Informationssicherheit für NetApp Workload Factory

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

Informationen zur Informationssicherheit für NetApp Workload Factory

Informationssicherheit ist ein zentraler Bestandteil des NetApp Workload Factory Designs und Betriebs. Teams für Informationssicherheit, Cloud-Plattform und Speicher können diese Details nutzen, um die Workload Factory so zu evaluieren und zu integrieren, dass die Sicherheitsanforderungen des Unternehmens unterstützt werden.

Was Workload Factory ist

Workload Factory ist eine SaaS-Lifecycle-Management-Plattform, die dazu entwickelt wurde, Sie bei der Optimierung und Verwaltung von Workloads (zum Beispiel Speicher, VMware-Migrationen, EDA-Projekte und Datenbankumgebungen) mit Amazon FSx for NetApp ONTAP zu unterstützen. Ihre Workloads laufen in AWS.

Workload Factory verwendet AWS APIs für alle FSx for ONTAP Operationen, die nativ über AWS verfügbar sind, und ONTAP REST APIs für Workload Factory Operationen, die von der Plattform unterstützt werden, aber nicht nativ über AWS APIs verfügbar sind.

In diesem Leitfaden verwendete Kernsicherheitsprinzipien

Vertraulichkeit
: Daten werden durch Identitätskontrollen, das Prinzip der minimalen Berechtigungen, Verschlüsselung und Netzwerkgrenzen vor unberechtigtem Zugriff geschützt.

Integrität
: Systeme und Konfigurationen werden durch Berechtigungs-Scoping, Änderungskontrolle und Auditierbarkeit vor unautorisierten oder unbeabsichtigten Änderungen geschützt.

Verfügbarkeit
: Es wird sichergestellt, dass autorisierte Benutzer über resiliente AWS-Designs und operative Überwachung auf den Service und die Workloads zugreifen können.

In diesem Leitfaden behandelte Informationsarten

Die folgenden Abschnitte enthalten Informationen, die bei der Bewertung und Integration von Workload Factory unterstützen, sodass die Sicherheitsanforderungen von Unternehmen erfüllt werden.

1. Sicherheitsmodell und Verantwortlichkeiten
   - "Sicherheitsmodell im Überblick"
   - "Grenzen der gemeinsamen Verantwortung"
2. Architektur und Konnektivität
   - "Konnektivitäts- und Vertrauenspfade"
   - "ONTAP Ausführungsoptionen"
3. Identität, Anmeldeinformationen und das Prinzip der minimalen Berechtigungen
   - "AWS Konto-Integration"
   - "Berechtigungsstufen mit geringsten Rechten"

4. Data Governance, Datenschutz und Lebenszyklus
    - "Datenverarbeitung und Datenresidenz"
    - "Checkliste zur Kontolöschung"
5. Beobachtbarkeit und Überwachung
    - "Metriken und Telemetrie"
6. KI-Steuerungen und VPC-Komponenten
    - "Übersicht der KI-Steuerungen"
    - "Lambda Link Übersicht"

Schneller Einstieg

- Mit den Berechtigungen *view, planning, and analysis* (nur Leserechte) beginnen und nur bei Bedarf erweitern.
- AWS CloudTrail kann verwendet werden, um die `sts:AssumeRole`Aktivität für die Integrationsrolle zu validieren.
- Im Voraus sollte festgelegt werden, ob ONTAP-native Vorgänge benötigt werden, die die Bereitstellung eines Lambda-Links oder eines NetApp Console Agenten erfordern.
- Im Vorfeld festlegen, ob generative KI zulässig ist und ob Aufenthaltsbeschränkungen die Verwendung von Inferenzprofilen für einzelne Regionen erfordern.

Sicherheitsmodell und Verantwortlichkeiten

Informationen zum Sicherheitsmodell für NetApp Workload Factory

NetApp Workload Factory ist eine SaaS-Steuerungsebene, die bei der Verwaltung und Optimierung von Workloads unterstützt, die auf Amazon FSx for NetApp ONTAP in Ihrer AWS-Umgebung ausgeführt werden. Die Sicherheitsergebnisse hängen von der gemeinsamen Verantwortung zwischen NetApp, AWS und Ihrem Unternehmen ab.

Sicherheitsmodell auf hoher Ebene

- Workload Factory verwendet ein IAM-Rollenübernahmemodell, um temporäre AWS STS-Anmeldeinformationen zu erhalten, um AWS-APIs in Ihrem Konto aufzurufen.
- Einige Workflows erfordern ONTAP-native Operationen, die nicht über AWS-APIs bereitgestellt werden. Diese Operationen können innerhalb Ihrer VPC mithilfe von kundenseitig bereitgestellten Ausführungskomponenten (zum Beispiel Lambda link) ausgeführt werden.
- Beobachtbarkeitssignale (Metriken, Telemetriedaten und Betriebsaufzeichnungen) unterstützen die Betriebsüberwachung und Untersuchungen.

Wichtige Prüfungsfragen

- Welche Zugriffsrechte benötigt Workload Factory für Ihr AWS-Konto (Rollenvertrauensstellung + Berechtigungen)?
- Welche Ausführungspfade gelten für Ihre geplanten Workflows (nur AWS API oder ONTAP native Operationen über eine VPC-Komponente)?
- Welche Datenkategorien werden verarbeitet (Konfiguration/Metadaten, Betriebsprotokolle/Ereignisse, Telemetrie) und wo werden sie gespeichert?
- Welche Überwachungssignale gibt es und welche Aufbewahrungseigenschaften haben sie?

Was kommt als Nächstes

- "Gemeinsame Verantwortungsgrenzen für NetApp Workload Factory"
- "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory"
- "Berechtigungsstufen mit minimalen Rechten für NetApp Workload Factory"

Gemeinsame Verantwortungsgrenzen für NetApp Workload Factory

Die Sicherheitsverantwortung der NetApp Workload Factory ist zwischen NetApp (SaaS-Betrieb), AWS (Cloud-Infrastruktur und Managed Services) und Ihnen (Kundenkonfiguration) aufgeteilt. Das Verständnis darüber, wo die Verantwortung der einzelnen Parteien beginnt und endet, unterstützt eine korrekte Konfiguration Ihrer AWS-Umgebung und hilft, Sicherheitslücken zu vermeiden. Diese Abgrenzungen verdeutlichen, was NetApp betreibt, was AWS absichert und was von Ihnen selbst

konfiguriert und gewartet werden muss.

NetApp Verantwortlichkeiten (Service-Seite)

NetApp ist für den Betrieb und die Sicherheit der Workload Factory SaaS Plattform verantwortlich. Dies umfasst die service-seitige Verwaltung gespeicherter Konfigurationsreferenzen und Betriebsdaten.

AWS Verantwortlichkeiten (Cloud-Plattform)

AWS ist verantwortlich für die Sicherheit der Cloud-Infrastruktur und der verwalteten Dienste, die von Ihrer Bereitstellung und Ihren Workflows verwendet werden (z. B. IAM/STS, FSx für ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda und Netzwerkprimitive).

Kundenverantwortlichkeiten (Ihre Konfiguration)

Sie sind verantwortlich für:

- AWS IAM Rollen, Vertrauensrichtlinien und Berechtigungen nach dem Prinzip der minimalen Berechtigungen
- VPC-Steuerung (Subnetze, Sicherheitsgruppen, Routing, Endpunkte und Egress)
- Verwaltung von Anmeldeinformationen (einschließlich ONTAP Anmeldeinformationen, falls dies für Ihre Workflows erforderlich ist)
- Entscheidungen zur Verschlüsselung und Schlüsselverwaltung (z. B. optionale vom Kunden verwaltete KMS-Schlüssel für FSx für ONTAP)
- Überwachung, Alarmierung, Aufbewahrungsrichtlinien und Prozesse zur Reaktion auf Sicherheitsvorfälle

Zu erfassende Beweise

- IAM-Rollen-Vertrauensbeziehung (einschließlich externer ID-Bedingung)
- Auswahl der IAM-Berechtigungsstufe und Richtlinienartefakte
- Entscheidung über die Netzwerkgrenze (nur AWS API vs VPC-Ausführungskomponente wie Lambda-Link)
- Beobachtbarkeitsentscheidungen und Erwartungen an die Aufbewahrung
- Entscheidung zur KI-Aktivierung (KI-Diagnose ist standardmäßig aktiviert, sofern nicht explizit deaktiviert)

NetApp Workload Factory Onboarding-Sicherheitsworkflow

Das Onboarding bei NetApp Workload Factory stellt einen sicheren Zugriff auf Ihre AWS-Umgebung her, bevor Sie das Produkt nutzen. Der Prozess kombiniert die AWS-Trust-Konfiguration, die Festlegung des Berechtigungsumfangs, die Einrichtung der Konnektivität, die Überprüfung der Observierbarkeit und optional die Aktivierung von KI-Diagnosefunktionen.

Schritt 1: Die Onboarding-Strategie festlegen

- AWS-Konten und Umgebungsgrenzen identifizieren (zum Beispiel Trennung zwischen Produktions- und Nicht-Produktionsumgebungen).
- Erforderliche Arbeitsabläufe identifizieren (Read-only Discovery vs Bereitstellung vs ONTAP-native

Vorgänge).

- Ob VPC-Ausführungskomponenten (zum Beispiel Lambda Link) bereitgestellt werden, hängt von den Anforderungen des Workflows ab.
- Es kann festgelegt werden, ob die KI Diagnose aktiviert wird (standardmäßig aktiviert).

Verwandte Informationen

- "Anmeldeinformationstypen"
- "Lambda Link Übersicht"
- "Übersicht der KI-Steuerungen"

Schritt 2: AWS-Vertrauensstellung und Zugriff herstellen

1. Eine IAM-Rolle in Ihrem AWS-Konto bereitstellen.
2. Gate-Rollenübernahme mithilfe einer externen ID in der Vertrauensrichtlinie.
3. Die Rollen-ARN und die externe ID in Workload Factory registrieren.

Verwandte Informationen

"AWS Konto-Integration"

Schritt 3: Berechtigungen nach dem Prinzip der minimalen Rechtevergabe anwenden

1. Wählen Sie die minimale Berechtigungsstufe aus, die Ihre gewünschten Workflows unterstützt.
2. Es wird validiert, dass sitzungsbezogene Richtlinien pro Anfrage die Aktionen auf die jeweils durchgeführte Operation beschränken.

Verwandte Informationen

"Berechtigungsstufen mit minimalen Rechten für NetApp Workload Factory".

Schritt 4: Konnektivität und VPC-Grenzen konfigurieren (falls erforderlich)

1. Erforderliche Netzwerkpfade zu den AWS-Endpunkten validieren.
2. Wenn ONTAP-native Operationen benötigt werden, sollte die entsprechende Ausführungsoption in Ihrer VPC bereitgestellt und validiert werden.

Verwandte Informationen

- "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory"
- "ONTAP Ausführungsoptionen für NetApp Workload Factory"

Schritt 5: Überprüfung der Beobachtbarkeit

1. Es wird bestätigt, dass Metriken und Telemetriedaten wie erwartet erfasst und gespeichert werden.
2. Es sollte sichergestellt sein, dass auf die erforderlichen Betriebsdaten für die Fehlersuche und Untersuchungen zugegriffen werden kann.

Verwandte Informationen

- "Überblick über die Observability für NetApp Workload Factory"

- "Metriken und Telemetrie für NetApp Workload Factory"

Schritt 6: KI Diagnose (optional)

KI Diagnose ist standardmäßig aktiviert. Bei Aktivierung ist zu prüfen, ob die Voraussetzungen erfüllt sind und die Berechtigungen auf das erforderliche Minimum beschränkt werden.

Verwandte Informationen

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

Compliance und Sicherheitsstatus für NetApp Workload Factory

NetApp Workload Factory wurde mit Compliance und Sicherheit als zentrale Prioritäten entwickelt. Alle Workloads in Workload Factory laufen auf Amazon FSx for NetApp ONTAP. Zusätzlich zu "AWS Sicherheitsfunktionen" verfügt NetApp Workload Factory über "SOC2 Typ 1, SOC2 Typ 2 und HIPAA-Konformität".

Amazon FSx for NetApp ONTAP for NetApp Workload Factory ist eine "AWS Lösung für die Bereitstellung von Unternehmensanwendungen" Lösung und folgt den AWS Well-Architected Best Practices.

Architektur und Konnektivität

Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory

NetApp Workload Factory kommuniziert mit AWS-APIs, kundenspezifischen AWS-Kontoressourcen, AWS Lambda Link und Amazon Bedrock, jeweils mit eigenen Protokollen, Ports und Authentifizierungsmethoden. Diese Verbindungen sind in Gruppen organisiert, die die AWS Management-Ebene, die ONTAP Datenebene und den Lambda Link-Datenverkehr voneinander trennen, sodass Vertrauensgrenzen unabhängig bewertet werden können.

Verbindungspfade

Workload Factory richtet mehrere separate Verbindungspfade ein, die jeweils einem spezifischen Zweck bei der Erkennung, Bereitstellung und Verwaltung Ihrer AWS und ONTAP Ressourcen dienen. Einige Pfade gehen direkt von Workload Factory aus und verwenden angenommene AWS-Anmeldeinformationen, während andere über Lambda Link laufen, das innerhalb Ihrer VPC ausgeführt wird, um ONTAP Management-Endpunkte zu erreichen, ohne diese öffentlich zugänglich zu machen. Ein optionaler Pfad zu Amazon Bedrock unterstützt KI-gestützte Diagnose und ist nur aktiv, wenn Ihre Organisation diese Funktion aktiviert.

Die folgenden Abschnitte beschreiben jeden Pfad, einschließlich der beteiligten AWS- oder ONTAP-APIs, der verwendeten Anmeldeinformationen oder Authentifizierung sowie aller Bedingungen, die bestimmen, ob der Pfad aktiv ist. Das Verständnis dieser Pfade unterstützt die Bewertung, welcher Netzwerkzugriff und welche Berechtigungen von Workload Factory benötigt werden und wo Daten Konto- oder VPC-Grenzen überschreiten.

