Contenu

Introduction

Un centre de Gestion de FireSIGHT ou une appliance de puissance de feu peut manquer d'espace disque pour différentes raisons. Quand se produit, l'utilisation de disque de haute déclenche l'alerte de santés ou peut échouer une tentative de mise à jour logicielle. Cet article décrit les causes principales de l'utilisation excessive de disque et de quelques étapes de dépannage.

Étapes de vérification

Déterminez la partition qui est fortement utilisée. La commande suivante affiche l'utilisation de disque :

Àun centre de Gestion de FireSIGHT,

```
admin@3DSystem:~# df -TH
```

Sur des appliances de gammes 7000 et 8000 et sur des périphériques virtuels NGIPS,

```
> show disk
```

Les deux commandes affichent un résultat comme ci-dessous :

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5 2.9G 566M 2.2G 21% /
/dev/sda1 99M 16M 79M 17% /boot
/dev/sda7 52G 8.5G 41G 18% /Volume
none 11G 20K 11G 1% /dev/shm
/dev/sdb1 418G 210M 395G 1% /var/storage
```

> Remarque: La taille et l'utilisation de disque peuvent varier sur de divers modèles d'appareils. Si c'est un périphérique virtuel NGIPS, vérifiez que la taille des partitions sont conformes aux espaces disque requis minimum.

Attention : N'importe quelle partition supplémentaire qui n'est pas affichée ci-dessus est sans support.

Sur des appliances de gammes 7000 et 8000 et sur des périphériques virtuels NGIPS, vous pouvez exécuter la commande suivante d'afficher des statistiques détaillées d'utilisation de disque :

```
> show disk-manager
```

Un exemple de sortie :

