Risoluzione dei problemi di utilizzo eccessivo del disco sull'appliance Sourcefire

Sommario

Introduzione

Un centro di gestione FireSIGHT o un'appliance FirePOWER può esaurire lo spazio su disco per vari motivi. In questo caso, l'elevato utilizzo del disco attiva un avviso di integrità o potrebbe non riuscire un tentativo di aggiornamento del software. In questo articolo vengono descritte le cause principali di un utilizzo eccessivo del disco e alcune procedure per la risoluzione dei problemi.

Fasi di verifica

Determinare la partizione utilizzata con maggiore frequenza. Il comando seguente mostra l'utilizzo del disco:

Su un centro di gestione FireSIGHT,

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

Sugli accessori serie 7000 e 8000 e sui dispositivi virtuali NGIPS:

```
> show disk
```

Entrambi i comandi mostrano un output simile al seguente:

```
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
```

Nota: Le dimensioni e l'utilizzo dei dischi possono variare a seconda del modello di appliance. Se si tratta di un dispositivo virtuale NGIPS, verificare che le dimensioni delle partizioni siano conformi ai requisiti minimi di spazio su disco.

Attenzione: Le partizioni aggiuntive non visualizzate in precedenza non sono supportate.

Sugli accessori serie 7000 e 8000 e sui dispositivi virtuali NGIPS, è possibile eseguire il comando seguente per visualizzare statistiche dettagliate sull'utilizzo del disco:

```
> show disk-manager
```

Un esempio di output:

```
> 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
```

Se la partizione /Volume è piena

Vecchi file di backup

- Se si archiviano nel sistema grandi volumi di vecchi file di backup, lo spazio su disco potrebbe essere eccessivo.

Procedura di risoluzione dei problemi

- Eliminare i vecchi file di backup utilizzando l'interfaccia utente Web. Per rimuovere i file di backup, selezionare **Sistema > Strumenti > Backup/Ripristino**.

  Suggerimento: Su un sistema FireSIGHT, è possibile configurare lo storage remoto per memorizzare i file di backup di grandi dimensioni.

Aggiornamenti software e file patch meno recenti

- Se si mantengono sempre i precedenti file di aggiornamento, aggiornamento e patch del software (ad esempio, 5.0 o 5.1), il sistema potrebbe esaurire lo spazio su disco.

Procedura di risoluzione dei problemi

- Eliminare i file di aggiornamento e di patch precedenti non più necessari. Per eliminarli, selezionare **Sistema > Aggiornamenti**.

Numero eccessivo di file di eventi archiviati

- Èpossibile che il dispositivo o il sensore gestito abbia interrotto l'invio di eventi al centro di gestione FireSIGHT.
- Èpossibile che un dispositivo stia generando più eventi di quelli che un centro di gestione è progettato per ricevere (al secondo).
- Potrebbe essersi verificato un problema di comunicazione tra il dispositivo gestito e il centro di gestione.

Procedura di risoluzione dei problemi

- Riapplicare i criteri correlati all'evento. Se ad esempio gli eventi di connessione non vengono visualizzati, riapplicare il criterio Controllo di accesso e verificare se il Centro di gestione sta ricevendo nuovi eventi.
- Se un centro di gestione FireSIGHT non è in grado di ricevere nuovi eventi IPS, verificare la presenza di eventuali problemi di comunicazione tra il dispositivo gestito e il centro di gestione.

Numero eccessivo di file sconosciuti

- Il sistema FireSIGHT memorizza i dati **sconosciuti di** Network Discovery (informazioni su sistema operativo, host e servizio).

Procedura di risoluzione dei problemi

- Se il sistema non è in grado di determinare il sistema operativo su un host della rete, è possibile utilizzare Nmap per eseguire una scansione attiva dell'host. Nmap utilizza le informazioni ottenute dalla scansione per valutare i possibili sistemi operativi. Viene quindi utilizzato il sistema operativo con la classificazione più alta come identificazione del sistema operativo host.
- Creare una regola di correlazione che viene attivata quando il sistema rileva un host con un sistema operativo sconosciuto.
  La regola deve essere attivata quando **si verifica un evento di individuazione** e **le informazioni sul sistema operativo per un host sono state modificate** e soddisfa le condizioni seguenti: **Nome del sistema operativo sconosciuto**.

Database di grandi dimensioni per l'archiviazione di eventi

- Se si aumenta il limite di eventi del database oltre le linee guida o le best practice, lo spazio su disco del centro di gestione FireSIGHT potrebbe esaurirsi.

Procedura di risoluzione dei problemi

- Controllare i valori del limite del database. Per migliorare l'utilizzo e le prestazioni del disco, è

necessario personalizzare i limiti degli eventi in base al numero di eventi utilizzati **regolarmente**. Per alcuni tipi di eventi è possibile disattivare l'archiviazione.
- Per modificare il limite del database, passare alla pagina Criteri di sistema, fare clic su **Modifica** accanto al nome del criterio di sistema e quindi su **Database** nella sezione a sinistra. Per accedere alla pagina **Criteri di sistema**, selezionare **Sistema > Locale > Criteri di sistema**.

Ricezione Di Avvisi Di Integrità Per Un Utilizzo Del Disco Superiore All'85%

Possibili motivi

- La frequenza degli eventi potrebbe essere molto alta. Pertanto, il dispositivo genera e memorizza numerosi eventi.
- Problemi di comunicazione tra il dispositivo gestito e FireSIGHT Management Center.

Procedura di risoluzione dei problemi

- Modificare il livello di soglia dell'avviso all'87% (Avviso) e al 92% (Critico) può essere una soluzione semplice per gli avvisi frequenti relativi allo stato di salute.
- Leggere le note sulla versione per verificare se si è verificato un problema noto con il sistema di potatura. Quando è disponibile una soluzione, aggiornare la versione del software all'ultima release per risolvere il problema.

I file /var/log/messages contengono dati più vecchi di 24 ore o più grandi di 25 MB

Possibili motivi

- Èpossibile che il daemon Logrotate non funzioni correttamente.

Procedura di risoluzione dei problemi

- Se si verifica questo problema, aggiornare la versione software dei sistemi FireSIGHT all'ultima release. Se si utilizza la versione più recente ma il problema persiste, contattare il Technical Assistance Center (TAC) di Cisco.

Se la partizione radice (/) è piena

I file utente vengono salvati nella partizione radice (/)

Possibili motivi

- La partizione radice (/) ha dimensioni fisse e non è destinata all'archiviazione personale.
- La directory /var/tmp viene utilizzata manualmente per la memorizzazione temporanea, anziché la directory /var/common.

Procedura di risoluzione dei problemi

- Verificare la presenza di file non necessari nella cartella /root, /home e /tmp. Poiché queste cartelle non vengono create per l'archiviazione personale, è possibile eliminare qualsiasi file personale con il comando rm.

Processi non supportati durante la scrittura nella partizione radice (/)

Possibili motivi

- Se si installa un software di terze parti che crea file nella partizione radice (/), è possibile che venga visualizzato un avviso di integrità per l'utilizzo elevato del disco.

Procedura di risoluzione dei problemi

- Verificare se sono installati pacchetti non supportati. Eseguire il comando seguente per trovare i pacchetti installati:

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

- Selezionare pstree e top per verificare se sono in esecuzione processi non supportati. Eseguire i comandi seguenti:

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

admin@3DSystem:~$ top
```