Workload Factory zu AWS APIs

Workload Factory verwendet `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` und EC2/VPC APIs zur Ermittlung von Subnetzen und Sicherheitsgruppen.

- Der Collector-Service scannt etwa alle fünf Stunden.
- CRUD-Operationen werden bei Bedarf ausgeführt.
- Alle Aufrufe verwenden von STS angenommene temporäre Anmeldeinformationen mit einer externen ID.

Workload Factory zu kundenspezifischen AWS-Kontoressourcen (Orchestrierung und Automatisierung)

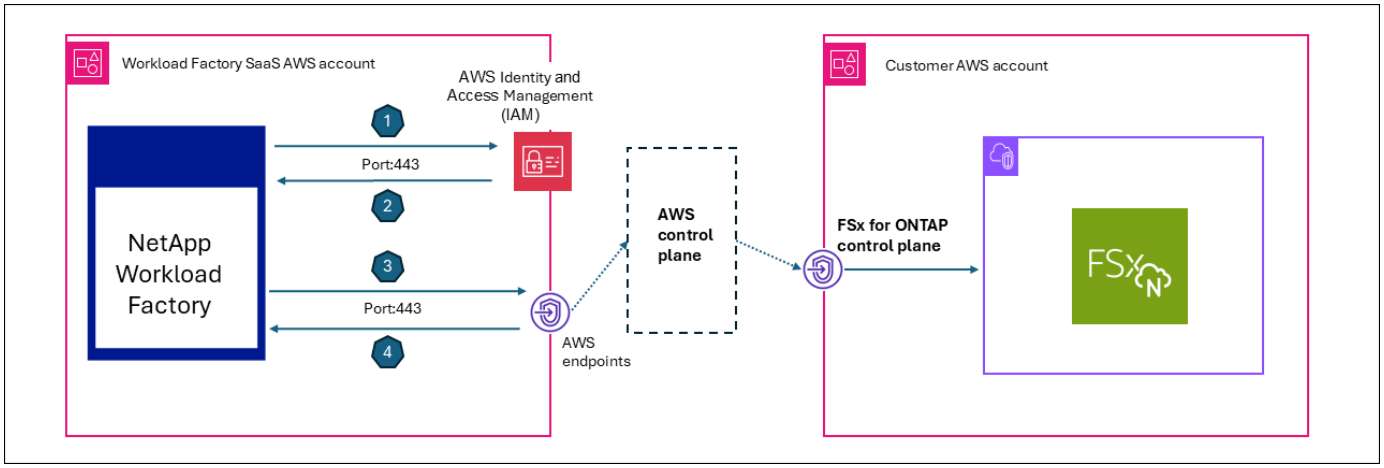
Workload Factory interagiert mit AWS, um zu kommunizieren und Ressourcen zu erstellen. Orchestrierung und Automatisierung erfolgen auf verschiedene Weise.

- AWS CloudFormation Vorlagen: Workload Factory verwendet AWS CloudFormation Vorlagen, um Ressourcen wie Rollen und Dateisysteme zu erstellen. Beispielsweise wird beim Erstellen eines Dateisystems über die Benutzeroberfläche Workload Factory CloudFormation direkt aufgerufen und eine Weiterleitung zu Ihrem AWS-Konto erfolgt.
- AWS API-Aufrufe: Workload Factory verwendet AWS API-Aufrufe (STS `AssumeRole`), um API-Befehle für

FSx for ONTAP-bezogene Aktivitäten zu senden.

- AWS Lambda: Workload Factory verwendet CloudFormation, um eine AWS Lambda-Funktion für die Verbindung bereitzustellen, die mit ONTAP kommuniziert.

Das folgende Diagramm zeigt, wie Workload Factory eine Vertrauensbeziehung zwischen einem NetApp AWS-Konto und AWS-Kundenkonten mit FSx for ONTAP Dateisystemen nutzt.



1. Workload Factory fordert AWS STS `AssumeRole`an, wobei die kundenspezifische externe ID aus dem AWS IAM-Service verwendet wird.
2. Der AWS IAM Service ruft eine Rolle ab und erstellt eine Sitzung.
3. Workload Factory sendet eine AWS API-Anfrage mit Sitzungsberechtigungen.
4. Workload Factory empfängt eine AWS API-Antwort von der FSx for ONTAP Steuerungsebene.

Lambda-Verbindung zum ONTAP Management-Endpunkt

Lambda-Links laufen innerhalb der Kunden-VPC für den Zugriff auf das private Subnetz, ohne ONTAP öffentlich zugänglich zu machen. Die gesamte Verbindung vom Link zum ONTAP Management-Endpunkt ist ausschließlich ausgehend, sodass keine eingehende Konnektivität oder freigegebene Endpunkte erforderlich sind. Der Link wird nur für ONTAP native Operationen verwendet, die die Amazon FSx for NetApp ONTAP API nicht bereitstellt.

Workload Factory verwendet die folgenden Protokolle für Volume-, Storage-VM- und Clusteroperationen sowie für schreibgeschützte Diagnose- und Leistungsdaten:

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

Lambda-Verbindung zu AWS Secrets Manager (ONTAP-Anmeldeinformationen-Abruf)

Wird nur verwendet, wenn ONTAP Administratoranmeldeinformationen im AWS Secrets Manager gespeichert sind (Alternative: Anmeldeinformationen, die in der Workload Factory mit Envelope-Verschlüsselung verschlüsselt werden).

- Der Proxy-Forwarder übergibt `x-aws-secret-arn` (Base64-kodiert) in Headern.
- Lambda-Link-Aufrufe `GetSecretValue` zur Ausführungszeit zum Abrufen des Passworts.

Dadurch bleibt das Passwort innerhalb Ihres Kontobereichs und wird nicht von Workload Factory übertragen.

Workload Factory und kundenspezifische Komponenten zu Amazon Bedrock (KI-Diagnose)

Dieser Pfad wird nur verwendet, wenn die KI-Diagnose aktiviert ist.

- Event Analyzer nutzt diesen Pfad für EMS-Analysen und Latenzdiagnose.
- Bedrock wird mit Ihren angenommenen Anmeldeinformationen und dem ARN des Inferenzprofils ausgeführt, sodass keine Daten an das Konto von NetApp fließen.

Die an Bedrock gesendeten Daten können EMS-Ereignis-JSON, QoS-Statistiken, Volumenkonfiguration, aggregierte Daten und Knoteninformationen umfassen. Der Pfad ist nur aktiv, wenn ein Inferenzprofil pro Organisation (`ai_analyzer_config` Tabelle konfiguriert ist.

Verbindungsgruppen (Protokolle, Ports und Authentifizierung)

Gruppe A, AWS Management Plane Trust Path (angenommene Anmeldeinformationen)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
STS AssumeRole	HTTPS	443	WF → AWS STS (Kundenkonto)	IAM-Anmeldeinformationen + ExternalId	Temporäre kontoübergreifende Anmeldeinformationen erhalten
FSx API (Beschreiben/Erstellen/Aktualisieren/Löschen)	HTTPS	443	WF → AWS FSx Endpoint (Kundenregion)	STS temporäre Anmeldeinformationen	Dateisystem und Volume Lebenszyklusverwaltung
EC2/VPC API	HTTPS	443	WF → AWS EC2 Endpoint	STS temporäre Anmeldeinformationen	Erkennung von Sicherheitsgruppen, Subnetzen und VPCs
CloudFormation API	HTTPS	443	WF → AWS CFN Endpoint	STS temporäre Anmeldeinformationen	Stack-Bereitstellung für IAM-Rollen und FSx-Bereitstellung
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager Endpoint (Kundenkonto)	STS temporäre Anmeldeinformationen	ONTAP Administratorpasswort abrufen (wenn im Secrets Manager gespeichert)
KMS Verschlüsselung/Entschlüsselung	HTTPS	443	WF → AWS KMS Endpoint	STS temporäre Anmeldeinformationen	Verschlüsselungsschlüssel-Operationen für Volumes

Alle AWS-API-Aufrufe verwenden den regionalen Endpunkt des Kunden und können über VPC-Endpunkte geleitet werden, sofern diese konfiguriert sind.

Gruppe B, ONTAP Datenebene

Die ONTAP Datenebene wird immer über Lambda link weitergeleitet, Workload Factory Services stellen niemals eine direkte Verbindung zu ONTAP her.

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
ONTAP REST API	HTTPS	443	Link (Kunden VPC) → ONTAP Management LIF	Basisauthentifizierung (Benutzername/Passwort) oder Secrets Manager ARN	Cluster, Volume und Storage-VM-Konfiguration; QoS; EMS-Ereignisse; ARP-Status
ONTAP SSH CLI	SSH	22	Link (Kunden VPC) → ONTAP Management LIF	Passwortauthentifizierung	Diagnosebefehle (QoS Statistiken, df, Ereignisprotokolle, Effizienz)

Routingstrategie (Prioritätsreihenfolge) für den Proxy-Forwarder:

1. Expliziter `x-link-id`Header: Lambda-ARN aus der Datenbank abrufen
2. Ziel-ID (FSx-Dateisystem-ID): den zugehörigen Link finden
3. Konsolenagenten-ID: Weiterleitung über den Message Broker zum Konsolenagenten

Gruppe C, AWS Lambda Link (in Ihrer VPC bereitgestellt)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
Lambda Invoke	HTTPS (AWS SDK)	443	WF → AWS Lambda API (Kundenkonto)	IAM (`lambda:InvokeFunction`)	ONTAP REST/SSH-Befehle können innerhalb der Kunden-VPC ausgeführt werden.
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (Kunden-VPC) → ONTAP Management LIF	Basisauthentifizierung / Passwort	Privater Subnetzzugang zu ONTAP ohne öffentliche Zugänglichkeit

Gruppe D, NetApp Console Agent (EC2 in Ihrer VPC, nur ausgehend)

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
Agentenabfrage	HTTPS	443	Konsolenagent (Kunden-VPC) → WF Message Broker	Bearer Token (occm-access scope)	Long-Polling für ausstehende ONTAP Befehle (7-Sekunden-Zeitüberschreitung; erneute Verbindungen)
Antwort des Agenten	HTTPS	443	Konsolenagent (Kunden-VPC) → WF Message Broker	Bearer Token	ONTAP-Befehlsausgaben zurückgeben (optional zlib-komprimiert)
Konsolenagent → ONTAP	HTTPS + SSH	443, 22	Konsolenagent (Kunden-VPC) → ONTAP Management LIF	Basisauthentifizierung / Passwort	Proxied ONTAP Vorgänge ausführen

Wesentliches Designmerkmal: Workload Factory initiiert niemals eingehende Verbindungen zum Console-Agenten. Die Arbeit wird in Redis-Streams in eine Warteschlange gestellt; der Console-Agent fragt `GET /messagebroker/v1/requests`ab und antwortet mit `POST /messagebroker/v1/responses`.

Gruppe E, CloudFormation kundenspezifische Ressourcen-Callbacks

Verbindung	Protokoll	Port	Richtung	Authentifizierung	Rechtfertigung
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (Kunde) → WF Lambda (NetApp)	JWT-Token + Referenztoken	Status der IAM-Rollenerstellung melden und Rollen-ARN zurückgeben
ONTAP CloudFormation Ressourcenanbieter → Link	HTTPS	443	CloudFormation Ressource Lambda (Kunde) → Link Lambda (Kunde)	IAM	ONTAP Ressourcen während Stack-Operationen erstellen, aktualisieren oder löschen

Zusammenfassung: Netzwerkanforderungen für Ihre VPC

Komponente	Eingehend	Ausgehend
FSx for ONTAP	Port 443 und 22 von der Link Lambda oder Console Agent Sicherheitsgruppe	k. A.
Lambda verknüpfen	Keine	Port 443 (ONTAP, AWS APIs) und Port 22 (ONTAP SSH)
Konsolen-Agent EC2	Keine	Port 443 (WF Endpunkte, ONTAP, AWS APIs) und Port 22 (ONTAP SSH)
VPC Endpunkte (optional)	k. A.	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

Für keine Komponente in der Kunden-VPC ist ein eingehender Internetzugang erforderlich. Alle Verbindungen werden entweder ausgehend initiiert (Konsolenagent-Polling) oder über AWS-Service-APIs aufgerufen (Lambda Invoke).

ONTAP Ausführungsoptionen für NetApp Workload Factory

Einige NetApp Workload Factory Workflows erfordern ONTAP-native Operationen, die nicht über AWS APIs bereitgestellt werden. Workload Factory bietet zwei Ausführungsoptionen, die diese Operationen innerhalb Ihres AWS-Kontorahmens halten: einen Lambda-Link, der ONTAP Operationen innerhalb Ihrer VPC ausführt, und einen NetApp Console Agent, der ausschließlich ausgehende Verbindungen von einer EC2-Instanz nutzt. Beide Optionen ermöglichen die Durchführung der erforderlichen ONTAP Operationen, wobei Netzwerk-, Anmeldeinformations- und Lebenszyklusentscheidungen innerhalb Ihres Sicherheitsmodells verbleiben.

Ausführungsoptionen

Lambda-Verknüpfung (AWS Lambda in Ihrer VPC)

Führt ONTAP REST und schreibgeschützte ONTAP CLI Diagnose innerhalb Ihrer VPC aus, ohne ONTAP öffentlich zugänglich zu machen.

NetApp Console Agent (EC2 in Ihrer VPC, nur ausgehend)

Führt proxied ONTAP Operationen aus, bei denen der Agent ausgehende Verbindungen initiiert und Workload Factory niemals eingehende Verbindungen zum Agenten initiiert.

