O sistema FireSIGHT retorna a mensagem "Input/Output Error"

Contents

Introduction

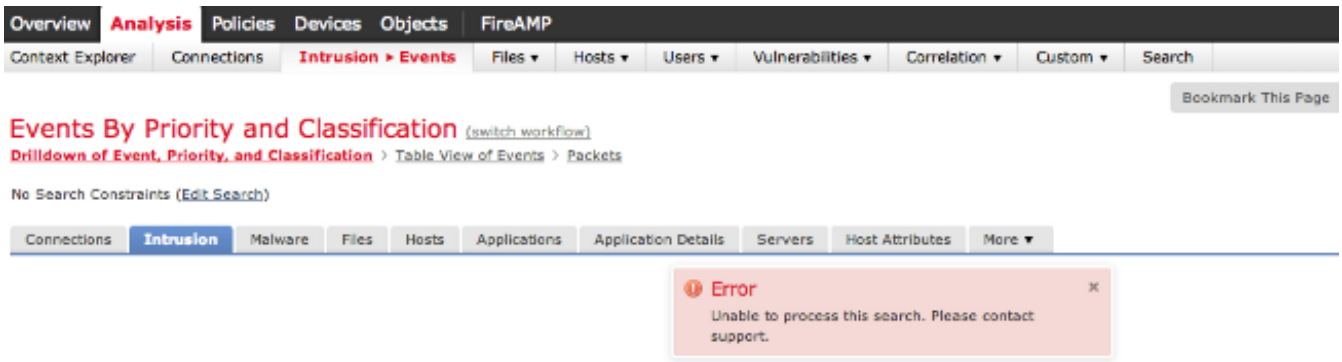
Quando estiver trabalhando em um sistema FireSIGHT, você poderá receber uma mensagem de erro de E/S ou erro de entrada/saída. Este documento descreve como investigar esse problema e como solucioná-lo.

Sintomas

- Não é possível aplicar a política de intrusão. O **Status da Tarefa** pode exibir a seguinte mensagem de erro:

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

- Falha na consulta de eventos de intrusão. O resultado da pesquisa pode mostrar o seguinte erro:



- Não é possível carregar o monitor de integridade na interface do usuário da Web.
- Não é possível exibir os dispositivos gerenciados.

Verificação

Para verificar o problema, siga as etapas abaixo:

Passo 1: Conecte-se ao seu sistema FireSIGHT via Secure Shell (SSH).

Passo 2: Eleve seu privilégio para o usuário raiz:

- No FireSIGHT Management Center e no FirePOWER Appliance, execute:

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

- No FirePOWER Appliance, execute:

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

Etapa 3: execute os seguintes comandos para investigar esse problema:

- A saída do comando **dmesg** mostra Input/Output Error. Por exemplo:

```
root@FireSIGHT:~# dmesg

-sh: /bin/dmesg: Input/output error
```

- O comando **ls** retorna Input/Output Error. Por exemplo:

```
admin@FireSIGHT:~$ ls

ls: reading directory .: Input/output error
```

- Uma tentativa de gerar um arquivo de solução de problemas gera um erro de entrada/saída. Por exemplo:

```
admin@FireSIGHT:~$ sudo sf_troubleshoot.pl

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

- As mensagens de erro de E/S são encontradas 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 de entrada/saída está no diretório /var/log/action_queue.log:

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

Solução

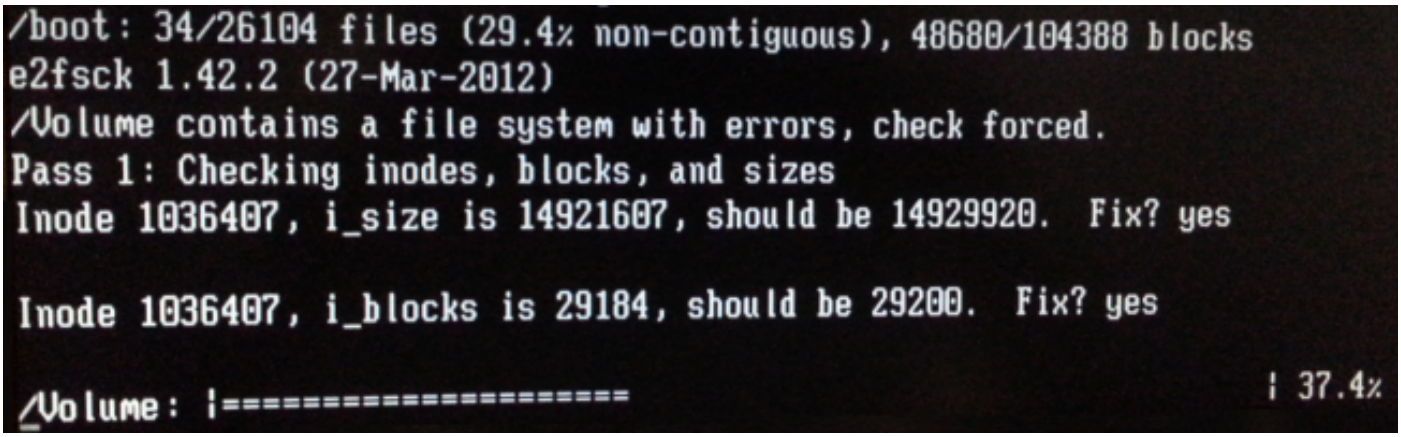
Reinicialize seu dispositivo com cuidado para executar uma verificação do sistema de arquivos:

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

Se isso não resolver o problema, execute uma reinicialização forçada no dispositivo:

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

Depois de executar o comando **reboot -f**, o sistema FireSIGHT é reiniciado e executa uma verificação do sistema de arquivos. Por exemplo:



Após uma reinicialização forçada, se ainda estiver com esse problema, entre em contato com o Suporte Técnico da Cisco para obter assistência.