Sourcefire/FirePOWER设备排除故障文件生成步骤

目录

简介

本文描述如何生成在Sourcefire/FirePOWER设备的一个排除故障文件。排除故障文件包含日志消息、配置数据和命令输出的一集。它用于为了确定Sourcefire/FirePOWER系统的状况。如果Cisco技术支持工程师请求您发送从您的Sourcefire/FirePOWER设备的一个排除故障文件，您在本文能使用提供的说明。

先决条件

要求

Cisco 建议您了解以下主题：

- Sourcefire管理设备，例如防御中心/FireSIGHT/FirePOWER管理中心(FMC)
- Sourcefire受管理设备，例如FirePOWER设备模型(Series-3)， 3D设备模型(Series-2)和有出于方框管理的虚拟设备/ASA FirePOWER模块。

注意：您能使用防御中心或管理中心为了生成一个排除故障文件管理设备的，或者受管理设备的。 FirePOWER设备(Series-3)型号包括7000系列， 7100系列和8000系列受管理设备。 Series-2受管理设备型号包括3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500、3D9900和ASA与FirePOWER服务。

使用的组件

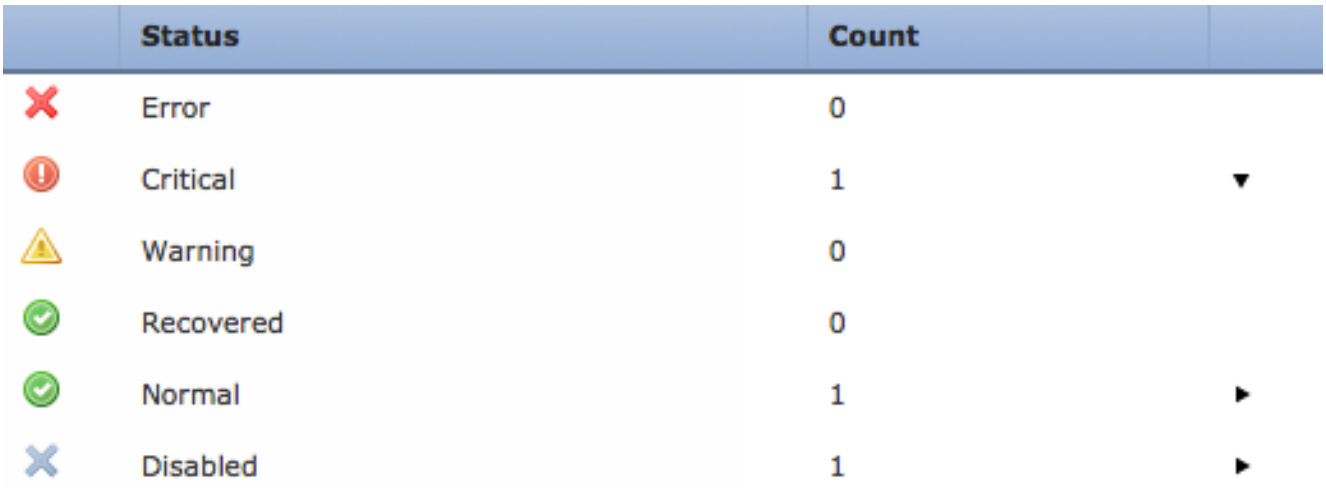
此本文档中的信息根据运行软件版本5.0或以上的Sourcefire /FirePOWER设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

