



Configurare l'accesso al client di audit

StorageGRID 11.7

NetApp
April 12, 2024

Sommario

- Configurare l'accesso al client di audit 1
 - Configurare l'accesso client di audit per NFS 1
 - Aggiungere un client di audit NFS a una condivisione di audit 3
 - Verificare l'integrazione dell'audit NFS. 4
 - Rimuovere un client di audit NFS dalla condivisione di audit. 5
 - Modificare l'indirizzo IP di un client di audit NFS 6

Configurare l'accesso al client di audit

Configurare l'accesso client di audit per NFS

Il nodo di amministrazione, tramite il servizio Audit Management System (AMS), registra tutti gli eventi di sistema controllati in un file di registro disponibile attraverso la condivisione dell'audit, che viene aggiunto a ciascun nodo di amministrazione al momento dell'installazione. La condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

Per accedere ai registri di audit, è possibile configurare l'accesso client per controllare le condivisioni per NFS. In alternativa, è possibile ["utilizzare un server syslog esterno"](#).

Il sistema StorageGRID utilizza il riconoscimento positivo per impedire la perdita dei messaggi di audit prima che vengano scritti nel file di log. Un messaggio rimane in coda in un servizio fino a quando il servizio AMS o un servizio di inoltro di audit intermedio non ne ha riconosciuto il controllo. Per ulteriori informazioni, vedere ["Esaminare i registri di audit"](#).

Prima di iniziare

- Hai il `Passwords.txt` file con la password root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

A proposito di questa attività

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

Se alcuni servizi non sono elencati come in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando. Premere **Ctrl+C**.
4. Avviare l'utility di configurazione NFS. Inserire: `config_nfs.rb`

Shares	Clients	Config
add-audit-share	add-ip-to-share	validate-config
enable-disable-share	remove-ip-from-share	refresh-config
		help
		exit

5. Aggiungere il client di audit: `add-audit-share`
 - a. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
 - b. Quando richiesto, premere **Invio**.
6. Se più di un client di audit è autorizzato ad accedere alla condivisione di audit, aggiungere l'indirizzo IP dell'utente aggiuntivo: `add-ip-to-share`
 - a. Inserire il numero della condivisione di controllo: `audit_share_number`
 - b. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
 - c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.
 - d. Ripetere questi passaggi secondari per ogni client di audit aggiuntivo che ha accesso alla condivisione di audit.
7. Se si desidera, verificare la configurazione.
 - a. Immettere quanto segue: `validate-config`

I servizi vengono controllati e visualizzati.
 - b. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.
 - c. Chiudere l'utility di configurazione NFS: `exit`
8. Determinare se è necessario abilitare le condivisioni di audit in altri siti.
 - Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
 - Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:
 - i. Accedere in remoto al nodo Admin del sito:
 - A. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - B. Immettere la password elencata in `Passwords.txt` file.
 - C. Immettere il seguente comando per passare a root: `su -`
 - D. Immettere la password elencata in `Passwords.txt` file.

- ii. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
- iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto. Inserire: `exit`

9. Disconnettersi dalla shell dei comandi: `exit`

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di controllo a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione oppure rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Aggiungere un client di audit NFS a una condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di audit a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione di audit.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share       | validate-config      |  
| enable-disable-share  | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. Inserire: `add-ip-to-share`

Viene visualizzato un elenco di condivisioni di controllo NFS attivate nel nodo di amministrazione. La condivisione dell'audit è elencata come: `/var/local/audit/export`

4. Inserire il numero della condivisione di controllo: `audit_share_number`
5. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`

Il client di audit viene aggiunto alla condivisione di audit.

6. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

7. Ripetere i passaggi per ogni client di audit da aggiungere alla condivisione di audit.
8. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati.

- a. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

9. Chiudere l'utility di configurazione NFS: `exit`
10. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

In caso contrario, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare facoltativamente queste condivisioni di controllo come richiesto:

- a. Accedere in remoto al nodo di amministrazione di un sito:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata in `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare a root: `su -`
 - iv. Immettere la password elencata in `Passwords.txt` file.
- b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
- c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

11. Disconnettersi dalla shell dei comandi: `exit`

Verificare l'integrazione dell'audit NFS

Dopo aver configurato una condivisione di audit e aggiunto un client di audit NFS, è possibile montare la condivisione del client di audit e verificare che i file siano disponibili dalla condivisione di audit.

Fasi

1. Verificare la connettività (o la variante per il sistema client) utilizzando l'indirizzo IP lato client del nodo di amministrazione che ospita il servizio AMS. Inserire: `ping IP_address`

Verificare che il server risponda, indicando la connettività.

2. Montare la condivisione di sola lettura dell'audit utilizzando un comando appropriato per il sistema operativo del client. Un comando Linux di esempio è (inserire su una riga):

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export  
myAudit
```

Utilizzare l'indirizzo IP del nodo di amministrazione che ospita il servizio AMS e il nome di condivisione predefinito per il sistema di audit. Il punto di montaggio può essere qualsiasi nome selezionato dal client (ad esempio, *myAudit* nel comando precedente).

3. Verificare che i file siano disponibili dalla condivisione dell'audit. Inserire: `ls myAudit /*`

dove *myAudit* è il punto di montaggio della condivisione dell'audit. Dovrebbe essere presente almeno un file di log.

Rimuovere un client di audit NFS dalla condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. È possibile rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).

A proposito di questa attività

Non è possibile rimuovere l'ultimo indirizzo IP consentito per accedere alla condivisione dell'audit.

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Avviare l'utilità di configurazione NFS: `config_nfs.rb`

Shares	Clients	Config
add-audit-share	add-ip-to-share	validate-config
enable-disable-share	remove-ip-from-share	refresh-config
		help
		exit

3. Rimuovere l'indirizzo IP dalla condivisione dell'audit: `remove-ip-from-share`

Viene visualizzato un elenco numerato di condivisioni di controllo configurate sul server. La condivisione dell'audit è elencata come: `/var/local/audit/export`

4. Inserire il numero corrispondente alla condivisione di audit: `audit_share_number`

Viene visualizzato un elenco numerato di indirizzi IP autorizzati ad accedere alla condivisione dell'audit.

5. Inserire il numero corrispondente all'indirizzo IP che si desidera rimuovere.

La condivisione di audit viene aggiornata e l'accesso non è più consentito da alcun client di audit con questo indirizzo IP.

6. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

7. Chiudere l'utility di configurazione NFS: `exit`

8. Se l'implementazione di StorageGRID è un'implementazione di più siti di data center con nodi amministrativi aggiuntivi negli altri siti, disattivare queste condivisioni di controllo secondo necessità:

- a. Accedere in remoto al nodo di amministrazione di ciascun sito:

- i. Immettere il seguente comando: `ssh admin@grid_node_IP`

- ii. Immettere la password elencata in `Passwords.txt` file.

- iii. Immettere il seguente comando per passare a root: `su -`

- iv. Immettere la password elencata in `Passwords.txt` file.

- b. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.

- c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

9. Disconnettersi dalla shell dei comandi: `exit`

Modificare l'indirizzo IP di un client di audit NFS

Se si desidera modificare l'indirizzo IP di un client di audit NFS, attenersi alla procedura descritta di seguito.

Fasi

1. Aggiungere un nuovo indirizzo IP a una condivisione di audit NFS esistente.
2. Rimuovere l'indirizzo IP originale.

Informazioni correlate

- ["Aggiungere un client di audit NFS a una condivisione di audit"](#)
- ["Rimuovere un client di audit NFS dalla condivisione di audit"](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.