# Esempio di integrazione di Nexus con ACS 5.2

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Dispositivo Nexus per autenticazione e autorizzazione con configurazione ACS 5.2 Configurazione ACS 5.x Verifica Informazioni correlate

## **Introduzione**

Questo documento offre un esempio di configurazione dell'autenticazione TACACS+ su uno switch Nexus. Per impostazione predefinita, se si configura lo switch Nexus per l'autenticazione tramite Access Control Server (ACS), viene assegnato automaticamente il ruolo di operatore di rete/operatore vdc, che consente l'accesso in sola lettura. Per essere assegnato al ruolo network-admin/vdc-admin, è necessario creare una shell su ACS 5.2. Questo documento descrive questo processo.

# **Prerequisiti**

### **Requisiti**

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Definire lo switch Nexus come client in ACS.
- Definire l'indirizzo IP e una chiave segreta condivisa identica su ACS e Nexus.

Nota: creare un checkpoint o un backup su Nexus prima di apportare modifiche.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ACS 5.2
- Nexus 5000, 5.2(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.

#### **Convenzioni**

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

### **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

### Dispositivo Nexus per autenticazione e autorizzazione con configurazione ACS 5.2

Attenersi alla seguente procedura:

1. Creare un utente locale sullo switch Nexus con privilegi completi per il fallback:

username admin privilege 15 password 0 cisco123!

2. Abilitare TACACS+, quindi fornire l'indirizzo IP del server TACACS+ (ACS):

feature tacacs+

tacacs-server host IP-ADDRESS key KEY

tacacs-server key KEY

tacacs-server directed-request

aaa group server tacacs+ ACS

**server** *IP-ADDRESS* 

**Nota:** la chiave deve corrispondere al segreto condiviso configurato nell'ACS per questo dispositivo Nexus.

3. Verificare la disponibilità del server TACACS:

#### test aaa group group-name username password

L'autenticazione di prova non deve riuscire con un messaggio di rifiuto dal server, poiché il server non è stato configurato. Questo messaggio di rifiuto conferma che il server TACACS+ è raggiungibile.

4. Configurare le autenticazioni di accesso:

```
aaa authentication login default group ACS
aaa authentication login console group ACS
aaa accounting default group ACS
aaa authentication login error-enable
aaa authorization commands default local
```

aaa authorization config-commands default local

Nota: Nexus utilizza l'autenticazione locale se il server di autenticazione non è raggiungibile.

### Configurazione ACS 5.x

Attenersi alla seguente procedura:

 Per creare un profilo shell, selezionare Elementi criteri > Autenticazione e autorizzazioni > Amministrazione dispositivi > Profili shell.

cisco Cisco Secure A	CS	acsadmin acs62 (Primary) Log Out About Help
» 💮 Ny Workspace	Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles	
+ 🎲 Network Resources	Shell Profiles	Showing 1-2 of 2 50 T per page Go
🖌 🎆 Users and Identity Stores		
+ 🔍 Pulicy Elements		
<ul> <li>Session Conditions</li> <li>Date and Time</li> </ul>	E NEXUS OS	
Custom	Permit Access	
Network Conditions     Authorization and Permissions     Network Access     Authorization Profiles     Device Administration     Sector Administration     Command Bets     Named Permission Objects     Access Policies     Monitoring and Reports     System Administration		

- 2. Immettere un nome per il profilo.
- 3. Nella scheda Attributi custom, immettere i seguenti valori:Attributo: cisco-av-pairRequisito: ObbligatorioValore: shell:roles\*"network-admin vdc-

<ul> <li>MyWorkspace</li> </ul>	Policy Elements > Authorizat	ion and Permissions > Device Ad	Ininistration > Shell Profiles > Edit: "NEXUS OS"	
<ul> <li>In Network Resources</li> <li>Users and Identity Stores</li> <li>Op Policy Demons</li> </ul>	General Common Common Tasks Adril	Tasks Custom Attributes butes Requirement	Value	
Session Conditions Date and Time Custom > Network Conditions Authorization and Permissions > Network Access Authorization Profiles > Device Administration	Nanually Entered			X
Command Sets	Atribute	Requirement	Value	
Named Permission Objects	cisco-av-pair	Mandatory	shell roles"network admin vdc-admin"	E
🔓 Access Policies				
Monitoring and Reports				
🧐 System Administration				
				-
	Add A Edit	Y Replace A Delete	1	
	Atribute:			
	Parious			

- 4. Inviare le modifiche per creare un ruolo basato su attributi per lo switch Nexus.
- 5. Creare una nuova regola di autorizzazione o modificare una regola esistente nel criterio di accesso corretto. Per impostazione predefinita, le richieste TACACS+ vengono elaborate dai criteri di accesso predefiniti di amministrazione dei dispositivi.
- Nell'area Condizioni (Conditions), selezionate le condizioni appropriate. Nell'area Risultati (Results), selezionate il profilo della shell del sistema operativo Nexus.

Wy Workspace Access Cisco Secure	e ACS - Mozilla Firefox 🛛 🕅	1
ha Network Resources	nes, Se https://192.168.26.52/acsadnin/Policy/InputAction.do	
3 Users and Identity Stores		
Policy Elements General	·	
Access Policies FD Name	Rule-1 Status: Enabled 💌 🛛	
Image: Services       Image: Services         Image: Service Selection Rules       Image: Service Selection Rules         Image: Service Service Admin       Image: Service Serv	The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	

7. Fare clic su OK.

# **Verifica**

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- show tacacs+: visualizza le statistiche di TACACS+.
- <u>show running-config tacacs+</u>: visualizza la configurazione di TACACS+ nella configurazione in esecuzione.
- <u>show startup-config tacacs+</u>: visualizza la configurazione TACACS+ nella configurazione di avvio.
- show tacacs-server: visualizza tutti i parametri configurati del server TACACS+.

### Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems