

# FireSIGHT-System gibt die Meldung "Eingabe/Ausgabe-Fehler" zurück

## Inhalt

[Einführung](#)

[Symptome](#)

[Überprüfung](#)

[Lösung](#)

## Einführung

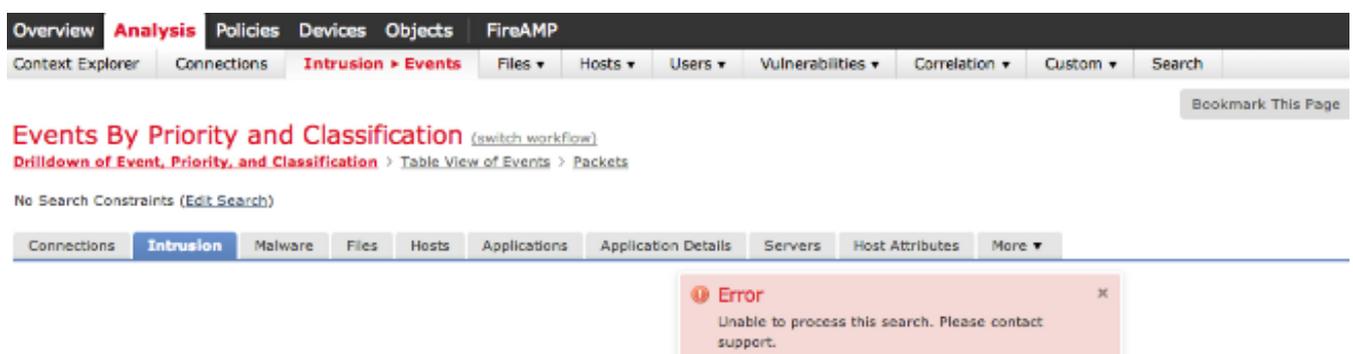
Wenn Sie an einem FireSIGHT-System arbeiten, erhalten Sie möglicherweise die Meldung E/A-Fehler oder Eingabe/Ausgabe-Fehler. Dieses Dokument beschreibt, wie dieses Problem untersucht und wie es behoben werden kann.

## Symptome

- Richtlinie für Sicherheitsrisiken kann nicht angewendet werden. Der **Aufgabenstatus** zeigt möglicherweise die folgende Fehlermeldung an:

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

- Eine Abfrage für Intrusion-Ereignisse schlägt fehl. Das Suchergebnis kann den folgenden Fehler anzeigen:



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'. The main content area is titled 'Events By Priority and Classification' with a '(switch workflow)' link. Below the title, there is a breadcrumb trail: 'Drilldown of Event, Priority, and Classification > Table View of Events > Packets'. A search bar is present with the text 'No Search Constraints (Edit Search)'. At the bottom of the interface, there is a horizontal menu with 'Connections', 'Intrusion', 'Malware', 'Files', 'Hosts', 'Applications', 'Application Details', 'Servers', 'Host Attributes', and 'More'. A red error message box is displayed at the bottom right, containing the text: 'Error: Unable to process this search. Please contact support.'

- Der Health Monitor kann nicht auf die Webbenutzeroberfläche geladen werden.
- Die verwalteten Geräte können nicht angezeigt werden.

# Überprüfung

Führen Sie zur Überprüfung des Problems die folgenden Schritte aus:

**Schritt 1:** Stellen Sie über Secure Shell (SSH) eine Verbindung zum FireSIGHT-System her.

**Schritt 2:** Erweitern Sie Ihre Berechtigung für Root-Benutzer:

- Führen Sie auf FireSIGHT Management Center und FirePOWER Appliance Folgendes aus:

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

- Führen Sie auf der FirePOWER-Appliance Folgendes aus:

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

**Schritt 3:** Führen Sie die folgenden Befehle aus, um dieses Problem zu untersuchen:

- Die Ausgabe des **Befehls dmesg** zeigt Eingabe-/Ausgabefehler an. Beispiel:

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

- Der Befehl **ls** gibt Eingabe-/Ausgabefehler zurück. Beispiel:

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

- Beim Versuch, eine Fehlerbehebungsdatei zu generieren, wird ein Eingabe-/Ausgabefehler generiert. Beispiel:

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

- E/A-Fehlermeldungen finden sich auf dem `/var/log/messages`. Beispiel:

```
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
```

- Der Eingabe-/Ausgabefehler finden Sie unter `/var/log/action_queue.log`:

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

## Lösung

Führen Sie einen sanften Neustart Ihres Geräts durch, um eine Dateisystemüberprüfung durchzuführen:

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

Wenn das Problem dadurch nicht behoben wird, führen Sie einen erzwungenen Neustart der Appliance durch:

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

Nachdem Sie den Befehl `reboot -f` ausgeführt haben, startet das FireSIGHT-System neu und führt eine Dateisystemüberprüfung durch. Beispiel:

```
/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%
```

Wenn Sie nach einem erzwungenen Neustart immer noch mit diesem Problem konfrontiert werden, wenden Sie sich an den technischen Support von Cisco.