Sicherheitsüberlegungen

- Netzwerkgrenzen: Erforderliche ausgehende Ports (443/22) und Zieladressen prüfen.
- Grenzen der Anmeldeinformationen: Es kann festgelegt werden, ob ONTAP-Anmeldeinformationen in Workload Factory (umschlagverschlüsselt) gespeichert oder aus AWS Secrets Manager referenziert werden.
- Prüfbarkeit: Betriebsaufzeichnungen für Komponentenaktivitäten und -ausfälle werden bestätigt.
- Lebenszyklusmanagement: Es wird bestätigt, wie Aktualisierungen und Entfernung erfolgen.

Verwandte Informationen

- "Lambda-Link-Übersicht für NetApp Workload Factory"
- "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory"
- "Verschlüsselung und Schlüsselverwaltung für NetApp Workload Factory"

Identität, Anmeldeinformationen und das Prinzip der minimalen Berechtigungen

AWS-Kontointegration für NetApp Workload Factory

Workload Factory verwendet AWS `sts:AssumeRole`, um temporäre Anmeldeinformationen für Ihr AWS-Konto zu erhalten, sodass langfristige AWS-Zugriffsschlüssel vom Dienst nicht gespeichert werden. Während des Onboardings wird eine IAM-Rolle konfiguriert, die Workload Factory für genehmigte AWS-API-Operationen übernehmen kann, wobei eine externe ID verwendet wird, um unberechtigten kontoübergreifenden Zugriff zu verhindern. Workload Factory verwendet die resultierenden kurzlebigen Anmeldeinformationen dann zur Laufzeit, die AWS nach jeder Sitzung automatisch ablaufen lässt.

AWS Konto Konfiguration

Damit Workload Factory auf Ihr AWS-Konto zugreifen kann:

1. Eine IAM-Rolle im AWS-Konto bereitstellen (mit CloudFormation oder manuell).
2. Es muss sichergestellt sein, dass die Rollenvertrauensrichtlinie dem Service Principal für Workload Factory erlaubt, sie unter Verwendung einer externen ID zu übernehmen.
3. Eine externe ID dient als eindeutiger geheimer Bezeichner (UUID v4), der ausschließlich zwischen dem Kunden und Workload Factory geteilt wird.

   Als Bedingung in die IAM-Rollenvertrauensrichtlinie einbetten (`sts:ExternalId`).

   Die externe ID verhindert Angriffe durch unberechtigte Stellvertreter. In einem kontoübergreifenden Zugriffsmodell kann ein Angreifer, der den Rollen-ARN eines Kunden ermittelt, diese Rolle nicht annehmen, ohne auch die zugehörige externe ID zu besitzen. AWS empfiehlt dieses Muster für den kontoübergreifenden Zugriff von Drittanbietern. Weitere Informationen enthält die AWS IAM-Dokumentationsseite "Zugriff auf AWS-Konten von Drittanbietern".

   Die externe ID wird einmalig während des Anmeldeinformations-Onboardings generiert und verschlüsselt zusammen mit dem Rollen-ARN in einer Workload Factory Datenbank gespeichert.
4. Die Rollen-ARN und die externe ID in Workload Factory registrieren.

Laufzeit

Zur Laufzeit übernimmt Workload Factory Ihre IAM-Rolle, um kurzlebige Anmeldeinformationen für jede AWS API-Operation zu erhalten:

1. Workload Factory ruft `sts:AssumeRole`mit Ihrer Rollen-ARN und der externen ID auf.
2. AWS gibt temporäre Anmeldeinformationen (Zugriffsschlüssel, geheimer Schlüssel und Sitzungstoken) zurück.
3. Workload Factory verwendet die temporären Anmeldeinformationen für AWS API-Operationen in Ihrem Konto.

4. Die Zugangsdaten verfallen automatisch (standardmäßig nach einer Stunde).

Wie AWS-Anmeldeinformationen durch die NetApp Workload Factory fließen

Der AWS-Anmeldeinformationsfluss beschreibt, wie NetApp Workload Factory Rollenkennungen, externe IDs und kurzlebige AWS STS-Anmeldeinformationen während des Onboardings und des laufenden Betriebs verarbeitet. Während der einmaligen Einrichtung wird eine IAM-Rolle in Ihrem AWS-Konto erstellt und eine Vertrauensrichtlinie konfiguriert, die den Workload Factory Service Principal und die korrekte externe ID erfordert. Zur Laufzeit verwendet Workload Factory den gespeicherten Rollen-ARN und die externe ID, um temporäre Anmeldeinformationen anzufordern, die durch eine sitzungsbasierte Richtlinie pro Anfrage eingeschränkt werden, und verwendet zwischengespeicherte Anmeldeinformationen bis zu deren Ablauf erneut.

Einmalige Einrichtung

Bei einer einmaligen Einrichtung verläuft der Ablauf wie folgt:

Schritte

1. Sie starten einen CloudFormation Stack oder erstellen manuell eine IAM-Rolle in Ihrem AWS-Konto.
2. Die IAM-Rollenvertrauensrichtlinie legt zwei Bedingungen fest:
    a. Nur der Dienstprinzipal für Workload Factory kann ihn übernehmen.
    b. Der Anrufer muss die korrekte externe Kennung angeben.
3. Workload Factory speichert den Rollen-ARN und die externe ID (verschlüsselt) in seiner Datenbank.

Laufzeit (jede API-Operation)

Zur Laufzeit verwendet Workload Factory den gespeicherten Rollen-ARN und die externe ID, um temporäre AWS STS-Anmeldeinformationen für jede API-Operation zu erhalten. Der Ablauf ist wie folgt:

Schritte

1. Workload Factory ruft den gespeicherten Rollen-ARN und die externe ID aus MySQL ab.
2. Es prüft Redis auf einen zwischengespeicherten Satz temporärer AWS STS-Anmeldeinformationen für diese Rolle.
3. Bei einem Cache-Miss ruft Workload Factory `sts:AssumeRole` mit dem Rollen-ARN und der externen ID auf. Der Aufruf enthält eine pro Anfrage definierte Inline-Sitzungsrichtlinie, die die Berechtigungen auf die für den jeweiligen Vorgang erforderlichen AWS-Aktionen beschränkt.
4. AWS STS gibt temporäre Anmeldeinformationen (Zugriffsschlüssel-ID, geheimer Zugriffsschlüssel, Sitzungstoken) mit einem Ablaufzeitstempel zurück.
5. Workload Factory speichert diese Anmeldeinformationen in Redis zwischen und verwendet sie, um die Ziel-AWS-APIs aufzurufen.
6. Bei Cache-Treffer überspringt Workload Factory den STS-Aufruf und verwendet die zwischengespeicherten Anmeldeinformationen direkt.

Sitzungsrichtlinie

Jeder STS-Aufruf beinhaltet eine Inline-Sitzungsrichtlinie, die auf die minimal erforderlichen AWS-Aktionen beschränkt ist.

Verwandte Informationen

- "Berechtigungsstufen mit geringsten Rechten"

Aufbewahrung von AWS-Anmeldeinformationen für NetApp Workload Factory

Workload Factory sichert die Verwaltung von Anmeldeinformationen durch kurzlebige AWS STS-Anmeldeinformationen, verschlüsselte Rollenmetadaten und begrenztes Aufbewahrungsverhalten. Das Anmeldeinformationsmodell trennt gespeicherte Rollenmetadaten von temporären AWS-Anmeldeinformationen, die für API-Operationen verwendet werden. Temporäre Anmeldeinformationen werden nur für einen begrenzten Zeitraum zwischengespeichert und laufen automatisch unter AWS-Durchsetzung ab. Das Entfernen einer Anmeldeinformation verhindert, dass Workload Factory neue Anmeldeinformationen für das Konto erhält, während zwischengespeicherte Anmeldeinformationen kurz darauf ablaufen.

Wichtige Verhaltensweisen

- Workload Factory speichert keine langfristigen AWS-Zugriffsschlüssel.

  Workload Factory speichert lediglich einen Zeiger (Rollen-ARN) und ein gemeinsames Geheimnis (externe ID). Keines von beiden gewährt allein Zugriff auf AWS.

- Temporäre AWS STS-Anmeldeinformationen haben eine maximale Gültigkeitsdauer von einer Stunde (von AWS vorgegeben).

  Workload Factory speichert sie für maximal 30 Minuten in Redis, bevor ein neuer STS-Aufruf erfolgt.

- Wenn ein zwischengespeicherter Satz von Anmeldeinformationen weniger als 15 Minuten gültig ist, verwirft Workload Factory ihn und erhält einen neuen.
- Die Löschung der Zugangsdaten durch den Kunden widerruft sofort die Möglichkeit für Workload Factory, auf dieses Konto zuzugreifen.

  Der nächste AssumeRole-Aufruf schlägt fehl, und die zwischengespeicherten Anmeldeinformationen verfallen innerhalb weniger Minuten.

Zusammenfassung zu Aufbewahrung und Speicherung

Daten	Speicherort	Retentionsdauer	Automatischer Ablauf?	Löschmethode
IAM Role ARN + externe ID	MySQL (verschlüsselt im Ruhezustand)	Unbefristet (wird gespeichert, bis der Kunde es explizit entfernt)	Nein	Der Kunde klickt in der Benutzeroberfläche auf „Anmeldeinformationen löschen“.
Temporäre AWS STS-Anmeldeinformationen (Zugriffsschlüssel + Geheimnis + Sitzungstoken)	Redis (In-Memory-Cache)	Maximal 30 Minuten (Cache-TTL). Die zugrunde liegenden STS-Anmeldeinformationen sind bis zu einer Stunde gültig (AWS-Standard). Der Cache wird fünf Minuten vor Ablauf als Sicherheitsmarge geleert.	Ja (Redis entfernt automatisch Einträge nach Ablauf der Gültigkeitsdauer; das Ablaufdatum der AWS-Anmeldeinformationen wird von AWS erzwungen)	Automatisch
ONTAP Administratorpasswort	MySQL (AES-256-CBC-Umschlagverschlüsselung mit KMS)	Unbefristet (wird gespeichert, bis der Kunde die Anmeldeinformationen entfernt oder das Dateisystem löscht)	Nein	Der Kunde löscht die Anmeldeinformationen oder das Löschen des Dateisystems löst die Bereinigung aus
Entschlüsseltes ONTAP Passwort (Klartext)	Nur im Arbeitsspeicher (niemals auf Festplatte oder Cache geschrieben)	Dauer einer einzelnen Anfrage (Millisekunden)	Ja (wird nach Abschluss der Anfrage automatisch bereinigt)	Automatisch

Sicherheitskontrollen

- Externe ID verhindert Angriffe durch verwirrte Stellvertreter.
- Sitzungsrichtlinien erzwingen das Prinzip der minimalen Berechtigungen pro Anfrage.
- Workload Factory aktualisiert kurzlebige temporäre AWS STS-Anmeldeinformationen, bevor risikoreiche Ablaufzeiträume erreicht werden.
- Die Handhabung regionaler und kontotypbezogener Aspekte unterscheidet sich für Standard-, GovCloud- und China-Umgebungen.

- Workload Factory speichert niemals langfristige AWS-Zugriffsschlüssel.
- Workload Factory ändert niemals die Berechtigungen Ihrer IAM-Rolle.
- Workload Factory überschreitet niemals die durch Ihre Rollenrichtlinie gewährten Berechtigungen.
- Sitzungsrichtlinien können Berechtigungen nur einschränken; Workload Factory erweitert sie niemals.

Anmeldeinformationstypen für NetApp Workload Factory

NetAppWorkload Factory verwendet ein Modell mit getrennten Anmeldeinformationen, um die Berechtigungen der AWS-Steuerungsebene vom direkten administrativen ONTAP-Zugriff zu trennen. Die AWS IAM-Rolle authentifiziert Workload Factory gegenüber AWS-APIs für Vorgänge wie Systemmanagement, Backup-Management und Ressourcenerkennung. ONTAP-Anmeldeinformationen authentifizieren den direkten Zugriff auf den ONTAP-Management-Endpunkt mit einer Lambda-Verbindung für Vorgänge, die administrative Konfiguration oder Diagnose erfordern. Einige Workflows erfordern beide Anmeldeinformationstypen, wenn AWS-API-Vorgänge mit direkten ONTAP-Managementaufgaben kombiniert werden.

Anmeldeinformationstypen

Die folgende Tabelle fasst die beiden in Workload Factory verwendeten Anmeldeinformationstypen und deren jeweilige Authentifizierungsziele zusammen.

