



Gerenciar pontos de acesso S3

Workload Factory for NetApp Console

NetApp

October 07, 2026

Índice

Gerenciar pontos de acesso S3	1
Crie pontos de acesso S3 para um volume no NetApp Workload Factory	1
Gerencie os pontos de acesso S3 para um volume no NetApp Workload Factory	2
Edite os pontos de acesso S3 para um volume	2
Veja os detalhes do ponto de acesso S3 para um volume	3
Exclua os pontos de acesso S3 para um volume no NetApp Workload Factory	3
Configure a infraestrutura da tabela de diário para NetApp Workload Factory	4
Sobre esta tarefa	4
Antes de começar	5
Configure a infraestrutura da tabela de diários	7
Solucionar problemas na configuração da infraestrutura da tabela de diário	8
Referência de permissões para a configuração da tabela de diário	11

Gerenciar pontos de acesso S3

Crie pontos de acesso S3 para um volume no NetApp Workload Factory

Crie e anexe pontos de acesso S3 para um volume no NetApp Workload Factory.

Sobre esta tarefa

Amazon FSx for NetApp ONTAP permite que sistemas de arquivos NFS e SMB acessem dados do S3 e se conectem a serviços da AWS como Amazon Bedrock, SageMaker, Athena, AWS Glue e mais. Você pode conectar serviços da AWS a todos os seus dados de storage de objetos.

Anexe pontos de acesso S3 a volumes NFS e SMB em um sistema de arquivos FSx for ONTAP para que os serviços da AWS acessem os arquivos como se estivessem em um bucket S3. Ao anexar o ponto de acesso, defina um ID exclusivo, selecione o tipo de acesso a arquivos (UNIX ou Windows) e adicione um nome de usuário para autorização de acesso.

Após conectar o ponto de acesso S3, ele aparece no Console de Gerenciamento da AWS com um alias exclusivo. Use esse alias como o nome do bucket S3 para serviços da AWS, como Amazon Bedrock, para acessar arquivos no volume FSx for ONTAP.

Você pode conectar vários pontos de acesso S3 a um único FSx for ONTAP volume, cada um com um nível de acesso exclusivo, para se conectar a vários serviços AWS.

Antes de começar

Cumpra os seguintes requisitos antes de começar.

- Você precisa ter um volume existente com um ponto de acesso S3. "[Crie um volume com um ponto de acesso S3](#)"
- Você deve "[Conceda credenciais com a política de permissão operações e remediação](#)" no Workload Factory para concluir esta tarefa.

Passos

1. Faça login no "[NetApp Console](#)".
2. Selecione o menu , **Workloads > Volumes explorer**.
3. Selecione o menu de ações para o volume que você deseja usar, depois selecione **Ações avançadas** e, em seguida, **Gerenciar pontos de acesso S3**.
4. Na página Gerenciar pontos de acesso S3, selecione **Criar e anexar ponto de acesso S3**.
5. Na página **Criar e conectar ponto de acesso S3**, forneça as seguintes informações:
 - **Nome do ponto de acesso S3**: insira o nome do ponto de acesso S3.
 - **User**: Selecione um usuário existente com acesso ao volume ou crie um novo usuário.
 - **Tipo de usuário**: selecione **UNIX** ou **Windows** como o tipo de usuário.
 - **Configuração de rede**: Selecione **Internet** ou **nuvem privada (VPC)**. O tipo de rede que você escolher determina se o ponto de acesso será acessível pela internet ou restrito a uma VPC específica. Para usar o recurso de tabela Journal, você deve selecionar **Internet** como configuração de rede.

- **Tabela de inventário:** Opcional. Requer a `getObject` permissão. Habilite a tabela de inventário no volume para gerar metadados para todos os objetos acessíveis ao ponto de acesso S3 e isso acarreta custos de solicitação do AWS S3. Consulte ["Documentação de preços do Amazon S3"](#) para obter mais informações. A tabela é atualizada a cada 24 horas.
- **Tags de ponto de acesso S3:** Opcionalmente, você pode adicionar até 50 tags ou remover tags.

