Esempio di integrazione di Nexus con ACS 5.2

Sommario

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 Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

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 strumento di ricerca dei comandi (solo utenti registrati).

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 hostIP-ADDRESS key KEY
   ```

   ```
   tacacs-server key KEY
   ```

   ```
   tacacs-server directed-request
   ```

   ```
   aaa group server tacacs+ ACS
   ```

   ```
   server IP-ADDRESS
   ```

   ```
   use-vrf management
   ```

```
source-interface mgmt0
```

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
```

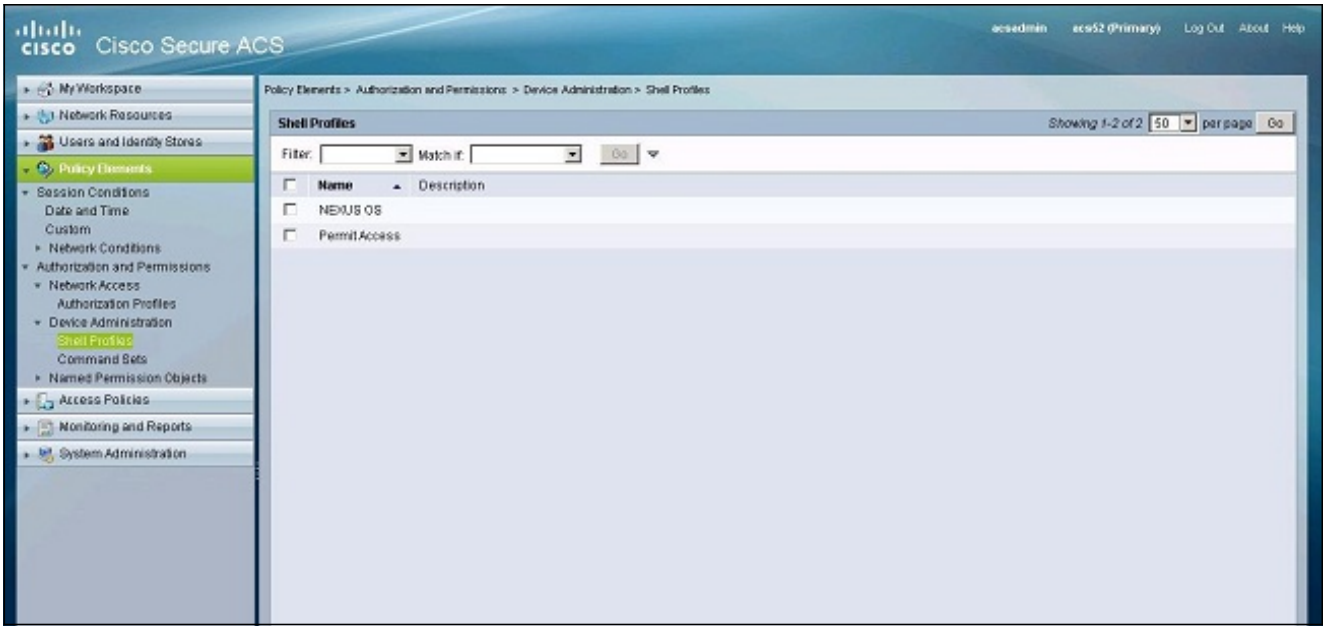
```
aaa authorization config-commands default local
```

