



# 監査クライアントアクセスを設定します

## StorageGRID 11.7

NetApp  
April 12, 2024

# 目次

監査クライアントアクセスを設定します	1
NFSの監査クライアントアクセスを設定します	1
監査共有に NFS 監査クライアントを追加します	3
NFS 監査の統合を確認	4
監査共有から NFS 監査クライアントを削除します	5
NFS 監査クライアントの IP アドレスを変更します	6

# 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

- 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。
- 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

- 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。
- 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

- 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。
- 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

Copyright © 2024 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随時、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 5252.227-19（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权を有し、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权については、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。