

# Il sistema FireSIGHT restituisce il messaggio "Errore di input/output"

## Sommario

[Introduzione](#)

[Sintomi](#)

[Verifica](#)

[Soluzione](#)

## Introduzione

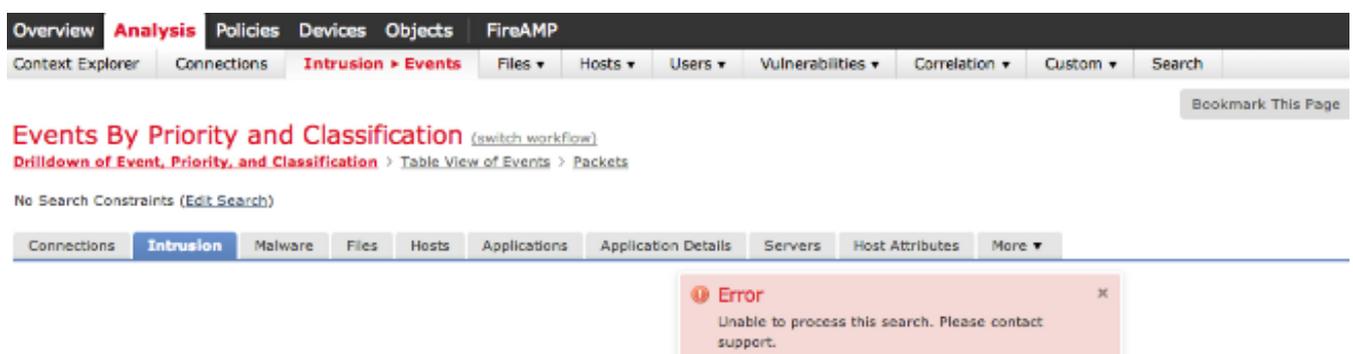
Quando si lavora su un sistema FireSIGHT, è possibile che venga visualizzato un messaggio di errore I/O o di errore Input/Output. In questo documento viene descritto come analizzare il problema e come risolverlo.

## Sintomi

- Impossibile applicare il criterio di intrusione. In **Stato attività** potrebbe essere visualizzato il seguente messaggio di errore:

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

- Query per eventi di intrusione non riuscita. Il risultato della ricerca potrebbe visualizzare il seguente errore:



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 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 constraint section shows 'No Search Constraints (Edit Search)'. At the bottom, there is a navigation bar with tabs for 'Connections', 'Intrusion', 'Malware', 'Files', 'Hosts', 'Applications', 'Application Details', 'Servers', 'Host Attributes', and 'More'. An error message box is displayed at the bottom right, containing the text: 'Error: Unable to process this search. Please contact support.'

- Impossibile caricare il monitoraggio dello stato sull'interfaccia utente Web.
- Impossibile visualizzare i dispositivi gestiti.

# Verifica

Per verificare il problema, procedere come segue:

**Passaggio 1:** Collegarsi al sistema FireSIGHT tramite Secure Shell (SSH).

**Passaggio 2:** Elevare il privilegio all'utente root:

- Su FireSIGHT Management Center e Appliance FirePOWER, eseguire:

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

- Sull'appliance FirePOWER, eseguire:

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

**Passaggio 3:** Per analizzare il problema, eseguire i comandi seguenti:

- L'output del comando **dmesg** visualizza l'errore di input/output. Ad esempio:

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

- Il comando **ls** restituisce un errore di input/output. Ad esempio:

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

- Un tentativo di generare un file per la risoluzione dei problemi genera un errore di input/output. Ad esempio:

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

- I messaggi di errore I/O sono disponibili in `/var/log/messages`. Ad esempio:

```
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
```

- L'errore di input/output è disponibile nella cartella /var/log/action\_queue.log:

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

## Soluzione

Riavviare correttamente l'accessorio per eseguire un controllo del file system:

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

Se il problema persiste, eseguire un riavvio forzato dell'accessorio:

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

Dopo aver eseguito il comando **reboot -f**, il sistema FireSIGHT si riavvia ed esegue un controllo del file system. Ad esempio:

```
/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%
```

Dopo un riavvio forzato, se il problema persiste, contattare il supporto tecnico Cisco per assistenza.