTAP admin password	MySQL (AES-256-CBC envelope encryption using KMS)	Indefinite (stored until the customer removes the credential or deletes the file system)	No	Customer deletes the credential, or file system deletion triggers cleanup

Data	Storage location	Retention duration	Autoexpires?	Deletion method
Decrypted ONTAP password (plaintext)	In-memory only (never written to disk or cache)	Duration of a single request (milliseconds)	Yes (garbage collected after the request completes)	Automatic

Security controls

- External ID prevents confused deputy attacks.
- Session policies enforce per-request least privilege.
- Workload Factory refreshes short-lived temporary AWS STS credentials before risky expiry windows.
- Regional and account-type handling differs for Standard, GovCloud, and China environments.
- Workload Factory never stores long-term AWS access keys.
- Workload Factory never modifies your IAM role's permissions.
- Workload Factory never escalates beyond the permissions granted by your role policy.
- Session policies can only reduce permissions; Workload Factory never expands them.

Credential types for NetApp Workload Factory

NetAppWorkload Factory uses a split-credential model to separate AWS control-plane permissions from direct ONTAP administrative access. The AWS IAM role authenticates Workload Factory to AWS APIs for operations such as file system management, backup management, and resource discovery. ONTAP credentials authenticate direct access to the ONTAP management endpoint with a Lambda link for operations that require administrative configuration or diagnostics. Some workflows require both credential types when they combine AWS API operations with direct ONTAP management tasks.

Credential types

The following table summarizes the two credential types used in Workload Factory and their respective authentication targets.

Credential type	Authenticates to	Used for
AWS credentials (AssumeRole)	AWS APIs	All operations that go through the AWS FSx service API
ONTAP credentials (admin password)	ONTAP management endpoint	Operations that require direct ONTAP REST API or CLI access

AWS credential-only operations

These operations interact solely with AWS APIs and require only the IAM role:

- File system creation and deletion
- File system capacity and throughput changes
- Backup creation and management
- VPC, subnet, and security group discovery
- KMS key enumeration
- CloudWatch metrics retrieval
- Cost Explorer queries
- Tag management using the FSx API

ONTAP credentials-only operations

These operations communicate directly with the ONTAP management endpoint through the Lambda link and require ONTAP admin credentials:

- Volume-level QoS policy configuration
- Export policy and rule management
- storage VM protocol configuration (NFS, CIFS, iSCSI)
- igroup and LUN management
- SnapMirror (replication) configuration
- Snapshot policy management (ONTAP-level)
- Performance diagnostics (QoS statistics, latency breakdown)
- EMS event retrieval and analysis
- Anti-ransomware protection status monitoring
- FlexCache management
- Network interface (LIF) queries

Operations requiring both AWS and ONTAP credentials

Workflow	AWS credential used for	ONTAP credential used for
AI-powered event analysis	Invoke Bedrock, describe file system	Retrieve EMS events, run diagnostics using SSH
File system creation with storage VM setup	Create file system (AWS API)	Configure storage VM protocols (ONTAP REST)
Volume creation with export policy	Create volume (AWS API)	Set export policy rules (ONTAP REST)
Storage capacity management	Update file system capacity (AWS API)	Check aggregate utilization (ONTAP SSH)

Related information

- ONTAP execution options
- Lambda link overview

Credential storage options for NetApp Workload Factory

NetApp Workload Factory supports credential handling patterns that preserve least privilege and reduce exposure of ONTAP administrative secrets. AI-powered diagnostic features use read-only ONTAP credentials when available so the diagnostic agent can observe and diagnose without modifying the storage environment. You can use Workload Factory-managed encrypted storage or store the ONTAP password in AWS Secrets Manager and provide Workload Factory with a reference. The choice affects where the password is stored, how it is encrypted, and how you manage requirements such as GovCloud support and credential rotation.

Read-only ONTAP access model

For AI-powered features like event analysis and latency diagnostics, Workload Factory uses read-only ONTAP credentials when available. The read-only credential model ensures the AI diagnostic agent cannot make modifications to your storage environment—it can only observe and diagnose.

Credential storage options comparison

AWS credentials

AWS credentials are always assumed through an IAM role. Workload Factory can either manage the role information internally or reference it from AWS Secrets Manager.

Option	AWS credentials	What's stored	Encryption
Workload Factory managed	IAM role ARN + external ID	IAM role ARN + external ID	Role ARN is not a secret (stored as-is)

ONTAP credentials

Workload Factory can manage ONTAP credentials internally with encrypted storage or reference them from AWS Secrets Manager. The choice affects how the password is stored, encrypted, and rotated.

ONTAP credentials are required for Workload Factory to interact with the ONTAP file system APIs through a Lambda link.

Option	ONTAP credentials	What's stored	Encryption
Workload Factory managed	Password (encrypted)	ONTAP admin password (encrypted)	ONTAP password uses AES-256 envelope encryption
AWS Secrets Manager	Secrets Manager ARN reference	Secrets Manager ARN	Secrets ARN is not a secret (stored as-is); AWS Secrets Manager encrypts the secret in your account

Additional considerations

GovCloud requirement

Standard IAM role is used; ONTAP credentials must use Secrets Manager (password storage not permitted).

Rotation

Role policies are updated in your account. Update the ONTAP password in Workload Factory (managed option) or rotate it in AWS Secrets Manager.

Least privilege permission tiers for NetApp Workload Factory

You can restrict Workload Factory IAM permissions at any time to align with least-privilege requirements, such as limiting access to specific resources (ARNs) and applying IAM conditions, for example, tags and CIDR ranges.

Tiered permission model

Workload Factory uses a tiered permission model aligned with least privilege. You choose which capability tiers to enable when adding AWS credentials. You can start with read-only discovery and expand as needed.

Workload Factory grants all permissions through an IAM role in your AWS account, which it assumes via STS with an external ID.

Workload Factory further scopes each API call with an inline session policy.

In the Workload Factory console, the AI chat feature *Ask Me* helps you safely refine permissions by suggesting restriction options and generating an updated policy to apply in AWS.

Granting permissions

When adding AWS credentials to Workload Factory, you can choose which permission tiers to enable. You can enable or disable tiers at any time.

Tiers are cumulative: enabling a higher tier automatically enables all lower tiers.

