管理ノードを管理する
StorageGRID 11.7

NetApp
April 12, 2024

目次

管理ノードを管理する 1
管理ノードとは 1
複数の管理ノードを使用する 2
プライマリ管理ノードを特定します 3
通知のステータスとキューを表示します 4
管理ノードによる確認済みアラームの表示（従来のシステム） 5
監査クライアントアクセスを設定します 5

管理ノードを管理する

管理ノードとは

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。各グリッドにはプライマリ管理ノードが 1 つ必要で、冗長性を確保するために任意の数の非プライマリ管理ノードを設定できます。

Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。ただし、メンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

管理ノードを使用して、 S3 および Swift クライアントトラフィックの負荷を分散することもできます。

優先送信者とは何ですか

StorageGRID 環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupport メッセージ、SNMPトラップとインフォーム、および従来のアラーム通知の優先送信者となります。

通常のシステム運用では、優先送信者のみが通知を送信します。ただし、他のすべての管理ノードで優先送信者を監視します。問題が検出された場合、他の管理ノードは_standby senders_として動作します。

次の場合、複数の通知が送信されることがあります。

- 管理ノードどうしが「孤立」すると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知のコピーが複数受信される可能性があります。
- スタンバイ送信者が優先送信者に関する問題を検出して通知の送信を開始すると、優先送信者は通知を再び送信できるようになることがあります。この場合、重複する通知が送信される可能性があります。優先送信者に関するエラーが検出されなくなると、スタンバイ送信者は通知の送信を停止します。

> AutoSupport メッセージのテスト時には、すべての管理ノードからテストEメールが送信されます。アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。

管理ノードのプライマリサービス

次の表に、管理ノードのプライマリサービスを示します。ただし、この表にはすべてのノードサービスが表示されるわけではありません。

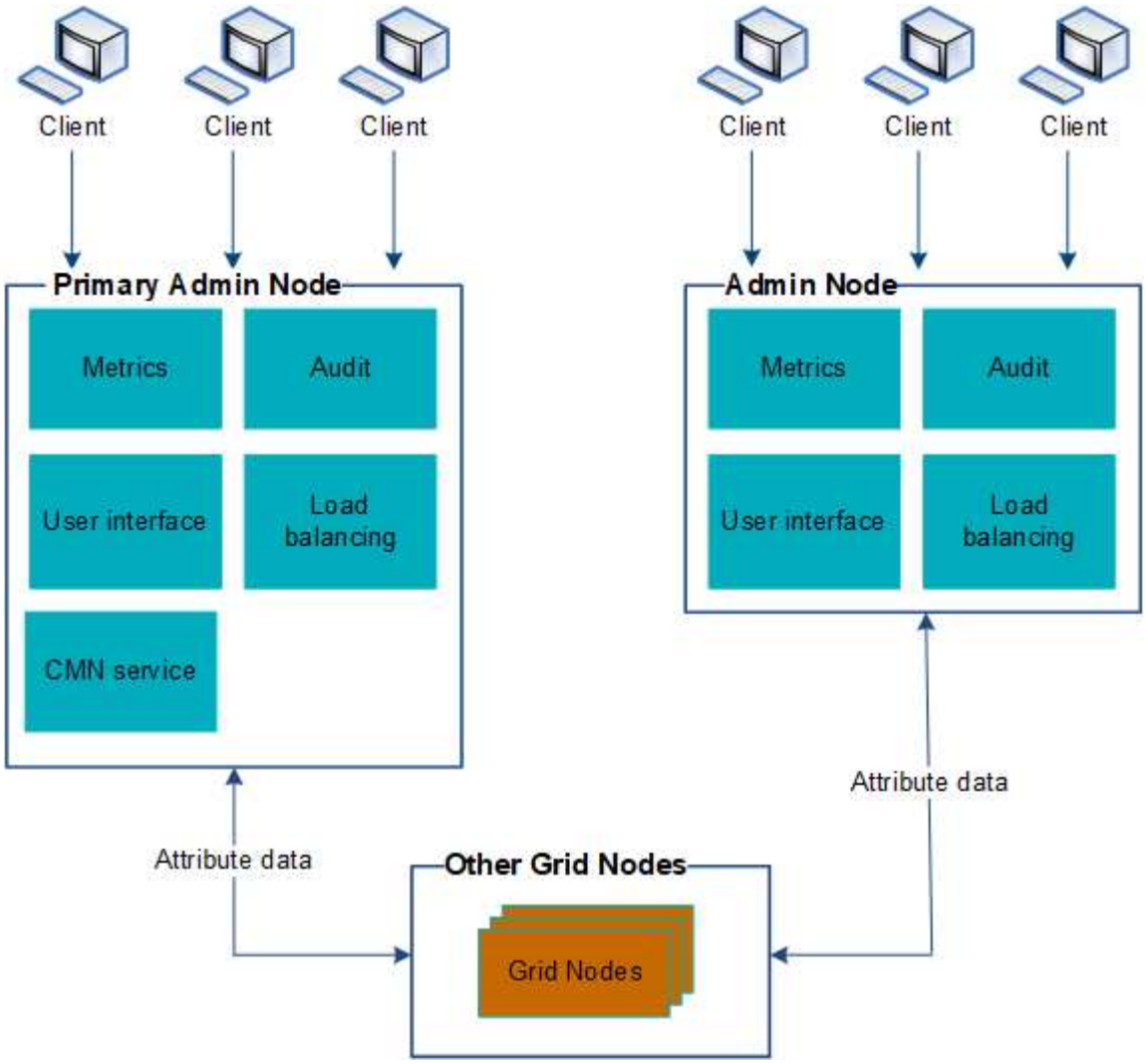
サービス	キー機能
Audit Management System （ AMS ）	システムアクティビティとイベントを追跡します。
Configuration Management Node （ CMN ）	システム全体の設定を管理します。プライマリ管理ノードのみ

