



管理ノードを管理する

StorageGRID

NetApp
October 03, 2025

目次

管理ノードを管理する	1
管理ノードとは	1
AMS サービスとは	1
CMN サービスとは	1
NMS サービスとは	1
Prometheus サービスとは	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
優先送信者を選択します	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	6
CIFS の監査クライアントを設定します	6
NFS の監査クライアントを設定します	17

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。

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。を参照してください [グリッド管理 API を使用します](#)。

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。

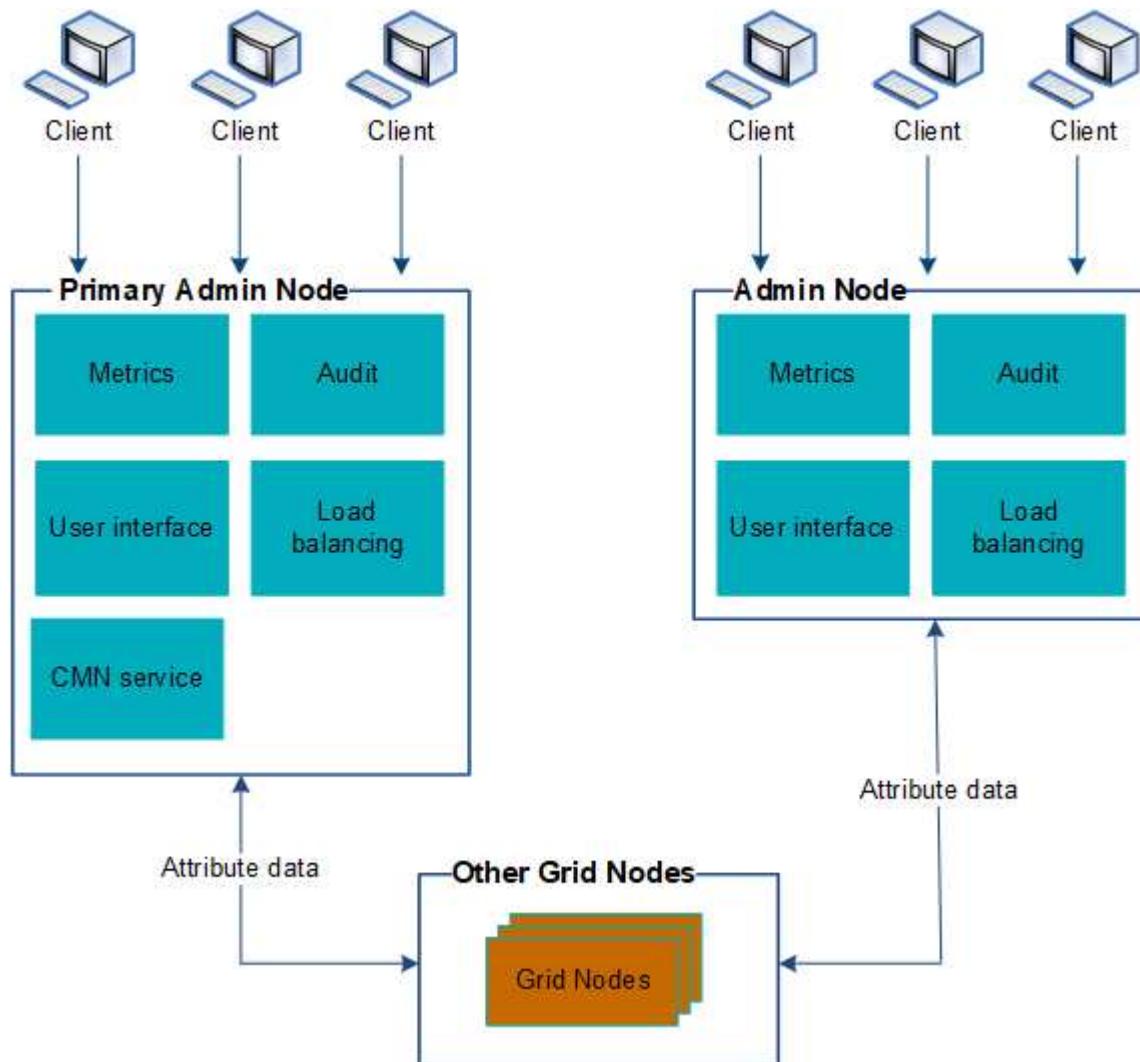
Prometheus サービスとは

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。

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、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。