6. Selecione **Criar**.

Informações relacionadas

Opcionalmente, você pode usar o recurso de tabela de registro (Journal table) com pontos de acesso S3 no Workload Factory. A infraestrutura da tabela de registro captura e armazena logs de auditoria de eventos de acesso do usuário e operações de objetos em pontos de acesso de volume do Amazon FSx para ONTAP. Para habilitar o recurso de tabela de registro, você deve configurar a infraestrutura AWS necessária, incluindo AWS CloudTrail, AWS CloudWatch, buckets do AWS S3, grupos de logs do AWS CloudWatch e funções e políticas do AWS Identity and Access Management (IAM). ["Configure a infraestrutura da tabela de diários para NetApp Workload Factory"](#).

Outros tópicos relacionados:

["Edite ou exclua pontos de acesso S3 para um volume na NetApp Workload Factory"](#)

Gerencie os pontos de acesso S3 para um volume no NetApp Workload Factory

Atualize os detalhes do ponto de acesso S3 ou exclua os pontos de acesso S3 de um volume na NetApp Workload Factory.

Você também pode habilitar ou desabilitar a **Inventory table** para o ponto de acesso. A inventory table gera metadados para todos os objetos acessíveis ao ponto de acesso S3 e incorre em custos de solicitação do AWS S3. Consulte ["Documentação de preços do Amazon S3"](#) para obter mais informações.

Edite os pontos de acesso S3 para um volume

Edite os pontos de acesso S3 para um volume no NetApp Workload Factory.

Passos

1. Faça login no ["NetApp Console"](#).
2. Selecione o menu , **Cargas de trabalho > Armazenamento > Explorador de volumes**.
3. Selecione o menu de ações do volume para o qual você deseja editar os pontos de acesso S3, depois selecione **Ações avançadas** e, em seguida, **Gerenciar pontos de acesso S3**.
4. Na tela **Gerenciar pontos de acesso S3**, selecione o menu de ações e depois selecione **Editar ponto de acesso**.
5. Faça as atualizações e depois selecione **Apply**.

Para configurar a infraestrutura para o recurso de tabela de diário, você deve selecionar **Internet** como a configuração de rede para o ponto de acesso S3. ["Aprenda como configurar a infraestrutura da tabela Journal para NetApp Workload Factory"](#).

Veja os detalhes do ponto de acesso S3 para um volume

Visualize detalhes do ponto de acesso S3, como o alias, o ARN e o URI do S3. Com as tabelas de inventário e registro em diário ativadas, você pode visualizar metadados e registros de auditoria de eventos de acesso do usuário e operações de objetos em todos os pontos de acesso S3.

Sobre esta tarefa

Quando a tabela de inventário está habilitada no volume, você pode visualizar os detalhes do ponto de acesso, da tabela de inventário e do bucket da tabela dos pontos de acesso S3 existentes conectados ao volume. O sistema também fornece um link para a tabela de inventário no Console de Gerenciamento da AWS.

Quando a tabela de registro (journal table) está habilitada, o Workload Factory gera logs nos pontos de acesso em uma tabela para sua referência. A tabela inclui CloudTrail eventos, trilhas (um registro das atividades da AWS), CloudTrail filtros, CloudWatch grupos de logs e muito mais.

Você pode copiar os detalhes do ponto de acesso para uso em outros aplicativos.

Passos

1. Faça login no "NetApp Console".
2. Selecione o menu , **Cargas de trabalho > Armazenamento > Explorador de volumes**.
3. Selecione o menu de ações do volume para o qual deseja visualizar os detalhes, depois selecione **Ações avançadas** e depois **Visualizar detalhes**.

Os detalhes aparecem em quatro abas: **Ponto de acesso**, **Tabela de inventário**, **Tabela de diário** e **Bucket da tabela**.

