Flujos de trabajo

ONTAP Automation

NetApp
October 21, 2024

Tabla de contenidos

Flujos de trabajo

Prepárese para usar los flujos de trabajo

Debe estar familiarizado con la estructura y el formato de los flujos de trabajo antes de utilizarlos con una implementación de ONTAP en directo.

Debe asegurarse de que la versión de ONTAP sea compatible con todas las llamadas API de los flujos de trabajo que planea utilizar. Consulte "Referencia de API" si quiere más información.

Introducción

Un *Workflow* es una secuencia de uno o más pasos necesarios para llevar a cabo una tarea o un objetivo administrativos específicos. Los flujos de trabajo de ONTAP incluyen los pasos y los parámetros esenciales necesarios para llevar a cabo cada tarea. Proporcionan un punto de inicio para personalizar el entorno de automatización de ONTAP.

Tipos de paso

Cada paso de un flujo de trabajo de ONTAP es uno de los siguientes tipos:

- Llamada a API REST (con detalles como ejemplos curl y JSON)
- Ejecute o llame a otro flujo de trabajo de ONTAP
- Tareas relacionadas varias (como tomar una decisión de configuración)

Llamadas a la API de REST

La mayoría de los pasos del flujo de trabajo son llamadas a la API de REST. Estos pasos utilizan un formato común que incluye un ejemplo de cURL y otra información. Consulte "Referencia de API" Para obtener más detalles sobre las llamadas a la API de REST.

Flujos de trabajo en un solo paso

Un flujo de trabajo sólo puede contener un paso. Estos *flujos de trabajo de un solo paso* tienen un formato ligeramente diferente al de los flujos de trabajo que contienen varios pasos. Por ejemplo, se elimina el nombre explícito del paso. La acción u operación debe ser clara en función del título del flujo de trabajo.

Variables de entrada

Los flujos de trabajo están diseñados para ser lo más general posible para poder utilizarlos en cualquier entorno ONTAP. Con esto en mente, las llamadas a la API REST utilizan variables en los ejemplos de curl y otras entradas. Las llamadas API DE REST se pueden adaptar fácilmente a distintos entornos de ONTAP.

Formato de URL base

Puede acceder a la API de REST DE ONTAP directamente mediante curl o un lenguaje de programación. En este caso, la URL base es diferente de la URL que utiliza al acceder a la documentación en línea de ONTAP o al Administrador del sistema.

Al acceder a la API directamente, debe agregar **api** al dominio o la dirección IP. Por ejemplo:

```
https://ontap.demo-example.com/api
```

Consulte "Cómo acceder a la API de REST de ONTAP" si quiere más información.

Parámetros de entrada comunes

Hay varios parámetros de entrada que se utilizan comúnmente con la mayoría de las llamadas a la API REST. Estos parámetros normalmente no se describen en los flujos de trabajo individuales. Debe estar familiarizado con los parámetros. Consulte "Variables de entrada que controlan una solicitud API" si quiere más información.

Si se necesitan parámetros adicionales para una llamada a la API REST específica, se incluyen en la sección **Parámetros de entrada adicionales para el ejemplo de cURL** para cada flujo de trabajo.

Formato de variable

Los valores de ID y otras variables que se utilizan con los ejemplos de flujo de trabajo son opacos y pueden variar con cada clúster de ONTAP. Para mejorar la legibilidad de los ejemplos, no se utilizan los valores reales. En su lugar, se utilizan variables. Este enfoque, basado en un formato coherente y un conjunto de nombres reservados, tiene varias ventajas, entre las que se incluyen:

- Las muestras de curl y JSON son más legibles y fáciles de entender.
- Debido a que todas las palabras clave utilizan el mismo formato, puede identificarlas rápidamente.
- No hay exposición de seguridad porque los valores no se pueden copiar ni reutilizar.

Las variables se formatean para ser utilizadas en un entorno de shell Bash. Cada variable comienza con un signo de dólar y está encerrada entre comillas dobles según sea necesario. Esto los hace reconocibles a Bash. Las mayúsculas se utilizan sistemáticamente para los nombres.

Estas son algunas de las palabras clave de variable común. Esta lista no es exhaustiva y se utilizan variables adicionales según sea necesario. Su significado debe ser obvio basado en el contexto.

Palabra clave	Tipo	Descripción
$FQDN_IP	URL	El nombre de dominio completo o la dirección IP de la LIF de gestión de ONTAP.
$CLUSTER_ID	Ruta	El valor UUIDv4 identifica el clúster de ONTAP donde se ejecutan las operaciones de API.
$BASIC_AUTH	Encabezado	Cadena de credenciales utilizada para la autenticación básica HTTP.

Ejemplos de entrada JSON

Algunas de las llamadas a la API de REST, como las que utilizan POST o PARCHE, requieren entrada JSON en el cuerpo de la solicitud. Los ejemplos de entrada JSON se presentan por separado de los ejemplos de rizo para mayor claridad. Puede utilizar los ejemplos de entrada JSON con una de las técnicas descritas a continuación.

Guardar en archivo local

Puede copiar el ejemplo de entrada JSON en un archivo y guardarlo localmente. El comando cURL hace referencia al archivo que utiliza `--data` parámetro con el valor que indica el nombre de archivo con a. `@` prefijo.

