保护基于角色的访问控制

系统为用户角色分配了权限，用于定义用户可以在系统上执行的操作。系统包含以下用户角色：

管理员

完成对整个系统的读写访问。默认情况下，此角色分配给默认的管理员帐户，并且不能对其进行更改。

只读

对系统配置进行只读访问，但无权修改系统状态。

运营

对NTP配置、用于智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。

AAA 管理员

对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。

通过 FXOS 机箱管理器 Web 界面或 FXOS CLI，您可以为系统中的每个用户帐户配置以下设置：

- User Role - 表示要分配给用户帐户的权限的角色。

  所有用户均默认分配了 Read-Only 角色，并且此角色无法取消选择。要分配多个角色，请按住 **Ctrl** 键并单击所需的角色。

- Account Expiration Date
- Account Status - 如果状态设置为**活动**，用户可以使用其登录 ID 和密码登录到 Firepower 机箱管理器和 FXOS CLI。

为了让经过本地身份验证的帐户获得最高的安全性，请为加密会话配置 SSH。

- 密码管理，第 2 页
- 强化经过本地身份验证的用户帐户，第 2 页
- 强化经过远程身份验证的用户帐户，第 2 页

密码管理

密码控制对资源或设备的访问，管理员定义密码以验证请求。当 FXOS 收到访问资源或设备的请求时，系统会质询请求并验证密码和身份，然后根据结果授予、拒绝或限制访问权限。最佳安全时间要求使用 LDAP、TACACS+ 或 RADIUS 身份验证服务器管理密码。但是，如果 LDAP、TACACS+ 或 RADIUS 服务出现问题，仍然需要本地配置的访问密码。设备还可以在其配置中包含其他密码信息，例如 NTP 密钥或 SNMP 社区字符串。

强化经过本地身份验证的用户帐户

配置单个内部用户角色时，管理员帐户用户可以使用以下设置通过 Web 界面登录机制强化系统以抵御攻击：

- 设置允许用户尝试登录的最大失败次数，如果超过该次数，用户会被锁定一段指定的时间 (**set max-login-attempts**)
- 设置在超出最大尝试登录次数后用户应被系统锁定的时间 (**set user-account-unlock-time**)
- 实施最小密码长度 (**set min-password-length**)
- 指定经过本地身份验证的用户在更改新建密码之前必须等待的最少小时数 (**set no-change-interval**)
- 设置本地用户帐户有效的天数 (**set expiration**)
- 需要强密码 (**set enforce-strong-password yes**)
- 分配仅适用于用户所需访问类型的用户访问权限 (**create role**)

强化经过远程身份验证的用户帐户

远程身份验证的用户账户是指任何通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的用户账户。远程身份验证最多允许 16 个 TACACS+ 服务器、16 个 RADIUS 服务器和 16 个 LDAP 提供程序，共计 48 个提供程序。

AAA 是一组服务，用于控制对计算机资源的访问、实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

请注意，如果用户同时持有本地用户帐户和远程用户帐户，则在本地用户帐户中定义的角色将覆盖在远程用户帐户中持有的角色。

TACACS+ 是 FXOS 机箱可用来对远程 AAA 服务器进行管理用户身份验证的身份验证协议。这些管理用户可以通过 SSH、HTTPS、telnet 或 HTTP 访问 FXOS 机箱。我们建议使用 SSH 以便在访问 FXOS 机箱时获得最大的安全性。许多身份验证方法提供增强的安全性。

TACACS+ 验证（或者更通用的 AAA 身份验证）使得每个网络管理员可以使用一个用户帐户。当您不依赖单个共享的密码时，网络的安全性会得到改善，您的问责制度也会得到加强。

RADIUS 是用途与 TACACS+ 类似的协议；但是，其仅加密网络中发送的密码。相反，TACACS+ 则为整个 TCP 负载（包括用户名和密码）加密。因此，我们建议您在 AAA 服务器支持 TACACS+ 时，优先使用 TACACS+。

LDAP 是用于访问目录服务的客户端-服务器协议，例如 Microsoft Active Directory。LDAP 对于客户端与服务器之间的安全性没有要求。但是，如果使用 SSL，LDAP 可以将客户端与服务器之间的用户会话加密。这样可保证在网络上的 LDAP 事务中传输的所有信息安全。因此，我们强烈建议您优先使用 LDAP 而非 TLS。

有关如何在 FXOS 机箱上配置 RADIUS、TACAS+ 和 LDAP 的详细信息和详细程序，请参阅《思科 *FIREPOWER 4100/9300 FXOS CLI* 配置指南》中“平台设置”一章的配置 AAA 部分。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。