SME インストールの計画

この付録では、正常に SME をインストールするために実行する必要がある手順とガイドラインの概要を示します。アプリケーションをインストールする前に、次のサービスおよび機能の要件と前提条件をお読みください。

SAN の考慮事項

SME をインストールする前に、SAN に関する次の情報を収集します。

- SAN または NX-OS オペレーティング システムのバージョン。

  （注） Cisco SAN-OS Release 3.1(1a) 以降、または NX-OS Release 4.x 以降のバージョンを使用することを推奨します。

- SAN スイッチ ベンダー。

  （注） SME は、Cisco 専用の SAN でサポートされます。ただし、他のベンダー提供のスイッチがある SAN も、ケースバイケースでサポートされる場合があります。

- SAN トポロジ（ホストとターゲットの配置、およびファブリックの数を含む）。
- バックアップ ホスト オペレーティング システム。
- バックアップ アプリケーションのタイプとバージョン。
- HBA のタイプとファームウェアのバージョン。

- テープ ライブラリおよびドライブのタイプ。
- ホストとテープ ドライブの数。
- SAN トポロジ図。
- ISL 接続に使用するモジュールのタイプ（Generation 1 または Generation 2）。

（注）　この情報は、大規模な SME のセットアップに必要です。

- ホストとテープ ドライブのゾーン分割、およびすべてのドライブがすべてのホストにアクセス可能かどうか。ホストとドライブ間に選択的アクセス可能性があることが推奨されます。

相互運用性マトリックス

使用する相互運用性マトリックスを確認します。必要に応じて、テープ ライブラリやドライブなどの、新しいタイプおよびバージョンの SAN コンポーネントの RPQ を依頼するか、または新しいバックアップ アプリケーション ソフトウェア バージョンを依頼します。

『*Cisco MDS 9000 Family Interoperability Support Matrix*』を参照してください。

MSM-18/4 モジュール

MSM-18/4 モジュールに関する次の情報を収集します。

- MSM-18/4 モジュールの総スループット要件と必要な数を決定します。スループット要件はバックアップ ウィンドウを満たしているか、各ドライブのライン レート スループットの到達のいずれかに基づくことができます。詳細については、『*Cisco Storage Media Encryption Design Guide*』を参照してください。
- MSM-18/4 モジュールの配置を決定します。サンプル トポロジと推奨の設計ガイドを参照してください。
- 大規模な SME セットアップでは、ISL に使用するライン カードが FC-Redirect 構成用に拡張できるかどうかを確認します。詳細については、『*Cisco Storage Media Encryption Design Guide*』を参照してください。

（注）　ISL の接続には Generation 2 モジュールを推奨します。

- 適切な数の SME ライセンスを発注します。

Key Management Center および DCNM-SAN サーバ

次のどのキー管理戦略およびポリシーが適しているかを判断します。

- データセンターには、RSA キー マネージャを備えた Cisco KMC または KMC を使用します。
- PostgreSQL データベースまたは Oracle Express をデータベースとして使用します。

  データベースには PostgreSQL を使用することを推奨します。
- 共有キー モードまたはテープごとの固有キーを使用します。

- キーオンテープ モードを設定します。
- テープ リサイクルを使用します。

（注）　キー ポリシーの詳細については、『*Storage Media Encryption Key Management White Paper* 』および 第 7 章「SME キー管理の設定」を参照してください。

- Basic、Standard、または Advanced の、いずれかのキー セキュリティ モードを使用します。

  マスター キーのセキュリティ モードの詳細については、第 4 章「SME クラスタ管理の設定」を参照してください。

Standard または Advanced セキュリティ モードでスマート カードを使用する場合は、次のことを必ず実行します。

- SME プロビジョニングに使用するホストに、GemPlus スマート カード リーダー ドライバをインストールします。これらのカード リーダー ドライバは、Cisco MDS 9000 Management Software and Documentation CD-ROM に収録されています。
- 必要な数のスマート カードとリーダーを発注します。
- DCNM-SAN および KMC のセットアップ用のユーザ環境内でホストを特定します。

