RBAC (Role Base Access Control) do Nexus N5500, 5600 e N6000

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Requisitos do usuário](#)
[Funções de usuário](#)
[Regras de função de usuário](#)
[Distribuição da função de usuário](#)
[Comandos configuration e show](#)
[Limpe a sessão de distribuição da função de usuário](#)
[Exemplo de configuração](#)
[Requisitos de licenciamento](#)
[Verificar](#)
[Troubleshoot](#)

Introduction

Este documento descreve como limitar um usuário a acessar os switches Nexus 5500, Nexus 5600 e Nexus 6000 usando RBAC (Role Base Access Control).

O RBAC permite definir as regras de uma função de usuário atribuída para restringir a autorização de um usuário que tenha acesso às operações de gerenciamento do switch.

Você pode criar e gerenciar uma conta de usuário e atribuir funções que limitam o acesso aos switches Nexus 5500, Nexus 5600 e Nexus 6000.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Comandos de configuração CLI dos switches Nexus 5500, Nexus 5600 e Nexus 6000
- Cisco Fabric Services (CFS).

Componentes Utilizados

As informações neste documento são baseadas nos switches Nexus 5500, Nexus 5600 e Nexus 6000 que executam o 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 do usuário

Estes são alguns requisitos do usuário que precisam ser atendidos:

- Somente usuários com função de administrador de rede podem criar funções.
- Somente usuários com função de administrador de rede podem exibir a saída de **show role**.
- Mesmo que os usuários tenham permissão para executar todos os comandos show, eles não têm permissão para exibir a saída **show role**, a menos que esses usuários recebam uma função network-admin.
- Uma conta de usuário deve ter pelo menos uma função de usuário.

Funções de usuário

Cada função pode ser atribuída a vários usuários e cada usuário pode fazer parte de várias funções.

Por exemplo, os usuários da função A podem emitir comandos show e os usuários da função B podem fazer alterações na configuração.

Se um usuário estiver atribuído à função A e à função B, ele poderá emitir o comando show e fazer alterações na configuração.

O comando Permit access tem prioridade sobre o comando deny access.

Por exemplo, se você pertencer a uma função que nega o acesso aos comandos de configuração.

No entanto, se você também pertencer a uma função que tenha acesso aos comandos de configuração, terá acesso aos comandos de configuração.

Há cinco funções de usuário padrão:

- network-admin - Acesso completo de leitura e gravação ao switch inteiro.
- operador de rede - acesso de leitura completo ao switch inteiro.
- vdc-admin - Acesso de leitura e gravação limitado a um VDC
- vdc-operator - Acesso de leitura limitado a um VDC
- san-admin - Acesso completo de leitura e gravação aos administradores de SAN.

Nota:Não é possível modificar/excluir funções de usuário padrão.

Note: O comando **show role** exibirá a função disponível no switch

Regras de função de usuário

A regra é o elemento básico de uma função.

Uma regra define quais operações a função permite que o usuário execute.

Você pode aplicar regras para estes parâmetros:

- Comando- Um comando ou grupo de comandos definido em uma expressão regular.
- Recurso - Comandos que se aplicam a uma função fornecida pelo software NX-OS.
- Grupo de recursos- Grupo de recursos padrão ou definido pelo usuário.

Esses parâmetros criam uma relação hierárquica. O parâmetro de controle mais básico é o comando.

O próximo parâmetro de controle é o recurso, que representa todos os comandos associados ao recurso.

O último parâmetro de controle é o grupo de recursos. O grupo de recursos combina recursos relacionados e permite que você gerencie regras facilmente.

O número de regra especificado pelo usuário determina a ordem na qual as regras são aplicadas.

As regras são aplicadas em ordem decrescente.

Por exemplo, a regra 1 é aplicada antes da regra 2, que é aplicada antes da regra 3, e assim por diante.

O comando rule especifica operações que podem ser executadas por uma função específica. Cada regra consiste em um número de regra, um tipo de regra (permitir ou negar),

um tipo de comando (por exemplo, configuração, show, exec, debug) e um nome de recurso opcional (por exemplo, FCOE, HSRP, VTP, interface).

Distribuição da função de usuário

As configurações baseadas em funções usam a infraestrutura do Cisco Fabric Services (CFS) para permitir o gerenciamento eficiente do banco de dados e para fornecer um único ponto de configuração na rede.

Quando você habilita a distribuição de CFS para um recurso em seu dispositivo, o dispositivo pertence a uma região de CFS que contém outros dispositivos na rede que você também habilitou para a distribuição de CFS para o recurso. A distribuição CFS para o recurso de função de usuário está desabilitada por padrão.

Você deve habilitar o CFS para funções de usuário em cada dispositivo para o qual deseja distribuir alterações de configuração.

