Cisco DCNM Fundamentals ガイド リリース 5.x

2011 年 7 月

Text Part Number: OL-25174-01-J

【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/）をご確認ください。

本書は、米国シスコ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. 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 アドレスは、実際のアドレス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、および図は、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 DCNM Fundamentals ガイド
© 2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2011–2012, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

新機能および変更された機能に関する情報 xxv

はじめに lxi

Cisco Data Center Network Manager の概要 lxix

PART 1 Cisco Data Center Network Manager

CHAPTER 1 Cisco DCNM Fundamentals 概要 1-1

- DCNM-SAN サーバ 1-1
- DCNM-SAN クライアント 1-2
- Device Manager 1-2
- DCNM-SAN Web クライアント 1-2
- Performance Manager 1-3
- DCNM-SAN クライアントでの認証 1-3
- Cisco Traffic Analyzer 1-4
- ネットワーク モニタリング 1-4
- パフォーマンス モニタリング 1-4

CHAPTER 2 Cisco DCNM Web クライアント 2-1

- Cisco DCNM Web クライアントの概要 2-1
  - Cisco DCNM-SAN クライアントのダウンロード 2-2
  - DCNM Web クライアントの起動 2-3
  - DCNM Web クライアントのナビゲーション 2-4
  - DCNM Web クライアントでの SSL の使用方法 2-5
- ヘルス情報の表示 2-8
  - アカウンティング情報の表示 2-8
  - イベント情報の表示 2-9
  - Syslog 情報の表示 2-9
  - Syslog アーカイブ情報の表示 2-9
- パフォーマンス情報の表示 2-10
  - スイッチ CPU 情報の表示 2-11
  - スイッチ メモリ情報の表示 2-11
  - スイッチの帯域幅とエラー情報の表示 2-12
  - ISL トラフィックとエラー情報の表示 2-12
  - すべてのポートに関するパフォーマンス情報の表示 2-13

ホスト ポートに関するパフォーマンス情報の表示 2-13
ストレージ ポートに関するパフォーマンス情報の表示 2-13
ホスト ラックに関するパフォーマンス情報の表示 2-14
ストレージ ラックに関するパフォーマンス情報の表示 2-14
ポート グループに関するパフォーマンス情報の表示 2-14
ISL のパフォーマンス情報の表示 2-15
NPV リンクのパフォーマンス情報の表示 2-16
フローのパフォーマンス情報の表示 2-16
ギガビット イーサネットとイーサネット ポートに関するパフォーマンス情報の表示 2-18
その他の統計情報の表示 2-18
インベントリ情報の表示 2-19
VSAN のインベントリ情報の表示 2-19
スイッチのインベントリ情報の表示 2-20
ライセンス情報の表示 2-20
モジュールのインベントリ情報の表示 2-21
エンド デバイスにあるすべてのポートのインベントリ情報の表示 2-21
エンド デバイスにあるホスト ポートのインベントリ情報の表示 2-22
エンド デバイスにあるストレージ ポートのインベントリ情報の表示 2-22
ISL の詳細情報の表示 2-23
NPV リンクのインベントリ情報の表示 2-23
標準ゾーンに関するインベントリ情報の表示 2-23
IVR ゾーンに関するインベントリ情報の表示 2-24
カスタム レポートの表示および作成 2-24
カスタム レポート テンプレートの作成 2-25
テンプレート別のカスタム レポートの表示 2-27
ユーザ別のカスタム レポートの表示 2-27
レポート テンプレートの削除 2-27
テンプレート別のカスタム レポートの作成 2-28
カスタム レポート テンプレートの修正 2-29
カスタム レポートの削除 2-29
レポート テンプレート別のスケジュール済みジョブの表示 2-30
DCNM Web クライアントの管理 2-30
サービスの開始、再開、停止 2-31
管理対象のファブリックの追加、編集、削除 2-31
LAN の追加、編集、および削除 2-33
VMWare Server の追加、編集、および削除 2-34
VMWare Server の再検出 2-35
コミュニティの追加と削除 2-35
ログ情報の表示 2-36

Cisco DCNM-SAN サーバのプロパティの設定 2-36
SFTP クレデンシャルの設定 2-36
トラップおよび Syslog 登録情報の表示 2-37
イベント通知転送の設定 2-37
EMC CallHome の設定 2-38
AAA プロパティの設定 2-38
ユーザの追加と削除 2-38
ロールの追加と削除 2-39
クライアントの表示と接続解除 2-40
パフォーマンス収集の作成、編集、および削除 2-40
RRD データベースの設定 2-41
RRD 統計インデックスのインポート 2-42
収集しきい値の設定 2-42
その他の統計情報の設定 2-43
Cisco DCNM-SAN Web 検索エンジン 2-43
Cisco DCNM-SAN 検索エンジンの使用方法 2-43
DCNM Web クライアントを使用したバックアップの設定 2-44
コンフィギュレーションの表示 2-44
コンフィギュレーションの編集 2-45
コンフィギュレーションの削除 2-45
コンフィギュレーションのコピー 2-45
コンフィギュレーションの比較 2-46
バックアップの作成 2-46
スケジュールされたジョブの表示 2-47
ホストおよび仮想ホスト情報の表示 2-47
ホスト ラックの表示 2-47
仮想ホストの表示 2-47
仮想マシンの表示 2-48
仮想マシンの CPU およびメモリ情報の表示 2-48
仮想マシンのディスク I/O 情報の表示 2-48
ダッシュボード サマリー情報の表示 2-49
ヘルス サマリー情報の表示 2-49
パフォーマンス サマリー情報の表示 2-49
インベントリ サマリー情報の表示 2-50

PART 2 **Cisco DCNM for SAN**

CHAPTER 3 **Cisco DCNM-SAN サーバの設定** 3-1
Cisco DCNM-SAN サーバに関する情報 3-1

DCNM-SAN サーバの機能 3-1
Cisco DCNM-SAN サーバのライセンス要件 3-2
Cisco DCNM-SAN サーバのインストールと設定 3-2
Cisco DCNM-SAN サーバのインストール 3-3
Cisco DCNM-SAN サーバでのデータ マイグレーション 3-5
Performance Manager 収集の確認 3-6
Cisco DCNM-SAN サーバ ファブリックの管理 3-6
継続的管理対象のファブリックの選択 3-6
Cisco DCNM-SAN サーバのプロパティ ファイル 3-7
Cisco DCNM-SAN サーバの変更 3-8
Cisco DCNM-SAN サーバのユーザの追加または削除 3-8
Cisco DCNM-SAN サーバのユーザ名およびパスワードの変更 3-9
ポーリング時間とファブリック再検出時間の変更 3-9
Cisco DCNM-SAN サーバの IP アドレスの変更 3-10
デバイス エイリアスまたは FC エイリアスの使用方法 3-10
サーバ フェデレーション 3-11
制約事項 3-11
Fabric ID から Server ID へのマッピング 3-11
ファブリックを別のサーバで開く 3-12
フェデレーション内のセッションの表示 3-12
フェデレーション内のサーバの表示 3-12
その他の関連資料 3-13

CHAPTER 4 **Cisco DCNM-SAN での認証の設定 4-1**
Cisco DCNM-SAN 認証の概要 4-1
ファブリック検出のベスト プラクティス 4-3
ファブリック検出の設定 4-3
Performance Manager の認証 4-4
Cisco DCNM-SAN Web クライアントの認証 4-4

CHAPTER 5 **Cisco DCNM-SAN クライアントの設定 5-1**
DCNM-SAN クライアントの概要 5-1
Cisco DCNM-SAN 拡張モード 5-2
Cisco DCNM-SAN クライアント クイック ツアー：サーバ管理者向けの表示 5-2
Cisco DCNM-SAN メイン ウィンドウ 5-2
メニュー バー 5-4
ツールバー 5-4
[Logical Domains] ペイン 5-4

[Physical Attributes] ペイン 5-5
[Information] ペイン 5-5
[Fabric] ペイン 5-6
Cisco DCNM-SAN クライアント クイック ツアー：管理者向けの表示 5-7
メニュー バー 5-8
ツールバー 5-12
[Logical Domains] ペイン 5-14
[Physical Attributes] ペイン 5-15
[Information] ペイン 5-18
[Fabric] ペイン 5-19
ステータス バー 5-24
DCNM-SAN クライアントの起動 5-24
Cisco SAN-OS Release 3.2(1) 以降で Fabric Manager Client を起動する 5-24
起動パッドを使用した Cisco DCNM-SAN クライアントの起動 5-27
Cisco DCNM-SAN プリファレンスの設定 5-28
ネットワーク ファブリックの検出 5-30
ネットワーク LAN の検出 5-30
イーサネット スイッチの表示 5-30
LAN の削除 5-30
デバイス グループの変更 5-31
ラックへのエイリアス名の使用方法 5-31
説明へのエイリアス名の使用方法 5-32
ユーザおよびロールによる管理者アクセスの制御 5-32
Cisco DCNM-SAN Wizard の使用方法 5-32
Cisco DCNM-SAN トラブルシューティング ツール 5-33
Cisco DCNM-SAN と Data Center Network Management ソフトウェアの統合 5-34
トポロジ マップからのスイッチの起動 5-34

CHAPTER 6 **Device Manager** 6-1

Device Manager の概要 6-1
Device Manager の機能 6-2
Device Manager インターフェイスの使用方法 6-2
メニュー バー 6-3
ツールバー アイコン 6-4
ダイアログボックス 6-5
タブ 6-6
用例 6-6
スーパーバイザおよびスイッチング モジュール 6-7

コンテキスト メニュー 6-7
Device Manager の起動 6-8
Device Manager のプリファレンスの設定 6-9

CHAPTER 7 **Performance Manager の設定 7-1**
Performance Manager の概要 7-1
データ補間 7-2
データ収集 7-2
パフォーマンスしきい値の使用方法 7-2
フロー統計 7-3
フロー セットアップ ウィザード 7-4
Performance Manager Flow Wizard を使用したフローの作成 7-4

CHAPTER 8 **ネットワークのモニタリング 8-1**
ネットワーク モニタリングの概要 8-1
ヘルスおよびイベントのモニタリング 8-1
デバイス ディスカバリ 8-2
トポロジ マッピング 8-3
インベントリ管理 8-4
Device Manager からのログの表示 8-5

CHAPTER 9 **パフォーマンスのモニタリング 9-1**
パフォーマンス モニタリングの概要 9-1
リアルタイム パフォーマンス モニタリング 9-1
パフォーマンス履歴のモニタリング 9-2
Performance Manager の設定 9-2
Performance Manager でのフローの作成 9-2
Performance Manager での収集の作成 9-2
パフォーマンスしきい値の使用方法 9-3
サマリー ビューの設定 9-4
Device Manager を使用したポート単位モニタリングの設定 9-5
DCNM-SAN リアルタイム ISL 統計情報の表示 9-5
Performance Manager Configuratino Wizard の使用方法 9-6
DCNM-SAN を使用したパフォーマンス統計情報の表示 9-6
Performance Manager レポートの表示 9-7
パフォーマンス サマリーの表示 9-7
パフォーマンス テーブルと詳細グラフの表示 9-8
ホスト最適化ポート グループのパフォーマンスの表示 9-8

Performance Manager イベントの表示 9-8
Performance Manager レポートの生成 9-8
Performance Manager での Top10 レポートの生成 9-8
スクリプトを使用した Top10 レポートの生成 9-9
Cisco Traffic Analyzer と併用するための Performance Manager の設定 9-9
収集データのエクスポート 9-11
収集データの XML ファイルへのエクスポート 9-11
読み取り可能フォーマットでの収集データのエクスポート 9-12
SAN ヘルスの分析 9-13
SAN Health Advisor ツールのインストール 9-14

CHAPTER 10 ソフトウェア イメージ 10-1
ソフトウェア イメージの概要 10-1
ソフトウェア アップグレード方法 10-2
ソフトウェアの互換性の判別 10-2
自動アップグレード 10-3
Software Install Wizard を使用した場合の利点 10-3
失敗するケースの特定 10-4
ソフトウェア イメージのインストールの前提条件 10-4
Cisco MDS 9100 シリーズ スイッチの正しいソフトウェア イメージの選択 10-5
Cisco MDS 9200 シリーズ スイッチの正しいソフトウェア イメージの選択 10-5
Cisco MDS 9500 ファミリ スイッチの正しいソフトウェア イメージの選択 10-6
不可欠なアップグレード要件 10-6
デフォルト設定 10-8
Software Install Wizard の使用方法 10-8
ファブリックおよびモジュラ スイッチの中断がないアップグレードの実行 10-11
ファブリックおよびモジュラ スイッチの中断のないアップグレードの準備 10-11
ファブリック スイッチでの中断がないアップグレードの実行 10-12
スーパーバイザ モジュールのメンテナンス 10-13
スーパーバイザ モジュールの交換 10-13
スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールへの移行 10-13
スタンバイ スーパーバイザ モジュールのブート変数バージョンの設定 10-14
スタンバイ スーパーバイザ モジュールのブートフラッシュ メモリの設定 10-14
スタンバイ スーパーバイザ モジュールのブート アラート 10-14
ジェネレーション 1 シャーシへのジェネレーション 2 モジュールの設置 10-14
モジュールの交換 10-15

CHAPTER 11 管理ソフトウェアの FAQ 11-1

インストールの問題 11-3

Windows から Cisco DCNM-SAN をインストールするときに、インストールをクリックできません 11-3

Solaris で Cisco DCNM-SAN を起動できません 11-3

ブラウザ上に JNLP ファイルの保存を促すプロンプトが表示されます 11-4

[Java Web Start not detected] エラーが表示されます 11-4

Cisco DCNM-SAN または Device Manager を新しいバージョンにアップグレードする方法を教えてください 11-4

Cisco DCNM-SAN または Device Manager をダウングレードする方法を教えてください 11-4

アップグレードできません 11-5

ダウンロード ダイアログで Java Web Start が停止します 11-5

Java Web Start を手動で設定する方法を教えてください 11-5

Java Web Start をコマンドラインから実行する方法を教えてください 11-6

Java Web Start のキャッシュをクリアする方法を教えてください 11-6

Cisco DCNM-SAN のアップグレード中、ショートカットを作成するプロンプトが表示されません 11-6

Cisco DCNM-SAN または Device Manager にログインできません 11-6

pcAnyWhere の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません 11-7

[Services] メニューで、Cisco DCNM-SAN または Performance Manager サービスが [disabled] と表示されます 11-7

McAfee Internet Suite 6.0 Professional の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません 11-7

全般 11-7

面グラフのモニタ中にエラーが表示されます。 11-7

[gen error] メッセージが表示されます。 11-7

Device Manager Summary View にディスク イメージが表示されません 11-8

Device Manager に D_S_TOV および E_D_TOV タイマーを同時に設定できません 11-8

Device Manager テーブルのカラムを大きくする方法を教えてください 11-8

ファブリックの変更がマップに伝播されません（リンクが消えないなど） 11-8

PortChannel の作成ダイアログボックスを何度か使用したら小さくなってしまいました 11-8

IPFC を設定するとエラーが表示されます 11-8

Cisco DCNM-SAN または Device Manager で正しいネットワーク インターフェイスが使用されません 11-9

Cisco DCNM-SAN または Device Manager の画面が正常に表示されません 11-9

[Physical Attributes] カテゴリがほとんど表示されなくなりました 11-9

[Information] ペインが表示されません 11-9

編集ゾーン内のアクティブ ゾーン セットが（正しくアクティブ化した場合でも）太字で表示されます 11-9
プレフィクスが IVRZ のゾーンまたは nozonset という名前のゾーン セットを作成できますか 11-10
ワンクリック ライセンス インストールが実行されず、シスコの Web サイトにもアクセスできません 11-10
Cisco DCNM-SAN クライアントでログ ウィンドウのサイズを拡大する方法を教えてください 11-10
FM Server Database が起動できません。またはファイル ロック エラーが発生します 11-10
Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバを再同期化する方法を教えてください 11-10
現在のファブリックを再検出する方法を教えてください 11-11
SCSI ターゲットを再検出する方法を教えてください 11-11
Windows の問題 11-11
表示されたテキスト フィールドが小さすぎてデータを入力できません 11-11
印刷するとアプリケーションがクラッシュします 11-11
Windows XP が停止しました（ブルー画面になりました） 11-11
Cisco DCNM-SAN および Device Manager のアイコンが表示されません 11-11
Windows XP で Device Manager または Cisco DCNM-SAN ウィンドウの内容が表示されません 11-12
ファイルをローカル マシンからスイッチにコピーすると SCP/SFTP にエラーが発生します 11-12
UNIX の問題 11-12
親メニューが表示されません 11-12
Web サーバは稼動しているのにブラウザで検出できません 11-12
[too many open files] エラーへの対処方法を教えてください 11-12
その他 11-13
Cisco DCNM-SAN の再起動後もマップ レイアウトを保持する方法を教えてください 11-13
スイッチは 1 台しかないのにマップには 2 つ表示されます 11-13
スイッチ内のレッド / オレンジ / 点線の意味を教えてください。 11-14
マップ設定を保持したままアップグレードする方法を教えてください 11-19
Cisco DCNM-SAN サーバを新規ホストに移行するときに履歴データを保持する方法を教えてください 11-20
FCIP 上で Cisco DCNM-SAN を使用するときの制限はありますか 11-20
[Please insure that FM server is running on localhost] メッセージへの対処法を教えてください 11-20
複数のインターフェイスを使用して Cisco DCNM-SAN を実行する方法を教えてください 11-21
HTTP プロキシ サーバの設定方法を教えてください 11-22
トポロジ マップをクリアする方法を教えてください 11-23

ソフトウェアの混在環境で Cisco DCNM-SAN を使用する方法を教えてください 11-23
Cisco DCNM-SAN 起動時に「corrupted jar file」エラーが表示されます。対処方法を教えてください 11-23
ファブリック内のデバイスの検索方法を教えてください 11-24
テーブルの検索方法を教えてください 11-24
複数のファブリックの管理方法を教えてください 11-25
ライセンス期限が切れるとスイッチに表示されるオレンジの X をクリアする方法を教えてください 11-25

PART 3 Cisco DCNM for LAN

CHAPTER 12 DCNM-LAN の概要 12-1
DCNM-LAN クライアントおよびサーバ 12-1
Cisco DCNM-LAN Release 5.2 の機能 12-2
プラットフォーム サポート 12-3
DCNM-LAN の関連資料 12-3

CHAPTER 13 Cisco DCNM-LAN クライアントのインストールおよび起動 13-1
DCNM-LAN クライアントのインストールおよび起動の概要 13-1
DCNM-LAN クライアントのインストールおよび起動の前提条件 13-2
セキュアなクライアント通信 13-2
デフォルトの管理者クレデンシャル 13-3
DCNM-LAN クライアントのダウンロードおよび起動 13-3
Web ブラウザを使用して DCNM-LAN クライアントをダウンロードおよび起動する 13-3
コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する 13-5
コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する（Java Web Start Launcher を使用しない場合） 13-6
DCNM-LAN クライアントの再起動 13-7
DCNM-LAN クライアントへのログイン 13-7
DCNM-LAN クライアントのアンインストール 13-9
その他の関連資料 13-9
関連資料 13-9
標準 13-10
DCNM-LAN クライアントのインストールおよび起動の機能の履歴 13-10

CHAPTER 14 Cisco DCNM-LAN クライアントの使用方法 14-1
DCNM-LAN クライアントの概要 14-1

ユーザ インターフェイス 14-2
[Feature Selector] ペイン 14-2
[Contents] ペイン 14-3
[Summary] ペイン 14-3
[Details] ペイン 14-3
[Association] ペイン 14-4
メニュー 14-5
ツールバー 14-7
キーボード コマンド 14-7
複数プラットフォームのサポート 14-7
DCNM-LAN クライアントの起動 14-8
DCNM-LAN クライアントの終了 14-10
変更の配置 14-10
統計情報および図の作業 14-11
統計情報および図の概要 14-11
統計情報および図のライセンス要件 14-11
図の表示 14-12
図の統計モニタリングの開始 14-12
図の統計モニタリングの停止 14-13
図の使用方法 14-13
概要図の使用方法 14-14
図のエクスポート 14-15
グローバル プリファレンスの設定 14-16
モニタリング プリファレンスの設定 14-16
サーバから取得するイベントの最大経過時間の設定 14-17
事前プロビジョニングの設定 14-17
オンライン ヘルプの使用方法 14-18
その他の関連資料 14-19
関連資料 14-19
標準 14-19
DCNM-LAN クライアントの使用の機能履歴 14-20

CHAPTER 15 **DCNM-LAN 認証設定の管理 15-1**
DCNM-LAN 認証設定の管理の概要 15-1
ユーザとユーザ ロール 15-2
ローカル認証と DCNM-LAN ローカル ユーザ 15-2
RADIUS および TACACS+ 認証 15-2
RADIUS および TACACS+ によるユーザ ロールの割り当て 15-3
ローカル認証へのフォールバック 15-3

パスワード回復 15-3
ユーザとデバイス クレデンシャル 15-4
仮想化のサポート 15-4
DCNM-LAN 認証設定を管理するためのライセンス要件 15-4
DCNM-LAN 認証設定を管理するための前提条件 15-4
DCNM-LAN 認証設定の管理に関する注意事項と制約事項 15-5
DCNM-LAN 認証の設定 15-5
認証モードの設定 15-5
DCNM-LAN ローカル ユーザの追加 15-6
DCNM-LAN ローカル ユーザのパスワードの変更 15-7
DCNM-LAN ローカル ユーザのフルネーム、ロール、説明の変更 15-8
DCNM-LAN サーバ ユーザの削除 15-8
認証サーバの追加 15-9
認証サーバ設定の変更 15-10
認証サーバの削除 15-11
DCNM-LAN ローカル ユーザの表示 15-12
認証サーバ設定の確認 15-12
DCNM-LAN 認証設定のフィールドの説明 15-13
[Authentication Mode] セクション 15-13
[DCNM-LAN Local Users] セクション 15-13
[Authentication Servers] セクション 15-14
その他の関連資料 15-14
関連資料 15-15
標準 15-15
DCNM-LAN 認証設定の機能の履歴 15-15

CHAPTER 16 **デバイス ディスカバリの管理 16-1**
デバイス ディスカバリの概要 16-1
デバイス ディスカバリ 16-2
ディスカバリ プロトコル 16-2
クレデンシャルとディスカバリ 16-3
ディスカバリ プロセス 16-3
Cisco NX-OS システム メッセージのロギング要件 16-3
ログ レベル自動設定のサポート 16-4
VDC のサポート 16-5
デバイス ディスカバリのライセンス要件 16-5
デバイス ディスカバリの前提条件 16-6
デバイス ディスカバリの注意事項と制約事項 16-6

デバイス ディスカバリの実行 16-7
Cisco NX-OS デバイスのディスカバリ準備状態の確認 16-7
デバイスの検出 16-9
デバイスの再検出 16-10
デバイス ディスカバリ タスクのステータスの表示 16-11
関連情報 16-12
デバイス ディスカバリのフィールドの説明 16-12
デバイス ディスカバリの [Contents] ペイン 16-12
関連フィールド 16-13
デバイス システム メッセージのログ レベルの参考情報 16-13
DCNM-LAN 機能別 Cisco Nexus 7000 NX-OS ログ レベル 16-14
DCNM-LAN 機能別 Cisco Nexus 5000 NX-OS ログ レベル 16-15
DCNM-LAN 機能別 Cisco Nexus 4000 NX-OS ログ レベル 16-16
DCNM-LAN 機能別 Cisco Nexus 1000V NX-OS ログ レベル 16-17
デバイス ディスカバリに関するその他の関連資料 16-17
関連資料 16-17
標準 16-18
デバイス ディスカバリ機能の履歴 16-18

CHAPTER 17 デバイスとクレデンシャルの管理 17-1
デバイスとクレデンシャルの概要 17-1
デバイス 17-1
クレデンシャル 17-2
デバイスのステータス 17-2
VDC のサポート 17-2
デバイスとクレデンシャル機能のライセンス要件 17-3
デバイスとクレデンシャル機能を管理するための前提条件 17-3
デバイスとクレデンシャル機能の注意事項と制約事項 17-3
デバイスとクレデンシャル機能の設定 17-3
デバイスの追加 17-4
デバイスの検出 17-4
デバイスの非管理対象化 17-5
デバイスの削除 17-6
デフォルトのデバイス クレデンシャルの設定 17-6
デフォルトのデバイス クレデンシャルの消去 17-7
デバイスの一意なクレデンシャルの設定 17-8
デバイスの一意なクレデンシャルの消去 17-9
デバイス クレデンシャルとステータスの表示 17-9

デバイスとクレデンシャル機能の各フィールドの説明 17-11
デバイスとクレデンシャルの [Contents] ペイン 17-11
デバイスとクレデンシャル機能のその他の関連資料 17-11
関連資料 17-12
標準 17-12
デバイスとクレデンシャル機能の履歴 17-12

CHAPTER 18 DCNM-LAN ライセンス デバイスの管理 18-1
DCNM-LAN ライセンス デバイスの概要 18-1
DCNM-LAN ライセンス デバイス管理のライセンス要件 18-2
DCNM-LAN ライセンス デバイス管理の前提条件 18-2
DCNM-LAN ライセンス デバイス管理の注意事項と制約事項 18-2
DCNM-LAN ライセンス デバイスの設定 18-2
ライセンス済みデバイス リストへのデバイスの追加 18-3
ライセンス済みデバイス リストからのデバイスの削除 18-3
DCNM-LAN ライセンス デバイスの表示 18-4
DCNM-LAN ライセンス デバイスのフィールドの説明 18-4
DCNM-LAN ライセンス デバイスの [Contents] ペイン 18-4
その他の関連資料 18-5
関連資料 18-5
標準 18-5
DCNM-LAN ライセンス デバイスの機能の履歴 18-6

CHAPTER 19 トポロジの作業 19-1
トポロジの概要 19-1
マップのビュー 19-2
レイアウト 19-5
vPC のサポート 19-6
DCNM-SAN のサポート 19-6
FabricPath のサポート 19-7
デバイス グループ 19-7
ネットワーク サーバ 19-7
トポロジのライセンス要件 19-8
トポロジ機能の前提条件 19-8
注意事項と制限 19-8
トポロジ機能の使用方法 19-8
トポロジ マップを開く 19-9
デバイス アイコンとリンクの説明 19-10

表示ツールの使用 19-11
[Details] ペインの表示、非表示、使用 19-12
トポロジ マップ上のデバイスの移動 19-13
レイアウトのロード 19-14
以前保存したレイアウトの再ロード 19-15
仮想シャーシまたは物理シャーシの表示 19-16
ネットワーク サーバの表示または非表示 19-16
ネットワーク サーバの管理 19-16
デバイス グループの表示または非表示 19-17
デバイス グループの展開と折りたたみ 19-18
デバイス グループの作成 19-18
デバイス グループ間でのデバイスの移動 19-19
デバイス グループからのデバイスの削除 19-20
実行コンフィギュレーションのスタートアップ コンフィギュレーションへのコピー 19-20
デバイス グループの削除 19-21
JPG イメージでのトポロジのエクスポート 19-22
トポロジ マップからの DCNM-LAN 機能へのアクセス 19-22
トポロジ マップからの Cisco DCNM-SAN 機能へのアクセス 19-23
トポロジ マップからの Cisco FabricPath 機能へのアクセス 19-24
vPC ウィザードの起動 19-27
vPC の管理 19-28
vPC 設定の不一致の検索と解決 19-28
トポロジ マップからのリモート接続された CNA へのアクセス 19-29
VSAN オーバーレイの使用方法 19-29
関連資料 19-30
トポロジの機能履歴 19-30

CHAPTER 20 ネットワーク サーバの設定 20-1
ネットワーク サーバの概要 20-1
アダプタとサーバの自動関連付け 20-2
アダプタとサーバの手動関連付け 20-2
ネットワーク サーバのライセンス要件 20-2
ネットワーク サーバの前提条件 20-3
ネットワーク サーバに関する注意事項および制約事項 20-3
ネットワーク サーバの設定 20-3
デフォルトのサーバ クレデンシャルの設定 20-3
デフォルトのサーバ クレデンシャルの消去 20-4
サーバの一意なクレデンシャルの設定 20-5

サーバの一意なクレデンシャルの消去 20-6
サーバの関連付け 20-6
サーバとアダプタの自動関連付け 20-9
アダプタとサーバの手動バインド 20-10
アダプタとサーバのアンバインド 20-10
サーバ接続情報の表示 20-11
ネットワーク サーバのフィールドの説明 20-11
サーバのフィールドの説明 20-11
[Static Server-Adapter Mapping] のフィールドの説明 20-13
[Server Credentials] のフィールドの説明 20-13
その他の関連資料 20-14
関連資料 20-14
標準 20-15
ネットワーク サーバの機能の履歴 20-15

CHAPTER 21 デバイス グループの設定 21-1
デバイス グループの概要 21-1
デバイス グループのライセンス要件 21-2
デバイス グループの前提条件 21-2
デバイス グループの注意事項と制約事項 21-2
デバイス グループの設定 21-2
デバイス グループの作成 21-2
グループへのデバイスの追加 21-4
グループからのデバイスの削除 21-5
デバイス グループの削除 21-5
関連情報 21-6
デバイス グループのフィールドの説明 21-6
[Summary] ペイン 21-6
[Device Group]：[Details]：[Global Settings] セクション 21-7
[Device Group]：[Details]：[Membership Details] セクション 21-7
その他の関連資料 21-7
関連資料 21-7
標準 21-7
デバイス グループ機能の履歴 21-8

CHAPTER 22 クラスタ管理の作業 22-1
クラスタ管理の概要 22-1
クラスタ管理 22-1

クラスタ サーバ環境 22-2
マスター サーバ ロール 22-2
分散サーバ タスク 22-2
サーバ タスク分散におけるクラスタ変更の影響 22-3
クラスタ管理のライセンス要件 22-3
クラスタ管理の前提条件 22-4
クラスタ管理の注意事項と制約事項 22-4
サーバ情報の表示 22-4
クラスタ管理のフィールドの説明 22-4
[Summary] ペイン 22-5
[Server] : [Details] タブ 22-5
その他の関連資料 22-5
関連資料 22-6
標準 22-6
クラスタ管理機能の履歴 22-6

CHAPTER 23 デバイスとの自動同期化の管理 23-1
デバイスとの自動同期化の概要 23-1
イベント データの自動消去および手動消去 23-2
仮想化のサポート 23-2
デバイスとの自動同期化のライセンス要件 23-2
デバイスとの自動同期化の前提条件 23-2
デバイスとの自動同期化の注意事項と制約事項 23-3
デバイスとの自動同期化の設定 23-3
ポーラーの開始と停止 23-3
ポーリング間隔の設定 23-4
デバイスとの同期化 23-4
イベント データベースからのデータの削除 23-5
自動イベント消去のイネーブル化およびディセーブル化 23-6
自動イベント消去の設定 23-6
イベントをすぐに消去する 23-7
自動同期化ポーラーのステータスの表示 23-8
デバイスとの自動同期化のフィールドの説明 23-8
[Poller Setting] タブ 23-9
[Events Database Administration] タブ 23-9
その他の関連資料 23-10
関連資料 23-10
標準 23-11

デバイスとの自動同期化機能の履歴 23-11

CHAPTER 24 しきい値ルールの作業 24-1

しきい値ルールに関する情報 24-1
しきい値ルールの概要 24-1
しきい値ルールの例 24-2
しきい値ルールのライセンス要件 24-4
しきい値ルールの設定 24-4
しきい値ルールの作成 24-5
しきい値ルールの削除 24-7
しきい値ルールの編集 24-7
しきい値ルールの表示 24-7
しきい値ルールの図への適用 24-8
その他の関連資料 24-8
関連資料 24-8
標準 24-8
しきい値ルールの機能履歴 24-9

CHAPTER 25 統計データ収集の管理 25-1

統計データの収集の概要 25-1
統計データの自動的な消去または手動での消去 25-2
仮想化のサポート 25-2
統計データ収集機能のライセンス要件 25-2
統計データ収集の前提条件 25-2
統計データ収集の注意事項と制約事項 25-3
統計データ収集の設定 25-3
統計データ収集の開始と停止 25-3
統計図でのモードの使用方法 25-4
コレクションからの統計データの削除 25-5
コレクションの削除 25-5
統計データベースからのデータの削除 25-6
統計データの自動的な消去のイネーブル化とディセーブル化 25-6
統計データの自動的な消去の設定 25-7
すぐに統計データを消去する 25-8
統計データ コレクタのステータスの表示 25-9
統計データ収集機能のフィールドの説明 25-9
[Summary] ペイン 25-9
[Statistical Database Administration] タブ 25-10

その他の関連資料 25-11
関連資料 25-11
標準 25-11
統計データ収集の機能履歴 25-11

CHAPTER 26 ネットワーク分析の作業 26-1
ネットワーク分析の概要 26-1
ネットワーク分析のライセンス要件 26-2
ネットワーク分析の前提条件 26-2
ネットワーク分析に関する注意事項および制約事項 26-2
ネットワーク分析機能の使用方法 26-2
ネットワーク分析の使用方法 26-2
New Path Latency Session ウィザードの使用方法 26-4
セッション統計情報の表示 26-8
関連資料 26-8
ネットワーク分析の機能の履歴 26-8

CHAPTER 27 DCNM-LAN サーバ ログ設定の管理 27-1
DCNM-LAN サーバ ログ設定の管理の概要 27-1
ログ レベル 27-2
ログ ファイルとその存在場所 27-2
仮想化のサポート 27-2
DCNM-LAN サーバ ログ設定の管理のライセンス要件 27-2
DCNM-LAN サーバ ログ設定の管理に関する前提条件 27-2
DCNM-LAN サーバ ログ設定の管理に関する注意事項と制約事項 27-3
DCNM-LAN サーバ ログの設定 27-3
デフォルトのログ レベルの設定 27-3
機能またはサーバ コンポーネントの一意なログ レベルの設定 27-3
デフォルトのログ レベルを使用させるための機能またはサーバ コンポーネントの設定 27-4
DCNM-LAN サーバ ログ設定の表示 27-5
DCNM-LAN サーバ ログ設定のフィールドの説明 27-5
DCNM-LAN サーバ ログ設定の [Contents] ペイン 27-5
その他の関連資料 27-6
関連資料 27-6
標準 27-7
DCNM-LAN サーバ ログ設定の機能の履歴 27-7

CHAPTER 28 Cisco DCNM-LAN サーバの起動と停止 28-1
DCNM-LAN サーバの起動と停止の概要 28-1
Cisco DCNM-LAN サーバの起動と停止のライセンス要件 28-1
DCNM-LAN サーバの起動 28-1
単一の DCNM-LAN サーバの起動 28-2
DCNM-LAN サーバ クラスタの起動 28-3
DCNM-LAN サーバの停止 28-5
単一の DCNM-LAN サーバの停止 28-5
DCNM-LAN サーバ クラスタの停止 28-6
関連資料 28-8
DCNM-LAN サーバの起動と停止の機能の履歴 28-9

CHAPTER 29 Cisco DCNM-LAN データベースのメンテナンス 29-1
データベース メンテナンスの概要 29-1
データの自動消去および手動消去 29-1
データベースのバックアップ 29-2
データベースのクリーンアップ 29-2
データベースの復元 29-2
データベース メンテナンスのライセンス要件 29-3
データベース メンテナンスの前提条件 29-3
データベース メンテナンスの注意事項と制約事項 29-3
データベース メンテナンスの実行 29-4
DCNM-LAN データベースのバックアップ 29-4
DCNM-LAN データベースのクリーンアップ 29-5
バックアップ ファイルからの DCNM-LAN データベースの復元 29-7
その他の関連資料 29-9
関連資料 29-9
標準 29-10
DCNM-LAN データベース メンテナンス機能の履歴 29-10

CHAPTER 30 DCNM-LAN のトラブルシューティング 30-1
DCNM-LAN を使用するときのヒント 30-1
[Events] タブに表示されるイベント数がイベント ブラウザに表示されるイベント数よりも少ない 30-1
イベント ブラウザの円グラフの表示が小さな数値に関して不正確である 30-2
DCNM-LAN サーバの起動に関する問題 30-2
DCNM-LAN サーバを起動できない 30-3
DCNM-LAN データベースに関する問題 30-3

PostgreSQL データベースに関する問題 30-4
Oracle データベースに関する問題 30-5
DCNM-LAN クライアントに関する問題 30-6
サーバから DCNM-LAN クライアントをダウンロードできない 30-7
DCNM-LAN クライアントをインストールできない 30-7
DCNM-LAN クライアントを起動できない 30-8
DCNM-LAN クライアントにログインできない 30-9
クライアントと DCNM-LAN サーバとの接続が失われる 30-10
デバイス ディスカバリまたはデバイス スタータスに関する問題 30-11
デバイス管理に関する問題 30-12
トポロジに関する問題 30-12
デバイス OS 管理に関する問題 30-13
イベント ブラウジングに関する問題 30-13

PART 4 付録

APPENDIX A Cisco SAN-OS Release 3.2(1) 以前のリリースでの Fabric Manager の起動 A-1
Cisco SAN-OS Release 3.1(1) ～ 3.2(1) のシード スイッチの設定 A-1
Cisco SAN-OS Release 3.1(1) 以前のリリースのシード スイッチの設定 A-3

APPENDIX B Cisco Fabric Manager でサポートされない機能のリスト B-1

APPENDIX C インターフェイスの非動作原因コード C-1

APPENDIX D Cisco FabricWare の管理 D-1
ファイバ チャネル サポート D-1
ゾーン設定 D-2
セキュリティ D-2
イベント D-2
Fabric Manager を使用した Cisco FabricWare メッセージ送信 D-3

INDEX

新機能および変更された機能に関する情報

Cisco DCNM Release 5.2 以降は、Cisco Fabric Manager と Cisco Data Center Network Manager for LAN が、LAN 環境と SAN 環境の両方を管理できる Cisco Data Center Network Manager（DCNM）という 1 つの製品に統合されています。この製品統合の一環として、Cisco Fabric Manager という名前は Cisco DCNM for SAN に変更されました。

次の文書変更によって、統合された Cisco DCNM 製品がサポートされます。

- Cisco DCNM Release 5.2 に対応する Cisco DCNM 製品のマニュアルのタイトルが、Cisco DCNM for LAN に変更されました。
- Cisco DCNM Release 5.2 に対応する Cisco Fabric Manager 製品のマニュアルのタイトルが、Cisco DCNM for SAN に変更されました。
- Cisco DCNM for SAN 製品のマニュアルが、次の URL にある Cisco.com の Data Center Network Manager リスト ページで公開されました。
  http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

  この URL は、Cisco DCNM for LAN 製品マニュアルのリスト ページと同じです。
- Cisco DCNM Release 5.2 以前のソフトウェア リリースに対応する Cisco Fabric Manager のマニュアルは、Cisco Fabric Manager という名前を使用し続けており、次の URL にある現在の Cisco.com リスト ページで入手できます。
  http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html

  Cisco DCNM Release 5.2 以前のリリースの Cisco Fabric Manager ソフトウェアを使用する場合は、引き続き、Cisco Fabric Manager のマニュアルを使用する必要があります。
- DCNM-SAN という名前は、Cisco Data Center Network Manager のユーザ インターフェイスで、Cisco DCNM for SAN の代わりに使用されます。同様に、DCNM-LAN という名前は、ユーザ インターフェイスで、Cisco DCNM for LAN の代わりに使用されます。ユーザ インターフェイスと合わせるために、製品マニュアルでも DCNM-SAN および DCNM-LAN という名前を使用します。
- 次の新しい資料では、Cisco DCNM for LAN と DCNM for SAN の両方をサポートし、新しいライセンス モデル、新しいインストール手順、および Cisco DCNM の新機能を取り扱います。
  - 『*Cisco DCNM Installation and Licensing Guide*』
  - 『*Cisco DCNM Release Notes*』
- Cisco DCNM のマニュアルの全リストについては、「はじめに」の「関連資料」を参照してください。

Cisco MDS NX-OS Release 4.2(1) より、新機能に固有のコンフィギュレーション ガイドでソフトウェア設定に関する次の情報を入手できます。

- システム管理

- インターフェイス
- ファブリック
- Quality of Service
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいガイドの情報は、以前は『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーション ガイドは、Cisco.com に用意されており、MDS NX-OS Release 4.2（1）以前のすべてのソフトウェア リリース用に参照できます。各ガイドには、特定のリリースで導入された機能や使用可能な機能が記載されています。ご使用のスイッチにインストールされているソフトウェアに対応したコンフィギュレーション ガイドを選択して参照してください。

