



Management von S3-Zugriffspunkten

Workload Factory for NetApp Console

NetApp

October 07, 2026

Inhalt

Management von S3-Zugriffspunkten	1
Erstellen Sie S3-Zugriffspunkte für ein Volume in NetApp Workload Factory	1
Verwaltung der S3-Zugriffspunkte für ein Volume in NetApp Workload Factory	2
S3 Zugriffspunkte für ein Volume bearbeiten	2
Details zum S3-Zugriffspunkt für ein Volume anzeigen	3
Löschen Sie die S3-Zugriffspunkte für ein Volume in NetApp Workload Factory	3
Einrichtung der Journaltabelleninfrastruktur für NetApp Workload Factory	4
Über diese Aufgabe	4
Bevor Sie beginnen	5
Einrichtung der Journaltabelleninfrastruktur	7
Beheben Sie Probleme bei der Infrastruktureinrichtung für die Journaltabelle	8
Berechtigungsreferenz für die Einrichtung der Journaltabelle	11

Management von S3-Zugriffspunkten

Erstellen Sie S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Erstellen und Zuordnen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory.

Über diese Aufgabe

Amazon FSx for NetApp ONTAP ermöglicht NFS- und SMB-Dateisystemen den Zugriff auf S3-Daten und die Anbindung an AWS-Services wie Amazon Bedrock, SageMaker, Athena, AWS Glue und mehr. Sie können AWS-Services mit all Ihren Objektspeicherdaten verbinden.

Binden Sie S3-Zugriffspunkte an NFS- und SMB-Volumes in einem FSx for ONTAP-Dateisystem an, damit AWS-Services auf Dateien zugreifen können, als befänden sie sich in einem S3-Bucket. Definieren Sie beim Anbinden des Zugriffspunkts eine eindeutige ID, wählen Sie den Dateizugriffstyp (UNIX oder Windows) aus und fügen Sie einen Benutzernamen für die Zugriffsberechtigung hinzu.

Nachdem Sie den S3-Zugriffspunkt eingebunden haben, wird er in der AWS Management Console mit einem eindeutigen Alias angezeigt. Verwenden Sie diesen Alias als S3-Bucket-Namen für AWS Services, wie Amazon Bedrock, um auf Dateien im FSx for ONTAP Volume zuzugreifen.

Sie können mehrere S3-Zugriffspunkte an ein einzelnes FSx for ONTAP volume anhängen, jeder mit einer eindeutigen Zugangsstufe, um eine Verbindung zu mehreren AWS Services herzustellen.

Bevor Sie beginnen

Bitte erfüllen Sie die folgenden Anforderungen, bevor Sie beginnen.

- Sie benötigen ein bestehendes Volume mit einem S3-Zugangspunkt. ["Erstellen Sie ein Volume mit einem S3-Zugriffspunkt"](#)
- Sie müssen ["Anmeldeinformationen mit der Berechtigungsrichtlinie operations and remediation gewähren"](#) in Workload Factory sein, um diese Aufgabe abzuschließen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume, das Sie verwenden möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Auf der Seite „S3-Zugriffspunkte verwalten“ wählen Sie **S3-Zugriffspunkt erstellen und zuordnen**.
5. Geben Sie auf der Seite **S3-Zugriffspunkt erstellen und verbinden** die folgenden Informationen an:
 - **Name des S3 access point:** Geben Sie den Namen des S3 access point ein.
 - **Benutzer:** Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp:** Wählen Sie **UNIX** oder **Windows** als Benutzerart.
 - **Netzwerkconfiguration:** Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Die Wahl des Netzwerktyps bestimmt, ob der Zugriffspunkt über das Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist. Um die Journal-Tabellenfunktion zu nutzen, müssen Sie **Internet** als

Netzwerkconfiguration auswählen.

- **Inventartabelle:** Optional. Erfordert die `getObject` Berechtigung. Aktivieren Sie die Inventartabelle auf dem Volume, um Metadaten für alle Objekte zu generieren, die über den S3-Zugriffspunkt zugänglich sind, und es entstehen AWS S3-Anfragekosten. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#). Die Tabelle wird alle 24 Stunden aktualisiert.
- **S3 access point tags:** Optional können Sie bis zu 50 Tags hinzufügen oder entfernen.

