



S3アクセスポイントを管理する Workload Factory for NetApp Console

NetApp
October 07, 2026

目次

S3アクセスポイントを管理する	1
NetApp Workload FactoryでボリュームのS3アクセスポイントを作成します	1
NetApp Workload FactoryでボリュームのS3アクセスポイントを管理する	2
ボリュームのS3アクセスポイントを編集する	2
ボリュームのS3アクセスポイントの詳細を表示します	3
NetApp Workload Factory でボリュームの S3 アクセスポイントを削除します	3
NetApp Workload Factoryのジャーナルテーブルインフラをセットアップします	4
タスク概要	4
開始する前に	5
ジャーナルテーブルのインフラストラクチャをセットアップする	7
ジャーナルテーブルのインフラストラクチャ設定のトラブルシューティング	8
ジャーナルテーブル設定の権限リファレンス	11

S3アクセスポイントを管理する

NetApp Workload FactoryでボリュームのS3アクセスポイントを作成します

NetApp Workload Factory でボリュームの S3 アクセスポイントを作成して接続します。

タスク概要

Amazon FSx for NetApp ONTAP を使用すると、NFS および SMB ファイルシステムが S3 データにアクセスし、Amazon Bedrock、SageMaker、Athena、AWS Glue などの AWS サービスに接続できます。すべてのオブジェクトストレージデータに AWS サービスを接続できます。

FSx for ONTAP ファイルシステムの NFS および SMB ボリュームに S3 アクセスポイントを接続すると、AWS サービスはファイルが S3 バケット内にあるかのようにファイルにアクセスできます。アクセスポイントを接続するときは、一意の ID を定義し、ファイルアクセスタイプ（UNIX または Windows）を選択し、アクセス許可用のユーザー名を追加します。

S3 アクセス ポイントを接続すると、一意のエイリアスとともに AWS マネジメント コンソールに表示されます。このエイリアスを Amazon Bedrock などの AWS サービスの S3 バケット名として使用して、Amazon FSx for NetApp ONTAP ボリューム内のファイルにアクセスします。

複数の S3 アクセス ポイントを単一の FSx for ONTAP ボリュームに接続できます。それぞれに独自のアクセス レベルがあり、複数の AWS サービスに接続できます。

開始する前に

開始する前に、以下の要件を満たしてください。

- S3アクセスポイントを持つ既存のボリュームが必要です。["S3アクセスポイントを使用してボリュームを作成する"](#)
- このタスクを完了するには、Workload Factory で["_operations and remediation_ 権限ポリシーで資格情報を付与する"](#)する必要があります。

手順

1. ["NetApp Console"](#)にログインします。
2. メニュー  から、ワークロード > ボリュームエクスプローラー を選択します。
3. 使用するボリュームのアクションメニューを選択し、高度なアクション、*S3アクセスポイントの管理*の順に選択します。
4. 「S3アクセスポイントの管理」ページで、*S3アクセスポイントを作成して接続する*を選択します。
5. *Create and attach S3 access point*ページで、次の情報を入力します。
 - **S3** アクセス ポイント名：S3 アクセス ポイントの名前を入力します。
 - **User**：ボリュームへのアクセス権を持つ既存のユーザーを選択するか、新しいユーザーを作成します。
 - ユーザー タイプ：ユーザー タイプとして **UNIX** または **Windows** を選択します。
 - ネットワーク構成：*インターネット*または*仮想プライベートクラウド（VPC）*を選択してください。

い。選択するネットワークの種類によって、アクセスポイントがインターネットからアクセス可能になるか、特定のVPC内に限定されるかが決まります。ジャーナルテーブル機能を使用するには、ネットワーク構成として*インターネット*を選択する必要があります。

- **Inventory table**：オプション。`getObject`権限が必要です。ボリューム上でインベントリテーブルを有効にすると、S3アクセスポイントからアクセス可能なすべてのオブジェクトのメタデータが生成され、AWS S3リクエストのコストが発生します。詳細については、"[Amazon S3 価格設定ドキュメント](#)"を参照してください。この表は24時間ごとに更新されます。
- **S3 アクセス ポイント タグ**：オプションで、最大 50 個のタグを追加したり、タグを削除したりできます。

