Data Governance, Datenschutz und Lebenszyklus

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

Data Governance, Datenschutz und Lebenszyklus

Datenverarbeitung und Datenresidenz für NetApp Workload Factory

NetApp Workload Factory ordnet die Datenverarbeitung in Kategorien, die die vom Dienst verarbeiteten Betriebsdaten beschreiben, wie jede Datenklasse in das Sicherheitsmodell passt, wo die Daten gespeichert werden, wie lange sie aufbewahrt werden und ob sie die Kundenumgebung verlassen. Zu den primären Datenklassen gehören Konfigurations- und Metadaten, Betriebsprotokolle und -ereignisse sowie Telemetrie. Aufbewahrte Daten können FSx for ONTAP Konfigurations-Snapshots, Anmeldeinformationsreferenzen, Daten zur KI-Nutzung und zu Kosten, Audit-Datensätze und kurzlebige Antwort-Caches umfassen. Speicher- und Verarbeitungsorte variieren je nach Datentyp: Einige Informationen verbleiben im AWS-Kundenkonto, während andere Betriebsdaten im NetApp Konto gespeichert werden.

Datenklassen, die von der Workload Factory verarbeitet werden

Workload Factory verarbeitet die folgenden Datenklassen:

- Konfiguration und Metadaten
- Betriebsprotokolle und Ereignisse
- Telemetrie

Von der Workload Factory beibehaltene Datenklassen

Workload Factory speichert folgende Daten:

- FSx Konfigurationssnapshots (werden bei jedem Scan aktualisiert)
- ONTAP Anmeldeinformationen oder Anmeldeinformationen, die mit KMS-Envelope-Verschlüsselung verschlüsselt wurden (abhängig vom gewählten Anmeldeinformationsmodus)
- EDA-Metriken
- CloudFormation templates (7-Tage `Expires` Header)
- KI-Nutzungs- und Kostendaten
- Prüfprotokolle
- Redis Caches (FSx-Antworten) mit einer TTL von 20 Minuten

Wo Informationen aufbewahrt werden

AWS-Konto

- ONTAP Administratorpasswörter werden in Ihrem AWS Secrets Manager gespeichert.
- Amazon Bedrock verarbeitet KI-Inferenz (EMS-Analyse) unter Verwendung Ihres Inferenzprofil-ARN über

eine von STS angenommene Rolle innerhalb Ihres AWS-Kontos.

NetApp-Konto

- FSx Konfigurationen, Lastverteilungspläne, ARP Konfigurationen und KI-Nutzungslimits
- Temporäre AWS STS-Anmeldeinformationen (in Redis zwischengespeichert), Antwortcaches, Sperren und Bereitstellungsstatus
- CloudFormation/Terraform-Vorlagen, WAD-Konfigurationsdeskriptoren und komprimierte Berichte
- KI-Nutzungsmessung und Leistungskennzahlen des Collectors
- EDA aggregierte Metriken
- Aktionsprotokolle
- OpenTelemetry-Spuren

Regionale Überlegungen

- Gespeichert in Regionen, in denen der Amazon Bedrock Service verfügbar ist.
- NetApp internal arbeitet in `us-east-1` und `us-west-2`.

Wie lange Informationen aufbewahrt werden

Dieser Abschnitt fasst die Aufbewahrungskategorien zusammen. Detaillierte Werte und das Verhalten der Aufbewahrungsrichtlinien sind auf den verlinkten Seiten zu finden.

- Aufbewahrung von Anmeldeinformationen und temporären AWS STS-Anmeldeinformationen: "Aufbewahrung von Anmeldeinformationen für NetApp Workload Factory"
- Speicherung von Betriebskennzahlen und Telemetriedaten: "Metriken- und Telemetrie-Referenz für NetApp Workload Factory"
- Aufbewahrung von Prüfprotokollen: unterliegt der NetApp Console Aufbewahrungsrichtlinie (nicht von Workload Factory gesteuert)

Welche Informationen verlassen die VPC

Dieser Abschnitt fasst die Kategorien ausgehender Daten zusammen. Einzelheiten zu Protokoll- und Funktionsebene sind auf den verlinkten Seiten verfügbar.

Management-Plane-Datenverkehr zum Workload Factory Service

Für Managementvorgänge fließen FSx-Konfiguration, Volume-Metadaten, Ressourcenkennungen und Betriebsbefehle über HTTPS zur Workload Factory Serviceebene.

