Konfigurieren des Zugriffs auf Audit-Clients

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-117/admin/configuring-audit-client-access.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren des Zugriffs auf Audit-Clients . . . 1
Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS . . . 1
Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu . . . 3
Prüfung der NFS-Audit-Integration . . . 4
Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe . . . 5
Ändern der IP-Adresse eines NFS-Audit-Clients . . . 6

Konfigurieren des Zugriffs auf Audit-Clients

Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS

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. Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Für den Zugriff auf Audit-Protokolle können Sie den Clientzugriff auf Audit-Freigaben für NFS konfigurieren. Sie können es auch "Verwenden Sie einen externen Syslog-Server".

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 unter "Prüfung von Audit-Protokollen".

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

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 Services nicht als „aktiv“ oder „geprüft“ 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.

Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu

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.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

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 Sie einen NFS-Audit-Client 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.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Überwachungsfreigabe 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

Führen Sie diese Schritte aus, wenn Sie die IP-Adresse eines NFS-Audit-Clients ändern müssen.

Schritte

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

Verwandte Informationen

- "Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu"
- "Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.