Security controls

- External ID (confused deputy protection)
- Per-operation session policies (least privilege per request)
- Tag-based conditions (security group modifications restricted to Workload Factory-created resources)
- Secret ARN scoping (Secrets Manager access restricted to `FSxSecret*`)
- Runtime permission validation (missing action/resource reported for targeted remediation)

Permissions documentation

The primary reference for Workload Factory permissions is the permissions reference in Workload Factory setup and administration documentation. You can find information about the impacts of removing permissions

from the Storage IAM policies in this reference.

Amazon CloudWatch monitoring permissions for NetApp Workload Factory

Amazon CloudWatch monitoring permissions are optional in NetApp Workload Factory and apply only when you deploy the separate monitoring stack. The monitoring stack provides operational visibility by collecting file system metrics, publishing event logs, managing CloudWatch dashboards and alarms, and sending alert notifications through Amazon SNS. The stack also requires access to retrieve ONTAP credentials when needed for monitoring.

Required CloudWatch monitoring permissions

The following permissions are required for the optional monitoring stack:

Permission	Purpose
fsx:Describe* / fsx:ListTagsForResource	Collect file system metrics
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Manage dashboards and alarms
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	Publish event logs
sns:Publish	Send alert notifications
secretsmanager:GetSecretValue	Retrieve ONTAP credentials for monitoring

Data governance, privacy, and lifecycle

Data handling and residency for NetApp Workload Factory

NetApp Workload Factory organizes data handling into categories that describe the operational data the service processes, how each data class fits within the security model, where data is stored, how long it's retained, and whether it leaves the customer environment. The primary data classes include configuration and metadata, operational logs and events, and telemetry. Retained data can include FSx for ONTAP configuration snapshots, credential references, AI usage and cost data, audit records, and short-lived response caches. Storage and processing locations vary by data type: some information stays in the customer AWS account, while other operational data is stored in the NetApp account.

Data classes handled by Workload Factory

Workload Factory handles the following data classes:

- Configuration and metadata
- Operational logs and events
- Telemetry

Data classes retained by Workload Factory

Workload Factory keeps the following data:

- FSx configuration snapshots (refreshed on each scan)
- ONTAP credential references, or credential material encrypted with KMS envelope encryption (depending on selected credential mode)
- EDA metrics
- CloudFormation templates (7-day `Expires` header)
- AI usage and cost data
- Audit records
- Redis caches (FSx responses) with a 20-minute TTL

Where information is kept

AWS account

- ONTAP admin passwords are stored in your AWS Secrets Manager.
- Amazon Bedrock processes AI inference (EMS analysis) using your inference profile ARN through an STS-assumed role within your AWS account.

NetApp account

- FSx configurations, balance plans, ARP configurations, and AI usage limits
- Temporary AWS STS credentials (cached in Redis), response caches, locks, and deployment state
- CloudFormation/Terraform templates, well-architected configuration descriptors, and compressed reports
- AI usage metering and collector performance metrics
- EDA aggregated metrics
- Action audit trails
- OpenTelemetry traces

Region considerations

- Stored in regions where the Amazon Bedrock service is available.
- NetApp internal operates in `us-east-1` and `us-west-2`.

How long information is kept

This section summarizes retention categories. Refer to the linked pages for detailed values and policy behavior.

- Credential and temporary AWS STS credential retention:
  Credential retention for NetApp Workload Factory
- Operational metric and telemetry retention:
  Metrics and telemetry reference for NetApp Workload Factory
- Audit record retention:
  governed by the NetApp Console retention policy (not controlled by Workload Factory)

What information leaves the VPC

This section summarizes outbound data categories. Refer to linked pages for protocol-level and feature-level details.

Management plane traffic to the Workload Factory service

For management operations, FSx configuration, volume metadata, resource identifiers, and operational commands flow over HTTPS to the Workload Factory service tier.

Audit records to the NetApp Console Audit Service

Every tracked operation sends the following information:

- `accountId`
- `actionName`
- `status`
- `resourceId`
- `userId`

- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

AI analysis traffic

FSx for ONTAP Emergency Management System (EMS) events, latency data, and error logs submitted for AI diagnostics travel to Amazon Bedrock through your AWS account using your configured inference profile, so this traffic stays within your environment rather than reaching NetApp systems.

For more information about AI analysis traffic, refer to:

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

AWS service API traffic

Refer to connectivity and trust paths for NetApp Workload Factory.

Telemetry and metrics collection

Refer to the metrics and telemetry reference.

Configuration and metadata collection scope

File system level

- File system configuration (deployment type Gen1/Gen2, throughput capacity, storage capacity, storage type)
- Preferred subnet, security groups, VPC configuration
- KMS encryption key metadata
- File system tags
- File system lifecycle status
- Maintenance window settings

Volume level (comprehensive)

- Identity and state: volume name, UUID, type (rw/dp/ls), style (FlexVol/FlexGroup), state (online/offline/restricted), creation time
- Capacity: total size, used, available, physical used, percent used, SSD footprint, capacity pool footprint, inactive data bytes/percent
- Tiering: policy (all/auto/none/snapshot_only), minimum cooling days
- QoS: assigned QoS policy name

- NAS configuration: junction path, export policy assignment, UNIX permissions, security style (unix/ntfs/mixed)
- Snapshots: snapshot reserve size/percent/used, autodelete settings
- Data efficiency: compression type/state, deduplication, compaction, space savings
- Autosize: mode (grow/grow_shrink/off), min/max size, grow/shrink thresholds
- SnapLock: type (compliance/enterprise/non_snaplock), retention periods (min/max/default), autocommit period
- Clone: parent volume/snapshot/storage VM, is FlexClone, split status
- Inodes/files: maximum possible, maximum configured, used count
- Encryption: enabled/disabled status
- Access time: atime update enabled/disabled and update period
- SnapMirror: protection status, destination types (cloud/ONTAP)
- FlexGroup rebalancing: imbalance percent, max threshold
- Volume movement: destination aggregate, movement state
- FlexCache endpoint type: none/cache/origin
- Tags: ONTAP-level volume tags

Snapshot data

- Snapshot name, UUID, creation time, expiry time
- Size in bytes
- SnapMirror label
- SnapLock expiry and lock status
- State (valid/invalid/partial)
- User comments
- Snapshot policies: name, enabled status, schedule copies (count, retention period, schedule name, prefix, SnapMirror label)

Export policies

- Policy name, ID, associated storage VM
- Rules: protocol list (NFS/CIFS/FlexCache), client match patterns, read-only rules, read/write rules, superuser rules, rule index/priority
- SUID, device creation, chown mode, anonymous user mapping, NTFS UNIX security settings