Prüfprotokolle an den NetApp Console Audit Service

Jeder überwachte Vorgang sendet die folgenden Informationen:

- `accountId`
- `actionName`
- `status`

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

KI-Analyse-Datenverkehr

FSx for ONTAP Emergency Management System (EMS)-Ereignisse, Latenzdaten und Fehlerprotokolle, die für KI-Diagnose eingereicht werden, gelangen über Ihr AWS-Konto mithilfe Ihres konfigurierten Inferenzprofils zu Amazon Bedrock, sodass dieser Datenverkehr innerhalb Ihrer Umgebung bleibt und nicht NetApp-Systeme erreicht.

Weitere Informationen zum Datenverkehr im Zusammenhang mit KI-Analysen sind verfügbar unter:

- "Übersicht der KI-Steuerung für NetApp Workload Factory"
- "Bedrock-Opt-in für NetApp Workload Factory AI-Diagnose"
- "KI-Tool-Grenzen für NetApp Workload Factory"

AWS Service-API-Verkehr

Siehe "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory".

Telemetrie und Metrikenerfassung

Siehe "Metriken und Telemetrie-Referenz".

Konfigurations- und Metadatenerfassungsbereich

Dateisystemebene

- Dateisystemkonfiguration (Bereitstellungstyp Gen1/Gen2, Durchsatzkapazität, Speicherkapazität, Speichertyp)
- Bevorzugtes Subnetz, Sicherheitsgruppen, VPC Konfiguration
- KMS-Verschlüsselungsschlüssel-Metadaten
- Dateisystem-Tags
- Lebenszyklusstatus des Dateisystems
- Einstellungen für das Wartungsfenster

Volume-Level (umfassend)

- Identität und Status: Volume-Name, UUID, Typ (rw/dp/ls), Stil (FlexVol/FlexGroup), Status (online/offline/eingeschränkt), Erstellungszeit
- Kapazität: Gesamtgröße, belegt, verfügbar, physisch belegt, prozentual belegt, SSD-Footprint, Capacity-

Pool-Footprint, inaktive Datenbytes/Prozent

- Tiering: Richtlinie (alle/automatisch/keine/nur Snapshot), Mindestkühltage
- QoS: zugewiesener QoS-Richtlinienname
- NAS-Konfiguration: Verbindungspfad, Exportrichtlinienzuweisung, UNIX-Berechtigungen, Sicherheitsstil (unix/ntfs/mixed)
- Snapshots: Snapshot-Reservegröße/Prozent/genutzt, Einstellungen für automatisches Löschen
- Dateneffizienz: Komprimierungstyp/-status, Deduplizierung, Verdichtung, Speicherplatzeinsparungen
- Automatische Größenanpassung: Modus (Vergrößern/Vergrößern-Verkleinern/Aus), minimale/maximale Größe, Schwellenwerte für Vergrößern/Verkleinern
- SnapLock: Typ (compliance/enterprise/non_snaplock), Aufbewahrungsfristen (min/max/Standard), Autocommit-Periode
- Klon: übergeordnetes Volume/Snapshot/Speicher-VM, ist FlexClone, Aufteilungsstatus
- Inodes/Dateien: maximal möglich, maximal konfiguriert, verwendet
- Verschlüsselung: aktiviert/deaktiviert Status
- Zugriffszeit: atime-Aktualisierung aktiviert/deaktiviert und Aktualisierungszeitraum
- SnapMirror: Schutzstatus, Zieltypen (Cloud/ONTAP)
- FlexGroup Neuausrichtung: Ungleichgewicht in Prozent, maximaler Schwellenwert
- Volumenbewegung: Zielaggregat, Bewegungszustand
- FlexCache Endpunkttyp: keiner/Cache/Ursprung
- Tags: ONTAP-Level Volume-Tags

Momentaufnahmedaten

- Snapshot Name, UUID, Erstellungszeit, Ablaufzeit
- Größe in Bytes
- SnapMirror Etikett
- SnapLock Ablauf- und Sperrstatus
- Status (gültig/ungültig/teilweise)
- Nutzerkommentare
- Snapshot-Richtlinien: Name, Aktivierungsstatus, geplante Kopien (Anzahl, Aufbewahrungszeitraum, Zeitplanname, Präfix, SnapMirror label)

Export-Richtlinien

- Richtlinienname, ID, zugehörige Storage-VM
- Regeln: Protokollliste (NFS/CIFS/FlexCache), Client-Match-Muster, Regeln für Nur-Lesen, Regeln für lesen/schreiben, Superuser-Regeln, Regelindex/Priorität
- SUID, Geräteerstellung, chown-Modus, anonyme Benutzerzuordnung, NTFS-UNIX-Sicherheitseinstellungen

