管理ノードの管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

管理ノードの管理

StorageGRID 環境の各サイトには管理ノードを1つ以上配置できます。

- "管理ノードとは"
- "複数の管理ノードを使用する"
- "プライマリ管理ノードの特定"
- "優先送信者を選択しています"
- "通知のステータスとキューの表示"
- "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）"
- "監査クライアントアクセスを設定しています"

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。

管理ノードは次のサービスをホストします。

- AMS サービス
- CMN サービス
- NMS サービス
- Prometheus サービス
- ロードバランササービスとハイアベイラビリティサービス（ S3 および Swift クライアントトラフィックをサポート）

管理ノードは、グリッド管理 API とテナント管理 API からの要求を処理する管理アプリケーションプログラムインターフェイス（ mgmt-api ）もサポートします。

AMS サービスとは

Audit Management System （ AMS ）サービスは、システムアクティビティとイベントを追跡します。

CMN サービスとは

Configuration Management Node （ CMN ）サービスは、すべてのサービスで必要とされる接続およびプロトコルの機能について、システム全体での設定を管理します。CMN サービスはグリッドタスクの実行および監

視にも使用されます。StorageGRID 環境ごとに CMN サービスは 1 つだけです。CMN サービスをホストする管理ノードをプライマリ管理ノードと呼びます。

NMS サービスとは

Network Management System （ NMS ）サービスは、 StorageGRID システムのブラウザベースのインターフェイスであるグリッドマネージャに表示される、監視、レポート、および設定のオプションを提供します。

Prometheus サービスとは

Prometheus サービスは、すべてのノードのサービスから時系列の指標を収集します。

関連情報

"グリッド管理APIを使用する"

"テナントアカウントを使用する"

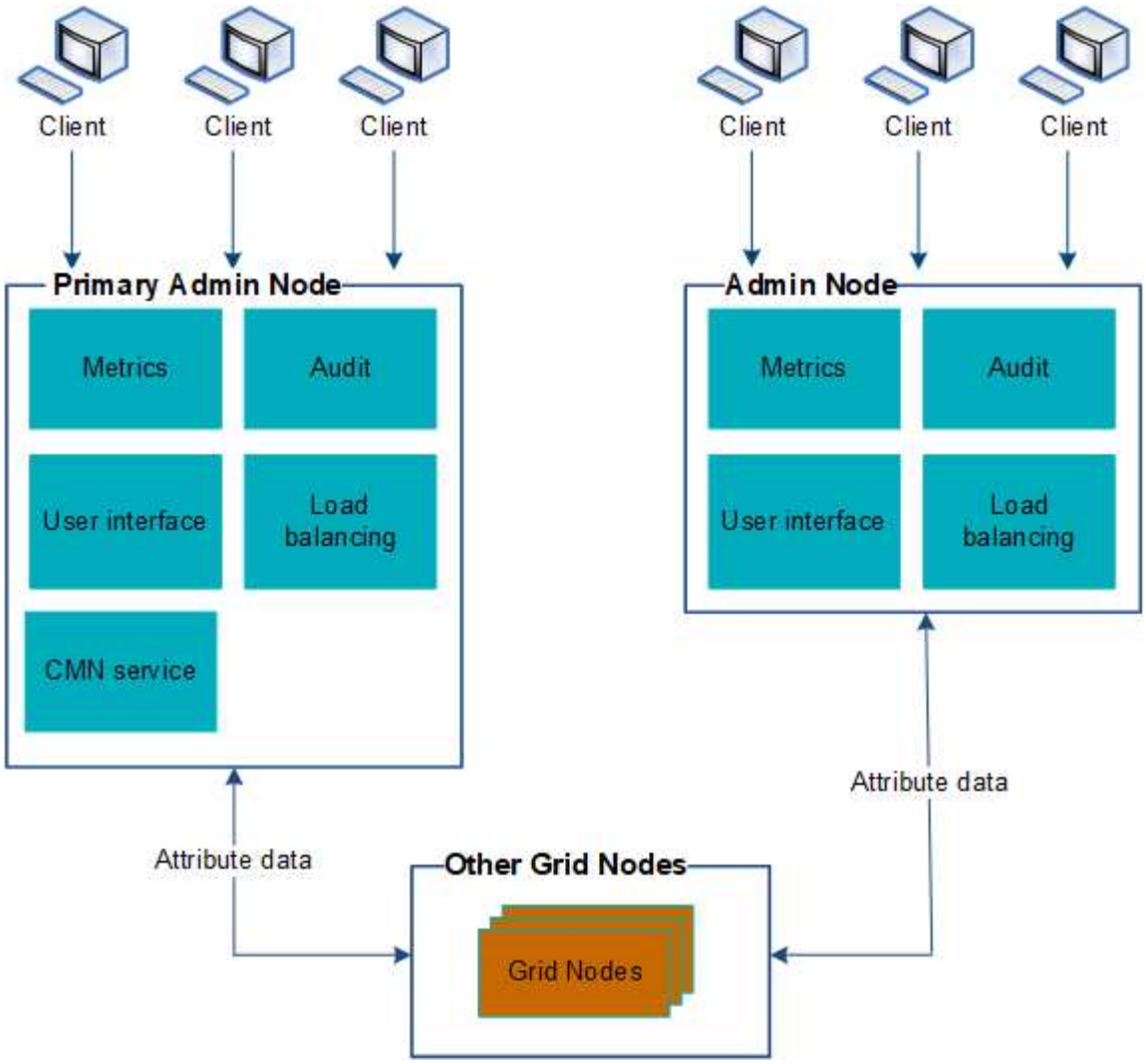
"負荷分散の管理"