```
> show disk-manager
Silo Used Minimum Maximum
Temporary Files 143.702 MB 402.541 MB 1.572 GB
Action Queue Results 0 KB 402.541 MB 1.572 GB
Connection Events 17.225 GB 3.931 GB 23.586 GB
User Identity Events 0 KB 402.541 MB 1.572 GB
UI Caches 587 KB 1.179 GB 2.359 GB
Backups 0 KB 3.145 GB 7.862 GB
Updates 13 KB 4.717 GB 11.793 GB
Other Detection Engine 0 KB 2.359 GB 4.717 GB
Performance Statistics 72.442 MB 805.082 MB 9.435 GB
Other Events 669.819 MB 1.572 GB 3.145 GB
IP Reputation & URL Filtering 0 KB 1.966 GB 3.931 GB
Archives & Cores & File Logs 1.381 GB 3.145 GB 15.724 GB
RNA Events 0 KB 3.145 GB 12.579 GB
File Capture 12.089 MB 4.717 GB 14.152 GB
IPS Events 3.389 GB 7.076 GB 15.724 GB
```

Si la partition de /Volume est pleine

Vieux fichiers de sauvegarde

- Si vous enregistrez de large volume de vieux fichiers de sauvegarde sur le système, il peut prendre l'espace excessif sur votre disque.

[Étapes de dépannage]

- Supprimez les vieux fichiers de sauvegarde utilisant l'interface utilisateur d'utilisateur web. Afin de retirer des fichiers de sauvegarde, naviguez vers le **système > les outils > la sauvegarde/restauration**.

  Conseil : Sur un système de FireSIGHT, vous pouvez configurer la mémoire distante pour enregistrer les grands fichiers de sauvegarde.

Des fichiers plus anciens de mise à jour logicielle et de correctif

- Si vous gardez toujours la mise à jour logicielle, la mise à jour, et les fichiers de correctif (comme, les 5.0 ou les 5.1) précédents, le système peut s'épuiser l'espace disque.

[Étapes de dépannage]

- Supprimez les fichiers plus anciens de mise à jour et de correctif qui ne sont plus nécessaires.

Afin de les supprimer, naviguez s'il vous plaît vers le **système > les mises à jour**.

Des fichiers excessifs d'événement sont enregistrés

- Le périphérique géré ou le capteur pourrait avoir arrêté envoyer des événements au centre de Gestion de FireSIGHT.
- Un périphérique peut générer plus d'événements qu'un centre de Gestion est conçu pour recevoir (par seconde).
- Il pourrait y a une question de transmission entre le périphérique géré et le centre de Gestion.

[Étapes de dépannage]

- Réappliquez la stratégie qui sont liés à l'événement. Par exemple, si vous ne voyez pas des événements de connexion, réappliquez la stratégie d'Access Controil et voyez si des nouveaux événements maintenant sont reçus par le centre de Gestion.
- Si un centre de Gestion de FireSIGHT ne peut pas recevoir de nouveaux événements IPS, vérifiez s'il vous plaît s'il y a des questions de transmission entre le périphérique géré et le centre de Gestion.

Fichiers inconnus excessifs

- Le système de FireSIGHT enregistre les données **`inconnues de`** détection de réseau (SYSTÈME D'EXPLOITATION, hôte et information).

[Étapes de dépannage]

- Si le système ne peut pas déterminer le système d'exploitation sur un hôte sur votre réseau, vous pouvez employer Nmap pour balayer activement l'hôte. Nmap utilise les informations qu'il obtient du balayage d'évaluer les systèmes d'exploitation possibles. Il utilise alors le système d'exploitation qui a l'évaluation la plus élevée comme identification de système d'exploitation d'hôte.
- Créez une règle de corrélation que des déclencheurs quand le système détecte un hôte avec un système d'exploitation inconnu.
  La règle devrait déclencher quand un **événement de détection se produit** et les **informations de SYSTÈME D'EXPLOITATION pour un hôte ont changé** et elles remplissent les conditions suivantes : **Le nom de SYSTÈME D'EXPLOITATION est inconnu**.

Grande base de données pour enregistrer des événements

- Si vous augmentez la limite d'événement de base de données au delà de l'instruction ou de la pratique recommandée, le centre de Gestion de FireSIGHT peut manquer d'espace disque.

[Étapes de dépannage]

- Vérifiez les valeurs de la limite de base de données. Pour améliorer l'utilisation et la représentation de disque, vous devriez concevoir en fonction des limites d'événement le nombre d'événements que vous travaillez **régulièrement** avec. Pour quelques types d'événement, vous pouvez désactiver la mémoire.
- Afin de changer la limite de base de données, naviguez s'il vous plaît vers la page de stratégie de système, cliquez sur Edit à côté du nom de la stratégie de système, et puis cliquez sur la **base de données** du côté gauche la section. Pour accéder à la page de **stratégie de système**, naviguez s'il vous plaît vers le **système > la stratégie de gens du pays > de système**.

Recevez les alertes de santés pour plus de l'utilisation de disque de 85%

Possibles raison

- Le débit d'événement peut être très élevé. Par conséquent le périphérique est générant et enregistrant un bon nombre d'événements.
- Les problèmes de communication entre le périphérique géré et la Gestion de FireSIGHT centrent.

[Étapes de dépannage]

- Changer le seuil d'avertissement vigilant à 87% (avertissement) et à 92% (essentiel) peut être une solution simple pour fréquenter des alertes de santés.
- Lisez les notes de mise à jour pour voir s'il y avait un problème connu avec le système d'élagage. Quand une solution est disponible, mettez à jour s'il vous plaît la version de logiciel à la dernière release pour aborder cette question.

Les fichiers de /var/log/messages contiennent heures plus anciennes de données des que 24, ou les plus grands que 25MB

Possibles raison

- Le démon de Logrotate peut ne pas fonctionner correctement.

[Étapes de dépannage]

- Si vous rencontrez cette question, mettez à jour s'il vous plaît la version de logiciel de vos systèmes de FireSIGHT à la dernière release. Si vous exécutez la dernière version, mais éprouvez toujours cette question, entrez en contact avec s'il vous plaît le centre d'assistance technique Cisco (TAC).

Si la partition de racine (/) est pleine

Des fichiers utilisateurs sont enregistrés sur la partition de racine (/)

Possibles raison

- La partition de racine (`/`) est une taille fixe et n'est pas destinée pour la mémoire personnelle.
- `/var/tmp` drectory est utilisé manuellement pour la mémoire temporaire, au lieu du répertoire de `/var/common`.

[Étapes de dépannage]

- Vérifiez les fichiers inutiles sur `/root`, `/home`, et le répertoire de `/tmp`. Puisque ces répertoires ne sont pas créés pour la mémoire personnelle, vous pouvez supprimer n'importe quel fichier personnel avec la commande de `rm`.

Les processus non vérifiés écrivent pour enraciner (/) la partition

Possibles raison

- Si vous installez le logiciel tiers qui crée des fichiers sur la partition de racine (/), vous pouvez éprouver l'alerte de santés pour l'utilisation du disque élevée.

Étapes de dépannage

- Vérifiez si des modules sans support sont installés. Exécutez la commande suivante de trouver les modules installés :

```
admin@3DSystem:~$ rpm -qa --last
```

- Vérifiez le pstree et complétez pour voir si les processus non vérifiés s'exécutent. Exécutez les commandes suivantes :

```
admin@3DSystem:~$ pstree -ap admin@3DSystem:~$ top
```