サービス	キー機能
管理アプリケーションプログラミングインターフェイス（ mgmt-api ）	グリッド管理 API とテナント管理 API からの要求を処理します。
高可用性	管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。 • 注： * このサービスはゲートウェイノードにも搭載されています。
ロードバランサ	クライアントからストレージノードへの S3 および Swift トラフィックのロードバランシングを実現します。 • 注： * このサービスはゲートウェイノードにも搭載されています。
ネットワーク管理システム（ NMS ）	Grid Manager の機能を提供します。
Prometheus	すべてのノードのサービスから時系列の指標を収集して格納します。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

複数の管理ノードを使用する

StorageGRID システムには複数の管理ノードを含めることができます。これにより、 1 つの管理ノードに障害が発生した場合でも、 StorageGRID システムを継続的に監視して設定することができます。

ある管理ノードが使用できなくなっても属性の処理は続行され、アラートとアラーム（従来のシステム）は引き続きトリガーされ、 E メール通知と AutoSupport メッセージは引き続き送信されます。ただし、通知と AutoSupport メッセージ以外のフェイルオーバー保護は提供されません。特に、ある管理ノードからのアラームの確認応答は他の管理ノードにはコピーされません。



管理ノードに障害が発生した場合、次の 2 つの方法で StorageGRID システムを引き続き表示および設定することができます。

- Web クライアントは使用可能な他の管理ノードに再接続できます。
- システム管理者が管理ノードのハイアベイラビリティグループを設定している場合、 Web クライアントは HA グループの仮想 IP アドレスを使用して引き続き Grid Manager または Tenant Manager にアクセスできます。を参照してください "ハイアベイラビリティグループを管理します"。

> HAグループを使用している場合、アクティブな管理ノードで障害が発生するとアクセスが中断されます。ユーザは、 HA グループの仮想 IP アドレスがグループ内の別の管理ノードにフェイルオーバーしたあとで、再度サインインする必要があります。

一部のメンテナンスタスクはプライマリ管理ノードでしか実行できません。プライマリ管理ノードに障害が発生した場合、そのノードをリカバリするまでは、 StorageGRID システムは完全に機能している状態ではありません。