4. Se o status para tabelas de inventário ou diário estiver habilitado, mas você não tiver a `get:Object` permissão, siga as instruções na caixa de diálogo para adicionar a permissão exigida.
5. Quando o status da tabela de registro em diário estiver pendente, você deverá fornecer o CloudTrail ARN para conectar a tabela de registro em diário à infraestrutura criada. Siga as instruções para implantar a pilha CloudFormation usando a AWS CLI ou o Console de Gerenciamento da AWS e, em seguida, retorne ao console do Workload Factory para inserir o CloudTrail ARN.

Exclua os pontos de acesso S3 para um volume no NetApp Workload Factory

Excluir pontos de acesso S3 existentes de um volume em NetApp Workload Factory.

Passos

1. Faça login no "NetApp Console".
2. Selecione o menu , **Cargas de trabalho > Armazenamento > Explorador de volumes**.
3. Selecione o menu de ações para o volume para o qual você deseja gerenciar os pontos de acesso S3, depois selecione **Ações avançadas** e, em seguida, **Gerenciar pontos de acesso S3**.
4. Selecione o menu de ações para o ponto de acesso S3 a ser excluído e, em seguida, selecione **Excluir**.
5. Na caixa de diálogo **Excluir um ponto de acesso S3**, selecione **Excluir** para excluir o ponto de acesso S3 do volume.

O Workload Factory não exclui a tabela de inventário ou a tabela de diário, mas você pode removê-las manualmente no AWS Management Console.

Informações relacionadas

- ["Configure a infraestrutura da tabela de diários"](#)

Configure a infraestrutura da tabela de diário para NetApp Workload Factory

Configure a infraestrutura da tabela Journal para capturar e armazenar logs de auditoria de eventos de acesso de usuários e operações de objetos em pontos de acesso de volumes do Amazon FSx for ONTAP. Várias etapas são necessárias para configurar a infraestrutura para serviços AWS como AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch log group, AWS Identity and Access Management (IAM) e AWS S3 Tables, para que os eventos de log sejam transmitidos corretamente pelo pipeline e lidos pelo Workload Factory.

Sobre esta tarefa

O recurso de tabela de diário captura eventos do plano de dados do S3 (PutObject, GetObject, DeleteObject, etc.) para pontos de acesso S3 do FSx for ONTAP monitorados. Ele utiliza uma cadeia de serviços da AWS implantada em sua conta da AWS. Quando a infraestrutura está configurada corretamente, ela se conecta ao ponto de acesso ao volume do FSx for ONTAP e estabelece o pipeline que captura eventos de auditoria de acesso do usuário e operação de objeto na tabela de diário.

A tabela a seguir lista os serviços da AWS que fazem parte da infraestrutura, seus respectivos padrões de nomenclatura de recursos e a finalidade do serviço no pipeline.

Serviço AWS	Padrão de nome de recurso	Propósito
AWS CloudFormation	netapp-metadata-*	Implanta toda a infraestrutura como uma pilha
Bucket S3 da AWS	netapp-metadata-cloudtrail-events-logs-{uuid}	Armazena arquivos de log brutos do CloudTrail
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Captura eventos de dados S3 para pontos de acesso específicos
Grupo de logs da AWS CloudWatch	eventos de dados de diário de metadados netapp-{uuid}	Recebe CloudTrail eventos como entradas de log estruturadas
Funções do IAM	• netapp-metadata-cloudtrail-cw-role-{uuid} • netapp-metadata-s3table-integration-role-{uuid}	Integração ativa
ObservabilityAdmin	S3TableIntegration	Integra os Logs do CloudWatch em uma tabela do S3 Tables
Tabelas S3	bucket aws-cloudwatch → logs.aws_cloudtrail__data	Armazena eventos CloudTrail estruturados e consultáveis no formato Iceberg

O {uuid} é um identificador aleatório de 8 caracteres gerado quando o modelo é criado.

Antes de começar

Para ativar o recurso de tabela de diário, siga estes passos:

- Possui um volume existente com um ponto de acesso S3. ["Crie um volume com um ponto de acesso S3"](#)
- Defina a configuração de rede como **Internet** para o ponto de acesso S3. ["Editar a configuração de rede para o ponto de acesso S3"](#).
- ["Conceda as permissões de operações e remediação"](#) às suas credenciais do Workload Factory.
- Adicione as seguintes permissões de política do IAM à conta da AWS que você usa para executar a implantação do CloudFormation para configurar a tabela Journal.

