Nexo N5500, 5600 e controle de acesso da base do papel N6000 (RBAC)

Índice

Introdução

Este documento descreve como limitar um usuário para alcançar 6000 Switch do nexo 5500, do nexo 5600 e do nexo usando o controle de acesso baixo do papel (RBAC).

RBAC permite que você defina as regras para que um papel de usuário atribuído restrinja a autorização de um usuário que tenha o acesso às operações do gerenciamento de switch.

Você pode criar e controlar uma conta de usuário e atribuir os papéis que limitam o acesso aos 6000 Switch do nexo 5500, do nexo 5600 e do nexo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Nexo 5500, nexo 5600, comandos de configuração de CLI dos 6000 Switch do nexo
- Serviços Cisco Fabric (CF).

Componentes Utilizados

A informação neste documento é baseada nos 6000 Switch do nexo 5500, do nexo 5600 e do nexo que executam NXOS 5.2(1)N1(9) 7.3(1)N1(1).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Requisições de usuário

Estas são algumas requisições de usuário que são necessidade de ser cumprido:

- Somente os usuários com papel rede-admin podem criar papéis.
- Somente os usuários com papel rede-admin podem ver a saída do **papel da mostra**.
- Mesmo se os usuários são permitidos para executar todos os comandos show, não estão permitidos ver a saída do **papel da mostra**, a menos que estes usuários forem atribuídos um papel rede-admin.
- Uma conta de usuário deve ter pelo menos um papel de usuário.

Papéis de usuário

Cada papel pode ser atribuído aos usuários múltiplos e cada usuário pode ser parte de papéis múltiplos.

Por exemplo, são permitidos aos usuários do papel A emitir comandos show e são permitidos aos usuários do papel B fazer alterações de configuração.

Se um usuário é atribuído ao papel A e ao papel B, este usuário pode emitir o comando show e fazer mudanças à configuração.

O comando do acesso da licença toma a prioridade sobre nega o comando do acesso.

Por exemplo, se você pertence a um papel que negue o acesso aos comandos configuration.

Contudo, se você igualmente pertence a um papel que tenha o acesso aos comandos configuration, você tem então o acesso aos comandos configuration.

Há cinco papéis de usuário padrão:

- rede-admin - Termine o acesso de leitura e gravação ao interruptor inteiro.
- operador de rede - Termine o acesso de leitura ao interruptor inteiro.
- VDC-admin - Acesso de leitura e gravação limitado a um VDC
- VDC-operador - Acesso de leitura limitado a um VDC
- SAN-admin - Termine o acesso de leitura e gravação aos administradores SAN.

Nota: Você não pode alterar/papéis usuário padrão da supressão.

Nota: o comando do **papel da mostra** indicará o papel disponível no interruptor

Papel de usuário das regras

A regra é o elemento básico de um papel.

Uma regra define que operações o papel permite que o usuário execute.

Você pode aplicar regras para estes parâmetros:

- Comando do comando A ou grupo de comandos definidos em uma expressão regular.
- Os comandos da característica que se aplicam a uma função forneceram pelo software NX-OS.
- Padrão do grupo da característica ou grupo definido pelo utilizador de características.

Estes parâmetros criam um relacionamento hierárquico. O parâmetro de controle o mais básico é o comando.

O parâmetro de controle seguinte é a característica, que representa os comandos all associados com a característica.

O último parâmetro de controle é o grupo da característica. O grupo da característica combina características relacionadas e permite que você controle facilmente regras.

O número especificado pelo utilizador da regra determina a ordem em que as regras são aplicadas.

As regras são aplicadas no 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 as operações que podem ser executadas por um papel específico. Cada regra consiste em um número da regra, um tipo da regra (o permit or deny),

um comando type (por exemplo, a configuração, mostra, executivo, debuga), e um nome dos recursos opcionais (por exemplo, FCOE, HSRP, VTP, relação).

Papel de usuário da distribuição

as configurações Papel-baseadas usam a infraestrutura dos Serviços Cisco Fabric (CF) para permitir o gerenciamento de base de dados eficiente e para fornecer um único ponto da configuração na rede.

Quando você permite a distribuição CF para uma característica em seu dispositivo, o dispositivo pertence a uma região CF que contém outros dispositivos na rede que você igualmente permitiu para a distribuição CF para a característica. A distribuição CF para o papel de usuário da característica é desabilitada à revelia.

Você deve permitir CF para papéis de usuário em cada dispositivo a que você quer distribuir alterações de configuração.

Depois que você permite a distribuição CF para papéis de usuário no interruptor, o primeiro papel de usuário do comando configuration que você incorpora causas o software do interruptor NX-OS

para tomar a estas ações:

1. Cria uma sessão CF no interruptor.
2. Trava o papel de usuário da configuração em todo o Switches na região CF com os CF permitidos para o papel de usuário da característica.
3. Salvar o papel de usuário das alterações de configuração em um buffer provisório no interruptor.