Pegue en el terminal después del ejemplo de cURL

Primero debe copiar y pegar el ejemplo de cURL en un shell de terminal. A continuación, edite el ejemplo para eliminar completamente el `--data` parámetro al final y sustitúyalo por el `--data-raw` parámetro. Por último, copie y pegue en el ejemplo JSON para que siga el comando cURL con el parámetro actualizado. Debe utilizar comillas simples para ajustar el ejemplo de entrada JSON.

Opciones de autenticación

La técnica de autenticación principal disponible para la API de REST es la autenticación básica HTTP. A partir de ONTAP 9,14, también tiene la opción de usar el marco de autorización abierta (OAuth 2,0) con autenticación y autorización basadas en tokens.

Autenticación básica HTTP

Cuando se utiliza la autenticación básica, las credenciales de usuario se deben incluir con cada solicitud HTTP. Hay dos opciones para enviar las credenciales.

Cree la cabecera de solicitud HTTP

Puede crear manualmente la cabecera Autorización e incluirla con las solicitudes HTTP. Esto se puede hacer cuando se utiliza un comando curl en la CLI o un lenguaje de programación con su código de automatización. Los pasos de alto nivel incluyen:

1. Concatenar los valores de usuario y contraseña con dos puntos:

   ```
   admin:david123
   ```

2. Convierta toda la cadena a base64:

   ```
   YWRtaW46ZGF2aWQxMjM=
   ```

3. Construya la cabecera de solicitud:

   ```
   Authorization: Basic YWRtaW46ZGF2aWQxMjM=
   ```

Los ejemplos de curl de flujo de trabajo incluyen este encabezado con la variable **$BASIC_AUTH** que debe actualizar antes de usar.

Utilice un parámetro cURL

Otra opción cuando se usa curl es quitar el encabezado de Autorización y usar el parámetro curl **user** en su lugar. Por ejemplo:

```
--user username:password
```

Debe sustituir las credenciales adecuadas para su entorno. Las credenciales no están codificadas en base64. Al ejecutar el comando curl con este parámetro, la cadena se codifica y se genera la cabecera de autorización.

OAuth 2,0

Al utilizar OAuth 2,0, es necesario solicitar un token de acceso desde un servidor de autorización externo e incluirlo con cada solicitud HTTP. Los pasos básicos de alto nivel se describen a continuación. Consulte también "Descripción general de la implementación de ONTAP OAuth 2,0" Para obtener más detalles sobre OAuth 2,0 y cómo usarlo con ONTAP.

Preparar el entorno ONTAP

Antes de usar la API de REST para acceder a ONTAP, debe preparar y configurar el entorno de ONTAP. En un nivel alto, los pasos incluyen:

- Identificar los clientes y los recursos protegidos por ONTAP
- Revise las definiciones de usuario y el rol REST DE ONTAP existentes
- Instale y configure el servidor de autorización
- Diseñar y configurar las definiciones de autorización del cliente
- Configure ONTAP y habilite OAuth 2,0

Solicitar un token de acceso

Con ONTAP y el servidor de autorización definido y activo, puede realizar una llamada a la API REST mediante un token OAuth 2,0. El primer paso es solicitar un token de acceso desde el servidor de autorización. Esto se realiza fuera de ONTAP usando una de las diversas técnicas diferentes basadas en el servidor. ONTAP no emite tokens de acceso ni realiza redirecciones.

Cree la cabecera de solicitud HTTP

Después de obtener un token de acceso, puede crear una cabecera de autorización e incluirla con las solicitudes HTTP. Independientemente de si usa curl o un lenguaje de programación para acceder a la API REST, debe incluir el encabezado con cada solicitud del cliente. Puede construir la cabecera de la siguiente manera:

```
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSld …
```

Usando los ejemplos con Bash

Si utiliza los ejemplos de cURL de flujo de trabajo directamente, debe actualizar las variables que contienen con los valores adecuados para su entorno. Puede editar manualmente los ejemplos o confiar en el shell Bash para realizar la sustitución por usted como se describe a continuación.

> Una ventaja del uso de Bash es que puede establecer los valores de variable una vez en una sesión de shell en lugar de una vez por comando cURL.

Pasos

1. Abra el shell Bash proporcionado con Linux o un sistema operativo similar.
2. Establezca los valores de variable incluidos en el ejemplo de cURL que desea ejecutar. Por ejemplo:

   ```
   CLUSTER_ID=ce559b75-4145-11ee-b51a-005056aee9fb
   ```

3. Copie el ejemplo cURL de la página de flujo de trabajo y péguelo en el terminal del shell.
4. Pulse **ENTER** que hará lo siguiente:
   a. Sustituya los valores de variable establecidos
   b. Ejecute el comando cURL

Clúster

Obtener la configuración del clúster

Puede recuperar la configuración de un clúster de ONTAP, incluidos los campos

específicos. Es posible que lo haga como parte de la evaluación del estado del clúster o antes de actualizar la configuración.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/clúster

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
campos	Consulta	No	Seleccione los valores que desea devolver. Los ejemplos incluyen `contact` y.. `version`.

Ejemplo de curl: Recupere la información de contacto del clúster

En este ejemplo se ilustra cómo recuperar un solo campo. Para obtener todo el objeto del clúster y la configuración, debe eliminar el `fields` parámetro de consulta.