6. 「作成」を選択します。

関連情報

オプションで、Workload Factory の S3 アクセスポイントでジャーナルテーブル機能を使用できます。ジャーナルテーブルインフラは、Amazon FSx for ONTAP ボリュームアクセスポイント全体でユーザーアクセスイベントとオブジェクト操作の監査ログをキャプチャして保存します。ジャーナルテーブル機能を有効にするには、AWS CloudTrail、AWS CloudWatch、AWS S3 バケット、AWS CloudWatch ロググループ、AWS Identity and Access Management (IAM) ロールとポリシーを含む、必要な AWS インフラをセットアップする必要があります。"[NetApp Workload Factoryのジャーナルテーブルインフラを設定します](#)"。

その他の関連トピック：

["NetApp Workload FactoryでボリュームのS3アクセスポイントを編集または削除する"](#)

NetApp Workload FactoryでボリュームのS3アクセスポイントを管理する

NetApp Workload FactoryでボリュームのS3アクセスポイントの詳細を更新するか、S3アクセスポイントを削除します。

アクセスポイントの*インベントリテーブル*を有効または無効にすることもできます。インベントリテーブルは、S3アクセスポイントからアクセス可能なすべてのオブジェクトのメタデータを生成し、AWS S3リクエストのコストが発生します。詳細については、"[Amazon S3 価格設定ドキュメント](#)"を参照してください。

ボリュームのS3アクセスポイントを編集する

NetApp Workload Factory でボリュームの S3 アクセスポイントを編集します。

手順

1. "[NetApp Console](#)"にログインします。
2. メニュー  から、ワークロード > ストレージ > *ボリュームエクスプローラー*を選択します。
3. S3アクセスポイントを編集するボリュームのアクションメニューを選択し、詳細アクション、*S3アクセスポイントの管理*の順に選択します。
4. *S3 アクセスポイントの管理*画面でアクションメニューを選択し、*アクセスポイントの編集*を選択します。
5. 更新を行い、* Apply * を選択します。

ジャーナルテーブル機能のインフラストラクチャを設定するには、S3アクセスポイントのネットワーク構成として*Internet*を選択する必要があります。["NetApp Workload Factoryのジャーナルテーブルインフラストラクチャを設定する方法について説明します"](#)。

ボリュームのS3アクセスポイントの詳細を表示します

S3アクセスポイントの詳細情報（エイリアス、ARN、S3 URIなど）を表示します。インベントリテーブルとジャーナルテーブルを有効にすると、S3アクセスポイント全体におけるユーザーアクセスイベントとオブジェクト操作のメタデータと監査ログを表示できます。

タスク概要

ボリューム上でインベントリテーブルが有効になっている場合、そのボリュームに接続されている既存のS3アクセスポイントのアクセスポイント、インベントリテーブル、およびテーブルバケットの詳細を表示できます。このシステムは、AWSマネジメントコンソールのインベントリテーブルへのリンクも提供します。

ジャーナルテーブルが有効になっている場合、Workload Factoryはアクセスポイントに関するログをテーブル形式で生成し、参照できるようにします。このテーブルには、CloudTrailイベント、トレイル（AWSアクティビティの記録）、CloudTrailフィルター、CloudWatchロググループなどが含まれます。

アクセスポイントの詳細をコピーして、他のアプリケーションで使用できます。

手順

1. ["NetApp Console"](#)にログインします。
2. メニュー  から、ワークロード > ストレージ > *ボリュームエクスプローラー*を選択します。
3. 詳細を表示したいボリュームのアクションメニューを選択し、次に*高度なアクション*を選択し、最後に*詳細を表示*を選択します。

詳細は、アクセスポイント、インベントリテーブル、ジャーナルテーブル、*テーブルバケット*の4つのタブに表示されます。

4. 在庫テーブルまたはジャーナルテーブルのステータスが有効になっているが、`get:Object`権限がない場合は、ダイアログの指示に従って必要な権限を追加してください。
5. ジャーナルテーブルのステータスが保留中の場合は、CloudTrail ARNを指定して、ジャーナルテーブルを作成されたインフラストラクチャに接続する必要があります。AWS CLIまたはAWS管理コンソールを使用してCloudFormationスタックを導入する手順に従い、Workload Factoryコンソールに戻ってCloudTrail ARNを入力してください。