Anmeldeinformationstyp	Authentifiziert gegenüber	Wird verwendet für
AWS-Anmeldeinformationen (AssumeRole)	AWS APIs	Alle Operationen, die über die AWS FSx Service API ausgeführt werden
ONTAP Zugangsdaten (Admin-Passwort)	ONTAP Management-Endpunkt	Operationen, die direkten Zugriff auf die ONTAP REST API oder die CLI erfordern

AWS-Anmeldeinformationsbasierte Operationen

Diese Operationen interagieren ausschließlich mit AWS-APIs und erfordern lediglich die IAM-Rolle:

- Dateisystemerstellung und -löschung
- Änderungen der Dateisystemkapazität und des Durchsatzes
- Backup-Erstellung und -Verwaltung
- VPC, Subnetz und Sicherheitsgruppenerkennung
- KMS-Schlüsselaufzählung
- CloudWatch Metrikenabruf
- Cost Explorer Abfragen
- Tag-Management über die FSx API

ONTAP Anmeldeinformationen Operationen

Diese Operationen kommunizieren direkt über die Lambda-Verbindung mit dem ONTAP-Verwaltungsendpunkt und erfordern ONTAP-Administratoranmeldeinformationen:

- Konfiguration der QoS-Richtlinie auf Volume-Ebene
- Export-Policy- und Regelmanagement
- Storage VM Protokollkonfiguration (NFS, CIFS, iSCSI)
- Initiatorgruppe und LUN Management
- SnapMirror (Replikationskonfiguration)
- Snapshot-Richtlinienmanagement (ONTAP-Ebene)
- Diagnose (QoS-Statistiken, Latenzanalyse)
- Abruf und Analyse von EMS-Ereignissen
- Überwachung des Status des Anti-Ransomware-Schutzes
- FlexCache Management
- Netzwerkschnittstellen (LIF) Abfragen

Vorgänge, die sowohl AWS- als auch ONTAP Anmeldeinformationen erfordern

Workflow	AWS-Anmeldeinformationen verwendet für	ONTAP Anmeldeinformationen verwendet für
KI-gestützte Ereignisanalyse	Bedrock aufrufen, Dateisystem beschreiben	EMS-Ereignisse abrufen und Diagnose per SSH ausführen
Dateisystemerstellung mit Storage-VM-Setup	Dateisystem erstellen (AWS API)	Speicher-VM-Protokolle konfigurieren (ONTAP REST)
Volumenerstellung mit Exportrichtlinie	Volume erstellen (AWS API)	Exportrichtlinienregeln festlegen (ONTAP REST)
Kapazitätsmanagement	Dateisystemkapazität aktualisieren (AWS API)	Aggregatauslastung prüfen (ONTAP SSH)

Verwandte Informationen

- "ONTAP Ausführungsoptionen"
- "Lambda Link Übersicht"

Optionen zur Speicherung von Anmeldeinformationen für NetApp Workload Factory

NetApp Workload Factory unterstützt Muster zur Verwaltung von Anmeldeinformationen, die das Prinzip der minimalen Berechtigungen wahren und die Offenlegung von ONTAP-Administrationsgeheimnissen reduzieren. KI-gestützte Diagnosefunktionen verwenden schreibgeschützte ONTAP-Anmeldeinformationen, sofern verfügbar, sodass der Diagnoseagent die Speicherumgebung beobachten und diagnostizieren kann, ohne sie zu verändern. Es kann entweder der von Workload Factory verwaltete verschlüsselte Speicher genutzt oder das ONTAP-Passwort im AWS Secrets Manager gespeichert und Workload Factory eine Referenz bereitgestellt werden. Die Wahl wirkt sich darauf aus, wo das Passwort gespeichert wird, wie es verschlüsselt wird und wie Anforderungen wie

GovCloud Support und Anmeldeinformationsrotation verwaltet werden.

Schreibgeschütztes ONTAP Zugriffsmodell

Für KI-gestützte Funktionen wie Ereignisanalyse und Latenzdiagnose verwendet Workload Factory, sofern verfügbar, schreibgeschützte ONTAP-Anmeldeinformationen. Das schreibgeschützte Anmeldemodell stellt sicher, dass der KI-Diagnoseagent keine Änderungen an Ihrer Speicherumgebung vornehmen kann, sondern sie nur beobachten und diagnostizieren kann.

Vergleich der Optionen zur Speicherung von Anmeldeinformationen

AWS Zugangsdaten

AWS-Anmeldeinformationen werden immer über eine IAM-Rolle angenommen. Workload Factory kann die Rolleninformationen entweder intern verwalten oder sie aus dem AWS Secrets Manager referenzieren.

Option	AWS Zugangsdaten	Was gespeichert wird	Verschlüsselung
Workload Factory verwaltet	IAM Role ARN + externe ID	IAM Role ARN + externe ID	Die Rollen-ARN ist kein Geheimnis (wird unverändert gespeichert)

ONTAP Zugangsdaten

Workload Factory kann ONTAP Zugangsdaten intern mit verschlüsselter Speicherung verwalten oder sie über AWS Secrets Manager referenzieren. Die Wahl beeinflusst, wie das Passwort gespeichert, verschlüsselt und rotiert wird.

Für die Interaktion von NetApp Workload Factory mit den ONTAP File System APIs über eine "Lambda Link" sind ONTAP-Zugangsdaten erforderlich.

Option	ONTAP Zugangsdaten	Was gespeichert wird	Verschlüsselung
Workload Factory verwaltet	Passwort (verschlüsselt)	ONTAP Administratorpasswort (verschlüsselt)	ONTAP Passwort verwendet AES-256-Umschlagverschlüsselung
AWS Secrets Manager	Secrets Manager ARN-Referenz	Secrets Manager ARN	Secrets ARN ist kein Geheimnis (wird unverändert gespeichert); AWS Secrets Manager verschlüsselt das Geheimnis in Ihrem Konto

Weitere Überlegungen

GovCloud Requirement

Es wird die Standard-IAM-Rolle verwendet; ONTAP Anmeldeinformationen müssen Secrets Manager

verwenden (Passwortspeicherung ist nicht zulässig).

Drehung

Die Rollenrichtlinien werden in Ihrem Konto aktualisiert. Das ONTAP Passwort in Workload Factory (verwaltete Option) sollte aktualisiert oder im AWS Secrets Manager rotiert werden.

Berechtigungsstufen mit minimalen Rechten für NetApp Workload Factory

Sie können die IAM-Berechtigungen der Workload Factory jederzeit einschränken, um sie an das Prinzip der minimalen Berechtigungen anzupassen, zum Beispiel durch Beschränkung des Zugriffs auf bestimmte Ressourcen (ARNs) und Anwendung von IAM-Bedingungen, etwa Tags und CIDR-Bereiche.

Gestuftes Berechtigungsmodell

Workload Factory verwendet ein gestaffeltes Berechtigungsmodell, das dem Prinzip der minimalen Rechtevergabe folgt. Die zu aktivierenden Berechtigungsstufen werden beim Hinzufügen von AWS-Anmeldeinformationen ausgewählt. Ein Start mit einer schreibgeschützten Erkennung ist möglich und kann bei Bedarf erweitert werden.

Workload Factory gewährt alle Berechtigungen über eine IAM-Rolle in Ihrem AWS-Konto, die über STS mit einer externen ID übernommen wird.

Workload Factory grenzt jeden API-Aufruf zusätzlich mit einer Inline-Sitzungsrichtlinie ein.

In der Workload Factory Konsole unterstützt die KI-Chatfunktion *Ask Me* dabei, Berechtigungen sicher zu verfeinern, indem Einschränkungsoptionen vorgeschlagen und eine aktualisierte Richtlinie zur Anwendung in AWS generiert werden.

Erteilung von Berechtigungen

Beim Hinzufügen von AWS-Anmeldeinformationen zu Workload Factory kann ausgewählt werden, welche Berechtigungsstufen aktiviert werden sollen. Die Stufen können jederzeit aktiviert oder deaktiviert werden.

Die Stufen sind kumulativ: Die Aktivierung einer höheren Stufe aktiviert automatisch alle niedrigeren Stufen.

Sicherheitskontrollen

- Externe ID (Schutz vor confused deputy)
- Sitzungsrichtlinien pro Vorgang (geringste Berechtigung pro Anfrage)
- Tagbasierte Bedingungen (Sicherheitsgruppenänderungen, die auf von Workload Factory erstellte Ressourcen beschränkt sind)
- Secret-ARN-Bereich (Zugriff auf Secrets Manager beschränkt auf `FSxSecret*`)
- Laufzeitberechtigungsprüfung (fehlende Aktion/Ressource für gezielte Behebung gemeldet)

Berechtigungsdokumentation

Die primäre Referenz für Workload Factory Berechtigungen ist die "Berechtigungsreferenz" in der Workload

Factory Setup- und Administrationsdokumentation. In dieser Referenz finden sich Informationen zu den Auswirkungen des Entfernens von Berechtigungen aus den Storage IAM-Richtlinien.

Amazon CloudWatch Überwachungsberechtigungen für NetApp Workload Factory

Amazon CloudWatch-Überwachungsberechtigungen sind in NetApp Workload Factory optional und gelten nur, wenn der separate Überwachungs-Stack bereitgestellt wird. Der Überwachungs-Stack bietet operative Transparenz durch das Sammeln von Dateisystemmetriken, das Veröffentlichen von Ereignisprotokollen, die Verwaltung von CloudWatch-Dashboards und Alarmen sowie das Versenden von Benachrichtigungen über Amazon SNS. Der Stack benötigt außerdem Zugriff, um bei Bedarf ONTAP-Anmeldeinformationen für die Überwachung abzurufen.

Erforderliche CloudWatch Überwachungsberechtigungen

Für den optionalen Monitoring-Stack sind folgende Berechtigungen erforderlich:

Berechtigung	Zweck
fsx:Describe* / fsx:ListTagsForResource	Dateisystemmetriken erfassen
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Dashboards und Alarme verwalten
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	Ereignisprotokolle veröffentlichen
sns:Publish	Warnmeldungen senden
secretsmanager:GetSecretValue	ONTAP Zugangsdaten für die Überwachung abrufen

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."

Beobachtbarkeit (Protokolle, Metriken, Telemetrie)

Informationen zur Observability in NetApp Workload Factory

Observability-Signale unterstützen die Betriebsüberwachung, Fehlerbehebung und Untersuchungen. In NetApp Workload Factory umfasst Observability Metriken, Telemetriedaten und Betriebsprotokolle, die Einblick in das Serviceverhalten, die KI-Nutzung und die über Workload Factory durchgeführten Aktionen bieten. Telemetriedaten und Betriebsprotokolle unterstützen die interne Überwachung und die Transparenz bei Kundenaudits, und Tracker ermöglicht die Überprüfung von Fortschritt, Status und Details der unterstützten Vorgänge.

Telemetrie und Betriebsaufzeichnungen

Workload Factory verwendet die folgenden Telemetrie- und Betriebsdatensatztypen:

- OpenTelemetry-Traces, die über OTLP HTTP an SigNoz (interne Observability) exportiert werden
- KI-Nutzungsmetriken (Token-Anzahl, Modellkosten) in AWS Timestream gespeichert
- NetApp Console Audit-Protokolle (Aktionsname, Status, Anfrage-/Antwort-Metadaten, Zeitstempel)

Audit Protokollierung in Workload Factory

Workload Factory bietet Tracker, eine Überwachungsfunktion, mit der überwacht werden kann, welche Vorgänge laufen und wann. Mit Tracker lassen sich der Fortschritt und Status von FSx for ONTAP, Anmeldeinformationen und Verbindungsvorgängen nachverfolgen, Details zu Vorgangsaufgaben und Unteraufgaben einsehen sowie etwaige Probleme oder Fehler diagnostizieren.

In Tracker stehen mehrere Aktionen zur Verfügung. Aufträge können nach Zeitraum (letzte 24 Stunden, 7 Tage, 14 Tage oder 30 Tage), Arbeitslast, Status und Benutzer gefiltert, mit der Suchfunktion gefunden und die Auftragstabelle als CSV-Datei heruntergeladen werden.

- "Vorgänge mit Tracker in Workload Factory überwachen"

Verwandte Informationen

- "Metriken und Telemetrie für NetApp Workload Factory"

Metriken und Telemetrie für NetApp Workload Factory

NetApp Workload Factory erfasst und speichert Metriken auf Volume- und Dateisystemebene in AWS CloudWatch, um operative Einblicke in Speicherleistung und Kapazität zu bieten. Berechnete Metriken wie der Durchsatz werden aus diesen erfassten Werten abgeleitet. Informationen zu den Metrikdefinitionen, der Erfassungsfrequenz, dem Aktualisierungsverhalten und den Aufbewahrungsdetails.

Enthaltene Kennzahlen

NetApp Workload Factory verwendet diese Metriken für Betriebsprotokolle und Ereignisse:

- Kennzahlen auf Volumenebene CloudWatch (pro Volumen erfasst)
- Dateisystemebene CloudWatch Metriken (pro Dateisystem erfasst)
- Berechnete Metriken
- Sammelplan und Aufbewahrung

Über operative Kennzahlen

Berechnete Kennzahlen verwenden diese Formel:

- Durchsatz (Bytes/Sekunde) = (NetworkSentBytes + NetworkReceivedBytes) / Periode

Aktualisierungsverhalten:

- Volumen- und Clustermetriken werden alle 12 Stunden aktualisiert.
- Die Latenzmetriken werden alle 20 Minuten aktualisiert.
- DynamoDB Elemente verfallen nach 14 Tagen automatisch.

