Crear o modificar sentencias de directiva de acceso

ONTAP 9

NetApp
September 12, 2024

Tabla de contenidos

Crear o modificar sentencias de directiva de acceso

Acerca de las políticas de servidor de almacenamiento de objetos y bloques

El acceso de usuario y grupo a recursos S3 está controlado por las políticas de servidores de almacén de objetos y bloques. Si tiene un pequeño número de usuarios o grupos, es probable que sea suficiente controlar el acceso a nivel de bloque, pero si tiene muchos usuarios y grupos, es más fácil controlar el acceso a nivel de servidor del almacén de objetos.

Modificar una política de bloques

Puede agregar reglas de acceso a la política de bloque predeterminada. El ámbito de su control de acceso es el cucharón que contiene, por lo que resulta más adecuado cuando hay un único cucharón.

Antes de empezar

Debe existir una máquina virtual de almacenamiento habilitada para S3 que contenga un servidor S3 y un bloque.

Debe haber creado usuarios o grupos antes de conceder permisos.

Acerca de esta tarea

Puede agregar nuevas sentencias para usuarios y grupos nuevos o modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server bucket policy` páginas de manual.

Los permisos de usuario y grupo se pueden otorgar cuando se crea el bloque o cuando se necesite más adelante. También puede modificar la asignación de capacidad de los bloques y del grupo de políticas de calidad de servicio.

A partir de ONTAP 9,9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y. `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Pasos

1. Edite la cuchara: Haga clic en **almacenamiento > Cuchos**, haga clic en la cuchara deseada y, a continuación, haga clic en **Editar**. Al agregar o modificar permisos, puede especificar los siguientes parámetros:
   - **Principal**: El usuario o grupo al que se concede acceso.
   - **Efecto**: Permite o deniega el acceso a un usuario o grupo.
   - **Acciones**: Acciones permitidas en el cucharón para un usuario o grupo determinado.
   - **Recursos**: Rutas y nombres de objetos dentro del bloque para los cuales se concede o deniega el acceso.

     Los valores predeterminados ***bucketname*** y ***bucketname/**** conceden acceso a todos los objetos del bloque. También puede otorgar acceso a objetos individuales; por ejemplo, ***bucketname/*_readme.txt**.
   - **Condiciones** (opcional): Expresiones que se evalúan cuando se intenta acceder. Por ejemplo, puede especificar una lista de direcciones IP para las que se permitirá o deniega el acceso.

> A partir de ONTAP 9.14.1, puede especificar variables para la política de depósitos en el campo **Recursos**. Estas variables son marcadores de posición que se reemplazan por valores contextuales cuando se evalúa la política. Por ejemplo, If `${aws:username}` se especifica como una variable para una política, a continuación, esta variable se sustituye por el nombre de usuario del contexto de solicitud y la acción de política se puede realizar como se ha configurado para ese usuario.

CLI

Pasos

1. Agregar una sentencia a una política de bloque:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Los siguientes parámetros definen los permisos de acceso:

`-effect`	La declaración puede permitir o denegar el acceso
`-action`	Puede especificar `*` para indicar todas las acciones, o una lista de una o varias de las siguientes: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` y.. `ListMultipartUploadParts`.

`-principal`	Una lista de uno o más grupos o usuarios de S3. • Se puede especificar un máximo de 10 usuarios o grupos. • Si se especifica un grupo de S3, debe estar en el formulario `group/group_name`. • `*` se puede especificar que significa acceso público; es decir, acceso sin clave de acceso y clave secreta. • Si no se especifica ningún principal, se concede acceso a todos los usuarios S3 de la máquina virtual de almacenamiento.
`-resource`	El bloque y cualquier objeto que contenga. Los caracteres comodín `*` y.. `?` se puede utilizar para formar una expresión regular para especificar un recurso. En el caso de un recurso, puede especificar variables en una política. Estas son variables de política que son marcadores de posición que se reemplazan por los valores contextuales cuando se evalúa la política.

