



## **Cisco MDS 9000** ファミリ **NX-OS** ストレージ メディア暗号化コンフィギュレーションガイド

2016 年 1 月 28 日

### **Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

シスコは世界各国 200 箇所にオフィスを開設しています。  
各オフィスの住所、電話番号、FAX 番号は  
当社の **Web** サイトをご覧ください。  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices)

**【注意】 シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。**

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。  
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco MDS 9000 ファミリー NX-OS ストレージメディア暗号化コンフィギュレーションガイド  
© 2016 Cisco Systems, Inc. All rights reserved.



---

## A

### Advanced セキュリティ

概要 [7-4](#)

---

## B

### Basic セキュリティ

概要 [7-3](#)

---

## C

CFS 要件 [1-15](#)

### Cisco Key Management Center

概要 [1-4, 7-3](#)

機能 [1-4](#)

利点 [7-3](#)

Cisco KMC [6-11](#)

### Cisco MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール(MSM-18/4)

交換 [11-6](#)

### Cisco SME

セキュリティの概要 [1-15](#)

#### 設定

初期 [2-21](#)

制限 [2-22](#)

必須エンジン [1-8](#)

ベスト プラクティス [10-1](#)

用語 [1-7](#)

### CLI

説明 [2-2](#)

---

## D

### DCNM-SAN

説明 [2-1](#)

DCNM-SAN Web クライアント [2-1](#)

DCNM-SAN サーバ [2-2](#)

バックアップ [D-1](#)

DCNM-SAN サーバ データベース

復元 [D-2](#)

Device Manager [2-2](#)

### DNS

イネーブル化 [2-16](#)

設定 [11-6](#)

代替手段 [2-17](#)

---

## F

### FC-Redirect

要件 [1-15](#)

### FCIP テープ アクセラレーション

要件 [2-4](#)

FC リダイレクト [1-6](#)

---

## I

IEEE 準拠の AES 256 暗号化 [1-3](#)

IVR ゾーンセット [1-15](#)

---

## J

Java 要件 [1-15](#)

---

**M**

MSM-18/4 1-12

**N**

NIST 1-3

**S**

## SME

サポート対象単一ファブリック トポロジ  
セキュリティ 1-15

## SME 設定

Basic 2-21

## SME ディスク

CLI を使用した設定 6-17

ISSU 6-16

SME 暗号化エンジンの追加 6-19

SME ディスク管理設定の確認 6-34

SME ディスク管理のモニタリング 6-35

SME ディスクの回復 6-28

SME ノードの追加 6-19

アーキテクチャ 6-2

オフライン データ準備 6-7

オンライン データ準備 6-9

キー管理 6-10

キー再生成 6-9

キーの生成 6-10

キー複製 6-13

クラスタのサポート 6-5

データ準備 6-6

データ レプリケーション 6-13

ディスク キー複製, 関係 6-15

ディスク キー複製, 機能 6-15

ディスク グループの消去 6-12

ディスク グループの設定 6-20

ディスク グループへのディスクの追加 6-21

ディスクの管理 6-22

ディスクの消去 6-12

ディスクの状態 6-11

ディスクへのパスの追加 5-5, 6-21

## Standard セキュリティ

概要 7-4

**あ**

暗号化 1-3

**お**

オフライン データ復元ツール

概要 C-1

**き**

## キー

SME テープの表示 7-12

SME ディスクの表示 7-13

## キー階層

概要 7-1

テープ ボリューム キー 7-2

テープ ボリューム グループ キー 7-2

ディスク キー 7-2

マスター キー 7-2

キー管理設定 7-4

キーオンテープ 7-5

共有 7-4

固有キー 7-5

キーの管理 1-4

**<**

クォーラム ディスク 6-13

## クラスタ

活性化 11-4

クォーラム 4-1

リカバリ シナリオ [11-1](#)  
 クラスタリング [1-6](#)

---

## こ

高可用性 KMC  
 概要 [7-5](#)  
 コマンドラインインターフェイス。「CLI」を参照 [2-2](#)

---

## さ

サーバ クラスタ [4-5](#)  
 サポート対象トポロジ  
 単一ファブリック [1-8, 1-9](#)  
 サポートへのお問い合わせ [11-8](#)

---

## し

自動キー レプリケーション  
 メディア キーの変換 [7-6](#)

---

## す

スマート カード  
 GemSafe ライブラリ ファイル [2-21](#)  
 インストール [2-21](#)  
 ドライバ [2-21](#)

---

## せ

セキュリティ  
 追加の機能 [1-16](#)

---

## て

データベース テーブルの移行  
 概要 [F-1](#)  
 手順 [F-1](#)

テープ  
 リサイクル [7-5](#)  
 テープ ドライブ  
 トラブルシューティング [11-8](#)  
 テープのリサイクル [7-5](#)  
 テープ ボリューム キー [7-2](#)  
 テープ ボリューム グループ キー [7-2](#)  
 テープをプロビジョニングするためのサーバ ベース  
 の検出 [1-6](#)  
 ディザスタ リカバリ  
 SME テープ [B-1](#)  
 SME ディスク [B-2](#)  
 ディスク キー [7-2](#)

---

## と

透過的なファブリック サービス [1-3](#)  
 トラブルシューティング [11-1](#)  
 「no paths found」 [11-7](#)  
 DNS [11-6](#)  
 MSM-18/4 モジュールの交換 [11-6](#)  
 新しく追加されたテープ ドライブ [11-8](#)  
 オフライン スイッチの削除 [11-2](#)  
 クラスタの活性化 [11-4](#)  
 クラスタの削除 [11-2, 11-3](#)  
 クラスタのリカバリ シナリオ [11-1](#)  
 シナリオ [11-6](#)

---

## は

ハードウェア  
 要件 [1-11](#)  
 Cisco MDS 18/4 ポート マルチサービス モ  
 ジュール (MSM-18/4) [1-12](#)  
 Cisco MDS 9222i マルチサービス モジュラ  
 スイッチ [1-12](#)  
 ハードウェア要件 [1-11](#)

へ

- ベストプラクティス
  - 概要 [10-1](#)
- 変換コンテキスト [7-6](#)

ま

- マスターキー [7-2](#)
- マスターキーセキュリティ
  - Advanced [7-4](#)
  - Basic [7-3](#)
  - Standard [7-4](#)
- マスターキーのセキュリティ
  - モード [7-3](#)
- マスタースイッチの選定 [4-1](#)
  - 3 スイッチ クラスタ シナリオ [4-4](#)
  - 4 スイッチ クラスタ シナリオ [4-5](#)

よ

- 要件
  - FC-Redirect [1-15](#)
  - Java Cryptography Extension [1-15](#)
- インストール [2-4](#)
- ゾーン分割 [1-15](#)
- ソフトウェア [1-11](#)
- ハードウェア [1-11](#)

ら

- ライセンス
  - MSM-18/4 モジュール用、SSM 対応 MDS 9200 シリーズ [2-3](#)
  - MSM-18/4 モジュール用、SSM 対応 MDS 9500 シリーズ [2-3](#)
  - 固定スロット用、MDS 9222i スイッチ [2-3](#)

れ

- レプリケーション関係 [7-6](#)

ろ

- ロードバランシング
  - 概要 [1-6](#)
- ロール
  - 概要 [1-3](#)



## 新機能および変更された機能に関する情報

---

Cisco MDS NX-OS Release 7.3(0)D1(1) のCisco MDS 9000 ファミリ NX-OS ストレージメディア暗号化コンフィギュレーションガイドには新機能はありません。







## はじめに

ここでは、Cisco MDS 9000 ファミリ NX-OS ストレージメディア暗号化コンフィギュレーションガイドの対象読者、構成、および表記法について説明します。さらに、関連資料の入手方法についても説明します。

## 対象読者

このマニュアルは、Cisco MDS 9000 Family Storage Media Encryption (SME) アプリケーションの計画、インストール、設定、および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

## マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	ストレージメディア暗号化の概要	Cisco MDS SME 機能の概要と、ソフトウェア要件およびハードウェア要件を示します。
第 2 章	SME の設定	インストール、事前設定作業、設定の制限事項について説明します。
第 3 章	SME インターフェイスの設定	SME インターフェイスとスイッチの設定、開始、追加、および削除について説明します。
第 4 章	SME クラスタ管理の設定	SME クラスタを設定、監視、および管理する方法について説明します。
第 5 章	SME テープの設定	テープグループ、デバイス、パス、テープボリュームグループを追加および削除する方法について説明します。
第 6 章	SME ディスクの設定	SME を使用してディスクを管理および設定する方法について説明します。
第 7 章	SME キー管理の設定	包括的で安全なキー階層システムについて、ボリュームグループのエクスポートおよびインポート方法について説明します。
第 8 章	証明書のプロビジョニング	SME での SSL の設定について説明します。

章	タイトル	説明
第 9 章	RSA キーマネージャと SME	SME と連携するように RSA キーマネージャをセットアップする手順について説明します。
第 10 章	SME ベスト プラクティス	SME の適正な動作を確認するための推奨手順について説明します。
第 11 章	SME のトラブルシューティング	SME の問題を解決するために使用する基本的なトラブルシューティング方法について説明します。
付録 A	SME CLI コマンド	Cisco MDS SME CLI コマンドの構文と使用に関するガイドラインが含まれています。
付録 B	SME のオフラインデータリカバリ	オフラインデータ復元ツール(ODRT)について説明します。
付録 C	データベースのバックアップと復元	DCNM-SAN Server データベースのバックアップと復元の方法について説明します。
付録 D	SME インストールの計画	正常な SME インストールを確認するための手順とガイドラインについて説明します。
付録 E	SME データベース テーブルの移行	SME データベース テーブルの移行用のユーティリティについて説明します。

## 表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[ x   y   z ]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

出力例では、次の表記法を使用しています。

screen フォント	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ(<>)で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



(注)

「注釈」を意味します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

## 関連資料

Cisco MDS 9000 ファミリのマニュアルセットには次のマニュアルが含まれます。オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

[http://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/roadmaps/doclocator.htm](http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm)

## リリースノート

- 『Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases』
- 『Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases』
- 『Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images』
- 『Cisco DCNM Release Notes』

## 準拠規格および安全性情報

- 『Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family』

## 互換性に関する情報

- 『Cisco Data Center Interoperability Support Matrix』
- 『Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists』
- 『Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide』

## ハードウェアの設置

- 『Cisco MDS 9500 Series Hardware Installation Guide』
- 『Cisco MDS 9200 Series Hardware Installation Guide』
- 『Cisco MDS 9100 Series Hardware Installation Guide』
- 『Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide』

## ソフトウェアのインストールおよびアップグレード

- 『Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide』

## Cisco NX-OS

- 『Cisco MDS 9000 Family NX-OS Licensing Guide』
- 『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Fabric Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Security Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide』
- 『Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide』
- 『Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS』

## Cisco DCNM

- 『Cisco DCNM Fundamentals Guide, Release 6.x』
- 『Cisco DCNM Installation and Licensing Guide, Release 6.x』

## Cisco DCNM-SAN

- 『System Management Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Interfaces Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Fabric Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Security Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『IP Services Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 6.x』
- 『SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 6.x』

## コマンドラインインターフェイス

- 『Cisco MDS 9000 Family Command Reference』

## インテリジェントストレージネットワークング サービス コンフィギュレーションガイド

- 『Cisco MDS 9000 Family I/O Acceleration Configuration Guide』
- 『Cisco MDS 9000 Family SANTap Deployment Guide』
- 『Cisco MDS 9000 Family Data Mobility Manager Configuration Guide』
- 『Cisco MDS 9000 Family Storage Media Encryption Configuration Guide』

## トラブルシューティングおよび参考資料

- 『Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference』
- 『Cisco MDS 9000 Family SAN-OS Troubleshooting Guide』
- 『Cisco MDS 9000 Family NX-OS MIB Quick Reference』
- 『Cisco DCNM for SAN Database Schema Reference』

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

- 『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。





# ストレージメディア暗号化の概要

データセンターのストレージメディアを暗号化することは、重大な問題となっています。テープおよびディスク デバイスの紛失や盗難という世間の注目を集める事件が多数発生していますが、これは機密情報が悪者の手に渡ったときに企業はリスクや暴露に直面するという事実を強く示しています。厳しさを増す要件を満たすため、Cisco MDS 9000 ファミリー スイッチ向けの Cisco MDS 9000 ファミリー ストレージメディア暗号化(SME)は、ファイバチャネル SAN のファブリック サービスとして暗号化を透過的に統合できるスケーラブルで信頼性の高い柔軟なソリューションを提供します。

この章では、SME の概要、および SME のハードウェアとソフトウェアの要件について説明します。ここで説明する内容は、次のとおりです。

- [SME について\(1-1 ページ\)](#)
- [MIB について\(1-10 ページ\)](#)
- [ソフトウェアおよびハードウェアの要件\(1-11 ページ\)](#)
- [SME の前提条件\(1-14 ページ\)](#)
- [SME のセキュリティの概要\(1-15 ページ\)](#)

## SME について

SME ソリューションは、既存および新しい SAN と透過的に連携するエンタープライズクラスのキー管理を利用した包括的なネットワーク統合型暗号化サービスです。シスコの革新的なネットワーク統合型ソリューションには、今日利用可能な競合ソリューションに比べて多くの利点があります。

- SME のインストールとプロビジョニングは、シンプルで、運用が中断されることはありません。その他のソリューションとは異なり、SME は再配線や SAN の再設定が不要です。
- 暗号化エンジンは Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)、Cisco MDS 9222i マルチサービス モジュラ スイッチ、および 16 ポート ギガビット イーサネット ストレージ サービス ノード(SSN-16)に統合されているため、余分なスイッチ ポート、ケーブル、アプライアンスを購入および管理する必要がありません。
- 仮想 SAN (VSAN)からのトラフィックは、SME を使用して暗号化できるため、複数の SAN に渡るネットワーク トラフィック管理を利用した柔軟で自動化されたロード バランシングを実現します。
- プロビジョニング、キー、およびユーザ ロール管理に追加のソフトウェアは必要はありません。SME は Cisco DCNM for SAN (DCNM-SAN)に統合されているため、運用コストを削減できます。

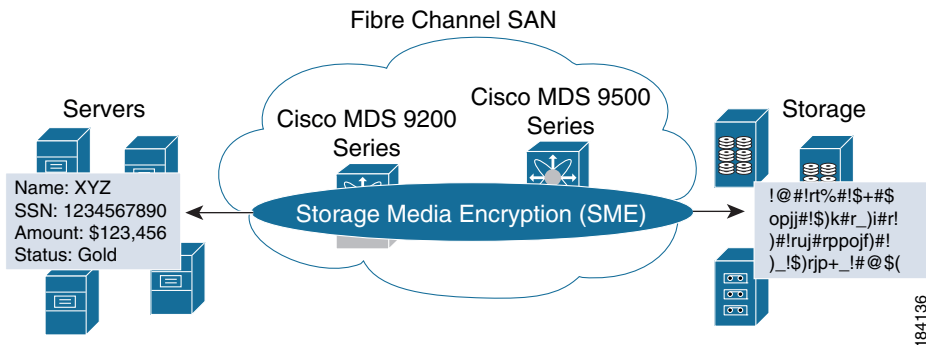


(注)

SME を使用するときは、SSI イメージを 18+4 カードや SSN-16 にロードおよびインストールしないでください。また、イメージをロードするように bootvar を設定しないでください。

図 1-1 に、データ暗号化をシームレスに管理するための SME と SAN ファブリックの統合を示します。

図 1-1 SME



この項では、次のトピックについて取り上げます。

- [SME の機能 \(1-2 ページ\)](#)
- [SME の用語 \(1-7 ページ\)](#)
- [サポートされるトポロジー \(1-8 ページ\)](#)
- [SME の In-Service Software Upgrade \(1-10 ページ\)](#)

## SME の機能

インテリジェントなディレクタでファブリック スイッチである Cisco MDS 9000 ファミリでは、インテリジェントなファブリック アプリケーションおよびサービスをホストするためのオープンで各種の標準規格に準拠したプラットフォームを提供します。プラットフォームとしての Cisco MDS 9000 ファミリ スイッチは、安全で可用性の高いエンタープライズクラスのファイバチャネルストレージエリアネットワーク (SAN) ファブリック サービスを提供するために必要となる不可欠な機能をすべて提供します。シスコは、このプラットフォームを最大限に活用できるように、保管中のデータの暗号化を透過的なファブリック サービスとして統合しました。

SME は、異種のディスク、テープ ライブラリ、および仮想テープ ライブラリのための、各種の標準規格に準拠した暗号化ソリューションです。SME は、Cisco DCNM-SAN およびコマンドライン インターフェイス (CLI) を使用して管理され、SAN 管理およびセキュリティ プロビジョニングを統合します。SME は、次の包括的な組み込みキー管理機能を備えています。

- [透過的なファブリック サービス \(1-3 ページ\)](#)
- [暗号化 \(1-3 ページ\)](#)
- [SME のロール \(1-3 ページ\)](#)
- [キーの管理 \(1-4 ページ\)](#)
- [クラスタリング \(1-6 ページ\)](#)



- [FC-Redirect \(1-6 ページ\)](#)
- [ディスクおよびテープをプロビジョニングするためのサーバベースの検出 \(1-6 ページ\)](#)
- [ターゲットベースのロードバランシング \(1-6 ページ\)](#)

## 透過的なファブリック サービス

シスコはファイバチャネルリダイレクトスキームを採用しています。これは、ファブリック内の任意の場所にある MSM-18/4 モジュール、MDS 9222i スイッチ、または SSN-16 モジュールヘトトラフィックフローを自動的にリダイレクトします。データパス内にインラインのアプライアンスはなく、SAN の再配線や再設定はありません。

## 暗号化

SME は強力な IEEE 準拠の AES 256 暗号化アルゴリズムを使用して、保管中のデータを保護します。セキュアシェル (SSH)、セキュアソケットレイヤ (SSL)、RADIUS、ファイバチャネルセキュリティプロトコル (FC-SP) など、Cisco MDS 9000 SAN-OS および NX-OS ソフトウェアの高度なセキュリティ機能は、安全なアーキテクチャに必要な基礎を提供します。

SME は NIST 承認取得済みの乱数標準規格を使用して、暗号化のキーを生成します。

暗号化サービスと圧縮サービスはホストとストレージデバイスに対して透過的です。

## 暗号化アルゴリズム

ディスクドライブの暗号化用の IEEE 承認取得済み標準規格は、IEEE 1619 (暗号化された共有ストレージメディア向け標準アーキテクチャ) です (1619.1 はテープドライブ用)。これはディスクの暗号化で一般に使用される XTS 暗号化モードを指定します。IEEE Security in Storage Working Group (SISWG) は、FIPS 140-2 認定を受けるために Approved Mode of Operation として検討するよう XTS モードを NIST に提出する可能性を調査していました。ナローブロック暗号化アルゴリズムを使用していますが、ワイドブロックアルゴリズムの標準化プロセスは 1619.2 として現在進行中です。検討すべきその他の暗号化アルゴリズムは、LRW-AES と AES-CBS です。IEEE 1619 標準規格のドラフト版では、XTS-AES に取って代わった LRW-AES を使用していました。

## SME のロール

SME サービスには次の 4 つの設定およびセキュリティロールが含まれています。

- SME Administrator
- SME Storage Administrator
- SME Key Management Center (KMC) Administrator
- SME Recovery Officer

SME Administrator は、SME を設定および管理します。このロールは、複数のストレージネットワーク管理者に設定できます。SME Storage Administrator は SME のプロビジョニング操作を担当し、SME KMC Administrator は SME KMC 管理操作を担当します。一部のシナリオでは、セキュリティ担当者に SME KMC Administrator ロールが割り当てられることがあります。



(注) SME Administrator ロールには、SME Storage Administrator と SME KMC Administrator というロールが含まれます。

SME リカバリ責任者はキー リカバリ操作を担当します。SME の設定中に、さらにリカバリ責任者を追加できます。SME リカバリ責任者は、非アクティブ化されたクラスタのキー データベースを回復する際に重要な役割を果たしており、マスター キーを保護する責任を負います。SME リカバリ責任者のロールは、マスター キーの管理と SME の管理および操作とを分離します。組織によっては、セキュリティ担当者がこのロールに割り当てられることがあります。

Advanced セキュリティ レベルでは、リカバリ手順を実行するために SME リカバリ責任者のクォーラムが必要です。デフォルトは 5 人中 2 人です。この場合、マスター キーをロック解除するために 5 人のリカバリ責任者のうち 2 人が必要です。

SME Administrator および SME Recovery Officer ロールの詳細については、「[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。

## キーの管理

Cisco Key Management Center(KMC)は、キーのアーカイブ、安全なエクスポートとインポート、およびキーの分割などの重要な機能を提供します。

以下のキー管理機能がサポートされます。

- マスター キーは、パスワード保護されたファイル、またはスマート カード内に存在します。
  - クラスタ セキュリティ モードが **Basic** に設定されている場合、マスター キーはパスワード保護されたファイル内に存在します。
  - クラスタ セキュリティ モードが **Standard** に設定されている場合、マスター キーはスマート カード 1 つのみに存在します。マスター キーを回復するには、同じスマート カードが必要です。
  - クラスタ セキュリティ モードが **Advanced** に設定されている場合、マスター キーは複数のスマート カードに存在します。マスター キーを回復するには、ユーザ選択に基づきスマート カードのクォーラム(3 のうち 2、5 のうち 2、または 5 のうち 3)が必要です。
- SME テープ クラスタに対してテープごとに一意のキー。
- SME ディスク クラスタに対して LUN ごとに一意のキー。
- キーは、FIPS 境界内でクリア テキストとしてのみ存在します。
- テープ キーと中間キーは、マスター キーでラップされ、CKMC で非アクティブ化されています。
- ディスク キーは、マスター キーでラップされ、CKMC で非アクティブ化されています。
- テープ メディアにテープ キーを保存するオプションがあります。

以下の一元的なキー ライフサイクル管理があります。

- メディア キーのアーカイブ、分割、回復、配布。
  - DCNM-SAN への統合。
  - キーの安全な転送。
- HTTPS/SSL/SSH を使用したエンドツーエンドのキー管理。
  - アクセス制御およびアカウンティング。
  - 既存の AAA 機能の使用。

Cisco KMC は SME に専用のキー管理を提供し、単一導入およびマルチサイト導入をサポートします。Cisco KMC は、キー管理操作を実行します。

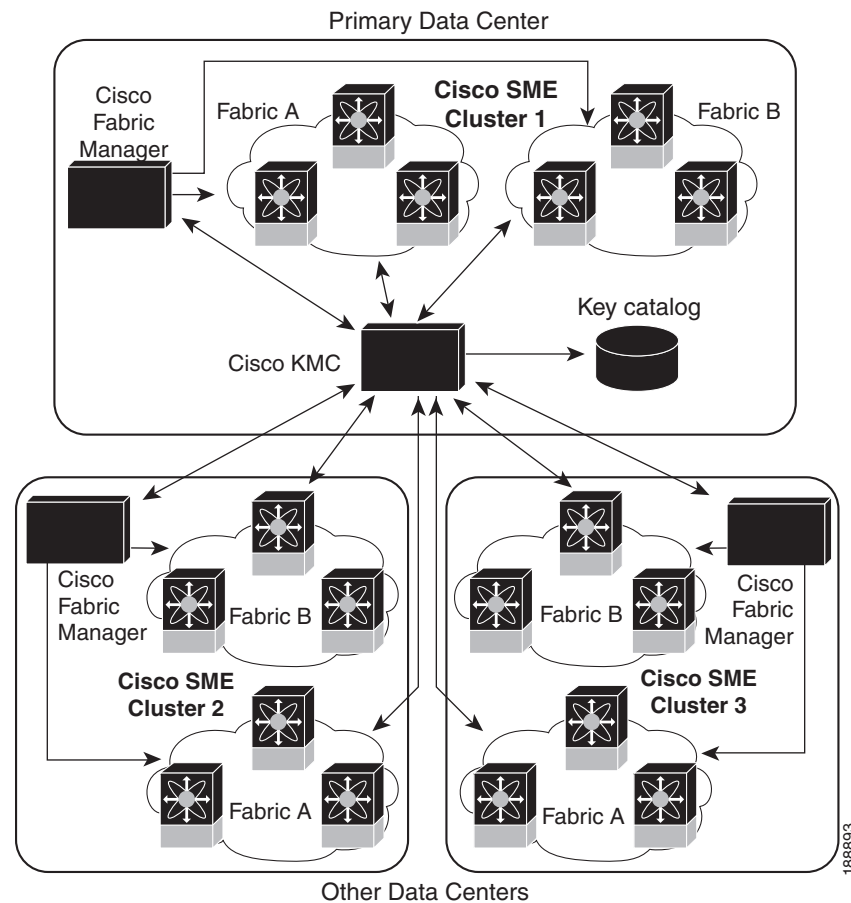
Cisco KMC は導入要件に従って DCNM-SAN に統合または分離されます。

単一サイト操作は、DCNM-SAN に Cisco KMC を統合することで管理できます。マルチサイト導入では、一元的な Cisco KMC をファブリック管理に使用されるローカル DCNM-SAN サーバと連携して使用できます。このような分離によって、KMC の堅牢性を実現し、同じ Cisco KMC を共有する別の場所における SME の導入をサポートします。

図 1-2 に、マルチサイト導入で Cisco KMC を DCNM-SAN から分離する方法を示します。

Cisco KMC はプライマリ データセンターでのみ設定し、DCNM-SAN サーバはすべてのデータセンターに設置して、ローカル ファブリックの管理と SME のプロビジョニングを実行します。SME のプロビジョニングはデータセンターごとに実行し、各データセンターのテープ デバイスとバックアップ グループは個別に管理します。

図 1-2 Cisco KMC のマルチサイト セットアップ



マルチサイト導入で Cisco KMC が DCNM-SAN から分離されると、Cisco KMC のインストール時にファブリック検出が必要ありません。Cisco KMC に接続しているクラスタはオンラインになり、接続されていないものの非アクティブではないクラスタはオフラインとして認識されます。ファブリックから削除された SME クラスタは、非アクティブとして認識されます。

ハイアベイラビリティ Cisco KMC サーバは、プライマリ サーバとセカンダリ サーバで構成されます。プライマリ サーバが使用できないとき、クラスタはセカンダリ サーバに接続し、プライマリ サーバが使用可能になるとプライマリ サーバにフェールオーバーします。ハイアベイラビリティ KMC は、DCNM-SAN Web クライアントで高可用性設定を設定すると使用できるようになります。

## クラスタリング

クラスタ技術は、信頼性、可用性、自動ロード バランシング、フェールオーバー機能、およびシングルポイント管理を提供します。

## FC-Redirect

Cisco MDS 9000 ファミリ スイッチまたはモジュールを追加するだけで SME のパフォーマンスを簡単に拡張できます。Cisco MDS 9000 NX-OS の革新的なファイバチャネルリダイレクト機能は、SAN の再設定や再配線を行わなくても、すべてのスイッチ ポートからのトラフィックを暗号化できます。

## ディスクおよびテープをプロビジョニングするためのサーバベースの検出

SME は、セッションの確立時にホストのアイデンティティを使用してバックエンド ターゲットを検出できます。

## ターゲット ベースのロード バランシング

SME クラスタは、SME アプリケーションを実行する一連のスイッチ(デュアル ファブリック環境の場合)で構成されています。クラスタリングによって、SME アプリケーション サービスをターゲット ベースでロード バランシングできます。クラスタ インフラストラクチャを使用することで、SME アプリケーションは一貫性および高可用性を維持するための通信および調整が可能になります。

ロード バランシングは、クラスタ全体でさまざまなメタデータ オブジェクトの所有権を分散することにより実現されます。SME は次のアルゴリズムを使用して、使用可能な SME インターフェイスにホストを割り当てます。

- 特定のターゲット ポートに対するすべてのホストは、常に同じ SME インターフェイスに割り当てられます。
- ターゲット ポートが SME スイッチの 1 つに接続されている場合は、ターゲットが接続しているスイッチからの負荷に基づいてインターフェイスが選択されます。つまり、ターゲットの SME インターフェイスを選択するときは、ターゲットの場所が考慮されます。
- ターゲットが SME インターフェイスのないスイッチに接続されている場合、ターゲットは SME クラスタで負荷が最も小さい利用可能なインターフェイスに割り当てられます。

ターゲット ベースのロード バランシングにおいて、インターフェイスの負荷とはそのインターフェイスに割り当てられているターゲットの数を意味します。



### 注意

SME にはロード バランシング CLI が用意されていて、クラスタ内で使用可能な SME インターフェイスに割り当てられているターゲットを再調整できます。ただし、**load balancing** コマンドは、トラフィックを中断します。このコマンドは、スケジュールされたダウンタイムに実行してください。そうしないと既存のトラフィックに影響を与えます。

## SME の用語

本書では次の SME 関連用語を使用します。

- **SME インターフェイス**:MSM-18/4 モジュール、または Cisco MDS 9222i ファブリック スイッチの固定スロットにおけるセキュリティ エンジン。各 MSM-18/4 モジュールおよび MDS 9222i スイッチは、セキュリティ エンジン を 1 つ搭載しています。
- **SME クラスタ**:SME 機能を提供するように設定された MDS スイッチのネットワーク。各スイッチは、1 つ以上の MSM-18/4 モジュールを搭載し、各モジュールはセキュリティ エンジン を搭載します。高可用性 (HA) とロード バランシングのために、1 つ以上のノードまたはスイッチを含みます。
- **ファブリック**:DCNM-SAN で認識される、SAN 内の物理ファブリック トポロジ。物理ファブリック内には複数の VSAN (論理ファブリック) が存在することがあります。
- **テープ グループ**:SAN のバックアップ環境。すべてのテープ バックアップ サーバ、およびテープ バックアップ サーバがアクセスするテープ ライブラリで構成されています。
- **テープ デバイス**:暗号化用に設定されているテープ ドライブ。
- **テープ ボリューム**:特定用途のために、バーコードで識別される物理テープ カートリッジ。
- **テープ ボリューム グループ**:特定用途のために設定されたテープ ボリュームの論理セット。たとえば、データベースをバックアップするために使用されるテープ ボリュームのグループ。
- **ディスク グループ**:ディスク グループを形成するために機能でグループ化されたディスク。
- **ディスク**:ディスクは LUN です。LUN とは、ストレージ コントローラによってホストにエクスポートされた論理ユニットです。
- **IT-Nexus**:ホストからターゲットへの接続を定義するイニシエータまたはターゲット pWWN。
- **SME ノード**:クラスタ内の各スイッチは SME ノードと呼ばれ、クラスタにクォーラムがあるかどうかを判断する役割を担います。
- **Cisco Key Management Center (CKMC)**:暗号化キーが保存されている DCNM-SAN のコンポーネント。
- **マスター キー**:SME クラスタの作成時に生成される暗号化キー。マスター キーはテープ ボリューム キーおよびテープ キーを暗号化します。暗号化されたデータを取得する際にこれらのキーを復号するために必要です。
- **メディア キー**:特定のテープ上にあるデータの暗号化と認証に使用されるキー。
- **ディスク キー**:特定のディスク上にあるデータの暗号化と認証に使用されるキー。
- **スマート カード**:認証に使用する組み込みマイクロプロセッサとメモリが搭載されたカード (ほぼクレジットカード サイズ)。
- **SME Administrator**:SME を設定する管理者。このロールには、SME 操作を管理するための Cisco Storage Administrator、および SME キー管理操作を担当するための SME KMC Administrator ロールが含まれます。
- **Storage Administrator**:SME 操作を管理する管理者。
- **SME KMC Administrator**:SME キー管理操作を担当する管理者。
- **SME リカバリ 責任者**:スマート カードおよび関連付けされた PIN を保持するデータ セキュリティ 担当者。各スマート カードにクラスタ マスター キーの共有が保存されます。リカバリ 責任者は、非アクティブ化されたクラスタのキー データベースを回復するために、カードと PIN を提示する必要があります。この操作を実行するには、リカバリ 責任者のクォーラムが必要です。

## サポートされるトポロジ

SME は、単一およびデュアル ファブリック トポロジをサポートします。Cisco MSM-18/4 モジュール、MDS 9222i スイッチ、および SSN-16 は、保管中のデータを暗号化および圧縮するために SME が使用する SME エンジンを提供します。複数のモジュールは、簡単にパフォーマンスを高め、単純化されたロード バランシングを有効にし、可用性を高めるため、ファイバ チャネル ファブリックで展開できます。通常の設定では、1 つの MSM-18/4 モジュールが各 SME クラスタが必要です。

SME クラスタには、指定のバックアップ サーバ、テープ ライブラリ、また Cisco SAN-OS リリース 3.2(2c)以降または NX-OS 4.x 以降が稼働する 1 つ以上の MDS スイッチが組み込まれています。1 つのクラスタ スイッチに MSM-18/4 モジュールが含まれている必要があります。使いやすいプロビジョニングでは、任意のホストとファブリックのテープ間のトラフィックは SME サービスを利用できます。

必須 SME エンジンには、次の Cisco 製品に含まれています。

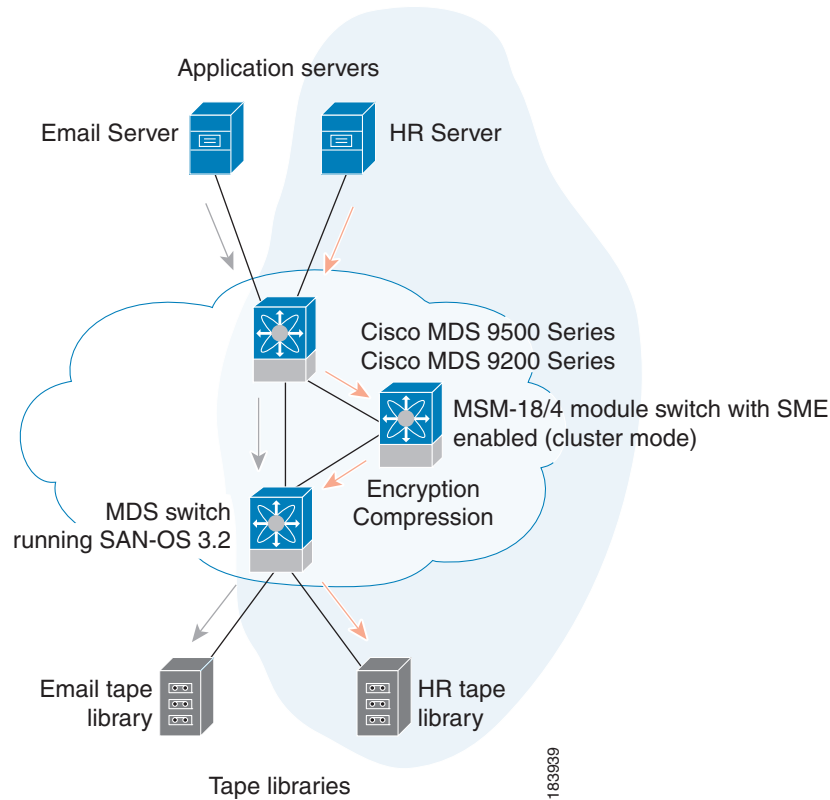
- Cisco MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール (MSM-18/4)
- Cisco MDS 9222i マルチサービス モジュラ スイッチ
- Cisco MDS 16 ポート ストレージ サービス ノード (SSN-16)

## テープの場合の単一ファブリック トポロジ

図 1-3 は、HR サーバからのデータが Cisco MSM-18/4 モジュールに転送される単一ファブリック トポロジを示しています。Cisco MSM-18/4 モジュールはファブリックの任意の場所にあります。SME は、ホストからターゲットに情報を 1 対 1 にマッピングし、暗号化データを専用 HR テープに転送します。また SME は各暗号化テープのバーコードを追跡し、バーコードをホストサーバに関連付けます。

図 1-3 は、HR サーバからの暗号化されたデータが圧縮されて HR テープ ライブラリに保存される様子を示しています。電子メール サーバからのデータは、専用の電子メール テープ ライブラリにバックアップされる場合は暗号化されません。

図 1-3 SME:単一ファブリック トポロジ



(注)

テープデバイスは、Cisco SAN-OS リリース 3.2(2c) 以降または Cisco NX-OS リリース 4.x 以降が稼働する MDS 9500 シリーズ スイッチや MDS 9222i スイッチなどのコア スイッチに接続してください。また、Cisco NX-OS 6.2(3) 以降が稼働している MDS 9710 シリーズ スイッチに接続することができ、またそのようにする必要があります。

暗号化サービスと圧縮サービスはホストとストレージ デバイスに対して透過的です。これらのサービスは、物理ファブリック内の仮想 SAN (VSAN) のデバイスに使用でき、再分割せずに使用できます。

## ディスクの場合の単一ファブリック トポロジ

HR サーバからのデータが Cisco MSM-18/4 モジュール、Cisco MDS 9222i スイッチ、または SSN-16 モジュールに転送される単一ファブリック トポロジ。Cisco MSM-18/4 モジュール、Cisco MDS 9222i スイッチ、または SSN-16 モジュールは、ファブリック内のどこにでも配置できます。SME は、ホストからターゲットに情報を 1 対 1 にマッピングし、暗号化データを専用 HR ディスクに転送します。



(注)

SME ディスクは、データをすべてのパスで暗号化できるデュアル ファブリック トポロジもサポートします。ディスク デバイスは、Cisco NX-OS リリース 5.2(1) 以降が稼働する MDS 9500 シリーズ スイッチや MDS 9222i スイッチなどのコア スイッチに接続してください。

暗号化はホストとストレージ デバイスに対して透過的です。これらのサービスは、物理ファブリック内の仮想 SAN (VSAN) のデバイスに使用でき、再分割せずに使用できます。

## SME の In-Service Software Upgrade

In-Service Software Upgrade (ISSU) は、トラフィックを中断せずに、新機能やサービスを追加する包括的で透過的なソフトウェア アップグレード機能です。

MDS 9222i スイッチをノードとして構成しているクラスタでは、ノードが通信できないと、最も低いノード ID (ノード ID) を持つノードがクラスタ内に残り、他のクラスタ ノードはクラスタから退出します。ただし、ISSU が最も低いノード ID を持つノードで実行されると、両方のノードがクラスタから退出するためにクラスタが完全に失われます。

この望ましくない状況は 2 ノード クラスタで次のように対処しています。

- アップグレード ノードがクラスタから退出しようとしている他のノードにメッセージを送信します。アップグレード ノードはマスター ノードまたはスレーブ ノードのいずれかです。
- 残りのノードはクラスタに残り、スレーブ ノードだった場合はマスター ノードの役割を果たします。このノードは、そのままの状態でもォーラムを備えたクラスタ内に残ります。
- ISSU が完了し、スイッチがブートすると、アップグレード済みのノードはスレーブ ノードとしてクラスタに再接続します。

SME ディスクには、ディスク固有の ISSU の制約事項と制限事項があります。この制約事項の詳細については、第 6 章「SME ディスクの設定」を参照してください。



(注)

この機能は ISSU のロジックの内部に結び付けられているため、このために追加コマンドを実行する必要はありません。

## MIB について

MIB モジュールは SME サービスを管理します。SME は、ストレージ デバイスのラインカード上に存在する暗号化ノードが提供する暗号化サービスです。これはホストからクリア テキストのデータを受信して暗号化し、テープまたはディスクに書き込まれるように送信します。逆方向に実行すると反転されるため、サービスはホストに対して完全に透過的です。このサービスは、テープまたはディスクの紛失時や盗難時のデータ セキュリティを高めることが目的です。

重要な他のサービスと同様に、ある程度の耐障害性を正常な方法で提供することをユーザは必要としています。SME は、暗号化ノードをクラスタへとグループ化できるようにすることで耐障害性を提供します。同じクラスタ内のノードは、障害が発生したノードの処理をただちに引き継ぐため、ユーザはサービスの中断を意識しません。



# ソフトウェアおよびハードウェアの要件

この項では、次のトピックについて取り上げます。

- [ソフトウェア要件\(1-11 ページ\)](#)
- [ハードウェア要件\(1-11 ページ\)](#)

## ソフトウェア要件

SME クラスタ内のすべての MDS スイッチは、Cisco SAN-OS リリース 3.2(2c) 以降の現在のリリース、または SME テープの場合は Cisco NX-OS 4.x 以降のソフトウェアを実行している必要があります。SME ディスクの場合は Cisco NX-OS リリース 5.2(1) 以降のソフトウェアが必要です。ソフトウェア要件には次の内容が含まれます。

- DCNM-SAN は、Cisco SAN-OS リリース 3.2(2c) 以降、または SME テープの場合は Cisco NX-OS 4.x 以降を実行している必要があります。
- テープデバイスに接続されている Cisco MDS スイッチは、Cisco SAN-OS リリース 3.2(2c) 以降または Cisco NX-OS リリース 4.x 以降を実行している必要があります。また、Cisco NX-OS 6.2(3) 以降が稼働している MDS 9710 シリーズ スイッチに接続されている必要があります。
- MSM-18/4 モジュールを搭載するすべてのスイッチは、Cisco SAN-OS リリース 3.2(2c) 以降、または SME テープの場合は Cisco NX-OS 4.x 以降のソフトウェアを実行している必要があります。
- SME ディスクの場合、DCNM-SAN は Cisco NX-OS リリース 5.2(1) を実行している必要があります。
- ディスクに対してイネーブルになっている SME クラスタ内のすべての Cisco MDS スイッチは、Cisco NX-OS リリース 5.2(1) を実行している必要があります。
- SME ディスクの場合、MSM-18/4 モジュール、MDS 9222i スイッチ、または SSN-16 モジュールを搭載するすべてのスイッチは、Cisco NX-OS リリース 5.2(1) を実行している必要があります。

## ハードウェア要件

SME は、各クラスタに少なくとも 1 つの暗号化サービス エンジンが必要です。必須モジュール上の SME エンジンは、ホストとストレージデバイスに対して透過的な暗号化および圧縮サービスを提供します。Standard および Advanced セキュリティ レベルを最大限に活用するには、スマートカードリーダーが必要です。

必須ハードウェアの詳細と必須ハードウェアをインストールする方法については、それぞれのインストール ガイドを参照してください。ハードウェアの発注については、<http://www.cisco.com/en/US/ordering/index.shtml> を参照してください。

ここでは、次の必須ハードウェアについて説明します。

- [MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール\(1-12 ページ\)](#)
- [Cisco MDS 9222i マルチサービス モジュラ スイッチ\(1-12 ページ\)](#)
- [Cisco MDS 16 ポート ストレージ サービス ノード\(1-13 ページ\)](#)
- [FC-Redirect 対応 スイッチ\(1-13 ページ\)](#)
- [スマートカードリーダー\(1-14 ページ\)](#)

## MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール

Cisco MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール (MSM-18/4) は、18 個自動検知 1、2、および 4 Gbps ファイバチャネルポートと、4 つのギガビットイーサネット IP サービスポートを提供します。MSM-18/4 モジュールは、ファイバチャネル、Fibre Channel over IP (FCIP)、Small Computer System Interface over IP (iSCSI)、IBM Fiber Connectivity (FICON)、FICON Control Unit Port (CUP) などのマルチプロトコル機能を提供します。

MSM-18/4 モジュールは、高性能な SAN およびメインフレーム接続用に 18 個の 4 Gbps ファイバチャネルインターフェイス、および FCIP および iSCSI ストレージサービス用に 4 つのギガビットイーサネットポートを提供します。個々のポートは、ホットスワップ可能な短波長、長波長、超長距離、低密度波長分割多重 (CWDM)、または高密度波長分割多重 (DWDM) 小型フォームファクタ (SFP) を使用して設定でき、最大 125 マイル (200 km) の接続に対応します。

MSM-18/4 モジュールは、FCIP 書き込みアクセラレーションおよび FCIP テープ読み書きアクセラレーションによって、ディスクおよびテープの遅延を最小限に抑えることができます。

MSM-18/4 モジュールは、トンネリングすることで、4 つの 1 ギガビットイーサネットポートで最大 16 の仮想 Inter-Switch Link (ISL) を実現し、1 つのファイバチャネルポートに割り当てることができる最大 4095 個のバッファツープバッファクレジットを提供します。

MSM-18/4 は統合された Call Home 機能によって、インテリジェントな診断、プロトコル復号化、およびネットワーク分析のツールを提供します。



(注)

Cisco SAN-OS リリース 3.2(2c) 以降または Cisco NX-OS リリース 4.x 以降を実行する Cisco MDS 9000 シリーズスイッチは、SME テープ用に MSM-18/4 モジュールをサポートしています。

Cisco NX-OS リリース 5.2(1) を実行する Cisco MDS 9000 シリーズスイッチは、SME ディスク用に MSM-18/4 および SSN-16 モジュールをサポートしています。

詳細については、『Cisco MDS 9500 Series Hardware Installation Guide』を参照してください。

## Cisco MDS 9222i マルチサービス モジュラ スイッチ

Cisco MDS 9222i マルチサービス モジュラ スイッチは、Cisco MDS 9222i スイッチの制御および管理機能を提供する統合スーパーバイザ モジュール (スロット 1) が含まれています。また、18 ポートファイバチャネルスイッチングおよび 4 ポートギガビットイーサネット IP サービスモジュールを提供します。Cisco MDS 9222i の組み込みスーパーバイザモジュールは、シングルポイント障害を回避するために、複数の通信および制御パスを提供します。Cisco MDS 9222i スーパーバイザモジュールは PowerPC PowerQUICC III クラスプロセッサ、1 GB の DRAM、およびソフトウェアイメージ用に 1 GB を提供する内蔵 CompactFlash カードが搭載されています。

Cisco MDS 9222i スイッチは、Cisco MDS 9000 ファミリースイッチングおよびサービスモジュールをホストするためのモジュラ拡張スロットを備えています。詳細については、『Cisco MDS 9200 Series Hardware Installation Guide』を参照してください。



(注)

Cisco MDS 9222i スイッチは、Cisco SAN-OS リリース 3.2(2c) 以降、または SME テープの場合は Cisco NX-OS 4.x 以降を実行している必要があります。

Cisco MDS 9222i スイッチは、SME ディスク用に Cisco NX-OS リリース 5.2(1) が必要です。

## Cisco MDS 16 ポートストレージサービス ノード

Cisco MDS 9000 ファミリー 16 ポートストレージサービス ノード(SSN-16)は、4つの独立したサービス エンジンがあります。これらは個別に段階的にイネーブルにできるため、ビジネス ニーズの拡大に応じて拡張できます。SSN-16 設定は、Cisco MDS 9000 ファミリー 18/4 ポート マルチサービス モジュールの単一サービス エンジンに基づいており、4対1の統合によって、ハードウェアを節約し、MDS 9500 シリーズ シャーシ内のスロットを解放します。

SSN-16 は Cisco MDS 9500 シリーズ マルチレイヤ ディレクタおよび Cisco MDS 9222i マルチサービス モジュラ スイッチをシームレスに統合します。4つのサービス エンジン、それぞれが4つのギガビットイーサネット IP ストレージ サービス ポートをサポートするため、Fibre Channel over IP (FCIP) 接続のポートは合計で 16 個になります。トラフィックは、Cisco MDS 9000 ファミリー スイッチの IP ポートと任意のファイバチャネル ポートの間で切り替えることができます。

SSN-16 は、その他の Cisco MDS 9000 ファミリー モジュールで利用可能なサービス (VSAN、セキュリティ、トラフィック管理など) をすべてサポートします。I/O アクセラレータ (IOA)、SME ディスク、SME テープ、FCIP などの機能は、単一 SSN-16 モジュール内の異なる octeon で設定できます。

4つのアプリケーションを1つのモジュールで同時に実行することで、SSN-16 は次の機能を提供します。

- ミッションクリティカルなアプリケーションに、より優れたディザスタ リカバリおよび継続性のソリューションを提供します。
- 必要なデバイス数を最小化して、信頼性を向上します。
- 単一のモジュールを使用して管理を統合することで、エンドツーエンド ネットワークの可視性を提供します。
- ソリューション レベルでパフォーマンスの最適化を実現します。

SSN-16 モジュールはファブリック内の任意のポートに透過的なサービスを提供し、SAN の再設定や再配線を行う必要はありません。モジュールにはホストまたはターゲットが直接接続される必要はなく、マルチモジュールのクラスタリングおよびロードバランシングで利用できます。

SSN-16 モジュールは、モジュールあたり最大で4つの SME インターフェイスをサポートし、MSM-18/4 モジュールおよび 9222i スイッチと比べて高い拡張性と最大 20 パーセントのパフォーマンス向上を実現します。



(注) Cisco NX-OS リリース 4.2(1) 以降を実行している Cisco MDS 9500 シリーズ スイッチは、SSN-16 をサポートしています。

詳細については、『Cisco MDS 9500 Series Hardware Installation Guide』を参照してください。

## FC-Redirect 対応スイッチ



(注) Cisco MDS NX-OS Release 5.2(x) では、DMM、SME、または IOA を実行しているスイッチに FCoE モジュールをインストールできません。

Cisco MDS NX-OS Release 5.2(x) では、DMM、SME、または IOA を実行しているスイッチに FCoE モジュールをインストールできません。

SME では、各ターゲットスイッチが FC-Redirect に対応している必要があります。FC-Redirect は次のスイッチではサポートされていません。

- Cisco MDS 9120 スイッチ
- Cisco MDS 9140 スイッチ
- Cisco MDS 9124 スイッチ
- Cisco MDS 9134 スイッチ
- Cisco MDS 9020 スイッチ



(注) Cisco MDS NX-OS リリース 6.2(1) では、Cisco MDS 9710 スイッチで FC-Redirect がサポートされていません。ファイバチャネルリダイレクト (FCR) のサポートは、Cisco NX-OS 6.2(3) 以降が稼働している Cisco MDS 9710 シリーズスイッチで導入されました。



(注) SME は、MDS FCoE ラインカード (DS-X9708-K9) で接続されたデバイスなど、FCoE 接続のデバイスをサポートしていません。



(注) ディスクデバイス、テープデバイス、およびテープライブラリは、これらのエッジスイッチではサポートされていません。ディスクとテープはこれらのスイッチに接続できません。

## スマートカードリーダー

Standard および Advanced セキュリティ レベルを採用するには、SME に次のものがが必要です。

- SME 用スマートカードリーダー (DS-SCR-K9)
- SME 用スマートカード (DS-SC-K9)

スマートカードリーダーは、管理ワークステーションに接続される USB デバイスです。管理ワークステーションは SME クラスタを設定するために使用されます。スマートカードリーダーにはインストール CD に含まれるスマートカードドライバが必要です。リーダーが接続されている管理ワークステーションにインストールする必要があります。



(注) スマートカードリーダーは Windows プラットフォームのみでサポートされています。このサポートには、Windows 4 64 ビットおよび Windows XP 32 ビットプラットフォームのみが含まれます。

新しくインストールしたスマートカードドライバがスマートカードリーダーと効率的に連携するには、Microsoft のすべてのスマートカードサービスを停止する必要があります。

## SME の前提条件

このセクションでは、次の要件について説明します。

- [Java Cryptography Extension の要件 \(1-15 ページ\)](#)
- [ゾーン分割の要件 \(1-15 ページ\)](#)
- [FC-Redirect の要件 \(1-15 ページ\)](#)

## Java Cryptography Extension の要件

SME では、Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5C0 (JRE 1.5 用) が必要です。local\_policy.jar および US\_export\_policy.jar ファイルを抽出して <DCNM install path>\dcm\java\jre1.6\lib\security\ にコピーする必要があります。これらのファイルは DCNM-SAN のインストール CD から取得できます。



(注) DCNM のアップグレードを実行するたびにこれらの JCE ポリシー ファイルを手動でコピーする必要があります。DCNM のアップグレードでこれらのファイルは保持されません。

## ゾーン分割の要件

ゾーン分割には、デフォルトゾーン内の SME によって作成される内部の仮想 N ポートが必要です。デフォルトゾーンは deny に設定する必要があります。また、これらの仮想 N ポートは他のホストやターゲットでゾーン分割されていないようにする必要があります。

ゾーン分割の詳細については、『Fabric Configuration Guide, Cisco DCNM for SAN』および『Cisco MDS 9000 Family NX-OS Fabric Configuration Guide』を参照してください。