生成排除故障有Web接口的文件

完成这些步骤为了生成排除故障文件：

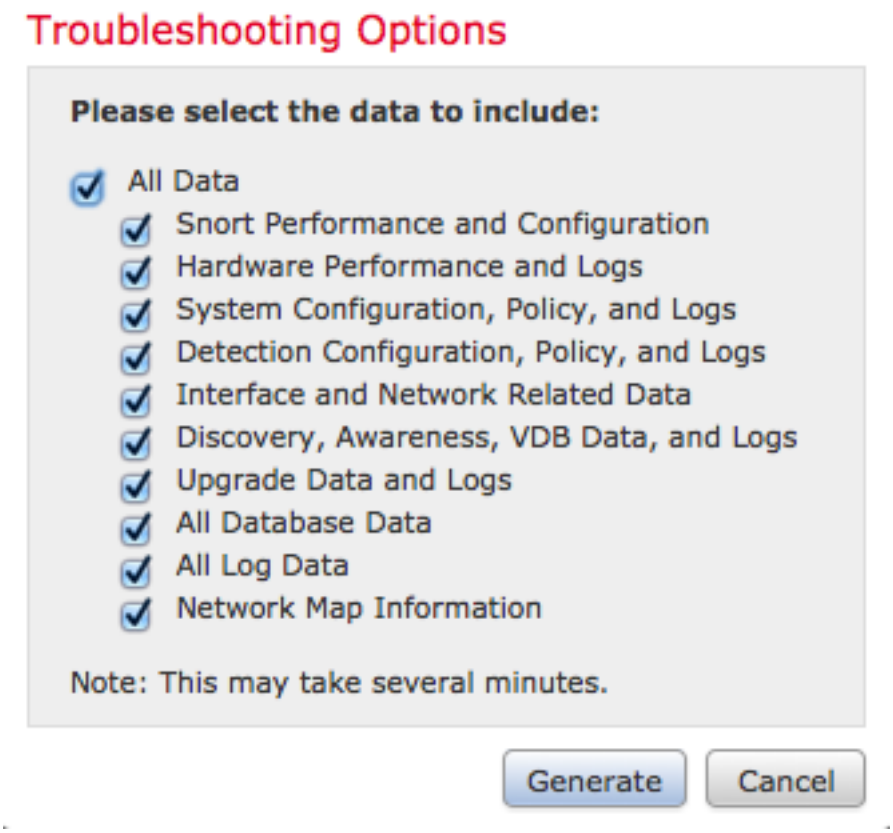
1. 在版本5.x.x，请导航到在管理设备Web接口的**健康>健康监控**为了到达健康监控页。
   在版本6.x.x，请导航到**系统>**在管理设备Web接口的**健康>监视器**为了到达健康监控页。
2. 为了展开设备请列出并且查看设备以一种特定的状态，单击箭头在行结束时：



   提示：如果箭头在下来状态水平点的行结束时，该状态的设备列表在更低表里出现。如果箭头指向权利，设备列表隐藏。
3. 在设备列表的设备列，请点击您要查看详细信息设备的名称。健康监控设备页出版。

4. 单击**生成故障排除文件**。故障排除选项弹出窗口出现。

5. 检查**所有数据校验**复选框为了生成与所有的一报告可能的故障排除数据或者检查各自的复选框为了定制您的报告：



6. 单击**生成，**并且管理中心生成排除故障文件。

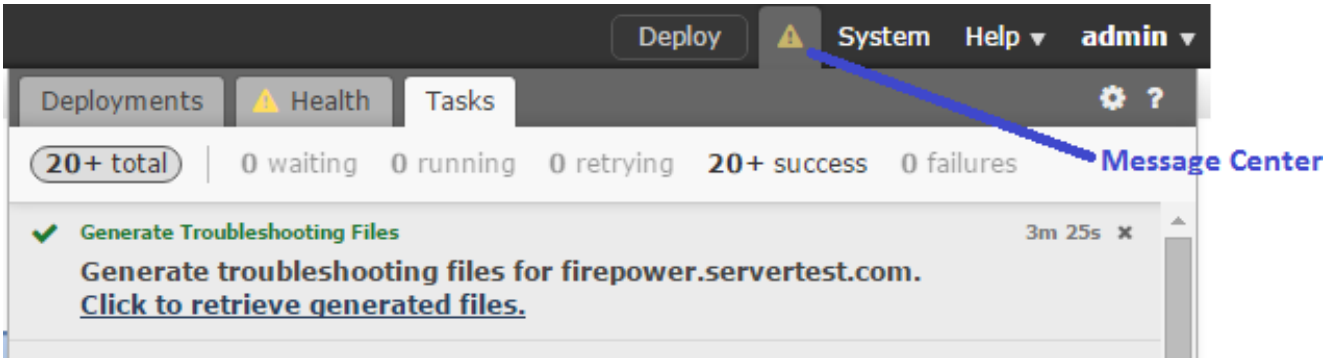
   提示：在版本5.x.x，为了监控在任务排队的文件生成过程，请导航对**系统> Monitoring>任务状态**。在版本6.x.x，为了监控在任务状态的文件生成过程，请导航对**消息中心图标**(之间选项部署和系统) **>任务。**

