Wiederherstellung bei Ausfällen von Admin-Nodes

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-115/maintain/copying-audit-logs-from-failed-primary-admin-node.html on October 03, 2025. Always check docs.netapp.com for the latest.

Inhalt

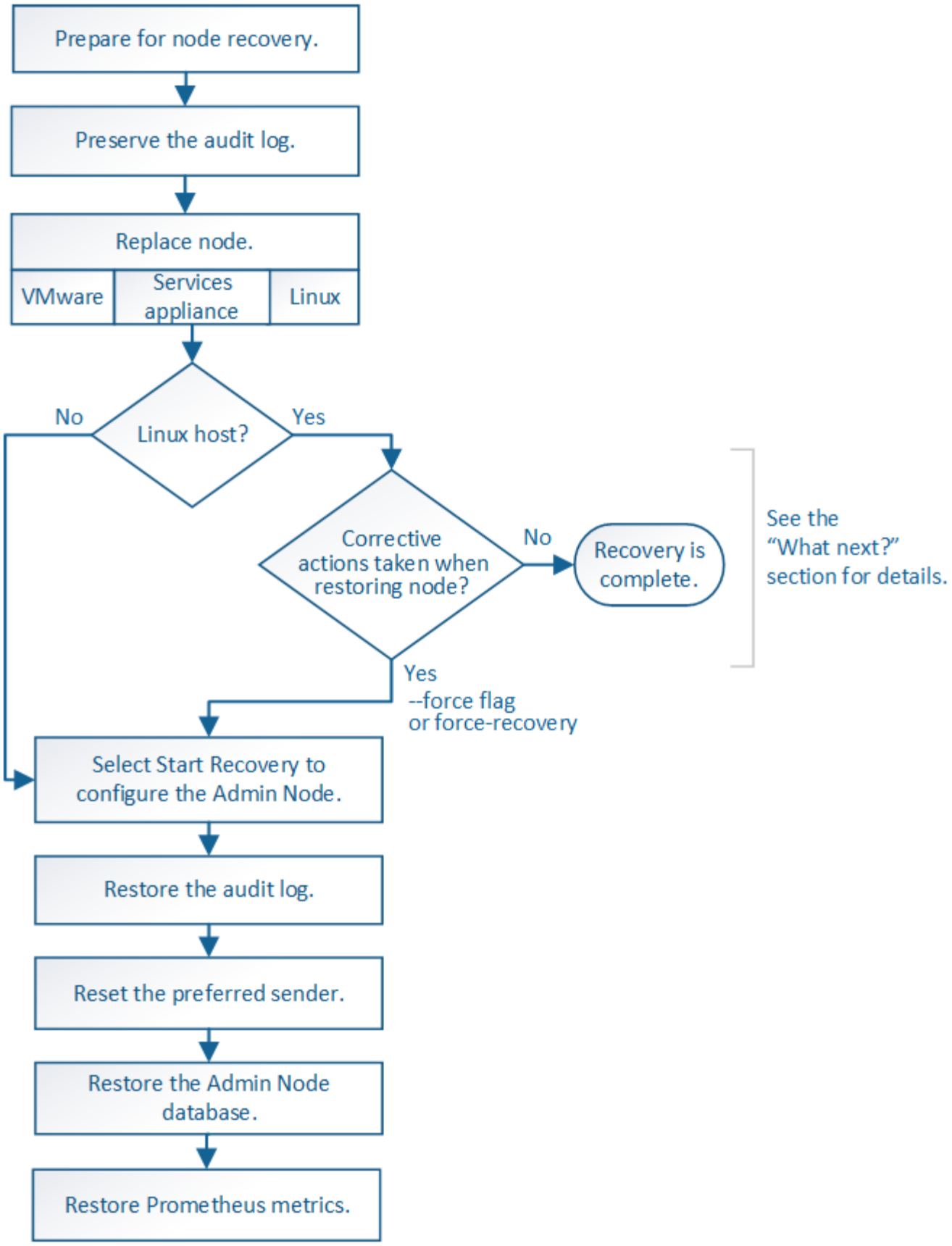
Wiederherstellung bei Ausfällen von Admin-Nodes . . . 1
Wiederherstellung nach Ausfällen des primären Admin-Nodes . . . 3
Prüfprotokolle werden vom fehlgeschlagenen primären Admin-Node kopiert . . . 3
Ersetzen des primären Admin-Knotens . . . 4
Konfigurieren des primären Ersatzadministratorknotens . . . 5
Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten primären Administrator-Knoten . . . 7
Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten primären Admin-Knoten . . . 8
Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines primären Admin-Knotens . . . 8
Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines primären Admin-Knotens . . . 10
Wiederherstellung nach Ausfällen eines Admin-Knotens außerhalb des primären Standorts . . . 11
Prüfprotokolle werden vom fehlgeschlagenen nicht-primären Admin-Node kopiert . . . 12
Ersetzen eines nicht-primären Admin-Knotens . . . 13
Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren . . . 14
Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten nicht-primären Admin-Knoten . . . 15
Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten nicht-primären Admin-Node . . . 17
Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines nicht-primären Admin-Knotens . . . 17
Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines nicht primären Admin-Nodes . . . 19

Wiederherstellung bei Ausfällen von Admin-Nodes

Der Wiederherstellungsprozess für einen Admin-Knoten hängt davon ab, ob es sich um den primären Admin-Knoten oder einen nicht-primären Admin-Knoten handelt.

Über diese Aufgabe

Die Schritte für die Wiederherstellung eines primären oder nicht primären Admin-Knotens auf hoher Ebene sind identisch, wobei sich die Details der einzelnen Schritte unterscheiden.



Befolgen Sie immer den richtigen Wiederherstellungsvorgang für den Admin-Knoten, den Sie wiederherstellen. Die Verfahren sehen auf hohem Niveau gleich aus, unterscheiden sich aber in den Details.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Wahlmöglichkeiten

- "Wiederherstellung nach Ausfällen des primären Admin-Nodes"
- "Wiederherstellung nach Ausfällen eines Admin-Knotens außerhalb des primären Standorts"

Wiederherstellung nach Ausfällen des primären Admin-Nodes

Sie müssen einen bestimmten Satz von Aufgaben ausführen, um nach einem Ausfall eines primären Admin-Knotens wiederherstellen zu können. Der primäre Admin-Node hostet den Configuration Management Node (CMN)-Service für das Grid.

Über diese Aufgabe

Ein fehlgeschlagener primärer Admin-Node sollte umgehend ersetzt werden. Der Configuration Management Node (CMN)-Dienst auf dem primären Admin-Node ist für die Ausgabe von Objektkennungen für das Grid verantwortlich. Diese Kennungen werden Objekten bei ihrer Aufnahme zugewiesen. Neue Objekte können erst dann aufgenommen werden, wenn Identifikatoren verfügbar sind. Die Objektaufnahme kann fortgesetzt werden, während das CMN nicht verfügbar ist, da die Identifikatoren ungefähr einen Monat im Grid zwischengespeichert werden. Nachdem jedoch die gecachten Kennungen erschöpft sind, können keine neuen Objekte hinzugefügt werden.

> Sie müssen einen fehlerhaften primären Administrator-Node innerhalb von etwa einem Monat reparieren oder ersetzen. Andernfalls kann das Grid die Aufnahme neuer Objekte verlieren. Der genaue Zeitraum hängt von der Geschwindigkeit der Objekterfassung ab: Wenn Sie eine genauere Bewertung des Zeitrahmens für Ihr Grid benötigen, wenden Sie sich an den technischen Support.

Schritte

- "Prüfprotokolle werden vom fehlgeschlagenen primären Admin-Node kopiert"
- "Ersetzen des primären Admin-Knotens"
- "Konfigurieren des primären Ersatzadministratorknotens"
- "Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten primären Administrator-Knoten"
- "Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten primären Admin-Knoten"
- "Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines primären Admin-Knotens"
- "Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines primären Admin-Knotens"

Prüfprotokolle werden vom fehlgeschlagenen primären Admin-Node kopiert

Wenn Sie Audit-Protokolle vom fehlgeschlagenen primären Admin-Node kopieren können, sollten Sie diese beibehalten, um den Datensatz der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem wiederhergestellten primären Admin-Knoten wiederherstellen, nachdem er in Betrieb ist.

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den

Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.

Wenn jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.
   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:

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

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:`service ams stop`
3. Benennen Sie die Datei audit.log um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

   Benennen Sie audit.log in einen eindeutigen nummerierten Dateinamen um, z. B. yyyy-mm-dd.txt.1. Beispielsweise können Sie die Datei audit.log in 2015-10-25.txt.1 umbenennen`cd /var/local/audit/export/`

4. AMS-Dienst neu starten: `service ams start`
5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

7. Melden Sie sich als Root an: `exit`

Ersetzen des primären Admin-Knotens

Um einen primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen fehlgeschlagenen primären Admin-Node durch einen primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen primären Admin-Node ersetzen, der auf einer Services-Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die primäre Admin-Knoten-Wiederherstellung geleitet.

Austauschplattform	Verfahren
VMware	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
SG100- und SG1000-Services-Appliances	"Ersetzen einer Service Appliance"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Konfigurieren des primären Ersatzadministratorknotens

Der Ersatzknoten muss als primärer Admin-Node für Ihr StorageGRID System konfiguriert sein.

Was Sie benötigen

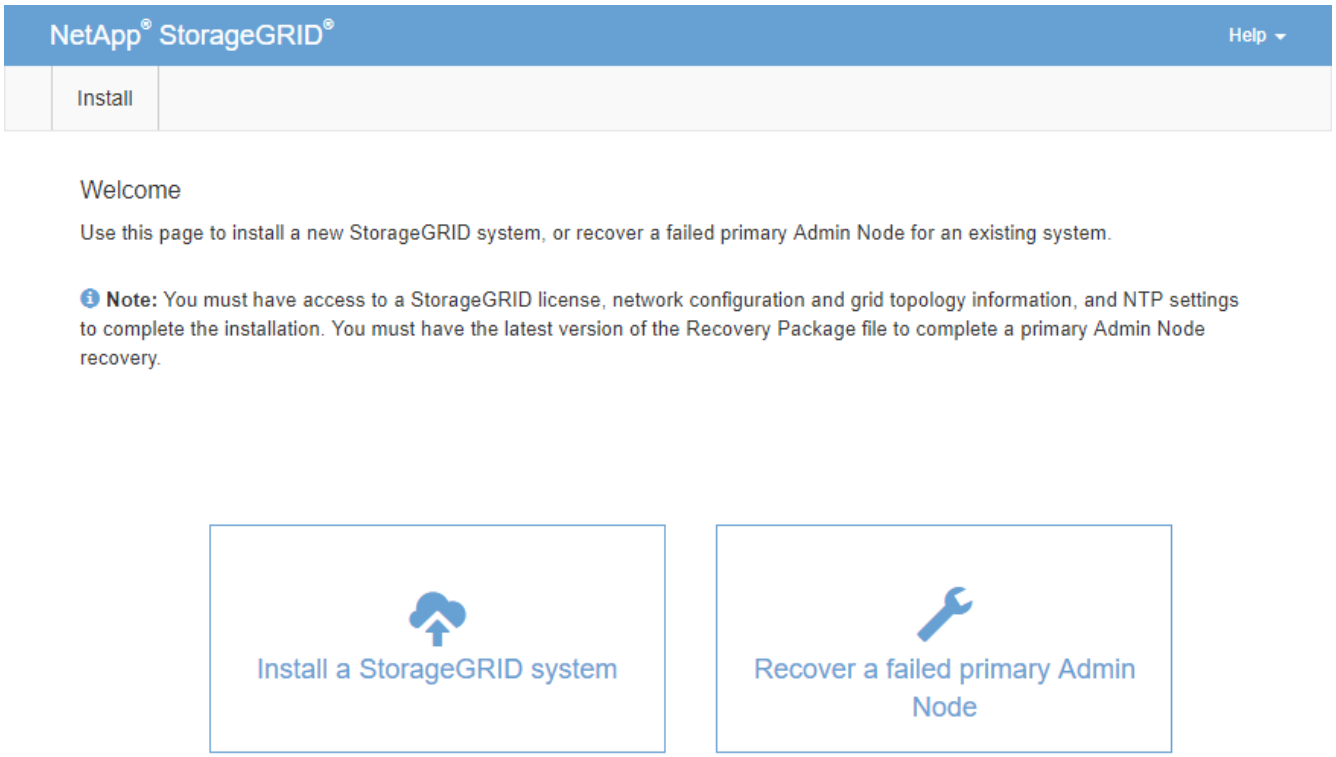
- Für primäre Admin-Knoten, die auf virtuellen Maschinen gehostet werden, muss die virtuelle Maschine bereitgestellt, eingeschaltet und initialisiert werden.
- Für primäre Admin-Nodes, die auf einer Services-Appliance gehostet werden, haben Sie die Appliance ersetzt und die installierte Software installiert. Informationen zum Gerät finden Sie im Installationshandbuch.