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。

必要なもの

- 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開き、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

- 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。

このタスクについて

設定 * > * System * > * Display options * ページには、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できます。

- 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

- * 設定 * > * システム * > * 表示オプション * を選択します。
- [表示オプション] メニューから、[* オプション *] を選択します。
- 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。

The screenshot shows the 'Display Options' configuration page. At the top, it says 'Display Options' and 'Updated: 2017-08-30 16:31:10 MDT'. Below that, there's a 'Current Sender' field showing 'ADMIN-DC1-ADM1'. The 'Preferred Sender' dropdown is also set to 'ADMIN-DC1-ADM1'. Under 'GUI Inactivity Timeout', the value is '900'. There's a checkbox for 'Notification Suppress All' which is unchecked. At the bottom right, there's a blue 'Apply Changes' button with a right-pointing arrow.

- 「* 変更を適用する *」を選択します。

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。



Overview: NMS (170-176) - Interface Engine

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

NMS Interface Engine Status:
Connected Services:

Connected
15



E-mail Notification Events

E-mail Notifications Status:
E-mail Notifications Queued:

No Errors
0



Database Connection Pool

Maximum Supported Capacity
Remaining Capacity:
Active Connections:

100
95 %
5

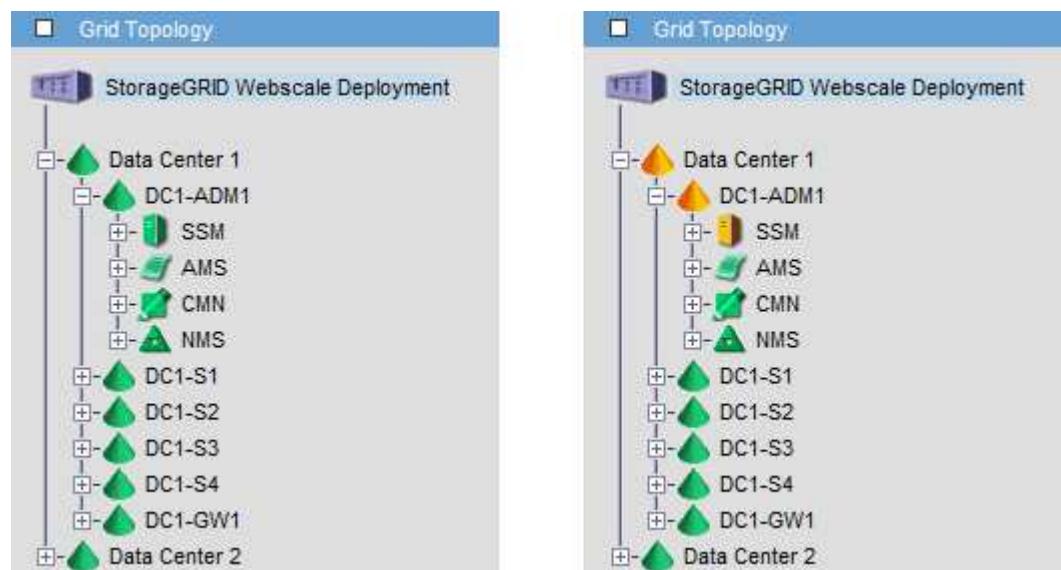


通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューから破棄された場合は、MINS（E メール通知ステータス） Minor アラームがトリガーされます。

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、を参照してください [監査ログを確認します。](#)



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。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 の監査クライアントを設定します

