

Message de « erreur d'entrée/sortie » de retours de système de FireSIGHT

Contenu

[Introduction](#)

[Symptômes](#)

[Vérification](#)

[Solution](#)

Introduction

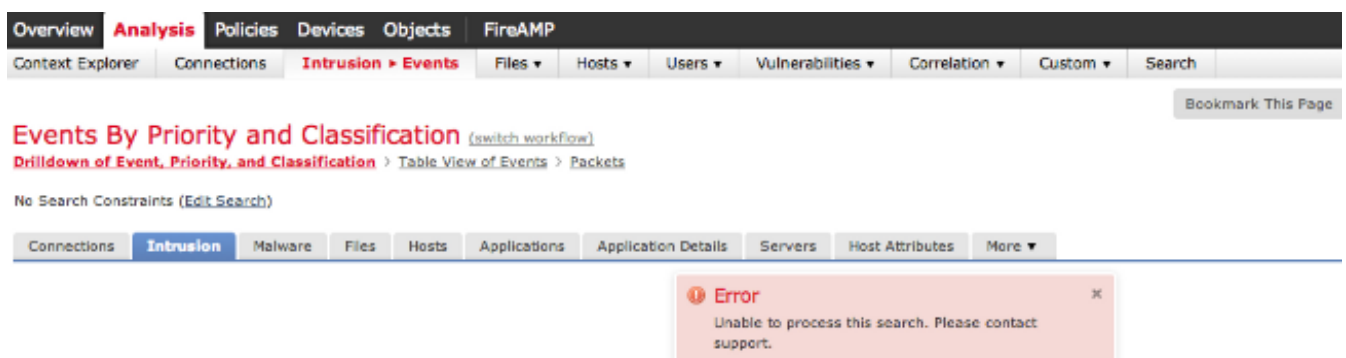
Quand vous fonctionnez sur un système de FireSIGHT, vous pouvez recevoir un message pour l'erreur E/S ou l'erreur d'entrée/sortie. Ce document décrit comment étudier cette question, et comment la dépanner.

Symptômes

- Incapable d'appliquer la stratégie d'intrusion. L'état de tâche peut afficher le message d'erreur suivant :

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

- Une requête pour des événements d'intrusion échoue. Le résultat de la recherche peut afficher l'erreur suivante :



The screenshot shows the FireSIGHT user interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, and FireAMP. Below this is a secondary navigation bar with options like Context Explorer, Connections, Intrusion > Events, Files, Hosts, Users, Vulnerabilities, Correlation, Custom, and Search. The main content area displays 'Events By Priority and Classification' with a link to 'switch workflow'. Below this, there are breadcrumb links: 'Drilldown of Event, Priority, and Classification > Table View of Events > Packets'. A search bar indicates 'No Search Constraints (Edit Search)'. At the bottom of the main content area, 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 overlaid on the bottom right, with a red header 'Error' and a close button 'x'. The message text reads: 'Unable to process this search. Please contact support.'

- Incapable de charger le moniteur de santé sur l'interface utilisateur d'utilisateur web.
- Incapable de visualiser les périphériques gérés.

Vérification

Afin de vérifier la question, suivez les étapes ci-dessous :

Étape 1 : Connectez à votre système de FireSIGHT par l'intermédiaire du Protocole Secure Shell (SSH).

Étape 2 : Élevez votre privilège à l'utilisateur de base :

- Au centre de Gestion de FireSIGHT et à l'appliance de puissance de feu, exécutez-vous :

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

- Sur l'appliance de puissance de feu, exécutez-vous :

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

Étape 3 : Exécutez les commandes suivantes d'étudier cette question :

- La sortie de commande de `dmesg` affiche l'erreur d'entrée/sortie. Exemple :

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

- La commande `ls` renvoie l'erreur d'entrée/sortie. Exemple :

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

- Une tentative de se produire dépannant le fichier génère l'erreur d'entrée/sortie. Exemple : `admin@FireSIGHT:~$ sudo sf_troubleshoot.pl`

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

- Des messages d'erreur E/S sont trouvés sur `/var/log/messages`. Exemple :

```
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'erreur d'entrée/sortie est trouvée sur `/var/log/action_queue.log` :
Error in tempdir() using /var/tmp/PolicyExport_XXXXX: Could not create directory
/var/tmp/PolicyExport_XXXXX: Input/output error

Solution

Redémarrez avec élégance votre appliance pour exécuter un contrôle du système de fichier :

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

Si ceci ne résout pas le problème, exécutez une réinitialisation obligatoire sur l'appliance :

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

Après que vous exécutiez la **réinitialisation** - commande **f**, les redémarrages du système de FireSIGHT et exécutiez un contrôle du système de fichier. Exemple :

```
/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%
```

Après une réinitialisation obligatoire, si vous rencontrez toujours cette question, entrez en contact avec s'il vous plaît le support technique de Cisco pour l'assistance.