



Verwalten Von Admin-Nodes

StorageGRID

NetApp
October 03, 2025

Inhalt

- Verwalten Von Admin-Nodes 1
 - Was ist ein Admin-Node 1
 - Was ist der AMS-Service 1
 - Was der CMN-Service ist 1
 - Was ist der NMS-Service 2
 - Was der Prometheus Service ist 2
 - Mehrere Admin-Nodes werden verwendet 2
 - Identifizieren des primären Admin-Knotens 4
 - Auswählen eines bevorzugten Senders 4
 - Anzeigen von Benachrichtigungsstatus und -Warteschlangen 5
 - So zeigen Admin-Knoten bestätigte Alarmer an (Legacy-System) 6
 - Konfigurieren des Zugriffs auf Audit-Clients 7
 - Konfigurieren von Audit-Clients für CIFS 7
 - Konfigurieren des Audit-Clients für NFS 19

Verwalten Von Admin-Nodes

Jeder Standort in einer StorageGRID Implementierung kann einen oder mehrere Admin-Nodes enthalten.

- "Was ist ein Admin-Node"
- "Mehrere Admin-Nodes werden verwendet"
- "Identifizieren des primären Admin-Knotens"
- "Auswählen eines bevorzugten Senders"
- "Anzeigen von Benachrichtigungsstatus und -Warteschlangen"
- "So zeigen Admin-Knoten bestätigte Alarmer an (Legacy-System)"
- "Konfigurieren des Zugriffs auf Audit-Clients"

Was ist ein Admin-Node

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Jedes Grid muss einen primären Admin-Node haben und kann eine beliebige Anzahl nicht primärer Admin-Nodes für Redundanz aufweisen.

Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch verwendet werden, um den S3- und Swift-Client-Datenverkehr auszugleichen.

Admin-Nodes hosten die folgenden Services:

- AMS-Service
- CMN-Service
- NMS-Service
- Prometheus Service
- Load Balancer- und High Availability-Services (zur Unterstützung von S3- und Swift-Client-Datenverkehr)

Admin-Nodes unterstützen außerdem die Management Application Program Interface (Management-API) zur Verarbeitung von Anfragen aus der Grid Management API und der Mandanten-Management-API.

Was ist der AMS-Service

Der Audit Management System (AMS)-Dienst verfolgt Systemaktivität und -Ereignisse.

Was der CMN-Service ist

Der Configuration Management Node (CMN)-Dienst verwaltet systemweite Konfigurationen von Konnektivität und Protokollfunktionen, die von allen Diensten benötigt werden. Darüber hinaus wird der CMN-Dienst zur Ausführung und Überwachung von Grid-Aufgaben verwendet. Es gibt nur einen CMN-Service pro StorageGRID-Implementierung. Der Admin-Node, der den CMN-Service hostet, wird als primärer Admin-Node

bezeichnet.

Was ist der NMS-Service

Der NMS-Dienst (Network Management System) steuert die Überwachungs-, Reporting- und Konfigurationsoptionen, die über den Grid Manager, die browserbasierte Schnittstelle des StorageGRID-Systems, angezeigt werden.

Was der Prometheus Service ist

Der Prometheus Service sammelt Zeitreihungsmetriken aus den Services auf allen Knoten.

Verwandte Informationen

["Verwenden der Grid-Management-API"](#)

["Verwenden Sie ein Mandantenkonto"](#)