S3 Access Points

- Lebenszyklusstatus (verfügbar/erstellung/löschung/fehlgeschlagen/falsch konfiguriert)

- Erstellungszeitpunkt, ARN, Alias, Name
- Dateibesitzer, Benutzer und Typ (UNIX/WINDOWS)
- Netzwerkkonfiguration (Internet- vs VPC-Zugriff, VPC-ID)
- AWS-Tags
- Metadaten-Scan-Aktivierung, Journaling-Aktivierung, CloudTrail ARN

Anti-Ransomware-Schutz (ARP)

Workload Factory erfasst sowohl den Konfigurationsstatus als auch Ereignisdetails:

- Status pro Volume (aktiviert/deaktiviert/dry_run/pausiert)
- Angriffswahrscheinlichkeit (keine/niedrig/mittel/hoch)
- Angriffsberichte mit Zeitstempeln
- Erkennungsparameter: Schwellenwerte für Dateierweiterungen, Anstieg der Umbenennungsrate (%), Anstieg der Entropierate (%), Anstieg der Datei-Erstellungs-/Löschrate (%)
- Verdächtige Dateien: Dateipfad, Dateiname, Dateiformat, verdächtiger Zeitpunkt, zugehöriges Volume

Replikation / SnapMirror

- Beziehungs-UUID, Status, Gesundheitszustand
- Quelle und Ziel (Storage-VM, Pfad, Cluster)
- Statistiken (übertragene Bytes, Dauer, Endzeit, Status)
- Richtlinie (Name, Typ: asynchron/synchron/kontinuierlich)
- Drosselungseinstellung
- Verzögerungszeit
- Unhealthy-Gründe (Nachricht und Code)
- Aktuelle Übertragungsfehler

iGroups

- Name, UUID, Protokoll (FCP/iSCSI/gemischt), Betriebssystemtyp
- Initiatoren (IQN/WWPN), Verbindungsstatus, Zeitpunkt des letzten Kontakts
- LUN-Zuordnungen (logische Einheitennummer, LUN-Details)

LUNs

- Name, UUID, Seriennummer, Betriebssystemtyp, Aktivierungsstatus
- Größe, belegter Speicherplatz, Thin Provisioning-Einstellungen
- Speicherort (Volume, Knoten, logischer Einheitenpfad)
- Einstellung für automatisches Löschen
- Containerstatus, zugeordneter Status, schreibgeschützter Status
- QoS Richtlinie
- Leistungskennzahlen (IOPS, Latenz, Durchsatz pro lesen/schreiben/gesamt)

- Mitgliedschaft in der Konsistenzgruppe

FlexCache

- Ursprungsvolume/Speicher-VM/Cluster, Cache-Größe, Pfad
- Writeback aktiviert, DR Cache-Status
- Konfiguration zur relativen Größenbestimmung
- Verzeichnispfade vorbelegen
- Verbindungsstatus zwischen Cache und Ursprung

Storage VM-Ebene

- Name, UUID, Status (läuft/stoppt), Subtyp
- Aktivierte/zugelassene Protokolle (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- DNS-Server und Domänen
- Konfiguration des Name-Service-Switch (passwd, group, hosts usw.)
- IP-Schnittstellen (Name, IP-Adresse, Services)
- Zugewiesene Aggregate
- Standardmäßiger Volume-Status für Anti-Ransomware
- Einstellungen zur Speicherplatzüberwachung
- Peer-Beziehungen (Anwendungen, Status, Remote-Cluster/Speicher-VM)

Aggregat-/Speicherebene

- Aggregatname, UUID, Status, RAID Status
- Blockspeicher: Anzahl der Festplatten, RAID-Größe, verfügbarer/belegter/gesamter Speicherplatz, physisch genutzter Speicherplatz
- Cloud-Speicher verwendet
- Effizienz: Verhältnis, logisch verwendet, Einsparungen
- Verschlüsselung, Spiegelung, SnapLock Einstellungen
- Leistungskennzahlen (IOPS, Latenz, Durchsatz)

Nutzungsmetriken (EDA)

- Erfassungsintervall: alle 12 Stunden für Kapazität/Durchsatz; alle 20 Minuten für Latenz
- Granularität: normalisiert auf ca. 60 Datenpunkte pro Zeitbereich
- Details zur Aufbewahrung und Speicherung: "Metriken und Telemetrie Referenz"

