

Firepower 4100/9300 FXOS - Wiederherstellung des lokalen Benutzerkennworts über TACACS Administrative Access

Inhalt

Problem

Das lokale Admin-Kennwort für FXOS auf Firepower 4100/9300-Appliances war unbekannt und musste zurückgesetzt werden, um wieder Administratorzugriff zu erhalten.

Allen vorhandenen TACACS-Benutzern wurde nur die Rolle "Read-Only" zugewiesen, wodurch sie keine administrativen Aufgaben auf dem FXOS-Chassis durchführen konnten.

Hinweis: Remote authentifizierten Benutzerkonten (LDAP, RADIUS, TACACS+, SSO) wird standardmäßig die Rolle "Schreibgeschützt" zugewiesen.

Umwelt

- Cisco Firepower 4100/9300 mit ASA/FTD
- FXOS-Standardauthentifizierung ist auf "remote" (Cisco ISE) festgelegt; lokale Authentifizierung ist als Fallback konfiguriert.

Auflösung

Erstellen eines administrativen TACACS-Benutzers

Erstellen Sie auf der Cisco ISE (oder Ihrem TACACS-Server) einen neuen TACACS-Benutzer (z. B. fxosadmin), und weisen Sie ihm die Administratorberechtigungen zu, wie in der Cisco-Dokumentation beschrieben:

[FXOS-Chassis-Authentifizierung/-Autorisierung für Remote-Management mit der ISE über TACACS+.](#)

1. Erstellen von Identitätsgruppen und Benutzern
2. Erstellen Sie das Shell-Profil für jede Benutzerrolle (verwenden Sie für die Rolle "admin" `cisco-av-pair=shell:roles="admin"`).
3. Erstellen der TACACS-Autorisierungsrichtlinie

Melden Sie sich mit dem neuen TACACS-Administrator-Benutzer an.

Verwenden Sie das neu erstellte fxosadmin-Konto, um sich bei der FXOS-GUI und -CLI anzumelden. Dieses Konto verfügt jetzt über vollständige Administratorberechtigungen.

Lokales Administratorkennwort zurücksetzen

Rufen Sie die FXOS-CLI auf, und führen Sie die folgenden Befehle aus:

```
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 #
```

Hinweise und Hinweise

- Wenn die Remote-Authentifizierung (TACACS, RADIUS, LDAP, SSO) die Standardmethode ist, können Sie sich mit einem lokalen Benutzerkonto nur dann beim Firewall Chassis Manager anmelden, wenn die Remote-Authentifizierung nicht verfügbar ist.
- Lokale und Remote-Benutzerkonten können nicht gleichzeitig verwendet werden, wenn die Remote-Authentifizierung aktiv ist.
- Wenn die Authentifizierungsmethode für den Konsolenport im Szenario auf "LOCAL" festgelegt ist, ermöglicht sie die Überprüfung der neuen Admin-Anmeldeinformationen. Andernfalls müssen Sie die Verbindung zum Remote-Authentifizierungsserver deaktivieren, um die Admin-Anmeldeinformationen zu testen.

Ursache

- Das lokale Administratorkennwort für das FXOS-Chassis ging verloren oder war unbekannt, wodurch ein direkter Administratorzugriff über das lokale Konto verhindert wurde.
- Alle vorhandenen TACACS-Benutzerkonten wurden mit Schreibschutzberechtigungen konfiguriert, wodurch die Möglichkeit eingeschränkt wurde, erforderliche Verwaltungsaufgaben wie Chassis-Neustart, Upgrades, FXOS-Backup vom Remote-Zugriff aus durchzuführen.
- Die Situation birgt das Risiko, dass das Gerät nicht verwaltet oder wiederhergestellt werden kann, wenn weitere Änderungen oder eine Fehlerbehebung erforderlich sind.
- Hierfür musste das Administratorkennwort zurückgesetzt werden, um mit den geplanten Wartungsarbeiten fortfahren zu können.

Verwandte Inhalte

- [FXOS-Benutzerverwaltung](#)
- [Verfahren zur Kennwortwiederherstellung für Firepower-Appliances der Serien 9300/4100](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.