



Gestionar puntos de acceso de S3

Workload Factory for NetApp Console

NetApp
October 07, 2026

Tabla de contenidos

- Gestionar puntos de acceso de S3 1
 - Crear puntos de acceso S3 para un volumen en NetApp Workload Factory 1
 - Gestionar los puntos de acceso a S3 de un volumen en NetApp Workload Factory 2
 - Edita los puntos de acceso de S3 para un volumen 2
 - Ver detalles del punto de acceso S3 de un volumen 3
 - Eliminar los puntos de acceso S3 para un volumen en NetApp Workload Factory 3
- Configura la infraestructura de la tabla Journal para NetApp Workload Factory 4
 - Acerca de esta tarea 4
 - Antes de empezar 5
 - Configura la infraestructura de la tabla de registro en diario 7
 - Soluciona problemas de la configuración de la infraestructura para la tabla de registro en diario 8
 - Referencia de permisos para la configuración de la tabla de registro en diario 11

Gestionar puntos de acceso de S3

Crear puntos de acceso S3 para un volumen en NetApp Workload Factory

Crea y adjunta puntos de acceso S3 para un volumen en NetApp Workload Factory.

Acerca de esta tarea

Amazon FSx for NetApp ONTAP permite que los sistemas de archivos NFS y SMB accedan a datos de S3 y se conecten a servicios de AWS como Amazon Bedrock, SageMaker, Athena, AWS Glue y más. Puedes conectar servicios de AWS a todos tus datos de almacenamiento de objetos.

Adjunta puntos de acceso S3 a volúmenes NFS y SMB en un sistema de archivos FSx for ONTAP para que los servicios de AWS accedan a los archivos como si estuvieran en un bucket S3. Al adjuntar el punto de acceso, define un ID único, selecciona el tipo de acceso a archivos (UNIX o Windows) y añade un nombre de usuario para la autorización de acceso.

Después de adjuntar el punto de acceso de S3, aparece en la consola de gestión de AWS con un alias único. Usa este alias como el nombre del bucket de S3 para los servicios de AWS, como Amazon Bedrock, para acceder a los archivos en el volumen de FSx for ONTAP.

Puedes adjuntar varios puntos de acceso S3 a un solo volumen FSx for ONTAP, cada uno con un nivel de acceso único, para conectarte a varios servicios de AWS.

Antes de empezar

Completa los siguientes requisitos antes de empezar.

- Debes tener un volumen existente con un punto de acceso S3. ["Crear un volumen con un punto de acceso S3"](#)
- Debes ["conceder credenciales con la política de permisos operations and remediation"](#) en Workload Factory para completar esta tarea.

Pasos

1. Inicia sesión en ["NetApp Console"](#).
2. Selecciona el menú  **Cargas de trabajo > Explorador de volúmenes**.
3. Selecciona el menú de acciones del volumen que quieras utilizar, luego selecciona **Acciones avanzadas** y después **Gestionar puntos de acceso a S3**.
4. En la página Gestionar puntos de acceso S3, selecciona **Crear y adjuntar punto de acceso S3**.
5. En la página **Crear y adjuntar punto de acceso S3**, proporciona la siguiente información:
 - **Nombre del punto de acceso S3:** Ingresa el nombre del punto de acceso S3.
 - **Usuario:** selecciona un usuario existente con acceso al volumen o crea un nuevo usuario.
 - **Tipo de usuario:** selecciona **UNIX** o **Windows** como tipo de usuario.
 - **Configuración de red:** selecciona **Internet** o **Virtual private cloud (VPC)**. El tipo de red que elijas determina si el punto de acceso es accesible desde internet o está restringido a una VPC específica. Para usar la función Journal table, debes seleccionar **Internet** como configuración de red.
 - **Tabla de inventario:** Opcional. Requiere el getObject permiso. Habilita la tabla de inventario en el

volumen para generar metadatos para todos los objetos accesibles al punto de acceso S3 e incurre en costes de solicitud de AWS S3. Consulta ["Documentación de precios de Amazon S3"](#) para obtener más información. La tabla se actualiza cada 24 horas.

- **Etiquetas de punto de acceso S3:** Opcionalmente, puedes añadir hasta 50 etiquetas o eliminar etiquetas.

6. Selecciona **Crear**.

Información relacionada

Opcionalmente, puedes usar la función de tabla de diario con puntos de acceso S3 en Workload Factory. La infraestructura de la tabla de diario captura y almacena registros de auditoría de eventos de acceso de usuario y operaciones de objetos en todos los puntos de acceso de volumen de Amazon FSx para ONTAP. Para habilitar la función de tabla de diario, debes configurar la infraestructura necesaria de AWS, incluyendo AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, grupos de logs de AWS CloudWatch y roles y políticas de AWS Identity and Access Management (IAM). ["Configura la infraestructura de la tabla de registro en diario para NetApp Workload Factory"](#).

Otros temas relacionados:

["Editar o eliminar puntos de acceso S3 para un volumen en NetApp Workload Factory"](#)

Gestionar los puntos de acceso a S3 de un volumen en NetApp Workload Factory

Actualiza los detalles de los puntos de acceso de S3 o elimina los puntos de acceso de S3 de un volumen en NetApp Workload Factory.

También puedes habilitar o deshabilitar la **Inventory table** para el punto de acceso. La inventory table genera metadatos para todos los objetos accesibles al punto de acceso S3 e incurre en costes de solicitud de AWS S3. Consulta ["Documentación de precios de Amazon S3"](#) para obtener más información.

Edita los puntos de acceso de S3 para un volumen

Edita los puntos de acceso S3 para un volumen en NetApp Workload Factory.

Pasos

1. Inicia sesión en ["NetApp Console"](#).
2. Selecciona el menú , **Cargas de trabajo > Almacenamiento > Explorador de volúmenes**.
3. Selecciona el menú de acciones del volumen para el que deseas editar los puntos de acceso a S3, luego selecciona **Acciones avanzadas** y después **Gestionar puntos de acceso a S3**.
4. Desde la pantalla **Manage S3 access points**, selecciona el menú de acciones y luego selecciona **Edit access point**.
5. Haz las actualizaciones y luego selecciona **Aplicar**.

Para configurar la infraestructura para la función de tabla de registro en diario, debes seleccionar **Internet** como configuración de red para el punto de acceso S3. ["Aprende cómo configurar la infraestructura de la tabla Journal para NetApp Workload Factory"](#).

Ver detalles del punto de acceso S3 de un volumen

Ver detalles del punto de acceso S3 como el alias, ARN y S3 URI. Con las tablas de inventario y registro en diario habilitadas, puedes ver metadatos y registros de auditoría de eventos de acceso de usuarios y operaciones de objetos a través de puntos de acceso S3.

Acerca de esta tarea

Cuando la tabla de inventario está habilitada en el volumen, puedes ver los detalles del punto de acceso, la tabla de inventario y el bucket de tabla de los puntos de acceso S3 existentes adjuntos al volumen. El sistema también proporciona un enlace a la tabla de inventario en la AWS Management Console.

Cuando la tabla de registro diario está habilitada, Workload Factory genera registros sobre los puntos de acceso en una tabla para tu referencia. La tabla incluye eventos de CloudTrail, rastros (un registro de las actividades de AWS), filtros de CloudTrail, grupos de registro de CloudWatch y más.

Puedes copiar los detalles del punto de acceso para usarlos en otras aplicaciones.

Pasos

1. Inicia sesión en "[NetApp Console](#)".
2. Selecciona el menú , **Cargas de trabajo > Almacenamiento > Explorador de volúmenes**.
3. Selecciona el menú de acciones del volumen cuyos detalles quieras consultar, luego selecciona **Acciones avanzadas** y, a continuación, **Ver detalles**.

Los detalles aparecen en cuatro pestañas: **Punto de acceso**, **Tabla de inventario**, **Tabla de diario** y **Tabla de bucket**.

4. Si el estado de las tablas de inventario o de registro en diario está activado, pero te falta el permiso `get:Object`, sigue las instrucciones del cuadro de diálogo para añadir el permiso necesario.
5. Cuando el estado de la tabla de registro en diario es pendiente, debes proporcionar el ARN de CloudTrail para conectar la tabla de registro en diario a la infraestructura creada. Sigue las instrucciones para implementar la pila de CloudFormation usando la AWS CLI o la consola de administración de AWS y luego vuelve a la consola de Workload Factory para ingresar el ARN de CloudTrail.

Eliminar los puntos de acceso S3 para un volumen en NetApp Workload Factory

Elimina los puntos de acceso S3 existentes de un volumen en NetApp Workload Factory.

Pasos

1. Inicia sesión en "[NetApp Console](#)".
2. Selecciona el menú , **Cargas de trabajo > Almacenamiento > Explorador de volúmenes**.
3. Selecciona el menú de acciones del volumen para el que quieres gestionar los puntos de acceso de S3, luego selecciona **Acciones avanzadas** y después **Gestionar puntos de acceso de S3**.
4. Selecciona el menú de acciones para el punto de acceso S3 que quieres eliminar y luego selecciona **Eliminar**.
5. En el cuadro de diálogo **Eliminar un punto de acceso S3**, selecciona **Eliminar** para borrar el punto de acceso S3 del volumen.

Workload Factory no elimina el inventario ni la tabla de registro, pero puedes eliminarlos manualmente desde la AWS Management Console.

Información relacionada

- ["Configura la infraestructura de la tabla de registro en diario"](#)

Configura la infraestructura de la tabla Journal para NetApp Workload Factory

Configura la infraestructura de la tabla Journal para capturar y almacenar registros de auditoría de eventos de acceso de usuarios y operaciones de objetos en los puntos de acceso de volúmenes de Amazon FSx para ONTAP. Se necesitan varios pasos para configurar la infraestructura para servicios de AWS como AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch log group, AWS Identity and Access Management (IAM) y AWS S3 Tables para que los eventos de registro viajen correctamente por la canalización y sean leídos por Workload Factory.

Acerca de esta tarea

La función de tabla Journal captura eventos del plano de datos de S3 (PutObject, GetObject, DeleteObject, etc.) para los puntos de acceso a S3 monitorizados de FSx para ONTAP. Utiliza una cadena de servicios de AWS implementados en tu cuenta de AWS. Cuando configuras la infraestructura correctamente, se conecta al punto de acceso al volumen de FSx para ONTAP y establece la canalización que captura los eventos de auditoría de acceso de usuarios y operaciones de objetos en la tabla Journal.

En la siguiente tabla se enumeran los servicios de AWS que forman parte de la infraestructura, sus respectivos patrones de nombres de recursos y la finalidad del servicio en la canalización.

Servicio AWS	Patrón de nombre de recurso	Propósito
AWS CloudFormation	netapp-metadata-*	Despliega toda la infraestructura como una pila
Bucket de AWS S3	netapp-metadatos-cloudtrail-eventos-registros-{uuid}	Almacena archivos de registro sin procesar CloudTrail
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Captura eventos de datos S3 para puntos de acceso específicos
Grupo de registros de AWS CloudWatch	netapp-metadatos-journal-datos-eventos-{uuid}	Recibe eventos de CloudTrail como entradas de registro estructuradas
Funciones IAM	• netapp-metadatos-cloudtrail-cw-role-{uuid} • netapp-metadata-s3table-integration-role-{uuid}	Integración activa
ObservabilityAdmin	S3TableIntegration	Conecta CloudWatch Logs a una tabla S3 Tables
Tablas S3	bucket aws-cloudwatch → logs.aws_cloudtrail__data	Almacena eventos estructurados y consultables de CloudTrail en formato Iceberg

El {uuid} es un identificador aleatorio de 8 caracteres generado al crear la plantilla.

Antes de empezar

Para activar la función de tabla de registro en diario, completa estos pasos:

- Tener un volumen existente con un punto de acceso S3. ["Crear un volumen con un punto de acceso S3"](#)
- Establece la configuración de red en **Internet** para el punto de acceso S3. ["Editar la configuración de red del punto de acceso S3"](#).
- ["Concede los permisos de operaciones y remediación"](#) a tus credenciales de Workload Factory.
- Agrega los siguientes permisos de la política de IAM a la cuenta de AWS que usas para ejecutar la implementación de CloudFormation y configurar la tabla Journal.

