Nexo N5500, 5600 y control de acceso de la base del papel N6000 (RBAC)

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Requisitos del usuario](#)
[Rol del usuario](#)
[Rol del usuario de las reglas](#)
[Rol del usuario de la distribución](#)
[Comandos configuration y show](#)
[Borre el rol del usuario de la sesión de la distribución](#)
[Ejemplo de configuración](#)
[Requisitos para obtener la licencia](#)
[Verificación](#)
[Troubleshooting](#)

Introducción

Este documento describe cómo limitar a un usuario para acceder el nexo 5500, el nexo 5600 y los 6000 Switch del nexo usando el papel basan el control de acceso (RBAC).

RBAC permite que usted defina las reglas para que un rol del usuario asignado restrinja la autorización de un usuario que tenga acceso a las operaciones del administrador de switches.

Usted puede crear y manejar una cuenta de usuario y asignar los papeles que acceso del límite a los 6000 Switch del nexo 5500, del nexo 5600 y del nexo.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Nexo 5500, nexo 5600, comandos de configuración CLI de los 6000 Switch del nexo
- Servicios de estructura de Cisco (CF).

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Requisitos del usuario

Éstos son algunos requisitos del usuario que son necesidad de ser satisfecho:

- Solamente los usuarios con el papel red-admin pueden crear los papeles.
- Solamente los usuarios con el papel red-admin pueden ver la salida del **papel de la demostración**.
- Incluso si permiten a los usuarios para realizar todos los comandos show, a les no se permite ver la salida del **papel de la demostración**, a menos que asignen estos usuarios un papel red-admin.
- Una cuenta de usuario debe tener por lo menos un rol del usuario.

Rol del usuario

Cada papel se puede asignar a los usuarios múltiples y cada usuario puede ser papeles del múltiplo de la parte de.

Por ejemplo, se permite a los usuarios del papel A publicar los comandos show y se permite a los usuarios del papel B realizar los cambios de configuración.

Si asignan un usuario al papel A y al papel B, este usuario puede publicar el comando show y realizar los cambios a la configuración.

El comando del acceso del permiso toma la prioridad encima niega el comando del acceso.

Por ejemplo, si usted pertenece a un papel que niegue el acceso a los comandos configuration.

Sin embargo, si usted también pertenece a un papel que tenga acceso a los comandos configuration, usted entonces tiene el acceso a los comandos configuration.

Hay cinco papeles de usuario predeterminado:

- red-admin - Acceso de lectura y escritura completo al Switch entero.
- operador de la red - Acceso de lectura completo al Switch entero.
- VDC-admin - Acceso de lectura y escritura limitado a un VDC
- VDC-operador - Acceso de lectura limitado a un VDC
- SAN-admin - Acceso de lectura y escritura completo a los administradores SAN.

Nota: Usted no puede modificarse/los papeles de usuario predeterminado de la cancelación.

Nota: el comando del **papel de la demostración** visualizará el papel disponible en el Switch

Rol del usuario de las reglas

La regla es el elemento básico de un papel.

Una regla define qué operaciones permite el papel que el usuario realice.

Usted puede aplicar las reglas para estos parámetros:

- Comando del comando A o grupo de comandos definidos en una expresión normal.
- Los comandos de la característica que se aplican a una función proporcionaron por el software NX-OS.
- Grupo predeterminado o definido por el usario del grupo de la característica de características.

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

El parámetro de control siguiente es la característica, que representa los comandos all asociados a la característica.

El parámetro de control más reciente es el grupo de la característica. El grupo de la característica combina las características relacionadas y permite que usted maneje fácilmente las reglas.

El número definido por el usuario de la regla determina la orden en la cual las reglas son aplicadas.

Las reglas se aplican en el orden descendente.

Por ejemplo, la regla 1 es aplicada antes de la regla 2, que es aplicada antes de la regla 3, y así sucesivamente.

El comando rule especifica las operaciones que se pueden realizar por un papel específico. Cada regla consiste en un número de la regla, un tipo de la regla (el permit or deny),

un comando type (por ejemplo, configuración, demostración, ejecutivo, debug), y un nombre de la característica opcional (por ejemplo, FCOE, HSRP, VTP, interfaz).

Rol del usuario de la distribución

las configuraciones Papel-basadas utilizan la infraestructura de los Servicios de estructura de Cisco (CF) para habilitar la administración de base de datos eficiente y para proporcionar un monopunto de la configuración en la red.

Cuando usted habilita la distribución CF para una característica en su dispositivo, el dispositivo pertenece a una región CF que contiene los otros dispositivos en la red que usted también ha habilitado para la distribución CF para la característica. La distribución CF para el rol del usuario de la característica se inhabilita por abandono.

Usted debe habilitar los CF para los rol del usuario en cada dispositivo al cual usted quiera distribuir los cambios de configuración.

Después de que usted habilite la distribución CF para los rol del usuario en el Switch, el primer rol

del usuario del comando configuration que usted ingresa las causas el software del Switch NX-OS para tomar a estas acciones:

1. Crea una sesión CF sobre el Switch.
2. Bloquea el rol del usuario de la configuración en todo el Switches en la región CF con los CF habilitados para el rol del usuario de la característica.
3. Guarda el rol del usuario de los cambios de configuración en un buffer temporal en el Switch.