S3 access points

- Lifecycle state (available/creating/deleting/failed/misconfigured)
- Creation time, ARN, alias, name
- Files owner user and type (UNIX/WINDOWS)
- Network configuration (Internet vs VPC access, VPC ID)
- AWS tags

- Metadata scan enablement, journaling enablement, CloudTrail ARN

Anti-Ransomware Protection (ARP)

Workload Factory collects both configuration status and event details:

- State per volume (enabled/disabled/dry_run/paused)
- Attack probability (none/low/moderate/high)
- Attack reports with timestamps
- Detection parameters: file extension thresholds, rename rate surge %, entropy rate surge %, file create/delete rate surge %
- Suspected files: file path, file name, file format, suspect time, associated volume

Replication / SnapMirror

- Relationship UUID, state, healthy status
- Source and destination (storage VM, path, cluster)
- Transfer statistics (bytes transferred, duration, end time, state)
- Policy (name, type: async/sync/continuous)
- Throttle setting
- Lag time
- Unhealthy reasons (message and code)
- Current transfer errors

iGroups

- Name, UUID, protocol (FCP/iSCSI/mixed), OS type
- Initiators (IQN/WWPN), connectivity state, last seen time
- LUN mappings (logical unit number, LUN details)

LUNs

- Name, UUID, serial number, OS type, enabled status
- Size, used space, thin provisioning settings
- Location (volume, node, logical unit path)
- Auto-delete setting
- Container state, mapped status, read-only status
- QoS policy
- Performance metrics (IOPS, latency, throughput per read/write/total)
- Consistency group membership

FlexCache

- Origin volume/storage VM/cluster, cache size, path

- Writeback enabled, DR cache status
- Relative sizing configuration
- Prepopulate directory paths
- Connection status between cache and origin

Storage VM level

- Name, UUID, state (running/stopped), subtype
- Protocols enabled/allowed (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- DNS servers and domains
- Name service switch configuration (passwd, group, hosts, etc.)
- IP interfaces (name, IP address, services)
- Assigned aggregates
- Anti-ransomware default volume state
- Space enforcement settings
- Peer relationships (applications, state, remote cluster/storage VM)

Aggregate / storage level

- Aggregate name, UUID, state, RAID state
- Block storage: disk count, RAID size, available/used/total space, physical used
- Cloud storage used
- Efficiency: ratio, logical used, savings
- Encryption, mirror, SnapLock settings
- Performance metrics (IOPS, latency, throughput)

Utilization metrics (EDA)

- Collection cadence: every 12 hours for capacity/throughput; every 20 minutes for latency
- Granularity: normalized to approximately 60 datapoints per time range
- Retention and storage details: Metrics and telemetry reference

Encryption and key management for NetApp Workload Factory

NetApp Workload Factory uses encryption at rest and defines clear key-management responsibilities across Workload Factory and AWS services. For Amazon FSx for NetApp ONTAP file systems, you can choose your own AWS KMS key or use the AWS-managed default key, and FSx for ONTAP performs the cryptographic operations with that key. Workload Factory also uses envelope encryption to protect stored ONTAP credentials.

KMS encryption-at-rest scope for FSx

When creating an FSx for ONTAP file system through Workload Factory, you can optionally specify your own AWS KMS key for data-at-rest encryption.
If you don’t specify a key, Workload Factory uses the AWS-managed default FSx key.

What is encrypted

All data stored on the underlying EBS volumes backing the FSx for ONTAP file system (AWS FSx encryption at rest).

Key ownership

The KMS key resides in your AWS account.

Permissions required for key selection and use

Workload Factory requires:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (to allow the FSx for ONTAP service to use the key)

Key access pattern

Workload Factory never directly encrypts or decrypts data with your KMS key. It passes the key ID to the Amazon FSx for NetApp ONTAP API during file system creation; Amazon FSx for NetApp ONTAP performs the cryptographic operations.

Credential protection (service-side envelope encryption)

When you store ONTAP credentials (admin passwords) through Workload Factory, it protects them using envelope encryption before persisting them.

Encryption method

AES-256-CBC with a unique data encryption key (DEK) per credential record.

Envelope encryption flow

1. A unique 256-bit DEK is generated per credential.
2. The DEK encrypts the credential (password).
3. The DEK itself is encrypted with a root key and stored alongside the encrypted credential.
4. The plaintext DEK is never stored.

Encryption context

Each data key is cryptographically bound to its specific credential record, preventing key reuse across records.

Alternative: AWS Secrets Manager

Instead of storing encrypted passwords in the service, you can store ONTAP credentials in AWS Secrets Manager in your own account.
Workload Factory never sees or stores the password; it passes the Secrets Manager ARN to Lambda link, which retrieves the password at runtime within your VPC.

AWS Secrets Manager is required for GovCloud accounts.

NetApp Workload Factory account deletion

Account deletion is not a self-service operation; it is an offboarding workflow that involves both the Workload Factory service and resources in your AWS account. The cleanup includes safely removing any data associated with the Workload Factory account, FSx for ONTAP file systems, credentials, links, notification channels, and related IAM, AWS Lambda, and Amazon CloudWatch resources. The operation is irreversible.

When you need to remove your Workload Factory account, you must contact NetApp Support.

Observability (logs, metrics, telemetry)

Learn about observability in NetApp Workload Factory

Observability signals help support operational monitoring, troubleshooting, and investigations. In NetApp Workload Factory, observability includes metrics, telemetry, and operational records that provide visibility into service behavior, AI usage, and actions performed through Workload Factory. Telemetry and operational records support internal monitoring and customer-facing audit visibility, and Tracker helps you review the progress, status, and details of supported operations.

Telemetry and operational records

Workload Factory uses the following telemetry and operational record types:

- OpenTelemetry traces exported via OTLP HTTP to SigNoz (internal observability)
- AI usage metering (token counts, model costs) stored in AWS Timestream
- NetApp Console audit records (action name, status, request/response metadata, timestamps)

Audit logging in Workload Factory

Workload Factory provides Tracker, a monitoring feature, so you can monitor which operations are running and when. With Tracker, you can track the progress and status of FSx for ONTAP, credentials, and link operations, review details for operation tasks and subtasks, and diagnose any issues or failures.

Several actions are available in Tracker. You can filter jobs by time frame (last 24 hours, 7 days, 14 days, or 30 days), workload, status, and user; find jobs using the search function; and download the jobs table as a CSV file.

