Konfigurieren des Zugriffs auf Audit-Clients

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Konfigurieren des Zugriffs auf Audit-Clients

Der Admin-Knoten protokolliert über den Service Audit Management System (AMS) alle überprüften Systemereignisse in eine Protokolldatei, die über die Revisionsfreigabe verfügbar ist und die zu jedem Admin-Knoten bei der Installation hinzugefügt wird. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, lässt sich der Client-Zugriff auf Audit-Freigaben für CIFS und NFS konfigurieren.

Das StorageGRID System verwendet eine positive Bestätigung, um den Verlust von Audit-Meldungen zu verhindern, bevor sie in die Protokolldatei geschrieben werden. Eine Meldung bleibt an einem Dienst in der Warteschlange, bis der AMS-Dienst oder ein Zwischenaudit-Relaisdienst die Kontrolle über ihn bestätigt hat.

Weitere Informationen finden Sie in den Anweisungen zum Verständnis von Überwachungsmeldungen.

> Wenn Sie CIFS oder NFS verwenden möchten, wählen Sie NFS.

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

Verwandte Informationen

"Was ist ein Admin-Node"

"Prüfung von Audit-Protokollen"

"Software-Upgrade"

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 GENANNTEN Paket verfügbar).

- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN 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.

   a. Geben Sie Ein: `set-authentication`
   b. Wenn Sie zur Installation von Windows Workgroup oder Active Directory aufgefordert werden, geben Sie Folgendes ein: `workgroup`
   c. Geben Sie bei der entsprechenden Aufforderung einen Namen für die Arbeitsgruppe ein: *`workgroup_name`*
   d. 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.

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

   Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Hinzufügen eines Audit-Clients:

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

      Die Freigabe wird automatisch als schreibgeschützt hinzugefügt.

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

   c. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen für die Prüfung ein: *`audit_user_name`*

   d. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den Benutzer der Prüfung ein: *`password`*

   e. 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 GENANNTEN Paket verfügbar).
- Sie müssen über den Benutzernamen und das Kennwort für das CIFS Active Directory verfügen.
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN 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.

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

   Verwenden Sie Großbuchstaben.

e. Geben Sie bei Aufforderung zur Aktivierung der Winbindunterstützung **y** ein.

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

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

   Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Treten Sie der Domäne bei:
   a. Wenn noch nicht gestartet, starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`
   b. 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 haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN 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 Befehlsshell 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 GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN 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     |                 |
------------------------------------------------------------------
```

3. 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.

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
5. 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.

6. 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.
```

7. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
8. Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, deaktivieren Sie die Revisionsfreigabe an jedem Standort nach Bedarf.
9. 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.

Konfigurieren des Audit-Clients für NFS

Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client muss NFS-Version 3 (NFSv3) verwenden.

Über diese Aufgabe

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

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 Dienste nicht als aktiv oder verifiziert aufgeführt sind, beheben Sie Probleme, bevor Sie fortfahren.

3. Zurück zur Kommandozeile. Drücken Sie **Strg+C**.
4. Starten Sie das NFS-Konfigurationsprogramm. Geben Sie Ein: `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. Fügen Sie den Audit-Client hinzu: `add-audit-share`

a. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`

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

6. Wenn mehr als ein Audit-Client auf die Revisionsfreigabe zugreifen darf, fügen Sie die IP-Adresse des zusätzlichen Benutzers hinzu: `add-ip-to-share`

   a. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*

   b. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *`client_IP_address`*

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

      Das NFS-Konfigurationsprogramm wird angezeigt.

   d. Wiederholen Sie diese Teilschritte für jeden zusätzlichen Audit-Client, der Zugriff auf die Revisionsfreigabe hat.

7. Überprüfen Sie optional Ihre Konfiguration.

   a. Geben Sie Folgendes ein: `validate-config`

      Die Dienste werden überprüft und angezeigt.

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

      Das NFS-Konfigurationsprogramm wird angezeigt.

   c. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`

8. Legen Sie fest, ob die Revisionsfreigaben an anderen Standorten 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 des 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 zusätzlichen Admin-Node zu konfigurieren.

     iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node. Geben Sie Ein: `exit`

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

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie der Freigabe ihre IP-Adresse hinzufügen oder einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Hinzufügen eines NFS-Audit-Clients zu einer Revisionsfreigabe

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie dessen IP-Adresse zur Revisionsfreigabe hinzufügen.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client muss NFS-Version 3 (NFSv3) verwenden.

