Nexus N5500, 5600 en N6000 Rol Base Access Control (RBAC)

Inhoud

Inleiding

In dit document wordt beschreven hoe een gebruiker toegang tot Nexus 5500, Nexus 5600 en Nexus 6000 switches kan beperken met Rollend Base Access Control (RBAC).

RBAC stelt u in staat de regels voor een toegewezen gebruikersrol te definiëren om de toestemming van een gebruiker die toegang heeft tot de schakelbeheeroperaties te beperken.

U kunt een gebruikersaccount maken en beheren en rollen toewijzen die de toegang beperken tot Nexus 5500, Nexus 5600 en Nexus 6000 switches.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Nexus 5500, Nexus 5600, Nexus 6000 switches CLI-configuratieopdrachten
- Cisco Fabric Services (CFS).

Gebruikte componenten

De informatie in dit document is gebaseerd op Nexus 5500, Nexus 5600 en Nexus 6000-switches met NXOS 5.2(1)N1(9) 7.3(1)N1(1).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Gebruikersvereisten

Dit zijn een aantal gebruikersvereisten waaraan moet worden voldaan:

- Alleen gebruikers met een netwerk-beheerrol kunnen rollen maken.
- Alleen gebruikers met een netwerk-beheerrol kunnen de output van **showrol** bekijken.
- Zelfs als gebruikers toestemming hebben om alle showopdrachten uit te voeren, mogen ze geen **show role** output bekijken, tenzij deze gebruikers een netwerk-admin rol toegewezen krijgen.
- Een gebruikersaccount moet ten minste één gebruikersrol hebben.

Rol van gebruikers

Elke rol kan aan meerdere gebruikers worden toegewezen en elke gebruiker kan deel uitmaken van meerdere rollen.

Bijvoorbeeld, rol A gebruikers worden toegestaan om tonen opdrachten uit te geven en rol B gebruikers mogen configuratie veranderingen aanbrengen.

Als een gebruiker is toegewezen aan zowel rol A als Rol B, kan deze gebruiker bevel tonen en veranderingen in configuratie aanbrengen.

De toegangsopdracht geeft voorrang boven het toegangsbevel ontkennen.

Bijvoorbeeld, als u tot een rol behoort die toegang tot configuratieopdrachten ontzegt.

Maar als u ook tot een rol behoort die toegang tot configuratieopdrachten heeft, hebt u dan de toegang tot configuratieopdrachten.

Er zijn vijf standaardingestelde gebruikersrollen:

- netwerk-beheerder - Complete lees-en-schrijftoegang tot de gehele schakelaar.
- netbeheerder - volledige toegang tot de gehele schakelaar.
- vdc-admin - toegang voor lezen en schrijven beperkt tot een VDC
- Vdc-operator - Lezen toegang beperkt tot een VDC
- san-admin - Complete lees-en-schrijftoegang tot SAN-beheerders.

Opmerking: u kunt de standaardgebruikersrollen niet wijzigen of verwijderen.

Opmerking: opdracht **rol tonen** zal de rol die beschikbaar is in de switch weergeven

Regels voor rolfuncties

De regel is het fundamentele element van een rol.

Een regel definieert welke bewerkingen de rol de gebruiker toestaat om uit te voeren.

U kunt regels voor deze parameters toepassen:

- Opdracht - Een opdracht of een groep opdrachten gedefinieerd in een reguliere expressie.
- Functie - opdrachten die van toepassing zijn op een functie die door de NX-OS-software wordt geleverd.
- Functiegroep - standaard of door de gebruiker ingestelde groep functies.

Deze parameters maken een hiërarchische relatie. De meest elementaire controle parameter is de opdracht.

De volgende parameter is de functie die alle opdrachten vertegenwoordigt die aan de functie zijn gekoppeld.

De laatste control parameter is de function group. De functiegroep combineert verwante functies en biedt u de mogelijkheid om regels eenvoudig te beheren.

Het door de gebruiker opgegeven regelnummer bepaalt de volgorde waarin de regels worden toegepast.

De regels worden in aflopende volgorde toegepast.

Bijvoorbeeld, regel 1 wordt toegepast vóór regel 2, die wordt toegepast vóór regel 3, enzovoort.

De regelopdracht specificeert bewerkingen die door een specifieke rol kunnen worden uitgevoerd. Elke regel bestaat uit een regelnummer, een regeltype (vergunning of ontkenning),

een opdrachttype (bijvoorbeeld configuratie, show, exec, debug) en een optionele functienaam (bijvoorbeeld FCOE, HSRP, VTP, interface).

Distributie van functies

Op rol gebaseerde configuraties gebruiken de Cisco Fabric Services (CFS) infrastructuur om efficiënt gegevensbeheer mogelijk te maken en één punt van configuratie in het netwerk te bieden.

Wanneer u de CFS-distributie voor een functie op uw apparaat in staat stelt, behoort het apparaat tot een CFS-gebied dat andere apparaten in het netwerk bevat die u ook voor de CFS-distributie voor de functie hebt ingeschakeld. De CFS-verdeling voor de functie voor de gebruikersrol is standaard uitgeschakeld.

U moet CFS voor gebruikersrollen op elk apparaat inschakelen waarop u configuratieveranderingen wilt distribueren.

Nadat u CFS-distributie voor gebruikersrollen op de schakelaar toelaat, veroorzaakt de eerste configuratieopdracht van de gebruikersrol die u ingaat de schakelaar NX-OS software om deze acties te ondernemen:

1. Maakt een CFS-sessie op de schakelaar.
2. Sluit de gebruikersrolconfiguratie op alle switches in de CFS-regio af met CFS die voor de gebruikersrolfunctie is ingeschakeld.
3. Hiermee slaat u de configuratiewijzigingen in de gebruikersrol op in een tijdelijke buffer op de schakelaar.

