

**CX3 UltraScale™ シリーズ、CXシリーズ、
AX4-5シリーズ
Solaris用iSCSIサーバ・セット
アップ・ガイド**

P/N 300-005-177、リビジョンA02

2007年11月19日

このドキュメントでは、CX3 UltraScale™シリーズ、CXシリーズ、AX4-5シリーズのストレージ・システムにおいて、iSCSIデータ・ポートに接続されたサーバにiSCSIセキュリティを設定する方法、およびiSCSIイニシエータ・ポートを構成する方法について説明します。このガイドは、ストレージ・システムのセットアップ・ガイド（Navisphere Expressを使用するAX4-5シリーズ、CX3シリーズ、CXシリーズのストレージ・システム）、ストレージ・システムの「ご使用にあたっての準備」ガイド（Navisphere Expressを使用するAX150シリーズ・ストレージ・システム）、またはインストール・ロードマップ（Navisphere Managerを使用するAX4-5シリーズまたはAX150シリーズ、CX3シリーズ、CXシリーズのストレージ・システム）とともに使用することを推奨します。ストレージ・システムのセットアップ・ガイド、「ご使用にあたっての準備」ガイド、およびインストール・ロードマップ（P/N 069001166）は[Powerlink](#)のWebサイトで入手できます。

このドキュメントでは、CX3モデル10システム、CX3モデル20システム、CX3モデル40システム、CX3モデル80システムを「CX3シリーズ」と呼びます。また、CX200、CX300シリーズ、CX400、CX500シリーズ、CX600、CX700のストレージ・システムを「CXシリーズ」と呼びます。また、このドキュメントでは、AX4-5SC、AX4-5SCi、AX4-5、AX4-5iストレージ・システムを「AX4-5シリーズ」と呼びます。また、AX150シリーズ・システムを「AXシリーズ」と呼びます。このシリーズには、AX150SC、AX150SCi、AX150、AX150iが含まれます。

サポート対象のオペレーティング・システムのリビジョン、ドライバ・タイプ、機能については、[Powerlink](#) WebサイトのE-Lab™ Interoperability NavigatorでCX3シリーズまたはCXシリーズのストレージ・システムの詳細、およびストレージ・システムのサポートWebサイトの[インストール]ページにある[サポートマトリックス]リンクでAX4-5シリーズまたはAXシリーズのストレージ・システムの詳細を参照してください。

現在はNIC（ネットワーク・インタフェース・カード）のみがサポートされています。

トピックは以下のとおりです。

- ◆ はじめる前に..... 3
- ◆ iSCSIサーバ・セットアップ・プロセスの概要 6
- ◆ SolarisサーバでのNICのTCP/IP構成ファイルの編集..... 7
- ◆ iSCSIターゲット・デバイスへのアクセスの構成 9
- ◆ Sun StorEdge Traffic ManagerのPowerPath使用の無効化..... 10
- ◆ CHAPセキュリティの準備..... 11
- ◆ iSCSIイニシエータでのCHAPの構成..... 12

はじめる前に

このガイドを使用してサーバにiSCSIイニシエータ・ポートまたはiSCSIセキュリティ（CHAP: Challenge Handshake Authentication Protocol）をセットアップする前に、以下の手順が必要です。

- ◆ ストレージ・システムのセットアップ・ガイド、ストレージ・システムの「ご使用にあたっての準備」ガイド、またはインストール・ロードマップ（Navisphere Managerを使用するストレージ・システムのみ）の説明に従って、ストレージ・システムのiSCSIポートを構成する。
- ◆ ストレージ・システムに同梱されている、またはカスタマイズされたストレージ・システムのサポートWebサイトから生成した、ストレージ・システム構成計画ガイドのワークシートを記入する。

AX4-5シリーズまたはAX150シリーズについては、ストレージ・システムのサポートWebサイトの[インストール]ページにある[プランニング]リンクを使用して計画ガイドを生成できます。

