



## システム：iSCSI設定 SANtricity 11.6

NetApp  
February 12, 2024

# 目次

システム：iSCSI設定 .....	1
概念 .....	1
方法 .....	2
よくある質問です .....	12

# システム：iSCSI設定

## 概念

### iSCSIの用語

ストレージアレイに関連するiSCSIの用語を次に示します。

期間	説明
CHAP	チャレンジハンドシェイク認証プロトコル（CHAP）方式では、初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、System Manager の機能を実装します。
DHCP	動的ホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワークでIPアドレスなどのネットワーク設定パラメータを動的に配布するために使用されるプロトコルです。
IB	InfiniBand（IB）は、ハイパフォーマンスのサーバとストレージシステムのためのデータ転送用の通信標準です。
ICMP PING応答	Internet Control Message Protocol（ICMP）は、ネットワークに接続されたコンピュータのオペレーティングシステムでメッセージの送信に使用されるプロトコルです。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。
IQN	iSCSI Qualified Name（IQN）は、iSCSIイニシエータまたはiSCSIターゲットの一意の名前です。
iSER	iSCSI Extensions for RDMA（iSER）は、InfiniBandやイーサネットなどのRDMAトランスポートを使用する処理用にiSCSIプロトコルを拡張したプロトコルです。
iSNS	Internet Storage Name Service（iSNS）は、TCP / IPネットワーク上のiSCSIデバイスとFibre Channelデバイスの自動検出、管理、構成が可能なプロトコルです。
MAC アドレス	メディアアクセス制御（MAC）アドレスはイーサネットで使用される識別子で、同じ物理トランスポートネットワークインターフェイス上の2つのポートを接続する別々の論理チャンネルを区別します。

期間	説明
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。
MTU	Maximum Transmission Unit（MTU；最大転送単位）は、ネットワークで送信可能なパケットまたはフレームの最大サイズです。
RDMA	Remote Direct Memory Access（RDMA）は、ネットワークコンピュータ同士が、それぞれのオペレーティングシステムを介さずにメインメモリ内でデータを交換できるテクノロジーです。
名前のない検出セッション	名前のない検出セッションのオプションが有効な場合、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。

## 方法

### iSCSIポートを設定

コントローラにiSCSIホスト接続が搭載されている場合、System（システム）ページからiSCSIポートを設定できます。

作業を開始する前に

- コントローラにiSCSIポートが搭載されている必要があります。そうでない場合、iSCSI設定は使用できません。
- ネットワーク速度（ポートとホストの間のデータ転送率）を把握しておく必要があります。



iSCSIの設定および機能は、ストレージアレイでiSCSIがサポートされている場合にのみ表示されます。

手順


1. 「\* MENU（\*メニュー）」：「Settings（設定）」 [ System（システム）
2. [\* iSCSI設定\*]で、[\* iSCSIポートの設定\*]を選択します。



Configure iSCSI Ports \*オプションは、System ManagerがコントローラでiSCSIポートを検出した場合にのみ表示されます。

3. iSCSIポートを設定するコントローラを選択します。
4. 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。
5. 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
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> <div>  <p>ポートへのアクセスを無効にする場合は、両方のチェックボックスを選択解除します。</p> </div>
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。

- 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。（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。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。
VLAN サポートを有効にします（* Show more settings * をクリックして使用可能）。	VLAN を有効にしてその ID を入力する場合は、このオプションを選択します。VLAN は、同じスイッチ、同じルータ、またはその両方でサポートされる他の物理 LAN（ローカルエリアネットワーク）および仮想 LAN から物理的に分離されたように動作する論理ネットワークです。
イーサネットの優先順位を有効にする（[詳細設定を表示する *] をクリックして使用可能）。	<p>ネットワークアクセスの優先度を決定するパラメータを有効にする場合は、このオプションを選択します。スライダを使用して優先度を1（最も低い）から7（最も高い）の間で選択します。</p> <p>共有 LAN 環境（イーサネットなど）では、多数のステーションがネットワークアクセスで競合する可能性があります。アクセスは先に行われたものから順に処理されます。2つのステーションが同時にネットワークにアクセスしようとする、両方のステーションがオフになり、再試行するまで待機します。スイッチイーサネットでは、1つのステーションだけがスイッチポートに接続されるため、このプロセスは最小限に抑えられます。</p>

7. [完了] をクリックします。

## iSCSI認証を設定

iSCSIネットワークのセキュリティを強化するために、コントローラ（ターゲット）とホスト（イニシエータ）の間に認証を設定できます。System Managerは、チャレンジハンドシェイク認証プロトコル（CHAP）方式を使用します。CHAPは初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAP\_secret\_\_という共有セキュリティキーに基づいて行われます。

作業を開始する前に

イニシエータ（iSCSIホスト）のCHAPシークレットは、ターゲット（コントローラ）のCHAPシークレットを設定する前でもあとでも設定できます。このタスクの手順を実行する前に、ホストがiSCSI接続を確立するのを待ってから、個々のホストでCHAPシークレットを設定する必要があります。接続が確立されると、iSCSI認証のダイアログボックス（このタスクで説明）にホストのIQN名とCHAPシークレットが表示され、手動で入力する必要はありません。

このタスクについて

次のいずれかの認証方法を選択できます。

- 一方方向認証--コントローラがiSCSIホストの識別情報を認証できるようにするには'この設定を使用します(一方方向認証)
- 双方方向認証--コントローラとiSCSIホストの両方が認証(双方方向認証)を実行できるようにするには'この設定を使用しますこの設定は、コントローラがiSCSIホストの識別情報を認証できるようにし、さらにiSCSIホストがコントローラの識別情報を認証できるようにすることで、二次的なセキュリティを提供します。



iSCSIの設定と機能は、ストレージレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

## 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム)
2. [\* iSCSI settings]で、[Configure Authentication\*]をクリックします。

[認証の設定\*]ダイアログボックスが開き、現在設定されている方式が表示されます。CHAPシークレットが設定されているホストがあるのかも表示されます。

3. 次のいずれかを選択します。
  - 認証なし--コントローラがiSCSIホストのIDを認証しないようにするには'このオプションを選択して'完了\*をクリックしますダイアログボックスが閉じ、設定が完了します。
  - 一方方向認証--コントローラがiSCSIホストのIDを認証できるようにするには'このオプションを選択して'次へをクリックします\*ターゲットCHAPの構成ダイアログ・ボックスを表示します
  - 双方方向認証--コントローラとiSCSIホストの両方が認証を実行できるようにするには'このオプションを選択して'次へ\*をクリックし'ターゲットCHAPの構成ダイアログ・ボックスを表示します
4. 一方方向認証または双方方向認証について、コントローラ（ターゲット）のCHAPシークレットを入力または確認します。CHAPシークレットは、12~57文字の印刷可能なASCII文字で指定する必要があります。



コントローラのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

5. 次のいずれかを実行します。
  - 一方方向認証を設定する場合は、\*完了\*をクリックします。ダイアログボックスが閉じ、設定が完了します。
  - \_2Way\_authenticationを設定する場合は、\* Next \*をクリックしてConfigure Initiator CHAPダイアログボックスを表示します。
6. 双方方向認証について、任意のiSCSIホスト（イニシエータ）のCHAPシークレット（12~57文字の印刷可能なASCII文字）を入力または確認します。特定のホストに双方方向認証を設定しない場合は、「\* Initiator CHAP Secret \*」 フィールドを空白のままにします。



ホストのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

7. [完了] をクリックします。

## 結果

認証なしを指定した場合を除き、iSCSIログインシーケンス中にコントローラとiSCSIホストの間で認証が行われます。

## iSCSI検出設定を有効にします

iSCSIネットワーク内のストレージデバイスの検出に関連する設定を有効にすることができます。ターゲット検出設定では、Internet Storage Name Service (iSNS) プロトコルを使用してストレージレイのiSCSI情報を登録し、名前のない検出セッションを許可するかどうかを設定できます。

作業を開始する前に

iSNSサーバで静的IPアドレスが使用されている場合は、そのアドレスをiSNSの登録に使用できる必要があります。IPv4とIPv6の両方がサポートされています。

このタスクについて

iSCSI検出に関連する次の設定を有効にすることができます。

- \* iSNSサーバによるターゲットの登録を有効にする\*--有効にすると'ストレージ・アレイはiSNSサーバからiSCSI Qualified Name (IQN) とポート情報を登録しますこの設定は、イニシエータがiSNSサーバからIQNとポート情報を取得できるように、iSNS検出を許可します。
- 名前のない検出セッションを有効にする--名前のない検出セッションを有効にすると'イニシエータ (iSCSIホスト) は'検出タイプ接続のログインシーケンス中にターゲットのIQN (コントローラ) を指定する必要はありません無効な場合、ホストはIQNを指定してコントローラへの検出セッションを確立する必要があります。ただし、通常の (I/Oベアリング) セッションでは常にターゲットIQNが必要です。この設定を無効にすると、権限のないiSCSIホストがIPアドレスのみを使用してコントローラに接続することを防止できます。



iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

### 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム) ]
2. [\* iSCSI settings]で、[\*ターゲット検出設定の表示/編集]をクリックします。

[\* Target Discovery Settings\* (ターゲット検出設定\*) ]ダイアログボックスが表示されます。[Enable iSNS server\*...]フィールドの下に、コントローラがすでに登録されているかどうかを示すダイアログボックスが表示されます。

3. コントローラを登録するには、[iSNSサーバーを有効にしてターゲットを登録する\*]を選択し、次のいずれかを選択します。
  - \* DHCPサーバから自動的に設定を取得\*--動的ホスト構成プロトコル(DHCP)サーバを使用してiSNSサーバを設定する場合は'このオプションを選択しますこのオプションを使用する場合は、コントローラのすべてのiSCSIポートでDHCPを使用するように設定する必要があります。必要に応じて、コントローラのiSCSIポートの設定を更新して、このオプションを有効にします。





DHCPサーバでiSNSサーバのアドレスを指定するには'オプション43のベンダー固有の情報'を使用するようにDHCPサーバを設定する必要があります このオプションでは、iSNSサーバのIPv4アドレスをデータバイト0xa-0xd (10-13) に含める必要があります。

- 静的な設定を手動で指定-- iSNSサーバの静的IPアドレスを入力する場合は'このオプションを選択します (必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます)。フィールドに、IPv4アドレスまたはIPv6アドレスを入力します。両方を設定した場合は、IPv4がデフォルトです。また、TCPリスニングポートを入力します (デフォルトの3205を使用するか、49152~65535の値を入力)。
- 4. ストレージアレイを名前のない検出セッションの対象にするには、\*名前のない検出セッションを有効にする\*を選択します。
  - 有効にすると、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要があります。
  - 無効にすると、イニシエータがターゲットIQNを指定しないかぎり、検出セッションは実行されません。名前のない検出セッションを無効にすると、セキュリティが向上します。
- 5. [ 保存 ( Save ) ] をクリックします。

## 結果

System ManagerがコントローラをiSNSサーバに登録しようとする間、進捗状況バーが表示されます。この処理には最大5分かかることがあります。

## iSCSI統計パッケージを表示します

ストレージアレイへのiSCSI接続に関するデータを表示できます。

### このタスクについて

System Managerには、次のタイプのiSCSI統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- **イーサネットMAC統計**--メディアアクセス制御(MAC)の統計情報を提供します。MACは、物理アドレスまたはMACアドレスと呼ばれるアドレス指定メカニズムも提供します。MACアドレスは、各ネットワークアダプタに割り当てられている一意のアドレスです。MACアドレスは、サブネットワーク内のデスティネーションへのデータパケットの配信に役立ちます。
- **イーサネットTCP/IP統計**-- iSCSIデバイスのTCP (Transmission Control Protocol)とIP (Internet Protocol)のTCP/IPの統計情報を提供しますTCPを使用すると、ネットワークホスト上のアプリケーションが相互に接続を作成し、パケットでデータを交換できます。IPは、パケット交換インターネットワークを介してデータを通信するデータ指向プロトコルです。IPv4統計とIPv6統計は個別に表示されます。
- **ローカル・ターゲット/イニシエータ (プロトコル) 統計**: ストレージ・メディアへのブロック・レベルのアクセスを提供するiSCSIターゲットの統計情報を表示します非同期ミラーリング処理でイニシエータとして使用される場合は'ストレージ・アレイのiSCSI統計情報を表示します
- **DCBXの運用状態統計**--さまざまなData Center Bridging Exchange (DCBX) 機能の運用状態を表示します。
- **\*LLDP TLV statistics \***-- Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) 統計を表示します。
- **DCBX TLV統計**-- Data Center Bridging (DCB) 環境内のストレージアレイのホストポートを識別する情報が表示されます。この情報は、識別や機能のためにネットワークピアと共有されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

#### 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム)
2. [View iSCSI Statistics Packages]を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. \*オプション : \*ベースラインを設定するには、\*新しいベースラインの設定\*をクリックします。

ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSCSI統計に同じベースラインが使用されます。

## iSCSI セッションを表示します

ストレージアレイへのiSCSI接続に関する詳細情報を表示できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立できます。

#### 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム)
2. 「\* iSCSIセッションの表示/終了\*」を選択します。

現在のiSCSIセッションのリストが表示されます。

3. 特定のiSCSIセッションに関する追加情報 を表示するには、セッションを選択し、\*詳細の表示\*をクリックします。

## フィールドの詳細

項目	説明
セッション識別子 (SSID)	iSCSIイニシエータとiSCSIターゲット間のセッションを識別する16進数の文字列。SSIDは、ISIDとTPGTで構成されます。
イニシエータセッションID (ISID)	セッション識別子のイニシエータの部分。イニシエータはログイン時にISIDを指定します。
ターゲットポータルグループ	iSCSIターゲット。
ターゲットポータルグループタグ (TPGT)	セッション識別子のターゲットの部分。iSCSIターゲットポータルグループの16ビットの数値識別子。
イニシエータのiSCSI名	世界規模で一意的なイニシエータの名前。
イニシエータのiSCSIラベル	System Managerで設定されたユーザラベル。
イニシエータのiSCSIエイリアス	iSCSIノードにも関連付けることができる名前。エイリアスを使用すると、組織がユーザにわかりやすい文字列をiSCSI名に関連付けることができます。ただし、エイリアスはiSCSI名に代わるものではありません。イニシエータのiSCSIエイリアスは、System Managerではなく、ホストでのみ設定できます
ホスト	ストレージアレイに入出力を送信するサーバ。
接続ID (CID)	イニシエータとターゲット間のセッション内における接続の一意の名前。イニシエータがこのIDを生成し、ログイン要求の際にターゲットに提供します。接続IDは、接続を閉じるログアウト時にも表示されます。
イーサネットポート識別子	接続に関連付けられているコントローラポート。
イニシエータのIPアドレス	イニシエータのIPアドレス。
ネゴシエーション済みのログインパラメータ	iSCSIセッションのログイン時に処理されるパラメータ。
認証方式	iSCSIネットワークへのアクセスを必要とするユーザを認証する手法。有効な値は* chap および None *です。

項目	説明
ヘッダーダイジェスト方式	iSCSIセッションに有効なヘッダー値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
データダイジェスト方式	iSCSIセッションに有効なデータ値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
最大接続数	iSCSIセッションに許可される接続の最大数。1~4を接続の最大数として指定できます。デフォルト値は* 1 *です。
ターゲットエイリアス	ターゲットに関連付けられているラベル。
イニシエータのエイリアス	イニシエータに関連付けられているラベル。
ターゲットのIPアドレス	iSCSIセッションのターゲットのIPアドレス。DNS名はサポートされません。
初期R2T	最初の転送準備完了ステータス。ステータスは「* Yes 」または「 No *」のいずれかになります。
最大バースト長	このiSCSIセッションの最大SCSIペイロード（バイト）。512~262、144（256KB）を最大バースト長として指定できます。デフォルト値は* 262,144（256KB） *です。
第1バースト長	このiSCSIセッションの未承諾データのSCSIペイロード（バイト単位）。512~131、072（128KB）を第1バースト長として指定できます。デフォルト値は*65,536（64KB） *です。
デフォルトの待機時間	接続の終了または接続のリセット後に接続を試行するまでの最小秒数。0~3600をデフォルトの待機時間の値として指定できます。デフォルトは* 2 *です。
デフォルトの保持時間です	接続の終了または接続のリセット後も接続が可能な最大秒数。0~3600をデフォルトの保持時間として指定できます。デフォルト値は*20*です。
最大未処理R2T	このiSCSIセッションの未処理の「準備が完了した転送」の最大数。1~16を未処理の「準備が完了した転送」の最大値として指定できます。デフォルトは* 1 *です。
エラーリカバリレベル	このiSCSIセッションのエラーリカバリのレベル。エラーリカバリレベルの値は常に* 0 *に設定されています。

項目	説明
受信データ最大セグメント長	イニシエータまたはターゲットがペイロードデータユニット（PDU）で受信できる最大データ量。
ターゲット名	ターゲットの正式名（エイリアスではありません）。iqn形式のターゲット名です。
イニシエータ名	イニシエータの正式名（エイリアスではありません）。iqn形式または_eui_formatを使用するイニシエータ名です。

4. \*オプション：\*レポートをファイルに保存するには、\*保存\*をクリックします。

ブラウザのDownloadsフォルダに'iscsi-session-connections.txt'というファイル名でファイルが保存されます

## iSCSIセッションを終了します

不要になったiSCSIセッションを終了できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立できます。

このタスクについて

iSCSIセッションを終了する理由としては、次のようなものが考えられます。

- 不正アクセス-- iSCSIイニシエータがログオンされていて、アクセスできない場合は、iSCSIセッションを終了して、iSCSIイニシエータをストレージアレイから強制的に切断できます。認証方法を「なし」にしたため、iSCSIイニシエータがログオンした可能性があります。
- システムダウンタイム--ストレージアレイを停止する必要があるiSCSIイニシエータがまだログオンしている場合はiSCSIセッションを終了してiSCSIイニシエータをストレージアレイから切断できます

手順

1. 「\* MENU (\*メニュー)」：「Settings (設定)」 [ System (システム)
2. 「\* iSCSIセッションの表示/終了\*」を選択します。

現在のiSCSIセッションのリストが表示されます。

3. 終了するセッションを選択します
4. [セッションの終了]をクリックし、操作を実行することを確認します。

## iSER over InfiniBandポートを設定します

コントローラにiSER over InfiniBandポートが搭載されている場合は、ホストとのネットワーク接続を設定できます。

作業を開始する前に

- コントローラにiSER over InfiniBandポートが搭載されている必要があります。そうでないと、System

ManagerでiSER over InfiniBand設定を使用できません。

- ホスト接続のIPアドレスを確認しておく必要があります。

#### 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム
2. iSER over InfiniBand setting\*で、\* Configure iSER over InfiniBand Ports]を選択します。
3. iSER over InfiniBandポートを設定するコントローラをクリックします。「\* 次へ \*」をクリックします。
4. ドロップダウンリストで設定するHICポートを選択し、ホストのIPアドレスを入力します。
5. [完了]をクリックします。
6. Yes (はい) \*をクリックしてiSER over InfiniBandポートをリセットします。