- Monitor operations using Tracker in Workload Factory

Related information

- Metrics and telemetry for NetApp Workload Factory

Metrics and telemetry for NetApp Workload Factory

NetApp Workload Factory collects and stores volume-level and file system-level metrics in AWS CloudWatch to give you operational visibility into storage performance and capacity. Computed metrics, such as throughput, are derived from these collected values. Learn about the metric definitions, collection cadence, refresh behavior, and retention details.

Metrics included

NetApp Workload Factory uses these metrics for operational logs and events:

- Volume-level CloudWatch metrics (collected per volume)

- File system-level CloudWatch metrics (collected per file system)
- Computed metrics
- Collection schedule and retention

About operational metrics

Computed metrics use this formula:

- Throughput (Bytes/Second) = (NetworkSentBytes + NetworkReceivedBytes) / period

Refresh behavior:

- Volume and cluster metrics are refreshed every 12 hours.
- Latency metrics are refreshed every 20 minutes.
- DynamoDB items auto-expire after 14 days.

About telemetry data collection

- OpenTelemetry traces exported via OTLP HTTP to SigNoz (internal observability)
- AI usage metering (token counts, model costs) stored in AWS Timestream
- NetApp Console audit records (action name, status, request/response metadata, timestamps)

Volume-level CloudWatch metrics (collected per volume)

Metric	AWS CloudWatch name	Unit	What it measures
Volume storage capacity	StorageCapacity	Bytes	Total provisioned capacity
Storage used	StorageUsed	Bytes	Actual data stored
Data read bytes	DataReadBytes	Bytes	Read throughput
Data write bytes	DataWriteBytes	Bytes	Write throughput
Data read operations	DataReadOperations	Count	Read IOPS
Data write operations	DataWriteOperations	Count	Write IOPS
Metadata operations	MetadataOperations	Count	Metadata IOPS
Data read operation time	DataReadOperationTime	Seconds	Read latency
Data write operation time	DataWriteOperationTime	Seconds	Write latency
Metadata operation time	MetadataOperationTime	Seconds	Metadata latency

File system-level CloudWatch metrics

Metric	AWS CloudWatch name	Unit	What it measures
SSD storage capacity	StorageCapacity	Bytes	Total SSD tier capacity
SSD storage used	StorageUsed (SSD tier)	Bytes	SSD tier consumption

Metric	AWS CloudWatch name	Unit	What it measures
Capacity pool used	StorageUsed (Capacity Pool)	Bytes	Capacity pool consumption
CPU utilization	CPUUtilization	Percent	File server CPU
SSD capacity utilization	StorageCapacityUtilization	Percent	SSD tier percent used
Network throughput utilization	NetworkThroughputUtilization	Percent	Network percent utilized
Disk IOPS utilization	DiskIopsUtilization	Percent	Disk IOPS percent utilized
Disk throughput utilization	FileServerDiskThroughputUtilization	Percent	Disk throughput percent utilized
Disk IOPS utilization (server)	FileServerDiskIopsUtilization	Percent	Server disk IOPS percent utilized
Storage efficiency savings	StorageEfficiencySavings	Bytes	Space saved by efficiency
Network received	NetworkReceivedBytes	Bytes	Inbound network
Network sent	NetworkSentBytes	Bytes	Outbound network

Collection schedule and retention

Time range	Collection period	Datapoints	Storage	Retention
1 day	24 minutes	~60	DynamoDB	14 days (TTL)
1 week	~2.8 hours	~60	DynamoDB	14 days (TTL)
1 month	12 hours	~60	DynamoDB	14 days (TTL)
3 months	~1.5 days	~60	DynamoDB	14 days (TTL)
1 year	~6 days	~60	DynamoDB	14 days (TTL)

Generative AI security controls

Learn about AI controls in NetApp Workload Factory

NetApp Workload Factory includes generative AI features that accelerate diagnosis while enforcing security controls for model access, data scope, and runtime behavior.

Workload Factory enables AI diagnostics by default. You can disable generative AI features at any time through the Workload Factory **Administration** settings. Learn more about managing GenAI features.

Security-scoped AI feature overview

Workload Factory currently applies generative AI to the following features:

- Ask Me assistant (RAG with curated NetApp documentation, source-backed responses)
- Latency analysis
- EMS event analysis
- Error log analysis

AWS Bedrock overview for AI diagnostics

Workload Factory uses Amazon Bedrock for AI inference. Inference runs in your AWS account, under your configured credentials and inference profile.

Related information

- Amazon Bedrock opt-in for NetApp Workload Factory AI diagnostics
- AI tool boundaries for NetApp Workload Factory
- AI model parameters and billing for NetApp Workload Factory

Amazon Bedrock opt-in for NetApp Workload Factory AI diagnostics

NetApp Workload Factory AI diagnostics use Amazon Bedrock to analyze events, and the feature is enabled by default. Before Workload Factory can invoke the selected Bedrock model and collect diagnostic data, you must configure IAM permissions, an inference profile, and a connected Lambda link with SSH capability. If any of these components is missing or the Bedrock configuration is removed, AI diagnostics become unavailable.

AI diagnostics are enabled by default.

Before you begin

- Make sure your account includes an AWS Bedrock inference profile.
- Have a connected Lambda link with SSH capability for diagnostic data collection.

Steps

1. Grant Bedrock permissions in your IAM role:
   - `bedrock:InvokeModel`
   - `bedrock:InvokeModelWithResponseStream`
   - `bedrock:ListInferenceProfiles`
   - `bedrock:GetInferenceProfile`
2. Configure the inference profile ARN in Workload Factory settings.

If any prerequisite is missing, the system reports the specific missing component and AI features remain inactive.

Disable AI diagnostics

To disable AI diagnostics:

- Remove the Bedrock permissions from your IAM role, or
- Delete the Bedrock configuration in Workload Factory settings.

AI diagnostics become unavailable immediately, and no residual data processing occurs.

Region and cross-region inference profiles

Bedrock inference executes in the AWS region specified by your inference profile. If you use a cross-region inference profile, AWS might route the request to any region in the profile's configuration per standard AWS Bedrock behavior. Data does not leave AWS infrastructure.

