# Nexus與ACS 5.2的整合配置示例

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>設定</u> <u>使用ACS 5.2配置進行身份驗證和授權的Nexus裝置</u> <u>ACS 5.x配置</u> <u>驗證</u> <u>相關資訊</u>

## <u>簡介</u>

本檔案將提供Nexus交換器上TACACS+驗證組態範例。預設情況下,如果設定Nexus交換器以便透 過存取控制伺服器(ACS)進行驗證,則會自動將您置於network-operator/vdc-operator角色中,此角 色提供只讀存取。要成為network-admin/vdc-admin角色,您需要在ACS 5.2上建立一個shell。本文 檔介紹了該過程。

## <u>必要條件</u>

#### <u>需求</u>

嘗試此組態之前,請確保符合以下要求:

• 將Nexus交換機定義為ACS中的客戶端。

• 在ACS和Nexus上定義IP地址和相同的共用金鑰。

注意:在進行任何更改之前,在Nexus上建立檢查點或備份。

#### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

• ACS 5.2

• Nexus 5000,5.2(1)N1(1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

### 設定

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

使用ACS 5.2配置進行身份驗證和授權的Nexus裝置

請完成以下步驟:

- 1. 在Nexus交換機上建立具有完全回退許可權的本地使用者: username admin privilege 15 password 0 cisco123!
- 2. 啟用TACACS+,然後提供TACACS+伺服器(ACS)的IP地址:

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* 

use-vrf management

source-interface mgmt0

**注意:**金鑰必須與ACS上為此Nexus裝置配置的共用金鑰匹配。 3. 測試TACACS伺服器的可用性:

test aaa group group-name username password

由於尚未配置伺服器,測試身份驗證應會失敗,並顯示來自伺服器的拒絕消息。此拒絕消息確認TACACS+伺服器可訪問。

4. 配置登入身份驗證:

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

注意:如果身份驗證伺服器無法訪問,Nexus將使用本地身份驗證。

#### <u>ACS 5.x配置</u>

請完成以下步驟:

1. 導航到Policy Elements > Authentication and Permissions > Device Administration > Shell Profiles以建立外殼配置檔案。

cisco Cisco Secure A	ACS	aesaedmin acs52 (Primary) Log Cut About Hep
<ul> <li>St My Workspace</li> </ul>	Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles	
Interview Resources	Shell Profiles	Showing 1-2 of 2 50 T per page Go
B Users and identity Stores     Op Pulicy Demonts     Session Conditions     Date and Time	Filer: 💌 Match it: 💌 🚳 💌	
	Name      Description     NEXUS 05	
Custom • Network Conditions	PermitAccess	
Authorization and Permissions     Network Access     Authorization Profiles     Device Administration     Stret Profiles     Command Bets     Named Permission Objects		
Access Policies		
<ul> <li>Monitoring and Reports</li> <li>System Administration</li> </ul>		

- 2. 輸入配置檔案的名稱。
- 3. 在自定義屬性頁籤下,輸入以下值:屬性:cisco-av-pair需求:必填值:shell:角色

#### \*"network-admin vdc-

#### admin"

<ul> <li>MyWorkspace</li> </ul>	Policy Elements > Authoriza	tion and Permissions > Device Ac	Ininistration > Shell Profiles > Edit: "WEXUS OS"	
1 Network Resources	General Commo	n Tasks Custom Attributes	1	
a osers and roeme otores	Common Tasks Attr	butes		
<ul> <li>Policy Bements</li> </ul>	Atribute	Requirement	Value	
Session Conditions Date and Time Custom > Network Conditions Authorization and Permissions > Network Access Authorization Profiles				*
Device Administration     Shell Profiles	Nanually Entered			
Command Sets	Attribute	Requirement	Value	
Named Permission Objects	cisco-av-pair	Mandatory	shell roles" network admin vdc-admin"	-
🔓 Access Policies				
Monitoring and Reports				
M System Administration				
20 C) CI				
				<u>×</u>
	Add A Ed	W Replace A Delete		
	Atribute			

- 4. 提交更改,以便為Nexus交換機建立基於屬性的角色。
- 5. 在正確的訪問策略中建立新的授權規則或編輯現有規則。預設情況下,TACACS+請求由預設 裝置管理員訪問策略處理。
- 6. 在條件區域中,選擇適當的條件。在結果區域中,選擇Nexus OS外殼配置檔案。

- Caracteria - Caracteria		
Sp Network Resources	👔 🖬 🖬 Alexan San San San San San San San San San S	
3 Users and identity Stores		
Policy Elements	General	
🛼 Access Policies	Name: Rule-1 Status Enabled 💌 🛛	
Access Services El Sanice Salaction Rules Contact Device Admin Identity Information Contact Network Access Identity Authorization Manifering and Reports System Administration	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. Conditions   Identity Oroug: ANN-   NOG Device Type: All Device Types switch   Results   Shell Profile:   VEXUES OS   Betext:	

7. 按一下「OK」(確定)。



使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具(</u>僅供<u>已註冊</u>客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析 。

- show tacacs+ 顯示TACACS+統計資訊。
- show running-config tacacs+ 顯示運行配置中的TACACS+配置。
- show startup-config tacacs+ 顯示啟動配置中的TACACS+配置。
- <u>show tacacs-server</u> 顯示所有已配置的TACACS+伺服器引數。



• 技術支援與文件 - Cisco Systems