Seguridad RBAC

ONTAP Automation

NetApp
April 21, 2024

Tabla de contenidos

Seguridad RBAC

Información general sobre la seguridad de RBAC

ONTAP incluye una funcionalidad de control de acceso basado en roles (RBAC) robusta y ampliable. Es posible asignar cada cuenta un rol diferente para controlar el acceso del usuario a los recursos expuestos mediante la API de REST y la CLI. Los roles definen distintos niveles de acceso administrativo para los distintos usuarios de ONTAP.

> La funcionalidad de control de acceso basado en roles de ONTAP ha seguido expandiéndose y se mejoró significativamente con ONTAP 9.11.1 (y versiones posteriores). Consulte "Resumen de la evolución de RBAC" y.. "Novedades de la API DE REST de ONTAP y la automatización" si quiere más información.

Roles de ONTAP

Un rol es un conjunto de privilegios que definen colectivamente qué acciones puede realizar el usuario. Cada privilegio identifica una ruta de acceso específica y el nivel de acceso asociado. Los roles se asignan a cuentas de usuario y ONTAP los aplica cuando se toman decisiones sobre el control de acceso.

Tipos de roles

Hay dos tipos de roles. Se introdujeron y se adaptaron a diferentes entornos a medida que ONTAP ha evolucionado.

> Hay ventajas y desventajas cuando se usa cada tipo de rol. Consulte "Comparación de los tipos de funciones" si quiere más información.

Tipo	Descripción
DESCANSO	Los roles DE REST se introdujeron con ONTAP 9.6 y se aplican generalmente a los usuarios que acceden a ONTAP a través de la API DE REST. La creación de un rol REST crea automáticamente un rol tradicional *mapping*.
Tradicional	Estas son las funciones heredadas que se incluyen antes de ONTAP 9.6. Se introdujeron para el entorno de interfaz de línea de comandos de ONTAP y siguen siendo fundamentales para la seguridad de RBAC.

Ámbito

Cada función tiene un ámbito o contexto dentro del cual se define y aplica. El ámbito determina dónde y cómo se utiliza una función específica.

> Las cuentas de usuario de ONTAP también tienen un ámbito similar que determina cómo se define y se usa un usuario.

Ámbito	Descripción
Clúster	Los roles con el alcance de un clúster se definen en el nivel del clúster de ONTAP. Se asocian con cuentas de usuario de nivel de clúster.

Ámbito	Descripción
SVM	Los roles con un alcance de SVM se definen para una SVM de datos específica. Se asignan a cuentas de usuario en la misma SVM.

Origen de las definiciones de roles

Hay dos formas de definir un rol de ONTAP.

Origen de la función	Descripción
Personalizado	El administrador de ONTAP puede crear roles personalizados. Estos roles pueden adaptarse a un entorno específico y a los requisitos de seguridad.
Incorporado	Aunque los roles personalizados proporcionan más flexibilidad, también cuenta con un conjunto de roles integrados disponibles a nivel del clúster y de SVM. Estas funciones están predefinidas y se pueden utilizar para muchas tareas administrativas comunes.

Asignación de roles y procesamiento de ONTAP

Según la versión de ONTAP que utilice, todas o casi todas las llamadas de la API DE REST se asignan a uno o más comandos de la CLI. Al crear un rol DE REST, también se crea un rol tradicional o heredado. Esta función tradicional **asignada** se basa en los comandos CLI correspondientes y no se puede manipular ni modificar.

> No se admite la asignación de roles en sentido inverso. Es decir, la creación de un rol tradicional no crea el rol DE REST correspondiente.

Resumen de la evolución de RBAC

Se incluyen los roles tradicionales en todas las versiones de ONTAP 9. Las funciones RESTANTES se introdujeron más tarde y han evolucionado como se describe a continuación.

ONTAP 9.6

Se introdujo la API DE REST con ONTAP 9.6. También se incluyeron los roles REST en esta versión. Además, al crear un rol DE REST, también se crea un rol tradicional correspondiente.

ONTAP 9.7 a 9.10.1

Cada versión de ONTAP de la 9.7 a la 9.10.1 incluye mejoras en la API DE REST. Por ejemplo, se han añadido otros extremos REST con cada versión. Sin embargo, la creación y gestión de los dos tipos de funciones se mantuvieron separadas. Además, ONTAP 9.10.1 añadió compatibilidad con RBAC de REST para el extremo DE REST de snapshots `/api/storage/volumes/{vol.uuid}/snapshots` que es un extremo calificado para recursos.