▼ Permissões de política IAM para configuração da tabela de diário

```
{
  "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"
  }
]
}

```

Configure a infraestrutura da tabela de diários

Configure a infraestrutura para capturar eventos de serviço da AWS a partir do ponto de acesso S3 na tabela de registro (journal).

Passos

1. Faça login no ["NetApp Console"](#).
2. Selecione o menu , **Workloads > Storage > FSx for ONTAP**.
3. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos com o volume que você deseja atualizar e, em seguida, selecione **Manage**.
4. Na visão geral do sistema de arquivos, selecione a guia **Volumes**.
5. Na guia Volumes, selecione o menu de ações do volume para o qual deseja gerenciar pontos de acesso S3, depois selecione **Ações avançadas** e, em seguida, **Gerenciar pontos de acesso S3**.
6. Na tela **Gerenciar pontos de acesso S3**, selecione o menu de ações e depois selecione **Editar ponto de acesso**.
7. Na caixa de diálogo **Editar ponto de acesso S3**, verifique se a configuração de rede está definida como **Internet**.
8. Siga as instruções na caixa de diálogo para configurar a infraestrutura para o recurso de tabela de journal.
9. Baixe o modelo CloudFormation.
10. Implante a pilha CloudFormation em sua conta da AWS.
 - a. Salve o modelo JSON em um arquivo.
 - b. Implante o modelo usando a AWS CLI ou o Console de Gerenciamento da AWS.

- c. Aguarde até que a pilha atinja `CREATE_COMPLETE` status.
- d. Obtenha o CloudTrail ARN a partir das saídas da pilha.
11. Retorne ao console do Workload Factory e volte ao volume para gerenciar os pontos de acesso S3.
12. Selecione **Ver detalhes** no menu de ações de volume.
13. Na aba **Tabela de diário**, insira o CloudTrail ARN.
14. Selecione **Aplicar**.

Se alguma das etapas falhar, [solucionar problemas de configuração de infraestrutura para a tabela de diário](#) ou entre em contato com o suporte da NetApp para obter ajuda.

Solucionar problemas na configuração da infraestrutura da tabela de diário

Você pode usar o Console de Gerenciamento da AWS ou a AWS CLI para solucionar problemas durante a implantação da pilha CloudFormation e dos recursos que ela cria.

Após resolver o problema, envie o CloudTrail ARN novamente para reiniciar a configuração da tabela de registro.

Falhas comuns de implantação do CloudFormation

Permissões IAM insuficientes

A função/usuário que realiza a implantação precisa de um conjunto específico de permissões. Consulte [Antes de começar](#) para a política completa.

Se a pilha falhar com um `AccessDenied` ou `InsufficientPermission` erro, verifique os eventos da pilha e procure pela permissão ausente no campo `ResourceStatusReason`.

CloudTrail limite

A AWS impõe um limite padrão de 5 trilhas por região. Se a conta já tiver 5 trilhas, the `FsxDataEventTrail` o recurso falhará com: Número máximo de trilhas (5) excedido. Você pode verificar o número de trilhas em nível regional com o seguinte comando:

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

Opções de resolução

- Opção 1: exclua uma trilha não utilizada na região para liberar espaço.
- Opção 2: Use uma trilha existente. Remova os recursos `FsxDataEventTrail`, `CloudTrailBucket`, `CloudTrailBucketPolicy` e `CloudTrailToCloudWatchRole` do modelo antes de implantar a pilha CloudFormation novamente. Em seguida, passe o ARN da sua trilha existente durante a etapa de inicialização. A trilha existente deve ter um CloudWatch Log Group configurado, uma `S3TableIntegration` associada ao grupo de logs e estar registrando eventos de dados.

A integração com a tabela S3 já existe

Se a conta já possuir uma `S3TableIntegration` para a fonte de dados `aws_cloudtrail`, o recurso `LogsToS3TableIntegration` falhará.