NetApp Workload Factory でボリュームの S3 アクセスポイントを削除します

NetApp Workload Factoryでボリュームから既存のS3アクセスポイントを削除します。

手順

1. ["NetApp Console"](#)にログインします。
2. メニュー  から、ワークロード > ストレージ > *ボリュームエクスプローラー*を選択します。
3. S3アクセスポイントを管理するボリュームのアクションメニューを選択し、詳細アクション、*S3アクセスポイントの管理*の順に選択します。

- 削除する S3 アクセス ポイントのアクション メニューを選択し、* Delete * を選択します。
- S3** アクセス ポイントの削除 ダイアログで、削除 を選択して、ボリュームから S3 アクセス ポイントを削除します。

Workload Factoryはインベントリテーブルやジャーナルテーブルを削除しませんが、AWSマネジメントコンソールから手動で削除することは可能です。

関連情報

- ["ジャーナルテーブルのインフラストラクチャをセットアップする"](#)

NetApp Workload Factoryのジャーナルテーブルインフラをセットアップします

Amazon FSx for ONTAPボリュームアクセスポイント全体でユーザーアクセスイベントとオブジェクト操作の監査ログをキャプチャして保存するためのジャーナルテーブルインフラストラクチャを設定します。AWS CloudTrail、AWS CloudWatch、AWS S3バケット、AWS CloudWatchロググループ、AWS Identity and Access Management (IAM)、およびAWS S3テーブルなどのAWSサービスのインフラストラクチャを設定するには、ログイベントがパイプラインを正しく通過し、Workload Factoryによって読み取られるようにするために、いくつかの手順が必要です。

タスク概要

ジャーナルテーブル機能は、監視対象の FSx for ONTAP S3 アクセスポイントの S3 データプレーンイベント (PutObject、GetObject、DeleteObject など) をキャプチャします。これは、お客様の AWS アカウントにデプロイされた一連の AWS サービスを使用します。インフラストラクチャを正しくセットアップすると、FSx for ONTAP ボリュームアクセスポイントに接続され、ユーザーアクセスとオブジェクト操作の監査イベントをジャーナルテーブルにキャプチャするパイプラインが確立されます。

以下の表は、インフラストラクチャの一部を構成するAWSサービス、それぞれのリソース名のパターン、およびパイプラインにおけるサービスの目的を示しています。

AWSサービス	リソース名のパターン	目的
AWS CloudFormation	netapp-metadata-*	すべてのインフラストラクチャをスタックとしてデプロイします
AWS S3バケット	netapp-metadata-cloudtrail-events-logs-{uuid}	生のCloudTrailログファイルを保存
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	特定のアクセスポイントのS3データイベントをキャプチャします
AWS CloudWatch ロググループ	netapp-metadata-journal-data-events-{uuid}	構造化されたログエントリとしてCloudTrailイベントを受信します
IAMロール	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	アクティブな統合

AWSサービス	リソース名のパターン	目的
ObservabilityAdmin	S3TableIntegration	CloudWatchログをS3 Tablesテーブルにブリッジします
S3テーブル	aws-cloudwatch バケット → logs.aws_cloudtrail__data	構造化され、クエリ可能なCloudTrailイベントをIceberg形式で保存

{uuid}は、テンプレート作成時に生成される、ランダムな8文字の識別子です。

開始する前に

ジャーナルテーブル機能を有効にするには、次の手順を実行します。

- S3アクセスポイントを持つ既存のボリュームがある。["S3アクセスポイントを使用してボリュームを作成する"](#)
- S3アクセスポイントのネットワーク設定を*インターネット*に設定します。["S3アクセスポイントのネットワーク構成を編集"](#)。
- ["_operations and remediation_"の権限を付与する](#)Workload Factoryクレデンシャルに移動します。
- CloudFormation デプロイメントを実行してジャーナルテーブルを設定するために使用する AWS アカウントに、次の IAM ポリシー権限を追加します。

▼ ジャーナルテーブルセットアップのIAMポリシー権限

```
{
  "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"
    }
]
}