"ハイアベイラビリティグループの管理"

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。

> HA グループを使用している場合、マスター管理ノードに障害が発生するとアクセスが中断します。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。

関連情報

"ハイアベイラビリティグループの管理"

プライマリ管理ノードの特定

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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [_site **管理ノード]を選択し、をクリックします ➕ 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。

優先送信者を選択しています

StorageGRID 環境に複数の管理ノードが含まれている場合は、通知の優先送信者となる管理ノードを選択できます。デフォルトでは、プライマリ管理ノードが選択されますが、任意の管理ノードを優先送信者にすることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

「* Configuration * System Settings * Display Options *」ページに、現在優先送信者として選択されている管理ノードが表示されます。デフォルトでは、プライマリ管理ノードが選択されます。

通常のシステム運用では、優先送信者のみが次の通知を送信します。

- AutoSupport メッセージ
- SNMP 通知
- アラート E メール
- アラーム E メール（レガシーシステム）

ただし、他のすべての管理ノード（スタンバイ送信者）が優先送信者を監視します。問題が検出された場合は、スタンバイ送信者もこれらの通知を送信できます。

次の場合、優先送信者とスタンバイ送信者の両方が通知を送信することがあります。

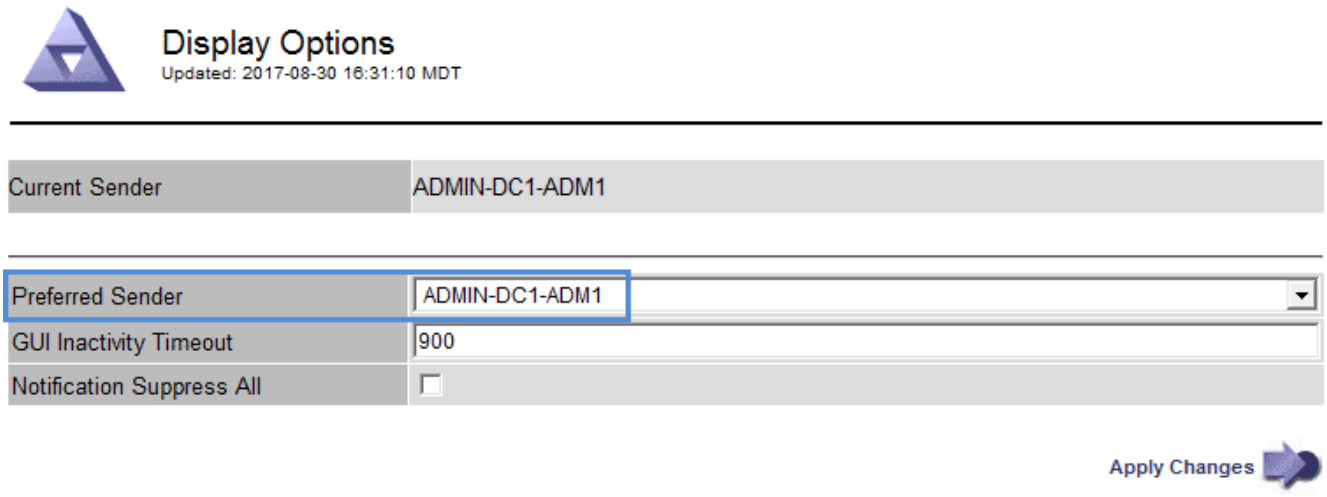
- 管理ノードどうしが「孤立した」状態になると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知が重複して届く可能性があります。

- 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したあとで、優先送信者が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。

アラーム通知と AutoSupport メッセージをテストするときは、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。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. [表示オプション] メニューから、 [* オプション *] を選択します。
3. 優先送信者として設定する管理ノードをドロップダウンリストから選択します。



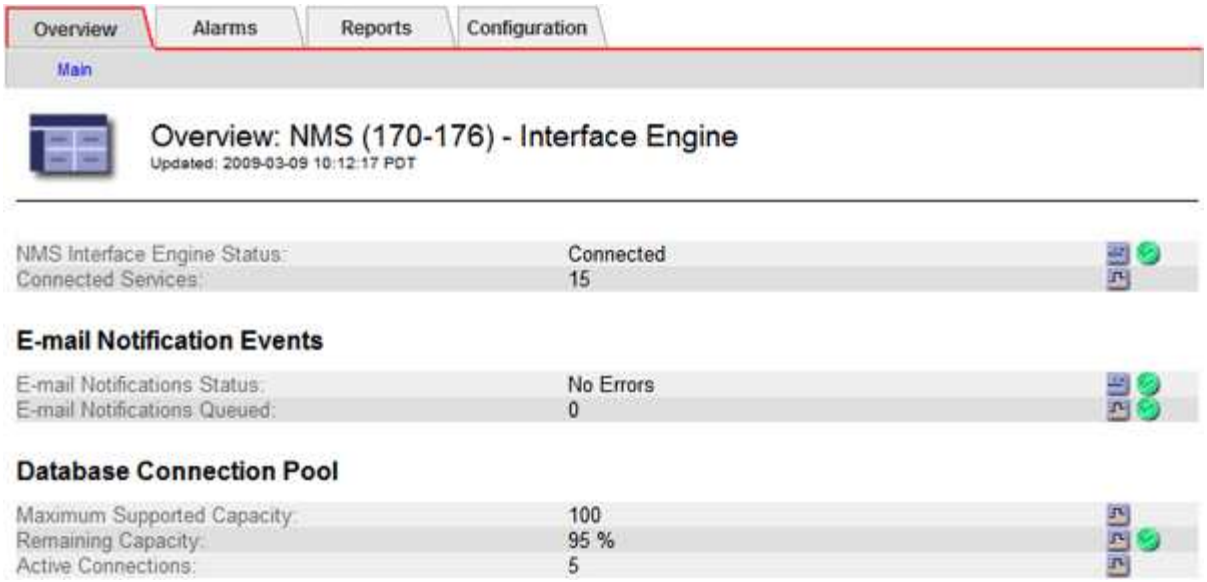
4. [変更の適用 *] をクリックします。

   管理ノードが通知の優先送信者として設定されます。

通知のステータスとキューの表示

管理ノードの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。

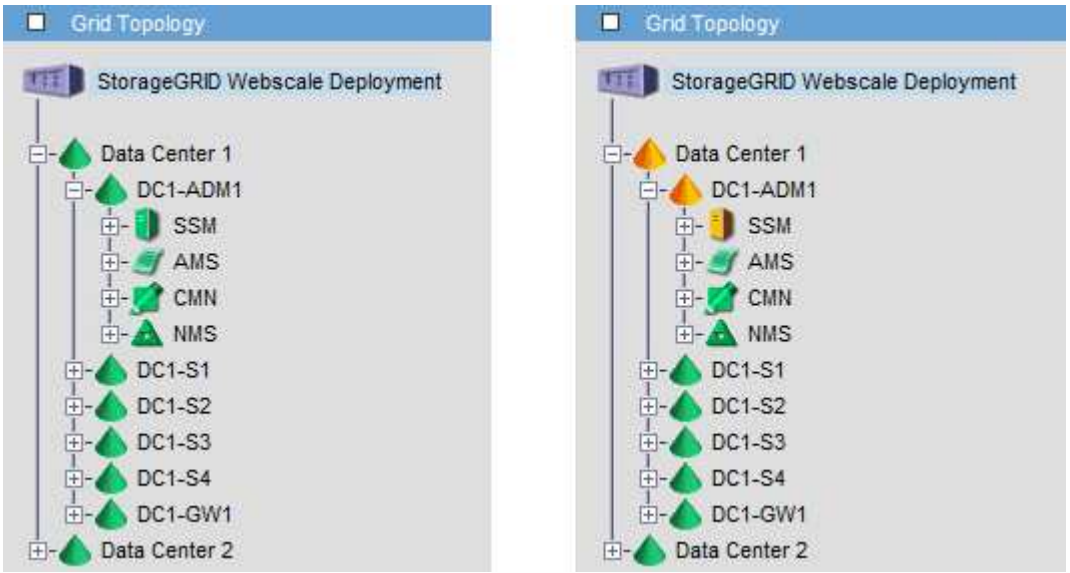


通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューから破棄された場合は、 MINS （ E メール通知ステータス） Minor アラームがトリガーされます。

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、グリッドトポロジツリーでは各管理ノードで同じように表示されない場合があります。

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ています

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。監査ログへのアクセスを簡単にするためには、 CIFS と NFS の両方についてクライアントから監査共有へのアクセスを設定します。

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、監査メッセージを確認する手順を参照してください。

CIFS または NFS を使用するオプションがある場合は、 nfs を選択します。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"管理ノードとは"

"監査ログを確認します"

"ソフトウェアをアップグレードする"

CIFSの監査クライアントを設定しています

監査クライアントの設定に使用する手順 は、認証方式 (Windows ワークグループまたは Windows Active Directory) によって異なります。追加した監査共有は、読み取り専用の共有として自動的に有効になります。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"ソフトウェアをアップグレードする"

ワークグループの監査クライアントの設定

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。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。

- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

