# Autorización de cliente

ONTAP 9

NetApp
January 08, 2026

# Tabla de contenidos

# Autorización de cliente

## Descripción general y opciones para la autorización del cliente de ONTAP

La implementación de ONTAP OAuth 2,0 está diseñada para ser flexible y robusta, proporcionando las características que necesita para proteger su entorno ONTAP. Hay varias opciones de configuración mutuamente excluyentes disponibles. Las decisiones de autorización se basan en última instancia en los roles REST DE ONTAP contenidos en o derivados de los tokens de acceso OAuth 2,0.

Sólo puede utilizarse "Roles DE REST de ONTAP" al configurar la autorización para OAuth 2,0. No se admiten los roles tradicionales de ONTAP anteriores.

ONTAP aplica la opción de autorización más adecuada en función de su configuración. Consulte "Cómo ONTAP determina el acceso" para obtener más información acerca de cómo ONTAP toma decisiones sobre el acceso de los clientes.

#### OAuth 2,0 ámbitos independientes

Estos ámbitos contienen uno o más roles REST personalizados, cada uno encapsulado dentro de una única cadena en el token de acceso. Son independientes de las definiciones de roles de ONTAP. Debe configurar las cadenas de ámbito en el servidor de autorización. Consulte "Alcances OAuth 2,0 autónomos" para obtener más información.

#### Roles DE REST DE ONTAP local

Se puede utilizar un único rol REST con nombre, ya sea Builtin o Custom. La sintaxis del ámbito para un rol con nombre es **ontap-role-**<URL-encoded-ONTAP-role-name>. Por ejemplo, si el rol ONTAP es `admin` la cadena de ámbito será `ontap-role-admin`.

#### Usuarios

Se puede utilizar el nombre de usuario en el token de acceso definido con acceso a la aplicación http. Un usuario se prueba en el siguiente orden según el método de autenticación definido: Contraseña, dominio (Active Directory), nsswitch (LDAP).

#### Grupos

Los servidores de autorización se pueden configurar para utilizar grupos ONTAP para su autorización. Si se examinan las definiciones de ONTAP locales pero no se puede tomar ninguna decisión de acceso, se utilizan los grupos de Active Directory («dominio») o LDAP («nsswitch»). La información del grupo se puede especificar de dos formas:

- Cadena de ámbito de OAuth 2,0

  Admite aplicaciones confidenciales mediante el flujo de credenciales de cliente donde no hay ningún usuario con una pertenencia a grupo. El ámbito debe denominarse **ontap-group-**<URL-encoded-ONTAP-group-name>. Por ejemplo, si el grupo está en «desarrollo», la cadena de alcance será «ontap-group-development».

- En el reclamo de “grupo”

  Esto está destinado a los tokens de acceso emitidos por ADFS mediante el flujo de propietario de recursos

(concesión de contraseña).

Ver "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" Para más información.

# Ámbitos OAuth 2.0 autónomos en ONTAP

Los ámbitos autónomos son cadenas que se llevan en el token de acceso. Cada una de ellas es una definición de función personalizada completa e incluye todo lo que ONTAP necesita para tomar una decisión de acceso. El ámbito está separado y distinto de cualquiera de los roles de REST definidos en el propio ONTAP.

## Formato de la cadena de ámbito

En un nivel base, el ámbito se representa como una cadena contigua y se compone de seis valores separados por dos puntos. Los parámetros utilizados en la cadena de ámbito se describen a continuación.

### ONTAP literal

El ámbito debe comenzar con el valor literal `ontap` en minúscula. Identifica el ámbito como específico de ONTAP.

### Clúster

Esto define al cluster de ONTAP al que se aplica el ámbito. Los valores pueden incluir:

- UUID del clúster

  Identifica un único clúster.

- Asterisco (*)

  Indica que el ámbito se aplica a todos los clusters.

Puede utilizar el comando de la CLI de ONTAP `cluster identity show` para mostrar el UUID de su clúster. Si no se especifica, el ámbito se aplica a todos los clusters. Obtenga más información sobre `cluster identity show` en el "Referencia de comandos del ONTAP".

### Función

Nombre del rol REST contenido en el ámbito autónomo. ONTAP no examina este valor ni se relaciona con ningún rol de REST existente definido con ONTAP. El nombre se utiliza para el registro.

### Nivel de acceso

Este valor indica el nivel de acceso aplicado a la aplicación cliente cuando se utiliza el punto final de API en el ámbito. Hay seis valores posibles, como se describe en la tabla siguiente.

| Nivel de acceso | Descripción |
|---|---|
| ninguno | Deniega todo el acceso al punto final especificado. |
| sólo lectura | Permite solo el acceso de lectura mediante GET. |

| Nivel de acceso | Descripción |
| --- | --- |
| read_create | Permite el acceso de lectura, así como la creación de nuevas instancias de recursos mediante POST. |
| read_modify | Permite el acceso de lectura, así como la capacidad de actualizar los recursos existentes MEDIANTE PARCHE. |
| read_create_modify | Permite todos los accesos excepto eliminar. Las operaciones permitidas incluyen GET (READ), POST (CREATE) y PARCHE (UPDATE). |
| todo | Permite un acceso completo. |

**SVM**

El nombre de la SVM dentro del clúster al que se aplica el ámbito. Utilice el valor * (asterisco) para indicar todas las SVM.

Esta función no es totalmente compatible con ONTAP 9.14.1. Puede ignorar el parámetro SVM y usar un asterisco como marcador de posición. Revise el "Notas de la versión de ONTAP" para comprobar si hay compatibilidad con SVM en el futuro.

