Sicherheitsmodell und Verantwortlichkeiten

Information Security for Workload Factory

NetApp
September 16, 2026

Inhalt

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.