Verwalten der lokalen Dateisystem-/Festplattennutzung in sicheren Netzwerkanalysen

Inhalt

Einleitung

In diesem Dokument werden allgemeine Schritte zur Reduzierung der Festplattennutzung auf Secure Network Analytics Manager- und Flow Collector-Geräten beschrieben.

Voraussetzungen

Anforderungen

Dieses Dokument gilt für Bereitstellungen von Secure Network Analytic ohne Datenspeicher.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Network Analytics Manager - v7.1+
- Secure Network Analytics FlowCollector - v7.1+
- Secure Network Analytics Flow Sensor - v7.1+
- Sichere Netzwerkanalysen UDP Director - v7.1+

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Es gibt zwei Partitionen, die auf die Festplattennutzung überwacht werden müssen: die Root-Partition (/) und die /lancope/var-Partition.

Die Root-Partition (/) ist der Speicherort für das Kernel-Image und einige Systemprotokolle. Dies ist normalerweise eine kleinere Partition mit 20G oder weniger. /lancope/var ist eine Volume-Gruppe und ist der Speicherort für die meisten Systemdaten, sodass der größte Teil des Festplattenspeichers für die Appliance belegt wird.

Daten sammeln

Es gibt zwei Stellen, an denen Sie Informationen zur Datenträgerverwendung abrufen können: die Admin-Webbenutzeroberfläche und die Befehlszeilenschnittstelle (Command Line Interface, CLI).

Befehlszeile

Führen Sie in der Befehlszeile Folgendes aus: **df -ah / /lancope/var** und notieren Sie die Leerzeichen zwischen (/) und /lancope/var.

```
732smc:/# df -ah / /lancope/var/
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 20G 8.3G 9.9G 46% /
/dev/mapper/vg_lancope-_var 108G 23G 83G 22% /lancope/var
732smc:/#
```

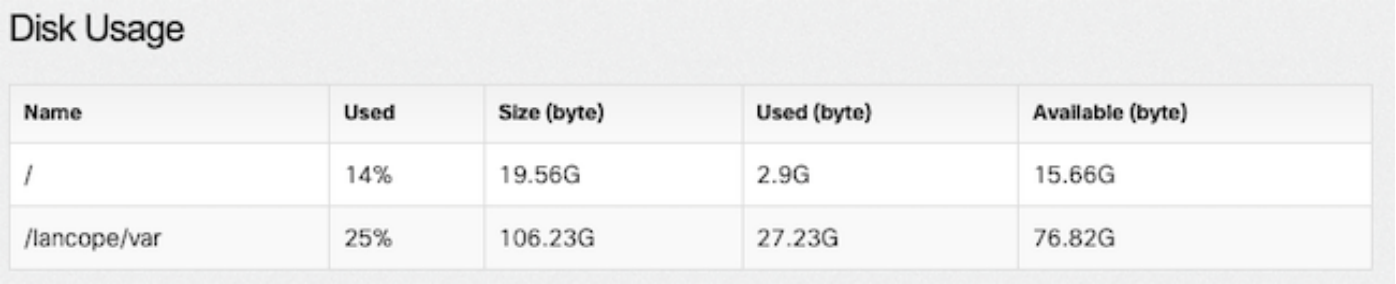
Die Ausgabe zeigt, dass die Root-Partition (/) 20 G beträgt und 8.3G verwendet wird, was 46 % beträgt. Die Ausgabe zeigt auch, dass die /lancope/var-Partition 108G ist und 23G verwendet wird, was 22% ist.

Webbasierte Benutzeroberfläche

Melden Sie sich je nach Modell bei der Admin-Benutzeroberfläche des Geräts an, und führen Sie einen Bildlauf nach unten durch.

Liste der Webadressen der Admin-Benutzeroberfläche:

- Secure Network Analytics Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (Sie müssen sich beim SMC anmelden, bevor Sie auf diese URL zugreifen können)
- Flow Collector für sichere Netzwerkanalysen: https://<FC-IP-OR-FQDN>/swa/index.html
- Secure Network Analytics Flow Sensor - https://<FS-IP-OR-FQDN>/fs/index.html
- Sichere Netzwerkanalysen - UDP Director (Flow Replicator) - https://<UDPD-IP-OR-FQDN>/fr/index.html



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	14%	19.56G	2.9G	15.66G
/lancope/var	25%	106.23G	27.23G	76.82G

Wenn die Partition eine hohe Auslastung von mindestens 75 % aufweist, wird die Partition hervorgehoben.