CX3シリーズまたはCXシリーズについては、ストレージ・システムのサポートWebサイトの[プランニング]リンクを使用して計画ガイドを生成できます。

以下の点も確認してください。

- ◆ NIC、スイッチ、ケーブルなどのネットワーク・ハードウェアがすべて取り付けられていること。取り付けるコンポーネントについては、ストレージ・システムの設置時に作成した構成計画ワークシートやスイッチのマニュアルなど、該当するドキュメントを参照してください。
- ◆ ストレージ・システムのiSCSIポートが構成されていること。
- ◆ Solaris 10 Update 3以降のバージョンまたはSolaris 10 Update 2が、**SUNWiscsir**および**SUNWiscsiu**パッケージとともにインストールされていること。

これらのパッケージは、Solarisサーバの以下の場所にインストールする必要があります。

- **SUNWiscsir** – Sun iSCSI Device Driver（ルート）
- **SUNWiscsiu** – Sun iSCSI Management Utilities（usr）

CHAPセキュリティの詳細については、以下のセクションを参照してください。それ以外については、「iSCSIサーバ・セットアップ・プロセスの概要」（6 ページ）を参照してください。

CHAPセキュリティの概要



CHAP（Challenge Handshake Authentication Protocol）は、iSCSI ユーザーを認証するための方法です。iSCSIストレージ・システムではCHAPを使用してイニシエータを認証でき、イニシエータも同様に、ストレージ・システムなどのターゲットを認証できます。

注意

ストレージ・システムのCHAPセキュリティを構成しない場合は、ストレージ・システムのiSCSIポートと同じIPネットワークに接続されたすべてのホストから、ストレージ・システムのリード/ライトが可能になります。ストレージ・システムがプライベート・ネットワーク上にある場合は、CHAPセキュリティを使用しない選択が可能です。ストレージ・システムがパブリック・ネットワーク上にある場合は、CHAPセキュリティを使用することを強く推奨します。

CHAPセキュリティを使用する場合は、サーバとストレージ・システムの両方でCHAPセキュリティを設定して有効にし、その後でデータを受信できるようにLUNまたは仮想ディスクを準備します。データを受信できるようにディスクを準備した後にCHAPセキュリティを設定して有効にすると、LUNまたは仮想ディスクにアクセスできなくなります。CHAPを設定して有効にするときに、サーバとストレージ・システム間の接続が一時的に解除される場合があります。

CHAPには、イニシエータCHAPと双方向CHAPの2種類があります。

- イニシエータCHAP - iSCSIイニシエータがターゲットへの接続に使用するアカウントを設定します。ターゲットがイニシエータを認証します。イニシエータCHAPは、主要なCHAP認証方法です。

Navisphere Expressには、イニシエータCHAPの[基本]オプションと[詳細]オプションがあります。基本CHAPでは、指定されたターゲットにログインするすべてのイニシエータに対してシークレット（パスワード）を1つ指定します。[詳細]オプションを使用

すると、イニシエータごとに異なるシークレットを指定でき、双方向CHAPも設定できます。

Sun Microsystemsのドキュメントでは、「単方向CHAP (unidirectional CHAP)」という用語はイニシエータCHAPを意味しています。

-
- ◆ **双方向CHAP** - イニシエータCHAPに加えて双方向CHAPを適用すると、イニシエータへの接続のためにターゲットが使用するアカウントが設定されます。イニシエータがターゲットを認証します。

