

Firepower 4100/9300 FXOS Local User Password Recovery via TACACS-beheerderstoegang

Inhoud

uitgeven

Het lokale beheerderswachtwoord voor FXOS op Firepower 4100/9300-toestellen was onbekend en moest opnieuw worden ingesteld om beheerderstoegang te herwinnen.

Alle bestaande TACACS-gebruikers kregen alleen de alleen-lezen rol toegewezen, waardoor ze geen beheertaken op het FXOS-chassis konden uitvoeren.

Opmerking: op afstand geverifieerde gebruikersaccounts (LDAP, RADIUS, TACACS+, SSO) krijgen standaard de rol Alleen-lezen toegewezen.

milieu

- Cisco Firepower 4100/9300 met ASA/FTD
- Standaard FXOS-verificatie ingesteld op extern (Cisco ISE); lokale verificatie geconfigureerd als terugvalbeveiliging.

resolutie

Een TACACS-gebruiker voor beheerders maken

Maak op Cisco ISE (of uw TACACS-server) een nieuwe TACACS-gebruiker (bijvoorbeeld fosadmin) en wijs beheerdersbevoegdheden toe zoals beschreven in de Cisco-documentatie:

[FXOS-chassisverificatie/autorisatie voor extern beheer met ISE met behulp van TACACS+](#).

1. Identiteitsgroepen en gebruikers aanmaken
2. Maak het Shell-profiel aan voor elke gebruikersrol (gebruik `cisco-av-pair=shell:roles="admin"` voor de rol 'admin')
3. Het TACACS-autorisatiebeleid maken

Inloggen met de nieuwe TACACS-beheerdersgebruiker

Gebruik de nieuw gemaakte xosadmin-account om in te loggen op de FXOS GUI en CLI. Deze account heeft nu volledige beheerdersrechten.

Het wachtwoord van de lokale beheerder opnieuw instellen

Open de FXOS CLI en voer de volgende opdrachten uit:

```
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 #
```

Opmerkingen en overwegingen

- Als externe verificatie (TACACS, RADIUS, LDAP, SSO) de standaardmethode is, kunt u zich niet aanmelden bij Chassisbeheer van Firewall met een lokale gebruikersaccount, tenzij externe verificatie niet beschikbaar is.
- Lokale en externe gebruikersaccounts kunnen niet onderling worden verwisseld wanneer externe verificatie actief is.
- Als de verificatiemethode voor de consolepoort is ingesteld op 'LOKAAL', kunt u in het scenario de nieuwe beheerdersreferenties verifiëren, anders moet u de connectiviteit van de externe verificatieserver verlagen om de beheerdersreferenties te testen.

Oorzaak

- Het lokale beheerderswachtwoord voor het FXOS-chassis is verloren gegaan of onbekend, waardoor directe beheerderstoegang via de lokale account is voorkomen.
- Alle bestaande TACACS-gebruikersaccounts werden geconfigureerd met alleen-lezen-bevoegdheden, waardoor de mogelijkheid om noodzakelijke beheertaken uit te voeren, zoals het opnieuw opstarten van het chassis, upgrades, FXOS-back-up, vanaf externe toegang, werd beperkt.
- De situatie leidde tot het risico dat het apparaat niet kon worden beheerd of hersteld als verdere wijzigingen of probleemoplossing nodig waren.
- Dit vereiste een admin-wachtwoordreset om door te gaan met geplande onderhoudsactiviteiten.

Verwante inhoud

- [FXOS-gebruikersbeheer](#)
- [Wachtwoordherstelprocedure voor FirePower-toestellen uit de 9300/4100-reeks](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.