



Gestisci i punti di accesso S3

Workload Factory for NetApp Console

NetApp

October 07, 2026

Sommario

- Gestisci i punti di accesso S3. 1
 - Crea punti di accesso S3 per un volume in NetApp Workload Factory 1
 - Gestisci i punti di accesso S3 per un volume in NetApp Workload Factory. 2
 - Modifica i punti di accesso S3 per un volume 2
 - Visualizza i dettagli del punto di accesso S3 per un volume 2
 - Eliminare i punti di accesso S3 per un volume in NetApp Workload Factory 3
- Configura l'infrastruttura della tabella Journal per NetApp Workload Factory 4
 - Informazioni su questa attività 4
 - Prima di iniziare 5
 - Configurare l'infrastruttura della tabella del giornale 7
 - Risoluzione dei problemi di configurazione dell'infrastruttura per la tabella del journal. 8
 - Riferimento alle autorizzazioni per la configurazione della tabella del giornale. 11

Gestisci i punti di accesso S3

Crea punti di accesso S3 per un volume in NetApp Workload Factory

Crea e collega i punti di accesso S3 per un volume in NetApp Workload Factory.

Informazioni su questa attività

Amazon FSx for NetApp ONTAP consente ai file system NFS e SMB di accedere ai dati S3 e di connettersi a servizi AWS come Amazon Bedrock, SageMaker, Athena, AWS Glue e altri. Puoi connettere i servizi AWS a tutti i tuoi dati di storage a oggetti.

Collega i punti di accesso S3 ai volumi NFS e SMB in un file system FSx for ONTAP in modo che i servizi AWS accedano ai file come se si trovassero in un bucket S3. Quando colleghi il punto di accesso, definisci un ID univoco, seleziona il tipo di accesso ai file (UNIX o Windows) e aggiungi un nome utente per l'autorizzazione all'accesso.

Dopo aver collegato l'access point S3, questo appare nella AWS Management Console con un alias univoco. Utilizza questo alias come nome del bucket S3 per i servizi AWS, come Amazon Bedrock, per accedere ai file nel volume FSx for ONTAP.

È possibile collegare più punti di accesso S3 a un singolo volume FSx for ONTAP, ciascuno con un livello di accesso univoco, per connettersi a più servizi AWS.

Prima di iniziare

Completa i seguenti requisiti prima di iniziare.

- È necessario disporre di un volume esistente con un punto di accesso S3. ["Crea un volume con un punto di accesso S3"](#)
- Devi ["concedere le credenziali con la policy di autorizzazione *operations and remediation*"](#) in Workload Factory per completare questa attività.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu delle azioni per il volume che vuoi utilizzare, poi seleziona **Azioni avanzate** e quindi **Gestisci punti di accesso S3**.
4. Nella pagina Gestisci punti di accesso S3, seleziona **Crea e collega punto di accesso S3**.
5. Nella pagina **Crea e collega punto di accesso S3**, fornisci le seguenti informazioni:
 - **Nome punto di accesso S3**: Inserisci il nome del punto di accesso S3.
 - **Utente**: Seleziona un utente esistente con accesso al volume o crea un nuovo utente.
 - **Tipo di utente**: seleziona **UNIX** o **Windows** come tipo di utente.
 - **Configurazione di rete**: Selezionare **Internet** o **Virtual private cloud (VPC)**. Il tipo di rete scelto determina se il punto di accesso è accessibile da Internet o limitato a una specifica VPC. Per utilizzare la funzionalità Journal table, è necessario selezionare **Internet** come configurazione di rete.
 - **Tabella di inventario**: facoltativa. Richiede l'`getObject` autorizzazione. Abilita la tabella di inventario

sul volume per generare metadati per tutti gli oggetti accessibili al punto di accesso S3 e comporta costi di richiesta AWS S3. Per ulteriori informazioni, consulta ["Documentazione sui prezzi di Amazon S3"](#). La tabella viene aggiornata ogni 24 ore.

- **Tag del punto di accesso S3:** Facoltativamente, puoi aggiungere fino a 50 tag o rimuovere tag.