Resolução

Remova os `LogsToS3TableIntegration` e `S3TableIntegrationRole` recursos do modelo antes de implantar a pilha CloudFormation novamente. O sistema usa automaticamente a integração existente, desde que você a configure para eventos de dados do `aws_cloudtrail`.

Para verificar se já existe uma integração:

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

O nome do bucket S3 já existe

O nome do bucket `netapp-metadata-cloudtrail-events-logs-{uuid}` é globalmente único. Se houver conflito, solicite novamente o template para obter um novo UUID.

A função IAM já existe

Se uma implantação parcial anterior deixou funções do IAM com o `netapp-metadata-*` padrão de nome, a criação da função falhará. Exclua primeiro as funções órfãs:

```
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>
```

Falhas após capacitação da tabela Journal

Após o envio do ARN do CloudTrail, o Workload Factory valida todo o pipeline de recursos enviando automaticamente um *seed*, ou evento de teste. Se bem-sucedido, o evento *seed* chega na tabela S3 Tables. O teste leva aproximadamente 10 minutos.

Se a validação do teste falhar, você poderá receber uma das seguintes mensagens de erro:

Mensagem de erro	Significado
A tabela <code>aws_cloudtrail__data</code> não foi criada em {bucket}. Verifique as permissões da tabela s3.	<code>S3TableIntegration</code> não criou a tabela gerenciada pelo CloudWatch. O pipeline entre os logs do CloudWatch e as tabelas do S3 está interrompido.
A tabela existe, mas o evento inicial do diário não aparece. Verifique as permissões do CloudTrail e do CloudWatch.	A tabela existe, mas o evento de inicialização específico nunca chegou. O pipeline está interrompido entre CloudTrail e a tabela S3 Tables.
Falha ao iniciar a configuração do diário. ...	Ocorreu um erro durante o fluxo de inicialização/verificação em segundo plano. Verifique a mensagem subsequente para obter detalhes.

Etapas de resolução

Quando o registro atingir o status `FAILED`, rastreie o evento inicial através dos estágios do pipeline para identificar exatamente onde ele parou. Cada etapa corresponde a um recurso específico da AWS criado pelo template.

1. Verifique o bucket S3 do CloudTrail.

O processo de trilha grava os registros de eventos brutos no bucket S3 `netapp-metadata-cloudtrail-events-logs`. Procure por arquivos de registro recentes.

Se não existirem arquivos de log, então o CloudTrail não está capturando eventos. Verifique o seguinte:

- A trilha está registrando (`IsLogging: true`)
- Os seletores de eventos avançados incluem o ARN do ponto de acesso correto
- Os seletores de eventos avançados incluem os filtros para `eventCategory = Data` e `resources.type = AWS::S3::AccessPoint`

2. Verifique o grupo de logs do CloudWatch.

A trilha também entrega eventos ao CloudWatch Log Group. O nome do grupo de registros começa com `netapp-metadata-journal-data-events-<uuid>`.

- Se o grupo de logs estiver vazio, então o CloudTrail não está entregando eventos ao CloudWatch. Verifique se a função do `CloudTrailToCloudWatchRole` IAM existe e possui `logs:CreateLogStream` e `logs:PutLogEvents` permissões, e se o trail está configurado com o `CloudWatchLogsLogGroupArn` e `CloudWatchLogsRoleArn` corretos.
- Se o evento inicial aparecer no grupo de logs, o problema está a jusante — prossiga para a Etapa 3.

3. Consulte a tabela S3 Tables (`aws-cloudwatch`).

A `S3TableIntegration` cria automaticamente um bucket de tabela chamado `aws-cloudwatch` e preenche uma tabela em `logs.aws_cloudtrail__data`. Essa tabela só é criada após o primeiro evento ser processado.

- Se o bucket da tabela `aws-cloudwatch` não existir, então o `S3TableIntegrationRole` está sem permissões. Ele precisa de `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` e `s3tables:PutTableBucketPolicy` — todos com escopo para `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Se o bucket da tabela existir mas `logs.aws_cloudtrail__data` não existir, então a integração não está roteando eventos. A integração deve mostrar `Status: ACTIVE` e incluir `aws_cloudtrail` como uma fonte de log.
- Se a tabela existir, mas o evento inicial não estiver nela, o evento pode ainda estar em trânsito. A ingestão de tabelas S3 tem alguma latência. Aguarde mais alguns minutos. Se ainda não aparecer após 15-20 minutos, a integração pode estar interrompida.

4. Consulte o evento inicial diretamente.

- Abra as tabelas do S3 no Console de Gerenciamento da AWS.
- Navegue até o bucket da tabela `aws-cloudwatch` → tabela `aws_cloudtrail__data` e use o botão **Preview** para executar uma consulta rápida diretamente no navegador.
- Se o evento estiver presente na tabela, mas o diário ainda mostrar `FAILED`, então a janela de pesquisa pode ter expirado antes da chegada do evento.

Após resolver o problema, retorne ao console do Workload Factory. Tente [Iniciando a configuração da tabela de diário](#) novamente enviando o Trail ARN.

1. Se a configuração continuar a falhar, entre em contato com o suporte da NetApp para obter assistência.

Referência de permissões para a configuração da tabela de diário

A função do IAM que implementa a pilha CloudFormation para habilitar o recurso de tabela Journal precisa das seguintes permissões. Consulte [Antes de começar](#) para uma política JSON copiável com as permissões necessárias.

Operações de pilha

Permissão	Recurso	Por que
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Crie a pilha
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Monitorar o status da pilha
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Diagnosticar falhas em nível de recurso no cloudformation:GetTemplateSummary * Validação prévia do template

CloudTrail

Permissão	Recurso	Por que
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Crie a trilha
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Ativar registro de logs
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Aplique a etiqueta de identificação
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Configurar captura de eventos de dados
cloudtrail:DescribeTrails	*	Resolver ARN de trilha para saída de stack

S3

Permissão	Recurso	Por que
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Crie o bucket de logs CloudTrail
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Permitir que o CloudTrail grave logs
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Aplique a etiqueta de identificação

IAM

Permissão	Recurso	Por que
iam:CreateRole	arn:aws:iam::*:role/netapp-metadata-*	Crie ambas as funções do IAM
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Anexar políticas embutidas
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Aplique a etiqueta de identificação
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Confirme se a função está ativa
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (condição: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Atribuir funções ao CloudTrail e aos CloudWatch Logs

Logs do CloudWatch

Permissão	Recurso	Por que
logs:CreateLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	Crie o grupo de logs
logs>DeleteLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	Limpar o grupo de logs se a criação falhar
registros:PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-metadata-*	Defina retenção de 30 dias
registros:TagResource	arn:aws:logs::*:log-group:netapp-metadata-*	Aplique a etiqueta de identificação
logs:AssociateSourceToS3TableIntegration	arn:aws:logs::*:log-group:netapp-metadata-*	Vincular a fonte CloudTrail às tabelas S3
registros:DescribeLogGroups	*	Verificar a existência do grupo de logs
logs:ListSourcesForS3TableIntegration	*	Confirmar associação de integração

ObservabilityAdmin

Permissão	Recurso	Por que
observabilityadmin:CreateS3TableIntegration	*	Crie a ponte CloudWatch → Tabelas S3
observabilityadmin:GetS3TableIntegration	*	Confirme se a integração está ativa
observabilityadmin:TagResource	*	Aplique a etiqueta de identificação

Permissão	Recurso	Por que
observabilityadmin:ListTagsForResource	*	Detecção de deriva

Tabelas S3

Permissão	Recurso	Por que
s3tables:CreateTableBucket	arn:aws:s3tables:*.*:bucket/aws-cloudwatch	Crie o bucket de tabelas S3 (via função de integração)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*.*:bucket/aws-cloudwatch	Configurar criptografia AES256
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*.*:bucket/aws-cloudwatch	Permitir acesso aos registros do CloudWatch

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.