Dell™ PowerVault™ Encryption Key Manager

LTO Ultrium 4 と LTO Ultrium 5 のスタートアップ・ガイド

このガイドでは、LTO Gen 4 および LTO Gen 5 テープ・ドライブにおける暗号化の***基本構成*** について説明します。 **http://support.dell.com** にアクセスして、最新のライブラリーおよびドライブ・ファームウェアをダウンロードしてから、Dell PowerVault Encryption Key Manager のインストールおよび構成を行い、問題がないことを確認してください。

Dell PowerVault Encryption Key Manager (以下、Encryption Key Manager と表す) は Java™ ソフトウェア・プログラムの 1 つで、暗号鍵の生成、保護、保管、および保守に際して暗号化対応テープ・ドライブを支援します。この鍵は、LTO テープ・メディアに書き込まれる情報の暗号化およびテープ・メディアから読み取られる情報の暗号化解除を行うのに使用します。 Encryption Key Manager は、Linux® および Windows® 上で稼働するもので、エンタープライズ内の複数の場所にデプロイされる共用リソースとして設計されています。

本書では、グラフィカル・ユーザー・インターフェース (GUI) またはコマンドを使用して、Encryption Key Manager のインストールおよびセットアップをいかに迅速に行えるかを説明しています。本書では、JCEKS 鍵ストア・タイプの使用法を説明しています。これは、JCEKS 鍵ストア・タイプが、サポート対象の鍵ストアの中で最も簡単で、また最もトランスポートしやすいためです。 ある特定のステップまたはサポート対象の別の鍵ストア・タイプについての詳細は、「*Dell Encryption Key Manager* ユーザーズ・ガイド」(**http://support.dell.com**、またはご使用の製品に付属の Dell Encryption Key Manager メディアにあります) を参照してください。

注: Encryption Key Manager ホスト・サーバーの重要な構成情報: データ損失のリスクを最小限にとどめるには、Dell Encryption Key Manager プログラムをホスティングするマシンが、ECC メモリーを使用することを推奨します。 Encryption Key Manager は、暗号鍵の生成を要求する機能、およびその鍵を LTO-4 と LTO-5 テープ・ドライブに引き渡す機能を実行します。鍵の構成要素は、Encryption Key Manager による処理時中は、折り返された形 (暗号化された形式) でシステム・メモリーに常駐します。鍵の構成要素は、カートリッジに書き込まれるデータがリカバリー (暗号化解除) できるように、エラーなしで適切なテープ・ドライブに転送される必要があります。システム・メモリー内のビット・エラーが発生した結果、何らかの理由で鍵の構成要素が破損しており、かつ、その鍵の構成要素をカートリッジへのデータ書き込みに使用する場合、そのカートリッジに書き込まれるデータはリカバリーすること (つまり、後日暗号化解除すること) ができません。このようなデータ・エラーの発生を確実に防ぐために配置されている安全機能があります。ただし、Encryption Key Manager をホスティングするマシンでエラー訂正コード (ECC) メモリーが使用されない場合は、システム・メモリー内にある間に鍵の構成要素が破損し、この破損によりデータ損失が発生する可能性が残されます。この状況が発生する可能性は少ないですが、重要なアプリケーション (Encryption Key Manager など) をホスティングするマシンでは、ECC メモリーを使用することを常に推奨します。

最初に行うこと: Encryption Key Manager ソフトウェアのインストール

1. Dell Encryption Key Manager CD を挿入します。Windows で自動的にインストールが開始しない場合、CD までナビゲートし、Install_Windows.bat をダブルクリックします。

   Linux の場合、インストールは自動的に開始しません。CD のルート・ディレクトリーにアクセスし、`Install_Linux.sh` と入力します。

エンド・ユーザーのご使用条件が表示されます。インストールを続行するには、このご使用条件を確認する必要があります。

インストールを行うと、ご使用のオペレーティング・システムに適したすべてのコンテンツ (資料、GUI ファイル、および構成プロパティー・ファイル) が CD からハード・ディスクにコピーされます。インストール時に、ご使用のシステムで適切な IBM Java ランタイム環境の有無が検査されます。この環境が検出されない場合は、自動的に作成されます。

