重置Firepower系统上管理员用户的密码

目录

简介

背景信息

Firepower 威胁防御：重置管理员密码

ASA FirePOWER 服务模块：重置管理员密码

- 在ASA 5512-X至ASA 5555-X和ASA 5506-X至ASA 5516-X（软件ASA Firepower模块）和ISA 3000设备上重置管理员密码
- 重置ASA 5585-X系列设备（硬件ASA Firepower模块）上的管理员密码

更改FMC和NGIPSv的CLI或外壳管理密码

更改FMC的Web界面管理员密码或7000和8000系列设备的Web界面管理员和CLI管理员密码

为FMC或NGIPSv重置丢失的CLI或外壳管理密码，或为7000和8000系列设备重置丢失的Web界面或CLI密码

- 选项1.安全地重新启动设备并在启动时进入单用户模式以重置密码
- 选项2.使用外部身份验证获得CLI访问权限以重置Firepower管理中心的密码

重置Firepower管理中心丢失的Web界面管理员密码

简介

本文档介绍重置Firepower系统管理员帐户密码的说明。

注意：使用默认凭证Admin/admin123登录Firepower系统，验证密码重置是否成功。

背景信息

Firepower管理中心(FMC)为CLI外壳和Web界面分别维护管理员帐户和密码。受管设备(例如Firepower和自适应安全设备(ASA)Firepower服务)使用单个管理员帐户进行CLI、外壳和网络界面访问。

注意：对Firepower管理中心CLI的引用仅适用于版本6.3+，而7000和8000系列设备在版本6.4中受支持。

Firepower 威胁防御：重置管理员密码

要重置Firepower 9300和4100平台上Firepower威胁防御(FTD)逻辑设备的丢失管理员密码，请执行通过FXOS机箱管理器更改或恢复FTD密码指南中的说明。

对于Firepower 1000/2100/3100上运行的FTD设备，必须重新映像该设备。有关这些平台上的重新映像程序，请参阅运行Firepower威胁防御的Firepower 1000/2100系列的Cisco FXOS故障排除指南。

对于ASA 5500-X和集成安全设备(ISA)3000型号上运行的FTD设备，必须重新映像设备。有关说明，请参阅Cisco ASA和Firepower威胁防御设备重新映像指南。

对于虚拟FTD设备，您必须使用新部署替换设备。

重新映像物理设备会清除其配置并将管理员密码重置为**Admin123**。

除了在Amazon Web Services(AWS)上使用Firepower 7.0+的FTDv外，新的FTDv部署没有配置，并且管理员密码为**Admin123**FTDv。对于在AWS上使用Firepower 7.0+的FTD，新部署没有配置，也没有默认密码；您在部署时提供管理员密码。

- 如果重新映像使用 Firepower 设备管理器管理的 FTD 设备，有以下选项可供选择：
  - 如果您有最近外部存储的备份，则可以在重新映像后恢复备份配置。有关详细信息，请参阅适用于您的版本的Cisco Firepower设备管理器的Cisco Firepower威胁防御配置指南。
  - 如果没有备份，您必须手动重新创建设备配置，包括接口、路由策略以及DHCP和动态域名系统(DDNS)设置。
- 如果重新映像由Firepower管理中心管理的FTD设备，以及FMC和运行版本6.3+的设备，则可以在重新映像之前使用FMC Web界面备份设备配置，并在重新映像之后恢复备份。有关详细信息，请参阅版本的《Firepower管理中心配置指南》。

注意：如果运行v6.0.1 - 6.2.3，则无法备份FTD配置。如果您运行v6.3.0 - 6.6.0，并从FMC Web界面备份和恢复，则不支持FTD容器实例。虽然可以在重新映像后从Firepower管理中心应用共享策略，但必须手动配置任何特定于设备的设置，例如接口、路由策略、DHCP和DDNS设置。

ASA FirePOWER 服务模块：重置管理员密码

您可以使用ASA常规操作CLI的session命令重置ASA Firepower模块CLI的管理密码。如果丢失了ASA CLI的密码，则可以按照CLI手册1:思科 ASA 系列常规操作 CLI 配置指南》 中的说明恢复密码。

在ASA 5512-X至ASA 5555-X和ASA 5506-X至ASA 5516-X（软件ASA Firepower模块）和ISA 3000设备上重置管理员密码

