

Recupero della password dell'utente locale di Firepower 4100/9300 FXOS tramite TACACS Administrative Access

Sommario

Problema

La password dell'amministratore locale per FXOS sugli accessori Firepower 4100/9300 era sconosciuta e doveva essere reimpostata per riottenere l'accesso amministrativo.

A tutti gli utenti TACACS esistenti è stato assegnato solo il ruolo di sola lettura, che ha impedito loro di eseguire attività amministrative sullo chassis FXOS.

Nota: agli account utente autenticati in remoto (LDAP, RADIUS, TACACS+, SSO) viene assegnato per impostazione predefinita il ruolo di sola lettura.

Ambiente

- Cisco Firepower 4100/9300 con ASA/FTD
- Autenticazione predefinita FXOS impostata su remota (Cisco ISE); autenticazione locale configurata come fallback.

Risoluzione

Creare un utente TACACS amministrativo

Su Cisco ISE (o sul server TACACS in uso), creare un nuovo utente TACACS (ad esempio, fxosadmin) e assegnare i privilegi amministrativi come indicato nella documentazione di Cisco:

[Autenticazione/autorizzazione dello chassis FXOS per la gestione remota con ISE tramite TACACS+.](#)

1. Creare i gruppi di identità e gli utenti
2. Creare il profilo Shell per ogni ruolo utente (per il ruolo 'admin', utilizzare cisco-av-pair=shell:roles="admin")
3. Creare il criterio di autorizzazione TACACS

Effettua l'accesso con il nuovo utente amministratore TACACS

Usare l'account fxosadmin appena creato per accedere alla GUI e alla CLI di FXOS. Questo

account ora ha tutti i privilegi amministrativi.

Reimpostare la password dell'amministratore locale

Accedere alla CLI di FXOS ed eseguire questi comandi:

```
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 #
```

Note e considerazioni

- Quando l'autenticazione remota (TACACS, RADIUS, LDAP, SSO) è il metodo predefinito, non è possibile accedere a Gestione chassis firewall con un account utente locale a meno che l'autenticazione remota non sia disponibile.
- Gli account utente locali e remoti non possono essere utilizzati in modo intercambiabile quando è attiva l'autenticazione remota.
- Nello scenario, se il metodo di autenticazione della porta della console è impostato su 'LOCAL', consente la verifica delle nuove credenziali dell'amministratore. In caso contrario, è necessario disattivare la connettività del server di autenticazione remota per verificare le credenziali dell'amministratore.

Causa

- La password dell'amministratore locale per lo chassis FXOS è stata persa o sconosciuta, impedendo l'accesso amministrativo diretto tramite l'account locale.
- Tutti gli account utente TACACS esistenti erano configurati con privilegi di sola lettura, che limitavano la capacità di eseguire le attività amministrative necessarie, come il riavvio dello chassis, gli aggiornamenti, il backup FXOS, dall'accesso remoto.
- La situazione ha creato il rischio di non essere in grado di gestire o ripristinare il dispositivo se sono necessarie ulteriori modifiche o la risoluzione dei problemi.
- È stata necessaria una reimpostazione della password amministratore per procedere con le attività di manutenzione pianificate.

Contenuto correlato

- [Gestione utenti FXOS](#)

- [Procedura Di Recupero Della Password Per Gli Appliance Firepower Serie 9300/4100](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).