## iSER over InfiniBandの統計を表示します

ストレージレイのコントローラにiSER over InfiniBandポートが搭載されている場合は、ホスト接続に関するデータを表示できます。

#### このタスクについて

System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット (プロトコル) 統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- \* iSER over InfiniBandインターフェイス統計\*- InfiniBandインターフェイス上のすべてのiSERポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

#### 手順

1. 「\* MENU (\*メニュー)」 : 「Settings (設定)」 [ System (システム
2. View iSER over InfiniBand Statistics \*を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. \*オプション : \*ベースラインを設定するには、\*新しいベースラインの設定\*をクリックします。

ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSER over InfiniBand統計に同じベースラインが使用されます。

## よくある質問です

**iSNS**サーバを登録に使用するとどうなりますか？

Internet Storage Name Service (iSNS) サーバの情報を使用する場合は、iSNSサーバを

照会してターゲット（コントローラ）から情報を取得するようにホスト（イニシエータ）を設定できます。

この登録により、コントローラのiSCSI Qualified Name（IQN）とポート情報がiSNSサーバに提供され、イニシエータ（iSCSIホスト）とターゲット（コントローラ）間の照会が可能になります。

**iSCSI**ではどの登録方法が自動的にサポートされますか。

iSCSIの実装では、Internet Storage Name Service（iSNS）検出方式またはSend Targetsコマンドの使用がサポートされます。

iSNS方式では、イニシエータ（iSCSIホスト）とターゲット（コントローラ）の間でiSNS検出を実行できます。ターゲットコントローラを登録して、コントローラのiSCSI修飾名（IQN）とポート情報をiSNSサーバに提供します。

iSNSを設定しない場合、iSCSIホストはiSCSI検出セッション中にSend Targetsコマンドを送信します。これに応答して、コントローラからポート情報（ターゲットIQN、ポートIPアドレス、リスニングポート、ターゲットポートグループなど）が返されます。iSNSを使用する場合は、ホストイニシエータがiSNSサーバからターゲットIPを取得できるため、この検出方式は必要ありません。

**iSER over InfiniBand**統計には何が表示されますか？

View iSER over InfiniBand Statisticsダイアログボックスには、ローカルターゲット（プロトコル）統計とiSER over InfiniBand（IB）インターフェイス統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット（プロトコル）統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- \* iSER over InfiniBandインターフェイス統計\*- InfiniBandインターフェイス上のすべてのiSER over InfiniBandポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

**iSER over InfiniBand**を設定または診断するためにほかに必要な作業は何ですか？

次の表に、iSER over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。



iSER over InfiniBandを設定できるのは、ストレージアレイのコントローラにiSER over InfiniBandホスト管理ポートが搭載されている場合のみです。

**iSER over InfiniBand**を設定して診断します

アクション	場所
iSER over InfiniBandポートを設定します	<ol style="list-style-type: none"> <li>1. 「* ハードウェア *」を選択します。</li> <li>2. Show back of shelf*を選択します。</li> <li>3. コントローラを選択します。</li> <li>4. iSER over InfiniBandポートの設定*を選択します。</li> </ol> <p>または</p> <ol style="list-style-type: none"> <li>1. 「* MENU (*メニュー)」 : 「Settings (設定)」 [ System (システム)</li> <li>2. 下にスクロールして* iSER over InfiniBand setting*を選択し、* iSER over InfiniBandポートの設定*を選択します。</li> </ol>
iSER over InfiniBandの統計を表示します	<ol style="list-style-type: none"> <li>1. 「* MENU (*メニュー)」 : 「Settings (設定)」 [ System (システム)</li> <li>2. 下にスクロールして* iSER over InfiniBand settings を表示し、 View iSER over InfiniBand Statistics *を選択します。</li> </ol>



## 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。