Cisco MDS NX-OS Release 4.2(x) に関する詳細については、『*Cisco MDS 9000 Family Release Notes*』を次のシスコ Web サイトから入手して参照してください。

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

このマニュアルについて

新しい『*Cisco Fabric Manager Fundamentals Configuration Guide*』の内容はこれまで『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』の「Part 1:Getting Started」、「Part 8: Network and Switch Monitoring」、および付録で説明されていました。

表 1 に、このガイドで追加および変更された機能を示します。

表 1　MDS NX-OS Release 5.0(0) で追加および変更された機能

機能	追加または変更された内容	変更されたリリース	参照先
サマリー ダッシュボード	ダッシュボード サマリー情報の表示	5.2(1a)	第 2 章「Cisco DCNM Web クライアント」
ホスト ダッシュボード	ホストおよび仮想ホスト情報の表示	5.2(1a)	第 2 章「Cisco DCNM Web クライアント」
FM と DCNM の統合	Fabric Manager とデータセンター ネットワークの統合	5.0(1)	第 5 章「Cisco DCNM-SAN クライアントの設定」
検索エンジン	Fabric manager Webclient の検索エンジン	5.0(1)	第 2 章「Cisco DCNM Web クライアント」
スイッチ コンフィギュレーション管理	Fabric Manager Webclient を使用したコンフィギュレーションのバックアップ	5.0(1)	第 2 章「Cisco DCNM Web クライアント」
SAN ヘルス アナライザ ツール	SAN のヘルス分析	5.0(1)	第 9 章「パフォーマンスのモニタリング」
ソフトウェア アップグレード ウィザードの強化	Software Install Wizard の使用方法	5.0(1)	第 10 章「ソフトウェア イメージ」
Web クライアント レポートの強化	レポート	5.0(1)	第 2 章「Cisco DCNM Web クライアント」
スコープ ディスカバリ	VSAN スコープ ディスカバリ	5.0(1)	第 5 章「Cisco DCNM-SAN クライアントの設定」

表 1　MDS NX-OS Release 5.0(0) で追加および変更された機能 （続き）

機能	追加または変更された内容	変更されたリリース	参照先
フェデレーション サーバ	サーバ フェデレーション	4.2(1)	第 3 章「Cisco DCNM-SAN サーバの設定」
Cisco Discovery Protocol - FM - DM の強化	Fabric Manager Client の起動	4.2(1)	第 5 章「Cisco DCNM-SAN クライアントの設定」
FM Web Client: レポート機能の強化	テンプレート別のカスタム レポートの表示。 テンプレート別のカスタム レポートの作成。	4.2(1)	第 2 章「Cisco DCNM Web クライアント」
Fabric Manager 起動パッド	起動パッドを使用した Fabric Manager Client の起動。	4.2(1)	第 5 章「Cisco DCNM-SAN クライアントの設定」
デバイス エイリアス名のデバイス説明への読み込み	説明へのエイリアス名の使用方法。	4.2(1)	第 5 章「Cisco DCNM-SAN クライアントの設定」
FM の履歴およびリアルタイム チャート	Fabric Manager を使用した統計の表示	4.2(1)	第 9 章「パフォーマンスのモニタリング」

はじめに

ここでは、『*Cisco DCNM Fundamentals 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。また、関連マニュアル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、マルチレイヤ ディレクタおよびファブリック スイッチの Cisco MDS 9000 ファミリの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

このマニュアルは、次の章で構成されています。

章	タイトル	説明
Part 1	Cisco Data Center Network Manager	Cisco DCNM にについて説明します。
第 1 章	「Cisco Data Center Network Manager の概要」	Cisco DCNM の基礎について概要を説明します。
第 2 章	「Cisco DCNM Web クライアント」	Cisco DCNM Web クライアントの GUI と機能について詳述します。
Part 2	Cisco DCNM for SAN	Cisco DCNM for SAN について説明します。
第 1 章	「Cisco DCNM Fundamentals 概要」	Cisco DCNM-SAN の概要を説明します。
第 3 章	「Cisco DCNM-SAN サーバの設定」	Cisco DCNM-SAN サーバの GUI と機能について詳述します。
第 4 章	「Cisco DCNM-SAN での認証の設定」	Cisco DCNM-SAN コンポーネントとファブリック スイッチ間での認証方法を説明します。
第 5 章	「Cisco DCNM-SAN クライアントの設定」	Cisco DCNM-SAN の GUI と機能について詳述します。
第 6 章	「Device Manager」	Device Manager の GUI と機能について詳述します。
第 7 章	「Performance Manager の設定」	Performance Manager アーキテクチャの概要を説明します。
第 8 章	「ネットワークのモニタリング」	ネットワークの監視について詳述します。

章	タイトル	説明
第 9 章	「パフォーマンスのモニタリング」	Performance Manager の使用方法について詳述します。
第 10 章	「ソフトウェア イメージ」	スイッチでのソフトウェアのインストールについて詳述します。
第 11 章	「管理ソフトウェアの FAQ」	Cisco Fabric Manager および Device Manager に関する主な FAQ について回答します。
Part 3	Cisco DCNM for LAN	Cisco DCNM for LAN について説明します。
第 12 章	「DCNM-LAN の概要」	Cisco Data Center Network Manager for LAN（DCNM-LAN）の使用を開始するために必要な作業の概要を説明します。
第 13 章	「Cisco DCNM-LAN クライアントのインストールおよび起動」	Cisco DCNM-LAN クライアントのインストールおよび設定の方法について説明します。
第 14 章	「Cisco DCNM-LAN クライアントの使用方法」	Cisco DCNM-LAN クライアントの概要および使用方法について説明します。
第 15 章	「DCNM-LAN 認証設定の管理」	Cisco DCNM-LAN サーバ ユーザ アカウントの管理方法について説明します。
第 16 章	「デバイス ディスカバリの管理」	デバイス ディスカバリ機能の使用方法について説明します。
第 17 章	「デバイスとクレデンシャルの管理」	デバイスとクレデンシャル機能の使用方法について説明します。
第 18 章	「DCNM-LAN ライセンス デバイスの管理」	DCNM-LAN ライセンス デバイス機能の使用方法について説明します。
第 19 章	「トポロジの作業」	トポロジ機能の使用方法について説明します。
第 20 章	「ネットワーク サーバの設定」	ネットワーク サーバ機能の使用方法について説明します。
第 21 章	「デバイス グループの設定」	デバイス グループ機能の使用方法について説明します。
第 22 章	「クラスタ管理の作業」	クラスタ管理機能の使用方法について説明します。
第 23 章	「デバイスとの自動同期化の管理」	デバイスとの自動同期化機能の使用方法について説明します。
第 24 章	「しきい値ルールの作業」	しきい値の規則を設定する方法について説明します。
第 25 章	「統計データ収集の管理」	統計データ収集の管理方法を説明します。
第 26 章	「ネットワーク分析の作業」	指定された 2 つのスイッチ間で遅延を追跡および監視する方法を説明します。
第 27 章	「DCNM-LAN サーバ ログ設定の管理」	Cisco DCNM-LAN サーバ ログの管理方法を説明します。
第 28 章	「Cisco DCNM-LAN サーバの起動と停止」	Cisco DCNM-LAN サーバの起動および停止方法を説明します。
第 29 章	「Cisco DCNM-LAN データベースのメンテナンス」	Cisco DCNM-LAN データベースのメンテナンス方法を説明します。
第 30 章	「DCNM-LAN のトラブルシューティング」	Cisco DCNM-LAN に関して発生する可能性がある問題の解決方法について説明します。

章	タイトル	説明
Part 4	付録	
付録 A	「Cisco SAN-OS Release 3.2(1) 以前のリリースでの Fabric Manager の起動」	Cisco SAN-OS Release 3.2(1) 以前で Fabric Manager Client を起動する手順について説明します。
付録 B	「Cisco Fabric Manager でサポートされない機能のリスト」	Cisco Fabric Manager または Device Manager によってサポートされない機能がリストにまとめられています。
付録 C	「インターフェイスの非動作原因コード」	インターフェイスが動作しているにもかかわらず、動作ステートが down の場合の非動作原因コードについて説明します。
付録 D	「Cisco FabricWare の管理」	ファイバ チャネル スイッチング サービスのパフォーマンスを最大限まで向上することができる MDS 9020 スイッチ上で実行される Cisco FabricWare ソフトウェア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*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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。

このマニュアルでは、次の省略名を使用します。

- Cisco Data Center Network Manager for SAN は DCNM-SAN とも表記されます。
- Cisco Data Center Network Manager for LAN は DCNM-LAN とも表記されます。

関連資料

ここでは、Cisco DCNM および Cisco DCNM が管理するプラットフォームに関するマニュアルについて説明します。

ここでは、次の内容について説明します。

- 「Cisco DCNM マニュアル」（P.lxiv）
- 「Cisco Nexus 1000V シリーズ スイッチのマニュアル」（P.lxv）
- 「Cisco Nexus 2000 シリーズ Fabric Extender マニュアル」（P.lxv）
- 「Cisco Nexus 3000 シリーズ スイッチのマニュアル」（P.lxv）
- 「Cisco Nexus 4000 シリーズ スイッチのマニュアル」（P.lxvi）
- 「Cisco Nexus 5000 シリーズ スイッチのマニュアル」（P.lxvi）
- 「Cisco Nexus 7000 シリーズ スイッチのマニュアル」（P.lxvi）

Cisco DCNM マニュアル

Cisco DCNM のマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Cisco DCNM のマニュアル セットには、次のドキュメントが含まれています。

リリース ノート

『*Cisco DCNM Release Notes, Release 5.x*』

インストールおよびライセンス

『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』

Cisco DCNM Fundamentals ガイド

『*Cisco DCNM Fundamentals ガイド、リリース 5.x*』

Cisco DCNM for LAN コンフィギュレーション ガイド

『*FabricPath Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Security Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Unicast Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
『*Virtual Device Context Quick Start, Cisco DCNM for LAN, Release 5.x*』
『*Web Services API Guide, Cisco DCNM for LAN, Release 5.x*』

Cisco DCNM for SAN コンフィギュレーション ガイド

『*System Management Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Interfaces Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Fabric Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Security Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*IP Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
『*SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 5.x*』
『*SME Configuration Guide, Cisco DCNM for SAN, Release 5.x*』

Cisco Nexus 1000V シリーズ スイッチのマニュアル

Cisco Nexus 1000V シリーズ スイッチ のマニュアルは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 2000 シリーズ Fabric Extender マニュアル

Cisco Nexus 2000 シリーズ Fabric Extender のマニュアルは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 シリーズ スイッチのマニュアル

Cisco Nexus 3000 シリーズ スイッチ のマニュアルは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 シリーズ スイッチのマニュアル

Cisco Nexus 4000 シリーズ スイッチ のマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 シリーズ スイッチのマニュアル

Cisco Nexus 5000 シリーズ スイッチ のマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 7000 シリーズ スイッチのマニュアル

Cisco Nexus 7000 シリーズ スイッチ のマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

その他の Cisco MDS 9000 関連マニュアル

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/doclocater.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*』

適合規格および安全に関する情報

- 『*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*』

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 ネットワーキング 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は、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。

Cisco Data Center Network Manager の概要

Cisco Data Center Network Manager（DCNM）は、シスコ ユニファイド ファブリック向けの管理システムです。データセンター ネットワーク インフラストラクチャのプロビジョニング、モニタリング、トラブルシューティングを可能にします。サービス レベル契約を満たすために必要な Quality of Service（QoS）について最適化できるように、統合型データセンターの可視化と制御を行う方法を提供します。

Cisco DCNM は、データセンター インフラストラクチャの総合的な稼動時間および信頼性を向上させ、それにより、ビジネスの継続性が向上します。また、データセンターにおけるルーティング、スイッチング、およびストレージの管理ニーズを満たす堅牢なフレームワークと包括的なフィーチャ セットも提供します。Cisco DCNM は、ユニファイド ファブリックのプロビジョニングを簡素化し、SAN コンポーネントおよび LAN コンポーネントを監視します。Cisco DCNM は、Cisco Nexus、Cisco MDS、および Cisco Unified Computing System の製品向けに、Web ベースの単一の管理コンソールによる高度な可視化および制御を提供します。

さらに、Cisco DCNM は、Cisco DCNM for SAN と Cisco DCNM for LAN の各コンポーネントのインストールを単一のインストーラでサポートしています。

次の文書変更によって、統合された Cisco DCNM 製品がサポートされます。

- Cisco DCNM Release 5.2 に対応する Cisco DCNM 製品のマニュアルのタイトルが、Cisco DCNM for LAN に変更されました。
- Cisco DCNM Release 5.2 に対応する Cisco Fabric Manager 製品のマニュアルのタイトルが、Cisco DCNM for SAN に変更されました。

Cisco DCNM for SAN と Cisco DCNM for LAN のすべての製品マニュアルは、Cisco.com 上の次の URL にある Data Center Network Manager のリスト ページに公開されています。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

PART 1

Cisco Data Center Network Manager

CHAPTER 1

Cisco DCNM Fundamentals 概要

この章では、Cisco DCNM-SAN のコンポーネントの概要について説明します。この章の内容は、次のとおりです。

- 「DCNM-SAN サーバ」（P.1-1）
- 「DCNM-SAN クライアントでの認証」（P.1-3）
- 「DCNM-SAN クライアント」（P.1-2）
- 「Device Manager」（P.1-2）
- 「DCNM-SAN Web クライアント」（P.1-2）
- 「Performance Manager」（P.1-3）
- 「Cisco Traffic Analyzer」（P.1-4）
- 「ネットワーク モニタリング」（P.1-4）
- 「パフォーマンス モニタリング」（P.1-4）

DCNM-SAN サーバ

Cisco DCNM-SAN サーバは高度な MDS モニタリング機能、トラブルシューティング機能、および設定機能を備えたプラットフォームです。Cisco DCNM-SAN サーバでは、一元的な MDS 管理サービスおよびパフォーマンス モニタリングが可能です。SNMP 操作を使用して、ファブリックの情報を効率的に収集できます。サーバ コンポーネントを含む Cisco DCNM-SAN ソフトウェアを使用するには、ワークステーションに約 60 MB のハードディスク スペースが必要です。Cisco DCNM-SAN サーバは、Windows 2000、Windows 2003、Windows 2008、Windows XP、Windows 7、Solaris 9 および 10、Red Hat Enterprise Linux AS Release 5 上で動作します。

Cisco DCNM-SAN サーバとして設定された各コンピュータは、複数のファイバ チャネル SAN ファブリックを監視できます。1 台の Cisco DCNM-SAN サーバに最大 16 台のクライアント（デフォルト）を同時に接続できます。Cisco DCNM-SAN サーバで監視されないファブリック内の MDS スイッチに、Cisco DCNM-SAN クライアントを直接接続することもできます。これにより、1 台のコンソールから任意の MDS デバイスを管理できます。

DCNM-SAN クライアント

Cisco DCNM-SAN クライアントは、Java および SNMP ベースのネットワーク ファブリックおよびデバイス管理ツールです。GUI を通じて、Cisco Nexus 5000 シリーズ スイッチ、Cisco MDS 9000 ファミリ スイッチやサードパーティ製スイッチ、ホスト、およびストレージ デバイスを含むネットワーク ファブリックをリアルタイムで表示できます。

Cisco DCNM-SAN クライアントには、Cisco MDS 9000 ファミリ スイッチおよび Cisco Nexus 5000 ファミリ スイッチの詳細な設定機能およびステータス モニタリング機能のほか、ファイバ チャネル トラブルシューティング ツールも用意されています。MDS 9000 ファミリ スイッチまたは Cisco Nexus 5000 シリーズ スイッチに対してこのヘルスおよび設定分析ツールを使用してファイバ チャネル ping および traceroute を実行できます。

Fabric Manager Release 4.1(1b) 以降では、アクセスできる機能が制限されたサーバ管理者ロールが追加されているので、マルチレベルのセキュリティ システムが利用できます。サーバ管理者の設定機能は FlexAttach の設定と関連データに制限されています。拡張モード オプションはネットワーク管理者専用で、セキュリティ、IVR、iSCSI、FICON を含む DCNM-SAN のあらゆる機能を利用できます。

Device Manager

Device Manager を使用すると、搭載されたスイッチング モジュール、スーパーバイザ モジュール、モジュールの各ポートのステータス、電源、およびファン アセンブリを含めて、Cisco MDS 9000 ファミリ スイッチ シャーシまたは Cisco Nexus 5000 シリーズ スイッチ シャーシをグラフィック表示できます。

DCNM-SAN の [Information] ペイン内のテーブルは、基本的に、Device Manager で表示されるダイアログボックスに対応しています。ただし、DCNM-SAN のテーブルには 1 つまたは複数のスイッチの値が表示されますが、Device Manager のダイアログボックスに表示されるのは 1 つのスイッチの値です。また、デバイス固有の設定の確認やトラブルシューティング用の情報は、FDCNM-SAN よりも Device Manager の方が詳細です。

Device Manager は、Device View と Summary View の 2 つのビューを提供します。Summary View では、スイッチのインターフェイスを監視できます。Device View では、次のようなスイッチ レベルの設定を実行できます。

- ファイバ チャネル インターフェイスの設定
- Fibre Channel over Ethernet（FCoE）の設定
- 複数の VSAN のゾーンの設定
- ポート、PortChannels、およびトランキングの管理
- スイッチへの SNMPv3 セキュリティ アクセスの管理
- スイッチへの CLI（コマンドライン インターフェイス）セキュリティ アクセスの管理
- アラーム、イベント、および通知の管理
- コンフィギュレーション ファイルおよびソフトウェア イメージの保存とコピー
- ハードウェア構成の表示
- シャーシ、モジュール、およびポートのステータスや統計情報の表示

DCNM-SAN Web クライアント

DCNM-SAN Web クライアントを使用すると、Web ブラウザを使用して離れた場所から Cisco MDS スイッチ イベント、パフォーマンス、およびインベントリを監視できます。

- **Performance Manager サマリー レポート**：Performance Manager サマリー レポートでは、ネットワーク パフォーマンスを詳細に表示できます。このレポートでは、スループットの平均とピークが表示され、詳細な統計を参照できるその他のパフォーマンス グラフやテーブルへのホットリンクが提供されています。Performance Manager によって監視されている相互接続すべてで表形式のレポートおよびグラフィック レポートを利用できます。
- **Performance Manager ドリル ダウン レポート**：Performance Manager では、日単位、週単位、および年単位で傾向を分析できます。インタラクティブなズーム機能を使用すると、特定の期間の分析結果を表示できます。レポートは Performance Manager を使用してデータを集計し、コレクタを開始した場合にだけ利用できます。
- **メンテナンス不要データベースの統計情報ストレージ**：Performance Manager のラウンドロビン データベースは長期間使用してもサイズが増大しないため、管理は不要です。事前定義した期間が経過すると、最も古いサンプルは平均（ロールアップ）され、保存されます。最高の精度を得るため、2 日分の生サンプルが保存されます。古いサンプルがロールアップされるごとに精度は向上していきます。

Performance Manager

DCNM-SAN の主な目的は、ネットワークの管理です。管理機能の中で重要なのは、ネットワーク パフォーマンス モニタリング機能です。Performance Manager はネットワーク デバイスの統計情報の履歴を収集し、ブラウザを使用してこの情報をグラフィック表示します。最近の統計情報は詳細が、古い統計情報はサマリーが表示されます。Performance Manager は Cisco Traffic Analyzer などの外部ツールとも統合されています。

Performance Manager には、3 つの処理ステージがあります。

- 定義：Flow Wizard でスイッチにフローをセットアップします。
- 収集：Web Server Performance Collection 画面で目的のファブリックに関する情報を収集します。
- 提示：DCNM-SAN Web サーバを通じて、収集したデータを表示する Web ページを生成します。

Performance Manager は ISL（スイッチ間リンク）、ホスト、ストレージ エレメント、および設定済みフローの統計情報を収集できます。フローの定義基準は、ホストからストレージ（またはストレージからホスト）のリンクです。Performance Manager は収集コンフィギュレーション ファイルに基づいて、ファブリックから統計情報を収集します。これらのファイルにより、Performance Manager が統計情報を収集する SAN エレメントおよび SAN リンクが決まります。この設定に基づいて、Performance Manager は適切なデバイス（スイッチ、ホスト、またはストレージ エレメント）と通信し、5 分間の規定時間内に適切な情報を収集します。

DCNM-SAN クライアントでの認証

管理者は DCNM-SAN クライアントを起動して、ファブリックの検出に使用されるシード スイッチを選択します。使用するユーザ名およびパスワードが DCNM-SAN サーバに渡され、シード スイッチの認証に使用されます。このユーザ名とパスワードが、認識されている SNMP ユーザ名およびパスワードと異なる場合、DCNM-SAN クライアントまたは DCNM-SAN サーバがスイッチに対する CLI セッションを開き（SSH または Telnet）、ユーザ名とパスワードのペアを再試行します。スイッチは、ローカル スイッチ認証データベースまたはリモート AAA サーバでユーザ名とパスワードを認識すると、DCNM-SAN クライアントと DCNM-SAN サーバで使用される一時的な SNMP ユーザ名を作成します。

Cisco Traffic Analyzer

Cisco Traffic Analyzer では、Web ブラウザ ユーザ インターフェイスを使用して SPAN のリアルタイム分析またはキャプチャされたトラフィックの分析を実行できます。1 つ以上の Port Analyzer Adapter によってカプセル化されたトラフィックは、Cisco Traffic Analyzer が実行されている 1 台のワークステーションを使用して同時に分析することができます。Cisco Traffic Analyzer は ntop をベースとしたパブリック ドメインのソフトウェアで、シスコのファイバ チャネル トラフィック分析機能によって強化されています。

Cisco Traffic Analyzer では、往復の応答時間、1 秒あたりの SCSI I/O、SCSI の読み取りまたはトラフィック スループットとフレーム カウント、SCSI セッション ステータス、および管理タスク情報が監視されます。ファイバ チャネルのフレーム サイズやネットワーク管理プロトコルに関する統計も利用できます。

ネットワーク モニタリング

DCNM-SAN には、広範囲な SAN 検出、トポロジ マッピング、および情報表示機能があります。DCNM-SAN は、接続先のスイッチに対して SNMP クエリーを実行し、ファブリック トポロジに関する情報を収集します。そしてファブリック トポロジを再作成し、カスタマイズ可能なマップに表示し、[fabric view]、[device view]、[summary view]、[operation view] など複数の表示オプションでインベントリおよび設定情報を提供します。

DCNM-SAN を起動すると、SAN 検出プロセスが開始されます。DCNM-SAN は、ネーム サーバ レジストレーション、Fibre Channel Generic Services（FC-GS）、Fabric Shortest Path First（FSPF）、SCSI-3 など、シード Cisco MDS 9000 ファミリ スイッチからポーリングした情報を使用して、1 つまたは複数のファブリック上のすべてのデバイスと相互接続を自動的に検出します。すべての使用可能なスイッチ、Host Bus Adapter（HBA）、およびストレージ デバイスが検出されます。Cisco MDS 9000 ファミリ スイッチは、Fabric Device Management Interface（FDMI）を使用して、ホストのエージェントを使用せずに、HBA のモデル、シリアル番号、ファームウェア バージョン、およびホスト オペレーティング システムのタイプおよびバージョンを検出します。DCNM-SAN は、各スイッチへの SNMP クエリーを通じてこの情報を収集します。検出されるデバイス情報は、デバイス名、ソフトウェア リビジョン レベル、ベンダー、ISL（スイッチ間リンク）、PortChannels、VSAN などです。

パフォーマンス モニタリング

DCNM-SAN および Device Manager には、ファブリック全体、SAN エレメント、および SAN リンクのパフォーマンスを監視する複数のツールが用意されています。ツールでは、リアルタイム統計やパフォーマンス モニタリング履歴などを利用できます。

リアルタイム パフォーマンス統計はファブリックのダイナミック トラブルシューティングや障害分離に便利です。リアルタイム統計では、ファブリックの一部についてユーザによって定義された期間のデータを収集し、結果を DCNM-SAN および Device Manager で表示します。

Device Manager には、Cisco MDS 9000 ファミリ スイッチのポートを簡単に監視できるツールが備えられています。このツールは設定された期間の統計を取得し、結果を表またはチャートで表示します。統計結果は、選択したポートのパフォーマンスをリアルタイムで表示し、パフォーマンス モニタリングおよびトラブルシューティングに利用できます。選択されたポートに対して、受信/送信トラフィック、エラー、クラス 2 トラフィック、および FICON データなどの任意の数の統計を監視することができます。ポーリングは 10 秒 ～ 1 時間の間隔で設定でき、選択したオプションの数だけ結果を表示できます。結果は絶対値、1 秒あたりの値、1 秒あたりの最小値と最大値などから選択できます。

CHAPTER 2

Cisco DCNM Web クライアント

この章では、パフォーマンスやインベントリなど、Web ブラウザを使用して離れた場所からモニタできる Cisco MDS 9000 ファミリ スイッチおよび Cisco Nexus 5000 シリーズ スイッチのさまざまなイベントについて説明します。

この章の内容は、次のとおりです。

- 「Cisco DCNM Web クライアントの概要」（P.2-1）
- 「ヘルス情報の表示」（P.2-8）
- 「パフォーマンス情報の表示」（P.2-10）
- 「インベントリ情報の表示」（P.2-19）
- 「カスタム レポートの表示および作成」（P.2-24）
- 「DCNM Web クライアントの管理」（P.2-30）
- 「Cisco DCNM-SAN Web 検索エンジン」（P.2-43）
- 「DCNM Web クライアントを使用したバックアップの設定」（P.2-44）
- 「ホストおよび仮想ホスト情報の表示」（P.2-47）
- 「ダッシュボード サマリー情報の表示」（P.2-49）

Cisco DCNM Web クライアントの概要

DCNM Web クライアントを使用すると、Cisco MDS 9000 ファミリ、Cisco Nexus 7000 シリーズ、または Cisco Nexus 5000 シリーズ スイッチのイベント、パフォーマンス、およびインベントリをモニタし、管理作業を簡単にすることができます。

DCNM Web クライアントには、次の機能があります。

- サマリー ダッシュボード：サマリー ダッシュボードでは、インベントリ、ヘルス、日常のパフォーマンス、上位ホスト、上位ストレージ、フェデレーション、およびトポロジを別個のウィンドウですばやく表示できます。また、トラフィックの変動を視覚的にすることでファブリックのリアルタイム モニタリングを可能にし、ベースライン トラフィック パターンを確立するのに役立ちます。ダッシュボードをダブルクリックすると、特定のウィンドウが拡大し、個々のネットワーク コンポーネントをより詳細に表示できます。また、ダッシュボードには、パフォーマンス チャート、インベントリ情報、イベント、および仮想マシンと VMware ESX の使用率情報など、仮想環境の管理に必要なすべての情報が表示されます。

- ホスト ダッシュボード：ホスト ダッシュボードでは、検出されたすべての SAN ホストおよび仮想ホストに関連するすべての情報を確認できます。ホスト ダッシュボードには、仮想ホストの上位に設定された個々のホストおよび仮想マシンに関する I/O トラフィック、ディスク レイテンシ、CPU、メモリの統計情報、トポロジ、およびイベントなど、ネットワークに関連する非常に詳細な情報が表示されます。ホスト ダッシュボードは、次の 4 つのパネルで構成されます。
  - [Host] パネル：SAN ホストと仮想ホストの情報を示します。
  - [Chart] パネル：個々のホストまたは仮想マシンに関する I/O 統計情報、CPU とメモリの情報、およびディスク レイテンシを示します。
  - [Topology] パネル：ホスト エンクロージャとストレージ エンクロージャ間のエンドツーエンドのトポロジ レイアウトおよびパス情報を示します。仮想マシン トポロジには、ファブリックを介した仮想マシンから物理ホスト、およびストレージ アレイへの依存関係がすべて表示され、パス属性の詳細表示にも簡単にアクセスできます。
  - [Event] パネル：特定のホスト ラックに設定されたすべてのスイッチ ポートのイベント情報を示します。
- サマリー レポートおよびドリル ダウン レポート：Performance Manager サマリー レポートでは、ネットワーク パフォーマンスを詳細に表示できます。このレポートでは、スループットの平均とピークが表示され、詳細な統計を参照できるその他のパフォーマンス グラフやテーブルへのホットリンクが提供されています。Performance Manager によって監視されている相互接続すべてで表形式のレポートおよびグラフィック レポートを利用できます。また、日単位、週単位、月単位、および年単位で傾向を分析できます。インタラクティブなズーム機能を使用すると、特定の期間の分析結果を表示できます。レポートは Performance Manager を使用してデータを集計し、コレクタを開始した場合にだけ利用できます。履歴パフォーマンス レポートを表示するには、Adobe Flash Player 10 以降をインストールしてください。
- メンテナンス不要の統計情報ストレージ：Performance Manager のラウンドロビン データベースは長期間使用してもサイズが増加しないため、管理は不要です。事前定義した期間が経過すると、最も古いサンプルは平均（ロールアップ）され、保存されます。最高の精度を得るため、2 日分の生サンプルが保存されます。古いサンプルのグループがまとめてロールアップされるにつれ、解像度は徐々に低下します。

ここでは、次の内容について説明します。

- 「Cisco DCNM-SAN クライアントのダウンロード」（P.2-2）
- 「DCNM Web クライアントの起動」（P.2-3）
- 「DCNM Web クライアントのナビゲーション」（P.2-4）
- 「DCNM Web クライアントでの SSL の使用方法」（P.2-5）

Cisco DCNM-SAN クライアントのダウンロード

Cisco DCNM-SAN クライアントを起動するには、DCNM Web クライアントを使用する必要があります。

手順の詳細

Cisco DCNM-SAN クライアントを起動する手順は、次のとおりです。

ステップ 1　DCNM Web クライアントにログインします。

ステップ 2　右上の隅から、[Download] を選択します。

ステップ 3　[Cisco DCNM-SAN client] のリンクをクリックします。

Cisco DCNM-SAN クライアントを初めて起動するときは、Cisco DCNM-SAN のショートカットを作成するかどうかを尋ねるメッセージが表示されます。

ステップ 4　Cisco DCNM-SAN のショートカットを作成する場合は、[Yes] をクリックします。

（注）　このメッセージが表示されるのは、Cisco DCNM-SAN クライアントの初回起動時のみです。

DCNM Web クライアントの起動

DCNM Web クライアントを使用してスイッチをモニタする前に、接続に使用したサーバ上でサービスを開始する必要があります。DCNM Web クライアントがインストールされたワークステーションと同じワークステーションに、ブラウザがなくてもかまいません。

手順の詳細

Cisco DCNM クライアントを起動する手順は、次のとおりです。

ステップ 1　DCNM Web クライアントがインストールされたワークステーションと同じワークステーションで作業している場合は、ブラウザを開き、[Location] フィールドに **http://localhost:***PORT* と入力します。インストール中に別のポートを指定した場合は、ポート番号を入力します。デフォルトでポート 80 を使用した場合は、ポート番号を省略できます。

Cisco DCNM Web クライアントをインストールしたワークステーションとは異なるワークステーションで作業する場合は、ブラウザを開き、[Location] フィールドに http://<*yourServerAddress*>:*PORT* と入力します。ここで、<*yourServerAddress*> は Cisco DCNM Web クライアントをインストールしたアドレス、*PORT* はデフォルトで 80 です。インストール中に別のポートを指定した場合は、ポート番号を入力します。

ヒント　[Start] > [Control Panel] > [Administrative Tools] > [Services] の順に選択して、DCNM Web クライアントが起動していることを確認します。Cisco DCNM Web クライアントを起動するには、ブラウザを使用してサービスのロケーションに移動します。

また、Cisco DCNM Web クライアントの [Admin] > [Status] メニューを使用して、この情報を表示することもできます。

UNIX ワークステーションで、次のコマンドを使用します。

```
$ /usr/local/cisco_mds9000/bin/FMWebClient.sh status
```

[DCNM Web Client Login] ダイアログボックスが表示されます。下部のテキスト フィールドに、ログイン先のサーバから [Message of the Day] が表示されます。

ステップ 2　ユーザ名およびパスワードを入力します。

ステップ 3　[Login] をクリックします。

（注）　新しく Cisco DCNM-SAN をインストールした場合、デフォルトのユーザ ID とパスワードは admin/password です。Cisco DCNM-SAN サーバの初回の使用時にパスワードを変更することを推奨します。新しくインストールしたのでなければ、既存のパスワードのいずれかを使用できます。

[DCNM Web Client] ウィンドウが表示されます。

（注）　Firefox を使用して DCNM Web クライアントにアクセスする場合は、Web サイトのセキュリティ証明書に問題があることを示す警告メッセージが表示される場合があります。この問題を解決するには、セキュリティ例外を追加してください。

セキュリティ例外を追加する手順は、次のとおりです。

ステップ 1　警告ページで [Or you can add an exception] をクリックします。

ステップ 2　[Add Exception] をクリックします。

[Add Security Exception] ダイアログが表示されます。

ステップ 3　[Get Certificate] をクリックします。

このサイトで発生している問題が表示されるので、確認します。

ステップ 4　[Confirm Security Exception] をクリックします。

DCNM Web クライアントのナビゲーション

DCNM Web クライアントのほとんどの画面は一定のナビゲーション規則で標準化されています。

ナビゲーション ツリー

左側のペインのフィルタ ナビゲーション ツリーを使用して、目的の領域にアクセスできます。

- [SAN] を選択すると、SAN 内のすべてのファブリックおよび VSAN に関する情報が表示されます。これを実行すると、テーブルの最初のカラムとして、[Fabric] カラムが追加されます。
- ファブリック フォルダをクリックすると、その特定のファブリックに関する情報が表示されます。
- 一部の画面でファブリック フォルダを展開すると（フォルダの前の [+] または [-] アイコンをクリック）、そのファブリック内の VSAN のリストが表示されます。[VSAN] を選択すると、その VSAN の情報が表示されます。

タブからアクセスできる機能の有効範囲は、フィルタ ツリーで選択された範囲に限定されます。

テーブルのフィルタリングとナビゲーション

いくつかのテーブルの表示をフィルタリングして、情報の一部を表示することができます。これらのテーブルの右上には、1 つまたは複数のドロップダウン リストがあります。これらのリストの項目を選択して、[Filter] をクリックすると、テーブル内のその項目に関する情報がフィルタリングされます。

各ページに表示される行数を変更するには、テーブルの左下にある [Rows per page] ドロップダウン リストで数を選択します。数を選択すると、新しい行数でテーブルがアップデートされます（ボタンをクリックする必要はありません）。

複数の情報ページからなるテーブルの場合は、次のことが可能です。

- [first page] アイコンまたは [last page] アイコン（前にバーのついた矢印）をクリックすると、テーブルの最初のページまたは最後のページに移動できます。
- [next page] アイコンまたは [previous page] アイコン（矢印）をクリックすると、次のページや前のページに移動できます。
- [Go to page] フィールドにページ番号を入力して [Go] ボタンをクリックすると、特定のページに移動できます。

テーブル カラムの見出しの隣に黒いアイコンがある場合は、テーブル内の特定のカラムで情報を検索できます。アイコンをクリックすると、[Search] ダイアログボックスが表示されます。

印刷

一部のテーブルには、右下の隅に [Print] アイコンがあります。このアイコンをクリックすると、印刷に適した形式でテーブルが表示されます。ブラウザからページを印刷できます。

ファイルのエクスポート

一部のテーブルには、右下の隅に [Export] アイコンがあります。このアイコンをクリックすると、Microsoft Excel などのプログラムで読み取り可能な CSV ファイルにデータをエクスポートできます。

カラムのソート

一部の画面では、カラムの見出しをクリックすると、そのカラムの情報がソートされます。

DCNM Web クライアントでの SSL の使用方法

DCNM Web クライアントはデフォルトで TCP ポート 80 を使用します。SSL 認証をインストールし、（TCP ポート 443 または別のカスタム ポートを使用して）HTTPS を介して DCNM Web クライアントを使用する場合は、セキュア接続を受け入れる外部 IP アドレスごとに証明書が必要です。これらの証明書は、既知の認証局（CA）から購入できます。

SSL をイネーブルにするには、自己署名証明書か、または VeriSign のような信頼できる第三者企業からの証明書を使用するためのキーストアを設定する必要があります。

手順の詳細

ローカル証明書を作成する手順は、次のとおりです。

ステップ 1　自己署名証明書（ローカル証明書）を使用するためのキーストアを設定します。コマンド ラインから、次のコマンドを実行します。

```
%JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\Program
Files\Cisco Systems\MDS 9000\keystore"
```

ステップ 2　自分の名前、組織、都道府県、国を入力します。キーストア パスワードを求めるプロンプトが表示されたら、**changeit** を入力します。自分自身のパスワード使用したい場合は、必ず、server.xml ファイルの keystorePass 属性を変更してください。キー パスワードを求めるプロンプトが表示されたら、**Enter** キーを押すか、またはキーストア パスワードと同じパスワードを使用します。

（注）　これで、次のセクションの手順を実行すれば、SSL を使用するように DCNM Web クライアントを変更できます。

任意の認証局から証明書を取得するには、Certificate Signing Request（CSR; 証明書署名要求）を作成する必要があります。認証局は、CSR を使用して、Web サイトを安全であると識別する証明書を作成します。

手順の詳細

CSR の作成手順は、次のとおりです。

ステップ 1　ローカル証明書を作成します（前のセクションを参照）。

（注）　作業証明書を作成するためには、氏名のフィールドに Web サイトのドメインを入力する必要があります。

ステップ 2　次のコマンドで CSR が作成されます。

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore "C:\Program
Files\Cisco Systems\MDS 9000\keystore"
```

これで、certreq.csr という名前のファイルができました。このファイルは PEM 形式で符号化されています。これを認証局に提出します。ファイルの提出方法は、認証局の Web サイトで調べることができます。提出すると、証明書を受け取ることができます。

ステップ 3　証明書を取得したら、それをローカル キーストアにインポートします。まず、チェーン証明書またはルート証明書をキーストアにインポートします。その後、自分の証明書をインポートできます。

ステップ 4　証明書を取得した認証局からチェーン証明書をダウンロードします。

- Verisign.com の商用証明書の場合は、次のサイトにアクセスします。
  http://www.verisign.com/support/install/intermediate.html
- Verisign.com の試用証明書の場合は、次のサイトにアクセスします。
  http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html
- Trustcenter.de の場合は、次のサイトにアクセスします。
  http://www.trustcenter.de/certservices/cacerts/en/en.htm#server
- Thawte.com の場合は、次のサイトにアクセスします。
  http://www.thawte.com/certs/trustmap.html
- 次のコマンドを実行して、チェーン証明書をキーストアにインポートします。
  keytool -import -alias root -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore" -trustcacerts -file *filename_of_the_chain_certificate*
- 新しい証明書を X509 形式でインポートします。

keytool -import -alias tomcat -keystore "C:\Program Files\Cisco Systems\MDS 9000\keystore" -trustcacerts -file *your_certificate_filename*

SSL を使用するように DCNM Web クライアントを変更する手順は、次のとおりです。

ステップ 1　DCNM Web クライアントをすでに起動している場合は停止します。Fabric Manager Web Client が Windows にインストールされている場合に、このサービスを停止するには、[Administrative Tools] の [Windows Services] を使用します。

ステップ 2　テキスト エディタを使用して、DCNM Web クライアントがインストールされているディレクトリから、**\jboss\server\default\deploy\jboss-web.deployer\server.xml** を開きます。著作権情報の直後に、次の行が表示されます。

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
           port="80" minProcessors="5" maxProcessors="75"
           enableLookups="false" redirectPort="8443"
           acceptCount="10" debug="0" connectionTimeout="60000"/>
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
           port="8443" minProcessors="5" maxProcessors="75"
           enableLookups="true"
           acceptCount="10" debug="0" scheme="https" secure="true">
  <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
           clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

ステップ 3　最初の <Connector> エレメントをコメント化し、2 番目のエレメントをアンコメントします。ポートが 8443 から 443 に変わり、キーストアとキーパスが追加されます。ファイルは、次の例のようになります。