6. Seleziona **Crea**.

Informazioni correlate

Facoltativamente, è possibile utilizzare la funzionalità Tabella di registro con i punti di accesso S3 in Workload Factory. L'infrastruttura Tabella di registro acquisisce e archivia i log di controllo degli eventi di accesso degli utenti e delle operazioni sugli oggetti su Amazon FSx for ONTAP volume access points. Per abilitare la funzionalità Tabella di registro, è necessario configurare l'infrastruttura AWS necessaria, inclusi AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, gruppi di log AWS CloudWatch e ruoli e policy di AWS Identity and Access Management (IAM). ["Configura l'infrastruttura della tabella di journaling per NetApp Workload Factory"](#).

Altri argomenti correlati:

["Modifica o elimina i punti di accesso S3 per un volume in NetApp Workload Factory"](#)

Gestisci i punti di accesso S3 per un volume in NetApp Workload Factory

Aggiorna i dettagli del punto di accesso S3 o elimina i punti di accesso S3 per un volume in NetApp Workload Factory.

È inoltre possibile abilitare o disabilitare la **tabella di inventario** per il punto di accesso. La tabella di inventario genera metadati per tutti gli oggetti accessibili al punto di accesso S3 e comporta costi di richiesta AWS S3. Per ulteriori informazioni, consulta ["Documentazione sui prezzi di Amazon S3"](#).

Modifica i punti di accesso S3 per un volume

Modifica i punti di accesso S3 per un volume in NetApp Workload Factory.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage > Volumes explorer**.
3. Seleziona il menu Azioni per il volume per cui vuoi modificare i punti di accesso S3, poi seleziona **Azioni avanzate** e quindi **Gestisci punti di accesso S3**.
4. Dalla schermata **Manage S3 access points**, seleziona il menu azioni e poi seleziona **Edit access point**.
5. Effettua gli aggiornamenti e quindi seleziona **Applica**.

Per configurare l'infrastruttura per la funzionalità della tabella di registro, è necessario selezionare **Internet** come configurazione di rete per il punto di accesso S3. ["Scopri come configurare l'infrastruttura della tabella Journal per NetApp Workload Factory"](#).

Visualizza i dettagli del punto di accesso S3 per un volume

Visualizza i dettagli del punto di accesso S3, come l'alias, l'ARN e l'URI S3. Con le tabelle di inventario e di

registro abilitate, puoi visualizzare metadati e i registri di controllo degli eventi di accesso degli utenti e delle operazioni sugli oggetti su tutti i punti di accesso S3.

Informazioni su questa attività

Quando la tabella di inventario è abilitata sul volume, è possibile visualizzare i dettagli del punto di accesso, della tabella di inventario e del bucket della tabella dei punti di accesso S3 esistenti collegati al volume. Il sistema fornisce anche un collegamento alla tabella di inventario nella AWS Management Console.

Quando la tabella del journal è abilitata, Workload Factory genera log sui punti di accesso in una tabella per tua consultazione. La tabella include CloudTrail eventi, trail (una registrazione delle attività AWS), CloudTrail filtri, CloudWatch gruppi di log e altro ancora.

È possibile copiare i dettagli del punto di accesso per utilizzarli in altre applicazioni.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage > Volumes explorer**.
3. Seleziona il menu Azioni per il volume di cui vuoi visualizzare i dettagli, quindi seleziona **Advanced actions** e poi **View details**.

I dettagli vengono visualizzati in quattro schede: **Punto di accesso**, **Tabella inventario**, **Tabella di registrazione** e **Table bucket**.

4. Se lo stato per le tabelle di inventario o di registro è abilitato, ma non si dispone dell'`get:Object` autorizzazione necessaria, seguire le istruzioni nella finestra di dialogo per aggiungere l'autorizzazione richiesta.
5. Quando lo stato della tabella di journal è in sospeso, è necessario fornire l'CloudTrail ARN per connettere la tabella di journal all'infrastruttura creata. Seguire le istruzioni per distribuire lo CloudFormation stack utilizzando l'AWS CLI o la AWS Management Console e quindi tornare alla console di Workload Factory per inserire l'CloudTrail ARN.

Eliminare i punti di accesso S3 per un volume in NetApp Workload Factory

Elimina i punti di accesso S3 esistenti da un volume in NetApp Workload Factory.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage > Volumes explorer**.
3. Seleziona il menu Azioni per il volume per cui vuoi gestire i punti di accesso S3, poi seleziona **Azioni avanzate** e quindi **Gestisci punti di accesso S3**.
4. Seleziona il menu delle azioni per il punto di accesso S3 da eliminare e poi seleziona **Elimina**.
5. Nella finestra di dialogo **Elimina un S3 access point**, selezionare **Elimina** per eliminare l'S3 access point dal volume.