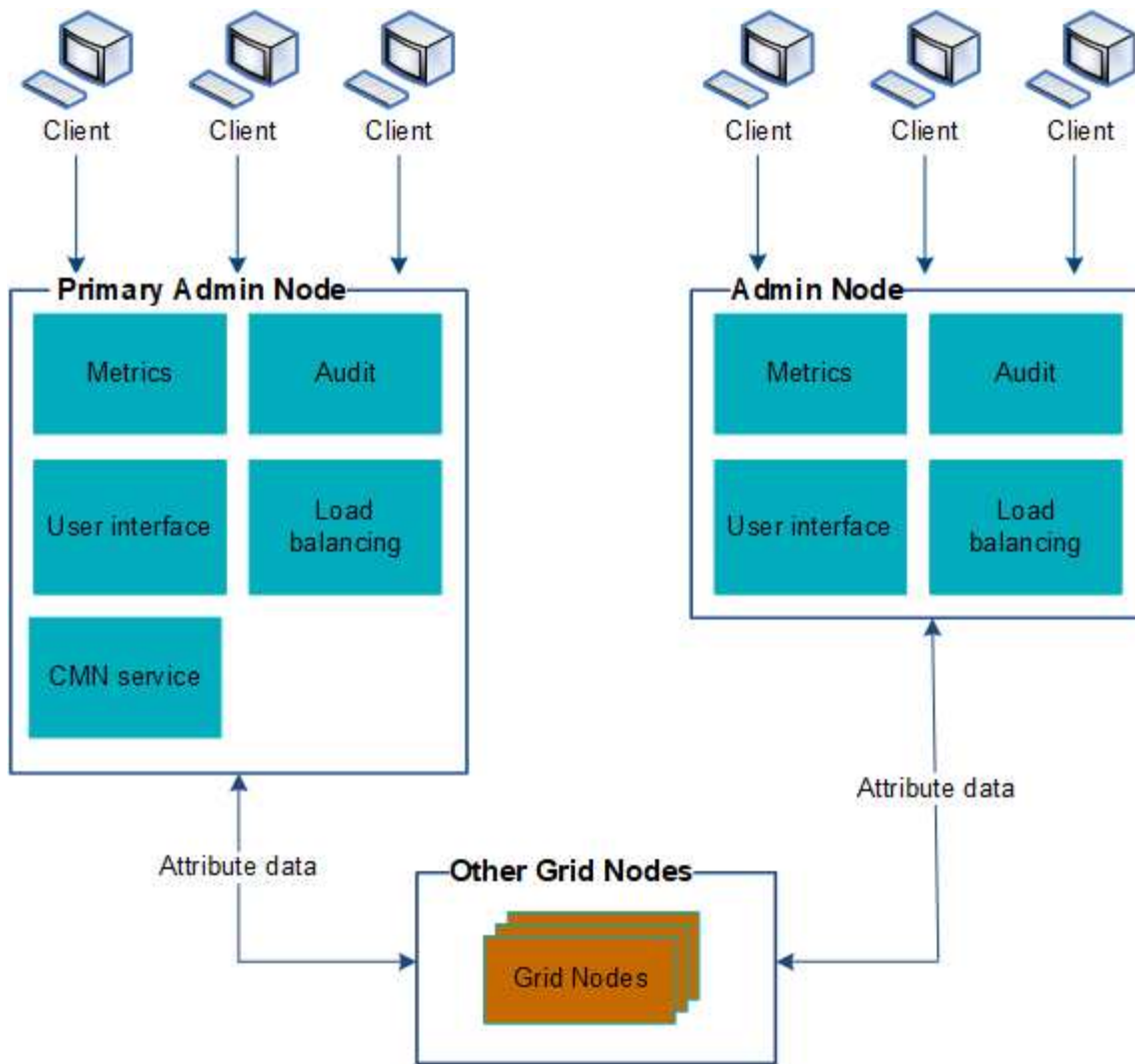
["Managen des Lastausgleichs"](#)

["Verwalten von Hochverfügbarkeitsgruppen"](#)

Mehrere Admin-Nodes werden verwendet

Ein StorageGRID-System kann mehrere Admin-Knoten enthalten, damit Sie Ihr StorageGRID-System kontinuierlich überwachen und konfigurieren können, auch wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Alarmer und Alarme (Legacy-System) werden immer noch ausgelöst und E-Mail-Benachrichtigungen und AutoSupport-Meldungen werden weiterhin gesendet. Das Vorhandensein mehrerer Admin-Nodes bietet jedoch keinen Failover-Schutz außer Benachrichtigungen und AutoSupport-Meldungen. Insbesondere werden die von einem Admin-Knoten ausgemachten Alarmbestätigungen nicht auf andere Admin-Knoten kopiert.



Es gibt zwei Optionen, um das StorageGRID-System weiterhin anzuzeigen und zu konfigurieren, wenn ein Admin-Knoten ausfällt:

- Webclients können sich mit jedem anderen verfügbaren Admin-Node verbinden.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Nodes konfiguriert hat, können Webclients unter Verwendung der virtuellen IP-Adresse der HA-Gruppe weiterhin auf den Grid Manager oder den Mandanten Manager zugreifen.



Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der Master Admin-Node ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Node in der Gruppe Failover erfolgt.

Einige Wartungsarbeiten können nur mit dem primären Admin-Node ausgeführt werden. Wenn der primäre Admin-Node ausfällt, muss er wiederhergestellt werden, bevor das StorageGRID System wieder voll funktionsfähig ist.

Verwandte Informationen

["Verwalten von Hochverfügbarkeitsgruppen"](#)

Identifizieren des primären Admin-Knotens

Der primäre Admin-Node hostet den CMN-Service. Einige Wartungsarbeiten können nur mit dem primären Admin-Node durchgeführt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support > Tools > Grid Topology** Aus.
2. Wählen Sie **site > Admin Node** und klicken Sie dann auf **+** So erweitern Sie die Topologiestruktur und zeigen die auf diesem Admin-Node gehosteten Services an.

Der primäre Admin-Node hostet den CMN-Service.

3. Wenn dieser Admin-Node den CMN-Dienst nicht hostet, prüfen Sie die anderen Admin-Nodes.

Auswählen eines bevorzugten Senders

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten enthält, können Sie auswählen, welcher Admin-Knoten der bevorzugte Absender von Benachrichtigungen sein soll. Standardmäßig ist der primäre Admin-Node ausgewählt, aber jeder Admin-Node kann der bevorzugte Absender sein.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Auf der Seite **Konfiguration > Systemeinstellungen > Anzeigeeoptionen** wird angezeigt, welcher Admin-Node derzeit als bevorzugter Absender ausgewählt wurde. Der primäre Admin-Node ist standardmäßig ausgewählt.

Bei normalen Systemvorgängen sendet nur der bevorzugte Absender folgende Benachrichtigungen:

- AutoSupport Nachrichten
- SNMP-Benachrichtigungen
- E-Mails benachrichtigen
- Alarm-E-Mails (älteres System)

Alle anderen Admin-Knoten (Standby-Sender) überwachen jedoch den bevorzugten Sender. Wenn ein Problem erkannt wird, kann ein Standby-Sender diese Benachrichtigungen auch senden.

In diesen Fällen können sowohl der bevorzugte Sender als auch ein Standby-Sender Benachrichtigungen senden:

- Wenn Admin-Knoten von einander "islanded" werden, werden sowohl der bevorzugte Sender als auch die Standby-Sender versuchen, Benachrichtigungen zu senden, und mehrere Kopien von Benachrichtigungen

können empfangen werden.

- Nachdem ein Standby-Sender Probleme mit dem bevorzugten Sender erkannt hat und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender seine Fähigkeit zum Senden von Benachrichtigungen wiederherstellen. In diesem Fall können doppelte Benachrichtigungen gesendet werden. Der Standby-Sender hört auf, Benachrichtigungen zu senden, wenn Fehler auf dem bevorzugten Sender nicht mehr erkannt werden.



Wenn Sie Alarmbenachrichtigungen und AutoSupport-Meldungen testen, senden alle Admin-Knoten die Test-E-Mail. Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen.

Schritte

1. Wählen Sie **Konfiguration > Systemeinstellungen > Anzeigeeoptionen**.
2. Wählen Sie im Menü Anzeigeeoptionen die Option **Optionen**.
3. Wählen Sie in der Dropdown-Liste den Admin-Knoten aus, den Sie als bevorzugten Sender festlegen möchten.



Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender

ADMIN-DC1-ADM1

Preferred Sender

ADMIN-DC1-ADM1

GUI Inactivity Timeout

900

Notification Suppress All



Apply Changes



4. Klicken Sie Auf **Änderungen Übernehmen**.

Der Admin-Node wird als bevorzugter Absender von Benachrichtigungen festgelegt.


Anzeigen von Benachrichtigungsstatus und -Warteschlangen

Der NMS-Dienst auf Admin Nodes sendet Benachrichtigungen an den Mail-Server. Sie können den aktuellen Status des NMS-Dienstes und die Größe der Benachrichtigungswarteschlange auf der Seite Interface Engine anzeigen.

Um auf die Seite Interface Engine zuzugreifen, wählen Sie **Support > Tools > Grid Topology**. Wählen Sie schließlich **site > Admin Node > NMS > Interface Engine** aus.