Festplattenspeicher leeren

Wenn Sie sich nicht sicher sind, welche Dateien sicher gelöscht werden können, öffnen Sie ein TAC-Ticket, oder wenden Sie sich an den Cisco Support über die Kontaktseite für den weltweiten Cisco Support im Abschnitt "Verwandte Informationen" am Ende dieses Dokuments.

Systemprotokolle

Eine der schnellsten Methoden zur Wiederherstellung von größerem Festplattenspeicher ist das Löschen von Journalprotokollen mit dem journalctl --vacuum-time 1d aus. Beachten Sie den doppelten Bindestrich vor dem Wort "Vakuum".

```
732smc:/# journalctl --vacuum-time 1d
Deleted archived journal /var/log/journal/639c60e1e407f646b5ed1751cde413fa
/user-1000@db376b09011842d5b247f6d31de6c241-00000000004ec2a8-0005e7838ecf15cc.journal (8.0M).
<the above line repeats>
Vacuuming done, freed 3.9G of archived journals from
/var/log/journal/639c60e1e407f646b5ed1751cde413fa.
732smc:/# df -ah / /lancope/var/
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 20G 8.3G 9.9G 46% /
/dev/mapper/vg_lancope-_var 108G 19G 87G 18% /lancope/var
732smc:/#
```

Etwa 4G Speicherplatz wurde aus diesen Schritten zurückgewonnen und führte zu einer Verringerung der Festplattennutzung von 22 % auf 18 % auf der /lancope/var-Partition.

Dateien in den aufgelisteten Verzeichnissen können im Allgemeinen sicher gelöscht werden:

```
/lancope/var/tcpdump
/lancope/var/tomcat/logs
/lancope/var/tmp
/lancope/var/admin/tmp/
```

Es wird empfohlen, entweder im Stammverzeichnis (/) oder im Verzeichnis /lancope/var zu starten, je nachdem, welche Partition Sie in der Web-UI identifiziert haben, die eine hohe Datenträgerauslastung aufweist. Ändern Sie das aktuelle Verzeichnis mit dem cd / aus.

Führen Sie du -xah --max-depth=1 | sort -hr -Befehl, um die größten Verbraucher des Speicherplatzes des aktuellen Verzeichnisses zu ermitteln. Beachten Sie den doppelten Bindestrich — vor der maximalen Tiefe.

Die Ausgabe zeigt, dass die Root-Partition (/) 8,3 G Speicherplatz belegt, wobei 5,5 G

Speicherplatz im Verzeichnis /lancope verwendet wird, gefolgt vom Verzeichnis /usr mit 1,5 G Nutzung.

```
732smc:~# cd /
732smc:/# du -xah --max-depth=1 | sort -hr | head -n4
8.3G .
5.5G ./lancope
1.5G ./usr
1.3G ./opt
732smc:/#
```

Wechseln Sie mit dem Befehl **cd lancope/** und gebe den Befehl du erneut mit dem Befehl !du aus. Dadurch wird nun angezeigt, dass von dem 5.5G, das im Verzeichnis /lancope/ verwendet wird, 5.1G im Admin-Verzeichnis vorhanden ist. Wechseln Sie mit dem cd aus.

```
732smc:/# cd lancope/
732smc:/lancope# !du
du -xah --max-depth=1 | sort -hr | head -n4
5.5G .
5.1G ./admin
212M ./services
59M ./mongodb
732smc:/lancope#
```

Sobald Sie Dateien identifiziert haben, die gelöscht werden können, können Sie dies mit dem **rm -i** aus. Wenn Sie sich nicht sicher sind, welche Dateien sicher gelöscht werden können, öffnen Sie ein TAC-Ticket, oder wenden Sie sich an den Cisco Support über die Kontaktseite für den weltweiten Cisco Support im Abschnitt "Verwandte Informationen" am Ende dieses Dokuments.

```
732smc:/lancope/admin# rm -i file
rm: remove regular empty file 'file'? yes
732smc:/lancope/admin#
```

Wiederholen Sie diese Schritte bei Bedarf.