6. **Erstellen** auswählen.

Verwandte Informationen

Optional können Sie die Journaltabellenfunktion mit S3-Zugriffspunkten in Workload Factory verwenden. Die Journaltabelleninfrastruktur erfasst und speichert Audit-Protokolle von Benutzerzugriffsereignissen und Objektoperationen über Amazon FSx for ONTAP volume access points hinweg. Um die Journaltabellenfunktion zu aktivieren, müssen Sie die erforderliche AWS-Infrastruktur einrichten, einschließlich AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch Protokollgruppen sowie AWS Identity and Access Management (IAM)-Rollen und -Richtlinien. ["Richten Sie die Journaltabelleninfrastruktur für NetApp Workload Factory ein."](#)

Weitere verwandte Themen:

["Bearbeiten oder Löschen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory"](#)

Verwaltung der S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Aktualisierung der S3-Zugriffspunktdetails oder Löschen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory.

Sie können die **Inventartabelle** für den Zugriffspunkt aktivieren oder deaktivieren. Die Inventartabelle generiert Metadaten für alle Objekte, auf die der S3-Zugriffspunkt zugreifen kann, und verursacht AWS S3-Anfragekosten. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#).

S3 Zugriffspunkte für ein Volume bearbeiten

Bearbeiten Sie die S3-Zugriffspunkte für ein Volume in NetApp Workload Factory.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das Sie die S3-Zugriffspunkte bearbeiten möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Wählen Sie auf dem Bildschirm **S3-Zugriffspunkte verwalten** das Menü Aktionen und dann **Zugriffspunkt bearbeiten** aus.
5. Nehmen Sie Aktualisierungen vor und wählen Sie dann **Anwenden**.

Um die Infrastruktur für die Journaltabellenfunktion einzurichten, müssen Sie **Internet** als Netzwerkconfiguration für den S3-Zugriffspunkt auswählen. ["Erfahren Sie, wie Sie die Journaltabelleninfrastruktur für NetApp Workload Factory einrichten."](#)

Details zum S3-Zugriffspunkt für ein Volume anzeigen

Zeigen Sie Details zu S3-Zugriffspunkten wie Alias, ARN und S3-URI an. Mit aktivierten Inventar- und Journaltabellen können Sie Metadaten und Audit-Protokolle von Benutzerzugriffsereignissen und Objektoperationen über alle S3-Zugriffspunkte hinweg einsehen.

Über diese Aufgabe

Wenn die Inventartabelle für das Volume aktiviert ist, können Sie Zugriffspunkt-, Inventartabellen- und Bucket-Details der vorhandenen S3-Zugriffspunkte, die mit dem Volume verbunden sind, anzeigen. Das System stellt außerdem einen Link zur Inventartabelle in der AWS Management Console bereit.

Wenn die Protokolltabelle aktiviert ist, generiert Workload Factory Protokolle zu Zugriffspunkten in einer Tabelle, die Ihnen als Referenz dient. Die Tabelle enthält CloudTrail-Ereignisse, Trails (eine Aufzeichnung der AWS-Aktivitäten), CloudTrail-Filter, CloudWatch-Protokollgruppen und mehr.

Sie können die Zugangspunktdetails kopieren, um sie in anderen Anwendungen zu verwenden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage > Volumes explorer**.
3. Im Aktionsmenü des Volumes, für das Details angezeigt werden sollen, erfolgt zunächst die Auswahl von **Erweiterte Aktionen** und anschließend **Details anzeigen**.

Die Details werden unter vier Registerkarten angezeigt: **Zugriffspunkt**, **Inventartabelle**, **Journaltabelle** und **Table bucket**.