Workload Factory non elimina l'inventario o la tabella del registro, ma è possibile rimuoverli manualmente dalla AWS Management Console.

Informazioni correlate

- ["Configurare l'infrastruttura della tabella del giornale"](#)

Configura l'infrastruttura della tabella Journal per NetApp Workload Factory

Configura l'infrastruttura della tabella Journal per acquisire e archiviare i log di controllo degli eventi di accesso degli utenti e delle operazioni sugli oggetti attraverso i punti di accesso ai volumi Amazon FSx for ONTAP. Sono necessari diversi passaggi per configurare l'infrastruttura per i servizi AWS come AWS CloudTrail, AWS CloudWatch, bucket AWS S3, gruppo di log AWS CloudWatch, AWS Identity and Access Management (IAM) e tabelle AWS S3, in modo che gli eventi di log vengano trasmessi correttamente attraverso la pipeline e letti da Workload Factory.

Informazioni su questa attività

La funzionalità della tabella Journal acquisisce gli eventi del piano dati S3 (PutObject, GetObject, DeleteObject, ecc.) per i punti di accesso S3 di FSx for ONTAP monitorati. Utilizza una catena di servizi AWS distribuiti nel tuo account AWS. Quando configuri correttamente l'infrastruttura, si connette al punto di accesso al volume di FSx for ONTAP e stabilisce la pipeline che acquisisce gli eventi di audit relativi agli accessi degli utenti e alle operazioni sugli oggetti nella tabella Journal.

La tabella seguente elenca i servizi AWS che fanno parte dell'infrastruttura, i rispettivi modelli di denominazione delle risorse e lo scopo del servizio nella pipeline.

Servizio AWS	Modello di denominazione della risorsa	Scopo
AWS CloudFormation	netapp-metadata-*	Distribuisce tutta l'infrastruttura come uno stack
Bucket AWS S3	netapp-metadata-cloudtrail-events-logs-{uuid}	Memorizza file di log raw CloudTrail
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Cattura gli eventi dati S3 per punti di accesso specifici
Gruppo di log AWS CloudWatch	netapp-metadata-journal-data-events-{uuid}	Riceve gli eventi CloudTrail come voci di registro strutturate
Ruoli IAM	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	Integrazione attiva
ObservabilityAdmin	S3TableIntegration	Bridges CloudWatch Logs effettua l'accesso a una tabella di S3 Tables
Tabelle S3	bucket aws-cloudwatch → logs.aws_cloudtrail__data	Memorizza eventi strutturati e interrogabili CloudTrail in formato Iceberg

Il {uuid} è un identificatore casuale di 8 caratteri generato al momento della creazione del modello.

Prima di iniziare

Per abilitare la funzionalità della tabella Journal, segui questi passaggi:

- Disporre di un volume esistente con un punto di accesso S3. ["Crea un volume con un punto di accesso S3"](#)
- Impostare la configurazione di rete su **Internet** per il punto di accesso S3. ["Modifica la configurazione di rete per il punto di accesso S3"](#).
- ["Concedi le autorizzazioni per le operazioni e la remediation"](#) alle tue credenziali di Workload Factory.
- Aggiungi le seguenti autorizzazioni della policy IAM all'account AWS che utilizzi per eseguire il deployment di CloudFormation per configurare la tabella Journal.

▼ Autorizzazioni della policy IAM per la configurazione della tabella Journal

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CFNStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
    },
    {
      "Sid": "StarResources",
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "cloudtrail:DescribeTrails",
        "logs:DescribeLogGroups",
        "logs:ListSourcesForS3TableIntegration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:TagResource",
        "observabilityadmin:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3Bucket",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketTagging"
    ],
    "Resource": "arn:aws:s3:::netapp-metadata-*"
},
{
    "Sid": "IAMRoles",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
},
{
    "Sid": "PassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "cloudtrail.amazonaws.com",
                "logs.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "CloudTrail",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:CreateTrail",
        "cloudtrail:StartLogging",
        "cloudtrail:AddTags",
        "cloudtrail:PutEventSelectors"
    ],
    "Resource": "arn:aws:cloudtrail::*:trail/netapp-metadata-
* "
},
{
    "Sid": "CWLogGroup",
    "Effect": "Allow",

```