双方向CHAPは現在、サポートされていません。

iSCSIサーバ・セットアップ・プロセスの概要

以下の概要では、iSCSIイニシエータ・ポートの構成とiSCSIセキュリティの設定に必要な手順を説明します。

iSCSIイニシエータ・ポートの構成

- 「SolarisサーバでのNICのTCP/IP構成ファイルの編集」（7ページ）の説明に従って、新規の各iSCSI NICのTCP/IP構成ファイルを作成または編集します。
- iSCSIターゲット・デバイスへのアクセスを、「iSCSIターゲット・デバイスへのアクセスの構成」（9ページ）の説明に従って構成します。
- 「Sun StorEdge Traffic ManagerのPowerPath使用の無効化」（10ページ）の説明に従って、Sun StorEdge Traffic Manager (MPxIO) フェイルオーバー・ソフトウェアを無効にします。

iSCSIセキュリティの設定

- 「CHAPセキュリティの準備」（11ページ）の説明に従って、サーバのCHAPの設定を準備します。
- 各NICまたはiSCSI HBAイニシエータのイニシエータCHAPを、「iSCSIイニシエータでのCHAPの構成」（12ページ）の説明に従って構成します。

SolarisサーバでのNICのTCP/IP構成ファイルの編集

サーバ内の新規の各iSCSI NICに対してTCP/IP構成ファイルを作成または編集します。これらのファイルは、サーバ内の新規の各iSCSI NICのデバイス名、IPアドレス、マスク・アドレスを構成します。構成を計画したときに作成した、iSCSIターゲットおよびイニエータ・ポートのネットワーク情報ワークシートを参照してください。

NICが失敗した場合、同じTCP/IPパラメータ値を代替のNICに割り当て、それが失敗したNICと同じiSCSIイニエータ設定およびオプションのCHAPセキュリティ設定を自動的に持つようにします。

PowerPathでは、別々のサブネットで複数のNICを構成する必要があります。

各NIC用のTCP/IP構成ファイルを作成または編集するには、次のようにします。

1. スーパーユーザーとしてログインしていることを確認します。
2. **/etc/hostname**.インタフェース・ファイルを作成または編集し、デバイス名を追加します。たとえば、ホスト**host24**にiSCSIポート**bge0**がある場合、**host24_bge0**などのデバイス名を割り当てられます。この例では、以下の行を**/etc/hostname.bge0**ファイルに割り当てられます。

```
host24_bge0
```

各インタフェースに個別の**/etc/hostname**.インタフェース・ファイルを作成する必要があります。

3. **/etc/hosts** ファイルを編集し、ホスト名とIPアドレスを関連づける行を追加します。たとえば、**128.111.222.28**と**host24_bge0**とを関連づけるには、以下の行を**/etc/hosts** ファイルに追加します。

```
128.111.222.28 host24_bge0
```

4. **/etc/netmask** ファイルを編集し、インタフェースのマスク・アドレスを追加します。たとえば、マスク・アドレス**255.255.255.0**を、IPアドレス**128.111.222.xxx**のサブネットにあるすべてのインタフェースに関連づけるには、以下の行を**/etc/netmask** ファイルに追加します。

```
128.111.222.0 255.255.255.0
```

5. **reboot -- -r**または**init 6**のいずれかのコマンドを使用してシステムを再起動します。

iSCSIターゲット・デバイスへのアクセスの構成

iSCSIイニシエータとストレージ・システムとの間でデータ送受信を行うには、NICイニシエータのネットワーク・パラメータを構成して、ストレージ・システムのストレージ・プロセッサ（SP）iSCSIターゲットに接続する必要があります。

iSCSIターゲット・デバイスへのアクセスを構成するには、次のようにします。

1. スーパーユーザー（ルート）としてログインしていることを確認します。
2. SendTargetsダイナミック検出を使用して、検出するターゲット・デバイスを構成します。

例：

```
iscsiadm add discovery-address 10.14.108.181:3260
```

ホストに特定のターゲットを認識させたくない場合は、Solarisサーバのドキュメントに記載されている固定検出方法を使用します。

3. SendTargetsターゲット検出方法を有効にします。例：

```
iscsiadm modify discovery -sendtargets enable
```

4. ローカル・システムのiSCSIデバイス・リンクを作成します。例：

```
devfsadm -i iscsi
```

Sun StorEdge Traffic ManagerのPowerPath使用の無効化

PowerPathフェイルオーバー・ソフトウェアを使用する場合、以下のようにご使用のSolarisのバージョンに応じて、Sun StorEdge Traffic Manager (MPxIO) を無効にする必要があります。

