

FireSIGHT系统回归“输入/输出错误”消息

目录

- [简介](#)
- [症状](#)
- [验证](#)
- [解决方案](#)

简介

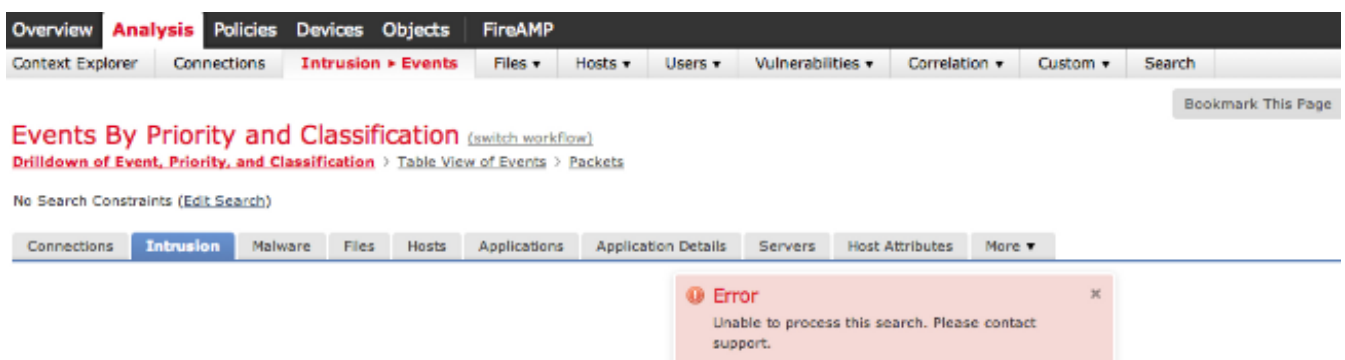
当您在FireSIGHT系统时工作，您可以收到I/O或/一个消息。本文描述如何调查此问题和如何排除故障它。

症状

- 无法运用入侵策略。任务状态可能显示以下错误消息：

```
Could not create directory /var/tmp/PolicyExport_XXXX:  
Input/output error
```

- 入侵事件的一查询发生故障。搜索结果可能显示以下错误：



- 无法装载在网页用户界面的健康监控。
- 无法查看受管理设备。

验证

为了验证问题，请遵从下面步骤：

步骤 1：对您的FireSIGHT系统的连接通过安全壳SSH。

步骤 2：举起您的权限给root用户：

- 在FireSIGHT管理中心和Firepower设备上，请运行：

```
admin@FireSIGHT:~$ sudo su -root@FireSIGHT:~#
```

- 在Firepower设备上，请运行：

```
> expert
admin@FirePOWER:~$ sudo su -
root@FirePOWER:~#
```

步骤 3：运行以下命令调查此问题：

- **dmesg**输出显示/。例如：

```
root@FireSIGHT:~# dmesg
-sh: /bin/dmesg: Input/output error
```

- **ls**回归/。例如：

```
admin@FireSIGHT:~$ ls
ls: reading directory .: Input/output error
```

- 尝试生成排除故障文件生成/。例如：

```
admin@FireSIGHT:~$ sudo sf_troubleshoot.pl
/usr/local/sf/bin/sf_troubleshoot.pl: Input/output error
```

- I/O在/var/log/messages被找到。例如：

```
admin@FireSIGHT:~$ grep -i error /var/log/messages

Sourcefire3D kernel: sd 2:2:0:0: scsi: Device offlined - not ready after error recovery
Sourcefire3D kernel: end_request: I/O error, dev sda, sector 1109804126
Sourcefire3D kernel: Buffer I/O error on device sda7, logical block 0
Sourcefire3D kernel: lost page write due to I/O error on sda7
Sourcefire3D kernel: Buffer I/O error on device sda7, logical block 137396224
Sourcefire3D kernel: lost page write due to I/O error on sda7
Sourcefire3D kernel: EXT2-fs error (device sda7): read_block_bitmap: Cannot read block
bitmap - block_group = 4208, block_bitmap = 13
```

- /在/var/log/action_queue.log被找到：

```
Error in tempdir() using /var/tmp/PolicyExport_XXXXX: Could not create directory
/var/tmp/PolicyExport_XXXX: Input/output error
```

解决方案

请温文地重新启动您的设备执行文件系统系统检查：

```
root@FireSIGHT:~# reboot
```

如果这不解决问题，请执行在设备的一辆牵强的重新启动：

```
root@FireSIGHT:~# reboot -f
```

在您运行`-f`，FireSIGHT系统重新启动和执行一个文件系统系统检查。例如：

```
/boot: 34/26104 files (29.4% non-contiguous), 48680/104388 blocks
e2fsck 1.42.2 (27-Mar-2012)
/Volume contains a file system with errors, check forced.
Pass 1: Checking inodes, blocks, and sizes
Inode 1036407, i_size is 14921607, should be 14929920. Fix? yes

Inode 1036407, i_blocks is 29184, should be 29200. Fix? yes

/Volume: |=====|                                     | 37.4%
```

在一辆牵强的重新启动以后，如果仍然遇到此问题，请与协助的思科技术支持联系。