TACACS Administrative Accessを介したFirepower 4100/9300 FXOSローカルユーザパスワードの回復

内容

お問い合わせ内容

Firepower 4100/9300アプライアンスのFXOSのローカル管理者パスワードが不明なため、管理アクセスを回復するためにリセットする必要がありました。

既存のすべてのTACACSユーザには読み取り専用のロールだけが割り当てられ、FXOSシャーシでの管理タスクの実行が制限されていました。

注：リモートで認証されたユーザアカウント(LDAP、RADIUS、TACACS+、SSO)には、デフォルトで読み取り専用ロールが割り当てられます。

環境

- ASA/FTDを実行するCisco Firepower 4100/9300
- FXOSのデフォルト認証がリモート(Cisco ISE)に設定され、ローカル認証がフォールバックとして設定されている。

解決策

管理TACACSユーザの作成

Cisco ISE（またはTACACSサーバ）で、新しいTACACSユーザ(たとえば、fxosadmin)を作成し、シスコのドキュメントの説明に従って管理者権限を割り当てます。

TACACS+を使用したISEによるリモート管理用のFXOSシャーシ認証/認可。

1. アイデンティティグループとユーザの作成
2. 各ユーザロールのシェルプロファイルを作成します（「admin」ロールには、cisco-av-pair=shell:roles="admin"を使用します）。
3. TACACS認可ポリシーの作成

新しいTACACS Adminユーザを使用したログイン

新しく作成したfxosadminアカウントを使用して、FXOS GUIおよびCLIにログインします。 このアカウントには、完全な管理者権限があります。

ローカル管理者パスワードのリセット

FXOS CLIにアクセスし、次のコマンドを実行します。

```
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 #
```

注意事項と考慮事項

- リモート認証(TACACS、RADIUS、LDAP、SSO)がデフォルトの方式である場合、リモート認証が使用できない場合を除き、ローカルユーザアカウントを使用してFirewall Chassis Managerにログインすることはできません。
- リモート認証がアクティブな場合、ローカルとリモートのユーザーアカウントを同じ意味で使用することはできません。
- このシナリオでは、コンソールポートの認証方式が「LOCAL」に設定されている場合、新しい管理者クレデンシャルの検証が可能です。そうでない場合は、リモート認証サーバの接続をダウンさせて管理者クレデンシャルをテストする必要があります。

原因

- FXOSシャーシのローカル管理者パスワードが失われたか不明なため、ローカルアカウントを使用した直接管理アクセスができません。
- 既存のTACACSユーザアカウントはすべて読み取り専用権限で設定されているため、シャーシのリブート、アップグレード、FXOSのバックアップなどの必要な管理タスクをリモートアクセスから実行する機能が制限されていました。
- この状況により、さらなる変更やトラブルシューティングが必要な場合に、デバイスを管理または回復できないというリスクが生じました。
- このため、計画されたメンテナンス作業を続行するために管理者パスワードをリセットする必要がありました。

関連コンテンツ

- FXOSユーザ管理
- FirePOWER 9300/4100 シリーズ アプライアンスのパスワード回復手順

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。