```
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
           port="80" minProcessors="5" maxProcessors="75"
           enableLookups="false" redirectPort="8443"
           acceptCount="10" debug="0" connectionTimeout="60000"/>
-->
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.catalina.connector.http.HttpConnector"
           port="443" minProcessors="5" maxProcessors="75"
           enableLookups="true"
           acceptCount="10" debug="0" scheme="https" secure="true">
  <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
           clientAuth="false" protocol="TLS"
           keystoreFile="C:\Program Files\Cisco Systems\MDS 9000\keystore"
           keystorePass="changeit"/>
</Connector>
```

ステップ 4　このファイルを保存します。

ステップ 5　DCNM Web クライアントを再起動します。

（注）　SSL がイネーブルの Cisco DCNM-SAN サーバを再起動する場合は、DCNM Web クライアントを再起動する必要があります。SSL がディセーブルの Cisco DCNM-SAN サーバを停止して再起動する場合は、DCNM Web クライアントを再起動する必要があります。

ホスト情報の表示

ホスト ダッシュボードには、トポロジ、イベント、および SAN トラフィックなど、選択したホストの詳細が表示されます。この情報を CSV 形式で ASCII ファイルにエクスポートし、Microsoft Excel などのアプリケーションで読み取ることができます。表の左上にある [Filter] ドロップダウン リストを使用して、検索できます。

ヘルス情報の表示

[Health] メニューには、選択された項目に関するイベントおよび問題点のうち、各ユーザ セッションに共通のものが表示されます。[Health] メニューには、次のサブ メニューがあります。

- [Summary] ：すべての SAN、または選択された SAN、ファブリック、またはスイッチに関するイベントおよび問題のサマリーを表示します。いずれかのブルー リンクをクリックすると、該当項目の詳細を表示できます。
- [Accounting] : アカウンティング イベントのリストを示します。
- [Events] : ファブリック イベントの詳細リストを示します。これらのイベントは、イベントのファブリック範囲、日付、およびタイプ別にフィルタリングできます。
- [Syslog] : システム メッセージの詳細なリストを表示します。これらのイベントは、イベントの重大度、日付、およびタイプ別にフィルタリングできます。
- [Syslog Archives] : システム メッセージのアーカイブ リストを示します。

ここでは、次の内容について説明します。

- 「アカウンティング情報の表示」（P.2-8）
- 「イベント情報の表示」（P.2-9）
- 「Syslog 情報の表示」（P.2-9）
- 「Syslog アーカイブ情報の表示」（P.2-9）

アカウンティング情報の表示

手順の詳細

アカウンティング情報を表示するには、次の手順を実行します。

ステップ 1　メニュー バーで、[Health] > [Accounting] の順に選択します。

[Accounting] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、スイッチのいずれかをクリックすると、そのスイッチのアカウンティング情報が表示されます。

イベント情報の表示

手順の詳細

イベントとハードウェアまたはアカウンティングの詳細リストを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Health] > [Events] の順に選択します。

[Events] ウィンドウが表示されます。

ステップ 2　ファブリックを展開すると、そのファブリックのイベント情報が表示されます。

Syslog 情報の表示

手順の詳細

システム メッセージの詳細リストを表示するには、次の手順を実行します。

ステップ 1　メニュー バーで、[Health] > [Syslog] の順に選択します。

Syslog テーブルが表示されます。

ステップ 2　ファブリックのいずれかを選択すると、そのファブリックの Syslog 情報のテーブルが表示されます。

ステップ 3　ファブリックを展開し、スイッチのいずれかをクリックすると、そのスイッチの Syslog 情報が表示されます。

ステップ 4　ファブリックを選択し、そのファブリックの 1 つまたは複数のスイッチにシステム メッセージがあると、[Files] カラムに [Events]、[Hardware]、[Accounting]、および [Link Incidents] が表示されます。これらのメッセージ タイプのいずれかをクリックすると、そのファブリック内のスイッチのシステム メッセージが、クリックしたメッセージ タイプでフィルタリングされ、表示されます。

（注）　システム メッセージを並べ替えるには、ウィンドウの右上の隅にある [filter] アイコンをクリックし、メッセージ タイプと間隔を選択して、[Filter] をクリックします。

Syslog アーカイブ情報の表示

手順の詳細

Syslog アーカイブの詳細リストを表示するには、次の手順を実行します。

ステップ 1　メニュー バーで、[Health] > [Syslog Archives] の順に選択します。

[Syslog Archives] ペインが表示されます。

ステップ 2　ファブリックのいずれかを選択すると、そのファブリックの Syslog アーカイブ情報のテーブルが表示されます。

ステップ 3　ファブリックを展開し、スイッチのいずれかを選択すると、そのスイッチの Syslog アーカイブ情報が表示されます。

ステップ 4　ファブリックを選択すると、[Files] カラムにスイッチ名、登録情報、およびリンク インシデントが表示されます。

（注）　MDS 設定の変更を表示するには、[Files] から accountingX.log を選択します。Device Manager を使用してスイッチの設定変更を表示するには、[Logs] > [DCNM-SAN Server] > [Accounting] > [Current] の順に選択します。

パフォーマンス情報の表示

[Performance] オプションには、SAN コンポーネントの平均スループットおよびリンク使用率の概要が表示されます。スループットおよび利用率が円グラフで表示されます。円グラフをクリックすると、データがテーブル形式で表示されます。これらのテーブル内のブルー リンクをクリックすると、該当するデータのグラフが適宜表示されます。画面右上にある [Filter] ドロップダウン リストを使用すると、さまざまな期間を基準としてデータをフィルタリングすることができます。

[Performance] メニューには、次のサブ メニューがあります。

- [Switch]：CPU、メモリ、および帯域幅の情報を表示します。
- [End Devices]：エンド デバイス（ホストまたはストレージ）、ポート トラフィック、およびエラーの詳細なリストを表示します。
- [ISLs]：ISL（スイッチ間リンク）のトラフィックおよびエラーの詳細を表示します。
- [NPV Links]：NPV デバイスとポートのトラフィックに関する詳細なリストを表示します。
- [Flows]：ホストからストレージへのトラフィックの詳細を表示します。
- [Ethernet]：ギガビット イーサネット ポートと Cisco Nexus 5000 シリーズ イーサネット ポート チャネルの詳細なリストを表示します。
- [Others]：その他の統計情報の詳細なリストを表示します。
- [Switch Bandwidth]：スイッチの総帯域幅を表示します。

ここでは、次の内容について説明します。

- 「スイッチ CPU 情報の表示」（P.2-11）
- 「スイッチ メモリ情報の表示」（P.2-11）
- 「スイッチの帯域幅とエラー情報の表示」（P.2-12）
- 「ISL トラフィックとエラー情報の表示」（P.2-12）
- 「すべてのポートに関するパフォーマンス情報の表示」（P.2-13）

- 「ホスト ポートに関するパフォーマンス情報の表示」（P.2-13）
- 「ストレージ ポートに関するパフォーマンス情報の表示」（P.2-13）
- 「ホスト ラックに関するパフォーマンス情報の表示」（P.2-14）
- 「ストレージ ラックに関するパフォーマンス情報の表示」（P.2-14）
- 「ポート グループに関するパフォーマンス情報の表示」（P.2-14）
- 「ISL のパフォーマンス情報の表示」（P.2-15）
- 「NPV リンクのパフォーマンス情報の表示」（P.2-16）
- 「フローのパフォーマンス情報の表示」（P.2-16）
- 「ギガビット イーサネットとイーサネット ポートに関するパフォーマンス情報の表示」（P.2-18）
- 「その他の統計情報の表示」（P.2-18）

スイッチ CPU 情報の表示

手順の詳細

スイッチ CPU 情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Switch] > [CPU] の順に選択します。

[CPU] ペインが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

スイッチ メモリ情報の表示

手順の詳細

スイッチ メモリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Switch] > [Memory] の順に選択します。

メモリ ペインが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのメモリ情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

スイッチの帯域幅とエラー情報の表示

手順の詳細

スイッチの帯域幅とエラー情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Switch] > [Bandwidth] の順に選択します。

メモリ ペインが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスの帯域幅情報が表示されます。

ISL トラフィックとエラー情報の表示

手順の詳細

ISL トラフィックとエラー情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [ISLs] の順に選択します。

メモリ ペインが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスの ISL 情報が表示されます。

[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ISL トラフィック情報ウィンドウが表示されます。

（注）　データ グリッドの脚注 NaN（Not a Number）は負の値ではないことを示します。

（注）　ほかにもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行して ISL の詳細情報を表示することもできます。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダ コントロールをドラッグして、表示する期間を指定します。
- グリッド形式で情報を表示するには、右下の [grid] アイコンをクリックします。
- データをスプレッドシートにエクスポートするには、グリッド形式を選択してから、[export to excel] リンクをクリックします。

- リアルタイム情報を表示するには、右上の隅のドロップダウン リストから [Real Time] を選択します。リアルタイム データは 10 秒ごとに更新されます。

すべてのポートに関するパフォーマンス情報の表示

手順の詳細

すべてのポート上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [All Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのすべてのポートに関するパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ホスト ポートに関するパフォーマンス情報の表示

手順の詳細

すべてのポート上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [Host Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのすべてのポートに関するパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ストレージ ポートに関するパフォーマンス情報の表示

手順の詳細

ストレージ ポート上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [Storage Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのストレージ ポートに関するパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ホスト ラックに関するパフォーマンス情報の表示

手順の詳細

ホスト ラック上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [Host Enclosure] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのホスト ラックに関するパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ストレージ ラックに関するパフォーマンス情報の表示

手順の詳細

ストレージ ラック上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [Storage Enclosure] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのストレージ ラックに関するパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間にそのデバイスを通過したトラフィックを示すグラフを表示します。

ポート グループに関するパフォーマンス情報の表示

手順の詳細

ストレージ ラック上のトラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [End Devices] > [Port Groups] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のエンド デバイスのポート グループに関するパフォーマンス情報が表示されます。

ステップ 3　ポート グループの名前をクリックして、そのポート グループのメンバーを表示します。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、エンド デバイスの詳細な情報を表示するのに次のことが可能です。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダ コントロールをドラッグして、表示する期間を指定します。
- グリッド形式で情報を表示するには、右下の [grid] アイコンをクリックします。
- スプレッドシートにデータをエクスポートするには、右上の隅の [excel] アイコンをクリックしてから [Save] をクリックします。
- リアルタイム情報を表示するには、右上の隅のドロップダウン リストから [Real Time] を選択します。リアルタイム データは 10 秒ごとに更新されます。

ISL のパフォーマンス情報の表示

手順の詳細

ISL トラフィックとエラーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [ISLs] の順に選択します。

[ISLs] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN の ISL のパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムのアイコンをクリックし、過去 24 時間にその ISL を通過したトラフィックを示すグラフを表示します。

NPV リンクのパフォーマンス情報の表示

手順の詳細

NPV デバイスとポート間のトラフィックを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [ISLs] の順に選択します。

[NPV Links] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN の NPV リンクのパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間のトラフィックのリストを表示します。

（注）　ほかにもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行して NPV リンクの詳細情報を表示することもできます。

- この情報の時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダ コントロールをドラッグして、表示する期間を指定します。
- グリッド形式で情報を表示するには、右下の隅の [grid] アイコンをクリックします。
- スプレッドシートにデータをエクスポートするには、右上の隅の [excel] アイコンをクリックしてから [Save] をクリックします。
- リアルタイム情報を表示するには、右上の隅のドロップダウン リストから [Real Time] を選択します。リアルタイム データは 10 秒ごとに更新されます。

フローのパフォーマンス情報の表示

手順の詳細

ホストとストレージ トラフィックを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Flows] の順に選択します。

[Flows] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のフローのパフォーマンス情報が表示されます。

ステップ 3　[Name] カラムの [chart] アイコンをクリックし、過去 24 時間のトラフィックのリストを表示します。

（注）　ほかにもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行してフローの詳細情報を表示することもできます。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダ コントロールをドラッグして、表示する期間を指定します。
- グリッド形式で情報を表示するには、右下の [grid] アイコンをクリックします。
- スプレッドシートにデータをエクスポートするには、右上の隅の [excel] アイコンをクリックしてから [Save] をクリックします。
- リアルタイム情報を表示するには、右上の隅のドロップダウン リストから [Real Time] を選択します。リアルタイム データは 10 秒ごとに更新されます。

ギガビット イーサネットとイーサネット ポートに関するパフォーマンス情報の表示

手順の詳細

ギガビット イーサネット ポートと、Cisco Nexus 5000 シリーズ イーサネット ポートおよびイーサネット ポートチャネルを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Ethernet] の順に選択します。

[Ethernet] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のギガビット イーサネット ポートと、Cisco Nexus 5000 シリーズ イーサネット ポートおよびポートチャネルが表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行することもできます。

- 時間範囲を選択して [Filter] をクリックすると、表示がフィルタリングされます。
- [Name] カラムからギガビット イーサネット ポート名を選択すると、過去 24 時間にそのギガビット イーサネット ポートを通過したトラフィックを示すグラフが表示されます。時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。

その他の統計情報の表示

手順の詳細

その他の統計情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Performance] > [Others] の順に選択します。

[Others] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN のその他の統計情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、次のことが可能です。

- 時間範囲を選択して [Filter] をクリックすると、表示がフィルタリングされます。
- [Name] カラムのスイッチの IP アドレスをクリックすると、過去 24 時間にそのスイッチを通過したトラフィックを示すグラフが表示されます。時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。

（注）　[Other Statistics] を設定するには、「その他の統計情報の設定」（P.2-43）の手順に従います。

インベントリ情報の表示

[Inventory] メニューには、選択した SAN、ファブリック、またはスイッチのインベントリが表示されます。この情報を CSV 形式で ASCII ファイルにエクスポートし、Microsoft Excel などのアプリケーションで読み取ることができます。行数およびカラム数はページ単位で設定できます。

[Inventory] メニューには、次のサブメニューがあります。

- [VSANs]：VSAN の詳細を表示します。
- [Switches]：スイッチの詳細を表示します。
- [Licenses]：そのファブリックで使用されているライセンスについての詳細を表示します。
- [Modules]：MDS スイッチング モジュールとサービス モジュール、ファン、および電源装置を表示します。
- [End Devices]：ホストおよびストレージ ポートを表示します。
- [ISLs]：ISL を表示します。
- [NPV Links]：NPV デバイスとポート間のリンクを表示します。
- [Active Zones]：標準ゾーンと IVR ゾーンを表示します。

ここでは、次の内容について説明します。

- 「VSAN のインベントリ情報の表示」（P.2-19）
- 「スイッチのインベントリ情報の表示」（P.2-20）
- 「ライセンス情報の表示」（P.2-20）
- 「モジュールのインベントリ情報の表示」（P.2-21）
- 「エンド デバイスにあるすべてのポートのインベントリ情報の表示」（P.2-21）
- 「エンド デバイスにあるホスト ポートのインベントリ情報の表示」（P.2-22）
- 「エンド デバイスにあるストレージ ポートのインベントリ情報の表示」（P.2-22）
- 「ISL の詳細情報の表示」（P.2-23）
- 「NPV リンクのインベントリ情報の表示」（P.2-23）
- 「標準ゾーンに関するインベントリ情報の表示」（P.2-23）
- 「IVR ゾーンに関するインベントリ情報の表示」（P.2-24）

VSAN のインベントリ情報の表示

手順の詳細

VSAN の詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [VSANs] の順に選択します。

[VSAN] ウィンドウが表示されます。

ステップ 2　ファブリックのいずれかを選択すると、そのファブリックの VSAN コンポーネント情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、次のことが可能です。

- ステータス レベルを選択して、[Filter] をクリックすると、すべての VSAN またはエラーのある VSAN だけを表示するようにフィルタリングされます。

スイッチのインベントリ情報の表示

手順の詳細

スイッチに関するインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [Swithces] の順に選択します。

[Switches] ウィンドウが表示されます。

ステップ 2　次のいずれか 1 つの処理を実行します。

- [SAN] を選択すると、その SAN のすべてのファブリックのスイッチ インベントリ情報が表示されます。
- ファブリックのいずれかを選択すると、そのファブリックのスイッチ コンポーネント情報が表示されます。
- ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のスイッチ コンポーネント情報が表示されます。

（注）　(u-a-t) はそれぞれ、ファイバ チャネル ポートの使用数（u）、利用可能数（a）、および合計（t）を示します。

ライセンス情報の表示

手順の詳細

スイッチに関するライセンス情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [Licenses] の順に選択します。

[Switch Licenses] ウィンドウが表示されます。

ステップ 2　ファブリックのいずれかを選択すると、そのファブリック内のスイッチのライセンス情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、次のことが可能です。

- ステータス レベルを選択して、[Filter] をクリックすると、すべてのライセンスまたはエラーのあるライセンスだけを表示するようにフィルタリングされます。

モジュールのインベントリ情報の表示

手順の詳細

モジュールの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [Modules] の順に選択します。

[Modules] ウィンドウが表示されます。

ステップ 2　次のどちらかを実行します。

- [SAN] を選択すると、その SAN のすべてのファブリックのモジュール インベントリ情報が表示されます。
- ファブリックのいずれかを選択すると、そのファブリックのモジュール コンポーネント情報が表示されます。
- ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のモジュール コンポーネント情報が表示されます。

エンド デバイスにあるすべてのポートのインベントリ情報の表示

手順の詳細

エンド デバイスの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [End Devices] > [All Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のエンド デバイス コンポーネント情報が表示されます。

（注）　ホストまたはラックでフィルタリングする場合は、結果テーブルでホストをクリックすれば、ホスト ラック パフォーマンス、ホストのリスト、デバイスの接続先ホストのリスト、および接続パスが表示されます。これによって、ホストおよびラックのパフォーマンス統計情報を見ることができます。

また、エンド デバイスやポート グループでフィルタリングすると、ピーク使用率や平均使用率など、それらのポート グループの集約情報を表示できます。

エンド デバイスにあるホスト ポートのインベントリ情報の表示

手順の詳細

エンド デバイスにあるホスト ポートのインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [End Devices] > [Host Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のエンド デバイス コンポーネント情報が表示されます。

（注）　ホストまたはラックでフィルタリングする場合は、結果テーブルでホストをクリックすれば、ホスト ラック パフォーマンス、ホストのリスト、デバイスの接続先ホストのリスト、および接続パスが表示されます。これによって、ホストおよびラックのパフォーマンス統計情報を見ることができます。

また、エンド デバイスやポート グループでフィルタリングすると、ピーク使用率や平均使用率など、それらのポート グループの集約情報を表示できます。

エンド デバイスにあるストレージ ポートのインベントリ情報の表示

手順の詳細

ストレージの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [End Devices] > [Storage Ports] の順に選択します。

[End Devices] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のエンド デバイス コンポーネント情報が表示されます。

（注）　ホストまたはラックでフィルタリングする場合は、結果テーブルでホストをクリックすれば、ホスト ラック パフォーマンス、ホストのリスト、デバイスの接続先ホストのリスト、および接続パスが表示されます。これによって、ホストおよびラックのパフォーマンス統計情報を見ることができます。

また、エンド デバイスやポート グループでフィルタリングすると、ピーク使用率や平均使用率など、それらのポート グループの集約情報を表示できます。

ISL の詳細情報の表示

手順の詳細

ISL の詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [ISLs] の順に選択します。

[ISLs] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN の ISL コンポーネント情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行することもできます。

- ステータス レベルを選択して、[Filter] をクリックすると、すべての ISL またはエラーのある ISL だけを表示するようにフィルタリングされます。

NPV リンクのインベントリ情報の表示

手順の詳細

NPV リンクの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [NPV Links] の順に選択します。

[NPV Links] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかを選択すると、その VSAN の NPV リンク情報が表示されます。

標準ゾーンに関するインベントリ情報の表示

手順の詳細

標準ゾーンの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [Active Zones] > [Regular Zones] の順に選択します。

[Regular Zones] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のゾーン コンポーネント情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、次のことが可能です。

- ステータス レベルを選択して、[Filter] をクリックすると、すべてのゾーンまたはエラーのあるゾーンだけを表示するようにフィルタリングされます。

IVR ゾーンに関するインベントリ情報の表示

手順の詳細

IVR ゾーンの詳細なインベントリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Inventory] > [Active Zones] > [IVR Zones] の順に選択します。

[IVR Zones] ウィンドウが表示されます。

ステップ 2　ファブリックを展開し、VSAN のいずれかをクリックすると、その VSAN のゾーン コンポーネント情報が表示されます。

（注）　ほかにもいくつかの方法で情報を表示できます。基本的な手順の他に、次のことが可能です。

- ステータス レベルを選択して、[Filter] をクリックすると、すべてのゾーンまたはエラーのあるゾーンだけを表示するようにフィルタリングされます。

カスタム レポートの表示および作成

[Reports] メニューでは、Cisco DCNM-SAN が収集した履歴パフォーマンス、イベント、およびインベントリの情報に基づいてカスタマイズされたレポートを作成できます。サマリー表示と詳細表示の集約レポートを作成できます。また、以前保存したレポートを表示することもできます。

[Report] メニューには、次のサブ メニューがあります。

- [View]：以前保存されたレポートを表示します。
- [Generate]：選択されたレポート テンプレートに基づくカスタム レポートを生成します。
- [Custom]：カスタム レポート テンプレートを作成します。イベント、パフォーマンス カテゴリ、インベントリの任意の組み合わせを選択できます。
- [Jobs]：選択されたレポート テンプレートに基づいてスケジューリングされたジョブを表示します。

ここでは、次の内容について説明します。

- 「カスタム レポート テンプレートの作成」（P.2-25）
- 「テンプレート別のカスタム レポートの表示」（P.2-27）
- 「ユーザ別のカスタム レポートの表示」（P.2-27）

- 「レポート テンプレートの削除」（P.2-27）
- 「テンプレート別のカスタム レポートの作成」（P.2-28）
- 「カスタム レポート テンプレートの修正」（P.2-29）
- 「カスタム レポートの削除」（P.2-29）
- 「レポート テンプレート別のスケジュール済みジョブの表示」（P.2-30）

カスタム レポート テンプレートの作成

Cisco DCNM-SAN によって取得される情報のすべてまたは任意のサブセットからカスタム レポートを作成できます。レポートに取り込みたいイベント、パフォーマンス、およびコンポーネントの統計情報を選択することによってレポートを作成し、対象とする SAN、ファブリック、または VSAN を設定してテンプレートの範囲を制限します。このテンプレートに基づいて、すぐに、またはあとで、ファブリックのレポートの生成や、スケジュール作成を実行できます。DCNM Web クライアントは、使用するレポート テンプレートとレポート作成時間に基づいて各レポートを保存します。

Cisco MDS NX-OS Release 5.0 より、以前のバージョンの制限を解消するためにレポート テンプレート設計が変更されました。新しい設計モデルでは、単一ページで追加機能、削除機能、および変更機能を実行できます。新しいナビゲーション システムでは複数のファブリックや VSAN を選択でき、将来的に新しい品目やカテゴリを追加するための拡張性に優れています。

新しい設計モデルには、次の 3 つのパネルがあります。

- [Customs] パネル
- [Configuration] パネル
- [User Selection] パネル

[Customs] パネルでは、新規テンプレートの追加、既存テンプレートの変更、および既存テンプレートの削除を行えます。

[Configuration] パネルでは、新規テンプレートを追加するときに設定したり、既存テンプレートを変更したりすることができます。[Configuration] パネル内のオプションは、新規テンプレートを追加するか、既存テンプレートを選択するまでディセーブルになります。[Configuration] パネルの上部には、選択して設定できる多数のカテゴリがあります。

[User Selection] パネルには、設定オプションがリアル タイムで表示されます。[Configuration] パネルには一度に 1 つのカテゴリに関する情報しか表示できませんが、[User Selection] パネルにはすべての選択または設定を表示できます。

手順の詳細

カスタム レポート テンプレートを作成する手順は、次のとおりです。

ステップ 1　メニュー バーで [Report] > [Configuration] の順に選択します。

[Report Configuration] ウィンドウが表示されます。

ステップ 2　[Customs] パネルの [CLICK TO ADD NEW CUSTOM] をクリックして、レポートの名前を新しく作成します。

ステップ 3　[Configuration] パネルの [Scope] をクリックして、範囲を定義します。

ステップ 4　[Configuration] パネルの [Health]、[Performance]、および [Inventory] などの各カテゴリに移動して、レポート内の必要な情報を表示します。

ステップ 5　（任意）イベントの重大度、コンポーネント情報のステータス、またはパフォーマンス情報およびコンポーネント情報のエンド デバイス タイプを選択します。

ステップ 6　[Save] をクリックして、このレポート テンプレートを保存します。

テンプレート別のカスタム レポートの表示

手順の詳細

特定のテンプレートに基づいたカスタム レポートを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Reports] > [View] の順に選択します。
レポート テーブル ウィンドウが表示されます。

ステップ 2　左側のペインで [Templates] を展開します。

ステップ 3　表示するレポートを選択します。レポート テーブル内のレポートをクリックすると、メイン画面または新しいブラウザ ウィンドウにレポートを表示できます。

ステップ 4　特定のレポートを削除するには、チェックボックスをオンにして [Remove] をクリックします。

ステップ 5　すべてのレポートを削除するには、ヘッダーにあるチェックボックスをオンにして [Remove] をクリックします。

ユーザ別のカスタム レポートの表示

手順の詳細

特定のユーザに基づいたカスタム レポートを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Reports] > [View] の順に選択します。
レポート テーブル ウィンドウが表示されます。

ステップ 2　左側ペインで [Users] をクリックして展開します。

ステップ 3　ユーザ名をダブルクリックします。

ステップ 4　表示するレポートを選択します。レポート テーブル内のレポートをクリックすると、メイン画面または新しいブラウザ ウィンドウにレポートを表示できます。

ステップ 5　特定のレポートを削除するには、チェックボックスをオンにして [Remove] をクリックします。

ステップ 6　すべてのレポートを削除するには、ヘッダーにあるチェックボックスをオンにして [Remove] をクリックします。

レポート テンプレートの削除

手順の詳細

カスタム レポートを削除する手順は、次のとおりです。

ステップ 1　[Template] パネルで、削除するレポート テンプレートをクリックして選択します。

ステップ 2　[Template] パネルの右下の隅にあるごみ箱まで、選択したレポート テンプレートをドラッグします。

ステップ 3　[Yes] をクリックしてテンプレートを削除します。

テンプレート別のカスタム レポートの作成

選択したテンプレートに基づいてレポートを生成したり、指定時間に実行するようにレポートのスケジュールを作成できます。

手順の詳細

レポートを生成する、またはレポートをスケジュールする手順は、次のとおりです。

ステップ 1　レポートの対象とする SAN、ファブリック、または VSAN を選択します。

ステップ 2　メニュー バーで、[Reports] > [Generate] の順に選択します。

[Generate Custom Report] ウィンドウが表示されます。

ステップ 3　[Available] ドロップダウン リストからレポート テンプレートを選択します。

ステップ 4　（任意）レポート名を変更します。デフォルトでは、レポート名は生成された日時に基づいて決まります。

ステップ 5　（任意）[Report is only visible to the Owner] チェックボックスをオンにして、レポートの属性を変更します。このチェックボックスをオンにすると、特定のユーザとネットワーク管理者だけがレポートを表示できます。

ステップ 6　（任意）[Export to CSV] チェックボックスをオンにして、レポートをテキストでエクスポートします。

ステップ 7　（任意）[Email Report] オプションで、次のいずれかのアクションを実行します。

- 電子メール通知を受信しない場合は、[No] を選択します。
- 電子メールでリンクを受信する場合は、[Link Only] を選択します。
- 電子メール通知を受信する場合は、[Contents] を選択します。

ステップ 8　[Create] をクリックし、このテンプレートに基づいたレポートを作成します。

新しいブラウザ ウィンドウにレポートの結果が表示されます。または、[Report] > [View] をクリックし、ナビゲーション ペインで使用したレポート テンプレートからレポートの名前を選択する方法でもレポートを表示できます。

ステップ 9　[Schedule] をクリックし、このテンプレートに基づいたレポートのスケジュールを作成します。スケジュール パネルが表示されます。

[Generate Custom Report] ウィンドウが表示されます。

ステップ 10　スケジュール パネルで、スケジュール実行時間およびレポートの実行頻度を指定します。

ステップ 11　[Start Date] または [End Date] の隣にあるカレンダーをクリックして、日付を修正します。

ステップ 12　[Start Time] または [End Time] ドロップダウン リストを選択して時刻を修正します。

ステップ 13　レポートを生成する頻度を選択します。

ステップ 14　[Job Name] フィールドにレポート名を入力し、[Create] をクリックしてレポートを保存します。

[Jobs] ページにスケジュール済みのレポートが表示されますが、スケジュールされたジョブは、実行されると [Scheduled Job] テーブルから削除されます。

（注）　[End Date] には [Start Date] より 5 分以上前の時刻を指定します。

カスタム レポート テンプレートの修正

手順の詳細

カスタム レポート テンプレートを編集する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Reports] > [Configuration] の順に選択します。

[Customs]、[Configuration]、および [User Selection] の各パネルが表示されます。

ステップ 2　[Customs] パネルのレポートをダブルクリックして選択します。

このレポートの現在の情報が [Configuration] パネルに表示されます。

ステップ 3　[Configuration] パネルで [Health]、[Performance]、および [Inventory] の各タブをクリックして、レポートに収集する情報を指定します。

ステップ 4　（任意）イベントの重大度、コンポーネント情報のステータス、またはパフォーマンス情報およびコンポーネント情報のエンド デバイス タイプを選択します。

ステップ 5　[Save] をクリックして、このレポート テンプレートを保存します。

（注）　レポートの対象とする SAN、ファブリック、VSAN は変更できません。新しい SAN、ファブリック、または VSAN のレポートを新たに生成してください。

カスタム レポートの削除

前提条件

生成したレポートは、DCNM Web クライアントによって保存されます。カスタム レポートを削除するにはまず、削除するレポートを選択します。

手順の詳細

特定のユーザに基づいたカスタム レポートを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Reports] > [View] の順に選択します。

ステップ 2　左側のペインで、[By User] を展開します。

ステップ 3　ユーザ名をダブルクリックします。

ステップ 4　右側のペインで、削除するレポートを選択し、[Remove] をクリックします。

レポート テンプレート別のスケジュール済みジョブの表示

手順の詳細

レポート テンプレート別のスケジュール済みジョブを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Reports] > [Jobs] の順に選択します。

スケジュール済みジョブ テーブル ウィンドウが表示されます。

ステップ 2　左のナビゲーション ペインでレポート テンプレートをクリックすると、選択されたテンプレートに基づくスケジュール済みジョブが表示されます。

DCNM Web クライアントの管理

[Admin] オプションを使用すると、Cisco DCNM-SAN サーバ上で簡単な管理作業および設定作業を実行し、Web クライアントにデータを送信できます。

[Admin] オプションには、次のサブメニューがあります。

- [Status]：ご使用のサーバ上の Database Server のステータスを表示し、Performance Collector サービスを開始および停止できるようにします。サービスの再起動が必要となるのは、何らかの機能が適切に機能していない場合、または大量のシステム リソースが消費されている場合だけです。

（注）　DCNM Web クライアントを使用して Database Server のサービスを開始または停止することはできません。Microsoft Windows オペレーティング システムを使用している場合は、Database Server の停止、開始、再開に Microsoft Management Console を使用します。

- [Logs]：Cisco DCNM-SAN サーバで実行している各サービスのログをすべて表示できます。
- [Data Sources]：ファブリック、LAN、VM Ware などのデータ ソースをすべて表示できます。
- [Clients]：Cisco DCNM-SAN サーバに接続しているクライアントをすべて表示できます。
- [Server Properties]：サーバ プロパティの config ファイルに定義されているフィールドをすべて表示できます。
- [SFTP Credentials]：SFTP クレデンシャルを表示できます。

（注）　データベース ログにデータベース ファイル ロック エラーが含まれている場合に、このエラーを修正するには、Web クライアントを使用してデータベース サーバをシャットダウンしてから、再起動します。

（注）　DCNM Web クライアントの Admin オプションにアクセスできるのは、ネットワーク管理者だけです。ネットワーク オペレータは Admin オプションを表示できません。

ここでは、次の内容について説明します。

- 「サービスの開始、再開、停止」（P.2-31）
- 「管理対象のファブリックの追加、編集、削除」（P.2-31）

- 「LAN の追加、編集、および削除」（P.2-33）
- 「VMWare Server の追加、編集、および削除」（P.2-34）
- 「VMWare Server の再検出」（P.2-35）
- 「AAA プロパティの設定」（P.2-38）
- 「コミュニティの追加と削除」（P.2-35）
- 「ロールの追加と削除」（P.2-39）
- 「Cisco DCNM-SAN サーバのプロパティの設定」（P.2-36）
- 「ユーザの追加と削除」（P.2-38）
- 「トラップおよび Syslog 登録情報の表示」（P.2-37）
- 「パフォーマンス収集の作成、編集、および削除」（P.2-40）
- 「その他の統計情報の設定」（P.2-43）
- 「収集しきい値の設定」（P.2-42）
- 「RRD 統計インデックスのインポート」（P.2-42）
- 「Cisco DCNM-SAN Web 検索エンジン」（P.2-43）
- 「Cisco DCNM-SAN Web 検索エンジン」（P.2-43）

サービスの開始、再開、停止

手順の詳細

サービスを開始、再開、または停止する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Status] の順に選択します。
サーバごとのサービスとそれぞれのステータスを示すテーブルが表示されます。

ステップ 2　開始、再開、または停止を実行したいサービスを選択します。

ステップ 3　[Start] または [Stop] をクリックします。
選択されたサービスが開始、再開、または停止されます。

管理対象のファブリックの追加、編集、削除

DCNM Web クライアントは、Cisco DCNM-SAN に通知されているファブリックについて、Cisco DCNM-SAN によって取得された情報をレポートします。

手順の詳細

DCNM Web クライアントからのファブリックの管理を開始する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

[Opened] カラムに、Cisco DCNM-SAN が管理しているファブリック（存在する場合）のリストが表示されます。

ステップ 2　[Add] をクリックします。

[Add Fabric] ダイアログボックスが表示されます。

ステップ 3　このファブリックのシード スイッチ IP アドレスを入力します。

ステップ 4　ファブリックのユーザ名とパスワードを入力します。

ステップ 5　（任意）[SNMPV3] チェックボックスをオンにします。SNMPV3 をオンにすると、[Read Community] と [Write Community] のフィールドが [User Name] と [Password] に変わります。ユーザ名およびパスワードを入力する必要があります。

ステップ 6　[Auth-Privacy] ドロップダウン リストからプライバシー設定を選択します。

ステップ 7　[Add] をクリックすると、このファブリックの管理が開始されます。

手順の詳細

DCNM Web クライアントからファブリックを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　削除するファブリックの隣のチェックボックスをオンにして [Remove] をクリックすると、そのファブリックのデータ収集が停止します。

手順の詳細

DCNM Web クライアントからファブリックを編集する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　編集するファブリックの隣のチェックボックスをオンにして、[Edit] をクリックします。

[Edit Fabric] ダイアログボックスが表示されます。

ステップ 3　新しいファブリック名、ユーザ名とパスワード、プライバシーを入力し、いずれかのステータス オプションを選択することで、DCNM Web クライアントでファブリックを管理する方法を指定します。

ステップ 4　（任意）[SNMPV3] チェックボックスをオンにします。SNMPV3 をオンにすると、[Community] フィールドが [User Name] および [Password] に変わります。ユーザ名およびパスワードを入力する必要があります。

ステップ 5　[Apply] をクリックして、変更内容を保存します。

（注）　一度に編集できるファブリックは 1 つだけです。

LAN の追加、編集、および削除

手順の詳細

DCNM Web クライアントからファブリックの管理を開始する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

Cisco DCNM-SAN によって管理されている LAN（存在する場合）のリストがテーブルに表示されます。

ステップ 2　[Add] をクリックします。

[Add LAN CDP Seed] ダイアログボックスが表示されます。

ステップ 3　CDP シード スイッチ IP アドレスを入力します。

ステップ 4　（任意）[SNMPV3] チェックボックスをオンにします。SNMPV3 をオンにすると、[Community] フィールドが [User Name] および [Password] に変わります。ユーザ名およびパスワードを入力する必要があります。

ステップ 5　この LAN のユーザ名とパスワードを入力します。

ステップ 6　[Add] をクリックすると、この LAN の管理が開始されます。

手順の詳細

DCNM Web クライアントから LAN を削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　削除する LAN の隣のチェックボックスをオンにして [Remove] をクリックし、その LAN のデータ収集を停止します。

手順の詳細

DCNM Web クライアントから LAN を編集する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　編集する LAN の隣のチェックボックスをオンにして、[Edit] をクリックします。

[Edit LAN CDP Seed] ダイアログボックスが表示されます。

ステップ 3　新しい LAN 名、ユーザ名とパスワード、プライバシーを入力し、いずれかのステータス オプションを選択することで、DCNM Web クライアントでファブリックを管理する方法を指定します。

ステップ 4　[Apply] をクリックして、変更内容を保存します。

VMWare Server の追加、編集、および削除

DCNM Web クライアントは、Cisco DCNM-SAN によってサポートされている VMWare Server について Cisco DCNM-SAN が収集した情報をレポートします。

手順の詳細

DCNM Web クライアントから VMWare Server の管理を開始する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

Cisco DCNM-SAN によって管理されている VMWare Server（存在する場合）のリストがテーブルに表示されます。

ステップ 2　[Add] をクリックします。

[Add VMWare] ダイアログボックスが表示されます。

ステップ 3　この VMWare Server のシード スイッチ IP アドレスを入力します。

ステップ 4　この VMWare Server のユーザ名とパスワードを入力します。

ステップ 5　[Add] をクリックすると、この VMWare Server の管理が開始されます。

手順の詳細

Cisco DCNM-SAN から VMWare Server を削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　削除する VMWare Server の隣のチェックボックスをオンにして [Remove] をクリックし、その VMWare のデータ収集を停止します。

手順の詳細

DCNM Web クライアントから VMWare を編集する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　編集する VMWare の隣のチェックボックスをオンにして、[Edit] をクリックします。

[Edit VMWare] ダイアログボックスが表示されます。

ステップ 3　新しい VMWare 名、ユーザ名とパスワード、プライバシーを入力し、いずれかのステータス オプションを選択することで、DCNM Web クライアントでファブリックを管理する方法を指定します。

ステップ 4　[Apply] をクリックして、変更内容を保存します。

VMWare Server の再検出

手順の詳細

VMWare を再検出する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　再検出する VMWare の隣のチェックボックスをオンにします。

ステップ 3　[Rediscover] をクリックします。

コミュニティの追加と削除

DCNM Web クライアントを使用してコミュニティの追加や削除を実行できます。

手順の詳細

コミュニティ ファブリックを追加する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　[Communities] パネルの [Add] をクリックします。

[Add Community] ダイアログボックスが表示されます。

ステップ 3　[IP Mask/Address] フィールドに、コミュニティの IP マスクまたはアドレスを入力します。

（注）　IP マスクにワイルドカード（0）を使用して、コミュニティをサブネットに割り当てることもできます。

ステップ 4　[Community] フィールドにコミュニティ名を入力します。

ステップ 5　[Add] をクリックして、コミュニティを追加します。

コミュニティを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Data Sources] の順に選択します。

ステップ 2　[Communities] パネルの [Remove] をクリックします。

ステップ 3　削除するコミュニティの隣のチェックボックスをオンにして、[Remove] をクリックします。

（注）　Cisco Fabric Manager Release 3.0(1) では、Cisco MDS 9020 スイッチまたはサードパーティ製デバイスを使用していても、communities.properties ファイルを変更する必要はありません。

ログ情報の表示

DCNM Web クライアント ログのようなログを表示する必要が生じる場合もあります。しかし、これらのプロセスには、ログ ファイルの情報を表示できる GUI はありません。エラーを調べる場合は、表示できるようにこれら 2 つのファイルを保存してください。

手順の詳細

ログ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [Logs] の順に選択します。

左のカラムに表示可能なログのリストが表示されます。

ステップ 2　表示するログ ファイルをクリックします。

Cisco DCNM-SAN サーバのプロパティの設定

Cisco DCNM-SAN サーバのプロパティを設定するには、メニューから [Admin] > [General] > [Server Properties] の順に選択します。画面の指示に従います。

SFTP クレデンシャルの設定

手順の詳細

SFTP クレデンシャルを設定する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [General] > [SFTP] の順に選択します。

[SFTP credentials] ページが表示されます。

ステップ 2　[SFTP Username] フィールドに、ユーザ名を入力します。

ステップ 3　[SFTP Password] フィールドにパスワードを入力します。

ステップ 4　[Root Directory] フィールドにルート ディレクトリ パスを入力します。

ステップ 5　[Verification Switch] フィールドからスイッチを選択します。

ステップ 6　[Apply] をクリックして、設定を適用します。

ステップ 7　[Apply] および [Verify] をクリックして設定を適用し、確認します。

トラップおよび Syslog 登録情報の表示

手順の詳細

DCNM Web クライアントからトラップおよび Syslog 登場情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Events] > [Registration] の順に選択します。

ステップ 2　ファブリックを選択すると、そのファブリックの登録情報が表示されます。

選択したファブリックの登録情報を示す [Registration] 画面が表示されます。

ステップ 3　（任意）情報をコピーする場合は、[Print] アイコンまたは [Export Report] アイコンをクリックします。

イベント通知転送の設定

手順の詳細

DCNM Web クライアントを使用して、システム メッセージの通知転送の追加および削除を実行できます。

（注）　DCNM Web クライアントは、ファブリック イベントを電子メールまたは SNMPv1 トラップで転送します。

通知転送を追加する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Events] > [Forwarding] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Notification] ダイアログボックスが表示されます。

ステップ 3　[Forwarding Method] で、[E-Mail] または [Trap] を選択します。[SNMP Trap] を選択した場合は、ダイアログボックスに [Port] フィールドが追加されます。

ステップ 4　[Address] フィールドに IP アドレスを入力します。

ステップ 5　[Scope] ドロップダウン リストから、通知用のファブリックを選択します。

ステップ 6　[VSAN Scope] で [All] または [List] を選択します。

ステップ 7　[Event Type] ドロップダウン リストから

ステップ 8　[Storage Ports Only] チェックボックスをオンにして、ストレージ ポートのみを選択します。

ステップ 9　[Minimum Severity] ドロップダウン リストから、受信するメッセージの重大度を選択します。

ステップ 10　[Add] をクリックして、通知を追加します。

（注）　[Minimum Severity] オプションは、[Event Type] が [All] に設定されている場合のみ使用できます。

（注）　Cisco DCNM-SAN が送信するトラップは、重大度のタイプとそれに続くテキスト記述に対応したものとなります。

