



Chiedimi assistente AI

Information Security for Workload Factory

NetApp

September 16, 2026

This PDF was generated from <https://docs.netapp.com/it-it/workload-infosec/ask-me-security-architecture.html> on September 16, 2026. Always check docs.netapp.com for the latest.

Sommario

- Chiedimi assistente AI 1
 - Chiedimi l'architettura di sicurezza per NetApp Workload Factory 1
 - Architettura RAG in Ask Me 1
 - Sicurezza multi-livello dei prompt..... 1
 - Isolamento e privacy dei dati del modello 1
 - Uso degli strumenti e sicurezza agentica 2
 - Chiedimi il controllo degli accessi per NetApp Workload Factory 2
 - Autenticazione 2
 - Protezione delle credenziali e gestione dei segreti 2
 - Sicurezza delle infrastrutture 2
 - Chiedimi le modalità di esecuzione per NetApp Workload Factory 3
 - Salvaguardie per l'esecuzione degli strumenti..... 3
 - controlli di output 3
 - Chiedimi informazioni su privacy e disponibilità per NetApp Workload Factory 3
 - Gestione dei dati e privacy..... 4
 - Controlli di disponibilità e isolamento..... 4

Chiedimi assistente AI

Chiedimi l'architettura di sicurezza per NetApp Workload Factory

Ask Me è un assistente generativo basato sull'intelligenza artificiale integrato in NetApp Workload Factory. Fornisce supporto conversazionale in real-time per Amazon FSx for NetApp ONTAP e argomenti di Workload Factory. Le risposte si basano su documentazione NetApp verificata e Ask Me non può accedere a Internet pubblico né utilizzare i dati dei clienti per addestrare il modello. Diversi livelli di sicurezza aiutano a bloccare le query dannose, limitare le risposte ai domini supportati e impedire che l'input dell'utente sovrascriva le istruzioni di sistema. Quando Ask Me utilizza strumenti, i limiti di autorizzazione, l'applicazione di query di sola lettura, una sandbox temporanea e la registrazione degli eventi aiutano a limitare e monitorare l'esecuzione.

Puoi disattivare Ask Me in qualsiasi momento tramite le impostazioni di **Amministrazione** di Workload Factory, il che disabilita l'assistente per il tuo account utente. ["Scopri di più sulla gestione delle funzionalità di GenAI."](#)

Architettura RAG in Ask Me

Ask Me utilizza la generazione aumentata tramite recupero (RAG).

- Base di conoscenza curata: le risposte si basano su un corpus gestito di documentazione NetApp verificata e pubblicata.
- Valutazione e filtraggio del recupero: solo i contenuti sufficientemente pertinenti sono inclusi nel contesto del modello.
- Nessun accesso a Internet: il modello non può recuperare, visualizzare o estrarre contenuti esterni.
- Attribuzione della fonte: le risposte includono riferimenti ai documenti di origine utilizzati.

Sicurezza multi-livello dei prompt

- Livello 1: il classificatore di sicurezza (LLM-as-a-judge) blocca le query dannose (iniezione di prompt, escalation dei privilegi, esfiltrazione di dati, ingegneria sociale, violazioni delle policy).

Il sistema registra le query bloccate e il modello generativo non le vede mai.

- Livello 2: L'irrobustimento del prompt di sistema impedisce che l'input dell'utente sovrascriva le istruzioni di sistema.
- Livello 3: l'ambito del dominio limita le risposte agli argomenti FSx ONTAP e Workload Factory.
- Livello 4: La governance dell'utilizzo degli strumenti convalida i parametri ed esegue le query in un ambiente protetto; il modello non può eseguire operazioni arbitrarie.

Isolamento e privacy dei dati del modello

- Nessun addestramento del modello sui dati dei clienti
- Isolamento a livello di richiesta (nessuna perdita di dati tra tenant)

- Contesto di conversazione a livello di sessione con cronologia delimitata
- Nessuna memoria modello persistente
- Infrastruttura di inferenza gestita

Uso degli strumenti e sicurezza agentica

- Strumenti con ambito di autorizzazione (limiti di autorizzazione utente applicati)
- Rigorosi timeout di esecuzione degli strumenti
- Sandbox effimera, limitata alla sessione, per i dati recuperati
- Applicazione delle query di sola lettura con allowlisting
- Tracciabilità delle chiamate degli strumenti con pulizia dei parametri sensibili

Chiedimi il controllo degli accessi per NetApp Workload Factory

In NetApp Workload Factory, la sicurezza di accesso di Ask Me si basa su sessioni autenticate, responsabilità a livello utente e gestione protetta dei segreti durante le operazioni in fase di esecuzione. I controlli di autenticazione convalidano ogni sessione e associano le interazioni a un utente specifico. Le credenziali sensibili vengono recuperate da un archivio di segreti gestito in fase di esecuzione e oscurate nei log. Il servizio applica anche controlli infrastrutturali, tra cui l'esecuzione di container senza privilegi di root e una lista di autorizzazioni CORS limitata.

