通过TACACS管理访问恢复Firepower 4100/9300 FXOS本地用户密码

目录

问题

Firepower 4100/9300设备上FXOS的本地管理员密码未知，需要重置以重新获得管理访问权限。

所有现有TACACS用户仅分配了只读角色，这限制他们在FXOS机箱上执行管理任务。

注意：默认情况下，远程身份验证用户帐户(LDAP、RADIUS、TACACS+、SSO)被分配只读角色。

环境

- 运行ASA/FTD的思科Firepower 4100/9300
- FXOS默认身份验证设置为远程（思科ISE）；本地身份验证配置为回退。

分辨率

创建管理TACACS用户

在Cisco ISE（或TACACS服务器）上，创建新的TACACS用户(例如fxosadmin)并分配管理权限，如思科文档中所述：

使用TACACS+通过ISE进行远程管理的FXOS机箱身份验证/授权。

1. 创建身份组和用户
2. 为每个用户角色创建外壳配置文件（对于“admin”角色，请使用cisco-av-pair=shell:roles="admin"）
3. 创建TACACS授权策略

使用新的TACACS管理员用户登录

使用新创建的fxosadmin帐户登录到FXOS GUI和CLI。此帐户现在具有完全的管理权限。

重置本地管理员密码

访问FXOS CLI并执行下列命令：

```
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 #
```

注意事项和注意事项

- 当远程身份验证(TACACS、RADIUS、LDAP、SSO)是默认方法时，除非远程身份验证不可用，否则无法使用本地用户帐户登录到防火墙机箱管理器。
- 当远程身份验证处于活动状态时，本地和远程用户帐户不能互换使用。
- 在这种情况下，如果控制台端口身份验证方法设置为“LOCAL”，则它允许验证新的管理员凭证，否则您需要关闭远程身份验证服务器连接以测试管理员凭证。

原因

- FXOS机箱的本地管理员密码丢失或未知，导致无法使用本地帐户直接管理访问。
- 所有现有TACACS用户帐户均配置为只读权限，这限制了从远程访问执行必要的管理任务（如机箱重启、升级、FXOS备份）的能力。
- 这种情况造成了在需要进一步更改或故障排除时无法管理或恢复设备的风险。
- 这需要重置管理员密码才能继续计划的维护活动。

相关内容

- FXOS用户管理
- Firepower 9300/4100系列设备的密码恢复过程

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。