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。

ワークグループの監査クライアントを設定します

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

- root/admin アカウントのパスワードを持つ「 passwords.txt 」ファイルがあります（ SAID パッケージ内にあります）。
- 「 Configuration.txt 」ファイルがあります（ 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. 「 passwords.txt 」ファイルに記載されたパスワードを入力します。

- c. root に切り替えるには、次のコマンドを入力します
- d. 「passwords.txt」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$」から「#」に変わります。

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. 「set-authentication」と入力します
- 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、「workgroup」と入力します
- c. プロンプトが表示されたら 'Workgroup' の名前を入力します :`workgroup_name`
- d. プロンプトが表示されたら '意味のある NetBIOS 名を作成します :`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. 「add-audit-share」と入力します



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「ユーザーまたはグループを追加します
- c. プロンプトが表示されたら「監査ユーザー名として'audit_user_name'を入力します
- d. プロンプトが表示されたら「監査ユーザーのパスワードとして'password'を入力します
- e. プロンプトが表示されたら「確認のために同じパスワードを再入力します
- 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。



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. 「add-user—to-share」と入力します

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として'share_number'を入力します
- c. プロンプトが表示されたら、ユーザまたはグループ「user」を追加します
- 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として'audit_user'または'audit_group'を入力します
- 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. オプションで、構成を確認します。「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
10. Samba サービス 「service smbd start」 を開始します
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_name
 - ii. 「passwords.txt」 ファイルに記載されたパスワードを入力します。
 - iii. root に切り替えるには、次のコマンドを入力します
 - iv. 「passwords.txt」 ファイルに記載されたパスワードを入力します。
 - 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

Active Directory の監査クライアントを設定します

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

- root/admin アカウントのパスワードを持つ「passwords.txt」 ファイルがあります（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。
- 「Configuration.txt」 ファイルがあります（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. 「passwords.txt」 ファイルに記載されたパスワードを入力します。

- c. root に切り替えるには、次のコマンドを入力します
- d. 「passwords.txt」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$`」から「#」に変わります。

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: 'set-authentication' の認証を設定します

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 'ad' と入力します
- 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。

- まだ起動していない場合は、 CIFS 設定ユーティリティを起動します
- ドメイン「join-domain」に参加します
- 管理ノード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、「no」と入力します
- プロンプトが表示されたら '管理者のユーザー名として `administrator_username`' を入力します

ここで '`administrator_username`' は StorageGRID ユーザー名ではなく CIFS Active Directory ユーザー名です

- プロンプトが表示されたら '管理者のパスワードとして `administrator_password`' を入力します

は StorageGRID パスワードではなく '`administrator_password`' は CIFS Active Directory のユーザー名です

- 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。

- ドメイン「join-domain」に参加します
- サーバが現在ドメインの有効なメンバーであるかどうかをテストするプロンプトが表示されたら、「y」と入力します

「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。

- 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 :addaudit-share

- 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、「user」と入力します
- 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。
- 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、「add-user-to-share」というユーザを追加します

有効な共有に番号が振られ、リストに表示されます。

- 監査エクスポート共有の数を入力します。
- 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、「group」と入力します

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. オプションで、構成を確認します。「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 /etc/samba/include/cifs-interfaces.inc` が見つかりません
- インクルード・ファイル /etc/samba/include/cifs-filesystem.inc` が見つかりません
- インクルード・ファイル /etc/samba/include/cifs-interfaces.inc` が見つかりません
- インクルード・ファイル /etc/samba/include/cifs-custom-config.inc` が見つかりません
- インクルード・ファイル /etc/samba/include/cifs-shares.inc` が見つかりません
- 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

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_name
 - ii. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - iii. root に切り替えるには、次のコマンドを入力します
 - iv. 「passwords.txt」ファイルに記載されたパスワードを入力します。
- 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

CIFS 監査共有にユーザまたはグループを追加する

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

- root/admin アカウントのパスワードを持つ「`passwords.txt`」ファイルがあります（SAID パッケージ内にあります）。
- 「`Configuration.txt`」ファイルがあります（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. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。
 - c. `root` に切り替えるには、次のコマンドを入力します
 - d. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。