  要件については、第 1 章「ストレージ メディア暗号化の概要」を参照してください。

セキュリティ

スイッチから KMC への通信に SSL を使用するかどうかを決定します。SSL を使用する場合は、次のタスクを実行します。

- 自己署名証明書が必要であるか、またはユーザが自身の証明書をルート証明書として使用するかどうかを確認します。
- 証明書がインストールされるスイッチの名前と IP アドレスをリストします。
- OpenSSL をインストールします。このアプリケーションは、DCNM-SAN および KMC に使用されるサーバにインストールできます。
  - Windows オペレーティング システムを稼働するサーバに対して、次の場所から OpenSSL をダウンロードしてインストールします。

    http://gnuwin32.sourceforge.net/packages/openssl.htm

    http://www.slproweb.com/products/Win32OpenSSL.html

    インストールされている SSL は、キーを生成するために使用する必要があります。
  - 次の場所にインストールされている OpenSSL アプリケーションを使用します。

    C:\Program Files\GnuWin32\bin\openssl.exe

（注）　Linux 上で稼働するサーバの場合、OpenSSL アプリケーションは事前にサーバ上で使用可能になっている必要があります。

- SAN（つまりローカル データベース TACACS+ または RADIUS）で使用される認証モードを確認します。

通信

次の作業を確実に実行します。

- ファイアウォール サーバ上で次のポートを許可します。
  - SME クラスタ通信用の TCP および UDP のためにポート 9333 ～ 9339
  - Cisco KMC 通信用のポート 8800 および 8900
  - SME Web クライアント通信用のポート HTTP（80）および HTTPS（443）
- SAN および KMC 通信用に、DNS または IP アドレスのいずれか（組み合わせではない）を使用します。

（注）　IP アドレスを使用する場合は、sme.useIP について、「IP アドレスまたは名前を選択するための sme.useIP」セクション（ 2-17 ページ）を参照してください。

設置準備の要件

SME をインストールする前に、次の作業を必ず実行してください。

- DCNM-SAN 上に Java 1.5 または 1.6 をインストールします。
- SSL を使用する場合は、SSL 証明書の生成に使用するサーバ上に OpenSSL をインストールします。
- 必要なポートがファイアウォールを通過して管理インターフェイスで許可されていることを確認します。
- DNS を使用する場合、すべてのスイッチおよび KMC サーバは、それぞれの DNS 名を使用して（**ping** コマンドで）相互に到達可能であることを確認します。
- SSL 証明書を生成するために使用されるすべてのスイッチ、KMC、およびサーバ間で時刻を同期します。NTP を必要に応じて設定します。
- ホストとテープ ドライブが適切にゾーン分割されていることを確認します。
- スイッチへの CLI アクセスがあることを確認します。
- スマート カード リーダーのドライバをインストールします。
- 必要数のスマート カードとリーダーが使用可能であることを確認します。
- 必要なスイッチのセット上に MSM-18/4 モジュールを取り付け、SME ライセンスをインストールします。

事前設定タスク

SME を設定する前に、DCNM-SAN をインストールし、サービスをイネーブルにし、ユーザとロールを割り当て、ファブリックを作成し、SSL 証明書をインストールし、SME をプロビジョニングする必要があります。続くいくつかの項では、実行する必要がある手順を説明しています。

- DCNM-SAN のインストール（E-5 ページ）
- FC-Redirect の CFS 地域の設定（E-5 ページ）
- SME サービスのイネーブル化（E-6 ページ）

- SME のロールとユーザの割り当て（E-6 ページ）
- SME ファブリックの作成（E-6 ページ）
- SSL 証明書のインストール（E-7 ページ）

DCNM-SAN のインストール

DCNM-SAN のインストール中に、次のタスクを実行します。

- Cisco DCNM-SAN のログイン名とパスワードが、スイッチのログイン名とパスワードと同じであることを確認します。
- 適切なデータベースを選択します。
- 適切な認証モードを選択します。
- インストール中に HTTPS を選択します。

（注）　DCNM-SAN のインストールの詳細を確認するには、『*Cisco DCNM-SAN Fundamentals Guide*』を参照してください。

FC-Redirect の CFS 地域の設定

FC-Redirect の CFS 地域を設定するには、次のタスクを実行します。

ステップ 1　次の例に示すように CFS 地域のスイッチを設定します。

```
switch# config t
switch# cfs region 2
switch# fc-redirect
switch# end
```