## FC-Redirect の要件

FC-Redirect の要件は、次のとおりです。

- MSM-18/4 モジュールを搭載する MDS スイッチ、または MDS 9222i スイッチは、Cisco MDS SAN-OS リリース 3.2(2c) 以降、または Cisco NX-OS リリース 4.x 以降を実行している必要があります。
- ターゲットは、Cisco SAN-OS リリース 3.2(2c) 以降または Cisco NX-OS リリース 4.x 以降が稼働する MDS 95XX、9216、または 9222i スイッチに接続されている必要があります。また、Cisco NX-OS 6.2(3) 以降が稼働している MDS 9710 シリーズ スイッチに接続する必要があります。
- MSM-18/4 モジュールあたり 32 のターゲットを FC リダイレクトできます。
- FC-Redirect された各ターゲットは、16 以下のホストにゾーン分割できます。
- CFS は FC-redirect のすべての必須スイッチで有効にしてください。
- SME サーバ、ディスク ターゲット、およびテープ デバイスは、IVR ゾーンセットの一部であってはなりません。
- Quality of Service (QoS)、論理ユニット番号 (LUN) ゾーニング、および読み取り専用 LUN などの高度なゾーン分割機能は、FC-Redirect のホストおよびターゲットには使用できません。

## SME のセキュリティの概要

SME は、ストレージ環境内のデータを透過的に暗号化および復号化します。ビジネスクリティカルなアプリケーションの速度低下や中断はありません。

SME テープでは、SME はマスター キー、テープ ボリューム キー、テープ キーを生成します。キーは階層に従って暗号化されます。つまり、マスター キーはテープ ボリューム キーとテープ キーを暗号化します。

SME ディスクでは、SME はマスター キーとディスク キーを生成します。キーは階層に従って暗号化されます。つまり、マスター キーはディスク キーを暗号化します。

キーは、バックアップとアーカイブのために Cisco KMC サーバのキー カタログにもコピーされます。最終的に非アクティブ キーはファブリックから削除されますが、Cisco KMC カタログ内には保持されます。そのキーが再度必要になった場合は、ファブリックの SME サービスによって Cisco KMC から自動的に取得できます。

必要に応じて、単一の Cisco KMC を複数ファブリック用に一元化されたキー リポジトリとして SME サービスで使用できます。複数の Cisco KMC サーバを備えた環境で異なるファブリックにテープ メディアを移動できるように、キー カタログのインポートおよびエクスポート機能も用意されています。保護を高めるために、バックアップ アプリケーションを使用してキー カタログをアーカイブできます。



(注) SME クラスタは、SME ディスク用または SME テープ用に設定できます。同じクラスタでテープ設定とディスク設定の両方は設定できません。1 つのクラスタは、いずれか一方の専用として設定できます。

## 追加のセキュリティ機能

Cisco NX-OS で提供される追加のセキュリティ機能によって、SME のソリューションは完成します。たとえば、RADIUS および TACACS+ サーバを使用して、SME 管理者に認証、認可、アカウントリング(AAA)を提供します。ルールベースのアクセス制御(RBAC)を使用して、SME の管理を承認済み管理者に制限できます。DCNM-SAN からクラスタ ノードへの通信が発生すると、セキュア シェル(SSHv2)プロトコルによってメッセージの整合性とプライバシーが提供されます。トラストポイント(SSL で保護された転送)を有効にするために、PKI 証明書を CKMC およびクラスタ ノードで設定できます。



## SME の設定

この章では、SME の設定、SME のインストール、および SME を設定する前に完了する必要がある事前作業に関する情報が含まれています。

この章では、次の事項について説明します。

- [SME の設定に関する情報 \(2-1 ページ\)](#)
- [SME 設定のライセンス要件 \(2-2 ページ\)](#)
- [SME 設定の前提条件 \(2-3 ページ\)](#)
- [注意事項および制約事項 \(2-4 ページ\)](#)
- [DCNM-SAN サーバのインストール \(2-7 ページ\)](#)
- [SME タスクの設定 \(2-15 ページ\)](#)
- [必要な設定タスク \(2-16 ページ\)](#)
- [SME 設定のフィールドの説明 \(2-22 ページ\)](#)
- [SME 設定の機能履歴 \(2-24 ページ\)](#)

## SME の設定に関する情報

SME の設定には、次に示す 2 つの設定管理ツールのいずれかを使用できます。

- [Cisco DCNM-SAN \(2-1 ページ\)](#)
- [コマンドライン インターフェイス \(2-2 ページ\)](#)

Web ブラウザを使用して SME を設定および管理するために、Cisco DCNM-SAN Web クライアントを使用できます。

## Cisco DCNM-SAN

Cisco DCNM-SAN は、Secure Simple Network Management Protocol version 3 (SNMPv3) をサポートする一連のネットワーク管理ツールです。Cisco DCNM-SAN には、次のアプリケーションが含まれています。

- DCNM-SAN Web クライアント: ネットワーク ファブリックをリアルタイムに表示するグラフィカル ユーザ インターフェイス (GUI) を備え、Cisco MDS 9000 ファミリのデバイスおよびサードパーティ製スイッチの設定を管理できます。



(注) SME 設定は、DCNM-SAN Web クライアントだけでサポートされています。

- DCNM-SAN: サーバにインストールされ、DCNM-SAN クライアントを実行する前に開始される必要があります。一度に 16 の DCNM-SAN クライアントからのアクセスに対応できます。
- Device Manager: 1 台のスイッチが 2 つのビューで表示されます。
  - Device View: スイッチ設定の表示が継続的にアップデートされ、1 つのスイッチの統計情報および設定情報にアクセスできます。
  - Summary View: スイッチのファイバ チャネルおよび IP 接続用のアクティブなインターフェイスおよびチャネルに関するリアルタイム パフォーマンス統計情報を表示できます。



(注) DCNM-SAN のインストール中に、`smeserver.properties` ファイルの `use_ip` フラグがデフォルトで `FALSE` に設定されます。IP アドレスを使用するように選択するには、DNS サーバをファブリック内のすべてのスイッチで設定するべきではなく、`smeserver.properties` ファイルの `use_ip` フラグを `TRUE` に設定する必要があります。

`smeserver.properties` ファイルは、`<fm install path>\dcm\fm\conf\` にあります。

`smeserver.properties` ファイルに変更を加えたら、DCNM-SAN ファイルを再起動する必要があります。

Cisco DCNM-SAN アプリケーションでは、ほとんどのスイッチ コンフィギュレーション コマンドについて、CLI の代わりに使用できます。

DCNM-SAN を使用した Cisco MDS スイッチ設定の詳細については、『*Cisco DCNM Fundamentals Guide*』を参照してください。

## コマンドラインインターフェイス

CLI を使用して、スイッチプロンプトにコマンドを入力し、**Enter** キーを押すと、そのコマンドが実行されます。CLI パーサーは、コマンドのヘルプ、コマンドの完了、およびバッファ履歴内の以前実行されたコマンドにアクセスできるようにするキーボード シーケンスを提供します。

## SME 設定のライセンス要件

SME 機能を使用するには、適切な SME ライセンスが必要です。ただし、ライセンス キーを指定しないで SME をイネーブルにすると、猶予期間カウンタが開始します。その後 120 日以内に、適切なライセンス キーをインストールするか、または SME をディセーブルにしてください。120 日の猶予期間の終了時に SME の有効なライセンス キーがスイッチにないと、自動的にディセーブルになります。



(注) DCNM-SAN のインストールは必要ですが、SME を使用するために DCNM-SAN のライセンスは必要ではありません。SME 対応で追加の DCNM-SAN 機能はデフォルトでイネーブルになっていないため、無償のパフォーマンス モニタリングなどの機能はありません。



SME 機能がアクティブかどうかを確認するには、`show license usage license-name` コマンドを使用します。

Cisco MDS 9000 SME パッケージは、暗号化エンジン単位でライセンスが供与されます。SAN ファブリックに必要なライセンスの総数は、Cisco MDS 9000 18/4-Port Multiservice Module の数、SME に使用する Cisco MDS 9222i スイッチの固定ポートの数、および Cisco MDS 9000 16 ポートストレージサービス ノード (SSN-16) の暗号化エンジンの数の合計に等しくなります。

SSN-16 モジュールの各インターフェイスは、個別にライセンス供与および価格設定されます。

表 2-1 に、使用可能な SME ライセンスを記載します。

表 2-1 SME ライセンス

部品番号	説明	適用可能な製品
M9500SME1MK9	MSM-18/4 モジュール用の SME パッケージ	MSM-18/4 モジュールが含まれる MDS 9500 シリーズ
M9200SME1MK9	MSM-18/4 モジュール用の SME パッケージ	MSM-18/4 モジュールが含まれる MDS 9200 シリーズ
M9200SME1FK9	固定スロット用の SME パッケージ	MDS 9222i スイッチのみ
M95SMESSNK9	SSN-16 モジュールの 1 つのサービス エンジン用の SME パッケージ、スペア	SSN-16 モジュールが含まれる MDS 9500 シリーズ
M92SMESSNK9	SSN-16 モジュールの 1 つのサービス エンジン用の SME パッケージ、スペア	SSN-16 モジュールが含まれる MDS 9200 シリーズ

次の表に、この機能のライセンス要件を示します。

ライセンス	ライセンスの説明
SME_FOR_IPS_184_PKG	MSM-18/4 モジュール用の SME パッケージをアクティベートします。 SSN-16 エンジン用の SME をアクティベートします。 Cisco MDS 9222i スイッチ用の SME をアクティベートします。
SME_FOR_SSN16_PKG	
SME_FOR_9222i_PKG	

SME ライセンスを取得してインストールするには、『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照してください。

## SME 設定の前提条件

この項では、次のトピックについて取り上げます。

- [SME のインストール要件 \(2-4 ページ\)](#)
- [FCIP 書き込みアクセラレーションおよびテープ アクセラレーションのトポロジ要件 \(2-4 ページ\)](#)

## SME のインストール要件

SME 設定には、次のインストール要件があります。

- Cisco MDS SAN-OS リリース 3.2(2c) 以降または Cisco NX-OS リリース 4.x 以降は、Cisco MDS 9222i スイッチ、または SME テープ用の MSM-18/4 モジュールを搭載する Cisco MDS 9000 ファミリー スイッチにインストールされている必要があります。
- Cisco NX-OS リリース 5.2(1) は、Cisco MDS 9222i スイッチ、または SME ディスク用の MSM-18/4 モジュールまたは SSN-16 モジュールを搭載する Cisco MDS 9000 ファミリー スイッチにインストールされている必要があります。
- Cisco DCNM-SAN は、一元的な MDS 管理サービスおよびパフォーマンス モニタリングを提供するために使用するサーバにインストールされている必要があります。Cisco Key Management Center (Cisco KMC) はこのサーバにあります。
- Web ブラウザを使用して SME を設定および管理するために、DCNM-SAN Web クライアントを使用できます。

SME に固有の DCNM-SAN サーバのインストールについては、[DCNM-SAN サーバのインストール\(2-7 ページ\)](#)を参照してください。

DCNM-SAN のインストールについては、『Cisco DCNM Installation and Licensing Guide』を参照してください。



注意

Cisco Key Management Center (CKMC) が DCNM-SAN の一部である場合、スイッチと DCNM-SAN を同時にアップグレードしないでください。

## FCIP 書き込みアクセラレーションおよびテープアクセラレーションのトポロジ要件

FCIP 書き込みアクセラレーションまたはテープアクセラレーション トポロジである SME ディスクおよび SME テープには、次の要件があります。

- イニシエータが FC-Redirect 非対応スイッチ上にある場合、SME スイッチは FCIP トンネルのターゲット側にある必要があります。
- イニシエータが FC-Redirect 対応スイッチ上にある場合、SME スイッチは FCIP トンネルのホスト側にある必要があります。

## 注意事項および制約事項

FC-Redirect の CFS 地域を設計するには、次の注意事項に従ってください。

- FC-Redirect の CFS 地域設定がすべての FC-Redirect 対応アプリケーションに適用できるようにします。アプリケーションには、SME、Cisco DMM、および今後のアプリケーションが含まれます。
- ホスト、ターゲット、およびアプリケーション スイッチ(クラスタの MSM-18/4 モジュールを備えたスイッチ)に接続されているすべての FC-Redirect 対応スイッチが同じ地域に設定されるようにします。

- ある地域に複数の SME クラスタがある場合、ターゲットは、1つのクラスタのみで SME 設定の一部になることができます。ターゲットを別のクラスタに変更するには、最初のクラスタの設定を削除してから、2番目のクラスタで設定を作成する必要があります。
- 地域内のすべてのスイッチは共通 VSAN が必要です。
- 既存の SME のインストールの場合に CFS 地域への移行手順については、「[FC-Redirect の CFS 地域の設定](#)」セクション (E-5 ページ) を参照してください。
- スイッチが地域に移動する、または地域から出るときに前の設定のすべてのインスタンスを削除します。

CFS 地域の設定については、「[FC-Redirect の CFS 地域の設定](#)」セクション (E-5 ページ) を参照してください。

表 2-2 は SME 設定と対応する制限値を示します。

表 2-2 SME テープ設定の制限

設定	制限
スイッチあたりのクラスタ数	1
クラスタ内のスイッチ数	4
ファブリック内の FC-Redirect 対応スイッチ数	10
クラスタ内のファブリック数	2
スイッチ内のモジュール数	11
クラスタ内の Cisco MSM-18/4 モジュール数	32
Initiator-Target-LUN (ITL) の数	1024
ターゲットの背後の LUN 数	32
クラスタ内のホストポートとターゲットポートの数	128
ターゲットあたりのホスト数	128
クラスタあたりのテープバックアップグループ数	4
テープバックアップグループ内のボリュームグループ数	32
テープボリュームグループ内のキー数	8000
ディスクグループ数	128
SME ディスク数 (LUN 数)	2000
Cisco Key Management Center (キー数)	32,000
FC-Redirect できるスイッチあたりのターゲット数	32

表 2-2 SME テープ設定の制限(続き)

設定	制限
SME インターフェイスあたりの IT 接続数(ソフトリミット)	256 (注) この制限を超えると、syslog メッセージが表示されます。クラスタ内でより多くの SME インターフェイスをプロビジョニングすることをお勧めします。 <sup>1</sup>
SME インターフェイスあたりの IT 接続数(ハードリミット)	512 (注) この制限を超えると、新しい IT 接続がその SME インターフェイスに割り当てられなくなり、重大な syslog が表示されます。 <sup>2</sup>

1. NX-OS リリース 4.2(1) 以降に適用されます。

2. NX-OS リリース 4.2(1) 以降に適用されます。

表 2-3 SME ディスク設定の制限

設定	クラスタあたり	スイッチあたり	暗号化ノードあたり
クラスタ数	該当なし	2	1
物理ファブリック数	2	該当なし	該当なし
スイッチ数	8	該当なし	該当なし
モジュール数(ラインカード数:SSN 16 または MSM-18/4 モジュール数)	該当なし	11	該当なし
Cisco SME インターフェイス数(暗号化に使用する暗号化ノード数)	32	32	該当なし
Initiator-Target-LUN(ITL)の数	2048	2048	512
ターゲットの背後の LUN 数	512	512	512
イニシエータポート数	128	該当なし	該当なし
ターゲットポート数	128	該当なし	該当なし
IT Nexus の最大数	128	該当なし	該当なし
LUN あたりのパス数(SME ディスクあたりの物理パス数)	8	8	8
ディスクグループ数	128	128	128
SME ディスク数(LUN 数)	2048	2048	512
Cisco Key Management Center(KMC)のキー数	32,000	32,000	32,000

表 2-3 SME ディスク設定の制限(続き)

設定	クラスタあたり	スイッチあたり	暗号化ノードあたり
同時データ準備の最大数(オフラインデータ準備数)	該当なし	該当なし	64
ディスク キー複製関係の総数	2048		

NA: 該当なし

## DCNM-SAN サーバのインストール

ここでは、SME 用に Cisco DCNM-SAN をインストールする方法について説明します。ここで説明するインストール手順は、Windows 用です。インストール手順は、サポートされているすべてのプラットフォームで類似しています。



(注)

既存の Cisco DCNM または Fabric Manager インストールがある場合は、Cisco DCNM のアップグレード手順とアップグレードパスに従ってください。Cisco DCNM をアップグレードする詳細については、『Cisco DCNM Installation and Licensing Guide, Release 6.x』を参照してください。

SME 用に既存の DCNM/FM インストールがある場合は、DCNM のアップグレードガイドに従い、記載されている DCNM アップグレードパスに従ってください。詳細については、DCNM のインストール/構成ガイドを参照してください。

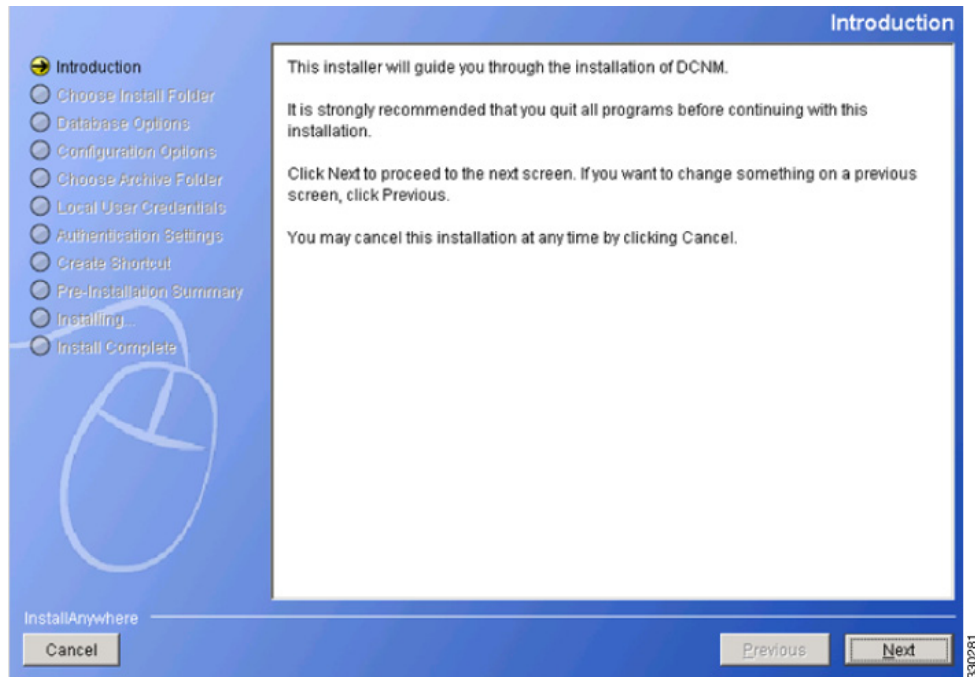
### ステップ 1

インストーラをダブルクリックします。

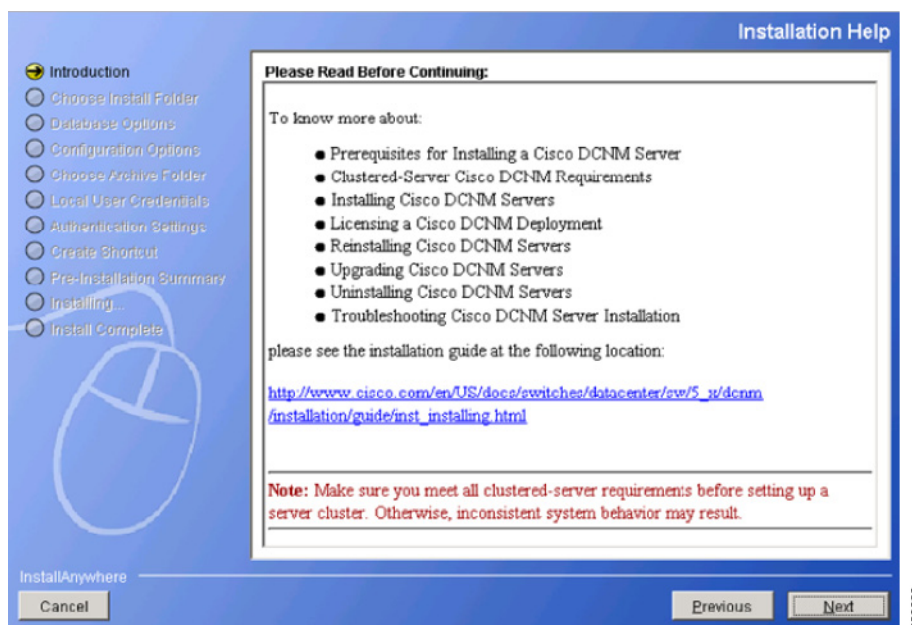
ファイルの抽出が開始します。完了したら、セットアップの進行状況を示す [Data Center Network Manager] 画面が表示されます。



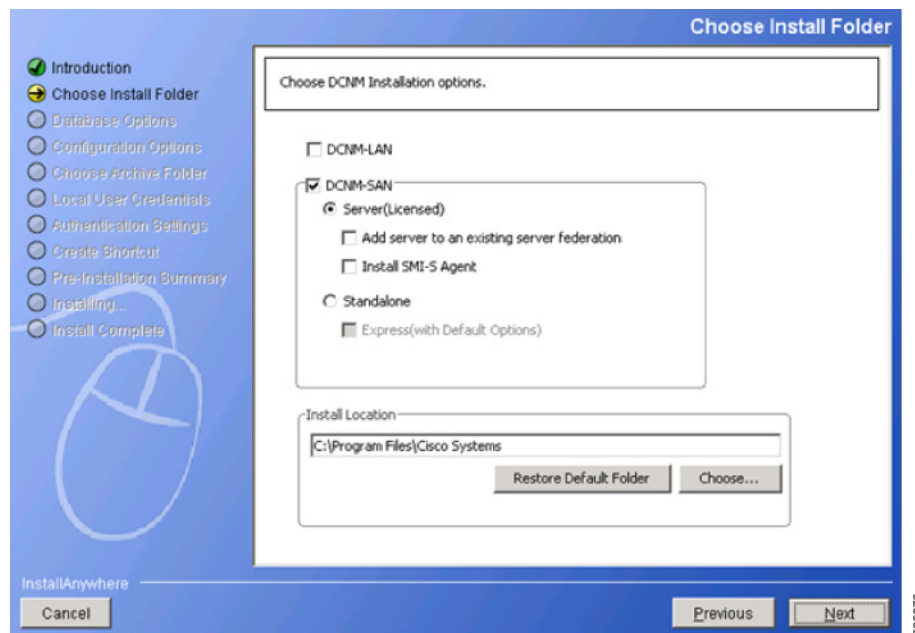
DCNM セットアップ プロセスが完了すると、DCNM インストール ウィザードの [Introduction] 画面が表示されます。



ステップ 2 [Next] をクリックします。[Installation Help] 画面が表示されます。



ステップ 3 [Next] をクリックします。[Choose Install Folder] 画面が表示されます。

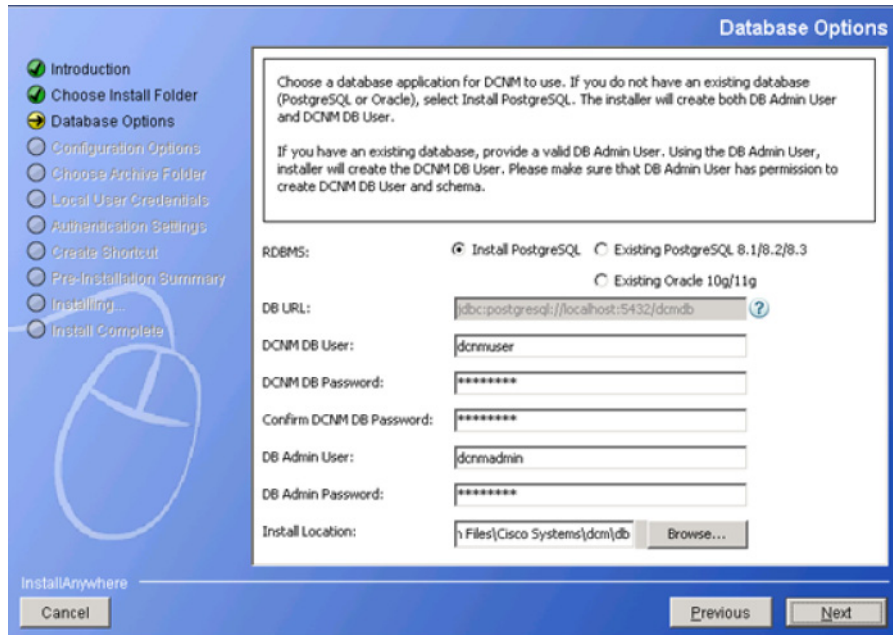


[DCNM-SAN] を選択し、[Server (Licensed)] を選択します。SME に対して具体的にこれらを選択する必要があります。



(注) KMC に関して高可用性を利用する場合は、[Add server to an existing server federation] オプションを選択する必要があります。プライマリおよびセカンダリとして機能する 2 つのサーバをリンクする必要がある場合は、最初のサーバでこのオプションを選択せずに DCNM をインストールする必要があります。ただし、セカンダリサーバにインストールするときは、プライマリサーバにリンクするために [Add server to an existing server federation] オプションを選択する必要があります。

ステップ 4 [Next] をクリックします。[Database Options] 画面が表示されます。



[Install PostgreSQL] オプションを選択して、DCNM パッケージに付属する PostgreSQL データベースを選択できます。また、[Existing PostgreSQL 8.1/8.2/8.3] または [Existing Oracle 10g/11g] オプションを選択して、既存またはインストール済みのデータベースを選択することもできます。



(注) DCNM パッケージのインストールでは、Oracle データベースが提供されません。

セカンダリ サーバで [Add server to an existing server federation] オプションを選択する場合は、既存のデータベース オプションを選択し、リンクが確立されているプライマリ サーバ データベースを指定する必要があります。Postgres を使用した設定により、KMC の高可用性が実現されますが、データベースの高可用性は実現されません。[Oracle database with the dataguard] オプションを使用した Cisco DCNM インストールのみ、高可用性が実現されます。

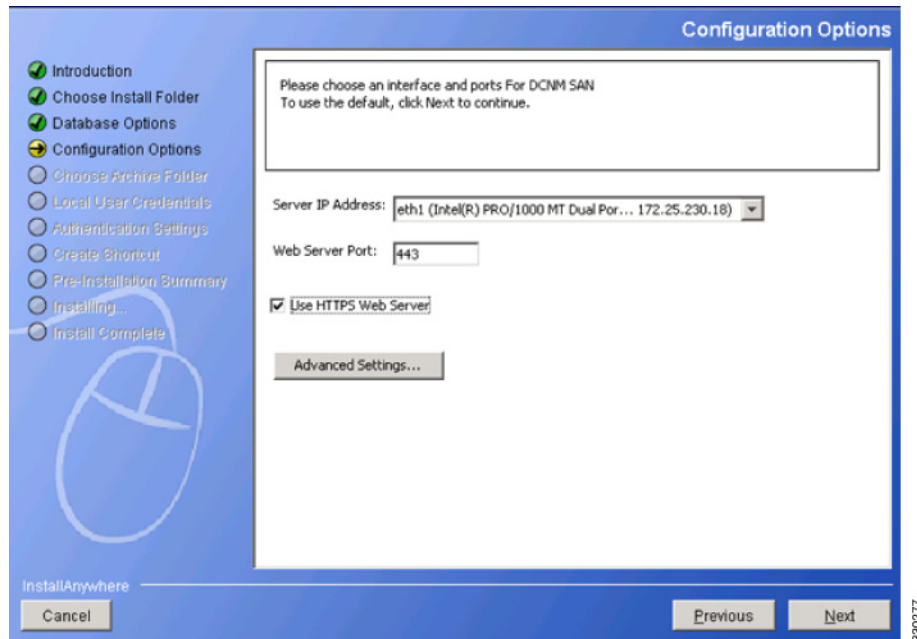
各ユーザがデータベースにアクセスできる DCNM DB User および DB Admin ユーザ クレデンシャルを入力する必要があります。このインストールが存在する場所を参照することもできます。



(注) DCNM データベースと DCNM 管理者ユーザ名は異なっている必要があります。

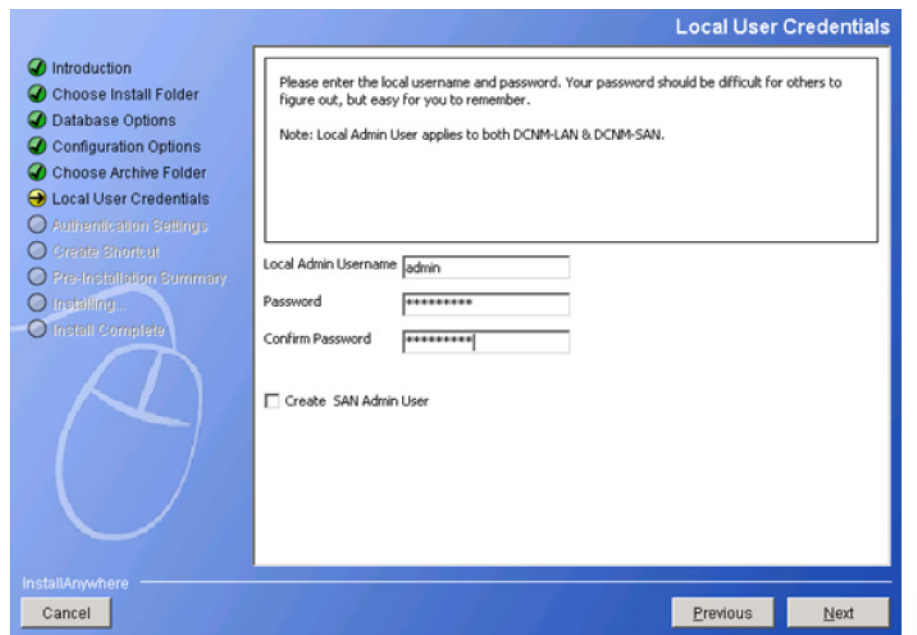


ステップ 5 [Next] をクリックします。[Configuration Options] 画面が表示されます。



SME に対して固有である [Use HTTPS Web Server] オプションを選択します。

ステップ 6 [Next] をクリックします。[Local User Credentials] 画面が表示されます。



DCNM サーバへのログインに必要なローカル管理者のユーザ名とパスワードの詳細を入力します。



(注)

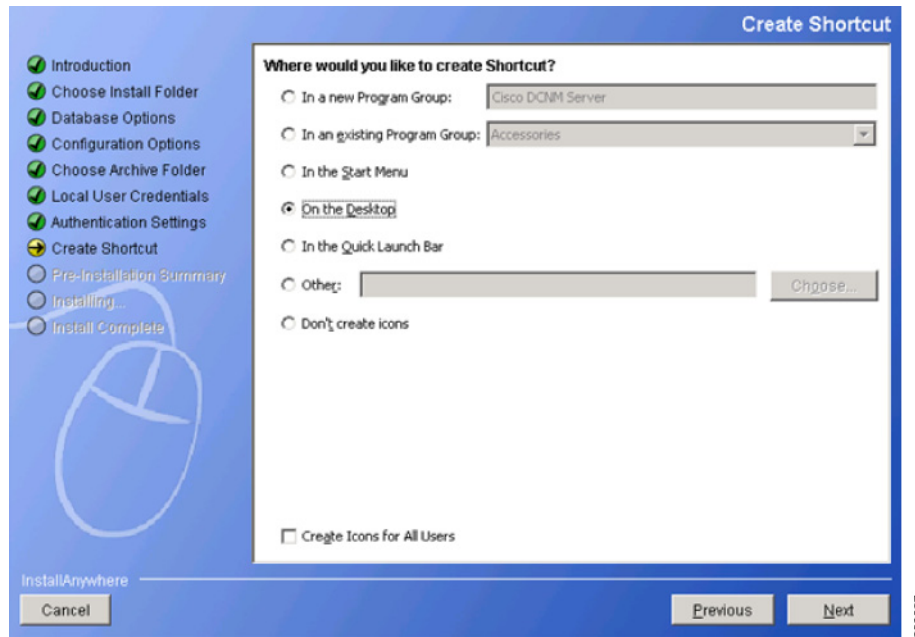
ローカル管理者のユーザ名とパスワードの値は、クラスタの一部であるスイッチのユーザ名とパスワードと同じである必要があります。そうでない場合、クラスタの作成が失敗します。

ステップ 7 [Next] をクリックします。[Authentication Settings] 画面が表示されます。

The screenshot shows the 'Authentication Settings' window. On the left sidebar, the following steps are listed: Introduction, Choose Install Folder, Database Options, Configuration Options, Choose Archive Folder, Local User Credentials, Authentication Settings (highlighted with a mouse cursor), Create Shortcut, Pre-Installation Summary, Installing..., and Install Complete. The main content area has a text box with the prompt 'Please select the authentication mode'. Below this, the 'Mode:' section has three radio buttons: 'Local' (selected), 'RADIUS', and 'TACACS+'. There are three sets of input fields for server addresses and keys: Primary, Secondary, and Tertiary. Each set includes a text box for the address and a text box for the key, with a 'Verify...' button to the right of the key field. At the bottom of the window are 'Cancel', 'Previous', and 'Next' buttons. The text 'InstallAnywhere' is visible in the bottom left corner, and '330275' is in the bottom right corner.

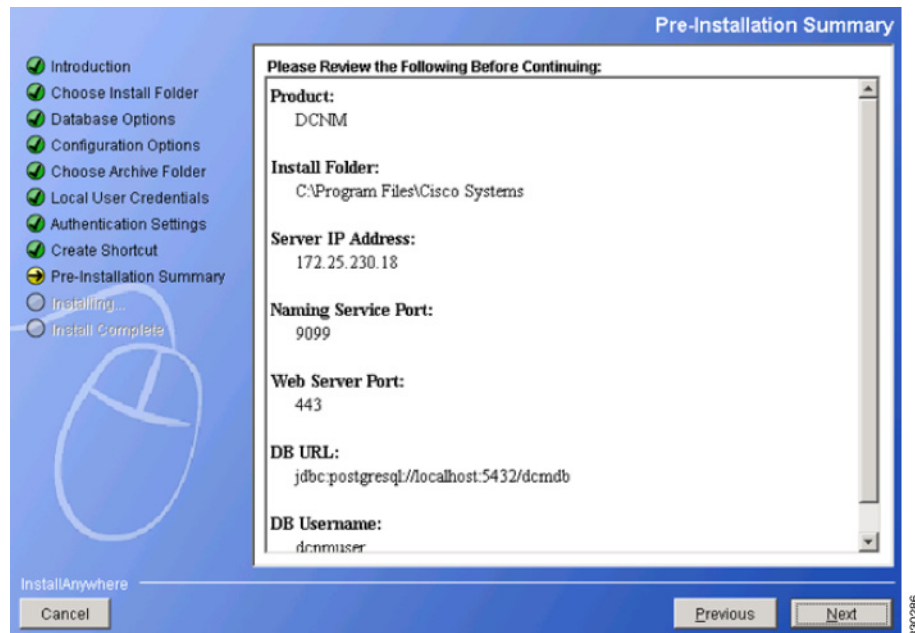
モードを [Local]、[RADIUS]、または [TACACS+] オプションのいずれかから選択します。  
[RADIUS] または [TACACS+] オプションを選択した場合、サーバアドレスと秘密鍵(リモート認証)を入力する必要があります。

ステップ 8 [Next] をクリックします。[Create Shortcut] 画面が表示されます。

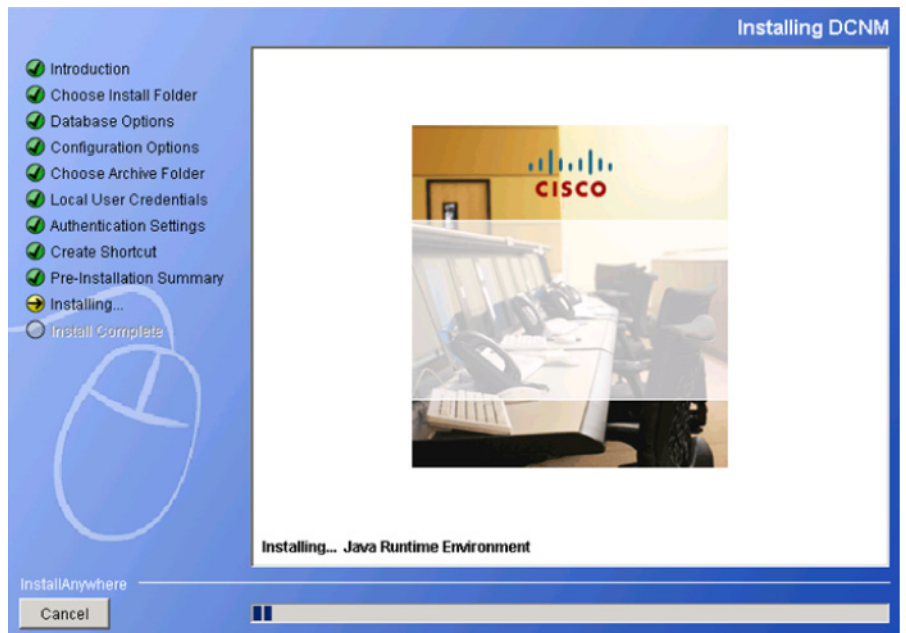


ショートカットを作成するオプションのいずれかを選択する必要があります。

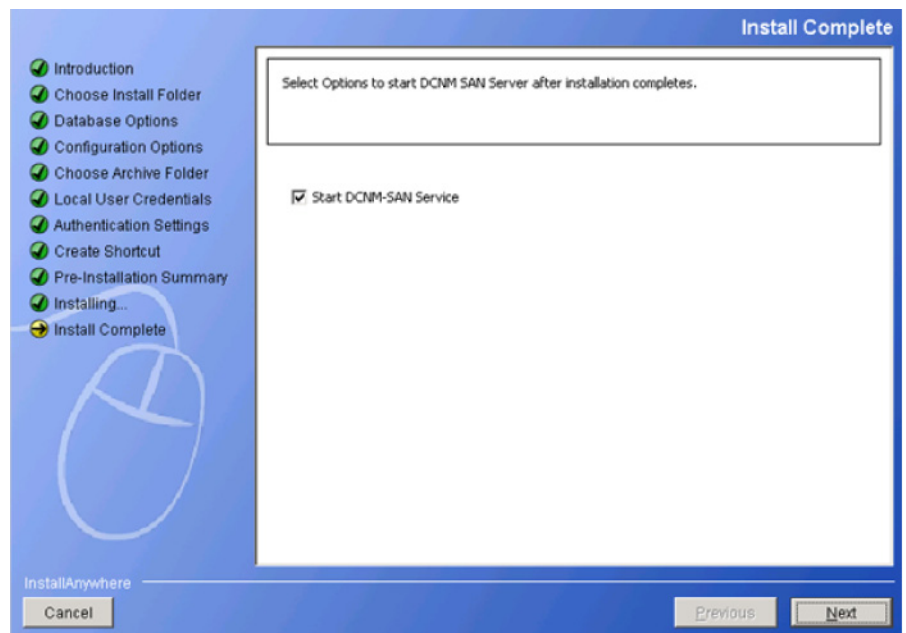
ステップ 9 [Next] をクリックします。[Pre-Installation Summary] 画面が表示されます。



ステップ 10 この情報を確認して [Next] をクリックします。インストールの進行状況を示す [Installing DCNM] 画面が表示されます。

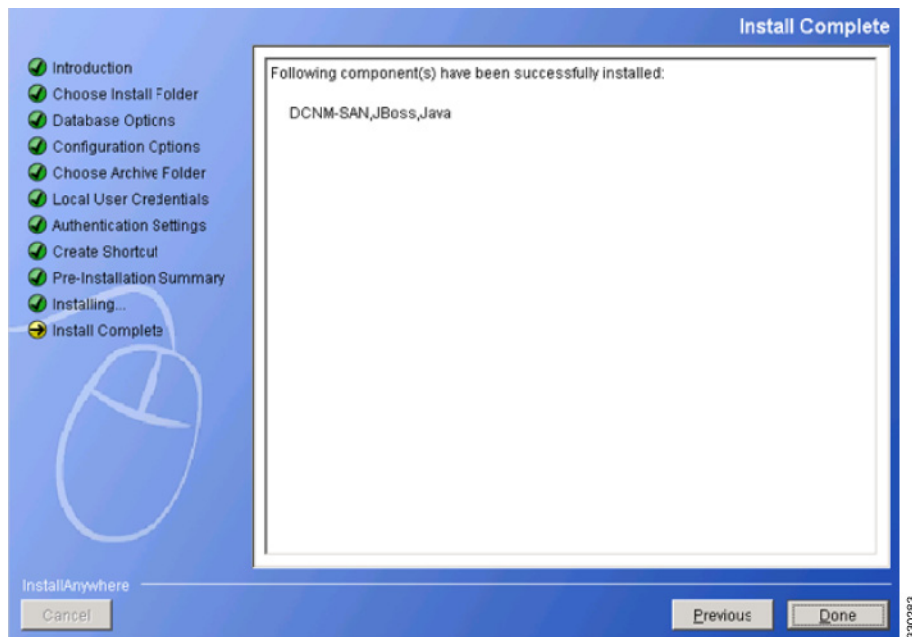


ステップ 11 インストールプロセスが完了すると、[Install Complete] 画面が表示されます。



[Start DCNM-SAN Service] を選択します。

ステップ 12 [Next] をクリックします。[Install Complete] 画面が表示されます。



ステップ 13 [Done] をクリックして、インストールを完了します。DCNM のインストールには、JBOSS および JAVA が含まれます。



(注)

インストールプロセスの完了後に、DCNM パッケージのインストールによって作成された JAVA ディレクトリにある JCE ポリシー ファイルを更新する必要があります。

## SME タスクの設定

MDS-18/4 モジュールまたは Cisco MDS 9222i スイッチ上で SME を構成するプロセスには、時系列順に従う必要があるさまざまな設定タスクが含まれます。

このプロセスには、次の設定作業があります。

1. Cisco MDS-18/4 モジュールまたは Cisco MDS SSN-16 モジュールで、または CLI 経由でクラスタリングを有効にします。
2. Cisco MDS-18/4 モジュールまたは Cisco MDS SSN-16 モジュールで、または CLI 経由で SME を有効にします。
3. Cisco MDS-18/4 モジュールまたは Cisco MDS SSN-16 モジュールに SME インターフェイスを追加します。
4. SME インターフェイスを搭載する Cisco MDS-18/4 モジュールまたは Cisco MDS SSN-16 モジュールを備えたファブリックを追加します。
5. クラスタを作成します。



(注) クラスタは、SME ディスクまたは SME テープに対して定義できます。デフォルトでは、クラスタはテープ対応です。ただし、クラスタで **cluster-capability disk** コマンドを実行すると、クラスタをディスク対応として定義します。詳細については、「[SME クラスタの作成](#)」セクション(4-6 ページ)を参照してください。

- a. クラスタに名前を付けます。
- b. クラスタの作成元になるファブリックを選択します。
- c. クラスタに含めているファブリックから SME インターフェイスを選択します。
- d. マスター キーのセキュリティ レベル(Basic、Standard、または Advanced)を選択します。
- e. セキュリティ キー(共有または一意)、テープの設定(テープへのキー保存、自動ボリューム グループ化、および圧縮)を選択します。
- f. Key Management Center サーバおよびキー証明書ファイルを指定します。
- g. マスタ キーを暗号化するためのパスワードを指定し、キー ファイルをダウンロードします。

## 必要な設定タスク

このセクションでは、SME を設定する前に完了する必要がある必要なタスクについて説明します。この項では、次のトピックについて取り上げます。

- [DNS のイネーブル化\(2-16 ページ\)](#)
- [管理インターフェイスの IP アクセス リスト\(2-17 ページ\)](#)
- [SME のロールと SME ユーザの作成および割り当て\(2-17 ページ\)](#)
- [CFS 地域による FC-Redirect の使用\(2-20 ページ\)](#)
- [スマート カード ドライバのインストール\(2-21 ページ\)](#)
- [SME の設定プロセス\(2-21 ページ\)](#)
- [SME 設定の制約事項\(2-22 ページ\)](#)

SME を設定する前に、MSM-18/4 モジュールが取り付けられた MDS スイッチ、または MDS 9222i スイッチで、クラスタリング、SME、SSH、および DNS を明示的にイネーブルにする必要があります。デフォルトで、これらはディセーブルです。SME の設定および確認操作を使用できるのは、スイッチ上でこれらがイネーブルに設定されている場合だけです。

## DNS のイネーブル化

DNS は、DNS サーバを介してホスト名と ネットワーク内の IP アドレスをマッピングするサービスを提供します。スイッチに DNS を設定すると、**ping**、**telnet**、**upload**、**download** など、すべての IP コマンドにおいて、IP アドレスの代わりにホスト名を使用できます。

DNS を使用する場合は、次の要件が適用されます。

- すべてのスイッチは、DNS を使用して設定される必要があります。
- ドメイン名(またはドメイン リスト)、および IP ネーム サーバは、リモート スイッチに到達するように設定される必要があります。
- DNS サーバは、DCNM-SAN がインストールされているサーバで設定される必要があります。

IP アドレスを使用する場合は、DNS をファブリック内のすべてのスイッチで設定するべきではなく、`smeserver.properties` の `use_ip` フラグを `TRUE` に設定する必要があります。

DNS の設定については、『*IP Services Configuration Guide, Cisco DCNM for SAN*』および『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』を参照してください。

## IP アドレスまたは名前を選択するための `sme.useIP`

クラスタ内の一部のスイッチで DNS が設定されていない場合は、`sme.useIP` を使用できます。`smeserver.properties` ファイルは、`<fm install path>\dcm\fm\conf\` にあります。

DCNM-SAN のインストール中に、`smeserver.properties` ファイルの `use_ip` フラグがデフォルトで `FALSE` に設定されます。IP アドレスを使用するように選択するには、DNS サーバをファブリック内のすべてのスイッチで設定するべきではなく、`smeserver.properties` ファイルの `use_ip` フラグを `TRUE` に設定する必要があります。`smeserver.properties` ファイルに変更を加えたら、DCNM-SAN ファイルを再起動する必要があります。

先にクラスタリングをイネーブルにしてから **SME** をイネーブルにしてください。

DNS を完全に使用するのか、ファブリック内で IP アドレスを徹底的に使用するのかを決定する必要があります。これらを組み合わせた場合は **SME** 機能を使用できません。

クラスタ内のあらゆる場所で DNS がイネーブルになっていることを確認するには、DCNM-SAN サーバと MDS スイッチとの間、および DNS 名を持つ MDS スイッチ間で、`ping` を実行します。

## 管理インターフェイスの IP アクセス リスト

クラスタ通信では、管理インターフェイスを使用する必要があります。IP ACL 設定では、ポート 9333、9334、9335、および 9336 で UDP および TCP トラフィックを許可する必要があります。

## SME のロールと SME ユーザの作成および割り当て

SME 機能には、SME Administrator と SME Recovery Officer という 2 つのプライマリ ロールがあります。SME Administrator ロールには、SME Storage Administrator と SME KMC Administrator というロールも含まれます。デフォルトで、SME は SME Administrator と SME Recovery Officer の両方に同じユーザを割り当てます。この割り当ては、SME の小規模導入に適しています。



(注)

DCNM-SAN ユーザ クレデンシャルは、スイッチ ユーザと同じである必要があります。

表 2-4 に、SME のロール、および各ロールについて考慮する必要があるユーザの数を示します。



(注)

SME は、DCNM-SAN Web クライアントから設定します。内部的には、実際のスイッチ操作は、ファブリックをモニタしているユーザではなく、Web クライアントにログインするユーザに代わって実行されます。そのため、マルチファブリック設定で SME 操作を実行するために、SME 管理者はすべてのファブリックで同じユーザ名とパスワードを使用する必要があります。

表 2-4 SME のロールと担当

SME のロール	マスター キーのセキュリティモード	このロールに必要なユーザ数	このロールが担当する操作
SME Administrator	Basic モード Standard モード	1 人のユーザが SME Administrator および SME Recovery Officer ロールを保持する必要があります。  日常業務には VSAN あたり 1 人が最小で、すべての VSAN にアクセスできる必要があります(多くの VSAN があり、複数の VSAN 管理者が SME 管理者に割り当てられている場合、キーリカバリ操作のために VSAN あたり 1 人の SME Administrator が存在することがあります)。	<ul style="list-style-type: none"> <li>• SME 管理</li> <li>• テープ管理</li> <li>• ディスク管理</li> <li>• テープ ボリューム グループのエキスポート/インポート</li> <li>• ディスク キーのエキスポート/インポート</li> </ul>
SME KMC Administrator	Basic モード Standard モード	ユーザの数は、SME Administrator ロールの場合と同じです。	<ul style="list-style-type: none"> <li>• キー管理操作</li> <li>• ボリュームのアーカイブ/消去</li> <li>• ボリューム グループの追加/削除</li> <li>• ディスク グループとディスク デバイスの追加/削除</li> <li>• ボリューム グループのインポート/エキスポート</li> <li>• ディスク キーのインポート/エキスポート</li> <li>• スマート カードのキー再生成/交換</li> </ul>
Cisco Storage Administrator	Basic モード Standard モード	ユーザの数は、SME Administrator ロールの場合と同じです。	<ul style="list-style-type: none"> <li>• SME プロビジョニング操作</li> <li>• クラスタの作成/更新/削除</li> <li>• テープ バックアップ グループの作成/更新/削除</li> <li>• ディスク グループの作成/更新/削除</li> <li>• テープ デバイスの追加/削除</li> <li>• ディスク デバイスの追加/削除</li> <li>• ボリューム グループの作成</li> <li>• スマート カードの表示</li> </ul>



表 2-4 SME のロールと担当(続き)

SME のロール	マスター キーのセキュリティ モード	このロールに必要なユーザ数	このロールが担当する操作
SME Recovery Officer	Advanced モード	5 人のユーザ(スマート カードごとに 1 人)。 クラスタ作成時は、ユーザのログインとパスワード情報、およびスマート カードの暗証番号を入力するために、各スマート カードの所有者がいる必要があります。	<ul style="list-style-type: none"> <li>マスター キー リカバリ</li> <li>スマート カードの交換</li> </ul>



(注) Basic および Standard セキュリティ モードでは、1 人のユーザが SME Administrator と SME Recovery Officer のロールを保持する必要があります。

## AAA ロールの設定

SME Administrator および SME Recovery Officer に AAA ロールを設定する方法については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』および『Security Configuration Guide, Cisco DCNM for SAN』を参照してください。

## CLI を使用した SME のロールの作成および割り当て

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。

### 前提条件

Basic および Standard セキュリティ モードでは、1 人のユーザが SME Administrator と SME Recovery Officer のロールを保持する必要があります。

### 制約事項

- network-admin ロールに属するユーザだけがロールを作成できます。
- SME に必要な 4 つのセキュリティ ロールは、**setup sme** コマンドを使用して暗黙的に作成できます。VSAN ベースのアクセス制御の場合は、カスタム ロールを作成する必要があります。

## 手順の詳細

SME ロールの作成または既存ロールのプロファイル修正を行うには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>role name sme-admin</b> switch(config-role)#	指定したロール(sme-admin)のモードを開始します。 <b>注意:</b> ロール サブモード プロンプトは、ロールのサブモードを開始したことを示します。このサブモードは SME に固有になりました。
ステップ 3	switch(config)# <b>no role name sme-admin</b>	sme-admin というロールを削除します。
ステップ 4	switch(config-role)# <b>rule 1 permit read-write feature sme-stg-admin</b>	SME 設定コマンドを追加できます。
ステップ 5	switch(config-role)# <b>rule 2 permit read feature sme-stg-admin</b>	SME show コマンドを追加できます。
ステップ 6	switch(config-role)# <b>rule 3 permit debug feature sme</b>	SME debug コマンドを sme-admin ロールに追加できます。
ステップ 7	switch(config-role)# <b>description SME Admins</b>	新しいロールに記述を割り当てます。記述は 1 行に制限され、スペースを含めることができます。
ステップ 8	switch(config)# <b>username usam role sme-admin</b>	sme-admin ロールに指定のユーザ(usam)を追加します。



注意

Cisco KMC が DCNM-SAN の一部である場合、スイッチと DCNM-SAN を同時にアップグレードしないでください。



(注)