```
trap type(s) = 40990 (emergency) 40991 (alert) 40992 (critical) 40993 (error) 40994
(warning) 40995 (notice) 40996 (info) 40997 (debug)textDescriptionOid = 1, 3, 6, 1, 4, 1,
9, 9, 40999, 1, 1, 3, 0
```

手順の詳細

通知転送を削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Events] > [Forwarding] の順に選択します。

ステップ 2　削除したい通知の前のチェックボックスをオンにします。

ステップ 3　[Remove] をクリックします。

EMC CallHome の設定

EMC Callhome を設定する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Events] > [EMC CallHome] の順に選択します。

ステップ 2　[Enable] チェックボックスをオンにして、この機能をイネーブルにします。

ステップ 3　対象のファブリックの隣にあるチェックボックスをオンにして、ファブリックを選択します。

ステップ 4　一般的な電子メール情報を入力します。

ステップ 5　[Apply] をクリックして、電子メール オプションを更新します。

ステップ 6　[Apply and Test] をクリックして、電子メール オプションを更新し、結果をテストします。

AAA プロパティの設定

AAA プロパティを設定するには、メニュー バーで、[Admin] > [Management Users] > [Remote AAA Properties] の順に選択します。画面の指示に従います。

ユーザの追加と削除

DCNM Web クライアントを使用して Web クライアント ユーザの追加や削除を実行できます。

手順の詳細

ユーザを追加するには、次の手順を実行します。

ステップ 1　メニュー バーで、[Admin] > [Management Users] > [Local] の順に選択します。

[Local Database] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Add User] ダイアログボックスが表示されます。

ステップ 3　[User Name] フィールドに、ユーザ名を入力します。

（注）　ユーザ名 **guest** は予約されています（大文字と小文字は区別されません）。guest ユーザにできるのは、レポートの表示だけです。guest ユーザは guest パスワードを変更できず、DCNM Web クライアントの Admin オプションにもアクセスできません。

ステップ 4　[Role] ドロップダウン リストからユーザのロールを選択します。

ステップ 5　[Password] フィールドにパスワードを入力します。

ステップ 6　[Confirm Password] フィールドに、パスワードを再入力します。

ステップ 7　[Add] をクリックすると、そのユーザがデータベースに追加されます。

ステップ 8　ユーザの追加を続行する場合は、ステップ 3 ～ 7 を繰り返します。

手順の詳細

ユーザを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Management Users] > [Local] の順に選択します。

ステップ 2　削除するユーザの隣のチェックボックスをオンにして、[Remove] をクリックします。

ロールの追加と削除

DCNM Web クライアントを使用して Web クライアントのロールの追加や削除を実行できます。

手順の詳細

ロールを追加する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Management Users] > [Local] の順に選択します。

[Local Roles] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Add Role] ダイアログボックスが表示されます。

ステップ 3　[Role Name] フィールドにロール名を入力します。

ステップ 4　[Select Group(s)] カラムから、ロールがアクセスできるファブリックを選択します。

ステップ 5　[Add] をクリックすると、そのロールがデータベースに追加されます。

ステップ 6　ロールの追加を続行する場合は、ステップ 3 ～ 5 を繰り返します。

ロールを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Management Users] > [Local] の順に選択します。

ステップ 2　削除するロールの隣のオプション ボタンをクリックして、[Remove] をクリックします。

クライアントの表示と接続解除

手順の詳細

DCNM Web クライアント サーバからクライアントを表示または接続解除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Management Users] > [Clients] の順に選択します。

[Clients] ページが表示されます。

ステップ 2　接続を解除するクライアントの隣のチェックボックスをオンにします。

ステップ 3　[Disconnect] をクリックします。

パフォーマンス収集の作成、編集、および削除

Performance Manager を使用してファブリックを管理する場合は、ファブリック上でフローおよび収集の初期セットを設定する必要があります。DCNM Web クライアントを使用してパフォーマンス収集の追加や削除を実行できます。ファブリックにはライセンス必要です。また、ファブリックの収集を作成する前に [Managed Continuously] ステートに設定する必要があります。

（注）　単一のポート インターフェイスからは、複数デバイスのパフォーマンス収集を管理できません。各インターフェイスの統計情報のセットは 1 つだけなので、DCNM Web クライアントが単一インターフェイスを通じて管理できるのは、表示可能な FL または iSCSI デバイス 1 つのパフォーマンス収集だけです。

手順の詳細

収集を追加する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Performance] > [Collections] の順に選択します。

[Collections] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Create Collection] ダイアログボックスが表示されます。

ステップ 3　[Scope] ドロップダウン リストから、パフォーマンス データを収集するファブリックを選択します。

ステップ 4　[VSAN] チェックボックスをオンにしてすべての VSAN の通知を受信するか、または [ID List] フィールドに VSAN ID を入力して、パフォーマンス データを収集する VSAN を限定します。

ステップ 5　パフォーマンス データを収集したいエンティティ タイプのチェックボックスをオンにします。

ステップ 6　イネーブルにしたいしきい値タイプのチェックボックスをオンにします。

ステップ 7　[Save] をクリックして収集を追加し、それをテーブルに追加します。

ステップ 8　ロールの追加を続行する場合は、ステップ 3 ～ 8 を繰り返します。

（注）　Performance Manager が表示する統計情報は、Collection Wizard を使用して設定した収集の対象となるファブリックに関するものです。

収集を削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Performance] > [Collections] の順に選択します。

ステップ 2　削除する収集の隣のチェックボックスをオンにして、[Remove] をクリックします。

RRD データベースの設定

RRD データベースを設定すると、データ サンプルが収集される間隔を設定できます。設定を適用したら、データベース ストレージ形式は指定した間隔で新しい形式に変換されます。データベースの形式は相互に互換性がないため、古いデータ（変換前）を $INSTALLDIR/pm ディレクトリにコピーします。「RRD 統計インデックスのインポート」（P.2-42）を参照してください。

手順の詳細

RRD データベースを設定する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Performance] > [Databases] の順に選択します。

[Performance Database (collection interval)] ページが表示されます。

ステップ 2　[Days] カラムの一番上の行に、5 分間隔でサンプルを収集する日数を入力します。

ステップ 3　[Days] カラムの 2 行めに、30 分間隔でサンプルを収集する日数を入力します。

ステップ 4　[Days] カラムの 3 行めに、2 時間間隔でサンプルを収集する日数を入力します。

ステップ 5　[Days] カラムの一番下の行に、1 日間隔でサンプルを収集する日数を入力します。

（注）　Cisco SAN-OS Release 3.1(1) 以降では、ISL のサンプリング間隔を設定できます。[ISLs] ドロップダウン リストからサンプリング間隔を選択します。

ステップ 6　[Apply] をクリックして変更を適用するか、または [Defaults] をクリックしてファイル サイズをデフォルト値にリセットします。

新しい値を適用する場合、または現在の値がデフォルト値ではない場合は、RRD ファイルの変換に一定の時間がかかり、その間データベースが利用できなくなるとのメッセージが表示されます。かかる時間は、新旧の値の差によって異なります。

（注）　システムが一度に処理できる変換は 1 つだけです。変換を開始すると、[Apply] と [Default] のボタンが [Refresh] と [Cancel] に変化し、他のプロセスが開始できなくなります。変換中にこのサーバにアクセスしているすべてのブラウザに、この同じ画面が表示されます。[Refresh] をクリックすると、最新の進行状況が表示されます。データの変換プロセスを中止する場合は [Cancel] をクリックします。ジョブが正常に取り消されると、再び [Apply] と [Default] のボタンが表示されます。ジョブが正常に取り消されなかった場合は、取り消しに失敗したことを示すメッセージが表示されます。

この手順を実行する場合は、多数のデータを収集するとデータ変換に時間がかかるため、この手順から先に実行してください。

RRD 統計インデックスのインポート

手順の詳細

RRD 統計インデックスを手動でインポートする手順は、次のとおりです。

ステップ 1　Cisco DCNM-SAN サーバを停止します。

ステップ 2　元の RRD ファイルを $INSTALLDIR/pm/db にコピーします。

ステップ 3　$INSTALLDIR/bin/pm.bat s を実行します。

ステップ 4　Cisco DCNM-SAN を再起動し、ファブリックを追加します。

収集しきい値の設定

手順の詳細

収集しきい値を設定する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Performance] > [Thresholds] の順に選択します。

[Thresholds] ページが表示されます。

ステップ 2　次の手順に従って、絶対値を使用したしきい値を設定します。

a. Critical 通知の送信条件を設定するには、[Generate Critical] チェックボックスをオンにします。[...when traffic exceeds] フィールドに数字（5 ～ 95）を入力して、Critical 通知が送信される時点のパーセンテージを指定します。たとえば、**10** を入力すると、所定の時間のトラフィックが許容量の 10% を超えると、通知が送信されます。

b. Warning 通知の送信条件を設定するには、[Generate Warning] チェックボックスをオンにします。[...when traffic exceeds] フィールドに数字（5 ～ 95）を入力して、Warning 通知が送信される時点のパーセンテージを指定します。たとえば、**9** を入力すると、所定の時間のトラフィックが許容量の 9% を超えると、通知が送信されます。

ステップ 3　[Apply] をクリックします。

その他の統計情報の設定

手順の詳細

その他の統計情報を設定する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Admin] > [Performance] > [Others] の順に選択します。

[Others] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Add OID] ダイアログボックスが表示されます。

ステップ 3　[Fabric] ドロップダウン リストから、その他の統計情報を追加するファブリックを選択します。

ステップ 4　[Other OID] ドロップダウン リストから OID を選択します。

ステップ 5　[Display Name] ボックスに新しい名前を入力します。

ステップ 6　[All] チェックボックスをオンにして、ファブリック内のすべてのスイッチを選択します。

ステップ 7　[Type] ドロップダウン リストから、該当するタイプを選択します。

ステップ 8　[Add] をクリックすると、この統計が追加されます。

Cisco DCNM-SAN Web 検索エンジン

検索エンジンは、特定の基準に一致するレコードを見つけるのに役立ちます。検索エンティティは、インベントリとパフォーマンスの 2 つのカテゴリに分かれます。インベントリ タイプでは、スイッチ（スイッチの名前、スイッチの IP アドレス、および WWN）、エンドポート（エイリアス、スイッチの IP アドレス、および WWN）、および VSAN（VSAN の名前、主要スイッチの IP アドレス、および WWN）によって検索できます。パフォーマンス タイプでは、エンド デバイス（エンドポート エイリアス、エンドポイント WWN）、フロー（フローの名前）、および ISL（ISL の名前、および ISL の WWN）によって検索できます。検索にはワイルドカード文字も使用できます。

Cisco DCNM-SAN 検索エンジンの使用方法

手順の詳細

検索の手順は、次のとおりです。

ステップ 1　メイン ウィンドウの右上の隅にある [Search box] をクリックします。

検索ボックスが表示されます。

ステップ 2　テキスト ボックスに検索する名前を入力します。

ステップ 3　リスト ボックスから適切なオプション ボタンを選択し、テキスト ボックスの右側にある [search] アイコンをクリックして検索を開始します。

結果を示すウィンドウが表示されます。

ステップ 4　エンティティ タイプをクリックして詳細を表示します。

右側のペインに、選択したエンティティの詳細が表示されます 。

DCNM Web クライアントを使用したバックアップの設定

DCNM Web クライアントを使用して、スイッチのスタートアップ コンフィギュレーションと実行コンフィギュレーションを定期的にバックアップできます。また、バックアップしたコンフィギュレーションの表示、コンフィギュレーション バックアップのスケジュール、バックアップした 2 つのコンフィギュレーションの比較、およびスイッチへのコンフィギュレーションの復元を行うことができます。

ここでは、次の内容について説明します。

- 「コンフィギュレーションの表示」（P.2-44）
- 「コンフィギュレーションの編集」（P.2-45）
- 「コンフィギュレーションの削除」（P.2-45）
- 「コンフィギュレーションのコピー」（P.2-45）
- 「コンフィギュレーションの比較」（P.2-46）
- 「バックアップの作成」（P.2-46）
- 「スケジュールされたジョブの表示」（P.2-47）

コンフィギュレーションの表示

手順の詳細

コンフィギュレーションを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [View] の順に選択します。

コンフィギュレーション情報が表示されます。

ステップ 2　[Scope] ドロップダウン リストからファブリック名を選択します。

ステップ 3　[Switch] ドロップダウン リストからスイッチを選択します。

ステップ 4　[Configuration file] ドロップダウン リストから、コンフィギュレーション ファイル名を選択します。

ステップ 5　[View] をクリックします。

コンフィギュレーションの編集

手順の詳細

コンフィギュレーション ファイルを編集する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [View] の順に選択します。
ステップ 2　[Scope] ドロップダウン リストからファブリック名を選択します。
ステップ 3　[Switch] ドロップダウン リストからスイッチを選択します。
ステップ 4　[Configuration file] ドロップダウン リストから、コンフィギュレーション ファイル名を選択します。
ステップ 5　[View] をクリックして、コンフィギュレーション ファイルを表示します。
ステップ 6　[Edit] チェックボックスをオンにして、コンフィギュレーション ファイルを編集します。
ステップ 7　[Save to Local file] をクリックして、変更したコンフィギュレーション ファイルをコンピュータに保存します。

コンフィギュレーションの削除

手順の詳細

DCNM Web クライアントからコンフィギュレーション ファイルを削除する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [View] の順に選択します。
ステップ 2　[Scope] ドロップダウン リストからファブリック名を選択します。
ステップ 3　[Switch] ドロップダウン リストからスイッチを選択します。
ステップ 4　[Configuration file] ドロップダウン リストから、コンフィギュレーション ファイル名を選択します。
ステップ 5　[Delete] をクリックします。

コンフィギュレーションのコピー

手順の詳細

ローカル コンフィギュレーション ファイルをデータベースにコピーする手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [View] の順に選択します。
ステップ 2　[Scope] ドロップダウン リストからファブリック名を選択します。

ステップ 3　[Switch] ドロップダウン リストからスイッチを選択します。

ステップ 4　[Configuration file] ドロップダウン リストから、コンフィギュレーション ファイル名を選択します。

ステップ 5　[Copy Local file to DB] をクリックします。

コンフィギュレーションの比較

手順の詳細

コンフィギュレーションを比較する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [Compare] の順に選択します。
コンフィギュレーションの比較情報が表示されます。

ステップ 2　[Scope] ドロップダウン リストからファブリック名を選択します。

ステップ 3　[Switch] ドロップダウン リストからスイッチを選択します。

ステップ 4　（任意）[Archive]、[Running]、または [Startup] オプション ボタンをクリックします。

ステップ 5　[Compare] をクリックします。

バックアップの作成

前提条件

コンフィギュレーションのバックアップ ジョブを格納するために、ブートフラッシュに十分な未使用領域があることを確認する必要があります。

手順の詳細

コンフィギュレーションのバックアップを作成する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [Create] の順に選択します。
バックアップ オプション ページが表示されます。

ステップ 2　[Fabric] ドロップダウン リストからファブリック名を選択します。

ステップ 3　バックアップの実行頻度（[Once]、[Daily]、[Weekly]、[Monthly]）をクリックして選択します。

ステップ 4　[calendar] アイコンをクリックして、開始日を選択します。

ステップ 5　[calendar] アイコンをクリックして、終了日を選択します。

ステップ 6　開始時間を入力します。

ステップ 7　コンフィギュレーション タイプ（[Archive]、[Running]、[Startup]）をクリックして選択します。

ステップ 8　[Create] をクリックして、このバックアップ スケジュールを保存します。

スケジュールされたジョブの表示

手順の詳細

スケジュールされたバックアップを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Backup] > [Jobs] の順に選択します。
スケジュールされたジョブの情報が表示されます。

ステップ 2　リストにあるジョブのいずれかをダブルクリックして、ジョブを表示します。

ホストおよび仮想ホスト情報の表示

ここでは、次の内容について説明します。

- 「ホスト ラックの表示」（P.2-47）
- 「仮想ホストの表示」（P.2-47）
- 「仮想マシンの表示」（P.2-48）
- 「仮想マシンの CPU およびメモリ情報の表示」（P.2-48）
- 「仮想マシンのディスク I/O 情報の表示」（P.2-48）

ホスト ラックの表示

手順の詳細

ホスト ラックを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [Hosts] の順に選択します。
ホスト ラック テーブルに、ホストのリストが表示されます。

ステップ 2　ホスト ラックの隣にある [show details] アイコンをクリックして、詳細を表示します。
トポロジ、SAN トラフィック、およびイベント情報などの詳細がダッシュボードに表示されます。

仮想ホストの表示

手順の詳細

仮想ホストを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [VHosts] の順に選択します。
仮想ホスト テーブルに仮想ホストのリストが表示されます。

ステップ 2　仮想ホストの隣にある [chart] アイコンをクリックして、詳細を表示します。
トポロジ、CPU とメモリ、およびイベント情報などの詳細がダッシュボードに表示されます。

仮想マシンの表示

手順の詳細

仮想ホストの下にある仮想マシンを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [VHosts] の順に選択します。
仮想ホスト テーブルに仮想ホストのリストが表示されます。

ステップ 2　仮想ホストの隣にある [chart] アイコンをクリックして、詳細を表示します。
トポロジ、CPU とメモリ、およびイベント情報などの詳細がダッシュボードに表示されます。

ステップ 3　仮想ホスト テーブルの [#VM] カラムにあるリンクをクリックします。
その仮想ホストの下にある仮想マシンのリストが、別個のウィンドウに表示されます。

仮想マシンの CPU およびメモリ情報の表示

仮想マシンの CPU およびメモリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [VHosts] の順に選択します。
仮想ホスト テーブルに仮想ホストのリストが表示されます。

ステップ 2　仮想ホストの隣にある [chart] アイコンをクリックして、詳細を表示します。
トポロジ、CPU とメモリ、およびイベント情報などの詳細がダッシュボードに表示されます。

ステップ 3　仮想ホスト テーブルの [#VM] カラムにあるリンクをクリックします。
その仮想ホストの下にある仮想マシンのリストが、別個のウィンドウに表示されます。

ステップ 4　仮想マシンの隣にある [chart] アイコンをクリックして、CPU およびメモリ情報を表示します。

仮想マシンのディスク I/O 情報の表示

仮想マシンの CPU およびメモリ情報を表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [VHosts] の順に選択します。
仮想ホスト テーブルに仮想ホストのリストが表示されます。

ステップ 2　仮想ホストの隣にある [chart] アイコンをクリックして、詳細を表示します。
トポロジ、CPU とメモリ、およびイベント情報などの詳細がダッシュボードに表示されます。

ステップ 3　仮想ホスト テーブルの [#VM] カラムにあるリンクをクリックします。

その仮想ホストの下にある仮想マシンのリストが、別個のウィンドウに表示されます。

ステップ 4　仮想マシンの隣にある [disc] アイコンをクリックして、ディスク I/O 情報を表示します。

ダッシュボード サマリー情報の表示

ここでは、次の内容について説明します。

- 「ヘルス サマリー情報の表示」（P.2-49）
- 「パフォーマンス サマリー情報の表示」（P.2-49）
- 「インベントリ サマリー情報の表示」（P.2-50）

ヘルス サマリー情報の表示

手順の詳細

イベントと問題のサマリーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [Summary] の順に選択し、[Health Summary] ビューをダブルクリックします。

[Summary] ウィンドウを表示します。左側には問題のサマリー テーブル、右側には過去 24 時間のイベントのサマリー テーブルが表示されます。

ステップ 2　[Switches]、[ISLs]、[Hosts]、または [Storage]（0 以外）の隣の警告をクリックすると、そのファブリックのスイッチ、ISL、またはエンド デバイスのコンポーネントが表示されます。

ステップ 3　イベント重大度（[Emergency]、[Alert]、[Critical]、[Error]、[Warning]、[Notice]、[Info]、または [Debug]）の隣のイベント数を選択すると、イベントのテーブルとそのファブリックの説明が表示されます。

パフォーマンス サマリー情報の表示

前提条件

パフォーマンス情報を表示するには、パフォーマンス コレクタをアクティブにします。

手順の詳細

合計使用率とスループットをサマリー形式で表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [Summary] の順に選択し、[Daily Performance] ビューをクリックします。

サマリー情報が表示されます。

ステップ 2　円グラフ（[Hosts]、[Storage]、または [ISLs]）をクリックして、詳細を表示します。

インベントリ サマリー情報の表示

手順の詳細

VSAN、スイッチ、ISL、ポート、およびエンド デバイスのサマリーを表示する手順は、次のとおりです。

ステップ 1　メニュー バーで、[Dashboard] > [Summary] の順に選択します。

ステップ 2　[Inventory] サマリー ページをダブルクリックします。

[Summary] ウィンドウを表示します。

PART 2

Cisco DCNM for SAN

CHAPTER 3

Cisco DCNM-SAN サーバの設定

この章では、高度な MDS モニタリング、トラブルシューティング、および設定機能を備えたプラットフォームである Cisco DCNM-SAN サーバについて説明します。他のソフトウェアのインストールは不要です。サーバ機能は Cisco DCNM-SAN ソフトウェアに統合されています。

この章の内容は、次のとおりです。

- 「Cisco DCNM-SAN サーバに関する情報」（P.3-1）
- 「Cisco DCNM-SAN サーバのライセンス要件」（P.3-2）
- 「Cisco DCNM-SAN サーバのインストールと設定」（P.3-2）
- 「Cisco DCNM-SAN サーバ ファブリックの管理」（P.3-6）
- 「Cisco DCNM-SAN サーバの変更」（P.3-8）
- 「サーバ フェデレーション」（P.3-11）
- 「その他の関連資料」（P.3-13）

Cisco DCNM-SAN サーバに関する情報

Cisco DCNM-SAN サーバをコンピュータにインストールすると、一元的な MDS 管理サービスとパフォーマンス モニタリングが可能になります。SNMP 操作を使用して、ファブリックの情報を効率的に収集できます。サーバ コンポーネントを含む Cisco DCNM-SAN ソフトウェアを使用するには、ワークステーションに約 60 MB のハードディスク スペースが必要です。Cisco DCNM-SAN サーバは Windows 2000、Windows 2003、Windows XP、Solaris 9 および 10、Red Hat Enterprise Linux AS Release 5 上で動作します。

Cisco DCNM-SAN サーバとして設定された各コンピュータは、複数のファイバ チャネル SAN ファブリックを監視できます。1 台の Cisco DCNM-SAN サーバに最大 16 台のクライアント（デフォルト）を同時に接続できます。Cisco DCNM-SAN サーバで監視されないファブリック内の MDS スイッチに、Cisco DCNM-SAN クライアントを直接接続することもできます。これにより、1 台のコンソールから任意の MDS デバイスを管理できます。

DCNM-SAN サーバの機能

Cisco DCNM-SAN サーバは次の機能を備えています。

- 複数のファブリックの管理：DCNM-SAN サーバは、同じユーザ インターフェイスで複数の物理ファブリックを監視します。この機能により、冗長ファブリックの管理が容易になります。ライセンスが付与された DCNM-SAN サーバでは、すべての設定済みファブリックに関する最新の検出情報が維持されるので、Fabric Manager Client を開くと、デバイス ステータスおよび相互接続をすぐに使用できます。
- 継続的なヘルス モニタリング：MDS の状態が継続的に監視されるため、前回 DCNM-SAN クライアントを開いたあとに発生したすべてのイベントが取り込まれます。
- ユーザ プロファイルのローミング：ライセンスが付与された DCNM-SAN サーバは、ローミング ユーザ プロファイル機能を使用して、プリファレンスおよびトポロジ マップ レイアウトをサーバに格納します。これにより、どのコンピュータでストレージ ネットワークが管理されていても、ユーザ インターフェイスの一貫性が維持されます。

（注） 同じリリースの Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバを使用する必要があります。

（注） DCNM-SAN サーバが IP NAT ファイアウォールを通って SAN ファブリックにアクセスしている場合、その SAN ファブリックを管理することはできません。SAN ファブリック内で検出されるすべての IP アドレスは、DCNM-SAN サーバから直接到達可能でなければなりません。

Cisco DCNM-SAN サーバのライセンス要件

DCNM-SAN をインストールすると、ライセンスが付いていない Cisco DCNM-SAN サーバの基本バージョンが一緒にインストールされます。Performance Manager、リモート クライアント サポート、ファブリックの継続的なモニタリングなどのライセンス機能を入手するには、Cisco DCNM-SAN サーバ パッケージを購入してインストールする必要があります。

ただし、これらのライセンス機能のトライアル バージョンを使用できます。機能のトライアル バージョンをイネーブルにするには、ライセンスを購入した場合と同様に各機能を実行します。この機能が一定期間だけ有効なデモ バージョンであることを示すダイアログボックスが表示されます。

Cisco DCNM-SAN サーバのインストールと設定

（注） Cisco DCNM-SAN サーバを実行する前に、ファブリック内またはリモート AAA サーバ上の各スイッチで専用の Cisco DCNM-SAN 管理ユーザを作成する必要があります。このユーザを使用して、ファブリック トポロジを検出します。

Cisco DCNM-SAN サーバをインストールして初期設定を行う手順は、次のとおりです。

ステップ 1　お使いのワークステーションに Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバをインストールします。「Cisco DCNM-SAN サーバのインストール」（P.3-3）を参照してください。

ステップ 2　DCNM-SAN にログインします。

ステップ 3　ファブリックを継続的に監視するように、Cisco DCNM-SAN サーバを設定します。「Cisco DCNM-SAN サーバ ファブリックの管理」（P.3-6）を参照してください。

ステップ 4　Cisco DCNM-SAN サーバで管理するファブリックごとに、ステップ 2 ～ステップ 3 を繰り返します。

ステップ 5　DCNM-SAN Web サーバをインストールします。「Performance Manager 収集の確認」（P.3-6）を参照してください。

ステップ 6　Performance Manager がデータを収集していることを確認します。「Performance Manager 収集の確認」（P.3-6）を参照してください。

Cisco DCNM-SAN サーバのインストール

DCNM-SAN をインストールすると、Cisco DCNM-SAN サーバの基本バージョン（ライセンスなし）が一緒にインストールされます。[DCNM-SAN] アイコンをクリックすると、DCNM-SAN サーバ コンポーネントが動作しているコンピュータの IP アドレスを入力するダイアログボックスが開きます。Cisco DCNM-SAN サーバの IP アドレスを入力するテキスト ボックスが表示されない場合は、[Options] をクリックして、設定オプション リストを展開します。Fabric Manager Server コンポーネントがローカル マシン上で稼動している場合は、このフィールドを **localhost** のままにします。有効なサーバを指定せずに DCNM-SAN を実行しようとすると、Cisco DCNM-SAN サーバをローカルで起動するように求めるプロンプトが表示されます。

Windows PC では、Cisco DCNM-SAN サーバはサービスとしてインストールされます。このサービスを管理するには、Microsoft Windows の管理ツールのサービスを使用します。デフォルト設定では、Windows PC を再起動すると Cisco DCNM-SAN サーバ サービスが自動的に起動されます。この動作を変更するには、サービスのプロパティを変更します。

Cisco MDS 9000 FabricWare を実行しているスイッチでは、スイッチに同梱されている CD-ROM から DCNM-SAN をインストールするか、Cisco.com から DCNM-SAN をダウンロードします。

（注）　1 台のコンピュータで実行できる Cisco DCNM-SAN サーバのインスタンスは 1 つだけです。コンピュータで DCNM-SAN のスタンドアロン バージョンをお使いの場合は、Cisco DCNM-SAN サーバをインストールする前に、スタンドアロン バージョンのアンインストールが必要な場合があります。

Cisco.com からソフトウェアをダウンロードする場合は、次の Web サイトにアクセスしてください。

http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

（注）　旧バージョンから 5.0(1a) 以降へのアップグレードを行っている場合、5.0(1a) 以降はユーザ自身がプロビジョニングした、あるいはサードパーティが発行した SSL 証明書を使用するように HTTPS が設定されているので、キーストア パスワードを設定してから、DCNM-SAN サーバを再起動してください。キーストア パスワードを設定するには、**$INSTALLDIR/dcm/fm/bin encrypter.bat ssl** を実行します。

Windows で DCNM-SAN サーバをインストールする手順は、次のとおりです。

ステップ 1　[Install Management Software] リンクをクリックします。

ステップ 2　[Management Software] > [Cisco DCNM-SAN] を選択します。

ステップ 3　[Installing DCNM-SAN] リンクをクリックします。

ステップ 4　[FM Installer] リンクをクリックします。

[Cisco DCNM-SAN Installer] ウィンドウにウェルカム メッセージが表示されます。

ステップ 5　[Custom] オプション ボタンをクリックし、[Next] をクリックしてインストールを開始します。

ステップ 6　[I accept the terms of the License Agreement] チェックボックスをオンにして、[Next] をクリックします。

[Install Options] ダイアログボックスが表示されます。

ステップ 7　[Cisco DCNM-SAN Server (Licensed)] オプション ボタンをクリックして、Cisco DCNM-SAN サーバのサーバ コンポーネントをインストールします。

ステップ 8　[Add server to an existing server federation] をクリックして、サーバをフェデレーションに追加します。

（注）　リモート ホストから PostgreSQL データベースに接続できるようにするには、pg-hba.conf file ファイルで **# IPv4 local connections** の下に次の行を追加する必要が生じる場合があります。

```
host    all         all         0.0.0.0/0           md5
```

追加後はコンフィギュレーション ファイルを保存し、PostgreSQL データベースを再起動してから、2 番めのサーバ ノードをインストールします。

（注）　3 つめの DCNM-SAN サーバをフェデレーションに追加している場合、次のように設定された Oracle データベースを使用する必要があります。

```
C:\Documents and Settings\Administrator>sqlplus /nolog
SQL*Plus: Release 10.2.0.1.0 - Production on Wed Jan 6 17:19:32 2010
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
SQL> connect / as sysdba;
Connected.

SQL> alter system set processes=100 scope=spfile;
System altered.
SQL> alter system set open_cursors=500 scope=spfile;
System altered.

SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup;
ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size             218714356 bytes
Database Buffers          583008256 bytes
Redo Buffers                2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;

Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size             218714356 bytes
Database Buffers          583008256 bytes
Redo Buffers                2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
```

```
aq_tm_processes                      integer     0
db_writer_processes                  integer     4
gcs_server_processes                 integer     0
job_queue_processes                  integer     4
log_archive_max_processes            integer     2
processes                            integer     100
```

ステップ 9　Cisco DCNM-SAN 用のワークステーションでインストール フォルダを選択します。Windows では、デフォルトのロケーションは C:¥Program Files¥Cisco Systems です。

ステップ 10　[Next] をクリックします。

[Database Options] ダイアログボックスが表示されます。

ステップ 11　[Install PostgreSQL] または [Use existing DB] オプション ボタンをクリックして、使用するデータベースを指定します。

Install PostgreSQL を選択した場合は、デフォルトを受け入れ、パスワードを入力します。PostgreSQL データベースがインストールされます。

（注）　PostgreSQL のインストールを選択した場合は、稼動中のすべてのセキュリティ ソフトウェアをディセーブルにする必要があります。そうしないと、一部のフォルダやユーザがインストールされないことがあります。

（注）　ご使用のシステムで Cygwin が稼動している場合は、PostgreSQL をインストールする前に、環境変数パスから cygwin/bin を削除してください。

ステップ 12　[Use existing DB] を選択した場合は、[PostgreSQL 8.1/8.2] オプション ボタンまたは [Oracle10g] オプション ボタンをクリックします。

ステップ 13　[Database Options] ダイアログボックスで、[Next] をクリックします。

[Configuration Options] ダイアログボックスが表示されます。

ステップ 14　[Install] をクリックして Cisco DCNM-SAN サーバをインストールします。

いずれかの Cisco DCNM-SAN サーバ機能を評価していて、その機能の評価期間を終了するには、Device Manager を使用します。

Cisco DCNM-SAN サーバでのデータ マイグレーション

データベースのマイグレーションは既存のデータベースでだけ実行してください。複数のデータベースのデータをマージすると、コリジョンが発生する可能性があります。

非フェデレーション モードのデータベースを初めてフェデレーション モードにアップグレードする場合、クラスタ シーケンス テーブルには、シーケンス テーブル内の対応する値よりも大きく、サーバ ID のクラスタ シーケンス番号形式に適した値が入力されます。

Performance Manager 収集の確認

Performance Manager の収集機能を 5 分以上実行したあとに、データが収集されたかどうかを確認するには、DCNM-SAN で [Performance Manager] > [Reports] を選択します。収集された最初の数個のデータ ポイントが、グラフおよび表形式で表示されます。

Cisco DCNM-SAN サーバ ファブリックの管理

Cisco DCNM-SAN サーバ ファブリックは、クライアントでそのファブリックが開かれているかどうかに関係なく、継続的に管理することができます。継続的管理の対象となるファブリックは、Cisco DCNM-SAN サーバを起動すると自動的にリロードされ、管理されます。

継続的管理対象のファブリックの選択

DCNM-SAN を使用してファブリックを継続的に管理する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

（注）　[Fabrics] タブにアクセスできるのは、ネットワーク管理者だけです。

（注）　ファブリック管理用のユーザ名とパスワードは事前に設定できます。このインスタンスでは、TACACS+ サーバではなく、ローカル スイッチのアカウントを使用する必要があります。

ステップ 2　次のいずれかの Admin オプションを選択します。

a. [Manage Continuously] : Cisco DCNM-SAN サーバ が起動すると、ファブリックは自動的に管理対象となり、このオプションが [Unmanage] に変更されるまで継続して管理されます。

b. [Manage] : ファブリックは、それを表示する DCNM-SAN のインスタンスがなくなるまで、Cisco DCNM-SAN サーバによって管理されます。

c. [Unmanage] : Cisco DCNM-SAN サーバはファブリックの管理を停止します。

ステップ 3　[Apply] をクリックします。

（注）　Performance Manager を使用してこれらのファブリックに関するデータを収集する場合は、ここでフローを設定し、データ収集を定義する必要があります。

Cisco DCNM-SAN サーバのプロパティ ファイル

Cisco DCNM-SAN サーバのプロパティ ファイル（**MDS 9000\server.properties**）には、Cisco DCNM-SAN サーバがどのように機能するかを示すプロパティのリストが格納されています。このファイルの編集にはテキスト エディタを使用します。プロパティを設定するには、[Admin] タブにある DCNM-SAN Web サービス GUI を使用します。

（注）　Cisco NX-OS Release 4.1(1b) 以降では、server.properties ファイルおよび AAA.properties ファイルのパスワードを任意で暗号化できます。

Fabric Manager Server プロパティ ファイルには、次に示す 9 つの一般セクションが含まれています。

- GENERAL：サーバの全般的な設定が格納されます。
- SNMP SPECIFIC：SNMP 要求、応答、およびトラップの各設定が格納されます。
- SNMP PROXY SERVER SPECIFIC：SNMP プロキシ サーバ コンフィギュレーションの設定および TCP ポート指定の設定が格納されます。
- GLOBAL FABRIC：検出やロードなどのファブリックの設定が格納されます。
- CLIENT SESSION：サーバにログインできる DCNM-SAN クライアントの設定が格納されます。
- EVENTS：Syslog メッセージの設定が格納されます。
- PERFORMANCE CHART：Performance Manager のチャート生成の終了時間を定義する設定値が格納されます。
- EMC CALL HOME：EMS の指定に基づいて、電子メールで XML データとしてトラップを転送するための設定が格納されます。
- EVENT FORWARD SETUP：Cisco DCNM-SAN サーバが記録したイベントを電子メールで転送するための設定が格納されます。

Cisco DCNM-SAN Release 3.x 以降では、次のサーバ プロパティが追加または変更されています。

SNMP Specific

- **snmp.preferTCP**：このオプションを true に設定すると、Cisco DCNM-SAN サーバがスイッチとの通信に使用するデフォルト プロトコルは TCP に設定されます。デフォルトでは、true が設定されています。スイッチで TCP がイネーブルになっていない場合、Cisco DCNM-SAN サーバは UDP を使用します。この設定のメリットはスイッチの SNMP ユーザそれぞれに対して TCP セッションが 1 つずつ割り当てられる点です。また、タイムアウトを削減し、スケーラビリティを向上することができます。

（注）　このオプションを false に設定した場合は、DCNM-SAN でも同様の設定を選択する必要があります。DCNM-SAN の snmp.preferTCP のデフォルト値は true です。

Performance Chart

- **pmchart.currenttime**：Performance Manager のチャート生成の終了時間を指定します。デバッグにだけ使用してください。

EMC Call Home

- **server.callhome.enable**：EMC Call Home をイネーブル化またはディセーブル化します。デフォルト設定は、ディセーブルです。
- **server.callhome.location**：[Location] パラメータを指定します。

- **server.callhome.fromEmail**：[From Email] リストを指定します。
- **server.callhome.recipientEmail**：[recipientEmail] リストを指定します。
- **server.callhome.smtphost**：発信電子メールの SMTP ホスト アドレスを指定します。
- **server.callhome.xmlDir**：XML メッセージ ファイルを保存するパスを指定します。
- **server.callhome.connectType**：サーバにリモート接続する方法を指定します。
- **server.callhome.accessType**：サーバとのリモート通信を確立する方法を指定します。
- **server.callhome.version**：接続タイプのバージョン番号を指定します。
- **server.callhome.routerIp**：RSC ルータのパブリック IP アドレスを指定します。

Event Forwarding

- **server.forward.event.enable**：イベント フォワーディングをイネーブル化またはディセーブル化します。
- **server.forward.email.fromAddress**：[From Email] リストを指定します。
- **server.forward.email.mailCC**：[CC Email] リストを指定します。
- **server.forward.email.mailBCC**：[BCC Email] リストを指定します。
- **server.forward.email.smtphost**：発信電子メールの SMTP ホスト アドレスを指定します。

Deactivation

- **deactivate.confirm=deactivate**：非アクティブ化するストリングを入力するよう要求します。

（注）　フェデレーションされたサーバ環境では、server.properties ファイルを変更して Cisco DCNM-SAN サーバのプロパティを変更しないでください。server.properties を変更するには、Web クライアントのメニューで [Admin] > [Configure] > [Preferences] を選択します。

Cisco DCNM-SAN サーバの変更

Fabric Manager Release 2.1(2) 以降では、サーバを停止したり再起動することなく、Cisco DCNM-SAN サーバの特定の設定値を変更できます。

- 「Cisco DCNM-SAN サーバのユーザの追加または削除」（P.3-8）
- 「Cisco DCNM-SAN サーバのユーザ名およびパスワードの変更」（P.3-9）
- 「ポーリング時間とファブリック再検出時間の変更」（P.3-9）
- 「デバイス エイリアスまたは FC エイリアスの使用方法」（P.3-10）

Cisco DCNM-SAN サーバのユーザの追加または削除

制約事項

ユーザを管理できるのは、ネットワーク管理者だけです。

手順の詳細

Cisco DCNM-SAN サーバのユーザの追加、または既存ユーザのパスワード変更を DCNM-SAN で行う手順は、次のとおりです。

ステップ 1　[Control Panel] ダイアログボックスで、[Local FM Users] タブをクリックします。DCNM-SAN ユーザのリストが表示されます。

ステップ 2　ユーザを追加する場合は [New] をクリックします。既存のユーザのパスワードを変更する場合は [Edit] をクリックします。

[FM Configuration] ダイアログボックスが表示されます。

ステップ 3　新規ユーザのユーザ名とパスワードを設定し、[Apply] をクリックします。

DCNM-SAN を使用して Cisco DCNM-SAN サーバのユーザを削除する手順は、次のとおりです。

ステップ 1　[Control Panel] ダイアログボックスで、[Local FM Users] タブをクリックします。DCNM-SAN ユーザのリストが表示されます。

ステップ 2　削除するユーザ名をクリックします。

ステップ 3　そのユーザを削除する場合 [Remove] をクリックします。

ステップ 4　削除を確認する場合は [Yes] をクリックし、削除を取り消す場合は [No] をクリックします。

Cisco DCNM-SAN サーバのユーザ名およびパスワードの変更

DCNM-SAN クライアントからファブリックへのアクセスに使用するユーザ名とパスワードは、Cisco DCNM-SAN サーバを再起動せずに変更できます。

Cisco DCNM-SAN サーバで使用されるユーザ名またはパスワードを変更する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

ステップ 2　Cisco DCNM-SAN サーバで監視している各ファブリックの名前またはパスワードを設定します。

ステップ 3　[Apply] をクリックして、変更を保存します。

ポーリング時間とファブリック再検出時間の変更

Cisco DCNM-SAN サーバは監視対象のファブリックを定期的にポーリングし、デフォルト間隔である 5 サイクルでファブリック全体を再検出します。これらの設定は Cisco DCNM-SAN クライアントで変更でき、Cisco DCNM-SAN サーバを再起動する必要はありません。

DCNM-SAN を使用して、Cisco DCNM-SAN サーバで使用されるポーリング期間またはファブリック全体の再検出に関する設定を変更する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

ステップ 2　Cisco DCNM-SAN サーバで監視している各ファブリックに対して [Polling Interval] を設定し、Cisco DCNM-SAN サーバでファブリック エレメントのステータスと統計情報をポーリングする頻度を指定します。

ステップ 3　Cisco DCNM-SAN サーバで監視している各ファブリックに対して [Rediscover Cycles] を設定し、Cisco DCNM-SAN サーバでファブリック全体を再検出する頻度を指定します。

ステップ 4　[Apply] をクリックして、変更を保存します。

Cisco DCNM-SAN サーバの IP アドレスの変更

Cisco DCNM-SAN サーバの IP アドレスを変更する手順は、次のとおりです。

ステップ 1　Cisco DCNM-SAN サーバを停止します。

ステップ 2　$INSTALLDIR/conf/FMServer.conf. で次のパラメータを変更します。

wrapper.app.parameter.4=127.0.0.1

ステップ 3　$INSTALLDIR/conf/server.properties. で次のパラメータを変更します。

server.bindaddrs = 127.0.0.1

ステップ 4　次のコマンドを入力して新しい IP アドレスを割り当てます。