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

Ejemplos

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento svm1.example.com y bucket1 que especifica el acceso permitido a una carpeta Léame para el usuario de servidor de almacén de objetos user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento svm1.example.com y bucket1 que especifica el acceso permitido a todos los objetos para el grupo de servidores de almacén de objetos group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir de ONTAP 9.14.1, puede especificar variables para una política de bloque. En el siguiente ejemplo se crea una sentencia de política de bloque de servidor para la máquina virtual de almacenamiento `svm1` y.. `bucket1`, y especifica `${aws:username}` como variable para un recurso de política. Cuando se evalúa la política, la variable de política se sustituye por el nombre de usuario de contexto de solicitud y la acción de política se puede realizar según se haya configurado para ese usuario. Por ejemplo, cuando se evalúa la siguiente sentencia de política, `${aws:username}` Se sustituye por el usuario que realiza la operación S3. Si es un usuario `user1` realiza la operación a la que

el usuario tiene acceso `bucket1` como `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Cree o modifique una política de servidor de almacenes de objetos

Puede crear políticas que se puedan aplicar a uno o varios bloques de un almacén de objetos. Las políticas de servidores de almacenamiento de objetos pueden conectarse a grupos de usuarios, lo cual simplifica la gestión del acceso a los recursos en varios bloques.

Antes de empezar

Debe haber una SVM habilitada para S3 que contenga un servidor S3 y un bloque.

Acerca de esta tarea

Puede habilitar las políticas de acceso en el nivel de SVM especificando una política predeterminada o personalizada en un grupo de servidores de almacenamiento de objetos. Las directivas no surten efecto hasta que se especifiquen en la definición del grupo.

> Cuando se utilizan directivas de servidor de almacenamiento de objetos, se especifican los principales (es decir, los usuarios y los grupos) en la definición de grupo, no en la propia directiva.

Hay tres políticas predeterminadas de solo lectura para el acceso a los recursos de ONTAP S3:

- Acceso completo
- NoS3Access
- ReadOnlyAccess

También puede crear nuevas directivas personalizadas y, a continuación, agregar nuevas sentencias para nuevos usuarios y grupos, o puede modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server policy` "referencia de comandos".

A partir de ONTAP 9,9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y. `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Edite la VM de almacenamiento: Haga clic en **Almacenamiento > VM de almacenamiento**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en S3.
2. Agregar un usuario: Haga clic en **Directivas** y, a continuación, haga clic en **Agregar**.
   a. Introduzca un nombre de política y selecciónelo de una lista de grupos.
   b. Seleccione una política predeterminada existente o agregue una nueva.

      Al agregar o modificar una política de grupo, se pueden especificar los siguientes parámetros:

      - Grupo: Los grupos a los que se concede acceso.
      - Efecto: Permite o deniega el acceso a uno o varios grupos.
      - Acciones: Acciones permitidas en uno o más cucharones para un grupo determinado.
      - Recursos: Rutas y nombres de objetos dentro de uno o más segmentos para los que se concede o deniega el acceso. Por ejemplo:
        - ***** Concede acceso a todos los bloques del equipo virtual de almacenamiento.
        - **bucketname** y **bucketname/*** conceden acceso a todos los objetos de un bloque específico.
        - **bucketname/readme.txt** otorga acceso a un objeto en un bloque específico.
   c. Si lo desea, agregue sentencias a las directivas existentes.

CLI

Utilice la CLI para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Cree una política de servidor de almacenamiento de objetos:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Crear una instrucción para la directiva:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Los siguientes parámetros definen los permisos de acceso:

`-effect`	La declaración puede permitir o denegar el acceso

`-action`	Puede especificar `*` para indicar todas las acciones, o una lista de una o varias de las siguientes: `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, y.. `ListMultipartUploadParts`.
`-resource`	El bloque y cualquier objeto que contenga. Los caracteres comodín `*` y.. `?` se puede utilizar para formar una expresión regular para especificar un recurso.

