Identità, credenziali e minimo privilegio

Information Security for Workload Factory

NetApp
September 16, 2026

Sommario

Identità, credenziali e minimo privilegio

Integrazione dell'account AWS per NetApp Workload Factory

Workload Factory utilizza AWS `sts:AssumeRole` per ottenere credenziali temporanee per il tuo account AWS, quindi le chiavi di accesso AWS a lungo termine non vengono memorizzate dal servizio. Durante l'onboarding, configuri un ruolo IAM che Workload Factory può assumere per le operazioni API AWS approvate, utilizzando un ID esterno per aiutare a prevenire accessi non autorizzati tra account. Workload Factory utilizza poi le credenziali di breve durata risultanti durante l'esecuzione, che AWS fa scadere automaticamente dopo ogni sessione.

configurazione account AWS

Per consentire a Workload Factory di accedere al tuo account AWS:

1. Distribuisci un ruolo IAM nel tuo account AWS (tramite CloudFormation o manualmente).
2. Assicurati che la policy di attendibilità del ruolo consenta al service principal di Workload Factory di assumerlo, controllato da un ID esterno.
3. Usa un ID esterno come identificatore segreto univoco (UUID v4) condiviso esclusivamente tra te e Workload Factory.

   Inseriscilo come condizione nella policy di attendibilità del tuo ruolo IAM (`sts:ExternalId`).

   L'ID esterno previene gli attacchi di tipo "confusione del vice". In un modello di accesso tra account, un utente malintenzionato che scopre l'ARN del ruolo di un cliente non può assumere tale ruolo senza possedere anche il corrispondente ID esterno. AWS raccomanda questo modello per l'accesso tra account da parte di terzi. Per ulteriori informazioni, consulta la pagina della documentazione AWS IAM "Accesso ad account AWS di proprietà di terzi".

   L'ID esterno viene generato una sola volta durante la fase di onboarding delle credenziali e memorizzato in forma crittografata insieme all'ARN del ruolo in un database Workload Factory.
4. Registra l'ARN del ruolo e l'ID esterno in Workload Factory.

Tempo di esecuzione

In fase di esecuzione, Workload Factory assume il tuo ruolo IAM per ottenere credenziali temporanee per ogni operazione API di AWS:

1. Workload Factory chiama `sts:AssumeRole` con il tuo ruolo ARN e l'ID esterno.
2. AWS restituisce credenziali temporanee (chiave di accesso, chiave segreta e token di sessione).
3. Workload Factory utilizza le credenziali temporanee per le operazioni API di AWS nel tuo account.
4. Le credenziali scadono automaticamente (per impostazione predefinita, dopo un'ora).

Come fluiscono le credenziali AWS attraverso NetApp Workload Factory

Il flusso delle credenziali AWS descrive come NetApp Workload Factory gestisce gli identificatori di ruolo, gli ID esterni e le credenziali AWS STS a breve termine durante l'onboarding e le operazioni in fase di esecuzione. Durante la configurazione iniziale, crei un ruolo IAM nel tuo account AWS e configuri una policy di attendibilità che richiede il service principal di Workload Factory e l'ID esterno corretto. In fase di esecuzione, Workload Factory utilizza l'ARN del ruolo e l'ID esterno memorizzati per richiedere credenziali temporanee definite da una policy di sessione per richiesta e riutilizza le credenziali memorizzate nella cache fino alla loro scadenza.

Configurazione una tantum

Per una configurazione una tantum, il flusso è il seguente:

Passaggi

1. Avvii uno stack CloudFormation o crei manualmente un ruolo IAM nel tuo account AWS.
2. La policy di attendibilità del ruolo IAM specifica due condizioni:
   a. Solo il service principal per Workload Factory può assumerlo.
   b. Chi effettua la chiamata deve presentare l'ID esterno corretto.
3. Workload Factory memorizza l'ARN del ruolo e l'ID esterno (crittografato) nel suo database.

Tempo di esecuzione (ogni operazione API)

In fase di esecuzione, Workload Factory utilizza l'ARN del ruolo memorizzato e l'ID esterno per ottenere credenziali AWS STS temporanee per ogni operazione API. Il flusso è il seguente:

Passaggi

1. Workload Factory recupera l'ARN del ruolo e l'ID esterno memorizzati da MySQL.
2. Verifica in Redis la presenza di un set memorizzato nella cache di credenziali temporanee AWS STS per questo ruolo.
3. In caso di cache miss, Workload Factory effettua una chiamata `sts:AssumeRole` con l'ARN del ruolo e l'ID esterno. La chiamata include una policy di sessione inline per richiesta che limita le autorizzazioni alle sole azioni AWS specifiche necessarie per tale operazione.
4. AWS STS restituisce credenziali temporanee (access key ID, secret access key, session token) con un timestamp di scadenza.
5. Workload Factory memorizza queste credenziali nella cache di Redis e le usa per chiamare le API AWS di destinazione.
6. In caso di cache hit, Workload Factory salta la chiamata STS e utilizza direttamente le credenziali memorizzate nella cache.