要将ASA Firepower软件模块或ISA 3000设备的管理员用户重置为默认密码，请在ASA提示符下输入以下命令：session sfr do password-reset

有关详细信息，请参阅Cisco ASA系列CLI手册2:思科 ASA 系列防火墙 CLI 配置指南》。

重置ASA 5585-X系列设备（硬件ASA Firepower模块）上的管理员密码

要将 ASA FirePOWER 硬件模块的 admin 用户重置为默认密码，请在 ASA 提示符下输入以下命令：session 1 do password-reset

有关详细信息，请参阅Cisco ASA系列CLI手册2:思科 ASA 系列防火墙 CLI 配置指南》。

更改FMC和NGIPSv的CLI或外壳管理密码

使用以下说明重置这些管理员帐户的已知密码：

- Firepower 管理中心：用于访问CLI或外壳的管理密码。
- 下一代信息保存系统虚拟(NGIPSv:用于访问CLI的管理员密码。

步骤:

1. 通过SSH或控制台登录设备管理员帐户。
    - 对于Firepower管理中心：
        - 如果您的Firepower管理中心运行Firepower v6.2或更低版本，则登录会让您直接访问Linux外壳。
        - 如果您的Firepower管理中心运行Firepower v6.3或6.4，并且Firepower管理中心CLI未启用，则登录会让您直接访问Linux外壳。
        - 如果您的Firepower管理中心运行Firepower v6.3或6.4，并且启用了Firepower管理CLI，则登录会让您直接访问Firepower管理中心CLI。输入expert命令访问Linux shell。
        - 如果您的Firepower管理中心运行Firepower v6.5+，则登录会让您直接访问Firepower管理中心CLI。输入expert命令访问Linux shell。
    - 对于受管设备，通过登录可以访问CLI。输入expert命令访问Linux shell。
2. 在外壳提示符下，输入以下命令：sudo passwd admin。
3. 出现提示时，输入当前管理员密码以提升根访问权限。
4. 为响应提示，输入两次新的管理密码。

注意：如果系统显示消息BAD PASSWORD，则此信息仅供参考。即使出现此消息，系统也会应用您提供的密码。但是，出于安全原因，思科建议您使用更复杂的密码。

1. 键入exit退出外壳。
2. 在受管设备或启用CLI的Firepower管理中心上，键入exit以退出CLI。

更改FMC的Web界面管理员密码或7000和8000系列设备的Web界面管理员和CLI管理员密码

使用以下说明重置这些管理员帐户的已知密码：

- Firepower 管理中心：用于访问Web界面的管理员密码。
- 7000 和 8000 系列设备：用于访问Web界面和CLI的管理密码。

步骤:

1. 以具有管理员访问权限的用户身份登录设备的网络界面。
2. 选择System > Users，然后点击管理员用户的Edit图标。
3. 为Password和Confirm Password字段输入值。
   值必须相同，并且必须与为用户设置的密码选项一致。
4. Click Save.

为FMC或NGIPSv重置丢失的CLI或外壳管理密码，或为7000和8000系列设备重置丢失的Web界面或CLI密码

使用以下说明重置这些管理员帐户的丢失密码：

- Firepower 管理中心：用于访问CLI或外壳的管理密码。
- 7000 和 8000 系列设备：用于访问Web界面和CLI的管理密码。
- NGIPSv:用于访问CLI的管理员密码。

注意：要重置这些管理员帐户丢失的密码，您必须与设备建立控制台或SSH连接（如果配置了外部用户的Firepower管理中心，您可以使用SSH连接）。 您还必须重新启动其管理员凭据已丢失的设备。您可以根据可用的设备访问类型以不同方式启动重新启动：
·对于Firepower管理中心，您必须拥有具有管理员访问权限的Web界面用户的登录凭证，或具有具有CLI/外壳访问权限的外部身份验证用户的登录凭证。
·对于7000或8000系列设备，必须具有具有管理员访问权限的Web界面用户、具有配置访问权

限的CLI用户或在托管Firepower管理中心具有管理员访问权限的用户的登录凭证。
·对于NGIPSv，您必须拥有具有配置访问权限的CLI用户或具有托管Firepower管理中心管理员访问权限的用户的登录凭证。
·对于Firepower管理中心、7000和8000系列设备以及NGIPSv设备，如果您有控制台连接（物理或远程），则无需登录凭证即可执行此任务。