プライマリ管理ノードを特定します

プライマリ管理ノードは CMN サービスをホストします。一部のメンテナンス手順は、

プライマリ管理ノードでしか実行できません。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _site * > * Admin Node * 」を選択し、を選択します ➕ をクリックしてトポロジツリーを展開し、この管理ノードでホストされているサービスを表示します。

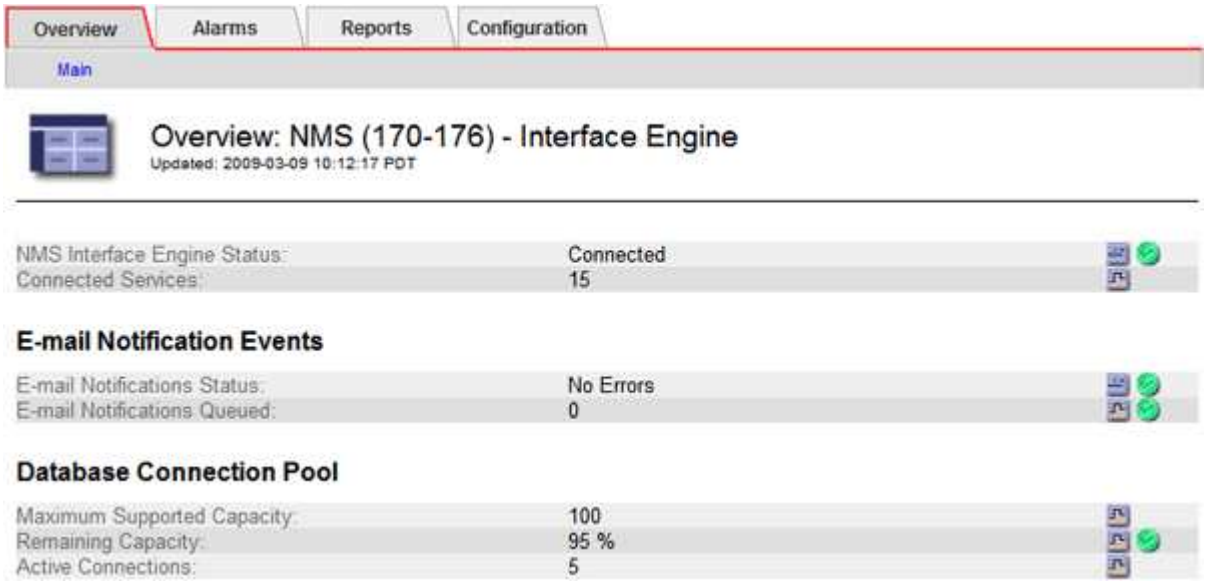
   プライマリ管理ノードは CMN サービスをホストします。

3. この管理ノードが CMN サービスをホストしていない場合、他の管理ノードを確認します。

通知のステータスとキューを表示します

管理ノードの Network Management System （ NMS ）サービスは、メールサーバに通知を送信します。NMS サービスの現在のステータスとその通知キューのサイズは、Interface Engine ページで確認できます。

Interface Engine ページにアクセスするには、 * support * > * Tools * > * Grid topology * を選択します。最後に、 * *site* _ * > * *_Admin Node** > * NMS * > * Interface Engine * を選択します。



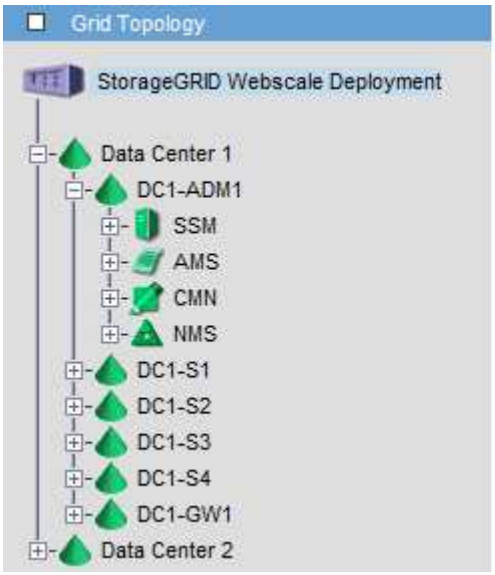
通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。

