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

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein Benutzer mithilfe von Role Base Access Control (RBAC) auf Nexus 5500-, Nexus 5600- und Nexus 6000-Switches zugreifen kann.

Mit RBAC können Sie die Regeln für eine zugewiesene Benutzerrolle definieren, um die Autorisierung eines Benutzers zu beschränken, der Zugriff auf die Switch-Managementvorgänge hat.

Sie können ein Benutzerkonto erstellen und verwalten und Rollen zuweisen, die den Zugriff auf Nexus 5500-, Nexus 5600- und Nexus 6000-Switches einschränken.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CLI-Konfigurationsbefehle für Nexus 5500, Nexus 5600, Nexus 6000 Switches
- Cisco Fabric Services (CFS)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Nexus 5500-, Nexus 5600- und Nexus 6000-Switches mit NXOS 5.2(1)N1(9) 7.3(1)N1(1).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Benutzeranforderungen

Dies sind einige Benutzeranforderungen, die erfüllt werden müssen:

- Nur Benutzer mit Netzwerkadministratorrolle können Rollen erstellen.
- Nur Benutzer mit Netzwerkadministratorrolle können die Ausgabe der **Rolle show** anzeigen.
- Auch wenn Benutzer alle Befehle zum Anzeigen ausführen dürfen, ist es ihnen nicht gestattet, die Ausgabe der **Show-Rolle** anzuzeigen, es sei denn, diesen Benutzern wird eine Netzwerkadmin-Rolle zugewiesen.
- Ein Benutzerkonto muss mindestens eine Benutzerrolle haben.

Benutzerrollen

Jede Rolle kann mehreren Benutzern zugewiesen werden, und jeder Benutzer kann Teil mehrerer Rollen sein.

Benutzer von Rolle A können beispielsweise Befehle zum Anzeigen ausgeben, und Benutzer von Rolle B können Konfigurationsänderungen vornehmen.

Wenn ein Benutzer sowohl Rolle A als auch Rolle B zugewiesen ist, kann dieser Benutzer den Befehl show ausgeben und Änderungen an der Konfiguration vornehmen.

Der Befehl "Zugriff zulassen" hat Vorrang vor dem Befehl "Zugriff verweigern".

Wenn Sie beispielsweise einer Rolle angehören, die den Zugriff auf Konfigurationsbefehle verweigert.

Wenn Sie jedoch auch einer Rolle angehören, die Zugriff auf Konfigurationsbefehle hat, haben Sie dann Zugriff auf Konfigurationsbefehle.

Es gibt fünf Standard-Benutzerrollen:

- network-admin - Vollständiger Lese- und Schreibzugriff auf den gesamten Switch.
- network-operator - Vollständiger Lesezugriff auf den gesamten Switch.
- vdc-admin - Lese- und Schreibzugriff, der auf einen VDC beschränkt ist
- vdc-operator - Lesezugriff beschränkt auf einen VDC
- san-admin - Vollständiger Lese- und Schreibzugriff für SAN-Administratoren.

Hinweis:Sie können Standardbenutzerrollen nicht ändern/löschen.

Hinweis: **Der** Befehl **show role** zeigt die auf dem Switch verfügbare Rolle an.

Regeln für die Benutzerrolle

Die Regel ist das Grundelement einer Rolle.

Eine Regel definiert, welche Operationen der Benutzer mithilfe dieser Rolle ausführen kann.

Sie können Regeln für die folgenden Parameter anwenden:

- Befehl: Ein Befehl oder eine Gruppe von Befehlen, die in einem regulären Ausdruck definiert sind.
- Feature - Befehle, die für eine von der NX-OS-Software bereitgestellte Funktion gelten.
- Funktionsgruppe: Standard- oder benutzerdefinierte Funktionsgruppe.

Diese Parameter erstellen eine hierarchische Beziehung. Der einfachste Steuerungsparameter ist der Befehl.

Der nächste Steuerungsparameter ist das Feature, das alle Befehle darstellt, die dem Feature zugeordnet sind.

Der letzte Steuerungsparameter ist die Funktionsgruppe. Die Funktionsgruppe kombiniert verwandte Funktionen und ermöglicht die einfache Verwaltung von Regeln.