AI tool boundaries for NetApp Workload Factory

NetApp Workload Factory enforces strict boundaries on how its AI features interact with your AWS and ONTAP environments, so you can trust AI-assisted diagnostics without risking unintended changes. Amazon Bedrock uses read-only AWS CLI and ONTAP CLI diagnostic tools that block mutating commands and limit output by size and execution, and any data used is only transient and not retained by NetApp Workload Factory or AWS.

Tool safety controls

Tool	Capability	Safety controls
AWS CLI (read-only)	Execute read-only AWS CLI commands (describe, list, get)	Blocks all mutating verbs (create, delete, modify, update, put, remove). Maximum 10 commands per step. Output truncated at 20 KB.
ONTAP CLI (read-only)	Execute read-only ONTAP CLI commands using SSH	Blocks all mutating verbs (delete, destroy, create, modify, move). Output truncated.

The agent cannot modify, create, or delete resources. It can only observe and diagnose.

Data retention and model training boundaries

Per AWS policy, Amazon Bedrock does not store or use your inputs and outputs to train or improve foundation models.
For on-demand inference (used by Workload Factory), AWS processes your data transiently and does not retain it after returning the response.

AI model parameters and billing for NetApp Workload Factory

NetApp Workload Factory defines the model configuration and usage and billing boundaries relevant to AI governance. The configured model uses deterministic parameters and returns structured JSON to support consistent analysis results. AWS bills Amazon Bedrock inference to your account, while Workload Factory tracks AI usage and provides per-account monthly cost visibility. These sections describe the model parameters and the limits that apply to AI consumption.

Model and parameters

Parameter	Value
Model	Anthropic Claude (using a cross-region inference profile)
Temperature	0 (deterministic, no randomness)
Max output tokens	2,048
Max reasoning steps	15 per analysis
Output format	Structured JSON (summary, severity, root cause, corrective actions)

Billing and usage limits

- AWS bills Bedrock inference to your account (your inference profile, your credentials).
- Workload Factory tracks AI usage internally.
- Workload Factory provides per-account monthly cost visibility.

Track storage costs in NetApp Workload Factory

Ask Me AI assistant

Ask Me security architecture for NetApp Workload Factory

Ask Me is a generative AI-powered assistant embedded within NetApp Workload Factory. It provides real-time, conversational support for Amazon FSx for NetApp ONTAP and Workload Factory topics. Responses are grounded in verified NetApp documentation, and Ask Me cannot access the public internet or use customer data to train the model. Multiple security layers help block malicious queries, limit responses to supported domains, and prevent user input from overriding system instructions. When Ask Me uses

tools, authorization boundaries, read-only query enforcement, an ephemeral sandbox, and audit logging help constrain and monitor execution.

You can opt out of Ask Me at any time through the Workload Factory **Administration** settings, which disables the assistant for your user account. Learn more about managing GenAI features.

RAG architecture in Ask Me

Ask Me uses retrieval-augmented generation (RAG).

- Curated knowledge base: responses are grounded in a managed corpus of verified, published NetApp documentation.
- Retrieval scoring and filtering: only sufficiently relevant content is included in the model context.
- No internet access: the model cannot fetch, browse, or scrape external content.
- Source attribution: responses include references to the source documents used.

Multi-layer prompt security

- Layer 1: Security classifier (LLM-as-a-judge) blocks malicious queries (prompt injection, privilege escalation, data exfiltration, social engineering, policy violations).

  The system logs blocked queries, and the generative model never sees them.

- Layer 2: System prompt hardening prevents user input from overriding system instructions.
- Layer 3: Domain scoping limits responses to FSx ONTAP and Workload Factory topics.
- Layer 4: Tool-use governance validates parameters and runs queries in a hardened sandbox; the model cannot execute arbitrary operations.

Model data isolation and privacy

- No model training on customer data
- Request-level isolation (no cross-tenant data leakage)
- Session-scoped conversation context with bounded history
- No persistent model memory
- Managed inference infrastructure

Tool-use and agentic security

- Authorization-scoped tools (user permission boundaries enforced)
- Strict tool execution timeouts
- Ephemeral, session-scoped sandbox for retrieved data
- Read-only query enforcement with allowlisting
- Tool call auditability with sensitive parameter scrubbing

Ask Me access control for NetApp Workload Factory

In NetApp Workload Factory, Ask Me access security centers on authenticated sessions,

user-level accountability, and protected secret handling during runtime operations. Authentication controls validate each session and associate interactions with a specific user. Sensitive credentials are retrieved from a managed secrets vault at runtime and redacted from logs. The service also applies infrastructure controls, including non-root container execution and a restricted CORS allowlist.

Authentication

- Signed JWT authentication with cryptographic validation (including audience, issuer, and algorithm checks such as RS256)
- Middleware-enforced authentication at the service boundary
- User identity scoping so interactions are attributable to a specific user

Credential protection and secret handling

- Secure vault storage: sensitive credentials used by the service are stored in a managed secrets vault and retrieved at runtime.
  No secrets are stored in application code, configuration files, or container images.
- Log scrubbing: sensitive values (credentials, tokens, passwords, access keys, certificates) are redacted from logs before they are written.

Infrastructure security

- Non-root container execution
- CORS restricted to an explicit allowlist of trusted NetApp domains

Ask Me execution modes for NetApp Workload Factory

NetApp Workload Factory provides multiple execution modes for Ask Me, each with different security and privacy characteristics. When Ask Me uses tool integrations, for example, querying the customer's own Workload Factory resources, tool execution is controlled through layered safeguards. Tool-enabled execution operates within the authenticated user's permissions and applies limits to the duration and scope of each operation. Retrieved data remains in an ephemeral session sandbox that blocks external access and is destroyed when the session ends. Independent prompt and code controls enforce read-only queries, while audit records capture tool activity with sensitive values scrubbed.

Tool execution safeguards

- Authorization-scoped tools operate within the authenticated user's permissions.
- Tool execution timeout limits long-running operations.
- Ephemeral data sandbox stores tool-retrieved data in session scope, blocks external access, file I/O, network calls, and extension loading at the engine level, and is destroyed when the session ends.
- Read-only query enforcement validates generated queries through a strict allowlist.
- Prompt-enforced and code-enforced security are applied independently.

- Tool call auditability logs tool name, parameters, timestamps, and result status with sensitive value scrubbing.