Politica della sessione

Ogni chiamata STS include una session policy inline limitata alle azioni AWS minime richieste.

Informazioni correlate

- "Livelli di autorizzazione a privilegio minimo"

Conservazione delle credenziali AWS per NetApp Workload Factory

Workload Factory protegge la gestione delle credenziali tramite credenziali AWS STS di breve durata, metadati di ruolo crittografati e un comportamento di conservazione limitato. Il modello di credenziali separa i metadati di ruolo conservati dalle credenziali AWS temporanee utilizzate per le operazioni API. Le credenziali temporanee vengono memorizzate nella cache solo per un periodo limitato e scadono automaticamente sotto l'applicazione delle regole AWS. La rimozione di una credenziale impedisce a Workload Factory di ottenere nuove credenziali per l'account, mentre le eventuali credenziali memorizzate nella cache scadono poco dopo.

Comportamenti chiave

- Workload Factory non memorizza le chiavi di accesso AWS a lungo termine.

  Workload Factory memorizza solo un puntatore (role ARN) e un segreto condiviso (external ID). Nessuno dei due concede l'accesso ad AWS da solo.

- Le credenziali temporanee AWS STS hanno una durata massima di un'ora (imposta da AWS).

  Workload Factory li memorizza nella cache di Redis per un massimo di 30 minuti prima di forzare una nuova chiamata STS.

- Se un set di credenziali memorizzato nella cache ha meno di 15 minuti rimanenti, Workload Factory lo scarta e ne ottiene uno nuovo.
- L'eliminazione delle credenziali da parte del cliente revoca immediatamente la possibilità per Workload Factory di accedere a tale account.

  La chiamata AssumeRole successiva fallisce e le credenziali memorizzate nella cache scadono entro pochi minuti.

Riepilogo della conservazione e dell'archiviazione

Dati	Posizione di storage	Durata della conservazione	Scadenza automatica?	Metodo di cancellazione
ARN del ruolo IAM + ID esterno	MySQL (crittografato a riposo)	Indefinito (conservato fino a quando il cliente non lo rimuove esplicitamente)	No	Il cliente fa clic su "Elimina credenziali" nell'interfaccia utente

Dati	Posizione di storage	Durata della conservazione	Scadenza automatica?	Metodo di cancellazione
Credenziali temporanee AWS STS (chiave di accesso + segreto + token di sessione)	Redis (cache in-memory)	Massimo 30 minuti (cache TTL). Le credenziali STS sottostanti sono valide fino a un'ora (AWS predefinito). La cache elimina i dati cinque minuti prima della scadenza come margine di sicurezza.	Sì (Redis esegue l'eliminazione automatica in base al TTL; la scadenza delle credenziali AWS è applicata da AWS)	Automatico
Password di amministratore ONTAP	MySQL (crittografia a busta AES-256-CBC tramite KMS)	Indefinita (conservata fino a quando il cliente non rimuove la credenziale o elimina il file system)	No	Il cliente elimina la credenziale oppure l'eliminazione del file system attiva la pulizia
Password ONTAP decrittografata (in chiaro)	Solo in memoria (mai scritto su disco o cache)	Durata di una singola richiesta (millisecondi)	Sì (raccolta dei rifiuti dopo il completamento della richiesta)	Automatico

Controlli di sicurezza

- L'External ID previene gli attacchi confused deputy.
- Le politiche di sessione applicano il principio del minimo privilegio per ogni richiesta.
- Workload Factory aggiorna le credenziali temporanee AWS STS di breve durata prima delle finestre di scadenza rischiose.
- La gestione a livello regionale e per tipologia di account differisce per gli ambienti Standard, GovCloud e Cina.
- Workload Factory non memorizza mai le chiavi di accesso AWS a lungo termine.
- Workload Factory non modifica mai le autorizzazioni del tuo ruolo IAM.
- Workload Factory non eleva mai i permessi oltre quelli concessi dalla policy del tuo ruolo.
- Le policy di sessione possono solo ridurre le autorizzazioni; Workload Factory non le espande mai.

Tipi di credenziali per NetApp Workload Factory

NetAppWorkload Factory utilizza un modello di credenziali separate per distinguere le autorizzazioni del piano di controllo AWS dall'accesso amministrativo diretto a ONTAP. Il ruolo AWS IAM autentica Workload Factory alle API AWS per operazioni come la gestione del file system, la gestione dei backup e l'individuazione delle risorse. Le credenziali ONTAP autenticano l'accesso diretto all'endpoint di gestione ONTAP tramite un collegamento Lambda per le operazioni che richiedono configurazione amministrativa o diagnostica. Alcuni flussi di lavoro richiedono entrambi i tipi di credenziali quando combinano operazioni API AWS con attività di gestione diretta di ONTAP.