```
run $INSTALLDIR/bin/PLMapping.bat -p newipaddress 0
```

ここでは、DCNM-SAN インストールの最上位ディレクトリは INSTALLDIR であると想定します。上記のコマンドは、サーバ ID が 0 の単一サーバ インスタンスに対応しています。

デバイス エイリアスまたは FC エイリアスの使用方法

DCNM-SAN が FC エイリアスまたはグローバル デバイス エイリアスのいずれを使用するかを DCNM-SAN クライアントで変更できます。Cisco DCNM-SAN サーバを再起動する必要はありません。

DCNM-SAN を使用して、DCNM-SAN が FC エイリアスまたはグローバル デバイス エイリアスを使用するように変更する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

ステップ 2　グローバル デバイス エイリアスを使用する場合は、DCNM-SAN サーバで監視している各ファブリックの [Device Alias] チェックボックスをオンにし、FC エイリアスを使用する場合はオフにします。

ステップ 3　[Apply] をクリックして、変更を保存します。

サーバ フェデレーション

サーバ フェデレーションは分散システムです。このシステムは、相互通信するサーバまたはコンピュータで構成されており、1 つの統合されたコンピューティング リソースとして利用されます。Cisco DCNM-SAN サーバ フェデレーションを使用すると、同時に複数のサーバと通信できます。これにより、フェデレーション内で実行されるデータとプログラムの拡張性が向上し、管理も容易になります。サーバ フェデレーションのコアには、Cisco DCNM-SAN サーバ、組み込みの Web サーバ、データベース、サーバにアクセスする DCNM-SAN クライアントなど、複数の機能ユニットが含まれます。

フェデレーション内の Cisco DCNM-SAN サーバは、同じデータベースを使用してデータを保存および検索します。このデータベースは複数のサーバによって共有され、情報が共有されます。DCNM-SAN クライアントまたは DCNM-SAN Web クライアントは、マッピング テーブルを使用して Cisco DCNM-SAN サーバからファブリックを開くことができます。ファブリックは論理サーバ間を移動できます。論理サーバは物理マシン間を移動できます。

制約事項

- 既存のフェデレーション内で複数の Cisco DCNM-SAN サーバをアップグレードすることはできません。同時にアップグレードする場合は、そのサーバにある Performance Manager の統計データやその他の情報を移行できません。
- フェデレーションされたサーバ環境では、すべての DCNM-SAN サーバで時間を同期させる必要があります。

Fabric ID から Server ID へのマッピング

物理サーバの IP アドレスは、Cisco DCNM-SAN サーバのインストール時にサーバ ID にマッピングされます。物理サーバの IP アドレスが変更された場合は、必ず Cisco DCNM-SAN サーバで提供されている PLMapping スクリプトを使用して、その IP アドレスをサーバ ID にマッピングする必要があります。ファブリックを開くあるいは検出した場合、ファブリック ID は必ずサーバ ID にマッピングされます。ファブリックを別のサーバ ID に移動するには、コントロール パネルを使用します。

別のサーバにファブリックを移動する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] が表示されます。

ステップ 2　別のサーバに移動するファブリックを選択し、[Move] をクリックします。

[Move Fabric] ダイアログボックスが表示されます。

ステップ 3　[Fabrics to Move] リスト ボックスで選択したファブリックが表示されます。[Move To Server] ドロップダウン リストからファブリックの移動先となるサーバを選択します。

ステップ 4　[Move] をクリックします。

ファブリックを別のサーバで開く

別のサーバでファブリックを開く手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。
[Control Panel] が表示されます。

ステップ 2　[Discover] をクリックします。
[Discover New Fabric] ダイアログボックスが表示されます。

ステップ 3　[Seed Switch] リスト ボックスにシード スイッチの IP アドレスを入力します。

ステップ 4　[User Name] フィールドにユーザ名を入力します。

ステップ 5　[Password] フィールドにパスワードを入力します。

ステップ 6　[Auth-Privacy] ドロップダウン リストから、適用するプライバシー プロトコルを選択します。

ステップ 7　選択したファブリックを別のサーバで開くには、[Server] ドロップダウン リストからサーバ ID を選択します。

ステップ 8　[Discover] をクリックします。

（注）　他の Cisco DCNM-SAN サーバをフェデレーションに追加中、そのフェデレーション内でファブリックの検出を実行すると、エラー メッセージが表示される場合があります。このファブリックはインストール後、またはアップグレード後に検出できます。

フェデレーション内のセッションの表示

フェデレーション内のセッションを表示する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

ステップ 2　[Connected Clients] タブをクリックします。
[Control Panel] が表示されます。

フェデレーション内のサーバの表示

フェデレーション内のサーバをすべて表示する手順は、次のとおりです。

ステップ 1　[Server] > [Admin] を選択します。

ステップ 2　[Servers] タブをクリックします。
[Control Panel] が表示されます。

その他の関連資料

- サーバ フェデレーション機能を使用するには、ライセンスが必要です。Cisco DCNM-SAN サーバのライセンスについては、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。
- フェデレーションでの Cisco DCNM-SAN サーバの配置については、『*Cisco DCNM-SAN Server Federation Deployment Guide*』を参照してください。

CHAPTER 4

Cisco DCNM-SAN での認証の設定

この章では、スイッチとの通信を行う Cisco DCNM-SAN の相互依存ソフトウェア コンポーネント、認証手順、および、ファブリックとコンポーネントで認証を設定するためのベスト プラクティスについて説明します。

この章の内容は、次のとおりです。

- 「Cisco DCNM-SAN 認証の概要」（P.4-1）
- 「ファブリック検出のベスト プラクティス」（P.4-3）
- 「Performance Manager の認証」（P.4-4）
- 「Cisco DCNM-SAN Web クライアントの認証」（P.4-4）

Cisco DCNM-SAN 認証の概要

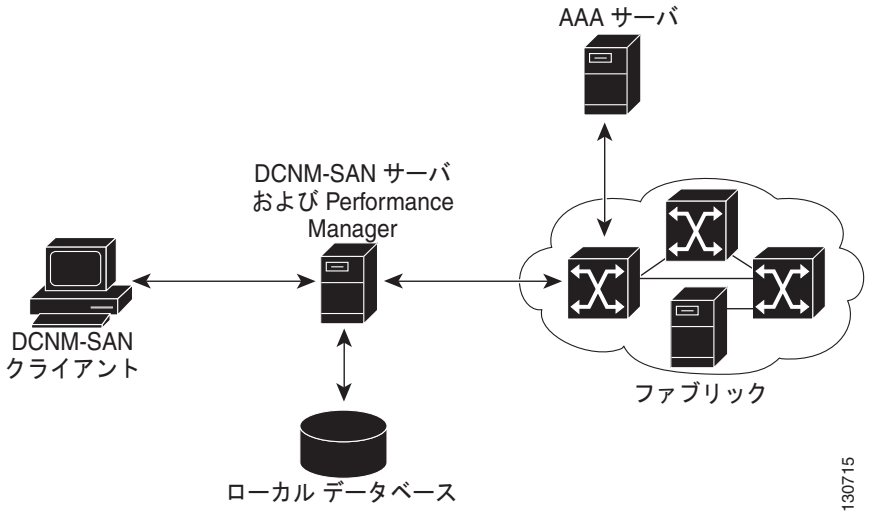
Cisco DCNM-SAN には複数のコンポーネントが含まれており、これらが相互に対話してファブリックを管理します。

次のコンポーネントが含まれます。

- Cisco DCNM-SAN クライアント
- Cisco DCNM-SAN サーバ
- Performance Manager
- Cisco MDS 9000 スイッチおよびストレージ デバイスが内部接続されたファブリック
- AAA サーバ（任意）

図 4-1 に、これらのコンポーネントの構成例を示します。

図 4-1　　Cisco DCNM-SAN の認証例



管理者は Cisco DCNM-SAN クライアントを起動して、ファブリックの検出に使用されるシード スイッチを選択します。使用するユーザ名およびパスワードが Cisco DCNM-SAN サーバに渡され、シード スイッチの認証に使用されます。このユーザ名とパスワードが、認識されている SNMP ユーザ名およびパスワードと異なる場合、Cisco DCNM-SAN クライアントまたは Cisco DCNM-SAN サーバがスイッチに対する CLI セッションを開き（SSH または Telnet）、ユーザ名とパスワードのペアを再試行します。スイッチは、ローカル スイッチ認証データベースまたはリモート AAA サーバでユーザ名とパスワードを認識すると、Cisco DCNM-SAN クライアントおよびサーバで使用される一時的な SNMP ユーザ名を作成します。

（注） リモート AAA サーバを使用して Cisco DCNM-SAN または Device Manager を認証する場合は、認証が遅くなることがあります。

（注） Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバ間にあるファイアウォールを CLI セッションが通過できるよう許可する必要があります。

（注） SNMPv3 ユーザ名認証のパスワードとプライバシー パスワード、および CLI ユーザ名とパスワードの照合には、同じパスワードを使用することを推奨します。

ファブリック検出のベスト プラクティス

Cisco DCNM-SAN サーバは、同じユーザ インターフェイスで複数の物理ファブリックを監視します。この機能により、冗長ファブリックの管理が容易になります。ライセンスが付与された Cisco DCNM-SAN サーバでは、すべての設定済みファブリックに関する最新の検出情報が維持されるので、Cisco DCNM-SAN クライアントを起動すると、デバイス ステータスおよび相互接続をすぐに使用できます。

注意　Cisco DCNM-SAN サーバの CPU 使用率が 50 パーセントを超える場合は、より高クラスの CPU システムに交換することを推奨します。

ネットワークの検出および Performance Manager の設定は、上記のベスト プラクティスに従うことをお勧めします。これにより、Cisco DCNM-SAN サーバでファブリックを詳細に表示できるようになります。以降の Cisco DCNM-SAN クライアント セッションでは、ログインしているクライアントの権限に基づいてこの詳細ビューをフィルタリングできます。たとえば、ファブリック内に複数の VSAN があり、これらの VSAN のサブセットに制限されたユーザを作成するとします。ネットワーク管理者ロール、またはネットワーク オペレータ ロールを使用して Cisco DCNM-SAN サーバでファブリックの検出を開始すると、ファブリック内のすべての VSAN を表示できます。VSAN 制限のあるユーザが Cisco DCNM-SAN クライアントを起動すると、管理が許可されている VSAN だけが表示されます。

（注）　Cisco DCNM-SAN サーバは、常にローカル スイッチ アカウントを使用してファブリックを監視します。AAA（RADIUS または TACACS+）サーバは使用しません。ファブリック サービスのプロビジョニングを目的としたクライアントへのログインには AAA ユーザ アカウントを使用できます。

ファブリック検出の設定

Cisco DCNM-SAN サーバがファブリック全体を検出できるようにするには、次の手順を実行します。

ステップ 1　ネットワーク管理者ロールまたはネットワーク オペレータ ロールを使用して、ファブリック内のスイッチごとに専用の Cisco DCNM-SAN 管理ユーザ名を作成します。または AAA サーバ内に専用の Cisco DCNM-SAN 管理ユーザ名を作成し、この AAA サーバを認証に使用するように、ファブリック内のすべてのスイッチを設定します。

ステップ 2　この Cisco DCNM-SAN 管理ユーザ名に使用されるロールがファブリック内のすべてのスイッチで同じであること、およびこのロールにすべての VSAN へのアクセス権が含まれていることを確認します。

ステップ 3　Cisco DCNM-SAN 管理ユーザを使用して Cisco DCNM-SAN クライアントを起動します。これにより、すべての VSAN がファブリック検出の対象になります。

ステップ 4　ファブリックを継続的に監視するように、Cisco DCNM-SAN サーバを設定します。

ステップ 5　Cisco DCNM-SAN サーバで管理するファブリックごとに、ステップ 4 を繰り返します。

Performance Manager の認証

Performance Manager は、Cisco DCNM-SAN サーバ データベースに格納されたユーザ名およびパスワード情報を使用します。Performance Manager の動作中にファブリック内のスイッチでこの情報が変更された場合は、Cisco DCNM-SAN サーバ データベースを更新して、Performance Manager を再起動する必要があります。Cisco DCNM-SAN サーバ データベースを更新するには、Cisco DCNM-SAN サーバからファブリックを削除し、そのファブリックを再検出する必要があります。

Performance Manager で使用されるユーザ名およびパスワード情報を更新するには、次の手順を実行します。

ステップ 1　Cisco DCNM-SAN で [Server] > [Admin] の順にクリックします。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

ステップ 2　ユーザ名およびパスワード情報を更新したファブリックをクリックします。

ステップ 3　[Admin] リストボックスから [Unmanage] を選択し、[Apply] をクリックします。

ステップ 4　正しいユーザ名とパスワードを入力し、[Apply] をクリックします。

ステップ 5　[Admin] リストボックスから [Manage] を選択し、[Apply] をクリックします。

ステップ 6　ファブリックを再検出するには、[Open] タブをクリックし、[Select] カラムから開くファブリックの横にあるチェックボックスをオンにします。

ステップ 7　[Open] をクリックして、ファブリックを再検出します。Cisco DCNM-SAN サーバでユーザ名とパスワードが更新されます。

ステップ 8　再検出する必要があるファブリックそれぞれに対して、ステップ 3 ～ステップ 7 を繰り返します。

ステップ 9　[Performance] > [Collector] > [Restart] の順に選択して Performance Manager を再起動し、新しいユーザ名およびパスワードを使用します。

Cisco DCNM-SAN Web クライアントの認証

Cisco DCNM-SAN Web サーバは、ファブリック内のスイッチと直接通信しません。Cisco DCNM-SAN Web サーバは、ローカルに格納される、あるいは AAA サーバでリモートに格納される、独自のユーザ名とパスワードの組み合わせを使用します。

Cisco DCNM-SAN Web サーバでのユーザ認証には、RADIUS または TACACS+ サーバを使用することを推奨します。

RADIUS 認証を使用するように Cisco DCNM-SAN Web サーバを設定するには、次の手順を実行します。

ステップ 1　Cisco DCNM-SAN Web クライアントを起動します。

ステップ 2　[Admin] > [Management Users] > [Remote AAA] の順に選択して、Cisco DCNM-SAN Web クライアントで使用される認証を更新します。

ステップ 3　認証モード属性を [radius] に設定します。

ステップ 4　最大 3 つの RADIUS サーバの RADIUS サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 5　[Modify] をクリックして、この情報を保存します。

TACACS+ 認証を使用するように Cisco DCNM-SAN Web サーバを設定するには、次の手順を実行します。

ステップ 1　Cisco DCNM-SAN Web クライアントを起動します。

ステップ 2　[Admin] > [Management Users] > [Remote AAA] の順に選択して、Cisco DCNM-SAN Web クライアントで使用される認証を更新します。

ステップ 3　認証モード属性を [tacacs] に設定します。

ステップ 4　最大 3 つの TACACS+ サーバの TACACS+ サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 5　[Modify] をクリックして、この情報を保存します。

（注）　Cisco DCNM-SAN は SNMP 認証と互換性がないため、SecureID をサポートしません。Cisco DCNM-SAN では、ファブリック内のすべてのスイッチに対応する同一のログイン クレデンシャルが使用されます。認証に SecureID を 2 回以上使用することはできないので、Cisco DCNM-SAN が SecureID を使用して 2 つ目のスイッチとの接続を確立することはできません。

CHAPTER 5

Cisco DCNM-SAN クライアントの設定

この章では、Java ベースの GUI アプリケーションである Cisco DCNM-SAN クライアントについて説明します。このアプリケーションを使用して、リモート ワークステーションから Cisco DCNM-SAN アプリケーションにアクセスすることができます。

この章の内容は、次のとおりです。

- 「DCNM-SAN クライアントの概要」（P.5-1）
- 「Cisco DCNM-SAN クライアント クイック ツアー：サーバ管理者向けの表示」（P.5-2）
- 「Cisco DCNM-SAN クライアント クイック ツアー：管理者向けの表示」（P.5-7）
- 「DCNM-SAN クライアントの起動」（P.5-24）
- 「Cisco DCNM-SAN プリファレンスの設定」（P.5-28）
- 「ネットワーク ファブリックの検出」（P.5-30）
- 「デバイス グループの変更」（P.5-31）
- 「ユーザおよびロールによる管理者アクセスの制御」（P.5-32）
- 「Cisco DCNM-SAN Wizard の使用方法」（P.5-32）
- 「Cisco DCNM-SAN トラブルシューティング ツール」（P.5-33）
- 「Cisco DCNM-SAN と Data Center Network Management ソフトウェアの統合」（P.5-34）

DCNM-SAN クライアントの概要

Cisco DCNM-SAN は Java および SNMP ベースのネットワーク ファブリックおよびデバイス管理ツールです。GUI を通じて、Cisco Nexus 5000 シリーズ スイッチ、Cisco MDS 9000 ファミリやサードパーティ製スイッチ、ホスト、およびストレージ デバイスを含むネットワーク ファブリックをリアルタイムで表示できます。

Cisco DCNM-SAN クライアントには、Cisco MDS 9000 ファミリ スイッチおよび Cisco Nexus 5000 シリーズ スイッチ向けの詳細な設定機能およびステータス モニタリング機能のほか、ファイバ チャネル トラブルシューティング ツールも用意されています。MDS 9000 ファミリ スイッチまたはCisco Nexus 5000 シリーズスイッチに対してこのヘルスおよび設定分析ツールを使用してファイバ チャネル ping および traceroute を実行できます。

Cisco DCNM-SAN Release 4.1(1b) 以降では、制限された機能のみにアクセスを許可するサーバ管理者ロールが追加されているので、マルチレベルのセキュリティ システムを利用できます。サーバ管理者の設定機能は FlexAttach と関連データに制限されています。

（注）　同じリリースの Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバを使用する必要があります。

Cisco DCNM-SAN 拡張モード

拡張モードはデフォルトでイネーブルであり、セキュリティ、IVR、iSCSI、FICON を含む Cisco DCNM-SAN 機能の完全なスイートを提供します。ユーザ インターフェイスを単純にするには、Cisco DCNM-SAN クライアントの右上にあるリスト ボックスで、[Simple] を選択します。簡易モードでは、VSAN（仮想 SAN）、ゾーン分割、インターフェイス設定など、基本的な MDS 9000 機能にアクセスできます。サーバ管理者ロールでは拡張モードは利用できません。

Cisco DCNM-SAN クライアント クイック ツアー：サーバ管理者向けの表示

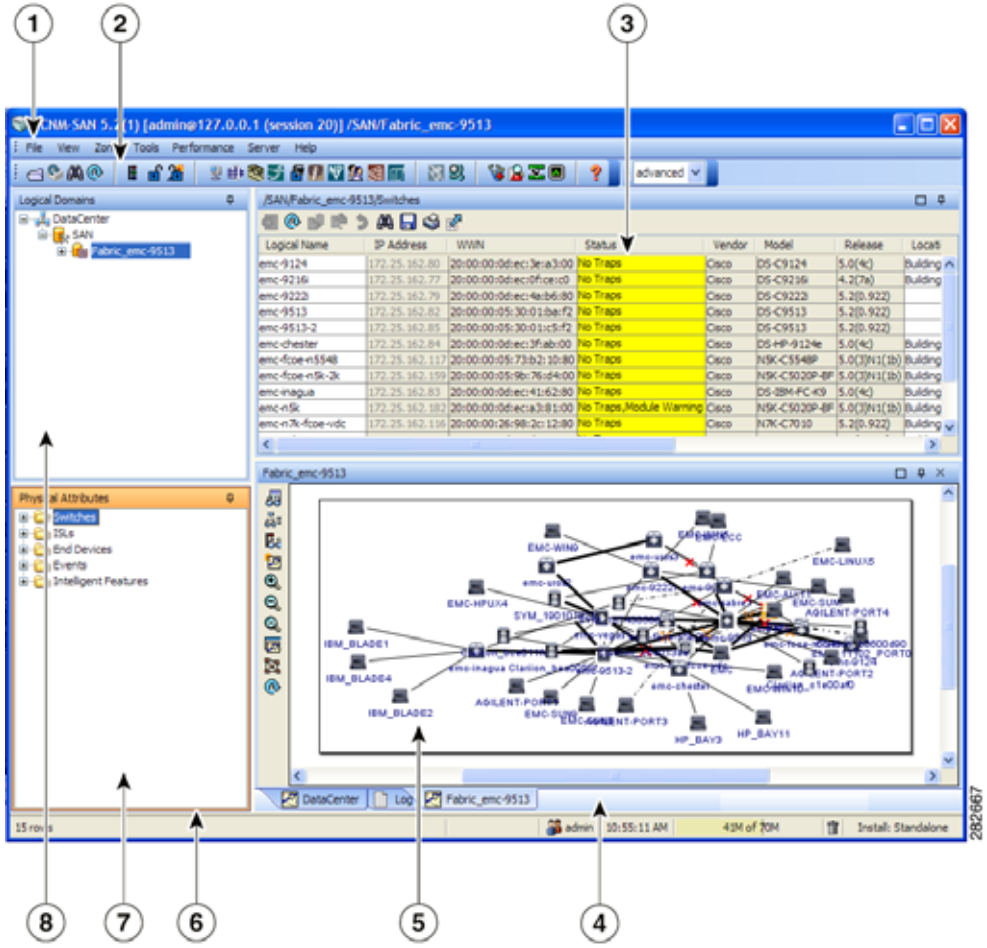
Cisco DCNM-SAN では、制限された機能のみにアクセスを許可するサーバ管理者ロールが追加されているので、マルチレベルのセキュリティ システムを利用できます。サーバ管理者ロールの設定機能は FlexAttach と関連データに制限されています。サーバ管理者は SAN 管理者の助けを借りることなく、新しいサーバに対して SAN を事前設定し、同じ NPV デバイスまたは他の NPV デバイスにサーバを移動して、障害が発生したサーバを同じポートに置換することができます。サーバ ロール管理者は、Cisco DCNM-SAN ユーザまたは接続されているクライアントを管理することはできません。

Cisco DCNM-SAN では、ユーザ インターフェイスが大幅に向上しました。ペインが移動可能でドック表示できるようになったため、ユーザのニーズに合わせて [Physical Attributes] ペイン、[Logical Domains] ペイン、[Fabric] ペインおよび [Information] ペインを並べ替えでき、ワークフロー管理が容易になりました。ドック表示可能なペインはドック表示フレームとも呼ばれます。ドック可能フレームはスタンダロン（フロート）表示、最小化、または最大化できます。[Logical] ペイン、[Physical] ペイン、[Information] ペイン、および [Fabric] ペインは必要に応じて折りたたむことも展開することもできます。これらのペインは作業スペースの右、左または下部にもドック表示できます。

Cisco DCNM-SAN メイン ウィンドウ

ここでは、図 5-1 に示すサーバ管理者ユーザ向けの Cisco DCNM-SAN クライアント インターフェイスについて説明します。

図 5-1　Cisco DCNM-SAN メイン ウィンドウ：サーバ管理者向けの表示



1	メニュー バー：メニュー別に編成されたオプションにアクセスできます。
2	ツールバー：[File]、[Tools]、および [Help] メニュー内で最も一般的に使用されるオプションに直接アクセスするためのアイコンが配置されています。
3	[Information] ペイン：メニュー ツリーで選択されたオプションに関する情報が表示されます。
4	ステータス バー（右側）：検出プロセスで表示された最後のエントリ、および有効なエラー メッセージが表示されます。
5	[Fabric] ペイン：スイッチ、ホスト、ストレージなどのネットワーク ファブリックのマップが表示されます。また、ログおよびイベント データを表示するためのタブも配置されています。
6	ステータス バー（左側）：テーブルに表示される行数などの一時的なメッセージが短期間表示されます。
7	[Physical Attributes] ペイン：上記で選択されたファブリック、VSAN、またはゾーンに応じて、使用可能な設定作業がツリー表示されます。論理的に選択されたスイッチが一覧表示されます。
8	[Logical Domains] ペイン：設定済みの SAN、ファブリックおよびユーザ定義グループをツリー表示します。

メニュー バー

Cisco DCNM-SAN メイン ウィンドウの上部にあるメニュー バーには、[Fabric] ペインでの情報表示を管理および制御するためのオプションが配置されています。サーバ管理者は SAN 管理者に付与された一部のオプションを使用できません。メニュー バーには、次のメニューがあります。

- [File]：新しいファブリックを開く、現在のファブリックの再検出、スイッチの位置の特定、プリファレンスの設定、マップの印刷を行います。
- [View]：マップの外観を変更します（[Fabric] ペイン ツールバーにもこれらのオプションと同じ機能が配置されています）。
- [Tools]：FlexAttach 仮想 pWWN 機能を使用してサーバおよび設定を管理します。
- [Help]：[Information] ペインに、特定のダイアログボックスに関するオンライン ヘルプ トピックが表示されます。

ツールバー

Cisco DCNM-SAN のメイン ツールバー（サーバ管理者専用）には、頻繁に使用されるメニュー バー オプションにアクセスするためのアイコンが配置されています（表 5-1 を参照）。

表 5-1　Cisco DCNM-SAN クライアントのメイン ツールバー

アイコン	説明
	スイッチ ファブリックを開きます。
	現在のファブリックを再検出します。
	マップを検索します。
	オンライン ヘルプが表示されます。

[Logical Domains] ペイン

[Logical Domains] ペインを使用してファブリックを表示し、ユーザ定義グループにアクセスします。グループを展開するさまざまなとユーザ定義グループを表示できます。各コア スイッチに作成された編集不能グループにはそれぞれの NPV スイッチが含まれます。

[Physical Attributes] ペイン

現在選択されているファブリックまたはグループ内のスイッチの管理に使用できるオプションをツリー表示するには、[Physical Attributes] ペインを使用します。

オプションを選択するには、フォルダをクリックして使用可能なオプションを表示し、オプションをクリックします。[Information] ペインに、選択したオプションに関する情報が表形式で表示されます。[Physical Attributes] ペインには次のメイン フォルダが配置されています。

- [Switches]：ハードウェア、システム、ライセンス、およびコンフィギュレーション ファイルの表示および設定を行います。
- [Interfaces]：FC 物理インターフェイス、FC 論理インターフェイス、VFC（FCoE）インターフェイス、イーサネット インターフェイス、SVC インターフェイス、および PortChannel インターフェイスを表示および設定できます。

[Information] ペイン

[Information] ペインには、[Logical Domains] ペインまたは [Physical Attributes] ペインのメニュー ツリーで選択されたオプションに対応する情報テーブルが表示されます。[Information] ペインのツールバーには、表 5-2 に示された処理を 1 つまたは複数実行するためのボタンが配置されています。

表 5-2　[Information] ペインのツールバー

アイコン	説明
	コンフィギュレーションの変更を適用します。
	テーブルの値を更新します。
	行のデータを他の行にコピーします。
	行のデータを他の行に貼り付けます。
	直前の変更を元に戻します。
	テーブルから指定されたストリングを検索します。
	情報をファイルにエクスポートし、保存します。

表 5-2　[Information] ペインのツールバー （続き）

アイコン	説明
	[Information] ペインの内容を出力します。
	[Information] ペイン内のテーブルの編集不可能なコピーを作成し、画面上で移動可能な独自のウィンドウに表示します。

[Fabric] ペイン

[Fabric] ペインにはファブリックがグラフィック表示されます。表 5-1 に、ファブリック内のデバイスに応じて表示されるグラフィックの説明を示します。

[Fabric] ペインの下部には、次のタブがあります。

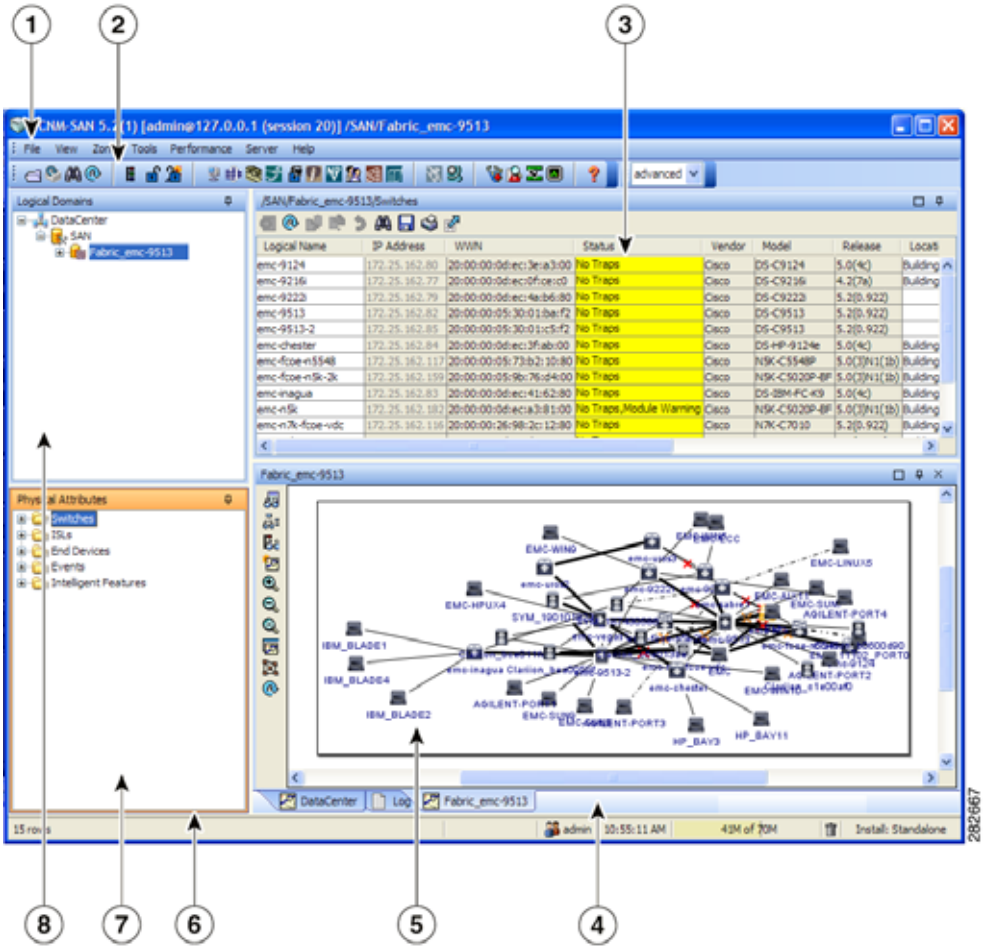
- [Fabric]：複数のファブリックを表示した場合は、ファブリックごとに独自のタブが表示されます。各タブをクリックして、ファブリックを切り替えることができます。
- [Log]：ファブリック検出など、Cisco DCNM-SAN での操作を説明するメッセージが表示されます。
- [Events]：管理ステーションで受信された SNMP トラップに関する情報を表示します。検出されたイベントと、ライセンス、SNMP、FICON などの重要なトラップが組み合わされて表示されます。

（注）　ファブリック マップは論理ドメイン ペインで選択した内容に基づいて表示されます。ファブリック ノードを選択すると、選択したファブリックに属するスイッチがすべてイネーブル化されます。グループ ノードを選択すると、グループ ノードの下位に表示されるスイッチがすべてイネーブル化されます。グループを 1 つだけ選択すると、選択したグループに属するスイッチだけがイネーブル化されます。

Cisco DCNM-SAN クライアント クイック ツアー：管理者向けの表示

ここでは、図 5-2 に示す Cisco DCNM-SAN クライアント インターフェイスについて説明します。

図 5-2　Cisco DCNM-SAN メイン ウィンドウ



1	メニュー バー：メニュー別に編成されたオプションにアクセスできます。
2	ツールバー：[File]、[Tools]、および [Help] メニュー内で最も一般的に使用されるオプションに直接アクセスするためのアイコンが配置されています。
3	[Information] ペイン：メニュー ツリーで選択されたオプションに関する情報が表示されます。
4	ステータス バー（右側）：検出プロセスで表示された最後のエントリ、および有効なエラー メッセージが表示されます。
5	[Fabric] ペイン：スイッチ、ホスト、ストレージなどのネットワーク ファブリックのマップが表示されます。また、ログおよびイベント データを表示するためのタブも配置されています。

6	ステータス バー（左側）：テーブルに表示される行数などの一時的なメッセージが短期間表示されます。
7	[Physical Attributes] ペイン：上記で選択されたファブリック、VSAN、またはゾーンに応じて、使用可能な設定作業がツリー表示されます。論理的に選択されたスイッチおよびエンド デバイスが一覧表示されます。
8	[Logical Domains] ペイン：設定済みの SAN、ファブリック、VSAN およびゾーンが表示され、ユーザ定義グループにアクセスできます。セグメント化された VSAN の横のラベルはセグメント数を表します。

（注）　各ペインのサイズを変更するには、各領域の境界をドラッグするか、[Minimize] または [Maximize] コントロールをクリックします。

メニュー バー

Cisco DCNM-SAN のメイン ウィンドウの上部にあるメニュー バーには、現在のファブリックの管理やトラブルシューティング、および [Fabric] ペインでの情報表示の制御を行うためのオプションが配置されています。メニュー バーには、次のメニューがあります。

- [File]：新しいファブリックを開く、現在のファブリックの再検出、スイッチの位置の特定、プリファレンスの設定、マップの印刷、[Fabric] ペイン ログのエクスポートを行います。
- [View]：マップの外観を変更します（[Fabric] ペイン ツールバーにもこれらのオプションと同じ機能が配置されています）。
- [Zone]：ゾーン、ゾーン セット、および Inter-VSAN Routing（IVR）を管理します。
- [Tools]：接続や設定の確認およびトラブルシューティングを行います（「Cisco DCNM-SAN トラブルシューティング ツール」（P.5-33）を参照）。
- [Performance]：Performance Manager および Cisco Traffic Analyzer を実行および設定し、レポートを生成します。
- [Server]：クライアントおよびファブリックの管理作業を実行します。Cisco DCNM-SAN サーバの管理と **purge** コマンドの実行が可能です。管理対象ファブリックが表示されます。
- [Help]：[Information] ペインに、特定のダイアログボックスに関するオンライン ヘルプ トピックが表示されます。

File

[File] メニューには、次のオプションがあります。

- [Open Fabric]：新しいスイッチ ファブリックを開きます。
- [Locate Switches and Devices]：SNMPv2 を使用し、読み取り専用コミュニティ ストリング public を指定して、SNMP 要求に応答するデバイスを検出します。サブネットに存在するファブリックに物理的に接続されていない他の Cisco MDS 9000 スイッチを検出する場合にこの機能を使用します。
- [Rediscover]：スイッチに最近加えられた変更のオンデマンド検出を実行し、Cisco DCNM-SAN クライアントを更新します。Cisco DCNM-SAN サーバがファブリック内のスイッチと非同期の状態で、次回のポーリング サイクルまで待てない場合にこのオプションを使用します。再検出オプションによって、ファブリックは削除されず追加し直されません。ファブリックを削除および追加できるのは、再検出オプションで Cisco DCNM-SAN サーバの更新に失敗した場合だけです。

- [Resync All Open Fabrics]：Cisco DCNM-SAN サーバによってすべてのファブリックが強制的に閉じられ、再度開かれます。Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバが同期していない場合にこのオプションを使用します。
- [Rediscover SCSI Targets]：SCSI ターゲット スイッチに最近加えられた変更のオンデマンド検出を開始します。Cisco DCNM-SAN サーバがファブリック内の SCSI ターゲット スイッチと非同期の状態で、次回のポーリング サイクルまで待てない場合にこのオプションを使用します。
- [Preferences]：プリファレンスを設定して、Cisco DCNM-SAN クライアントの動作をカスタマイズします。
- [Import Enclosures]：保存されたラックをインポートします。
- [Export]
  - [Map Image]：マップを指定された場所に生成およびエクスポートします。
  - [Visio]：マップを Visio ファイルにエクスポートします。
  - [Table]：テーブル データをテキスト ファイルにエクスポートします。
  - [Log]：ログをテキスト ファイルにエクスポートします。
  - [Events]：イベントをテキスト ファイルにエクスポートします。
  - [Enclosures]：ラックの値をテキスト ファイルにエクスポートします。
- [Print]：マップを印刷します。
- [Exit]：Cisco DCNM-SAN を終了します。

View

[View] メニューには、次のオプションがあります。

- [Refresh Map]：現在のマップを更新します。
- [Layout]
  - [Cancel]：現在のレイアウトをキャンセルします。
  - [Spring]：スプリング アルゴリズムに基づいてレイアウトを表示します。
  - [Quick]：スイッチに複数のエンド デバイスが存在している場合にレイアウトを素早く表示します。
- [Zoom]
  - [In]：ビューを拡大します。
  - [Out]：ビューを縮小します。
  - [Fit]：[Fabric] ペインに合わせてビューを表示します。
- [Grid]：グリッド ビューをイネーブル化します。
- [Overview Window]：表示するファブリック エリアの中央に [Fabric] ペインを移動します。この機能は、[Fabric] ペイン内に全体を表示できない大規模なファブリックの場合に役立ちます。
- [Legend]：ファブリック マップで使用されている凡例をすべて表示します。
- [Find in Map]：ファブリック マップからデバイスを検出します。

Zone

[Zone] メニューには、次のオプションがあります。

- [Edit Local Full Zone Database]：複数のスイッチに対してゾーンを作成できます。ゾーンは、アクセス コントロールを指定するための方法を提供します。ゾーン セットは、ファブリックでアクセス コントロールを実行するゾーンのグループです。ゾーン分割機能はすべて [Edit Local Full Zone Database] ダイアログボックスからアクセスできます。
- [Deactivate Zoneset]：アクティブ ゾーン セットを非アクティブ化します。
- [Copy Full Zone Database]：新しいゾーン セットを作成します。Cisco MDS ファミリ スイッチでは、アクティブ ゾーン セットを編集できません。ただし、アクティブ ゾーン セットをコピーして、編集可能な新しいゾーン セットを作成できます。
- [Merge Analysis]：Cisco MDS スイッチを 2 つ相互接続した場合にゾーンを正常にマージできるか判断できます。相互接続されたスイッチ ポートで同じ名前の VSAN を使用できる場合、またはこれらのポートに同じ名前のゾーンが含まれている場合、Cisco DCNM-SAN はこのゾーンに同じメンバーが含まれているか確認します。マージ分析ツールは、マージの実行前、またはファブリックを相互接続した後にゾーン マージ障害の原因を判別するのに実行できます。
- [Merge Fail Recovery]：隣接スイッチのアクティブなゾーン セット データベースをインポートして現在アクティブなゾーン セットと置換するか、現在のデータベースを近隣スイッチにエクスポートしてポートを分離状態から回復します。
- [Migrate Non-MDS Database]：Cisco DCNM-SAN を使用して MDS 以外のデータベースを移行します（このタスクを実行するには Zone Migration Wizard が必要になる場合もあります）。
- IVRivr
  - [Deactivate Zoneset]：アクティブ ゾーン セットを非アクティブ化します。
  - [Copy Full Zone Database]：他のスイッチから IVR のフル ゾーン データベースをコピーして IVR ゾーン データベースを回復します。
  - [Copy Full Topology]：アクティブ ゾーン データベースまたはフル ゾーン データベースからコピーしてトポロジを回復します。

Tools

[Tools] メニューには、次のオプションがあります。

- Health
  - [Switch Health]：特定のスイッチのコンポーネントのステータスを判断します。
  - [Fabric Configuration]：現在の設定を特定のスイッチまたはポリシー ファイルと比較してスイッチの設定を分析します。スイッチの設定をファイルに保存し、ファイル内の設定とすべてのスイッチを比較することができます。
  - [Show Tech Support]：トラブルシューティングするため、スイッチに関する情報を大量に収集します。ファブリックに存在する 1 つ以上のスイッチに対して Cisco DCNM-SAN から **show tech support** コマンドを発行すると、各コマンドの結果はテキスト ファイルに出力されます。指定されたディレクトリ内で、スイッチごとに 1 つのファイルが作成されます。その後、Cisco DCNM-SAN を使用してこれらのファイルを表示できます。
- Connectivity
  - [End to End Connectivity]：スイッチ ファブリック内のデバイス間の接続およびルートを判別します。このツールは ping テストを使用し、エンド デバイスの各ペアが同じ VSAN 内または同じアクティブ ゾーン内にあるかを調べて、各ペアが相互に通信可能かどうかをチェックします。
  - [Ping]：他のスイッチからユーザのスイッチのポートへの接続状態を判断します。

  - [Trace Route] : [Fabric] ペインで現在選択されている 2 つのエンド デバイス間の接続を確認します。
  - [Compact Flash Report] : ファブリックを自動的にスキャンして、コンパクト フラッシュのステータスを表示したレポートを生成します。
- NPV
  - CFS Static Peer Setup : NPV イネーブル スイッチに対する CFS 実行時に使用されるピア リストを管理します。スタティック ピア リストを設定すると、スイッチに関する CFS 検出結果がリストすべてのピアに対してスタティック モードに変更されます。Cisco DCNM-SAN では、スタティック ピア リストは自動更新されません。新しいスイッチをファブリックに追加した場合は、CFS Static Peer Setup Wizard を使用してリストを更新してください。
  - Traffic Map Setup : 外部インターフェイスのリストをサーバに対して設定し、中断ロード バランシングをイネーブル化またはディセーブル化します。[Traffic Map Setup] を使用して、サーバがトラフィック管理に使用する外部ポートを指定できます。
  - Flex Attach Pre-Configure Server : スイッチのポートすべてに対してポート設定（FlexAttach のイネーブル化/ディセーブル化、デフォルト VSAN ID の設定、インターフェイス ステータスの設定など）を変更します。
  - Flex Attach Move Server : 同じ NPV デバイス内の他のポートまたは他の NPV デバイスにサーバを移動します。
  - Flex Attach Replace Server : SAN を変更することなく障害が発生したサーバを同じポート上の新しいサーバと置換します。
- Data Mobility Manager
  - Server Based : サーバ ベースのデータ マイグレーションを実行します。
  - Storage based : ストレージ ベースのデータ マイグレーションを実行します。
  - Server LUN Discovery : LUN 検出を実行して移行可能な LUN を選択します。また、既存および新しいストレージに存在する LUN を一致させてセッションの作成を自動化します。
- FCoE : FCoE Configuration Wizard を起動して、仮想ファイバ チャネル インターフェイスを作成します。
- Port Channel : 選択された ISL から PortChannels を手動または自動で作成できます。
- DPVM Setup : ダイナミック ポート VSAN メンバシップの確立、自動学習機能のイネーブル化、DPVM データベースのアクティブ化を実行します。
- IP SAN
  - FCIP Tunnel : ギガビット イーサネット ポート間に FCIP リンクを作成します。ファイバ チャネルの書き込みアクセラレーションと IP 圧縮をイネーブル化します。
  - iSCSI Setup : iSCSI イニシエータのゾーンを作成し、ターゲットに許可された VSAN リストに VSAN を追加します。
  - SAN Extension Tuner : FCIP のパフォーマンスを最適化します。直接アクセス（磁気ディスク）またはシーケンシャル アクセス（磁気テープ）SCSI I/O コマンドを生成して対象のトラフィックを指定された仮想ターゲットに転送します。このオプションは設定オプションに基づいて仮想ターゲット SCSI I/O コマンド（読み取り、書き込み）を生成するのに使用されます。
- Security