```

ジャーナルテーブルのインフラストラクチャをセットアップする

S3アクセスポイントからジャーナルテーブルにAWSサービスイベントをキャプチャするためのインフラストラクチャをセットアップします。

手順

1. "NetApp Console"にログインします。
2. メニュー 、ワークロード > ストレージ > **FSx for ONTAP** を選択します。
3. **FSx for ONTAP** から、更新するボリュームを含むファイルシステムのアクションメニューを選択し、管理を選択します。
4. ファイルシステムの概要から、*ボリューム*タブを選択します。
5. [ボリューム] タブから、S3 アクセス ポイントを管理するボリュームのアクション メニューを選択し、[詳

細アクション] を選択してから、[S3 アクセス ポイントの管理] を選択します。

6. *S3 アクセスポイントの管理*画面でアクションメニューを選択し、*アクセスポイントの編集*を選択します。
7. *S3アクセスポイントの編集*ダイアログで、ネットワーク構成が*インターネット*に設定されていることを確認してください。
8. ダイアログの指示に従って、ジャーナルテーブル機能のインフラストラクチャを設定してください。
9. CloudFormationテンプレートをダウンロードします。
10. AWS アカウントに CloudFormation スタックをデプロイします。
 - a. テンプレート JSON をファイルに保存します。
 - b. AWS CLI または AWS マネジメントコンソールを使用してテンプレートをデプロイします。
 - c. スタックが `CREATE\_COMPLETE` ステータスに達するまで待ちます。
 - d. スタック出力からCloudTrail ARNを取得します。
11. Workload Factoryコンソールに戻り、S3アクセスポイントを管理するボリュームに戻ります。
12. ボリュームアクションメニューから*詳細を表示*を選択します。
13. 「ジャーナルテーブル」 タブで、CloudTrail ARNを入力します。
14. 「適用」を選択します。

いずれかの手順が失敗した場合は、[ジャーナルテーブルのインフラストラクチャ設定のトラブルシューティング](#)または[NetAppサポート](#)にお問い合わせください。

ジャーナルテーブルのインフラストラクチャ設定のトラブルシューティング

AWS 管理コンソールまたは AWS CLI を使用して、CloudFormation スタックのデプロイメント中の障害とそれが作成するリソースのトラブルシューティングを行うことができます。

問題を解決したら、CloudTrail ARN を再度送信してジャーナルテーブルのセットアップを再開してください。

一般的なCloudFormation展開の失敗

IAM権限が不足しています

デプロイを行う役割／ユーザーには、特定の権限セットが必要です。ポリシー全文については[開始する前](#)にを参照してください。

スタックが `AccessDenied` または `InsufficientPermission` エラーで失敗した場合は、スタックイベントを確認し、`ResourceStatusReason` フィールドで不足している権限を探してください。

CloudTrail制限

AWSでは、リージョンごとにデフォルトで5つのトレイルという制限が設けられています。アカウントにすでに5つのトレイルがある場合、`the FsxDataEventTrail` リソースは次のエラーで失敗します：最大トレイル数 (5) を超えました。以下のコマンドを使用すると、リージョンレベルでのトレイルの数を確認できます：

```
aws cloudtrail describe-trails \
```

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

解像度オプション

- オプション1：リージョン内の未使用のトレイルを削除して空き容量を確保する。
- オプション2：既存のトレイルを使用する。FsxDataEventTrail、CloudTrailBucket、CloudTrailBucketPolicy、および `CloudTrailToCloudWatchRole` リソースをCloudFormationスタックを再度デプロイする前にテンプレートから削除します。次に、初期化ステップで既存のトレイルのARNを渡します。既存のトレイルには、CloudWatchロググループが設定され、ロググループに関連付けられたS3TableIntegrationがあり、データイベントをログに記録している必要があります。

S3 Table統合は既に存在します

アカウントに既にaws_cloudtrailデータソース用のS3TableIntegrationが存在する場合、LogsToS3TableIntegrationリソースは失敗します。

解決策

`LogsToS3TableIntegration`と `S3TableIntegrationRole`のリソースを、CloudFormationスタックを再度デプロイする前にテンプレートから削除します。aws_cloudtrailデータイベント用に設定している限り、システムは既存の統合を自動的に使用します。

既存の統合を確認するには：

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

S3 バケット名は既に存在します

バケット名 `netapp-metadata-cloudtrail-events-logs-{uuid}`はグローバルに一意です。競合が発生した場合は、テンプレートを再要求して新しい UUID を取得します。