Über die Telemetriedatenerfassung

- OpenTelemetry-Traces, die über OTLP HTTP an SigNoz (interne Observability) exportiert werden
- KI-Nutzungsmetriken (Token-Anzahl, Modellkosten) in AWS Timestream gespeichert
- NetApp Console Audit-Protokolle (Aktionsname, Status, Anfrage-/Antwort-Metadaten, Zeitstempel)

Kennzahlen auf Volumenebene CloudWatch (pro Volumen erfasst)

Metrik	AWS CloudWatch-Name	Einheit	Was gemessen wird
Volume-Speicherkapazität	StorageCapacity	Bytes	Gesamte bereitgestellte Kapazität
Genutzter Speicherplatz	StorageUsed	Bytes	Tatsächlich gespeicherte Daten
gelesene Datenbytes	DataReadBytes	Bytes	Lesedurchsatz
Daten-Schreibbytes	DataWriteBytes	Bytes	Schreibdurchsatz
Datenlesevorgänge	DataReadOperations	Anzahl	Lese-IOPS
Schreibvorgänge für Daten	DataWriteOperations	Anzahl	Schreib-IOPS
Metadatenoperationen	MetadataOperations	Anzahl	Metadaten IOPS
Zeit für Lesevorgänge von Daten	DataReadOperationTime	Sekunden	Leselatenz
Zeit für den Schreibvorgang	DataWriteOperationTime	Sekunden	Schreiblatenz
Metadaten-Operationszeit	MetadataOperationTime	Sekunden	Metadatenlatenz

Dateisystemebene CloudWatch-Metriken

Metrik	AWS CloudWatch-Name	Einheit	Was gemessen wird
SSD Speicherkapazität	StorageCapacity	Bytes	Gesamtkapazität der SSD-Ebene
SSD-Speicher verwendet	StorageUsed (SSD-Stufe)	Bytes	SSD-Tier-Verbrauch
Kapazitätspool genutzt	StorageUsed (Kapazitätspool)	Bytes	Kapazitätspoolverbrauch
CPU-Auslastung	CPU-Auslastung	Prozent	Dateiserver CPU
SSD Kapazitätsauslastung	StorageCapacityUtilization	Prozent	SSD-Tier-Prozentsatz genutzt
Netzwerkdurchsatz-Auslastung	NetworkThroughputUtilization	Prozent	Prozentuale Netzwerkauslastung
Festplatten-IOPS-Auslastung	DiskIopsUtilization	Prozent	Festplatten-IOPS prozentual ausgelastet
Festplatten-Durchsatz-Auslastung	FileServerDiskThroughputUtilization	Prozent	Festplattendurchsatz prozentuale Auslastung
Festplatten-IOPS-Auslastung (Server)	FileServerDiskIopsUtilization	Prozent	Prozentuale Auslastung der Serverfestplatten-IOPS
Einsparungen bei der Speichereffizienz	StorageEfficiencySavings	Bytes	Platzersparnis durch Effizienz
Netzwerk empfangen	NetworkReceivedBytes	Bytes	Eingehendes Netzwerk
Netzwerk gesendet	NetworkSentBytes	Bytes	Ausgehendes Netzwerk

Sammelplan und Aufbewahrung

Zeitbereich	Sammelzeitraum	Datenpunkte	Storage	Aufbewahrung
1 Tag	24 Minuten	~60	DynamoDB	14 Tage (TTL)
1 Woche	ca. 2,8 Stunden	~60	DynamoDB	14 Tage (TTL)
1 Monat	12 Stunden	~60	DynamoDB	14 Tage (TTL)
3 Monate	ca. 1,5 Tage	~60	DynamoDB	14 Tage (TTL)
1 Jahr	~6 Tage	~60	DynamoDB	14 Tage (TTL)

Sicherheitskontrollen für generative KI

Informationen zu KI-Steuerungen in NetApp Workload Factory

NetApp Workload Factory beinhaltet generative KI-Funktionen, die die Diagnose beschleunigen und gleichzeitig Sicherheitskontrollen für den Modellzugriff, den Datenumfang und das Laufzeitverhalten durchsetzen.

Workload Factory aktiviert KI-Diagnose standardmäßig. Generative KI-Funktionen können jederzeit über die Workload Factory **Administration**-Einstellungen deaktiviert werden. "Weitere Informationen zur Verwaltung von GenAI-Funktionen."

Überblick über Security-scoped KI-Funktionen

Workload Factory wendet generative KI derzeit auf die folgenden Funktionen an:

- Ask Me assistant (RAG mit kuratierter NetApp Dokumentation, quellenbasierte Antworten)
- Latenzanalyse
- EMS-Ereignisanalyse
- Fehlerprotokollanalyse

AWS Bedrock Übersicht für KI-Diagnose

Workload Factory nutzt Amazon Bedrock für KI-Inferenz. Die Inferenz läuft in Ihrem AWS-Konto unter Ihren konfigurierten Anmeldeinformationen und Ihrem Inferenzprofil.

Verwandte Informationen

- "Amazon Bedrock Opt-in für NetApp Workload Factory AI-Diagnose"
- "KI-Tool-Grenzen für NetApp Workload Factory"
- "KI-Modellparameter und Abrechnung für NetApp Workload Factory"

Amazon Bedrock Opt-in für NetApp Workload Factory AI-Diagnose

NetApp Workload Factory KI-Diagnose verwendet Amazon Bedrock zur Analyse von Ereignissen, und die Funktion ist standardmäßig aktiviert. Bevor Workload Factory das ausgewählte Bedrock-Modell aufrufen und Diagnosedaten erfassen kann, müssen IAM-Berechtigungen, ein Inferenzprofil und eine verbundene Lambda-Verbindung mit SSH-Fähigkeit konfiguriert werden. Fehlt eine dieser Komponenten oder wird die Bedrock-Konfiguration entfernt, ist die KI-Diagnose nicht verfügbar.

KI-Diagnose ist standardmäßig aktiviert.

Bevor Sie beginnen

- Ihr Konto muss ein AWS Bedrock Inferenzprofil enthalten.
- Eine verbundene Lambda-Verbindung mit SSH-Funktionalität für die Erfassung von Diagnosedaten ist vorhanden.

Schritte

1. Bedrock-Berechtigungen in Ihrer IAM-Rolle gewähren:
    - `bedrock:InvokeModel`
    - `bedrock:InvokeModelWithResponseStream`
    - `bedrock:ListInferenceProfiles`
    - `bedrock:GetInferenceProfile`
2. Der ARN des Inferenzprofils wird in den Workload Factory Einstellungen konfiguriert.

Falls eine Voraussetzung fehlt, meldet das System die spezifische fehlende Komponente und die KI-Funktionen bleiben inaktiv.

KI-Diagnose deaktivieren

KI Diagnose deaktivieren:

- Die Bedrock-Berechtigungen aus Ihrer IAM-Rolle entfernen oder
- Die Bedrock Konfiguration in den Workload Factory Einstellungen löschen.

KI-Diagnose ist sofort nicht mehr verfügbar und es findet keine weitere Datenverarbeitung statt.

Regionale und regionsübergreifende Inferenzprofile

Die Bedrock-Inferenz wird in der AWS-Region ausgeführt, die in Ihrem Inferenzprofil angegeben ist. Bei Verwendung eines regionsübergreifenden Inferenzprofils kann AWS die Anfrage gemäß dem Standardverhalten von AWS Bedrock an eine beliebige Region in der Profilkonfiguration weiterleiten. Daten verlassen die AWS-Infrastruktur nicht.

KI-Tool-Grenzen für NetApp Workload Factory

NetApp Workload Factory legt strenge Grenzen dafür fest, wie seine KI-Funktionen mit Ihren AWS- und ONTAP Umgebungen interagieren, sodass KI-gestützte Diagnose genutzt werden kann, ohne unbeabsichtigte Änderungen zu riskieren. Amazon Bedrock verwendet schreibgeschützte AWS CLI- und ONTAP CLI-Diagnosetools, die verändernde Befehle blockieren und die Ausgabe hinsichtlich Größe und Ausführung begrenzen, und alle verwendeten Daten sind nur vorübergehend und werden weder von NetApp Workload Factory noch von AWS gespeichert.

Werkzeugsicherheitskontrollen

Werkzeug	Fähigkeit	Sicherheitskontrollen
AWS CLI (schreibgeschützt)	Schreibgeschützte AWS CLI-Befehle ausführen (describe, list, get)	Blockiert alle verändernden Verben (Erstellen, Löschen, Ändern, Aktualisieren, Einfügen, Entfernen). Maximal 10 Befehle pro Schritt. Ausgabe auf 20 KB gekürzt.
ONTAP CLI (schreibgeschützt)	Schreibgeschützte ONTAP CLI-Befehle können über SSH ausgeführt werden.	Blockiert alle verändernden Verben (löschen, zerstören, erstellen, modifizieren, verschieben). Ausgabe gekürzt.

Der Agent kann Ressourcen weder verändern, erstellen noch löschen. Er kann sie lediglich beobachten und diagnostizieren.

Grenzen der Datenspeicherung und des Modelltrainings

Gemäß den AWS-Richtlinien speichert oder verwendet Amazon Bedrock Ihre Eingaben und Ausgaben nicht zum Trainieren oder Verbessern von Basismodellen. Für bedarfsgesteuerte Inferenz (verwendet von Workload Factory) verarbeitet AWS Ihre Daten nur vorübergehend und speichert sie nach der Rückgabe der Antwort nicht.

KI-Modellparameter und Abrechnung für NetApp Workload Factory

NetApp Workload Factory definiert die Modellkonfiguration sowie die Nutzungs- und Abrechnungsgrenzen für die KI-Governance. Das konfigurierte Modell verwendet deterministische Parameter und gibt strukturiertes JSON zurück, um konsistente Analyseergebnisse zu unterstützen. AWS rechnet die Amazon Bedrock Inferenz über Ihr Konto ab, während Workload Factory die KI-Nutzung verfolgt und monatliche Kostentransparenz pro Konto bietet. Diese Abschnitte beschreiben die Modellparameter und die Grenzen, die für den KI-Verbrauch gelten.

Modell und Parameter

Parameter	Wert
Modell	Anthropic Claude (unter Verwendung eines regionsübergreifenden Inferenzprofils)
Temperatur	0 (deterministisch, keine Zufälligkeit)
Maximale Ausgabetokens	2.048
Maximale Anzahl an Schlussfolgerungsschritten	15 pro Analyse
Ausgabeformat	Strukturiertes JSON (Zusammenfassung, Schweregrad, Ursache, Korrekturmaßnahmen)

Abrechnungs- und Nutzungslimits

- AWS stellt Bedrock Inference Ihrem Konto in Rechnung (Ihr Inference-Profil, Ihre Anmeldeinformationen).

- Workload Factory verfolgt die KI-Nutzung intern.
- Workload Factory bietet monatliche Kostentransparenz pro Account.

  "Speicherkosten in NetApp Workload Factory nachverfolgen"

Ask Me AI Assistant

Ask Me Sicherheitsarchitektur für NetApp Workload Factory

Ask Me ist ein generativer KI-gestützter Assistent, der in NetApp Workload Factory eingebettet ist. Es wird Echtzeit-Unterstützung in Dialogform für Amazon FSx for NetApp ONTAP und Workload Factory Themen bereitgestellt. Antworten basieren auf verifizierter NetApp Dokumentation, und Ask Me kann nicht auf das öffentliche Internet zugreifen oder Kundendaten zur Modellschulung verwenden. Mehrere Sicherheitsebenen helfen, schädliche Anfragen zu blockieren, Antworten auf unterstützte Domänen zu beschränken und zu verhindern, dass Benutzereingaben Systemanweisungen überschreiben. Wenn Ask Me Tools verwendet, helfen Autorisierungsgrenzen, die Durchsetzung von schreibgeschützten Abfragen, eine temporäre Sandbox und die Protokollierung, die Ausführung einzuschränken und zu überwachen.

Sie können „Ask Me“ jederzeit über die **Administration**-Einstellungen von Workload Factory abwählen, wodurch der Assistent für Ihr Benutzerkonto deaktiviert wird."Weitere Informationen zur Verwaltung von GenAI-Funktionen."

RAG Architektur in Ask Me

Ask Me verwendet Retrieval-Augmented Generation (RAG).

- Kuratierte Wissensdatenbank: Die Antworten basieren auf einem verwalteten Korpus verifizierter, veröffentlichter NetApp-Dokumentation.
- Bewertung und Filterung der Suchergebnisse: Nur ausreichend relevante Inhalte werden in den Modellkontext aufgenommen.
- Kein Internetzugang: Das Modell kann keine externen Inhalte abrufen, durchsuchen oder extrahieren.
- Quellenangabe: Die Antworten enthalten Verweise auf die verwendeten Quelldokumente.

Mehrschichtige Prompt-Sicherheit

- Schicht 1: Der Sicherheitsklassifikator (LLM-as-a-judge) blockiert bösartige Abfragen (Prompt Injection, Privilege Escalation, Datenexfiltration, Social Engineering, Richtlinienverstöße).

  Das System protokolliert blockierte Anfragen, und das generative Modell sieht sie nie.

- Schicht 2: Die System-Prompt-Härtung verhindert, dass Benutzereingaben Systemanweisungen überschreiben.
- Layer 3: Die Domänenbereichsbegrenzung beschränkt die Antworten auf FSx ONTAP und Workload Factory Themen.
- Ebene 4: Die Tool-Nutzungssteuerung validiert Parameter und führt Abfragen in einer gehärteten Sandbox aus; das Modell kann keine beliebigen Operationen ausführen.

Modelldatenisolation und Datenschutz

- Kein Modelltraining mit Kundendaten
- Isolation auf Anfrageebene (keine mandantenübergreifende Datenweitergabe)
- Sitzungsbezogener Gesprächskontext mit begrenzter Historie
- Kein persistenter Modellspeicher
- Verwaltete Inferenzinfrastruktur

Werkzeugnutzung und agentenbasierte Sicherheit

- Autorisierungsbezogene Tools (Benutzerberechtigungsgrenzen werden durchgesetzt)
- Strenge Tool-Ausführungs-Timeouts
- Kurzlebige, sitzungsbezogene Sandbox für abgerufene Daten
- Durchsetzung schreibgeschützter Abfragen mit Allowlisting
- Prüfbarkeit von Toolaufrufen mit sensibler Parameterbereinigung

Ask Me Zugriffskontrolle für NetApp Workload Factory

In NetApp Workload Factory konzentriert sich die Zugriffssicherheit von Ask Me auf authentifizierte Sitzungen, Benutzer-Nachverfolgbarkeit und den geschützten Umgang mit Geheimnissen während des Laufzeitbetriebs. Authentifizierungskontrollen validieren jede Sitzung und ordnen Interaktionen einem bestimmten Benutzer zu. Sensible Anmeldeinformationen werden zur Laufzeit aus einem verwalteten Geheimnisspeicher abgerufen und in den Protokollen unkenntlich gemacht. Der Dienst wendet außerdem Infrastrukturkontrollen an, einschließlich der Ausführung von Containern ohne Root-Rechte und einer eingeschränkten CORS-Allowlist.