ONTAP 9.11.1

Con esta versión se ha añadido la capacidad para configurar y gestionar roles tradicionales mediante la API DE REST. También se añadieron niveles de acceso adicionales para los roles DE REST.

Trabajar con roles y usuarios

Después de comprender las funcionalidades básicas de RBAC, es posible empezar a

trabajar con los roles y usuarios de ONTAP.

> Consulte "Flujos de trabajo de RBAC" Para obtener ejemplos de cómo crear y utilizar roles con la API de REST DE ONTAP.

Acceso administrativo

Es posible crear y gestionar los roles ONTAP mediante la API DE REST o la interfaz de línea de comandos. Los detalles de acceso se describen a continuación.

API REST

Existen varios extremos que se pueden usar cuando se trabajan con roles de RBAC y cuentas de usuario. Los primeros cuatro de la tabla se utilizan para crear y gestionar los roles. Las dos últimas se utilizan para crear y administrar cuentas de usuario.

> Puede acceder a la ONTAP en línea "Referencia de API" Documentación para obtener más información, incluidos ejemplos de cómo usar la API.

Extremo	Descripción
`/security/roles`	Este extremo permite crear un nuevo rol de REST. A partir de ONTAP 9.11.1, también puede crear un rol tradicional. En este caso, ONTAP determina el tipo de rol en función de los parámetros de entrada. También puede recuperar una lista de los roles definidos.
`/security/roles/{owner.UUID}/{name}`	Puede recuperar o eliminar un rol de ámbito de SVM o clúster específico. El valor de UUID identifica la SVM donde se define el rol (clúster o SVM de datos). El valor del nombre es el nombre del rol.
`/security/roles/{owner.UUID}/{name}/privileges`	Este extremo permite configurar los privilegios para un rol específico. Los roles integrados se pueden recuperar, pero no se pueden actualizar. Consulte la documentación de referencia de API para su versión de ONTAP si desea obtener más información.
`/security/roles/{owner.UUID}/{name}/privileges/[path]`	Puede recuperar, modificar y eliminar el nivel de acceso y el valor de consulta opcional de un privilegio específico. Consulte la documentación de referencia de API para su versión de ONTAP si desea obtener más información.
`/security/accounts`	Este extremo le permite crear una nueva cuenta de usuario del clúster o de la SVM. Antes de que la cuenta esté operativa, se deben incluir o agregar posteriormente varios tipos de información. También puede recuperar una lista de las cuentas de usuario definidas.
`/security/accounts/{owner.UUID}/{name}`	Puede recuperar, modificar y eliminar una cuenta de usuario específica de un clúster o de una SVM. El valor de UUID identifica la SVM donde se define el usuario (clúster o SVM de datos). El valor del nombre es el nombre de la cuenta.

Interfaz de línea de comandos

A continuación se describen los comandos de la CLI de ONTAP relevantes. A todos los comandos se accede en el nivel del clúster mediante una cuenta de administrador.

Comando	Descripción
`security login`	Este es el directorio que contiene los comandos necesarios para crear y gestionar un inicio de sesión de usuario.
`security login rest-role`	Este es el directorio que contiene los comandos necesarios para crear y gestionar un rol DE REST asociado con un inicio de sesión de usuario.
`security login role`	Este es el directorio que contiene los comandos necesarios para crear y gestionar un rol tradicional asociado con un inicio de sesión de usuario.

Definiciones de roles

El RESTO y los roles tradicionales se definen mediante un conjunto de atributos.

Propietario y ámbito

El rol puede ser propiedad del clúster de ONTAP o de una SVM de datos específica dentro del clúster. El propietario también determina implícitamente el alcance del rol.

Nombre exclusivo

Cada rol debe tener un nombre único dentro de su ámbito. El nombre de un rol de clúster debe ser único en el nivel de clúster de ONTAP, mientras que los roles de SVM deben ser únicos en la SVM específica.

> El nombre de un nuevo rol DE REST debe ser único entre los demás roles y los tradicionales. Esto se debe a que la creación de una función REST también da como resultado una nueva función tradicional *mapping* con el mismo nombre.

Conjunto de privilegios

Cada función contiene un conjunto de uno o más privilegios. Cada privilegio identifica un recurso o comando específico y el nivel de acceso asociado.

Privilegios

Un rol puede contener uno o más privilegios. Cada definición de privilegio es una tupla y establece el nivel de acceso a un recurso o una operación específica.