ファブリック名は、**Fabric\_** とスイッチ名で識別されます。別のシードスイッチを備えたファブリックを開き直した場合は、ファブリック名が同じまになるように、ファブリック名を以前の名前に手動で変更する必要があります。別のシードスイッチを備えたファブリックを開き直したのにファブリック名を手動で変更しないと、新しいスイッチ名を反映してファブリック名が変更される可能性があります。この場合、MDS スイッチで設定された SME 名と競合します。簡単に識別可能な一意の名前を選択してください。

## CFS 地域による FC-Redirect の使用

Fibre Channel リダイレクト (FC-Redirect) 機能は、Cisco Fabric Services (CFS) 地域を使用して FC-Redirect 設定を配布します。

デフォルトでは、設定はファブリック内のすべての FC-Redirect 対応スイッチに伝播されます。CFS 地域を使用して FC-Redirect 設定の配布を制限します。



(注)

FC-Redirect と CFS 地域の併用はオプションです。

CFS 地域の詳細については、『*System Management Configuration Guide, Cisco DCNM for SAN*』および『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

## スマートカードドライバのインストール

スマートカードリーダーは、SME の設定に使用する管理ワークステーションに接続されている必要があります。スマートカードドライバおよびスマートカードドライバライブラリファイルは、ワークステーションにインストールされている必要があります。

DCNM-SAN Web クライアントの [Config] > [Install Smartcard Driver] リンクから最新のドライバをダウンロードできます。

### 制約事項

スマートカードリーダーは、Windows プラットフォーム上のみでサポートされます。これには、Windows XP 32 ビット、Windows Server 2003 32 ビット、および Windows 7 64 ビット プラットフォームのみが含まれます。



(注) Windows 7 64 ビット スマートカードシステムの場合、64 ビット システム用 Classic Client 6.1 へのアクセスについて、Gemalto に問い合わせる必要があります。スマートカードは、6.10.020.001 のみでテストされています。Windows 7 64 ビット用の Classic Client のその他のバージョンはベストエフォートのみであり、シスコのサポート対象ではありません。Windows 7 32 ビットはサポートされていません。

### トラブルシューティングのヒント

スマートカードドライバのインストール後に新しいスマートカードリーダーを接続するときは、コンピュータの再起動が必要になることがあります。ワークステーションでカードリーダーが認識されない場合は、最新のスマートカードドライバのインストールが必要になることがあります。

## SME の設定プロセス

スイッチで SME を設定する前に、SME 設定プロセスに精通しておくことが重要です。ここでは、SME の設定プロセスについて概説します。

- [SME の初期設定 \(2-21 ページ\)](#)
- [SME クラスタ設定の保存 \(2-22 ページ\)](#)

### SME の初期設定



(注) SME を設定する前に実行する必要がある作業については、「[必要な設定タスク](#)」セクション (2-16 ページ) を参照してください。

Cisco MSM-18/4 モジュールを備えたスイッチ、または Cisco MDS 9222i スイッチで、SME 設定タスクを実行します。

以下の基本的な設定タスクで、基本的な SME 設定プロセスの概要を説明しています。

- SME インターフェイスを作成します (第3章「[SME インターフェイスの設定](#)」)。
- SME 用のクラスタを作成します (第4章「[SME クラスタ管理の設定](#)」)。

- クラスタにインターフェイスを追加します(第4章「SME クラスタ管理の設定」)。
- テープグループを作成します(バックアップサーバの選択とバックアップライブラリの検出を含む)(第5章「SME テープの設定」)。

## SME クラスタ設定の保存



(注)

正しくクラスタを操作できるように、設定の変更はクラスタ内のすべてのスイッチに保存する必要があります。これは、最初のクラスタ作成後に実行する必要があり、その後のすべての変更はクラスタ設定に対して実行されます。

クラスタに対してスイッチまたはインターフェイスを追加または削除したときは、常に設定の変更を保存する必要があります。

## SME 設定の制約事項

ここでは、SME 設定の制約事項について説明します。次の項目を取り上げます。

- [FICON の制約事項 \(2-22 ページ\)](#)
- [iSCSI の制約事項 \(2-22 ページ\)](#)

### FICON の制約事項

SME は FICON デバイスではサポートされておらず、SME クラスタ デバイスは FICON VSAN の一部になることはできません。

### iSCSI の制約事項

SME は iSCSI ポート インデックスを使用するため、SME と iSCSI を同じ Cisco MDS MSM-18/4 モジュール上で設定できません。

## SME 設定のフィールドの説明

ここでは、SME 設定で使用される以下のフィールドについて説明します。

- [メンバー \(2-22 ページ\)](#)
- [SME インターフェイス \(2-23 ページ\)](#)
- [ホスト \(2-23 ページ\)](#)

### メンバー

フィールド	説明
クラスタ	SME クラスタ名。
状態	SME クラスタの動作状態。

フィールド	説明
Master	SME クラスタ マスターの IP アドレスを示します。
Members	SME クラスタのメンバーであるスイッチの IP アドレスを示します。
IsLocal?	スイッチがこのクラスタのローカル メンバーかリモート メンバーかを示します。

## SME インターフェイス

フィールド	説明
クラスタ	この SME インターフェイスが属するクラスタを示します。
スイッチ	スイッチ名。
インターフェイス	SME インターフェイスを示します。
状態	この SME インターフェイスの動作状態。
クラスタの状態	クラスタの動作状態。
クラスタ名	クラスタの名前。
説明	スイッチの説明。
Speed Admin	設定されたポートの速度。
Speed Oper	動作速度。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。
StatusFailureCause	ポートの現在の動作状態の理由。
StatusLastChange	インターフェイスが現在の動作ステータスを開始したときの sysUpTime の値。ローカル ネットワーク管理サブシステムの前回の初期化以前に現在の状態であった場合、この値はゼロ値になります。

### 関連項目

[SME インターフェイスの設定。](#)

## ホスト

フィールド	説明
ホスト	ホスト Nx_Port のファイバ チャネル ポート名 (P_WWN)。
クラスタ	このホスト ポートが属するクラスタを示します。

# SME 設定の機能履歴

表 2-5 に、この機能のリリース履歴を示します。

表 2-5 SME 設定の機能履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
Fabric Manager を使用したクラスタリングのイネーブル化	3.3(1c)	enable 機能では、Fabric Manager を使用してクラスタリングをイネーブルにできます。  3.3(1c) では、Fabric Manager を使用してクラスタリングをイネーブルにできるように [Control] タブのコマンドメニューが変更されました。  次のコマンドが導入または変更されました。 <b>enable</b> コマンド。
Fabric Manager を使用した SME のイネーブル化	3.3(1c)	SME の enable 機能では、Fabric Manager を使用して SME をイネーブルにできます。  3.3(1c) では、Fabric Manager を使用して SME をイネーブルにできるように [Control] タブのコマンドメニューが変更されました。  次のコマンドが導入または変更されました。 <b>enable</b> コマンド。
Fabric Manager を使用した SSH のイネーブル化	3.3(1c)	Device Manager または CLI を使用して SSH キーを生成する前に Fabric Manager GUI を使用して SSH をイネーブルにした場合は、エラー メッセージ ダイアログボックスが表示されます。  3.3(1c) では、エラー メッセージ ダイアログボックスを表示するように Fabric Manager の [Error] ダイアログボックスが変更されました。
Device Manager を使用した SSH のイネーブル化	3.3(1c)	3.3(1c) では、この機能をサポートするように SSH Telnet ウィンドウが変更されました。ユーザは、Device Manager を使用して SSH を作成してからイネーブルにする必要があります。
SME のロール	4.1(1c)	SME 機能には、SME Administrator と SME Recovery Officer という 2 つのプライマリ ロールがあります。SME Administrator ロールには、SME Storage Administrator と SME KMC Administrator というロールも含まれます。  4.1(1c) では、Cisco Storage Administrator および Cisco SME KMC Administrator ロールが追加されました。
キーの管理	4.1(1c)	4.1(1c) では、マルチサイト導入用に Cisco KMC を Fabric Manager から分離できます。

表 2-5 SME 設定の機能履歴(続き)

機能名	リリース	機能情報
キー マネージャ設定	4.1(1c)	<p>Cisco SME を設定する前に、キー マネージャを選択する必要があります。使用可能なキー マネージャのオプションが3つになりました。</p> <p>4.1(1c) では、DCNM-SAN Web クライアントの [Key Manager Settings] ページに新しいオプション [None] が追加されました。</p>
FC-Redirect と CFS 地域	4.1(1c)	<p>4.1(1c) では、CFS 地域および SME のサポートを利用できます。</p>
16 ポート ストレージ サービス ノード (SSN-16) モジュール	4.2(1)	<p>Cisco MDS 9000 ファミリ 16 ポート ストレージ サービス ノードは、エンタープライズクラスのディザスタ リカバリおよびビジネス継続性ソリューションのための高性能統合プラットフォームを提供する新しいハードウェアで、将来的にはインテリジェントなファブリック アプリケーションをサポートします。</p>
高可用性 KMC サーバ	4.1(3)	<p>高可用性 KMC は、プライマリ サーバとセカンダリ サーバを使用して設定できます。</p> <p>4.1(3) では、HA の設定は [Key Manager Settings] ページで確認できます。</p> <p>プライマリ サーバとセカンダリ サーバは、クラスタの作成時に選択できます。</p> <p>プライマリ サーバとセカンダリ サーバの設定は、[Cluster Detail] ページで変更できます。</p>







## SME インターフェイスの設定

この章では、DCNM-SAN および Device Manager を使用して SME インターフェイスを設定および開始する方法について説明します。

事前作業が完了したら、MSM-18/4 モジュールまたは SSN-16 モジュールを搭載する Cisco MDS スイッチ上、または Cisco MDS 9222i スイッチ上の SME インターフェイスを設定する必要があります。

この章では、次の事項について説明します。

- [SME インターフェイスの設定 \(3-1 ページ\)](#)
- [SME インターフェイス設定の確認 \(3-5 ページ\)](#)
- [SME インターフェイスの機能履歴 \(3-6 ページ\)](#)

## SME インターフェイスの設定

SME インターフェイスは、Device Manager または CLI を使用して設定されます。

ここでは、次の内容について説明します。

- [ローカルまたはリモート スイッチからの SME インターフェイスの追加 \(3-1 ページ\)](#)
- [SME インターフェイスの作成 \(3-2 ページ\)](#)
- [SME インターフェイスの削除 \(3-3 ページ\)](#)
- [CLI を使用した SME インターフェイス情報の表示 \(3-4 ページ\)](#)

## ローカルまたはリモート スイッチからの SME インターフェイスの追加

### 前提条件

- SME インターフェイスを追加する前に、クラスタリングのイネーブル化、SME のイネーブル化、スイッチで SME インターフェイスの開始、およびクラスタへのインターフェイス追加を実行してください。



(注) SME インターフェイスはローカル スイッチまたはリモート スイッチから追加できます。

## 手順の詳細

ローカル スイッチから SME インターフェイスを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>fabric fabricname1</b>	ファブリックを指定します。
ステップ 4	switch(config-sme-cl)# <b>node local</b> switch(config-sme-cl-node)#	SME クラスタ ノードサブモードを開始し、ローカル スイッチを指定します。
ステップ 5	switch(config-sme-cl-node)# <b>fabric-membership fabricname1</b>	クラスタのファブリック メンバーシップを指定します。
ステップ 6	switch(config-sme-cl-node)# <b>interface sme 4/1 force</b>	ファブリック f1 のローカル スイッチから SME インターフェイス (4/1) を追加します。

リモート スイッチから SME インターフェイスを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>fabric fabricname</b>	ファブリックを指定します。
ステップ 4	switch(config-sme-cl)# <b>node A.B.C.D X:X::X DNS name</b> switch(config-sme-cl-node)#	SME クラスタ ノードサブモードを開始し、リモート スイッチを指定します。形式は <i>A.B.C.D X:X::X DNS name</i> です。
ステップ 5	switch(config-sme-cl-node)# <b>fabric-membership fabricname1</b>	クラスタのファブリック メンバーシップを指定します。
ステップ 6	switch(config-sme-cl-node)# <b>interface sme 3/1 force</b>	ファブリック f2 のリモート スイッチから SME インターフェイス (3/1) を追加します。

## SME インターフェイスの作成

クラスタをイネーブル化および SME をイネーブル化したら、スイッチの SME インターフェイスを設定します。

MSM-18/4 モジュール スロットのポート 1 で SME インターフェイスを設定します。



(注)

クラスタに対してインターフェイスまたはスイッチを追加または削除した後は、**copy running-config startup-config** CLI コマンドを入力する必要があります。

## 手順の詳細

SME インターフェイスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>interface sme x/y</b>	スロット <i>x</i> のポート <i>y</i> の SME インターフェイスを設定します。 <i>x</i> は MSM-18/4 または SSN-16 モジュール スロットです。MDS 9222i でスロット 1 の場合、ポート番号は 1 です。ポート <i>y</i> は、MSM-18/4 の場合は 1、SSN-16 の場合は 1～4 です。インターフェイス サブモードを開始します。
ステップ 3	switch(config-if)# <b>no shutdown</b>	スロット <i>x</i> のポート <i>y</i> のインターフェイスをイネーブルにします。

SME インターフェイスを設定した後で、**show int** コマンドを入力すると、SME インターフェイスはクラスタに追加されるまでダウンしていると表示されます。

## 例

SME インターフェイスを設定すると、次のようなメッセージが表示されます。

```
2007 Jun 6 21:34:14 switch %DAEMON-2-SYSTEM_MSG: <<%SME-2-LOG_WARN_SME_LICENSE_GRACE>>
No SME Licence.Feature will be shut down after a grace period of approximately 118 days.
```

## SME インターフェイスの削除

## 前提条件

- SME インターフェイスを削除する前に、クラスタからスイッチを削除する必要があります。

## 制約事項

- クラスタの一部である SME インターフェイスは削除できません。**no sme cluster cluster name** コマンドを入力してスイッチをクラスタから削除してから、SME インターフェイスを削除してください。

## 手順の詳細

SME インターフェイスを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>no interface sme x/y</b>	スロット <i>x</i> のポート <i>y</i> から SME インターフェイスを削除します。 <i>x</i> は MSM-18/4 または SSN-16 モジュール スロットです。ポート <i>y</i> は、MSM-18/4 の場合は 1、SSN-16 の場合は 1～4 です。MDS 9222i でスロット 1 の場合、ポート番号は 1 です。

## CLI を使用した SME インターフェイス情報の表示

SME インターフェイスの設定および統計情報に関する情報を取得するには、**show interface sme** CLI コマンドを使用します。

```
switch# show interface sme 3/1
sme3/1 is up
In fabric Cisco_fabric1
SME                IOs          IO/s          Bytes          Rate
-----
Host Reads          0            0             0              0.00 B/s
Host Writes         270134566    0             35407048474624 0.00 B/s
Host Total          270134566    0             35407048474624 0.00 B/s

Tgt Reads           0            0             0              0.00 B/s
Tgt Writes          540268684    0             232408631520   0.00 B/s
Tgt Total           540268684    0             232408631520   0.00 B/s

Clear              IOs          IO/s          Bytes          Rate
-----
Host Reads          0            0             0              0.00 B/s
Host Writes         3512         0             460324864      0.00 B/s
Host Total          3512         0             460324864      0.00 B/s

Tgt Reads           0            0             0              0.00 B/s
Tgt Writes          3512         0             460324864      0.00 B/s
Tgt Total           3512         0             460324864      0.00 B/s

Compression Ratio   455.11 : 1
SME to Clear        100.00 %
Read to Write       0.00 %

Clear Luns 4, Encrypted Luns 1

Error Statistics
 0 CTH, 0 Authentication 3 Compression
69 Key Generation, 0 Incorrect Read Size
0 Overlap Commands, 0 Stale Key Accesses
0 Overload Condition, 0 Incompressible
210 XIPC Task Lookup, 0 Invalid CDB
0 Ili, 88881729 Eom, 0 Filemark, 0 Other
last error at Wed May 18 09:41:12 2011
```

表 3-1 に **show interface sme** コマンドのエラー統計情報を示します。

表 3-1 エラー統計情報

パラメータ	説明
Authentication	テープブロックの整合性の検証中に生成されたエラー。このエラーは、テープが破損したときに発生します。
Bad Target Responses	ターゲットから生成されたエラー。このエラーは頻繁に発生し、通常、FileMark、Incorrect Length Indicators (ILI) などが含まれます。
CTH	Cisco Tape Header (CTH) に関連するエラー。CTH は論理ブロック 0 にあり、メディアなどベンダー固有の情報が含まれています。
Incorrect Read Size	書き込みサイズが読み取りサイズと異なっているときに生成されたエラー。

表 3-1 エラー統計情報(続き)

パラメータ	説明
Invalid CDB	不明または不正な SCSI コマンドがあるときに生成されたからの出力が生成されたエラー。Invalid CDB のカウンタは、転送サイズが不適切なホストからの読み取りまたは書き込みコマンドの数を表示します。
Incompressible	圧縮性不可能なデータがあるときに生成されたエラー。
Key Generation	キーの生成に関連するエラー。
Overload	ホストからの読み取り操作が重複しているときに発生したエラー。  SME に対する同時で複数の読み取り操作は、BUSY チェック条件で拒否されます。そのような場合は、Overload エラーとして表示されます。
Overlap	同一の Initiator-Target-LUN (ITL) に対して複数の重複するコマンドがあるときに生成されたエラー。
Stale Key Access	アーカイブされたキーがテープ書き込み操作でアクセスされるときに生成されたエラー。  ボリューム グループまたはクラスタが削除されるか新しいクラスタにインポートされると、キーがアーカイブされます。これらのキーは、テープへの書き込みに使用しないでください。Stale Key Access のカウンタは、このような場合の発生数を表示します。
XIPC Task Lookup	eXtensible Inter-Process Communication (XIPC) に関連するエラー。このようなエラーは、交換ルックアップ障害が発生したときに生成されます。

## SME インターフェイス設定の確認

SME インターフェイス設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
<code>show interface sme</code>	SME インターフェイスの設定と統計情報を表示します。
<code>show int</code>	SME インターフェイスがクラスタに追加されるまでダウンしているかどうかを表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『Cisco MDS 9000 Family NX-OS Command Reference』を参照してください。

# SME インターフェイスの機能履歴

表 3-2 に、この機能のリリース履歴を示します。

表 3-2 SME インターフェイスの機能履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
16 ポートストレージ サービス ノード (SSN-16) モジュール	4.2(1)	Cisco MDS 9000 ファミリー 16 ポートストレージ サービス ノードは、エンタープライズクラスのディザスタリカバリおよびビジネス継続性ソリューションのための高性能統合プラットフォームを提供する新しいハードウェアで、将来的にはインテリジェントなファブリックアプリケーションをサポートします。
SME インターフェイスの設定および開始	3.3(1c)	ユーザは、Fabric Manager を使用してインターフェイスを作成する前に、Device Manager または CLI を使用して SME インターフェイスを作成する必要があります。



## SME クラスタ管理の設定

DCNM-SAN は、ネットワーク ファブリックをリアルタイム ビューで表示する Web ブラウザ インターフェイスを提供し、使いやすいウィザードで SME を設定できます。

この章では、DCNM-SAN を使用して SME クラスタを管理するために実行する、SME の初期設定と作業に関する情報を記載しています。

この章では、次の事項について説明します。

- [SME クラスタ管理に関する情報\(4-1 ページ\)](#)
- [CLI を使用した SME クラスタ管理の設定\(4-6 ページ\)](#)
- [SME クラスタ管理設定の確認\(4-10 ページ\)](#)
- [SME クラスタ管理のモニタリング\(4-11 ページ\)](#)
- [SME クラスタ管理の機能履歴\(4-14 ページ\)](#)

## SME クラスタ管理に関する情報

SME クラスタは、各スイッチがメンバーまたはノードである単一のファブリック環境内の、SME アプリケーションを実行する MDS スイッチのグループで構成されます。クラスタ インフラストラクチャにより、SME アプリケーションは、他のメンバーとの通信や連携によってアプリケーションの設定や動作状態の一貫した分散ビューが維持できるようになるため、高可用性とロード バランシングを実現できます。

Cisco MSM-18/4 モジュールまたは SSN-16 モジュールが取り付けられている MDS スイッチ上、あるいは Cisco MDS 9222i スイッチ上での SME の設定プロセスには、時系列順で従う必要がある多数の設定作業が関係しています。DCNM-SAN Web サーバの「Before You Begin」オンライン ヘルプにあるトピックを参照してください。SSH を設定します。SME クラスタの作成前に完了させる必要がある作業については、[第 2 章「SME の設定」](#)および[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 クォーラムおよびマスター スイッチの選択

この項では、クラスタでマスター スイッチを選定するための SME クラスタ クォーラムとプロセスについて説明します。

- [クラスタ クォーラム\(4-2 ページ\)](#)
- [マスター スイッチの選定\(4-2 ページ\)](#)

### ノード ID

クラスタ内のすべてのスイッチにノード ID があります。これをクラスタに追加するときに、SME は新しい各スイッチにノード ID を割り当てます。クラスタが作成されるスイッチにはノード ID 1 が割り当てられます。これはマスター スイッチです。新しいスイッチをクラスタに追加するときに、次に使用可能な上位ノード ID が割り当てられます。たとえば、2 番目のスイッチがクラスタに追加される場合、ノード ID 2 となり、3 番目のスイッチは、ノード ID 3 などとなります。

### クラスタ ビュー

クラスタ ビューは運用クラスタの一部であるスイッチのセットです。

## クラスタ クォーラム

クラスタが動作するには、クラスタにはクラスタ ビューに設定されたスイッチの半分以上が含まれている必要があります。N スイッチ クラスタでは、 $N/2 + 1$  スイッチがクラスタ クォーラムを形成します。

N が偶数の場合、クラスタ クォーラムには  $N/2$  スイッチが必要で、また、最も低いノード ID を持つスイッチが存在する必要があります。

クォーラム ロジックにより、クラスタがパーティションに区分されている場合、最大で 1 つのパーティションが動作できます。他のすべてのスイッチは動作不能です。これにより、クラスタの一貫性が確保されます。

## マスター スイッチの選定

クラスタが作成されると、クラスタが作成されているスイッチはクラスタ マスター スイッチになります。マスター スイッチに障害が発生するか、リブートされると、別のスイッチがマスター スイッチの役割を引き継ぎます。マスター選定のロジックでは、ノード ID と最新のクラスタ設定を使用して、クラスタ内のどのスイッチがマスター スイッチになるか判断します。次に、マスター選定ロジックについて説明します。

- マスター スイッチが動作中のクラスタで障害が発生した場合、次に低いノード ID を持つスイッチがマスター スイッチの役割を引き継ぎます。運用クラスタでは、全スイッチが同じクラスタ設定で動作することに注意してください。
  - 前のマスター スイッチがオンラインに復帰し、クラスタに接続した場合、すぐにはマスターにはなりません。
- クラスタのすべてのスイッチが起動すると、最新のクラスタ設定があるスイッチがマスター スイッチになります。同じ設定の複数のスイッチがある場合、最も低いノード ID を持つスイッチがマスター スイッチとして選択されます。
  - マスター スイッチを選択して、クラスタが運用している(クォーラムがある)と、下位ノード ID を持つスイッチが後でクラスタに接続しても、マスター スイッチは変更されません。

たとえば、それぞれノード ID が 1、2、および 3 の 3 つのスイッチ S1、S2、S3 があるとし、スイッチ S2 と S3 がクォーラムを形成している場合、スイッチ S2 がマスター スイッチになります。ノード ID が 1 のスイッチ S1 が起動して、後でクラスタに接続しても、スイッチ S2 が引き続きマスターになります。ただし、スイッチ S2 が何らかの理由でダウンした場合、スイッチ S1 がマスター スイッチになります。





(注) マスター スイッチに変更が加えられる可能性があるため、クラスタ内のすべてのスイッチは、SNMP 設定、SME ロール、ユーザ クレデンシャル、および SSH を扱うように設定する必要があります。クラスタ内のスイッチは、KMC と直接通信する必要があります。

## 2 スイッチ クラスタ シナリオ

クラスタ クォーラム ロジックによると(「[クラスタ クォーラム](#)」セクション(4-2 ページ)を参照)、設定済みの2つのスイッチ両方が動作しているか、最も低いノード ID を持つスイッチが動作している場合、設定済みの2つのスイッチが設定されたクラスタは動作できます。

後者の場合、最も低いノード ID を持つスイッチは、1 スイッチ クラスタのマスターです。その他のスイッチは障害が発生した、または単に動作可能なスイッチへの接続が失われた可能性があります。いずれにしても、より高いノード ID を持つスイッチが動作不能になります。下位ノード ID を持つスイッチに障害が発生すると、もう片方のスイッチは運用クラスタを形成することはできません。

次の例では、こうしたシナリオについて説明します。最初の3つの例では、単一のスイッチ障害を考慮します。

1. スイッチ S1(ノード ID 1)および S2(ノード ID 2)による2スイッチ クラスタで、S1 がマスターである(下位ノード ID がマスター)と仮定します。  
スイッチが相互の接続を失うと、マスター スイッチ S1 のノード ID が下位であり、(N/2) スイッチ クラスタを形成できるため、マスター スイッチ S1 は引き続き動作します。スイッチ S2 は動作不能になります。
2. スイッチ S1(ノード ID 1)および S2(ノード ID 2)による2スイッチ クラスタで、S2 がマスターであると仮定します(両方のスイッチがオンラインになったときマスターの設定が最新であるため、マスターのノード ID は上位になる点に注意してください)。  
スイッチが相互の接続を失うと、スイッチ S2 が動作不能になり、S1 がマスターの役割を引き継いで1スイッチ クラスタを形成します。これは、2 スイッチ クラスタ(最低ノード ID を持つ N/2)のクォーラム ロジックと一致しています。
3. スイッチ S1(ノード ID 1)および S2(ノード ID 2)による2スイッチ クラスタを仮定します。S1 に障害が発生した場合(どのスイッチがマスターかに関係なく)は、S1 がダウンしている限り、S2 も動作不能になります。  
S1 が起動した場合、S1 および S2 は、2 スイッチ クラスタを形成します。

次の例では、両方のスイッチ(ノード ID 1 の S1 およびノード ID 2 の S2)のリブートについて説明します。



注意

クラスタの設定変更を行う場合、リブートの前に **copy running-config startup-config CLI** コマンドをすべてのスイッチで入力して、実行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する必要があります。そうしないと、クラスタは、リブート後に正しく形成されない場合があります。

4. リブート後、スイッチ S1 と S2 の両方がほぼ同時に起動すると、2 スイッチ クラスタが形成されます。
  - a. クラスタ設定が同じ場合、S1(下位ノード ID)がマスターになります。
  - b. クラスタ構成が異なっていると、クラスタ設定が最新のスイッチがマスターになります。
5. リブート後、スイッチ S2 が最初に起動すると、S1 も起動するまでクラスタを形成できません。その後、前のケースで説明したアルゴリズムが使用されます。

6. リブート後、スイッチ S1 が最初に起動すると、1 スイッチ クラスタ (最低ノード ID を持つ N/2) が形成されます。S2 が起動すると、クラスタに接続して 2 スイッチ クラスタを形成します。  
S2 が起動し、スタートアップ コンフィギュレーションで偶然最新のクラスタ設定になっている場合 (S1 で実行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なかったが、S2 では保存した場合に発生する可能性があります)、S2 は S1 によって形成されたクラスタに接続することができません。



注意

---

リブートを行う前に、すべてのスイッチで実行コンフィギュレーションを保存することが重要です。

---

### 3 スイッチ クラスタ シナリオ

3 スイッチ クラスタでは、クォーラムには 2 つのスイッチがクラスタ ビューになければなりません (N/2 + 1)。下記の例では、スイッチ S1 (ノード ID 1)、S2 (ノード ID 2)、S3 (ノード ID 3) を備えた 3 スイッチ クラスタの 3 つのシナリオについて説明します。S1 はマスター スイッチです。

1. 3 スイッチ運用クラスタで、スイッチ S3 に障害が発生するか、他の 2 つのスイッチとの接続が失われると、S3 が動作不能になります。スイッチ S1 と S2 は運用クラスタを形成します。S3 が再起動すると、クラスタに再接続します。
2. 3 スイッチ運用クラスタで、マスター スイッチ S1 に障害が発生するか、他の 2 つのスイッチとの接続が失われると、S1 が動作不能になります。スイッチ S2 と S3 は運用クラスタを形成し、S2 がマスターになります。S1 が再起動すると、クラスタに再接続します。S2 が引き続きマスターであることに注意してください。
3. 2 つのスイッチが故障すると、クラスタは動作不能になります。

次の例では、クラスタのすべてのスイッチのリブートについて説明します。



注意

---

クラスタの設定変更を行う場合、リブートの前に **copy running-config startup-config** コマンドをすべてのスイッチで入力して、実行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する必要があります。そうしないと、クラスタは、リブート後に正しく形成されない場合があります。

---

4. リブート後、すべてのスイッチがほぼ同時に起動すると、まず 2 スイッチ クラスタが形成され、次に 3 つ目のスイッチが追加されます。
  - a. クラスタ設定が同じ場合、S1 (下位ノード ID) がマスター スイッチになり、まず 2 スイッチ クラスタが形成され、次に 3 つ目のスイッチが追加されます。
  - b. クラスタ設定が異なっている場合、最新の設定を実行しているスイッチがマスター スイッチになり、2 スイッチ クラスタが形成され、次に 3 つ目のスイッチが追加されます。
5. リブート後、スイッチが一度に起動すると、最初の 2 つのスイッチが起動した後に 2 スイッチ クラスタが形成されます。後で 3 つ目のスイッチがオンラインになると、クラスタに接続します。

3 つ目のスイッチがスタートアップ コンフィギュレーションで偶然最新のクラスタ設定を実行している場合 (他の 2 つのスイッチではなく、このスイッチでのみ実行コンフィギュレーションを保存した場合に発生する可能性があります)、3 つ目のスイッチはクラスタに接続することができません。



注意

---

リブートを行う前に、すべてのスイッチで実行コンフィギュレーションを保存することが重要です。

---

## 4 スイッチ クラスタ シナリオ

4 スイッチ クラスタ シナリオは、上記の例と非常によく似ています。クラスタ ビューに少なくとも3つのスイッチ ( $N/2 + 1$ )がある場合、またはクラスタ ビューに最も低いノード ID のスイッチを含む2つのスイッチ (最低ノード ID を持つ  $N/2$ )がある場合、クラスタは動作します。

## 2 ノード クラスタの In-Service Software Upgrade

In-Service Software Upgrade (ISSU) は、バグ修正を展開し、トラフィックを中断せずに、新機能やサービスを追加する包括的で透過的なソフトウェア アップグレード アプリケーションです。

MDS 9222i スイッチをメンバーとして構成されているクラスタで、スイッチが通信できない場合、最下位のノード ID を持つスイッチがクラスタ内に残り、他のスイッチはクラスタのメンバーではなくなります。ただし、ISSU が最も低いノード ID を持つスイッチで実行されると、両方のスイッチがクラスタから退出するためにクラスタが完全に失われます。

この望ましくない状況は2 スイッチ クラスタで次のように対処しています。

- アップグレード スイッチが、クラスタから退出しようとしている他のスイッチにメッセージを送信します。アップグレード スイッチはマスター スイッチまたはスレーブ スイッチのいずれかです。
- 残りのスイッチはクラスタに残り、スレーブ スイッチであった場合はマスター スイッチの役割を果たします。このスイッチは、そのままの状態でもコアラムを備えたクラスタ内に残ります。
- ISSU が完了し、スイッチがブートすると、アップグレード済みのスイッチはスレーブ スイッチとしてクラスタに再接続します。



(注)

この機能は内部的に ISSU ロジックに結び付けられ、追加コマンドを実行する必要はありません。

## サーバ クラスタ

クラスタは、一般的なタスクを実行するために関連付けられているサーバのグループです。

クラスタには次の機能があります。

- 高可用性: クラスタ内の1つのサーバがダウンしても、そのサーバに割り当てられている作業は、クラスタ内の別のサーバに移行されます。
- ロード バランシング: クラスタは、異なる複数のサーバ間で作業を分散できます。

クラスタは、共有モデルまたは非共有モデルを使用できます。共有モデルは、共有リソースへの同時アクセスを管理するための分散ロック マネージャ (DLM) が必要です。非共有モデルは DLM が不要であり、結果として、必要なオーバーヘッドは少なくなります。たとえば、MSCS (Microsoft クラスタ) は非共有モデルを使用します。これは、あるノードがリソースを所有しており、その所有者ノードに障害が起きた場合に、リソースの所有権を別のノードが引き受けることを意味します。

クラスタ コアラムの詳細については、「[クラスタ コアラム](#)」セクション(4-2 ページ)を参照してください。

## CLI を使用した SME クラスタ管理の設定

CLI を使用して、SME クラスタ管理を設定できます。この項では、次のトピックについて取り上げます。

- [SME クラスタの作成 \(4-6 ページ\)](#)
- [クラスタリングのイネーブル化とディセーブル化 \(4-8 ページ\)](#)
- [SME サービスのイネーブル化とディセーブル化 \(4-8 ページ\)](#)
- [SME クラスタ セキュリティ レベルの設定 \(4-9 ページ\)](#)
- [SME 管理者およびリカバリ オフィス ロールのセットアップ \(4-10 ページ\)](#)



(注) SSH 機能は、クラスタを構成するすべてのスイッチでイネーブルにする必要があります。

## SME クラスタの作成

SME テープ クラスタを作成するには、クラスタに含めるファブリックを特定し、以下を設定します。

- 自動ボリューム グループ
- Key Management Center (KMC)
- ターゲットの検出
- テープ グループ
- キーオンテープ モード
- リカバリ
- 共有キー モード
- リカバリのためのクラスタのシャットダウン
- ボリューム テープ グループ
- テープ圧縮

SME ディスク クラスタを作成するには、クラスタに含めるファブリックを特定し、以下を設定します。

- CKMC
- ターゲットの検出
- ディスク グループ
- ディスク デバイス
- ディスク パス
- リカバリ
- リカバリのためのクラスタのシャットダウン

## 手順の詳細

テープまたはディスクのいずれかの SME クラスタを作成できます。



注意

デフォルトでは、クラスタは SME テープに対応できます。ただし、**cluster-capability disk** コマンドを入力すると、このクラスタはディスク デバイスにしか使用できなくなります。

テープ用の SME クラスタを作成するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername1</i> switch(config-sme-cl)#	クラスタ名を指定し、SME クラスタ設定サブモードを開始します。クラスタ名には最大 32 文字を使用できます。
ステップ 3	switch(config-sme-cl)# <b>fabric f1</b>	ファブリック f1 をクラスタに追加します。



注意

最初の SME インターフェイスを追加する前に、**cluster-capability disk** コマンドをイネーブルにする必要があります。

## 前提条件

ディスク クラスタを作成する前に、必ず FC-Redirect バージョン 2 を、ディスク クラスタを構成するすべてのスイッチ上でイネーブルにします。FC\_Redirect のバージョン レベルを確認するには、次のコマンドを入力します。コンフィギュレーション モードでの予期される出力は、Mode V2 です。

```
switch# show fc-redirect configs
Configuration Mode    = MODE_V2
```



(注)

SME ディスク クラスタが設定されているファブリック内のすべてのスイッチを、FC-Redirect バージョン 1 にすることはできません。

## 手順の詳細

ディスク用の SME クラスタを作成するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername1</i> switch(config-sme-cl)#	クラスタ名を指定し、SME クラスタ設定サブモードを開始します。クラスタ名には最大 32 文字を使用できます。
ステップ 3	switch(config-sme-cl)# <b>cluster-capability disk</b>	SME ディスクの SME クラスタ機能を定義します。

	コマンド	目的
ステップ 4	switch(config-sme-cl)# <b>fabric f1</b>	ファブリック f1 をクラスタに追加します。
ステップ 5	switch(config-sme-cl)# <b>fabric f2</b>	ファブリック f2 をクラスタに追加します。 (注) SME ディスクの場合、最大で 2 つのファブリックを追加できます。



注意

同じファブリック内にあるスイッチに対しては、CLI で設定するファブリック メンバーシップは同じである必要があります。

## クラスタリングのイネーブル化とディセーブル化

SME の設定プロセスの最初のステップは、クラスタリングをイネーブルにすることです。

### 手順の詳細

クラスタをイネーブルまたはディセーブルにするには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>conf t</b> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>feature cluster</b>	クラスタリングをイネーブルにします。
ステップ 3	switch(config)# <b>no feature cluster</b>	クラスタリングをディセーブルにします。

## SME サービスのイネーブル化とディセーブル化

SME の暗号化およびセキュリティ機能を利用するには、SME サービスをイネーブルにする必要があります。SME クラスタをイネーブルにした後の、SME 設定プロセスにおける 2 番目の手順は、SME サービスのイネーブル化です。

### 手順の詳細


SME サービスをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>feature sme</b>	SME 機能をイネーブルにします。
ステップ 3	switch(config)# <b>no feature sme</b>	SME 機能をディセーブルにします。

## SME クラスタ セキュリティ レベルの設定

セキュリティには、Basic、Standard、Advanced の 3 つのレベルがあります。Standard および Advanced セキュリティ レベルには、スマート カードが必要です。

表 4-1 マスター キーのセキュリティ レベル

セキュリティ レベル	定義
Basic	マスター キーはファイルに保存され、パスワードを使用して暗号化されます。マスター キーを取得するには、ファイルとパスワードにアクセスする必要があります。
Standard	Standard セキュリティでは、1 つのスマート カードが必要です。クラスタを作成してマスター キーを生成するときに、スマート カードを求められます。次にマスター キーがスマート カードに書き込まれます。マスター キーを取得するには、スマート カードとスマート カードの暗証番号が必要です。
Advanced	Advanced セキュリティでは、5 つのスマート カードが必要です。クラスタを作成して Advanced セキュリティ モードを選択するときには、データ取得の必要がある場合にマスター キーを回復するために必要なスマート カードの数(5 つのスマート カードのうちの 2 つまたは 3 つ、あるいは 3 つのスマート カードのうちの 2 つ)を指定します。リカバリには、カードのクォーラム(3 つのうちの 2 つ、5 つのうちの 2 つ、5 つのうちの 3 つ)が必要です。たとえば、「5 つのスマート カードのうちの 2 つ」と指定すると、マスター キーの回復には 5 つのスマート カードのうちの 2 つが必要になります。それぞれのスマート カードは、SME リカバリ責任者が所有しています。
	 <p>(注) 必要とされるスマート カードの数が大きくなると、それだけセキュリティも向上します。ただし、スマート カードを紛失したり破損したりすると、マスター キーの回復に使用できるスマート カードの数は減ることになります。</p>

SME クラスタ セキュリティ レベルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername1</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>security-mode</b> <b>basic</b>	クラスタ セキュリティ レベルを Basic に設定します。



(注) Standard または Advanced セキュリティ モードをイネーブルにするための CLI は、サポートされていません。Basic モードでは、DCNM-SAN Web クライアントによってもサポートされます。

## SME 管理者およびリカバリ オフィス ロールのセットアップ

SME 管理者、SME ストレージ管理者、SME KMC 管理者、および SME リカバリ 責任者をセットアップするには、この手順を実行します。

コマンド	目的
switch# <b>setup sme</b>	4 つのセキュリティ ロールをセットアップします。

詳細については、付録 2「CLI を使用した SME のロールの作成および割り当て」を参照してください。



(注) Cisco DCNM から SME への初回のアクセス時には、特定の DCNM のキー管理ロールを選択するように求められます。詳細については、「キー管理操作の設定」セクション(6-32 ページ)を参照してください。

[Disk Signature Mode] チェック ボックスを選択すると、署名モードのクラスタが作成されます。



(注) クラスタをアクティブにするには、マスター キー ファイルをダウンロードする必要があります。ファイルをダウンロードする前にウィンドウを閉じる場合は、[Cluster Detail] ページに移動してマスター キー ファイルをダウンロードし、クラスタのセットアップを完了します。



(注) カードにキー共有を保存しているときにエラーが発生した場合は、クラスタを削除して再作成する必要があります。



(注) カードにキー共有を保存しているときにエラーが発生した場合は、クラスタを削除して再作成する必要があります。

## SME クラスタ管理設定の確認

SME クラスタ管理の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show sme</b>	特定のクラスタ構成、内部情報、および転送情報を表示します。
<b>show sme cluster</b>	追加のクラスタ情報を表示します。
<b>show sme cluster key</b>	クラスタ キー データベースに関する情報を表示します。
<b>show sme cluster node</b>	ローカルまたはリモート スイッチに関する情報を表示します。
<b>show sme cluster recovery officer</b>	特定のリカバリ 責任者に関する情報、または特定のクラスタのすべてのリカバリ 責任者の情報を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『Cisco MDS 9000 Family NX-OS Command Reference』を参照してください。



## SME クラスタ管理のモニタリング

この項では、次のトピックについて取り上げます。

- [CLI を使用した SME クラスタ詳細の表示 \(4-11 ページ\)](#)

### CLI を使用した SME クラスタ詳細の表示

この項では、次のトピックについて取り上げます。

- [SME クラスタ、内部、および転送情報の表示 \(4-11 ページ\)](#)
- [SME クラスタ詳細の表示 \(4-11 ページ\)](#)
- [クラスタ キー情報の表示 \(4-12 ページ\)](#)
- [クラスタ ノード情報の表示 \(4-13 ページ\)](#)
- [リカバリ 責任者情報の表示 \(4-13 ページ\)](#)

### SME クラスタ、内部、および転送情報の表示

SME クラスタ設定を確認するには、**show sme cluster** コマンドを使用して、特定のクラスタ構成、内部情報、および転送情報を表示できます。

**show sme cluster** コマンドの出力例を次に示します。

```
switch# show sme cluster clustername1
SME Cluster is clustername1
Cluster ID is 2e:00:00:05:30:01:ad:f4
Cluster is Operational
Cluster is Not Shutdown
Cluster config version is 27
Security mode is basic
Cluster status is online
Total Nodes are 1
Recovery Scheme is 1 out of 1
Fabric[0] is f1
CKMC server has not been provisioned
Master Key GUID is 8c57a8d82d2098ee-3b27-6c2b116a950e, Version: 0
Shared Key Mode is Enabled
Auto Vol Group is Not Enabled
```

### SME クラスタ詳細の表示

追加のクラスタ情報は、**show sme cluster** コマンドで表示できます。このコマンドは、次の情報を表示するために使用します。

- SME クラスタの詳細
- SME クラスタ インターフェイス情報
- クラスタ内のホストとターゲット
- SME クラスタ キー データベース
- クラスタ ノード
- SME クラスタのリカバリ 責任者情報
- SME クラスタ情報の要約

- クラスタ内のテープ
- テープ ボリューム グループ情報
- クラスタ内のディスク グループ
- クラスタ内のディスク
- SME ロール コンフィギュレーション

**show sme cluster** コマンドのサンプル出力は、次のとおりです。

```
switch# show sme cluster clustername1 ?
detail      Show sme cluster detail
interface   Show sme cluster interface
it-nexus    Show it-nexuses in the cluster
key         Show sme cluster key database
node        Show sme cluster node
recovery    Show sme cluster recovery officer information
summary     Show sme cluster summary
tape        Show tapes in the cluster
tape-bkgrp  Show crypto tape backup group information
|           Output modifiers.
>           Output Redirection.
<cr>       Carriage return.
```

```
switch# show sme cluster clustername1 interface
Interface sme4/1 belongs to local switch
Status is up
```

```
switch# show sme cluster clustername1 interface it-nexus
```

```
-----
      Host WWN                VSAN    Status    Switch    Interface
      Target WWN
-----
10:00:00:00:c9:4e:19:ed,
2f:ff:00:06:2b:10:c2:e2      4093    online    switch    sme4/1
```

## クラスタ キー情報の表示

クラスタ キー データベースに関する情報を表示するには、**show sme cluster key** コマンドを使用します。

SME テープに対する **show sme cluster key** コマンドのサンプル出力は、次のとおりです。

```
switch# show sme cluster clustername1 key database
Key Type is tape volumegroup shared key
  GUID is 3b6295e111de8a93-e3f9-e4ae372b1626
  Cluster is clustername1, Tape backup group is HR1
  Tape volumegroup is Default

Key Type is tape volumegroup wrap key
  GUID is 3e9ef70e0185bb3c-ad12-c4e489069634
  Cluster is clustername1, Tape backup group is HR1
  Tape volumegroup is Default

Key Type is master key
  GUID is 8c57a8d82d2098ee-3b27-6c2b116a950e
  Cluster is clustername1, Master Key Version is 0
```

SME ディスクに対する **show sme cluster key** コマンドのサンプル出力は、次のとおりです。

```
switch# show sme cluster clustername1 key database
Key Type is disk key
  GUID is aa8c86a783c8a0d9-34ba9cf3af0a17af
  Cluster is C_SSL, Crypto disk group is DG
  Crypto disk is Disk0

Key Type is master key
  GUID is fc66b503982e816d-a68eba9850f29450
  Cluster is C_SSL, Master Key Version is 0
```

## クラスタ ノード情報の表示

ローカルまたはリモート スイッチに関する情報を表示するには、**show sme cluster node** コマンドを使用します。

**show sme cluster node** コマンドのサンプル出力は、次のとおりです。

```
switch# show sme cluster clustername1 node
Node switch is local switch
  Node ID is 1
  Status is online
  Node is the master switch
  Fabric is f1
```

## リカバリ 責任者情報の表示

特定のリカバリ 責任者に関する情報、または特定のクラスタのすべてのリカバリ 責任者の情報を表示できます。

```
switch# show sme cluster clustername1 recovery officer
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
  Cluster is clustername1, Master Key Version is 0
  Recovery Share Version is 0, Share Index is 1
```

```
switch# show sme cluster clustername1 summary
-----
Cluster          ID                               Security Mode   Status
-----
clustername1    2e:00:00:05:30:01:ad:f4        basic           online
```

## SME クラスタ管理の機能履歴

表 4-2 に、この機能のリリース履歴を示します。

表 4-2 SME クラスタ管理の機能履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
高可用性 KMC サーバ	4.1(3)	高可用性 KMC は、プライマリ サーバとセカンダリ サーバを使用して設定できます。 4.1(3) では、HA の設定は [Key Manager Settings] ページで確認できます。 プライマリ サーバとセカンダリ サーバは、クラスタの作成時に選択できます。 プライマリ サーバとセカンダリ サーバの設定は、[Cluster Detail] ページで変更できます。
ホスト名は、サーバアドレスとして受け入れられます	4.1(3)	サーバ用に IP アドレスまたはホスト名を入力できます。
ターゲット ベースのロード バランシング	3.3(1c)	クラスタリングにより、SME サービスのターゲット ベースでのロード バランシングが可能になります。
転送設定	3.3(1c)	SME の転送設定は、ユーザがイネーブルまたはディセーブルにできます。



## SME テープの設定

この章では、SME を使用して暗号化されるテープの管理に関する情報が含まれています。  
この章では、次の事項について説明します。

- [SME テープ管理に関する情報 \(5-1 ページ\)](#)
- [CLI を使用した SME テープ管理の設定 \(5-2 ページ\)](#)
- [SME テープ管理設定の確認 \(5-7 ページ\)](#)
- [SME テープ管理のモニタリング \(5-7 ページ\)](#)
- [SME テープ管理の機能履歴 \(5-11 ページ\)](#)

## SME テープ管理に関する情報

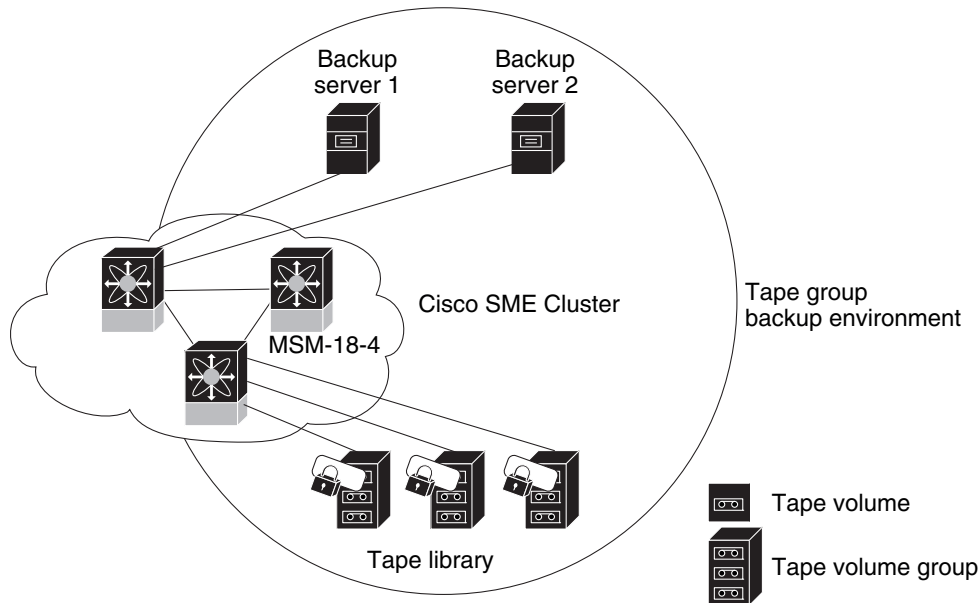
プロビジョニングしたら、SME は、ホストとターゲットに透過性を提供します。ホストからテープデバイスへのパスを管理するために、SME を次のものを使用します。

- **テープグループ:** SAN のバックアップ環境。すべてのテープバックアップサーバ、およびテープバックアップサーバがアクセスするテープライブラリで構成されています。
- **テープデバイス:** 暗号化用に設定されているテープドライブ。
- **テープボリューム:** 特定の用途のためにバーコードで識別される物理テープカートリッジ。
- **テープボリュームグループ:** 特定の用途のために設定されているテープボリュームの論理セット。SME を使用して、テープボリュームグループは、バーコードの範囲または指定の正規表現を使用して設定できます。自動ボリュームグループでは、テープボリュームグループは、バックアップアプリケーションで設定されているボリュームプール名にすることができます。

SME は、暗号化パスワードを使用してボリュームグループをエクスポートする機能が提供されます。このファイルは、後からボリュームグループにインポートできます。また、ボリュームグループフィルタリングオプションでは、特定のボリュームグループに含める情報のタイプを指定できます。たとえば、バーコードの範囲を指定して、ボリュームグループ内に含める情報をフィルタリングできます。

図 5-1 は、SME のテープ バックアップ環境を示しています。

図 5-1 SME のテープバックアップ環境と設定



185917

次の概念は、テープ管理手順で使用されます。

- キー管理設定
- 自動ボリューム グループ
- キーオンテープ
- 圧縮
- ボリューム グループの設定



(注)

データが部分的に非 SME 暗号化のテープに書き込まれると、クリア テキストのまま残ります。テープは、リサイクル時またはラベル再作成時に、SME により暗号化されます。

## CLI を使用した SME テープ管理の設定

この項では、次のトピックについて取り上げます。

- [テープ圧縮のイネーブル化とディセーブル化\(5-3 ページ\)](#)
- [キーオンテープのイネーブル化とディセーブル化\(5-3 ページ\)](#)
- [テープ ボリューム グループの設定\(5-3 ページ\)](#)
- [自動ボリューム グループのイネーブル化およびディセーブル化\(5-4 ページ\)](#)
- [テープ グループへのテープ デバイスの追加\(5-5 ページ\)](#)
- [テープ デバイスへのパスの追加\(5-5 ページ\)](#)

## テープ圧縮のイネーブル化とディセーブル化

### 手順の詳細

テープ圧縮をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>tape-compression</b> switch(config-sme-cl)#	テープ圧縮をイネーブルにします。
ステップ 4	switch(config-sme-cl)# <b>no tape-compression</b> switch(config-sme-cl)#	テープ圧縮をディセーブルにします。

## キーオンテープのイネーブル化とディセーブル化

SME には、バックアップ テープ上に暗号化されたセキュリティ キーを保存するオプションがあります。

### 手順の詳細

キーオンテープ機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>key-ontape</b> switch(config-sme-cl)#	キーオンテープ機能をイネーブルにします。
ステップ 4	switch(config-sme-cl)# <b>no key-ontape</b> switch(config-sme-cl)#	キーオンテープ機能をディセーブルにします。

