Résoudre l'erreur de disque plein de Secure Web Appliance

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Erreurs liées au disque plein

Surveiller l'utilisation du disque

- Afficher l'utilisation du disque dans l'interface graphique
- Afficher l'utilisation du disque dans CLI

Structure du disque et dépannage de la partition complète

- La partition racine est pleine
- La partition racine suivante est pleine
- La partition Var est pleine
- Partition du système d'exploitation à XX % de capacité
- La partition de signalement/consignation est pleine
  - Les fichiers journaux occupent trop d'espace disque
  - Fichiers principaux sur le périphérique
  - Les rapports occupent trop d'espace disque
  - Les journaux internes occupent le disque

Autres informations utiles

Introduction

Ce document décrit les étapes à suivre pour résoudre les erreurs d'espace disque total dans l'appliance Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès FTP à SWA

- Accès à la CLI de SWA
- Accès administratif à SWA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Erreurs liées au disque plein

Plusieurs erreurs et avertissements dans SWA indiquent que le disque est plein ou que l'espace disque est presque plein. Il s'agit d'une liste d'erreurs et d'avertissements. Ces journaux varient dans chaque version du logiciel en raison des méthodes de livraison, telles que les alertes, les journaux système ou le résultat de la commande à partir de l'interface de ligne de commande (CLI) displayalerts.

```
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage
User admin  Disk space for /data has exceeded threshold value 90% with current capacity of 99 %

The reporting/logging disk is full on a WSA
This appliance has disk usage that is higher than expected.
WARNING: Data partition utilization on appliance is high and can cause issues
```

Surveiller l'utilisation du disque

Vous pouvez surveiller et afficher l'utilisation du disque à partir de l'interface graphique et de la CLI.

Afficher l'utilisation du disque dans l'interface graphique

Après vous être connecté à l'interface graphique utilisateur de SWA, dans la page My-Dashboard, vous pouvez afficher l' **Reporting / Logging Disk**utilisation à partir de la **System Overview** section.

Remarque : Les rapports et les journaux SWA sont stockés dans une seule partition, appelée partition DATA.

Dans l'interface utilisateur graphique, sous le **Reporting**Menu, accédez également à System Status. Vous pouvez également afficher l'utilisation du disque à partir de la **Overview** section, sous le menu Reporting.

Afficher l'utilisation du disque dans CLI

À partir de la sortie de l'état ou des détails d'état, vous pouvez afficher l'utilisation du disque de création de rapports / de journalisation :

```
SWA.CLI> status

Enter "status detail" for more information.

Status as of:                  Sun Feb 19 19:55:13 2023 CET
Up since:                      Sat Feb 11 14:00:56 2023 CET (8d 5h 54m 17s)
System Resource Utilization:
  CPU                                  25.9%
  RAM                                  13.6%
  Reporting/Logging Disk               58.1%
```

À partir du résultat de **ipcheck**, vous pouvez afficher l'espace disque alloué à chaque partition et le pourcentage d'espace utilisé par partition :

```
SWA.CLI> ipcheck
...
  Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            200GB
=== Skipped ===
  Root                  4GB 65%
  Nextroot              4GB 1%
  Var                   400MB 29%
  Log                   130GB 8%
  DB                    2GB 0%
  Swap                  8GB
  Proxy Cache           50GB
=== Skipped ===
```

Dans les journaux SHD, l'utilisation du disque de création de rapports / de journalisation pour chaque minute est affichée sous la forme DskUtil. Pour accéder aux journaux SHD, procédez comme suit :

1. Tapez grep ou tail dans la CLI.

2. Rechercher le type shd_logs : Récupération des journaux SHD : Sondage FTP, dans la liste et saisissez le numéro associé.

3. Dans Entrez l'expression régulière à grep, vous pouvez entrer une expression régulière pour effectuer une recherche dans les journaux. Par exemple, vous pouvez taper la date et l'heure.

4. Voulez-vous que cette recherche ne respecte pas la casse ? [Y]**>**, vous pouvez conserver cette valeur par défaut, sauf si vous devez rechercher la distinction majuscules/minuscules, ce qui, dans les journaux SHD, n'est pas nécessaire.

5. Voulez-vous rechercher des lignes non correspondantes ? [N]**>**, vous pouvez définir cette ligne comme valeur par défaut, sauf si vous devez rechercher tout sauf votre expression grep normale.

6. Voulez-vous suivre les journaux ? [N]**>**, Cette option n'est disponible que dans la sortie du grep, si vous la conservez comme valeur par défaut (N), elle affiche les journaux SHD de la première ligne du fichier courant.

7. Voulez-vous paginer le résultat ? [N]**>**, Si vous sélectionnez Y, le résultat est le même que celui de la commande less. Vous pouvez naviguer entre les lignes et les pages. Vous pouvez également effectuer une recherche dans les journaux (tapez / puis le mot-clé et appuyez sur Entrée). Pour quitter le journal, tapezq.

Dans cet exemple, 52,2 % de la **Reporting / Logging Disk** quantité est consommée :

```
Mon Feb 20 23:46:14 2023 Info: Status: CPULd 66.4 DskUtil 52.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cac
```

Structure du disque et dépannage de la partition complète

Comme indiqué précédemment dans la sortie de ipcheck, il existe sept partitions dans SWA :

Nom de partition	Description
Racine	Conserve les fichiers système internes
Nextroot	Cette partition est utilisée pour les mises à niveau
Var	Conserve les fichiers système internes
Journal	Contient des journaux et des fichiers de rapports
DB	Configuration et bases de données internes
Échange	Mémoire SWAP
Cache proxy	Conserve les données en cache

La partition racine est pleine

Si la partition racine (connue sous le nom de rootfs ou /) est pleine ou supérieure à 100 %, ce qui est parfois attendu, et que le SWA supprime les fichiers inutiles. Si vous voyez une baisse des performances du système, essayez d'abord de redémarrer l'appliance, puis vérifiez la capacité du disque de la partition racine. Si le problème persiste, contactez le service client Cisco pour ouvrir un dossier TAC.

La partition racine suivante est pleine

Si votre mise à niveau échoue, assurez-vous que votre partition racine suivante dispose de suffisamment d'espace libre pour la mise à niveau.

Initialement, les images SMA virtuelles SWA, ESA (Email Security Appliance) et SMA (Virtual Security Management Appliance) ont été créées avec une partition racine suivante d'une taille inférieure à 500 Mo. Au fil des ans, et avec les nouvelles versions d'AsyncOS qui incluent des fonctionnalités supplémentaires, les mises à niveau ont utilisé cette partition tout au long du processus de mise à niveau. Lorsque vous essayez de mettre à niveau des versions plus anciennes, les mises à niveau échouent en raison de la taille de la partition.

Dans les journaux de mise à niveau de la CLI, vous pouvez afficher les erreurs suivantes :

```
Finding partitions... done.
Setting next boot partition to current partition as a precaution... done.
Erasing new boot partition... done.
Extracting eapp done.
Extracting scanerroot done.
Extracting splunkroot done.
Extracting savroot done.
Extracting ipasroot done.
Extracting ecroot done.
Removing unwanted files in nextroot done.
Extracting distroot
/nextroot: write failed, filesystem is full
./usr/share/misc/termcap: Write failed
./usr/share/misc/pci_vendors: Write to restore size failed
./usr/libexec/getty: Write to restore size failed
./usr/libexec/ld-elf.so.1: Write to restore size failed
./usr/lib/libBlocksRuntime.so: Write to restore size failed
./usr/lib/libBlocksRuntime.so.0: Write to restore size failed
./usr/lib/libalias.so: Write to restore size failed
./usr/lib/libarchive.so: Write to restore size failed
```

Pour un SWA virtuel, téléchargez un nouveau fichier image à partir du Guide d'installation de l'appliance virtuelle de messagerie électronique et Web sécurisée Cisco. Importez ensuite la sauvegarde de la configuration de l'ancienne version vers le SWA nouvellement installé. Si une erreur d'importation de configuration s'affiche, ouvrez un dossier de demande de service.

Pour SMA et ESA, vous pouvez trouver une solution de contournement pour ce problème : Comment appliquer la solution de contournement pour la mise à niveau de Cisco vESA/vSMA échouée en raison de la petite taille de partition - Cisco.

La partition Var est pleine

Si la **var** partition est pleine, vous pouvez recevoir ces erreurs lorsque vous vous connectez à CLI ou à partir de la commande Displayalerts dans CLI :

```
/var: write failed, filesystem is full
The temporary data partition is at 99% capacity
```

Pour résoudre ce problème, redémarrez d'abord l'appliance. Si la capacité de la partition /var est supérieure à 100 %, contactez l'assistance du centre d'assistance technique Cisco.

Partition du système d'exploitation à XX % de capacité

Si vous recevez l'erreur « La partition du système d'exploitation est à 91 % de sa capacité », cela est généralement lié à la partition /nextroot. À partir de la CLI, exécutez la commande ipcheck :

```
SWA_CLI> ipcheck
...

  Disk 0                1024GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            1024GB

  Root                  2GB 95%
  Nextroot              2GB 92%
  Var                   400MB 60%
  Log                   808GB 21%
  DB                    2GB 0%
  Swap                  8GB
  Proxy Cache           200GB
```

Si la taille de la partition racine suivante est de 2 Go, en raison de la notice de champ : FN72230, vous devez installer une nouvelle version de machine virtuelle supérieure à 14.5 dans la partition racine suivante et elle doit être de 4 Go. Vous devez également migrer de l'ancien SWA vers le nouveau.