4. Wenn der Status für Inventar- oder Journaltabellen aktiviert ist, Ihnen aber die `get: Object` Berechtigung fehlt, folgen Sie den Anweisungen im Dialogfeld, um die erforderliche Berechtigung hinzuzufügen.
5. Wenn der Status der Journaltabelle „Ausstehend“ ist, müssen Sie die CloudTrail-ARN angeben, um die Journaltabelle mit der erstellten Infrastruktur zu verbinden. Befolgen Sie die Anweisungen zur Bereitstellung des CloudFormation-Stacks mithilfe der AWS CLI oder der AWS Management Console und kehren Sie anschließend zur Workload Factory Konsole zurück, um die CloudTrail-ARN einzugeben.

Löschen Sie die S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Löschen Sie vorhandene S3-Zugriffspunkte von einem Volume in NetApp Workload Factory.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das Sie S3-Zugriffspunkte verwalten möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Wählen Sie das Aktionsmenü für den S3-Zugriffspunkt, den Sie löschen möchten, und wählen Sie dann **Löschen**.
5. Im Dialogfeld **S3-Zugriffspunkt löschen** wählen Sie **Löschen**, um den S3-Zugriffspunkt vom Volume zu löschen.

Workload Factory löscht weder die Inventar- noch die Journaltabelle, aber Sie können sie manuell über die AWS Management Console entfernen.

Verwandte Informationen

- ["Einrichtung der Journaltabelleninfrastruktur"](#)

Einrichtung der Journaltabelleninfrastruktur für NetApp Workload Factory

Richten Sie die Journaltabelleninfrastruktur ein, um Audit-Logs von Benutzerzugriffsereignissen und Objektoperationen über Amazon FSx for ONTAP Volumezugriffspunkte hinweg zu erfassen und zu speichern. Mehrere Schritte sind erforderlich, um die Infrastruktur für AWS-Services wie AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch log group, AWS Identity and Access Management (IAM) und AWS S3 Tables einzurichten, damit die Protokollereignisse korrekt durch die Pipeline gelangen und von Workload Factory gelesen werden.

Über diese Aufgabe

Die Journaltabellenfunktion erfasst S3-Datenebenenereignisse (PutObject, GetObject, DeleteObject usw.) für überwachte FSx for ONTAP S3-Zugriffspunkte. Sie nutzt eine Kette von AWS-Services, die in Ihrem AWS-Konto bereitgestellt werden. Wenn Sie die Infrastruktur korrekt einrichten, stellt sie eine Verbindung zum FSx for ONTAP-Volume-Zugriffspunkt her und richtet die Pipeline ein, die Benutzerzugriffs- und Objektoperations-Audit-Ereignisse in der Journaltabelle erfasst.

Die folgende Tabelle listet die AWS-Services auf, die Teil der Infrastruktur sind, ihre jeweiligen Ressourcennamensmuster und den Zweck des Services in der Pipeline.

AWS-Service	Ressourcennamensmuster	Zweck
AWS CloudFormation	netapp-metadata-*	Stellt die gesamte Infrastruktur als Stack bereit
AWS S3-Bucket	netapp-metadata-cloudtrail-events-logs-{uuid}	Speichert rohe CloudTrail-Protokolldateien
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Erfasst S3-Datenereignisse für bestimmte Zugriffspunkte
AWS CloudWatch-Protokollgruppe	netapp-metadata-journal-data-events-{uuid}	Empfängt CloudTrail-Ereignisse als strukturierte Protokolleinträge
IAM-Rollen	• netapp-metadata-cloudtrail-cw-role-{uuid} • netapp-metadata-s3table-integration-role-{uuid}	Aktive Integration
ObservabilityAdmin	S3TableIntegration	Bridges CloudWatch Logs in eine S3 Tables-Tabelle
S3-Tabellen	aws-cloudwatch Bucket → logs.aws_cloudtrail__data	Speichert strukturierte, abfragbare CloudTrail-Ereignisse im Iceberg-Format

Das {uuid} ist eine zufällige 8-stellige Kennung, die beim Erstellen der Vorlage generiert wird.

