通過TACACS管理訪問恢復Firepower 4100/9300 FXOS本地使用者密碼

目錄

問題

Firepower 4100/9300裝置上FXOS的本地管理員密碼未知，需要重置以重新獲得管理訪問許可權。

所有現有TACACS使用者僅分配了只讀角色，這限制了他們在FXOS機箱上執行管理任務。

注意：預設情況下，遠端身份驗證使用者帳戶(LDAP、RADIUS、TACACS+、SSO)被分配只讀角色。

環境

- 執行ASA/FTD的Cisco Firepower 4100/9300
- FXOS預設身份驗證設定為遠端（思科ISE）；本地身份驗證配置為回退。

解析

建立管理TACACS使用者

在Cisco ISE（或您的TACACS伺服器）上，建立新的TACACS使用者(例如fxosadmin)並分配管理許可權，如思科文檔中所述：

使用TACACS+通過ISE進行遠端管理的FXOS機箱身份驗證/授權。

1. 建立身份組和使用者
2. 為每個使用者角色建立外殼配置檔案（對於「admin」角色，請使用cisco-av-pair=shell:roles="admin"）
3. 建立TACACS授權策略

使用新的TACACS管理員使用者登入

使用新建立的fxosadmin帳戶登入到FXOS GUI和CLI。此帳戶現在具有完全的管理許可權。

重置本地管理員密碼

訪問FXOS CLI並執行下列命令：

```
FP4100# scope security
FP4100 /security # show local-user
User Name       First Name      Last name
--------------- --------------- ---------
admin
FP4100 /security # enter local-user admin
FP4100 /security/local-user # set password
Enter a password:
Confirm the password:
FP4100 /security/local-user* # commit-buffer
FP4100 /security/local-user #
```

注意事項和注意事項

- 當遠端身份驗證(TACACS、RADIUS、LDAP、SSO)是預設方法時，除非遠端身份驗證不可用，否則無法使用本地使用者帳戶登入到防火牆機箱管理器。
- 當遠端身份驗證處於活動狀態時，本地和遠端使用者帳戶不能互換使用。
- 在此場景中，如果控制檯埠身份驗證方法設定為「LOCAL」，它允許驗證新的管理員憑據，否則您需要關閉遠端身份驗證伺服器連線以測試管理員憑據。

原因

- FXOS機箱的本地管理員密碼丟失或未知，導致無法使用本地帳戶進行直接管理訪問。
- 所有現有TACACS使用者帳戶均配置為只讀許可權，這限制了從遠端訪問執行必要管理任務（如機箱重新引導、升級、FXOS備份）的能力。
- 這種情況造成了在需要進一步更改或故障排除時無法管理或恢復裝置的風險。
- 這就需要重置管理員密碼以繼續計畫的維護活動。

相關內容

- FXOS使用者管理
- Firepower 9300/4100系列裝置的密碼恢復過程

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。