Pour plus d'informations, référez-vous à Comment appliquer la solution de contournement pour la mise à niveau échouée de Cisco vESA/vSMA en raison de la petite taille de partition.

La partition de signalement/consignation est pleine

Si la partition Création de rapports / Journalisation est pleine, voici quelques erreurs que vous pouvez rencontrer :

```
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage
User admin  Disk space for /data has exceeded threshold value 90% with current capacity of 99 %

The reporting/logging disk is full on a WSA

WARNING: Data partition utilization on appliance is high and can cause issues
```

La cause première de ces erreurs peut être classée comme suit :

1. Les fichiers journaux occupent trop d'espace disque.

2. Certains fichiers principaux générés sur le périphérique entraînent une utilisation complète du disque.

3. Les rapports occupent trop d’espace disque.

4. Le suivi Web occupe trop d’espace disque.

5. Certains journaux internes occupent trop d’espace disque.

Les fichiers journaux occupent trop d'espace disque

Pour afficher les fichiers journaux, vous pouvez vous connecter au SWA via FTP à l'interface de gestion.

 Remarque : FTP est désactivé par défaut.

Pour activer le protocole FTP à partir de l'interface utilisateur graphique, procédez comme suit :

1. Connectez-vous à l'interface utilisateur graphique.

2. Cliquez sur Interfaces dans le menu Network.

3. Cliquez sur Modifier les paramètres.

4. Sélectionnez FTP dans la section Appliance Management Services.

5. (facultatif) : Vous pouvez modifier le port FTP par défaut.

6. Cliquez sur Soumettre.

7. Validez les modifications.

Après la connexion FTP, vous pouvez afficher les journaux, la date de création et la taille de chaque fichier journal. Si vous devez archiver les journaux, vous pouvez les télécharger via FTP. Vous pouvez également supprimer d'anciens journaux pour libérer de l'espace disque.

Pour résoudre ce problème, procédez comme suit :

Conseil : Si vous voyez que les fichiers journaux n'occupaient pas beaucoup d'espace disque, le problème est probablement lié aux rapports ou aux fichiers de base.

Fichiers principaux sur le périphérique

Pour savoir si SWA possède des fichiers de base, procédez comme suit à partir de l'interface CLI :

1. Connectez-vous à CLI.

2. Exécutez la commande diagnostic (il s’agit d’une commande masquée qui ne peut pas être remplie automatiquement avec la touche TAB).

3. Tapez PROXY.

4. Tapez LIST.

Le résultat indique s'il existe des fichiers de base. Pour supprimer les fichiers de base, contactez le service d'assistance Cisco. Un ingénieur TAC doit rechercher la cause des fichiers de base, puis il peut supprimer les fichiers.

Les rapports occupent trop d'espace disque

Il existe deux types de rapports dans SWA : Rapports et suivi Web. WebTracking occupe la plus grande partie de l'espace disque. Pour vérifier l'historique de WebTracking, accédez à WebTracking à partir de l'interface utilisateur graphique. Dans le menu Reporting, dans la section Time Range, sélectionnez Custom Range.. Les dates mises en surbrillance affichent l'historique des rapports de suivi WebTracking.

Pour effectuer une sauvegarde à partir de WebTracking, vous pouvez exporter le rapport au format .CSV à partir du lien Téléchargement imprimable du rapport.

Conseil : Évitez de générer des rapports WebTracking pendant de longues périodes, qui dépendent du trafic Web quotidien normal. Les rapports de plus longue durée peuvent entraîner l'inactivité de SWA.

Au moment de la rédaction de cet article, il n'y a aucune fonctionnalité pour supprimer manuellement les rapports plus anciens (ID de bogue Cisco : CSCun82094).

Pour supprimer certains de vos rapports, vous devez contacter l'assistance TAC. Vous pouvez également supprimer tous les rapports de l'interface de ligne de commande en procédant comme suit :

1. Connectez-vous à CLI.

2. Exécutez la commande diagnostic (il s'agit d'une commande masquée qui ne peut pas être exécutée automatiquement avec la touche TAB).

3. Tapez REPORTING et appuyez sur Entrée.

4. Tapez DELETEDB et appuyez sur Entrée.

Mise en garde : Cette commande supprime toutes les données des rapports et ne peut pas être abandonnée.

Si vous avez SWA S195 ou S190, considérez également ce défaut : ID de bogue Cisco CSCwd83093.

Les journaux internes occupent le disque

Si votre périphérique présente les conditions de l'ID de bogue Cisco : CSCvy69039, vous devez ouvrir un dossier TAC pour vérifier les journaux internes du back-end et supprimer manuellement les fichiers journaux volumineux.

Il s'agit d'une solution de contournement temporaire, mais sur la version concernée, le fichier journal est automatiquement créé après la suppression et la taille du fichier augmente de nouveau de 0 à plusieurs reprises.

Autres informations utiles

- Notes de version de WSA AsyncOS
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.