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

Sommario

Introduzione

In questo documento viene descritto come limitare l'accesso di un utente agli switch Nexus 5500, Nexus 5600 e Nexus 6000 tramite il controllo di accesso alla base dei ruoli (RBAC).

La funzione RBAC consente di definire le regole per un ruolo utente assegnato per limitare l'autorizzazione di un utente che ha accesso alle operazioni di gestione dello switch.

Èpossibile creare e gestire un account utente e assegnare ruoli che limitino l'accesso agli switch Nexus 5500, Nexus 5600 e Nexus 6000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comandi di configurazione CLI degli switch Nexus 5500, Nexus 5600, Nexus 6000
- Servizi fabric Cisco (CFS).

Componenti usati

Il riferimento delle informazioni contenute in questo documento è gli switch Nexus 5500, Nexus 5600 e Nexus 6000 con NXOS 5.2(1)N1(9) 7.3(1)N1(1).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Requisiti utente

Di seguito sono riportati alcuni requisiti utente che devono essere soddisfatti:

- Solo gli utenti con ruolo di amministratore di rete possono creare ruoli.
- Solo gli utenti con ruolo network-admin possono visualizzare l'output del **ruolo show**.
- Anche se agli utenti è consentito eseguire tutti i comandi show, non è consentito visualizzare l'output del **ruolo show**, a meno che a questi utenti non sia assegnato un ruolo di amministratore di rete.
- Un account utente deve avere almeno un ruolo utente.

Ruoli utente

Ogni ruolo può essere assegnato a più utenti e ogni utente può far parte di più ruoli.

Ad esempio, gli utenti del ruolo A possono eseguire comandi show e gli utenti del ruolo B possono apportare modifiche alla configurazione.

Se un utente è assegnato sia al ruolo A che al ruolo B, può eseguire il comando show e apportare modifiche alla configurazione.

Il comando Permit access ha la priorità sul comando deny access.

Ad esempio, se si appartiene a un ruolo che nega l'accesso ai comandi di configurazione.

Tuttavia, se si appartiene anche a un ruolo che ha accesso ai comandi di configurazione, si avrà accesso ai comandi di configurazione.

Sono disponibili cinque ruoli utente predefiniti:

- network-admin: accesso completo in lettura e scrittura all'intero switch.
- operatore di rete - Accesso in lettura completo all'intero switch.
- vdc-admin: accesso in lettura e scrittura limitato a un VDC
- operatore vdc - Accesso in lettura limitato a un VDC
- san-admin: accesso completo in lettura e scrittura agli amministratori SAN.

Nota: non è possibile modificare o eliminare i ruoli utente predefiniti.

Nota: il comando **show role** visualizzerà il ruolo disponibile sullo switch

Regole ruolo utente

La regola è l'elemento di base di un ruolo.

Una regola definisce le operazioni che il ruolo consente all'utente di eseguire.

Èpossibile applicare regole per i seguenti parametri:

- Comando: un comando o un gruppo di comandi definiti in un'espressione regolare.
- Funzionalità: comandi applicabili a una funzione fornita dal software NX-OS.
- Gruppo di feature: gruppo di feature predefinito o definito dall'utente.

Questi parametri creano una relazione gerarchica. Il parametro di controllo di base è il comando.

Il parametro di controllo successivo è la feature, che rappresenta tutti i comandi associati alla feature.

L'ultimo parametro di controllo è il gruppo di feature. Il gruppo di feature combina le feature correlate e consente di gestire facilmente le regole.

Il numero di regola specificato dall'utente determina l'ordine di applicazione delle regole.

Le regole vengono applicate in ordine decrescente.

Ad esempio, la regola 1 viene applicata prima della regola 2, che viene applicata prima della regola 3 e così via.

Il comando rule specifica le operazioni che possono essere eseguite da un ruolo specifico. Ogni regola è costituita da un numero di regola, un tipo di regola (autorizzazione o negazione),

un tipo di comando (ad esempio, configuration, show, exec, debug) e un nome di funzionalità facoltativo (ad esempio, FCOE, HSRP, VTP, interface).

Distribuzione ruoli utente

Le configurazioni basate sui ruoli utilizzano l'infrastruttura Cisco Fabric Services (CFS) per consentire una gestione efficiente del database e fornire un singolo punto di configurazione nella rete.

Quando si abilita la distribuzione CFS per una funzionalità nel dispositivo, il dispositivo appartiene a un'area CFS contenente altri dispositivi nella rete che sono stati abilitati anche per la distribuzione CFS per la funzionalità. La distribuzione di CFS per la funzionalità del ruolo utente è disabilitata per impostazione predefinita.

Ènecessario abilitare CFS per i ruoli utente su ciascun dispositivo a cui si desidera distribuire le modifiche di configurazione.

Dopo aver abilitato la distribuzione CFS per i ruoli utente sullo switch, il primo comando di configurazione del ruolo utente immesso determina l'esecuzione da parte del software NX-OS dello switch delle azioni seguenti:

1. Crea una sessione CFS sullo switch.
2. Blocca la configurazione del ruolo utente su tutti gli switch nell'area CFS con CFS abilitato per la funzionalità del ruolo utente.

3. Salva le modifiche alla configurazione del ruolo utente in un buffer temporaneo sullo switch.

Le modifiche rimangono nel buffer temporaneo sullo switch finché non vengono confermate esplicitamente per la distribuzione ai dispositivi nell'area CFS.