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=contact" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "contact": "support@company-demo.com"
}
```

Actualice el contacto del clúster

Puede actualizar la información de contacto de un clúster de. Debido a que la solicitud se procesa de forma asíncrona, también debe determinar si el trabajo en segundo plano asociado se completó correctamente.

Paso 1: Actualice la información de contacto del clúster

Puede emitir una llamada API para actualizar la información de contacto del clúster.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PARCHE	/api/clúster

Tipo de procesamiento

Asíncrona

Ejemplo de curl

```
curl --request PATCH \
--location "https://$FQDN_IP/api/cluster" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "contact": "support@company-demo.com"
}
```

Ejemplo de resultado JSON

Se devuelve un objeto de trabajo. Debe guardar el identificador de trabajo para utilizarlo en el siguiente paso.

```
{ "job": {
    "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo "Obtener instancia de trabajo" y confirme el `state` el valor es `success`.

Paso 3: Confirme la información de contacto del clúster

Realice el flujo de trabajo "Obtener la configuración del clúster". Debe configurar la `fields` parámetro de consulta a. `contact`.

Obtener instancia de trabajo

Puede recuperar la instancia de un trabajo de ONTAP específico. Normalmente, lo haría para determinar si el trabajo y la operación asociada se han completado correctamente.

> Necesita el UUID del objeto de trabajo, que normalmente se proporciona después de emitir una solicitud asíncrona. También revise "Procesamiento asíncrono mediante el objeto Job" Antes de trabajar con trabajos internos de ONTAP.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/cluster/jobs/{uuid}

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
$JOB_ID	Ruta	Sí	Necesario para identificar el trabajo que se solicita.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster/jobs/$JOB_ID" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

El valor de estado y otros campos se incluyen en el objeto de trabajo devuelto. El trabajo de este ejemplo se ejecutó como parte de la actualización de un clúster de ONTAP.

```
{
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
  "description": "PATCH /api/cluster",
  "state": "success",
  "message": "success",
  "code": 0,
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
    }
  }
}
```

NAS

Permisos de seguridad de archivos

Prepárese para gestionar la seguridad de archivos y las políticas de auditoría

Puede gestionar los permisos y las políticas de auditoría para los archivos disponibles a través de las máquinas virtuales de almacenamiento en un clúster de ONTAP.

Descripción general

ONTAP utiliza las listas de control de acceso del sistema (SACL) y las listas de control de acceso discrecional (DACL) para asignar permisos a los objetos de archivo. A partir de ONTAP 9,9.1, la API DE REST incluye soporte para gestionar los permisos SACL y DACL. Puede utilizar la API para automatizar la administración de los permisos de seguridad de archivos. En muchos casos, puede usar una sola llamada a la API DE REST en lugar de varios comandos de la CLI o llamadas a ONTAPI (ZAPI).

> Para versiones de ONTAP anteriores a 9,9.1, puede automatizar la administración de los permisos SACL y DACL mediante la función de paso de CLI. Consulte "Consideraciones sobre migración" y.. "Utilizando el traspaso de interfaz de línea de comandos privada con la API REST de ONTAP" si quiere más información.

Hay varios ejemplos de flujos de trabajo disponibles para ilustrar cómo se gestionan los servicios de seguridad de archivos ONTAP mediante la API de REST. Antes de usar los flujos de trabajo y emitir alguna de las llamadas a la API DE REST, asegúrese de revisarlos "Prepárese para usar los flujos de trabajo".

Si usas Python, también consulta el script "file_security_permissions.py" para obtener ejemplos de cómo automatizar algunas de las actividades de seguridad de archivos.

API REST de ONTAP frente a comandos de la CLI de ONTAP

En muchas tareas, el uso de la API DE REST DE ONTAP requiere menos llamadas que los comandos equivalentes de la CLI de ONTAP o llamadas a ONTAPI (ZAPI). La siguiente tabla incluye una lista de llamadas API y el equivalente a los comandos CLI necesarios para cada tarea.

API REST de ONTAP	CLI de ONTAP
`GET /protocols/file-security/effective-permissions/`	`vserver security file-directory show-effective-permissions`
`POST /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs create` 2. `vserver security file-directory ntfs dacl add` 3. `vserver security file-directory ntfs sacl add` 4. `vserver security file-directory policy create` 5. `vserver security file-directory policy task add` 6. `vserver security file-directory apply`
`PATCH /protocols/file-security/permissions/`	`vserver security file-directory ntfs modify`
`DELETE /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs dacl remove` 2. `vserver security file-directory ntfs sacl remove`

Información relacionada

- "Script de Python que ilustra los permisos de archivo"
- "Gestión simplificada de permisos de seguridad de archivos con API DE REST de ONTAP"
- "Utilizando el traspaso de interfaz de línea de comandos privada con la API REST de ONTAP"

Obtenga los permisos efectivos para un archivo

Puede recuperar los permisos efectivos actuales para un archivo o carpeta específicos.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/protocols/file-security/effective-permissions/{svm.uuid}/{path}

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-security/effective-
permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```

Obtener la información de auditoría de un archivo

Puede recuperar la información de auditoría de un archivo o carpeta específicos.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
        "append_data": true,
```

```
        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
      },
      "access_control": "file_directory"
    },
    {
      "user": "BUILTIN\\Users",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
        "append_data": true,
        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
      },
      "access_control": "file_directory"
    }
  ],
  "inode": 64,
```

