Management Center Virtual 初始管理和配置

在完成 Management Center Virtual 的初始设置过程并验证其成功后，我们建议您完成各种管理任务，以使部署更易于管理。此外，还应该完成在初始设置过程中跳过的所有任务，例如许可。有关以下各部分中描述的任何任务的详细信息，以及有关如何开始配置部署的信息，请参阅适用于您的版本的完整《Cisco Secure Firewall Management Center 配置指南》。

- 单个用户账户，第 1 页
- 设备注册，第 2 页
- 运行状况和系统策略，第 2 页
- 软件和数据库更新，第 2 页
- 故障排除，第 3 页

单个用户账户

完成初始设置后，系统上的唯一 Web 界面用户是**管理员**用户，此用户具备管理员角色和访问权限。管理员角色用户具有对系统的完整菜单和配置访问权限。建议限制使用**管理员**帐户（和管理员角色），以保障安全，便于审计。在 Management Center Virtual GUI 的**系统 (System)** > **用户 (Users)** > **用户 (User)**页面管理用户账户。

注释 通过外壳访问 Management Center Virtual 的**管理员**帐户与使用 Web 界面访问 Management Center Virtual 的管理员帐户并不相同，两者可能使用不同的密码。

为使用系统的每个人创建独立帐户，不仅可以让公司审计每个用户所做的操作和更改，还能限制每个人的相关用户访问角色。这点对于Management Center Virtual来说尤其重要，因为您需要在其中执行大多数的配置和分析任务。例如，分析师需要访问事件数据来分析网络的安全性，但不需要访问用于部署的管理功能。

系统包含 10 个专为使用 Web 界面的各种管理员和分析师设计的预定义用户角色。还可以创建具有专用访问权限的自定义用户角色。

设备注册

管理中心 可以管理当前支持的任何物理或虚拟设备：

- 威胁防御- 提供统一的下一代防火墙和下一代 IPS 设备。
- Threat Defense Virtual- 可运行于多种虚拟机监控程序环境、旨在减少管理开销并提高运营效率的 64 位虚拟设备。
- 思科 具备 FirePOWER 服务的 ASA（或 ASA FirePOWER 模块）- 提供最重要的系统策略，并将流量传递到系统进行发现和访问控制。但是无法使用 管理中心 的 Web 界面来配置 ASA FirePOWER 接口。思科具备 FirePOWER 服务的 ASA提供 ASA 平台特有的软件和 CLI，可以用于安装系统以及执行平台特定的其他管理任务。
- 7000 和 8000 系列 设备 - 专为系统打造的专用物理设备。7000 和 8000 系列 设备吞吐量各异，但是大部分功能都相同。一般来说，8000 系列设备比 7000 系列设备功能更强大；它们还支持其他功能，如 8000 系列快速路径规则、链路汇聚和堆叠。在将设备注册至 管理中心 之前，必须在设备上配置远程管理。
- NGIPSv - 在 VMware VSphere 环境中部署的 64 位虚拟设备。NGIPSv 设备不支持系统任何基于硬件的功能，如冗余和资源共享、交换和路由等。

要注册托管设备到 管理中心，请使用 管理中心 GUI 的**设备 (Devices)** > **设备管理 (Device Management)** 页面；请参阅您的版本对应的《Cisco Secure Firewall Management Center 配置指南》中的设备管理信息。

运行状况和系统策略

默认情况下，所有设备都应用了初始系统策略。系统策略管理同一部署中多台设备可能使用的相似设置，例如邮件中继主机首选项和时间同步设置。建议使用 管理中心 将同一系统策略应用到管理中心本身以及它管理的所有设备上。

默认情况下，管理中心还应用了运行状况策略。作为运行状况监控功能的一部分，运行状况策略为系统提供了用以持续监控部署中设备的性能的标准。建议使用 管理中心 将运行状况策略应用到其管理的所有设备上。

软件和数据库更新

在开始任何部署之前，应更新设备上的系统软件。建议部署的所有设备都运行系统的最新版本。如果您正在部署中使用这些设备，还应当安装最新的入侵规则更新、VDB 和 GeoDB。

⚠

注意 在更新系统的任何部分之前，必须阅读随更新提供的版本说明或建议文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。

如果您的 管理中心 运行的是 6.5 以上版本：

作为配置的一部分，管理中心 建立以下活动以保持系统处于最新状态，并持续备份您的数据：

- 每周自动更新 GeoDB
- 为 管理中心 及其托管设备下载最新软件的每周任务

重要事项 此任务仅将软件更新下载到 管理中心。您负责安装此任务下载的任何更新。有关详细信息，请参阅《*Cisco Secure Firewall Management Center* 升级指南》《》。

- 执行本地存储的仅配置 管理中心 备份的每周任务

如果您的 管理中心 运行版本 6.6+，则作为初始配置的一部分，管理中心 会从 Cisco 支持站点下载并安装最新漏洞 (VDB) 更新。这是一次性操作。

您可以使用 Web 界面消息中心观察这些活动的状态。如果系统无法配置任何活动，并且您的 管理中心 有互联网访问权限，我们建议您根据您的版本对应的《*Cisco Secure Firewall Management Center* 配置指南》中所述，自行配置这些活动。

故障排除

本节提供与虚拟机上的 Management Center Virtual 部署相关的一些基本故障排除步骤。

SSH 连接失败

除 SSH 连接外，Management Center Virtual 完全正常运行，用户界面和控制台连接正常。在某些情况下，SSH 主机密钥文件可能会在 Management Center Virtual 初始启动时损坏，从而导致 SSH 连接失败。

您可以检查以下表明 SSH 连接失败的迹象：

1. 在 Management Center Virtual 初始启动期间，尤其是在 SSH 后台守护程序 (sshd) 启动时，可能会发生磁盘 I/O 错误。这会导致 SSH 密钥文件（由 sshd 生成的 ssh_host* 文件）为空。

   `ls -lrt /etc/ssh total 16`

   ```
   -rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
   -rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
   -rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
   ```

2. 对于磁盘 I/O 问题，可以检查 `/var/log/messages` 文件，其中可能包含与 SSH 密钥文件生成时间相同的错误数据（表示 I/O 错误）。

要解决 Management Center Virtual 初始启动期间可能出现的 SSH 故障（如上所述），您应执行以下步骤：

1. 登录 Management Center Virtual。
2. 在**专家**模式下，在 Management Center Virtual CLI 上运行 **sudo reboot** 命令以启动正常重启。
3. 运行以下命令以删除空的 SSH 密钥文件：

```
cd /etc/ssh/
rm ssh_host*
```

4. 运行以下命令重新启动 `sshd` 服务，以便正确重新生成 SSH 密钥文件。

```
/etc/rc.d/init.d/sshd stop
/etc/rc.d/init.d/sshd start
```

注释 只有在确定 SSH 密钥文件为空时，才能执行此解决方法步骤。如果不确定，建议您提交 TAC 案例以作进一步调查。

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。