Bevor Sie beginnen

Um die Journaltabellenfunktion zu aktivieren, führen Sie folgende Schritte aus:

- Sie haben ein bestehendes Volume mit einem S3-Zugangspunkt. ["Erstellen Sie ein Volume mit einem S3-Zugriffspunkt"](#)
- Stellen Sie die Netzwerkkonfiguration für den S3-Zugangspunkt auf **Internet** ein. ["Netzwerkkonfiguration für den S3-Zugangspunkt bearbeiten"](#).
- ["Gewähren Sie die Berechtigungen für *operations and remediation*"](#) zu Ihren Workload Factory-Anmeldeinformationen.
- Fügen Sie dem AWS-Konto, das Sie zum Ausführen der CloudFormation-Bereitstellung verwenden, die folgenden IAM-Richtlinienberechtigungen hinzu, um die Journaltabelle einzurichten.

▼ IAM-Richtlinienberechtigungen für die Journaltabelleneinrichtung

```
{
  "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"
}
]
}

```

Einrichtung der Journaltabelleninfrastruktur

Richten Sie die Infrastruktur so ein, dass AWS-Serviceereignisse vom S3-Zugriffspunkt in der Journaltabelle erfasst werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem zu aktualisierenden Volume.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Wählen Sie auf der Registerkarte „Volumes“ das Aktionsmenü für das Volume aus, für das Sie S3-Zugriffspunkte verwalten möchten, dann wählen Sie **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
6. Wählen Sie auf dem Bildschirm **S3-Zugriffspunkte verwalten** das Menü Aktionen und dann **Zugriffspunkt bearbeiten** aus.
7. Im Dialogfeld **S3-Zugriffspunkt bearbeiten** stellen Sie sicher, dass die Netzwerkkonfiguration auf **Internet** eingestellt ist.
8. Folgen Sie den Anweisungen im Dialogfeld, um die Infrastruktur für die Journaltabellenfunktion einzurichten.
9. Laden Sie die CloudFormation-Vorlage herunter.

10. Stellen Sie den CloudFormation Stack in Ihrem AWS-Konto bereit.
 - a. Speichern Sie die JSON-Vorlage in einer Datei.
 - b. Stellen Sie die Vorlage mithilfe der AWS CLI oder der AWS Management Console bereit.
 - c. Warten Sie, bis der Stapel den `CREATE_COMPLETE` Status erreicht hat.
 - d. Ermitteln Sie den CloudTrail ARN aus den Stack-Ausgaben.
11. Kehren Sie zur Workload Factory-Konsole zurück und dann zurück zum Volume, für das Sie S3-Zugriffspunkte verwalten möchten.
12. Wählen Sie im Menü für Volume-Aktionen die Option **Details anzeigen** aus.
13. Geben Sie im Tab **Journaltabelle** die CloudTrail ARN ein.
14. **Anwenden** auswählen.

Sollte einer der Schritte fehlschlagen, [Fehlerbehebung bei der Infrastruktureinrichtung für die Journaltabelle](#) oder wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Beheben Sie Probleme bei der Infrastruktureinrichtung für die Journaltabelle

Mithilfe der AWS Management Console oder der AWS CLI können Sie Fehler während der CloudFormation-Stack-Bereitstellung und der von ihr erstellten Ressourcen beheben.

Nach Behebung des Problems übermitteln Sie den CloudTrail ARN erneut, um die Einrichtung der Journaltabelle neu zu starten.

Häufige CloudFormation Bereitstellungsfehler

Unzureichende IAM-Berechtigungen

Die Rolle/der Benutzer, der die Bereitstellung durchführt, benötigt bestimmte Berechtigungen. Siehe [Bevor Sie beginnen](#) für die vollständige Richtlinie.

Falls der Stack mit einem `AccessDenied` oder `InsufficientPermission` Fehler fehlschlägt, überprüfen Sie die Stack-Ereignisse und suchen Sie im `ResourceStatusReason` Feld nach der fehlenden Berechtigung.