```

        "Action": [
            "logs:CreateLogGroup",
            "logs>DeleteLogGroup",
            "logs:PutRetentionPolicy",
            "logs:TagResource",
            "logs:AssociateSourceToS3TableIntegration"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:netapp-metadata-*"
    },
    {
        "Sid": "S3Table",
        "Effect": "Allow",
        "Action": [
            "s3tables:CreateTableBucket",
            "s3tables:PutTableBucketEncryption",
            "s3tables:PutTableBucketPolicy"
        ],
        "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    }
]
}

```

Configurare l'infrastruttura della tabella del giornale

Configura l'infrastruttura per acquisire gli eventi del servizio AWS dal punto di accesso S3 nella tabella del registro.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu delle azioni del file system con il volume da aggiornare, quindi seleziona **Gestisci**.
4. Dalla panoramica del file system, seleziona la scheda **Volumi**.
5. Dalla scheda Volumes, seleziona il menu azioni per il volume per cui desideri gestire S3 access points, quindi seleziona **Advanced actions** e poi **Manage S3 access points**.
6. Dalla schermata **Manage S3 access points**, seleziona il menu azioni e poi seleziona **Edit access point**.
7. Nella finestra di dialogo **Modifica punto di accesso S3**, assicurarsi che la configurazione di rete sia impostata su **Internet**.
8. Segui le istruzioni nella finestra di dialogo per configurare l'infrastruttura per la funzionalità della tabella del journal.
9. Scarica il modello CloudFormation.
10. Distribuisci lo CloudFormation stack nel tuo account AWS.
 - a. Salva il modello JSON in un file.

- b. Distribuisce il template utilizzando l'AWS CLI o l'AWS Management Console.
 - c. Attendi che lo stack raggiunga lo stato `CREATE_COMPLETE`.
 - d. Ottieni l'CloudTrail ARN dagli output dello stack.
11. Torna alla console di Workload Factory e poi al volume per gestire i punti di accesso S3.
 12. Seleziona **Visualizza dettagli** dal menu delle azioni del volume.
 13. Nella scheda **Tabella del giornale**, inserire l'CloudTrail ARN.
 14. Seleziona **Applica**.

Se uno qualsiasi di questi passaggi non dovesse funzionare, [risolvere i problemi di configurazione dell'infrastruttura per la tabella del registro](#) o contatta il supporto NetApp per assistenza.

Risoluzione dei problemi di configurazione dell'infrastruttura per la tabella del journal

È possibile utilizzare la Console di gestione AWS o l'AWS CLI per risolvere i problemi relativi agli errori durante la distribuzione dello stack CloudFormation e delle risorse che esso crea.

Dopo aver risolto il problema, inviare nuovamente l'ARN di CloudTrail per riavviare la configurazione della tabella del giornale.

Errori comuni durante l'implementazione di CloudFormation

Autorizzazioni IAM insufficienti

Il ruolo/utente che effettua la distribuzione necessita di un set specifico di autorizzazioni. Consultare [Prima di iniziare](#) per la policy completa.

Se lo stack fallisce con un `AccessDenied` o `InsufficientPermission` errore, controlla gli eventi dello stack e cerca l'autorizzazione mancante nel campo `ResourceStatusReason`.

Limite di CloudTrail

AWS impone un limite predefinito di 5 trail per regione. Se l'account ha già 5 trail, the `FsxDataEventTrail` la risorsa fallirà con: `Maximum number of trails (5) exceeded`. È possibile verificare il numero di trail a livello regionale con il seguente comando:

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList)"
```

Opzioni di risoluzione

- Opzione 1: Eliminare un trail inutilizzato nella regione per fare spazio.
- Opzione 2: Utilizzare un percorso esistente. Rimuovere le risorse `FsxDataEventTrail`, `CloudTrailBucket`, `CloudTrailBucketPolicy` e `CloudTrailToCloudWatchRole` dal modello prima di distribuire nuovamente lo stack CloudFormation. Quindi, passare l'ARN del percorso esistente durante la fase di inizializzazione. Il percorso esistente deve avere un gruppo di log CloudWatch configurato, una `S3TableIntegration` associata al gruppo di log e deve registrare eventi di dati.

L'integrazione con le tabelle S3 esiste già

Se l'account dispone già di un `S3TableIntegration` per l'origine dati `aws_cloudtrail`, la risorsa `LogsToS3TableIntegration` non funzionerà.