IAMロールは既に存在します

以前の部分的な展開で `netapp-metadata-\*`名前パターンの IAM ロールが残っていた場合、ロール作成時にスタックが失敗します。まず、孤立したロールを削除してください：

```
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>
```

ジャーナルテーブル有効化後の障害

CloudTrail ARN を送信すると、Workload Factory は *seed* (テストイベント) を自動的に送信してリソースパイプライン全体を検証します。成功すると、シードイベントが S3 Tables テーブルに到着します。テストには約 10 分かかります。

テスト検証が失敗した場合、以下のいずれかのエラーメッセージが表示される可能性があります：

エラー メッセージ	説明
テーブル <code>aws_cloudtrail__data</code> は{bucket}に作成されませんでした。s3table の権限を確認してください。	S3TableIntegration は CloudWatch 管理テーブルを作成しませんでした。CloudWatch Logs と S3 Tables 間のパイプラインが壊れています。
テーブルは存在するが、ジャーナルシードイベントが表示されない。CloudTrailとCloudWatchの権限を確認する。	テーブルは存在するが、特定のシードイベントは発生しなかった。CloudTrailとS3 Tablesテーブルとのパイプラインが壊れています。
ジャーナル設定の開始に失敗しました。...	バックグラウンドでのシード/ポーリング処理中にエラーが発生しました。詳細は末尾のメッセージをご確認ください。

解決手順

ジャーナルがFAILEDに達したら、シードイベントをパイプラインの各ステージに沿って追跡し、停止した正確な場所を特定します。各ステップは、テンプレートによって作成される特定のAWSリソースに対応しています。

1. CloudTrail S3 バケットを確認します。

このトレイルは、生のイベントログをS3バケットに書き込みます `netapp-metadata-cloudtrail-events-logs`。最新のログファイルを探してください。

ログファイルが存在しない場合は、CloudTrailがイベントを捕捉していません。以下の点を確認してください：

- トレイルはログ記録中です(`IsLogging: true`)
- 高度なイベントセレクトタには、正しいアクセスポイント ARN が含まれています。
- 高度なイベントセレクトタには、``eventCategory = Data``および``resources.type = AWS::S3::AccessPoint``のフィルターが含まれます

2. CloudWatchロググループを確認します。

このトレイルは、CloudWatchロググループにイベントも配信します。ロググループ名は``netapp-metadata-journal-data-events-<uuid>``で始まります。

- ロググループが空の場合、CloudTrailはCloudWatchにイベントを配信していません。``CloudTrailToCloudWatchRole`` IAMロールが存在し、``logs:CreateLogStream``および``logs:PutLogEvents`` 権限があること、およびトレイルが正しい``CloudWatchLogsLogGroupArn``および``CloudWatchLogsRoleArn``で構成されていることを確認してください。
- シードイベントがロググループに現れる場合は、問題は下流側にあるため、ステップ3に進んでください。

3. S3 Tables テーブルを確認してください(`aws-cloudwatch`)。

S3TableIntegration は、aws-cloudwatch という名前のテーブルバケットを自動的に作成し、logs.aws_cloudtrail__data というテーブルにデータを投入します。このテーブルは、最初のイベントが通過した後にのみ作成されます。

- aws-cloudwatch テーブルバケットが存在しない場合、 S3TableIntegrationRole`に権限がありません。 `s3tables:CreateTableBucket、 s3tables:PutTableBucketEncryption、 および `s3tables:PutTableBucketPolicy`が必要です。すべて `arn:aws:s3tables:\*:\*:bucket/aws-cloudwatch`にスコープされます。
- テーブルバケットが存在するが `logs.aws\_cloudtrail\_\_data`が存在しない場合、統合はイベントをルーティングしていません。統合は `Status: ACTIVE`を表示し、 `aws\_cloudtrail`をログソースとして含める必要があります。
- テーブルは存在するものの、シードイベントがテーブルに含まれていない場合、そのイベントはまだ転送中である可能性があります。S3 Tablesの取り込みには若干の遅延が発生します。あと数分お待ちください。15〜20分経っても表示されない場合は、統合が失敗している可能性があります。