指定した地域に含まれるすべてのスイッチに対して、この手順を繰り返します。

ステップ 2　**show fc-redirect peer-switches** コマンドを入力して、CFS 地域で必要なすべてのスイッチを使用できることを確認します。「show fc-redirect peer-switches」セクション（ A-26 ページ）を参照してください。

ステップ 3　既存の SME インストールを FC-Redirect の CFS 地域に移行するには、各スイッチのその他の地域のスイッチで作成されたすべての既存の FC-Redirect 設定を削除します。設定を削除するには、次の手順に従います。

a. **show fc-redirect configs** を入力して、すべての FC-Redirect 設定のリストを入手します。「show fc-redirect configs」セクション（ A-25 ページ）を参照してください。

b. **clear fc-redirect configs** コマンドを使用して、他の地域のスイッチで作成されたすべての設定を削除します。設定はスイッチから削除されますが、スイッチは作成された地域でアクティブのままになります。

（注）　詳細については、「clear fc-redirect config」セクション（ A-2 ページ）を参照してください。

SME サービスのイネーブル化

SME サービスをイネーブル化するには、次の作業を実行します。

- FC-Redirect のバージョンを 2 に設定します（SAN-OS Release 3.1(1a) 以降または NX-OS Release 4.x を使用している場合）。version2 モードのイネーブル化の詳細については、「fc-redirect version2 enable」セクション（ A-9 ページ）を参照してください。

（注）　これらのサービスをイネーブルにするための詳細については、第 2 章「SME の設定」を参照してください。

SME のロールとユーザの割り当て

SME 機能は、SME 管理者（sme-admin）と SME リカバリ責任者（sme-recovery）の 2 つの主要なロールを提供しています。SME 管理者のロールには、SME ストレージ管理者（sme-stg-admin）および SME KMC 管理者（sme-kmc-admin）のロールも含まれています。

ロールとユーザを設定するには、次の点に注意してください。

- 適切な SME のロール（sme-admin と sme-stg-admin の両方または一方、sme-kmc-admin、および sme-recovery）を、Advanced マスター キー セキュリティ モードで作成します。
- キー管理と SME プロビジョニングの責任を切り離すために、sme-kmc-admin ロールと sme-stg-admin ロールには別々のユーザを選択します。それらの責任を 1 つのロールに結合するには、stg-admin ロールを選択します。
- DCNM-SAN を使用して、必要に応じて sme-admin、sme-stg-admin、および sme-kmc-admin のロールのユーザを作成します。
- Advanced マスター キー モードでは、sme-recovery ロールの下で 3 ～ 5 のユーザを作成します。
- これらのロールのすべてについて、スイッチ上でユーザを作成します。

ロールと責任に関する詳細については、「SME のロールと SME ユーザの作成および割り当て」セクション（ 2-17 ページ）を参照してください。ロールの作成と割り当ての詳細については、『*Security Configuration Guide, Cisco DCNM for SAN*』および『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

SME ファブリックの作成

SME ファブリックを作成する場合は、次の点に注意してください。

- DCNM-SAN Web クライアントを使用して SME ファブリックを追加します。名前を変更して、ファブリック名からスイッチ名を除外します。
- ファブリック名は一定している必要があります。SME の設定後には、ファブリック名は変更できません。

SSL 証明書のインストール

SSL 証明書を作成するには、次のタスクを実行します。

- 第 8 章「証明書のプロビジョニング」に指定されている手順に従って、スイッチおよび KMC 上に SSL 証明書をインストールします。
- プロセスを簡素化するために、インストール手順のすべてのステップで同じパスワードを使用します。
- SSL 証明書をインストールしたら、DCNM-SAN と KMC を再起動します。

SME のプロビジョニング

SME をプロビジョニングおよび設定する際には、次の作業を実行します。

- ストレージ メディア暗号化に使用される MSM-18/4 モジュールごとに SME インターフェイスを作成します。詳細については、第 3 章「SME インターフェイスの設定」を参照してください。
- クラスタの作成を含め、第 4 章「SME クラスタ管理の設定」で説明されている手順と、テープ バックアップ グループの設定手順に従います。
- 実行中のコンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

詳細については、SME のソリューション ガイドを参照してください。それには特定の設定で SME ディスクをインストールするための詳細と要件が記載されています。