Risoluzione

Rimuovere le `LogsToS3TableIntegration` e `S3TableIntegrationRole` risorse dal modello prima di distribuire nuovamente lo stack `CloudFormation`. Il sistema utilizza automaticamente l'integrazione esistente a condizione che sia configurata per gli eventi dati di `aws_cloudtrail`.

Per verificare la presenza di un'integrazione esistente:

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

Il nome del bucket S3 esiste già

Il nome del bucket `netapp-metadata-cloudtrail-events-logs-{uuid}` è univoco a livello globale. Se va in conflitto, richiedere nuovamente il template per ottenere un nuovo UUID.

Il ruolo IAM esiste già

Se una precedente distribuzione parziale ha lasciato ruoli IAM con il nome che segue lo schema `netapp-metadata-*`, la creazione dello stack fallirà. Elimina prima i ruoli orfani:

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

Errori successivi all'abilitazione della tabella Journal

Dopo aver inviato l'ARN di `CloudTrail`, `Workload Factory` convalida l'intera pipeline delle risorse inviando automaticamente un `seed`, ovvero un evento di prova. In caso di esito positivo, l'evento `seed` arriva nella tabella `S3 Tables`. Il test richiede circa 10 minuti.

Se la convalida del test non riesce, potresti ricevere uno dei seguenti messaggi di errore:

Messaggio di errore	Significato
La tabella <code>aws_cloudtrail__data</code> non è stata creata in {bucket}. Verificare i permessi di <code>s3table</code> .	<code>S3TableIntegration</code> non ha creato la tabella gestita da <code>CloudWatch</code> . La pipeline tra i log di <code>CloudWatch</code> e le tabelle S3 è interrotta.
La tabella esiste, ma l'evento di seeding del journal non viene visualizzato. Verificare le autorizzazioni <code>CloudTrail</code> e <code>CloudWatch</code> .	La tabella esiste, ma l'evento <code>seed</code> specifico non è mai arrivato. La pipeline è interrotta tra <code>CloudTrail</code> e la tabella <code>S3 Tables</code> .
Impossibile avviare la configurazione del journal. ...	Si è verificato un errore durante il flusso di <code>seed/poll</code> in background. Controllare il messaggio successivo per i dettagli.

Passaggi per la risoluzione

Quando il registro raggiunge lo stato FAILED, traccia l'evento seed attraverso le fasi della pipeline per identificare esattamente dove si è interrotto. Ogni passaggio corrisponde a una specifica risorsa AWS creata dal template.

1. Controlla il bucket S3 CloudTrail.

Il trail scrive i log degli eventi raw nel bucket S3 `netapp-metadata-cloudtrail-events-logs`. Cerca i file di log più recenti.

Se non esistono file di registro, significa che CloudTrail non sta acquisendo eventi. Verificare quanto segue:

- Il trail sta registrando (`IsLogging: true`)
- I selettori di eventi avanzati includono l'ARN del punto di accesso corretto
- I selettori di eventi avanzati includono i filtri per `eventCategory = Data` e `resources.type = AWS::S3::AccessPoint`

2. Controlla il CloudWatch Log Group.

Il percorso invia anche eventi al CloudWatch Log Group. Il nome del gruppo di log inizia con `netapp-metadata-journal-data-events-<uuid>`.

- Se il gruppo di log è vuoto, allora CloudTrail non sta recapitando eventi a CloudWatch. Verificare che il `CloudTrailToCloudWatchRole` ruolo IAM esista e abbia `logs:CreateLogStream` e `logs:PutLogEvents` autorizzazioni, e che il trail sia configurato con il corretto `CloudWatchLogsLogGroupArn` e `CloudWatchLogsRoleArn`.
- Se l'evento iniziale compare nel gruppo di log, il problema si trova a valle — procedere al passaggio 3.

3. Controlla la tabella S3 Tables (`aws-cloudwatch`).

`S3TableIntegration` crea automaticamente un bucket di tabelle chiamato `aws-cloudwatch` e popola una tabella in `logs.aws_cloudtrail__data`. Questa tabella viene creata solo dopo che il primo evento è stato elaborato.