  "SG100 SG1000 Services-Appliances"

- Sie müssen über die neueste Sicherung der Wiederherstellungspaket-Datei verfügen (`sgws-recovery-package-`*`id-revision`*`.zip`).
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu `https://primary_admin_node_ip`.



2. Klicken Sie auf **Wiederherstellen eines fehlgeschlagenen primären Admin-Knotens**.
3. Laden Sie das aktuellste Backup des Wiederherstellungspakets hoch:
   a. Klicken Sie Auf **Durchsuchen**.
   b. Suchen Sie die aktuellste Wiederherstellungspakedatei für Ihr StorageGRID-System und klicken Sie auf **Öffnen**.
4. Geben Sie die Provisionierungs-Passphrase ein.
5. Klicken Sie Auf **Wiederherstellung Starten**.

   Der Wiederherstellungsprozess beginnt. Der Grid Manager ist möglicherweise einige Minuten lang nicht mehr verfügbar, wenn die erforderlichen Dienste gestartet werden. Wenn die Wiederherstellung abgeschlossen ist, wird die Anmeldeseite angezeigt.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Standardzertifikat für Verwaltungsschnittstellen-Server konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Knotens auf die Vertrauensbasis in Active Directory-Föderationsdienste (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.

   Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

7. Bestimmen Sie, ob Sie einen Hotfix anwenden müssen.

a. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.

b. Wählen Sie **Knoten**.

c. Wählen Sie in der Liste links den primären Admin-Node aus.

d. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.

e. Wählen Sie einen beliebigen anderen Grid-Knoten aus.

f. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.

   - Wenn die in den Feldern **Software Version** angezeigten Versionen identisch sind, müssen Sie keinen Hotfix anwenden.
   - Wenn die in den Feldern **Softwareversion** angezeigten Versionen anders sind, müssen Sie einen Hotfix anwenden, um den wiederhergestellten primären Admin-Knoten auf dieselbe Version zu aktualisieren.

Verwandte Informationen

"StorageGRID verwalten"

"StorageGRID Hotfix Verfahren"

Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten primären Administrator-Knoten

Wenn Sie das Revisionsprotokoll vom fehlgeschlagenen primären Admin-Knoten erhalten konnten, können Sie es in den primären Admin-Knoten kopieren, den Sie wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein: `ssh admin@recovery_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:

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

2. Prüfen Sie, welche Audit-Dateien erhalten wurden: `cd /var/local/audit/export`
3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.
4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.
5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten: `chown ams-user:bycast *`
6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten primären Admin-Knoten

Wenn der primäre Admin-Knoten, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmanmeldungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung neu konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"StorageGRID verwalten"

Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines primären Admin-Knotens

Wenn Sie die historischen Informationen über Attribute, Alarme und Alarme auf einem primären Admin-Node, der ausgefallen ist, behalten möchten, können Sie die Admin-

Node-Datenbank wiederherstellen. Sie können diese Datenbank nur wiederherstellen, wenn Ihr StorageGRID-System einen anderen Admin-Knoten enthält.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **Support Tools Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Knoten-Datenbank von einem nicht-primären Admin-Knoten (der_Quell-Admin-Knoten_) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur einen primären Admin-Knoten hat, können Sie die Admin-Knoten-Datenbank nicht wiederherstellen.