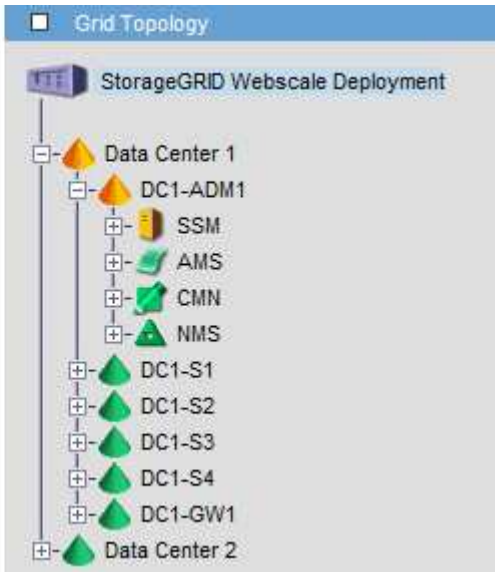
通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューからドロップされると、MINS（E-mail Notification Status ）Minorアラームがトリガーされます。

管理ノードによる確認済みアラームの表示（従来のシステム）

ある管理ノードのアラームを確認しても、確認済みのアラームは他の管理ノードにはコピーされません。確認応答は他の管理ノードにはコピーされないため、[Grid Topology] ツリーの表示が各管理ノードで同じにならないことがあります。

この違いは、 Web クライアントに接続する場合に役立ちます。Web クライアントでは、管理者のニーズに基づいて、 StorageGRID システムをさまざまな方法で表示できます。





通知は、確認応答が発生した管理ノードから送信されます。

監査クライアントアクセスを設定します

NFSの監査クライアントアクセスを設定します

管理ノードは、 Audit Management System （ AMS ）サービスを介して、監査対象のすべてのシステムイベントを、監査共有からアクセス可能なログファイルに記録します。監査共有はインストール時に各管理ノードに追加されます。監査共有は読み取り専用の共有として自動的に有効になります。

監査ログにアクセスするには、NFSの監査共有へのクライアントアクセスを設定します。または、できます "外部syslogサーバを使用します"。

StorageGRID システムは、確認応答を使用して、ログファイルに書き込まれる前に監査メッセージが失われないようにします。AMS サービスまたは中間の監査リレーサービスがメッセージの制御を確認するまで、メッセージはサービスのキューに残ります。詳細については、を参照してください "監査ログを確認します"。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminパスワードが設定されたファイル。
- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。
- 監査クライアントが NFS バージョン 3 （ NFSv3 ）を使用している。

このタスクについて

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   「Running」または「Verified」と表示されないサービスがある場合は、問題を解決してから続行してください。

3. コマンドラインに戻ります。Ctrl キーを押しながら * C キーを押します。
4. NFS 設定ユーティリティを起動します。入力するコマンド `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. 監査クライアントを追加します。 `add-audit-share`
   a. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 `client_IP_address`
   b. プロンプトが表示されたら、 * Enter * を押します。
6. 複数の監査クライアントに監査共有へのアクセスを許可する場合は、ユーザのIPアドレスを追加します。 `add-ip-to-share`
   a. 監査共有の番号を入力します。 *`audit_share_number`*
   b. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*
   c. プロンプトが表示されたら、 * Enter * を押します。

      NFS 設定ユーティリティが表示されます。

d. 監査共有に追加する監査クライアントごとに、上記の手順を繰り返します。

7. 必要に応じて、設定を確認します。

a. 次のように入力します。 `validate-config`

サービスがチェックされて表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

c. NFS設定ユーティリティを閉じます。 `exit`

8. 他のサイトで監査共有を有効にする必要があるかどうかを確認します。

◦ StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

◦ StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

i. サイトの管理ノードにリモートからログインします。

A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

B. に記載されているパスワードを入力します `Passwords.txt` ファイル。

C. 次のコマンドを入力してrootに切り替えます。 `su -`

D. に記載されているパスワードを入力します `Passwords.txt` ファイル。

ii. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。

iii. リモート管理ノードへのリモートの Secure Shell ログインを終了します。入力するコマンド `exit`

9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに共有に IP アドレスを追加して監査共有へのアクセスを許可するか、または IP アドレスを削除して既存の監査クライアントを削除します。