```
  "security_style": "mixed",
  "effective_style": "ntfs",
  "dos_attributes": "10",
  "text_dos_attr": "----D---",
  "user_id": "0",
  "group_id": "0",
  "mode_bits": 777,
  "text_mode_bits": "rwxrwxrwx"
}
```

Aplicar nuevos permisos a un archivo

Puede aplicar un nuevo descriptor de seguridad a un archivo o carpeta específicos.

Paso 1: Aplique los nuevos permisos

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"acls\": [ { \"access\": \"access_allow\", \"advanced_rights\": {
\"append_data\": true, \"delete\": true, \"delete_child\": true,
\"execute_file\": true, \"full_control\": true, \"read_attr\": true,
\"read_data\": true, \"read_ea\": true, \"read_perm\": true,
\"write_attr\": true, \"write_data\": true, \"write_ea\": true,
\"write_owner\": true, \"write_perm\": true }, \"apply_to\": { \"files\":
true, \"sub_folders\": true, \"this_folder\": true }, \"user\":
\"administrator\" } ], \"control_flags\": \"32788\", \"group\": \"S-1-5-
21-2233347455-2266964949-1780268902-69700\", \"ignore_paths\": [
\"/parent/child2\" ], \"owner\": \"S-1-5-21-2233347455-2266964949-
1780268902-69304\", \"propagation_mode\": \"propagate\"}'
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo "Obtener instancia de trabajo" y confirme el `state` el valor es `success`.

Actualice la información del descriptor de seguridad

Puede actualizar un descriptor de seguridad específico a un archivo o carpeta específicos, incluidos los indicadores de propietario, grupo o control principal.

Paso 1: Actualice el descriptor de seguridad

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PARCHE	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"control_flags\": \"32788\", \"group\": \"everyone\", \"owner\":
\"user1\"}'
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo "Obtener instancia de trabajo" y confirme el `state` el valor es `success`.

Eliminar una entrada de control de acceso

Puede eliminar una entrada de control de acceso (ACE) existente de un archivo o carpeta específicos. El cambio se propaga a cualquier objeto secundario.

Paso 1: Eliminar el ACE

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
ELIMINAR	/api/protocols/file-security/permissions/{svm.uuid}/{path}

Tipo de procesamiento

Asíncrona

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene el archivo.
RUTA_FILE	Ruta	Sí	Esta es la ruta al archivo o carpeta.

Ejemplo de curl

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"access\": \"access_allow\", \"apply_to\": { \"files\": true,
\"sub_folders\": true, \"this_folder\": true }, \"ignore_paths\": [
\"/parent/child2\" ], \"propagation_mode\": \"propagate\"}'
```

Ejemplo de resultado JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Paso 2: Recuperar el estado del trabajo

Realice el flujo de trabajo "Obtener instancia de trabajo" y confirme el `state` el valor es `success`.

Redes

Enumere las interfaces IP

Puede recuperar las LIF IP asignadas al clúster y las SVM. Puede hacer esto para confirmar la configuración de red o cuando se piensa añadir otra LIF.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/network/ip/interfaces

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
campos	Consulta	No	Devuelve una lista limitada de los valores de configuración relevantes.

Ejemplo de curl: Devuelve todas las LIF con los valores de configuración predeterminados

```
curl --request GET \
--location "https://$FQDN_IP/api/network/ip/interfaces" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de curl: Devuelve todas las LIF con cuatro valores de configuración específicos

```
curl --request GET \
--location
"https://$FQDN_IP/api/network/ip/interfaces?fields=name,scope,svm.name,ip.
address" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "uuid": "5ded9e38-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_mgmt1",
      "ip": {
        "address": "172.29.151.116"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/5ded9e38-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "bb03c162-999e-11ee-acad-005056ae6bd8",
      "name": "cluster_mgmt",
      "ip": {
        "address": "172.29.186.156"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/bb03c162-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c5ffbd03-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data1",
      "ip": {
        "address": "172.29.186.150"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c5ffbd03-999e-11ee-acad-
005056ae6bd8"
```

```
        }
      }
    },
    {
      "uuid": "c6612abe-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data2",
      "ip": {
        "address": "172.29.186.151"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c6612abe-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c6b21b94-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data3",
      "ip": {
        "address": "172.29.186.152"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c6b21b94-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c7025322-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data4",
      "ip": {
        "address": "172.29.186.153"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
```

```
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c7025322-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c752cc66-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data5",
      "ip": {
        "address": "172.29.186.154"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c752cc66-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c7a03719-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data6",
      "ip": {
        "address": "172.29.186.155"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c7a03719-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "ccd4c59c-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data4_inet6",
      "ip": {
```

```
        "address": "fd20:8b1e:b255:300f::ac5"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/ccd4c59c-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d9144c30-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data6_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac7"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9144c30-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d961c13b-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac2"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d961c13b-999e-11ee-acad-
005056ae6bd8"
        }
      }
```

```
    },
    {
      "uuid": "d9ac8d6a-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data5_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac6"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9ac8d6a-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d9fce1a3-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data2_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac3"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9fce1a3-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "da4995a0-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data3_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac4"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
```

