Identität, Anmeldeinformationen und das Prinzip der minimalen Berechtigungen

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

Identität, Anmeldeinformationen und das Prinzip der minimalen Berechtigungen . . . 1
- AWS-Kontointegration für NetApp Workload Factory . . . 1
  - AWS Konto Konfiguration . . . 1
  - Laufzeit . . . 1
- Wie AWS-Anmeldeinformationen durch die NetApp Workload Factory fließen . . . 2
  - Einmalige Einrichtung . . . 2
  - Laufzeit (jede API-Operation) . . . 2
  - Sitzungsrichtlinie . . . 3
  - Verwandte Informationen . . . 3
- Aufbewahrung von AWS-Anmeldeinformationen für NetApp Workload Factory . . . 3
  - Wichtige Verhaltensweisen . . . 3
  - Zusammenfassung zu Aufbewahrung und Speicherung . . . 3
  - Sicherheitskontrollen . . . 4
- Anmeldeinformationstypen für NetApp Workload Factory . . . 5
  - Anmeldeinformationstypen . . . 5
  - AWS-Anmeldeinformationsbasierte Operationen . . . 5
  - ONTAP Anmeldeinformationen Operationen . . . 5
  - Vorgänge, die sowohl AWS- als auch ONTAP Anmeldeinformationen erfordern . . . 6
  - Verwandte Informationen . . . 6
- Optionen zur Speicherung von Anmeldeinformationen für NetApp Workload Factory . . . 6
  - Schreibgeschütztes ONTAP Zugriffsmodell . . . 7
  - Vergleich der Optionen zur Speicherung von Anmeldeinformationen . . . 7
  - Weitere Überlegungen . . . 7
- Berechtigungsstufen mit minimalen Rechten für NetApp Workload Factory . . . 8
  - Gestuftes Berechtigungsmodell . . . 8
  - Erteilung von Berechtigungen . . . 8
  - Sicherheitskontrollen . . . 8
  - Berechtigungsdokumentation . . . 8
- Amazon CloudWatch Überwachungsberechtigungen für NetApp Workload Factory . . . 9
  - Erforderliche CloudWatch Überwachungsberechtigungen . . . 9

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