Ruta de recursos

La ruta de recursos se identifica como extremo DE REST o como ruta de acceso al directorio de comandos/comandos de la CLI.

Extremo de REST

Un extremo de la API identificó el recurso de destino para un rol de REST.

Comando de la CLI

Un comando de la CLI identifica el destino para un rol tradicional. También se puede especificar un directorio de comandos, que incluirá todos los comandos descendentes en la jerarquía de la CLI de ONTAP.

Nivel de acceso

El nivel de acceso define el tipo de acceso que tiene la función a la ruta de acceso o el comando de recursos específicos. Los niveles de acceso se identifican mediante un conjunto de palabras clave predefinidas. Con ONTAP 9.6 se introdujeron tres niveles de acceso. Se pueden usar para roles tradicionales y de REST.

Además, se han añadido tres nuevos niveles de acceso con ONTAP 9.11.1. Estos nuevos niveles de acceso solo se pueden usar con roles DE REST.

> Los niveles de acceso siguen el modelo CRUD. Con REST, se basa en los métodos HTTP principales (POST, GET, PATCH, DELETE). Las operaciones de la CLI correspondientes generalmente se asignan a las operaciones DE REST (crear, mostrar, modificar, eliminar).

Nivel de acceso	Primitivos DE REST	Añadido	Solo rol de REST
ninguno	n.a.	9.6	No
sólo lectura	OBTENGA	9.6	No
todo	OBTENER, PUBLICAR, APLICAR PARCHE, ELIMINAR	9.6	No
read_create	GET, POST	9.11.1	Sí
read_modify	GET, PATCH	9.11.1	Sí
read_create_modify	OBTENGA, PUBLIQUE, PARCHE	9.11.1	Sí

Consulta opcional

Al crear una función tradicional, puede incluir opcionalmente un valor **query** para identificar el subconjunto de objetos aplicables para el directorio de comandos o comandos.

Resumen de los roles incorporados

Hay varios roles predefinidos incluidos en ONTAP que se pueden usar en el nivel del clúster o de SVM.

Roles de ámbito del clúster

Hay varios roles integrados disponibles en el ámbito del clúster.

Consulte "Roles predefinidos para administradores de clúster" si quiere más información.

Función	Descripción
admin	Los administradores con esta función tienen derechos sin restricciones y pueden hacer cualquier cosa en el sistema ONTAP. Pueden configurar todos los recursos a nivel de clúster y de SVM.
AutoSupport	Se trata de un rol especial diseñado para la cuenta de AutoSupport.
Backup	Esta función especial para el software de backup que necesita hacer copia de seguridad del sistema.
SnapLock	Se trata de un rol especial diseñado para la cuenta de SnapLock.
sólo lectura	Los administradores con esta función pueden ver todos los elementos a nivel de clúster, pero no pueden realizar ningún cambio.
ninguno	No se proporcionan funcionalidades administrativas.

Roles con ámbito de SVM

Hay varios roles integrados disponibles en el ámbito de SVM. El **vsadmin** proporciona acceso a las capacidades más generales y poderosas. Existen varios roles adicionales adaptados a tareas administrativas específicas, como:

- vsadmin-volumen
- protocolo vsadmin
- vsadmin-backup
- vsadmin-snaplock
- vsadmin-readonly

Consulte "Roles predefinidos para administradores de SVM" si quiere más información.

Comparación de los tipos de funciones

Antes de seleccionar un rol **REST** o **tradicional**, debe ser consciente de las diferencias. A continuación se describen algunas de las formas en que se pueden comparar los dos tipos de funciones.

> Para casos de uso de RBAC más avanzados o complejos, normalmente debería usar un rol tradicional.

Cómo accede el usuario a ONTAP

Antes de crear un rol, es importante saber cómo accederá el usuario al sistema ONTAP. Se puede determinar en función de esto un tipo de función.

Acceso	Tipo recomendado
Solo API DE REST	El rol DE REST se ha diseñado para usarse con la API DE REST.
API REST Y CLI	Puede definir un rol DE REST que también cree un rol tradicional correspondiente.
Solo CLI	Se puede crear un rol tradicional.

Precisión de la ruta de acceso

La ruta de acceso definida para un rol DE REST se basa en un extremo de REST. La ruta de acceso de un rol tradicional se basa en un comando de la CLI o un directorio de comandos. Además, puede incluir un parámetro de consulta opcional con un rol tradicional para restringir aún más el acceso en función de los valores de parámetros del comando.