Tipi di credenziali

La tabella seguente riassume i due tipi di credenziali utilizzati in Workload Factory e i rispettivi target di autenticazione.

Tipo di credenziale	Autentica su	Utilizzato per
Credenziali AWS (AssumeRole)	API AWS	Tutte le operazioni che passano attraverso l'API del servizio AWS FSx
Credenziali ONTAP (password admin)	Endpoint di gestione ONTAP	Operazioni che richiedono l'accesso diretto all'API REST o alla CLI di ONTAP

Operazioni solo con credenziali AWS

Queste operazioni interagiscono esclusivamente con le API di AWS e richiedono solo il ruolo IAM:

- Creazione ed eliminazione del file system
- Modifiche alla capacità e al throughput del file system
- Creazione e gestione dei backup
- Rilevamento di VPC, subnet e security group
- Enumerazione delle chiavi KMS
- CloudWatch recupero delle metriche
- Query di Cost Explorer
- Gestione dei tag tramite l'API FSx

Operazioni ONTAP con sole credenziali

Queste operazioni comunicano direttamente con l'endpoint di gestione ONTAP tramite il collegamento Lambda e richiedono le credenziali di amministratore ONTAP:

- Configurazione della policy QoS a livello di volume
- Gestione della policy di esportazione e delle regole
- Configurazione del protocollo della storage VM (NFS, CIFS, iSCSI)
- Gestione di igroup e LUN

- SnapMirror (replica) configurazione
- Gestione delle policy di Snapshot (a livello ONTAP)
- Diagnostica delle prestazioni (statistiche QoS, analisi della latenza)
- Recupero e analisi degli eventi EMS
- Monitoraggio dello stato di protezione anti-ransomware
- Gestione FlexCache
- Query dell'interfaccia di rete (LIF)

Operazioni che richiedono sia le credenziali AWS che ONTAP

Flusso di lavoro	Credenziale AWS utilizzata per	Credenziali ONTAP utilizzate per
analisi degli eventi basata sull'intelligenza artificiale	Richiama Bedrock, descrivi file system	Recupera gli eventi EMS ed esegui la diagnostica tramite SSH
Creazione del file system con configurazione della storage VM	Crea file system (AWS API)	Configura i protocolli della macchina virtuale di storage (ONTAP REST)
Creazione di volumi con policy di esportazione	Crea volume (API AWS)	Imposta le regole della policy di esportazione (ONTAP REST)
gestione della capacità	Aggiorna la capacità del file system (API AWS)	Verifica l'utilizzo dell'aggregato (ONTAP SSH)

Informazioni correlate

- "Opzioni di esecuzione ONTAP"
- "Panoramica del collegamento Lambda"

Opzioni di archiviazione delle credenziali per NetApp Workload Factory

NetApp Workload Factory supporta modelli di gestione delle credenziali che preservano il principio del minimo privilegio e riducono l'esposizione dei segreti amministrativi di ONTAP. Le funzionalità di diagnostica basate sull'IA utilizzano credenziali ONTAP di sola lettura, quando disponibili, così l'agente di diagnostica può osservare e diagnosticare senza modificare l'ambiente di storage. Puoi usare lo storage crittografato gestito da Workload Factory oppure archiviare la password ONTAP in AWS Secrets Manager e fornire a Workload Factory un riferimento. La scelta influisce su dove viene archiviata la password, su come viene crittografata e su come gestisci requisiti come il supporto GovCloud e la rotazione delle credenziali.

Modello di accesso ONTAP in sola lettura

Per funzionalità basate sull'intelligenza artificiale come l'analisi degli eventi e la diagnostica della latenza, Workload Factory utilizza credenziali ONTAP di sola lettura, quando disponibili. Il modello di credenziali di sola lettura garantisce che l'agente diagnostico AI non possa apportare modifiche all'ambiente di storage: può solo

osservare e diagnosticare.

Confronto tra le opzioni di archiviazione delle credenziali

Credenziali AWS

Le credenziali AWS vengono sempre assunte tramite un ruolo IAM. Workload Factory può gestire le informazioni sul ruolo internamente oppure farvi riferimento da AWS Secrets Manager.

Opzione	Credenziali AWS	Cosa viene memorizzato	Crittografia
Gestito da Workload Factory	ARN del ruolo IAM + ID esterno	ARN del ruolo IAM + ID esterno	L'ARN del ruolo non è un segreto (viene memorizzato così com'è)

Credenziali ONTAP

Workload Factory può gestire le credenziali ONTAP internamente con archiviazione crittografata oppure farvi riferimento da AWS Secrets Manager. La scelta influisce su come la password viene archiviata, crittografata e ruotata.