`root` としてログインすると、プロンプトは「\$」から「#」に変わります。
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`」と入力します
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):`audit_share_number` の番号を入力します 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「user」または「group」を追加します
 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. オプションで、構成を確認します。「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
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 環境が单一サイトの場合は、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_name
 - B. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - C. root に切り替えるには、次のコマンドを入力します
 - D. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - 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 監査共有からユーザまたはグループを削除する

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

- root アカウントのパスワードを含む「passwords.txt」ファイルがあります（SAID パッケージ内にあります）。
- 「Configuration.txt」ファイルがあります（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. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - c. root に切り替えるには、次のコマンドを入力します
 - d. 「passwords.txt」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$`」から「#」に変わります。

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. 監査共有の番号として 'audit_share_number' を入力します
5. ユーザーまたはグループの削除を求めるメッセージが表示されたら、「user」または「group」を選択

します

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

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. 構成が完了したら '各コマンド・シェルからログアウトします :exit'

CIFS 監査共有のユーザ名またはグループ名を変更します

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

- [CIFS 監査共有にユーザまたはグループを追加する](#)
- [CIFS 監査共有からユーザまたはグループを削除する](#)

CIFS 監査の統合を確認

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 のエクスプローラー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を設定します

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。

必要なもの

- root/admin パスワードを持つ「`passwords.txt`」ファイルがあります（SAID パッケージ内にあります）。
- 「`Configuration.txt`」ファイルがあります（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。

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. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。
 - c. root に切り替えるには、次のコマンドを入力します
 - d. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$」から「#」に変わります。
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`」と入力します
「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。 「`config_nfs.rb`」と入力します

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「add-audit-share」を追加します
 - a. プロンプトが表示されたら、監査共有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が監査共有へのアクセスを許可されている場合は、追加ユーザ「add-ip-to-share」の IP アドレスを追加します
 - a. 監査共有の番号として 'audit_share_number' を入力します
 - b. プロンプトが表示されたら、監査共有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
 - 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. 「validate-config」と入力します
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
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_name
 - B. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - C. root に切り替えるには、次のコマンドを入力します
 - D. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - 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。「exit」と入力します
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。

必要なもの

- root/admin アカウントのパスワードを持つ「`passwords.txt`」ファイルがあります（SAID パッケージ内にあります）。
- 「`Configuration.txt`」ファイルがあります（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。

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. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。
 - c. root に切り替えるには、次のコマンドを入力します
 - d. 「`passwords.txt`」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$`」から「#」に変わります。
2. NFS 構成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. 「`add-ip-to-share`」と入力します

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 '`/var/local/audit/export`' として表示されます

4. 監査共有の番号として '`audit_share_number`' を入力します
5. プロンプトが表示されたら、監査共有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
- 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. オプションで、構成を確認します。「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

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_name
- ii. 「passwords.txt」ファイルに記載されたパスワードを入力します。
- iii. root に切り替えるには、次のコマンドを入力します
- iv. 「passwords.txt」ファイルに記載されたパスワードを入力します。

- 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。「ping ip_address」と入力します

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（前のコマンドでは'myAudit'など）

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。「ls myAudit/*」と入力します

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。

必要なもの

- root/admin アカウントのパスワードを持つ「passwords.txt」ファイルがあります（SAID パッケージ内にあります）。
- 「Configuration.txt」ファイルがあります（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. 「passwords.txt」ファイルに記載されたパスワードを入力します。
 - c. root に切り替えるには、次のコマンドを入力します
 - d. 「passwords.txt」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$」から「#」に変わります。

2. NFS 構成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 「remove-ip-from-share」 を削除します

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 '/var/local/audit/export' として表示されます

4. 監査共有に対応する番号として 'audit_share_number' を入力します

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

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_name

ii. 「passwords.txt」ファイルに記載されたパスワードを入力します。

iii. root に切り替えるには、次のコマンドを入力します

iv. 「passwords.txt」ファイルに記載されたパスワードを入力します。

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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。