

Mensagem do erro entrada/saída” dos retornos do sistema do “de FireSIGHT

Índice

[Introdução](#)

[Sintomas](#)

[Verificação](#)

[Solução](#)

Introdução

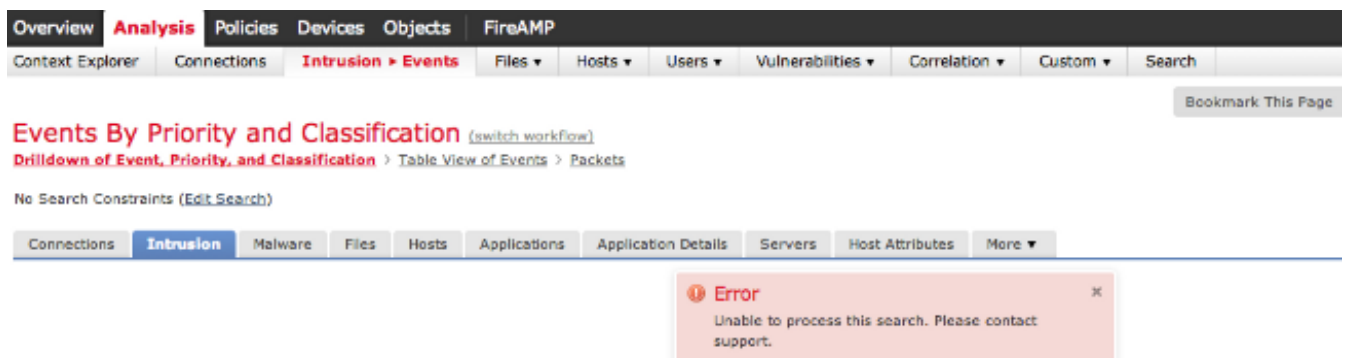
Quando você está trabalhando em um sistema de FireSIGHT, você pode receber uma mensagem para o erro I/O ou o erro do entrada/saída. Este documento descreve como investigar esta edição, e como pesquisá-la defeitos.

Sintomas

- Incapaz de aplicar a política da intrusão. O estado da tarefa pode indicar o seguinte Mensagem de Erro:

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

- Uma pergunta para eventos da intrusão falha. O resultado da busca pode mostrar o seguinte erro:



The screenshot shows the FireSIGHT web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. Below this, there are tabs for 'Context Explorer', 'Connections', 'Intrusion > Events', 'Files', 'Hosts', 'Users', 'Vulnerabilities', 'Correlation', 'Custom', and 'Search'. A 'Bookmark This Page' button is visible on the right. The main content area is titled 'Events By Priority and Classification' with a '(switch workflow)' link. Below the title, there are links for 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. A search bar contains the text 'No Search Constraints (Edit Search)'. At the bottom of the interface, there is a horizontal menu with tabs for 'Connections', 'Intrusion', 'Malware', 'Files', 'Hosts', 'Applications', 'Application Details', 'Servers', 'Host Attributes', and 'More'. An error message box is displayed in the bottom right corner, containing the text: 'Error: Unable to process this search. Please contact support.'

- Incapaz de carregar o monitor de funcionamento na relação de usuário de web.
- Incapaz de ver os dispositivos gerenciado.

Verificação

A fim verificar a edição, siga as etapas abaixo:

Passo 1: Conecte a seu sistema de FireSIGHT através do Shell Seguro (ssh).

Passo 2: Eleve seu privilégio ao usuário de raiz:

- No centro de gerenciamento de FireSIGHT e no dispositivo da potência de fogo, seja executado:

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

- No dispositivo da potência de fogo, seja executado:

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

Passo 3: Execute os comandos seguintes investigar esta edição:

- A saída do comando `dmesg` mostra o erro do entrada/saída. Por exemplo:

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

- O comando `ls` retorna o erro do entrada/saída. Por exemplo:

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

- Uma tentativa de gerar pesquisa defeitos o arquivo gereencie o erro do entrada/saída. Por exemplo:admin@FireSIGHT:~\$ sudo sf_troubleshoot.pl

```
/usr/local/sf/bin/sf_troubleshoot.pl: Input/output error
```

- Os Mensagens de Erro I/O são encontrados em `/var/log/messages`. Por exemplo:

```
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
```

- O erro do entrada/saída é encontrado em `/var/log/action_queue.log`:
Error in tempdir() using /var/tmp/PolicyExport_XXXXX: Could not create directory
/var/tmp/PolicyExport_XXXXX: Input/output error

Solução

Recarregue graciosamente seu dispositivo para executar uma verificação de sistema de arquivos:

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

Se isto não resolve a edição, execute uma repartição forçada no dispositivo:

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

Depois que você executa o comando `-f` da repartição, os reinícios do sistema de FireSIGHT e executam uma verificação de sistema de arquivos. Por exemplo:

```
/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%
```

Após uma repartição forçada, se você ainda está encontrando esta edição, contacte por favor o Suporte técnico de Cisco para o auxílio.