**URI DE LA API DE REST**

Ruta de acceso completa o parcial a un recurso o juego de recursos relacionados. La cadena debe comenzar por `/api`. Si no especifica un valor, el alcance se aplica a todos los extremos de API en el clúster de ONTAP.

## Ejemplos de ámbito

A continuación se presentan algunos ejemplos de ámbitos autónomos.

**ontap:*:joes-role:read_create_modify:*:/api/cluster**

Proporciona al usuario asignado a este rol acceso de lectura, creación y modificación al `/cluster` punto final.

## Herramienta administrativa de la CLI

Para que la administración de los ámbitos autónomos sea más fácil y menos propensa a errores, ONTAP proporciona el comando CLI `security oauth2 scope` para generar cadenas de alcance basadas en los parámetros de entrada.

El comando `security oauth2 scope` tiene dos casos de uso basados en su entrada:

- Parámetros de CLI para la cadena de ámbito

  Puede utilizar esta versión del comando para generar una cadena de ámbito basada en los parámetros de entrada.

- Cadena de ámbito para parámetros de CLI

  Puede utilizar esta versión del comando para generar los parámetros del comando basados en la cadena de ámbito de entrada.

**Ejemplo**

El siguiente ejemplo genera una cadena de ámbito con la salida incluida después del siguiente ejemplo de comando. La definición se aplica a todos los clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Obtenga más información sobre `security oauth2 scope` en el "Referencia de comandos del ONTAP".

# Mapeo de roles externos de OAuth 2.0 en ONTAP

Un rol externo se define en un proveedor de identificación configurado para su uso por ONTAP. Es posible crear y administrar relaciones de asignación entre estos roles externos y los roles de ONTAP mediante la CLI de ONTAP.

También es posible configurar la función de asignación de roles externos mediante la API DE REST DE ONTAP. Obtenga más información en el "Documentación de automatización de ONTAP".

## Roles externos en un token de acceso

Aquí hay un fragmento de un token de acceso JSON que contiene dos roles externos.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

## Configuración

Puede utilizar la interfaz de línea de comandos de ONTAP para administrar la función de asignación de roles externos.

### Crear

Puede definir una configuración de asignación de roles con `security login external-role-mapping create` el comando. Debe estar en el nivel de privilegio **admin** de ONTAP para emitir este comando, así como las opciones relacionadas.

#### Parámetros

A continuación se describen los parámetros utilizados para crear una asignación de grupo.

| Parámetro | Descripción |
|---|---|
| `external-role` | Nombre del rol definido en el proveedor de identidad externo. |
| `provider` | Nombre del proveedor de identidad. Este debe ser el identificador del sistema. |
| `ontap-role` | Indica el rol de ONTAP existente al que está asignado el rol externo. |

#### Ejemplo

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Obtenga más información sobre `security login external-role-mapping create` en el "Referencia de comandos del ONTAP".

#### Operaciones de CLI adicionales

El comando admite varias operaciones adicionales, entre las que se incluyen:

- Mostrar
- Modificar
- Eliminar

#### Información relacionada

- "Referencia de comandos del ONTAP"

# Cómo determina ONTAP el acceso del cliente

Para diseñar e implementar correctamente OAuth 2,0, es necesario comprender cómo ONTAP utiliza su configuración de autorización para tomar decisiones de acceso para los clientes. Los pasos principales utilizados para determinar el acceso se presentan a continuación en función de la versión de ONTAP.

No hubo actualizaciones significativas de OAuth 2,0 con ONTAP 9.15,1. Si utiliza la versión 9.15.1, consulte la descripción de ONTAP 9.14,1.

#### Información relacionada

- "Funciones de OAuth 2,0 admitidas en ONTAP"

## ONTAP 9.16.1

ONTAP 9.16,1 amplía la compatibilidad estándar con OAuth 2,0 para incluir extensiones específicas de Microsoft Entra ID para grupos nativos de Entra ID, así como la asignación de roles externos.

**Determine el acceso de clientes para ONTAP 9.16,1**

**Paso 1: Ámbitos autónomos**

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

**Paso 2: Compruebe el indicador de roles locales**

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

**Paso 3: Se denomina rol REST ONTAP**

Si el token de acceso contiene un rol REST con nombre en el `scope` campo o `scp`, o como una reclamación, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

**Paso 4: Usuarios**

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

**Paso 5: Grupos**

Si se incluyen uno o más grupos, se examina el formato. Si los grupos se representan como UUID, se busca en una tabla interna de mapeo de grupos. Si hay una coincidencia de grupo y un rol asociado, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento finaliza. Para más información, consulte "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" .

Si los grupos se representan como nombres y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo de Active Directory o LDAP, respectivamente. Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

## ONTAP 9.14.1

OAuth 2,0 inicial admitido se introduce con ONTAP 9.14,1 basado en las características estándar de OAuth 2,0.

**Determine el acceso de clientes para ONTAP 9.14,1**

**Paso 1: Ámbitos autónomos**

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

**Paso 2: Compruebe el indicador de roles locales**

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

**Paso 3: Se denomina rol REST ONTAP**

Si el token de acceso contiene un rol REST con nombre en el `scope` campo OR `scp`, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

**Paso 4: Usuarios**

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

**Paso 5: Grupos**

Si se incluyen uno o más grupos y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo LDAP o Active Directory, respectivamente.

Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.