  - Port Security : Cisco MDS 9000 ファミリのスイッチ ポートへの不正アクセスを防止します。侵入に関する試みを拒否し、管理者にこれらの侵入を報告します。
  - IP ACL : IPv4-ACL Wizard を使用して指定された IPv4-ACL または IPv6-ACL プロファイルの整理された IP フィルタ リストを作成します。

- Install
  - License：ファブリック内の選択したスイッチで、ライセンスのダウンロードおよびインストールを容易に実行できるようにします。
  - Software：ファブリック内の選択したスイッチでイメージの互換性を確認し、ソフトウェアイメージをインストールします。
- Flow Load Balance Calculator：FICON フローに最適な最適なロードバランスを設定します。この計算機能は、ファブリック内のスイッチ検出またはフロー検出に依存しません。
- Device Manager：スイッチの Device Manager を呼び出します。
- Command Line Interface：コマンドラインを使用して操作できます。
- Run CLI Commands：複数のスイッチに対してコマンドライン操作を一括で実行します。

Performance

[Performance] メニューには、次のオプションがあります。

- Create Flows：ホストからストレージへのフロー、ストレージからホストへのフロー、または双方向フローを作成します。フローは収集コンフィギュレーション ファイルに追加してホストまたはストレージ要素のペア間のトラフィックを監視します。

Server

[Server] メニューには、次のオプションがあります。

- Admin：コントロール パネルを開きます。
- Purge Down Elements：ファブリックの停止している要素をすべて消去します。

Help

[Help] メニューには、次のオプションがあります。

- Contents：オンライン ヘルプ コンテンツを起動します。
- Config Guide：『Cisco DCNM-SAN Configuration Guide』を起動します。
- About：Cisco DCNM-SAN に関する情報を表示します。

ツールバー

Cisco DCNM-SAN のメイン ツールバーには、頻繁に使用されるメニュー バー オプションにアクセスするためのアイコンが配置されています（表 5-3 を参照）。

表 5-3　Cisco DCNM-SAN クライアントのメイン ツールバー

アイコン	説明
	スイッチ ファブリックを開きます。
	現在のファブリックを再検出します。
	マップを検索します。
	VSAN を作成します。
	DPVM ウィザードを起動します。
	Port Security ウィザードを起動します。
	フル ゾーン データベースを編集します。
	IVR ゾーン ウィザードを起動します。
	FCoE 設定ウィザードを起動します。
	PortChannel ウィザードを起動します。
	FCIP ウィザードを起動します。
	iSCSI ウィザードを起動します。
	NPVM ウィザードを起動します。
	QoS ウィザードを起動します。

表 5-3　Cisco DCNM-SAN クライアントのメイン ツールバー （続き）

アイコン	説明
	ユーザおよびロールを設定します。
	IP-ACL ウィザードを起動します。
	License Install ウィザードを起動します。
	Software Install ウィザードを起動します。
	スイッチ ヘルス分析を実行します。
	ファブリック設定分析を実行します。
	エンドツーエンド接続分析を実行します。
	ISL パフォーマンスを監視します。[Information] ペインに、ファブリック内のすべてのインターフェイスのリアルタイム ISL パフォーマンス情報が表示されます。
	オンライン ヘルプが表示されます。

[Logical Domains] ペイン

[Logical Domains] ペインでは、ファブリック、VSAN、およびゾーンの属性を管理したり、ユーザ定義グループにアクセスしたりできます。NX-OS Release 4.2(0) 以降では、[SAN] および [LAN] ノードは [Datacenter] ノードの下位に表示され、ファブリックはすべて [SAN] ノードの下位に表示されるようになりました。Cisco DCNM-SAN のツリーから [Datacenter] ノードを選択すると、すべてのスイッチと ISL が表示されます。[LAN] ノードを選択すると、イーサネット スイッチおよびイーサネット リンクだけが表示されます。ファブリック ノードの VSAN は、VSAN ID に基づいてソートされます。セグメント化された VSAN はファブリック ノードの下位に表示されます。セグメント化された VSAN の横のラベルはセグメント数を表します。セグメント化された VSAN および VSAN の下位のセグメントを展開できます。ツリー内のいずれかのフォルダを右クリックして、ポップアップ メニューのメニュー項目をクリックします。該当する設定ダイアログボックスが表示されます。

ファブリックのデフォルト名は VSAN 1 の主要スイッチの名前、IP アドレス、または WWN です。VSAN 1 がセグメント化されている場合、デフォルト名は最も小さい WWN の主要スイッチから選択されます。ファブリック名は次のように表示されます。

- Fabric <sysName>
- Fabric <ipAddress>
- Fabric <sWWN>

Cisco DCNM-SAN を使用してファブリック名を変更するには、次の手順を実行します。

ステップ 1　[Server] > [Admin] を選択します。

[Control Panel] ダイアログボックスが表示されます。

ステップ 2　ファブリックの名前をダブルクリックし、そのファブリックの新しい名前を入力します。

ステップ 3　[Apply] をクリックすると、名前が変更されます。

フィルタリング

Cisco DCNM-SAN は、ユーザに必要なデータだけを表示できるフィルタリング機能を備えています。フィルタリングするには、[Logical Domains] ペインからファブリックおよび VSAN を選択します。これにより、[Fabric] ペインの表示範囲が絞られます。選択した項目に属さない情報はすべて薄く表示されます。選択した項目に属さない情報は、[Information] ペインの表にも表示されません。選択したフィルタは Cisco DCNM-SAN ウィンドウの右上に表示されます。

さらに範囲を絞り込むには、Physical Attributes で属性を選択します。それに応じて Cisco DCNM-SAN テーブル、表示、フィルタ条件が変更されます。

[Physical Attributes] ペイン

現在選択されているファブリック、VSAN、またはゾーン内のスイッチの管理に使用できるオプションをツリー表示するには、[Physical Attributes] ペインを使用します。

オプションを選択するには、フォルダをクリックして使用可能なオプションを表示し、オプションをクリックします。[Information] ペインに、選択したオプションに関する情報が表形式で表示されます。[Physical Attributes] ペインには次のメイン フォルダが配置されています。

- Switches：ハードウェア、システム、ライセンス、およびコンフィギュレーション ファイルの表示および設定を行います。
- Interfaces：FC 物理インターフェイス、FC 論理インターフェイス、VFC（FCoE）インターフェイス、イーサネット インターフェイス、SVC インターフェイス、および PortChannel インターフェイスを表示および設定できます。
- FC Services：ファイバ チャネル ネットワーク設定の表示および設定を行います。
- IP：IP ストレージおよび IP サービスの表示および設定を行います。
- Events：イベント、アラーム、しきい値、通知、およびインフォームの表示および設定を行います。
- Security：MDS 管理および FC-SP セキュリティの表示および設定を行います。
- FCoE：FCoE インターフェイスの表示および設定を行います。
- ISLs：スイッチ間リンクの表示および設定を行います。
- End Devices：エンド デバイスの表示および設定を行います。

（注）　データセンター スイッチの詳細な物理属性の表示または接続の監視はできません。[Datacenter] ノードまたは [LAN] ノードを選択すると、[Physical Attributes] ペインには何も表示されません。

テーブルのコンテキスト メニュー

テーブルを右クリックすると、ポップアップ メニューが表示されます。メニューのオプションは [Physical Attributes] ペインで選択したオプションによって異なります。テーブルに表示されたデバイスを右クリックすることで、さまざまなオプションを実行できます。スイッチ、ISL、およびエンド デバイスで利用できるオプションを表示するには、次のセクションで説明される手順に従ってください。

スイッチ オプション

[Datacenter] ノードを選択すると、検出されたすべてのスイッチがスイッチ テーブルに表示されます。[SAN] ノードまたはファブリック ノードを選択すると、スイッチ テーブルにファイバ チャネル スイッチがすべて表示され、[LAN] ノードを選択すると、スイッチ テーブルにイーサネット スイッチがすべて表示されます。

スイッチ テーブルのオプションをすべて表示するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[Switches] をクリックします。

ステップ 2　テーブルのデバイスを右クリックします。

ポップアップ メニューには、次のオプションがあります。

- Apply Changes：スイッチに変更が適用されます。
- Refresh Values：現在の値が更新されます。
- Undo Changes：スイッチに加えられた変更を元に戻します。
- Export to File：値をファイルにエクスポートします。
- Print Table：テーブルを印刷します。
- Detach Table：テーブルを分離します。
- Switch Attributes：スイッチのプロパティを変更します。
- Interface Attributes：インターフェイスのプロパティを変更します。
- Element Manager：スイッチを管理します。
- Command Line Interface：コマンドラインを使用して操作できます。
- Copy：スイッチをコピーします。
- Purge：スイッチを消去します。
- Fix Location：スイッチを現在のロケーションに固定します。
- Align：スイッチに対してアライメントを実行します。
- Show End Devices：エンド デバイスを表示します。
- Expand Multiple Links：スイッチのリンクを展開します。
- Other：その他のオプションです。
- Group：スイッチをグループ化します。

ISL オプション

[Datacenter] ノードを選択すると、ISL テーブルにファイバ チャネル リンクとイーサネット リンクがすべて表示されます。[LAN] ノードを選択すると、ISL テーブルにイーサネット リンクがすべて表示されます。

ISL テーブルのオプションをすべて表示するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[ISLs] をクリックして、[Summary] タブをクリックします。

ステップ 2　テーブルのデバイスを右クリックします。

ポップアップ メニューには、次のオプションがあります。

- Refresh Values：現在の値が更新されます。
- Copy：指定されたフィールドの情報をコピーします。
- Find：入力されたストリングに基づいて検索します。
- Export to File：値をファイルにエクスポートします。
- Print Table：テーブルを印刷します。
- Detach Table：テーブルを分離します。
- Interface Attributes：インターフェイスのプロパティを変更します。
- Element Manager：デバイスを管理します。
- FCIP Tunnel Attributes：FCIP のトンネリング プロパティを変更します。
- Create Port Channel：ポート チャネルを作成します。
- Re-enable：ディセーブル化したデバイスをイネーブル化します。
- Enable FC-SP：FC-SP をイネーブル化します。
- SAN Extention Tuner：FCIP のパフォーマンスを最適化します。
- Purge：デバイスを消去します。

（注）　テーブルからポート チャネルを選択すると、ポップアップ メニューには次のオプションが追加されます。

- Member Attributes：メンバーのプロパティを変更します。
- Channel Attributes：ポート チャネルのプロパティを変更します。
- Edit：チャネルのプロパティを編集します。

エンド デバイスのオプション

デバイス オプション テーブルのオプションを表示するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[End Devices] をクリックして、[Summary] タブをクリックします。

ステップ 2　テーブルのデバイスを右クリックします。

ポップアップ メニューには、次のオプションがあります。

- Apply Changes：デバイスに変更が適用されます。
- Refresh Values：現在の値が更新されます。

- Copy：フィールド固有の情報をコピーします。
- Paste：コピーされたテキストを貼り付けます。
- Undo Changes：デバイスに加えられた変更を元に戻します。
- Find：入力されたストリングに基づいて情報を検索します。
- Export to File：値をファイルにエクスポートします。
- Print Table：テーブルを印刷します。
- Detach Table：テーブルを分離します。
- Device Attributes：デバイスのプロパティを変更します。
- Interface Attributes：インターフェイスのプロパティを変更します。
- Element Manager：デバイスを管理します。
- Command Line Interface：コマンド ラインを使用して操作できます。
- Copy：スイッチをコピーします。
- Purge：スイッチを消去します。
- Fix Location：スイッチを現在のロケーションに固定します。
- Align：スイッチに対してアライメントを実行します。
- Ping：他のデバイスに ping を実行します。
- Trace Route：ネットワークを通過したパケットのルートを判別します。
- Select Dependent Ports：依存関係があるポートを選択します。
- Group：デバイスをグループ化します。

[Information] ペイン

[Information] ペインには、[Logical Domains] ペインまたは [Physical Attributes] ペインのメニュー ツリーで選択されたオプションに対応する情報テーブルが表示されます。[Information] ペインのツールバーには、表 5-4 に示された処理を 1 つまたは複数実行するためのボタンが配置されています。

表 5-4　[Information] ペインのツールバー

アイコン	説明
	コンフィギュレーションの変更を適用します。
	テーブルの値を更新します。
	テーブル内に新しい行を作成するためのダイアログボックスを開きます。
	現在強調表示されている行をテーブルから削除します。

表 5-4　[Information] ペインのツールバー （続き）

アイコン	説明
	行のデータを他の行にコピーします。
	行のデータを他の行に貼り付けます。
	直前の変更を元に戻します。
	テーブルから指定されたストリングを検索します。
	情報をファイルにエクスポートし、保存します。
	[Information] ペインの内容を出力します。
	[Information] ペイン内のテーブルの編集不可能なコピーを作成し、画面上で移動可能な独自のウィンドウに表示します。

（注）　変更を加えた場合はコンフィギュレーションを保存する必要があります。保存しないとデバイスの再起動後に変更が失われます。

（注）　ツールバーに配置されるボタンは、選択したオプションによって変わります。[Information] ペインで選択されたフィールドなどのオブジェクトに応じて、ボタンがアクティブまたは非アクティブ（薄い表示）になります。

分離可能なテーブル

Cisco DCNM-SAN で分離可能なテーブルを使用すると、テーブルを分離し、デスクトップ上の別のエリアに移動して、各 VSAN の類似テーブルを比較することができます。1 つのビューで情報テーブルを開いたまま、Cisco DCNM-SAN の別のエリアを調べることができます。テーブルを分離するには、Cisco DCNM-SAN の [Information] ペインで [Detach Table] アイコンをクリックします。

[Fabric] ペイン

[Fabric] ペインにはファブリックがグラフィック表示されます。表 5-5 に、ファブリック内のデバイスに応じて表示されるグラフィックの説明を示します。

表 5-5　Cisco DCNM-SAN のグラフィック

アイコンまたはグラフィック	説明
	ディレクタ クラスの MDS 9000 ファイバ チャネル スイッチ。
	ディレクタ クラス以外の MDS 9000 ファイバ チャネル スイッチ。
	Nexus 7000 スイッチ。
	Nexus FCoE またはファイバ チャネル スイッチ。
	Catalyst LAN スイッチ。
	一般的なファイバ チャネル スイッチ。
	Cisco SN5428。
	デバイス内にオレンジの破線または点線が引かれている場合、このデバイスは管理できますが、動作時に問題が発生します。
	デバイスまたはリンク内にオレンジの「X」が破線または点線で示されている場合、そのデバイスまたは ISL は正常に動作していません。
	デバイス内にレッドの直線が引かれている場合は、このデバイスを管理できません。
	デバイスまたはリンク内にレッドの「X」が示されている場合は、デバイスがダウンしているか、または ISL がダウンしています。
	ファイバ チャネル HBA（またはラック）。
	ファイバ チャネル ターゲット（またはラック）。
	iSCSI ホスト。

表 5-5　Cisco DCNM-SAN のグラフィック （続き）

アイコンまたはグラフィック	説明
	ファイバ チャネル ISL およびエッジ接続。
	ファイバ チャネル PortChannel。
	IP ISL およびエッジ接続。
	IP PortChannel。
	DWDM 接続。
	NPV 接続。
	ファイバ チャネル ループ（ストレージ）。
	IP クラウド（ホスト）。このアイコンは、Cisco DCNM-SAN の [Fabric] ペインで SAN（複数のファブリック）を表示する際の、ファブリックの表示にも使用されます。
	ボックスで囲まれているデバイス、クラウド、またはループには、非表示リンクが接続されています。

スイッチまたはディレクタがグレー表示されている場合、Cisco DCNM-SAN はそれらと通信できません。

[Fabric] ペインの下部には、次のタブがあります。

- [Fabric]：複数のファブリックを表示した場合は、ファブリックごとに独自のタブが表示されます。各タブをクリックして、ファブリックを切り替えることができます。
- [Log]：ファブリック検出など、Cisco DCNM-SAN での操作を説明するメッセージが表示されます。
- [Events]：管理ステーションで受信された SNMP トラップに関する情報を表示します。検出されたイベントと、ライセンス、SNMP、FICON などの重要なトラップが組み合わされて表示されます。

[Fabric] ペインで大きいファブリックを表示する場合は、次のタスクを実行すると便利です。

- エンド デバイス ラベルをオフにします。
- ループを折りたたみます。

- 展開された複数のリンクを折りたたみます（折りたたまれた複数のリンクは、太い一重線で表示されます）。
- VSAN でファブリックの一部を薄い表示にするか非表示にします。

（注）　VSAN ツリーで VSAN、ゾーン、またはゾーン メンバーを選択すると、マップの強調表示が変更され、選択されたオブジェクトが識別されます。強調表示を解除するには、[Fabric] ペイン ツールバーの [Clear Highlight] ボタンをクリックするか、またはポップアップ メニューで [Clear Highlight] を選択します。

コンテキスト メニュー

[Fabric] ペインのアイコンを右クリックすると、ポップアップ メニューが開き、選択されたアイコンのタイプに応じて異なるオプションが表示されます。オブジェクトに応じて、次の機能を持つオプションが表示されます。

- 選択されたスイッチに対して Device Manager のインスタンスを開きます。
- 選択されたスイッチの CLI（コマンドライン インターフェイス）セッションを開きます。
- 選択されたオブジェクトの表示名をコピーします。
- デバイスに **ping** または **traceroute** コマンドを実行します。
- エンド デバイスを表示または非表示にします。
- 属性を表示します。
- PortChannels のメンバーを停止して、ディセーブルにします。
- ISL のトランキング モードを設定します。
- 選択された ISL に PortChannel を作成または追加します。

[Fabric] ペインには、マップの外観を保存、出力、および変更するためのオプションが配置されたツールバーがあります。マップを右クリックすると、ポップアップ メニューが開き、マップの外観を変更するためのオプション（ツールバーと同じ機能）が表示されます。

（注）　[Fabric] ペインから Web ベース アプリケーションまたは Web ベースでないアプリケーションを起動できます。これには、IP アドレスをストレージ ポートまたはラックに割り当てます。次に、右クリックしてポップアップ メニューを開き、[Device Manager] を選択します。

マップの保存

[Fabric] ペインのマップは、イメージとして、または編集可能な Visio 図として保存できます。また、リンク ラベル付きで保存することも、リンク ラベルなしで保存することも可能です。作成された Visio 図は編集が可能で、次の 2 つのレイヤに保存できます。

- デフォルト レイヤには、ファブリック内のすべてのスイッチおよびリンクが含まれます。
- エンド デバイス レイヤには、エンド デバイスが含まれ、これをオフにすることにより、Visio 図からエンド デバイスを削除できます。

Visio 図としてマップを保存するには、[Files] > [Export] > [Visio] を選択し、[Map] または [Map with link labels] を選択します。保存された Visio 図には、[Fabric] ペインで選択した表示オプションが保持されます。たとえば、マップ内の複数のリンクを折りたたんで、そのリンクを Visio 図としてエクスポートすると、その Visio 図にはこれらの複数のリンクが 1 つの太いリンクとして表示されます。

[Tools] メニューの Show Tech Support オプションでも、マップを Visio 図として保存できます。

要素の消去

[Fabric] ペインでは、[Refresh Map] アイコンをクリックすることによって、いつでもマップをリフレッシュできます。[Refresh Map] アイコンを使用すると、マップは再描画されますが、停止している要素は消去されません。停止している要素を消去するには次のいずれかを実行します。

- [Server] > [Purge Down Elements] をクリックします。これによって、ファブリック内の停止している要素がすべて消去されます。
- [Fabric] ペインを右クリックし、[Purge Down Elements] を選択します。
- 停止している要素を右クリックし、[Purge] を選択します。この操作によって消去されるのは、ファブリック内の要素のうち、選択したものだけです。

（注） 停止していない要素を選択して消去した場合、その要素は次回のファブリック検出サイクルで再表示されます。

複数のファブリックの表示

Cisco DCNM-SAN では、同じペイン内に複数のファブリックを表示できます。

シード スイッチを選択しなくても、両方のファブリックの情報が表示されます。ファブリックの詳細を表示するには、[Fabric] ペインの下部でそのファブリックのタブを選択するか、または [SAN] タブのそのファブリックの [Cloud] アイコンをダブルクリックします。

（注） ラックの名前は一意でなければなりません。各ポートに同じラック名が使用されている場合、Cisco DCNM-SAN には両方のファブリックに接続されているホスト/ターゲット ラックが表示されます。auto-creation をディセーブルにするか、または一意のラック名を作成することによって、この問題を回避できます。

グループによるフィルタリング

スイッチまたはエンド ポートのグループを作成することによって、[Fabric] ペインの表示をフィルタリングできます。Cisco DCNM-SAN でグループを作成するには、次の手順を実行します。

ステップ 1　[Fabric] ペインのマップでスイッチまたはエンド ポートを右クリックし、[Group] > [Create] を選択します。

[Edit User Defined Group] ダイアログボックスが表示されます。

ステップ 2　[Name] フィールドにグループ名を入力します。

ステップ 3　矢印を使用して、[Available] カラムから [Selected] カラムに、追加するスイッチまたはエンド ポートを移動します。

ステップ 4　[OK] をクリックして、グループを保存します。

Cisco DCNM-SAN の既存のグループにスイッチまたはエンド ポートを追加するには、次の手順を実行します。

ステップ 1　スイッチまたはエンド ポートを右クリックして、[Group] > [Add To] > [*YourGroupName*] を選択します。

[Edit User Defined Group] ダイアログボックスが表示されます。

ステップ 2　矢印を使用して、[Available] カラムから [Selected] カラムに、追加するスイッチまたはエンド ポートを移動します。

ステップ 3　[OK] をクリックして、更新されたグループを保存します。

作成したグループに基づいて表示をフィルタリングするには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインの [Groups] フォルダを展開します。

作成したグループのリストが表示されます。

ステップ 2　フィルタリングするグループ名をクリックします。

[Fabric] ペインで、グループ内のスイッチまたはエンド デバイスは通常どおりに表示され、その他のスイッチおよびエンド デバイスはすべてグレーに表示されます。

ステップ 3　[Logical Domains] ペインで [Groups] フォルダをクリックすると、通常の表示に戻ります。

（注）　すべての CFS メンバー スイッチが表示される場合、誤設定を避けるため、ユーザ定義グループのテーブルは、CFS 制御機能がイネーブルに設定されているスイッチを除くグループ内のスイッチに基づいてフィルタリングされます。

ステータス バー

[Cisco DCNM-SAN] ウィンドウの下部にあるステータス バーの右側には、検出プロセスで表示された最後のエントリと、有効なエラー メッセージが表示されます。ファブリックに変更が行われた場合は、新規検出が必要であることを示すメッセージが表示されます。ステータス バーには、一時的なメッセージ（テーブルに表示される行数など）が短期間表示されたり、検出時の問題点が長期間表示されたりします。

DCNM-SAN クライアントの起動

Cisco SAN-OS 3.x および NX-OS Release 4.x 以降、Fabric Manager Client のログイン手順が変更されました。Cisco SAN-OS 3.2(1) 以前の Cisco SAN-OS を実行している場合は、「Cisco SAN-OS Release 3.1(1) ～ 3.2(1) のシード スイッチの設定」（P.A-1）または 「Cisco SAN-OS Release 3.1(1) 以前のリリースのシード スイッチの設定」（P.A-3）の場合は、ログイン手順に従ってください。

Cisco SAN-OS Release 3.2(1) 以降で Fabric Manager Client を起動する

Fabric Manager Client を起動するには、次の手順を実行します。

（注）　次の手順で説明されているとおり、ネットワーク管理者は最初に、Cisco DCNM-SAN Web サーバを使用して Cisco DCNM-SAN クライアントを起動する必要があります。管理者によって [Cisco DCNM-SAN Client] アイコンがデスクトップにインストールされると、ユーザはそのアイコンをダブルクリックして Cisco DCNM-SAN クライアントを起動できます。

ステップ 1　ブラウザを開き、Cisco DCNM-SAN サーバをインストールした IP アドレスを入力します。Cisco DCNM-SAN サーバをローカル ワークステーションにインストールした場合は、localhost と入力します。

[Cisco DCNM Web Client Login] ダイアログボックスが表示されます。

ステップ 2　ユーザ名およびパスワードを入力し、[Login] をクリックします。

[Cisco DCNM Web Client Summary] ページが表示されます。

ステップ 3　このページの右上にある [Download] リンクをクリックします。

Cisco DCNM-SAN 用と Device Manager 用の [Download] ページが表示されます。

ステップ 4　**Cisco DCNM-SAN** 用のリンクをクリックします。

Cisco DCNM-SAN クライアントを初めて起動するときは、Cisco DCNM-SAN のショートカットを作成するかどうかを尋ねるメッセージが表示されます。

ステップ 5　Cisco DCNM-SAN のショートカットを作成する場合は、[Yes] をクリックします。

（注）　このメッセージが表示されるのは、Cisco DCNM-SAN クライアントの初回起動時のみです。[No] を選択すると、選択が記憶され、以降選択する必要がなくなります。その場合は、Cisco DCNM-SAN Web クライアントを使用して Cisco DCNM-SAN クライアントを起動する必要があります。

ステップ 6　ソフトウェアがインストールされ、デスクトップにアイコンが作成されたら、[Cisco DCNM-SAN] アイコンをダブルクリックして Cisco DCNM-SAN を起動します。

[Cisco DCNM-SAN Login] ダイアログボックスが表示されます。

ステップ 7　Cisco DCNM-SAN サーバのユーザ名とパスワードを入力します。

ステップ 8　TCP ベースのプロキシ サーバを介して Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバとの通信を行いたい場合は、[Use SNMP Proxy] チェックボックスをオンにします。

ステップ 9　[Login] をクリックします。Cisco DCNM-SAN サーバに正しくログインしたら、シード スイッチを設定してアクセス権があるファブリックを開くことができます。

（注）　Cisco DCNM-SAN クライアントの初回起動時、または使用可能なファブリックがない場合には、[Discover New Fabric] ダイアログボックスが表示されます。

[Discover New Fabric] ダイアログボックスが表示されます。

（注）　新しいファブリックを検出できるのは、ネットワーク管理者だけです。

ステップ 10　[Ethernet (CDP)] オプション ボタンをクリックし、Cisco Discovery Protocol（CDP）を使用して検出を実行します。

ステップ 11　NX-OS Release 4.2(0) 以降、Fabric Manager では、Nexus 5000 スイッチ、Nexus 7000 スイッチ、Catalyst 4000 スイッチおよび Catalyst 6000 スイッチなどのイーサネット スイッチの検出に Cisco Discovery Protocol を使用します。CDP 検出には CDP シード スイッチを使用してください。Fabric Manager で使用する Cisco MDS 9000 ファミリ スイッチまたは Cisco Nexus 5000 シリーズにファブリック シード スイッチを設定します。

ステップ 12　スイッチに設定したプライバシー プロトコルに応じて、[Auth-Privacy] オプションを選択します。

a.　スイッチにまだプライバシー プロトコルを設定していない場合は、MD 5（プライバシーなし）の Auth-Privacy オプションを選択します。

b.　スイッチにプライバシー プロトコルを設定している場合は、設定に適した [Auth-Privacy] オプションを選択してください。

（注）　Catalyst スイッチでは設定に MD5-DES がほとんど使用されないため、CDP 検出に SNMP v2 クレデンシャルを使用できます。

（注）　クリーン ファブリック検出を実行する場合は、ファブリックを削除してから再検出します。クリーン LAN 検出を実行するには、LAN を非管理にして、CDP シード スイッチを削除し再検出します。

ステップ 13　スイッチのユーザ名とパスワードを入力します。

ステップ 14　（任意）検出を制限するには、VSAN 範囲を指定します。
スコーピングを設定すると、Cisco DCNM-SAN クライアントで検出されるリソースが制限されます。一定範囲内の VSAN を検出対象に含めるか、検出対象から除外することができます。

a.　検出対象を一定範囲内の VSAN に制限するには、[Included VSAN List] オプション ボタンをクリックします。VSAN の範囲を指定します。

b.　一定範囲内の VSAN を検出対象から除外するには、[Excluded VSAN List] オプション ボタンをクリックします。除外する VSAN の範囲を指定します。

ステップ 15　[Discover] をクリックします。

[Control Panel] ダイアログボックスが表示されます。

[Fabric] タブの下に検出対象と検出対象外の VSAN リストが表示されます。

（注）　サーバとクライアントが同じワークステーションで稼動していて、データベース内にライセンスのないファブリックがあると、ダイアログボックスにメッセージが表示されます。管理対象外のファブリック（ライセンスの状態は unknown）がある場合もメッセージが表示されます。

（注）　コントロール パネルの開いたタブには検出されたファブリックがすべて表示されます。検出されたイーサネット スイッチをすべて表示するには [Open] ボタンをクリックします。

ステップ 16　[Select] カラムで開くファブリックの隣のチェックボックスをオンにするか、[Discover] をクリックして、新しいファブリックを追加します。

（注）　ファブリックを継続管理または非管理にできるのはネットワーク管理者だけです。詳細については、「継続的管理対象のファブリックの選択」（P.3-6）を参照してください。

ステップ 17　[Open] をクリックして、選択したファブリックを開きます。

（注）
- ファブリックの表示が不完全な場合は、VSAN の制約がないユーザを使用してファブリックを再検出します。
- ファブリックに Cisco Nexus 5000 シリーズ スイッチが含まれている場合は、[Physical Attributes] ペインの
  [Switches] > [Interfaces] > [Ethernet] ツリーにレイヤ 2 ノード、
  [Switches] > [Interfaces] ツリーに VFC（FCoE）ノード、
  [Switches] ツリーに FCoE ノードが表示されます。
- ファブリック内の Cisco Nexus 5000 シリーズ スイッチについては、スイッチのツールチップに、仮想ファイバ チャネル インターフェイスとそれに対応するイーサネット インターフェイスのバインド情報、たとえば vfc2(eth1/4) などが表示されます。

Cisco DCNM-SAN の実行中のインスタンスから Cisco DCNM-SAN クライアントを起動するには、次の手順を実行します。

ステップ 1　[File] > [Open] を選択するか、Cisco DCNM-SAN ツールバーの [Open Switch Fabric] アイコンをクリックします。

[Control Panel] ダイアログボックスが表示されます。

ステップ 2　[Select] カラムで開くファブリックの隣のチェックボックスをオンにして、[Open] をクリックします。

（注）　Cisco DCNM-SAN を使用して行われた変更は、管理対象スイッチの実行コンフィギュレーションに適用されます。コンフィギュレーションの変更やゾーンのアクティブ化などの操作を行うと、Cisco DCNM-SAN を終了する前に変更を保存するように求めるプロンプトが表示されます。

起動パッドを使用した Cisco DCNM-SAN クライアントの起動

Cisco NX-OS Release 4.2(0) 以降では、Cisco DCNM-SAN 起動パッドを使用してサーバの IP アドレスを指定するだけで任意のサーバに接続できます。起動パッドを使用すると、Cisco DCNM-SAN サーバ バージョン 3.3(0) 以降の任意のサーバに接続できます。起動パッドでは、HTTP プロトコルを使用するサーバとの接続を確立できます。

起動パッドを使用して Cisco DCNM-SAN クライアントを起動するには、次の手順を実行します。

ステップ 1　ブラウザを開き、Cisco DCNM-SAN サーバをインストールした IP アドレスを入力します。Cisco DCNM-SAN サーバをローカル ワークステーションにインストールした場合は、localhost と入力します。

[Cisco DCNM-SAN Web Server Login] ダイアログボックスが表示されます。

ステップ 2　ユーザ名およびパスワードを入力し、[Login] をクリックします。

[Cisco DCNM-SAN Web Client Summary] ページが表示されます。

ステップ 3　このページの右上にある [Download] リンクをクリックします。

Cisco DCNM-SAN 用と Device Manager 用の [Download] ページが表示されます。

ステップ 4　**Cisco DCNM-SAN** 用のリンクをクリックします。

Cisco DCNM-SAN サーバ起動パッドが表示されます。

ステップ 5　[Server URL] ドロップダウン リストにサーバのホスト名または IP アドレスを入力します。

ステップ 6　[Start] をクリックします。

（注）　起動パッドには過去に使用したサーバ URL の履歴が保持されます。過去に使用したサーバ URL をドロップダウン リストから 1 つ選択できます。

Cisco DCNM-SAN プリファレンスの設定

Cisco DCNM-SAN の動作に関するプリファレンスを設定するには、Cisco DCNM-SAN のメニューバーで、[File] > [Preferences] の順に選択します。[Preferences] ダイアログボックスが表示され、アプリケーションの各コンポーネントを設定するための次のタブが表示されます。

- General
- SNMP
- Map

Cisco DCNM-SAN のデフォルト General プリファレンスは次のとおりです。

- Show Switch Name by : IP アドレス、DNS 名、または論理名別に [Fabric] ペインにスイッチを表示します。デフォルト設定は Logical Name です。
- Show WorldWideName (WWN) Vendor : Cisco DCNM-SAN によって表示された任意のテーブルまたはリストに、World Wide Name ベンダー名を表示します。スイッチの IP アドレスの前に名前を表示するには、**Prepend Name** チェックボックスをオンにします。IP アドレスの代わりに名前を表示するには、**Replacing Vendor Bytes** チェックボックスをオンにします。デフォルトは Prepend Name オプションです。
- Show End Device Using : エイリアスまたは pWWN エイリアスを使用して [Fabric] ペインにエンド デバイスを表示します。デフォルト設定は Alias です。
- Show Shortened iSCSI Names : デフォルト設定は [OFF] です。
- Show Timestamps as Date/Time : タイムスタンプを日付/時刻フォーマットで表示します。この設定がオフの場合、タイムスタンプは経過時間で表示されます。デフォルト設定はイネーブル（ON）です。
- Telnet Path : システムの telnet.exe ファイルのパスを設定します。デフォルトは telnet.exe ですが、正しい場所を参照する必要があります。

（注）　パスを参照するか、パスを入力した場合に、パス名にスペースが入っていると（c:¥program files¥telnet.exe など）、パスは無効になります。パスを有効にするには、手動でパスを引用符で囲む必要があります（"c:¥program files¥telnet.exe" など）。

- Use Secure Shell instead of Telnet：CLI を使用してスイッチと通信する場合に、SSH または Telnet のどちらを使用するかを指定します。イネーブルの場合は、SSH アプリケーションのパスを指定する必要があります。デフォルト設定はディセーブルです。
- Confirm Deletion：Cisco DCNM-SAN を使用して設定の一部を削除する場合に、確認用のポップアップ ウィンドウを表示します。デフォルト設定はイネーブル（ON）です。
- Export Tables with Format：Device Manager を使用してテーブルをエクスポートした場合に作成されるファイルのタイプを指定します。Tab-Delimited（タブ区切り）、または XML から選択できます。デフォルト設定は Tab-Delimited です。
- Show CFS Warnings：選択した機能に関してすべてのスイッチで CFS がイネーブルでない場合に警告メッセージを表示します。

Cisco DCNM-SAN のデフォルト SNMP プリファレンスは次のとおりです。

- Retry request 1 time(s) after 5 sec timeout：再試行値を 0 ～ 5、タイムアウト値を 3 ～ 30 に設定できます。
- Trace SNMP packets in Log：デフォルト設定は [ON] です。
- Enable Audible Alert when Event Received：デフォルト設定は [OFF] です。

Cisco DCNM-SAN のデフォルト Map プリファレンスは次のとおりです。

- Display Unselected VSAN Members：[Fabric] ペインに選択されていない VSAN メンバーを表示します。デフォルト設定は [ON] です。
- Display End Devices：[Fabric] ペインにファブリックのエンド デバイスを表示します。デフォルト設定は [ON] です。