▼ Permisos de la política IAM para la configuración de la tabla 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"
  }
]
}

```

Configura la infraestructura de la tabla de registro en diario

Configura la infraestructura para capturar eventos de servicio de AWS desde el punto de acceso S3 en la tabla de diario.

Pasos

1. Inicia sesión en ["NetApp Console"](#).
2. Selecciona el menú  **Workloads > Storage > FSx for ONTAP**.
3. En **FSx for ONTAP**, selecciona el menú de acciones del sistema de archivos que contiene el volumen que deseas actualizar y, a continuación, selecciona **Manage**.
4. En la vista general del sistema de archivos, selecciona la pestaña **Volúmenes**.
5. En la pestaña Volúmenes, selecciona el menú de acciones del volumen para el que quieres gestionar los puntos de acceso S3, luego selecciona **Acciones avanzadas** y después **Gestionar puntos de acceso S3**.
6. Desde la pantalla **Manage S3 access points**, selecciona el menú de acciones y luego selecciona **Edit access point**.
7. En el cuadro de diálogo **Editar punto de acceso S3**, asegúrate de que la configuración de red está establecida en **Internet**.
8. Sigue las instrucciones en el cuadro de diálogo para configurar la infraestructura de la función de tabla de diario.
9. Descarga la plantilla CloudFormation.
10. Implementa la pila CloudFormation en tu cuenta de AWS.
 - a. Guarda el JSON de la plantilla en un archivo.

- b. Implementa la plantilla usando la CLI de AWS o la consola de gestión de AWS.
 - c. Espera a que la pila alcance el estado `CREATE_COMPLETE`.
 - d. Obtén el ARN de CloudTrail en las salidas de la pila.
11. Vuelve a la consola Workload Factory y al volumen para el que quieres gestionar los puntos de acceso S3.
 12. Selecciona **Ver detalles** en el menú de acciones de volumen.
 13. En la pestaña **Tabla de registro en diario**, introduce el ARN de CloudTrail.
 14. Selecciona **Aplicar**.

Si alguno de los pasos falla, [solucionar problemas de configuración de la infraestructura para la tabla de registro](#) o contacta al soporte de NetApp para obtener ayuda.

Soluciona problemas de la configuración de la infraestructura para la tabla de registro en diario

Puedes usar la consola de administración de AWS o la CLI de AWS para solucionar fallos durante la implementación de la pila CloudFormation y los recursos que crea.

Después de resolver el problema, envía de nuevo el ARN de CloudTrail para reiniciar la configuración de la tabla journal.

Fallos habituales en la implementación de CloudFormation

Permisos IAM insuficientes

El rol/usuario que realiza el despliegue necesita un conjunto específico de permisos. Consulta [Antes de empezar](#) para ver la política completa.

Si la pila falla con un error `AccessDenied` o `InsufficientPermission`, revisa los eventos de la pila y busca el permiso que falta en el campo `ResourceStatusReason`.

CloudTrail límite

AWS aplica un límite predeterminado de 5 trails por región. Si la cuenta ya tiene 5 trails, the `FsxDataEventTrail` el recurso fallará con: `Maximum number of trails (5) exceeded`. Puedes comprobar el número de trails a nivel regional con el siguiente comando:

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

Opciones de resolución

- Opción 1: elimina un trail no utilizado en la región para hacer espacio.
- Opción 2: Usa una ruta existente. Elimina los recursos `FsxDataEventTrail`, `CloudTrailBucket`, `CloudTrailBucketPolicy` y `CloudTrailToCloudWatchRole` de la plantilla antes de desplegar de nuevo la pila de CloudFormation. Luego pasa el ARN de tu ruta existente durante el paso de iniciación. La ruta existente debe tener un grupo de registros CloudWatch configurado, una `S3TableIntegration` asociada con el grupo de registros y estar registrando eventos de datos.

La integración de la tabla S3 ya existe

Si la cuenta ya tiene una `S3TableIntegration` para el origen de datos `aws_cloudtrail`, el recurso `LogsToS3TableIntegration` fallará.

Resolución

Elimina los recursos `LogsToS3TableIntegration` y `S3TableIntegrationRole` de la plantilla antes de desplegar la pila `CloudFormation` de nuevo. El sistema utiliza automáticamente la integración existente siempre que la configures para eventos de datos `aws_cloudtrail`.

Para comprobar si existe una integración:

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

El nombre del bucket S3 ya existe

El nombre del cubo `netapp-metadata-cloudtrail-events-logs-{uuid}` es único a nivel mundial. Si colisiona, vuelve a solicitar la plantilla para obtener un nuevo UUID.

La función IAM ya existe

Si un despliegue parcial anterior dejó roles IAM con el patrón de nombres `netapp-metadata-*`, la pila fallará al crear el rol. Elimina primero los roles huérfanos:

```
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>
```

Fallos tras la habilitación de la tabla Journal

Después de enviar el ARN de `CloudTrail`, `Workload Factory` valida toda la canalización de recursos enviando un `seed`, o evento de prueba, automáticamente. Si tiene éxito, el evento `seed` llega a la tabla `S3 Tables`. La prueba dura aproximadamente 10 minutos.

Si falla la validación de la prueba, es posible que recibas uno de los siguientes mensajes de error:

Mensaje de error	Significado
La tabla <code>aws_cloudtrail__data</code> no fue creada en {bucket}. Verifica los permisos de <code>s3table</code> .	<code>S3TableIntegration</code> no creó la tabla gestionada por <code>CloudWatch</code> . La canalización entre <code>CloudWatch Logs</code> y <code>S3 Tables</code> está rota.
La tabla existe, pero el evento semilla del diario no aparece. Verifica los permisos de <code>CloudTrail</code> y <code>CloudWatch</code> .	La tabla existe pero el evento semilla específico nunca llegó. El pipeline está roto entre <code>CloudTrail</code> y la tabla <code>S3 Tables</code> .
Error al iniciar la configuración del journal. ...	Se ha producido un error durante el flujo de siembra/colecta en segundo plano. Revisa el mensaje final para más detalles.

Pasos de resolución

Cuando el diario llega a FAILED, rastrea el evento semilla hacia adelante a través de las etapas de la canalización para identificar exactamente dónde se detuvo. Cada paso se asigna a un recurso de AWS específico creado por la plantilla.

1. Revisa el CloudTrail S3 Bucket.

El rastro escribe registros de eventos sin procesar en el bucket de S3 `netapp-metadata-cloudtrail-events-logs`. Busca archivos de registro recientes.

Si no existen archivos de registro, entonces CloudTrail no está capturando eventos. Revisa lo siguiente:

- El registro está en curso (`IsLogging: true`)
- Los selectores de eventos avanzados incluyen el ARN correcto del punto de acceso
- Los selectores avanzados de eventos incluyen los filtros para `eventCategory = Data` y `resources.type = AWS::S3::AccessPoint`

2. Revisa el grupo de registros de CloudWatch.

La ruta también envía eventos al grupo de registro CloudWatch. El nombre del grupo de registro empieza por `netapp-metadata-journal-data-events-<uuid>`.

- Si el grupo de registro está vacío, entonces CloudTrail no está enviando eventos a CloudWatch. Verifica que el rol IAM `CloudTrailToCloudWatchRole` exista y tenga `logs:CreateLogStream` y `logs:PutLogEvents` permisos, y que el trail esté configurado con el `CloudWatchLogsLogGroupArn` y `CloudWatchLogsRoleArn` correctos.
- Si el evento semilla aparece en el grupo de registro, entonces el problema es descendente — continúa con el paso 3.

3. Consulta la tabla S3 Tables (`aws-cloudwatch`).

La `S3TableIntegration` crea automáticamente un bucket de tabla llamado `aws-cloudwatch` y rellena una tabla en `logs.aws_cloudtrail__data`. Esta tabla solo se crea después de que fluya el primer evento.

- Si el bucket de la tabla `aws-cloudwatch` no existe, entonces a `S3TableIntegrationRole` le faltan permisos. Necesita `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` y `s3tables:PutTableBucketPolicy` — todos con alcance a `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Si el bucket de tabla existe pero `logs.aws_cloudtrail__data` no, entonces la integración no está enrutando eventos. La integración debe mostrar `Status: ACTIVE` e incluir `aws_cloudtrail` como fuente de registro.
- Si la tabla existe pero el evento semilla no está en ella, es posible que el evento aún esté en tránsito. La ingesta de tablas S3 tiene algo de latencia. Espera unos minutos más. Si aún no aparece después de 15-20 minutos, puede que la integración esté rota.

4. Consultar directamente el evento semilla.

- Abre las Tablas S3 en la consola de gestión de AWS.
- Navega hasta el bucket de tablas `aws-cloudwatch` → `aws_cloudtrail__data` table, y usa el botón **Preview** para ejecutar una consulta rápida directamente en el navegador.