Verschlüsselung und Schlüsselverwaltung für NetApp Workload Factory

NetApp Workload Factory verwendet Verschlüsselung ruhender Daten und definiert klare Verantwortlichkeiten für das Schlüsselmanagement innerhalb von Workload Factory und AWS Services. Für Amazon FSx for NetApp ONTAP Dateisysteme kann ein eigener AWS

KMS Schlüssel gewählt oder der von AWS verwaltete Standardschlüssel verwendet werden, und FSx for ONTAP führt die kryptografischen Operationen mit diesem Schlüssel durch. Workload Factory verwendet außerdem Envelope Verschlüsselung zum Schutz gespeicherter ONTAP Anmeldeinformationen.

KMS Verschlüsselung ruhender Daten für FSx

Beim Erstellen eines FSx for ONTAP Dateisystems mit Workload Factory kann optional ein eigener AWS KMS-Schlüssel für die Verschlüsselung ruhender Daten angegeben werden. Wird kein Schlüssel angegeben, verwendet Workload Factory den von AWS verwalteten Standard-FSx-Schlüssel.

Was ist verschlüsselt

Alle Daten, die auf den zugrunde liegenden EBS-Volumes gespeichert sind, die das FSx for ONTAP Dateisystem unterstützen (AWS FSx Verschlüsselung im Ruhezustand).

Schlüsselbesitz

Der KMS-Schlüssel befindet sich in Ihrem AWS-Konto.

Für die Auswahl und Verwendung von Schlüsseln sind Berechtigungen erforderlich.

Workload Factory benötigt:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (um dem FSx for ONTAP Dienst die Verwendung des Schlüssels zu ermöglichen)

Schlüsselzugriffsmuster

Workload Factory verschlüsselt oder entschlüsselt Daten niemals direkt mit Ihrem KMS-Schlüssel. Die Schlüssel-ID wird während der Dateisystemerstellung an die Amazon FSx for NetApp ONTAP API übergeben; Amazon FSx for NetApp ONTAP führt die kryptografischen Operationen durch.

Schutz der Anmeldeinformationen (dienstseitige Umschlagverschlüsselung)

Wenn Sie ONTAP Zugangsdaten (Administratorpasswörter) über Workload Factory speichern, werden diese vor der Speicherung mittels Envelope-Verschlüsselung geschützt.

Verschlüsselungsmethode

AES-256-CBC mit einem eindeutigen Datenverschlüsselungsschlüssel (DEK) pro Anmeldeinformationsdatensatz.

Ablauf der Hüllkurvenverschlüsselung

1. Für jede Anmeldeinformation wird ein eindeutiger 256-Bit-DEK generiert.
2. Der DEK verschlüsselt die Anmeldeinformationen (Passwort).
3. Der DEK selbst ist mit einem Root-Schlüssel verschlüsselt und wird zusammen mit den verschlüsselten Anmeldeinformationen gespeichert.
4. Der Klartext-DEK wird niemals gespeichert.

Verschlüsselungskontext

Jeder Datenschlüssel ist kryptografisch an seinen spezifischen Anmeldeinformationsdatensatz gebunden, wodurch eine Wiederverwendung des Schlüssels über mehrere Datensätze hinweg verhindert wird.

Alternative: AWS Secrets Manager

Anstatt verschlüsselte Passwörter im Dienst zu speichern, können Sie ONTAP Anmeldeinformationen im AWS Secrets Manager in Ihrem eigenen Konto speichern. Workload Factory sieht oder speichert das Passwort nie, sondern übergibt den Secrets Manager ARN an Lambda link, das das Passwort zur Laufzeit innerhalb Ihrer VPC abruft.

AWS Secrets Manager ist für GovCloud-Konten erforderlich.

NetApp Workload Factory Kontolöschung

Die Kontolöschung ist keine Selbstbedienungsaktion, sondern ein Offboarding-Workflow, der sowohl den Workload Factory Service als auch Ressourcen in Ihrem AWS-Konto umfasst. Die Bereinigung umfasst das sichere Entfernen aller mit dem Workload Factory Konto, FSx for ONTAP Dateisystemen, Anmeldeinformationen, Verknüpfungen, Benachrichtigungskanälen und zugehörigen IAM, AWS Lambda und Amazon CloudWatch Ressourcen verbundenen Daten. Der Vorgang ist irreversibel.

Wenn Sie Ihr Workload Factory Konto entfernen müssen, müssen Sie"Den NetApp Support kontaktieren."