インストールが完了すると、グラフィカル・ユーザー・インターフェース (GUI) が起動します。

方式 1: GUI を使用して Encryption Key Manager をセットアップする

ここでは、基本構成を作成する手順を説明します。正常に終了すると、Encryption Key Manager サーバーが始動します。

1. GUI が開始していない場合、次のようにして開きます。

   Windows の場合

   c:¥ekm¥gui までナビゲートし、`LaunchEKMGui.bat` をクリックします。

   Linux プラットフォームの場合

   /var/ekm/gui にナビゲートして、`. ./LaunchEKMGui.sh` と入力します。

   注: Linux シェル・コマンドの前に「. ./ (ピリオド スペース ピリオド スラッシュ)」を指定して、シェルがスクリプトを確実に検出できるようにしてください。

2. EKM サーバー構成ページ (図 1) で、すべての必須フィールド (アスタリスク * で示されている) にデータを入力します。データ・フィールドの右方にある疑問符をクリックすると、説明を見ることができます。「**次へ**」をクリックして「EKM サーバー証明書構成」ページに進んでください。

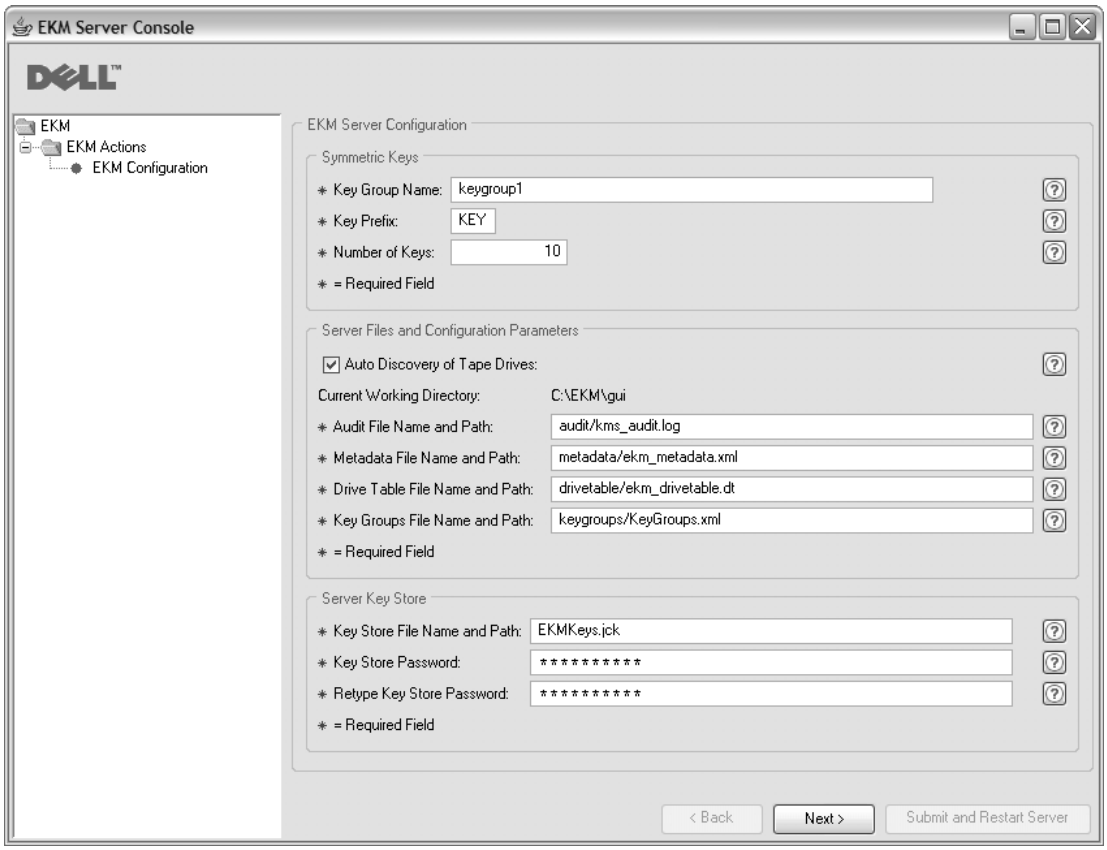

図 1. EKM サーバー構成ページ

注:

a. オートディスカバリーによってドライブが追加されたら、GUI を使用して Encryption Key Manager サーバーをリフレッシュし、そのドライブがドライブ・テーブルに保管されていることを確認する必要があります。

b. 鍵ストア・パスワードを設定したら、セキュリティーが侵害されない限りそのパスワードを**変更しないでください。**パスワードは機密漏れを防ぐために暗号化されています。鍵ストア・パスワードを変

更するには、その鍵ストア内にあるすべての鍵のパスワードを、**keytool** コマンドを使用して個別に変更する必要があります。「*Dell Encryption Key Manager* ユーザーズ・ガイド」の「鍵ストア・パスワードの変更」を参照してください。

3. EKM サーバー証明書構成ページ (図 2) で鍵ストアの別名を入力し、証明書およびその目的を確認するのに役立つ追加フィールドがあれば、入力します。「**Submit and Start Server (サブミットしてサーバーを始動)**」をクリックします。

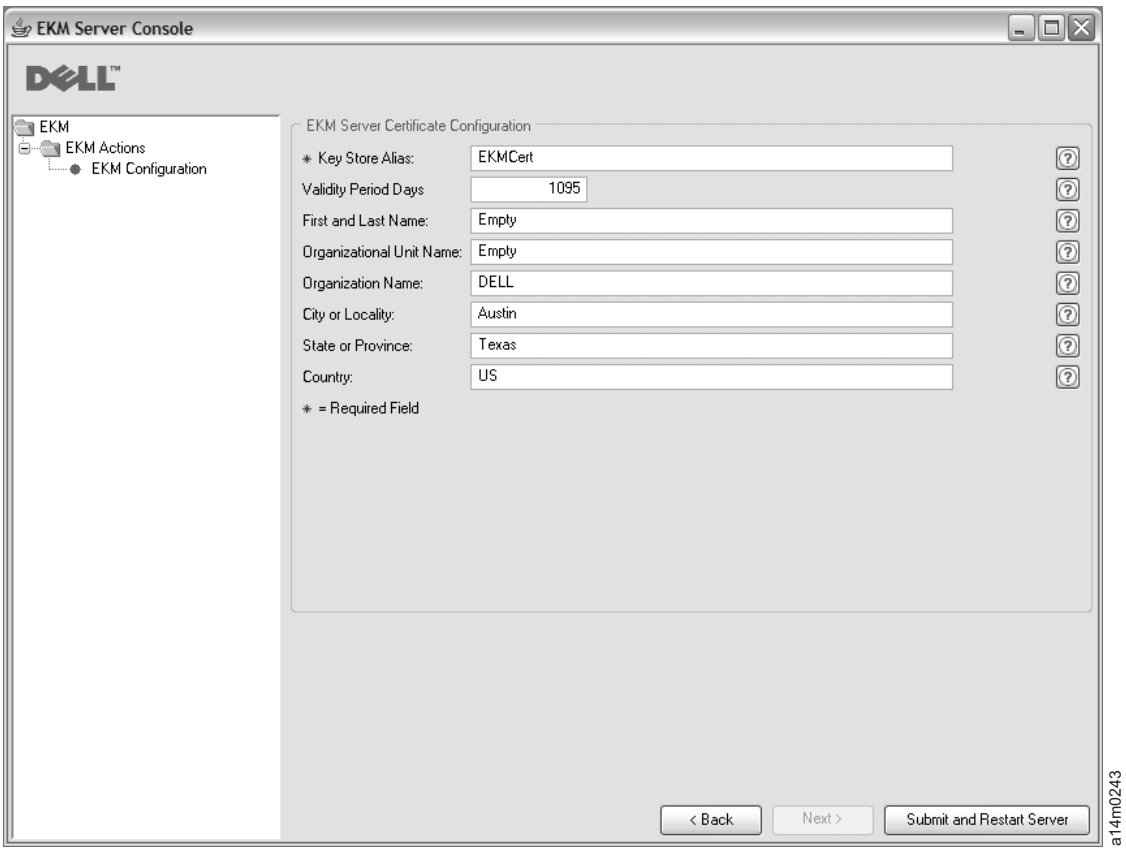

図 2. EKM サーバー証明書構成ページ

注: 鍵生成中に Encryption Key Manager GUI を中断した場合、Encryption Key Manager の再インストールが必要になります。

Encryption Key Manager の鍵生成プロセスが完了する前に停止された場合、鍵ストア・ファイルが破損します。このイベントからリカバリーするには、以下のステップに従ってください。

