Control de acceso a base de roles (RBAC) Nexus N5500, 5600 y N6000

Contenido

Introducción

Este documento describe cómo limitar el acceso de un usuario a los switches Nexus 5500, Nexus 5600 y Nexus 6000 mediante Control de acceso a base de roles (RBAC).

RBAC le permite definir las reglas para una función de usuario asignada para restringir la autorización de un usuario que tiene acceso a las operaciones de administración del switch.

Puede crear y administrar una cuenta de usuario y asignar funciones que limiten el acceso a los switches Nexus 5500, Nexus 5600 y Nexus 6000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comandos de configuración CLI de switches Nexus 5500, Nexus 5600 y Nexus 6000
- Servicios Cisco Fabric Services (CFS).

Componentes Utilizados

La información de este documento se basa en los switches Nexus 5500, Nexus 5600 y Nexus 6000 que ejecutan NXOS 5.2(1)N1(9) 7.3(1)N1(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Requisitos del usuario

Estos son algunos de los requisitos de los usuarios que deben cumplirse:

- Sólo los usuarios con función de administrador de red pueden crear funciones.
- Sólo los usuarios con función de administrador de red pueden ver el resultado de **show role**.
- Incluso si a los usuarios se les permite realizar todos los comandos show, no se les permite ver el resultado **show role**, a menos que se les asigne una función de administrador de red.
- Una cuenta de usuario debe tener al menos una función de usuario.

Roles de usuario

Cada función se puede asignar a varios usuarios y cada usuario puede formar parte de varias funciones.

Por ejemplo, se permite a los usuarios de la función A ejecutar los comandos show y a los usuarios de la función B realizar cambios en la configuración.

Si se asigna un usuario a las funciones A y B, este usuario puede ejecutar el comando show y realizar cambios en la configuración.

El comando Permit access tiene prioridad sobre el comando deny access.

Por ejemplo, si pertenece a una función que deniega el acceso a los comandos de configuración.

Sin embargo, si también pertenece a una función que tiene acceso a los comandos de configuración, tendrá acceso a los comandos de configuración.

Existen cinco funciones de usuario predeterminadas:

- network-admin - Acceso completo de lectura y escritura al switch completo.
- network-operator - Acceso de lectura completo al switch completo.
- vdc-admin: acceso de lectura y escritura limitado a un VDC
- vdc-operator - Acceso de lectura limitado a un VDC
- san-admin: acceso completo de lectura y escritura a los administradores de SAN.

Nota: No puede modificar ni eliminar las funciones de usuario predeterminadas.

Nota: show role mostrará la función disponible en el switch

Reglas de rol de usuario

La regla es el elemento básico de una función.

Una regla define las operaciones que la función permite realizar al usuario.

Puede aplicar reglas para estos parámetros:

- Comando: comando o grupo de comandos definido en una expresión regular.
- Función: Comandos que se aplican a una función proporcionada por el software NX-OS.
- Grupo de funciones: grupo de funciones predeterminado o definido por el usuario.

Estos parámetros crean una relación jerárquica. El parámetro de control más básico es el comando.

El siguiente parámetro de control es la función, que representa todos los comandos asociados a la función.

El último parámetro de control es el grupo de características. El grupo de funciones combina funciones relacionadas y le permite administrar reglas fácilmente.

El número de regla especificado por el usuario determina el orden en que se aplican las reglas.

Las reglas se aplican en orden descendente.

Por ejemplo, la regla 1 se aplica antes de la regla 2, que se aplica antes de la regla 3, y así sucesivamente.

El comando rule especifica las operaciones que puede realizar una función específica. Cada regla consta de un número de regla, un tipo de regla (permit o deny),

un tipo de comando (por ejemplo, configuration, show, exec, debug) y un nombre de función opcional (por ejemplo, FCOE, HSRP, VTP, interface).

Distribución de funciones de usuario

Las configuraciones basadas en funciones utilizan la infraestructura de Cisco Fabric Services (CFS) para permitir una gestión eficaz de las bases de datos y proporcionar un único punto de configuración en la red.

Cuando habilita la distribución CFS para una función en su dispositivo, el dispositivo pertenece a una región CFS que contiene otros dispositivos en la red que también ha habilitado para la distribución CFS para la función. La distribución de CFS para la función de rol de usuario está desactivada de forma predeterminada.

Debe habilitar CFS para las funciones de usuario en cada dispositivo al que desee distribuir los cambios de configuración.

Después de habilitar la distribución CFS para las funciones de usuario en el switch, el primer comando de configuración de rol de usuario que ingresa hace que el software NX-OS del switch realice estas acciones:

1. Crea una sesión CFS en el switch.
2. Bloquea la configuración del rol de usuario en todos los switches de la región CFS con CFS

habilitado para la función de rol de usuario.
3. Guarda los cambios en la configuración de la función de usuario en un búfer temporal en el switch.

Los cambios permanecen en el búfer temporal en el switch hasta que se comprometen explícitamente a que se distribuyan a los dispositivos en la región CFS.