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。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、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、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `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. Windows ワークグループの認証を設定します。

   認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

   a. 入力するコマンド `set-authentication`
   b. WindowsワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のように入力します。 `workgroup`

c. プロンプトが表示されたら、ワークグループの名前を入力します。 *workgroup_name*

d. プロンプトが表示されたら、わかりやすいNetBIOS名を設定します。 *netbios_name*

または

Enter * キーを押して管理ノードのホスト名を NetBIOS 名として使用します。

スクリプトによって Samba サーバが再起動され、変更が適用されます。この処理にかかる時間は 1 分未満です。認証を設定したら、監査クライアントを追加します。

a. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

6. 監査クライアントを追加します。

a. 入力するコマンド `add-audit-share`

共有は読み取り専用として自動的に追加されます。

b. プロンプトが表示されたら、ユーザまたはグループを追加します。 *user*

c. プロンプトが表示されたら、監査ユーザ名を入力します。 *audit_user_name*

d. プロンプトが表示されたら、監査ユーザのパスワードを入力します。 *password*

e. プロンプトが表示されたら、確認のためにもう一度同じパスワードを入力します。 *password*

f. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

ディレクトリを入力する必要はありません。監査ディレクトリ名は事前に定義されています。

7. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。

a. 入力するコマンド `add-user-to-share`

有効な共有に番号が振られ、リストに表示されます。

b. プロンプトが表示されたら、監査エクスポート共有の番号を入力します。 *share_number*

c. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user`

または `group`

d. プロンプトが表示されたら、監査ユーザまたはグループの名前を入力します。 *audit_user or audit_group*

e. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

f. 監査共有に追加するユーザまたはグループごとに、上記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。次のメッセージは無視してかまいません。