如果无法使用下列方法之一访问设备，则无法使用以下说明重置管理员密码；请联系思科TAC。

选项1.安全地重新启动设备并在启动时进入单用户模式以重置密码

1. 为丢失 admin 密码的设备打开与设备控制台的连接：
   ·对于7000/8000系列设备和Firepower管理中心，请使用键盘/显示器或串行连接。
   ·对于虚拟设备，请使用虚拟平台提供的控制台。有关详细信息，请参阅Cisco Firepower管理中心虚拟入门指南或适用于VMware的Cisco Firepower NGIPSv快速入门指南。
   ·或者，对于Firepower管理中心、7000/8000系列和虚拟设备，如果您使用远程键盘视频/鼠标(KVM)与设备建立了控制台连接，则可以访问该界面。
2. 重新启动丢失管理员密码的设备，您有以下选择：
   ·对于Firepower管理中心：
   a.以具有管理员访问权限的用户身份登录Firepower管理中心的网络界面。
   b.按照您的版本的Firepower管理中心配置指南中的说明重新启动Firepower管理中心。

   ·对于7000或8000系列设备或NGIPSv，如果您拥有在托管Firepower管理中心具有管理员访问权限的Web界面用户的凭证：
   a.以具有管理员访问权限的用户身份登录到托管Firepower管理中心的网络界面。
   b.按照您的版本的Firepower管理中心配置指南中所述，关闭并重新启动受管设备。

   ·对于7000或8000系列设备，如果您拥有具有管理员访问权限的Web界面用户的凭证：
   a.以具有管理员访问权限的用户身份登录设备的Web界面。
   b.按照您的版本的Firepower管理中心配置指南中的说明重新启动设备。

   ·对于7000或8000系列设备或NGIPSv，如果您拥有具有配置访问权限的CLI用户的凭证：
   a.通过具有CLI配置访问权限的用户名使用shell登录到设备。
   b.在提示符下，输入system reboot命令。

·对于具有控制台的Firepower管理中心、7000和8000系列以及虚拟设备，如果您使用远程KVM，请按CTRL-ALT-DEL (i**CTRL-ALT-DEL**键，KVM界面提供了一种向设备发送消息的方式，不会干扰KVM本身)。

注意：当您重新启动Firepower管理中心或受管设备时，这会将您从设备注销，并且系统会

运行数据库检查，完成检查最多可能需要一个小时。

⚠ 警告：请勿使用电源按钮关闭设备或拔下电源线；它可能会损坏系统数据库。使用Web界面完全关闭设备。

3.在设备控制台显示时，观察重新启动过程并根据重新启动的设备类型继续操作：

✎ 注意：如果系统正在进行数据库检查，您可以看到以下消息："系统尚未运行。正在检查和修复数据库。这可能需要很长时间才能完成。"

·对于型号750、1500、2000、3500或4000的Firepower管理中心，或者对于Firepower 7000或8000系列设备或NGIPSv，中断重新启动过程：
a.设备开始启动后，按键盘上的任意键取消LILO启动菜单上的倒计时。
b.在LILO引导菜单中显示的版本号。在本示例中，版本号为7.4.1



c.在boot提示符下，键入"command_version single"，其中版本是版本号(例如"7.4.1 single")。 如果系统启用了United Capabilities Approved Products List(UCAPL)compliance，系统会提示您输入密码；输入密码Sourcefire。

·对于Firepower管理中心型号1000、1600、2500、2600、4500或4600:

- 出现启动菜单时，选择选项4, Cisco Firepower管理控制台密码恢复模式。

4.分配新的管理员密码；使用适用于您的设备的说明：

·对于Firepower管理中心或NGIPSv的新CLI和外壳管理密码：

a.当系统显示以井号(#)结尾的操作系统提示符时，请输入以下命令：
passwd admin。

b.在提示时输入新的管理员密码（两次）。

注意：如果系统显示消息BAD PASSWORD，则此信息仅供参考。即使出现此消息，系统也会应用您提供的密码。但是，出于安全原因，建议您使用更复杂的密码。

·对于7000和8000系列设备的新Web和CLI管理员密码：

·在操作系统提示符后以井号(#)结束，输入以下命令：

usertool.pl -p '管理员密码'

