



# iSCSI セットアップ

## E-Series storage systems

NetApp  
January 20, 2026

# 目次

iSCSI セットアップ .....	1
Eシリーズ (iSCSI) でのLinux構成のサポートの確認 .....	1
Eシリーズ- LinuxでのDHCPを使用したIPアドレスの設定 (iSCSI) .....	1
SANtricity Storage Manager for SMcliのインストール (11.53以前) - Linux (iSCSI) .....	2
SANtricity System Managerを使用したストレージの設定- Linux (iSCSI) .....	3
Eシリーズでのマルチパスソフトウェアの設定 (iSCSI) .....	5
Eシリーズ- Linux (iSCSI) でのmultipath.confファイルの設定 .....	6
Eシリーズでのスイッチの設定- Linux (iSCSI) .....	6
Eシリーズ- Linuxでのネットワークの設定 (iSCSI) .....	7
Eシリーズ- Linuxでのアレイ側のネットワークの設定 (iSCSI) .....	7
Eシリーズ- Linuxでのホスト側のネットワークの設定 (iSCSI) .....	10
Eシリーズ- Linux (iSCSI) でのIPネットワーク接続の確認 .....	14
Eシリーズでのパーティションとファイルシステムの作成 (iSCSI) .....	15
Eシリーズ- Linux (iSCSI) のホストでのストレージアクセスの確認 .....	17
Eシリーズ- LinuxでのiSCSI構成の記録 .....	17
推奨される構成 .....	17
ターゲット IQN .....	18
マッピングホスト名 .....	18

# iSCSI セットアップ

## Eシリーズ（iSCSI）でのLinux構成のサポートの確認

安定した稼働を確保するために、導入計画を作成し、NetApp Interoperability Matrix Tool（IMT）を使用して構成全体がサポートされることを確認します。

### 手順

1. にアクセスします ["NetApp Interoperability Matrix Tool で確認できます"](#)。
2. [ 検索（解決策 Search） ] タイルをクリックします。
3. [Protocols [SAN Host]（プロトコル [SAN ホスト]）領域で、\* E シリーズ SAN ホスト \* の横の \* 追加ボタンをクリックします。
4. [ \* 検索条件の絞り込み検索の表示 \* ] をクリックします。

[ 検索条件の絞り込み ] セクションが表示されます。このセクションでは、適用するプロトコル、およびオペレーティングシステム、ネットアップ OS、ホストマルチパスドライバなど、構成のその他の条件を選択できます。

5. 構成に必要な条件を選択し、互換性のある構成要素を確認します。
6. 必要に応じて、使用するオペレーティングシステムとプロトコルに対して IMT に記載された更新を実行します。

選択した構成の詳細情報には、右ページ矢印をクリックして、[View Supported Configurations] ページからアクセスできます。

## Eシリーズ- LinuxでのDHCPを使用したIPアドレスの設定（iSCSI）

管理ステーションとストレージアレイ間の通信を設定するには、動的ホスト構成プロトコル（DHCP）を使用して IP アドレスを指定します。

作業を開始する前に

次のものがあることを確認します。

- ストレージ管理ポートと同じサブネットに DHCP サーバをインストールして設定します。

このタスクについて

各ストレージアレイにはコントローラが 1 台（シンプレックス）または 2 台（デュプレックス）含まれ、コントローラごとにストレージ管理ポートが 2 つあります。各管理ポートには IP アドレスが割り当てられます。

以下の手順では、コントローラを 2 台搭載したストレージアレイ（デュプレックス構成）を使用します。

### 手順

1. 管理ステーションと各コントローラ（A および B）の管理ポート 1 にイーサネットケーブルを接続しま

す（まだ接続していない場合）。

DHCP サーバは、各コントローラのポート 1 に IP アドレスを割り当てます。



どちらのコントローラの管理ポート 2 も使用しないでください。ポート 2 はネットアップのテクニカルサポート用に予約されています。



イーサネットケーブルを外して再接続するか、ストレージアレイの電源を再投入すると、DHCP によって IP アドレスが再度割り当てられます。このプロセスは、静的 IP アドレスが設定されるまで行われます。ケーブルを外したり、アレイの電源を再投入したりしないことを推奨します。

DHCP によって割り当てられた IP アドレスをストレージアレイが 30 秒以内に取得できない場合は、次のデフォルトの IP アドレスが設定されます。

- コントローラ A、ポート 1 : 169.254.128.101
- コントローラ B、ポート 1 : 169.254.128.102
- サブネットマスク : 255.255.0.0

2. 各コントローラの背面にある MAC アドレスラベルを確認し、ネットワーク管理者に各コントローラのポート 1 の MAC アドレスを伝えます。

MAC アドレスは、ネットワーク管理者が各コントローラの IP アドレスを特定するために必要です。ブラウザからストレージシステムに接続するには、IP アドレスが必要です。

## SANtricity Storage Manager for SMcliのインストール（11.53 以前） - Linux（iSCSI）

SANtricity ソフトウェア 11.53 以前を使用している場合は、管理ステーションに SANtricity Storage Manager ソフトウェアをインストールして、アレイの管理に役立てることができます。

SANtricity Storage Manager には、管理タスクを実行するためのコマンドラインインターフェイス（CLI）と、I/O パスを介してストレージアレイコントローラにホスト構成情報をプッシュするためのホストコンテキストエージェントがあります。



SANtricity ソフトウェア 11.60 以降を使用している場合は、次の手順は実行する必要はありません。SANtricity Secure CLI（SMcli）は SANtricity OS に含まれており、SANtricity System Manager からダウンロードできます。SANtricity システムマネージャから SMcli をダウンロードする方法の詳細については、["SANtricity System Manager オンラインヘルプのコマンドラインインターフェイス（CLI）のダウンロードのトピック"](#)



SANtricity ソフトウェアバージョン 11.80.1 以降では、ホストコンテキストエージェントはサポートされなくなりました。

作業を開始する前に

次のものがあることを確認します。

- SANtricity ソフトウェア 11.53 以前。
- 適切な管理者権限またはスーパーユーザ権限
- SANtricity Storage Manager クライアント用のシステム。次の最小要件があります。
  - **RAM:** Java Runtime Engine 用に 2GB
  - \* ディスク容量 \* : 5GB
  - \* OS / アーキテクチャ \* : サポートされているオペレーティング・システムのバージョンとアーキテクチャーを判断するためのガイダンスについては、を参照してください ["ネットアップサポート"](#)
    - Downloads \* タブで、ダウンロード [E-Series SANtricity Storage Manager] に移動します。

#### このタスクについて

このタスクでは、Windows と Linux の両方の OS プラットフォームに SANtricity Storage Manager をインストールする方法について説明します。データホストに Linux を使用する場合の管理ステーションプラットフォームは Windows と Linux の両方で共通です。

#### 手順

1. SANtricity ソフトウェアリリースは、からダウンロードします ["ネットアップサポート"](#)。Downloads \* タブで、ダウンロード [E-Series SANtricity Storage Manager] に移動します。
2. SANtricity インストーラを実行します。

Windows の場合	Linux の場合
SMIA*.exe インストールパッケージをダブルクリックして、インストールを開始します。	a. SMIA * 。 bin インストールパッケージが格納されているディレクトリに移動します。 b. 一時マウントポイントに実行権限がない場合は 'IATEMPDIR' 変数を設定します例： 'IATEMPDIR=/root./SMIA-LINUX64-11.25.0A0002.bin' c. chmod +x SMIA*.bin コマンドを実行して、ファイルに実行権限を付与します。 d. 「./SMIA *.bin」 コマンドを実行してインストーラを起動します。

3. インストールウィザードを使用して、管理ステーションにソフトウェアをインストールします。

## SANtricity System Managerを使用したストレージの設定-Linux (iSCSI)

ストレージアレイを設定するには、SANtricity System Manager のセットアップウィザードを使用します。

SANtricity System Manager は、各コントローラに組み込まれている Web ベースのインターフェイスです。ユーザーインターフェイスにアクセスするには、ブラウザでコントローラの IP アドレスを指定します。セットアップウィザードを使用してシステムを設定できます。

作業を開始する前に

次のものがあることを確認します。

- アウトオブバンド管理：
- 次のいずれかのブラウザを使用して SANtricity System Manager にアクセスするための管理ステーション。

ブラウザ	最小バージョン
Google Chrome	八九
Microsoft Edge の場合	90
Mozilla Firefox	88
Safari	14

このタスクについて

iSCSI を使用している場合は、iSCSI を設定する際にセットアップウィザードを閉じています。

ウィザードは、System Manager を開くかブラウザを更新したときに、次の条件の少なくとも 1 つに該当していれば自動的に再度起動されます。

- プールとボリュームグループが検出されていません。
- ワークロードが検出されていません。
- 通知が設定されていません。

手順

1. ブラウザで、「+ <https://<DomainNameOrIPAddress>+>」という URL を入力します

「IPAddress」は、ストレージアレイコントローラの 1 つのアドレスです。

設定されていないアレイで初めて SANtricity システムマネージャを開くと、管理者パスワードの設定プロンプトが表示されます。ロールベースアクセス管理では、admin、support、security、monitor の 4 つのローカルロールが設定されます。最後の 3 つのロールには、推測されにくいランダムなパスワードが設定されています。admin ロールのパスワードを設定したら、admin クレデンシャルを使用してすべてのパスワードを変更できます。4 つのローカルユーザロールの詳細については、SANtricity System Manager ユーザーインターフェイスのオンラインヘルプを参照してください。

2. 管理者パスワードの設定フィールドとパスワードの確認フィールドに管理者ロールの System Manager パスワードを入力し、\* パスワードの設定 \* をクリックします。

プール、ボリュームグループ、ワークロード、または通知が設定されていない場合は、セットアップウィザードが起動します。

3. セットアップウィザードを使用して、次のタスクを実行します。

- \* ハードウェア（コントローラとドライブ）の確認 \* — ストレージアレイ内のコントローラとドライブの数を確認しますアレイに名前を割り当てます。

- \* ホストとオペレーティング・システムの確認 \* — ストレージ・アレイがアクセスできるホストとオペレーティング・システムの種類を確認します
  - \* Accept pools \* — 高速インストール方法の推奨されるプール構成を受け入れますプールはドライブの論理グループです。
  - \* アラートの設定 \* — ストレージアレイで問題が発生した場合に、System Manager が自動通知を受信できるようにします。
  - \* AutoSupport を有効にする \* — ストレージアレイの状態を自動的に監視し、テクニカルサポートにデイスパッチを送信します。
4. ボリュームをまだ作成していない場合は、メニューからストレージ [ ボリューム ]、[ 作成 ]、[ ボリューム ] の順に選択してボリュームを作成します。

詳細については、SANtricity System Manager のオンラインヘルプを参照してください。

## Eシリーズでのマルチパスソフトウェアの設定 (iSCSI)

ストレージアレイへのパスを冗長化するには、マルチパスソフトウェアを設定します。

作業を開始する前に

必要なパッケージをシステムにインストールする必要があります。

- Red Hat (RHEL) ホストの場合、パッケージがインストールされていることを確認するには、「rpm -q device-mapper-multipath」を実行します。
- SLES ホストの場合 'rpm -q multipath-tools' を実行してパッケージがインストールされていることを確認します

オペレーティングシステムがまだインストールされていない場合は、オペレーティングシステムのベンダーから提供されたメディアを使用してください。

このタスクについて

マルチパスソフトウェアは、物理パスの 1 つが中断された場合に備えて、ストレージアレイへのパスを冗長化します。マルチパスソフトウェアは、ストレージへのアクティブな物理パスを 1 つの仮想デバイスとしてオペレーティングシステムに提示します。また、フェイルオーバープロセスも管理して仮想デバイスを更新します。

Linux 環境では、Device Mapper Multipath (DM-MP) ツールを使用します。RHEL および SLES では、デフォルトでは DM-MP は無効になっています。ホストで DM-MP コンポーネントを有効にするには、次の手順を実行します。

手順

1. multipath.conf ファイルがまだ作成されていない場合は、「# touch /etc/multipath.conf」コマンドを実行します。
2. multipath.conf ファイルを空白のままにして、デフォルトのマルチパス設定を使用します。
3. マルチパスサービスを開始します。

```
# systemctl start multipathd
```

