



Configurare l'accesso al client di audit

StorageGRID

NetApp
April 10, 2024

Sommario

- Configurare l'accesso al client di audit 1
 - Configurare i client di audit per CIFS 1
 - Configurare il client di audit per NFS 11

Configurare l'accesso al client di audit

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. Per un facile accesso ai registri di audit, è possibile configurare l'accesso client per le condivisioni di audit per CIFS e NFS.

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](#).



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID. Se hai la possibilità di utilizzare CIFS o NFS, scegli NFS.

Configurare i client di audit per CIFS

La procedura utilizzata per configurare un client di audit dipende dal metodo di autenticazione: Windows Workgroup o Windows Active Directory (ad). Una volta aggiunta, la condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Configurare i client di audit per Workgroup

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

Di cosa hai bisogno

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

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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: `storagegrid-status`

Se tutti i servizi non sono 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 CIFS: `config_cifs.rb`

Shares	Authentication	Config	

add-audit-share	set-authentication	validate-config	
enable-disable-share	set-netbios-name	help	
add-user-to-share	join-domain	exit	
remove-user-from-share	add-password-server		
modify-group	remove-password-server		
	add-wins-server		
	remove-wins-server		

5. Impostare l'autenticazione per Windows Workgroup:

Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

a. Inserire: `set-authentication`

b. Quando viene richiesto di installare Windows Workgroup o Active Directory, immettere: `workgroup`

c. Quando richiesto, immettere un nome per il gruppo di lavoro: `workgroup_name`

d. Quando richiesto, creare un nome NetBIOS significativo: `netbios_name`

oppure

Premere **Invio** per utilizzare il nome host del nodo di amministrazione come nome NetBIOS.

Lo script riavvia il server Samba e le modifiche vengono applicate. Questa operazione dovrebbe richiedere meno di un minuto. Dopo aver impostato l'autenticazione, aggiungere un client di audit.

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

Viene visualizzata l'utility di configurazione CIFS.

6. Aggiungere un client di audit:

a. Inserire: `add-audit-share`



La condivisione viene aggiunta automaticamente in sola lettura.

- b. Quando richiesto, aggiungere un utente o un gruppo: *user*
- c. Quando richiesto, inserire il nome utente per l'audit: *audit_user_name*
- d. Quando richiesto, inserire una password per l'utente di controllo: *password*
- e. Quando richiesto, immettere nuovamente la stessa password per confermarla: *password*
- f. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.



Non è necessario inserire una directory. Il nome della directory di controllo è predefinito.

7. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere gli utenti aggiuntivi:

- a. Inserire: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni abilitate.

- b. Quando richiesto, inserire il numero della condivisione audit-export: *share_number*
- c. Quando richiesto, aggiungere un utente o un gruppo: *user*

oppure *group*

- d. Quando richiesto, inserire il nome dell'utente o del gruppo di controllo: *audit_user* or *audit_group*
- e. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

- f. Ripetere questi passaggi secondari per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

8. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

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

Viene visualizzata la configurazione del client di audit.

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

Viene visualizzata l'utility di configurazione CIFS.

9. Chiudere l'utilità di configurazione CIFS: `exit`
10. Avviare il servizio Samba: `service smb start`
11. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

oppure

Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare questa condivisione 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 la procedura per configurare la condivisione di controllo per ogni nodo amministrativo aggiuntivo.
 - c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
12. Disconnettersi dalla shell dei comandi: `exit`

Configurare i client di audit per Active Directory

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

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Si dispone del nome utente e della password di CIFS Active Directory.
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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: `storagegrid-status`

Se tutti i servizi non sono 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 CIFS: `config_cifs.rb`

Shares	Authentication	Config	

add-audit-share	set-authentication	validate-config	
enable-disable-share	set-netbios-name	help	
add-user-to-share	join-domain	exit	
remove-user-from-share	add-password-server		
modify-group	remove-password-server		
	add-wins-server		
	remove-wins-server		

5. Impostare l'autenticazione per Active Directory: `set-authentication`

Nella maggior parte delle implementazioni, è necessario impostare l'autenticazione prima di aggiungere il client di audit. Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

- a. Quando viene richiesto di installare Workgroup o Active Directory: `ad`
- b. Quando richiesto, inserire il nome del dominio `ad` (nome di dominio breve).
- c. Quando richiesto, inserire l'indirizzo IP o il nome host DNS del controller di dominio.
- d. Quando richiesto, inserire il nome completo del dominio.

Utilizzare lettere maiuscole.

- e. Quando viene richiesto di attivare il supporto winbind, digitare **y**.

Winbind viene utilizzato per risolvere le informazioni di utenti e gruppi dai server `ad`.

- f. Quando richiesto, inserire il nome NetBIOS.

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

Viene visualizzata l'utility di configurazione CIFS.

