

# FireSIGHT System Retourenbericht "I/O Error"

## Inhoud

[Inleiding](#)

[Symptomen](#)

[Verificatie](#)

[Oplossing](#)

## Inleiding

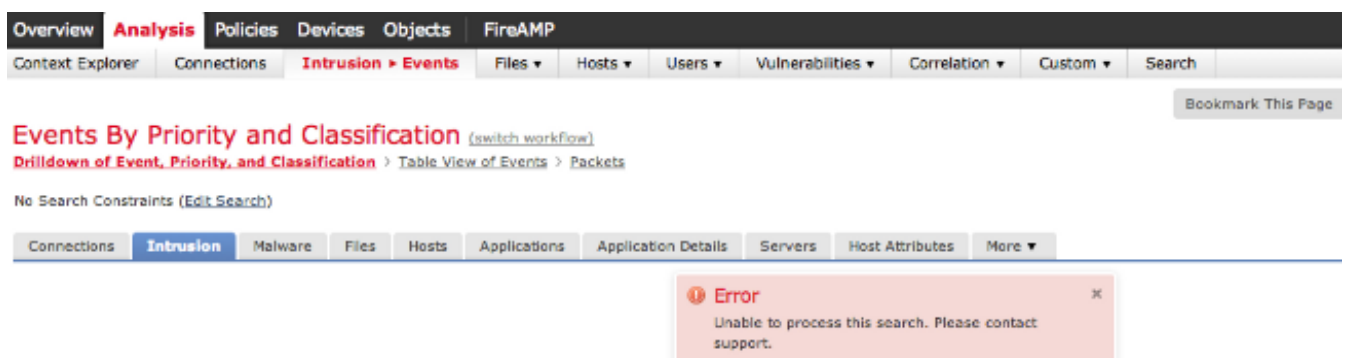
Wanneer u aan een FireSIGHT System werkt, kunt u een bericht ontvangen voor I/O-fout of I/O-fout. Dit document beschrijft hoe u deze kwestie wilt onderzoeken en hoe u de problemen kunt oplossen.

## Symptomen

- Kan geen inbraakbeleid toepassen. De **taakstatus** kan de volgende foutmelding weergeven:

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

- Een query voor inbraakgebeurtenissen faalt. Het zoekresultaat kan de volgende fout weergeven:



The screenshot shows the FireSIGHT System 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 displays 'Events By Priority and Classification' with a '(switch workflow)' link. Below this, there are links for 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. A search bar is present with the text 'No Search Constraints (Edit Search)'. At the bottom, there are 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.'

- Kan de gezondheidsmonitor niet op de webgebruikersinterface laden.
- Kan de beheerde apparaten niet weergeven.

## Verificatie

Volg onderstaande stappen om het probleem te verifiëren:

**Stap 1:** Connect met uw FireSIGHT System via Secure Shell (SSH).

**Stap 2:** Verhoog uw recht om gebruiker te worstelen:

- Start op FireSIGHT Management Center en FirePOWER-applicatie:

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

- Start op FirePOWER-applicatie:

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

**Stap 3:** Start de volgende opdrachten om dit probleem te onderzoeken:

- De opdrachtoutput van **dmesg** toont I/O-fout. Bijvoorbeeld:

```
root@FireSIGHT:~# dmesg

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

- De opdracht **ls** retourneert I/O fout. Bijvoorbeeld:

```
admin@FireSIGHT:~$ ls

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

- Een poging om problemen op te lossen genereert I/O-fout. Bijvoorbeeld:

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

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

- I/O-foutmeldingen worden gevonden in de `/var/log/berichten`. Bijvoorbeeld:

```
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
```

- De I/O-fout is te vinden op `/var/log/action_queue.log`:

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

# Oplossing

Start uw wasmachine zorgvuldig opnieuw op om een systeemcontrole uit te voeren:

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

Als dit probleem niet wordt opgelost, voert u een gedwongen herstart op het apparaat uit:

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

Nadat u de opdracht **rebootf** hebt uitgevoerd, start het FireSIGHT System opnieuw en voert u een bestandssysteemcontrole uit. Bijvoorbeeld:

```
/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: i===== i 37.4%
```

Als u na een gedwongen herstart nog steeds dit probleem tegenkomt, neemt u contact op met technische ondersteuning van Cisco voor assistentie.