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

De forma predeterminada, las nuevas sentencias se agregan al final de la lista de sentencias, que se procesan en orden. Cuando agregue o modifique sentencias más tarde, tiene la opción de modificar las sentencias `-index` configuración para cambiar la orden de procesamiento.

Configure el acceso S3 para los servicios de directorio externos

A partir de ONTAP 9.14.1, los servicios para directorios externos se han integrado con el almacenamiento de objetos S3 de ONTAP. Esta integración simplifica la administración de usuarios y accesos a través de servicios de directorio externos.

Puede proporcionar grupos de usuarios que pertenecen a un servicio de directorio externo con acceso al entorno de almacenamiento de objetos de ONTAP. El protocolo ligero de acceso a directorios (LDAP) es una interfaz para la comunicación con servicios de directorio, como Active Directory, que proporcionan una base de datos y servicios para la gestión de identidades y accesos (IAM). Para proporcionar acceso, debe configurar los grupos LDAP en el entorno de ONTAP S3. Después de configurar el acceso, los miembros del grupo tienen permisos para los buckets de ONTAP S3. Para obtener más información sobre LDAP, consulte "Información general sobre cómo usar LDAP".

También puede configurar grupos de usuarios de Active Directory para el modo de enlace rápido, de modo que las credenciales de usuario se puedan validar y las aplicaciones S3 de terceros y de código abierto se puedan autenticar a través de conexiones LDAP.

Antes de empezar

Asegúrese de lo siguiente antes de configurar los grupos LDAP y habilitar el modo de enlace rápido para el acceso de grupos:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte "Cree una SVM para S3".
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte "Crear un bucket".
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte "Configure los servicios DNS".

4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte "Instale el certificado de CA raíz autofirmado en la SVM".
5. Se configura un cliente LDAP con TLS habilitado en la SVM. Consulte "Cree una configuración de cliente LDAP" y.. "Asocie la configuración del cliente LDAP con las SVM para obtener información".

Configure el acceso S3 para los servicios de directorio externos

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Cree una sentencia de política de cubo de almacén de objetos con `principal` Defina el grupo LDAP al que desea otorgar acceso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Ejemplo: En el siguiente ejemplo se crea una sentencia de política de bloque para `buck1`. La política permite el acceso al grupo LDAP `group1` al recurso (bloque y sus objetos) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique que un usuario del grupo LDAP `group1` Es capaz de realizar operaciones S3 desde el cliente S3.

Use el modo de enlace rápido LDAP para la autenticación

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Asegúrese de que un usuario LDAP que acceda al bloque de S3 tenga permisos definidos en las políticas de bloque. Para obtener más información, consulte "Modificar una política de bloques".
3. Verifique que un usuario del grupo LDAP pueda realizar las siguientes operaciones:
   a. Configure la clave de acceso en el cliente S3 en este formato:
      `"NTAPFASTBIND" + base64-encode(user-name:password)`
      Ejemplo: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), lo que resulta en `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      > Es posible que el cliente S3 solicite una clave secreta. En ausencia de una clave secreta, se puede introducir cualquier contraseña de al menos 16 caracteres.

   b. Realice operaciones S3 básicas desde el cliente S3 para el que el usuario tenga permisos.

Autenticación de recursos para Active Directory para usuarios sin UID ni GID

Si el grupo nasgroup especificado en la sentencia bucket-policy o los usuarios que forman parte del grupo nasgroup no tienen UID ni GID definidos, las consultas fallarán cuando no se encuentren estos atributos.