4. `uname -r` コマンドを実行して 'カーネル・バージョン' を保存します

```
# uname -r
3.10.0-327.el7.x86_64
```

この情報は、ホストにボリュームを割り当てるときに使用します。

5. を有効にします `multipathd` デーモンが起動します。

```
systemctl enable multipathd
```

6. `initramfs` イメージまたは `initrd` イメージを `/boot` ディレクトリに再構築します

```
dracut --force --add multipath
```

7. を使用します ["ホストを手動で作成する"](#) ホストが定義されているかどうかを確認するには、オンラインヘルプの手順を参照してください。各ホストタイプの設定が、で収集したカーネル情報に基づいていることを確認します [手順4.](#)



自動ロードバランシングは、カーネル3.9以前を実行しているホストにマップされているボリュームでは無効になります。

8. ホストをリブートします。

## Eシリーズ- Linux (iSCSI) でのmultipath.confファイルの設定

`multipath.conf` ファイルは、マルチパスデーモン `multipathd` の構成ファイルです。

`multipath.conf` ファイルは、`multipathd` の組み込みの構成テーブルよりも優先されます。



SANtricity OS 8.30 以降では、デフォルト設定をそのまま使用することを推奨します。

`/etc/multipath.conf` を変更する必要はありません。

## Eシリーズでのスイッチの設定- Linux (iSCSI)

iSCSI に関するベンダーの推奨事項に従ってスイッチを設定します。これらの推奨事項には、設定の指示とコードの更新が含まれる場合があります。

次の点を確認する必要があります。

- 高可用性を実現するために 2 つのネットワークを用意しておきます。iSCSI トラフィックを別々のネットワークセグメントに分離してください。



- フロー制御 \* エンドツーエンド \* を有効にする必要があります。
- 必要に応じて、ジャンボフレームを有効にしておきます。



コントローラのスイッチポートでは、ポートチャネル / LACP がサポートされません。ホスト側 LACP は推奨されません。マルチパスを使用すると、同等のメリットが得られますが、場合によってはより優れたメリットも得られます。

## Eシリーズ- Linuxでのネットワークの設定 (iSCSI)

iSCSI ネットワークは、データストレージの要件に応じて、さまざまな方法でセットアップできます。

環境に最適な構成を選択するには、ネットワーク管理者に相談してください。

iSCSI ネットワークに基本的な冗長性を設定するには、各ホストポートと各コントローラの 1 つのポートを別々のスイッチに接続し、ホストポートとコントローラポートの各セットを別々のネットワークセグメントまたは VLAN にパーティショニングします。

送受信ハードウェアフロー制御 \* エンドツーエンド \* を有効にする必要があります。優先度フロー制御は無効にする必要があります。

パフォーマンス上の理由から IP SAN 内でジャンボフレームを使用している場合は、アレイ、スイッチ、およびホストでジャンボフレームを使用するように設定してください。ホストおよびスイッチでジャンボフレームを有効にする方法については、使用するオペレーティングシステムとスイッチのドキュメントを参照してください。アレイでジャンボフレームを有効にするには、の手順を実行します ["アレイ側のネットワークを設定"](#)。



多くのネットワークスイッチは 9,000 バイトを超える IP オーバーヘッドを設定する必要があります。詳細については、スイッチのマニュアルを参照してください。

## Eシリーズ- Linuxでのアレイ側のネットワークの設定 (iSCSI)

SANtricity System Manager の GUI を使用して、アレイ側の iSCSI ネットワークを設定します。

作業を開始する前に

次のものがあることを確認します。

- いずれかのストレージアレイコントローラの IP アドレスまたはドメイン名。
- System Manager GUI、ロールベースアクセス制御 (RBAC)、または LDAP のパスワード、およびストレージアレイへの適切なセキュリティアクセスのために設定されたディレクトリサービス。アクセス管理の詳細については、SANtricity システムマネージャオンラインヘルプを参照してください。

このタスクについて

このタスクでは、System Manager のハードウェアページから iSCSI ポートの設定にアクセスする方法について説明します。設定には、System (設定) > Configure iSCSI Ports (iSCSI ポートの設定) メニューからもアクセスできます。

手順

1. ブラウザで、「+ <https://<DomainNameOrIPAddress>+`>」という URL を入力します

「IPAddress」は、ストレージアレイコントローラの 1 つのアドレスです。

設定されていないアレイで初めて SANtricity システムマネージャを開くと、管理者パスワードの設定プロンプトが表示されます。ロールベースアクセス管理では、admin、support、security、monitor の 4 つのローカルロールが設定されます。最後の 3 つのロールには、推測されにくいランダムなパスワードが設定されています。admin ロールのパスワードを設定したら、admin クレデンシャルを使用してすべてのパスワードを変更できます。4 つのローカルユーザロールの詳細については、SANtricity System Manager ユーザーインターフェイスのオンラインヘルプを参照してください。

2. 管理者パスワードの設定フィールドとパスワードの確認フィールドに管理者ロールの System Manager パスワードを入力し、\*パスワードの設定\*をクリックします。

プール、ボリュームグループ、ワークロード、または通知が設定されていない場合は、セットアップウィザードが起動します。

3. セットアップウィザードを閉じます。

このウィザードは、あとで追加のセットアップタスクを実行する際に使用します。

4. 「\*ハードウェア\*」を選択します。

5. 図にドライブが表示されている場合は、\*シェルフの背面を表示\*をクリックします。

図の表示が切り替わり、ドライブではなくコントローラが表示されます。

6. iSCSI ポートを設定するコントローラをクリックします。

コントローラのコンテキストメニューが表示されます。


7. Configure iSCSI Port\*（iSCSI ポートの設定）を選択します。

Configure iSCSI Ports（iSCSI ポートの設定）ダイアログボックスが開きます。

8. ドロップダウンリストで、設定するポートを選択し、\*Next\*をクリックします。

9. 構成ポートの設定を選択し、\*次へ\*をクリックします。

すべてのポート設定を表示するには、ダイアログボックスの右側にある \*Show more port settings\* リンクをクリックします。

ポートの設定	説明
イーサネットポート速度の設定	<p>目的の速度を選択します。ドロップダウンリストに表示されるオプションは、ネットワークがサポートできる最大速度（10Gbps など）によって異なります。</p> <div data-bbox="873 331 1481 594">  <p>コントローラで使用可能なオプションの 25Gb iSCSI ホストインターフェイスカードは速度を自動ネゴシエートしません。各ポートの速度を 10Gb または 25Gb に設定する必要があります。すべてのポートを同じ速度に設定する必要があります。</p> </div>
IPv4 を有効にする / IPv6 を有効にする	<p>一方または両方のオプションを選択して、IPv4 ネットワークと IPv6 ネットワークのサポートを有効にします。</p>
TCP リスニングポート（[Show more port settings] をクリックすると使用可能）	<p>必要に応じて、新しいポート番号を入力します。</p> <p>リスニングポートは、コントローラがホスト iSCSI イニシエータからの iSCSI ログインをリスンするために使用する TCP ポート番号です。デフォルトのリスニングポートは 3260 です。3260、または 49152~65535 の値を入力する必要があります。</p>
MTU サイズ（* Show more port settings* をクリックすると使用可能）	<p>必要に応じて、Maximum Transmission Unit（MTU；最大伝送ユニット）の新しいサイズをバイト単位で入力します。</p> <p>デフォルトの Maximum Transmission Unit（MTU；最大転送単位）サイズは 1500 バイト / フレームです。1500~9000 の値を入力する必要があります。</p>
ICMP PING 応答を有効にします	<p>Internet Control Message Protocol（ICMP）を有効にする場合は、このオプションを選択します。ネットワーク接続されたコンピュータのオペレーティングシステムは、このプロトコルを使用してメッセージを送信します。ICMP メッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。</p>

[\*IPv4 を有効にする\*] を選択した場合は、[次へ\*] をクリックすると、IPv4 設定を選択するためのダイアログボックスが開きます。[\*IPv6 を有効にする\*] を選択した場合、[次へ\*] をクリックすると、IPv6 設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、IPv4 設定のダイアログボックスが最初に開き、\*次へ\* をクリックすると、IPv6 設定のダイアログボックスが開きます。

10. IPv4 と IPv6 、またはその両方を自動または手動で設定します。すべてのポート設定を表示するには、ダイアログボックスの右側にある \* Show more settings \* リンクをクリックします。

ポートの設定	説明
自動的に設定を取得します	設定を自動的に取得するには、このオプションを選択します。
静的な設定を手動で指定します	このオプションを選択した場合は、フィールドに静的アドレスを入力します。IPv4 の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。IPv6 の場合は、ルーティング可能な IP アドレスとルータの IP アドレスも指定します。

11. [ 完了 ] をクリックします。
12. System Manager を終了します。

## Eシリーズ- Linuxでのホスト側のネットワークの設定 (iSCSI)

ホスト側のネットワークを設定するには、いくつかの手順を実行する必要があります。

このタスクについて

ホスト側の iSCSI ネットワークを設定するには、物理パスあたりのノードセッション数を設定し、適切な iSCSI サービスをオンにし、iSCSI ポートのネットワークを設定し、iSCSI iface バインドを作成し、イニシエータとターゲットの間に iSCSI セッションを確立します。

ほとんどの場合、iSCSI CNA / NIC には標準で実装されているソフトウェアイニシエータを使用できます。最新のドライバ、ファームウェア、BIOS をダウンロードする必要はありません。を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#) コードの要件を確認します。

手順

1. /etc/iscsi/iscsid.conf ファイルの「node.session.nr\_sessions」変数で、物理パスあたりのデフォルトのセッション数を確認します。必要に応じて、デフォルトのセッション数を 1 に変更します。

```
node.session.nr_sessions = 1
```

2. /etc/iscsi/iscsid.conf ファイルの「node.session.timeo.replacement\_timeout」変数をデフォルト値の「120」から「20」に変更します。

```
node.session.timeo.replacement_timeout = 20
```

3. 必要に応じて、を設定できます node.startup = automatic /etc/iscsi/iscsid.confで、を実行する前にします iscsiadm セッションを保持するコマンドはリブート後も維持されます。
4. 'iscsid' および '(open-)iSCSI' サービスがオンであり 'ブートが有効になっていることを確認します

```
# systemctl start iscsi
# systemctl start iscsid
# systemctl enable iscsi
# systemctl enable iscsid
```

5. ホスト IQN イニシエータ名を取得します。この名前は、アレイに対してホストを設定する際に使用します。

```
# cat /etc/iscsi/initiatorname.iscsi
```

6. iSCSIポートのネットワークを設定します。次に、RHELおよびSLESでの手順の例を示します。



iSCSI イニシエータは、パブリックネットワークポートに加えて、別々のプライベートセグメントまたは VLAN 上で 2 つ以上の NIC を使用する必要があります。

- a. `ifconfig -a` コマンドを使用して iSCSI ポート名を確認します
- b. iSCSI イニシエータポートの IP アドレスを設定します。イニシエータポートは、iSCSI ターゲットポートと同じサブネット上にある必要があります。

#### Red Hat Enterprise Linux (RHEL) 8

サンプルファイルを作成します `/etc/sysconfig/network-scripts/ifcfg-<NIC port>` 次のコンテンツを含む。

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=<NIC port>
UUID=<unique UUID>
DEVICE=<NIC port>
ONBOOT=yes
IPADDR=192.168.xxx.xxx
PREFIX=24
NETMASK=255.255.255.0
NM_CONTROLLED=no
MTU=
```

IPv6に関するオプションの追加：

```
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=fdxx::192:168:xxxx:xxxx/32
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=eui64
```

## Red Hat Enterprise Linux 9 および 10 (RHEL 9 および RHEL 10) および SUSE Linux Enterprise Server 16 (SLES 16)

を使用します nmtui 接続を活動化および編集するためのツール。ツールによって生成されます <NIC port>.nmconnection 内のファイル /etc/NetworkManager/system-connections/。

- SUSE Linux Enterprise Server 12 および 15 ( SLES 12 および SLES 15 ) \*

サンプルファイルを作成します /etc/sysconfig/network/ifcfg-<NIC port> 次のコンテンツを含む。

```
IPADDR='192.168.xxx.xxx/24'
BOOTPROTO='static'
STARTMODE='auto'
```

+ IPv6に関するオプションの追加：