Output controls

- Token limit enforcement
- Deterministic output for classification/security-critical operations (temperature 0)
- Streaming with early termination and cleanup

Ask Me privacy and availability for NetApp Workload Factory

In NetApp Workload Factory, Ask Me privacy controls limit data exposure, keep session processing isolated, and maintain privacy boundaries for user interactions. Your inputs are processed by a managed AI service that does not use them to train or improve foundation models. Retrieved operational data remains in ephemeral, in-memory storage for the duration of the session and is not persisted or shared. A multi-model fallback chain across multiple cloud regions supports availability when the primary model is throttled or unavailable, while the same security controls apply across the fallback models.

Data handling and privacy

- User data in prompts: processed by a managed AI service that does not use your inputs to train or improve foundation models.
- Knowledge base content: curated, published NetApp documentation only; your data isn’t included.
- Operational data: retrieved only when a user queries their own resources; held in ephemeral, in-memory storage for the duration of the session and not persisted or shared.
- Audit logging: query metadata (anonymized user ID, timestamps, durations) logged, with sensitive fields scrubbed.
- Feedback data: stored separately and linked to a query ID, not to personally identifiable information beyond the anonymized user ID.

Availability and isolation controls

Ask Me employs a multi-model fallback chain across multiple cloud regions.

If the primary model is throttled or unavailable, the system can fail over to alternative models.

All models are subject to the same security controls, system prompt hardening, and isolation guarantees.

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.

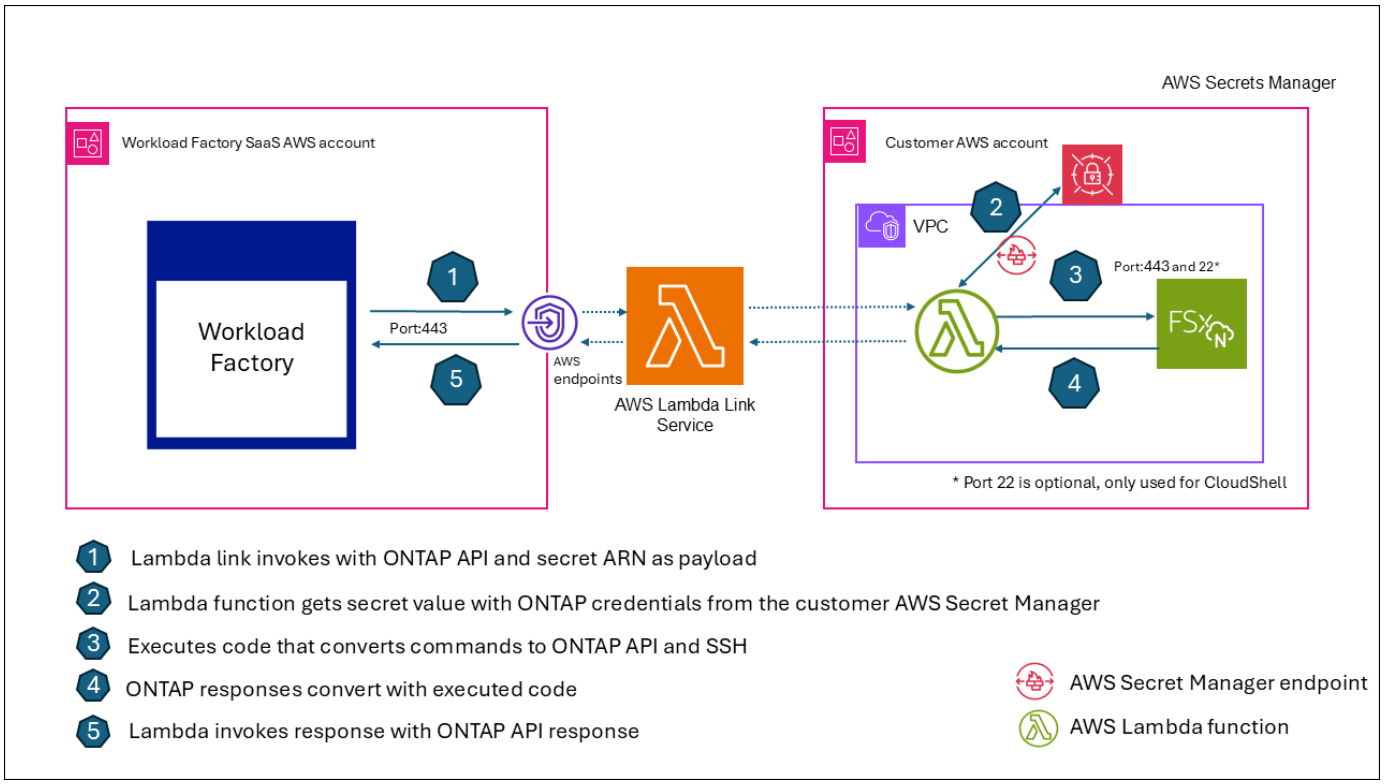
Link security architecture

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

Knowledge and support

Register with NetApp support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Workload Factory and then register for support.

Support registration is required to receive technical support specific to NetApp Workload Factory and its storage solutions and services. You must register for support from the NetApp Console, which is a separate web-based console from Workload Factory.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the Workload Factory documentation for that product.

Amazon FSx for ONTAP

Support registration overview

Registering your account ID support subscription (your 20 digit 960xxxxxxxx serial number located on the Support Resources page in the NetApp Console) serves as your single support subscription ID. Each NetApp account-level support subscription must be registered.

Registering enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to the NetApp Console as described below.

Register your account for NetApp support

To register for support and activate support entitlement, one user in your account must associate a NetApp Support Site account with their NetApp Console login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

If you're a NetApp customer with an NSS account, you simply need to register for support through the NetApp Console.

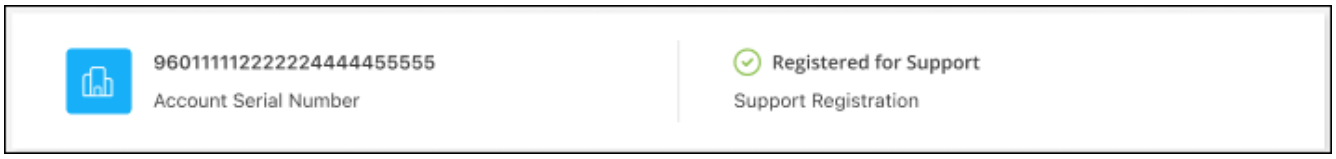
Steps

1. In the upper right of the Workload Factory console, select **Help > Support**.

   Selecting this option opens the NetApp Console in a new browser tab and loads the Support dashboard.

