Identity, credentials, and least privilege

Information Security for Workload Factory

NetApp
September 16, 2026

Table of Contents

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

Copyright information

Trademark information