Data governance, privacy, and lifecycle

Information Security for Workload Factory

NetApp
September 16, 2026

Table of Contents

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, WAD config 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.

Copyright information

Trademark information