- Se il bucket della tabella `aws-cloudwatch` non esiste, allora `S3TableIntegrationRole` mancano le autorizzazioni. Sono necessarie `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption`, e `s3tables:PutTableBucketPolicy` — tutte con ambito `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Se il bucket della tabella esiste ma `logs.aws_cloudtrail__data` non è presente, l'integrazione non sta instradando gli eventi. L'integrazione deve mostrare `Status: ACTIVE` e includere `aws_cloudtrail` come sorgente di log.
- Se la tabella esiste ma l'evento di origine non è presente al suo interno, l'evento potrebbe essere ancora in transito. L'inserimento dei dati nelle tabelle S3 presenta una certa latenza. Attendi ancora qualche minuto. Se dopo 15-20 minuti l'evento non compare ancora, l'integrazione potrebbe essere interrotta.

4. Interroga direttamente l'evento seed.

- Apri le tabelle S3 nella console di gestione AWS.
- Accedi al bucket della tabella `aws-cloudwatch` → tabella `aws_cloudtrail__data` e utilizza il pulsante **Anteprima** per eseguire una query rapida direttamente nel browser.

- c. Se l'evento è presente nella tabella ma il registro mostra ancora `FAILED`, è possibile che la finestra di polling sia scaduta prima che l'evento arrivasse.

Dopo aver risolto il problema, torna alla console di Workload Factory. Riprova [avvio della configurazione della tabella del giornale](#) inviando nuovamente il Trail ARN.

1. Se la configurazione continua a non riuscire, contatta l'assistenza NetApp per ricevere supporto.

Riferimento alle autorizzazioni per la configurazione della tabella del giornale

Il ruolo IAM che distribuisce lo CloudFormation stack per abilitare la funzionalità della tabella Journal necessita delle seguenti autorizzazioni. Fare riferimento a [Prima di iniziare](#) per una policy JSON copiabile con le autorizzazioni richieste.

Operazioni sullo stack

Permesso	Risorsa	Perché
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Crea lo stack
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Monitora lo stato dello stack
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Diagnosi dei guasti a livello di risorsa cloudformation:GetTemplateSummary * Validazione preliminare del template

CloudTrail

Permesso	Risorsa	Perché
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Crea il trail
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Abilita la registrazione
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Applicare il cartellino identificativo
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Configura l'acquisizione degli eventi dati
cloudtrail:DescribeTrails	*	Risolvi l'ARN del trail per l'output dello stack

S3

Permesso	Risorsa	Perché
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Crea il bucket di log CloudTrail

Permesso	Risorsa	Perché
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Consenti a CloudTrail di scrivere i log
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Applicare il cartellino identificativo

IAM

Permesso	Risorsa	Perché
iam:CreateRole	arn:aws:iam::*:role/netapp-metadata-*	Creare entrambi i ruoli IAM
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Allega le policy inline
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Applicare il cartellino identificativo
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Conferma che il ruolo è attivo
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (condizione: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Passa i ruoli a CloudTrail e CloudWatch Logs

Log di CloudWatch

Permesso	Risorsa	Perché
log:CreateLogGroup	arn:aws:logs::*:log-group:netapp-metadatai-*	Crea il gruppo di log
log>DeleteLogGroup	arn:aws:logs::*:log-group:netapp-metadatai-*	Pulizia del gruppo di log se la creazione non è riuscita
log:PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-metadatai-*	Imposta la conservazione di 30 giorni
log:TagResource	arn:aws:logs::*:log-group:netapp-metadatai-*	Applicare il cartellino identificativo
logs:AssociateSourceToS3TableIntegration	arn:aws:logs::*:log-group:netapp-metadatai-*	Collega l'origine CloudTrail alle tabelle S3
log:DescribeLogGroups	*	Verifica l'esistenza del gruppo di log
logs:ListSourcesForS3TableIntegration	*	Conferma associazione integrazione

ObservabilityAdmin

Permesso	Risorsa	Perché
observabilityadmin:CreateS3TableIntegration	*	Crea il bridge CloudWatch → S3 Tables
observabilityadmin:GetS3TableIntegration	*	Conferma che l'integrazione è attiva
observabilityadmin:TagResource	*	Applicare il cartellino identificativo
observabilityadmin:ListTagsForResource	*	Rilevamento della deriva

Tabelle S3

Permesso	Risorsa	Perché
s3tables:CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Creare il bucket S3 Tables (tramite ruolo di integrazione)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Imposta la crittografia AES256
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Consenti l'accesso ai registri CloudWatch

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.