Modello di sicurezza e responsabilità

Information Security for Workload Factory

NetApp
September 16, 2026

Sommario

Modello di sicurezza e responsabilità

Scopri il modello di sicurezza per NetApp Workload Factory

NetApp Workload Factory è un piano di controllo SaaS che ti aiuta a gestire e ottimizzare i carichi di lavoro che vengono eseguiti su Amazon FSx for NetApp ONTAP nel tuo ambiente AWS. I risultati in termini di sicurezza dipendono dalla condivisione delle responsabilità tra NetApp, AWS e la tua organizzazione.

Modello di sicurezza di alto livello

- Workload Factory utilizza un modello IAM assume-role per ottenere credenziali AWS STS temporanee per chiamare le API AWS nel tuo account.
- Alcuni flussi di lavoro richiedono operazioni native di ONTAP non esposte tramite le API di AWS; puoi eseguire tali operazioni all'interno della tua VPC utilizzando componenti di esecuzione distribuiti dal cliente (ad esempio, Lambda link).
- I segnali di osservabilità (metriche, telemetria e registrazioni operative) supportano il monitoraggio operativo e le indagini.

Domande chiave della revisione

- Di quali accessi ha bisogno Workload Factory al tuo account AWS (attendibilità del ruolo + autorizzazioni)?
- Quali percorsi di esecuzione si applicano ai flussi di lavoro previsti (solo API AWS o operazioni native ONTAP tramite un componente VPC)?
- Quali categorie di dati vengono gestite (configurazione/metadati, log/eventi operativi, telemetria) e dove vengono memorizzate?
- Quali segnali di monitoraggio esistono e quali sono le loro caratteristiche di conservazione?

Cosa c'è dopo

- "Confini di responsabilità condivisa per NetApp Workload Factory"
- "Connettività e percorsi di fiducia per NetApp Workload Factory"
- "Livelli di autorizzazione a privilegio minimo per NetApp Workload Factory"

Confini di responsabilità condivisa per NetApp Workload Factory

La responsabilità della sicurezza di NetApp Workload Factory è condivisa tra NetApp (gestione SaaS), AWS (infrastruttura cloud e servizi gestiti) e te (configurazione del cliente). Capire dove inizia e finisce la responsabilità di ciascuna parte ti aiuta a configurare correttamente il tuo ambiente AWS ed evitare falle di sicurezza. Questi confini chiariscono cosa gestisce NetApp, cosa protegge AWS e cosa devi configurare e mantenere tu stesso.

NetApp responsabilità (lato servizio)

NetApp è responsabile del funzionamento e della sicurezza della piattaforma SaaS Workload Factory. Questo include la gestione lato servizio dei riferimenti di configurazione memorizzati e dei dati operativi.

Responsabilità di AWS (piattaforma cloud)

AWS è responsabile della sicurezza dell'infrastruttura cloud e dei servizi gestiti utilizzati dalla tua implementazione e dai tuoi flussi di lavoro (ad esempio, IAM/STS, FSx per ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda e primitive di rete).

Responsabilità del cliente (la tua configurazione)

Sei responsabile di:

- Ruoli AWS IAM, criteri di attendibilità e autorizzazioni basate sul principio del minimo privilegio
- Controlli VPC (sottoreti, gruppi di sicurezza, routing, endpoint ed egress)
- Gestione delle credenziali (incluse le credenziali ONTAP, se richieste dai tuoi flussi di lavoro)
- Decisioni relative alla crittografia e alla gestione delle chiavi (ad esempio, chiavi KMS gestite dal cliente opzionali per FSx per ONTAP)
- Monitoraggio, allerta, politiche di conservazione e processi di risposta agli incidenti

Prove da catturare

- Relazione di trust del ruolo IAM (inclusa la condizione di external ID)
- Selezione del livello di autorizzazione IAM e artefatti delle policy
- Decisione sul confine della rete (solo API AWS vs componente di esecuzione VPC come Lambda link)
- Decisioni relative all'osservabilità e aspettative di conservazione
- Decisione sull'abilitazione dell'AI (la diagnostica dell'AI è abilitata per impostazione predefinita, a meno che non venga disabilitata esplicitamente)

NetApp Workload Factory flusso di lavoro di sicurezza per l'onboarding

La procedura di onboarding a NetApp Workload Factory stabilisce un accesso sicuro al tuo ambiente AWS prima che tu inizi a utilizzare il prodotto. Il processo combina la configurazione della fiducia AWS, la definizione dell'ambito delle autorizzazioni, la configurazione della connettività, la verifica dell'osservabilità e l'abilitazione opzionale della diagnostica AI.