- Si el suceso está presente en la tabla pero el diario sigue mostrando FAILED, es posible que la ventana de sondeo haya expirado antes de que llegara el suceso.

Una vez resuelto el problema, vuelve a la consola Workload Factory. Intenta de nuevo [iniciando la configuración de la tabla de registro en diario](#) enviando otra vez el ARN de Trail.

1. Si la configuración sigue fallando, contacta al soporte de NetApp para obtener ayuda.

Referencia de permisos para la configuración de la tabla de registro en diario

La función de IAM que despliega la pila CloudFormation para habilitar la función de tabla Journal necesita los siguientes permisos. Consulta [Antes de empezar](#) para obtener una política JSON copiable con los permisos necesarios.

Operaciones de pila

Permiso	Recurso	Por qué
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Crear la pila
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Supervisar el estado de la pila
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Diagnostica fallos a nivel de recursos cloudformation:GetTemplateSummary * Validación previa de la plantilla

CloudTrail

Permiso	Recurso	Por qué
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Crear el trail
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Activar el registro
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Aplicar etiqueta de identificación
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Configura la captura de eventos de datos
cloudtrail:DescribeTrails	*	Resolver el trail ARN para la salida del stack

S3

Permiso	Recurso	Por qué
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Crea el bucket de registros CloudTrail
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Permitir que CloudTrail escriba registros
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Aplicar etiqueta de identificación

IAM

Permiso	Recurso	Por qué
iam:CreateRole	arn:aws:iam::*:role/netapp-metadata-*	Crear ambos roles IAM
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Adjuntar políticas en línea
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Aplicar etiqueta de identificación
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Confirma que el rol está activo
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (condición: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Pasar roles a CloudTrail y CloudWatch Logs

Logs de CloudWatch

Permiso	Recurso	Por qué
logs:CreateLogGroup	arn:aws:logs::*:log-group:netapp-metadatos-*	Crear el grupo de registro
logs>DeleteLogGroup	arn:aws:logs::*:log-group:netapp-metadatos-*	Limpiar grupo de registro si falló la creación
logs:PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-metadatos-*	Establecer retención de 30 días
logs:TagResource	arn:aws:logs::*:log-group:netapp-metadatos-*	Aplicar etiqueta de identificación
logs:AsociarFuenteATablaS3Integración	arn:aws:logs::*:log-group:netapp-metadatos-*	Vincula la fuente de CloudTrail a las tablas S3
logs:DescribeLogGroups	*	Comprobar la existencia del grupo de registro
logs:ListSourcesForS3TableIntegration	*	Confirmar la asociación de integración

ObservabilityAdmin

Permiso	Recurso	Por qué
observabilityadmin:CreateS3TableIntegration	*	Crea el puente CloudWatch → Tablas S3
observabilityadmin:GetS3TableIntegration	*	Confirma que la integración está activa
observabilityadmin:TagResource	*	Aplicar etiqueta de identificación

Permiso	Recurso	Por qué
observabilityadmin:ListTagsForResource	*	Detección de deriva

Tablas S3

Permiso	Recurso	Por qué
s3tables:CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Crear el bucket S3 Tables (a través del rol de integración)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Establece el cifrado AES256
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Permitir el acceso a CloudWatch Logs

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.