監査共有に **NFS** 監査クライアントを追加します

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに監査共有へのアクセスを許可するには、そのクライアントの IP アドレスを監査共有に追加します。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminアカウントのパスワードが設定されたファイル。
- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。
- 監査クライアントが NFS バージョン 3 （ NFSv3 ）を使用している。

手順

1. プライマリ管理ノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `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. 入力するコマンド `add-ip-to-share`

管理ノードで有効になっている NFS 監査共有のリストが表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*

監査クライアントが監査共有に追加されます。

6. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

7. 監査共有に追加する監査クライアントごとに、この手順を繰り返します。
8. 必要に応じて、設定を確認します。 `validate-config`

サービスがチェックされて表示されます。

a. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

9. NFS設定ユーティリティを閉じます。 `exit`
10. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有

効にします。

a. サイトの管理ノードにリモートからログインします。

   i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   iii. 次のコマンドを入力してrootに切り替えます。 `su -`

   iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。

c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

11. コマンドシェルからログアウトします。 `exit`

NFS 監査の統合を確認

監査共有を設定して NFS 監査クライアントを追加したら、監査クライアント共有をマウントし、監査共有のファイルにアクセスできることを確認します。

手順

1. AMS サービスをホストしている管理ノードのクライアント側 IP アドレスを使用して、接続（またはクライアントシステムでの操作）を検証します。入力するコマンド `ping IP_address`

   サーバが応答して接続を示していることを確認します。

2. クライアントのオペレーティングシステムに適したコマンドを使用して、読み取り専用の監査共有をマウントします。Linux コマンドの例は次のとおりです（ 1 行で入力します）。

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

   AMS サービスをホストしている管理ノードの IP アドレスと、監査システムの事前定義された共有名を使用します。マウントポイントには、クライアントが選択した任意の名前を使用できます（例： *myAudit* 前のコマンドを参照）。

3. 監査共有のファイルにアクセスできることを確認します。入力するコマンド `ls myAudit /*`

   ここで、 *myAudit* は、監査共有のマウントポイントです。少なくとも 1 つのログファイルが表示されている必要があります。

監査共有から NFS 監査クライアントを削除します

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。既存の監査クライアントを削除するには、その IP アドレスを削除します。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminアカウントのパスワードが設定されたファイル。

- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。

このタスクについて

監査共有へのアクセスを許可した最後のIPアドレスは削除できません。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `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. 監査共有からIPアドレスを削除します。 `remove-ip-from-share`

   サーバで設定されている監査共有に番号が振られ、リストに表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有に対応する番号を入力します。 *`audit_share_number`*

   監査共有へのアクセスを許可している IP アドレスに番号が振られ、リストに表示されます。

5. 削除する IP アドレスに対応する番号を入力します。

   監査共有が更新され、この IP アドレスの監査クライアントからのアクセスは許可されなくなります。

6. プロンプトが表示されたら、 * Enter * を押します。

   NFS 設定ユーティリティが表示されます。

7. NFS設定ユーティリティを閉じます。 `exit`
8. StorageGRID 環境が複数データセンターサイトの環境であり、他のサイトにも管理ノードが含まれている場合は、必要に応じてこれらの監査共有を無効にします。

a. 各サイトの管理ノードにリモートからログインします。
   i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   iii. 次のコマンドを入力してrootに切り替えます。 `su -`
   iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントの IP アドレスを変更します

NFS 監査クライアントの IP アドレスを変更する必要がある場合は、次の手順を実行します。

手順

1. 既存の NFS 監査共有に新しい IP アドレスを追加します。
2. 元の IP アドレスを削除します。

関連情報

- "監査共有に NFS 監査クライアントを追加します"
- "監査共有から NFS 監査クライアントを削除します"

著作権に関する情報

商標に関する情報