```
        "self": {
          "href": "/api/network/ip/interfaces/da4995a0-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "da9e7afd-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_cluster_mgmt_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac8"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/da9e7afd-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "e6db58b4-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_mgmt1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:3008::1a0"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/e6db58b4-999e-11ee-acad-
005056ae6bd8"
        }
      }
    }
  ],
  "num_records": 16,
  "_links": {
    "self": {
      "href":
"/api/network/ip/interfaces?fields=name,scope,svm.name,ip.address"
    }
  }
}
```

Seguridad

Cuentas

Enumere las cuentas

Puede recuperar una lista de las cuentas. Puede hacer esto para evaluar su entorno de seguridad o antes de crear una nueva cuenta.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/cuentas

Tipo de procesamiento

Síncrona

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "owner": {
        "uuid": "642573a8-9d14-11ee-9330-005056aed3de",
        "name": "vs0",
        "_links": {
          "self": {
            "href": "/api/svm/svms/642573a8-9d14-11ee-9330-
005056aed3de"
          }
        }
      },
      "name": "vsadmin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/642573a8-9d14-11ee-9330-
005056aed3de/vsadmin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "admin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
005056aed3de/admin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "autosupport",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
005056aed3de/autosupport"
```

```
          }
        }
      }
    ],
    "num_records": 3,
    "_links": {
      "self": {
        "href": "/api/security/accounts"
      }
    }
  }
```

Certificados y claves

Enumere los certificados instalados

Es posible enumerar los certificados instalados en el clúster de ONTAP. Puede hacer esto para ver si hay un certificado en particular disponible o para obtener el ID de un certificado específico.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/certificados

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
max_records	Consulta	No	Especifique el Núm. De registros que desea devolver.

Ejemplo de curl: Devuelve tres certificados

```
curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "uuid": "dad822c2-573c-11ee-a310-005056aecc29",
      "name": "vs0_17866DB5C933E2EA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad822c2-573c-11ee-a310-
005056aecc29"
        }
      }
    },
    {
      "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",
      "name": "BuypassClass3RootCA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-
005056aecc29"
        }
      }
    },
    {
      "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",
      "name": "EntrustRootCertificationAuthority",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-
005056aecc29"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/certificates?max_records=3"
    },
    "next": {
      "href": "/api/security/certificates?start.svm_id=sti214nscluster-
1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"
    }
  }
}
```

Instalar un certificado

Puede instalar un certificado X,509 firmado en el clúster de ONTAP. Puede hacerlo como parte de la configuración de una característica o un protocolo ONTAP que requiera una autenticación fuerte.

Antes de empezar

Debe tener el certificado que desea instalar. También debe asegurarse de que todos los certificados intermedios estén instalados según sea necesario.

> Antes de usar los ejemplos de entrada JSON que se incluyen a continuación, asegúrese de actualizar el `public_certificate` valor con el certificado para su entorno.

Paso 1: Instale el certificado

Puede emitir una llamada API para instalar el certificado.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/certificados

Ejemplo de curl: Instale un certificado de CA raíz en el nivel de clúster

```
curl --request POST \
--location "https://$FQDN_IP/api/security/certificates" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON


```
{
    "type": "server_ca",
    "public_certificate":
    "-----BEGIN CERTIFICATE-----
MIID0TCCArkCFGYdznvTVvaY1VZPNfy4yCCyPph6MA0GCSqGSIb3DQEBCwUAMIGk
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEWMBQGA1UE
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwwT
Ki5vbnRhcC1leGFtcGxlLmNvbTEvMC0GCSqGSIb3DQEJARYgZGF2aWQucGV0ZXJz
b25Ab250YXAtZXhhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjQxMDA0MTUy
OTE4WjCBpDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSVFAx
FjAUBgNVBAoMDU9OVEFQIEV4YW1wbGUxEzARBgNVBAsMCk9OVEFQIDkuMTQxHDAa
BgNVBAMMEyoub250YXAtZXhhbXBsZS5jb20xLzAtBgkqhkiG9w0BCQEWIGRhdmlk
LnBldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAxQgy8mhb1Jhkf0D/MBodpzgW0aSp2jGbWJ+Zv2G8BXkp1762
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjH/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea
tMtA/ZpQdZbQFZ5RKtdWz7dzzPYEl2x8Q1Jc8Kh7NxERNMtgupGWZZn7mfXKYr4O
N/+vgahIhDibS8YK5rf1w6bfmrik9E2D+PEab9DX/1DL5RX4tZ1H2OkyN2UxoBR6
Fq7l6n1Hi/5yR0Oi1xStN6sO7EPoGak+KSlK41q+EcIKRo0bP4mEQp8WMjJuiTkb
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQABfBqOuROmYxdfrj93OyIiRoDcoMzvo8cHGNUsuhnlBDnL2O3qhWEs97s0
mIy6zFMGnyNYa0t4i1cFsGDKP/JuljmYHjvv+2lHWnxHjTo7AOQCnXmQH5swoDbf
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUq1sbbM7w03tthBVMgo/h1
E9I2jVOZsqMFujm2CYfMs4XkZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB
WB/FE9n+P+FfJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvABc
IpYuBcuKXLwAarhDEacXttVjC+Bq
-----END CERTIFICATE-----"
}
```


Paso 2: Confirme que se ha instalado el certificado

Realice el flujo de trabajo "Enumere los certificados instalados" y confirme que el certificado está disponible.

RBAC

Prepárese para el uso de RBAC

Es posible usar la funcionalidad de control de acceso basado en roles de ONTAP de varias formas diferentes, según el entorno. En esta sección se presentan algunos escenarios comunes como flujos de trabajo. En cada caso, el enfoque se centra en un objetivo administrativo y de seguridad específico.

Antes de crear cualquier rol y asignar un rol a una cuenta de usuario de ONTAP, debe prepararse revisando los requisitos y opciones de seguridad principales que se presentan a continuación. También asegúrese de revisar los conceptos generales del flujo de trabajo en "Prepárese para usar los flujos de trabajo".

¿Qué versión de ONTAP utiliza?

La versión de ONTAP determina qué extremos DE REST y las funciones RBAC están disponibles.

Identificar los recursos y el alcance protegidos

Debe identificar los recursos o comandos que se van a proteger y el alcance (clúster o SVM).

¿Qué acceso debería tener el usuario?

Después de identificar los recursos y el ámbito, debe determinar el nivel de acceso que se concederá.

¿Cómo accederán los usuarios a ONTAP?

El usuario puede acceder a ONTAP a través de la API de REST o la interfaz de línea de comandos o ambos.

¿Es suficiente uno de los roles integrados o se necesita un rol personalizado?

Es más conveniente utilizar una función integrada existente, pero se puede crear una nueva función personalizada si es necesario.

¿Qué tipo de rol es necesario?

En función de los requisitos de seguridad y del acceso a ONTAP, debe elegir si desea crear UN rol tradicional o DE REST.

Crear roles

Limite el acceso a las operaciones de volumen de SVM

Puede definir un rol para restringir la administración de volúmenes de almacenamiento dentro de una SVM.

Acerca de este flujo de trabajo

Se crea en primer lugar un rol tradicional para permitir inicialmente el acceso a todas las funciones principales de administración de volúmenes, excepto la clonación. El rol se define con las siguientes características:

- Es capaz de realizar todas las operaciones de volumen CRUD, incluidos Get, CREATE, Modify y DELETE
- No se puede crear un clon de volumen

A continuación, puede actualizar opcionalmente el rol según sea necesario. En este flujo de trabajo, se cambia el rol en el segundo paso para que el usuario pueda crear un clon de volumen.

Paso 1: Crear el rol

Puede emitir una llamada API para crear el rol de RBAC.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      { "path": "volume create", "access": "all" },
      { "path": "volume delete", "access": "all" }
    ]
}
```

Paso 2: Actualice el rol

Puede emitir una llamada API para actualizar el rol existente.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	Este es el UUID de la SVM que contiene la definición de rol.
$ROLE_NAME	Ruta	Sí	Es el nombre del rol dentro de la SVM que se va a actualizar.

Ejemplo de curl

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "path": "volume clone",
  "access": "all"
}
```

Permita la administración de la protección de datos

Puede proporcionar a un usuario funcionalidades de protección de datos limitadas.

Acerca de este flujo de trabajo

El rol tradicional creado se define con las siguientes características:

- Es posible crear y eliminar copias Snapshot, así como actualizar las relaciones de SnapMirror
- No se pueden crear ni modificar objetos de nivel superior como volúmenes o SVM

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "volume snapshot create", "access": "all"},
      {"path": "volume snapshot delete", "access": "all"},
      {"path": "volume show", "access": "readonly"},
      {"path": "vserver show", "access": "readonly"},
      {"path": "snapmirror show", "access": "readonly"},
      {"path": "snapmirror update", "access": "all"}
  ]
}
```

Permitir la generación de informes de ONTAP

Puede crear un rol DE REST para proporcionar a los usuarios la capacidad de generar informes de ONTAP.

Acerca de este flujo de trabajo

El rol creado se define con las siguientes características:

- Se puede recuperar toda la información sobre objetos de almacenamiento relacionada con la capacidad y el rendimiento (como volumen, qtree, LUN, agregados, nodo, Y las relaciones de SnapMirror)
- No se pueden crear ni modificar objetos de nivel superior (como volúmenes o SVM).

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api/storage/volumes", "access": "readonly"},
      {"path": "/api/storage/qtrees", "access": "readonly"},
      {"path": "/api/storage/luns", "access": "readonly"},
      {"path": "/api/storage/aggregates", "access": "readonly"},
      {"path": "/api/cluster/nodes", "access": "readonly"},
      {"path": "/api/snapmirror/relationships", "access": "readonly"},
      {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

Crear un usuario con un rol

Es posible utilizar este flujo de trabajo para crear un usuario con un rol DE REST asociado.

Acerca de este flujo de trabajo

Este flujo de trabajo incluye los pasos típicos necesarios para crear un rol REST personalizado y asociarlo con una nueva cuenta de usuario. Tanto el usuario como el rol tienen un ámbito de SVM y están asociados con una SVM de datos específica. Es posible que algunos de los pasos sean opcionales o que deban cambiar según tu entorno.

Paso 1: Enumere las SVM de datos en el clúster

Realice la siguiente llamada de API REST para enumerar las SVM en el clúster. El UUID y el nombre de cada SVM se proporcionan en la salida.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/svm/svm

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Después de terminar

Seleccione la SVM deseada en la lista donde va a crear el usuario y el rol nuevos.