- Display End Device Labels：[Fabric] ペインにファブリックのエンド デバイス ラベルを表示します。デフォルト設定は [OFF] です。
- Expand Loops：[Fabric] ペインに、ファブリックのループを個別の接続として表示します。デフォルト設定は [OFF] です。
- Expand Multiple Links：[Fabric] ペインに、複数のリンクを 1 本の太い線でなく、個別の線として表示します。デフォルト設定は [OFF] です。
- Open New Device Manager Each Time：ファブリック内のスイッチから Device Manager を起動するたびに、新しいインスタンスをオープンします。デフォルト値は [OFF] です。つまり、一度にオープンされる Device Manager のインスタンスは 1 つだけです。
- Select Switch or Link from Table：[Fabric] ペイン内のスイッチまたはリンクを、Information ペイン内のテーブルのスイッチまたはリンクをクリックして選択できます。デフォルト設定はディセーブル（OFF）です。つまり、テーブル内のスイッチまたはリンクをクリックしても、[Fabric] ペイン内のスイッチまたはリンクの選択は変更されません。
- Layout New Devices Automatically：[Fabric] ペインに追加された新規デバイスを、最適な位置に自動的に配置します。デフォルト設定は [OFF] です。このモードで新規デバイスを追加した場合、最初の位置が要求を満たさないときは、手動で位置を変更する必要があります。
- Use Quick Layout when Switch has 30 or more End Devices：この値のデフォルト設定値（30）を表示します。このフィールドに任意の番号を入力できます。Quick Layout をディセーブルにするには、**0** を入力します。
- Override Preferences for Non-default Layout：この値のデフォルト設定値を（ON）を表示します。
- Automatically Save Layout：このオプションがイネーブルの場合、レイアウトに関するすべての変更が自動的に保存されます。デフォルト設定は [ON] です。
- Detach Overview Window：表示するファブリック エリアの中央に [Fabric] ペインを簡単に移動できるようになります。（この機能は、[Fabric] ペイン内に全体を表示できない大規模なファブリックの場合に最も役立ちます）。概要ウィンドウを起動するには、[Show/Hide Overview Window] ボ

タンをクリックします。[Show/Hide Overview Window] ボタンを再びクリックするまで、概要ウィンドウはファブリック ウィンドウ上にオーバーレイされたままになります。この設定がイネーブルの場合は、概要ウィンドウを切り離して片側に移動し、その間に [Fabric] ペインにアクセスできます。デフォルト設定はディセーブル（OFF）です。

ネットワーク ファブリックの検出

Cisco DCNM-SAN では、Cisco DCNM-SAN に接続されたスイッチに対して SNMP クエリーを実行し、ファブリック トポロジに関する情報を収集します。スイッチは、ファブリックに接続されたすべてのデバイスを検出したあとに応答します。デバイスの検出には、FSPF テクノロジー データベースおよび Name Server データベース内の情報や、FC-GS-3/4 標準で定義された Fabric Configuration Server の要求/応答メカニズムによって収集された情報が使用されます。Cisco DCNM-SAN を起動する場合は、検出のためにシード スイッチの IP アドレス（またはホスト名）を入力します。

Cisco DCNM-SAN を起動し、検出が完了すると、検出されたすべてのスイッチ、ホスト、ストレージ デバイスを含むネットワーク ファブリックのビューが表示されます。

ネットワーク LAN の検出

NX-OS Release 4.2(0) 以降では、Cisco Discovery Protocol（CDP）を使用して Nexus および Catalyst イーサネット スイッチを検出できます。DataCenter 3（DC3）スイッチは [Datacenter] ノードおよび [LAN] ノードの下位に表示されます。Cisco DCNM-SAN に、DC3 スイッチとその ISL に関する情報が表示されます。

イーサネット スイッチの表示

イーサネット スイッチに関する情報を表示するには、次の手順を実行します。

ステップ 1　[Datacenter] ノードの下位にある [LAN] ノードをクリックします。

ステップ 2　[Information] ペインの [Switches] タブをクリックします。

スイッチ情報が表示されます。

（注）　[Datacenter] ノードは [SAN] ノードおよび [LAN] ノードの上位ノードです。[SAN] ノードはファブリックすべての上位ノードとして常にツリーに表示されます。

LAN の削除

サーバから検出された LAN を削除するには、次の手順を実行します。

ステップ 1　[Server] > [Admin] を選択します。

スイッチ情報が表示されます。

ステップ 2　削除する LAN のスイッチ IP をクリックして選択します。

ステップ 3　[Remove] をクリックします。

デバイス グループの変更

すべてのデバイスが FC-GS-3 リクエストに応答できるわけではないので、単一のサーバまたはストレージ サブシステム上の異なるポートが、Cisco DCNM-SAN マップで個別のエンド デバイスとして表示されることがあります。

エンド デバイスを 1 つのラックにまとめ、Cisco DCNM-SAN のマップ上で 1 つのアイコンとして表示されるようにするには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[End Devices] を展開し、[Storage] または [Hosts] を選択します。

[Information] ペインにエンド デバイスが表示されます。

ステップ 2　[Fabric] ペインのデバイスの 1 つをクリックするか、または [Information] ペインの [Enclosures] タブをクリックして、ラックに入れるデバイスの名前（[Name] フィールド内）をクリックします。

ステップ 3　[Fabric] ペインのマップに新しいラックの名前を入力します。

ステップ 4　[Name] フィールドのデバイス名を 1 回クリックします。複数の名前を選択する場合は、**Shift** キーを押しながらその他の名前をそれぞれクリックします。

ステップ 5　**Ctrl+C** キーを押して、選択された名前をコピーします。

ステップ 6　**Ctrl+V** キーを押して、[Name] フィールドにデバイス名を貼り付けます。

（注）　ラックからデバイスを削除するには、目的のデバイスの名前をトリプルクリックし、**Delete** キーを押します。ラックを削除するには、ラック内のデバイスごとにこのステップを繰り返します。

ラックへのエイリアス名の使用方法

名前にエイリアス名を使用するラックを Cisco DCNM-SAN で作成するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [End Devices] を展開し、[Hosts] または [Storage] を選択します。

[Information] ペインにデバイスのリストが表示されます。[NxPorts] タブがデフォルトです。

ステップ 2　エイリアス名に変換するラック名を右クリックし、[Alias] > [Enclosure] の順に選択します。

[Ailas] > [Enclosures] ウィンドウが表示されます。ウィンドウには、式がリスト表示されます。リストには式を追加することも、リストにある式を変更することもできます。

ステップ 3　[Apply Changes] アイコンをクリックして変更内容を保存し、[Close] をクリックします。

（注）　Cisco DCNM-SAN では、複数のエイリアス名を 1 つのラックに変換するのに正規表現を使用します。エイリアス名には、必ず同じ式のパターン規則を使用してください。ラック名は正規表現リストを使用して選択したエイリアスから作成できます。

説明へのエイリアス名の使用方法

名前にエイリアス名を使用する説明を Cisco DCNM-SAN で作成するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [End Devices] を選択します。

ステップ 2　[General] タブをクリックします。

[Information] ペインにデバイスのリストが表示されます。

ステップ 3　説明にエイリアス名を読み込むデバイス名を選択し、[Alias] > [Enclosure] ボタンを選択します。

エイリアス名が説明カラムの対応する列にコピーされます。

（注）　コピー中、Cisco DCNM-SAN はエイリアス名の解析またはフォーマットは行いません。

ユーザおよびロールによる管理者アクセスの制御

Cisco MDS 9000 ファミリ スイッチは、CLI または Cisco DCNM-SAN のいずれを使用しているかに関係なく、ロールベースの管理アクセスをサポートします。これにより、特定のロールに特定の管理権限を割り当てたあと、各ロールに 1 つまたは複数のユーザを割り当てることができます。

デフォルト ロールには、ユーザが GUI（Cisco DCNM-SAN および Device Manager）にアクセスするために必要なアクセス権限が含まれます。これらのアクセス権限は、ユーザが GUI を使用できるようにするために、すべてのユーザに自動的に付与されます。

Cisco DCNM-SAN は、SNMPv3 を使用してロールベースの管理アクセスを設定します。セットアップ ルーチンを完了すると、単一のロール、ユーザ名、およびパスワードが確立されます。このユーザに割り当てられたロールを使用すると、ユーザおよびロールの作成を含む、最高レベルの権限が使用可能になります。Cisco DCNM-SAN を使用すると、ロールやユーザを作成したり、ネットワーク内のセキュア管理アクセスの必要性に応じてパスワードを割り当てたりすることができます。

Cisco DCNM-SAN Wizard の使用方法

Cisco DCNM-SAN クライアントには、一般的な設定タスクに役立つ次のウィザードが用意されています。

- [VSAN] : ファブリック内の複数のスイッチに VSAN を作成し、interop モード、ロードバランス、FICON などの VSAN 属性を設定します。
- [Zone Edit Tool] : ゾーン セット、ゾーン、およびエイリアスを作成します。ゾーンにメンバーを追加し、ゾーン データベースを編集します。
- [IVR Zone] : IVR ゾーン セット、ゾーン、およびエイリアスを作成します。IVR NAT および自動トポロジをイネーブル化します。IVR ゾーンにメンバーを追加し、IVR ゾーン データベースを編集します。
- [FCoE] : 仮想ファイバ チャネル（FC）インターフェイスと VLAN-VSAN マッピングを作成し、仮想 FC インターフェイスをイーサネット インターフェイスまたは PortChannels にバインドします。
- [PortChannel] : 選択された ISL から PortChannels を手動または自動的に作成できます。チャネル ID やトランキング モードなどの PortChannel 属性を設定します。
- [FCIP] : ギガビット イーサネット ポート間に FCIP リンクを作成します。ファイバ チャネルの書き込みアクセラレーションと IP 圧縮をイネーブル化します。
- [DPVM] : ダイナミック ポート VSAN メンバシップの確立、自動学習機能のイネーブル化、DPVM データベースのアクティブ化を実行します。
- [Port Security] : Cisco MDS スイッチへの不正アクセスを防止し、管理者に侵入を報告します。
- [iSCSI] : iSCSI イニシエータのゾーンを作成し、ターゲットに許可された VSAN リストに VSAN を追加します。
- [NPV] : SAN に存在するファイバ チャネル ドメイン ID の数を削減します。
- [QoS] : 選択された VSAN のゾーンに QoS 属性を設定します。
- [IP ACL] : 順序付きの IP Access Control List（ACL; アクセス コントロール リスト）を作成し、ファブリック内の選択したスイッチに配布します。
- [License Install] : ファブリック内の選択したスイッチで、ライセンスのダウンロードおよびインストールを容易に実行できるようにします。
- [Software Install] : ファブリック内の選択したスイッチでイメージの互換性を確認し、ソフトウェア イメージをインストールします。

Cisco DCNM-SAN トラブルシューティング ツール

Cisco DCNM-SAN には、ツールバーまたは [Tools] メニューから使用可能なトラブルシューティング ツールがいくつかあります。

- Zone Merge Analysis : ゾーン マージ分析ツール（[Zone] メニューから使用可能）を使用すると、2 つの Cisco MDS スイッチが相互接続されている場合に、ゾーンが正常にマージされるかどうかを判別できます。相互接続されたスイッチ ポートで同じ名前の VSAN を使用できる場合、またはこれらのポートに同じ名前のゾーンが含まれている場合、Cisco DCNM-SAN はこのゾーンに同じメンバーが含まれているか確認します。マージ分析ツールは、マージの実行前、またはファブリックを相互接続してゾーン マージ障害原因を判別したあとに実行できます。
- End-to-End Connectivity : Cisco DCNM-SAN のエンドツーエンド接続分析ツールは FC ping を使用して、特定の VSAN 内の Cisco MDS スイッチとエンド デバイス（HBA およびストレージ デバイス）間の相互接続を検証します。Cisco DCNM-SAN では基本的な接続のほか、以下の項目についても任意で検証できます。
  - パスが冗長である。
  - ゾーンに 2 つ以上のメンバーが含まれる。

エンド デバイスが管理可能なスイッチに接続されている（帯域内または帯域外管理パスで現在アクティブである）

- Switch Health Analysis：Cisco DCNM-SAN を使用して詳細なスイッチ ヘルス分析を実行できます。重要な Cisco MDS スイッチ、モジュール、ポート、およびファイバ チャネル サービスのステータスがすべて検証されます。40 を超える条件がチェックされます。このツールを使用すると、Cisco MDS スイッチの状態にすばやく、容易に、かつ完全にアクセスできます。
- Fabric Configuration Analysis：Cisco DCNM-SAN はファブリック分析ツールを備えています。ファブリック内のすべての Cisco MDS スイッチの設定が、参照スイッチまたはポリシー ファイルと比較されます。チェックする機能、および実行するチェック タイプを定義することができます。分析では一致しない値、失われた値、または余分な値を検索できます。すべての機能に対してすべての設定チェックを行った場合、Cisco MDS スイッチにつき 200 以上のチェックが実行されます。

分析を実行すると、検出された問題点の詳細とともに結果が表示されます。設定が異なっている場合、この設定を選択して [Resolve] ボタンをクリックして自動的に解決できます。参照スイッチまたはポリシー ファイルに合わせて、設定が自動的に変更されます。

Cisco DCNM-SAN と Data Center Network Management ソフトウェアの統合

Cisco DCNM-SAN と Data Center Network Management（DCNM）ソフトウェアは、シスコの次世代データセンター環境における 2 つの主要コンポーネントです。Cisco DCNM-SAN では、Cisco Nexus 5000 シリーズ スイッチと Cisco MDS 9000 シリーズ スイッチを設定します。DCNM ソフトウェアでは、Cisco Nexus 5000 および Cisco Nexus 7000 シリーズ スイッチを設定します。Cisco DCNM-SAN ソフトウェアは SAN に、DCNM-LAN ソフトウェアは LAN ネットワークに対象範囲が制限されています。

一般的なデータセンター環境では、SAN と LAN のトポロジを組み合わせるのが主流になりつつあります。2 つの管理ソフトウェアはトポロジの制限を超えて動作するようには設計されていないので、ユーザは DCNM-LAN ソフトウェアから Cisco DCNM-SAN、またはその逆に移動することはできません。

Cisco DCNM-SAN と DCNM-LAN を統合することで、データセンター 3.0 内のネットワークを 1 つのプラットフォームで管理し、個々のコンフィギュレーションに円滑なユーザ エクスペリエンスを提供することができます。Cisco MDS NX-OS Release 4.2 以降では、Cisco DCNM-SAN と Cisco Nexus 5000 シリーズ製品の統合に対応できるようディレクトリ構造が変更されています。

トポロジ マップからのスイッチの起動

DCNM のスイッチを Cisco DCNM-SAN から起動する手順は、次のとおりです。

ステップ 1　Cisco DCNM-SAN の [Fabric] ペインで、DCNM を使用して開く LAN マップの Nexus スイッチを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　ポップアップ メニューで [DCNM] をクリックし、適切なコンテキストを選択します。

CHAPTER 6

Device Manager

ここでは、Cisco MDS 9000 Device Manager の特徴と使用方法について説明します。この章の内容は、次のとおりです。

- 「Device Manager の概要」（P.6-1）
- 「Device Manager の機能」（P.6-2）
- 「Device Manager インターフェイスの使用方法」（P.6-2）
- 「Device Manager のプリファレンスの設定」（P.6-9）

Device Manager の概要

Device Manager を使用すると、搭載されたスイッチング モジュール、スーパーバイザ モジュール、各モジュール内の各ポートのステータス、電源装置、およびファン アセンブリを含めて、Cisco MDS 9000 ファミリ スイッチ シャーシまたは Cisco Nexus 5000 シリーズ スイッチ シャーシをグラフィック表示できます。

Device Manager を使用すると、搭載されたスイッチング モジュール、スーパーバイザ モジュール、モジュールの各ポートのステータス、電源、およびファン アセンブリを含めて、Cisco MDS 9000 ファミリ スイッチ シャーシまたは Cisco Nexus 5000 シリーズ スイッチ シャーシをグラフィック表示できます。

DCNM-SAN の [Information] ペイン内のテーブルは、基本的に、Device Manager で表示されるダイアログボックスに対応しています。ただし、DCNM-SAN のテーブルには 1 つまたは複数のスイッチの値が表示されますが、Device Manager のダイアログボックスに表示されるのは 1 つのスイッチの値です。また、デバイス固有の設定の確認や、トラブルシューティング用の情報は、DCNM-SAN よりも Device Manager の方が詳細です。

Device Manager Release 4.2 以降では、複数の表示方法（簡易および詳細）で強化されたセキュリティを利用でき、機能のアクセスをロール ベースで管理できます。Device Manager の表示方法を選択することでユーザに最適なメニュー項目だけを表示することができます。サーバ管理ロールを持つユーザはファブリック関連機能の一部にだけアクセスできます。また、Device Manager ユーザまたは接続されているクライアントを管理できません。

Device Manager Release 5.0 以降では、Cisco MDS 9148 および 9124 マルチレイヤ ファブリック スイッチによって提供されるすべてのソフトウェア機能がサポートされます。Cisco MDS 9148 マルチレイヤ ファブリック スイッチは Sabre ASIC に基づいた 48 ポート（1/2/4/8G）FC 1RU スイッチであり、Cisco MDS 9124 マルチレイヤ ファブリック スイッチは Sabre ASIC に基づいた HP ブレードサーバ対応の 1/2/4/8G スイッチ モジュールです。Device Manager および DCNM-SAN では、この両方の新規スイッチを検出、表示、設定、モニタ、および処理できます。また、Device Manager は、Cisco NX-OS Release 5.0(1) を実行する Cisco Nexus 5000 シリーズ スイッチ上の Cisco Nexus 2000 Series Fabric Extender をサポートします。

- Cisco Nexus 2148T Fabric Extender：親の Cisco Nexus 5000 シリーズ スイッチへのアップリンク接続用に、4 個の 10 ギガビット イーサネット ファブリック インターフェイスを備え、サーバまたはホストへのダウンリンク接続用に、8 個の 1 ギガビット イーサネットまたは 10 ギガビット イーサネット ホスト インターフェイスを備えています。
- Cisco Nexus 2232PP Fabric Extender：親の Cisco Nexus 5000 シリーズ スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタ付きの 8 個の 10 ギガビット イーサネット ファブリック インターフェイスを備え、サーバまたはホストへのダウンリンク接続用に、SFP+ インターフェイス アダプタ付きの 32 個の 10 ギガビット イーサネット ファブリック インターフェイスを備えています。
- Cisco Nexus N2248TP Fabric Extender：親の Cisco Nexus 5000 シリーズ スイッチへのアップリンク接続用に、Small Form-Factor Pluggable（SFP+）インターフェイス アダプタ付きの 4 個の 10 ギガビット イーサネット ファブリック インターフェイスを備え、サーバまたはホストへのダウンリンク接続用に、48 個の 1000BASE-T（1 ギガビット）イーサネット ホスト インターフェイスを備えています。

Device Manager では、これらの Fabric Extender の検出および表示が可能です。Cisco Device Manager および Cisco DCNM-SAN クライアントは、48 ポート 8 Gbps の拡張ファイバ チャネル スイッチング モジュール（DS-X9248-256K9）と 32 ポート 8 Gbps の拡張ファイバ チャネル スイッチ モジュール（DS-X9232-256K9）のプロビジョニングおよびモニタリングをサポートします。

Device Manager の機能

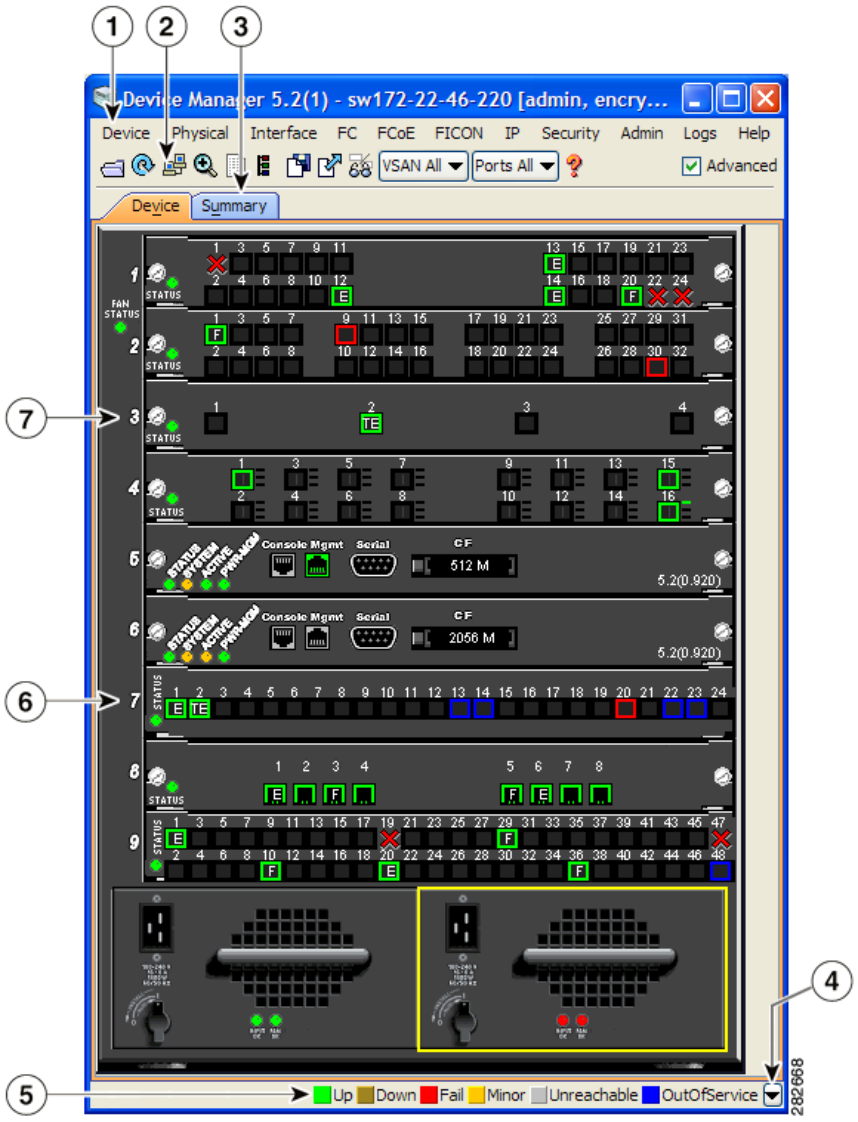
Device Manager は、Device View と Summary View の 2 つのビューを提供します。Summary View では、スイッチのインターフェイスを監視できます。Device View では、次のようなスイッチ レベルの設定を実行できます。

- 仮想ファイバ チャネル インターフェイスの設定。
- Fibre Channel over Ethernet（FCoE）接続の設定。
- 複数の VSAN のゾーンの設定。
- ポート、PortChannels、およびトランキングの管理。
- スイッチへの SNMPv3 セキュリティ アクセスの管理。
- スイッチへの CLI（コマンドライン インターフェイス）セキュリティ アクセスの管理。
- アラーム、イベント、および通知の管理。
- コンフィギュレーション ファイルおよびソフトウェア イメージの保存とコピー。
- ハードウェア構成の表示。
- シャーシ、モジュール、およびポートのステータスや統計情報の表示。

Device Manager インターフェイスの使用方法

ここでは、Device Manager インターフェイスについて説明します。

図 6-1　Device Manager の [Device] タブ



1	メニュー バー	5	ステータス
2	ツールバー	6	スーパーバイザ モジュール
3	タブ	7	スイッチングまたはサービス モジュール
4	用例		

メニュー バー

Device Manager メイン ウィンドウの上部にあるメニュー バーでは、1 台のスイッチの管理およびトラブルシューティングを行うことができます。メニュー バーには、次のオプションがあります。

- [Device] : Device Manager のインスタンスのオープン、管理プリファレンスの設定、ページ レイアウトの設定、現在のスイッチとの Telnet/Secure Shell（SSH; セキュア シェル）セッションのオープン、デバイス イメージのエクスポート、および Device Manager アプリケーションのクローズを行います。
- [Physical] : コンポーネント、モジュール、温度センサ、電源モジュール、ファン、およびシステム全体を表示し、管理できます。
- [Interface] : PortChannels、ファイバ チャネル ポート、イーサネット ポート、iSCSI ポート、FICON ポートを設定して管理できます。診断、管理、モニタリング機能、および Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）とポートのトラッキング機能も提供します。

（注）　Cisco Nexus 5000 シリーズ スイッチが NPV モードであり、4.2(1) よりも前の Cisco NX-OS リリースを実行している場合、[Interface] > [Port Channels] メニュー オプションは表示されません。

- [FC] : VSAN（仮想 SAN）、ドメイン、およびネーム サーバの特性を設定して管理できます。高度な設定機能も提供します。
- [FCoE] : Cisco Nexus 5000 シリーズ スイッチで FCoE パラメータを設定し、VSAN から VLAN にマッピングできます。

（注）　FCoE メニュー オプションは、Cisco Nexus 5000 シリーズ スイッチが Cisco NX-OS Release 4.0(1a) 以降で実行されている場合にだけ表示されます。

- [FICON] : FICON VSAN の設定と管理、RLIR ERL 情報の設定、選択した FICON ポートの交換、FICON ポート番号の表示を実行できます。
- [IP] : FCIP、iSCSI、iSNS、ルート、VRRP、および CDP を設定および管理できます。
- [Security] : FCSP、ポート セキュリティ、iSCSI セキュリティ、SNMP セキュリティ、共通のロール、SSH、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、および IP Access Control List（ACL; アクセス コントロール リスト）を設定して管理できます。
- [Admin] : スイッチ設定の保存、コピー、編集、および消去、イベントのモニタ、フラッシュ ファイルの操作、ライセンスの管理、NTP の設定、CFS の使用、およびスイッチのリセットを実行できます。**show tech support**、**show cores**、および **show image** コマンドを使用することもできます。
- [Logs] : メッセージ、ハードウェア、イベント、およびアカウンティングの各ログを表示します。FICON リンク インシデントを表示し、Syslog 設定を変更することもできます。
- [Help] : [Information] ペインに、特定のダイアログボックスに関するオンライン ヘルプ トピックが表示されます。

ツールバー アイコン

Device Manager ツールバーを使用すると、多くの Device Manager 機能にすばやくアクセスできます。アイコンを選択すると、機能を設定するためのダイアログボックスが開くことがあります。ツールバーには、Device View および Summary View の主なアイコンが配置されています（表 6-1 を参照）。

表 6-1　Device Manager のメイン ツールバー

アイコン	説明
Open Device	他のスイッチの Device Manager ビューを開きます。このビューを別のウィンドウで開くオプションがあります。
Refresh Display	スイッチと通信し、Device Manager ビューに情報を表示します。
Command-Line Interface	スイッチに対する CLI コマンド ウィンドウを別個に開きます。
Configure Selected	選択されたコンポーネント（ライン カードまたはポート）の設定ダイアログボックスを開きます。
SysLog	スイッチに発生した最新のシステム メッセージのリストを表示するウィンドウを開きます。
VSANs	スイッチの VSAN 設定を行う VSAN ダイアログボックスを開きます。
Save Configuration	現在の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ます。
Copy	サーバとスイッチ間でコンフィギュレーション ファイルをコピーします。
Toggle FICON/Interface Port Labels	FICON およびインターフェイス ポート ラベルを切り替えます。
Select VSAN	ポートの表示をフィルタリングして、選択された VSAN に属すポートだけを表示します。
Help	Device Manager のオンライン ヘルプにアクセスします。

ダイアログボックス

ツールバー アイコンを選択すると、選択された機能を設定するためのダイアログボックスが開くことがあります。このダイアログボックスには、テーブル操作用アイコンが配置されている場合があります。これらのアイコンの詳細については、「[Information] ペイン」（P.5-5）を参照してください。

タブ

スイッチ シャーシおよびコンポーネントをグラフィックで表示するには、Device Manager メイン ウィンドウの [Device] タブをクリックします。

（注）　Device View には、Cisco NX-OS Release 5.0(1) を実行する Cisco Nexus 5000 シリーズ スイッチに接続された、Cisco Nexus 2000 Series Fabric Extender（FEX）のスイッチ シャーシ情報も表示されます。

Device Manager メイン ウィンドウの [Summary] タブをクリックすると、1 台のスイッチおよびファイバ チャネルや IP 近接デバイス上のアクティブなインターフェイスのサマリーが表示されます。Summary View にはポート速度、リンク使用率、およびその他のトラフィック統計情報も表示されます。[Summary View] タブの左上に、トラフィック監視用のボタンが 2 つあります。選択されたオブジェクトのトラフィックを監視するには、[Monitor Selected Interface Traffic Util%] ボタンをクリックします。選択されたオブジェクトの詳細な統計情報を表示するには、[Monitor Selected Interface Traffic Details] ボタンをクリックします。ポーリング インターバル、タイプまたは Rx/Tx 表示、およびしきい値を設定できます。

（注）　[Summary] タブには、Cisco NX-OS Release 4.2 を実行する Cisco Nexus 5000 シリーズ スイッチの仮想ファイバ チャネル インターフェイスの利用率の統計（Util%）は表示されません。

用例

Device Manager の右下にある凡例は、次のようにポート ステータスを示します。

カラー

- グリーン：ポートが起動しています。
- ブラウン：ポートは管理上のダウン状態です。
- レッド：ポートはダウンしているか、または障害があります。
- オレンジ：ポートにマイナー障害が発生しています。
- グレー：ポートに到達できません。
- ブルー：ポートはアウト オブ サービス状態です。

ラベル

- X：リンク障害
- E：ISL（スイッチ間リンク）
- TE：Multi-VSAN ISL
- F：ホスト/ストレージ
- FL：F ループ
- I：iSCSI
- SD：スパンの終点
- CH：チャネル
- CU：制御ユニット
- NP：プロキシ N ポート（NPV モード）

- TNP：トランキング NP_Port（NPV モード）
- TF：トランキング F_Port
- f：vFC あり（Cisco Nexus 5000 シリーズスイッチだけ）

スーパーバイザおよびスイッチング モジュール

Device View でオブジェクトを右クリックして、その情報を取得したり、設定することができます。モジュールを右クリックすると、メニューにモジュール番号が表示され、モジュールの設定やリセットを実行できます。ポートを右クリックすると、メニューにポート番号が表示され、そのポートに関する設定、監視、イネーブル化、ディセーブル化、ビーコン モードの設定、または診断を実行できます。

ヒント　Device Manager では複数のポートを選択し、選択したすべてのポートにオプションを一度に適用できます。ポートを選択するには、マウスをクリックしたまま、選択するポートを囲むようにドラッグするか、**Cntl** キーを押したまま各ポートをクリックします。

ポートをイネーブルまたはディセーブルにするには、ポートを右クリックし、ポップアップ メニューで [Enable] または [Disable] をクリックします。複数のポートをイネーブルまたはディセーブルにするには、マウスをドラッグしてポートを選択し、選択されたポートを右クリックします。さらに、ポップアップ メニューで [Enable] または [Disable] をクリックします。

1 つまたは複数のポートのトランキングを管理するには、選択されたポートを右クリックし、[Configure] をクリックします。表示されたダイアログボックスの Trunk カラムの現在の値を右クリックし、プルダウン リストで [nonTrunk]、[trunk]、または [auto] をクリックします。

Device Manager を使用してポートチャネルを作成するには、[Interface] メニューで [PortChannels] をクリックします。

（注）　PortChannel を作成するには、リンク両端のすべてのポートでポート速度、トランキング タイプ、および管理ステートを同じにする必要があります。

コンテキスト メニュー

両方の Device Manager ビューでコンテキスト メニューを使用可能にするには、デバイスまたはテーブルを右クリックします。

Device View ビュー：

- Device：システム、モジュール、または電源モジュールを右クリックするとメニューが表示され、デバイスの設定またはリセットに関するオプションを選択できます。
- Port：ポートを右クリックすると、クリックしたポートの番号を示すメニューが起動し、そのポートに関する設定、モニタリング、イネーブル化、ディセーブル化、ビーコン モードの設定、またはポート診断を実行できます。

Summary View ビュー：

- Table：テーブルのヘッダーを右クリックすると、そのテーブルに表示されるカラムのリストが表示されます（Interface、Description、VSANs、Mode、Connected To、Speed (Gb)、Rx、Tx、Errors、Discards、および Log）。ポート タイプに該当する設定ダイアログボックスを起動するには、[Description] フィールドをクリックします。

Device Manager の起動

デスクトップから Device Manager を起動するには、[Device Manager] アイコンをダブルクリックし、『*Cisco DCNM Installation and Licensing Guide*』に記載された手順に従います。

Device Manager を起動する手順は、次のとおりです。

ステップ 1　次の 3 つの手順のうち、いずれかを選択できます。

a. [Fabric] ペインのマップで、管理するスイッチを右クリックし、表示されたメニューで [Device Manager] を選択します。

b. [Fabric] ペインのマップでスイッチをダブルクリックします。

c. [Fabric] ペインのマップでスイッチを選択し、[Tools] > [Device Manager] を選択します。

[Device Manager open] ダイアログボックスが表示されます。

ステップ 2　デバイスの IP アドレスを入力します。

ステップ 3　ユーザ名とパスワードを入力します。

ステップ 4　Device Manager クライアントで TCP ベースのプロキシ サーバを使用するには、[Proxy SNMP through FMS] チェックボックスをオンにします。

ステップ 5　スイッチに設定したプライバシー プロトコルに応じて、[Auth-Privacy] オプションを選択します。

a. スイッチにまだプライバシー プロトコルを設定していない場合は、MD 5（プライバシーなし）の Auth-Privacy オプションを選択します。

b. スイッチにプライバシー プロトコルを設定している場合は、設定に適した [Auth-Privacy] オプションを選択してください。

ステップ 6　[Open] をクリックして Device Manager を開きます。

Device Manager のプリファレンスの設定

Device Manager アプリケーションのプリファレンスを設定するには、[Device] メニューで [Device] > [Preferences] を選択します。設定できるプリファレンスは次のとおりです。

- **Retry Requests x Time(s) After x sec Timeout**：再試行要求値を設定できます。デフォルト設定は、5 秒間のタイムアウト後に 1 回です。
- **Enable Status Polling Every x secs** : ステータス ポーリング値を設定できます。デフォルト設定はイネーブル（ON）で、期間は 40 秒です。
- **Trace SNMP Packets in Message Log** : Device Manager が SNMP パケットをトレースし、トレースを記録するかどうかを設定できます。デフォルト設定は、ディセーブル（OFF）です。
- **Register for Events After Open, Listen on Port 1163**：Device Manager を開いたあとにイベントが記録されるように、現在のスイッチを登録できます。デフォルト設定はイネーブル（ON）です。
- **Show WorldWideName (WWN) Vendor** : Device Manager によって表示された任意のテーブルまたはリスト内で、WWN ベンダー名を表示します。**Prepend** がオンの場合は、スイッチの IP アドレスの前に名前が表示されます。**Replace** がオンの場合は、IP アドレスの代わりに名前が表示されます。デフォルト設定では、**Prepend** オプションがイネーブル（ON）です。
- **Show Timestamps as Date/Time**：タイムスタンプを日付/時刻フォーマットで表示します。この設定がオフの場合、タイムスタンプは経過時間で表示されます。デフォルト設定はイネーブル（ON）です。
- **Telnet Path**：システムの telnet.exe ファイルのパスを設定します。デフォルトは **telnet.exe** ですが、正しい場所を参照する必要があります。

  （注） パスを参照するか、パスを入力した場合に、パス名にスペースが入っていると（**c:\program files\telnet.exe** など）、パスは無効になります。パスを有効にするには、手動でパスを引用符で囲みます（**"c:\program files\telnet.exe"** など）。

- **CLI Session Timeout x secs (0= disable)** : CLI セッションのタイムアウト インターバルを指定します。ディセーブル（タイムアウト値なし）にするには、0 を入力します。デフォルト設定は 30 秒です。
- **Show Tooltips in Physical View** : Physical（Device）View にツールチップを表示するかどうかを決定します。デフォルト設定はイネーブル（ON）です。
- **Label Physical View Ports With** : Physical（Device）View を使用している場合に、ポートに割り当てるラベル タイプを指定します。FICON および Interface を選択できます。デフォルト設定は Interface です。
- **Export Table**：Device Manager を使用してテーブルをエクスポートした場合に作成されるファイルのタイプを指定します。Tab-Delimited（タブ区切り）、または XML から選択できます。デフォルト設定は Tab-Delimited です。

CHAPTER 7

Performance Manager の設定

この章では、DCNM-SAN を使用してネットワークのモニタリングと管理を行う方法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。

- 「Performance Manager の概要」（P.7-1）
- 「フロー統計」（P.7-3）
- 「フロー セットアップ ウィザード」（P.7-4）

Performance Manager の概要

ここでは、次の内容について説明します。

- 「データ補間」（P.7-2）
- 「データ収集」（P.7-2）
- 「パフォーマンスしきい値の使用方法」（P.7-2）
- 「Performance Manager Flow Wizard を使用したフローの作成」（P.7-4）

Performance Manager はネットワーク デバイスの統計情報の履歴を収集し、ブラウザを使用してこの情報をグラフィック表示します。最近の統計情報は詳細が、古い統計情報はサマリーが表示されます。Performance Manager は Cisco Traffic Analyzer などの外部ツールとも統合されています。

Performance Manager には、3 つの処理ステージがあります。

- 定義：Flow Wizard でスイッチにフローをセットアップします。
- 収集：Web Server Performance Collection 画面で目的のファブリックに関する情報を収集します。
- 提示：DCNM-SAN Web サーバを通じて、収集したデータを表示する Web ページを生成します。

Performance Manager は ISL（スイッチ間リンク）、ホスト、ストレージ エレメント、および設定済みフローの統計情報を収集できます。フローの定義基準は、ホストからストレージ（またはストレージからホスト）のリンクです。Performance Manager は収集コンフィギュレーション ファイルに基づいて、ファブリックから統計情報を収集します。これらのファイルにより、Performance Manager が統計情報を収集する SAN エレメントおよび SAN リンクが決まります。この設定に基づいて、Performance Manager は適切なデバイス（スイッチ、ホスト、またはストレージ エレメント）と通信し、5 分間の規定時間内に適切な情報を収集します。