Cuando realiza los cambios, el software NX-OS realiza las siguientes acciones:

1. Aplica los cambios a la configuración en ejecución en el switch.
2. Distribuye la configuración de rol de usuario actualizada a los otros switches de la región CFS.
3. Desbloquea la configuración del rol de usuario en los dispositivos de la región CFS.
4. Termina la sesión CFS.

Estas configuraciones se distribuyen:

- Nombres y descripciones de funciones
- Lista de reglas para las funciones

Comandos configuration y show

	Comando	Propósito
Paso 1.	**configure terminal** Ejemplo: switch# **configure terminal** switch(config)#	Ingresa en el modo de configuración global.
Paso 2.	**nombre de rol** *role-name* Ejemplo: switch(config)# **nombre de rol UsuarioA** switch(config-role)#	Especifica un rol de usuario e ingresa en el modo de configuración de rol.
Paso 3.	**VLAN Policy deny** Ejemplo: switch(config-role)# **denegación de política vlan** switch(config-role-vlan)#	Ingresa en el modo de configuración de política de VLAN de rol.
Paso 4.	**permit vlan** vlan-*id* Ejemplo: switch(config-role-vlan)# **permit vlan 1**	Especifica la vlan a la que puede acceder el rol. Repita este comando para tantas vlan como sea necesario.
Paso 5.	**salir** Ejemplo: switch(config-role-vlan)# **exit** switch(config-role)#	Sale del modo de configuración de política de VLAN de rol.
Paso 6.	**show role** Ejemplo: switch(config-role)#	(Opcional) Muestra la configuración de la función.

Paso 7.	**show role** **show role** {**pending** | **pending-diff**} Ejemplo: switch(config-role)# **show role pendiente**	(Opcional) Muestra la configuración de la función de usuario pendiente de distribución
Paso 8.	**confirmación de rol** Ejemplo: **confirmación de rol** switch(config-role)#	(Opcional) Aplica los cambios de configuración de rol de usuario en la base de datos temporal a la configuración en ejecución y distribuye la configuración de rol de usuario a otros switches si ha activado la distribución de configuración de CFS para la función de rol de usuario.
Paso 9.	**copy running-config startup-config** Ejemplo: switch# **copy running-config startup-config**	(Opcional) Copia la configuración en ejecución en la configuración de inicio.

Estos pasos habilitan la distribución de la configuración de roles:

	Comando	Propósito
Paso 1.	switch# **config t** switch(config)#	Ingresa en el modo de configuración.
Paso 2.	switch(config)# **role distribute** switch(config)#**no role distribute**	Habilita la distribución de la configuración de roles. Inhabilita la distribución de la configuración de roles (valor predeterminado).

Estos pasos confirman los cambios de configuración de roles:

	Comando	Propósito
Paso 1	Nexus# **config t** Nexus(config)#	Ingresa en el modo de configuración.
Paso 2	Nexus(config)# **confirmación de rol**	Confirma los cambios en la configuración de la función.

Estos pasos descartan los cambios de configuración de roles:

	Comando	Propósito
Paso 1	Nexus# **config t** Nexus(config)#	Ingresa en el modo de configuración.
Paso 2	Nexus(config)# **rol abort**	Descarta los cambios en la configuración de la función y borra la base de datos configuración pendiente.

Para mostrar la información de configuración de la cuenta de usuario y RBAC, realice una de estas tareas:

Comando	Propósito
show role	Muestra la configuración del rol de usuario.
show role feature	Muestra la lista de funciones.
show role feature-group	Muestra la configuración del grupo de funciones.

Borrar la sesión de distribución de funciones de usuario

Puede borrar la sesión de distribución de Cisco Fabric Services en curso (si la hay) y desbloquear el fabric para la función de rol de usuario.

Precaución: Cualquier cambio en la base de datos pendiente se perderá cuando ejecute este comando.

	Comando	Propósito
Paso 1	**sesión de** switch# **clear role** **Ejemplo:** sesión de rol clear de switch#	Borra la sesión y desbloquea el fabric.
Paso 2	**show role session status** **Ejemplo:** switch# show role session status	(Opcional) Muestra el estado de la sesión de CFS de rol de usu

Ejemplo de configuración

En este ejemplo, vamos a crear un TAC de cuenta de usuario con estos permisos de acceso:

- Acceso al comando clear
- Acceso al comando de configuración
- Acceso al comando debug
- Acceso al comando exec
- Acceso al comando show
- Acceso a vlan 1-10 solamente

```
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end

C5548P-1# show role name Cisco

Role: Cisco
  Description: new role
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 1-10
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  5       permit  command                         show
  4       permit  command                         exec
  3       permit  command                         debug
  2       permit  command                         config
  1       permit  command                         clear
```

```
C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
        this user account has no expiry date
        roles:Cisco
```

Requisitos de licencia

Producto	Requisito de licencia
NX-OS	Las cuentas de usuario y RBAC no requieren licencia.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.