Die vom Benutzer angegebene Regelnummer legt die Reihenfolge fest, in der die Regeln angewendet werden.

Die Regeln werden in absteigender Reihenfolge angewendet.

So wird beispielsweise Regel 1 vor Regel 2 angewendet, die vor Regel 3 angewendet wird usw.

Der Regelbefehl gibt Operationen an, die von einer bestimmten Rolle ausgeführt werden können. Jede Regel besteht aus einer Regelnummer, einem Regeltyp (Zulassen oder Ablehnen),

einen Befehlstyp (z. B. Konfiguration, show, exec, debug) und einen optionalen Funktionsnamen (z. B. FCOE, HSRP, VTP, Schnittstelle).

Rollenverteilung für Benutzer

Rollenbasierte Konfigurationen nutzen die Cisco Fabric Services (CFS)-Infrastruktur, um ein effizientes Datenbankmanagement zu ermöglichen und einen zentralen Konfigurationspunkt im Netzwerk bereitzustellen.

Wenn Sie die CFS-Verteilung für eine Funktion auf Ihrem Gerät aktivieren, gehört das Gerät zu einer CFS-Region, die andere Geräte im Netzwerk enthält, die Sie auch für die CFS-Verteilung für diese Funktion aktiviert haben. Die CFS-Verteilung für die Benutzerrollenfunktion ist standardmäßig deaktiviert.

Sie müssen CFS für Benutzerrollen auf jedem Gerät aktivieren, an das Sie Konfigurationsänderungen verteilen möchten.

Nachdem Sie die CFS-Verteilung für Benutzerrollen auf dem Switch aktiviert haben, veranlasst der erste von Ihnen eingegebene Befehl zur Konfiguration der Benutzerrolle die Switch-NX-OS-Software, die folgenden Schritte auszuführen:

1. Erstellt eine CFS-Sitzung auf dem Switch.
2. Sperrt die Benutzerrollenkonfiguration auf allen Switches in der CFS-Region, wobei CFS für die Benutzerrollenfunktion aktiviert ist.
3. Speichert die Änderungen der Benutzerrollenkonfiguration in einem temporären Puffer auf dem Switch.

Die Änderungen verbleiben im temporären Puffer auf dem Switch, bis Sie sie explizit auf die Geräte in der CFS-Region verteilen.

Wenn Sie die Änderungen übernehmen, ergreift die NX-OS-Software die folgenden Aktionen:

1. Änderungen werden auf die aktuelle Konfiguration des Switches angewendet.
2. Verteilt die aktualisierte Benutzerrollenkonfiguration auf die anderen Switches in der CFS-Region.
3. Entsperrt die Benutzerrollenkonfiguration auf den Geräten in der CFS-Region.
4. Beendet die CFS-Sitzung.

Diese Konfigurationen werden verteilt:

- Rollenbezeichnungen und -beschreibungen
- Regelliste für die Rollen

Konfiguration und Anzeigen von Befehlen

	Befehl	Zweck
	Terminal konfigurieren	
Schritt 1:	Beispiel: switch# **configure terminal** switch(config)#	Wechselt in den globalen Konfigurationsmodus.
	Name der Rolle *Rollenname*	
Schritt 2:	Beispiel: switch(config)# **Rollenname BenutzerA** switch(config-role)#	Gibt eine Benutzerrolle an und wechselt in den Rollenkonfigurationsmodus.
	VLAN-Richtlinie verweigern	
Schritt 3:	Beispiel: switch(config-role)# **VLAN-Richtlinienverweigerung** switch(config-role-vlan)#	Wechselt in den Konfigurationsmodus für die VLAN-Richtlinie.
	permit vlan vlan-*id*	
Schritt 4:	Beispiel: switch(config-role-vlan)# **permit vlan 1**	Gibt das VLAN an, auf das die Rolle zugreifen kann. Wiederholen Sie diesen Befehl für so viele VLANs wie erforderlich.
	Ausgang	
Schritt 5:	Beispiel: switch(config-role-vlan)# **exit** switch(config-role)#	Beendet den Konfigurationsmodus für die RollenvLAN-Richtlinie.
	Rolle anzeigen	
Schritt 6:	Beispiel: switch(config-role)# **show role**	(Optional) Zeigt die Rollenkonfiguration an.
Schritt	**Rolle anzeigen** {**ausstehend** |	(Optional) Zeigt die Benutzerrollenkonfiguration an, die für die

	ausstehend-diff}	
7:	Beispiel: switch(config-role)# **ausstehende Rolle anzeigen**	Verteilung aussteht.
Schritt 8:	**Rolle bestätigen** Beispiel: switch(config-role)# **Rolle commit**	(Optional) Wendet die Konfigurationsänderungen der Benutzerrolle in der temporären Datenbank auf die aktuelle Konfiguration an und verteilt die Benutzerrollenkonfiguration auf andere Switches, wenn Sie die CFS-Konfigurationsverteilung für die Benutzerrollenfunktion aktiviert haben.
Schritt 9:	**copy running-config startup-config** Beispiel: switch# **copy running-config startup-config**	(Optional) Kopiert die aktuelle Konfiguration in die Startkonfiguration.

Diese Schritte ermöglichen die Verteilung der Rollenkonfigurationen:

	Befehl	**Zweck**
Schritt 1:	switch# **config t** switch(config)#	Wechselt in den Konfigurationsmodus.
Schritt 2:	switch(config)# **role distribute**	Ermöglicht die Verteilung von Rollenkonfigurationen.
	switch(config)#**no role distribute**	Deaktiviert die Rollenkonfigurationsverteilung (Standard).

Diese Schritte bestätigen Änderungen der Rollenkonfiguration:

	Befehl	**Zweck**
Schritt 1	Nexus# **Konfiguration t** Nexus(config)#	Wechselt in den Konfigurationsmodus.
Schritt 2	Nexus(config)#-**Rollenbestätigung**	Führt die Rollenkonfigurationsänderungen durch.

In diesen Schritten werden Rollenkonfigurationsänderungen verworfen:

	Befehl	**Zweck**
Schritt 1	Nexus# **Konfiguration t** Nexus(config)#	Wechselt in den Konfigurationsmodus.
Schritt 2	Nexus(config)# **Rollenabbruch**	Verwirft die Rollenkonfigurationsänderungen und löscht die ausstehende Konfigurationsdatenbank.

So zeigen Sie Informationen zum Benutzerkonto und zur RBAC-Konfiguration an:

Befehl	**Zweck**
Rolle anzeigen	Zeigt die Benutzerrollenkonfiguration an.
Funktion anzeigen	Zeigt die Funktionsliste an.
Bereich "Rolle" anzeigen	Zeigt die Konfiguration der Funktionsgruppe an.

Löschen Sie die Benutzerrollen-Verteilungssitzung.

Sie können die laufende Cisco Fabric Services-Distribution-Session (sofern vorhanden) löschen und die Fabric für die Benutzerrollenfunktion entsperren.

> **Vorsicht**: Alle Änderungen in der ausstehenden Datenbank gehen verloren, wenn Sie diesen Befehl ausgeben.

	Befehl	Zweck
Schritt 1	switch# **clear role session** **Beispiel:** switch# clear role session	Löscht die Sitzung und entsperrt die Fabric.
Schritt 2	**Status der Rollensitzung anzeigen** **Beispiel:** Switch# Status der Rollensitzung anzeigen	(Optional) Zeigt den Status der CFS-Sitzung für die Benutzerrolle an.

Konfigurationsbeispiel

In diesem Beispiel erstellen wir ein Benutzerkonto TAC mit folgenden Zugriffsberechtigungen:

- Zugriff auf den Befehl clear
- Zugriff auf den Konfigurationsbefehl
- Zugriff auf den Befehl debug
- Zugriff auf den exec-Befehl
- Zugriff auf den Befehl show
- Nur Zugriff auf 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
```

Lizenzierungsanforderungen

Produkt	Lizenzanforderung
NX-OS	Benutzerkonten und RBAC erfordern keine Lizenz.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.