Authentifizierung

- Signierte JWT Authentifizierung mit kryptografischer Validierung (einschließlich Überprüfung von Adressat, Aussteller und Algorithmus wie RS256)
- Middleware-gestützte Authentifizierung an der Dienstgrenze
- Benutzeridentitätseingrenzung, sodass Interaktionen einem bestimmten Benutzer zugeordnet werden können

Schutz von Zugangsdaten und Umgang mit Geheimnissen

- Sichere Tresorspeicherung: Sensible Zugangsdaten, die vom Dienst verwendet werden, werden in einem verwalteten Geheimnis-Tresor gespeichert und zur Laufzeit abgerufen. Es werden keine Geheimnisse im Anwendungscode, in Konfigurationsdateien oder in Container-Images gespeichert.
- Protokollbereinigung: Sensible Werte (Anmeldeinformationen, Token, Passwörter, Zugriffsschlüssel, Zertifikate) werden aus den Protokollen entfernt, bevor sie geschrieben werden.

Infrastruktursicherheit

- Ausführung eines Nicht-Root-Containers
- CORS ist auf eine explizite Zulassungsliste vertrauenswürdiger NetApp-Domains beschränkt.

Ask Me Ausführungsmodi für NetApp Workload Factory

NetApp Workload Factory bietet mehrere Ausführungsmodi für Ask Me, die sich in ihren Sicherheits- und Datenschutzeigenschaften unterscheiden. Wenn Ask Me Tool-Integrationen verwendet, beispielsweise zum Abfragen der eigenen Workload Factory Ressourcen des Kunden, wird die Tool-Ausführung durch mehrstufige Sicherheitsvorkehrungen kontrolliert. Die Tool-gestützte Ausführung erfolgt innerhalb der Berechtigungen des authentifizierten Benutzers und begrenzt die Dauer und den Umfang jeder Operation. Abgerufene Daten verbleiben in einer temporären Sitzungs-Sandbox, die externen Zugriff verhindert und beim Sitzungsende zerstört wird. Unabhängige Prompt- und Code-Kontrollen erzwingen reine Leseabfragen, während Audit-Protokolle die Tool-Aktivitäten erfassen und sensible Werte entfernt werden.

Sicherheitsvorkehrungen für die Werkzeugausführung

- Tools mit Autorisierungsbezug arbeiten innerhalb der Berechtigungen des authentifizierten Benutzers.
- Die Zeitüberschreitung bei der Toolausführung begrenzt lang andauernde Operationen.
- Die temporäre Datensandbox speichert die vom Tool abgerufenen Daten im Sitzungsbereich, blockiert externen Zugriff, Datei-I/O, Netzwerkaufrufe und das Laden von Erweiterungen auf Engine-Ebene und wird beim Ende der Sitzung zerstört.
- Die Durchsetzung von Read-only-Abfragen validiert generierte Abfragen anhand einer strikten Allowlist.
- Prompt-erzwungene und Code-erzwungene Sicherheit werden unabhängig voneinander angewendet.
- Die Protokollierung von Toolaufrufen umfasst den Toolnamen, die Parameter, die Zeitstempel und den Ergebnisstatus, wobei sensible Werte bereinigt werden.

Ausgangssteuerungen

- Durchsetzung des Token-Limits
- Deterministische Ausgabe für Klassifizierungs-/sicherheitskritische Operationen (Temperatur 0)
- Streaming mit vorzeitigem Abbruch und Bereinigung

Datenschutz und Verfügbarkeit für NetApp Workload Factory

In NetApp Workload Factory beschränken die Datenschutzkontrollen von Ask Me die Datenexponierung, halten die Sitzungsverarbeitung isoliert und wahren die Datenschutzgrenzen bei Benutzerinteraktionen. Ihre Eingaben werden von einem verwalteten KI-Dienst verarbeitet, der sie nicht zum Trainieren oder zur Verbesserung von Basismodellen verwendet. Abgerufene Betriebsdaten verbleiben für die Dauer der Sitzung im flüchtigen Arbeitsspeicher und werden weder gespeichert noch weitergegeben. Eine Multi-Model-Fallback-Kette über mehrere Cloud-Regionen hinweg unterstützt die Verfügbarkeit, wenn das primäre Modell gedrosselt oder nicht verfügbar ist, wobei dieselben Sicherheitskontrollen auch für die Fallback-Modelle gelten.

Datenverarbeitung und Datenschutz

- Benutzerdaten in Eingabeaufforderungen: werden von einem verwalteten KI-Dienst verarbeitet, der Ihre

Eingaben nicht zum Trainieren oder Verbessern von Basismodellen verwendet.

- Inhalte der Wissensdatenbank: ausschließlich kuratierte, veröffentlichte NetApp Dokumentation; Ihre Daten sind nicht enthalten.
- Betriebsdaten: werden nur abgerufen, wenn ein Benutzer seine eigenen Ressourcen abfragt; werden für die Dauer der Sitzung in einem temporären Speicher im Arbeitsspeicher gehalten und nicht persistent gespeichert oder weitergegeben.
- Audit Protokollierung: Abfragemetadaten (anonymisierte Benutzer-ID, Zeitstempel, Dauer) werden protokolliert, wobei sensible Felder entfernt werden.
- Feedbackdaten: werden separat gespeichert und mit einer Abfrage-ID verknüpft, jedoch nicht mit personenbezogenen Daten über die anonymisierte Benutzer-ID hinaus.

Verfügbarkeits- und Isolationskontrollen

Ask Me verwendet eine Multi-Modell-Fallback-Kette über mehrere Cloud-Regionen.

Wenn das primäre Modell gedrosselt wird oder nicht verfügbar ist, kann das System auf alternative Modelle ausweichen.

Alle Modelle unterliegen denselben Sicherheitskontrollen, der gleichen Systemhärtung und den gleichen Isolationsgarantien.

ONTAP Operationen und Lambda Verbindung (Kunden VPC Komponente)

Informationen zur Lambda-Verbindung für NetApp Workload Factory

NetApp Workload Factory verwendet einen Link, eine in Ihrer VPC bereitgestellte AWS Lambda-Funktion, um ONTAP-native Operationen innerhalb Ihres AWS-Kontos zu belassen, wenn die Amazon FSx for NetApp ONTAP API diese Operationen nicht bereitstellt. Der Link läuft in Ihren Subnetzen und Sicherheitsgruppen, sodass die Ausführungskomponente innerhalb Ihrer AWS-Umgebung bleibt. Workload Factory nutzt den Link nur für Operationen, die direkten ONTAP Zugriff erfordern, anstatt eine verfügbare AWS Service API zu verwenden. Die Architektur des Links wird mit dem Sicherheits- und Betriebsprofil des NetApp Console Agenten verglichen.

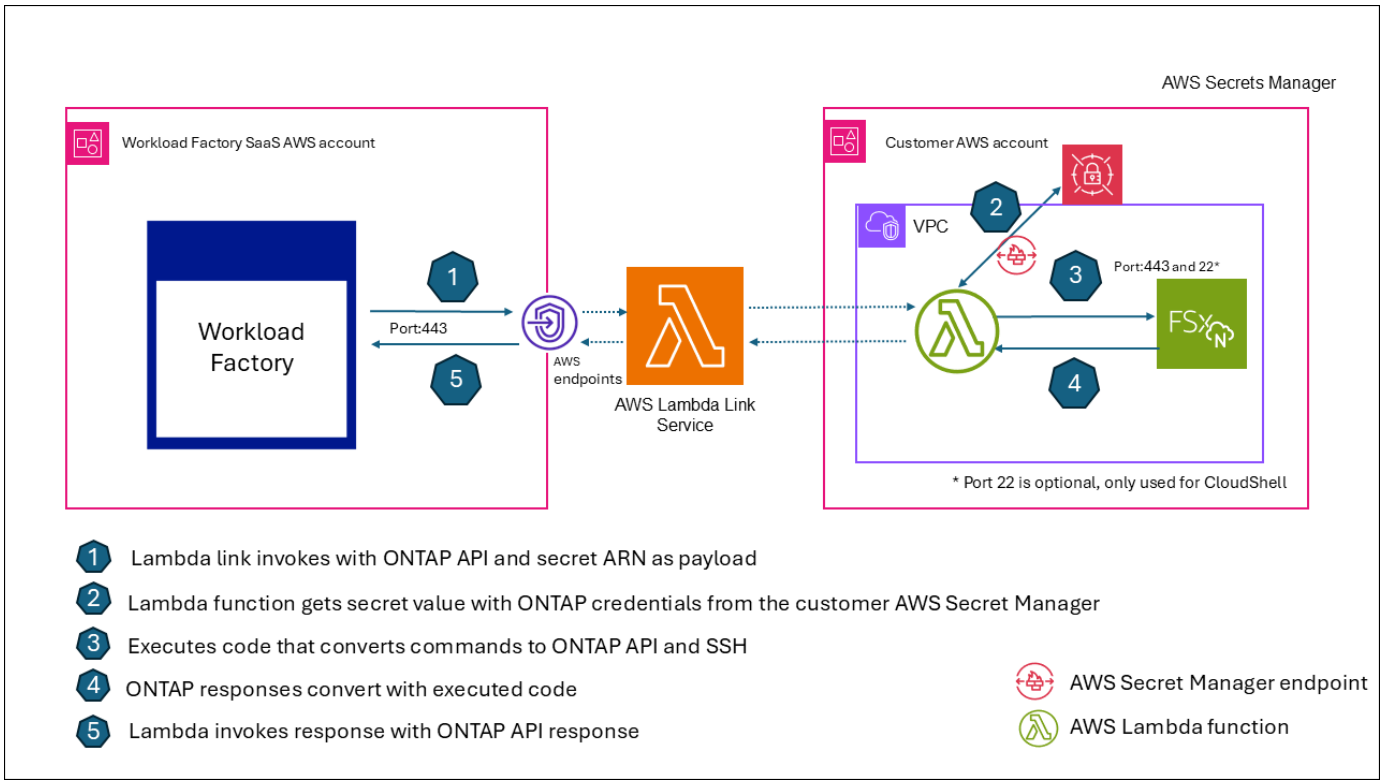
Sicherheitsarchitektur für Verbindungen

Ein Workload Factory Link erstellt eine Vertrauensbeziehung und eine indirekte Konnektivität zwischen einem Workload Factory Account und einem oder mehreren FSx for ONTAP File Systemen.

Die folgende Tabelle bietet einen Überblick über die Lambda Link-Sicherheitsarchitektur. Diese Informationen geben Aufschluss darüber, wie die Lambda-Funktion in Ihrem AWS-Konto bereitgestellt und ausgeführt wird, einschließlich ihrer Netzwerkkonfiguration, Laufzeitumgebung und Betriebsgrenzen.

Eigenschaft	Detail
Compute	AWS Lambda (Container Image)
Laufzeit	Node.js 22
Bereitstellung	CloudFormation Stack in Ihrem AWS Account
VPC Platzierung	Ihre Subnetze, Ihre Sicherheitsgruppen
Zeitüberschreitung	10 Sekunden pro Aufruf
Aufruf	Synchron (RequestResponse)
Pakettyp	Container-Image (aus NetApp ECR)

Das folgende Diagramm zeigt die Sicherheitsarchitektur der Lambda-Verbindung.



Lambda link versus NetApp Console Agent

Die Lambda-Verbindung und der NetApp Console Agent dienen unterschiedlichen Zwecken und haben unterschiedliche Auswirkungen auf Sicherheit und Betrieb.

Dimension	Link (Lambda-basiert)	NetApp Console Agent (VM/Pods-basiert)
Laufzeitmodell	Serverless (AWS Lambda), kundenseitig bereitgestellt	Vom Kunden bereitgestellte VMs/Container; führt NetApp Console Service Pods aus
Primärer Umfang	Control plane ONTAP REST-Operationen (nur wenn AWS-APIs die Operation nicht unterstützen)	Orchestrierung plus Unterstützung für Datendienste
Unterstützung von Datendiensten	Bietet keine Datendienste an	Kann Datendienste hosten (führt NetApp Console Service Pods aus)
Betriebsaufwand	Keine ständig laufende VM	VM Lifecycle Management und Upgrades

Verwandte Informationen

Die vollständige Karte der systemübergreifenden Verbindungen ist unter "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory" zu finden.

Lambda-Link-Ports und Aufrufe für NetApp Workload Factory

NetApp Workload Factory verwendet Lambda-Link-Anfragen und Portgrenzen, um die

erforderliche ausgehende Konnektivität und die durch IAM autorisierte Ausführung zu definieren. Der Link unterstützt HTTPS-Anfragen an den ONTAP Management-Endpunkt, schreibgeschützte SSH-Befehle für Diagnose und Integritätsprüfungen. Die gesamte Konnektivität erfolgt ausgehend vom Link innerhalb Ihrer VPC, sodass keine eingehende Konnektivität oder freigelegte Endpunkte erforderlich sind. Workload Factory nutzt die AWS Lambda API mit IAM-basierter Autorisierung, um den Link aufzurufen.

Anfragetypen

- HTTPS (ONTAP REST API): Proxys HTTPS-Aufrufe an den ONTAP Management-Endpunkt (Port 443) für Volume-, Storage-VM- und Cluster-Operationen.
- SSH (ONTAP CLI): Führt schreibgeschützte ONTAP CLI-Befehle auf Port 22 für Diagnose- und Leistungsdaten aus.
- Gesundheitscheck: Gibt Status und unterstützte Funktionen zurück.

Ausgehende Netzwerkgrenzen

Richtung	Port	Ziel	Zweck
Ausgehend	443	ONTAP Management-IP (innerhalb Ihrer VPC)	REST API-Operationen
Ausgehend	22	ONTAP Management-IP (innerhalb Ihrer VPC)	SSH CLI-Befehle
Ausgehend	443	AWS Secrets Manager Endpoint (optional)	Abruf von Anmeldeinformationen bei Verwendung von Secrets Manager

Es ist keine eingehende Verbindung erforderlich. Der Link stellt keine Endpunkte bereit. Workload Factory ruft ihn mithilfe der AWS `lambda:InvokeFunction` API auf.