> Das Kopieren der Admin-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-Node an:
   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:
2. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
3. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
4. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      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. Beenden SIE DEN MI-Dienst: `service mi stop`

c. Beenden Sie den Management API-Service: `service mgmt-api stop`

d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`

e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

   Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.

h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`

5. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines primären Admin-Knotens

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem primären Admin-Node gewartet wurden, der ausgefallen ist. Die Prometheus Kennzahlen können nur wiederhergestellt werden, wenn Ihr StorageGRID System einen anderen Admin-Knoten enthält.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank von einem nicht-primären Admin-Knoten (den *Source Admin-Knoten*) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur einen primären Admin-Knoten hat, können Sie die Prometheus-Datenbank nicht wiederherstellen.

> Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-Node an:

   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:

2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:

a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

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. Stoppen Sie den Prometheus Service: `service prometheus stop`

c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`

d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Der folgende Status wird angezeigt:

Datenbank geklont, Dienste starten

a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`

4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.`service prometheus start`

Wiederherstellung nach Ausfällen eines Admin-Knotens außerhalb des primären Standorts

Sie müssen die folgenden Aufgaben durchführen, um nach einem Ausfall eines nicht primären Admin-Knotens wiederherzustellen. Ein Admin-Node hostet den Configuration Management Node (CMN)-Service und ist als primärer Admin-Node bekannt. Obwohl Sie mehrere Admin-Nodes haben können, enthält jedes StorageGRID-System nur einen primären Admin-Node. Alle anderen Admin-Nodes sind nicht primäre Admin-Nodes.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Schritte

- "Prüfprotokolle werden vom fehlgeschlagenen nicht-primären Admin-Node kopiert"

- "Ersetzen eines nicht-primären Admin-Knotens"
- "Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren"
- "Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten nicht-primären Admin-Knoten"
- "Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten nicht-primären Admin-Node"
- "Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines nicht-primären Admin-Knotens"
- "Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines nicht primären Admin-Nodes"

Prüfprotokolle werden vom fehlgeschlagenen nicht-primären Admin-Node kopiert

Wenn Sie in der Lage sind, Audit-Protokolle vom fehlgeschlagenen Admin-Node zu kopieren, sollten Sie diese beibehalten, um die Aufzeichnung der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem Wiederherstellen des nicht-primären Admin-Knotens wiederherstellen, nachdem er ausgeführt wurde.

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.

> ⓘ Wenn jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.
   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:

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

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:`service ams stop`
3. Benennen Sie die Datei audit.log um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

   Benennen Sie audit.log in einen eindeutigen nummerierten Dateinamen um, z. B. yyyy-mm-dd.txt.1.

Beispielsweise können Sie die Datei audit.log in 2015-10-25.txt.1 umbenennen`cd /var/local/audit/export/`

4. AMS-Dienst neu starten: `service ams start`
5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

7. Melden Sie sich als Root an: `exit`

Ersetzen eines nicht-primären Admin-Knotens

Um einen nicht-primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen nicht primären Admin-Node durch einen nicht-primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen nicht-primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen nicht-primären Admin-Node ersetzen, der auf einer Services Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung eines nicht-primären Admin-Knotens geleitet.

Austauschplattform	Verfahren
VMware	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
SG100- und SG1000-Services-Appliances	"Ersetzen einer Service Appliance"
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren

Nach dem Ersetzen eines nicht-primären Admin-Knotens müssen Sie im Grid-Manager die Option Wiederherstellung starten wählen, um den neuen Knoten als Ersatz für den fehlgeschlagenen Knoten zu konfigurieren.