- 初期インストール中に Encryption Key Manager が中断された場合は、インストールが行われていたディレクトリー (例えば、x:¥ekm) にナビゲートします。そのディレクトリーを削除し、インストールを再開します。
- 新規のキー・グループを追加中に Encryption Key Manager が中断された場合は、Encryption Key Manager サーバーを停止し、最新のバックアップ鍵ストア (このファイルは、x:¥ekm¥gui¥backupfiles フォルダー内にあります) を使用して、鍵ストア・ファイルを復元してください。バックアップ・ファイルには、ファイル名の一部として日時スタンプが含まれていることに注意してください (例えば、2007_11_19_16_38_31_EKMKeys.jck)。この日時スタンプは、ファイルを x:¥ekm¥gui ディレクトリーにコピーしたら、削除する必要があります。Encryption Key Manager サーバーを再始動して、以前に中断されたキー・グループを追加します。

4. バックアップ・ウィンドウ (図 3) に、ご使用の Encryption Key Manager データ・ファイルのバックアップを促すメッセージが表示されます。バックアップ・データを保存するパスを入力します。「**Backup (バックアップ)**」をクリックします。

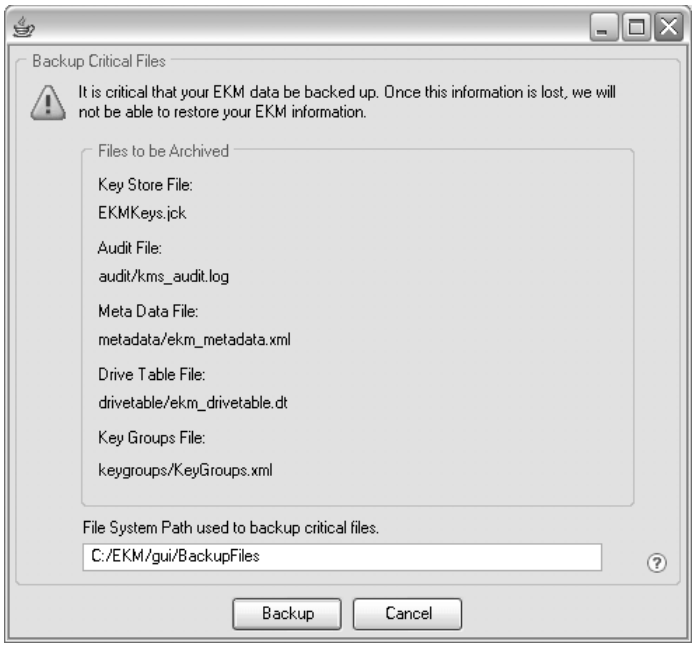

図 3. 「Backup Critical Files (重要なファイルのバックアップ)」ウィンドウ

5. 「User Login (ユーザーのログイン)」ページが表示されます。デフォルトのユーザー名 EKMAdmin およびデフォルトのパスワード changeME を入力します。「**Login (ログイン)**」をクリックします。