Autenticazione

- Autenticazione JWT firmata con convalida crittografica (inclusi controlli su audience, issuer e algoritmo come RS256)
- Autenticazione imposta dal middleware al confine del servizio
- Definizione dell'ambito dell'identità utente così che le interazioni siano attribuibili a un utente specifico

Protezione delle credenziali e gestione dei segreti

- Archiviazione sicura nel vault: le credenziali sensibili utilizzate dal servizio vengono archiviate in un vault di segreti gestito e recuperate in fase di esecuzione. Nessun segreto viene memorizzato nel codice dell'applicazione, nei file di configurazione o nelle immagini dei container.
- Pulizia dei log: i valori sensibili (credenziali, token, password, chiavi di accesso, certificati) vengono oscurati dai log prima che siano scritti.

Sicurezza delle infrastrutture

- Esecuzione di container non root
- CORS limitato a una lista esplicita di domini attendibili NetApp

Chiedimi le modalità di esecuzione per NetApp Workload Factory

NetApp Workload Factory offre diverse modalità di esecuzione per Ask Me, ognuna con caratteristiche di sicurezza e privacy differenti. Quando Ask Me utilizza integrazioni con strumenti, ad esempio interrogando le risorse Workload Factory del cliente, l'esecuzione dello strumento è controllata tramite misure di sicurezza a più livelli. L'esecuzione abilitata dallo strumento opera entro i limiti delle autorizzazioni dell'utente autenticato e applica limiti alla durata e all'ambito di ciascuna operazione. I dati recuperati rimangono in una sandbox di sessione temporanea che blocca l'accesso esterno e viene eliminata al termine della sessione. Controlli indipendenti su prompt e codice impongono query di sola lettura, mentre i registri di audit registrano l'attività dello strumento con i valori sensibili rimossi.

Salvaguardie per l'esecuzione degli strumenti

- Gli strumenti con ambito di autorizzazione operano entro le autorizzazioni dell'utente autenticato.
- Il timeout di esecuzione dello strumento limita le operazioni di lunga durata.
- La sandbox di dati effimeri memorizza i dati recuperati dagli strumenti nell'ambito della sessione, blocca l'accesso esterno, l'I/O dei file, le chiamate di rete e il caricamento delle estensioni a livello del motore e viene distrutta al termine della sessione.
- L'applicazione della modalità di sola lettura alle query convalida le query generate tramite una rigorosa allowlist.
- La sicurezza basata su prompt e quella basata su codice vengono applicate in modo indipendente.
- La tracciabilità delle chiamate agli strumenti registra il nome dello strumento, i parametri, i timestamp e lo stato del risultato, con la rimozione dei valori sensibili.

controlli di output

- applicazione del limite di token
- Output deterministico per operazioni di classificazione/sicurezza-critical (temperatura 0)
- Streaming con terminazione anticipata e pulizia

Chiedimi informazioni su privacy e disponibilità per NetApp Workload Factory

In NetApp Workload Factory, i controlli sulla privacy di Ask Me limitano l'esposizione dei dati, mantengono isolata l'elaborazione delle sessioni e preservano i confini della privacy per le interazioni con gli utenti. I tuoi input vengono elaborati da un servizio di intelligenza artificiale gestito che non li utilizza per addestrare o migliorare i modelli di base. I dati operativi recuperati rimangono in una memoria temporanea, in-memory, per la durata della sessione e non vengono memorizzati o condivisi. Una catena di fallback multi-modello distribuita su più regioni cloud garantisce la disponibilità quando il modello principale è limitato o non disponibile, mentre gli stessi controlli di sicurezza si applicano

ai modelli di fallback.

Gestione dei dati e privacy

- Dati utente nei prompt: elaborati da un servizio AI gestito che non utilizza i tuoi input per addestrare o migliorare i foundation models.
- Contenuto della knowledge base: solo documentazione curata e pubblicata NetApp; i tuoi dati non sono inclusi.
- Dati operativi: recuperati solo quando un utente interroga le proprie risorse; conservati in memoria temporanea per la durata della sessione e non persistenti né condivisi.
- Registrazione degli eventi di controllo: metadati delle query (ID utente anonimizzato, timestamp, durate) registrati, con i campi sensibili oscurati.
- Dati di feedback: memorizzati separatamente e collegati a un ID di query, non a informazioni di identificazione personale oltre all'ID utente anonimizzato.

Controlli di disponibilità e isolamento

Ask Me utilizza una catena di fallback multi-modello su più regioni cloud.

Se il modello principale è sovraccarico o non disponibile, il sistema può passare a modelli alternativi.

Tutti i modelli sono soggetti agli stessi controlli di sicurezza, allo stesso hardening del sistema e alle stesse garanzie di isolamento.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.