Zuschneiden der verteilten Datenbank (DDS) - Flow-Statistiken

Standardmäßig versuchen die FlowCollector- und SMC-Appliances in der DDS-Umgebung, täglich so viele Flow-Daten wie möglich rotiert zu speichern. Wenn die Grenzwerte für die Festplattennutzung erreicht werden, beginnt das System, die ältesten Daten zuerst zu löschen, um Platz für neue zu speichernde Daten zu schaffen.

Melden Sie sich zur Anzeige der FlowCollector-Datenbankstatistiken in der FlowCollector-Admin-Benutzeroberfläche an, und wählen Sie dann Support > Database Storage Statistics .

- Das Bild zeigt, dass die aufgenommenen Flow-Details (Netflow-Daten) durchschnittlich etwa 455 MB pro Tag betragen und dieser Flow Collector etwa 25,5 G Daten gespeichert hat.
- Das Bild zeigt, dass die aufgenommenen Flow-Schnittstellendetails (schnittstellenspezifische Statistiken) durchschnittlich etwa 800 MB pro Tag betragen. In diesem Flow Collector sind etwa 6 G Daten gespeichert.
- Das Bild zeigt, dass die Flow-Daten durchschnittlich 1,2 GB pro Tag ausmachen und dass dieser Flow Collector ca. 32 GB an gesamten Daten speichert.
- Wenn Sie die Datenbank auf ca. 5G Gesamtdaten reduzieren möchten, teilen Sie diese durch den Tagesdurchschnitt von 1,2G auf, was 4 entspricht.

Um die Datenbank auf eine Gesamtgröße von ca. 5 GB zu reduzieren, ändern Sie **Summary_retention_days** auf 4. Navigieren Sie anschließend zu Support > Advanced Settings . Suchen summary_retention_days und ändern Sie den Wert auf den gewünschten Wert.

Fügen Sie anschließend am Ende der Liste eine neue Option hinzu. Die Fehlermeldung Add New Option Wert ist strict_retention_days und **Option Value** -Wert auf 1 gesetzt, wie im Bild dargestellt. Klicken Sie auf Hinzufügen. Diese strict_retention_days weist die Engine an, nur die Anzahl der Tage zu behalten, die in **Summary_retention_days** .

Sobald ich die **summary_retention_days** zu 4 und ich habe den neuen Optionswert hinzugefügt, drücken Sie Apply unten auf der Seite.

Wenn Sie diese Schritte für ein Upgrade durchführen möchten, löschen Sie **strict_retention_days** - Wert ein, wenn das Upgrade abgeschlossen ist, damit die Daten so lange wie möglich gespeichert werden.

Zuschneiden der verteilten Datenbank (DDS) - Details der Datenflussschnittstelle

1. Protokoll inzu Ihre StealthWatch Desktop Kunde als Die Fehlermeldung Administrator Benutzer.

2. Suchen Sie den FlowCollector in der Enterprise-Struktur. Klicken Sie auf das Plus (+) um den Container zu erweitern.

3. Klicken Sie mit der rechten Maustaste auf den gewünschten FlowCollector.
Auswählen Configuration > Properties.

4. In Die Fehlermeldung DurchflussCollector Eigenschaften Dialog Feld, Klicken Sie auf Advanced.

5. Auswählen Die Fehlermeldung Store **flow interface data**feld. Festlegen Die Fehlermeldung Grenzwert zu Up zu 15 Tage Oder 30 Tage.

6. Klicken Sie auf OK .

Mehr Speicherplatz (nur virtuelle Appliances)

Schalten Sie das virtuelle System aus, und erhöhen Sie die dem virtuellen System über den Hypervisor zugewiesene Festplattengröße. Der zusätzliche Speicherplatz wird der /lancope/var/-Partition zugewiesen.

Möglicherweise sind zusätzliche Schritte erforderlich, damit StealthWatch diesen nicht zugewiesenen Speicherplatz nach einem Neustart belegt. Lesen Sie die Datenspeicherung des Installationsleitfadens für Ihre Virtual Machine Edition nach, um die erforderliche Festplattengröße zu ermitteln.

Die Größe der Stamm-Partition (/) ist statisch und kann nicht angepasst werden. Eine Neuinstallation auf eine Version mit einer größeren Root-Partition, die während der Installation erstellt wurde, ist erforderlich.

Zugehörige Informationen

- Installationsanleitungen
- Secure Network Analytics - Technischer Support und Dokumentation - Cisco Systems
- Weltweiter Kontakt zum Cisco Support

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.