## テープ ボリューム グループの設定

テープ ボリューム グループは、通常は機能別に分類されているテープのグループです。たとえば、HR1 はすべての人事部門のテープ バックアップ用の指定されたテープ ボリューム グループ、EM1 はすべての電子メールのバックアップテープ用の指定されたテープ ボリューム グループなどとなります。

テープ グループの追加により、SME が暗号化されたデータ用に使用する、VSAN、ホスト、ストレージデバイス、およびパスを選択することができます。たとえば、HR データ用のテープ グループを追加することで、SME のマッピングはデータを HR ホストから専用の HR バックアップ テープに転送するように設定されます。

## 手順の詳細

テープ ボリューム グループを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# sme cluster clustername1</code> <code>switch(config-sme-cl)#</code>	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	<code>switch(config-sme-cl)# tape-bkgrp groupname1</code> <code>switch(config-sme-cl-tape-bkgrp)#</code>	テープ ボリューム グループを指定し、SME テープ ボリューム グループ サブモードを開始します。
ステップ 4	<code>switch(config-sme-cl-tape-bkgrp)# tape-device devicename1</code> <code>switch(config-sme-cl-tape-bkgrp-tapedevice)#</code>	テープ デバイス名を指定し、SME テープ デバイス サブモードを開始します。
ステップ 5	<code>switch(config-sme-cl-tape-bkgrp-tapedevice)# tape-device devicename1 D</code> <code>switch(config-sme-cl-tape-bkgrp-tapedevice)#</code>	テープ カートリッジ ID を指定します。
ステップ 6	<code>switch(config-sme-cl-tape-bkgrp-tapedevice)# host 10:00:00:00:c9:4e:19:ed target 2f:ff:00:06:2b:10:c2:e2 vsan 4093 lun 0 fabric f1</code> <code>switch(config-sme-cl-tape-bkgrp-tapedevice)#</code>	テープ ボリューム グループ用のホストとターゲット、VSAN、LUN、およびファブリック (f1) を指定します。
ステップ 7	<code>switch(config-sme-cl-tape-bkgrp-tapedevice)# enable</code>	テープ デバイスをイネーブルにします。

## 自動ボリューム グループのイネーブル化およびディセーブル化

テープ バーコードが既存のボリューム グループに属していないことを SME が認識すると、SME は自動ボリューム グループ化をイネーブルにして、新しいボリューム グループを作成します。

デフォルトでは、自動ボリューム グループ化はディセーブルになっています。

## 手順の詳細

自動ボリューム グループ化をイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# sme cluster clustername1</code> <code>switch(config-sme-cl)#</code>	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	<code>switch(config-sme-cl)# auto-volgrp</code> <code>switch(config-sme-cl)#</code>	自動ボリューム グループを指定します。
ステップ 4	<code>switch(config-sme-cl)# no auto-volgrp</code> <code>switch(config-sme-cl)#</code>	自動ボリューム グループを指定しません。



## テープ グループへのテープ デバイスの追加

テープ デバイスは、テープ グループの一部として指定され、エイリアスとしての名前で認識されます。

### 手順の詳細

テープ デバイスをテープ グループを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>tape-bkgrp groupname1</b> switch(config-sme-cl-tape-bkgrp)#	テープ ボリューム グループを指定し、SME テープ ボリューム グループ サブモードを開始します。
ステップ 4	switch(config-sme-cl-tape-bkgrp)# <b>tape-device devicename1</b> switch(config-sme-cl-tape-bkgrp-tape device)#	テープ デバイス名を指定し、SME テープ デバイス サブモードを開始します。
ステップ 5	switch(config-sme-cl-tape-bkgrp-tape device)# <b>tape-device devicename1 D</b> switch(config-sme-cl-tape-bkgrp-tape device)#	テープ カートリッジ ID を指定します。

## テープ デバイスへのパスの追加



### 注意

サーバとストレージの間のパスをホストするすべての IT-Nexus を設定に追加する必要があります。そのようにしないとデータの整合性は危険にさらされます。

テープ デバイスは、テープ グループの一部として指定され、エイリアスとしての名前で認識されます。クラスタ内のテープ デバイスへのすべてのパスは、ホスト、ターゲット、LUN、VSAN、およびファブリックを使用して指定される必要があります。

### 手順の詳細

クラスタ内のテープ デバイスへのパスを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>tape-bkgrp groupname1</b> switch(config-sme-cl-tape-bkgrp)#	テープ ボリューム グループを指定し、SME テープ ボリューム グループ サブモードを開始します。

	コマンド	目的
ステップ 4	switch(config-sme-cl-tape-bkgrp)# <b>tape-device devicename1</b> switch(config-sme-cl-tape-bkgrp-tape device)#	テープ デバイス名を指定し、SME テープ デバイス サ ブモードを開始します。
ステップ 5	switch(config-sme-cl-tape-bkgrp-tape device)# <b>tape-device devicename1 D</b> switch(config-sme-cl-tape-bkgrp-tape device)#	テープ カートリッジ ID を指定します。
ステップ 6	switch(config-sme-cl-tape-bkgrp-tape device)# <b>host</b> <b>10:00:00:00:c9:4e:19:ed target</b> <b>2f:ff:00:06:2b:10:c2:e2 vsan 4093</b> <b>lun 0 fabric f1</b> switch(config-sme-cl-tape-bkgrp-tape device)#	テープ ボリューム グループ用のホストとターゲット、 VSAN、LUN、およびファブリック (f1) を指定します。
ステップ 7	switch(config-sme-cl-tape-bkgrp-tape device)# <b>no host</b> <b>10:00:00:00:c9:4e:19:ed target</b> <b>2f:ff:00:06:2b:10:c2:e2 vsan 4093</b> <b>lun 0</b> switch(config-sme-cl-tape-bkgrp-tape device)#	指定されたパスをテープ ドライブから削除します。



(注)

上記のパスで指定された IT-Nexus が SME で設定されていない場合、SME は、設定済みのパスを指定のテープ デバイスに追加するとともに、IT-Nexus の検出をトリガーします。スクリプト化された環境では、パスを追加するときに、IT-Nexus 検出が完了できるように 1 分間の遅延を設定することをお勧めします。

## テープ暗号化のバイパス

テープ デバイスを作成したら、バイパス機能をイネーブルまたはディセーブルにできます。



(注)

デフォルトでは、暗号化のバイパスはディセーブルになっています。クリア テキストテープがロードされると、書き込みは失敗します。

### 手順の詳細

テープ暗号化のバイパスをイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <b>clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを 開始します。
ステップ 3	switch(config-sme-cl)# <b>tape-bkgrp</b> <b>groupname1</b> switch(config-sme-cl-tape-bkgrp)#	テープ ボリューム グループを指定し、SME テープ ボ リューム グループ サブモードを開始します。

	コマンド	目的
ステップ 4	switch(config-sme-cl-tape-bkgrp)# <b>tape-device tapename1</b> switch(config-sme-cl-tape-bkgrp tape-device tapename1)#	クリア テキスト データがあるテープを指定します。
ステップ 5	switch(config-sme-cl-tape-bkgrp-tape device)# <b>no by pass</b>	クリア テキスト テープの使用時に書き込みを拒否する、テープデバイスのバイパス ポリシーを指定します。
	switch(config-sme-cl-tape-bkgrp-tape device)# <b>by pass</b>	クリア テキストでのデータの通過を許可する、テープデバイスのバイパス ポリシーを指定します。



## 注意

サーバとストレージの間のパスをホストするすべての IT-Nexus を設定に追加する必要があります。そのようにしないとデータの整合性は危険にさらされます。

## SME テープ管理設定の確認

SME テープ管理の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show sme cluster tape</b>	テープに関する要約または詳細情報を表示します。
<b>show sme cluster tape detail</b>	テープ カートリッジに関する情報を表示します。
<b>show sme cluster tape-bkgrp</b>	すべてのテープ ボリューム グループまたは特定のグループに関する情報を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『Cisco MDS 9000 Family NX-OS Command Reference』を参照してください。

## SME テープ管理のモニタリング

この項では、次のトピックについて取り上げます。

- [ホストの詳細の表示 \(5-7 ページ\)](#)
- [テープの詳細情報の表示 \(5-8 ページ\)](#)
- [CLI を使用した SME テープ情報の表示 \(5-8 ページ\)](#)

### ホストの詳細の表示

SME クラスタ内のホストに関する詳細情報を表示できます。特定のホストに関する情報には、テープ グループ メンバーシップ、ホストからターゲットへのパス、VSAN、ファブリック、ステータス、およびテープ デバイスが含まれます。

## テープの詳細情報の表示

SME クラスタのテープデバイスに関する詳細情報を表示できます。特定のテープデバイスに関する情報には、テープグループメンバーシップ、デバイスの説明、シリアル番号、ホストとターゲットの PWWN が含まれます。

## CLI を使用した SME テープ情報の表示

テープの概要についての詳細情報を表示するには、**show sme cluster tape** コマンドを使用します。

```
switch# show sme cluster clusternam1 tape summary
-----
Host WWN                Description                Crypto-Tape                Status
                        Backup Group
-----
10:00:00:00:c9:4e:19:ed  HP Ultrium 2-SCSI        HR1                        online
```

## テープカートリッジ情報の表示

テープカートリッジに関する情報を表示するには、**show sme cluster tape detail** を使用します。

```
switch# show sme cluster clusternam1 tape detail
Tape 1 is online
  Is a Tape Drive
  HP Ultrium 2-SCSI
  Serial Number is 2b10c2e22f
  Is a member of HR1
  Paths
    Host 10:00:00:00:c9:4e:19:ed Target 2f:ff:00:06:2b:10:c2:e2 LUN 0x0000
```

## テープボリュームグループ情報の表示

すべてのテープボリュームグループまたは特定のグループに関する情報を表示するには、**show sme cluster tape-bkgrp** コマンドを使用します。

```
switch# show sme cluster clusternam1 tape-bkgrp
-----
Name                Tape Devices                Volume Groups
-----
HR1                  1                            1

switch# show sme cluster clusternam1 tape-bkgrp HR1
Tape Backupgroup HR1
  Compression is Disabled
  Number of tape devices is 1
  Number of volume groups is 1

Tape device td1 is online
  Is a tape drive
  Description is HP Ultrium 2-SCSI
  Serial number is 2b10c2e22f
  Paths
    Host 10:00:00:00:c9:4e:19:ed Target 2f:ff:00:06:2b:10:c2:e2 Lun 0x0000 vsan 4093[f1]
```

## テープデバイスのステータスの表示

テープ情報を表示するには、**show sme internal info cluster <cname> tape-all** コマンドを使用します。

```
Switch# show sme internal info cluster tie1 tape-all
```

```
Tape Backup Groups : 1
Last Seq Id       : 1

Tape Backup Group : tb2
Memory Address    : 0x10788854
Seq Id           : 1
Compression      : Enabled
Key on Tape      : Disabled
Tape Key Recycle : Enabled
Shared Key Mode  : Disabled
Auto Volume Group : Disabled
Tape Devices     : 1
Last Device Seq Id : 4
Tape Volgrps    : 1
Last Volgrp Seq Id : 1

Tape Devices : 1
Last Seq Id  : 4

Tape Device : td0
Memory Address : 0x107ba054
Seq ID       : 4
SME (Encryption) : Enabled
Compression  : Enabled
Bypass-Policy : BYPASS DISABLED
Cached Lun Path : (nil)
FSM State    : SME_CTAPE_DEVICE_G_ST_STABLE
ITL Count    : 1
Tape Drive   : 0x107d123c
LUN FSM State : SME_LUN_ST_STABLE

Lun Path :0x107d185c
IT       :V 3 I 40:00:00:00:00:00:00:01 T 40:00:00:00:00:00:00:02
LUN      :0x0000
Is Configured
Status   :2
Error    :0x0
Flags    :0x1
```

特定のテープバックアップグループの特定のテープデバイスに関する情報を表示するには、**sh sme internal info cluster tie1 tape-bkgrp tb2 tape-device td0**を使用します。

```
Switch# sh sme internal info cluster tie1 tape-bkgrp tb2 tape-device td0
```

```
Tape Device : td0
Memory Address : 0x107ba054
Seq ID       : 4
SME (Encryption) : Enabled
Compression  : Enabled
Bypass-Policy : BYPASS DISABLED
Cached Lun Path : (nil)
FSM State    : SME_CTAPE_DEVICE_G_ST_STABLE
ITL Count    : 1
Tape Drive   : 0x107d123c
LUN FSM State : SME_LUN_ST_STABLE
```

```

Lun Path :0x107d185c
IT       :V 3 I 40:00:00:00:00:00:00:01 T 40:00:00:00:00:00:00:02
LUN      :0x0000
Is Configured
Status   :2
Error    :0x0
Flags    :0x1

```

暗号用に設定されている SME インターフェイスに関する統計情報を表示するには、**Show Interface smex/y** を使用します。

```

Switch# sh int smel/1
smel/1 is up

```

```

  In fabric Fabric_sw119
  Member of cluster tie1

```

SME	IOs	IO/s	Bytes	Rate
Host Reads	0	0	0	0.00 B/s
Host Writes	0	0	0	0.00 B/s
Host Total	0	0	0	0.00 B/s
Tgt Reads	0	0	0	0.00 B/s
Tgt Writes	0	0	0	0.00 B/s
Tgt Total	0	0	0	0.00 B/s
Clear	IOs	IO/s	Bytes	Rate
Host Reads	0	0	0	0.00 B/s
Host Writes	0	0	0	0.00 B/s
Host Total	0	0	0	0.00 B/s
Tgt Reads	0	0	0	0.00 B/s
Tgt Writes	0	0	0	0.00 B/s
Tgt Total	0	0	0	0.00 B/s

```

Compression Ratio      0 : 0
SME to Clear           0.00 %
Read to Write          0.00 %

```

```

Clear Luns 1, Encrypted Luns 0

```

#### Error Statistics

```

0 CTH, 0 Authentication 0 Compression
0 Key Generation, 0 Incorrect Read Size
0 Overlap Commands, 0 Stale Key Accesses
0 Overload Condition, 0 Incompressible
0 XIPC Task Lookup, 0 Invalid CDB
0 Ili, 0 Eom, 0 Filemark, 0 Other

```

```

2 FAILED WRITE Count - BYPASS DISABLED by USER =====> If write fails for clear text

```

```
tape
```

```
last error at Tue Jun 26 13:39:49 2012
```

モジュール コマンドを使用して、LUN 固有の情報を表示します。

```
show sme internal info crypto-node 1 lun all
```

```
module-1# sh sme internal info crypto-node 1 lun all
```

```
TAPE LUN TREE
```

```
LUN
```

```
---
```

```

cpp_lun_ndx          0x5
serial no.           0003-0000-00000000:0000000000000000
type                  sequential
sme_enabled          1

```

```

crypto_status          0
vendor_id              SONY
product_id             SDZ-130
asl_id
prod_rev_level        0201
vendor_specific
cluster_name          tie1
enable_pad            False
pad to                 0x0
bkgrp_name            tb2
device_name           td0
flags                 0
granularity           2
max_block_len_lim     1000
min_block_len_lim     4
block_length          512
compression           1
key_ontape            0
Bypass_Policy         BYPASS DISABLED
has tape              yes
position              200
has cth               no
bypass enc            no
wrap_guid             0000000000000000-0000000000000000
media guid            0000000000000000-0000000000000000
total itl count       1
active itl count      1
cmd_send_err          0
Not locked

```

## SME テープ管理の機能履歴

表 5-1 に、この機能のリリース履歴を示します。

表 5-1 SME テープ設定の機能履歴

機能名	リリース	機能情報
新しい SME テープ コマンドが追加されました	5.2(6)	新しい SME テープ コマンドが追加されました。
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリースは変更されておらず、参照はすべて維持されています。







## SME ディスクの設定

この章では、SME ディスク管理と呼ばれる、SME を使用したディスクの管理について説明します。



(注)

SME ディスクを設定する際には、すべての注意をよくお読みください。

この章では、次の事項について説明します。

- [SME ディスク管理について \(6-1 ページ\)](#)
- [DKR に関する注意事項および制約事項 \(6-14 ページ\)](#)
- [CLI を使用した SME ディスク管理の設定 \(6-17 ページ\)](#)
- [SME ディスク管理設定の確認 \(6-34 ページ\)](#)
- [SME ディスク管理のモニタリング \(6-35 ページ\)](#)

## SME ディスク管理について

SME ディスク管理では、次の項目を取り上げます。

- [SME ディスク アーキテクチャ \(6-2 ページ\)](#)
- [複製 \(6-3 ページ\)](#)
- [スナップショット \(6-4 ページ\)](#)
- [SME による複製の管理 \(6-4 ページ\)](#)
- [SME でのスナップショット管理 \(6-5 ページ\)](#)
- [データ準備 \(6-6 ページ\)](#)
- [キー再生成 \(6-9 ページ\)](#)
- [SME が有効な MDS スイッチの交換 \(6-9 ページ\)](#)
- [SME ディスクのキー管理 \(6-10 ページ\)](#)
- [Cisco KMC \(6-11 ページ\)](#)
- [データ レプリケーション \(6-13 ページ\)](#)
- [SME ディスクキー複製 \(6-13 ページ\)](#)
- [SME ディスクと ISSU \(6-16 ページ\)](#)

## SME ディスク アーキテクチャ

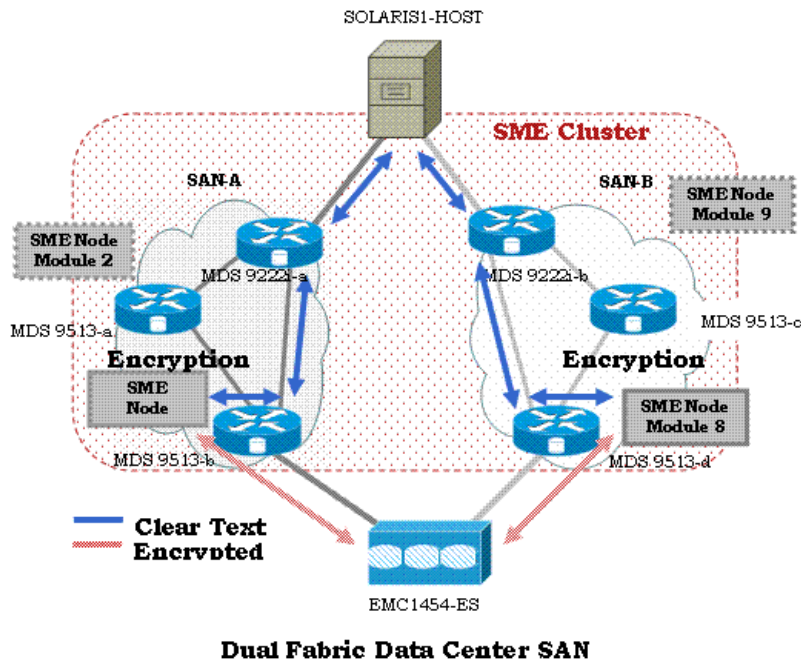
SME ディスク機能は、ディスクに格納されているデータを暗号化します。

SME ディスクのソフトウェア アーキテクチャは、SME テープをサポートする既存の SME インフラストラクチャに似ています。ディスク サポートは、MDS NX-OS リリース 5.2.1 から既存の SME アーキテクチャに追加されました。図 6-1 は、一般的なデュアルファブリック生産データセンターを示しています。SME ディスク機能は、次の Cisco MDS ハードウェアで提供されます。

- 16 ポート ストレージ サービス ノード (SSN-16) モジュール
- 18/4 マルチサービス モジュール (MSM-18/4)
- 9222i スイッチ

図 6-1 は、SME ディスク アーキテクチャを示しています。

図 6-1 SME ディスク アーキテクチャ



この図では、スイッチを SME ノードと呼びます。モジュールには、SME をサポートする 1 つ以上のインターフェイスがあります。SME ノードは、ホストとストレージの間を流れるトラフィックを暗号化および復号化します。暗号化または復号化されるファイバチャネルトラフィックは、SAN の FC-Redirect 機能を使用して SME ノードに転送されます。たとえば、SSN-16 は 4 つの SME インターフェイスをサポートでき、MSM-18/4 は 1 つの SME インターフェイスをサポートします。

SME ディスク機能はデュアルファブリックトポロジで動作します。これは、ホストとストレージの間に存在するすべてのパスで暗号化と復号化を実行します。



注意

SME ディスクは、ディスクのシンプロビジョニングをサポートしていません。

SME ディスクは、両方のファブリックでディスクへのすべてのパスを管理する必要があります。SME クラスタがこの機能を提供します。SME クラスタは、SME ノードのコレクションで構成されます。クラスタ内にある SME ノードは、同じクラスタ内の別のノードをトリガーして、暗号化や復号化のアクティビティを制御します。

SME ディスクが暗号化や復号化の機能を提供するディスクは、既存のデータのないディスクでも、既存のデータのあるディスクでも構いません。ディスクに既存のデータがある場合、既存のデータは暗号化される必要があります。既存のクリア データを暗号化されたデータに変換するプロセスは、データ準備と呼ばれます。

データ準備はオフライン モードで実行できます。オフライン データ準備モードでは、ディスクにアクセスするホスト上のアプリケーションが休止され、ディスクに I/O は送信されません。SME ディスク機能によって、ホストがディスクに対してデータを読み書きしようとする、特定の I/O がホストにフェールバックされるようになります。

オンライン モードでは、SME がディスク上の既存のデータをクリア テキストから暗号化されたテキストに変換しているときに、ホスト上のアプリケーションがディスクで I/O を実行し続けることができます。

ディスクは、クラスタ名、ディスク グループ名、およびディスク名によって、設定で一意的に識別されます。

暗号化または復号化のために、SME ディスクには暗号キーが必要です。ディスク暗号化ごとにキーが生成されます。SME ディスクのキー管理では、SME の既存の Key Management Center (KMC) インフラストラクチャが使用されます。各ディスクのキーは、Storage Media Encryption コプロセッサによって生成され、SME Key Management Center に保存されます。

**注意**

SME ディスクでは、LUN の動的なサイズ変更を許可しません。

リリース 5.2.1 では、サポートされる最大ディスク サイズは 2 テラバイト (TB) より 1 ブロック少ないサイズです。最大 LBA は 0xFFFFFFFFE です。

リリース 5.2.6 からは、シグニチャおよび非シグニチャ モードのクラスタでサポートされるディスク サイズが 2 TB を超えます。

SME ディスクでは、512 バイトのディスク ブロック サイズのみをサポートしています。

リリース 5.2.1 では、ディスク上の既存のクリア データから暗号化されたデータへのオンライン変換がサポートされていません。

## 複製

複製には次の 2 種類があります。

- ミラーまたはクローン: ディスク アレイによって送信元ディスクのデータが同じストレージシステム内の別のディスクに複製されると、宛先ディスクは送信元ディスクのミラーまたはクローンと呼ばれます。これは、ローカル複製と呼ばれます。
- リモート複製: ディスク アレイによって送信元ディスクのデータがリモート ストレージシステム内の別のディスクに複製されると、送信元ディスクとリモート ディスクは複製関係になります。ローカルとリモート サイトの間の距離と帯域幅の可用性に基づいて、リモート複製は次のタイプに分類されます。

- 同期: ローカル ディスク アレイは、データがリモート LUN にも書き込まれるまで、ローカル LUN での書き込みコマンドに応答しません。
- 非同期: ローカル ディスク アレイは、リモート LUN にただちにデータを書き込みません。ローカル LUN への変更は、デルタ データセットにバッチ処理されて、リモート LUN に定期的に送信されます。

## スナップショット

スナップショットは、送信元ディスクに対してすぐに作成可能なポイントインタイム コピーです。スナップショットが作成されると、送信元ディスクへの書き込みによって、変更前に以前のデータが別の場所に保存されます。これにより、ディスク アレイは送信元ディスクの特定のポイントインタイム コピーを示すことができます。

## SME による複製の管理

SME は、ディスク キー複製(DKR)を通じて複製をサポートします。DKR は、送信元ディスクのキーを宛先ディスクに伝達する処理を自動化することによって、送信元と宛先のディスクのキー管理を簡素化します。SME ディスク クラスタには、2つのモードがあります。

- 非シグニチャ クラスタ
- シグニチャ クラスタ

複製管理は両方のクラスタ モードとも同じです。複製管理は次の手順で構成されています。

- アレイ ベンダー固有の技術を使用した複製関係の抽出。この手順の出力によって、ベンダー、製品、およびデバイス識別子の SCSI プロパティを基に、送信元と宛先ディスクの関係を特定できます。
- DCNM を使用し DKR を介した SME への複製関係情報のインポート。



(注) DCNM のみを使用して、DKR 関係にあるディスク上ですべての SME 設定操作を管理してください。

## DCNM for DKR でのキー変更操作の管理

キー変更操作には、次のオプションがあります。

- データ準備なし: ローカル キー変更によって、DKR はリモート ディスクへのホスト アクセスを中断します。ローカル キー変更でデータの整合性が検証され、リモート エンドへのデータ レプリケーションが同期されたら、管理者は対応する関係を選択し、DKR で同期処理を実行できます。この操作により、送信元と宛先のキーが同期され、リモート ディスクへのホスト アクセスが再開されます。
- データ準備: 送信元ディスクでデータ準備を開始する前に、DKR 関係、および送信元と宛先ディスクの間の複製を無効にしてください。これは、ディスク アレイ ベンダー固有の操作です。データ準備が完了し、データの整合性を確認したら、次の手順に従ってください。
  - ディスク アレイ ベンダー固有の操作を使用して、送信元と宛先の間でのデータ レプリケーションを有効にします。
  - データが送信元と宛先のディスクの間で同期されたら、DKR 関係を有効にします。この操作は、送信元と宛先のキーを同期します。



(注) 宛先ディスク上のホストアクセスは、上記の2つの手順が完了するまで一時停止される必要があります。

## SME でのスナップショット管理

このセクションでは、暗号化ディスクのスナップショットを管理する方法について説明します。スナップショット管理は、シグニチャクラスタと非シグニチャクラスタで異なります。

送信元ディスクと同じ SME クラスタを介して同じホストによって検出される暗号化スナップショットを管理するには、次の手順に従ってください。

- ステップ 1 スナップショット ディスクを設定するために、SME でディスクカバリを開始します。
- ステップ 2 Key Management Center (KMC) 内に対応するアクティブ キーがないディスク メディアで有効な SME メタデータを SME が検出した場合、ディスクは SME によって失敗状態になります。
- ステップ 3 管理者には、メタデータからの回復オプションを使用してディスクを回復するオプションがあります。
- ステップ 4 上記のリカバリが実行されると、スナップショットは暗号化ディスクとして起動し、ホストからアクセスできるようになります。

送信元とは異なる SME クラスタを介して別のホストによって検出されたスナップショットを管理するには、DKR を使用して次の手順に従います。

- ステップ 1 スナップショット ディスクを設定するために、SME でディスクカバリを開始します。
- ステップ 2 スナップショット ディスクが SME に設定されたら、送信元とスナップショットディスクの間の DKR 関係を作成します。
- ステップ 3 DKR 関係で送信元とスナップショット キーを同期できるようにします。
- ステップ 4 送信元とスナップショットの間の DKR 関係を破棄します。
- ステップ 5 ホストはスナップショット ディスクにアクセスできるようになります。



(注) キーの同期後に、送信元とスナップショットの間の DKR 関係を破棄したことを確認します。送信元キーが再生成されると、スナップショットでデータの整合性に関する問題が発生する可能性があります。

## クラスタのサポート

リリース 5.2.1 では、スイッチで最大 2 つの SME クラスタをサポートできます。複数のクラスタをサポートするには、次の前提条件を満たす必要があります。前提条件が満たされない場合、データ損失が発生する可能性があります。

- SME ディスクでは、SME クラスタがディスク対応として設定される必要があります。

- SME テープおよび SME ディスクは、同じ SME クラスタ上で共存できません。SME ディスクと SME テープには異なるクラスタを使用してください。
- 次の条件を満たす同一の MDS シャーシで、複数の SME クラスタをサポートできます。
  - SME テープ クラスタ ノードは、一方の Cisco MSM 18/4 スイッチング モジュール上にある。
  - SME ディスク クラスタ ノードは、もう一方の Cisco MSM 18/4 スイッチング モジュール上にある。
  - SSN-16 では、SME テープおよびディスクは別々の暗号化ノードに属し、異なるクラスタに属している。
- 異なるクラスタで同じターゲット ポートを使用しないでください。
- 同一のディスクが複数の SME クラスタに属することはできません。そうしないと、データ損失が発生します。
- 2つの異なるクラスタ内で同じ SME インターフェイスを追加しないでください。

MDS リリース 5.2(6) 以降、ディスクを暗号化ディスクとして識別するように SME ディスクはメディアにシグニチャを書き込むことができます。これらの SME クラスタは、シグニチャ クラスタと呼ばれます。非シグニチャ クラスタは、ディスクで暗号化を特定するためのシグニチャをメディアに書き込まない SME ディスクです。

## データ準備

データ準備は、ディスク上のクリア データと暗号化されたデータとを相互に変換するプロセスです。クリア データを含む既存のディスクで SME ディスク機能が有効な場合、既存のクリア データを暗号化されたデータに変換する必要があります。このプロセスには、次の 2 つの方法があります。

- データにアクセスするホストを使用する。これはオンライン データ準備モードと呼ばれます。
- ホストにアクセスできないディスクを使用する。これはオフライン データ準備モードと呼ばれます。



(注) オフライン データ準備モードのみがサポートされています。

以前のデータが含まれない新しいディスクで SME ディスク機能が有効になると、ホスト I/O の読み取り/書き込みはキーを使用して復号化または暗号化されます。この暗号化プロセスは、アプリケーションに透過的です。これらのディスクでは、データ準備プロセスは必要ではありません。



(注) データ準備が進行中の場合はクラスタの設定を変更しないでください。また、データ準備が進行中の場合はノードを削除したり新しいノードを追加したりしないでください。

データ準備が必要なディスクでは、クリア データから暗号化されたデータへの変換を開始する前に、データをバックアップしておく必要があります。

SME クラスタでは、特定の暗号化ディスクに関連付けられた ITL を処理する複数の SME ノードを設定できます。暗号化ディスクに対して書き込み/読み取りされるデータを複数の SME ノードで暗号化または復号化します。ただし、暗号化ディスクのデータ準備またはキー再生は、データ準備ノードである 1 つの SME ノードにその処理が割り当てられます。クラスタ マスターは、次に基づいてデータ準備ノードを処理します。

- LUN の可視性(LUN や INQ などのレポート)またはアクセシビリティ(予約)
- ターゲット ポート アフィニティ
- SME ノードの負荷要因

シグニチャ モードでは、クリア ディスクを暗号化ディスクに変換するときに、管理者は SME ディスクの最後に 64 MB の予約領域を確保できることを確認する必要があります。



(注) 送信元ディスクでデータ準備を実行するときは、ディスク キー複製(DKR)を無効にする必要があります。

## データ準備が失敗したときの SME ディスクの回復

データ準備が失敗すると、SME ディスクは失敗状態になります。ディスクはホストにアクセスできず、ディスクのすべてのパスは、I/O 拒否状態になります(すべてのホスト I/O を拒否する状態)。ディスクを失敗状態から回復するには、次の手順を実行します。

- ステップ 1** ディスクはホストからアクセスできないため、バックエンドストレージで失敗したディスクのコンテンツを復元します。
- ステップ 2** 適切な引数を指定して **recover** コマンドを入力し、バックアップデータに基づいてディスクを適切な暗号化状態に回復します。CLI を使用した **recover** コマンドシンタックスの詳細については「[SME ディスクの回復](#)」セクション(6-28 ページ)を参照してください。

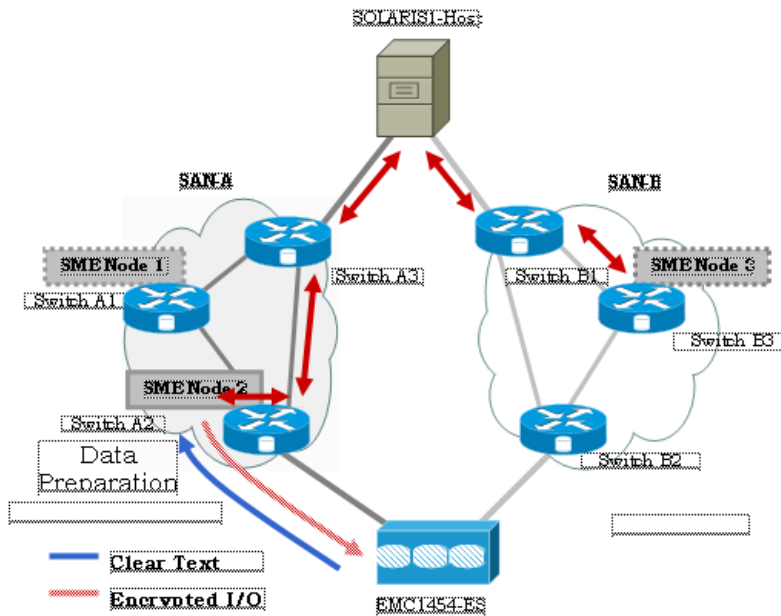
シグニチャ モードでは、メディア上のシグニチャ情報を使用してディスクを回復できます。

## オフラインデータ準備

オフラインデータ準備は、ホスト上で実行されているアプリケーションがデータ準備中のディスクのデータにアクセスしていないときに実行されます。

図 6-2 は、SME ディスクのオフラインデータ準備アーキテクチャを示しています。

図 6-2 SME ディスクのオフラインデータ準備アーキテクチャ



オフラインデータ準備には次のアクションが含まれます。

- ホスト I/O トラフィックを停止することで、ホストアプリケーションを一時停止する。
- ターゲットディスク内のクリアデータをバックアップする。バックアップ先は、別のディスクまたは外部テープにできます。このバックアップは、エラーから回復するために使用されます。
- オフラインデータ準備期間中のサーバ I/O は、SME ノードによって拒否されます。



注意

ホスト I/O がブロックされる間、ホストバスのアイデンティティが暗号化エンジンによって使用されるため、そのホストバスはオフラインデータ準備中にオンラインである必要があります。ディスクを利用するすべての DKR 関係は無効状態になっている必要があります。ディスクキー複製 (DKR) は、リモート複製関係を管理するために使用されます。



注意

ディスクのデータ準備を開始する前に、そのディスクのすべての複製リンクを無効にしてください。



注意

キー再生成が成功したら、古いスナップショットを破棄してください。古いスナップショットは、データ準備やキー再生成が失敗した場合に回復するために、バックアップとして保持できません。成功後、SME ディスクは以前のキーを使用した古いスナップショットの読み取りをサポートしません。



- オフラインデータ準備は、データ準備関連の I/O が発行されたディスクの選択パスのホスト アイデンティティを使用する 1 つの SME ノードで実行されます。このプロセスにおいて、ターゲット ディスクに対する I/O は、SCSI チェック状態が **not ready** であるホストにフェールバックされます。オフライン データ準備期間中のサーバ I/O は、SCSI チェック状態としてホストに送信されます。
- ホスト アプリケーションの一時停止の解除。データ準備が完了すると、ホスト上で実行されているアプリケーションはオンラインになり、暗号化された暗号化ディスクのデータにアクセスできるようになります。

## オンラインデータ準備

オンラインデータ準備は、ホスト上のアプリケーションが暗号化ディスク上のデータにアクセスしているときに実行されます。サーバの読み取りまたは書き込み I/O は、データ準備プロセスが進行中のときに SME ノードによって復号化または暗号化されます。



(注)

このリリースでは、オフラインデータ準備モードのみがサポートされます。

## キー再生成

ディスクのデータが暗号化されると、セキュリティ上の理由から、暗号化されたデータと関連付けられているキーを変更する必要があります。変更ポリシーは、組織固有です。ディスクの暗号化されたデータと関連付けられているキーを古いキーから新しいキーに変更するプロセスは、キー再生成プロセスと呼ばれます。

キー再生成はデータ準備作業の特別な機能であり、ディスクの現在の暗号化されたコンテンツが読み取られ、現在の(古い)キーを使用して復号化され、新しいキーを使用して暗号化され、ディスクに書き戻されます。



(注)

マスターキーのキー再生成中は、クォーラムまたはマスターノードを変更できません。

## SME が有効な MDS スイッチの交換

1 つ以上の SME クラスタ内でノードとして機能する MDS スイッチを交換する手順は、現在のトポロジと設定によって異なります。

### マルチノードクラスタ

交換する MDS スイッチが 1 つ以上の SME クラスタでマスターノードになっている場合は、最初にマスターノードに失敗してから、失敗したマスターノードを削除する必要があります。

交換する MDS スイッチがマルチノード SME クラスタで非マスターノードになっている場合は、DCNM SME 管理 UI を使用して SME インターフェイス(ある場合)およびノードをクラスタから削除する必要があります。

## シングルノードクラスタ

交換する MDS スイッチが SME クラスタ内で唯一のノードである場合、操作は SME クラスタに対して完全に破壊的です。付録 B「SME のディザスタ リカバリ」の手順に従って、新しいスイッチで新しい SME クラスタを構築してください。

## 暗号化の解除

シングニチャ モードで暗号化を無効にすると、ホストはディスクの正確なサイズを確認できます。ディスクの正確なサイズは、暗号化中に確認できるディスクのサイズより 64 MB 多くなります。

## スナップショットのサポート

サポートされるスナップショットには、次の 2 つのタイプがあります。

- 非シングニチャ モード: 非シングニチャ モードでは、スナップショットが最初に検出されたときに、SME は暗号化 LUN のスナップショットとして検出しません。管理者は、送信元 LUN のキーを使用し、新しい LUN でのデータ準備なしで暗号化を有効にする必要があります。
- シングニチャ モード: シングニチャ モードでは、ディスクカバリ時に SME ディスクはスナップショットを検出します。SME ディスクはメディアのシングニチャを検出し、これらのディスクを失敗状態に移行して、暗号化スナップショットの可能性があると説明を付記します。暗号化スナップショットで暗号化を有効にするには、メタデータからの回復オプションを使用できます。

## SME ディスクのキー管理

SME ディスクは、2 つのレベルのキー階層を使用します。SME クラスタはディスク グループに機能分類されるさまざまなディスクから構成されます。次に、キー階層を示します。

- マスター キー: SME クラスタの作成時に生成されます。マスター キーは、クラスタのディスク キーをラップするために使用されます。マスター キーは、パスワードで常にラップされず。マスター キーを保存するための 3 つのセキュリティ モードは、Basic、Standard、および Advanced です。SME キーの詳細およびセキュリティ モードの詳細については、「[SME キー管理の設定](#)」セクション(7-1 ページ)を参照してください。
- ディスク キー: 暗号化を有効にしたときのみ生成されます。有効な場合のみ、ディスクの状態が Crypto になります。ディスク キーは、マスター キーで常にラップされます。

キーはグローバル一意識別子(GUID)を使用して識別され、ディスク キーは Cisco Key Management Center(KMC)に保存されます。これらのディスク キーは、マスター キーを使用して暗号化されます。

## キーの生成

セキュア キーは、暗号化を使用してクラスタの SME ノード内の SME ディスクごとに生成されます。FIPS の乱数生成を使用してランダムなキー番号が生成されます。使用されるキーのサイズは 256 ビットです。

新しいキーは、有効な各 SME ディスクに生成できます。キーは、キー ファイルからインポートすることもできます。キーは、ディスク キー複製機能を使用して複製することもできます。

## ディスクの状態

ディスクの状態には、次のタイプがあります。

- **Clear**: ディスクはオンラインであり、暗号化は無効になっています。
- **Crypto**: ディスクはオンラインであり、暗号化が有効になっています。
- **Suspend**: ディスクは中断していて、ホスト I/O アクセスが中断しています。
- **Data-preparing**: ディスクのデータは SME ディスクによって現在変換中です。
- **Failed**: データ準備に失敗したため、ディスクのデータを復元する必要があります。
- **Failed**: シグニチャと KMC の間の不一致により失敗します。
- **Pending enable no-dataprepare (Wait SME enable)**: スイッチの永続的データと CKMC の間にディスク状態の不一致があるとき。この状態は、顧客がスイッチをリブートする前に保存済みの設定に実行コンフィギュレーションをコピーしないときに発生します。

MKR は、ディスクが次の状態にあると失敗します。

- **Failure**: メタデータと KMC の間に不一致があるときに MKR が失敗します。
- **Failure**: メタデータが存在するものの、KMC にキーがないときに MKR が失敗します。
- **Failure**: メタデータの書き込みが失敗すると、MKR が失敗します。
- **Preparing (progress 2%, remainin.....)**: MKR はステータスが準備状態であると表示して失敗します。
- 設定済みパスのステータス
- **Offline**: ディスク ITL ディスカバリが保留中の場合に、MKR が失敗します。
- **Is online**: ディスク ITL が障害 I/O 状態であって設定済みの場合に、MKR が失敗します。
- **Crypto**: KMC の検証が保留中のままの場合に、MKR が失敗します。
- メタデータの更新が保留中の場合に、MKR が失敗します。
- **Crypto**: FSM の更新が保留中の場合に、MKR が失敗します。



(注) ディスクへのすべてのパスが検出されていて、オンラインになっていることを確認してください。

## Cisco KMC

Cisco KMC は、SME ディスクでの暗号化と復号化に必要なアクティブ キーおよびアーカイブ済みキーを保存する一元的なキー管理システムです。

各 SME ディスクには、0 個以上のアクティブ キーと 0 個以上のアーカイブ済みキーがあります。

各キー エントリは次の情報で構成されます。

- SME 構成で設定済みディスクを特定するために必要なクラスタ名、ディスク グループ名、ディスク名
- SAN 内で対応する物理ディスクを特定するために必要なベンダー ID、製品 ID、デバイス ID
- アクティブまたはアーカイブ状態
- 作成およびアーカイブのタイムスタンプ

SME クラスタは設定の変更時に CKMC に接続し、CKMC を検証および更新します。CKMC には次の機能があります。

- ディスク キーをアーカイブ、消去、回復、および配布する一元化されたキー管理。
- 導入要件に応じた DCNM-SAN サーバへの統合。
- AAA メカニズムを使用した統合アクセス制御。

セキュリティ モードおよびキー管理設定の詳細については、「[SME キー管理の設定](#)」セクション (7-1 ページ) を参照してください。

Cisco KMC は、SME ディスク関連の操作をサポートします。KMC 操作に関して、次の内容について説明します。

- [クラスタのアーカイブ](#) (6-12 ページ)
- [ディスクまたはディスク グループの消去](#) (6-12 ページ)
- [キー再生成](#) (6-12 ページ)
- [アカウントिंग](#) (6-13 ページ)

## クラスタのアーカイブ

アーカイブによって、スイッチからクラスタが削除されますが、Cisco KMC 内にキーが保持されます。

## ディスクまたはディスク グループの消去

リース期限やアップグレードなどによりストレージ アレイが廃止される際には、ディスクに関連付けられているキーを消去できます。キーの消去は、ディスク レベルまたはディスク グループ レベルで実行できます。アクティブなディスク グループを削除すると、すべてのキーがアーカイブされます。アーカイブされたディスク グループを削除すると、すべてのキーが消去されます。



注意

キーの消去は、回復不能な操作です。キー データベースのエクスポートされたバックアップがなければ、消去されたキーは二度と取得できません。

## キー再生成

ディスクやディスク グループ内のデータは、セキュリティを向上させるために定期的に、またはキーのセキュリティが侵害されたときに必要に応じて、キー再生成できます。



(注)

リリース 5.2.6 からは、マスター キーのキー再生成がサポートされます。

個々のディスク レベルでのキー再生成操作では、ディスクの新しいキーを生成し、古いキーをアーカイブします。古いキーを使用してデータを復号化し、新しいキーでデータを暗号化し、そのデータをディスクに書き戻すために、データ準備作業がトリガーされます。

ディスク グループ レベルで実行されるキー再生成操作は、ディスク グループ内のすべてのディスクまたはディスクのサブセットで実行されます。KMC は、すべてのディスクのキーの履歴を保持します。

## アカウンティング

Cisco KMC は、すべてのキー関連操作、その結果、およびその他の関連情報を記録するためにアカウンティング ログを保持します。ビューでは、パターンに基づいてログ レコードをフィルタリングするためのサポートを提供します。詳細については、[Cisco KMC \(6-11 ページ\)](#) を参照してください。

## クォーラム ディスク

クラスタはサーバのグループであるため、クラスタが機能するにはクォーラムが存在する必要があります。クォーラムは、クラスタ内の  $N/2 + 1$  台のサーバが稼働中であるとして定義されます。 $N$  はクラスタ内のサーバの総数です。偶数のサーバから成るクラスタでスプリットブレインシナリオを避けるため、クラスタ メンバーの半数が残りのクラスタ メンバーとの通信が失われた場合は、クラスタ内に残留するために、クォーラム ディスクを使用してどのパーティションにクォーラムがあるのかが判断されます。

SME クラスタに障害が発生してもサーバクラスタは機能する必要があるため、クォーラム ディスクが暗号化ディスクとして設定されていないことが重要です。

## データ レプリケーション

複製は、ディスク アレイがデータを LUN 間で自動的に複製するディスク アレイ ベースの技術です。

データ レプリケーション関係には、次の 2 つのタイプがあります。

- 同期モード
- 非同期モード

リモート複製では、プライマリ ストレージアレイのデータをセカンダリ サイトのセカンダリ ストレージアレイへ WAN リンク上で移動します。リモート複製では、プライマリ サイトの障害や地理的な障害が発生してもデータの損失を防止します。

SME は、データ レプリケーションを実行しません。SME は、他のサードパーティ製データ レプリケーション ソリューションをサポートするように設計されています。

## SME ディスクキー複製

SME ディスク キー複製 (DKR) 機能は、サードパーティのデータ ミーリング ソリューションをサポートするためのキー複製を管理します。DKR 機能では以下がサポートされています。

- ミラーまたはクローン: 送信元ディスク内のデータのコピーは、ディスク アレイによって同じストレージシステムの別のディスク (ミラーまたはクローン) に複製されます。
- 複製: 送信元ディスクのデータは、ディスク アレイによってリモート ストレージ システムの別のディスクに複製されます。同期と非同期という 2 つのタイプの複製を利用できます。



(注) ディスク キー複製は、キー複製のみを処理します。ユーザがデータ レプリケーションを保証する必要があります。



(注) 同じタイプの同じ SME ディスク クラスタ間でのみ DKR 関係が許可されます。たとえば、シグニチャ SME ディスク クラスタは、非シグニチャ SME ディスク クラスタとの DKR には使用できません。

送信元と宛先のディスクには、クリア、暗号化、および失敗という 3 つの安定状態があります。ディスク キー複製関係が同期すると、送信元ディスクの状態とアクティブな暗号化キーの両方が宛先ディスクに複製されます。

DKR 機能は DCNM-SAN によって維持されます。DKR を使用してディスクのすべての SME キーを変更する操作は、DCNM-SAN を介して実行される必要があります。



注意

ディスクでデータ準備またはキー再生成が実行されているときは、キー複製が無効になっている必要があります。併用はサポートされていません。



(注) 適切なキー関連付けを保証するため、複製またはスナップショット関係に関わるすべてのディスクを同じ KMC (データベース) が管理する必要があります。



(注) 非シグニチャ SME ディスク クラスタをシグニチャ SME ディスク クラスタに変換するときは、DKR が無効になっている必要があります。

## DKR の前提条件

DKR には、次の前提条件があります。

- DKR 機能が接続してデータを転送するためには、CKMC が同じである必要があります。ディスク複製で管理される送信元および宛先ディスクで同じ KMC を使用してください。
- ディスク複製はキー複製のみを処理し、データ レプリケーションは処理しません。データ レプリケーションはストレージ ベンダーによって実行されます。キーを同期するときは、適切な手順に従う必要があります。



注意

ディスクが DKR 関係に追加されると、そのディスクにおけるすべての SME 操作は DCNM-SAN のみを介して実行される必要があります。SME ディスク構成は、DKR 関係に関連するディスクに対して CLI を使用できません。CLI を使用すると予期しない結果が生じ、ディスク上のデータが危険にさらされることがあります。

## DKR に関する注意事項および制約事項

ここでは、ディスク レプリケーション サポートに関する注意事項と制限事項について説明します。

- ポイント I/O 回復ジャーナル スナップショットは、キー変更操作でサポートされていません。
- 暗号化が有効な場合、暗号化が無効な場合、またはキー再生成操作中は、どのタイプのスナップショットもサポートされません。



注意

非シグニチャ クラスタでは、上記の操作が正常に完了したらスナップショットを破棄することをお勧めします。シグニチャ クラスタでは、キー再生成操作でスナップショットがサポートされません。

## 複製またはミラーリングの要件

複製またはミラーリングの要件は次のとおりです。

- 送信元ディスクでのキーの更新によって、送信元ディスクと複製関係にある宛先ディスクでキーの更新が発生します。
- 送信元ディスクは、複数の宛先ディスクの送信元ディスクになることができます。
- 複製関係にある宛先ディスクが複製関係の宛先になることができるのは1つのみです。

## DKR の機能

DKR の主要な機能を次に示します。

- DKR マップ ファイル:複製関係に関する情報を DCNM-SAN に送信できる XML 形式の情報が含まれます。
- DKR データベース:DCNM-SAN は DKR マップ ファイルを処理し、関係をデータベースに *source disk:destination disk:type of relationship:state of relationship* という形式で保存します。
- SME ディスクのキー変更操作の管理:送信元ディスクにおけるすべてのキー変更操作は、宛先ディスクで複製される必要があります。

## DKR 関係

DKR 関係は、DKR マップ ファイルを使用して作成されます。DKR 関係にある送信元および宛先ディスクを指定します。これにより、1つの操作で多くのエントリーを入力できます。DKR 関係は、次の2つの方法で設定できます。

- リモート複製関係:宛先ディスクはホストにエクスポートでき、デバイス検出を通じて SME ディスクで認識できるようになります。

## DKR マッピング ファイル

複製およびスナップショット関係を含むマップ ファイルを DCNM-SAN に指定することで、DKR データベースに入力できます。各 DKR 関係は、送信元および宛先ディスクから構成されます。

ディスクは、次の形式で特定できます。

```
<?xml version="1.0" encoding="UTF-8"?>
<SME_DKR xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="DKR.xsd">
<Version>Version</Version>
<Options>SME_DKR_NONE</Options>
<Relations>
<Type>SME_DKR_MIRROR</Type>
<Source>
<Label>grp-1</Label>
<Cluster_Name>source-1</Cluster_Name>
<Disk_Group_Name>primary-cx400</Disk_Group_Name>
<Disk_Name>pry0</Disk_Name>
<Identifier>
```

```

<VPW>
<Vendor>DGC      </Vendor>
<Product>VRAID   </Product>
<WWN>600601609bc12a008ca7298a9c44e011</WWN>
</VPW>
</Identifier>
</Source>
<Destination>
<Label>grp-2emote</Label>
<Cluster_Name>destination-1</Cluster_Name>
<Disk_Group_Name>secondary-cx400</Disk_Group_Name>
<Disk_Name>sec0</Disk_Name>
<Identifier>
<VPW>
<Vendor>DGC      </Vendor>
<Product>VRAID   </Product>
<WWN>600601600e602a00b461b7289b44e011</WWN>
</VPW>
</Identifier>
</Destination>
</Relations>
</SME_DKR>

```



(注) DCNM-SAN は宛先クラスタ内の宛先ディスクを設定しないため、管理者は宛先ディスクを明示的に設定および検出する必要があります。

## SME ディスクと ISSU

In-Service Software Upgrade (ISSU) には、次の要件があります。

- ISSU の処理中は、SME 設定の変更が進行中または開始済みである必要があります。
- ISSU をスケジュールする前に、データ準備作業が進行中ではないことを確認します。
- ISSU では、ファームウェア アップグレード中に暗号化ノード (DPP) がオフラインになります。これにより、ホスト I/O トラフィックが中断されます。
- 暗号化ノードにバインドされた IT-Nexus は、別の暗号化へ完全に移行する可能性があります。このとき、負荷分散のバランスが取れなくなることがあります。



(注) SME ディスクでは、5.2(1) 以前の Cisco NX-OS リリースからの ISSU はサポートされておらず、SME ディスク構成は拒否されます。

リリース 5.2.1 からリリース 5.2.6 にアップグレードするときは、クラスタが非シグニチャ モードになっている必要があります。また、リリース 5.2.6 からリリース 5.2.1 にダウングレードするときは、シグニチャ クラスタが削除される必要があります。