Le credenziali ONTAP sono necessarie perché Workload Factory possa interagire con le API del file system ONTAP tramite un "Collegamento Lambda".

Opzione	Credenziali ONTAP	Cosa viene memorizzato	Crittografia
Gestito da Workload Factory	Password (crittografata)	Password di amministratore ONTAP (crittografata)	La password ONTAP utilizza la crittografia a busta AES-256
AWS Secrets Manager	Riferimento ARN di Secrets Manager	ARN di Secrets Manager	L'ARN dei segreti non è un segreto (viene memorizzato così com'è); AWS Secrets Manager crittografa il segreto nel tuo account

Considerazioni aggiuntive

Requisito GovCloud

Viene utilizzato il ruolo IAM standard; le credenziali ONTAP devono utilizzare Secrets Manager (l'archiviazione delle password non è consentita).

Rotazione

Le policy relative ai ruoli sono aggiornate nel tuo account. Aggiorna la password ONTAP in NetApp Workload Factory (opzione gestita) oppure ruotala in AWS Secrets Manager.

Livelli di autorizzazione a privilegio minimo per NetApp Workload Factory

Puoi limitare le autorizzazioni IAM di Workload Factory in qualsiasi momento per

soddisfare i requisiti del principio del minimo privilegio, ad esempio limitando l'accesso a risorse specifiche (ARN) e applicando condizioni IAM, come tag e intervalli CIDR.

Modello di autorizzazioni a livelli

Workload Factory utilizza un modello di autorizzazioni a livelli, basato sul principio del minimo privilegio. Scegli tu quali livelli di funzionalità abilitare quando aggiungi le credenziali AWS. Puoi iniziare con la scoperta in sola lettura ed espandere secondo le necessità.

Workload Factory concede tutte le autorizzazioni tramite un ruolo IAM nel tuo account AWS, che assume tramite STS con un ID esterno.

Workload Factory definisce ulteriormente l'ambito di ogni chiamata API con una session policy inline.

Nella console di Workload Factory, la funzionalità di chat basata sull'AI *Ask Me* ti aiuta a perfezionare le autorizzazioni in modo sicuro suggerendo opzioni di restrizione e generando una policy aggiornata da applicare in AWS.

Concessione delle autorizzazioni

Quando aggiungi le credenziali AWS a Workload Factory, puoi scegliere quali livelli di autorizzazione abilitare. Puoi abilitare o disabilitare i livelli in qualsiasi momento.

I livelli sono cumulativi: l'attivazione di un livello superiore abilita automaticamente tutti i livelli inferiori.

Controlli di sicurezza

- ID esterno (protezione dal deputy confuso)
- Politiche di sessione per singola operazione (minimo privilegio per richiesta)
- Condizioni basate su tag (modifiche ai gruppi di sicurezza limitate alle risorse create da Workload Factory)
- Ambito ARN segreto (accesso a Secrets Manager limitato a `FSxSecret*`)
- Validazione delle autorizzazioni in fase di esecuzione (azione/risorsa mancante segnalata per una correzione mirata)

Documentazione sulle autorizzazioni

Il riferimento principale per le autorizzazioni di Workload Factory è la "riferimento ai permessi" nella documentazione di configurazione e amministrazione di Workload Factory. Puoi trovare informazioni sull'impatto della rimozione delle autorizzazioni dalle policy IAM di Storage in questa documentazione.

Autorizzazioni di monitoraggio Amazon CloudWatch per NetApp Workload Factory

Le autorizzazioni di monitoraggio di Amazon CloudWatch sono facoltative in NetApp Workload Factory e si applicano solo quando distribuisci lo stack di monitoraggio separato. Lo stack di monitoraggio offre visibilità operativa raccogliendo le metriche del file system, pubblicando i registri degli eventi, gestendo le dashboard e gli allarmi di CloudWatch e inviando notifiche di avviso tramite Amazon SNS. Lo stack richiede anche l'accesso per recuperare le credenziali ONTAP quando necessario per il monitoraggio.

Autorizzazioni di monitoraggio richieste per CloudWatch

Per lo stack di monitoraggio opzionale sono necessarie le seguenti autorizzazioni:

Permesso	Scopo
fsx:Describe* / fsx:ListTagsForResource	Raccogli metriche del file system
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Gestisci dashboard e allarmi
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	Pubblica i registri degli eventi
sns:Publish	Invia notifiche di avviso
secretsmanager:GetSecretValue	Recupera le credenziali ONTAP per il monitoraggio