Was Sie benötigen

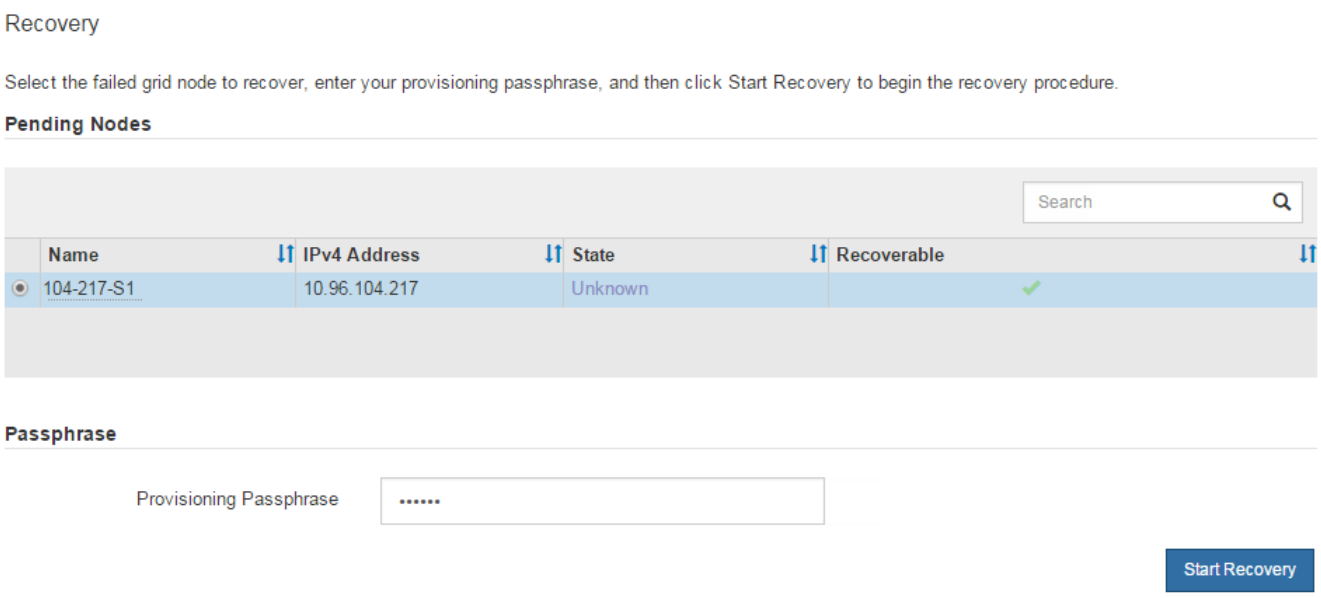
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