Workload Factory ruft Lambda Link auf

Workload Factory ruft die Lambda-Verbindung über die AWS Lambda API (`lambda:InvokeFunction` unter Verwendung einer IAM-basierten Autorisierung auf.

Die Aufrufnutzlast enthält:

- Ziel ONTAP Management-Endpunkt (IP/Hostname)
- Auszuführender Vorgang (REST API-Pfad oder SSH-Befehl)
- Authentifizierungsinformationen (Inline-Anmeldeinformationen oder eine Secrets Manager ARN-Referenz)

Verwandte Informationen

Die vollständige Karte der systemübergreifenden Konnektivität befindet sich unter "Konnektivitäts- und Vertrauenspfade für NetApp Workload Factory".

Lambda Link IAM-Berechtigungen für NetApp Workload Factory

NetApp Workload Factory verwendet Lambda link permission boundaries, um den für die Lambda-Ausführung und den Workload Factory-Aufruf erforderlichen IAM-Zugriff zu definieren. Diese Berechtigungen sind optional, aber für ONTAP native Operationen erforderlich. Bei der Konfiguration der Secrets Manager-Unterstützung ruft der Link ONTAP-Anmeldeinformationen zur Laufzeit direkt aus Ihrem AWS Secrets Manager ab, und das Passwort wird ausschließlich innerhalb Ihrer VPC übertragen, vom Secrets Manager zur Lambda-Funktion und anschließend zum ONTAP Endpoint.

Informationen zu Anfragepfad und Portanforderungen sind unter "Lambda Link-Ports und -Aufrufe" zu finden.

Berechtigungen der Lambda-Ausführungsrolle

Die Lambda-Ausführungsrolle benötigt beim Bereitstellen eines Links in Ihrer VPC die folgenden Berechtigungen:

Berechtigung	Zweck
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	Standardmäßige VPC-gebundene Lambda-Netzwerke
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP Management
secretsmanager:GetSecretValue (beschränkt auf FSxSecret*)	ONTAP Anmeldeinformationen abrufen (nur wenn Secrets Manager aktiviert ist)
CloudWatch Logs (verwaltete Richtlinie)	Lambda-Ausführungsprotokollierung

Berechtigungen zum Aufruf der Workload Factory

Die ressourcenbasierte Richtlinie für Lambda link gewährt dem Serviceprinzipal der Workload Factory die folgenden Berechtigungen:

Berechtigung	Zweck
lambda:InvokeFunction	Die Lambda-Funktion ausführen
lambda:GetFunction	Gesundheits- und Statusprüfungen
lambda:UpdateFunctionCode	Versionsaktualisierungen (Image-Updates)
lambda:GetFunctionConfiguration	Konfigurationsprüfung

Lebenszyklus der Lambda-Verbindung für NetApp Workload Factory

NetApp Workload Factory nutzt Lambda-Link-Lebenszyklussteuerungen, um Bereitstellung, Zustandsüberwachung und kontrollierte Image-Updates mit minimalem

Betriebsaufwand zu verwalten. Das Container-Image des Lambda-Links kann aktualisiert werden, um Verbesserungen oder Sicherheitspatches bereitzustellen, ohne den Amazon CloudFormation Stack neu bereitzustellen, unter Verwendung der `lambda:UpdateFunctionCode` Berechtigung. Die Lebenszyklussteuerungen definieren außerdem, wie die Link-Gesundheit überwacht wird und wie der Lambda-Link sowie die zugehörigen Ressourcen entfernt werden, wenn sie nicht mehr benötigt werden.

Lebenszyklus-Kontrollpunkte

- Bereitstellung: automatisiert über Amazon CloudFormation oder Terraform Stack-Bereitstellung
- Überwachung: Systemprüfungen erkennen Verbindungsprobleme; Fehlerzähler verfolgen die Zuverlässigkeit
- Entfernung: Das Löschen des CloudFormation Stacks entfernt die Lambda-Funktion und die zugehörigen Ressourcen aus Ihrem AWS-Konto.

Wissen und Unterstützung

Bei NetApp Support registrieren

Bevor ein Support-Ticket beim NetApp technischen Support eröffnet werden kann, ist es erforderlich, ein NetApp Support Site-Konto zu Workload Factory hinzuzufügen und sich anschließend für den Support zu registrieren.

Für den Erhalt von technischem Support speziell für NetApp Workload Factory sowie deren Speicherlösungen und Services ist eine Supportregistrierung erforderlich. Die Registrierung für den Support erfolgt über die NetApp Console, eine separate webbasierte Konsole, die sich von Workload Factory unterscheidet.

Die Registrierung für den Support aktiviert keinen NetApp Support für einen Dateidienst eines Cloud-Anbieters. Technischer Support zu einem Dateidienst eines Cloud-Anbieters, dessen Infrastruktur oder zu Lösungen, die diesen Dienst nutzen, ist im Abschnitt „Getting help“ in der Workload Factory Dokumentation für das jeweilige Produkt zu finden.

"Amazon FSx for ONTAP"

Übersicht der Supportregistrierung

Die Registrierung Ihres Support-Abonnements mit Ihrer Konto-ID (Ihre 20-stellige Seriennummer 960xxxxxxxx, die auf der Seite „Support Resources“ in der NetApp Console zu finden ist) dient als Ihre einzelne Support-Abonnement-ID. Jedes NetApp Support-Abonnement auf Kontoebene muss registriert werden.

Durch die Registrierung werden Funktionen wie das Erstellen von Support-Tickets und die automatische Fallgenerierung freigeschaltet. Die Registrierung wird abgeschlossen, indem NetApp Support Site (NSS)-Konten der NetApp Console wie unten beschrieben hinzugefügt werden.

Registrieren Sie Ihr Konto für den NetApp Support

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer Ihres Kontos ein NetApp Support Site-Konto mit seinem NetApp Console-Login verknüpfen. Wie die Registrierung für den NetApp Support erfolgt, hängt davon ab, ob bereits ein NetApp Support Site-Konto (NSS-Konto) vorhanden ist.

Bestandskunde mit einem NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, ist lediglich eine Registrierung für den Support über die NetApp Console erforderlich.

Schritte

1. Oben rechts in der Workload Factory Console **Hilfe > Support** auswählen.

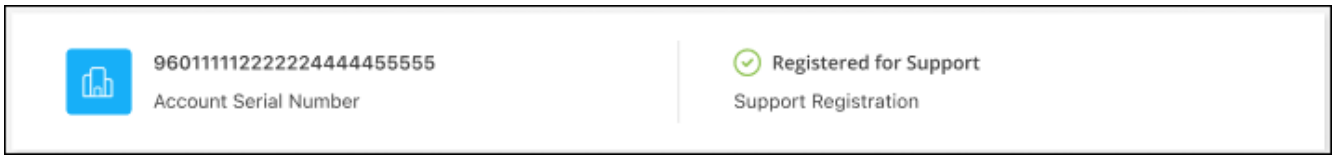
   Durch Auswahl dieser Option öffnet sich die NetApp Console in einem neuen Browser-Tab und das Support-Dashboard wird geladen.

2. Im NetApp Console-Menü **Administration** auswählen und dann **Anmeldeinformationen** auswählen.
3. **Benutzeranmeldeinformationen** auswählen.
4. **NSS-Anmeldeinformationen hinzufügen** auswählen und der Authentifizierungsaufforderung der NetApp

Support Site (NSS) folgen.

5. Zur Bestätigung, dass der Registrierungsvorgang erfolgreich war, das Hilfesymbol auswählen und anschließend **Support** wählen.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konto für den Support registriert ist.



   Beachten Sie, dass andere NetApp Console-Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie kein NetApp Support Site-Konto mit ihrem NetApp Console-Login verknüpft haben. Das bedeutet jedoch nicht, dass Ihr NetApp Konto nicht für den Support registriert ist. Solange mindestens ein Benutzer im Konto diese Schritte durchgeführt hat, ist Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über bestehende Lizenzen und Seriennummern, aber *kein* NSS-Konto verfügen, ist die Erstellung eines NSS-Kontos erforderlich, das mit Ihrem NetApp Console Login verknüpft wird.

Schritte

1. Ein NetApp Support Site-Konto kann erstellt werden, indem das "NetApp Support Site Benutzerregistrierungsformular" Formular ausgefüllt wird.
   a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
   b. Stellen Sie sicher, dass Sie die oben verwendete NetApp Kontoseriennummer (960xxxx) für das Feld Seriennummer kopieren. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ihr neues NSS-Konto kann mit Ihrem NetApp Console-Login verknüpft werden, indem die Schritte unter Bestandskunde mit einem NSS-Konto abgeschlossen werden.

Ganz neu bei NetApp

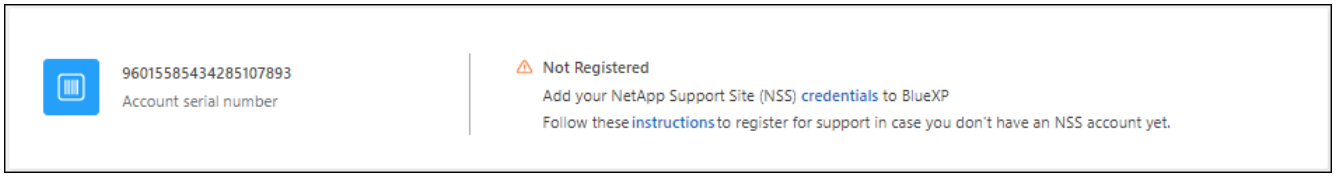
Wenn Sie ganz neu bei NetApp sind und kein NSS-Konto haben, führen Sie die folgenden Schritte aus.

Schritte

1. Oben rechts in der Workload Factory Console **Hilfe > Support** auswählen.

   Durch Auswahl dieser Option öffnet sich die NetApp Console in einem neuen Browser-Tab und das Support-Dashboard wird geladen.

2. Die Konto-ID-Seriennummer befindet sich auf der Seite „Supportressourcen“.



3. Navigieren Sie zu "NetApp’s Support-Registrierungsseite" und wählen Sie **Ich bin kein registrierter NetApp Customer** aus.

4. Füllen Sie die Pflichtfelder (die mit roten Sternchen) aus.
5. Im Feld **Produktlinie** wird **Cloud Manager** ausgewählt und anschließend der entsprechende Abrechnungsanbieter.
6. Kopieren Sie Ihre Kontoseriennummer aus Schritt 2 oben, führen Sie die Sicherheitsprüfung durch und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

   Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an die angegebene Adresse gesendet. Es empfiehlt sich, den Spam-Ordner zu überprüfen, falls die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Die Aktion wird direkt in der E-Mail bestätigt.

   Mit der Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, ein NetApp Support Site-Konto zu erstellen.

8. Ein NetApp Support Site-Konto kann erstellt werden, indem das "NetApp Support Site Benutzerregistrierungsformular" Formular ausgefüllt wird.
   a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
   b. Bitte kopieren Sie die oben angegebene Kontoseriennummer (960xxxx) in das Feld „Seriennummer“. Dies beschleunigt die Kontoverarbeitung.

Nachdem Sie fertig sind

NetApp sollte sich während dieses Prozesses mit Ihnen in Verbindung setzen. Dies ist eine einmalige Einführungsmaßnahme für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, kann das Konto mit Ihrem NetApp Console-Login verknüpft werden, indem die Schritte unter Bestandskunde mit einem NSS-Konto abgeschlossen werden.

Hilfe zu FSx for ONTAP für NetApp Workload Factory erhalten

NetApp bietet Unterstützung für Workload Factory und seine Cloud-Services auf vielfältige Weise. Umfangreiche kostenlose Selbsthilfeoptionen stehen 24x7 zur Verfügung, wie zum Beispiel Knowledgebase (KB)-Artikel und ein Community-Forum. Die Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Support für FSx für ONTAP erhalten

Technische Unterstützung zu FSx for ONTAP, seiner Infrastruktur oder einer Lösung, die diesen Dienst nutzt, ist im Abschnitt „Hilfe erhalten“ in der Workload Factory Dokumentation für dieses Produkt zu finden.

"Amazon FSx for ONTAP"

Technischer Support speziell für Workload Factory sowie die zugehörigen Speicherlösungen und -dienste steht über die nachfolgend beschriebenen Supportoptionen zur Verfügung.

Selbsthilfeoptionen verwenden

Diese Optionen stehen Ihnen kostenlos 24 Stunden am Tag, 7 Tage die Woche zur Verfügung:

- Dokumentation

  Die Workload Factory Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  In der Workload Factory Wissensdatenbank finden sich hilfreiche Artikel zur Fehlerbehebung.

- "Communities"

  Der Workload Factory Community beitreten, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

Einen Fall beim NetApp Support erstellen

Zusätzlich zu den oben genannten Selbsthilfeoptionen können Sie nach der Aktivierung des Supports mit einem NetApp Support-Spezialisten zusammenarbeiten, um etwaige Probleme zu lösen.

Bevor Sie beginnen

Um die Funktion **Create a Case** zu nutzen, ist zunächst eine Registrierung für den Support erforderlich. Die NetApp Support Site-Anmeldedaten müssen mit dem Workload Factory-Login verknüpft werden. "Informationen zur Registrierung für den Support".

Schritte

1. Oben rechts in der Workload Factory Console **Hilfe > Support** auswählen.

   Durch Auswahl dieser Option öffnet sich die NetApp Console in einem neuen Browser-Tab und das Support-Dashboard wird geladen.

2. Auf der Seite **Ressourcen** steht unter Technischer Support eine der verfügbaren Optionen zur Auswahl:

   a. **Kontaktieren Sie uns** kann ausgewählt werden, wenn ein Telefongespräch mit einer Ansprechperson gewünscht ist. Eine Weiterleitung erfolgt auf eine Seite auf netapp.com, auf der die Telefonnummern aufgeführt sind, die angerufen werden können.

