Nexus Integration in ACS 5.2 - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält ein Beispiel für eine TACACS+-Authentifizierungskonfiguration auf einem Nexus-Switch. Wenn Sie den Nexus-Switch standardmäßig für die Authentifizierung über den Access Control Server (ACS) konfigurieren, werden Sie automatisch in die Rolle "Netzbetreiber/VDC-Operator" eingefügt, die einen schreibgeschützten Zugriff bereitstellt. Um in die Rolle "network-admin/vdc-admin" eingefügt zu werden, müssen Sie eine Shell auf ACS 5.2 erstellen. Dieses Dokument beschreibt diesen Prozess.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Definieren Sie Ihren Nexus-Switch als Client im ACS.
- Definieren Sie die IP-Adresse und einen identischen geheimen Schlüssel auf dem ACS und Nexus.

Hinweis: Erstellen Sie einen Prüfpunkt oder eine Sicherung auf Nexus, bevor Sie Änderungen vornehmen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ACS 5.2
- Nexus 5000, 5.2(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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Nexus-Gerät für Authentifizierung und Autorisierung mit ACS 5.2-Konfiguration

Gehen Sie wie folgt vor:

1. Erstellen Sie auf dem Nexus-Switch einen lokalen Benutzer mit vollen Berechtigungen für das Fallback:

```
username admin privilege 15 password 0 cisco123!
```

2. Aktivieren Sie TACACS+, und geben Sie dann die IP-Adresse des TACACS+-Servers (ACS) an:

```
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
```

Hinweis: Der Schlüssel muss mit dem auf dem ACS für dieses Nexus-Gerät konfigurierten gemeinsamen geheimen Schlüssel übereinstimmen.

3. Testen Sie die Verfügbarkeit des TACACS-Servers:

```
test aaa group group-name username password
```

Die Testauthentifizierung sollte mit einer Ablehnungsmeldung vom Server fehlschlagen, da der Server nicht konfiguriert wurde. Diese Ablehnungsmeldung bestätigt, dass der TACACS+-Server erreichbar ist.

4. Konfigurieren der Anmeldeauthentifizierung:

```
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
```

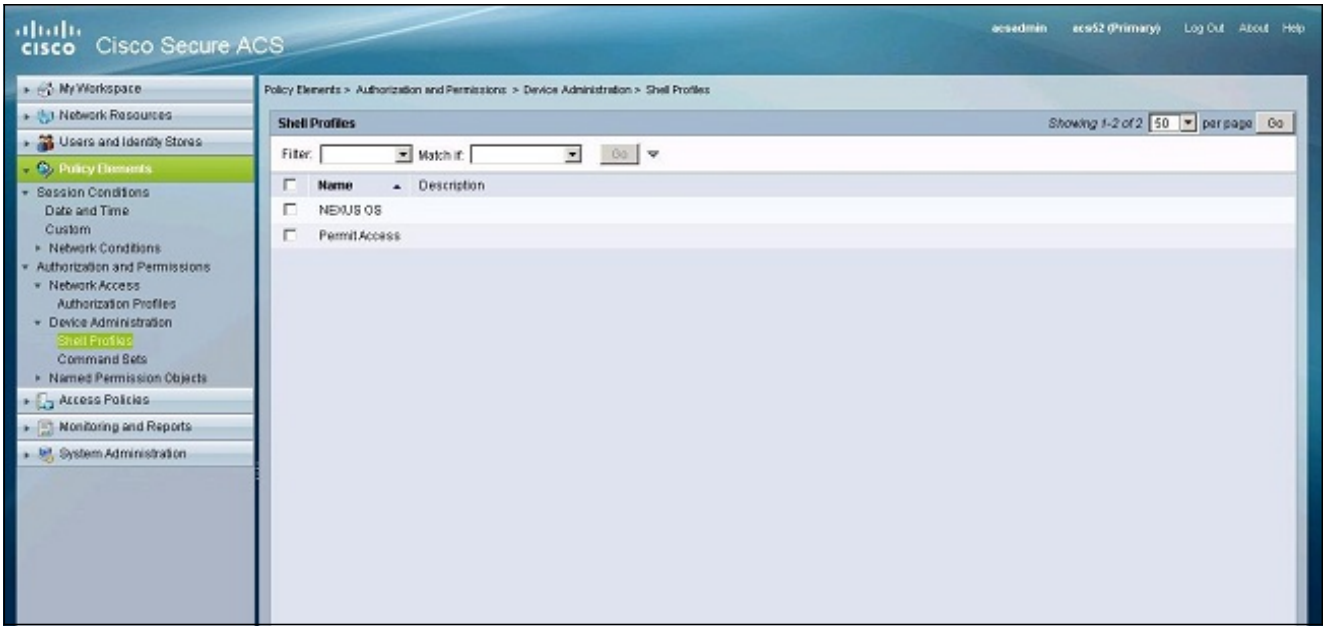
```
aaa authorization config-commands default local
```