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

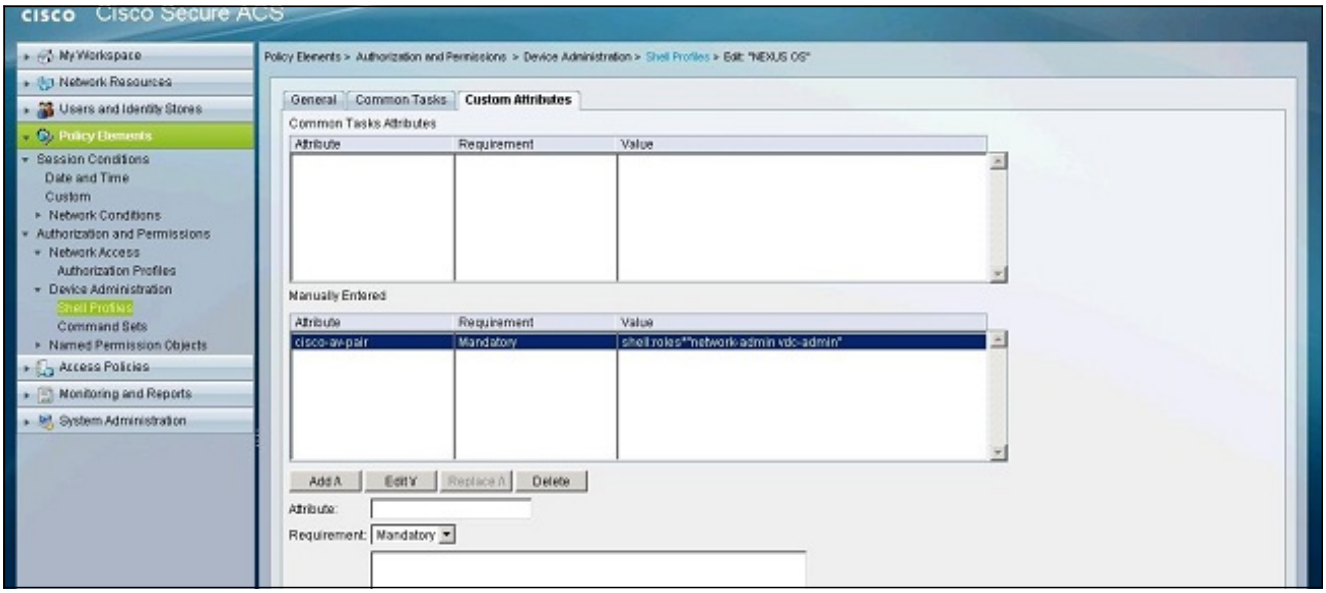
Configurazione ACS 5.x

Attenersi alla seguente procedura:

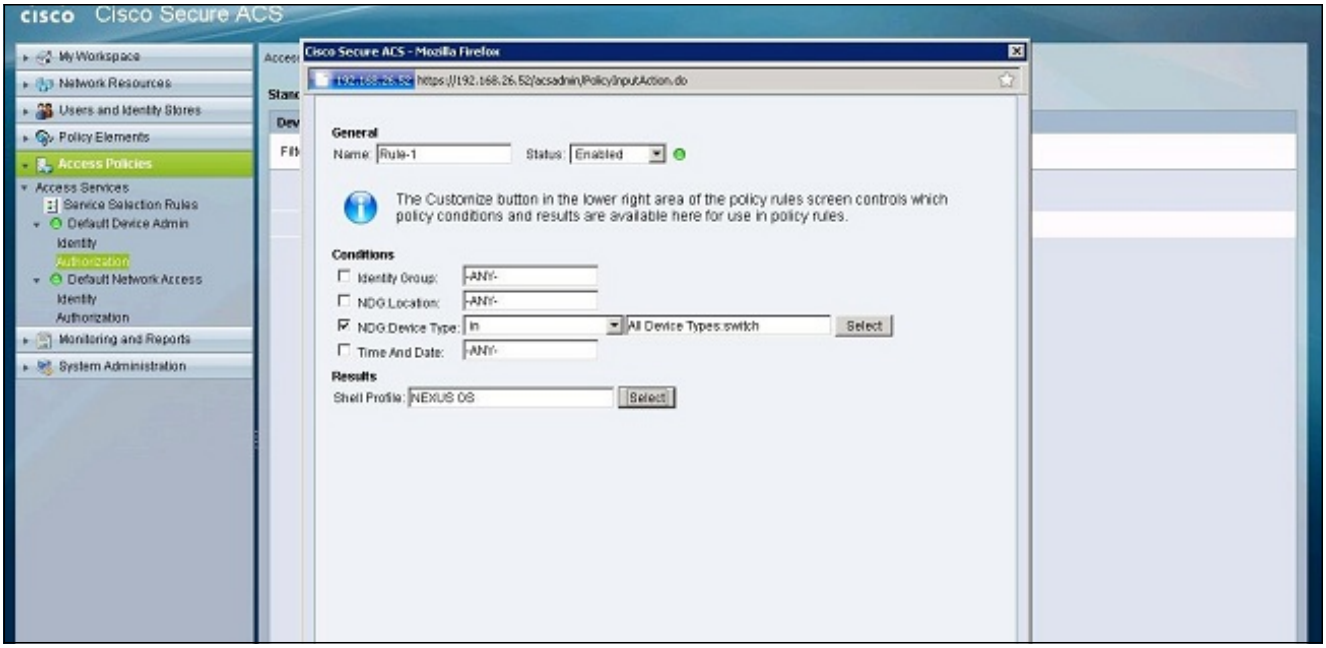
1. Per creare un profilo shell, selezionare **Elementi criteri > Autenticazione e autorizzazioni > Amministrazione dispositivi > Profili shell**.



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-admin"



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.
6. Nell'area Condizioni (Conditions), selezionate le condizioni appropriate. Nell'area Risultati (Results), selezionate il profilo della shell del sistema operativo Nexus.



7. Fare clic su **OK**.

Verifica

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

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

- **show tacacs+**: visualizza le statistiche di TACACS+.
- **show running-config tacacs+**: visualizza la configurazione di TACACS+ nella configurazione in esecuzione.
- **show startup-config tacacs+**: 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