Paso 2: Enumere los usuarios definidos para la SVM

Realice la siguiente llamada de API de REST para enumerar los usuarios definidos en la SVM seleccionada. Se puede identificar la SVM mediante el parámetro owner.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/cuentas

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Después de terminar

Según los usuarios ya definidos en la SVM, elija un nombre único para el nuevo usuario.

Paso 3: Enumera los roles REST definidos para la SVM

Realice la siguiente llamada de API de REST para enumerar los roles definidos en la SVM seleccionada. Se puede identificar la SVM mediante el parámetro owner.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/seguridad/roles

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Después de terminar

Según los roles ya definidos en la SVM, elija un nombre único para el nuevo rol.

Paso 4: Crear un rol REST personalizado

Realice la siguiente llamada de API DE REST para crear un rol de REST personalizado en la SVM. El rol tiene inicialmente sólo un privilegio que establece un acceso por defecto de **ninguno** para que se deniegue todo acceso.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api", "access": "none"},
  ]
}
```

Después de terminar

De manera opcional, vuelva a ejecutar el paso 3 para mostrar el nuevo rol. También puede mostrar los roles en la interfaz de línea de comandos de ONTAP.

Paso 5: Actualice el rol agregando más privilegios

Realice la siguiente llamada a la API de REST para modificar el rol, añadiendo privilegios según sea necesario.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/roles/{owner.uuid}/{name}/privilegios

Parámetros de entrada adicionales para ejemplos de cURL

Además de los parámetros comunes con todas las llamadas a la API REST, los siguientes parámetros también se utilizan en el ejemplo curl de este paso.

Parámetro	Tipo	Obligatorio	Descripción
$SVM_ID	Ruta	Sí	El UUID de la SVM que contiene la definición de rol.
$ROLE_NAME	Ruta	Sí	El nombre del rol dentro de la SVM que se va a actualizar.

Ejemplo de curl

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

Después de terminar

De manera opcional, vuelva a ejecutar el paso 3 para mostrar el nuevo rol. También puede mostrar los roles en la interfaz de línea de comandos de ONTAP.

Paso 6: Crear un usuario

Realice la siguiente llamada a la API DE REST para crear una cuenta de usuario. El rol **dprole1** creado arriba está asociado con el nuevo usuario.

> Es posible crear el usuario sin un rol. En este caso, se asigna al usuario un rol predeterminado (ya sea `admin` o. `vsadmin`) En función de si el usuario está definido con el ámbito del clúster o de SVM. Tendrás que modificar el usuario para asignar un rol diferente.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/seguridad/cuentas

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "owner": {"uuid":"daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
      {"application":"ssh",
       "authentication_methods":["password"],
       "second_authentication_method":"none"}
  ],
  "role":"dprole1",
  "password":"netapp123"
}
```

Después de terminar

Puede iniciar sesión en la interfaz de gestión de SVM con las credenciales del nuevo usuario.

Reducida

Enumere los agregados

Puede recuperar una lista de agregados en el clúster. Puede hacerlo para evaluar la

utilización y el rendimiento.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/storage/disks

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
node.name	Consulta	No	Se puede utilizar para identificar el nodo al que está conectado cada agregado.

Ejemplo de curl: Devuelve todos los agregados con los valores de configuración predeterminados

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/aggregates" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de curl: Devuelve todos los agregados con un valor de configuración específico

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/aggregates?fields=node.name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "uuid": "760d8137-fc59-47da-906a-cc28db0a1c1b",
      "name": "sti214_vsim_sr027o_aggr1",
      "node": {
        "name": "sti214-vsim-sr027o"
      },
      "_links": {
        "self": {
          "href": "/api/storage/aggregates/760d8137-fc59-47da-906a-
cc28db0a1c1b"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/storage/aggregates?fields=node.name"
    }
  }
}
```


Enumere los discos

Puede recuperar una lista de discos en el clúster. Puede hacerlo para localizar uno o varios repuestos para usar como parte de la creación de un agregado.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/storage/disks

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
estado	Consulta	No	Se puede usar para identificar los discos de repuesto disponibles para nuevos agregados.

Ejemplo de Curl: Devuelve todos los discos

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de curl: Devolver discos de repuesto

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks?state=spare" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "name": "NET-1.20",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.20"
        }
      }
    },
    {
      "name": "NET-1.12",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.12"
        }
      }
    },
    {
      "name": "NET-1.7",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.7"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/storage/disks?state=spare"
    }
  }
}
```


Soporte técnico

SAL

Prepararse para gestionar los servicios de soporte EMS

Es posible configurar el procesamiento de Event Management System (EMS) para un clúster de ONTAP y recuperar mensajes de EMS según sea necesario.

Descripción general

Existen varios flujos de trabajo de ejemplo disponibles que muestran cómo usar los servicios de EMS de ONTAP. Antes de usar los flujos de trabajo y emitir alguna de las llamadas a la API DE REST, asegúrese de revisarlos "Prepárese para usar los flujos de trabajo".

Si usas Python, también puedes ver el scripy "events.py" Para obtener ejemplos de cómo automatizar algunas de las actividades relacionadas con EMS.

API REST de ONTAP frente a comandos de la CLI de ONTAP

En muchas tareas, si se utiliza la API DE REST DE ONTAP se requieren menos llamadas que los comandos de la CLI de ONTAP equivalentes. La siguiente tabla incluye una lista de llamadas API y el equivalente a los comandos CLI necesarios para cada tarea.