CloudTrail-Limit

AWS legt standardmäßig ein Limit von 5 Trails pro Region fest. Wenn das Konto bereits 5 Trails enthält, schlägt die `FsxDataEventTrail` die Ressource mit folgender Fehlermeldung fehl: `Maximum number of trails (5) exceeded`. Sie können die Anzahl der Trails auf regionaler Ebene mit folgendem Befehl überprüfen:

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

Auflösungsoptionen

- Option 1: Löschen Sie einen nicht verwendeten Pfad in der Region, um Platz zu schaffen.
- Option 2: Verwenden Sie einen vorhandenen Trail. Entfernen Sie die `FsxDataEventTrail`,

CloudTrailBucket, CloudTrailBucketPolicy, und CloudTrailToCloudWatchRole Ressourcen aus der Vorlage, bevor Sie den CloudFormation Stack erneut bereitstellen. Übergeben Sie dann den ARN Ihres vorhandenen Trails während des Initialisierungsschritts. Der vorhandene Trail muss eine CloudWatch Loggruppe konfiguriert haben, eine mit der Loggruppe verknüpfte S3TableIntegration besitzen und Datenereignisse protokollieren.

Die S3-Tabellenintegration ist bereits vorhanden.

Wenn das Konto bereits eine S3TableIntegration für die Datenquelle aws_cloudtrail besitzt, schlägt die Ressource LogsToS3TableIntegration fehl.

Auflösung

Entfernen Sie die LogsToS3TableIntegration und S3TableIntegrationRole Ressourcen aus der Vorlage, bevor Sie den CloudFormation-Stack erneut bereitstellen. Das System verwendet automatisch die bestehende Integration, solange Sie diese für aws_cloudtrail data events konfigurieren.

Um zu prüfen, ob eine Integration bereits besteht:

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

S3-Bucket-Name existiert bereits

Der Bucket-Name netapp-metadata-cloudtrail-events-logs-{uuid} ist weltweit eindeutig. Bei einer Namenskollision muss die Vorlage erneut angefordert werden, um eine neue UUID zu erhalten.

IAM-Rolle existiert bereits

Falls bei einer vorherigen Teilbereitstellung IAM-Rollen mit dem netapp-metadata-* Namensmuster zurückgeblieben sind, schlägt die Rollenerstellung im Stack fehl. Löschen Sie zuerst die verwaisten Rollen:

```
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>
```

Fehler nach Aktivierung der Journaltabelle

Nach der Übermittlung des CloudTrail ARN validiert Workload Factory die gesamte Ressourcenpipeline, indem automatisch ein Seed- (Test-)Ereignis gesendet wird. Bei Erfolg wird das Seed-Ereignis in der S3 Tables-Tabelle angezeigt. Der Test dauert etwa 10 Minuten.

Wenn die Testvalidierung fehlschlägt, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

Fehlermeldung	Bedeutung
Die Tabelle aws_cloudtrail__data wurde nicht in {bucket} erstellt. Überprüfen Sie die Berechtigungen für s3table.	S3TableIntegration hat die von CloudWatch verwaltete Tabelle nicht erstellt. Die Pipeline zwischen CloudWatch Logs und S3-Tabellen ist unterbrochen.

Fehlermeldung	Bedeutung
Die Tabelle ist vorhanden, aber das Journal-Seed-Ereignis wird nicht angezeigt. Überprüfen Sie CloudTrail und CloudWatch Berechtigungen.	Die Tabelle existiert, aber das entsprechende Seed-Ereignis ist nie eingetroffen. Die Pipeline ist zwischen CloudTrail und der S3 Tables-Tabelle unterbrochen.
Die Einrichtung des Journals ist fehlgeschlagen. ...	Beim Hintergrundprozess (Seed/Poll) ist ein Fehler aufgetreten. Prüfen Sie die nachfolgende Meldung für Details.

Lösungsschritte

Wenn das Journal den Status „FEHLGESCHLAGEN“ erreicht, verfolgen Sie das Ausgangsereignis durch die Pipeline-Phasen, um genau zu ermitteln, wo es abgebrochen wurde. Jeder Schritt ist einer bestimmten AWS-Ressource zugeordnet, die von der Vorlage erstellt wurde.