As mudanças ficam no buffer provisório no interruptor até que você as comprometa explicitamente a ser distribuídas aos dispositivos na região CF.

Quando você compromete as mudanças, o software NX-OS toma estas ações:

1. Aplica as mudanças à configuração running no interruptor.
2. Distribui o papel de usuário actualizado da configuração ao outro Switches na região CF.
3. Destrava o papel de usuário da configuração nos dispositivos na região CF.
4. Termina a sessão CF.

Estas configurações são distribuídas:

- Nomes e descrições do papel
- Lista de regras para os papéis

Comandos configuration e show

	Comando	Propósito
Etapa 1.	Exemplo: o switch# **configura o terminal** switch(config)#	Incorpora o modo de configuração global.
Etapa 2.	*papel-nome do* **nome do papel** Exemplo: **nome UserA do papel do** switch(config)# interruptor (configuração-papel) #	Especifica um papel de usuário e incorpora o modo de configuração do papel.
Etapa 3.	**a política vlan nega** Exemplo: o interruptor (configuração-papel) # **política vlan nega** interruptor (configuração-papel-VLAN) #	Incorpora o modo de configuração da política vlan do papel.
Etapa 4.	ID de VLAN **vlan da licença** Exemplo: interruptor (configuração-papel-VLAN) # **licença 1 vlan**	Especifica o vlan que o papel pode alcançar. Repita este comando para tantos como vlans como necessários.
Etapa 5.	**saída**	Retira o modo de configuração da política vlan do papel.

	Exemplo: interruptor (configuração-papel-VLAN) # **saída** interruptor (configuração-papel) # **mostre o papel**	
Etapa 6.	Exemplo: interruptor (configuração-papel) # **papel da mostra mostre o papel** {**pendente** | **pendente-diff**}	(Opcional) indica a configuração do papel.
Etapa 7.	Exemplo: interruptor (configuração-papel) # **papel da mostra pendente**	(Opcional) indica o papel de usuário da configuração pendente para a distribuição
Etapa 8.	Exemplo: o interruptor (configuração-papel) # **papel compromete**	(Opcional) aplica o papel de usuário das alterações de configuração no base de dados temporário à configuração running e distribui o papel de usuário da configuração a outros swithces se você permitiu a distribuição da configuração CF para o papel de usuário da característica.
Etapa 9.	**copie a partida-configuração da executar-configuração** Exemplo: **partida-configuração da executar-configuração da cópia do** switch#	(Opcional) copia a configuração running à configuração de inicialização.

Estas etapas permitem a distribuição da configuração do papel:

	Comando	Propósito
Etapa 1.	**config t do** switch# switch(config)#	Incorpora o modo de configuração.
Etapa 2.	**o papel do** switch(config)# **distribui** **o papel do** switch(config)#no **distribui**	Permite a distribuição da configuração do papel. Distribuição da configuração do papel das inutilizações (padrão).

Estas etapas comprometem alterações de configuração do papel:

	Comando	Propósito
Passo 1	**Config t de** Nexus# Nexus(config)#	Incorpora o modo de configuração.
Passo 2	**O papel de** Nexus(config)# **compromete**	Compromete as alterações de configuração do papel.

Estas etapas rejeitam alterações de configuração do papel:

	Comando	Propósito
Passo 1	**Config t de** Nexus# Nexus(config)#	Incorpora o modo de configuração.
Passo 2	**Aborto do papel de** Nexus(config)#	Rejeita as alterações de configuração do papel e cancela o base de da da configuração pendente.

Para indicar a conta de usuário e a informação de configuração RBAC, execute uma destas tarefas:

Comando	Propósito
mostre o papel	Indica o papel de usuário da configuração.
mostre a característica do papel	Indica a lista de recurso.
mostre o característica-grupo do papel	Indica a configuração de grupo da característica.

Cancele o papel de usuário da sessão da distribuição

Você pode cancelar a sessão em curso da distribuição dos Serviços Cisco Fabric (eventualmente) e destravar a tela para o papel de usuário da característica.

> Cuidado: Todas as mudanças no base de dados pendente serão perdidas quando você emite este comando.

	Comando	Propósito
Passo 1	**sessão clara do papel do** switch# **Exemplo:** sessão clara do papel do switch#	Cancela a sessão e destrava a tela.
Passo 2	**mostre o estado da sessão do papel Exemplo:** estado da sessão do papel da mostra do switch#	(Opcional) indica CF o papel de usuário do estado sessão.

Exemplo de configuração

Neste exemplo, nós estamos indo criar uma conta de usuário TAC com os estes permissão de acesso:

- Alcance ao comando clear
- Alcance ao comando configuration
- Alcance ao comando debug
- Alcance ao comando exec
- Alcance ao comando show
- Alcance a 1-10 vlan somente

```
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	Exigência da licença
NX-OS	As contas de usuário e RBAC não exigem nenhuma licença.

Verificar

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

Troubleshooting

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