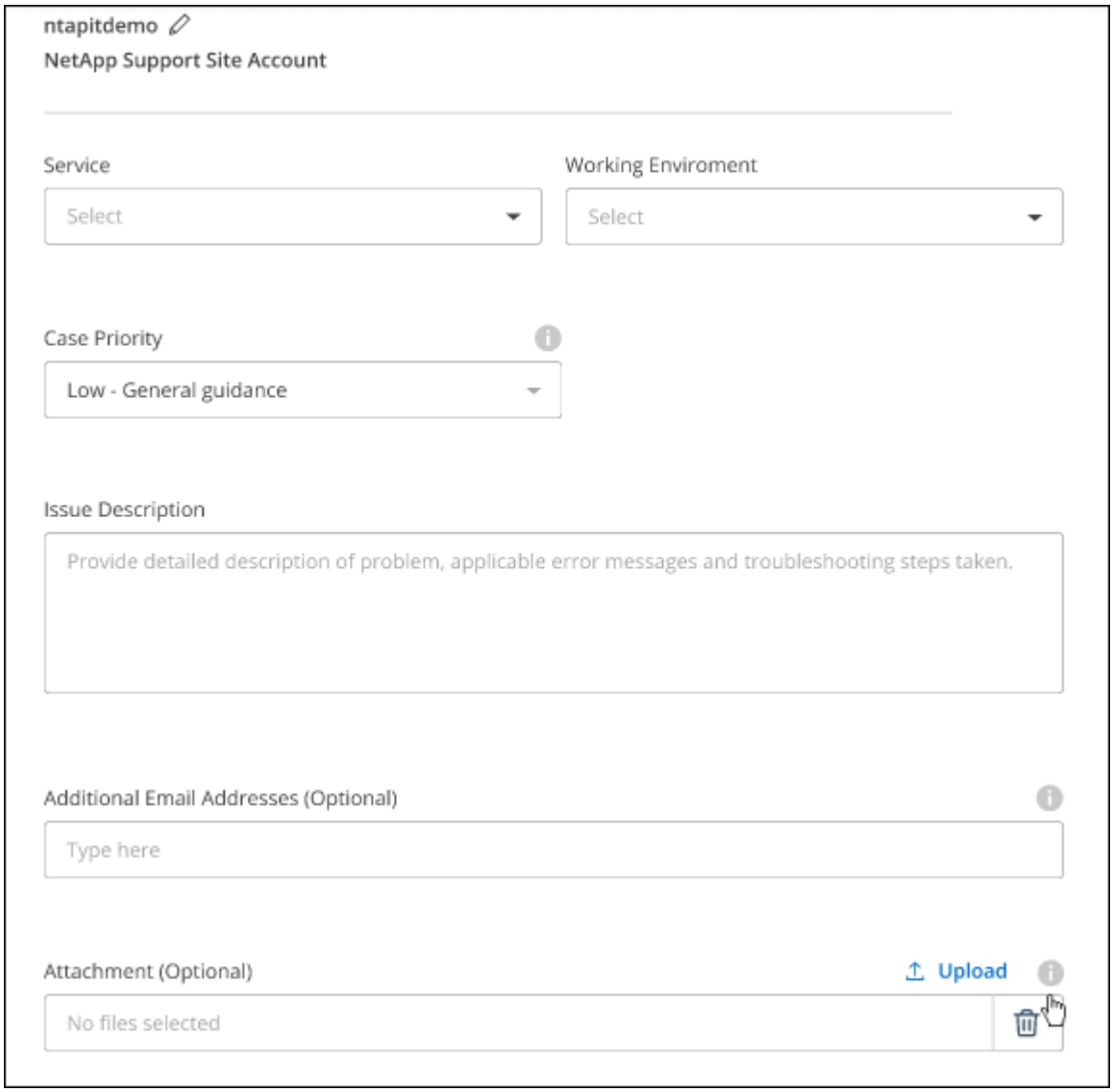
   b. **Fall erstellen** auswählen, um ein Ticket bei einem NetApp Support-Spezialisten zu eröffnen:

      - **Service**: **Workload Factory** auswählen.
      - **Fallpriorität**: Die Priorität des Falls kann auf Niedrig, Mittel, Hoch oder Kritisch gesetzt werden.

        Weitere Details zu diesen Prioritäten werden angezeigt, wenn der Mauszeiger über das Informationssymbol neben dem Feldnamen gehalten wird.

      - **Problembeschreibung**: Eine detaillierte Beschreibung des Problems, einschließlich aller relevanten Fehlermeldungen oder durchgeführten Schritte zur Fehlerbehebung.
      - **Weitere E-Mail-Adressen**: Zusätzliche E-Mail-Adressen können eingegeben werden, um eine andere Person auf dieses Problem aufmerksam zu machen.
      - **Anhang (optional)**: Bis zu fünf Anhänge können einzeln hochgeladen werden.

        Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nachdem Sie fertig sind

Es erscheint ein Pop-up mit Ihrer Support-Fallnummer. Ein NetApp Support-Spezialist prüft Ihren Fall und meldet sich in Kürze bei Ihnen.

Für eine Historie Ihrer Supportfälle kann **Einstellungen > Zeitleiste** ausgewählt und nach Aktionen mit dem Namen „Supportfall erstellen“ gesucht werden. Eine Schaltfläche ganz rechts ermöglicht das Erweitern der Aktion, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Case für den ausgewählten Service zu erstellen.“

Dieser Fehler kann bedeuten, dass das NSS-Konto und das zugehörige Unternehmen nicht mit dem Unternehmen übereinstimmen, das für die NetApp Console-Konto-Seriennummer (z. B. 960xxxx) oder die Systemseriennummer als Unternehmen der Registrierung geführt ist. Hilfe ist über eine der folgenden Optionen erhältlich:

- Den In-Product-Chat verwenden
- Einen nicht-technischen Fall einreichen unter https://mysupport.netapp.com/site/help

Supportfälle verwalten (Vorschau)

Aktive und abgeschlossene Supportfälle lassen sich direkt über die NetApp Console anzeigen und verwalten. Die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle lassen sich verwalten.

Das Fallmanagement ist als Vorschauversion verfügbar. Es ist vorgesehen, diese Funktion in zukünftigen Versionen weiter zu optimieren und zu erweitern. Feedback kann über den In-App-Chat übermittelt werden.

Dabei ist Folgendes zu beachten:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der in den letzten 3 Monaten über das von Ihnen angegebene NSS-Benutzerkonto eröffneten Fälle.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die sich auf die von Ihnen ausgewählte Ansicht beziehen.
- Sie können Spalten Ihrer Wahl hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten lediglich Sortierfunktionen.

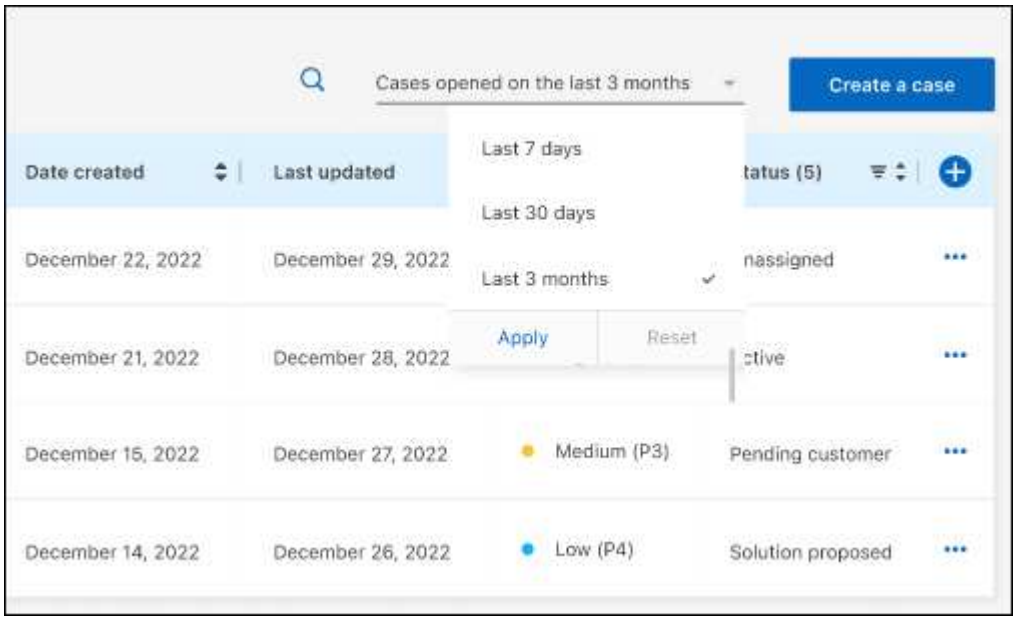
  Die folgenden Schritte enthalten weitere Details.
- Auf Ebene einzelner Fälle besteht die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Vorläufig abgeschlossen“ befindet.

Schritte

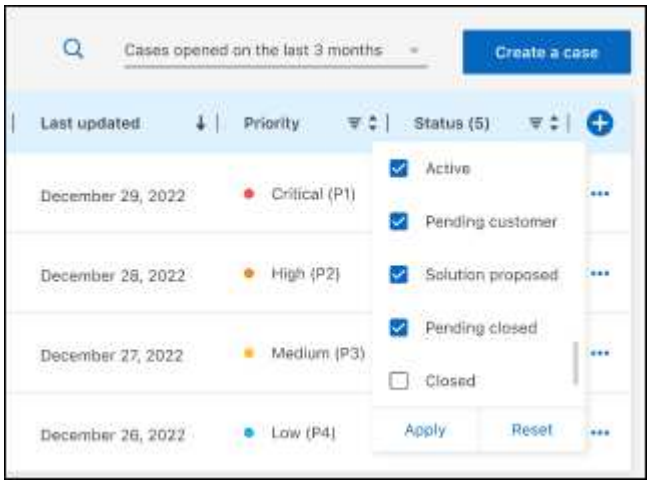
1. Oben rechts in der Workload Factory Console **Hilfe > Support** auswählen.

   Durch Auswahl dieser Option wird die NetApp Console in einem neuen Browser-Tab geöffnet und das Support-Dashboard geladen.
2. **Fallmanagement** auswählen und gegebenenfalls das NSS-Konto zur NetApp Console hinzufügen.

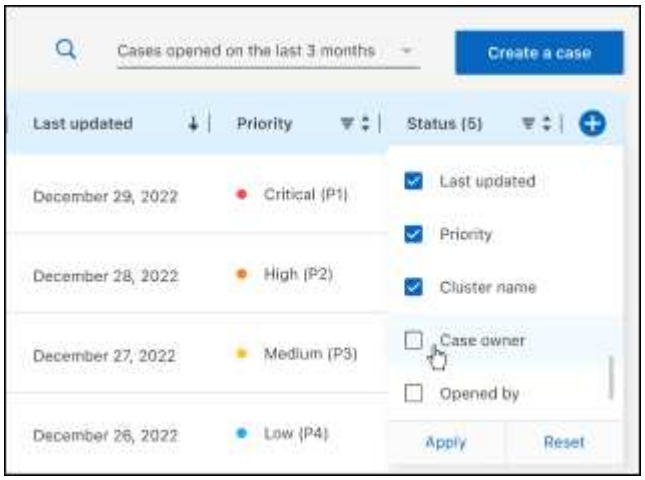
   Die Seite **Fallverwaltung** zeigt offene Fälle an, die mit dem NSS-Konto verknüpft sind, das Ihrem NetApp Console-Benutzerkonto zugeordnet ist. Dies ist dasselbe NSS-Konto, das oben auf der Seite **NSS management** angezeigt wird.
3. Optional können die in der Tabelle angezeigten Informationen geändert werden:
   - Unter **Fälle der Organisation** auf **Anzeigen** auswählen, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
   - Der Datumsbereich kann geändert werden, indem entweder ein genauer Datumsbereich oder ein anderer Zeitraum ausgewählt wird.



- Der Inhalt der Spalten filtern.



- Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie ⊕ auswählen und dann die Spalten wählen, die Sie anzeigen möchten.

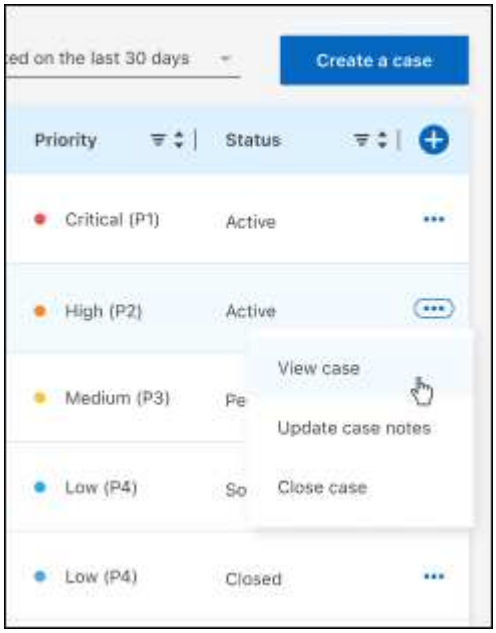


4. Verwalten Sie einen bestehenden Fall, indem Sie ••• eine der verfügbaren Optionen auswählen:

   - **Fall ansehen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Zusätzliche Details zu Ihrem Problem können angegeben oder **Dateien hochladen** ausgewählt werden, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Einzelheiten dazu an, warum Sie den Fall schließen, und wählen Sie **Fall schließen** aus.



Rechtliche Hinweise für NetApp Workload Factory

Rechtliche Hinweise bieten Zugriff auf Urheberrechtsvermerke, Marken, Patente und mehr.

Copyright

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

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp Trademarks-Seite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

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

Patente

Eine aktuelle Liste der NetApp owned patents finden Sie unter:

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

Datenschutzrichtlinie

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

Open Source

Hinweisdateien enthalten Informationen über Urheberrechte und Lizenzen Dritter, die in NetApp Software verwendet werden.

"NetApp Workload Factory"