Quando si esegue il commit delle modifiche, il software NX-OS esegue le azioni seguenti:

1. Applica le modifiche alla configurazione in esecuzione sullo switch.
2. Distribuisce la configurazione aggiornata del ruolo utente agli altri switch dell'area CFS.
3. Sblocca la configurazione del ruolo utente nei dispositivi nell'area CFS.
4. Termina la sessione CFS.

Queste configurazioni sono distribuite:

- Nomi e descrizioni dei ruoli
- Elenco di regole per i ruoli

Comandi Configuration e Show

	Comando	Scopo
	configurare il terminale	
Passaggio 1.	Esempio: switch# **configure terminal**	Attiva la modalità di configurazione globale.
	switch(config)# **nome ruolo** *nome-ruolo*	
Passaggio 2.	Esempio: switch(config)# **nome ruolo UserA**	Specifica un ruolo utente ed entra nella modalità di configurazione del ruolo.
	switch(config-role)# **negazione criteri vlan**	
Passaggio 3.	Esempio: switch(config-role)#**vlan policy deny**	Entra nella modalità di configurazione dei criteri VLAN di ruolo.
	switch(config-role-vlan)# **allow vlan** vlan-*id*	
Passaggio 4.	Esempio: switch(config-role-vlan)# **allow vlan 1**	Specifica la vlan a cui può accedere il ruolo. Ripetere questo comando per tutte le vlan necessarie.
	esci	
Passaggio 5.	Esempio: switch(config-role-vlan) # **exit**	Esce dalla modalità di configurazione dei criteri VLAN di ruolo.
	switch(config-role)# **mostra ruolo**	
Passaggio 6.	Esempio: switch(config-role)# **show role**	(Facoltativo) Visualizza la configurazione del ruolo.
	show role {**pending** | **pending-diff**}	
Passaggio 7.	Esempio: switch(config-	(Facoltativo) Visualizza la configurazione del ruolo utente in attesa di distribuzione

	role)#**show role in sospeso**	
Passaggio 8.	**commit del ruolo** Esempio: switch(config-role)#**role commit**	(Facoltativo) Applica le modifiche della configurazione del ruolo utente nel database temporaneo alla configurazione in esecuzione e distribuisce la configurazione del ruolo utente ad altri switch se è stata abilitata la distribuzione della configurazione CFS per la funzionalità del ruolo utente.
Passaggio 9.	**copy running-config startup-config** Esempio: switch# **copy running-config startup-config**	(Facoltativo) Copia la configurazione in esecuzione nella configurazione di avvio.

I passaggi seguenti consentono la distribuzione della configurazione del ruolo:

	Comando	Scopo
Passaggio 1.	switch# **config** switch(config)#	Accede alla modalità di configurazione.
Passaggio 2.	switch(config)# **ruolo distribute**	Abilita la distribuzione della configurazione dei ruoli.
	switch(config)#**no role distribute**	Disabilita la distribuzione della configurazione dei ruoli (impostazi predefinita).

I passaggi seguenti eseguono il commit delle modifiche alla configurazione del ruolo:

	Comando	Scopo
Passaggio 1	Nexus# **config** Nexus(config)#	Accede alla modalità di configurazione.
Passaggio 2	**commit del ruolo** Nexus(config)#	Esegue il commit delle modifiche alla configurazione del ru

Queste operazioni annullano le modifiche alla configurazione del ruolo:

	Comando	Scopo
Passaggio 1	Nexus# **config** Nexus(config)#	Accede alla modalità di configurazione.
Passaggio 2	**Interruzione del ruolo** Nexus(config)#	Elimina le modifiche alla configurazione del ruolo e cancella il database di configurazione in sospeso.

Per visualizzare l'account utente e le informazioni di configurazione RBAC, eseguire una delle seguenti attività:

Comando	Scopo
mostra ruolo	Visualizza la configurazione del ruolo utente.
mostra funzionalità ruolo	Visualizza l'elenco delle feature.
show role feature-group	Visualizza la configurazione del gruppo di funzionalità.

Cancella la sessione di distribuzione ruoli utente

Èpossibile cancellare la sessione di distribuzione di Servizi fabric Cisco in corso (se presente) e sbloccare l'infrastruttura per la funzionalità del ruolo utente.

Attenzione: Se si utilizza questo comando, tutte le modifiche apportate al database in

sospeso andranno perse.

	Comando	Scopo
Passaggio 1	switch# **cancella sessione ruolo** **Esempio:** switch# cancella sessione ruolo	Cancella la sessione e sblocca l'infrastruttura.
Passaggio 2	**mostra stato sessione ruolo** **Esempio:** switch# mostra stato sessione ruolo	(Facoltativo) Visualizza lo stato della sessione CFS del ruo utente.

Esempio di configurazione

Nell'esempio seguente viene creato un TAC per l'account utente con le seguenti autorizzazioni di accesso:

- Accesso al comando clear
- Accesso al comando di configurazione
- Accesso al comando debug
- Accesso al comando exec
- Accesso al comando show
- Accesso solo alla 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
```

Requisiti delle licenze

Prodotto	Requisiti di licenza
NX-OS	Gli account utente e i requisiti RBAC non richiedono alcuna licenza.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.