## Cisco DCNM for DKR でのキー変更操作の管理

2 つのキー変更操作は次のとおりです。

- データ準備なし: ローカル キー変更によって、DKR はリモート ディスクへのホスト アクセスを中断します。ローカル キー変更でデータの整合性が検証され、リモート エンドへのデータ レプリケーションが同期されたら、管理者は必要な関係を選択し、DKR で同期処理を実行できます。この操作により、送信元と宛先のキーが同期され、リモート ディスクへのホスト アクセスが再開されます。



- データ準備:送信元ディスクのデータ準備を開始する前に、次の操作を完了してください。
  - DKR 関係を無効にします。
  - 送信元と宛先ディスクの間の複製を無効にします。これは、ディスク アレイ ベンダー固有の操作です。

データ準備が完了してデータの整合性を確認したら、次の操作を実行します。

- ディスク アレイ ベンダー固有の操作を使用して、送信元と宛先間のデータ レプリケーションを有効にします。
- データが送信元と宛先のディスクの間で同期されたら、DKR 関係を有効にします。この操作は、送信元と宛先のキーを同期します。



注意

データ準備が完了するまで、宛先ディスクでホストへのアクセスを停止します。データ準備中にホストにアクセスすると、データ損失が発生します。

## 読み取り専用ディスク

読み取り専用ディスクを使用すると、ホストは暗号化キーを指定して、失敗状態のディスクのコンテンツを読み取ることができます。これはディスクの内容を回復するためのソリューションです。ディスクに対して可能性のある一連のキーがわかっているような状況では、このモードを使用して、可能性のあるキーを1つずつ試し、ディスクの内容を読み取るための正しいキーを探することができます。このモードは通常の構成で使用することや、本書に記載されている通常のリカバリ手順で使用することは想定されていません。

読み取り専用モードを使用してデータを回復するには、次の手順を実行します。

- ステップ 1 [Manage Disk Encryption:Settings] ページで、[Make Read-Only] を選択します。  
正しいキーを取得すると、リカバリ ウィザードを使用してディスクを回復できます。

## 書き込みシグニチャ

この機能は、シグニチャ クラスタ モードで使用できます。ディスクがシグニチャ モードに変換されていない場合は、ディスクにシグニチャを手動で書き込むことができます。これは、ディスクの詳細ページから実行することも、クラスタの詳細ページを使用からバッチ モードで実行することもできます。



(注)

非シグニチャ ディスク クラスタをシグニチャ ディスク クラスタに変換するには、このコマンドを使用します。

## CLI を使用した SME ディスク管理の設定



注意

設定変更中は、Cisco KMC が常にオンラインである必要があります。



(注) SME ディスク対応クラスタを作成または設定するために、クラスタをディスク対応として定義する必要があります。この定義を設定する方法の詳細については、「[SME クラスタの作成](#)」セクション(4-6 ページ)を参照してください。



(注) SME ディスク クラスタは、次の FCIP 設定と互換性がありません。

- IP 圧縮が有効な FCIP
- IPsec および WA を使用する FCIP

この項では、次のトピックについて取り上げます。

- [IT-Nexus の検出](#) (6-18 ページ)
- [クラスタへの SME ノードの追加](#) (6-19 ページ)
- [クラスタへの SME 暗号化エンジンの追加](#) (6-19 ページ)
- [ディスク グループの設定](#) (6-20 ページ)
- [ディスク グループへのディスクの追加](#) (6-21 ページ)
- [ディスクへのパスの追加](#) (6-21 ページ)
- [ディスクの管理](#) (6-22 ページ)

## IT-Nexus の検出



注意

サーバとストレージの間のパスをホストするすべての IT-Nexus を設定に追加する必要があります。そのようにしないとデータの整合性は危険にさらされます。

IT-Nexus ディスクを検出するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i>	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>[no] discover</b> <b>host</b> <i>wwn1</i> <b>target</b> <i>wwn2</i> <b>vsan</b> <i>vsanid</i> <b>fabric</b> <i>fabricname</i>	検出する必要がある IT-Nexus を指定します。

Initiator-Target-LUN Nexus (ITL) の検出では、CKMC に照会して、暗号化状態および該当する場合はディスクのアクティブ キーを確認します。暗号化ディスクの状態の詳細については、「[ディスクの状態](#)」セクション(6-11 ページ)を参照してください。



(注) ディスクおよび各ディスクへの複数のパスは、ベンダー ID、製品 ID、およびデバイス ID (VPD) の SCSI 照会データで識別されます。



(注) 複数の IT-Nexus の検出が同時に発行されるようなスクリプト化された環境では、結果として CKMC に対する多数の照会を引き起こす可能性があります。これによって、一部の照会がタイムアウトする可能性があります。回避策は、IT-Nexus を再検出することです。スクリプト化された環境でのこのような事態を防ぐため、検出コマンド間で 1 分間の遅延を設定することをお勧めします。

## IT-Nexus の表示

クラスタに追加されるすべての IT-Nexus を表示するには、次のコマンドを入力します。

```
switch(config-sme-cl)# show sme cluster c52 it-nexus
```

```
-----
Host WWN,          VSAN   Status   Switch      Interface
Target WWN
-----
21:00:00:1b:32:84:ca:4a,
20:04:00:a0:b8:1f:4a:c6    5      online   172.23.146.52sme10/1
-----
```



(注) スイッチ、および IT-Nexus がバインドされている暗号化ノードも表示されます。上記の例では、IT-Nexus は以下によってホストされています。

- IP アドレス 172.23.146.52 のスイッチ
- モジュール 10 のライン カードの制御パス プロセッサ (CPP) 上
- I/O トラフィックは、モジュール 10 のライン カードのデータ パス プロセッサ (DPP) 1 によってホストされます。

## クラスタへの SME ノードの追加

### 手順の詳細

クラスタに SME ノードを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername</b>	作成するディスク名を指定します。
ステップ 3	switch(config-sme-cl)# <b>node local</b>	クラスタに追加するローカル ノードを指定します。
ステップ 4	switch(config-sme-cl)# <b>node remote node ID</b>	クラスタに追加するリモート ノードの IP アドレス または名前を指定します。

## クラスタへの SME 暗号化エンジンの追加

### 手順の詳細

暗号化エンジンがマスター ノードにローカルであるときに SME 暗号化エンジンをクラスタに追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i>	作成するディスク名を指定します。
ステップ 3	switch(config-sme-cl)# <b>node local</b>	クラスタに追加するローカル ノードを指定します。
ステップ 4	switch(config-sme-cl-node)# <b>fabric-membership</b> <i>fabricname</i>	ローカル スイッチ ファブリック名前を指定します。
ステップ 5	switch(config-sme-cl-node)# <b>interface</b> <b>sme 1/1 force</b>	クラスタに暗号化エンジンを追加するように指定します。

非マスター ノード上にある暗号化エンジンを追加するには、マスター ノードに移動し、SME インターフェイスを作成してから、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster enable</b>	クラスタ機能をイネーブルにします。
ステップ 3	switch(config)# <b>sme enable</b>	SME 機能をイネーブルにします。
ステップ 4	switch(config-sme-cl-node)# <b>interface</b> <b>sme 1/1 force</b>	クラスタに暗号化エンジンを追加するように指定します。

マスター ノードで、次のようにリモート暗号化エンジンをクラスタに追加します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i>	作成するディスク名を指定します。
ステップ 3	switch(config)# <b>node</b> <node alias> <i>ip-address</i> <ip address of remote <i>switch</i> >	クラスタにリモート ノードを追加します。
ステップ 4	switch(config)# <b>fabric-membership</b> <name of fabric>	リモート スイッチ ファブリック名前を指定します。
ステップ 5	switch(config-sme-cl-node)# <b>interface</b> <b>sme 1/1 force</b>	クラスタに暗号化エンジンを追加するように指定します。

## ディスク グループの設定

SME クラスタ内のディスクは、ディスク グループに機能分類できます。

### 手順の詳細

ディスク グループを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# [no] <b>sme cluster</b> clustername	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# [no] <b>disk-group</b> dg-name	ディスク グループを設定します。

## ディスク グループへのディスクの追加

ディスクはディスク グループの一部として指定され、名前をエイリアスとして使用して認識されます。

### 手順の詳細

ディスク グループにディスクを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# [no] <b>sme cluster</b> clustername	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# [no] <b>disk-group</b> dg-name	ディスク グループを設定します。
ステップ 4	switch(config-sme-cl-dg)# [no] <b>disk</b> disk-name	作成するディスク名を指定します。

## ディスクへのパスの追加



### 注意

ターゲット LUN に対するホストのすべてのパス (ITL) は、データ破損を防止するために同じディスクに存在する必要があります。

ディスクはディスク グループの一部として指定され、名前をエイリアスとして使用して認識されます。クラスタ内のディスクに対するすべてのパスは、ホスト、ターゲット、LUN、VSAN、およびファブリックを使用して指定される必要があります。

### 手順の詳細

ディスクを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# [no] <b>sme cluster</b> clustername	クラスタを指定し、SME クラスタ設定サブモードを開始します。

	コマンド	目的
ステップ 3	switch(config-sme-cl)# [no] <b>disk-group</b> <i>dg-name</i>	ディスク グループを設定します。
ステップ 4	switch(config-sme-cl-dg)# [no] <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# [no] <b>host</b> <i>wwn1</i> <b>target</b> <i>wwn2</i> <b>lun</b> <i>l1</i> <b>vsan</b> <i>v1</i> <b>fabric</b> <i>f1</i>	クラスタ内のディスクへのパスを指定します。



(注) 上記のパスで指定された IT-Nexus が SME で設定されていない場合、SME は IT-Nexus の検出をトリガーし、指定されたディスクに設定済みパスを追加します。スクリプト化された環境では、パスを追加するときに、IT-Nexus 検出が完了できるように 1 分間の遅延を設定することをお勧めします。

## ITL-Nexus の表示

SUP で検出されたパスのリストを表示するには、次のコマンドを入力します。

```
switch(config-sme-cl)# show sme cluster c52 disk detail
Disk 1 is crypto
  Model is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0b80001f4ac4000032454a3a69ce
  ASL ID is 581688B7
  Is configured as disk device d1 in disk group dg1
  Paths
    Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
    Is online (SUCCESS), configured
```

IT-Nexus がバインドされている CPP で検出されたパスのリストを表示するには、次のコマンドを入力します。

```
switch# attach module 10
Attaching to module 10 ...
To exit type 'exit', to abort type '$.'
module-10# show sme internal info crypto-node 1 itl brief
-----
  if-ndx          host          tgt          vsan lun  type
sme  locking event      state
-----
    0x12480000  21:00:00:1b:32:84:ca:4a  20:04:00:a0:b8:1f:4a:c6    5 0x0000
  1   1              Unlocked  SMED_ISAPI_ITL_ST_UP_CRYPTO
```

## ディスクの管理

この項では、次のトピックについて取り上げます。

- [データ準備を使用した SME ディスクにおける暗号化の有効化 \(6-23 ページ\)](#)
- [SME ディスク キーの変更 \(6-27 ページ\)](#)
- [SME ディスクの回復 \(6-28 ページ\)](#)

## データ準備を使用した SME ディスクにおける暗号化の有効化

既存のデータがある一連のディスクで SME 暗号化をイネーブルにすると、ディスク上の既存のデータはクリアから暗号化に変換される必要があります。このプロセスは、データ暗号化と呼ばれます。

この操作では、ディスクからデータを読み取り、データを暗号化し、ディスクに書き戻します。暗号化エンジンは、ホスト ポート ID を利用して、上記の操作を実行します。

データ準備を実行するアクションは **enable offline** です。



注意

データ準備を進めている Initiator-Target-LUN パス (ITL) は、データ準備が完了するまでオンラインである必要があります。ホスト ポートまたはターゲット ポートのフラップにより、データ準備が失敗します。



(注)

現在のところ、オフライン データ準備のみがサポートされています。



注意

データ準備プロセス中、キーの GUID を手動で入力することは推奨されません。SME がキーを自動的に生成します。

### 手順の詳細

ディスクでデータ準備を実行するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを作成します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>enable offline</b>	SME ディスクでオフライン データ準備を実行し、クリア データを暗号化されたデータに変換します。
ステップ 6	switch(config-sme-cl-dg-disk)# <b>no enable offline</b>	SME ディスクでオフライン データ準備を実行し、暗号化されたデータをクリア データに変換します。



注意

暗号化の有効化または無効化操作がディスクで実行されるときは、すべてのスイッチで **copy running-config startup-config** コマンドを実行する必要があります。そうしないと、スイッチの永続ストレージ サービス (PSS) が CKMC に記録されているディスクの状態と矛盾します。



## 注意

有効化操作がシグニチャ モード クラスタで初めて実行されるときは、ディスクの末尾で予約された 64 MB の SME ディスク領域に対して十分な LUN サイズがあることを確認してください。そうしないと、データ損失が発生する可能性があります。

## SME ディスクのキー再生成

ディスク グループに含まれるディスク内のデータは、オン デマンドでキー再生成できます。たとえば、キーのセキュリティが侵害されたときに実行します。

個々のディスク レベルでのキー再生成操作では、ディスクの新しいキーを生成し、古いキーをアーカイブします。古いキーを使用してデータを復号化し、新しいキーでデータを暗号化し、そのデータをディスクに書き戻すために、データ準備作業がトリガーされます。

キー再生成は、ディスク グループ内のディスクのすべてのサブセットで実行できます。KMC は、すべてのディスクのキーの履歴を保持します。

## 手順の詳細

SME ディスクをキー再生成するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername</b>	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group dg-name</b>	ディスク グループを作成します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk disk-name</b>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>rekey offline</b>	SME ディスクでオフラインのキー再生成を実行します。

## データ準備のモニタリング

データ準備の進行状況をモニタするには、次のコマンドを入力します。

```
switch# show sme cluster c52 disk-group dg1 disk d1
Disk d1 is data-preparing (progress 0%, remaining time d:0 h:0 m:0 s:26)
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0b80001f4ac4000032454a3a69ce
Encryption is Enabled
Key guid is 5b2a0bb9c3ea2428-961579da480ed56f
Paths
Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
[f52]
Is online (disk it1 in IO reject state), configured, data prepare
```

## データ準備を使用しない SME ディスクにおける暗号化の有効化

SME 暗号化が既存のデータがない一連の新しいディスクで有効になると、SME をデータ準備なしで有効にできます。



SME は、指定されたディスクに対してのみ有効にできます。SME が有効になると、ディスク グループ内のディスクに対するホスト I/O が暗号化または復号化されます。



(注) ディスク グループ レベルで SME を有効にすることはサポートされていません。



(注) シグニチャ モードのクラスタでは、ディスクに対する I/O 対応パスが 1 つ以上ある場合のみ、暗号化を有効にできます。



(注) 非対称デバイスでは、I/O 対応パスは、アクティブな最適化済み(AO)パスを意味します。



注意 ディスクへのすべてのパスは、暗号化を有効にする前に SME に追加される必要があります。そうしないとデータの整合性が危険にさらされます。

ディスクで暗号化を有効にするには、オプションのキーワード **no-dataprep** を使用します。



注意 パスが検出されても設定されていないディスクで暗号化を有効にすると、そのパスで発行されたホスト I/O は失敗します。ホスト I/O を可能にするには、そのようなパスがディスクで設定される必要があります。



注意 データ準備操作なしの暗号化は、既存のデータがないディスクでのみ有効化する必要があります。そうしないと、データ損失が発生する可能性があります。

## 手順の詳細

ディスクで暗号化を実行するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを作成します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>enable</b> <b>no-dataprep</b>	ディスクで暗号化を有効にします。
ステップ 6	switch(config-sme-cl-dg-disk)# <b>no enable</b> <b>no-dataprep</b>	ディスクで暗号化を無効にします。

## 設定済みのディスクの表示

設定済みのディスクを表示するには、次のコマンドを入力します。

```
switch# show sme cluster c52 disk-group dg1 disk d1
```

```

Disk d1 is crypto
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0b80001f4ac4000032454a3a69ce
Encryption is Enabled
Key guid is 1f09c7425d706a2e-6e00de45a53aa68
Paths
Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (SUCCESS), configured

```

## パス状態

使用可能なパス状態のタイプは次のとおりです。

- **Online:** パスが検出され、オンラインです。

- 設定済み、検出済み、およびホスト I/O アクセスに利用できるパス。

```

Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (success), configured

```



(注) 上記の出力は、正しく設定されて正常に検出されたパスで予想される状態です。

- 設定済み、検出済み、ただしホスト I/O アクセスに利用できないパス。

```

Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (disk itl in IO reject state), configured

```



(注) 正常に設定および検出後も I/O 拒否状態が継続する場合は、IT-Nexus を再検出してください。

- 設定済みではなく、検出済みでホスト I/O アクセスに利用できるパス(ディスクで暗号化が有効ではない)。

```

Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (success), NOT configured

```

- 設定済みではなく、検出済みではなく、ホスト I/O アクセスに利用できないパス(ディスクで暗号化が有効であるか、ディスクが中断中)。

```

Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (disk itl in IO reject state), NOT configured

```



注意

ディスクが完全に正しく設定されているときは、すべてのパスがオンラインであり、ホスト I/O アクセスに利用できることが想定されています。

- **Offline:** 設定されたパスはまだ検出されていません。

```

Host 21:01:00:1b:32:a4:ca:4a Target 20:05:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is offline (disk itl discovery pending), configured

```

- **Failed:** パスは失敗状態であるため、ホスト I/O を防止するためにパスはダウンしています。

```

Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is failed (disk itl dp fail), configured

```

- **Misconfigured path:** このディスクに追加されたパスは、別のディスクに属しています。
  - 誤設定のパスは認証失敗であるとマークされ、ホスト I/O は許可されません。
  - 回復するには、そのようなパスを削除してから、再検出し、適切に再設定する必要があります。

```
Host 21:00:00:1b:32:84:ca:4a Target 20:05:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is failed (disk itl auth fail vpd mismatch), configured
```
- **Unconfigured path:** パスは検出されたものの、ユーザによってこのディスクにまだ追加されていません。出力には「Not configured」と表示されます。
  - 設定されている場合、ディスクは暗号化が有効になっておらず、パスではホスト I/O を許可します。
  - 設定されているディスクで暗号化が有効な場合、パスではホスト I/O を許可しません。

## SME ディスク キーの変更

この手順では、ディスクの暗号化キーを手動で変更できます。



(注)

ディスクの暗号化キーを手動で変更することは、ディスクが中断状態になっているときのみ可能です。中断状態では、ディスクへのホスト I/O アクセスは許可されません。

### 手順の詳細

SME ディスク キーを変更するには、次の手順に従います。

	コマンド	目的
ステップ 1	<code>switch# <b>config t</b></code>	コンフィギュレーションモードに入ります。
ステップ 2	<code>switch(config)# <b>sme cluster</b> <i>clustername</i></code>	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	<code>switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i></code>	ディスク グループを指定します。
ステップ 4	<code>switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i></code>	作成するディスク名を指定します。
ステップ 5	<code>switch(config-sme-cl-dg-disk)# <b>suspend</b></code>	SME ディスクを中断します。
ステップ 6	<code>switch(config-sme-cl-dg-disk)# <b>modify-key</b> <i>guid guid</i></code>	SME ディスク キーを変更します。ディスクの新しいアクティブ キーにする必要があるキー GUID を入力として指定します。
ステップ 7	<code>switch(config-sme-cl-dg-disk)# <b>no suspend</b></code>	SME ディスクを再開します。



注意

この設定は、管理者が CLI から直接指定することは想定されていません。DNCM-SAN 複製キーコンテキスト (DKR) は、キー変更機能を利用してディスク キー複製関係を管理します。

### 中断されたディスクの表示

中断されたディスクの情報を表示するには、次のコマンドを入力します。

```
switch(config-sme-cl-dg-disk)# show sme cluster c52 disk-group dg1 disk d1
Disk d1 is suspend
```

```

Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0b80001f4ac4000032454a3a69ce
Encryption is Enabled
Key guid is 1f09c7425d706a2e-6e00de45a53aa68c
Paths
Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
Is online (disk itl in IO reject state), configured

```

## SME ディスクの回復

失敗したディスクでリカバリを実行するには、最初にバックアップからディスクのコンテンツを復元する必要があります。これはストレージの操作です。次に、**recover** コマンドを使用して、SME 設定で失敗したディスクの状態を更新する必要があります。

リカバリには、次の2つの方法があります。

- [SME ディスクのクリア状態への回復\(6-28 ページ\)](#)
- [SME ディスクの暗号化状態への回復\(6-29 ページ\)](#)



注意

SME **recover** CLI コマンドは、暗号化キーのリカバリにのみ使用され、データには使用されません。

### SME ディスクのクリア状態への回復

クリア データが含まれるバックアップからディスクが回復した場合は、SME ディスクをクリア状態に回復する必要があります。



(注)

シグニチャ モード クラスタでは、リカバリが成功するために少なくとも1つの I/O 対応パスが必要です。リカバリの一環として、SME はディスクのシグニチャ部分からシグニチャをクリアします。

### 手順の詳細

SME ディスクをクリア状態に回復するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを指定します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>recover</b>	ディスクの暗号化状態をクリア状態にリセットします。つまり、ディスクで発行されたホスト I/O では暗号化が実行されません。

## SME ディスクの暗号化状態への回復

暗号化されたデータが含まれるバックアップからディスクが回復した場合は、SME ディスクを暗号化状態に回復する必要があります。



(注) シグニチャ モード クラスタでは、回復が成功するために少なくとも 1 つの I/O 対応パスが必要です。リカバリの一環として、SME はディスクのシグニチャ部分にシグニチャを書き込みます。

### 手順の詳細

SME ディスクを暗号化状態に回復するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを指定します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>recover guid</b> <i>guid</i>	ディスクの暗号化ステータスを暗号化ディスクに設定し、GUI でディスクの暗号化キーとして指定されているキーを使用します。



注意 **recover** コマンドはディスクのコンテンツを回復しません。ディスクに回復されるデータに基づいて、ディスクの暗号化状態を回復します。ディスク上のデータは、**recover** コマンドを使用する前に復元される必要があります。

## KMC からの SME ディスクの回復



(注) これは、シグニチャ モード クラスタのみに適用されます。

KMC から SME ディスクを回復するために、SME ディスクは KMC 内でアクティブなキーを探します。アクティブなキーが見つかったら、そのアクティブなキーは、ディスクが暗号化状態に回復するときにディスクに書き込まれるシグニチャを生成するために使用されます。



(注) 暗号化キーは、KMC で記録されたアクティブなキーです。



(注) KMC にディスクのアクティブなキーがない場合、ディスクはクリア状態に回復し、予約エリアのシグニチャはクリアされます。

KMC から SME ディスクを回復するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを指定します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>recover from</b> <b>-kmc</b>	ディスクの暗号化ステータスを暗号化ディスクに設定します。

### ディスクのシグニチャからの SME ディスクの回復



(注) このオプションは、シグニチャ モードクラスタの場合にのみ使用できます。

SME ディスクは、ディスクの予約エリアからシグニチャを取得します。シグニチャが有効であれば、SME ディスクはシグニチャからの GUID を使用して KMC 内を検索します。KMC の検索に成功すると、ディスクは暗号化状態に回復します。



(注) KMC の検索が失敗すると、回復操作は失敗し、ディスクは失敗状態のままになります。



(注) ディスクでシグニチャが見つからない場合、ディスクはクリア状態に回復します。

シグニチャ モードクラスタから SME ディスクを回復するには、次の手順に従います。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster</b> <i>clustername</i> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>disk-group</b> <i>dg-name</i> switch(config-sme-cl)#	ディスク グループを指定します。
ステップ 4	switch(config-sme-cl-dg)# <b>disk</b> <i>disk-name</i>	作成するディスク名を指定します。
ステップ 5	switch(config-sme-cl-dg-disk)# <b>recover from</b> <b>-metadata</b>	ディスクの暗号化ステータスを暗号化ディスクに設定します。

SME クラスタ内のディスクは、ディスク グループに機能分類できます。



(注) ディスクをシグニチャ モードクラスタに追加したときに、ボリュームにデータが含まれている場合は、ボリュームの最後に Cisco SME シグニチャ情報用の領域を 64 MB 以上予約するようにディスクのサイズを変更する必要があります。

## シグニチャ モードの設定



(注) SME ディスク クラスタを非シグニチャ モードからシグニチャ モードに変換すると、すべての設定済みの暗号化ディスクにシグニチャが書き込まれます。変換が完了したら、すべての暗号化ディスクとそのパスがオンライン状態であることを確認し、ディスクのシグニチャを確認します。

クラスタをシグニチャ モードに切り替えるには、次の手順を実行します。

[Cluster Details] 画面が表示されます。

ステップ 2 [Convert to Signature Mode] をクリックします。



(注) すでにシグニチャ モードになっているディスクに対してはこのオプションが表示されません。

[Signature Mode Conversion] 画面が表示されます。

ステップ 3 [Next] をクリックします。

[Convert Cluster] 画面が表示されます。

変換が完了したら、失敗ディスクがないことを確認し、暗号化ディスクでそのシグニチャが正しいことを確認します。

## ディスクのシグニチャ モードへの変換

クラスタをシグニチャ モードに切り替えるには、次の手順を実行します。

[Cluster Details] 画面が表示されます。

ステップ 4 [Convert Disks to Signature Mode] をクリックします。

[Signature Mode Conversion] 画面が表示されます。

ステップ 5 [Next] をクリックします。

[Convert Cluster] 画面が表示されます。

## ディスクのシグニチャの確認

ディスクのシグニチャを確認するには、次の手順を実行します。

ステップ 1 DCNM-SAN Web クライアントで、[SME] タブをクリックします。

ステップ 2 [Disk Groups] で、シグニチャを検証するディスクを選択します。

[Disk Details] 画面が表示されます。

ステップ 3 [Disk Signature] で、[Verify Signature] をクリックします。

シグニチャが確認され、シグニチャの検証が成功したことを示すメッセージが表示されます。

シグニチャモードでは、SME は KMC 内のディスク情報と比較して、ディスクのシグニチャを確認します。KMC 内の情報とシグニチャの間に不一致がある場合、ディスク障害が発生します。

## メタデータ シグニチャを使用したディスクの回復



(注) シグニチャ ディスクのみを回復できます。

### 手順の詳細

メタデータを使用して障害のあるディスクを回復するには、次の手順に従います。

## キー マネージャからのディスクの回復

# キー管理操作の設定

この項では、次のトピックについて取り上げます。

- [スマート カードの交換\(6-32 ページ\)](#)
- [マスター キーのキー再生成の設定\(6-32 ページ\)](#)

## スマート カードの交換

このセクションでは、クラスタのスマート カードを交換する方法について説明します。

### 手順の詳細

- ステップ 1 スマート カードを交換するには(Advanced セキュリティ モード)、次の手順を実行します。[Data Center Network Manager] で、[SME] をクリックします。クラスタのリストが表示されます。
- ステップ 2 [Smartcards] をクリックします。リカバリ共有の詳細、およびスマート カードの関連リストが表示されます。
- ステップ 3 交換するスマート カードを選択し、[Replace Smartcard and Rekey Master Key] をクリックします。

## マスター キーのキー再生成の設定

次のいずれかの方法を使用して、マスター キーのキー再生成操作を開始できます。

- [Data Center Network Manager] で、[SME] をクリックします。クラスタのリストが表示されます。必要なクラスタをクリックします。[Cluster Details] > [Security Mode] にある [Rekey Master Key] をクリックします。



- [Data Center Network Manager] で、[SME] をクリックします。クラスタのリストが表示されず、[Smartcards] をクリックします。リカバリ共有の詳細、およびスマートカードの関連リストが表示されます。[Recovery Shares] で、[Rekey Master Key] をクリックします。

## 前提条件

- MKR が開始された Web クライアントにスマートカードドライバがインストールされていることを確認します。
- Cisco DCNM サーバ、プライマリ サーバ、セカンダリ サーバ、CKMC、およびスイッチの間に IP 通信があることを確認します。
- Cisco DCNM-SAN サービスが実行中であることを確認します。
- MKR プロセス全体でクラスタがオンラインになっていることを確認します。
- MKR を開始する前にキーをエクスポートしてあることを確認します。
- スマートカードに新しい共有のための空き領域があることを確認します。
- 常に起動したばかりのブラウザで MKR を起動し、実行中の DCNM クライアントのインスタンスがないことを確認します。
- ディスクが次のいずれかの状態になっている場合は、MKR を開始していないことを確認します。
  - DP エラー
  - DP 進行中
  - KMC 更新保留中
  - ITL オフライン
  - パスなし (VPD 不明) の暗号化状態
  - パスなし (VPD 不明) の中断状態
  - データ準備 (検出保留中)
  - 待機有効

## 手順の詳細

**ステップ 1** マスターキーのキー再生成操作を開始すると、確認のダイアログボックスが表示されます。[OK] をクリックします。

[Get Keyshares] ダイアログボックスが表示されます。



**(注)** マスターキーのキー再生成操作が完了するまで、クラスタに含まれるすべてのノードはオンラインのままになっている必要があります。

**ステップ 2** スマートカードを挿入します。  
マスターキーのキー再生成設定が成功しました。

## 同期の再開

スマート カードにすべての共有が保存されていて、ファブリックに不一致があり、MKR が失敗した場合は、[Resume Sync] をクリックして MKR 操作を再開します。

## SME ディスク管理設定の確認

SME ディスク管理の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show sme cluster</b>	クラスタに関する詳細情報を表示します。
<b>show sme cluster detail</b>	クラスタに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i></b>	特定のクラスタに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> detail</b>	特定のクラスタに関する詳細情報を表示します。
<b>show sme cluster summary</b>	クラスタに関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> summary</b>	特定のクラスタに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> it-nexus</b>	特定のクラスタ内の IT-Nexus に関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> disk-group</b>	ディスク グループの概要とディスクの総数を表示します。
<b>show sme cluster <i>clustername</i> disk-group <i>diskgroup-name</i></b>	特定のディスク グループ内のディスクに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> disk-group <i>diskgroup-name</i> disk</b>	特定のディスク グループ内のディスクに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> disk-group <i>diskgroup-name</i> disk <i>diskname</i></b>	特定のディスク グループ内のディスクに関する詳細情報、および ITL の状態を表示します。
<b>show sme cluster <i>clustername</i> disk detail</b>	クラスタ内のディスクに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> disk summary</b>	クラスタ内のディスクに関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> disk-data prepare detail</b>	クラスタでデータ準備中であるディスクに関する詳細情報を表示します。  (注) これは現在サポートされていません。
<b>show sme cluster <i>clustername</i> disk-data prepare summary</b>	クラスタでデータ準備中であるディスクに関する概要情報を表示します。  (注) これは現在サポートされていません。
<b>show sme cluster <i>clustername</i> interface detail</b>	クラスタ内の SME インターフェイスに関する詳細情報を表示します。

コマンド	目的
<b>show sme cluster <i>clustername</i> interface summary</b>	クラスタ内の SME インターフェイスに関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> interface sme <i>sme-interface</i></b>	クラスタ内の特定の SME インターフェイスに関する情報を表示します。
<b>show sme cluster <i>clustername</i> interface node <i>remote-switch</i></b>	クラスタ内のリモート ノードの SME インターフェイスに関する情報を表示します。
<b>show sme cluster <i>clustername</i> key database</b>	クラスタ内のキーに関する情報を表示します。
<b>show sme cluster <i>clustername</i> key database detail</b>	クラスタ内のキーに関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> key database summary</b>	クラスタ内のキーに関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> key database guid <i>guid</i></b>	特定の GUID についてクラスタ内のキー情報を表示します。
<b>show sme cluster <i>clustername</i> load-balancing</b>	クラスタのロードバランシング状態を表示します。
<b>show sme cluster <i>clustername</i> lun crypto-status</b>	クラスタ内の LUN の暗号化状態を表示します。
<b>show sme cluster <i>clustername</i> node</b>	クラスタ内のノードに関する情報を表示します。
<b>show sme cluster <i>clustername</i> node summary</b>	クラスタ内のノードに関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> node <i>remote-switch</i></b>	クラスタ内の特定のリモート ノードに関する情報を表示します。
<b>show sme cluster <i>clustername</i> recovery officer</b>	SME クラスタ リカバリ 責任者に関する情報を表示します。
<b>show sme cluster <i>clustername</i> recovery officer <i>recovery-index</i></b>	特定の SME クラスタ リカバリ 責任者に関する情報を表示します。
<b>show sme cluster <i>clustername</i> recovery officer detail</b>	SME クラスタ リカバリ 責任者に関する詳細情報を表示します。
<b>show sme cluster <i>clustername</i> recovery officer summary</b>	SME クラスタ リカバリ 責任者に関する概要情報を表示します。
<b>show sme cluster <i>clustername</i> recovery officer summary <i>recovery-index</i></b>	特定の SME クラスタ リカバリ 責任者に関する概要情報を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『Cisco MDS 9000 Family NX-OS Command Reference』を参照してください。

## SME ディスク管理のモニタリング

この項では、次のトピックについて取り上げます。

- [ホストの詳細の表示 \(6-36 ページ\)](#)
- [ディスク グループの詳細の表示 \(6-36 ページ\)](#)
- [CLI を使用した SME ディスク情報の表示 \(6-36 ページ\)](#)

## ホストの詳細の表示

SME クラスタ内のホストに関する詳細情報を表示できます。特定のホストに関する情報には、ディスク グループのメンバーシップ、ホストからターゲットへのパス、VSAN、ファブリック、ステータス、およびディスク デバイスが含まれます。

## ディスク グループの詳細の表示

SME クラスタ内のディスク グループに関する詳細情報を表示できます。特定のディスクに関する情報には、ディスク グループのメンバーシップ、デバイスの説明、シリアル番号、およびホストとターゲットの PWWN が含まれます。

## ディスクの詳細の表示

SME クラスタ内のディスク グループのディスクに関する詳細および情報を表示できます。特定のディスクに関する情報には、パス情報とディスク状態が含まれます。

## ディスク パスの詳細の表示

SME クラスタ内のディスク グループのディスクに関するディスク パスの詳細を表示できます。特定のディスクに関する情報には、パス情報とディスク状態が含まれます。

## シグニチャ モード クラスタの表示

シグニチャ モードである SME クラスタの詳細情報を表示できます。クラスタの詳細を表示するには、ナビゲーション ウィンドウでクラスタをクリックします。

## CLI を使用した SME ディスク情報の表示

クラスタに関する情報を表示するには、**show sme cluster** コマンドを使用します。

```
switch# show sme cluster
SME Cluster is dest1
  Cluster ID is 0x29ab000dec3f1402
  Cluster status is online
  Security mode is basic
  Total Nodes are 2
  Recovery Scheme is 1 out of 1
  Fabric[0] is Fabric_jlwu9216i-19
  Fabric[1] is Fabric_jlwu9222i-15
  Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
  Secondary KMC server has not been provisioned
```

```

Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
Shared Key Mode is Not Enabled
Auto Vol Group is Not Enabled
Tape Compression is Enabled
Tape Key Recycle Policy is Enabled
Key On Tape is Not Enabled
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 2445
SSL for KMC : Not Configured
SSL for ICN : Not Configured
Cluster is Disk capable
Cluster Metadata On Disk is Set: 64 megabytes <!---64 megabytes indicates a signature
mode cluster>

```



(注)

Cluster Config Version は、スイッチに保存されているコンフィギュレーションのバージョンを指定します。クラスタ情報の取得やクラスタの活性化が必要なシナリオでは、コンフィギュレーションバージョンが最も高いスイッチが使用される必要があります。

クラスタに関する詳細情報を表示するには、**show sme cluster detail** コマンドを使用します。

```

switch# show sme cluster detail
SME Cluster is dest1
Cluster ID is 0x29ab000dec3f1402
Cluster status is online
Security mode is basic
Total Nodes are 2
Recovery Scheme is 1 out of 1
Fabric[0] is Fabric_jlwu9216i-19
Fabric[1] is Fabric_jlwu9222i-15
Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
Secondary KMC server has not been provisioned
Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
Shared Key Mode is Not Enabled
Auto Vol Group is Not Enabled
Tape Compression is Enabled
Tape Key Recycle Policy is Enabled
Key On Tape is Not Enabled
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 2445
SSL for KMC : Not Configured
SSL for ICN : Not Configured
Cluster is Disk capable
Cluster Metadata On Disk is Set: 64 Megabytes

```

クラスタに関する概要情報を表示するには、**show sme cluster summary** コマンドを使用します。

```

switch# show sme cluster summary
-----
Cluster          ID                               Security Mode    Status
-----
C                 0x20eb000dec3f45c2             basic           online
-----

```

特定のクラスタに関する情報を表示するには、**show sme cluster *clustername*** コマンドを使用します。

```
switch# show sme cluster c
SME Cluster is C
Cluster ID is 0x29ab000dec3f1402
Cluster status is online
Security mode is basic
Total Nodes are 2
Recovery Scheme is 1 out of 1
Fabric[0] is Fabric_jlwu9216i-19
Fabric[1] is Fabric_jlwu9222i-15
Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
Secondary KMC server has not been provisioned
Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
Shared Key Mode is Not Enabled
Auto Vol Group is Not Enabled
Tape Compression is Enabled
Tape Key Recycle Policy is Enabled
Key On Tape is Not Enabled
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 2445
SSL for KMC : Not Configured
SSL for ICN : Not Configured
Cluster is Disk capable
Cluster Metadata On Disk is Set: 64 Megabytes
```

特定のクラスタに関する詳細情報を表示するには、**show sme cluster *clustername* detail** コマンドを使用します。

```
switch# show sme cluster c detail
SME Cluster is C
Cluster ID is 0x29ab000dec3f1402
Cluster status is online
Security mode is basic
Total Nodes are 2
Recovery Scheme is 1 out of 1
Fabric[0] is Fabric_jlwu9216i-19
Fabric[1] is Fabric_jlwu9222i-15
Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
Secondary KMC server has not been provisioned
Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
Shared Key Mode is Not Enabled
Auto Vol Group is Not Enabled
Tape Compression is Enabled
Tape Key Recycle Policy is Enabled
Key On Tape is Not Enabled
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 2445
SSL for KMC : Not Configured
SSL for ICN : Not Configured
Cluster is Disk capable
Cluster Metadata On Disk is Set: 64 Megabytes
```

特定のクラスタに関する概要情報を表示するには、**show sme cluster *clustername* summary** コマンドを使用します。

```
switch# show sme cluster c summary
-----
Cluster          ID                      Security Mode      Status
-----
C                 0x20eb000dec3f45c2    basic              online
-----
```

特定のクラスタ内のディスク グループ情報を表示するには、**show sme cluster *clustername* disk group** コマンドを使用します。

```
switch# show sme cluster c disk-group
-----
Disk Group Name      Total Disks
-----
DG                    8
-----
```

クラスタ内のディスク グループに関する情報を表示するには、**show sme cluster *clustername* disk-group DG** コマンドを使用します。

```
switch# show sme cluster scluster20 disk-group dg1
Disk group dg1
  Number of disks is 16

Disk group dg1
  Number of disks is 16

Disk Disk0 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb000000005006218003813000
  Encryption is Not Enabled

Disk Disk1 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000015006218003813000
  Encryption is Not Enabled

Disk Disk10 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000a5006218003813000
  Encryption is Not Enabled

Disk Disk11 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000b5006218003813000
  Encryption is Not Enabled

Disk Disk12 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000c5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk13 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000d5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk14 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000e5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk15 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000f5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk2 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000025006218003813000
  Encryption is Not Enabled
```

```
Disk Disk3 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000035006218003813000
  Encryption is Not Enabled
```

```
Disk Disk4 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000045006218003813000
  Encryption is Not Enabled
```

```
Disk Disk5 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000055006218003813000
  Encryption is Not Enabled
```

```
Disk Disk6 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000065006218003813000
  Encryption is Not Enabled
```

```
Disk Disk7 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000075006218003813000
  Encryption is Not Enabled
```



```
Disk Disk8 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000085006218003813000
  Encryption is Not Enabled
```

```
Disk Disk9 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000095006218003813000
  Encryption is Not Enabled
```

ディスク グループ内のディスクに関する情報を表示するには、**show sme cluster clustername disk-group disk-group name DG disk** コマンドを使用します。

```
switch# show sme cluster scluster20 disk-group dg1 disk
Disk group dg1
```

```
  Number of disks is 16
```

```
Disk group dg1
```

```
  Number of disks is 16
```

```
Disk Disk0 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000005006218003813000
  Encryption is Not Enabled
```

```
Disk Disk1 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb0000000015006218003813000
  Encryption is Not Enabled
```

```
Disk Disk10 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000a5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk11 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000b5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk12 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000c5006218003813000
  Encryption is Not Enabled
```

```
Disk Disk13 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
```

```
Device ID is 600a0bb00000000d5006218003813000
Encryption is Not Enabled

Disk Disk14 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000e5006218003813000
Encryption is Not Enabled

Disk Disk15 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000f5006218003813000
Encryption is Not Enabled

Disk Disk2 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000025006218003813000
Encryption is Not Enabled

Disk Disk3 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000035006218003813000
Encryption is Not Enabled

Disk Disk4 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000045006218003813000
Encryption is Not Enabled

Disk Disk5 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000055006218003813000
Encryption is Not Enabled

Disk Disk6 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000065006218003813000
Encryption is Not Enabled

Disk Disk7 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000075006218003813000
Encryption is Not Enabled

Disk Disk8 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000085006218003813000
Encryption is Not Enabled
```

```
Disk Disk9 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000095006218003813000
Encryption is Not Enabled
```

ディスク グループ内のディスクに関する情報を表示するには、**show sme cluster clustername disk-group disk-group name disk disk name** コマンドを使用します。

```
switch# show sme cluster scluster20 disk-group dg1 disk Disk 0
Disk Disk0 is clear
Description is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000005006218003813000
Encryption is Not Enabled
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0000 vsan 100
    [Fabric_sw-A-9222i-95]
    Is online (SUCCESS), configured
```

クラスタ内のディスクに関する詳細情報を表示するには、**show sme cluster clustername disk detail** コマンドを使用します。

```
switch# show sme cluster scluster20 disk detail
Disk 1 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000095006218003813000
Is configured as disk device Disk9 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0009 vsan 100
    Is online (SUCCESS), configured

Disk 2 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000005006218003813000
Is configured as disk device Disk0 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0000 vsan 100
    Is online (SUCCESS), configured

Disk 3 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000f5006218003813000
Is configured as disk device Disk15 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000f vsan 100
    Is online (SUCCESS), configured

Disk 4 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000025006218003813000
```

```
Is configured as disk device Disk2 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0002 vsan 100
  Is online (SUCCESS), configured

Disk 5 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000085006218003813000
Is configured as disk device Disk8 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0008 vsan 100
  Is online (SUCCESS), configured

Disk 6 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000b5006218003813000
Is configured as disk device Disk11 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000b vsan 100
  Is online (SUCCESS), configured

Disk 7 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000065006218003813000
Is configured as disk device Disk6 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0006 vsan 100
  Is online (SUCCESS), configured

Disk 8 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000055006218003813000
Is configured as disk device Disk5 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0005 vsan 100
  Is online (SUCCESS), configured

Disk 9 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000075006218003813000
Is configured as disk device Disk7 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0007 vsan 100
  Is online (SUCCESS), configured

Disk 10 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000035006218003813000
Is configured as disk device Disk3 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0003 vsan 100
  Is online (SUCCESS), configured
```

```
Disk 11 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000045006218003813000
Is configured as disk device Disk4 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0004 vsan 100
  Is online (SUCCESS), configured

Disk 12 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb0000000015006218003813000
Is configured as disk device Disk1 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0001 vsan 100
  Is online (SUCCESS), configured

Disk 13 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000d5006218003813000
Is configured as disk device Disk13 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000d vsan 100
  Is online (SUCCESS), configured

Disk 14 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000c5006218003813000
Is configured as disk device Disk12 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000c vsan 100
  Is online (SUCCESS), configured

Disk 15 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000a5006218003813000
Is configured as disk device Disk10 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000a vsan 100
  Is online (SUCCESS), configured

Disk 16 is clear
Model is LSI INF-01-00
Vendor ID is LSI
Product ID is INF-01-00
Device ID is 600a0bb00000000e5006218003813000
Is configured as disk device Disk14 in disk group dg1
Paths
  Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000e vsan 100
  Is online (SUCCESS), configured
```

クラスタ内の特定のディスクに関する概要情報を表示するには、**show sme cluster *clustername* disk summary** コマンドを使用します。

```
switch# show sme cluster c disk summary
-----
Target WWN                Lun      Description                Crypto-Disk      Status
-----
50:06:01:6b:30:60:06:d6  0x0002  DGC DISK                   Disk7            clear
50:06:01:6b:30:60:06:d6  0x0000  DGC DISK                   Disk5            clear
50:06:01:6b:30:60:06:d6  0x0001  DGC DISK                   Disk6            clear
50:06:01:63:30:60:06:d6  0x0003  DGC RAID 5                 Disk3            clear
50:06:01:63:30:60:06:d6  0x0004  DGC RAID 5                 Disk4            clear
50:06:01:63:30:60:06:d6  0x0001  DGC RAID 5                 Disk1            clear
50:06:01:63:30:60:06:d6  0x0002  DGC RAID 5                 Disk2            clear
50:06:01:63:30:60:06:d6  0x0000  DGC RAID 5                 Disk0            clear
```

特定のクラスタ内の IT-Nexus に関する詳細情報を表示するには、**show sme cluster *clustername* it-nexus** コマンドを使用します。

```
switch# show sme cluster c it-nexus
-----
Host WWN,                  VSAN    Status   Switch      Interface
Target WWN
-----
21:00:00:1b:32:8a:1d:4c,   2       online  172.28.234.68 sme1/1
50:06:01:63:30:60:06:d6

21:01:00:1b:32:aa:49:4c,   2       online  172.28.234.68 sme1/1
50:06:01:6b:30:60:06:d6

21:02:00:1b:32:ca:49:4c,   2       online  172.28.234.68 sme1/1
50:06:01:6b:30:60:06:d6
```

クラスタ内の SME インターフェイスに関する詳細情報を表示するには、**show sme cluster *clustername* interface detail** コマンドを使用します。

```
Interface sme1/1 belongs to local switch
Status is up
  RSA Certificate is (len 247 fingerprint SHA1::
87:2f:16:6d:91:ec:8f:cb:95:3a:df:6b:c6:49:c3:67:c4:a9:39:6f:)
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMJGt4JoIhfV3KU6eJPdfmzIjYLqbZ2mA3VdJ7T86btzyMhpZZI4x76O
uCvLxEIEuKW+p/XRqhpV4AN7YQDVCw0OB3dacXfRQjM8EdoC6lMXDGsKCzYzti51H
ZqQvAKCMYdz/P3CSbVx3MsoOeDuvv/Hj6wvIngtdGfVHkWms9b1lAgED
-----END RSA PUBLIC KEY-----
```

クラスタ内の SME インターフェイスに関する概要情報を表示するには、**show sme cluster *clustername* interface summary** コマンドを使用します。

```
switch# show sme cluster c interface summary
-----
Switch                Interface      Status
-----
local switch          sme1/1         up
```

クラスタ内の特定の SME インターフェイスに関する情報を表示するには、**show sme cluster clustername interface sme sme-interface** コマンドを使用します。

```
switch# show sme cluster c interface sme 1/1
Interface sme1/1 belongs to local switch
Status is up
```

クラスタ内の LUN の暗号化状態を表示するには、**show sme cluster clustername lun crypto-status** コマンドを使用します。

```
switch# show sme cluster c lun crypto-status
LUN (Serial Number)                               Encryption
-----
LUN
---
cpp_lun_ndx                0x29
sme_enabled                0
vendor_id                  DGC
product_id                 DISK
device_id                  10493CF4
prod_rev_level             0216
vendor_specific            860000AB71CL
cluster_name               C
dg_name                    DG
device_name                Disk7
max_lba                    0x27ffff
blk_sz                     0x200
disk_state                 0x1
current disk fsm state     SMED_CPP_DISK_ST_CLEAR_DISK
cur_key_guid               0000000000000000-0000000000000000
new_key_guid               0000000000000000-0000000000000000
cur_key_obj                (nil)
new_key_obj                (nil)
dp                         (nil)
total itl count            2
active itl count           2
lun hold count             0
Not locked
  I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0002
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
  I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0002
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
cpp_lun_ndx                0x27
sme_enabled                0
vendor_id                  DGC
product_id                 DISK
device_id                  93B1508B
prod_rev_level             0216
vendor_specific            8000009529CL
cluster_name               C
dg_name                    DG
device_name                Disk5
max_lba                    0x27ffff
blk_sz                     0x200
disk_state                 0x1
current disk fsm state     SMED_CPP_DISK_ST_CLEAR_DISK
cur_key_guid               0000000000000000-0000000000000000
new_key_guid               0000000000000000-0000000000000000
cur_key_obj                (nil)
new_key_obj                (nil)
dp                         (nil)
```

```

total itl count          2
active itl count         2
lun hold count           0
Not locked
  I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0000
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
  I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0000
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
  cpp_lun_ndx             0x28
  sme_enabled             0
  vendor_id               DGC
  product_id              DISK
  device_id               F074E188
  prod_rev_level          0216
  vendor_specific          850000AA73CL
  cluster_name            C
  dg_name                  DG
  device_name              Disk6
  max_lba                  0x27ffffff
  blk_sz                   0x200
  disk_state               0x1
  current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid             0000000000000000-0000000000000000
  new_key_guid             0000000000000000-0000000000000000
  cur_key_obj              (nil)
  new_key_obj              (nil)
  dp                       (nil)
  total itl count          2
  active itl count         2
  lun hold count           0
  Not locked
  I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0001
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
  I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0001
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
  cpp_lun_ndx             0x25
  sme_enabled             0
  vendor_id               DGC
  product_id              RAID 5
  device_id               3C2590FB
  prod_rev_level          0216
  vendor_specific          39000061BDCL
  cluster_name            C
  dg_name                  DG
  device_name              Disk3
  max_lba                  0x9ffffff
  blk_sz                   0x200
  disk_state               0x1
  current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid             0000000000000000-0000000000000000
  new_key_guid             0000000000000000-0000000000000000
  cur_key_obj              (nil)
  new_key_obj              (nil)
  dp                       (nil)
  total itl count          1
  active itl count         1
  lun hold count           0
  Not locked
  I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0003
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])

```



```

LUN
---
  cpp_lun_ndx          0x26
  sme_enabled         0
  vendor_id           DGC
  product_id          RAID 5
  device_id           8B09E6E9
  prod_rev_level      0216
  vendor_specific     3A000061D3CL
  cluster_name        C
  dg_name             DG
  device_name         Disk4
  max_lba             0x9fffff
  blk_sz              0x200
  disk_state          0x1
  current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid         0000000000000000-0000000000000000
  new_key_guid         0000000000000000-0000000000000000
  cur_key_obj         (nil)
  new_key_obj         (nil)
  dp                  (nil)
  total itl count     1
  active itl count    1
  lun hold count      0
  Not locked
  I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0004
  (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
  cpp_lun_ndx          0x23
  sme_enabled         0
  vendor_id           DGC
  product_id          RAID 5
  device_id           90D80D94
  prod_rev_level      0216
  vendor_specific     3700006182CL
  cluster_name        C
  dg_name             DG
  device_name         Disk1
  max_lba             0x9fffff
  blk_sz              0x200
  disk_state          0x1
  current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid         0000000000000000-0000000000000000
  new_key_guid         0000000000000000-0000000000000000
  cur_key_obj         (nil)
  new_key_obj         (nil)
  dp                  (nil)
  total itl count     1
  active itl count    1
  lun hold count      0
  Not locked
  I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0001
  (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
  cpp_lun_ndx          0x24
  sme_enabled         0
  vendor_id           DGC
  product_id          RAID 5
  device_id           930ED44F
  prod_rev_level      0216
  vendor_specific     38000061A5CL
  cluster_name        C