6. Unirsi al dominio:

- a. Se non è già stato avviato, avviare l'utility di configurazione CIFS: `config_cifs.rb`
- b. Unirsi al dominio: `join-domain`
- c. Viene richiesto di verificare se l'Admin Node è attualmente un membro valido del dominio. Se questo nodo di amministrazione non ha precedentemente aderito al dominio, immettere: `no`

d. Quando richiesto, fornire il nome utente dell'amministratore: `administrator_username`

dove `administrator_username` È il nome utente di CIFS Active Directory, non il nome utente di StorageGRID.

e. Quando richiesto, fornire la password dell'amministratore: `administrator_password`

erano `administrator_password` È il nome utente di CIFS Active Directory, non la password di StorageGRID.

f. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

7. Verificare di aver inserito correttamente il dominio:

a. Unirsi al dominio: `join-domain`

b. Quando viene richiesto di verificare se il server è attualmente un membro valido del dominio, immettere: `y`

Se viene visualizzato il messaggio "Join is OK," significa che l'accesso al dominio è stato eseguito correttamente. Se non si ottiene questa risposta, provare a impostare nuovamente l'autenticazione e ad accedere al dominio.

c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

8. Aggiungere un client di audit: `add-audit-share`

a. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `user`

b. Quando viene richiesto di inserire il nome utente per l'audit, inserire il nome utente per l'audit.

c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

9. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere altri utenti: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni abilitate.

a. Inserire il numero della condivisione audit-export.

b. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `group`

Viene richiesto il nome del gruppo di audit.

c. Quando viene richiesto il nome del gruppo di audit, immettere il nome del gruppo di utenti di audit.

d. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

e. Ripetere questo passaggio per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

10. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-filesystem.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-custom-config.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-shares.inc`
- `Rlimit_max`: Aumento di `rlimit_max` (1024) al limite minimo di Windows (16384)



Non combinare l'impostazione 'security=ads' con il parametro 'password server'. (Per impostazione predefinita, Samba rileverà automaticamente il DC corretto da contattare).

- i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
- ii. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

11. Chiudere l'utilità di configurazione CIFS: `exit`

12. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

oppure

Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare 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: `exit`

13. Disconnettersi dalla shell dei comandi: `exit`

Aggiungere un utente o un gruppo a una condivisione di audit CIFS

È possibile aggiungere un utente o un gruppo a una condivisione di audit CIFS integrata con l'autenticazione ad.

Di cosa hai bisogno

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

- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

La seguente procedura riguarda una condivisione di controllo integrata con l'autenticazione ad.



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- 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 tutti i servizi non sono 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 CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Iniziare ad aggiungere un utente o un gruppo: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni di controllo configurate.

6. Quando richiesto, inserire il numero per la condivisione dell'audit (audit-export): `audit_share_number`

Viene richiesto se si desidera concedere a un utente o a un gruppo l'accesso a questa condivisione di controllo.

7. Quando richiesto, aggiungere un utente o un gruppo: `user` oppure `group`

8. Quando viene richiesto il nome dell'utente o del gruppo per questa condivisione di audit ad, immettere il nome.

L'utente o il gruppo viene aggiunto in sola lettura per la condivisione di controllo sia nel sistema operativo del server che nel servizio CIFS. La configurazione di Samba viene ricaricata per consentire all'utente o al gruppo di accedere alla condivisione del client di audit.

9. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

10. Ripetere questa procedura per ogni utente o gruppo che ha accesso alla condivisione di controllo.

11. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

- Impossibile trovare il file include `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-filesystem.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-custom-config.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-shares.inc`
 - i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
 - ii. Quando richiesto, premere **Invio**.

12. Chiudere l'utilità di configurazione CIFS: `exit`

13. Determinare se è necessario attivare ulteriori condivisioni di audit, come segue:

- 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 di amministrazione di un 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 questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
 - iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

14. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere un utente o un gruppo da una condivisione di audit CIFS

Non è possibile rimuovere l'ultimo utente o gruppo autorizzato ad accedere alla condivisione di controllo.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con le password dell'account root (disponibili in DETTO pacchetto).

- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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 CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

3. Iniziare a rimuovere un utente o un gruppo: `remove-user-from-share`

Viene visualizzato un elenco numerato delle condivisioni di audit disponibili per il nodo di amministrazione. La condivisione dell'audit è etichettata `audit-export`.

4. Inserire il numero della condivisione di controllo: `audit_share_number`

5. Quando viene richiesto di rimuovere un utente o un gruppo: `user` oppure `group`

Viene visualizzato un elenco numerato di utenti o gruppi per la condivisione dell'audit.

6. Inserire il numero corrispondente all'utente o al gruppo che si desidera rimuovere: `number`

La condivisione di controllo viene aggiornata e l'utente o il gruppo non può più accedere alla condivisione di controllo. Ad esempio:

```
Enabled shares
  1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
  1. audituser
  2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Chiudere l'utilità di configurazione CIFS: `exit`
8. Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, disattivare la condivisione di controllo in ciascun sito secondo necessità.
9. Disconnettersi da ogni shell dei comandi al termine della configurazione: `exit`

Modificare il nome di un utente o di un gruppo di condivisione dell'audit CIFS

È possibile modificare il nome di un utente o di un gruppo per una condivisione di audit CIFS aggiungendo un nuovo utente o gruppo ed eliminando quello precedente.

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Aggiungere un nuovo utente o gruppo con il nome aggiornato alla condivisione di controllo.
2. Eliminare il vecchio nome utente o gruppo.

Informazioni correlate

- [Aggiungere un utente o un gruppo a una condivisione di audit CIFS](#)
- [Rimuovere un utente o un gruppo da una condivisione di audit CIFS](#)

Verificare l'integrazione dell'audit CIFS

La condivisione dell'audit è di sola lettura. I file di log devono essere letti dalle applicazioni del computer e la verifica non include l'apertura di un file. Si ritiene sufficiente verificare che i file di registro di controllo vengano visualizzati in una finestra di Esplora risorse. Dopo la verifica della connessione, chiudere tutte le finestre.

Configurare il client di audit per NFS

La condivisione di controllo viene attivata automaticamente come condivisione di sola

lettura.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).
- 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.

Di cosa hai bisogno

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

- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).
- Il client di audit utilizza NFS versione 3 (NFSv3).

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- 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.

- 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.

Di cosa hai bisogno

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

A proposito di questa attività

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