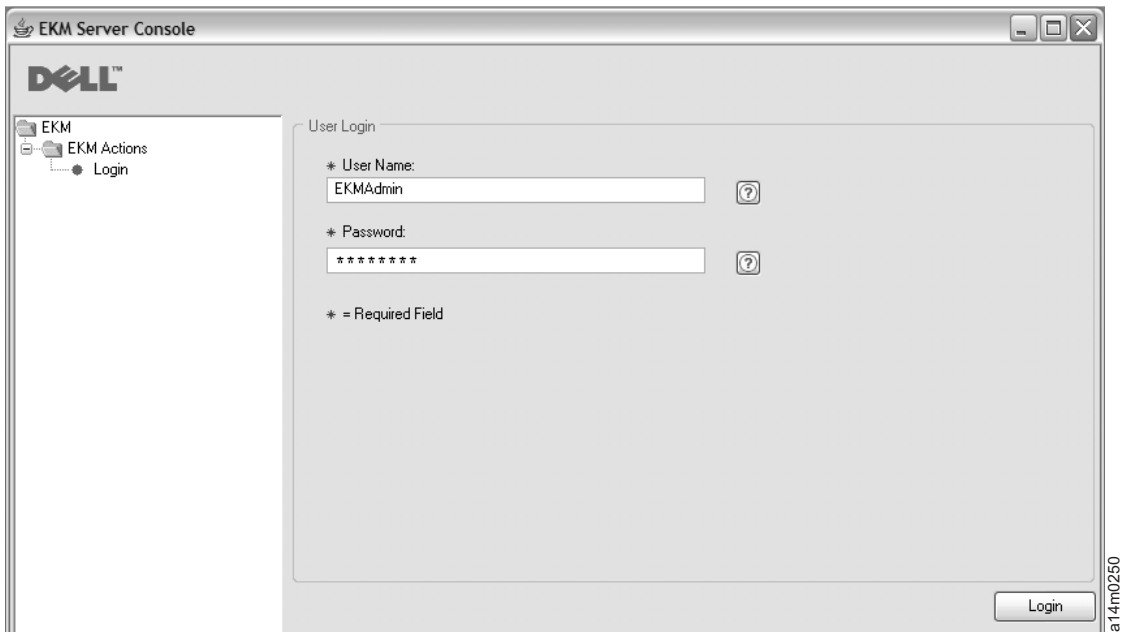

図 4. 「User Login (ユーザーのログイン)」ページ

Dell Encryption Key Manager サーバーがバックグラウンドで起動します。

6. GUI ナビゲーターで「**Server Health Monitor (サーバーの正常性モニター)**」を選択し、Encryption Key Manager サーバーが起動していることを確認します。

適切なホスト IP アドレスを見つける方法

現在の Encryption Key Manager GUI における制限により、Encryption Key Manager のホスト IP アドレスが「Server Health Monitor (サーバーの正常性モニター)」に表示されない場合があります。

- ホストが IPv6 アドレスで構成されている場合、Encryption Key Manager アプリケーションは IP アドレスを表示できません。
- Encryption Key Manager アプリケーションが Linux システムにインストールされている場合、Encryption Key Manager アプリケーションは実際にアクティブである IP ポートではなく、ローカル・ホスト・アドレスを表示します。

a. ホスト・システムの実際の IP アドレスを取得するには、ネットワーク構成にアクセスし、IP ポート・アドレスを見つけてください。
   - Windows システムでは、コマンド・ウィンドウを開き、`ipconfig` と入力します。
   - Linux の場合は、`isconfig` と入力します。