OverviewAlarmsReportsConfiguration

Main




Overview: NMS (170-176) - Interface Engine

Updated: 2009-03-09 10:12:17 PDT


NMS Interface Engine Status:

Connected



Connected Services:


15



E-mail Notification Events


E-mail Notifications Status:

No Errors



E-mail Notifications Queued:


0



Database Connection Pool


Maximum Supported Capacity:

100




Remaining Capacity:

95 %



Active Connections:

5

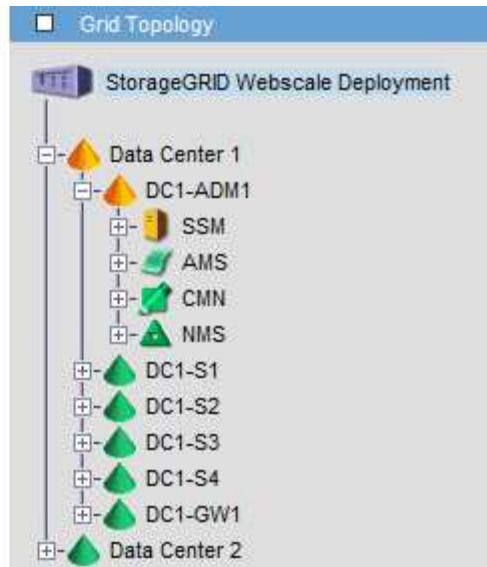
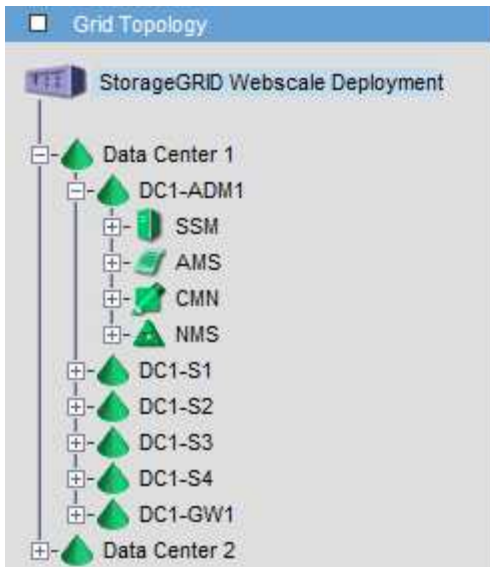


Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und an den Mail-Server gesendet, einer nach dem anderen in der Reihenfolge, in der sie ausgelöst werden. Wenn ein Problem auftritt (z. B. ein Netzwerkverbindungsfehler) und der Mail-Server nicht verfügbar ist, wenn versucht wird, die Benachrichtigung zu senden, wird der Versuch unternommen, die Benachrichtigung an den Mailserver erneut zu senden, 60 Sekunden lang fortgesetzt. Wenn die Benachrichtigung nach 60 Sekunden nicht an den Mailserver gesendet wird, wird die Benachrichtigung aus der Benachrichtigungswarteschlange gelöscht und es wird versucht, die nächste Benachrichtigung in der Warteschlange zu senden. Da Benachrichtigungen aus der Benachrichtigungswarteschlange gelöscht werden können, ohne gesendet zu werden, ist es möglich, dass ein Alarm ausgelöst werden kann, ohne dass eine Benachrichtigung gesendet wird. Wenn eine Benachrichtigung aus der Warteschlange gelöscht wird, ohne gesendet zu werden, wird der Minor-Alarm FÜR MINUTEN (E-Mail-Benachrichtigungsstatus) ausgelöst.

So zeigen Admin-Knoten bestätigte Alarme an (Legacy-System)

Wenn Sie einen Alarm an einem Admin-Knoten bestätigen, wird der bestätigte Alarm nicht auf einen anderen Admin-Knoten kopiert. Da Danksagungen nicht auf andere Admin-Knoten kopiert werden, sieht die Struktur der Grid Topology für jeden Admin-Knoten möglicherweise nicht gleich aus.

Dieser Unterschied kann nützlich sein, wenn Web-Clients verbunden werden. Web-Clients können je nach Administratoranforderungen unterschiedliche Ansichten des StorageGRID-Systems haben.



Beachten Sie, dass Benachrichtigungen vom Admin-Knoten gesendet werden, wo die Bestätigung erfolgt.

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 `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

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 `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 `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 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 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	

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

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"](#)

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 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.