1. Überprüfen Sie den CloudTrail S3-Bucket.

Der Trail schreibt Rohereignisprotokolle in den S3-Bucket `netapp-metadata-cloudtrail-events-logs`. Suchen Sie nach den neuesten Protokolldateien.

Wenn keine Protokolldateien vorhanden sind, erfasst CloudTrail keine Ereignisse. Überprüfen Sie Folgendes:

- Der Trail wird protokolliert (`IsLogging: true`)
- Die erweiterten Ereignisselektoren enthalten den korrekten Zugriffspunkt-ARN
- Die erweiterten Ereignisselektoren umfassen die Filter für `eventCategory = Data` und `resources.type = AWS::S3::AccessPoint`

2. Überprüfen Sie die CloudWatch Log Group.

Der Pfad übermittelt außerdem Ereignisse an die CloudWatch Log Group. Der Name der Log Group beginnt mit `netapp-metadata-journal-data-events-<uuid>`.

- Wenn die Protokollgruppe leer ist, liefert CloudTrail keine Ereignisse an CloudWatch. Überprüfen Sie, ob die `CloudTrailToCloudWatchRole` IAM-Rolle existiert und über `logs:CreateLogStream` und `logs:PutLogEvents` Berechtigungen verfügt und ob der Trail mit den korrekten `CloudWatchLogsLogGroupArn` und `CloudWatchLogsRoleArn` konfiguriert ist.
- Wenn das Ausgangsereignis in der Protokollgruppe erscheint, liegt das Problem in einem nachfolgenden Schritt – fahren Sie mit Schritt 3 fort.

3. Überprüfen Sie die Tabelle S3 Tables (`aws-cloudwatch`).

Die `S3TableIntegration` erstellt automatisch einen Tabellen-Bucket namens `aws-cloudwatch` und füllt eine Tabelle unter `logs.aws_cloudtrail__data`. Diese Tabelle wird erst erstellt, nachdem das erste Ereignis verarbeitet wurde.

- Wenn der `aws-cloudwatch`-Tabellen-Bucket nicht existiert, dann fehlen die `S3TableIntegrationRole` Berechtigungen. Es benötigt `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` und `s3tables:PutTableBucketPolicy` — alle beschränkt auf `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Wenn der Tabellen-Bucket existiert, aber `logs.aws_cloudtrail__data` nicht, dann leitet die Integration keine Ereignisse weiter. Die Integration muss `Status: ACTIVE` anzeigen und `aws_cloudtrail` als Protokollquelle einbinden.

- Existiert die Tabelle, ist das entsprechende Ereignis aber nicht darin enthalten, befindet es sich möglicherweise noch in der Übertragung. Die Datenaufnahme in S3-Tabellen kann eine gewisse Latenz aufweisen. Warten Sie einige Minuten. Sollte das Ereignis nach 15–20 Minuten immer noch nicht angezeigt werden, ist die Integration möglicherweise fehlgeschlagen.

4. Fragen Sie das Seed-Ereignis direkt ab.

- Öffnen Sie die S3-Tabellen in der AWS-Managementkonsole.
- Navigieren Sie zum `aws-cloudwatch table bucket → aws_cloudtrail__data table` und verwenden Sie die Schaltfläche **Vorschau**, um eine Schnellabfrage direkt im Browser auszuführen.
- Wenn das Ereignis in der Tabelle vorhanden ist, das Journal aber immer noch `FAILED` anzeigt, dann ist das Abfragefenster möglicherweise abgelaufen, bevor das Ereignis eingetreten ist.

Nachdem das Problem behoben wurde, kehren Sie zur Workload Factory-Konsole zurück. Versuchen Sie es [Initialisierung der Journaltabelleneinrichtung](#) erneut, indem Sie den Trail-ARN erneut übermitteln.

- Sollte die Einrichtung weiterhin fehlschlagen, wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

Berechtigungsreferenz für die Einrichtung der Journaltabelle

Die IAM-Rolle, die den CloudFormation-Stack zur Aktivierung der Journaltabellenfunktion bereitstellt, benötigt die folgenden Berechtigungen. Siehe [Bevor Sie beginnen](#) für eine kopierbare JSON-Richtlinie mit den erforderlichen Berechtigungen.