Hinweis: Nexus verwendet die lokale Authentifizierung, wenn der Authentifizierungsserver nicht erreichbar ist.

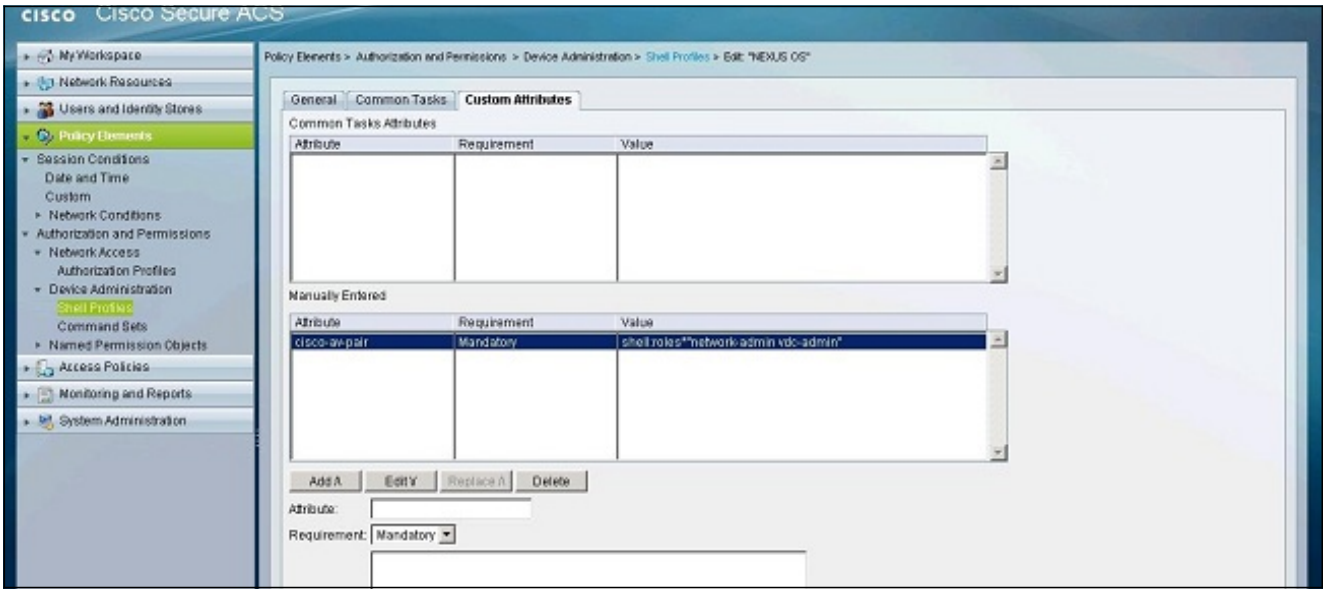
ACS 5.x-Konfiguration

Gehen Sie wie folgt vor:

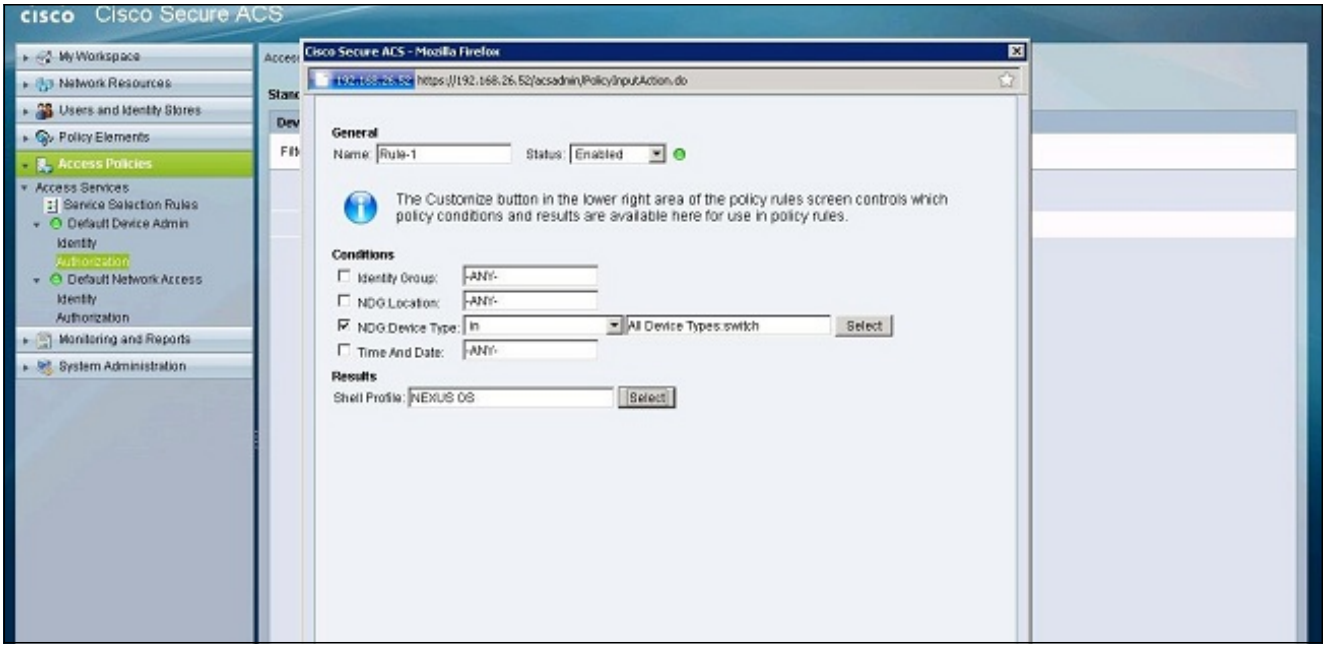
1. Navigieren Sie zu **Richtlinienelemente > Authentifizierung und Berechtigungen > Geräteverwaltung > Shell-Profile**, um ein Shell-Profil zu erstellen.



2. Geben Sie einen Namen für das Profil ein.
3. Geben Sie auf der Registerkarte Benutzerdefinierte Attribute die folgenden Werte ein:Attribut: cisco-av-pairAnforderung: ObligatorischWert: shell:roles*"network-admin vdc-admin"



4. Senden Sie die Änderungen, um eine attributbasierte Rolle für den Nexus-Switch zu erstellen.
5. Erstellen Sie eine neue Autorisierungsregel, oder bearbeiten Sie eine vorhandene Regel in der richtigen Zugriffsrichtlinie. In der Standardeinstellung werden TACACS+-Anforderungen von der Richtlinie für den Administrator-Standardzugriff für Geräte verarbeitet.
6. Wählen Sie im Bereich Bedingungen die entsprechenden Bedingungen aus. Wählen Sie im Bereich Ergebnisse das Nexus OS-Shell-Profil
   aus.



7. Klicken Sie auf **OK**.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show tacacs+:** Zeigt die TACACS+-Statistiken an.
- **show running-config tacacs+:** Zeigt die TACACS+-Konfiguration in der aktuellen Konfiguration an.
- **show startup-config tacacs+:** Zeigt die TACACS+-Konfiguration in der Startkonfiguration an.
- show tacacs-server: Zeigt alle konfigurierten TACACS+-Serverparameter an.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems