



Konfigurieren von Audit-Clients für CIFS

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Konfigurieren von Audit-Clients für CIFS 1
 - Konfigurieren von Audit-Clients für Workgroup 1
 - Konfigurieren von Audit-Clients für Active Directory 4
 - Hinzufügen eines Benutzers oder einer Gruppe zu einer CIFS-Revisionsfreigabe 8
 - Entfernen eines Benutzers oder einer Gruppe aus einer CIFS-Revisionsfreigabe 10
 - Ändern eines CIFS-Revisionsfreigabe-Benutzers oder Gruppennamens 12
- Überprüfung der Integration von CIFS-Audits 12

Konfigurieren von Audit-Clients für CIFS

Das Verfahren zum Konfigurieren eines Audit-Clients hängt von der Authentifizierungsmethode ab: Windows Workgroup oder Windows Active Directory (AD). Wenn diese Option hinzugefügt wird, wird die Revisionsfreigabe automatisch als schreibgeschützte Freigabe aktiviert.



Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Verwandte Informationen

["Software-Upgrade"](#)

Konfigurieren von Audit-Clients für Workgroup

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen:
`storagegrid-status`

Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `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. Legen Sie die Authentifizierung für die Windows Workgroup fest:

Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

- Geben Sie Ein: `set-authentication`
- Wenn Sie zur Installation von Windows Workgroup oder Active Directory aufgefordert werden, geben Sie Folgendes ein: `workgroup`
- Geben Sie bei der entsprechenden Aufforderung einen Namen für die Arbeitsgruppe ein:
`workgroup_name`
- Erstellen Sie bei Aufforderung einen aussagekräftigen NetBIOS-Namen: `netbios_name`

Oder

Drücken Sie **Enter**, um den Hostnamen des Admin-Knotens als NetBIOS-Name zu verwenden.

Das Skript startet den Samba-Server neu und es werden Änderungen vorgenommen. Dies sollte weniger als eine Minute dauern. Fügen Sie nach dem Festlegen der Authentifizierung einen Audit-Client hinzu.

- Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Hinzufügen eines Audit-Clients:

- Geben Sie Ein: `add-audit-share`



Die Freigabe wird automatisch als schreibgeschützt hinzugefügt.

- Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user`
- Geben Sie bei der entsprechenden Aufforderung den Benutzernamen für die Prüfung ein:
`audit_user_name`
- Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den Benutzer der Prüfung ein:
`password`
- Geben Sie bei der entsprechenden Aufforderung dasselbe Passwort erneut ein, um es zu bestätigen:

password

- f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.



Es ist nicht erforderlich, ein Verzeichnis einzugeben. Der Name des Überwachungsverzeichnisses ist vordefiniert.

7. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie die zusätzlichen Benutzer hinzu:

- a. Geben Sie Ein: `add-user-to-share`

Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

- b. Geben Sie bei der entsprechenden Aufforderung die Nummer der Freigabe für den Audit-Export ein:
share_number

- c. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user`

Oder `group`

- d. Geben Sie bei Aufforderung den Namen des Audit-Benutzers oder der Gruppe ein: `audit_user` or
`audit_group`

- e. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

- f. Wiederholen Sie diese Teilschritte für jeden weiteren Benutzer oder jede Gruppe, die Zugriff auf die Revisionsfreigabe hat.

8. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

```
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. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Die Konfiguration des Audit-Clients wird angezeigt.

- b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`

10. Starten Sie den Samba-Dienst: `service smbd start`
11. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

Oder

Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie diese Revisionsfreigabe nach Bedarf:

- a. Remote-Anmeldung beim Admin-Node eines Standorts:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - b. Wiederholen Sie die Schritte, um die Revisionsfreigabe für jeden zusätzlichen Admin-Knoten zu konfigurieren.
 - c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
12. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

["Software-Upgrade"](#)

Konfigurieren von Audit-Clients für Active Directory

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANTEN Paket verfügbar).
- Sie müssen über den Benutzernamen und das Kennwort für das CIFS Active Directory verfügen.
- Sie müssen die haben `Configuration.txt` Datei (im GENANTEN Paket verfügbar).



Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen:

```
storagegrid-status
```

Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.

4. Starten Sie das CIFS-Konfigurationsprogramm: `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. Legen Sie die Authentifizierung für Active Directory fest: `set-authentication`

In den meisten Bereitstellungen müssen Sie die Authentifizierung festlegen, bevor Sie den Audit-Client hinzufügen. Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

- Bei Aufforderung zur Workgroup- oder Active Directory-Installation: `ad`
- Geben Sie bei der entsprechenden Aufforderung den Namen der AD-Domäne ein (kurzer Domain-Name).
- Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den DNS-Hostnamen des Domänencontrollers ein.
- Geben Sie bei entsprechender Aufforderung den vollständigen Domänennamen ein.

Verwenden Sie Großbuchstaben.

- Geben Sie bei Aufforderung zur Aktivierung der Winbindunterstützung `y` ein.

Winbind wird verwendet, um Benutzer- und Gruppeninformationen von AD-Servern zu lösen.

- Geben Sie bei entsprechender Aufforderung den NetBIOS-Namen ein.
- Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Treten Sie der Domäne bei:

- Wenn noch nicht gestartet, starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`
- Treten Sie der Domäne bei: `join-domain`

- c. Sie werden aufgefordert zu testen, ob der Admin-Knoten derzeit ein gültiges Mitglied der Domain ist. Wenn dieser Admin-Node der Domäne noch nicht beigetreten ist, geben Sie Folgendes ein: `no`
- d. Geben Sie bei entsprechender Aufforderung den Benutzernamen des Administrators an:
`administrator_username`

Wo `administrator_username` Ist der Benutzername für das CIFS Active Directory, nicht der StorageGRID-Benutzername.

- e. Geben Sie bei entsprechender Aufforderung das Administratorpasswort an:
`administrator_password`

Waren `administrator_password` Ist der Benutzername für das CIFS-Active-Verzeichnis und nicht das StorageGRID-Kennwort.

- f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

7. Vergewissern Sie sich, dass Sie der Domäne ordnungsgemäß beigetreten sind:

- a. Treten Sie der Domäne bei: `join-domain`
- b. Wenn Sie aufgefordert werden, zu testen, ob der Server derzeit ein gültiges Mitglied der Domäne ist, geben Sie Folgendes ein: `y`

Wenn Sie die Meldung „Join is OK,“ erhalten, haben Sie sich erfolgreich der Domäne angeschlossen. Wenn diese Antwort nicht angezeigt wird, versuchen Sie, die Authentifizierung zu aktivieren und die Domain erneut anzuschließen.

- c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

8. Hinzufügen eines Audit-Clients: `add-audit-share`

- a. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `user`
- b. Wenn Sie zur Eingabe des Benutzernamens für die Prüfung aufgefordert werden, geben Sie den Benutzernamen für die Prüfung ein.
- c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie weitere Benutzer hinzu: `add-user-to-share`

Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

- a. Geben Sie die Nummer der Freigabe für den Audit-Export ein.
- b. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `group`

Sie werden aufgefordert, den Namen der Überwachungsgruppe anzugeben.

- c. Wenn Sie zur Eingabe des Namens der Überwachungsgruppe aufgefordert werden, geben Sie den Namen der Benutzergruppe für die Prüfung ein.
- d. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

- e. Wiederholen Sie diesen Schritt für jeden weiteren Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.

10. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

- Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
- Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-filesystem.inc`
- Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
- Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-custom-config.inc`
- Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-shares.inc`
- `Rlimit_max`: Anstieg von `rlimit_max` (1024) auf Windows-Minimum (16384)



Kombinieren Sie die Einstellung 'security=ads' nicht mit dem Parameter 'Password Server'. (Standardmäßig erkennt Samba das korrekte DC, um automatisch Kontakt aufzunehmen).

- i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.
- ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

11. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`

12. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

Oder

Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie optional die folgenden Audit-Shares nach Bedarf:

a. Remote-Anmeldung beim Admin-Node eines Standorts:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.

c. Schließen Sie die sichere Remote-Shell-Anmeldung beim Admin-Node: `exit`

13. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

["Software-Upgrade"](#)

Hinzufügen eines Benutzers oder einer Gruppe zu einer CIFS-Revisionsfreigabe

Sie können einen Benutzer oder eine Gruppe zu einer CIFS-Revisionsfreigabe hinzufügen, die in die AD-Authentifizierung integriert ist.

Was Sie benötigen

- Sie müssen die `passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANTEN Paket verfügbar).
- Sie müssen die `configuration.txt` Datei (im GENANTEN Paket verfügbar).

Über diese Aufgabe

Das folgende Verfahren gilt für eine mit AD-Authentifizierung integrierte Audit-Freigabe.



Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `passwords.txt` Datei:

Wenn Sie als `root` angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `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. Beginnen Sie mit dem Hinzufügen eines Benutzers oder einer Gruppe: `add-user-to-share`

Eine nummerierte Liste der konfigurierten Audit-Shares wird angezeigt.

6. Wenn Sie dazu aufgefordert werden, geben Sie die Nummer für die Revisionsfreigabe ein (Audit-Export):
audit_share_number

Sie werden gefragt, ob Sie einem Benutzer oder einer Gruppe Zugriff auf diese Revisionsfreigabe gewähren möchten.

7. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user` Oder `group`

8. Wenn Sie zur Eingabe des Benutzer- oder Gruppennamens für diese AD-Revisionsfreigabe aufgefordert werden, geben Sie den Namen ein.

Der Benutzer oder die Gruppe wird als schreibgeschützt für die Revisionsfreigabe sowohl im Betriebssystem des Servers als auch im CIFS-Dienst hinzugefügt. Die Samba-Konfiguration wird neu geladen, damit der Benutzer oder die Gruppe auf die Audit-Client-Freigabe zugreifen können.

9. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

10. Wiederholen Sie diese Schritte für jeden Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.

11. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

- Kann die Datei `/etc/samba/includes/cifs-interfaces.inc` nicht finden
- Kann die Datei `/etc/samba/includes/cifs-filesystem.inc` nicht finden
- Kann die Datei `/etc/samba/includes/cifs-custom-config.inc` nicht finden
- Kann die Datei `/etc/samba/includes/cifs-shares.inc` nicht finden

- i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.

- ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.
12. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
13. Ermitteln Sie wie folgt, ob zusätzliche Audit-Shares aktiviert werden müssen:
 - Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.
 - Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie die folgenden Audit-Freigaben nach Bedarf:
 - i. Remote-Anmeldung beim Admin-Node eines Standorts:
 - A. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - B. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - C. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - D. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - ii. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.
 - iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
14. Melden Sie sich aus der Befehlshell ab: `exit`

Entfernen eines Benutzers oder einer Gruppe aus einer CIFS-Revisionsfreigabe

Sie können den letzten Benutzer oder die letzte Gruppe, der Zugriff auf die Revisionsfreigabe hat, nicht entfernen.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit den Passwörtern des Root-Kontos (im GENANTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das CIFS-Konfigurationsprogramm: `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	

- Starten Sie das Entfernen eines Benutzers oder einer Gruppe: `remove-user-from-share`

Eine nummerierte Liste der verfügbaren Audit-Shares für den Admin-Knoten wird angezeigt. Die Revisionsfreigabe wird als Audit-Export bezeichnet.

- Geben Sie die Nummer der Revisionsfreigabe ein: `audit_share_number`
- Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe zu entfernen: `user` Oder `group`

Eine nummerierte Liste von Benutzern oder Gruppen für die Revisionsfreigabe wird angezeigt.

- Geben Sie die Nummer für den Benutzer oder die Gruppe ein, die Sie entfernen möchten: `number`

Die Revisionsfreigabe wird aktualisiert, und der Benutzer oder die Gruppe ist nicht mehr berechtigt, auf die Revisionsfreigabe zuzugreifen. Beispiel:

```
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.
```

- Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
- Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, deaktivieren Sie die Revisionsfreigabe an jedem Standort nach Bedarf.
- Melden Sie sich bei Abschluss der Konfiguration von jeder Befehlshaber ab: `exit`

Verwandte Informationen

["Software-Upgrade"](#)

Ändern eines CIFS-Revisionsfreigabe-Benutzers oder Gruppennamens

Sie können den Namen eines Benutzers oder einer Gruppe für eine CIFS-Revisionsfreigabe ändern, indem Sie einen neuen Benutzer oder eine neue Gruppe hinzufügen und dann den alten löschen.

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Fügen Sie einen neuen Benutzer oder eine neue Gruppe mit dem aktualisierten Namen zur Revisionsfreigabe hinzu.
2. Löschen Sie den alten Benutzer- oder Gruppennamen.

Verwandte Informationen

["Software-Upgrade"](#)

["Hinzufügen eines Benutzers oder einer Gruppe zu einer CIFS-Revisionsfreigabe"](#)

["Entfernen eines Benutzers oder einer Gruppe aus einer CIFS-Revisionsfreigabe"](#)

Überprüfung der Integration von CIFS-Audits

Die Revisionsfreigabe ist schreibgeschützt. Die Protokolldateien sind für Computeranwendungen gedacht, und die Überprüfung beinhaltet nicht das Öffnen einer Datei. Es wird als ausreichend überprüft, ob die Audit-Log-Dateien in einem Windows Explorer-Fenster angezeigt werden. Schließen Sie nach der Verbindungsüberprüfung alle Fenster.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.