Dépannage de l'utilisation excessive des disques sur les appliances Sourcefire

Contenu

Introduction

Un FireSIGHT Management Center ou un appareil FirePOWER peut manquer d'espace disque pour diverses raisons. Lorsque cela se produit, l'utilisation élevée du disque déclenche une alerte d'intégrité ou peut échouer une tentative de mise à jour logicielle. Cet article décrit les causes profondes de l'utilisation excessive des disques et quelques étapes de dépannage.

Étapes de vérification

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

Sur FireSIGHT Management Center,

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

Sur les appareils des gammes 7000 et 8000 et sur les appareils 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
```

Note: La taille et l'utilisation des disques peuvent varier selon les différents modèles d'appareils. S'il s'agit d'un périphérique virtuel NGIPS, vérifiez que la taille des partitions est conforme aux exigences minimales en matière d'espace disque.

Attention : Toute partition supplémentaire qui n'est pas affichée ci-dessus n'est pas prise en charge.

Sur les appliances des gammes 7000 et 8000 et sur les périphériques virtuels NGIPS, vous pouvez exécuter la commande suivante pour afficher des statistiques détaillées sur l'utilisation des disques :

```
> show disk-manager
```

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 /Volume est pleine

Anciens fichiers de sauvegarde

- Si vous stockez un volume important d'anciens fichiers de sauvegarde sur le système, il peut prendre trop d'espace sur votre disque.

Étapes de dépannage

- Supprimez les anciens fichiers de sauvegarde à l'aide de l'interface utilisateur Web. Pour supprimer des fichiers de sauvegarde, accédez à **System > Tools > Backup/Restore**.

  Astuce : Sur un système FireSIGHT, vous pouvez configurer le stockage à distance pour stocker les fichiers de sauvegarde volumineux.

Fichiers de mise à jour et de correctifs logiciels plus anciens

- Si vous conservez toujours les fichiers de mise à jour, de mise à niveau et de correctifs logiciels précédents (tels que, 5.0 ou 5.1), le système peut manquer d'espace disque.

Étapes de dépannage

- Supprimez les anciens fichiers de mise à jour et de correctifs qui ne sont plus nécessaires. Pour les supprimer, accédez à **System > Updates**.

Les Fichiers D'Événement Excessifs Sont Stockés

- Le périphérique ou le capteur géré a peut-être cessé d'envoyer des événements à FireSIGHT Management Center.
- Un périphérique peut générer plus d'événements qu'un Management Center n'est conçu pour recevoir (par seconde).
- Il peut y avoir un problème de communication entre le périphérique géré et le centre de gestion.

Étapes de dépannage

- Réappliquez la stratégie associée à l'événement. Par exemple, si vous ne voyez pas d'événements de connexion, réappliquez la stratégie de contrôle d'accès et vérifiez si de nouveaux événements sont maintenant reçus par Management Center.
- Si FireSIGHT Management Center ne peut pas recevoir de nouveaux événements IPS, vérifiez s'il existe des problèmes de communication entre le périphérique géré et le centre de gestion.

Nombre excessif de fichiers inconnus

- FireSIGHT System stocke les données de découverte de réseau **inconnues** (informations sur le système d'exploitation, l'hôte et le service).

Étapes de dépannage

- Si le système ne peut pas déterminer le système d'exploitation d'un hôte sur votre réseau, vous pouvez utiliser Nmap pour analyser activement l'hôte. Nmap utilise les informations qu'il obtient de l'analyse pour évaluer les systèmes d'exploitation possibles. Il utilise ensuite le système d'exploitation qui a la plus haute qualification comme identification du système d'exploitation hôte.
- Créez une règle de corrélation qui se déclenche lorsque le système détecte un hôte avec un système d'exploitation inconnu.
  La règle doit se déclencher lorsqu'**un événement de découverte se produit** et que **les informations du système d'exploitation d'un hôte ont changé** et remplissent les conditions suivantes : **Nom du système d'exploitation inconnu**.

Base de données volumineuse pour stocker les événements

- Si vous augmentez la limite d'événements de base de données au-delà des directives ou des meilleures pratiques, FireSIGHT Management Center peut manquer d'espace disque.

Étapes de dépannage

- Vérifiez les valeurs de la limite de base de données. Pour améliorer l'utilisation et les performances des disques, vous devez adapter les limites d'événements au nombre d'événements que vous traitez **régulièrement**. Pour certains types d'événements, vous pouvez désactiver le stockage.
- Afin de modifier la limite de base de données, accédez à la page Stratégie système, cliquez sur **Modifier** en regard du nom de la stratégie système, puis cliquez sur **Base de données** dans la section gauche. Pour accéder à la page **Stratégie système**, accédez à **Système > Local > Stratégie système**.

Recevoir Des Alertes D'État De Santé Pour Plus De 85 % D'Utilisation Des Disques

Raisons possibles

- Le taux d'événements peut être très élevé. Par conséquent, le périphérique génère et stocke de nombreux événements.
- Problèmes de communication entre le périphérique géré et FireSIGHT Management Center.

Étapes de dépannage

- La modification du seuil d'alerte à 87 % (Avertissement) et 92 % (Critique) peut constituer une solution simple pour les alertes fréquentes.
- Lisez les Notes de version pour voir s'il y a eu un problème connu avec le système d'élagage. Lorsqu'une solution est disponible, mettez à jour la version du logiciel vers la dernière version pour résoudre ce problème.

Les fichiers /var/log/messages contiennent des données de plus de 24 heures ou de plus de 25 Mo

Raisons possibles

- Le démon de logrotate ne fonctionne peut-être pas correctement.

Étapes de dépannage

- Si vous rencontrez ce problème, mettez à jour la version logicielle de vos systèmes FireSIGHT vers la dernière version. Si vous utilisez la dernière version, mais que vous rencontrez toujours ce problème, contactez le centre d'assistance technique Cisco (TAC).

Si la partition racine (/) est pleine

Les fichiers utilisateur sont enregistrés sur la partition racine (/)

Raisons possibles

- La partition racine (/) est de taille fixe et n'est pas destinée au stockage personnel.
- Le répertoire /var/tmp est utilisé manuellement pour le stockage temporaire, au lieu du répertoire /var/common.

Étapes de dépannage

- Recherchez les fichiers inutiles dans le dossier /root, /home et /tmp. Comme ces dossiers ne sont pas créés pour le stockage personnel, vous pouvez supprimer n'importe quel fichier personnel avec la commande rm.

Les processus non pris en charge écrivent sur la partition racine (/)

Raisons possibles

- Si vous installez un logiciel tiers qui crée des fichiers sur la partition racine (/), vous pouvez recevoir une alerte d'intégrité pour une utilisation élevée du disque.

Étapes de dépannage

- Vérifiez si des paquets non pris en charge sont installés. Exécutez la commande suivante pour rechercher les packages installés :

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

- Vérifiez pstree et top pour voir si des processus non pris en charge sont en cours d'exécution. Exécutez les commandes suivantes :

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

```
admin@3DSystem:~$ top
```