Sicherheitskontrollen für generative KI

Information Security for Workload Factory

NetApp
September 16, 2026

This PDF was generated from https://docs.netapp.com/de-de/workload-infosec/ai-controls-overview.html on September 16, 2026. Always check docs.netapp.com for the latest.

Inhalt

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.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.