```
IPADDR_0='fdxx::192:168:xxxx:xxxx/32'
```

+



必ず両方の iSCSI イニシエータポートのアドレスを設定してください。

- a. ネットワークサービスを再起動します。

```
# systemctl restart network
```

- b. Linux サーバから iSCSI ターゲットポートのすべてに ping を実行できることを確認します。

## 7. イニシエータとターゲットの間にiSCSIセッションを確立します（合計4つ）。確立する方法は2つあります。

- a. （オプション）ifaceを使用する場合は、iSCSI ifaceバインドを2つ作成してiSCSIインターフェイスを設定します。

```
# iscsiadm -m iface -I iface0 -o new
# iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v
<NIC port1>
```

```
# iscsiadm -m iface -I iface1 -o new
# iscsiadm -m iface -I iface1 -o update -n iface.net_ifacename -v
<NIC port2>
```



インタフェースを一覧表示するには 'iscsiadm -m iface' を使用します

- b. iSCSI ターゲットを検出します。次の手順のために、IQN（各検出で同じ）をワークシートに保存します。

#### 方法1（ifaceを使用）

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port> -I iface0
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I iface0
```

#### 方法2（ifaceなし）

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port>
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260
```



IQN は次のような形式です。

```
iqn.1992-01.com.netapp:2365.60080e50001bf1600000000531d7be3
```

- c. iSCSI イニシエータと iSCSI ターゲット間の接続を作成します。

#### 方法1（ifaceを使用）

```
# iscsiadm -m node -T <target_iqn> -p
<target_ip_address>:<target_tcp_listening_port> -I iface0 -l
# iscsiadm -m node -T iqn.1992-
01.com.netapp:2365.60080e50001bf1600000000531d7be3 -p
192.168.0.1:3260 -I iface0 -l
```

#### 方法2（ifaceなし）

```
# iscsiadm -m node -L all
```

- a. ホストで確立されている iSCSI セッションの一覧を表示します。

```
# iscsiadm -m session
```

## Eシリーズ- Linux (iSCSI) でのIPネットワーク接続の確認

インターネットプロトコル (IP) ネットワーク接続を確認するには、ping テストを使用してホストとアレイが通信できることを確認します。

### 手順

1. ジャンボフレームが有効かどうかに応じて、ホストから次のいずれかのコマンドを実行します。

- ジャンボフレームが有効になっていない場合は、次のコマンドを実行します。

```
ping -I <hostIP\> <targetIP\>
```

- ジャンボフレームが有効な場合は、ペイロードサイズに 8、972 バイトを指定して ping コマンドを実行します。IP と ICMP を組み合わせたヘッダーは 28 バイトで、これがペイロードに追加されて 9、000 バイトになります。-s スイッチは 'packet size ビットを設定します' オプションはデバッグオプションを設定します。これらのオプションにより、iSCSI イニシエータとターゲットの間で 9、000 バイトのジャンボフレームを正常に送信できます。

```
ping -I <hostIP\> -s 8972 -d <targetIP\>
```

この例では、iSCSI ターゲットの IP アドレスは「192.0.2.8」です。

```
#ping -I 192.0.2.100 -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. 各ホストのイニシエータ・アドレス (iSCSI に使用されるホスト・イーサネット・ポートの IP アドレス) から各コントローラの iSCSI ポートへの ping コマンド問題構成内の各ホストサーバから、必要に応じ



て IP アドレスを変更してこの操作を実行します。



コマンドが失敗した場合（たとえば、「Packet needs to be fragmented but DF set」が返された場合）は、ホストサーバ、ストレージコントローラ、およびスイッチポートのイーサネットインターフェイスの MTU サイズ（ジャンボフレームのサポート状況）を確認します。

## Eシリーズでのパーティションとファイルシステムの作成 (iSCSI)

Linux ホストで初めて検出された時点では、新しい LUN にはパーティションやファイルシステムがないため、使用する前に LUN をフォーマットする必要があります。必要に応じて、LUN にファイルシステムを作成できます。

作業を開始する前に

次のものがあることを確認します。

- ホストによって検出された LUN。
- 使用可能なディスクのリスト。(利用可能なディスクを表示するには '/dev/mapper フォルダで ls コマンドを実行します)