EKM SSL ポートを識別する方法

a. コマンド行を使用して、Encryption Key Manager サーバーを始動します。
   - Windows では、cd `c:¥ekm` にナビゲートし、**startServer.bat** をクリックします。
   - Linux プラットフォームでは、`/var/ekm` にナビゲートし、`startServer.sh` と入力します。
   - 詳細については、「*Dell Encryption Key Manager ユーザーズ・ガイド*」の「Key Manager サーバーの始動、リフレッシュ、および停止」を参照してください。

b. コマンド行を使用して、CLI クライアントを開始します。
   - Windows では、cd `c:¥ekm` にナビゲートし、**startClient.bat** をクリックします。
   - Linux プラットフォームでは、`/var/ekm` にナビゲートし、`startClient.sh` と入力します。
   - 詳細については、「*Dell Encryption Key Manager ユーザーズ・ガイド*」の「コマンド行インターフェース・クライアントの開始」を参照してください。

c. 以下のコマンドを使用して、Encryption Key Manager サーバー上の CLI クライアントにログインします。

   `login -ekmuser` ***userID*** `-ekmpassword` ***password***

   ここで、*userID* = EKMAdmin であり、*password* = changeME (これがデフォルトのパスワードです。既にデフォルトのパスワードを変更している場合は、ご使用の新規パスワードを使用してください) です。

   ログインが成功すると、`User successfully logged in (ユーザーのログインが成功しました)` と表示されます。

d. 次のコマンドを入力し、SSL ポートを識別します。

   `status`

   以下のような応答が表示されます。`server is running. TCP port: 3801, SSL port: 443 (サーバーは稼働中です。TCP ポート: 3801、SSL ポート: 443)`

   構成済みの SSL ポートをメモし、これがライブラリー管理の暗号化設定を構成するのに使用するポートであることを確認してください。

e. コマンド行からログアウトします。次のコマンドを入力してください。

```
exit
```

コマンド・ウィンドウを閉じます。

方式 2: コマンドを使用して Encryption Key Manager をセットアップする

ステップ 1. JCEKS 鍵ストアの作成

注意: Encryption Key Manager および関連するすべてのファイルのコピーを通常の基準で作成することを強くお勧めします。 Encryption Key Manager 暗号鍵が失われたり破損した場合、暗号化されたデータをリカバリーする方式はありません。

鍵ストアを作成し、その鍵ストアを証明書および秘密鍵付きで追加します。この証明書を使用して、Encryption Key Manager サーバー間の通信および Encryption Key Manager CLI クライアントとの通信をセキュアにします。この **keytool** コマンドによって、EKMKeys.jck という新規の JCEKS 鍵ストアが作成され、証明書および ekmcert という別名の秘密鍵と共に、その鍵ストアが追加されます。この証明書は、5 年間有効です。この証明書の有効期限が切れると、Encryption Key Manager サーバー間の通信、および Encryption Key Manager CLI クライアントと Encryption Key Manager サーバーとの通信は機能しなくなります。有効期限が切れた古い証明書を削除して、このステップで指定された方法で新規の証明書を作成してください。

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048 -validity 1825
```

keytool コマンドによって、ご使用の Encryption Key Manager の識別を可能にする証明書を作成するのに使用される情報を求めるプロンプトが出されます。このプロンプトは、サンプルとなる応答を加えると、以下のようなものになります。

```
What is your first and last name? [Unknown]:  ekmcert
What is the name of your organizational unit?   [Unknown]:  EKM
What is the name of your organization? [Unknown]:  Dell
What is the name of your City or Locality?   [Unknown]: Austin
What is the name of your State or Province?   [Unknown]:  TX
What is the two-letter country code for this unit? [Unknown]:  US
Is CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US correct?(type "yes" or "no"):
```

「yes」と入力し、Enter キーを押してください。

ステップ 2. 暗号鍵の生成

注: いかなるセッションにおいても、keytool を初めて使用する前に、 **updatePath** スクリプトを使用して適切な環境を設定してください。

Windows の場合

cd c:¥ekm までナビゲートし、updatePath.bat をクリックします。

Linux プラットフォームの場合

/var/ekm までナビゲートし、`. ./updatePath.sh` と入力します。

注: Linux シェル・コマンドの前に「. ./ (ピリオド スペース ピリオド スラッシュ)」を指定して、シェルがスクリプトを確実に検出できるようにしてください。

LTO 暗号化の場合、Encryption Key Manager では、事前作成して鍵ストアに保管されるべき多数の対称鍵が必要になります。この **keytool** コマンドによって 32 個の 256 ビット AES 鍵が作成され、ステップ 3

で作成される鍵ストアに保管されます。このコマンドを Encryption Key Manager ディレクトリーから実行し、そのディレクトリー内に鍵ストア・ファイルが作成されるようにします。結果として生成された鍵の名前は、key000000000000000000 から key0000000000000000001f になります。