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 NFS-Konfigurationsprogramm: `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. Geben Sie Ein: `add-ip-to-share`

   Es wird eine Liste der auf dem Admin-Knoten aktivierten NFS-Audit-Freigaben angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
5. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *`client_IP_address`*

   Der Audit-Client wird der Revisionsfreigabe hinzugefügt.

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

   Das NFS-Konfigurationsprogramm wird angezeigt.

7. Wiederholen Sie die Schritte für jeden Audit-Client, der zur Revisionsfreigabe hinzugefügt werden soll.
8. Überprüfen Sie optional die Konfiguration: `validate-config`

   Die Dienste werden überprüft und angezeigt.

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

      Das NFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
10. 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 andernfalls optional diese 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 am Remote-Admin-Node: `exit`
11. Melden Sie sich aus der Befehlsshell ab: `exit`

Prüfung der NFS-Audit-Integration

Nachdem Sie eine Audit-Freigabe konfiguriert und einen NFS-Audit-Client hinzugefügt haben, können Sie die Audit-Client-Freigabe mounten und überprüfen, ob die Dateien über die Audit-Freigabe verfügbar sind.

Schritte

1. Überprüfen Sie die Konnektivität (oder Variante für das Clientsystem) mithilfe der clientseitigen IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet. Geben Sie Ein: `ping IP_address`

   Stellen Sie sicher, dass der Server antwortet, und geben Sie die Konnektivität an.

2. Mounten Sie die schreibgeschützte Revisionsfreigabe mit einem dem Client-Betriebssystem entsprechenden Befehl. Ein Beispiel für Linux lautet (geben Sie in einer Zeile ein):

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

   Verwenden Sie die IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet, und den vordefinierten Freigabennamen für das Audit-System. Der Mount-Punkt kann ein beliebiger Name sein, der vom Client ausgewählt wurde (z. B. *myAudit* Im vorherigen Befehl).

3. Stellen Sie sicher, dass die Dateien über die Revisionsfreigabe verfügbar sind. Geben Sie Ein: `ls`

*myAudit /**

Wo *myAudit* Ist der Bereitstellungspunkt der Revisionsfreigabe. Es sollte mindestens eine Protokolldatei aufgeführt sein.

Entfernen eines NFS-Audit-Clients aus der Revisionsfreigabe

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Sie können einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Was Sie benötigen

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

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Revisionsfreigabe zulässig ist, nicht entfernen.

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 NFS-Konfigurationsprogramm: `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. Entfernen Sie die IP-Adresse aus der Revisionsfreigabe: `remove-ip-from-share`

   Eine nummerierte Liste der auf dem Server konfigurierten Audit-Freigaben wird angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer für die Revisionsfreigabe ein: *audit_share_number*

Eine nummerierte Liste mit IP-Adressen, die Zugriff auf die Revisionsfreigabe ermöglichen, wird angezeigt.

5. Geben Sie die Nummer für die IP-Adresse ein, die Sie entfernen möchten.

   Die Revisionsfreigabe wird aktualisiert, und der Zugriff ist von keinem Audit-Client mit dieser IP-Adresse mehr gestattet.

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

   Das NFS-Konfigurationsprogramm wird angezeigt.

7. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
8. Wenn es sich bei Ihrer StorageGRID-Bereitstellung um mehrere Datacenter-Standortimplementierungen mit zusätzlichen Admin-Nodes an anderen Standorten handelt, deaktivieren Sie diese Revisionsfreigaben nach Bedarf:
   a. Remote-Anmeldung bei jedem Standort Admin-Node:
      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 zusätzlichen Admin-Node zu konfigurieren.
   c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
9. Melden Sie sich aus der Befehlsshell ab: `exit`

Ändern der IP-Adresse eines NFS-Audit-Clients

1. Fügen Sie einer vorhandenen NFS-Revisionsfreigabe eine neue IP-Adresse hinzu.
2. Entfernen Sie die ursprüngliche IP-Adresse.

Verwandte Informationen

"Hinzufügen eines NFS-Audit-Clients zu einer Revisionsfreigabe"

"Entfernen eines NFS-Audit-Clients aus der Revisionsfreigabe"