Depois de habilitar a distribuição CFS para funções de usuário no switch, o primeiro comando de configuração de função de usuário inserido faz com que o software NX-OS do switch execute estas ações:

1. Cria uma sessão CFS no switch.
2. Bloqueia a configuração da função de usuário em todos os switches na região CFS com CFS ativado para o recurso de função de usuário.
3. Salva as alterações de configuração da função de usuário em um buffer temporário no switch.

As alterações permanecem no buffer temporário no switch até que você as confirme explicitamente para serem distribuídas aos dispositivos na região CFS.

Ao confirmar as alterações, o software NX-OS executa estas ações:

1. Aplica as alterações à configuração em execução no switch.
2. Distribui a configuração atualizada da função de usuário para os outros switches na região CFS.
3. Desbloqueia a configuração da função de usuário nos dispositivos na região CFS.
4. Termina a sessão do CFS.

Essas configurações são distribuídas:

- Nomes e descrições das funções
- Lista de regras para as funções

Comandos configuration e show

	Comando	Propósito
Etapa 1.	**configure terminal** Exemplo: switch# **configure terminal** switch(config)#	Entra no modo de configuração global.
Etapa 2.	**nome da função** *nome da função* Exemplo: switch(config)# **nome da função Usuário A** switch(config-role)#	Especifica uma função de usuário e entra no modo de configuração de função.
Etapa 3.	**vlan policy deny** Exemplo: switch(config-role)# **vlan policy deny** switch(config-role-vlan)#	Entra no modo de configuração de política de vlan de função.
Etapa 4.	**permit vlan** vlan-*id* Exemplo: switch(config-role-vlan)# **permit vlan 1**	Especifica a vlan que a função pode acessar. Repita esse comando para quantas vlans forem necessárias.
Etapa 5.	**sair** Exemplo: switch(config-role-vlan)# **exit** switch(config-role)#	Sai do modo de configuração de política de vlan de função.
Etapa	**show role**	(Opcional) Exibe a configuração da função.

6.	Exemplo: switch(config-role)# **show role** **show role** {**pending** | **pending-diff**}	
Passo 7.	Exemplo: switch(config-role)# **show role pending**	(Opcional) Exibe a configuração da função de usuário pendente para distribuição
Etapa 8.	**confirmação de função** Exemplo: switch(config-role)# **atribuição**	(Opcional) Aplica as alterações da configuração da função de usuário no banco de dados temporário à configuração em execução e distribui a configuração da função de usuário para outros switches se você tiver ativado a distribuição da configuração do CFS para o recurso de função de usuário.
Etapa 9.	**copy running-config startup-config** Exemplo: switch# **copy running-config startup-config**	(Opcional) Copia a configuração atual para a configuração de inicialização.

Estas etapas permitem a distribuição da configuração da função:

	Comando	Propósito
Etapa 1.	switch# **config t** switch(config)#	Entra no modo de configuração.
Etapa 2.	switch(config)# **função distribute** switch(config)#**nenhuma distribuição de função**	Ativa a distribuição da configuração de funções. Desativa a distribuição da configuração da função (padrão).

Estas etapas confirmam alterações na configuração da função:

	Comando	Propósito
Passo 1	Nexus# **config t** Nexus(config)#	Entra no modo de configuração.
Passo 2	Nexus(config)# **confirmação de função**	Confirma as alterações na configuração da função.

Estas etapas descartam as alterações de configuração de função:

	Comando	Propósito
Passo 1	Nexus# **config t** Nexus(config)#	Entra no modo de configuração.
Passo 2	Nexus(config)# **cancelamento de função**	Descarta as alterações de configuração da função e limpa o banco d dados de configuração pendente.

Para exibir informações de configuração de RBAC e conta de usuário, execute uma destas tarefas:

Comando	Propósito
show role	Exibe a configuração da função de usuário.
show role feature	Exibe a lista de recursos.
show role feature-group	Exibe a configuração do grupo de recursos.

Limpe a sessão de distribuição da função de usuário

Você pode limpar a sessão de distribuição contínua do Cisco Fabric Services (se houver) e desbloquear a estrutura do recurso de função do usuário.

> **Caution**: Qualquer alteração no banco de dados pendente será perdida quando você emitir esse comando.

	Comando	Propósito
Passo 1	switch# **clear role session** **Exemplo:** switch#clear role session	Limpa a sessão e desbloqueia a estrutura.
Passo 2	**show role session status** **Exemplo:** switch#show role session status	(Opcional) Exibe o status da sessão da função de usuário CFS

Exemplo de configuração

Neste exemplo, vamos criar um TAC de conta de usuário com a seguinte permissão de acesso:

- Acesso ao comando clear
- Acesso ao comando de configuração
- Acesso ao comando debug
- Acesso ao comando exec
- Acesso ao comando show
- Acesso somente à vlan 1-10

```
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 licenciamento

Produto	Requisito de licença
NX-OS	As contas de usuário e o RBAC não exigem licença.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.