2. From the NetApp Console menu, select **Administration**, and then select **Credentials**.
3. Select **User Credentials**.
4. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
5. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your account is registered for support.



Note that other NetApp Console users will not see this same support registration status if they have not associated a NetApp Support Site account with their NetApp Console login. However, that doesn't mean that your NetApp account is not registered for support. As long as one user in the account has followed these steps, then your account has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your NetApp Console login.

Steps

1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the NetApp account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your NetApp Console login by completing the steps under Existing customer with an NSS account.

Brand new to NetApp

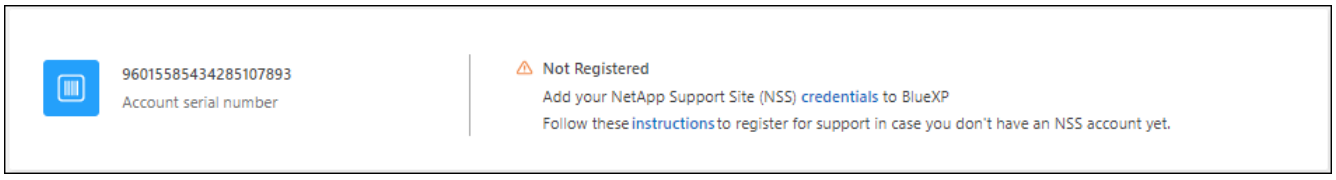
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the Workload Factory console, select **Help > Support**.

   Selecting this option opens the NetApp Console in a new browser tab and loads the Support dashboard.

2. Locate your account ID serial number from the Support Resources page.



3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your NetApp Console login by completing the steps under Existing customer with an NSS account.

Get help with FSx for ONTAP for NetApp Workload Factory

NetApp provides support for Workload Factory and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for FSx for ONTAP

For technical support related to FSx for ONTAP, its infrastructure, or any solution using the service, refer to "Getting help" in the Workload Factory documentation for that product.

Amazon FSx for ONTAP

To receive technical support specific to Workload Factory and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- Documentation

  The Workload Factory documentation that you're currently viewing.

- Knowledge base

  Search through the Workload Factory knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Workload Factory community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

To use the **Create a Case** capability, you must first register for support. associate your NetApp Support Site credentials with your Workload Factory login. Learn how to register for support.

Steps

1. In the upper right of the Workload Factory console, select **Help > Support**.

   Selecting this option opens the NetApp Console in a new browser tab and loads the Support dashboard.

2. On the **Resources** page, choose one of the available options under Technical Support:

   a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

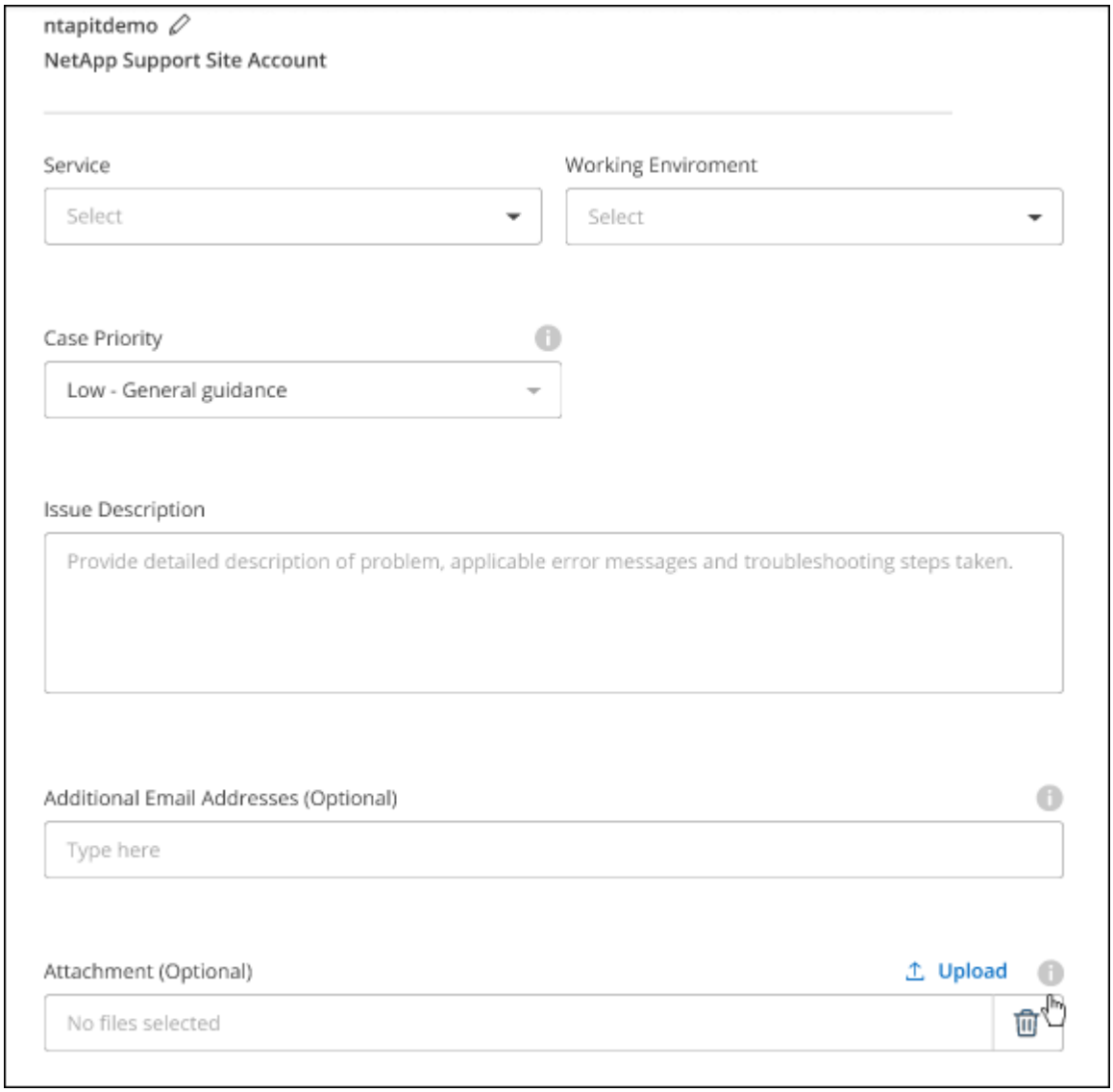
   b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

      - **Service**: Select **Workload Factory**.
      - **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

        To learn more details about these priorities, hover your mouse over the information icon next to the field name.