現在、iSCSIを使用したSun StorEdge Traffic Managerはサポートされていません。

/kernel/drv/iscsi.conf ファイルの次の行のコメントを解除します。

```
mpxio-disable="yes"
```

さらに、次の行が**iscsi.conf** ファイルにある場合：

```
mpxio-disable="no"
```

ここで示すように、コメント (#) を追加する必要があります。

```
matrix 5.10 (64 bit): more /kernel/drv/iscsi.conf
#
# CDDL HEADER START
.
.
# Global mpxio-disable property:
#
# To globally enable MPxIO on all iscsi ports set:
# mpxio-disable="no";
#
# To globally disable MPxIO on all iscsi ports set:
mpxio-disable="yes";
#
matrix 5.10 (64 bit):
```

CHAPセキュリティの準備

CHAPセキュリティを使用するためには、以下の準備が必要です。

- ストレージ・システムに同梱されているか、またはカスタマイズされたストレージ・システムのサポートWebサイトから生成した、適切な構成計画ガイドのiSCSI構成に関する章で、CHAPワークシートを完成すること。

iSCSI イニシエータでのCHAPの構成

iSCSI イニシエータでCHAPセキュリティを構成する前に、前のセクション「CHAPセキュリティの準備」に示したステップが完了していることを確認してください。

Sun Microsystemsのドキュメントでは、「単方向CHAP (unidirectional CHAP)」という用語はイニシエータCHAPを意味しています。

イニシエータCHAPを構成するには、「Solarisサーバ内のNICイニシエータのイニシエータCHAPの構成」(12ページ)を続行します。

Navisphere Expressでは、イニシエータCHAPを基本CHAPと呼びます。

Solarisサーバ内のNICイニシエータのイニシエータCHAPの構成



注意

ストレージ・システムでCHAPを構成する前に、NICまたはiSCSI HBAでCHAPセキュリティを有効にする必要があります。CHAPを設定して有効にするときに、サーバとストレージ・システム間の接続が一時的に解除される場合があります。

イニシエータCHAPを構成するには、次の手順を行います。

1. Solarisにスーパーユーザーとしてログインしていることを確認します。
2. **iscsiadm** コマンドを使用して、イニシエータのシークレット・キーを設定します。

iscsiadm modify initiator-node -CHAP-secret

CHAPシークレットの入力を促すメッセージが表示されます。

CHAPシークレットは12~16文字である必要があります。

3. イニシエータ上でCHAP名を設定します。デフォルトでは、イニシエータのCHAP名がイニシエータのノード名に設定されます。イニシエータのCHAP名を変更するには、**iscsiadm**コマンドを使用します。

iscsiadm modify initiator-node -CHAP-name *CHAP_name*

4. **iscsiadm**コマンドを使用して、イニシエータのCHAP認証を有効にします。

iscsiadm modify initiator-node -authentication CHAP

イニシエータにはユーザー名とシークレット（パスワード）が必要です。ターゲットは、ユーザー名を使用してシークレットを検索します。デフォルトでは、CHAP名はイニシエータのノード名に設定されます。CHAP名は、512バイト未満の任意の文字列に設定できます。

Copyright© 2007 EMC Corporation.All Rights Reserved.

このドキュメントに記載されている情報は、ドキュメントの出版日現時点の情報です。また情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。EMC Corporationは、このドキュメントに記載されている情報についていかなる種類の表現または保証もいたしかねます。また、特に、特定の目的のための、市販性または適合性の暗黙の保証を否定します。

このドキュメント中説明されているいかなるEMCソフトウェアの使用、コピー、配布に関しても、適切なソフトウェア・ライセンスが必要です。

EMC製品名の最新のリストについては、www.EMC2.co.jpサイトの「EMC Corporation Trademarks」を参照してください。

この文書に記載されているその他すべての商標は、各所有者の所有物です。