·其中密码是新的管理员密码。

5.如果管理员帐户由于登录尝试失败次数过多而被锁定，您必须解锁该帐户。使用适用于您的设备的说明：

·要在Firepower管理中心或NGIPSv上解锁CLI和外壳管理帐户，请在操作系统提示符后输入以下命令，以井号(#)结尾：

pam_tally —user admin —reset

·要解锁7000和8000系列设备上的Web和CLI管理员帐户，请在操作系统提示符后输入此命令，以井号(#)结尾：

usertool.pl -u admin

6.在操作系统提示符后以井号(#)结束，输入reboot命令。

7.允许重新启动过程完成。

选项2.使用外部身份验证获得CLI访问权限以重置Firepower管理中心的密码

如果您仍能使用具有管理员访问权限的帐户访问FMC Web界面，则可以使用外部身份验证功能来访问CLI。此方法允许您登录FMC的CLI，访问Linux外壳，提升到根目录，以及手动重置CLI/外壳管理密码。此选项不需要重启或访问控制台。此选项要求您在要重置管理员密码的Firepower管理中心上正确配置了外部身份验证（使用SSH访问）(有关说明，请查看您的版本的Firepower管理中心配置指南)。 完成此配置后，请完成以下步骤：

1. 使用外部身份验证的帐户登录Firepower管理中心，该帐户使用SSH或控制台具有CLI/外壳访问权限：
   ·如果您的FMC运行v6.2或更低版本，则您可以直接访问Linux外壳。
   ·如果您的FMC运行v6.3或6.4且未启用FMC CLI，则您可以直接访问Linux外壳。
   ·如果您的FMC运行v6.3或6.4且启用了Firepower管理中心CLI，则您可以访问Firepower管理中心CLI。输入expert命令访问Linux外壳。
   ·如果您的FMC运行v6.5+，则您可以访问Firepower管理中心CLI。输入expert命令访问Linux外壳。
2. 在带美元符号($)的shell提示符下，运行此命令以重置管理员用户的CLI密码：
   sudo passwd admin
3. 在Password提示符下，输入您当前登录时所用用户名的密码。
4. 在提示时输入新的管理员密码（两次）。

注意：如果系统显示 BAD PASSWORD（密码错误）消息，此信息仅供参考。即使出现此消息，系统也会应用您提供的密码。但出于安全考虑，思科建议您使用更复杂的密码。

---

1. 如果admin帐户由于登录尝试失败次数过多而被锁定，则必须解锁该帐户，运行pam_tally命令，并在出现提示时输入密码：
   sudo pam_tally —user —reset
2. 键入exit退出shell。
3. 在启用了CLI的Firepower管理中心上，键入exit以退出CLI。

重置Firepower管理中心丢失的Web界面管理员密码

按照以下说明更改用于访问Firepower管理中心Web界面的管理员帐户的密码。

步骤:

1. 使用CLI管理员帐户和SSH或控制台登录设备。
2. 访问Linux shell:
   ·如果您的FMC运行的是6.2或更低版本，则登录可让您直接访问Linux shell。
   ·如果您的FMC运行6.3或6.4且未启用Firepower管理中心CLI，则登录可让您直接访问Linux外壳。
   ·如果您的FMC运行6.3或6.4且启用了Firepower管理中心CLI，则日志记录可让您访问Firepower管理中心CLI。运行expert命令以访问Linux外壳。
   ·如果您的FMC运行的是6.5+，登录会让您访问Firepower管理中心CLI。运行expert命令以访问Linux外壳。
3. 在shell提示符下，运行此命令以重置Web界面管理员用户的密码：
   sudo usertool.pl -p 'admin password'
   其中password是Web界面管理员用户的新密码。
4. 在密码提示符下，输入您当前登录的用户名的密码。
5. 如果Web管理员帐户因登录尝试失败次数过多而被锁定，则必须解锁该帐户。运行usertool命令，在出现提示时输入您的CLI管理员密码：
   sudo usertool.pl -u admin
6. 键入exit退出shell。
7. 在启用了CLI的Firepower管理中心上，键入exit以退出CLI。

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）。