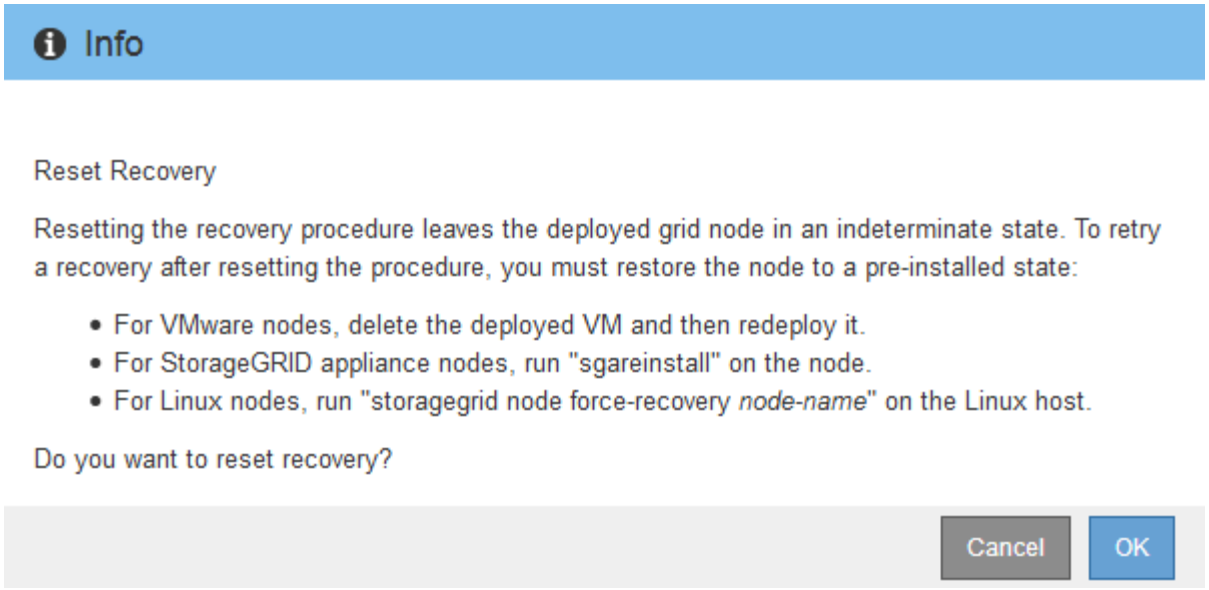
   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware**: Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux**: Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen: `storagegrid node force-recovery node-name`
- **Appliance**: Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Geräteknoten durch Ausführen in einen vorinstallierten Zustand wiederherstellen `sgareinstall` Auf dem Node.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Standardzertifikat für Verwaltungsschnittstellen-Server konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Knotens auf die Vertrauensbasis in Active Directory-Föderationsdienste (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.

> Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

Verwandte Informationen

"StorageGRID verwalten"

"Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"

Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten nicht-primären Admin-Knoten

Wenn Sie das Audit-Protokoll vom fehlgeschlagenen nicht-primären Admin-Node erhalten konnten, damit die Informationen des historischen Audit-Protokolls beibehalten werden,

können Sie es in den nicht-primären Admin-Node kopieren, den Sie wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein:
   `ssh admin@recovery_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:

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

2. Prüfen Sie, welche Audit-Dateien erhalten wurden:

   ```
   cd /var/local/audit/export
   ```

3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten:

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.
5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten:

   ```
   chown ams-user:bycast *
   ```

6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten nicht-primären Admin-Node

Wenn der nicht-primäre Admin-Node, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmbenachrichtigungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung im StorageGRID-System neu konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"StorageGRID verwalten"

Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines nicht-primären Admin-Knotens

Wenn Sie die historischen Informationen zu Attributen, Alarmen und Warnmeldungen bei einem nicht primären Admin-Node behalten möchten, der ausgefallen ist, können Sie die Admin-Knoten-Datenbank vom primären Admin-Node wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **Support Tools Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen nicht-primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Node-Datenbank vom primären Admin-Knoten (den_Quell-Admin-Node_) auf den wiederhergestellten Knoten kopieren.

> Das Kopieren der Admin-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quellknoten angehalten werden.

1. Melden Sie sich beim Quell-Admin-Node an:
   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:
2. Führen Sie den folgenden Befehl vom Quell-Admin-Knoten aus. Geben Sie dann die Provisionierungs-Passphrase ein, wenn Sie dazu aufgefordert werden. `recover-access-points`
3. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
4. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
5. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      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. Beenden SIE DEN MI-Dienst: `service mi stop`
   c. Beenden Sie den Management API-Service: `service mgmt-api stop`
   d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
   e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
   f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

      Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.

   h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`
6. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines nicht primären Admin-Nodes

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem nicht primären Admin-Node gewartet wurden, der ausgefallen ist.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen nicht-primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank vom primären Admin-Knoten (den_Source Admin-Node_) auf den wiederhergestellten Admin-Knoten kopieren.

> ⓘ Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-Node an:
   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:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
   a. Melden Sie sich beim wiederhergestellten Admin-Knoten an:
      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. Stoppen Sie den Prometheus Service: `service prometheus stop`
   c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
   d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
   e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue

Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Der folgende Status wird angezeigt:

Datenbank geklont, Dienste starten

a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`

4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.`service prometheus start`

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.