このタスクについて

ディスクは、GUID パーティションテーブル (GPT) またはマスターブートレコード (MBR) を使用して、ベーシックディスクとして初期化することができます。

LUN は ext4 などのファイルシステムでフォーマットします。一部のアプリケーションではこの手順が不要です。

手順

1. 「anlun lun lun show -p」コマンドを発行して、マッピングされたディスクの SCSI ID を取得します。

SCSI ID は、3 から始まる 33 文字の 16 進数値です。ユーザにわかりやすい名前の使用が有効になっている場合、SCSI ID の代わりに mpath がレポートされます。

```
# sanlun lun show -p

E-Series Array: ictml619s01c01-
SRP(60080e50002908b40000000054efb9d2)
Volume Name:
Preferred Owner: Controller in Slot B
Current Owner: Controller in Slot B
Mode: RDAC (Active/Active)
UTM LUN: None
LUN: 116
LUN Size:
Product: E-Series
Host Device:
mpathr(360080e50004300ac000007575568851d)
Multipath Policy: round-robin 0
Multipath Provider: Native
```

host	controller		host	controller
path	path	/dev/	path	target
state	type	node	adapter	port
up	secondary	sdcx	host14	A1
up	secondary	sdat	host10	A2
up	secondary	sdbv	host13	B1

## 2. Linux OS のリリースに応じた方法で新しいパーティションを作成します。

通常、ディスクのパーティションを識別する文字（数字の 1 や p3 など）が SCSI ID に追加されます。

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

## 3. パーティションにファイルシステムを作成します。

ファイルシステムの作成方法は、選択したファイルシステムによって異なります。

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

## 4. 新しいパーティションをマウントするフォルダを作成します。

```
# mkdir /mnt/ext4
```

5. パーティションをマウントします。

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

## Eシリーズ- Linux (iSCSI) のホストでのストレージアクセスの確認

ボリュームを使用する前に、ホストがボリュームに対してデータの読み取りと書き込みを実行できることを確認します。

作業を開始する前に

次のものがあることを確認します。

- ファイルシステムでフォーマットされた初期化済みボリューム。

手順

1. ホストで、1 つ以上のファイルをディスクのマウントポイントにコピーします。
2. ファイルを元のディスク上の別のフォルダにコピーします。
3. 「IFF」コマンドを実行して、コピーしたファイルを元のファイルと比較します。

完了後

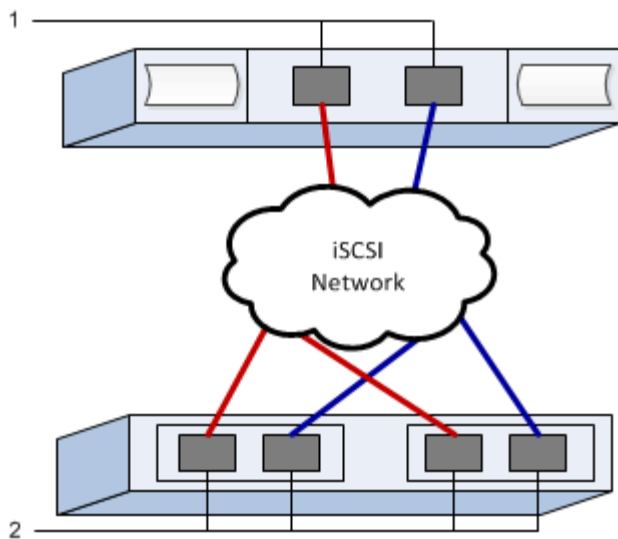
コピーしたファイルとフォルダを削除します。

## Eシリーズ- LinuxでのiSCSI構成の記録

このページの PDF を生成して印刷し、次のワークシートを使用して iSCSI ストレージの構成情報を記録できます。この情報は、プロビジョニングタスクを実行する際に必要になります。

### 推奨される構成

推奨構成は、2 つのイニシエータポートと 4 つのターゲットポートを 1 つ以上の VLAN で接続した構成です。



## ターゲット IQN

番号	ターゲットポート接続	IQN
2.	ターゲットポート	

## マッピングホスト名

番号	ホスト情報	名前とタイプ
1.	マッピングホスト名	
	ホスト OS タイプ	

## 著作権に関する情報

Copyright © 2026 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。