Passaggio 1: Decidi il tuo approccio all'onboarding

- Identifica gli account AWS e i confini degli ambienti (ad esempio, separazione tra prod e non-prod).
- Identifica i flussi di lavoro richiesti (scoperta in sola lettura, provisioning o operazioni native di ONTAP).
- Decidi se implementare i componenti di esecuzione VPC (ad esempio, Lambda link) in base alle esigenze del flusso di lavoro.

- Decidi se abilitare la diagnostica AI (abilitata per impostazione predefinita).

Informazioni correlate

- "Tipi di credenziali"
- "Panoramica del collegamento Lambda"
- "Panoramica dei controlli dell'IA"

Passaggio 2: Stabilire la fiducia e l'accesso ad AWS

1. Distribuisci un ruolo IAM nel tuo account AWS.
2. Assunzione del ruolo gate tramite un ID esterno nella trust policy.
3. Registra l'ARN del ruolo e l'ID esterno in Workload Factory.

Informazioni correlate

"Integrazione account AWS"

Passaggio 3: Applica le autorizzazioni con privilegi minimi

1. Seleziona il livello minimo di autorizzazione che supporta i flussi di lavoro che intendi utilizzare.
2. Verifica che le policy di sessione per richiesta limitino le azioni all'operazione in corso di esecuzione.

Informazioni correlate

"Livelli di autorizzazione a privilegio minimo per NetApp Workload Factory".

Passaggio 4: Configura la connettività e i limiti VPC (se necessario)

1. Convalida i percorsi di rete richiesti per gli endpoint AWS.
2. Se hai bisogno di operazioni native di ONTAP, distribuisci e convalida l'opzione di esecuzione appropriata nella tua VPC.

Informazioni correlate

- "Connettività e percorsi di fiducia per NetApp Workload Factory"
- "Opzioni di esecuzione ONTAP per NetApp Workload Factory"

Fase 5: Verifica dell'osservabilità

1. Conferma che metriche e dati di telemetria vengano raccolti e conservati come previsto.
2. Conferma che puoi accedere ai registri operativi necessari per la risoluzione dei problemi e le indagini.

Informazioni correlate

- "Panoramica sull'osservabilità per NetApp Workload Factory"
- "Metriche e telemetria per NetApp Workload Factory"

Passaggio 6: Abilita la diagnostica AI (facoltativo)

La diagnostica basata sull'AI è abilitata per impostazione predefinita. Se la abiliti, verifica di soddisfare i prerequisiti e di limitare le autorizzazioni al minimo necessario.

Informazioni correlate

- "Bedrock opt-in per la diagnostica AI di NetApp Workload Factory"
- "Limiti degli strumenti di intelligenza artificiale per NetApp Workload Factory"

Compliance e sicurezza per NetApp Workload Factory

NetApp Workload Factory è stato progettato con la conformità e la sicurezza come priorità principali. Tutti i carichi di lavoro in Workload Factory vengono eseguiti su Amazon FSx per NetApp ONTAP. Oltre a "funzionalità di sicurezza AWS", NetApp Workload Factory dispone di "Conformità a SOC2 Type 1, SOC2 Type 2 e HIPAA".

Amazon FSx for NetApp ONTAP for NetApp Workload Factory è un'architettura consolidata "Soluzione AWS per la distribuzione di applicazioni aziendali" e segue le best practice AWS Well-Architected.

Informazioni sul copyright

Informazioni sul marchio commerciale