下载排除故障文件

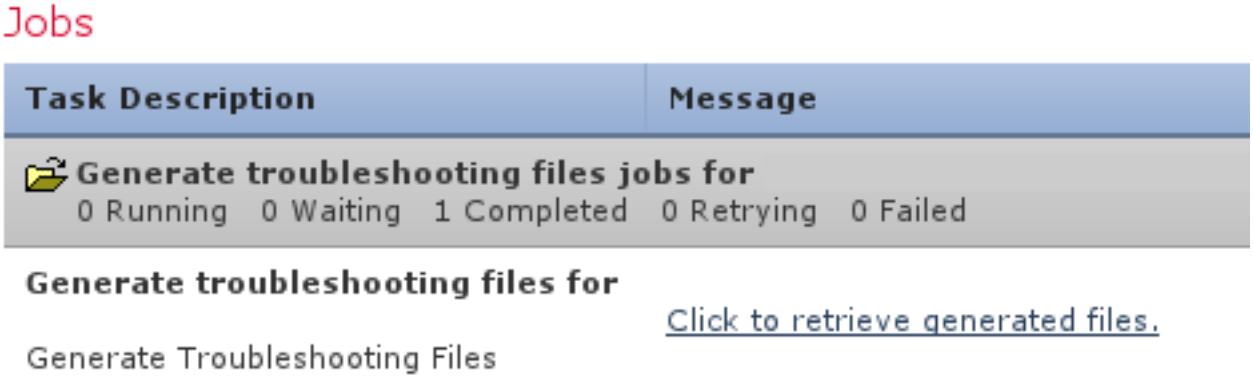
完成这些步骤为了下载生成的复制的您排除故障文件：

1. 在版本5.x.x，请导航对在管理设备Web接口的**系统> Monitoring>任务状态**为了到达Status页的任务。
   在版本6.x.x**，请**导航对**消息中心图标**(之间选项部署和系统) **>**在管理设备Web接口的**任务**为了到达Status页的任务。
2. 在设备生成排除故障文件和任务状态变化对**完成后**，请找出对应于排除故障文件您生成的任务。
3. 点击**单击获取生成的**文件链接和按照浏览器提示符为了下载文件。

   版本6.x.x



版本5.x.x



4. **注意**：文件下载到您的在单个.tar.gz文件的桌面。

代替生成方法

如果尝试使用在前面部分描述并且无法访问管理设备Web接口的生成方法，或者，如果有在管理设备和受管理设备之间的连通性问题，然后不能生成排除故障文件。在这种情况下，您能使用您的设备CLI为了生成排除故障文件。

生成排除故障有CLI的文件

防御中心和Series-2设备

输入此in命令防御中心、管理中心和Series-2受管理设备为了生成排除故障文件：

```
admin@3DSystem:~$ sudo sf_troubleshoot.pl

Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
Troubleshooting information successfully created at /var/common/xxxxxx.tar.gz
```

FirePOWER和虚拟设备

输入此on命令FirePOWER设备/模块和虚拟受管理设备为了生成排除故障文件：

```
> system generate-troubleshoot all
Starting /usr/local/sf/bin/sf_troubleshoot.pl... Please, be patient. This may take several
minutes. The troubleshoot option code specified is ALL. Troubleshooting information successfully
created at /var/common/xxxxxx.tar.gz
```

复制排除故障文件

防御中心和Series-2设备

输入此in命令防御中心、管理中心和Series-2受管理设备为了复制排除故障文件：

```
admin@3DSystem:~$ sudo scp troubleshoot_file_name username@destination_host:
 destination_folder
```

FirePOWER和虚拟设备

输入此on命令FirePOWER设备和虚拟受管理设备为了复制排除故障文件：

```
> system file secure-copy hostname username destination_folder troubleshoot_file
```

> **注意**：在本例中，**主机名**是指目标远程主机的名称或IP地址，**用户名**指定用户的名称远程主机的， **destination_folder**指定远程主机的目的地路径，并且**troubleshoot_file**指定本地排除故障转移的文件。