4. シードイベントを直接照会します。

- a. AWS Management ConsoleでS3 Tablesを開きます。
- b. aws-cloudwatch テーブルバケット → aws_cloudtrail__data テーブルに移動し、 **Preview** ボタンを使用して、ブラウザで直接クイッククエリを実行します。
- c. テーブルにイベントが存在するが、ジャーナルにはまだ `FAILED`が表示される場合、イベントが到着する前にポーリングウィンドウが期限切れになった可能性があります。

問題が解決したら、Workload Factoryコンソールに戻ってください。Trail ARNを再度送信して[ジャーナルテーブルのセットアップを開始しています](#)を再試行してください。

- 1. セットアップが引き続き失敗する場合は、NetApp サポートにお問い合わせください。

ジャーナルテーブル設定の権限リファレンス

CloudFormation スタックを展開してジャーナルテーブル機能を有効にする IAM ロールには、以下の権限が必要です。必要な権限を含むコピー可能な JSON ポリシーについては、[開始する前に](#)を参照してください。

スタック操作

権限	リソース	なぜ
cloudformation : CreateStack	arn:aws:cloudformation:*:*:stack/nextapp-metadata-/	スタックを作成する
cloudformation : DescribeStacks	arn:aws:cloudformation:*:*:stack/nextapp-metadata-/	スタックステータスを監視
cloudformation : DescribeStackEvents	arn:aws:cloudformation:*:*:stack/nextapp-metadata-/	リソースレベルの障害を診断する cloudformation:GetTemplateSummary * プリフライトテンプレート検証

CloudTrail

権限	リソース	なぜ
cloudtrail : CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	トレイルを作成する
cloudtrail : StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	ログ記録を有効にする
cloudtrail : AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	識別タグを適用する
cloudtrail : PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	データイベントキャプチャの設定
cloudtrail : DescribeTrails	*	スタック出力のトレイル ARN を解決します

S3

権限	リソース	なぜ
s3 : CreateBucket	arn:aws:s3:::netapp-metadata-*	CloudTrailログバケットを作成します
s3 : PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	CloudTrailによるログの書き込みを許可する
s3 : PutBucketTagging	arn:aws:s3:::netapp-metadata-*	識別タグを適用する

IAM

権限	リソース	なぜ
iam : CreateRole	arn:aws:iam:*:*:role/netapp-metadata-*	IAMロールを両方とも作成します
iam : PutRolePolicy	arn:aws:iam:*:*:role/netapp-metadata-*	インラインポリシーを添付
iam : TagRole	arn:aws:iam:*:*:role/netapp-metadata-*	識別タグを適用する
iam : GetRole	arn:aws:iam:*:*:role/netapp-metadata-*	ロールがアクティブであることを確認します
iam : PassRole	arn:aws:iam:*:*:role/netapp-metadata-* (条件 : PassedToService = cloudtrail.amazonaws.com、logs.amazonaws.com)	CloudTrailおよびCloudWatch Logs にロールを渡す

CloudWatchログ

権限	リソース	なぜ
ログ : CreateLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	ロググループを作成する

権限	リソース	なぜ
ログ：DeleteLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	作成に失敗した場合はロググループをクリーンアップします
ログ：PutRetentionPolicy	arn:aws:logs:*:*:log-group:netapp-metadata-*	30日間の保持期間を設定
ログ：TagResource	arn:aws:logs:*:*:log-group:netapp-metadata-*	識別タグを適用する
logs:AssociateSourceToS3TableIntegration	arn:aws:logs:*:*:log-group:netapp-metadata-*	CloudTrailソースをS3 Tablesにリンク
ログ：DescribeLogGroups	*	ロググループの存在を確認する
logs：S3テーブル統合のソース一覧	*	統合の関連付けを確認

ObservabilityAdmin

権限	リソース	なぜ
observabilityadmin:CreateS3TableIntegration	*	CloudWatch → S3 Tables ブリッジを作成します
observabilityadmin:GetS3TableIntegration	*	統合がアクティブであることを確認
observabilityadmin：TagResource	*	識別タグを適用する
observabilityadmin ：ListTagsForResource	*	ドリフト検出

S3テーブル

権限	リソース	なぜ
s3tables：CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	S3 Tablesバケットを作成する（統合ロール経由）
s3tables ：PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	AES256暗号化を設定する
s3tables：PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	CloudWatch Logs へのアクセスを許可

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。