      - **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
      - **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.
      - **Attachment (Optional)**: Upload up to five attachments, one at a time.

        Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the NetApp Console account serial number (ie. 960xxxx) or the system serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from the NetApp Console. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

  The results in the table reflect the cases related to the view that you selected.
- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

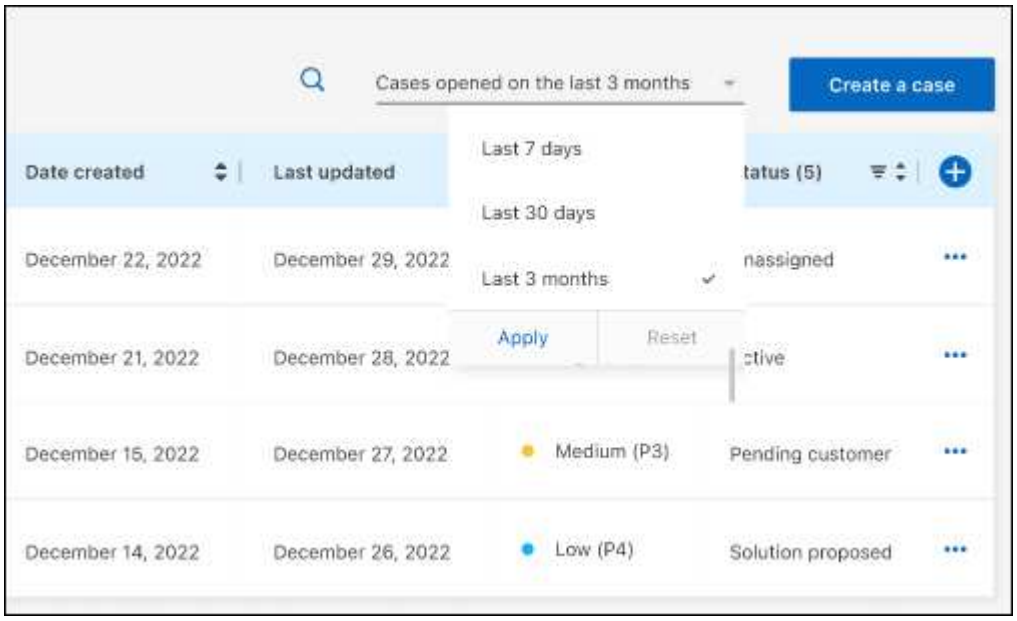
  View the steps below for more details.
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

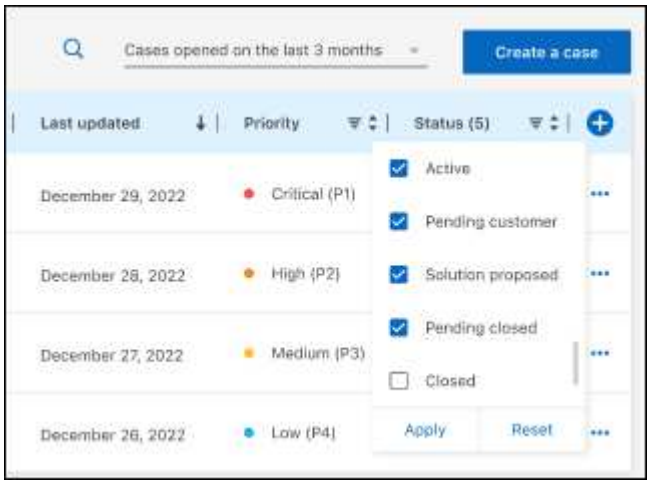
1. In the upper right of the Workload Factory console, select **Help > Support**.

   Selecting this option opens the NetApp Console a new browser tab and loads the Support dashboard.
2. Select **Case Management** and if you're prompted, add your NSS account to the NetApp Console.

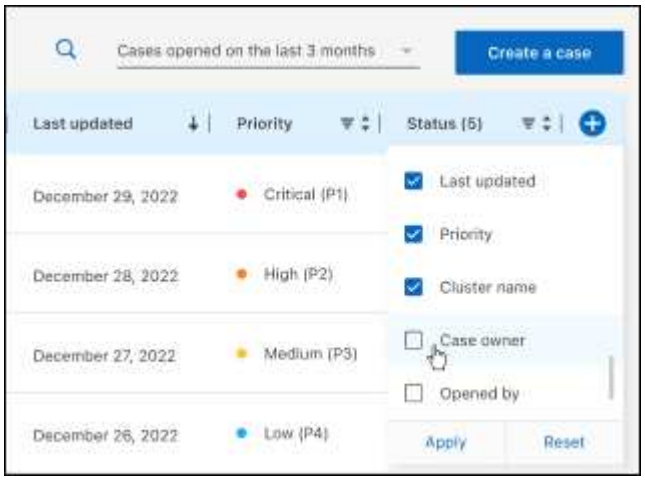
   The **Case management** page shows open cases related to the NSS account that is associated with your NetApp Console user account. This is the same NSS account that appears at the top of the **NSS management** page.
3. Optionally modify the information that displays in the table:
   - Under **Organization's cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.



- Filter the contents of the columns.



- Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.

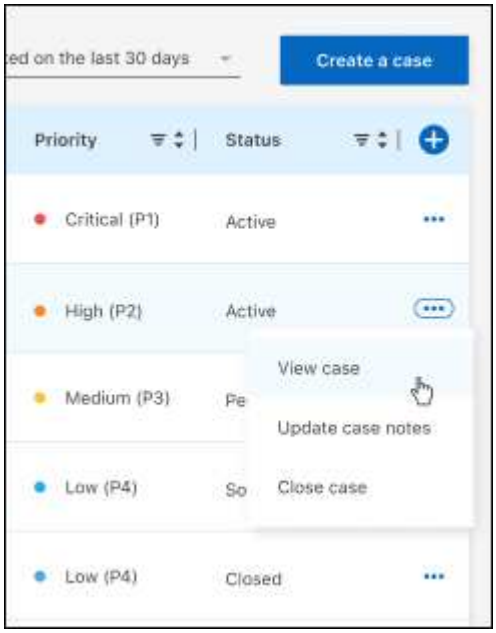


4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

   - **Close case**: Provide details about why you're closing the case and select **Close case**.



Legal notices for NetApp Workload Factory

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

NetApp Workload Factory

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.