Stapeloperationen

Berechtigung	Ressource	Warum
<code>cloudformation:CreateStack</code>	<code>arn:aws:cloudformation:*:*:stack/netapp-metadata-/*</code>	Erstellen Sie den Stapel
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation:*:*:stack/netapp-metadata-/*</code>	Stack-Status überwachen
<code>cloudformation:DescribeStackEvents</code>	<code>arn:aws:cloudformation:*:*:stack/netapp-metadata-/*</code>	Diagnose von Fehlern auf Ressourcenebene <code>cloudformation:GetTemplateSummary</code> * Vorabprüfung der Vorlage

CloudTrail

Berechtigung	Ressource	Warum
<code>cloudtrail:CreateTrail</code>	<code>arn:aws:cloudtrail:*:*:trail/netapp-metadata-/*</code>	Erstelle den Pfad
<code>cloudtrail:StartLogging</code>	<code>arn:aws:cloudtrail:*:*:trail/netapp-metadata-/*</code>	Protokollierung aktivieren
<code>cloudtrail:AddTags</code>	<code>arn:aws:cloudtrail:*:*:trail/netapp-metadata-/*</code>	Identifikationsetikett anbringen
<code>cloudtrail:PutEventSelectors</code>	<code>arn:aws:cloudtrail:*:*:trail/netapp-metadata-/*</code>	Datenerfassungsereignisse konfigurieren

Berechtigung	Ressource	Warum
cloudtrail:DescribeTrails	*	Trail-ARN für Stack-Ausgabe auflösen

S3

Berechtigung	Ressource	Warum
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Erstelle den CloudTrail Log-Bucket
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Erlauben Sie CloudTrail, Protokolle zu schreiben
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Identifikationsetikett anbringen

IAM

Berechtigung	Ressource	Warum
iam:CreateRole	arn:aws:iam::*:role/netapp-metadata-*	Erstellen Sie beide IAM-Rollen
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Inline-Richtlinien anhängen
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Identifikationsetikett anbringen
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Bestätigen, dass die Rolle aktiv ist
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (Bedingung: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Rollen an CloudTrail und CloudWatch Logs übergeben

CloudWatch Logs

Berechtigung	Ressource	Warum
Protokolle:CreateLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	Protokollgruppe erstellen
Protokolle>DeleteLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	Protokollgruppe bereinigen, falls die Erstellung fehlgeschlagen ist
Protokolle:PutRetentionPolicy	arn:aws:logs:*:*:log-group:netapp-metadata-*	30-tägige Aufbewahrungsfrist festlegen
Protokolle:TagResource	arn:aws:logs:*:*:log-group:netapp-metadata-*	Identifikationsetikett anbringen
logs:AssociateSourceToS3TableIntegration	arn:aws:logs:*:*:log-group:netapp-metadata-*	Verknüpfen Sie die CloudTrail-Quelle mit S3-Tabellen

Berechtigung	Ressource	Warum
Protokolle:DescribeLogGroups	*	Prüfen Sie, ob die Protokollgruppe existiert
logs:ListSourcesForS3TableIntegration	*	Integrationsassoziation bestätigen

ObservabilityAdmin

Berechtigung	Ressource	Warum
observabilityadmin:CreateS3TableIntegration	*	Erstellen Sie die CloudWatch → S3-Tabellen-Brücke
observabilityadmin:GetS3TableIntegration	*	Bestätigen Sie, dass die Integration aktiv ist.
observabilityadmin:TagResource	*	Identifikationsetikett anbringen
observabilityadmin:ListTagsForResource	*	Drifterkennung

S3-Tabellen

Berechtigung	Ressource	Warum
s3tables:CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Erstellen Sie den S3-Tables-Bucket (über die Integrationsrolle)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	AES256-Verschlüsselung einstellen
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Zugriff auf CloudWatch Logs zulassen

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 IRGEND EINER 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.