```
keytool -keystore EKMKeys.jck -storetype jceks -genseckey -keyAlg aes -keysize 256 -aliasrange key00-1f
```

このコマンドによって、鍵ストアにアクセスするための鍵ストアのパスワードを求めるプロンプトが出されます。必要なパスワードを入力し、Enter キーを押してください。鍵のパスワードを求めるプロンプトが出された場合は、その情報は不必要なため、もう一度 Enter キーを押します。新規の、または別のパスワードを入力しないでください。これにより、鍵のパスワードが鍵ストアのパスワードと同様のものになります。ここで入力した鍵ストアのパスワードは Encryption Key Manager の開始の際に必要になりますので、記録しておいてください。

注: 鍵ストア・パスワードを設定したら、セキュリティーが侵害されない限りそのパスワードを変更しないでください。鍵ストア・パスワードを変更するには、構成ファイル内のすべての鍵の属性も変更する必要があります。パスワードは機密漏れを防ぐために暗号化されています。

ステップ 3. Encryption Key Manager サーバーの始動

GUI を使用せずに Encryption Key Manager サーバーを始動する場合は、以下のようにして startServer スクリプトを起動します。

Windows の場合

`cd c:¥ekm¥ekmserver` までナビゲートし、startServer.bat をクリックします。

Linux プラットフォームの場合

/var/ekm/ekmserver までナビゲートし、`. ./startServer.sh` と入力します。

注: Linux シェル・コマンドの前に「. ./ (ピリオド スペース ピリオド スラッシュ)」を指定して、シェルがスクリプトを確実に検出できるようにしてください。

注意: Encryption Key Manager および関連するすべてのファイルのコピーを通常の基準で作成することを強くお勧めします。 Encryption Key Manager 暗号鍵が失われたり破損した場合、暗号化されたデータをリカバリーする方式はありません。

ステップ 4. Encryption Key Manager コマンド行インターフェース・クライアントの開始

Encryption Key Manager CLI クライアントを開始するには、以下のようにして startClient スクリプトを起動します。

Windows の場合

`cd c:¥ekm¥ekmclient` までナビゲートし、startClient.bat をクリックします。

Linux プラットフォームの場合

/var/ekm/ekmclient までナビゲートし、`. ./startClient.sh` と入力します。

注: Linux シェル・コマンドの前に「. ./ (ピリオド スペース ピリオド スラッシュ)」を指定して、シェルがスクリプトを確実に検出できるようにしてください。

CLI クライアントが鍵マネージャーのサーバーに正常にログインすると、すべての CLI コマンドが実行可能になります。完了したら、終了コマンドを使用して CLI クライアントをシャットダウンしてください。10 分間使用されないと、クライアントは自動的にシャットダウンします。 CLI コマンドの情報については、「*Dell Encryption Key Manager ユーザーズ・ガイド*」(**http://support.dell.com**、またはご使用の製品に付属の Dell Encryption Key Manager メディアにあります) を参照してください。

詳細情報の参照先

詳細については、以下の資料を参照してください。

- *Dell Encryption Key Manager User's Guide* (Dell Encryption Key Manager CD に含まれています。また、**http://support.dell.com** でも参照可能です)
- *Library Managed Encryption for Tape* (LTO テープの暗号化について、ベスト・プラクティスを提案するホワイト・ペーパー。**http://www.dell.com** で参照可能です)