   ```
   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. プロンプトが表示されたら、 * Enter * を押します。

      監査クライアント設定が表示されます。

   b. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

9. CIFS設定ユーティリティを閉じます。 `exit`
10. Sambaサービスを開始します。 `service smbd start`
11. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

    または

    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、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`
12. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

Active Directoryの監査クライアントを設定しています

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。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- CIFS Active Directoryのユーザ名とパスワードが必要です。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

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。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、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、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `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. Active Directoryの認証を設定します。 `set-authentication`

   ほとんどの環境では、監査クライアントを追加する前に認証を設定する必要があります。認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

   a. ワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のよう `ad`

   b. プロンプトが表示されたら、 AD ドメインの名前（短いドメイン名）を入力します。

   c. プロンプトが表示されたら、ドメインコントローラの IP アドレスまたは DNS ホスト名を入力します。

   d. プロンプトが表示されたら、完全なドメインレルム名を入力します。

      大文字を使用します。

   e. winbind サポートの有効化を求めるプロンプトが表示されたら、「 * y * 」と入力します。

      Winbind は AD サーバのユーザおよびグループの情報を解決するために使用されます。

   f. プロンプトが表示されたら、 NetBIOS 名を入力します。

   g. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

6. ドメインに参加します。

   a. CIFS設定ユーティリティが起動していない場合は、起動します。 `config_cifs.rb`

   b. ドメインに参加します。 `join-domain`

   c. 管理ノードが現在ドメインの有効なメンバーかどうかテストするよう求めるプロンプトが表示されます。この管理ノードがドメインに参加していない場合は、次のように入力します。 `no`

   d. プロンプトが表示されたら、管理者のユーザ名を指定します。 *`administrator_username`*

      ここで、 *`administrator_username`* は、StorageGRID ユーザ名ではなく、CIFS Active Directoryのユーザ名です。

   e. プロンプトが表示されたら、管理者のパスワードを入力します。 *`administrator_password`*

      はい *`administrator_password`* は、StorageGRID パスワードではなく、CIFS Active Directoryのユーザ名です。

   f. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

7. ドメインに参加したことを確認します。

   a. ドメインに参加します。 `join-domain`

   b. サーバが現在ドメインの有効なメンバーかどうかをテストするよう求められたら、次のように入力します。 `y`

「 Join is OK 」というメッセージが表示される場合は、ドメインに正常に参加しています。このメッセージが表示されない場合は、もう一度認証を設定してドメインに参加してください。

c. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

8. 監査クライアントを追加します。 `add-audit-share`

a. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `user`

b. 監査ユーザ名の入力を求めるプロンプトが表示されたら、監査ユーザ名を入力します。

c. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

9. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。 `add-user-to-share`

有効な共有に番号が振られ、リストに表示されます。

a. 監査エクスポート共有の数を入力します。

b. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `group`

監査グループ名の入力を求められます。

c. 監査グループ名を求めるプロンプトが表示されたら、監査ユーザグループの名前を入力します。

d. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

e. 監査共有に追加するユーザまたはグループごとに、この手順を繰り返します。

10. 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。次のメッセージは無視してかまいません。

- インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
- インクルードファイルが見つかりません `/etc/samba/includes/cifs-filesystem.inc`
- インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
- インクルードファイルが見つかりません `/etc/samba/includes/cifs-custom-config.inc`
- インクルードファイルが見つかりません `/etc/samba/includes/cifs-shares.inc`
- RLIMIT_max ： rlimit_max （ 1024 ）を Windows の最小制限（ 16384 ）に増やす

「 security=ads 」と「 password server 」パラメータは同時に指定しないでください（ Samba は、接続する正しい DC を自動的に検出します）。

i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。

ii. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

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

または

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. 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`

13. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

CIFS監査共有へのユーザまたはグループの追加

AD 認証と統合されている CIFS 監査共有にユーザまたはグループを追加できます。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

次の手順 は、 AD 認証と統合されている監査共有用です。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

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`

すべてのサービスが「 Running 」または「 Verified 」でない場合は、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、 * Ctrl * + * C * を押します。

4. CIFS設定ユーティリティを起動します。 `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. ユーザまたはグループの追加を開始します。 `add-user-to-share`

設定済みの監査共有に番号が振られ、リストに表示されます。

6. プロンプトが表示されたら、監査共有（audit-export）の番号を入力します。 *`audit_share_number`*

この監査共有へのアクセスをユーザまたはグループに許可するかどうかの確認を求められます。

7. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user` または `group`

8. プロンプトが表示されたら、この AD 監査共有のユーザまたはグループ名を入力します。

サーバのオペレーティングシステムと CIFS サービスの両方で、ユーザまたはグループが読み取り専用として監査共有に追加されます。Samba 設定がリロードされ、ユーザまたはグループが監査クライアント共有にアクセスできるようになります。

9. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

10. 監査共有に追加するユーザまたはグループごとに、上記の手順を繰り返します。

11. 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。次のメッセージは無視してかまいません。

- include ファイル /etc/samba/include/cifs-interfaces.in が見つかりません
- include ファイル /etc/samba/include/cifs-filesystem.in が見つかりません
- include ファイル /etc/samba/include/cifs-custom-config.in が見つかりません
- include ファイル /etc/samba/include/cifs-shares.in が見つかりません

i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。

ii. プロンプトが表示されたら、 * Enter * を押します。

12. CIFS設定ユーティリティを閉じます。 `exit`
13. 次の状況に応じて、追加の監査共有を有効にする必要があるかどうかを判断します。
    - 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、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。 `exit`
14. コマンドシェルからログアウトします。 `exit`

CIFS監査共有からのユーザまたはグループの削除

監査共有にアクセス可能な最後のユーザまたはグループを削除することはできません。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

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. CIFS設定ユーティリティを起動します。 `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. ユーザまたはグループの削除を開始します。 `remove-user-from-share`

管理ノードで使用可能な監査共有に番号が振られ、リストに表示されます。監査共有には「 audit-export 」というラベルが付けられています。

4. 監査共有の番号を入力します。 *`audit_share_number`*

5. ユーザまたはグループの削除を求めるプロンプトが表示されたら、次のように入力します `user` または `group`

監査共有のユーザまたはグループに番号が振られ、リストに表示されます。

6. 削除するユーザまたはグループに対応する番号を入力します。 *`number`*

監査共有が更新され、ユーザまたはグループは監査共有にアクセスできなくなります。例：