Los cambios permanecen en el buffer temporal en el Switch hasta que usted los confíe explícitamente que se distribuirán a los dispositivos en la región CF.

Cuando usted confía los cambios, el software NX-OS toma estas medidas:

1. Aplica los cambios a la configuración corriente en el Switch.
2. Distribuye el rol del usuario actualizado de la configuración al otro Switches en la región CF.
3. Desbloquea el rol del usuario de la configuración en los dispositivos en la región CF.
4. Termina la sesión CF.

Se distribuyen estas configuraciones:

- Nombres de la función y descripciones
- Lista de reglas para los papeles

Comandos configuration y show

	Comando	Propósito
	configure terminal	
Paso 1.	Ejemplo: switch# **configurado terminal** switch(config)#	Ingresa en el modo de configuración global.
Paso 2.	*nombre de la función del* **nombre de la función** Ejemplo: **nombre de la función UserA del** switch(config)#	Especifica un rol del usuario y ingresa al modo de configuración del papel.
Paso 3.	Switch (config-papel) # **la política de VLAN niega** Ejemplo: el Switch (config-papel) # **política de VLAN niega**	Ingresa al modo de configuración de la política de VLAN del papel.
Paso 4.	Switch (config-papel-VLAN) # VLAN-identificación **vlan del permiso** Ejemplo: Switch (config-	Especifica el vlan que el papel puede acceder. Relance este comando para tanto vlans según las necesidades.

	papel-VLAN) # **vlan1 del permiso salida**	
Paso 5.	Ejemplo: Switch (config-papel-VLAN) # **salida**	Da salida al modo de configuración de la política de VLAN del papel.
	Switch (config-papel) # **muestre el papel**	
Paso 6.	Ejemplo: Switch (config-papel) # **papel de la demostración muestre el papel** {**pendiente** | **p endiente-diff**}	(Opcional) visualiza la configuración del papel.
Paso 7.	Ejemplo: Switch (config-papel) # **papel de la demostración pendiente**	(Opcional) visualiza el rol del usuario de la configuración pendiente para la distribución
	cometer del papel	(Opcional) aplica el rol del usuario de los cambios de configuración en la base de datos temporaria a la configuración corriente y distribuye el rol del usuario de la configuración a otros swithces si usted ha habilitado la distribución de la configuración CF para el rol del usuario de la característica.
Paso 8.	Ejemplo: Switch (config-papel) # **cometer del papel**	
	copie los lanzamiento-config de los ejecutar-config	(Opcional) copia la configuración corriente a la configuración de inicio.
Paso 9.	Ejemplo: **lanzamiento-config de los ejecutar-config de la copia del** switch#	

Estos pasos habilitan la distribución de la configuración del papel:

	Comando	Propósito
Paso 1.	**config t del** switch# switch(config)#	Ingresa al modo de configuración.
Paso 2.	**el papel del** switch(config)# **distribuye**	Habilita la distribución de la configuración del papel.
	el papel del switch(config)#**no distribuye**	Distribución de la configuración del papel de las neutralizaciones (valor por defecto).

Estos cambios de configuración del papel del cometer de los pasos:

	Comando	Propósito
Paso 1	**Config t de** Nexus# Nexus(config)#	Ingresa al modo de configuración.
Paso 2	**Cometer del papel de** Nexus(config)#	Confía los cambios de configuración del papel.

Estos pasos desechan los cambios de configuración del papel:

	Comando	Propósito
Paso 1	**Config t de** Nexus# Nexus(config)#	Ingresa al modo de configuración.
Paso 2	**Aborto del papel de** Nexus(config)#	Desecha los cambios de configuración del papel y borra la base de dato la configuración pendiente.

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

Comando	Propósito
muestre el papel	Visualiza el rol del usuario de la configuración.
muestre la característica del papel	Visualiza la lista de características.
muestre al característica-grupo del papel	Visualiza la configuración de grupo de la característica.

Borre el rol del usuario de la sesión de la distribución

Usted puede borrar la sesión en curso de la distribución de los Servicios de estructura de Cisco (eventualmente) y desbloquear la tela para el rol del usuario de la característica.

> Precaución: Cualquier cambio en la base de datos pendiente será perdido cuando usted publica este comando.

	Comando	Propósito
Paso 1	**sesión clara del papel del** switch# **Ejemplo:** sesión clara del papel del switch#	Borra la sesión y desbloquea la tela.
Paso 2	**muestre el estatus de la sesión del papel Ejemplo:** estatus de la sesión del papel de la demostración del switch#	(Opcional) visualiza el rol del usuario CF del est de la sesión.

Ejemplo de configuración

En este ejemplo, vamos a crear una cuenta de usuario TAC con estos permiso de acceso:

- Acceso al comando clear
- Acceso al comando configuration
- Acceso al comando debug
- Acceso al comando exec
- Acceso al comando show
- Acceso a 1-10 vlan 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 para obtener la licencia

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

Verificación

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

Troubleshooting

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