```

```

dg_name                DG
device_name            Disk2
max_lba                0x9fffff
blk_sz                 0x200
disk_state             0x1
current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
cur_key_guid           0000000000000000-0000000000000000
new_key_guid           0000000000000000-0000000000000000
cur_key_obj            (nil)
new_key_obj            (nil)
dp                     (nil)
total itl count        1
active itl count        1
lun hold count         0
Not locked
  I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0002
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
```

```

cpp_lun_ndx            0x22
sme_enabled            0
vendor_id              DGC
product_id             RAID 5
device_id              CC1BCB3A
prod_rev_level         0216
vendor_specific        360000616BCL
cluster_name           C
dg_name                DG
device_name            Disk0
max_lba                0x9fffff
blk_sz                 0x200
disk_state             0x1
current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
cur_key_guid           0000000000000000-0000000000000000
new_key_guid           0000000000000000-0000000000000000
cur_key_obj            (nil)
new_key_obj            (nil)
dp                     (nil)
total itl count        1
active itl count        1
lun hold count         0
Not locked
  I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0000
    (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])

```

クラスタのロードバランシング状態を表示するには、**show sme cluster *clustername* load-balancing** コマンドを使用します。

```

switch# show sme cluster c load-balancing
Load balancing status is enabled for cluster C

```

クラスタ内のノードに関する情報を表示するには、**show sme cluster *clustername* node** コマンドを使用します。

```

switch# show sme cluster c node
Node 172.28.234.54 is remote switch
  Node ID is 2
  Status is online
  Node is not master switch
  Fabric is Fabric_sw-sme-9513-54
Node 172.28.234.68 is local switch
  Node ID is 1

```

```
Status is online
Node is the master switch
Fabric is Fabric_sw-sme-9513-54
```

クラスタ内の特定のリモートノードに関する情報を表示するには、**show sme cluster *clustername* node remote-switch** コマンドを使用します。

```
switch# show sme cluster c node 172.28.234.54
Node 172.28.234.54 is remote switch
Node ID is 2
Status is online
Node is not master switch
Fabric is Fabric_sw-sme-9513-54
```

クラスタ内のノードに関する概要情報を表示するには、**show sme cluster *clustername* node summary** コマンドを使用します。

```
switch# show sme cluster c node summary
-----
Switch                Status           Master           Node ID
-----
172.28.234.54         online           no                2
local switch          online           yes               1
```

クラスタ内のキーに関する情報を表示するには、**show sme cluster *clustername* key database** コマンドを使用します。

```
switch# show sme cluster c key database
Key Type is master key
GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
Cluster is C, Master Key Version is 0

Key Type is disk key
GUID is 5a8adb8aca98106f-dd61016f5fb8b543
Cluster is C, Crypto disk group is DG
Crypto disk is Disk1

Key Type is disk key
GUID is dc203fa33cd267ad-dd2e7513e307521f
Cluster is C, Crypto disk group is DG
Crypto disk is Disk0
```

クラスタ内のキーに関する詳細情報を表示するには、**show sme cluster *clustername* key database detail** コマンドを使用します。

```
switch# show sme cluster c key database detail
Key Type is master key
GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
Cluster is C, Master Key Version is 0
Key status is active
Key was created at Mon Oct 04 13:38:41 UTC 2010
Key length is 32

Key Type is disk key
GUID is 5a8adb8aca98106f-dd61016f5fb8b543
Cluster is C, Crypto disk group is DG
Crypto disk is Disk1
Key status is active
Key was created at Mon Oct 04 13:58:23 UTC 2010
Key length is 32
```

```

Key data type is symmetric key wrap
Symmetric key wrapping version is 0
Symmetric crypto algorithm is aes-cbc
Authentication algorithm used is sha-256 and value
  G5UvNvtQC67CGfbJBWV1xs+zUKF4CIOIrk+tfG+dPQY=
IV length is 16 and value
  jAMWrbbtDou2DmSmlddmQAAAAAAAAAAAAAAAAAAAA=
Key Object is wrapped by 2ebddb1dbf180660-c0e4add77be8e8a0
Key data length is 80
Encrypted data is
  qL0Tc/pr9NvMcRTgwePgzwPJaBoDxzLevYXh1gw9c+fbZ1p4
  kabTYUM7QGTrZKFkkJPOPO/XPSn9VVKVYvNSCguQV0teq6Vo
  vdUqeDyht9g=

```

```

Key Type is disk key
GUID is dc203fa33cd267ad-dd2e7513e307521f
  Cluster is C, Crypto disk group is DG
  Crypto disk is Disk0
Key status is active
Key was created at Mon Oct 04 13:57:56 UTC 2010
Key length is 32
Key data type is symmetric key wrap
Symmetric key wrapping version is 0
Symmetric crypto algorithm is aes-cbc
Authentication algorithm used is sha-256 and value
  8Isr/LRaHdqQmlGPagCq9reDOYLQiFdImmQfmIRsu9s=
IV length is 16 and value
  gJfKQqKtS08iJ5HrGQR3GwAAAAAAAAAAAAAAAAAAAA=
Key Object is wrapped by 2ebddb1dbf180660-c0e4add77be8e8a0
Key data length is 80
Encrypted data is
  zL+syhPqSQfXy8zAwLfrntbIcjIux+dIjPQWQ0Jk/zpVTmRD
  KT6R1zFmkN3ibXaqzba6yrFCXUGMmWX/KK7CdEQtkWk1ecUz
  k+zvbYtdq50=

```

クラスタ内のキーに関する概要情報を表示するには、**show sme cluster *clustername* key database summary** コマンドを使用します。

```
switch# show sme cluster c key database summary
```

```

-----
Key Type                GUID
-----
master key              2ebddb1dbf180660-c0e4add77be8e8a0
disk key                5a8adb8aca98106f-dd61016f5fb8b543
disk key                dc203fa33cd267ad-dd2e7513e307521f

```

特定の GUID についてクラスタ内のキー情報を表示するには、**show sme cluster *clustername* key database guid *GUID*** コマンドを使用します。

```

switch# show sme cluster c key database guid 2ebddb1dbf180660-c0e4add77be8e8a0
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
  Cluster is C, Master Key Version is 0

```

GUID についてクラスタ内のキーに関する概要情報を表示するには、**show sme cluster *clustername* key database guid *GUID* summary** コマンドを使用します。

```

switch# show sme cluster C key database guid 2ebddb1dbf180660-c0e4add77be8e8a0 summary
-----
Key Type                GUID
-----
master key              2ebddb1dbf180660-c0e4add77be8e8a0

```

特定の GUID についてクラスタ内のキーに関する詳細情報を表示するには、**show sme cluster *clustername* key database guid *GUID* detail** コマンドを使用します。

```
switch# show sme cluster c key database guid 2ebddb1dbf180660-c0e4add77be8e8a0 detail
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
  Cluster is C, Master Key Version is 0
  Key status is active
  Key was created at Mon Oct 04 13:38:41 UTC 2010
  Key length is 32
```

SME クラスタ リカバリ責任者に関する情報を表示するには、**show sme cluster *clustername* recovery officer** コマンドを使用します。

```
switch# show sme cluster c recovery officer
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password
```

```
Key Type is master key share
  Cluster is C, Master Key Version is 0
  Recovery Share Version is 0, Share Index is 1
```

SME クラスタ リカバリ責任者に関する詳細情報を表示するには、**show sme cluster *clustername* recovery officer detail** コマンドを使用します。

```
switch# show sme cluster c recovery officer detail
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
  Cluster is C, Master Key Version is 0
  Recovery Share Version is 0, Share Index is 1
  Key status is active
  Key was created at Mon Oct 04 13:44:45 UTC 2010
  Key length is 81
  Key data type is password key wrap
  Password key wrapping version is 0
  Password scheme used is pkcs5_2
  Password scheme digest algorithm used by password scheme is sha-1
  Authentication algorithm used is sha-256, key length is 32 and value
    58 63 71 59 69 6a 6d 44 50 74 2f 6e 63 77 46 30 38 41 59 31 74 55 54 6e 72 58 37 4d
50 4b 41 6b 55 56 7a 53 6b 6e
52 44 6a 50 45 3d 00 00 00 00

  Salt length is 8 and value
    54 65 79 45 32 65 39 46 33 64 77 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

  IV length is 16
```

```

Iteration count is 2048
Key data length is 96
Encrypted data is
 69 76 77 4d 52 66 37 44 7a 79 45 30 4f 38 58 34 77 77 69 32 43 34 79 6a 68 54 74 6a
50 77 50 6e 62 71 4e 69 48 77
39 62 57 37 4a 4b 45 37 47 30
 4c 41 46 33 54 6d 6f 31 69 78 4a 39 62 47 65 55 36 4c 67 43 74 5a 49 61 30 49 6a 49
41 66 6c 74 2f 6c 46 57 37 41
38 77 44 75 64 63 32 50 77 45
 4d 68 63 54 54 45 33 4f 4f 48 4f 41 74 4f 66 6a 59 47 32 6d 5a 49 35 34 45 6c 30 30
37 37 77 76 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

```

SME クラスタ リカバリ 責任者に関する概要情報を表示するには、**show sme cluster *clustername* recovery officer summary** コマンドを使用します。

```
switch# show sme cluster c recovery officer summary
```

```

-----
Share      Status   Label           Smartcard      Serial No
-----
1          Set                       No

```

特定の SME クラスタ リカバリ 責任者に関する情報を表示するには、**show sme cluster *clustername* recovery officer *recovery-index*** コマンドを使用します。

```
switch# show sme cluster c recovery officer 1
```

```

Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
  Cluster is C, Master Key Version is 0
  Recovery Share Version is 0, Share Index is 1

```

特定の SME クラスタ リカバリ 責任者に関する詳細情報を表示するには、**show sme cluster *clustername* recovery officer detail *recovery-index*** コマンドを使用します。

```
switch# show sme cluster c recovery officer detail 1
```

```

Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
  Cluster is C, Master Key Version is 0
  Recovery Share Version is 0, Share Index is 1
  Key status is active
  Key was created at Mon Oct 04 13:44:45 UTC 2010
  Key length is 81
  Key data type is password key wrap
  Password key wrapping version is 0
  Password scheme used is pkcs5_2
  Password scheme digest algorithm used by password scheme is sha-1
  Authentication algorithm used is sha-256, key length is 32 and value

```

```

58 63 71 59 69 6a 6d 44 50 74 2f 6e 63 77 46 30 38 41 59 31 74 55 54 6e 72 58 37 4d
50 4b 41 6b 55 56 7a 53 6b 6e
52 44 6a 50 45 3d 00 00 00 00

Salt length is 8 and value
54 65 79 45 32 65 39 46 33 64 77 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

IV length is 16
Iteration count is 2048
Key data length is 96
Encrypted data is
69 76 77 4d 52 66 37 44 7a 79 45 30 4f 38 58 34 77 77 69 32 43 34 79 6a 68 54 74 6a
50 77 50 6e 62 71 4e 69 48 77
39 62 57 37 4a 4b 45 37 47 30
4c 41 46 33 54 6d 6f 31 69 78 4a 39 62 47 65 55 36 4c 67 43 74 5a 49 61 30 49 6a 49
41 66 6c 74 2f 6c 46 57 37 41
38 77 44 75 64 63 32 50 77 45
4d 68 63 54 54 45 33 4f 4f 48 4f 41 74 4f 66 6a 59 47 32 6d 5a 49 35 34 45 6c 30 30
37 37 77 76 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

```

特定の SME クラスタ リカバリ 責任者に関する概要情報を表示するには、**show sme cluster <clustername> recovery officer summary <recovery-index>** コマンドを使用します。

```
switch# show sme cluster c recovery officer summary 1
```

```

-----
Share      Status   Label           Smartcard      Serial No
-----
1          Set      Label           No

```

## SME ディスク管理の機能履歴

表 6-1 に、この機能のリリース履歴を示します。

表 6-1 SME ディスク設定の機能履歴

機能名	リリース	機能情報
マスター キーのキー再生成	5.2(6)	マスター キーは、クラスタのディスク キーをラップするために使用されます。
シグニチャおよび非シグニチャ モード クラスタ	5.2(6)	クラスタを設定する 2 つのモード。
SME ディスク設定	5.2(1)	SME ディスクはリリース 5.2(1) で導入された新しい機能です。







## SME キー管理の設定

この章には、SME の包括的なキー管理に関する情報が記載されています。  
この章では、次の事項について説明します。

- [SME キー管理に関する情報 \(7-1 ページ\)](#)
- [CLI を使用した SME キー管理の設定 \(7-7 ページ\)](#)
- [SME キー管理のモニタリング \(7-8 ページ\)](#)
- [SME キー管理の機能履歴 \(7-13 ページ\)](#)

## SME キー管理に関する情報

SME キー管理についての次の項目を取り上げます。

- [キー階層について \(7-1 ページ\)](#)
- [Cisco Key Management Center について \(7-3 ページ\)](#)
- [マスター キーのセキュリティ モードについて \(7-3 ページ\)](#)
- [キー管理設定について \(7-4 ページ\)](#)
- [高可用性 Key Management Center について \(7-5 ページ\)](#)
- [データセンター間でのキーの自動キー レプリケーションについて \(7-6 ページ\)](#)
- [アカウンティング ログ情報について \(7-7 ページ\)](#)

## キー階層について

SME には、セキュリティ キーの階層を使用して暗号化データを保護するための、包括的でセキュアなシステムが含まれています。最高レベルのキーは、クラスタの作成時に生成されるマスター キーです。すべてのクラスタには固有のマスター キーがあります。SME テープでは、マスター キーはテープ グループ ボリューム キーを暗号化し、テープ グループ ボリューム キーはキー ラッピングを使用してテープ ボリューム キーを暗号化します。SME ディスクでは、マスター キーはキー ラッピングを使用してディスク キーを暗号化します。

回復用に、マスター キーは、パスワードで保護されたファイルまたは 1 つ以上のスマート カードに保存できます。クラスタの状態が **Archived** (キー データベースがアーカイブ済み) であるときにキーを回復しようとする場合に、それらのマスター キー ファイルまたはスマート カードが必要です。マスター キーは、MSM-18/4 モジュールまたはスマート カードを改ざんすることで不適切に取り出すことはできません。

キーは暗号化データを守る上で不可欠であり、セキュリティ侵害を受けないようにする必要があります。キーは Cisco Key Management Center に保存する必要があります。また、固有のテープキーはテープカートリッジに直接保存することもできます。キーは、グローバル固有 ID (GUID) により、システム全体で識別されます。

SME キー管理システムには、SME テープ用の以下のタイプのキーがあります。

- マスター キー
- テープ ボリューム グループ キー
- テープ ボリューム キー

すべてのバックアップ テープには、関連するテープ ボリューム キー、テープ ボリューム グループ キー、およびマスター キーがあります。

SME キー管理システムには、SME ディスク用の以下のタイプのキーがあります。

- マスター キー
- ディスク キー

## マスター キー

SME クラスタが作成されると、セキュリティ エンジン はマスター キーを生成します。1 つのファブリックで複数のクラスタをホストできるということを考えると、たとえば、同じ組織内の複数のビジネス グループのニーズをサポートするためには、クラスタと同数のマスター キーが存在することになります。各マスター キーは固有であり、すべてのクラスタ メンバー間で共有されます。マスター キーはテープ ボリューム グループ キーをラップするために使用されます。

## テープ ボリューム グループ キー

テープ ボリューム グループ キーは、テープ ボリューム キー (同じテープ ボリューム グループに属するすべてのテープを暗号化するキー) の暗号化と認証に使用されます。テープ ボリューム グループは、一連のバックアップ テープのバーコード範囲に基づいて作成することも、特定のバックアップ アプリケーションに関連付けることもできます。テープ ボリューム グループ キーは、セキュリティを向上させる場合や、キーのセキュリティが侵害された場合など、状況に応じてキー再生成が行われます。

## テープ ボリューム キー

テープ ボリューム キーは、テープ上のデータの暗号化と認証に使用されます。

固有キー モードでは、テープ ボリューム キーは物理テープごとに固有であり、Cisco KMC またはテープに保存できます。Cisco KMC データベースは、キーがテープ自体に保存されている場合は、テープ ボリューム キーを保存する必要はありません。テープにキーを保存することを選択すると、Cisco KMC に保存するキーの数を大幅に減らすことができます。

共有キー モードでは、ボリューム グループにあるすべてのボリュームの暗号化に使用される 1 つのテープ ボリューム キーがあります。

## ディスク キー

ディスク キーは、ディスク上でデータを暗号化および復号化するために使用されます。

## Cisco Key Management Center について

Cisco Key Management Center (Cisco KMC) は、アクティブなアーカイブ済みのキーをキー データベースに保存するための集中制御システムです。Cisco KMC に保存されるキーは、マスター キーなしでは使用できません。テープ ボリューム キーが増大する可能性に対応するため、SME では、テープ ボリューム キーをテープ自体に保存するオプションを提供しています。この場合、Cisco KMC はテープ ボリューム グループ キーを保存します。

このオプションでは、Cisco KMC に保存されるキーの数を減らすことで、管理対象のテープの数は飛躍的に増えます。ただし、このオプションは、後からキーを消去する機能が制限されています。

Cisco KMC には、次の利点があります。

- Centralized Key Management により、テープ キーをアーカイブ、消去、回復、および配布します。
- 導入要件に従って DCNM-SAN サーバに統合されます。
- AAA メカニズムを使用した統合アクセス制御。



(注) Cisco KMC はキーの更新を監視し、TCP ポート上でスイッチからの要求を取得します。デフォルト ポートは 8800 です。ただし、ポート番号は `smeserver.properties` ファイルで変更できます。

## マスター キーのセキュリティ モードについて


保存されている暗号化データを特定のテープから回復するには、特定のテープ カートリッジ用に作成されたキーにアクセスする必要があります。マスター キーは他のすべてのキーの保護に使用されるため、SME は、マスター キーを保護するための、Basic、Standard、Advanced の、3 つのマスター キー セキュリティ モードを備えています。クラスタの設定中に、マスター キーのセキュリティ レベルを指定します。Basic セキュリティでは、暗号化されたマスター キーをディスクに書き込みます。マスター キーのロックを解除するには、ファイルへのアクセス権が必要です。ファイルは暗号化され、マスター キーを取得するにはパスワードが必要になります。Standard および Advanced セキュリティ モードでは、マスター キーにアクセスするにはスマートカードの使用が必要です。Standard セキュリティを選択すると、マスター キーをロック解除するには 1 つのスマートカードが必要になります。クラスタ設定中に Advanced セキュリティを選択すると、マスター キーをロック解除するために必要なスマートカードの最小数を設定するように求められます。

表 7-1 では、マスター キーのセキュリティ モードを説明しています。

表 7-1 マスター キーのセキュリティ レベル

セキュリティ レベル	定義
Basic	マスター キーはファイルに保存され、パスワードを使用して暗号化されます。マスター キーを取得するには、ファイルとパスワードにアクセスする必要があります。

表 7-1 マスター キーのセキュリティ レベル(続き)

セキュリティ レベル	定義
Standard	Standard セキュリティでは、1 つのスマート カードが必要です。クラスタを作成してマスター キーを生成するときに、スマート カードを求められます。次にマスター キーがスマート カードに書き込まれます。マスター キーを取得するには、スマート カードとスマート カードの暗証番号が必要です。
Advanced	Advanced セキュリティでは、5 つのスマート カードが必要です。クラスタを作成して Advanced セキュリティ モードを選択するときには、データ取得の必要がある場合にマスター キーを回復するために必要なスマート カードの数(5 つのスマート カードのうちの 2 つまたは 3 つ、あるいは 3 つのスマート カードのうちの 2 つ)を指定します。たとえば、「5 つのスマート カードのうちの 2 つ」と指定すると、マスター キーの回復には 5 つのスマート カードのうちの 2 つが必要になります。それぞれのスマート カードは、SME リカバリ責任者が所有しています。  (注) マスター キーを回復するために必要なスマート カードの数が大きければ、それだけセキュリティは向上します。ただし、スマート カードを紛失したり破損したりすると、マスター キーの回復に使用できるスマート カードの数は減ります。

## キー管理設定について

テープ ボリューム グループの作成時に、キー管理設定をイネーブルまたはディセーブルにするかどうかを判断する必要があります。

表 7-2 では、キーの設定、検討事項、および特定の設定を選択した場合に消去できるキーのタイプについて説明しています。すべてのキーの設定は、クラスタ レベルで行います。



(注) 次に示すキー管理設定表は、SME テープのみに適用されます。

表 7-2 キー管理設定

	説明	考慮事項
共有	共有キー モードでは、テープ ボリューム グループ キーのみが生成されます。テープ ボリューム グループの一部であるすべてのテープ ボリュームは、同じキーを共有します。	<p><b>Cisco KMC キー データベース:</b> テープ ボリューム グループ キーのみを保存する、小規模なデータベースです。</p> <p><b>セキュリティ:</b> 普通。1 つのテープ ボリューム グループ キーのセキュリティが侵害されると、そのテープ ボリューム グループを構成するすべてのテープにあるデータが危険にさらされます。</p> <p><b>消去:</b> ボリューム グループ レベルでのみ使用可能です。</p>

表 7-2 キー管理設定(続き)

	説明	考慮事項
固有キー	固有キー モードでは、各テープが独自の固有キーを持ちます。 デフォルト値はイネーブルです。	<b>Cisco KMC キー データベース:</b> テープ ボリューム グループ キーおよびすべての固有なテープ ボリューム キーを保存する、大規模なデータベースです。 <b>セキュリティ:</b> 高。テープ ボリューム キーのセキュリティが侵害されても、他のテープ ボリューム上のデータの整合性が危険にさらされることはありません。 <b>消去:</b> ボリューム グループとボリューム レベルで使用可能です。
キーオンテープの固有キー	キー テープ モードでは、固有の各テープ ボリューム キーは、個別のテープに保存されます。 最もセキュアでスケーラブルなキー管理システムを設定するには、キーオンテープを(固有キーモードの選択時に)選択できます。 デフォルト値は [disabled] です。 (注) キーオンテープ モードを有効にすると、テープ メディアに保存されるキーは、テープ ボリューム グループの ラップ キーで暗号化されます。	<b>Cisco KMC キー データベース:</b> Cisco KMC キー データベースのサイズを縮小することで、多数のテープ ボリュームをサポートする拡張性が向上します。Cisco KMC には、テープ ボリューム グループ キーのみが保存されます。 <b>セキュリティ:</b> 高。テープ ボリューム キーのセキュリティが侵害されても、他のテープ ボリューム上のデータの整合性が危険にさらされることはありません。 <b>消去:</b> ボリューム グループ レベルで使用可能です。

## テープのリサイクル

テープ リサイクルをイネーブルにすると、テープのラベルが再作成され、新しいキーが作成されて Cisco KMC と同期すると、テープ ボリュームの古いキーは Cisco KMC から消去されます。再作成される予定の、以前のバックアップ データ用の古いキーが不要な場合には、この設定を選択する必要があります。

デフォルト設定は [Yes] です。このオプションを [No] に設定することは、テープ複製が SME テープ グループ外で実行される場合にのみ必要です。

## 高可用性 Key Management Center について

Cisco KMC サーバは、高可用性と信頼性を実現する KMC サーバ(KMS)のペアで構成されています。これらの高可用性サーバは、同期と冗長性によって、ダウンタイムとデータ損失の両方を回避できます。KMS は、同じデータベースを指すプライマリとセカンダリの KMC サーバで構成されます。

高可用性を実現するために、どちらの KMS も同じ Oracle 11g Enterprise インストールを使用する必要があります。Oracle 11g Enterprise インストールをそれら 2 つのサーバにインストールし、Oracle Active Data Guard を使用して同期する必要があります。

各 SME クラスタは、プライマリおよびセカンダリ KMC サーバで設定されます。プライマリサーバはセカンダリサーバに優先します。

クラスタはプライマリサーバに接続していますが、なんらかの障害の兆候があると、セカンダリサーバに接続します。クラスタは、プライマリサーバが使用可能であることを定期的に確認し、プライマリサーバが使用可能になったら接続を再開します。

クラスタ内のすべてのスイッチは、同じ KMC サーバを使用します。スイッチがセカンダリサーバに接続すると、セカンダリサーバにクラスタ全体が自動的にフェールオーバーします。クラスタ内のスイッチは、プライマリサーバが使用可能になればそれにフェールオーバーします。



(注) プライマリおよびセカンダリサーバをクラスタの作成時に設定するか、または作成したクラスタのキーマネージャ設定を更新します。

## データセンター間でのキーの自動キーレプリケーションについて



(注) データセンター間でのキーの自動キーレプリケーションは、SME テープのみに適用されます。

メディアキーの自動レプリケーションにより、データセンター間でテープを移動させることができます。キーのレプリケーションにより、同じテープメディアを複数の SME クラスタでアクセスできるようになります。たいいていの場合、SME クラスタは、プライマリデータセンターやディザスタリカバリサイトなど、さまざまな場所にあります。SME により、ユーザはメディアキーを1つの SME クラスタから1つ以上のクラスタに自動的に複製することができます。キーを自動的に複製するプロセスにより、手動でのキーのエクスポートとインポートの手順が不要になります。メディアキーの自動レプリケーションは、テープボリュームグループ単位で設定されます。

1つの KMC ですべてのデータセンターを管理し、複製されたキーは KMC に保存されます。

## メディアのキーの変換

各クラスタは、変換コンテキストに関連付けられます。変換コンテキストには、いずれかのクラスタの暗号モジュールによって生成されたキーペアの公開キーが含まれています。

レプリケーション関係は、異なるクラスタにあるボリュームグループの間で設定され、宛先クラスタのレプリケーションコンテキストを取得する必要があります。クラスタ間でこの関係がセットアップされると、ソースクラスタでキーが生成される場合はいつでも、そのキーは宛先クラスタ向けに自動的に変換されます。

キーの変換はスケジュールされたプロセスであり、プリセットされた頻度に基づいて、期間内に生成されたすべてのキーペアは、宛先クラスタ向けに変換されます。最後のジョブ開始時刻以降の、生成されてレプリケーションがスケジュールされているすべてのキーは、宛先クラスタの公開キーであるレプリケーションコンテキストを使用して変換されます。

データセンター間のキーレプリケーションには、キー階層の変換が必要です。ソースクラスタからのキーは、宛先クラスタの公開キーを使用して変換されてから、宛先クラスタに送信されます。宛先クラスタで、キーは宛先クラスタの秘密キーでアンラップされ、次に宛先クラスタのキー階層でラップされます。

## アカウントिंग ログ情報について

この項では、KMC アカウントिंग ログ メッセージについて説明します。

DCNM-SAN ログ ディレクトリ内の `accounting.log` ファイルは、KMC アカウントिंग ログ メッセージを表示します。アカウントング ログには、キー関連操作、結果のステータス、および関連情報が記録されます。

ログ ファイルは、リレーショナル データベースに保存され、検索可能、アーカイブ可能、およびポータブルです。

ログ エントリは次の情報で構成されます。

- `hostname`: 操作が実行されたホスト マシンの名前。
- `timestamp`: アカウントング ログ システムにイベントが記録された時刻。
- `username`: 操作に関連するユーザ名。
- `clusterName`: 操作が実行されたクラスタの名前。
- `clusterId`: 操作が実行されたクラスタの ID。
- `operation`: 操作のタイプ。
- `status`: イベントがログに記録されたときの操作のステータス。
- `details`: 操作のタイプに応じての、追加データ。

## CLI を使用した SME キー管理の設定

このセクションでは、固有キー モードまたは共有キー モードの設定について説明しています。

### 固有キー モードまたは共有キー モードの設定



(注) 固有キー モードまたは共有キー モードは、SME テープにのみ適用されます。

共有キー モードは、バックアップ テープのグループに使われる単一のキーを生成するために使用します。

固有キー モードは、各テープ カートリッジ用の固有または特定のキーを生成するために使用します。



(注) キー モードを設定する前に、Cisco KMC を設定します。「[Cisco Key Management Center について](#)」セクション(7-3 ページ)を参照してください。

## 手順の詳細

共有キー モードまたは固有キー モードを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster clustername1</b> switch(config-sme-cl)#	クラスタを指定し、SME クラスタ設定サブモードを開始します。
ステップ 3	switch(config-sme-cl)# <b>shared-key mode</b> switch(config-sme-cl)#	共有キー モードを指定します。
ステップ 4	switch(config-sme-cl)# <b>no shared-key mode</b> switch(config-sme-cl)#	共有の固有キー モードを指定します。

## SME キー管理のモニタリング

- [KMC アカウンティング ログ メッセージ出力の表示\(7-8 ページ\)](#)
- [アカウンティング ログ情報の表示\(7-143 ページ\)](#)
- [SME テープのキーの表示\(7-12 ページ\)](#)
- [SME ディスクのキーの表示\(7-13 ページ\)](#)

## KMC アカウンティング ログ メッセージ出力の表示

ログ エントリの出力は、次の形式で表示されます。

```
"<timestamp> User: <username> Host: <host> Cluster: <cluster name> Id:
<cluster id> Operation: <operation> Status: <status> Details: <details>"
```

The following is a complete listing of logged SME operations and expected status values. The logged details for an operation depends upon the resulting status of the operation and/or other criteria documented below.

```
-----
Operation: STORE_KEY          Logged as: "Store key"
Description: A new key is being written to the keystore. The details
for the accounting log of a STORE_KEY operation depends upon the
KEY_TYPE and the STATUS for the operation.

Details:

KEY_TYPE: MasterKey

SUCCESS: "key type: <key type> GUID: <guid>"
FAILURE: "key type: <key type> GUID: <guid> error: <description>"

KEY_TYPE: TapeVolumeGroupSharedKey

SUCCESS: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name>"
FAILURE: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> error: <description>"
```



```
KEY_TYPE: TapeVolumeGroupWrapKey

SUCCESS: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name>"
FAILURE: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> error: <description>"

KEY_TYPE: TapeVolumeKey

SUCCESS: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> barcode: <barcode>"
FAILURE: "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> barcode: <barcode>
error: <description>"

-----
Operation: GET_KEY          Logged as: "Retrieve key"
Description: A key is being requested from keystore.The details for
the accounting log of a GET_KEY operation depend upon the query
parameter and STATUS for the operation.

Details:

QUERY PARAMETER: Guid

SUCCESS: "GUID: <guid>"
FAILURE: "GUID: <guid>"

QUERY PARAMETER: Cloned from Guid

SUCCESS: "Cloned from GUID: <guid>"
FAILURE: "Cloned from GUID: <guid>"

-----
Operation: ARCHIVE_KEY     Logged as: "Archive key"
Description: A key is removed from "active" state and moved to
"archived" state.

Details:

SUCCESS: "GUID: <guid>"
FAILURE: "GUID: <guid> error: <description>"

-----
Operation: ARCHIVE_ALL_KEYS Logged as: "Archive all keys"
Description: All keys are archived for an instance of a KEY_TYPE.
The details for the accounting log of a ARCHIVE_ALL_KEYS operation
depends upon the KEY_TYPE and the STATUS for the operation.

Details:

KEY_TYPE: TapeVolumeGroupSharedKey

SUCCESS: "tape group: <tape group name> tape volume group: <tape
volume group name>"
FAILURE: "tape group: <tape group name> tape volume group: <tape
volume group name> error: <description>"

KEY_TYPE: TapeVolumeGroupWrapKey

SUCCESS: "tape group: <tape group name> tape volume group: <tape
volume group name>"
FAILURE: "tape group: <tape group name> tape volume group: <tape
volume group name> error: <description>"
```

KEY\_TYPE: TapeVolumeKey

SUCCESS: "tape group: <tape group name> tape volume group: <tape volume group name> barcode: <barcode>"

FAILURE: "tape group: <tape group name> tape volume group: <tape volume group name> barcode: <barcode> error: <description>"

-----  
 Operation: PURGE\_KEY Logged as: "Purge key"  
 Description: A key and references to it are removed from the keystore.

Details:

SUCCESS: "GUID: <guid>"

FAILURE: "GUID: <guid> error: <description>"

-----  
 Operation: DELETE\_ALL\_TAPE\_VOLUME\_KEYS Logged as: "Delete Tape Volume Keys"

Description: All tape volume keys for the given tape volume are removed from the keystore.

Details:

SUCCESS: "tape group: <tape group name> tape volume group: <tape volume group name>"

-----  
 Operation: DELETE\_ALL\_TAPE\_VOLUME\_SHARED\_KEYS Logged as: "Delete Tape Volume Group Shared Keys for cluster"

Description: All shared keys for the given tape volume are removed from the keystore.

Details:

SUCCESS: "tape group: <tape group name> tape volume group: <tape volume group name>"

-----  
 Operation: DELETE\_ALL\_TAPE\_VOLUME\_WRAP\_KEYS Logged as: "Delete Tape Volume Group Wrap Keys for cluster"

Description: All wrap keys for the given tape volume are removed from the keystore.

Details:

SUCCESS: "tape group: <tape group name> tape volume group: <tape volume group name>"

-----  
 Operation: EXPORT\_ARCHIVED Logged as: "Export archived cluster"  
 Description: An archived cluster is being exported. The operation is being logged per tape volume group exported for the requested cluster.

Details:

INITIATED: "tape group: <tape group name> tape volume group: <tape volume group name> keys exported: null"

SUCCESS: "tape group: <tape group name> tape volume group: <tape volume group name> keys exported: <count>"

FAILURE: "tape group: <tape group name> tape volume group: <tape volume group name> keys exported: <count> error: <description>"

```
-----
Operation: EXPORT          Logged as: "Export cluster"
Description: A cluster is being exported.The operation is being
logged per tape volume group exported from the requested cluster.

Details:

INITIATED:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: null"
SUCCESS:    "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count>"
FAILURE:    "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count> error: <description>"

-----
Operation: IMPORT          Logged as: "Import keys"
Description: Keys are imported into a cluster.The operation is being
logged per tape volume group.

Details:

INITIATED:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: null"
SUCCESS:    "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: <count>"
FAILURE:    "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: <count> of <total count> total.
Skipped : <count> error: <description>"

-----
Operation: REKEY_MASTER_KEY      Logged as: "Master key rekey"
Description: A master key is being "re-keyed" or replaced with a new
master key.All keys wrapped w/ the old master key are unwrapped and
re-wrapped with the new master key.

Details:

INITIATED:  ""
SUCCESS:    ""
FAILURE:    "error: <description>"

-----
Operation: ABORT_REKEY_MASTER_KEY      Logged as: "Abort master key
rekey"
Description: A re-key operation has been aborted.If the operation
cannot be aborted, the failure is logged.

Details:

SUCCESS:    ""
FAILURE:    "error: <description>"

-----
Operation: GET_MASTER_KEY_SHARE      Logged as: "Master key share
retrieved"
Description: When storing master key shares on smartcards, the share
is verified as being written correctly by reading the share and
comparing.This logs the result of that GET operation.

Details:

SUCCESS:    "share index: <share index> smartcard label: <smartcard
label> smartcard serial number: <serial number> GUID: <guid>"
```

```
FAILURE: "share index: <share index> smartcard label: <smartcard
label> smartcard serial number: <serial number> GUID: <guid> error:
<description>"
```

```
-----
Operation: REKEY_CLONE_WRAP_KEYS          Logged as: "Clone tape volume-
group wrap keys"
```

```
Description: Part of Master Key re-key involves cloning wrap keys and
re-wrapping them with the new master key.This logs the result of
that cloning and re-wrap operation.
```

```
Details:
```

```
SUCCESS: "<count> keys of <total count> cloned successfully"
```

```
FAILURE: "<count> keys of <total count> cloned successfully"
```

SME アカウンティング ログは、4.2.x として設定できます。アカウンティング エントリはデータベースで作成され、定義されたスケジュールでファイルにフラッシュされます。デフォルトでは、これは週単位で実行されます。ログは固有の名前を持つファイル(たとえば、**smc\_accounting\_log.2011-01-30-12-00-01.log**)に書き込まれます。このファイルは、DCNM アプリケーションを実行しているホストの、たとえば **<Install Path>/dcm/fm/logs** ディレクトリから入手できます。

ステップ 1 **<Install Path>/dcm/fm/conf/smeserver.properties** ファイルを編集します。

ステップ 2 **smc.kmc.archive.accounting.log.frequency=** を追加します。

有効な値は次のとおりです。

- hourly
- daily
- weekly
- monthly
- test(検証する場合は、5 分おきに実行されます)。これはイネーブルのままにしておいてはなりません。そのようにすると、マシンはファイルでフラッシュすることになります。



(注) ファイルの性質上、SME がこれらのファイルを削除したり、上書きしたりすることはありません。test や hourly を設定しても、時間の経過とともにかなりの数のファイルが生成されます。データベースからまだフラッシュされていないアカウンティング ログ エントリは、[Accounting Log] タブに表示されます。

## SME テープのキーの表示

固有のテープ ボリューム キー、テープ ボリューム グループ キー、および共有テープ ボリューム グループ キーに関する情報を表示できます。DCNM-SAN Web クライアントを使用して、Cisco KMC に保存されるキーを表示できます。キーの生成時に、それらはアクティブとしてマーキングされます。インポートされたキーは非アクティブとマーキングされます。キーがクリア テキストで表示されることは絶対にありません。

## SME ディスクのキーの表示

ディスク キーに関する情報を表示できます。DCNM-SAN Web クライアントを使用して、Cisco KMC に保存されるキーを表示できます。キーの生成時に、それらはアクティブとしてマーキングされます。インポートされたキーは非アクティブとマーキングされます。キーがクリア テキストで表示されることは絶対にありません。

## SME キー管理の機能履歴

表 7-3 に、この機能のリリース履歴を示します。

表 7-3 SME キー管理の機能履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
KMC サーバの移行	4.1(1c)	4.1(1c) では、KMC サーバを移行できます。
アカウントिंग ログ	4.1(1c)	4.1(1c) 以降では、ユーザは Fabric Manager Web Client の [SME] タブに、キー再生成操作とそのステータスを表示できます。
高可用性 KMC サーバ	4.1(3)	高可用性 KMC は、プライマリ サーバとセカンダリ サーバを使用して設定できます。 4.1(3) では、HA の設定は [Key Manager Settings] ページで確認できます。 プライマリ サーバとセカンダリ サーバは、クラスタの作成時に選択できます。 プライマリ サーバとセカンダリ サーバの設定は、[Cluster Detail] ページで変更できます。
メディア キーの自動レプリケーション	4.1(3)	4.1(3) では、テープ キー レプリケーションは、リモート レプリケーションと呼ばれていました。リモート レプリケーション関係は、ボリューム グループ間で設定できます。SME により、ユーザはメディア キーを 1 つの SME クラスタから 1 つ以上のクラスタに自動的に複製することができます。 4.1(3) では、リモート レプリケーション関係の設定を使用できます。
ホスト名は、サーバアドレスとして受け入れられます。	4.1(3)	サーバ用に IP アドレスまたはホスト名を入力できます。

表 7-3 SME キー管理の機能履歴(続き)

機能名	リリース	機能情報
ボリューム キーの再生成	3.3(1c)	ボリューム キーのキー再生成は、セキュリティをさらに強化するために実行されます。またはセキュリティが侵害された場合にも実行されます。
マスター キーの再生成	3.3(1c)	Advanced モードでは、スマートカードの交換により、マスター キーのキー再生成がトリガされ、マスター キーの新しいバージョンがクラスタ用に生成されます。マスター キー共有の新しいセットがスマートカードに保存されます。すべてのボリューム グループ キーも、新しいマスター キーと同期します。



## 証明書のプロビジョニング

Secure Sockets Layer (SSL) プロトコルにより、ネットワーク通信を保護し、送信前のデータを暗号化し、セキュリティを実現することができます。多くのアプリケーションサーバと Web サーバは、SSL 設定用の keystore の使用をサポートしています。スイッチと KMC との間での SSL するには、公開キー インフラストラクチャのプロビジョニングが必要です。

この章では、次の事項について説明します。

- [公開キー インフラストラクチャ証明書に関する情報 \(8-1 ページ\)](#)
- [SSL の前提条件 \(8-1 ページ\)](#)
- [CLI を使用した SSL の設定 \(8-2 ページ\)](#)
- [SSL の機能履歴 \(8-6 ページ\)](#)

## 公開キー インフラストラクチャ証明書に関する情報

証明書は、サーバや企業などのエンティティを識別し、その ID を公開キーに関連付けるために使用される電子ドキュメントです。

認証局 (CA) は、ID を確認して証明書を発行する機関です。CA が発行する証明書により、その証明書が特定するエンティティ名 (サーバ名やデバイス名など) に、特定の公開キーがバインドされます。証明書で認証された公開キーだけが、証明書が特定するエンティティが所有している対の秘密キーと機能します。証明書により、偽装目的の疑似公開キーの使用を防ぐことができます。

## SSL の前提条件

SSL を設定する前に、次の点に注意してください。

- キー、証明書、および証明書署名要求を生成するために、無料で使用できる OpenSSL アプリケーションなどのサードパーティ製ツールをインストールする必要があります。Windows 用の OpenSSL を次のリンクからダウンロードします。  
<http://gnuwin32.sourceforge.net/packages/openssl.htm> Windows にインストールした場合、openssl.exe はデフォルトでは c:\openssl\bin にあります。
- すべてのスイッチ、DCNM-SAN、および OpenSSL コマンドを実行しているシステムの時刻が同期していることを確認します。
- CA 証明書と KMC 証明書にそれぞれ異なる ID を指定します。
- JRE1.6 JAVA keytool のみが、Java Keystores (JKS) ファイルへの PKCS12 証明書のインポートをサポートします。

## CLIを使用したSSLの設定

ここでは、SSLの設定に関する次の内容について説明します。

- [CA 証明書の作成 \(8-2 ページ\)](#)
- [トラストポイントの設定 \(8-2 ページ\)](#)
- [トラストポイントの削除 \(8-4 ページ\)](#)
- [KMC 証明書の生成 \(8-5 ページ\)](#)

### CA 証明書の作成

組織は事前に CA 証明書を所有している可能性があります。セキュリティ管理者に CA を要求する場合には、PEM フォーマットの CA 証明書を必要としており、SME 設定の一部として証明書に署名されている必要があることを伝えます。既存の CA がないかまたはそれを使用したくない場合は、OpenSSL コマンドを使用して新しい CA を作成できます。

このコマンドを使用して、認証局 (CA) を作成します。このコマンドは、証明書 (ID と公開キー) および秘密キーを作成します。秘密キーは必ず保護する必要があります。一般的な企業組織では、秘密キーは必ず事前に備えているはずです。

OpenSSL アプリケーションを使用して CA 証明書を作成します。365 日証明書に対しては、次のコマンドを入力します。

```
OpenSSL> req -x509 -days 365 -newkey rsa:2048 -out cacert.pem -outform PEM
```

このコマンドは、cacert.pem および privkey.pem という 2 つのファイルを、OpenSSL.exe があるディレクトリ内に作成します。cacert.pem ファイルは、証明書です。privkey.pem ファイルは、安全な場所に保存する必要があります。

### トラストポイントの設定

この一連の手順は、DCNM-SAN サーバが管理するすべてのスイッチに対して実行する必要があります。必ず同じトラストポイント名をすべてのスイッチに使用します。

#### 手順の詳細

トラストポイントを設定するには、次の手順を実行します。

**ステップ 1** コンフィギュレーション モードを開始します。

```
switch# config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

**ステップ 2** my\_ca という名前のトラストポイントを作成します。

```
switch(config)# crypto ca trustpoint my_ca
```

**ステップ 3** トラストポイント サブモードで、スイッチの RSA キーのペアを作成します。

```
switch(config-trustpoint)# rsakeypair my_ca_key 2048
```

**ステップ 4** トラストポイント サブモードを終了します。

```
switch(config-trustpoint)# exit
```



- ステップ 5** 手順1で作成した `cacert.pem` の内容をカットアンドペーストして、トラストポイントの `cacert.pem` ファイルを認証します。

```
switch(config)# crypto ca authenticate my_ca

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
----BEGIN CERTIFICATE-----
MIIDnjCCAwegAwIBAgIBADANBgkqhkiG9w0BAQQFADCBzELMAkGA1UEBhMCVVMx
EzARBGNVBAgTCkNhbG1mb3JuaWEwEzETAPBgNVBACrCFNhb3N1MR0wGAYDVQQK
ExF0aXNjbyBTZXR0ZXRlc3R1ZIEluYzEOMAwGA1UECXMFRGV2ZWwxEzETAPBgNV
bWFzc2V5MSEwHwYJKoZIhvcNAQkBFhJtYWIhczNleUBjaXNjby5jb20wHhcNMDCx
MTIyMDgzNDMlWhcNMDg2MTIxMDgzNDMlWjCBzELMAkGA1UEBhMCVVMxEzARBGNV
BAgTCkNhbG1mb3JuaWEwEzETAPBgNVBACrCFNhb3N1MR0wGAYDVQQKEzF0aXNj
byBTZXR0ZXRlc3R1ZIEluYzEOMAwGA1UECXMFRGV2ZWwxEzETAPBgNVBAMTCG1h
bWFzc2V5MSEwHwYJKoZIhvcNAQkBFhJtYWIhczNleUBjaXNjby5jb20wGz8wDQYJ
KoZIhvcNAQEBBQADGQY0AMIGJAoGBAMbZAv0+Ka/FS3/jwdaqItc8Ow3alpw9gyqEzA
3uFLjNtXSFHRu9OsrP5tliHHlJP+fezeAUUvfmMTPROIxURcF2c7Yq1Ux5s4Ua3cmGf9B
G AgMBAAAGjGfcwgfQwHQYDVR0OBBYEfGxsBg7f7FJcL/741j+M2dgI7rIyMIHEBGN
VHSMEgbbwgbmAFGXsBg7f7FJcL/741j+M2dgI7rIyoYGdpIGAmIGXMQswCQYDVQQG
EwJVVUzETMBEQA1UECBMkQ2FsaWZvcj5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGjAY
BgNVBAoTTEUENpc2NvIFN5c3RlRlYwMjM2ZmM2MDg0MzJmMDQ4WDAYDVQQLZWwEVEZ
XZlbnRMA8GA1UEAxMIbWFTYXNzZXkxITAfBgkqhkiG9w0BCQEWEmlhbWwzV5QGNpc2Nv
LmNvbYIBADAMBGNVHRMTEBATAQH/MAOGCSqGSIb3DQEBAUUA4GBAFmDucZ1BZFJK09Ii
Em5wd4oouxHsKPQroyG/CYShv1XXAyEGYtXUCAITDzMQ2IJiFbz0kIiyuP9YRQLNR
z47G4IRJGp5J2HnOc2cdF8Mc0DDApdgdndUiIX/lv7vuQfyxqX45oSncwQct3y38/
FPEbcRgZgnOgwcrqBzKV0Y3+
----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=1E:18:10:69:7B:C1:CC:EA:82:08:67:FB:90:7D:58:EB

Do you accept this certificate? [yes/no]:yes
```

- ステップ 6** 手順2で作成したトラストポイントに登録するための証明書要求を生成します。この要求は、CA がスイッチの証明書に署名するために使用します。

```
switch(config)# crypto ca enroll my_ca

Create a challenge password.You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:nbv123
The subject name in the certificate will be: ips-vegas8.cisco.com
Include the switch serial number in the subject name? [yes/no]:no
Include an IP address in the subject name [yes/no]:no
The certificate request will be displayed...