```
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. CIFS設定ユーティリティを閉じます。 `exit`
8. 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、必要に応じて各サイトで監査共有を無効にします。
9. 設定が完了したら、各コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

CIFS監査共有のユーザ名またはグループ名を変更する

CIFS 監査共有のユーザまたはグループの名前を変更するには、新しいユーザまたはグループを追加してから古いユーザまたはグループを削除します。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. 名前を更新した新しいユーザまたはグループを監査共有に追加します。
2. 古いユーザ名またはグループ名を削除します。

関連情報

"ソフトウェアをアップグレードする"

"CIFS監査共有へのユーザまたはグループの追加"

"CIFS監査共有からのユーザまたはグループの削除"

CIFS監査の統合の検証

監査共有は読み取り専用です。ログファイルはコンピュータアプリケーションによって読み取られることを目的としていますが、ファイルを開けるかどうかは検証の対象に含

まれていません。Windows のエクスプローラウィンドウに監査ログファイルが表示されれば、検証は十分とみなされます。接続を検証したら、すべてのウィンドウを閉じます。

NFSの監査クライアントの設定

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。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootまたはadminのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

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 」で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。

監査共有への**NFS**監査クライアントの追加

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。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

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. 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監査の統合の検証

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。

監査共有からの**NFS**監査クライアントの削除

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。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

監査共有にアクセス可能な最後の IP アドレスを削除することはできません。

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**アドレスの変更

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

"監査共有へのNFS監査クライアントの追加"

"監査共有からのNFS監査クライアントの削除"

著作権に関する情報

商標に関する情報