API REST de ONTAP	CLI de ONTAP
OBTENGA /support/ems	`event config show`
POST /support/ems/destinations	1. `event notification destination create` 2. `event notification create`
`GET /support/ems/events`	`event log show`
`POST /support/ems/filters`	1. `event filter create -filter-name <filtername>` 2. `event filter rule add -filter-name <filtername>`

Información relacionada

- "Script de Python que ilustra EMS"
- "API DE REST de ONTAP: Automatice la notificación de eventos de alta gravedad"

Enumere los eventos del registro de EMS

Puede recuperar todos los mensajes de notificación de eventos o sólo aquellos con características específicas.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/support/ems/events

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
campos	Consulta	No	Se utiliza para solicitar que se incluyan campos específicos en la respuesta.
max_records	Consulta	No	Se puede utilizar para limitar el número de registros devueltos en una sola solicitud.
mensaje_log	Consulta	No	Se utiliza para buscar un valor de texto específico y devolver sólo los mensajes coincidentes.
message.severity	Consulta	No	Limite los mensajes devueltos a aquellos con una gravedad específica como `alert`.

Ejemplo de Curl: Devuelve el último mensaje y el valor del nombre

```
curl --request GET \
--location
"https://$FQDN_IP/api/support/ems/events?fields=message.name&max_records=1
" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de Curl: Devuelve un mensaje que contiene texto y gravedad específicos

```
curl --request GET \
--location
"https://$FQDN_IP/api/support/ems/events?log_message=*disk*&message.severi
ty=alert" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "node": {
        "name": "malha-vsim1",
        "uuid": "da4f9e62-9de3-11ec-976a-005056b369de",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/da4f9e62-9de3-11ec-976a-
005056b369de"
          }
        }
      },
      "index": 4602,
      "time": "2022-03-18T06:37:46-04:00",
      "message": {
        "severity": "alert",
        "name": "raid.autoPart.disabled"
      },
      "log_message": "raid.autoPart.disabled: Disk auto-partitioning is
disabled on this system: the system needs a minimum of 4 usable internal
hard disks.",
      "_links": {
        "self": {
          "href": "/api/support/ems/events/malha-vsim1/4602"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href":
"/api/support/ems/events?log_message=*disk*&message.severity=alert&max_rec
ords=1"
    },
    "next": {
      "href": "/api/support/ems/events?start.keytime=2022-03-
18T06%3A37%3A46-04%3A00&start.node.name=malha-
vsim1&start.index=4602&log_message=*disk*&message.severity=alert"
    }
  }
}
```

Obtenga la configuración de EMS

Puede recuperar la configuración actual de EMS para un clúster de ONTAP. Puede hacer esto antes de actualizar la configuración o crear una nueva notificación de EMS.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/support/ems

Tipo de procesamiento

Síncrona

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/support/ems" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON

```
{
  "proxy_url": "https://proxyserver.mycompany.com",
  "proxy_user": "proxy_user",
  "mail_server": "mail@mycompany.com",
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "pubsub_enabled": "1",
  "mail_from": "administrator@mycompany.com"
}
```

Cree una notificación EMS

Puede utilizar el siguiente flujo de trabajo para crear un nuevo destino de notificación de EMS para recibir los mensajes de eventos seleccionados.

Paso 1: Configure la configuración del correo electrónico en todo el sistema

Puede emitir la siguiente llamada API para configurar los ajustes del correo electrónico para todo el sistema.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PARCHE	/api/support/ems

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
mail_de	Consulta	Sí	Establece el `from` en los mensajes de correo electrónico de notificación.
servidor_correo	Consulta	Sí	Configura el servidor de correo SMTP de destino.

Ejemplo de curl

```
curl --request PATCH \
--location
"https://$FQDN_IP/api/support/ems?mail_from=administrator@mycompany.com&ma
il_server=mail@mycompany.com" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Paso 2: Defina un filtro de mensajes

Puede emitir una llamada API para definir una regla de filtro que coincida con los mensajes.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/support/ems/filters

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
Filtro	Cuerpo	Sí	Incluye los valores para la configuración del filtro.

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/filters" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "test-filter",
  "rules.type": ["include"],
  "rules.message_criteria.severities": ["emergency"]
}
```

Paso 3: Crear un destino de mensaje

Puede emitir una llamada API para crear un destino de mensaje.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/api/support/ems/destinations

Tipo de procesamiento

Síncrona

Parámetros de entrada adicionales para los ejemplos de Curl

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
Configuración de destino	Cuerpo	Sí	Incluye los valores del destino del evento.

Ejemplo de curl

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/destinations" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Ejemplo de entrada JSON

```
{
  "name": "test-destination",
  "type": "email",
  "destination": "administrator@mycompany.com",
  "filters.name": ["important-events"]
}
```

SVM

Enumere las SVM

Puede mostrar las máquinas virtuales de almacenamiento (SVM) definidas en un clúster de ONTAP. Puede hacerlo como parte de la búsqueda del identificador de una SVM específica o para garantizar la singularidad de los nombres antes de crear una nueva SVM.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/api/svm/svm

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "uuid": "71bd74f8-40dc-11ee-b51a-005056aee9fa",
      "name": "vs0",
      "_links": {
          "self": {
            "href": "/api/svm/svms/71bd74f8-40dc-11ee-b51a-005056aee9fa"
          }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/svm/svms"
    }
  }
}
```