----BEGIN CERTIFICATE REQUEST-----
MIIBJTCB0AIBADAfMR0wGwYDVQQDEXRpcHMTdmVnYXk0LmNpc2NvLmNvbTBcMAOG
CSqGSIb3DQEBAQUAA0sAMEgCQCeAzn5w9d32YpPfYdNYoFjOW0yRVbYEE+mNH18
b2VPOVZ6UoFdhISlIm0/Xv1Bpcuy4TRktu7whNyyvvu3niVdAgMBAAAGTDAVBGkq
hkiG9w0BCQcxCBMGBmJ2MTIzMDMGCSqGSIb3DQEBJdJEmMCQwIgyYDVR0RAQH/BBgw
FoIUaXBzLXZlZ2FzOC5jaXNjby5jb20wDQYJKoZIhvcNAQEBBQADQQBzPcKE3Eje
TjODnPXNkz1WsU3oUdsuxOT/m1OSBZvhBfHICQZzPfs2ILqaQP16LiZCYdHWwIn
Q+9LmHUZ4BDG
----END CERTIFICATE REQUEST-----

switch(config)#
```

**ステップ 7** OpenSSL.exe があるディレクトリ内に switch.csr というファイルを作成します。手順 6 で作成した証明書要求をカット アンド ペーストします。

ファイルの内容に、BEGIN CERTIFICATE REQUEST 行と END CERTIFICATE REQUEST 行を必ず組み込みます。

**ステップ 8** 次のコマンドを入力して、OpenSSL アプリケーションでスイッチ証明書要求を使用して証明書を生成します。

```
OpenSSL> x509 -req -days 365 -in switch.csr -CA cacert.pem -CAkey privkey.pem -set_serial 01 -out switch.pem
```

これが、CA によって署名されたスイッチのパブリック証明書になります。



(注) セキュリティ管理者が CA を制御している場合、セキュリティ管理者に switch.csr ファイルを送信し、この手順の実行と switch.pem ファイルでの応答を依頼する必要があります。

**ステップ 9** 手順 8 で作成された switch.pem ファイルの内容をカット アンド ペーストして、スイッチ上に署名付き証明書をインポートします。

```
switch(config)# crypto ca import my_ca certificate
input (cut & paste) certificate in PEM format:
----BEGIN CERTIFICATE----
MIIB4jCCAUsCAQEWdQYJKoZIhvcNAQEEBQAwwGZcxZAJBgNVBAYTA1VTMRMwEQYD
VQQLIExpDyWxpZm9ybmlhMREwDwYDVQQHEWhTYW4gSm9zZTEaMBGGA1UEChMRQ21z
Y28gU31zdGVtcyBJbmMxMjQjAMBgNVBAsTBUR1dmVsMREwDwYDVQQDEWhTYW1hc3Nl
eTEhMB8GCSqGSIb3DQEJARYSBWFTYXNzZX1AY21zY28uY29tMB4XDTA3MTIxNDAY
MzIzOVVhZDQ4MTIxMzAyMzIzOVVhZEdMBSGA1UEAxMUaXBzLXZlZ2FzOC5jaXNj
by5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEAangM7+cPXd9mKT32HTWKBYz1t
MkVW2BHvpjR4vG91Tz1wElDhXYSEtSjtP179QaXLSuE0ZLbu8ITcsr77t541XQID
AQABMA0GCSqGSIb3DQEBAUAA4GBAKR3WAAF/9zMb2u9A42I2cB2G51ucSzn4cP
+04sYZF5pBt7UpyAs1GKAqivGXVq2FJ2JetX78Fqy7jYCzanWm0tck0/G1dSfr/X
lCFXUuVed9de02yqxARSEx8mX4ifqzYHERHdbi+vDAaMzkUEvHWthOuUZ7fvpNH
+xhRAuBo
----END CERTIFICATE----
```

これで、スイッチ上のトラストポイントの設定が完了しました。これには定義されたトラストポイント、認識される CA、公開キーと秘密キーのペア、およびスイッチを識別する CA 署名付き証明書が含まれます。署名付き証明書は、CA を認識するすべてのエンティティとの PKI 通信にも使用できます。ファブリック内のすべてのスイッチに対して、手順 1 ~ 9 を繰り返します。

## トラストポイントの削除

この一連の手順は、暗号化された CA 署名済みトラストポイントを削除するために、すべてのスイッチに対して実行する必要があります。

### 手順の詳細

トラストポイントを削除するには、次の手順を実行します。

**ステップ 1** コンフィギュレーション モードを開始します。

```
switch# config t
```

Enter configuration commands, one per line. End with CNTL/Z.

- ステップ 2    トラストポイント モードに入ります。  
switch(config)# **crypto ca trustpoint my\_ca**
- ステップ 3    トラストポイントに対応する証明書を削除します。  
switch(config-trustpoint)# **delete certificate force**
- ステップ 4    トラストポイント サブモードでスイッチの RSA キー ペアを削除します。  
switch(config-trustpoint)# **no rsakeypair my\_ca\_key**
- ステップ 5    トラストポイントに対応する CA 証明書を削除します。  
switch(config-trustpoint)# **delete ca-certificate**
- ステップ 6    トラストポイント サブモードを終了します。  
switch(config-trustpoint)# **exit**
- ステップ 7    設定されているトラストポイントを削除します。  
switch(config)# **no crypto ca trustpoint my\_ca**
- 

## KMC 証明書の生成

### 手順の詳細

KMC 証明書を生成するには、次の手順に従います。OpenSSL アプリケーションで次のコマンドを入力して、KMC 証明書を生成します。

- ステップ 1    KCM サーバの秘密キーを作成します。  
OpenSSL> **genrsa -out sme\_kmc\_server.key 2048**
- ステップ 2    手順 1 で作成した秘密キーを使用して、証明書署名要求を作成します。  
OpenSSL> **req -new -key sme\_kmc\_server.key -out sme\_kmc\_server.csr -config openssl.conf**
- ステップ 3    証明書と秘密キーを使用して、KMC サーバの署名付き証明書を生成します。  
OpenSSL> **x509 -req -days 365 -in sme\_kmc\_server.csr -CA cacert.pem -CAkey privkey.pem -CAcreateserial -out sme\_kmc\_server.cert**



(注)    セキュリティ管理者が CA を制御している場合、セキュリティ管理者に sme\_kmc\_server.csr ファイルを送信し、この手順の実行と sme\_kmc\_server.cert での応答を依頼する必要があります。

- ステップ 4    署名付き KMC 証明書を pkcs12 フォーマットにエクスポートします。  
OpenSSL> **pkcs12 -export -in sme\_kmc\_server.cert -inkey sme\_kmc\_server.key -out sme\_kmc\_server.p12**
- ステップ 5    この PKCS12 キーストアを Java キーストアに、JAVA keytool (JRE 1.6) を使用してインポートします。  
**"<JAVA\_HOME>\bin\keytool" -importkeystore -srckeystore sme\_kmc\_server.p12 -srcstoretype PKCS12 -destkeystore sme\_kmc\_server.jks -deststoretype JKS**



(注) パスワードはプロパティ ファイル内で更新する必要があるため、覚えておいてください。

ステップ 6 CA 証明書を Java キーストアに、JAVA keytool (JRE 1.6) を使用してインポートします。  
`"<JAVA_HOME>\bin\keytool" -importcert -file cacert.pem -keystore sme_kmc_trust.jks -storetype JKS`

ステップ 7 キーストア ファイルを <install path>dcm\fm\conf\cert ディレクトリ内に配置します。

ステップ 8 DCNM-SAN Web クライアントのキー マネージャ設定にある、KMC SSL の設定を変更します。

ステップ 9 DCNM-SAN サーバを再起動します。



(注) さらに、手順 5 と 6 で作成した Java キーストアを使用する代わりに、sme\_kmc\_server.p12 を KMC 証明書として、および cacert.pem を KMC トラスト証明書として使用することもできます。



(注) クラスタが SSL ON オプションで稼働している場合、すべての DCNM のアップグレードにキーストア ファイルの配置が必要です。DCNM のアップグレードでは、キーストア ファイルは保持されません。

## SSL の機能履歴

表 8-1 に、この機能のリリース履歴を示します。

表 8-1 SSL の機能履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
自己署名証明書の生成およびインストール	4.1(1c)	Release 4.1(1c) 以降、KMC の場合の SSL 設定は、Fabric Manager Server からは独立しています。
Secure Sockets Layer (SSL) の導入	3.3(1c)	SME ウィザードで SME に対して SSL を設定し、SSL の設定を編集する方法を説明します。



## RSA キーマネージャと SME

この章では、SME と連携するように RSA キーマネージャ (RKM) をセットアップする際に従うべき手順について説明します。

この章では、次の事項について説明します。

- [RKM の前提条件 \(9-1 ページ\)](#)
- [RKM の設定 \(9-1 ページ\)](#)
- [RKM の機能の履歴 \(9-6 ページ\)](#)



(注) RSA キーマネージャは SME ディスクではサポートされません。これは SME テープにのみ適用されます。

### RKM の前提条件

Cisco KMC と RKM との間で完全に機能するセキュリティ ソリューションを実装するには、RKM アプリケーションをインストールしてセットアップする必要があります。

次のアプリケーションが必要です。

- Windows WK2、XP、または W2K3 ホスト
- DCNM-SAN サーバリリース 3.2(3)
- OpenSSL
- JAVA JDK または JRE

### RKM の設定

SME と連携するように RKM をセットアップするプロセスには、次の作業が含まれます。

- [RKM アプリケーションのインストール \(9-2 ページ\)](#)
- [CA 証明書の生成 \(9-2 ページ\)](#)
- [Java Keytool を使用した JKS ファイルの作成 \(9-4 ページ\)](#)
- [RKM での証明書の配置 \(9-5 ページ\)](#)
- [Cisco KMC から RKM への移行 \(9-5 ページ\)](#)

これらの作業が完了すると、SME のキーマネージャとして RSA を選択して、クラスタを作成できます。

## RKM アプリケーションのインストール

RKM アプリケーションをインストールするには、『*RSA Install Guide*』に記載されている説明に従ってください。

## CA 証明書の生成

このプロセスで作成したファイルは、OpenSSL プログラムの /bin ディレクトリに保存されます。

### 前提条件

- CA 証明書を生成するには、OpenSSL システムへのアクセスが必要です。Windows バージョンは、<http://gnuwin32.sourceforge.net/packages/openssl.htm> で取得できます。

### 手順の詳細

CA 証明書を生成するには、次の手順を実行します。

**ステップ 1** ディレクトリ内の `openssl.exe` をダブルクリックします。

**ステップ 2** OpenSSL アプリケーションを使用してキーを作成します。次のコマンドを入力します。

```
OpenSSL> genrsa -out rt.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.+++++
.....+++++
e is 65537 (0x10001)
```

**ステップ 3** 証明書が有効である期間を設定します。この日付を追跡します。



(注) クライアント証明書とサーバ証明書に異なる共通名を使用します。

```
OpenSSL> req -new -key rt.key -x509 -days 365 -out rt.cert
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:home
Email Address []:
```

**ステップ 4** 適切な pkcs12 証明書を作成します。エクスポートパスワードは、RSA SME のインストールに必要なパスワードです。

```
OpenSSL> pkcs12 -export -in rt.cert -inkey rt.key -out rt.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
```

ステップ 5 クライアント用の新しいキーを生成します。

```
OpenSSL> genrsa -out client.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
....+++++
e is 65537 (0x10001)
```

ステップ 6 client.csr ファイルを作成します。これは所有者です。共通名は、発行元のホームとは異なってなければなりません。

```
OpenSSL> req -new -key client.key -out client.csr
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:cae
Common Name (eg, YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

ステップ 7 証明書が有効である期間を設定します。この日付を追跡します。

```
OpenSSL> x509 -req -days 365 -in client.csr -CA rt.cert -CAkey rt.key -CAcreateserial -out
client.cert
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=wi/L=hudson/O=cisco/OU=cae/CN=mikef/emailAddress=mikef@cisco.com
Getting CA Private Key
```

ステップ 8 pkcs12 証明書を作成します。

```
OpenSSL> pkcs12 -export -in client.cert -inkey client.key -out client.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL> genrsa -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..+++++
.....+++++
e is 65537 (0x10001)
```

ステップ 9 新しいサーバキーを作成します。これは所有者です。共通名は、発行元のホームとは異なってなければなりません。

```
OpenSSL> req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```

If you enter '.', the field will be left blank.
--
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```

**ステップ 10** 証明書が有効である期間を設定します。この日付を追跡します。

```

OpenSSL> x509 -req -days 365 -in server.csr -CA rt.cert -CAkey rt.key -CAcreateserial -out
server.cert
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=wi/L=town/O=cisco/OU=tac/CN=bill/emailAddress=bill@cisco.com
Getting CA Private Key

```

**ステップ 11** serverpub の pkcs12 証明書を作成します。

```

OpenSSL> pkcs12 -export -in server.cert -inkey server.key -nokeys -out serverpub.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

```

**ステップ 12** サーバ用の pkcs12 証明書を再作成します。

```

OpenSSL> pkcs12 -export -in server.cert -inkey server.key -out server.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>

```

## Java Keytool を使用した JKS ファイルの作成

### 手順の詳細

JAVA Keytool を使用して DCNM-SAN に必要な JKS ファイルを作成するには、次の手順を実行します。

**ステップ 1** OpenSSL /bin ディレクトリにある client.p12 および serverpub.p12 を、DCNM-SAN Java ツールのディレクトリ C:\Program Files\Java\jre1.5.0\_11\bin にコピーします。

**ステップ 2** Java /bin ディレクトリの DOS ウィンドウから、SME KMC により必要とされる JKS ファイルを作成します。

```

Import client PKCS12 keystore to JKS
keytool -importkeystore -srckeystore client.p12 -srcstoretype PKCS12 -destkeystore
sme_rkm_client.jks -deststoretype JKS

```



```
Import server PKCS12 keystore to JKS
keytool -importkeystore -srckeystore serverpub.p12 -srcstoretype PKCS12 -destkeystore
sme_rkm_trust.jks -deststoretype JKS
```

これらのキーストア ファイルを mds9000/conf/cert ディレクトリ内に配置して、DCNM-SAN を再起動します。

## RKM での証明書の配置

### 手順の詳細

RKM で証明書を配置するには、次の手順を実行します。

- ステップ 1 すべての証明書を生成したら、rt.p12 ファイルを C:\rkm-2.1.2-trial\certs\rt ディレクトリにコピーします。
- ステップ 2 server.p12 ファイルを C:\rkm-2.1.2-trial\certs\server ディレクトリにコピーします。
- ステップ 3 RKM を再起動します。

## Cisco KMC から RKM への移行

RKM は SME のインストール時に使用できます。または SME を統合 Cisco KMC とともに後で展開することもできます。Cisco KMC を単独で使用した後に RKM を展開する場合は、RKM を SME とともに使用する前に、明示的なキー移行手順を実行する必要があります。

この項では、暗号キー、ラップ キー、および暗号ポリシー情報を、Cisco KMC から RKM に移行する手順を説明します。



(注) 移行手順は、Cisco KMC が PostgreSQL データベースまたは Oracle Express データベースをキーカタログ用に使用している場合は異なるものとなります。その相違点については、該当する箇所で説明されます。



(注) Cisco MDS 9000 NX-OS Software Release 4.1(1c) 以降では、キーは移行前と同じ状態(アクティブまたは非アクティブ)に復元されます。

## RKM の機能の履歴

表 9-1 に、この機能のリリース履歴を示します。

表 9-1 RKM の機能の履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN (DCNM-SAN) という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
RKM の移行手順	4.1(1c)	Cisco KMC から RKM への以降の手順は説明済みです。



## SME ベスト プラクティス

この章では、SME のベスト プラクティスについて説明します。この章で説明されているベスト プラクティスを順守すると、SME を設定する際の問題を回避できます。

### ベスト プラクティスの概要

ベスト プラクティスとは、SME が正常に動作していることを確認するために従う、推奨手順です。SME 設定には次のベスト プラクティスを推奨します。

- [一般的なプラクティス \(10-1 ページ\)](#)
- [SME 設定のプラクティス \(10-1 ページ\)](#)
- [SME ディスクおよび VAAI またはシンプロビジョニングのサポート \(10-2 ページ\)](#)
- [KMC のプラクティス \(10-2 ページ\)](#)
- [ファブリック管理のプラクティス \(10-2 ページ\)](#)

### 一般的なプラクティス

- すべての Cisco MDS スイッチ間で、一貫性のある Cisco NX-OS リリースを維持します。
- 事前設定の情報および手順については、「[SME インストールの計画](#)」の付録を参照してください。
- システム メッセージ ロギングをイネーブルにします。システム メッセージについては、『[Cisco MDS 9000 Family Troubleshooting Guide](#)』を参照してください。
- Cisco SAN-OS または NX-OS リリースのリリース ノートを参照して、最新の機能、制限事項、および注意事項を確認します。

### SME 設定のプラクティス

- 変更を実装したら、新しい設定変更のトラブルシューティングを実施します。
- クラスタを正しく動作させるために、クラスタ内のすべてのスイッチ上ですべての設定変更を保存します。
- バックアップ環境を設計する際には、Cisco SAN-OS または NX-OS でスイッチあたり 1 つのクラスタをサポートすることを検討してください。

- サーバとストレージの間のパスをホストするすべての IT-Nexus を設定に追加する必要があります。そのようにしないとデータの整合性は危険にさらされます。
- SME テープ グループに設定変更を行う場合、設定変更中には、バックアップ アプリケーションを休止しておくことをお勧めします。
- SME インターフェイスのサイジングと配置の指針については、『[Cisco Storage Media Encryption Design Guide](#)』を参照してください。

## SME ディスクおよび VAAI またはシンプロビジョニングのサポート

SME 設定では、VAAI コマンドとシンプロビジョニングはサポートされていません。

次の VAAI コマンドは、SME ではサポートされません。

- Extended Copy
- Compare および Swap
- Compare および Write
- Write Same
- Unmap

## KMC のプラクティス

- データ ストレージが大きくなるにつれて、テープ キーの数も時間の経過とともに増加します。これは、固有キー モードを選択するときに特に当てはまります。Cisco KMC データベースには、アクティブなキーのみを保存することをお勧めします。
- 冗長性と可用性を確実にするために、Cisco KMC データベースは定期的にバックアップすることが重要です。
- Cisco KMC はキーの更新を監視し、TCP ポート上でスイッチからの要求を取得します。デフォルト ポートは 8800 です。ただし、ポート番号は `smeserver.properties` ファイルで変更できます。



(注) 詳細については、『[Storage Media Encryption Key Management White Paper](#)』を参照してください。

## ファブリック管理のプラクティス

DCNM-SAN および Device Manager を使用してファブリックを事前対処的に管理し、危険な状況に陥る前に問題を検出します。



(注) SME のサイジングとトポロジの指針に関する詳細およびケース スタディについては、『[Cisco Storage Media Encryption Design Guide](#)』を参照してください。



## SME のトラブルシューティング

この章では、Cisco Storage Media Encryption の問題を解決するための基本的なトラブルシューティングについて説明します。

この章は、次の項で構成されています。

- [トラブルシューティング リソース\(11-1 ページ\)](#)
- [クラスタ リカバリのシナリオ\(11-1 ページ\)](#)
- [一般的な問題に関するトラブルシューティング\(11-5 ページ\)](#)
- [トラブルシューティング シナリオ\(11-6 ページ\)](#)

### トラブルシューティング リソース

トラブルシューティングの詳細については、『*Cisco MDS 9000 Family NX-OS Troubleshooting Guide*』に、Cisco MDS 9000 ファミリのスイッチを使用してストレージエリア ネットワーク (SAN) を展開するときに起きることがある問題の、トラブルシューティングの指針が記載されています。『*Cisco MDS 9000 NX-OS Family Troubleshooting Guide*』では、問題を認識し、その原因を判別し、可能な解決策を見つけるために使用できるツールと方法論を紹介しています。

### クラスタ リカバリのシナリオ

この項では、SME クラスタ内で 1 つ以上のスイッチがオフラインであるか、または 1 つのスイッチから別のスイッチにマスター スイッチの割り当てを変更するときに使用する、リカバリ手順について説明します。手順は次のとおりです。

- [SME クラスタからのオフライン スイッチの削除\(11-2 ページ\)](#)
- [マスター スイッチがオンライン中の 1 つ以上のオフライン スイッチがある SME クラスタの削除\(11-2 ページ\)](#)
- [すべてのスイッチがオフラインの場合の SME クラスタの削除\(11-3 ページ\)](#)
- [SME クラスタの活性化\(11-4 ページ\)](#)



(注) この項の手順では、CLI を使用するトラブルシューティング ソリューションについて説明します。



(注) オフラインスイッチ向け SME クラスタ設定は、CLI を使用して行う必要があります。オンラインスイッチ向け SME クラスタ設定は、DCNM-SAN または CLI を使用して実行できます。

## SME クラスタからのオフラインスイッチの削除

1つ以上のスイッチがオフラインで、マスタースイッチがオンラインの場合にオフラインスイッチを削除するには、次の手順を実行します。

オフラインスイッチ(たとえば、switch2)で、この作業を実行してクラスタをシャットダウンします。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>shutdown</b>	オフラインスイッチの ABC クラスタをシャットダウンします。



(注) すべてのオフラインスイッチで手順を繰り返します。

クラスタ マスター スイッチで、この作業を実行してオフラインスイッチ(たとえば、switch2)を削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>no node switch2</b>	ABC クラスタ設定から switch2 を削除します。 (注) 手順 1 でシャットダウンされたあらゆるオフラインスイッチに対して、この手順を繰り返します。

オフラインスイッチ(switch2)では、この作業を実行してクラスタを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# <b>no sme cluster ABC</b>	ABC クラスタ設定を削除します。



(注) 最初の手順でシャットダウンされたあらゆるオフラインスイッチでクラスタを削除します。

## マスタースイッチがオンライン中の1つ以上のオフラインスイッチがある SME クラスタの削除

1つ以上のオフラインスイッチおよびオンラインマスタースイッチが含まれている SME クラスタを削除するには、次の手順を実行します。



注意

クラスタ マスター スイッチをクラスタから削除せずに、オフライン スイッチのクラスタを活性化させるようにしてください。オフライン スイッチは運用クラスタの一部でなかったため、クラスタ マスターはオフライン スイッチの状態を超えて進行していた可能性があります。クラスタ マスターを削除し、オフライン スイッチ上のクラスタを活性化させると、データの破損が発生する可能性があります。

オフライン スイッチ (switch2) で、この作業を実行してクラスタをシャットダウンします。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>shutdown</b>	オフライン スイッチの ABC クラスタをシャットダウンします。



(注)

すべてのオフライン スイッチで手順を繰り返します。

クラスタ マスター スイッチで、オフライン スイッチ (switch2) を削除し、この作業を実行してクラスタを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>no node switch2</b>	ABC クラスタ設定から switch2 を削除します。 (注) 最初の手順でシャットダウンされたすべてのオフライン スイッチに対して、この手順を繰り返します。
ステップ 3	switch(config)# <b>no sme cluster ABC</b>	ABC クラスタ設定を削除します。

オフライン スイッチ (switch2) では、この作業を実行してクラスタを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>no sme cluster ABC</b>	ABC クラスタ設定を削除します。



(注)

最初の手順でシャットダウンされたあらゆるオフライン スイッチでクラスタを削除します。

## すべてのスイッチがオフラインの場合の SME クラスタの削除

マスター スイッチと他のすべてのスイッチでオフラインになっている場合に SME クラスタを削除するには、次の手順を実行します。



(注)

すべてのスイッチがオフラインの場合、クラスタはオフラインです。

オフライン スイッチ(たとえば、switch2)で、この作業を実行してクラスタをシャットダウンします。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>shutdown</b>	オフライン スイッチの ABC クラスタをシャットダウンします。



(注) すべてのオフライン スイッチでこの手順を繰り返します。

クラスタ マスター スイッチで、クラスタをシャットダウンしてからこの作業を実行してクラスタを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b> switch(config-sme-cl)# <b>shutdown</b>	ABC クラスタをシャットダウンします。
ステップ 3	switch(config)# <b>no sme cluster ABC</b>	ABC クラスタ設定を削除します。

オフライン スイッチ (switch2) では、この作業を実行してクラスタを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>no sme cluster ABC</b>	ABC クラスタ設定を削除します。



(注) 最初の手順でシャットダウンされたあらゆるオフライン スイッチでクラスタを削除します。

## SME クラスタの活性化

SME 設定が最新版のスイッチでクラスタを活性化するには、次の手順を実行します。

1 つ以上のスイッチがオフラインで、クラスタが動作不能(たとえば、クォーラム損失による)の場合、次の手順を実行してクラスタを活性化します。このリカバリ手順には、1 つ以上のオフライン スイッチの削除、また残りのスイッチのクラスタの活性化が含まれます。



注意

SME クラスタは、**show sme cluster detail** コマンドに表示されているように、SME 設定が最新版のスイッチでのみ活性化する必要があります。設定のバージョンが最も高いものではないスイッチのクラスタを活性化させると、データが損傷する可能性があります。

次のタスクに従って、すべてのスイッチ上のクラスタ設定をシャットダウンします。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b>	ABC という名前の SME クラスタを作成します。



	コマンド	目的
ステップ 3	<pre>switch(config-sme-cl)# shutdown This change can be disruptive.Please ensure you have read the "SME Cluster Recovery Procedure" in the configuration guide.-- Are you sure you want to continue? (y/n) [n] y switch(config-sme-cl)#</pre>	スイッチの ABC クラスタをシャットダウンします。

前の項でシャットダウンした、オフライン スイッチ上のクラスタ設定を、次の作業を実行して削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>no sme cluster ABC</b>	オフライン スイッチの ABC クラスタをシャットダウンします。

クラスタ マスター スイッチ上で、次の作業を実行して、すべてのスイッチを削除します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b>	ABC という名前の SME クラスタを作成します。
ステップ 3	<pre>switch(config-sme-cl)# no node switchname switch(config)#</pre>	設定からスイッチを削除します。 (注) 削除する必要のあるすべてのスイッチに繰り返します。

残りのスイッチ上のクラスタ設定を、次の作業を実行して再起動します。

	コマンド	目的
ステップ 1	switch# <b>config t</b>	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# <b>sme cluster ABC</b>	ABC という名前の SME クラスタを作成します。
ステップ 3	<pre>switch(config-sme-cl)# no shutdown This change can be disruptive.Please ensure you have read the "SME Cluster Recovery Procedure" in the configuration guide.-- Are you sure you want to continue? (y/n) [n] y switch(config-sme-cl)#</pre>	スイッチ上の ABC クラスタを起動します。

## 一般的な問題に関するトラブルシューティング

SME 命名規則には、英数字、ダッシュ、およびアンダースコア文字が含まれます。他のタイプの文字は、クラスタ構成で問題が生じる原因となります。

# トラブルシューティングシナリオ

この項では、次のシナリオについて説明します。

- DNS がクラスタ内のすべてのスイッチ上で設定されているのではない場合(11-6 ページ)
- MSM-18/4 モジュールを別の MSM-18/4 モジュールに交換することが必要な場合(11-6 ページ)
- SME クラスタが正常に作成されていない場合(11-7 ページ)
- SME インターフェイスの作成エラー(11-7 ページ)
- クラスタで SME インターフェイスが起動しません(11-7 ページ)
- パスを選択すると、メッセージ「no paths found」メッセージが表示されます(11-7 ページ)
- 新しく追加したテープ ドライブがクラスタ内に表示されません(11-8 ページ)
- カスタマー サポート担当者または Cisco TAC への問い合わせが必要な場合(11-8 ページ)
- 起動コンフィギュレーション内で SME により設定されている Cisco MDS スイッチのブート時に syslog メッセージが表示されます(11-8 ページ)
- ボリューム グループ ファイルをインポートすると「wrap key object not found」メッセージが出されます(11-8 ページ)
- アカウンティング ログ ファイルに、キーのレプリケーションが失敗したことが示されます(11-8 ページ)
- スマート カードまたはカードリーダーに関する問題(11-8 ページ)

## DNS がクラスタ内のすべてのスイッチ上で設定されているのではない場合

DNS がクラスタ内のすべてのスイッチ上で設定されているのではない場合には、IP アドレスまたは名前の選択に `sme.useIP` を使用できます。

`sme.useIP` を `smeserver.properties` で使用して、スイッチ名の代わりに IP アドレスを使用可能にできます。デフォルトでは、`sme.useIP` は `[false]` に設定されており、DNS 名が使用されます。DNS が設定されていないと、DCNM-SAN はスイッチ名を解決できません。

`sme.useIP` を `[true]` に設定すると、DCNM-SAN は IP アドレスを使用して、SSH でクラスタ内のスイッチと通信します。すべてのスイッチが、IP アドレスでクラスタに追加されます。ローカル スイッチを追加すると、ネーム サーバがスイッチ上で設定されていればスイッチ名が使用され、そうでない場合は IP アドレスが使用されます。

`sme.useIP` が `[false]` である場合、DCNM-SAN はスイッチ名を使用してインターフェイスを選択します。クラスタに追加したすべてのスイッチは、名前で識別されます。このタイプの設定には、ネーム サーバが必要です。それがない場合には、スイッチは他のスイッチと通信してクラスタを形成することができず、DCNM-SAN はスイッチ名を解決できません。

## MSM-18/4 モジュールを別の MSM-18/4 モジュールに交換することが必要な場合

既存の MDS 9000 ファミリー プラットフォームでは、モジュールを別のモジュールに交換しても設定の変更はありません。SME では、セキュリティ上の理由により、MSM-18/4 モジュールがクラスタの一部として設定されていると、別の MSM-18/4 モジュールと交換することはできません。設定されていない場合には、SME インターフェイスは非アクティブ状態で起動します。正しい手順として、SME インターフェイスをクラスタから削除し、それからインターフェイスをクラスタに再び追加します。

**SME クラスタが正常に作成されていない場合**

SME クラスタを正常に作成できない場合には、次の3つの主な理由があります。

- SSHは、SME クラスタの一部であるすべてのスイッチ上でイネーブルでなければなりません。



(注) DCNM-SAN Web クライアントを使用する SME クラスタ設定では、SSH/dsa または SSH/rsa のみがサポートされます。DCNM-SAN Web クライアント 3.2.2 (SME 機能があるバージョン) による SME クラスタ設定では、SSH/rsa1 はサポートされません。これは将来のリリースでサポートされる可能性があります (サポートされない場合もあります)。

- SME スイッチが (ホスト名または FQDN の代わりに) その IP アドレスで管理されている場合には、「sme.useIP=true」エントリを smeserver.properties ファイル内に設定する必要があります。smeserver.properties ファイルを変更した後に、必ず DCNM-SAN を再起動してください。
- DNS サーバを設定する必要があります。
- また、不適切に設定された (Cisco DCNM-SAN で稼働する) 個人用ファイアウォール ソフトウェアが原因で、作成された SME クラスタが「保留中」状態になってしまう場合もあります。DCNM-SAN、DCNM-SAN Web クライアント、スイッチの間での必要なトラフィックを許可する適正なファイアウォール規則を作成してください。

**SME インターフェイスの作成エラー**

SME インターフェイスの作成中にエラーが発生した場合は、次の点を確認します。

- サービス モジュールのステータスがオンラインであることを確認します。
- ストレージ サービス インターフェイス (SSI) のブート変数がサービス モジュールに対して設定されていないことを確認します。SSI ブート変数がサービス モジュール用に設定されている場合、SME インターフェイスの作成は失敗します。

**クラスタで SME インターフェイスが起動しません**

SME インターフェイスが起動しない場合は、次の事柄が原因である可能性があります。

- SME ライセンスがインストールされていないか、またはライセンスの有効期限が切れています。
- MSM-18/4 モジュールが、SME インターフェイスを設定した後に交換されています。
- **copy running-config startup-config** コマンドが、クラスタで SME インターフェイスを追加または削除した後、あるいはスイッチをリブートする前に入力されていません。

2 番目と 3 番目のシナリオでは、まずインターフェイスをクラスタから削除して再び追加し、次に **copy running-config startup-config** コマンドを入力する必要があります。

**パスを選択すると、メッセージ「no paths found」メッセージが表示されます**

テープライブラリのコントローラやロボットは、[Select Tape Drives] ウィザードでターゲットとして表示される場合があります。コントローラまたはロボットをターゲットとして選択すると、「no paths found」というメッセージが表示されます。選択したターゲットがコントローラまたはロボットでないかどうかを確認する必要があります。

「no paths found」メッセージが表示される場合は、**show tech** コマンドと **show tech-support sme** コマンドを入力します。

### 新しく追加したテープドライブがクラスタ内に表示されません

SME がすでに使用可能なテープドライブを検出した後に、新しいテープドライブを LUN としてテープライブラリに追加した場合は、新しい LUN を検出するためにホストからの再スキャンが必要です。

### カスタマーサポート担当者または Cisco TAC への問い合わせが必要な場合

追加の支援を受けるために、カスタマーサポート担当者または Cisco TAC への問い合わせが必要になることがあります。これを行う前に、**show tech details** コマンドと **show tech sme** コマンドを入力して、すべてのログを **C:\Program Files\Cisco Systems\MDS 9000\logs** ディレクトリから収集しておき、それからサポート組織に問い合わせます。

### 起動コンフィギュレーション内で SME により設定されている Cisco MDS スイッチのブート時に syslog メッセージが表示されます

起動コンフィギュレーションファイルにクラスタ設定を保存している Cisco MDS スイッチがリブートすると、次の syslog メッセージが表示される場合があります。

```
<timestamp> <switch name> %CLUSTER-2-CLUSTER_DB_SYNC_FAIL: Cluster <cluster-id>
application 3 dataset 1 database synchronization failed, reason="Invalid cluster API
registration"
```

このエラーメッセージは予期されており、無視しても構いません。

ボリュームグループファイルをインポートすると「**wrap key object not found**」メッセージが出されます。テープボリュームグループが作成され、ボリュームグループがファイルにエクスポートされました。テープボリュームグループは削除され、新しいテープボリュームグループが作成されました。同じボリュームグループのインポート時に、インポート操作が失敗し、エラーメッセージ「**wrap key object not found**」が表示されます。

このエラーは、インポート操作の実行先になる現在のボリュームグループと同じインデックス（ただしバージョンは異なる）を持つ Key Management Center 内に、別のアクティブなボリュームグループキーがあるために発生します。

### アカウントングログファイルに、キーのレプリケーションが失敗したことが示されます

クラスタのキーのレプリケーションは、トランザクションコンテキストが無効であるかまたは期限切れである場合には失敗します。キーエントリは、**Sme\_repl\_error\_key** テーブルに移されます。このレコードを **Sme\_repl\_error\_key** テーブルから手動で削除して **Sme\_repl\_pending\_key** テーブルに移し、レプリケーションプロセスを再試行する必要があります。

### スマートカードまたはカードリーダーに関する問題

スマートカードの動作に問題がある場合、次のようにすると正常であるかどうかを確認できます。

- リブート後に、サポートされている 1 インスタンスのブラウザのみを使用します。
- アプレット/ウィザードがロードを開始するときに、リーダーにスマートカードがないことを確認します。
- カードを挿入したもののウィザードで変更が認識されない場合は、カードを取り出して、再び挿入します。場合によってはこれで正しい認識がトリガーされることがあります。
- 最後の手段として、Java classloader キャッシュのクリアが効果的である場合があります。classloader キャッシュをクリアするには、Java コンソールを開いて **x** を押します。ブラウザを再起動して、再試行してください。



## SME CLI コマンド

この付録のコマンドは、マルチレイヤディレクタとファブリック スイッチの Cisco MDS 9000 ファミリーに適用されます。各コマンドの適切なモードを決定するには、「コマンドモード」セクションを参照してください。

### SME コマンド

この付録では、SME 機能に固有のコマンドをアルファベット順に記載します。

#### auto-volgrp

自動ボリュームグループ化を設定するには、**auto-volgrp** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**auto-volgrp**

**no auto-volgrp**

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### デフォルト

ディセーブル

#### コマンドモード

SME クラスタ コンフィギュレーション サブモード。

#### コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## clear fc-redirect config

**使用上のガイドライン** テープ バーコードが既存のボリューム グループに属していないことを SME が認識すると、自動ボリューム グループ化がイネーブルになるときに、新しいボリューム グループが作成されます。

**例** 次に、自動ボリューム グループ化をイネーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

次に、自動ボリューム グループ化をディセーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

**関連コマンド**

コマンド	説明
show sme cluster	SME クラスタ情報を表示します。

## clear fc-redirect config

スイッチの FC-Redirect 設定を削除するには、**clear fc-redirect config** コマンドを使用します。

**clear fc-redirect config {vt vt-pwwn local-switch-only}**

**構文の説明**

<b>vt vt-pwwn</b>	削除する設定の仮想ターゲット (VT) を指定します。フォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
<b>local-switch-only</b>	ローカル スイッチでのみ設定を削除します。

**デフォルト**

なし。

**コマンドモード**

EXEC モード

**コマンド履歴**

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

**使用上のガイドライン**

このコマンドは、SME や DMM などのアプリケーションによって作成された FC-Redirect の設定 (アクティブな設定を含む) を削除します。このコマンドは、ホスト サーバがストレージアレイと通信できるようにします。個々の Intelligent Service Application (ISA) を直接バイパスするため、データ破損が発生します。

アプリケーション(SME や DMM)から削除できない残った設定をクリアする最後のオプションとしてのみ、このコマンドを使用してください。

このコマンドはスイッチの運用を廃止するときに使用してください。

**例** 次に、スイッチで FC-Redirect 設定をクリアする例を示します。

```
switch# clear fc-redirect config vt 2f:ea:00:05:30:00:71:64
Deleting a configuration MAY result in DATA CORRUPTION.
Do you want to continue? (y/n) [n] y
```

#### 関連コマンド

コマンド	説明
<code>show fc-redirect active configs</code>	スイッチのすべてのアクティブ設定を表示します。

## cluster

クラスタ機能を設定するには、**cluster** コマンドを使用します。

### cluster enable

#### 構文の説明

<b>enable</b>	クラスタをイネーブルまたはディセーブルにします。
---------------	--------------------------

#### デフォルト

なし。

#### コマンドモード

コンフィギュレーション モード

#### コマンド履歴

リリース	変更内容
3.2(2)	このコマンドが導入されました。
NX-OS 4.1(1b)	このコマンドは廃止されました。

#### 使用上のガイドライン

Cisco NX-OS 4.x のリリース以降、**cluster** コマンドは **feature** コマンドで置き換えられます。

**例** 次に、SME クラスタリングをイネーブルにする例を示します。

```
switch# config terminal
switch(config)# cluster enable
switch(config)#
```

関連コマンド	コマンド	説明
	<code>show sme cluster</code>	SME クラスタに関する情報を表示します。

## debug sme

SME 機能のデバッグをイネーブルにするには、`debug sme` コマンドを使用します。debug コマンドをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
debug sme {all | demux vsan vsan id | deque | error | event vsan vsan id | ha vsan vsan id | trace vsan vsan id | trace-detail vsan vsan id | warning vsan vsan id | wwn-janitor {disable | enable | set-timer-value}}
```

```
no debug sme {all | demux vsan vsan id | deque | error | event vsan vsan id | ha vsan vsan id | trace vsan vsan id | trace-detail vsan vsan id | warning vsan vsan id | wwn-janitor {disable | enable | set-timer-value}}
```

構文の説明		
<code>all</code>		すべての SME 機能のデバッグをイネーブルにします。
<code>demux</code>		SME メッセージ分離のデバッグをイネーブルにします。
<code>vsan vsan id</code>		デバッグを指定した VSAN ID に制限します。指定できる範囲は 1 ~ 4094 です。
<code>deque</code>		SME メッセージデキューのデバッグをイネーブルにします。
<code>error</code>		SME エラーのデバッグをイネーブルにします。
<code>event</code>		SME の有限状態マシン (FSM) マシンとイベントのデバッグをイネーブルにします。
<code>ha</code>		SME 高可用性 (HA) のデバッグをイネーブルにします。
<code>trace</code>		SME トレースのデバッグをイネーブルにします。
<code>trace-detail</code>		SME trace-detail のデバッグをイネーブルにします。
<code>warning</code>		SME 警告のデバッグをイネーブルにします。
<code>wwn-janitor</code>		SME WWN ジャニタ 関連情報を表示します。
<code>disable</code>		SME WWN ジャニタ タスク タイマーをディセーブルにします。
<code>enable</code>		SME WWN ジャニタ タスク タイマーをイネーブルにします。
<code>set-timer-value</code>		SME WWN ジャニタ タスク タイマーの値をマイクロ秒単位で設定します。範囲は 2000 ~ 240000 です。

デフォルト	なし。
-------	-----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。



使用上のガイドライン なし。

例 次に、**debug sme all** コマンドのシステム出力例を示します。

```
switch# debug sme all
2007 Sep 23 15:44:44.490796 sme: fu_priority_select: - setting fd[5] for select
call
2007 Sep 23 15:44:44.490886 sme: fu_priority_select_select_queue: round credit(8)
2007 Sep 23 15:44:44.490918 sme: curr_q - FU_PSEL_Q_CAT_CQ, usr_q_info(2), p
riority(7), credit(4), empty
2007 Sep 23 15:44:44.490952 sme: fu_priority_select: returning FU_PSEL_Q_CAT_MTS
queue, fd(5), usr_q_info(1)
2007 Sep 23 15:44:44.491059 sme: sme_get_data_from_queue(1031): dequeued mts msg
(34916564), MTS_OPC_DEBUG_WRAP_MSG
2007 Sep 23 15:44:44.491096 sme: fu_fsm_engine: line[2253]
2007 Sep 23 15:44:44.492596 sme: fu_fsm_execute_all: match_msg_id(0), log_alread
y_open(0)
```

#### 関連コマンド

コマンド	説明
<b>no debug all</b>	すべてのデバッグをディセーブルにします。
<b>show sme</b>	SME に関するすべての情報を表示します。

## discover

ホストの検出を開始するには、**discovery** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**discover host host port target target port vsan vsan id fabric fabric name**

**no discover host host port target target port vsan vsan id fabric fabric name**

#### 構文の説明

<b>host host port</b>	ホスト ポートの WWN を指定します。フォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
<b>target target port</b>	ターゲット ポートの WWN を指定します。フォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
<b>vsan vsan id</b>	VSAN 識別子を選択します。指定できる範囲は 1 ~ 4093 です。
<b>fabric fabric name</b>	検出するファブリックを指定します。最大長は 32 文字です。

デフォルト なし。

コマンドモード SME クラスタ コンフィギュレーション サブモード。

## do

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

**使用上のガイドライン** **discover** コマンドが設定済みまたは検出済みの可能性がある既存ホストで発行された場合、SME は検出済みのすべての既存 LUN を削除し、LOGO 通知をホストに送信してから、検出を再実行します。

**例** 次に、ホストを検出し、検出するターゲット、VSAN、およびファブリックを指定する例を示します。

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# discover host 20:00:00:00:c9:49:28:47 target
21:01:00:e0:8b:29:7e:0c vsan 2345 fabric sw-xyz
```

次に、discovery 機能をディセーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# no discover
```

関連コマンド	コマンド	説明
	<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

## do

任意のコンフィギュレーションモードまたはサブモードから EXEC レベルの **show** コマンドを実行するには、**do** コマンドを使用します。

**do command**

構文の説明	command	実行する EXEC コマンドを指定します。
-------	---------	-----------------------

**デフォルト** なし。

**コマンドモード** すべてのコンフィギュレーションモード。

コマンド履歴	リリース	変更内容
	1.1(1)	このコマンドが導入されました。

## 使用上のガイドライン

スイッチを設定するときに EXEC レベルの **show** コマンドを実行するには、このコマンドを使用します。EXEC コマンドを実行すると、システムは **do** コマンドを発行したモードに戻ります。

## 例

次に、SME テープ ボリューム コンフィギュレーション サブモードでクラスタ テープの詳細に関する情報を表示する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-c1)# tape-bkgrp group1
switch(config-sme-c1-tape-bkgrp)# tape-device devicename1
switch(config-sme-c1-tape-bkgrp-tapedevice)# do show sme cluster clustername1 tape detail
Tape t1 is online
  Is a Tape Drive
  Model is HP Ultrium 2-SCSI
  Serial Number is HUM4A00184
  Is configured as tape device b1 in tape group b1
  Paths
    Host 12:01:00:e0:8b:a2:08:90 Target 52:06:0b:11:00:20:4c:4c LUN 0x0000
    Is online
```

次に、SME 暗号テープ ボリューム グループ コンフィギュレーション サブモードでインターフェイスのカウンタを表示する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-c1)# tape-bkgrp group1
switch(config-sme-c1-tape-bkgrp)# tape-volgrp t1
switch(config-sme-c1-tape-bkgrp-volgrp)# do show interface sme 3/1 description
sme3/1
  5 minutes input rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
  5 minutes output rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
  SME statistics
    input 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
      clear 0 bytes, encrypt 0 bytes, decrypt 0
      compress 0 bytes, decompress 0 bytes
    output 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
      clear 0 bytes, encrypt 0 bytes, decrypt 0
      compress 0 bytes, decompress 0 bytes
      compression ratio 0:0
    flows 0 encrypt, 0 clear
    clear luns 0, encrypted luns 0
  errors
    0 CTH, 0 authentication
    0 key generation, 0 incorrect read
    0 incompressible, 0 bad target responses
```

## fabric

クラスタにファブリックを追加するには、SME クラスタ コンフィギュレーション サブモードで **fabric** コマンドを使用します。

**fabric** *fabric name*

## 構文の説明

*fabric name* ファブリック名を指定します。最大長は 32 文字です。

## ■ fabric-membership

デフォルト なし。

コマンドモード SME クラスタ コンフィギュレーション サブモード。

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、クラスタに sw-xyz という名前のファブリックを追加する例を示します。

```
switch# config terminal
switch(config)# sme cluster c1
switch(config-sme-c1)# fabric sw-xyz
```

関連コマンド	コマンド	説明
	<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

## fabric-membership

ファブリックにノードを追加するには、**fabric-membership** コマンドを使用します。ファブリックからノードを削除するには、このコマンドの **no** 形式を使用します。

**fabric-membership** *fabric name*

**no fabric-membership** *fabric name*

構文の説明	<i>fabric name</i>	ファブリック名を指定します。最大長は 32 文字です。
-------	--------------------	-----------------------------

デフォルト なし。

コマンドモード SME クラスタ ノード コンフィギュレーション サブモード。

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

ファブリックにノードを配置するには、**fabric-membership** コマンドを使用します。

このコマンドは、**interface sme slot/port [force]** コマンドが受け付けられる前に設定する必要があります。このコマンドは、**interface sme slot/port [force]** コマンドがイネーブルの場合、削除できません。

## 例

次に、ノードが属するファブリックを指定する例を示します。

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)# fabric-membership f1
```

## 関連コマンド

コマンド	説明
<b>interface sme</b>	クラスタに SME インターフェイスを設定します。
<b>show interface sme</b>	インターフェイス情報を表示します。
<b>shutdown</b>	インターフェイスをイネーブルまたはディセーブルにします。

## fc-redirect version2 enable



(注)

SME ディスク クラスタでは、クラスタの一部であるすべてのスイッチで FC-Redirect バージョン 2 がイネーブルになっている必要があります。

FC-Redirect で version2 モードをイネーブルにするには、コンフィギュレーション モードで **fc-redirect version2 enable** コマンドを使用します。FC-Redirect で version2 モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

**fc-redirect version2 enable**

**no fc-redirect version2 enable**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

コンフィギュレーション モード

## コマンド履歴

リリース	変更内容
3.3(1c)	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドは、FC-Redirect の拡張性を向上させるために使用します。

ファブリックでイネーブルになった version2 モードをディセーブルにすることは推奨されません。もし version2 モードをディセーブルにする場合は、すべての FC-Redirect 設定が削除されるまで version2 モードをディセーブルにすることはできません。FC-Redirect 設定の削除は、対応するすべてのアプリケーション設定を削除することによってのみ可能です。

Cisco SAN-OS 3.2.x を実行している MDS スイッチは、version2 モードをイネーブルにした後はファブリックに追加できません。スイッチが追加されると、ファブリック上の以降の FC-Redirect 設定変更はすべて失敗します。これにより、SME および DMM などのアプリケーションのトラフィックが中断される可能性があります。

**show fc-redirect configs** コマンドを使用して、FC-Redirect 設定を作成するアプリケーションのリストを確認します。

version2 モードがファブリックでイネーブルになっており、スイッチを異なるファブリックに移動する場合、スイッチを異なるファブリックに移動する前に **clear fc-redirect decommission-switch** コマンドを使用します。それ以外の場合、新しいファブリック内のすべてのスイッチが自動的に version2 モードに変換されます。



(注)

ファブリック内のすべてのスイッチが SAN-OS リリース 3.3.x または NX-OS 4.x を実行している必要があります。ファブリックの変更またはアップグレードが進行中でないことを確認します。**show fc-redirect peer-switches** コマンド(アップ状態)を使用して、ファブリックのすべてのスイッチを確認します。

## 例

次に、FC-Redirect で version2 モードをイネーブルにする例を示します。

```
switch# fc-redirect version2 enable
```

Please make sure to read and understand the following implications before proceeding further:

- 1) This is a Fabric wide configuration. All the switches in the fabric will be configured in Version2 mode. Any new switches added to the fabric will automatically be configured in version2 mode.
- 2) SanOS 3.2.x switches CANNOT be added to the Fabric after Version2 mode is enabled. If any 3.2.x switch is added when Version2 mode is enabled, all further FC-Redirect Configuration changes will Fail across the fabric. This could lead to traffic disruption for applications like SME.
- 3) If enabled, Version2 mode CANNOT be disabled till all FC-Redirect configurations are deleted. FC-Redirect configurations can be deleted ONLY after all the relevant application configurations are deleted. Please use the command 'show fc-redirect configs' to see the list of applications that created FC-Redirect configurations.
- 4) 'write erase' will NOT disable this command. After 'write erase' on ANY switch in the fabric, the user needs to do:
 

```
'clear fc-redirect decommission-switch'
```

 on that that switch. Without that, if the user moves the switch to a different fabric it will try to convert all the switches in the fabric to Version2 mode automatically. This might lead to Error conditions and hence Traffic disruption.

```

Do you want to continue? (Yes/No) [No]Yes
Before proceeding further, please check the following:
  1) All the switches in the fabric are seen in the output of
      'show fc-redirect peer-switches' command and are in 'UP' state.

  2) All switches in the fabric are running SanOS version 3.3.x or
      higher.