Para evitar errores de búsqueda, NetApp recomienda utilizar dominios de confianza para la autorización de recursos en formato UPN: Nasgroup/group@trusted_domain.com

Para generar las claves de acceso de usuario para usuarios de dominio de confianza cuando no se utiliza el enlace rápido LDAP

Utilice el `s3/services/<svm_uuid>/users` punto final con los usuarios especificados en formato UPN. Ejemplo:

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn](https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M
"}'
```

Habilite LDAP o usuarios de dominio para generar sus propias claves de acceso S3

A partir de ONTAP 9.14.1, como administrador de ONTAP, puede crear roles personalizados y concederles a grupos de dominio locales o a grupos de protocolo ligero

de acceso a directorios (LDAP), de modo que los usuarios que pertenecen a esos grupos puedan generar sus propias claves secretas y de acceso para el acceso de clientes S3.

Debe realizar algunos pasos de configuración en la máquina virtual de almacenamiento, de manera que el rol personalizado se pueda crear y asignar al usuario que llama a la API para la generación de claves de acceso.

Antes de empezar

Asegúrese de lo siguiente:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte "Cree una SVM para S3".
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte "Crear un bucket".
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte "Configure los servicios DNS".
4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte "Instale el certificado de CA raíz autofirmado en la SVM".
5. Se configura un cliente LDAP con TLS habilitado en la máquina virtual de almacenamiento. Consulte "Cree una configuración de cliente LDAP" y .
6. Asocie la configuración del cliente al Vserver. Consulte "Asocie la configuración del cliente LDAP con las SVM" y.. "creación de ldap de servicio de nombres de servicios vserver".
7. Si utiliza una máquina virtual de almacenamiento de datos, cree una interfaz de red de gestión (LIF) y en la máquina virtual, así como una política de servicio para la LIF. Consulte "se crea la interfaz de red" y.. "interfaz de red service-policy create" comandos.

Configurar usuarios para la generación de claves de acceso

1. Especifique LDAP como la base de datos del servicio *name* de la máquina virtual de almacenamiento para el grupo y la contraseña a LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Cree un rol personalizado con acceso al extremo de la API de REST DE S3 usuarios:
   `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
   En este ejemplo, la `s3-role` Se genera el rol para los usuarios en la máquina virtual de almacenamiento `svm-1`, a los que se otorgan todos los derechos de acceso, leer, crear y actualizar.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Para obtener más información acerca de este comando, consulte "creación de rest-role de conexión de seguridad" comando.

3. Cree un grupo de usuarios LDAP con el comando security login y añada el nuevo rol personalizado para acceder al punto final de la API DE REST DE usuarios de S3. Para obtener más información acerca de este comando, consulte "seguridad de inicio de sesión creado" comando.

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

En este ejemplo, el grupo LDAP `ldap-group-1` se crea en `svm-1`, y el rol personalizado `s3role` Se ha añadido a él para acceder al punto final de la API, junto con la habilitación del acceso LDAP en el modo de enlace rápido.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Para obtener más información, consulte "Utilice el enlace rápido LDAP para la autenticación nsswitch".

Al agregar el rol personalizado al dominio o grupo LDAP, los usuarios de ese grupo tendrán acceso limitado a la ONTAP `/api/protocols/s3/services/{svm.uuid}/users` extremo. Al invocar la API, los usuarios del grupo de dominio o LDAP pueden generar su propio acceso y claves secretas para acceder al cliente S3. Pueden generar las claves solo para ellos mismos y no para otros usuarios.

Como usuario S3 o LDAP, genere sus propias claves de acceso

A partir de ONTAP 9.14.1, puede generar sus propias claves de acceso y secretas para acceder a clientes S3, si su administrador le ha otorgado el rol para generar sus propias claves. Puede generar claves únicamente para usted mediante el siguiente extremo de la API REST DE ONTAP.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo. Para obtener información sobre los otros métodos de este punto final, consulte la referencia "Documentación de API".

Método HTTP	Ruta
PUBLICAR	/api/protocols/s3/services/{svm.uid}/usuarios

Ejemplo de curl

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```