De veranderingen blijven in de tijdelijke buffer op de schakelaar tot u zich uitdrukkelijk ertoe verbindt ze te verdelen onder de apparaten in de CFS-regio.

Wanneer u de wijzigingen doorvoert, voert de NX-OS-software de volgende handelingen uit:

1. Past de wijzigingen in de actieve configuratie op de schakelaar toe.
2. Verdeelt de bijgewerkte gebruikersrolconfiguratie aan de andere switches in de CFS-regio.
3. Ontgrendel de gebruikersrolconfiguratie in de apparaten in de CFS-regio.
4. Hiermee wordt de CFS-sessie beëindigd.

Deze configuraties worden verdeeld:

- Rol- en beschrijvingen
- Lijst van regels voor de rollen

Configuratie- en weergave van opdrachten

	Opdracht aanvalsterrein	**doel**
Stap 1.	Voorbeeld: schakelaar**#configureer terminal**	Hiermee voert u de mondiale configuratiemodus in.
Stap 2.	schakelaar (totaal)# **achternaam** *naam* Voorbeeld: schakelaar (configuratie)**#rolnaam GebruikerA**	Specificeert een gebruikersrol en voert de rolconfiguratiemodus in.
Stap 3.	schakelaar (-rol)# **vlan - politiek ontkennen** Voorbeeld: schakelaar (-rol)**#vlan beleid ontkent**	Hiermee voert u de modus voor de configuratie van het VLAN-beleid in.
Stap 4.	schakelaar (-rol-VLAN)# **licentie VLAN**-VLAN-*id* Voorbeeld: schakelaar (-rol-VLAN)**#vergunning vlan 1**	Specificeert het VLAN dat de rol toegang kan hebben. Herhaal deze opdracht voor zoveel ventilatoren als nodig.
Stap 5.	**uitgang** Voorbeeld: schakelaar (-rol-VLAN)# **exit**	Sluit de rol VLAN beleidsconfiguratiemodus af.

Stap 6.	schakelaar (-rol)# **toonrol** Voorbeeld: schakelaar (-rol)# **show role**	(Optioneel) Hiermee geeft u de rolconfiguratie weer.
Stap 7.	**Toon rol {hangende | hangende-diff}** Voorbeeld: schakelaar (-rol)#**show rol in behandeling**	(Optioneel) Hier wordt de gebruikersrolconfiguratie weergegeven die in behandeling is
Stap 8.	**rol** Voorbeeld: schakelaar (-rol)#**role**	(Optioneel) past de configuratieveranderingen in de gebruikersrol in de tijdelijke database toe op de actieve configuratie en verdeelt de configuratie van de gebruikersrol naar andere switches als u CFS-configuratie voor de gebruikersrolfunctie hebt ingeschakeld.
Stap 9.	**kopie van het in werking stellen van de configuratie-configuratie** Voorbeeld: schakelaar# **kopie in werking stellen-configuratie**	(Optioneel) Kopieert de actieve configuratie naar de opstartconfiguratie.

Deze stappen maken de verdeling van de rolconfiguratie mogelijk:

	Opdracht	doel
Stap 1.	schakelaar# **configuratie t** schakelaar (totaal)#	Voert de configuratie in.
Stap 2.	schakelaar (configuratie)# **rol distribueren** schakelaar ()#**no rol distribueert**	Maakt rolconfiguratie distributie mogelijk. schakelt rolconfiguratie-distributie uit (standaard).

Deze stappen begaan rollconfiguratie wijzigingen:

	Opdracht	doel
Stap 1	Nexus# **t** Nexus (configuratie)#	Voert de configuratie in.
Stap 2	Nexus (configuratie)# **rol**	Voert de rolconfiguratie aan.

Deze stappen wijzen rolconfiguratie te veranderen:

	Opdracht	doel
Stap 1	Nexus# **t** Nexus (configuratie)#	Voert de configuratie in.
Stap 2	Nexus (configuratie)# **rol afbreken**	Hiermee wordt de rollconfiguratie gewijzigd en wordt de hangende configuratiedatabase gewist.

Voer een van deze taken uit om gebruikersaccount en RBAC-configuratieinformatie weer te geven:

Opdracht	doel
toonrol	Toont de gebruikersrolconfiguratie.
kenmerken	Toont de functielijst.
functiegroep tonen	Toont de configuratie van de functiegroep.

De gebruikersroldistributiesessie wissen

U kunt de bestaande distributiesessie voor Cisco Fabric Services (indien aanwezig) verwijderen en de stof voor de gebruikersfunctie ontgrendelen.

> **Voorzichtig:** Alle wijzigingen in de hangende database gaan verloren wanneer u deze opdracht geeft.

	Opdracht	doel
Stap 1	switch# **duidelijke rolsessie** **Voorbeeld:** schakelaar# duidelijke rolsessie	Verwijdert de sessie en ontgrendelt het weefsel.
Stap 2	**status van rolsessie tonen** **Voorbeeld:** schakelaar# de status van de rolsessie tonen	(Optioneel) Hier wordt de status van de gebruikersrol als CFS sessie weergegeven.

Configuratievoorbeeld

In dit voorbeeld gaan we een TAC voor gebruikersaccount maken met deze toegangsvergunning:

- Toegang tot een duidelijk bevel
- Toegang tot configuratieopdracht
- Toegang tot debug-opdracht
- Toegang tot exec-opdracht
- Toegang tot show opdracht
- Alleen toegang tot 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
```

Licentie-vereisten

Product	Licentievereiste
NX-OS	Voor gebruikersrekeningen en RBAC is geen licentie vereist.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.