  3) Please make sure the Fabric is stable ie.,
      No fabric changes/upgrades in progress

Do you want to continue? (Yes/No) [No] Yes

```

### 関連コマンド

コマンド	説明
<b>no fc-redirect version2 enable mode</b>	FC-Redirect で version2 モードをディセーブルにします。

## feature

SME 機能をイネーブルおよびディセーブルにするには、**feature** コマンドを使用します。機能を削除するには、このコマンドの **no** 形式を使用します。

```
feature {cluster | sme}
```

```
no feature {cluster | sme}
```

### 構文の説明

<b>cluster</b>	クラスタリング機能をイネーブルまたはディセーブルにします。
<b>sme</b>	ストレージメディア暗号化(SME)サービスをイネーブルまたはディセーブルにします。

### デフォルト

ディセーブル

### コマンドモード

コンフィギュレーション モード

### コマンド履歴

リリース	変更内容
NX-OS 4.1(1b)	このコマンドが導入されました。

### 使用上のガイドライン

なし。

例 次に、クラスタリングをイネーブルにして SME サービスを設定する例を示します。

```
switch# config terminal
switch(config)# feature cluster
switch(config)# feature sme
switch(config)#
```

#### 関連コマンド

コマンド	説明
<code>show sme cluster</code>	SME クラスタ情報を表示します。

## interface sme

スイッチの SME インターフェイスを設定するには、**interface sme** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**interface sme slot /port**

**no interface sme slot /port**

#### 構文の説明

<i>slot</i>	MSM-18/4 モジュール スロット番号を指定します。
<i>port</i>	SME ポート番号を特定します。

#### デフォルト

ディセーブル

#### コマンドモード

コンフィギュレーション モード

#### コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

#### 使用上のガイドライン

このコマンドを使用するには、**feature cluster** コマンドを使用してクラスタリングをイネーブルにし、**feature sme** コマンドを使用して SME サービスをイネーブルにする必要があります。

インターフェイスを設定したら、**no shutdown** コマンドを使用してインターフェイスをイネーブルにします。

SME インターフェイスを削除するには、クラスタからスイッチを削除する必要があります。**no sme cluster** コマンドを使用してスイッチをクラスタから削除してから、**no interface** コマンドを使用してインターフェイスを削除します。

`interface` コマンドは、(**config-if**) サブモードで使用できます。



**例** 次に、MSM-18/4 モジュール スロットとデフォルトの SME ポートで SME インターフェイスを設定およびイネーブルにする例を示します。

```
switch# config terminal
switch(config)# interface sme 3/1
switch(config-if)# no shutdown
```

**関連コマンド**

コマンド	説明
<b>show interface sme</b>	インターフェイス情報を表示します。
<b>shutdown</b>	インターフェイスをイネーブルまたはディセーブルにします。

## interface sme (SME クラスタ ノード コンフィギュレーション サブモード)

ローカルまたはリモート スイッチからクラスタに SME インターフェイスを追加するには、**interface sme** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**interface sme** (*slot/port*) [**force**]

**no interface sme** (*slot/port*) [**force**]

**構文の説明**

<i>slot</i>	MSM-18/4 モジュール スロットを指定します。
<i>port</i>	SME ポートを指定します。
<b>force</b>	(任意) インターフェイスで以前のインターフェイス コンテキストを強制クリアします。

**デフォルト**

ディセーブル

**コマンドモード**

SME クラスタ ノード コンフィギュレーション サブモード。

**コマンド履歴**

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

**使用上のガイドライン**

このコマンドを実行する前に、**fabric-membership** コマンドを使用してノードを設定する必要があります。

このコマンドを使用するには、**feature cluster** コマンドを使用してクラスタリングをイネーブルにし、**feature sme** コマンドを使用して SME サービスをイネーブルにする必要があります。

SME インターフェイスを削除するには、先にクラスタからスイッチを削除します。**no sme cluster** コマンドを使用してスイッチをクラスタから削除してから、**no interface** コマンドを使用してインターフェイスを削除します。

## 例

次に、ノードが属するファブリックを指定してから、**force** オプションを使用してローカル スイッチから SME インターフェイス (4/1) を追加する例を示します。

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 force
```

次に、ノードが属するファブリックを指定してから、**force** オプションを使用してリモート スイッチから SME インターフェイス (4/1) を追加する例を示します。

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 fabric sw-xyz
```

## 関連コマンド

コマンド	説明
<b>fabric-membership</b>	ファブリックにノードを追加します。
<b>show interface</b>	SME インターフェイスの詳細を表示します。

## key-ontape

テープ モードでキーを設定し、バックアップ テープに暗号化されたセキュリティ キーを保存するには、**key-ontape** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**key-ontape**

**no key-ontape**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

ディセーブル

## コマンドモード

SME クラスタ コンフィギュレーション サブモード。

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドでは、暗号化されたセキュリティ キーをバックアップ テープに保存できます。



(注)

この機能は、固有キーについてのみサポートされています。

このコマンドを使用する前に、**auto-volgrp** コマンドを使用して自動ボリューム グループ化をディセーブルにする必要があります。

## 例

次に、**key-ontape** 機能をイネーブルにする例を示します。

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# key-ontape
```

次に、**key-ontape** 機能をディセーブルにする例を示します。

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme0-cl)# no key-ontape
```

## 関連コマンド

コマンド	説明
<b>no auto-volgrp</b>	自動ボリューム グループ化をディセーブルにします。
<b>no shared-key</b>	固有キー モードを指定します。
<b>show sme cluster key</b>	クラスタ キー データベースに関する情報を表示します。
<b>show sme cluster &lt;clustername&gt; tape summary</b>	テープに関する情報を表示します。

## link-state-trap

インターフェイス上での Simple Network Management Protocol (SNMP) リンク ステート トラップをイネーブルにするには、**link-state-trap** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**link-state-trap**

**no link-state-trap**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

インターフェイス コンフィギュレーション サブモード。

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、SME インターフェイスで link-state-trap をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# link-state-trap
```

次に、SME インターフェイスで link-state-trap をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# no link-state-trap
```

## node

SME スイッチを設定するには、**node** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
node {local | {A.B.C.D | X:X::X /n| DNS name}}
```

```
no node {local | {A.B.C.D | X:X::X /n| DNS name}}
```

構文の説明	local	ローカル スイッチを設定します。
	A.B.C.D	IPv4 形式でリモート スイッチの IP アドレスを指定します。
	X:X::X/n	IPv6 形式でリモート スイッチの IP アドレスを指定します。
	DNS name	リモート データベースの名前を指定します。

デフォルト なし。

コマンドモード SME クラスタ コンフィギュレーション サブモード。

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

## 例

次に、ローカル スイッチから SME インターフェイスを追加する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)#
```

次に、リモート スイッチから SME インターフェイスを追加する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)#
```

## 関連コマンド

コマンド	説明
<code>show sme cluster node</code>	ローカルまたはリモート スイッチに関する SME ノード情報を表示します。

## odrt.bin

SME によって暗号化されたテープのオフライン データ リカバリを実行するには、Linux ベースのシステムで **odrt.bin** コマンドを使用します。このコマンドでは、MSM-18/4 モジュールまたは Cisco MDS 9222i ファブリック スイッチを使用できないときにデータを回復できます。

```
odrt.bin [--help][--version]{-h|-l|-r|-w}{if=input_device_or_file|of=output_device_or_file|
kf=key_export_file|verbose=level}
```

## 構文の説明

<code>--help</code>	(任意) ツールに関する情報を表示します。
<code>--version</code>	(任意) ツールのバージョンを表示します。
<code>-h</code>	テープのテープ ヘッダー情報を読み取り、出力します。
<code>-l</code>	すべての SCSI デバイスを一覧表示します。
<code>-r</code>	テープ デバイスを読み取り、中間ファイルにデータを書き込みます。
<code>-w</code>	ディスク上の中間ファイルを読み取り、テープにデータを書き込みます。
<code>if</code>	入力デバイスまたはファイルを指定します。
<code>of</code>	出力デバイスまたはファイルを指定します。
<code>kf</code>	キー エクスポート ファイル名を指定します。
<code>verbose</code>	レベルを指定します。

## デフォルト

なし。

## コマンドモード

なし。このコマンドは、Linux シェルから実行します。

## コマンド履歴

リリース	変更内容
3.3(1c)	このコマンドが導入されました。

## 使用上のガイドライン

**odrt.bin** コマンドは、次の手順で実行します。

- テープからディスク: このモードでは、**odrt.bin** コマンドはテープから暗号化データを読み取って、それをディスク上の中間ファイルに保存します。このモードは、**-r** フラグを使用して呼び出されます。入力パラメータはテープ デバイス名であり、ディスク上のファイル名が出力パラメータです。
- ディスクからテープ: このモードでは、**odrt.bin** コマンドはディスク上の中間ファイルを読み取り、データを復号化および(必要な場合は)圧縮解除して(該当する場合)、クリアテキストデータとしてテープに書き込みます。復号キーは、Cisco Key Management Center (KMC) からエクスポートされるボリューム グループ ファイルから取得します。このモードは、**-w** フラグを使用して呼び出されます。入力パラメータはディスク上のファイル名であり、テープ デバイス名が出力パラメータです。ボリューム グループ ファイル名(キー エクスポート ファイル)も、パラメータとして受け付けられます。キー エクスポート パスワードをコマンド プロンプトで入力する必要があります。



(注)

ボリューム グループをエクスポートする方法については、[第 7 章「SME キー管理の設定」](#)を参照してください。

## 例

次のコマンドは、テープの Cisco テープ ヘッダー情報を読み取り、出力します。

```
odrt -h if=/dev/sg0
```

次に、テープ上のデータをディスク上の中間ファイルに読み取る例を示します。

```
odrt -r if=/dev/sg0 of=diskfile
```

次のコマンドは、中間ファイル内で暗号化/圧縮されたデータを読み取り、復号化/圧縮解除されたデータをテープに書き戻します。

```
odrt -w if=diskfile of=/dev/sg0 kf=c1_tb1_Default.dat
```

**odrt.bin** コマンドの出力例を次に示します。

```
[root@ips-host06 odrt]# ./odrt.bin -w if=c of=/dev/sg2 kf=sme_L700_IBMLT03_Default.dat
verbose=3
Log file: odrt30072
Please enter key export password:
Elapsed 0:3:39.28, Read 453.07 MB, 2.07 MB/s, Write 2148.27 MB, 9.80 MB/s
Done
```

## rule

テープ ボリューム グループの正規表現を指定するには、**rule** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
rule {range range | regexp regular expression}
```

```
no rule {range range | regexp regular expression}
```

構文の説明	<b>range</b> <i>range</i>	暗号テープ ボリューム バーコードの範囲を指定します。最大長は 32 文字です。
	<b>regexp</b> <i>regular expression</i>	ボリューム グループの正規表現を指定します。最大長は 32 文字です。
デフォルト	なし。	
コマンドモード	SME 暗号テープ ボリューム グループ コンフィギュレーション サブモード。	
コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。
使用上のガイドライン	なし。	
例	次に、ボリューム グループの正規表現を指定する例を示します。 <pre>switch# config t switch(config)# sme cluster c1 switch(config-sme-cl)# tape-bkgrp tbgr1 switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1 switch(config-sme-cl-tape-bkgrp-volgrp)#rule regexp r1</pre>	
関連コマンド	コマンド	説明
	<b>show sme cluster</b>	SME クラスタに関する情報を表示します。
	<b>tape-bkgrp</b> <i>groupname</i>	暗号バックアップ グループを設定します。
	<b>tape-volgrp</b> <i>volume groupname</i>	暗号バックアップ ボリューム グループを設定します。

## scaling batch enable



(注) SME ディスク クラスタでは、バッチ モードが自動的にイネーブルになります。

SME コンフィギュレーションで拡張性をイネーブルにするには、**scaling batch enable** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**scaling batch enable**

**no scaling batch enable**

## security-mode

**構文の説明** このコマンドには引数またはキーワードはありません。

**デフォルト** なし。

**コマンドモード** SME クラスタ コンフィギュレーション サブモード。

リリース	変更内容
4.1(3)	このコマンドが導入されました。

**使用上のガイドライン** なし。

**例** 次に、SME 拡張性をイネーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# scaling batch enable
switch(config-sme-cl)#
```

## security-mode

SME セキュリティ設定を設定するには、**security-mode** コマンドを使用します。セキュリティ設定を削除するには、このコマンドの **no** 形式を使用します。

**security-mode** {basic | standard | advanced {schema threshold *threshold* total *total* }}

**no security-mode** {basic | standard | advanced {schema threshold *threshold* total *total* }}

<b>basic</b>	SME セキュリティ レベルを basic に設定します。
<b>standard</b>	SME セキュリティ レベルを standard に設定します。
<b>advanced</b>	SME セキュリティ レベルを advanced に設定します。
<b>schema</b>	リカバリ スキーマを設定します。
<b>threshold</b> <i>threshold</i>	リカバリ スキーマのしきい値を設定します。制限は 2 ~ 3 です。
<b>total</b> <i>total</i>	リカバリ スキーマの合計を設定します。制限は 5 ~ 5 です。

**デフォルト** なし。

**コマンドモード** SME クラスタ コンフィギュレーション サブモード。



コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、セキュリティ モードを basic に設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# security-mode basic
```

次に、セキュリティ モードを advanced に設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# security-mode advanced schema threshold 3 total 5
```

関連コマンド	コマンド	説明
	<b>show sme cluster</b>	セキュリティ設定に関する情報を表示します。

## setup

基本セットアップ機能を実行するには、**setup** コマンドを使用します。

```
setup ficon | sme
```

構文の説明	ficon	説明
	<b>ficon</b>	基本 FICON セットアップ コマンド ファシリティを実行します。
	<b>sme</b>	基本 SME セットアップ コマンド ファシリティを実行します。

デフォルト なし。

コマンドモード EXEC

コマンド履歴	リリース	変更内容
	3.3(1c)	このコマンドが導入されました。

使用上のガイドライン SME の sme-admin および sme-recovery ロールを作成するには **setup sme** コマンドを使用します。

例 次に、sme-admin および sme-recovery ロールを作成する例を示します。

```
switch(config)# setup sme
Set up four roles necessary for SME, sme-admin, sme-stg-admin, sme-kmc-admin and
sme-recovery? (yes/no) [no] yes
If CFS is enabled, please commit the roles so that they can be available.
SME setup done.
```

#### 関連コマンド

コマンド	説明
<b>show role</b>	さまざまな SME ロール コンフィギュレーションに関する情報を表示します。

## shared-keymode

共有キー モードを設定するには、**shared-keymode** コマンドを使用します。固有キー モードを指定するには、このコマンドの **no** 形式を使用します。

**shared-keymode**

**no shared-keymode**

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### デフォルト

なし。

#### コマンドモード

SME クラスタ コンフィギュレーション サブモード。

#### コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

#### 使用上のガイドライン

**shared-keymode** コマンドは、バックアップ テープのグループに使用される単一キーを生成します。

**no shared-keymode** コマンドは、各テープ カートリッジに固有または特定のキーを生成します。



(注)

共有固有キー モードは、key-ontape 機能をイネーブルにする場合に指定する必要があります。

例 次に、共有キー モードを指定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# shared-keymode
```

次に、共有固有キー モードを指定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no shared-keymode
```

#### 関連コマンド

コマンド	説明
<code>show sme cluster</code>	SME クラスタ情報を表示します。

## show debug

スイッチに設定されているすべての SME 関連デバッグ コマンドを表示するには、`show debug` コマンドを使用します。

```
show debug {cluster {bypass | sap sap bypass} | sme bypass}
```

#### 構文の説明

クラスタ	すべてのデバッグ フラグを表示します。
<code>bypass</code>	バイパス フラグを表示します。
<code>sap sap</code>	SAP のすべてのデバッグ フラグを表示します。1 ~ 65535 の範囲で SAP を指定します。
<code>sme</code>	SME のすべてのデバッグ フラグを表示します。

#### デフォルト

なし。

#### コマンドモード

EXEC モード

#### コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

#### 使用上のガイドライン

なし。

## ■ show fc-redirect active-configs

例 次に、スイッチに設定されているすべての **debug** コマンドを表示する例を示します。

```
switch# show debug
ILC helper:
  ILC_HELPER errors debugging is on
  ILC_HELPER info debugging is on
```

## 関連コマンド

コマンド	説明
debug sme	SME 機能をデバッグします。

## show fc-redirect active-configs

スイッチのすべてのアクティブ設定を表示するには、**show fc-redirect active-configs** コマンドを使用します。

### show fc-redirect active-configs

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

EXEC モード

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドは、次の手順中にスイッチで実行しているアクティブ設定があるかどうかを確認するために使用されます。

- Cisco SAN-OS 3.2(1) イメージ(FC-Redirect をサポートしている)から FC-Redirect がサポートされていない古いイメージにダウングレードする。
- ローカル スイッチの運用を廃止する。



(注)

アクティブ設定とは、現在のスイッチで実行中のアプリケーションまたはリモート スイッチ (ローカル スイッチに接続されたターゲットとホストを除く) で作成されたアプリケーションによって作成された設定を指します。

## 例

次に、スイッチで実行中のアクティブ設定を表示する例を示します。

```
switch# show fc-redirect active-configs
Config#1
=====
App1 UUID = 0x00D8 (ISAPI CFGD Service)
SSM Slot = 2
SSM Switch WWN = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN = 2f:ea:00:05:30:00:71:64
Tgt PWWN = 21:00:00:20:37:38:63:9e (LOCAL)
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6
Config#2
=====
App1 UUID = 0x00D8 (ISAPI CFGD Service)
SSM Slot = 2
SSM Switch WWN = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN = 2f:ea:00:05:30:00:71:65
Tgt PWWN = 21:00:00:20:37:18:67:2c
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6

Config#3
=====
App1 UUID = 0x00D8 (ISAPI CFGD Service)
SSM Slot = 2
SSM Switch WWN = 20:00:00:0d:EC:20:13:00 (REMOTE)
Vt PWWN = 2f:ea:00:05:30:00:71:66
Tgt PWWN = 21:00:00:20:37:18:64:92
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6
```

## 関連コマンド

コマンド	説明
<code>clear fc-redirect vt</code>	ローカル スイッチ上のアクティブ設定をクリアします。

## show fc-redirect configs

スイッチのすべての現在のコンフィギュレーション モードを表示するには、`show fc-redirect configs` コマンドを使用します。

### show fc-redirect configs

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

EXEC モード

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## ■ show fc-redirect peer-switches

使用上のガイドライン なし。

例 次に、スイッチの現在のコンフィギュレーション モードを表示する例を示します。

```
switch# show fc-redirect configs
Configuration Mode    = MODE_V1
Config#1
=====
Appl UUID             = 0x00D8 (ISAPI CFGD Service)
SSM Slot              = 2
SSM Switch WWN       = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN              = 2f:ea:00:05:30:00:71:61
Tgt PWWN             = 21:00:00:20:37:38:89:86
Host 1: Host PWWN    = 21:00:00:e0:8b:0d:12:c6
                   VI PWWN = 2f:ec:00:05:30:00:71:61

Config#2
=====
Appl UUID             = 0x00D8 (ISAPI CFGD Service)
SSM Slot              = 2
SSM Switch WWN       = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN              = 2f:ea:00:05:30:00:71:62
Tgt PWWN             = 21:00:00:20:37:38:a9:0a
Host 1: Host PWWN    = 21:00:00:e0:8b:0d:12:c7
                   VI PWWN = 2f:ec:00:05:30:00:71:62
```

## 関連コマンド

コマンド	説明
<b>show fc-redirect active-configs</b>	スイッチのすべてのアクティブ設定を表示します。

## show fc-redirect peer-switches

FC-Redirect を実行しているファブリックのすべてのピア スイッチを表示するには、**show fc-redirect peer-switches** コマンドを使用します。

### show fc-redirect peer-switches

## 構文の説明

このコマンドには、キーワードや引数はありません。

## デフォルト

なし。

## コマンドモード

EXEC モード

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドは、ファブリックの状態の確認やトラブルシューティングに使用されます。



(注)

スイッチ WWN のリストでスイッチの IP アドレスを見つけるには、**show cfs peers** コマンドを使用します。

## 例

次に、FC-Redirect を実行しているファブリックのピア スイッチを表示する例を示します。

```
switch# show fc-redirect peer-switches
-----
num          Switch WWN          State
-----
1            20:00:00:05:30:00:90:9e  UP
2            21:00:00:05:30:00:90:9f  DOWN
3            22:00:00:05:30:00:90:91  SYNCING
4            23:00:00:05:30:00:90:92  ERROR
```

この表は、FC-Redirect ピア スイッチの概要を示しています。

フィールド	説明
Up	ピア スイッチはローカル スイッチと完全に同期されています。
Down	ピア スイッチとの通信に障害があります。
Syncing	ローカル スイッチは、ピア スイッチと設定を同期しています。
Error	ピア スイッチとの接続は使用できません。

## 関連コマンド

コマンド	説明
<b>clear fc-redirect vt</b>	ローカル スイッチ上のアクティブ設定をクリアします。

## show interface sme

SME インターフェイスに関する情報を表示するには、**show interface sme** コマンドを使用します。

```
show interface sme slot/port {brief | counters brief | description}
```

## 構文の説明

<i>slot</i>	MSM-18/4 モジュール スロット番号を指定します。
<i>port</i>	SME ポート番号を特定します。
<b>brief</b>	SME インターフェイスについての簡単な情報を表示します。
<b>counters</b>	インターフェイス カウンタを表示します。
<b>brief</b>	簡単なカウンタ情報を表示します。
<b>description</b>	インターフェイスの説明を表示します。

## デフォルト

なし。

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、SME インターフェイスの簡単な説明を表示する例を示します。

```
switch# show interface sme 3/1 brief
```

```
-----
Interface          Status      Cluster
-----
sme3/1             up         c2
```

次に、インターフェイスのカウンタを表示する例を示します。

```
switch# show interface sme 3/1 description
```

```
sme3/1
 5 minutes input rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
 5 minutes output rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
SME statistics
 input 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
  clear 0 bytes, encrypt 0 bytes, decrypt 0
   compress 0 bytes, decompress 0 bytes
 output 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
  clear 0 bytes, encrypt 0 bytes, decrypt 0
   compress 0 bytes, decompress 0 bytes
   compression ratio 0:0
 flows 0 encrypt, 0 clear
 clear luns 0, encrypted luns 0
 errors
   0 CTH, 0 authentication
   0 key generation, 0 incorrect read
   0 incompressible, 0 bad target responses
```

関連コマンド	コマンド	説明
	<b>interface sme</b>	スイッチ上で SME インターフェイスを設定します。

## show role

さまざまな SME ロール コンフィギュレーションについての説明を表示するには、**show role** コマンドを使用します。

```
show role
```



**構文の説明** このコマンドには引数またはキーワードはありません。

**デフォルト** なし。

**コマンドモード** EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1c)	このコマンドが導入されました。
	NX-OS 4.1(1b)	出力例が変更されました。

**使用上のガイドライン** **setup sme** コマンドを実行して SME 管理者および SME リカバリ役割を設定してから、**show role** コマンドを使用してロールの詳細を表示します。

**例** 次に、SME ロール コンフィギュレーションを表示する例を示します。

```
switch(config)# setup sme
Set up four roles necessary for SME, sme-admin, sme-stg-admin, sme-kmc-admin and
sme-recovery? (yes/no) [no] yes
If CFS is enabled, please commit the roles so that they can be available.
SME setup done.
```

```
switch# show role
Role: sme-admin
Description: new role
Vsan policy: permit (default)
-----
Rule      Type      Command-type  Feature
-----
1         permit   show          sme
2         permit   config        sme
3         permit   debug         sme
```

```
Role: sme-stg-admin
Description: new role
Vsan policy: permit (default)
-----
Rule      Type      Command-type  Feature
-----
1         permit   show          sme-stg-admin
2         permit   config        sme-stg-admin
3         permit   debug         sme-stg-admin
```

```
Role: sme-kmc-admin
Description: new role
Vsan policy: permit (default)
-----
Rule      Type      Command-type  Feature
-----
1         permit   show          sme-kmc-admin
2         permit   config        sme-kmc-admin
3         permit   debug         sme-kmc-admin
```

```

Role: sme-recovery
Description: new role
Vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
1         permit   config            sme-recovery-officer

```

## 関連コマンド

コマンド	説明
<b>setup sme</b>	SME 管理者および SME リカバリ ロールを設定します。

## show sme cluster

SME クラスタに関する情報を表示するには、**show sme cluster** コマンドを使用します。

```

show sme cluster { cluster name { detail | interface { detail | node { A.B.C.D | X:X::X | DNS name
sme slot/port } | sme slot/port | summary } | it-nexus | key database { detail | guid guid name
{ detail | summary } | load-balancing | lun crypto-status | node { { A.B.C.D |
X:X::X | DNS name } | summary } | recovery officer { index | detail index | summary index } |
summary | tape { detail | summary } | tape-bkgrp tape group name volgrp volume group
name } | detail | summary }

```

## 構文の説明

<b>cluster</b> <i>cluster name</i>	SME クラスタ情報を表示します。最大長は 32 文字です。
<b>detail</b>	SME クラスタの詳細を表示します。
<b>interface</b>	SME クラスタ インターフェイスに関する情報を表示します。
<b>node</b>	SME クラスタ リモート インターフェイスに関する情報を表示します。
<i>A.B.C.D</i>	IPv4 形式でリモート スイッチの IP アドレスを指定します。
<i>X:X::X</i>	IPv6 形式でリモート スイッチの IP アドレスを指定します。
<i>DNS name</i>	リモート データベースの名前を指定します。
<b>sme</b>	SME インターフェイスを指定します。
<i>slot</i>	MSM-18/4 モジュール スロットを指定します。
<i>port</i>	SME ポートを指定します。
<b>interface summary</b>	SME クラスタ インターフェイスの概要を表示します。
<b>it-nexus</b>	SME クラスタ内のイニシエータからターゲットへの接続 (IT-Nexus) を表示します。
<b>key database</b>	SME クラスタ キー データベースを示します。
<b>detail</b>	SME クラスタ キー データベースの詳細を示します。
<b>guid</b> <i>guid name</i>	SME クラスタ キー データベースの GUID を表示します。最大 64 文字まで可能です。
<b>summary</b>	SME クラスタ キー データベースの概要を表示します。
<b>load-balancing</b>	クラスタのロード バランシングのステータスを表示します。

<b>lun</b>	クラスタの論理ユニット番号(LUN)を表示します。
<b>crypto-status</b>	LUN の暗号化状態を表示します。
<b>node summary</b>	SME クラスタ ノードの概要を表示します。
<b>recovery officer detail</b>	SME クラスタ リカバリ 責任者の詳細を表示します。
<b>recovery officer summary</b>	SME クラスタ リカバリ 責任者の概要を表示します。
<b>index</b>	リカバリ 責任者のインデックスを指定します。指定できる範囲は 1～8 です。
<b>detail index</b>	リカバリ 責任者の詳細のインデックスを指定します。指定できる範囲は 1～8 です。
<b>summary index</b>	リカバリ 責任者の概要のインデックスを指定します。指定できる範囲は 1～8 です。
<b>tape detail</b>	SME テープの詳細を表示します。
<b>tape summary</b>	テープの概要を表示します。
<b>tape-bkgrp</b> <i>tape group name</i>	暗号テープ バックアップ グループ名を表示します。最大長は 32 文字です。
<b>volgrp</b> <i>volume group name</i>	テープ ボリューム グループ名を表示します。最大長は 32 文字です。
<b>detail</b>	SME クラスタの詳細を表示します。
<b>summary</b>	SME クラスタの概要を表示します。

デフォルト なし。

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、クラスタの設定の詳細を表示する例を示します。

```
switch# show sme cluster c1
Cluster ID is 0x2b2a0005300035e1
Cluster status is online
Security mode is advanced
Total Nodes are 1
Recovery Scheme is 2 out of 5
Fabric[0] is Fabric_name-excal10
KMC server 10.21.113.117:8800 is provisioned, connection state is initializing

Master Key GUID is 10af119cfd79c17f-ee568878c049f94d, Version: 0
Shared Key Mode is Not Enabled
Auto Vol Group is Not Enabled
```

## show sme transport

```
Tape Compression is Not Enabled
Tape Key Recycle Policy is Not Enabled
Key On Tape is Not Enabled
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 24
```

次に、クラスタ インターフェイス情報を表示する例を示します。

```
switch# show sme cluster clusternam1 interface it-nexus
```

```
-----
Host WWN              VSAN   Status   Switch   Interface
Target WWN
-----
10:00:00:00:c9:4e:19:ed,
2f:ff:00:06:2b:10:c2:e2      4093   online   switch   sme4/1
```

次に、クラスタの特定のリカバリ責任者を表示する例を示します。

```
switch# show sme cluster clusternam1 recovery officer
```

```
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
Cluster is clusternam1, Master Key Version is 0
Recovery Share Version is 0, Share Index is 1
```

## 関連コマンド

コマンド	説明
<b>clear sme</b>	SME コンフィギュレーションをクリアします。
<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

## show sme transport

SME クラスタ トランスポート情報を表示するには、**show sme transport** コマンドを使用します。

**show sme transport ssl truspoint**

## 構文の説明

<b>ssl</b>	トランスポートの Secure Socket Layer(SSL)情報を表示します。
<b>trustpoint</b>	トランスポート SSL トラストポイント情報を表示します。

## デフォルト

なし。

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン なし。

例 次に、内部クラスタ エラーを表示する例を示します。

```
switch# show sme transport ssl trustpoint
SME Transport SSL trustpoint is trustpoint-label
```

関連コマンド	コマンド	説明
	<b>clear sme</b>	SME コンフィギュレーションをクリアします。
	<b>show sme cluster</b>	SME クラスタのすべての情報を表示します。

## show tech-support sme

SME テクニカル サポートの情報を表示するには、**show tech-support sme** コマンドを使用します。

**show tech-support sme compressed bootflash: | tftp:**

構文の説明	構文	説明
	<b>compressed</b>	圧縮された SME を保存します
	<b>bootflash:</b>	保存する必要があるファイル名を指定します。
	<b>tftp:</b>	保存する必要があるファイル名を指定します。

デフォルト なし。

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1c)	このコマンドが導入されました。

使用上のガイドライン なし。

## ■ shutdown(インターフェイス コンフィギュレーションサブモード)

## 例

次に、SME テクニカル サポートの情報を表示する例を示します。

```
sw-sme-n1# show tech-support sme

'show startup-config'
version 4.1(1b)
username admin password 5 $1$jC/GIid6$PuNDstXwdAnwGaxxjdx150 role network-admin
no password strength-check
feature telnet
ntp server 10.81.254.131
kernel core target 0.0.0.0
kernel core limit 1
aaa group server radius radius
snmp-server user admin network-admin auth md5 0x7eedfdadb219506ca61b0e2957cc7ef5
  priv 0x7eedfdadb219506ca61b0e2957cc7ef5 localizedkey
snmp-server host 171.71.49.157 informs version 2c public udp-port 2162
snmp-server enable traps license
snmp-server enable traps entity fru
device-alias database
  device-alias name sme-host-171-hba0 pwwn 21:01:00:e0:8b:39:d7:57
  device-alias name sme-host-171-hba1 pwwn 21:00:00:e0:8b:19:d7:57
  device-alias name sme-host-172-hba0 pwwn 21:01:00:e0:8b:39:c2:58
  device-alias name sme-host-172-hba1 pwwn 21:00:00:e0:8b:19:c2:58
  device-alias name sme-sanblaze-port0-tgt0 pwwn 2f:ff:00:06:2b:0d:39:08
  device-alias name sme-sanblaze-port0-tgt1 pwwn 2f:df:00:06:2b:0d:39:08
--More--
```

## shutdown(インターフェイス コンフィギュレーションサブモード)

SME インターフェイスをディセーブルにするには、**shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

**shutdown**

**no shutdown**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

インターフェイス コンフィギュレーション サブモード。

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

**使用上のガイドライン** SME インターフェイスのデフォルト状態は **shutdown** です。インターフェイスでトラフィックを送送できるようにするには、**no shutdown** コマンドを使用します。

インターフェイスがクラスタに追加されるまで、**show interfaces** コマンドは SME インターフェイスがダウンしていると示します。

**例** 次に、SME インターフェイスをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# no shutdown
```

次に、SME インターフェイスをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# shutdown
```

#### 関連コマンド

コマンド	説明
<b>show interface sme</b>	SME インターフェイスに関する情報を表示します。

## shutdown (SME クラスタ コンフィギュレーションサブモード)

リカバリのためにクラスタをディセーブルにするには、**shutdown** コマンドを使用します。リカバリのためにクラスタをイネーブルにするには、このコマンドの **no** 形式を使用します。

**shutdown**

**no shutdown**

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### デフォルト

なし。

#### コマンドモード

SME クラスタ コンフィギュレーション サブモード。

#### コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

リカバリのためにクラスタの動作をディセーブルにするには、**shutdown** コマンドを使用します。通常使用のためにクラスタをイネーブルにするには、**no shutdown** コマンドを使用します。

クラスタのデフォルト状態は **no shutdown** です。**shutdown** コマンドはクラスタをリカバリするために使用します。リカバリ シナリオの詳細については、[第 11 章「SME のトラブルシューティング」](#)を参照してください。

## 例

次に、リカバリが完了した後でクラスタを再起動する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no shutdown
```

次に、リカバリを開始するためにクラスタの動作をディセーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# shutdown
```

## 関連コマンド

コマンド	説明
<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

## sme

SME サービスをイネーブルまたはディセーブルにするには、**sme** コマンドを使用します。

```
sme {cluster name | transport ssl trustpoint trustpoint label}
```

## 構文の説明

<b>cluster</b>	クラスタを設定します。
<i>name</i>	クラスタ名を指定します。
<b>transport</b>	トランスポート情報を設定します。
<b>ssl</b>	トランスポート SSL 情報を設定します。
<b>trustpoint</b>	トランスポート SSL トラストポイントを設定します。
<i>trustpoint label</i>	トラストポイント ラベルを指定します。

## デフォルト

ディセーブル

## コマンドモード

コンフィギュレーション モード

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。



**使用上のガイドライン** 暗号化およびセキュリティ機能を利用するには、SME サービスをイネーブルにする必要があります。

このコマンドを使用するには、**feature cluster** コマンドを使用して SME クラスタリングをイネーブルにする必要があります。

**例** 次に、クラスタを設定する例を示します。

```
switch# config t
sw-sme-n1(config)# sme cluster clustername
sw-sme-n1(config-sme-cl)#
```

## ssl

Secure Sockets Layer (SSL) を設定するには、**ssl** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ssl kmc
```

```
no ssl kmc
```

<b>構文の説明</b>	<b>kmc</b> Key Management Center (KMC) 通信で SSL をイネーブルにします。
--------------	--

<b>デフォルト</b>	なし。
--------------	-----

<b>コマンドモード</b>	SME クラスタ コンフィギュレーション モード サブモード。
----------------	---------------------------------

<b>コマンド履歴</b>	リリース	変更内容
	3.3(1c)	このコマンドが導入されました。

<b>使用上のガイドライン</b>	なし。
-------------------	-----

**例** 次に、SSL をイネーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# ssl kmc
```

# tape-bkgrp

暗号テープ バックアップ グループを設定するには、**tape-bkgrp** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**tape-bkgrp** *groupname*

**no tape-bkgrp** *groupname*

構文の説明	<i>groupname</i> バックアップ テープ グループを指定します。31 文字以内で指定します。
-------	---

デフォルト	なし。
-------	-----

コマンドモード	SME クラスタ コンフィギュレーション モードサブモード。
---------	--------------------------------

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

使用上のガイドライン	<p>テープ ボリューム グループは、機能別に分類されているテープのグループです。たとえば、HR1 をすべての人事バックアップ テープ用のテープ ボリューム グループに指定できます。</p> <p>テープ グループの追加により、SME が暗号化されたデータ用に使用する、VSAN、ホスト、ストレージ デバイス、およびパスを選択することができます。たとえば、HR データ用のテープ グループを追加することで、SME のマッピングはデータを HR ホストから専用の HR バックアップ テープに転送するように設定されます。</p>
------------	---

例	次に、バックアップ テープ グループを追加する例を示します。
---	--------------------------------

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

次に、バックアップ テープ グループを削除する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

関連コマンド	コマンド	説明
	<b>clear sme</b>	SME コンフィギュレーションをクリアします。
	<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

# tape-compression

テープ圧縮を設定するには、**tape-compression** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**tape-compression**

**no tape-compression**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

なし。

## コマンドモード

SME クラスタ コンフィギュレーション サブモード。

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

暗号化されたデータを圧縮するには、このコマンドを使用します。

## 例

次に、テープ圧縮をイネーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-c1)# tape-compression
```

次に、テープ圧縮をディセーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-c1)# no tape-compression
```

## 関連コマンド

コマンド	説明
<b>clear sme</b>	SME コンフィギュレーションをクリアします。
<b>show sme cluster</b>	SME クラスタに関する情報を表示します。
<b>show sme cluster tape</b>	すべてのテープ ボリューム グループまたは特定のグループに関する情報を表示します。

# tape-device

暗号テープ デバイスを設定するには、**tape-device** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**tape-device** *device name*

**no tape-device** *device name*

## 構文の説明

*device name*                      テープ デバイスの名前を指定します。

## デフォルト

なし。

## コマンドモード

SME テープ ボリューム コンフィギュレーション サブモード。

## コマンド履歴

リリース	変更内容
3.2(2c)	このコマンドが導入されました。

## 使用上のガイドライン

テープ デバイス コマンドは、(**config-sme-cl-tape-bkgrp-tapedevice**) サブモードで使用できます。

## 例

次に、暗号テープ デバイスを設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

次に、暗号テープ デバイスを削除する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# no tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

## 関連コマンド

コマンド	説明
<b>clear sme</b>	SME コンフィギュレーションをクリアします。
<b>show sme cluster</b>	SME クラスタに関する情報を表示します。
<b>show sme cluster tape</b>	すべてのテープ ボリューム グループまたは特定のグループに関する情報を表示します。

# tape-keyrecycle

テープ キー リサイクル ポリシーを設定するには、**tape-keyrecycle** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

**tape-keyrecycle**

**no tape-keyrecycle**

**構文の説明** このコマンドには引数またはキーワードはありません。

**デフォルト** なし。

**コマンドモード** SME クラスタ コンフィギュレーション サブモード。

コマンド履歴	リリース	変更内容
	3.2(2c)	このコマンドが導入されました。

**使用上のガイドライン** SME ではテープ キーをリサイクルできます。テープ キー リサイクルをイネーブルにすると、テープ キーのすべての以前のインスタンスが削除されます。

**例** 次に、テープ キー リサイクルをイネーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-keyrecycle
```

次に、テープ キー リサイクルをディセーブルにする例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no tape-keyrecycle
```

関連コマンド	コマンド	説明
	<b>clear sme</b>	SME コンフィギュレーションをクリアします。
	<b>show sme cluster</b>	SME クラスタに関する情報を表示します。

# tape-volgrp

暗号テープ ボリューム グループを設定するには、**tape-volgrp** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

**tape-volgrp** *group name*

**no tape-volgrp** *group name*

構文の説明	<i>group name</i> テープ ボリューム グループ名を指定します。						
デフォルト	なし。						
コマンドモード	SME 暗号バックアップ テープ グループ コンフィギュレーション サブモード。						
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>3.2(2c)</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	3.2(2c)	このコマンドが導入されました。		
リリース	変更内容						
3.2(2c)	このコマンドが導入されました。						
使用上のガイドライン	テープ ボリューム グループ コマンドは、SME 暗号テープ ボリューム グループ ( <b>config-sme-cl-tape-bkgrp-volgrp</b> ) サブモードで使用できます。						
例	<p>次に、暗号テープ ボリューム グループを設定する例を示します。</p> <pre>switch# config t switch(config)# sme cluster c1 switch(config-sme-cl)# tape-bkgrp tbg1 switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1 switch(config-sme-cl-tape-bkgrp-volgrp)#</pre> <p>次に、暗号テープ ボリューム グループを削除する例を示します。</p> <pre>switch# config t switch(config)# sme cluster c1 switch(config-sme-cl)# tape-bkgrp tbg1 switch(config-sme-cl-tape-bkgrp)# no tape-volgrp tv1</pre>						
関連コマンド	<table border="1"> <thead> <tr> <th>コマンド</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td><b>clear sme</b></td> <td>SME コンフィギュレーションをクリアします。</td> </tr> <tr> <td><b>show sme cluster tape</b></td> <td>テープに関する情報を表示します。</td> </tr> </tbody> </table>	コマンド	説明	<b>clear sme</b>	SME コンフィギュレーションをクリアします。	<b>show sme cluster tape</b>	テープに関する情報を表示します。
コマンド	説明						
<b>clear sme</b>	SME コンフィギュレーションをクリアします。						
<b>show sme cluster tape</b>	テープに関する情報を表示します。						

# tune-timer

SME タイマーを調整するには、**tune-timer** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
tune-timer { global_lb_timer global_lb_timer_value | rscn_suppression_timer
rscn_suppression_timer_value | tgt_lb_timer tgt_lb_timer_value }
```

```
no tune-timer { global_lb_timer global_lb_timer_value | rscn_suppression_timer
rscn_suppression_timer_value | tgt_lb_timer tgt_lb_timer_value }
```

## 構文の説明

<b>global_lb_timer</b>	グローバル ロードバランシング タイマー値を指定します。
<i>global_lb_timer_value</i>	タイマー値を指定します。範囲は 5 ～ 30 秒です。デフォルト値は 5 秒です。
<b>rscn_suppression_timer</b>	SME Registered State Change Notification (RSCN) 抑制タイマー値を指定します。
<i>rscn_suppression_timer_value</i>	タイマー値を指定します。有効な範囲は 1 ～ 10 秒です。デフォルト値は 5 秒です。
<b>tgt_lb_timer</b>	ターゲット ロードバランシング タイマー値を指定します。
<i>tgt_lb_timer_value</i>	タイマー値を指定します。範囲は 2 ～ 30 秒です。デフォルト値は 2 秒です。

## デフォルト

なし。

## コマンドモード

SME クラスタ コンフィギュレーション サブモード。

## コマンド履歴

リリース	変更内容
3.3(1c)	このコマンドが導入されました。

## 使用上のガイドライン

**tune-timer** コマンドは、RSCN 抑制、グローバル ロードバランシング、およびターゲット ロードバランシングのタイマーといったさまざまな SME タイマーを調整するために使用されます。これらのタイマーは大規模セットアップでのみ使用してください。タイマー値は、クラスタ全体で同期されます。

## 例

次に、グローバル ロードバランシング タイマーの値を設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-c1)# tune-timer tgt_lb_timer 6
switch(config-sme-c1)#
```

次に、SME RSCN 抑制タイマーの値を設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```

次に、ターゲット ロード バランシング タイマーの値を設定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```





## SME のディザスタ リカバリ

この付録は、次の項で構成されています。

- [SME テープのディザスタ リカバリ シーケンス \(B-1 ページ\)](#)
- [SME ディスクのディザスタ リカバリ シーケンス \(B-2 ページ\)](#)

### SME テープのディザスタ リカバリ シーケンス



注意

SME クラスタがオンライン/アクティブ状態に回復できない場合にのみ、この手順を使用します。新しい SME クラスタを作成し、既存のキーをその新しい SME クラスタにインポートする必要があります。

SME テープを回復するには、次の手順を実行します。

- ステップ 1** SME クラスタの ASCII 設定がスイッチ上に存在している場合は、変更を実行する前に、`save the show SME tech support` コマンドおよび `show running config` コマンドをスイッチから削除する必要があります。これらのファイルは新しい SME クラスタを設定するときに役立ちます。
- ステップ 2** 主要な操作 (`admin`, `sme-kmc-admin`, `network-operator`) を実行できる資格情報でキー マネージャ (DCNM Web クライアント) にログインします。
- ステップ 3** 元のクラスタからすべてのボリューム グループをエクスポートします。最新のエクスポートされたバックアップがあれば、この手順は省略できます。古い SME クラスタのマスター キーはこの手順を実行する必要があります。クラスタのセキュリティ モードが「Basic」である場合、マスター キー ファイルが必要です。クラスタのセキュリティ モードが「Standard」または「Advanced」である場合、マスター キーを再構成するには、必要な数のスマート カードを備える必要があります。
- テープ グループを表示し、各ボリューム グループを選択して、[Export] をクリックします。Web クライアントによりオフライン エクスポートが手引きされ、各エクスポートのマスター キーの入力が求められます。
  - キーはパスワードで保護されたファイルにエクスポートされます。
  - 複数のテープ グループが存在する場合、この手順は、すべてのボリューム グループを含む、各テープ グループに対して実行する必要があります。エクスポートがどのテープ グループに属しているかがわかるように、ファイルには明確なラベルを付ける必要があります。
- ステップ 4** DCNM の UI を使用して、同じクラスタ設定で新しい名前を持つ新しいクラスタを作成します。

- ステップ 5** それぞれの古いテープ グループに対応する新しいテープ グループを作成します。
- 元のクラスタから各ボリューム グループに対応する新しいボリューム グループを作成します。
  - テープ デバイスを追加します。
- ステップ 6** 既存のテープへの書き込みを引き続き行いたい場合は、FMS conf ディレクトリ内の **smeserver.properties** を変更します。この手順を省略すると、テープは読み取り専用になります。
- smeserver.properties** を編集し、**smeserver.imported.key.state=true** を追加します。
  - DCNM サーバを再起動します。
  - FMS の再起動を待機し、再度ログインします。
- ステップ 7** 手順 3 のボリューム グループを、新しいクラスタの各テープ グループ ボリューム グループにインポートします。
- ステップ 8** 手順 7 を省略しなかった場合は、次の手順を実行します。
- smeserver.properties** を編集し、**smeserver.imported.key.state=true** を削除します。
  - Fabric Manager Server を再起動します。
  - FMS の再起動を待機し、再度ログインします。
- これで新しい SME クラスタは、KMC への安定した接続でオンラインになります。古い SME クラスタからのキーは、新しい SME クラスタにインポートされました。バックアップ操作を再開できます。

## SME ディスクのディザスタリカバリ シーケンス

SME ディスクを回復するには、次の手順を実行します。

- ステップ 9** SME クラスタの ASCII 設定がスイッチ上に存在している場合は、変更を実行する前に、**save the show sme tech support** コマンドおよび **show running config** コマンドをスイッチから削除する必要があります。これらのファイルは新しい SME クラスタを設定するときに役立ちます。
- ステップ 10** 主要な操作 (**admin**、**sme-kmc-admin**、**network-operator**) を実行できる資格情報でキー マネージャ (DCNM Web クライアント) にログインします。
- ステップ 11** 元のクラスタからすべてディスク キーをエクスポートします。最新のエクスポートされたバックアップがあれば、この手順は省略できます。古い SME クラスタのマスター キーはこの手順を実行する必要があります。クラスタのセキュリティ モードが「**Basic**」である場合、マスター キーファイルが必要です。クラスタのセキュリティ モードが「**Standard**」または「**Advanced**」である場合、マスター キーを再構成するには、必要な数のスマート カードを備える必要があります。
- ディスク グループを表示し、すべてのディスクを選択し、**[Export]** をクリックします。Web クライアントによりオフラインエクスポートが手引きされ、各エクスポートのマスター キーの入力が求められます。
  - キーは、パスワードで保護されたファイルにエクスポートされます。
  - 複数のディスク グループが存在する場合、この手順は、各ディスク グループに対して実行する必要があります。エクスポートがどのディスク グループに属しているかがわかるように、ファイルには明確なラベルを付ける必要があります。
- ステップ 12** DCNM の GUI を使用して、同じクラスタ設定で新しい名前を持つ新しいクラスタを作成します。

- ステップ 13 それぞれの古いディスク グループに対応する新しいディスク グループを作成します。
- 元のクラスタから各ディスク グループに対応する新しいディスク グループを作成します。
- ステップ 14 既存のディスクへの書き込みを引き続き行いたい場合は、FMS conf ディレクトリ内の **smeserver.properties** を変更します。この手順を省略すると、既存のディスクは読み取り専用になります。
- a. **smeserver.properties** を編集し、**smeserver.imported.key.state=true** を追加します。
  - b. Fabric Manager Server を再起動します。
  - c. FMS の再起動を待機し、再度ログインします。
- ステップ 15 手順 3 のキーを、各ディスク グループの新しいクラスタにインポートします。必要に応じて、各ディスク名を一致させます。
- ステップ 16 手順 7 を省略しなかった場合は、次の手順を実行します。
- a. **smeserver.properties** を編集し、**smeserver.imported.key.state=true** を削除します。
  - b. Fabric Manager Server を再起動します。
  - c. FMS の再起動を待機し、再度ログインします。

これで新しい SME クラスタは、KMC への安定した接続でオンラインになります。古い SME クラスタからのキーは、新しい SME クラスタにインポートされました。バックアップ操作を再開できます。

---





## SME のオフラインデータ リカバリ

SME ソリューションは、ハードウェアベースの暗号化エンジンによってシームレスな暗号化サービスを提供します。MSM-18/4 モジュールまたは Cisco MDS 9222i ファブリック スイッチが使用できない場合は、オフライン データ復元ツール(ODRT)を使用できます。



(注) SME オフラインデータ リカバリは、SME テープにのみ適用されます。

この付録では、このソフトウェア アプリケーションの基本機能と動作について説明し、次のトピックについて取り上げます。

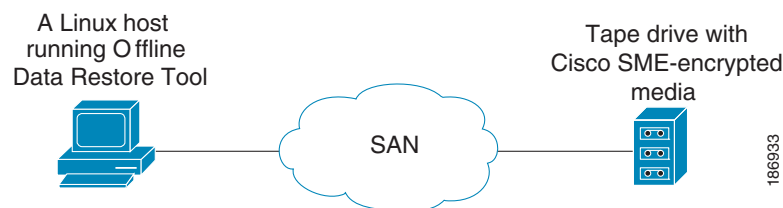
- [オフラインデータ復元ツールに関する情報\(C-1 ページ\)](#)
- [ODRT 要件\(C-2 ページ\)](#)

## オフラインデータ復元ツールに関する情報

オフラインデータ復元ツール(ODRT)は、スタンドアロン Linux アプリケーションであり、MSM-18/4 モジュールまたは Cisco MDS 9222i スイッチが使用できない場合にテープ ボリューム グループ上の暗号化データを回復するための包括的なソリューションです。ODRT は、SME により暗号化されたテープ ボリュームを読み取り、データを復号して圧縮解除し、クリアテキスト データとしてテープ ボリュームに書き込んで戻します。

☒ C-1 は、ODRT でサポートされるトポロジを示しています。

☒ C-1 オフラインデータ復元ツール(ODRT)のトポロジ



データの暗号化と復号化は、次の 2 つのステップで実行されます。

- テープからディスク:ODRT はテープから暗号化データを読み取って、それをディスク上の中間ファイルに保存します。
- ディスクからテープ:ODRT はディスク上の中間ファイルを読み取り、データを復号化および(必要な場合は)圧縮解除して(該当する場合)、クリアテキストデータとしてテープに書き込みます。

復号キーは、Cisco Key Management Center (KMC) からエクスポートする必要があるボリュームグループファイルから取得します。ボリュームグループをエクスポートする方法については、[第 7 章「SME キー管理の設定」](#)を参照してください。

ODRT 機能は、Linux シェルから **odrt.bin** コマンドを入力して呼び出します。**odrt.bin** コマンドの詳細については、[付録 A「SME CLI コマンド」](#)を参照してください。

## ODRT 要件

ODRT ツールの実行の前提条件は、次のとおりです。

- プラットフォーム:ODRT は現在、Red Hat Enterprise Linux 5 でサポートされています。
- CPU:x86 ファミリのマイクロプロセッサなどの、リトルエンディアン CPU 設計がサポートされています。高速 CPU の使用を推奨します。
- メモリ:具体的な制限はなく、1 GB から 2 GB のメモリ量で十分です。
- ディスク サイズ:ディスクは 1 TB のデータを保持する必要があります。
- テープドライブへのファイバチャネル(FC)接続が必要です。



## データベースのバックアップと復元

データにアクセスできなくなるリスクを負わないようにするために、データベースには適正に定義され、十分にテストされたバックアップと復元の計画が必要です。データベースのバックアップとリカバリには、機器の故障時または災害発生時に、データベースのコピーを作成し、必要な場合にコピーしたデータベースを取得するプロセスが関係しています。

この付録では、DCNM-SAN データベースのバックアップと復元の方法を説明します。

DCNM-SAN は、PostgreSQL データベース管理システムをデフォルトのデータベースとして使用します。PostgreSQL データベースは、**pg\_dump** コマンドでバックアップされます。**pg\_dump** ユーティリティは、PostgreSQL データベースの内容を ASCII ダンプ ファイルにダンプします。バックアップ ダンプ ファイルとは、バックアップ時のデータベースのスナップショットのことです。

データベースは、**pg\_restore** ユーティリティを使用して復元します。**pg\_restore** ユーティリティは、**psql** を使用して、**pg\_dump** により作成されたダンプ ファイルから PostgreSQL データベースを再構築します。



(注)

Oracle Database Server は、Cisco DCNM および SME でサポートされます。Oracle データベースの管理、バックアップ、および復元については、このドキュメントの範囲外です。Oracle データベースのバックアップおよび復元計画の詳細については、お客様の地域の Oracle DBA にお問い合わせください。

**pg\_dump** コマンドの詳細については、次の URL を参照してください。

<http://www.postgresql.org/docs/current/interactive/app-pgdump.html>

この付録は、次の項で構成されています。

- [DCNM-SAN データベースのバックアップ \(D-1 ページ\)](#)
- [DCNM-SAN データベースの復元 \(D-2 ページ\)](#)
- [データベースのバックアップ/復元操作 \(D-2 ページ\)](#)

## DCNM-SAN データベースのバックアップ

DCNM-SAN データベースをバックアップするには、次のように PostgreSQL **pg\_dump** コマンドを使用します。

```
cd $INSTALLDIR/bin
./pgbackup.sh 02252008.data (on Linux and Solaris operation systems)
pgbackup.bat 02252008.data (on Windows operating system)
```

INSTALLDIR は DCMN-SAN インストールの最上位ディレクトリであり、バックアップ ファイル (02252008.data) は \$INSTALLDIR/bin ディレクトリ内に作成されます。

標準バックアップ ディレクトリ内にバックアップ ファイルを作成するには、ダンプ ファイルのフルパス名を指定します。



(注) すべてのオペレーティング システムで、スクリプトは **pg\_dump** コマンドを実行してデータベースをバックアップします。

## DCNM-SAN データベースの復元

DCNM-SAN データベースを復元するには、**pg\_restore** コマンドを使用します。

```
cd $ INSTALLDIR/bin
./pgrestore.sh 02252008.data (on Linux and Solaris operating systems)
pgrestore.bat 02252008.data (on Windows operating system)
```

バックアップ復元プロセスでは、サーバを停止させる必要があります。



(注) すべてのオペレーティング システムで、スクリプトにより **pg\_restore** コマンドを実行してデータベースを復元します。

## データベースのバックアップ/復元操作

DCNM-SAN のバックアップおよび復元操作を実行するときは、次の点に注意してください。

- バックアップ コピーに最新のメディア キーがないため、データベースのバックアップ後に作成される新しいメディア キーは、復元操作後に失われます。
- データベースのバックアップ後に作成された新しいテープ バックアップ グループとテープ ボリューム グループがある場合は、DCNM-SAN を開始する前に、`smeserver.properties` でプロパティを `true` に設定する必要があります。これは新しいボリューム グループ キーを KMC に同期します。

```
sme.kmc.sync.model.at.startup=true
```

このプロパティは、テープ ボリューム グループのキー再生成操作にも適用可能です。

- マスター キーがデータベースのバックアップ後にキー再生成された場合、以前のデータベースのデータを復元すると、クラスタは使用できなくなります。マスター キーのキー再生成操作後には、データベースのバックアップを作成し、以前のデータベース バックアップのコピーは破棄します。





## 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 \(E-1 ページ\)](#)
- [相互運用性マトリックス \(E-2 ページ\)](#)
- [MSM-18/4 モジュール \(E-2 ページ\)](#)
- [Key Management Center および DCNM-SAN サーバ \(E-2 ページ\)](#)
- [セキュリティ \(E-3 ページ\)](#)
- [通信 \(E-4 ページ\)](#)
- [設置準備の要件 \(E-4 ページ\)](#)
- [事前設定タスク \(E-4 ページ\)](#)
- [SME のプロビジョニング \(E-7 ページ\)](#)

### 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。

- 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。
- 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。







## SME データベース テーブルの移行



(注) 現在のところ、データの移行は、SME テープのみでサポートされています。これはまだ、SME ディスクではサポートされていません。

この付録では、データベース移行ユーティリティについて説明し、別のデータベースに SME テーブルを移行するために従う必要のある手順について概説します。

データベース移行ユーティリティは、Oracle Express インストールまたは PostgreSQL にあるデータベース テーブルの内容を、Oracle Enterprise インストールに転送します。

このユーティリティ、NX-OS Software Release 4.1(3) 以降の Cisco DCNM for SAN の CD にパッケージされており、/software/SMEdbmigrate.zip で入手できます。



(注) DCNM-SAN アプリケーションは、DCNM-SAN テーブルが宛先データベースに作成されるように、移行プロセスの前に宛先データベースを使用してインストールする必要があります。

ソース データベースから宛先データベースにデータベース ファイルを移行するには、次の手順を実行します。

**ステップ 1** SMEdbmigrate.zip ファイルの内容をディレクトリ フォルダに展開します。ファイルの内容は次のようになります。

- SMEdbmigrate.jar
- ojdbc14.jar
- postgresql-8.1.jar
- smedbigrate.bat
- smedbigrate.sh
- smedbmigration.properties

**ステップ 2** smedbmigration.properties ファイルを右クリックして、テキスト エディタで開きます。既存のデータベースの URL、タイプ、およびユーザ名と、宛先データベースの URL、タイプ、およびユーザ名を変更します。

**ステップ 3** データ ファイルを移行するには、次のシェル スクリプトまたはバッチ ファイルを実行します。

- `sh smedbigrate.sh` (Unix 用)
- `smedbigrate.bat` (Windows 用)

シェル スクリプトまたはバッチ ファイルは、ソース データベースと宛先データベースの両方にアクセスするどのサーバからでも実行できます。

**ステップ 4** プロンプトが表示されたら、ソースおよび宛先データベースのパスワードを入力します。

サンプル出力は、次のようになります。

```
[root@test-vm-236 SMEdbmigrate]# ./smedbigrate.sh
[INFO] File /root/download/SMEdbmigrate/smedbmigration.properties found
Please enter the password for user admin on source database
jdbc:postgresql://172.28.233.186:5432/dcmdb *****

Please enter the password for user admin on destination database
jdbc:postgresql://172.28.255.110:5432/dcmdb *****
*[INFO] Migrating database from jdbc:postgresql://172.28.233.186:5432/dcmdb to
jdbc:postgresql://172.28.255.110:5432/dcmdb
[INFO] Migration Start for SME_SETTINGS
...
...
...
[INFO] Migration complete
[root@test-vm-236 SMEdbmigrate]#
```




---

(注) 移行が正常に行われたことを確認するために、キー取得操作を実行します。

---