Performance Manager はラウンドロビン データベースを使用して、ファブリックから収集された統計データを保持します。このデータは収集コンフィギュレーション ファイル内で設定されたパラメータに基づいて、格納されます。ポーリング インターバルごとに、Performance Manager は関連する統計情報を収集し、ラウンドロビン データベース内に格納します。このデータベースのサイズは固定されていて、設定された上限を超えることはありません。

Performance Manager は一連のアーカイブ データを作成し、リアルタイム ラウンドロビン データベース内のサマリー情報を保持します。このアーカイブ データを使用して、日次、週次、月次、および年次の統合レポートが生成されます。Performance Manager はこの方法を使用して、重要な履歴データを維持します。増え続けるデータベース サイズを拡張するためのコストは不要です。

（注）　DCNM-SAN サーバでユーザ クレデンシャルを変更する場合は、Performance Manager を再起動する必要があります。

データ補間

Performance Manager 固有の機能の 1 つとして、統計的なポーリング結果が失われたり、遅延した場合にデータを補間する機能があります。その他のパフォーマンス ツールでは失われたデータ ポイントがゼロとして格納されることがありますが、この方法では過去の傾向が正しく反映されないことがあります。Performance Manager は失われたデータの前のデータ ポイントと、失われたデータのあとのポーリング インターバル中に格納されたデータ ポイントを比較して、失われたデータ ポイントを補間します。これによって、パフォーマンス情報の継続性が保たれます。

データ収集

2 つの変数（受信バイト数と送信バイト数）に関するデータを 1 年分収集するには、76 KB のサイズの Round-Robin Database（RRD）ファイルが必要です。エラーおよび廃棄数も収集する場合、RRD ファイル サイズは 110 KB になります。デフォルト内部値は次のとおりです。

- 5 分間のサンプル× 600 回（2 日と 2 時間）
- 30 分間のサンプル× 700 回（12.5 日）
- 2 時間のサンプル× 775 回（50 日）
- 1 日のサンプル× 300 回

1000 ポート SAN の履歴データを、エラー数および廃棄数を含めて 1 年分収集するには、110 MB が必要です。この SAN にファブリック ポートが同じように配置された 20 台のスイッチが存在する場合、データを監視するために、スイッチごとに約 2 ～ 3 個の SNMP（簡易ネットワーク管理プロトコル）パケット、合計で約 100 個の要求/応答 SNMP パケットが 5 分おきに送信されます。

変数カウンタ要求が関係するため、フローのストレージ スペース要件の予測は困難ですが、一般的にこの要件は予想できます。フローが追加されるたびに 76 KB ずつ増加します。

（注）　Performance Manager は、管理不能なスイッチおよび MDS 以外のスイッチに関する統計情報は収集しません。ループ デバイス（FL/NL）は収集されません。

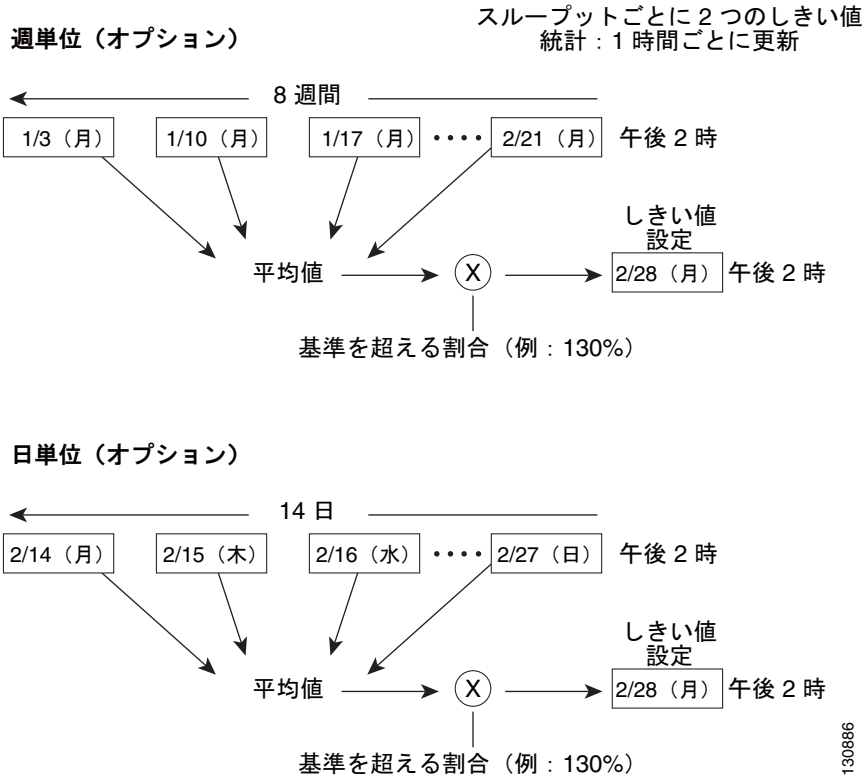
パフォーマンスしきい値の使用方法

Performance Manager Configuration Wizard では、監視対象のトラフィックが、設定した使用率を超えた場合にイベントをトリガーする 2 つのしきい値を設定できます。イベント トリガーは、DCNM-SAN Web クライアントの [Events] ブラウザ ページに通知される Critical または Warning のどちらかのイベントとして設定できます。

絶対値しきい値は、収集された統計情報に直接適用されます。統計情報が、合計リンク容量のパーセンテージとして、しきい値に設定された使用率と比較されます。統計が、設定されたしきい値を超えていると、DCNM-SAN Web クライアントの [Events] タブにイベントが表示されます。

同じタイム ウィンドウ（毎日、毎週、または 2 週間おき）のリンクごとに、典型的なトラフィック パターンに適合するしきい値が、基準しきい値に基づいて作成されます。基準しきい値は平均の割合（110% ～ 500%）として設定されます。100% は計算された重み付き平均です。図 7-1 に、毎週または毎日のオプションに対応する基準しきい値の設定例を示します。

図 7-1　　基準しきい値の例



しきい値を、月曜日午後 2 時に設定し、基準しきい値はこの統計情報の平均の 130% に設定します。平均は、これまでの月曜午後 2 時 に発生した統計値（オプションが毎週の場合）、またはこれまでの毎日午後 2 時に発生した 統計値（オプションが毎日の場合）から計算されます。

フロー統計

フロー統計情報は、集約統計情報テーブル内の入力トラフィックをカウントします。次の 2 種類の統計情報を収集できます。

- 集約フロー統計（VSAN のトラフィックをカウント）。
- VSAN 内の送信元/宛先 ID ペアに対応するトラフィックをカウントするフロー統計情報。

フロー カウンタをイネーブルにすると、集約フロー統計とフロー統計に最大 1 K のエントリが使用可能になります。各新フローのモジュールに必ず未使用のフロー インデックスを割り当ててください。フロー インデックスはモジュール全体で繰り返し使用できます。フロー インデックスの数値スペースは集約フロー統計とフロー統計で共用されます。

第 1 世代のモジュールは、モジュールあたり最大 1024 のフロー ステートメントを許容します。第 2 世代のモジュールは、モジュールあたり最大 2048 ～ 128 のフロー ステートメントを許容します。

表 7-1 に、監視対象のトラフィックのタイプを定義する Flow Type オプション ボタンの説明を示します。

表 7-1　Performance Manager のフロー タイプ

フロー タイプ	説明
Host->Storage	ホストからストレージ エレメントまでのデータを監視する一方向フロー
Storage->Host	ストレージ エレメントからホストまでのデータを監視する一方向フロー
Both	ホストとストレージ エレメント間のデータを監視する双方向フロー

フロー セットアップ ウィザード

Performance Manager Flow および Performance Manager Setup Wizard を使用すると、設定が大幅に簡単になります。必要な処理は、取り込む統計情報のカテゴリを選択することだけです。この選択を行うと、監視するフローおよびリンクのリストが表示されます。必要に応じてエントリを削除したり、表示されたリストを単に受け入れてデータ収集を開始できます。ホストおよびストレージ リンクの統計情報はスイッチ上の特定のポートと関連していないため、接続を別のポートに移動した場合、長期間の統計情報が失われることはありません。

Performance Manager Flow Wizard を使用したフローの作成

DCNM-SAN を使用して Performance Manager フローを作成する手順は、次のとおりです。

ステップ 1　[Performance] > [Create Flows] を選択します。

[Define Traffic Flows] ダイアログボックスが表示されます。

ステップ 2　[VSAN] フィールドのドロップダウン メニューをクリックします。

ステップ 3　フロー設定ウィザードに表示された VSAN のリストを選択します。

ステップ 4　[Zone] フィールドのドロップダウン メニューをクリックします。

ステップ 5　フロー設定ウィザードに表示されたゾーンのリストを選択します。

ステップ 6　[Next] をクリックして、次のウィンドウに進みます。

ステップ 7　[Possible Flow Pairs] エリアで項目を選択します。

[Review Traffic Flows] ウィンドウの [Exisitng Flows for Vsan] 領域に VSAN フロー ペアがすべて表示されます。

ステップ 8　[Add] をクリックし、選択したフローを作成します。

ステップ 9　[Existing Flows for Vsan] 領域から項目を選択します。

ステップ 10　[Remove] をクリックし、選択したフローを削除します。

ステップ 11　[Finish] をクリックし、Performance Manager の収集を再開します。

[Confirmation] ダイアログボックスが表示されます。

新しく作成したフローを確認するには、[Physical Attributes] > [End Devices] > [Flow Statistics] を選択します。作成したフローが表示されます。

CHAPTER 8

ネットワークのモニタリング

この章では、DCNM-SAN によるネットワークの管理方法について説明します。特に重要なネットワーク管理機能は、Storage Area Network（SAN; ストレージ エリア ネットワーク）の検出およびネットワーク モニタリングの 2 つです。

この章の内容は、次のとおりです。

- 「ネットワーク モニタリングの概要」（P.8-1）
- 「デバイス ディスカバリ」（P.8-2）
- 「トポロジ マッピング」（P.8-3）

ネットワーク モニタリングの概要

DCNM-SAN には、広範囲な SAN 検出、トポロジ マッピング、および情報表示機能があります。DCNM-SAN は、接続先のスイッチに対して SNMP クエリーを実行し、ファブリック トポロジに関する情報を収集します。そしてファブリック トポロジを再作成し、カスタマイズ可能なマップに表示し、[fabric view]、[device view]、[summary view]、[operation view] など複数の表示オプションでインベントリおよび設定情報を提供します。

DCNM-SAN を起動すると、SAN 検出プロセスが開始されます。DCNM-SAN は、ネーム サーバ レジストレーション、Fibre Channel Generic Services（FC-GS）、Fabric Shortest Path First（FSPF）、SCSI-3 など、シード Cisco MDS 9000 ファミリ スイッチからポーリングした情報を使用して、1 つまたは複数のファブリック上のすべてのデバイスと相互接続を自動的に検出します。すべての使用可能なスイッチ、Host Bus Adapter（HBA）、およびストレージ デバイスが検出されます。Cisco MDS 9000 ファミリ スイッチは、Fabric Device Management Interface（FDMI）を使用して、ホストのエージェントを使用せずに、HBA のモデル、シリアル番号、ファームウェア バージョン、およびホスト オペレーティング システムのタイプおよびバージョンを検出します。DCNM-SAN は、各スイッチへの SNMP クエリーを通じてこの情報を収集します。検出されるデバイス情報は、デバイス名、ソフトウェア リビジョン レベル、ベンダー、ISL（スイッチ間リンク）、PortChannels、VSAN などです。

ヘルスおよびイベントのモニタリング

DCNM-SAN では、Cisco MDS 9000 ファミリ スイッチと連動して、ファブリックおよびスイッチのヘルスおよびステータスを表示できます。ファブリックおよびコンポーネントの情報は、Online System Health Management、Call Home、システム メッセージ、および SNMP 通知など、複数の情報源から収集されます。これらの情報は、DCNM-SAN または Device Manager の複数のメニューから表示できます。

DCNM-SAN の [Events] タブ

トポロジ ウィンドウから使用できる DCNM-SAN の [Events] タブには、DCNM-SAN がファブリック内のソースから受信したイベントが表示されます。情報源には、SNMP イベント、RMON イベント、システム メッセージ、システム ヘルス メッセージが含まれます。[Events] タブには、イベント名、イベントの発信元および時刻、重大度、イベントの説明を含むイベント テーブルが表示されます。テーブルは、任意のカラムのヘッダーによりソートできます。

DCNM-SAN Web サーバ レポート内のイベント情報

DCNM-SAN Web サーバのクライアントに、Performance Manager により収集された情報を表示できます。この情報には、ファブリックから DCNM-SAN サーバに送信されたイベントが含まれます。レポートを表示するには、[Performance Manager] > [Reports] を選択します。Web ブラウザ上に Web クライアントが開き、DCNM-SAN サーバがモニタしているすべてのファブリックのサマリーが表示されます。特定のファブリックを選択して [Events] タブをクリックすると、選択したファブリックで発生したイベントのサマリーまたは詳細レポートを表示できます。サマリーには、ファブリック上でダウンしているスイッチ数、ISL 数、ホスト数、またはストレージ エレメント数、およびその SAN エンティティに対してロギングされた警告メッセージ数が表示されます。詳細ビューには、ファブリックからロギングされたすべてのイベントのリストが表示されます。表示するイベントは重大度、時刻範囲、タイプによって制限できます。

Device Manager のイベント

Device Manager で [Logs] > [Events] を選択すると、イベントが表示されます。Device Manager では、現在のイベントのリスト、または DCNM-SAN のホストに保管されている古いイベントのリストを表示できます。イベント テーブルには、時刻、情報源、重大度、簡単な説明を含む各イベントの詳細が表示されます。

SAN 検出およびトポロジ マッピング

DCNM-SAN には、広範囲な SAN 検出、トポロジ マッピング、および情報表示機能があります。DCNM-SAN は、接続先のスイッチに対して SNMP クエリーを実行し、ファブリック トポロジに関する情報を収集します。そしてファブリック トポロジを再作成し、カスタマイズ可能なマップで提示し、複数の表示オプションにより、インベントリおよび設定情報を提供します。

デバイス ディスカバリ

DCNM-SAN を起動すると、SAN 検出プロセスが開始されます。DCNM-SAN は、ネーム サーバ レジストレーション、Fibre Channel Generic Services（FC-GS）、Fabric Shortest Path First（FSPF）、SCSI-3 など、シード Cisco MDS 9000 ファミリ スイッチからポーリングした情報を使用して、1 つまたは複数のファブリック上のすべてのデバイスと相互接続を自動的に検出します。すべての使用可能なスイッチ、Host Bus Adapter（HBA）、およびストレージ デバイスが検出されます。Cisco MDS 9000 ファミリ スイッチは、Fabric Device Management Interface（FDMI）を使用して、ホストのエージェントを使用せずに、HBA のモデル、シリアル番号、ファームウェア バージョン、およびホスト オペレーティング システムのタイプおよびバージョンを検出します。DCNM-SAN は、各スイッチへの SNMP クエリーを通じてこの情報を収集します。検出されるデバイス情報は、デバイス名、ソフトウェア リビジョン レベル、ベンダー、ISL（スイッチ間リンク）、PortChannels、VSAN などです。

サードパーティ製スイッチが関連する VSAN の変更では、混合 VSAN 環境での依存関係を検出して正しいトポロジを示すため、DCNM-SAN で 2 回検出を実行する必要があります。1 回目の検出ではサードパーティ製スイッチが検出され、2 回目の検出ではスイッチが参加する VSAN と VSAN に接続されたエンド デバイスが検出されます。2 回目の検出が自動的に開始するのを待つことも、手動検出をトリガーすることもできます。

トポロジ マッピング

DCNM-SAN は、ファブリックのトポロジ表示を基盤にしています。デバイス検出情報に基づくトポロジ マップを表示することにより、DCNM-SAN では、単一ウィンドウに複数のファブリックが正確に表示されます。トポロジ マップのアイコン レイアウトは、ドラッグアンドドロップ方式のインターフェイスにより簡単に変更できます。トポロジ マップにはデバイスの相互接続が図示されるほか、使用しきい値を超えているゾーン、VSAN、ISL などの設定情報がハイライト表示されます。また、CLI（コマンドライン インターフェイス）セッションの起動、PortChannels の設定、Device Manager のオープンのビジュアル コンテキストも用意されています。

トポロジ マップの使用方法

DCNM-SAN のトポロジ マップのファブリック表示は、すべてのスイッチ、エンド デバイス、およびリンクの表示から、スイッチ間の複数リンクを単一の太線で示したコア スイッチだけの表示まで、任意にカスタマイズできます。表示を変更するには、トポロジ マップの左側にあるアイコンを使用するか、トポロジ マップ内の任意の場所を右クリックして表示されるマップ コントロールを使用します。

トポロジ マップを拡大または縮小して、SAN の全体図を表示したり、重要な領域だけを拡大して表示できます。また、ファブリック全体を示すオーバービュー ウィンドウを開くこともできます。このウィンドウ内を右クリックし、表示したい領域をボックスで囲んで指定すれば、その領域をメインのトポロジ マップ ビューに表示できます。

Logical Domains ペインからファブリックまたは VSAN を選択し、トポロジ表示の範囲を限定することもできます。選択したファブリックまたは VSAN だけがトポロジ マップに表示されます。

リンクまたはスイッチ上にマウス ポインタを移動すると、その SAN コンポーネントの簡単な説明がステータス情報とともに表示されます。コンポーネント上を右クリックすると、ポップアップ メニューが表示されます。コンポーネントの詳細情報を表示したり、コンポーネントの設定を聞いたり、そのコンポーネントの機能をテストすることができます。

リンクをダブルクリックすると、Information ペインにリンクのステータスおよび設定情報が表示されます。スイッチをダブルクリックすると、そのスイッチの Device Manager が起動します。

カスタマイズしたトポロジ マップ レイアウトの保存

トポロジ マップの変更を保存しておくと、特定のファブリックの DCNM-SAN クライアントの起動時に、いつでもカスタマイズしたビューを表示できます。

手順の詳細

DCNM-SAN で、カスタマイズしたレイアウトを保存する手順は、次のとおりです。

ステップ 1　[File] > [Preferences] の順にクリックし、[DCNM-SAN preferences] ダイアログボックスを開きます。

ステップ 2　[Map] タブをクリックし、[Automatically Save Layout] チェックボックスをオンにして、トポロジ マップの変更を保存します。

ステップ 3　[Apply] をクリックし、次に [OK] をクリックして変更を保存します。

DCNM-SAN トポロジ マップでのラックの使用

すべてのデバイスが FC-GS-3 リクエストに応答できるわけではないので、単一のサーバまたはストレージ サブシステム上の異なるポートが、トポロジ マップ上に個々のエンド デバイスとして表示されることがあります。これらのポートを DCNM-SAN 用の単一ラックにグループ化する方法については、「デバイス グループの変更」（P.5-31）を参照してください。

[Alias] > [Enclosure] をクリックすると、ホストおよびストレージ エレメントが [Information] ペインに表示されます。これはラックの名前を指定するためのショートカットです。このショートカットを使用するには、ホストまたはストレージのテーブルで単一ラックとしてグループ化する各行を強調表示し、[Alias] > [Enclosure] をクリックします。選択した各行のラック名として、エイリアスの最初のトークンが自動的に設定されます。

複数ファブリックのマッピング

複数のファブリックにログインするには、同じユーザ名およびパスワードを使用する必要があります。シード スイッチを選択しなくても、両方のファブリックの情報が表示されます。ファブリックの詳細を表示するには、[Fabric] ペインの下部でそのファブリックのタブを選択するか、またはファブリックの [Cloud] アイコンをダブルクリックします。引き続き DCNM-SAN を使用してファブリックを管理するには、「Cisco DCNM-SAN サーバ ファブリックの管理」（P.3-6）の手順に従います。

インベントリ管理

DCNM-SAN の [Information] ペインには、ファブリック内のすべてのスイッチ、リンク、およびホストのインベントリ、設定、およびステータス情報が表示されます。コンポーネント管理には、ベンダーの名前とモデル、およびソフトウェアまたはファームウェアのバージョンが含まれます。ファブリック内の VSAN、スイッチ、ホスト、およびストレージ エレメントの数を表示するには、[Logical Domains] ペインでファブリックまたは VSAN を選択し、[Information] ペインで [Summary] タブを選択します。DCNM-SANDCNM-SAN ユーザ インターフェイスの詳細については、「Cisco DCNM-SAN クライアント クイック ツアー：管理者向けの表示」（P.5-7）を参照してください。

DCNM-SAN Web サーバからの [Inventory] タブの使用方法

DCNM-SAN Web サーバが設定されていれば、このアプリケーションを起動して [Inventory] タブを選択し、DCNM-SAN サーバが管理しているファブリックのサマリーを表示できます。[Inventory] タブには、選択した SAN、ファブリック、またはスイッチのコンポーネントが表示されます。
DCNM-SAN Web サーバの設定および使用方法の詳細については、第 2 章「Cisco DCNM Web クライアント」を参照してください。

手順の詳細

DCNM-SAN Web サーバを使用してシステム メッセージをリモートで表示する手順は、次のとおりです。

ステップ 1　DCNM-SAN Web サーバで使用するブラウザを指定します。「DCNM Web クライアントの起動」（P.2-3）を参照してください。

ステップ 2　[Events] タブをクリックし、次に [Details] タブをクリックするとシステム メッセージが表示されます。イベント テーブル内のカラムはソートできます。また、[Filter] ボタンを使用して、テーブル内のメッセージの範囲を制限できます。

Device Manager からのログの表示

DCNM-SAN サーバと同じワークステーションから Device Manager を実行している場合には、Device Manager からシステム メッセージを表示できます。Device Manager で [Logs] > [Events] > [current] を選択すると、システム メッセージが表示されます。イベント テーブル内のカラムはソートできます。また、[Find] ボタンを使用して、テーブル内のテキストを検索できます。

スイッチに保存されているログは、ローカル Syslog サーバが設定されていなくても、またはスイッチの Syslog サーバ リストにローカル PC が含まれていなくても表示できます。ただし、メモリに制限があるため、特定のサイズに達すると古いログは消去されます。スイッチの Syslog には、2 つのログがあります。Critical 以上の重大度のメッセージが限定数だけ保存される NVRAM ログ、および Notice 以上の重大度のメッセージが保存される非永続的なログです。ハードウェア メッセージは、これらのログに含まれます。

（注）　Syslog のローカル ログを参照するには、Syslog ホストにある DCNM-SAN サーバの IP アドレスを設定します。

CHAPTER 9

パフォーマンスのモニタリング

この章では、Cisco DCNM-SAN および Device Manager 用にパフォーマンス モニタリング ツールを設定する方法について説明します。ツールでは、リアルタイム統計やパフォーマンス モニタリング履歴などを利用できます。

この章の内容は、次のとおりです。

- 「パフォーマンス モニタリングの概要」（P.9-1）
- 「Performance Manager の設定」（P.9-2）
- 「サマリー ビューの設定」（P.9-4）
- 「Device Manager を使用したポート単位モニタリングの設定」（P.9-5）
- 「DCNM-SAN リアルタイム ISL 統計情報の表示」（P.9-5）
- 「Performance Manager レポートの表示」（P.9-7）
- 「Performance Manager レポートの生成」（P.9-8）
- 「収集データのエクスポート」（P.9-11）
- 「SAN ヘルスの分析」（P.9-13）

パフォーマンス モニタリングの概要

Device Manager には、Cisco MDS 9000 ファミリ スイッチのポートを簡単にモニタできるツールが備えられています。このツールは設定された期間の統計を取得し、結果を表またはチャートで表示します。リアルタイム パフォーマンス統計はファブリックのダイナミック トラブルシューティングや障害分離に便利です。リアルタイム統計では、ファブリックの一部についてユーザによって定義された期間のデータを収集し、結果を DCNM-SAN および Device Manager で表示します。選択されたポートに対して、受信/送信トラフィック、エラー、クラス 2 トラフィック、および FICON データなどの任意の数の統計を監視することができます。

リアルタイム パフォーマンス モニタリング

Device Manager には、Cisco MDS 9000 ファミリ スイッチのポートを簡単に監視できるツールが備えられています。このツールは設定された期間の統計を取得し、結果を表またはチャートで表示します。統計結果は、選択したポートのパフォーマンスをリアルタイムで表示し、パフォーマンス モニタリングおよびトラブルシューティングに利用できます。選択されたポートに対して、受信/送信トラフィック、エラー、クラス 2 トラフィック、および FICON データなどの任意の数の統計を監視することができます。ポーリングは 10 秒 ～ 1 時間の間隔で設定でき、選択したオプションの数だけ結果を表示できます。結果は絶対値、1 秒あたりの値、1 秒あたりの最小値と最大値などから選択できます。

Device Manager で、関連モジュールの 4 つのポートからなるホストで最適化されたグループの加入過多をチェックします。モジュールのポート グループを右クリックし、ポップアップ メニューから [Check Oversubscription] を選択します。

Device Manager では、[Summary View] タブと、設定可能なポート単位のモニタ オプションを使用してパフォーマンスを表示できます。

パフォーマンス履歴のモニタリング

Performance Manager はネットワーク デバイスの統計情報の履歴を収集し、DCNM-SAN クライアントと Web ブラウザでこの情報を表示します。最近の統計情報は詳細が、古い統計情報はサマリーが表示されます。Performance Manager は Cisco Traffic Analyzer などの外部ツールとも統合されています。Performance Manager の概要については、「Performance Manager の概要」（P.7-1）を参照してください。

Performance Manager の設定

ここでは、次の内容について説明します。

- 「Performance Manager でのフローの作成」（P.9-2）
- 「Performance Manager での収集の作成」（P.9-2）
- 「パフォーマンスしきい値の使用方法」（P.9-3）

Performance Manager でのフローの作成

Flow Configuration Wizard を使用して、ホストからストレージ、ストレージからホスト、または両方向のフローを作成できます。いったん定義した後は、フローを収集コンフィギュレーション ファイルに追加してホストとストレージ エレメントのペア間のトラフィックをモニタできます。作成したフローは、Performance Manager Configuration Wizard の収集オプションの一部になります。

Performance Manager での収集の作成

Performance Manager Configuration Wizard により、コンフィギュレーション ファイルを使用して収集を簡単に作成できます。収集は、ファブリック内の 1 つの VSAN、またはすべての VSAN に対して定義します。収集には、表 9-1 に示す SAN のエレメント タイプの統計情報を含めることができます。

表 9-1　Performance Manager の収集タイプ

収集タイプ	説明
ISL	ISL のリンク統計を収集。
ホスト	SAN ホストのリンク統計を収集。
ストレージ	ストレージ エレメントのリンク統計を収集。
フロー	Flow Configuration Wizard で定義したフローの統計を収集。

パフォーマンスしきい値の使用方法

Performance Manager Configuration Wizard では、監視対象のトラフィックが、設定した使用率を超えた場合にイベントをトリガーする 2 つのしきい値を設定できます。イベント トリガーは、DCNM-SAN Web クライアントの [Events] ブラウザ ページに通知される Critical または Warning のどちらかのイベントとして設定します。

絶対値しきい値またはベースラインしきい値のどちらかを選択し、収集に定義されたすべての送信または受信トラフィックに適用する必要があります。収集した統計に直接適用するしきい値を設定するには、Performance Manager Configuration Wizard の最後の画面で、[Use absolute values] オプション ボタンをクリックします。統計情報が、合計リンク容量のパーセンテージとして、しきい値に設定された使用率と比較されます。統計が、設定されたしきい値を超えていると、DCNM-SAN Web クライアントの [Events] タブにイベントが表示されます。

たとえば、収集の絶対値しきい値として、利用率 60%（warning）および 80%（critical）を設定したとします。この場合、Performance Manager により、1 ギガビット リンク上のトラフィック量が 600 Mbps を超えていることが検出されると、warning イベントがトリガーされます。また、トラフィック量が 800 Mbps を超えると、critical イベントがトリガーされます。

ベースラインしきい値は、日数または週に対して定義します（1 日、1 週間、または 2 週間）。ベースラインでは、1 日、1 週間、または 2 週間単位で、その間の統計結果の平均値が計算されます。表 9-2 に、水曜日の午後 4 時に定義した収集のベースライン値の計算に使用される統計情報の例を示します。

表 9-2　水曜日の午後 4 時に開始された収集でのベースライン期間

ベースライン タイム ウィンドウ	平均値の計算に使用される統計情報
1 日	前日の午後 4 時からの統計
1 週間	1 週前の水曜日の午後 4 時からの統計
2 週間	2 週前の水曜日の午後 4 時からの統計

同じタイム ウィンドウ（毎日、毎週、または 2 週間おき）のリンクごとに、典型的なトラフィック パターンに適合するしきい値が、基準しきい値に基づいて作成されます。ベースラインしきい値は、計算された平均値を 100% とし、平均値のパーセンテージ（110 ～ 500%）として設定します。

たとえば、水曜日の午後 4 時に作成された収集で、1 週間のベースラインしきい値を平均値の 150%（warning）、および 200%（critical）に設定したとします。Performance Manager は、毎週水曜日の午後 4 時に、収集を開始して以降の水曜日ごとの午後 4 時に収集した統計情報を各リンクの平均値を再計算します。この値を新しい平均値として使用して、受信したトラフィックの統計値とこの値が比較され、リンク上のトラフィック量が平均値の 150% 以上であれば warning イベント、200% 以上であれば critical イベントが送信されます。

表 9-3 に、1 ギガビット リンクの収集で、2 つの異なる平均値に対して warning および critical イベントが送信されるトラフィック量を示します。

表 9-3　1 ギガビット リンクに対して生成されるイベントの例

平均値	150% で warning イベント送信	200% で critical イベント送信
400 Mbps	600 Mbps	800 Mbps
200 Mbps	300 Mbps	400 Mbps

これらのしきい値を設定するには、Collections Configuration Wizard の最後の画面で [Send events if traffic exceeds threshold] チェックボックスを選択します。

サマリー ビューの設定

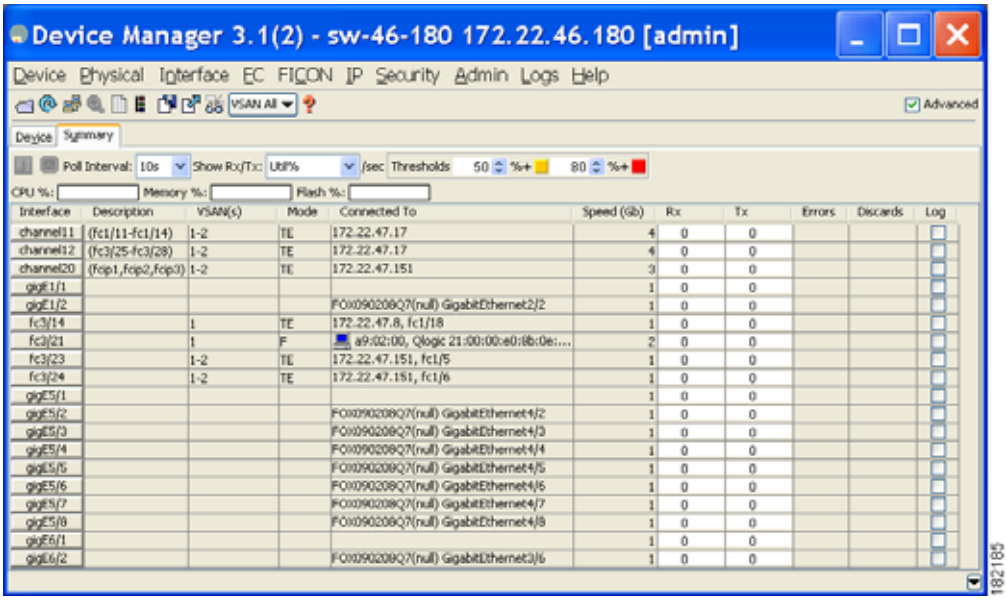
手順の詳細

Device Manager でサマリー ビューを表示する手順は、次のとおりです。

ステップ 1　メイン ディスプレイで [Summary] タブをクリックします。

サマリー ビューにスイッチ上のすべてのアクティブ ポートと、使用できる設定オプションが表示されます。

図 9-1　Device Manager の [Summary] タブ



ステップ 2　[Poll Interval] ドロップダウン リストから値を選択します。

ステップ 3　[Show Rx/Tx] ドロップダウン メニューを参照してデータの解釈方法を指定します。ポーリング インターバルごとに、スイッチのアクティブ ポートごとの受信および送信データの概要がテーブル内で更新されます。

ステップ 4　[Show Rx/Tx] ドロップダウン リストから値を選択します。[Util%] を選択すると、[Show Rx/Tx] > [%Util/sec] ドロップダウン リストのどちらの値も選択する必要があります。最初の値はイベント レポートの warning レベル、2 番目の値は critical しきい値レベルです。

ポートを選択し、[Monitor Selected Interface Traffic Util %] アイコンをクリックして、あるポートの利用率（パーセンテージ）を表示することもできます。

Device Manager を使用したポート単位モニタリングの設定

ポート単位で設定できるモニタ オプションにより、ポートの着信 / 発信トラフィック、エラー、クラス 2 トラフィック、その他のデータの統計を表示できます。一定時間のデータをグラフ表示することにより、ポートのパフォーマンスをリアルタイムで把握できます。

手順の詳細

Device Manager を使用してポート モニタリングを設定する手順は、次のとおりです。

ステップ 1　[Device] タブをクリックします。

ステップ 2　モニタするポートを右クリックし、ドロップダウン メニューから [Monitor] を選択します。

ポートのリアルタイム モニタ ダイアログボックスが表示されます。

ステップ 3　[Interval] ドロップダウン リストから値を選択し、このテーブルのデータを更新する頻度を指定します。

ステップ 4　テーブルから統計値をクリックし、グラフ アイコンの 1 つをクリックして、一定時間の統計グラフをリアルタイム表示します。グラフ タイプの変更オプションを含む、グラフ ウィンドウが表示されます。

ヒント　スイッチ上の任意のアクティブ ポートについて、複数の統計グラフを表示できます。

DCNM-SAN リアルタイム ISL 統計情報の表示

ここでは、次の内容について説明します。

- 「Performance Manager Configuratino Wizard の使用方法」（P.9-6）
- 「DCNM-SAN を使用したパフォーマンス統計情報の表示」（P.9-6）

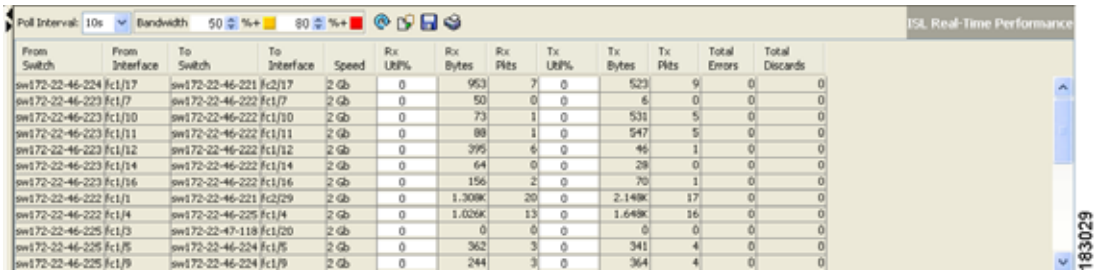
DCNM-SAN を設定して、ISL 統計情報をリアルタイムで収集できます。ISL 統計には、各 ISL の受信および送信の利用率、1 秒あたりのバイト数、エラーおよび廃棄数が含まれます。

DCNM-SAN を使用して ISL 統計情報を設定する手順は、次のとおりです。

ステップ 1　[Performance] > [ISL in Real-Time] を選択します。

[Information] ペインに任意の ISL 統計情報が表示されます。

図 9-2　リアルタイムの ISL パフォーマンス



ステップ 2　[Poll Interval] ドロップダウン リストから値を選択します。

ステップ 3　[Bandwidth] 利用率しきい値ドロップダウン リストから、マイナーとメジャーの 2 つのしきい値を選択します。

表示されたテーブル内で、ファブリック内すべての設定済み ISL の統計情報がポーリング インターバルごとに更新されます。

ステップ 4　テーブル内の行を選択すると、その ISL がトポロジ マップにブルーで強調表示されます。

Performance Manager Configuratino Wizard の使用方法

「パフォーマンス収集の作成、編集、および削除」（P.2-40）を参照してください。

DCNM-SAN を使用したパフォーマンス統計情報の表示

DCNM-SAN は、ISL またはエンド デバイスの履歴統計およびリアルタイム統計を収集するように設定できます。統計には、各 ISL またはエンド デバイスの受信および送信の利用率、1 秒あたりのバイト数、エラーおよび廃棄数が含まれます。

DCNM-SAN を使用して ISL またはエンド デバイスの履歴統計およびリアルタイム統計を表示する手順は、次のとおりです。

ステップ 1　[Fabric] ペインで ISL またはエンド デバイスを右クリックします。

コンテキスト メニューが表示されます。

ステップ 2　[Show Statics] を選択します。

（注）　[Show Statics] メニューはファブリックを Perfomance Manager の収集に追加している場合にだけイネーブルになります。

Performance Manager レポートの表示

ここでは、次の内容について説明します。

- 「パフォーマンス サマリーの表示」（P.9-7）
- 「パフォーマンス テーブルと詳細グラフの表示」（P.9-8）
- 「ホスト最適化ポート グループのパフォーマンスの表示」（P.9-8）
- 「Performance Manager イベントの表示」（P.9-8）

Performance Manager の統計データを表示するには、オンデマンドで作成され、Web ブラウザに表示される設定済みレポートを使用します。これらのレポートでは、日、週、月、年単位の結果のサマリーおよび詳細な統計情報を見ることができます。

手順の詳細

Performance Manager レポートを表示する手順は、次のとおりです。

ステップ 1　DCNM-SAN から Performance Manager レポートを表示するには、[Performance] > [Reports] の順に選択します。

Web ブラウザのウィンドウが開き、デフォルトで DCNM-SAN Web クライアントのイベント サマリー レポートが表示されます。

ステップ 2　Performance Manager レポートを表示するには、[Performance] タブをクリックします。

Performance Manager は、収集開始から 10 分後にデータのレポートを開始します。

（注）　レポートを有効にするには、DCNM-SAN Web サーバが実行されている必要があります。

パフォーマンス サマリーの表示

Performance Summary ページには、ホスト、ISL、ストレージ、およびフローについて直前の 24 時間のスループットとリンク使用率がダッシュボード形式で表示されます。ホットスポットがハイライト表示されるので、ファブリックの帯域幅の消費の概要をすばやく確認できます。

レポートには、ネットワーク スループットの円グラフ、およびリンク使用率の円グラフが表示されます。左側のナビゲーション ツリーを使用すると、モニタ対象のファブリックまたは VSAN のサマリー レポートを表示できます。このサマリーには、すべてのホスト、ストレージ エレメント、ISL、およびフローのグラフが表示されます。円グラフには、6 つの定義済み範囲について測定されたスループットまたはリンク使用率が、エンティティ（リンク、ホスト、ストレージ、ISL、フロー）についてパーセンテージで表示されます。円グラフ上にマウスを移動すると、統計データ範囲のエンティティ数を確認できます。円グラフをダブルクリックすると、ホスト、ストレージ エレメント、ISL、またはフローの統計テーブルが表示されます。

パフォーマンス テーブルと詳細グラフの表示

すべてのホスト、ストレージ、ISL、またはフローについて、前日のトラフィック量を表示するには、[Host]、[Storage]、[ISL] または [Flow] をそれぞれクリックします。テーブルに、選択したエンティティがすべて一覧表示され、送受信トラフィック、エラー、および廃棄数が表示されます（該当する場合）。テーブルは、任意カラムのヘッダーによりソートできます。また、日、週、月、年の各単位で表示できます。各カテゴリの統計情報テーブルには、平均およびピーク スループット値、および詳細情報へのホットリンクが示されます。

テーブル内のリンクをクリックすると、詳細ページが開き、日、週、月、年単位のグラフが表示されます。ポートにフローが存在する場合には、データを送信したストレージ ポートが表示されます。詳細ページには、統計の収集によりエラーおよび廃棄が検出された場合かつ 0 ではない場合、これらのグラフも表示されます。

詳細レポート上のグラフをダブルクリックすると、ファイバ チャネルの Cisco Traffic Analyzer が起動します（設定されている場合）。Cisco Traffic Analyzer には、ファブリック内のホスト、ストレージ、デバイス、および VSAN に対応するエイリアスが渡されるので、簡単に識別できます。

ホスト最適化ポート グループのパフォーマンスの表示

ホスト最適化ポート グループのパフォーマンスをモニタするには、[Performance] > [End Devices] の順にクリックし、[Type] ドロップダウン リストから [Port Groups] を選択します。

Performance Manager イベントの表示

Performance Manager イベントは、DCNM-SAN Web サーバから表示できます。DCNM-SAN Web サーバの問題およびイベントを表示するには、任意のファブリックを選択して [Events] タブをクリックします。選択したファブリック内で発生した問題やイベントのサマリーまたは詳細レポートが表示されます。

Performance Manager レポートの生成

- 「Performance Manager での Top10 レポートの生成」（P.9-8）
- 「スクリプトを使用した Top10 レポートの生成」（P.9-9）

Performance Manager での Top10 レポートの生成

履歴の Top10 レポートを生成し、保存してあとから確認できます。このレポートには、データ収集のエンティティがリストされ、最もアクティブなエンティティが最初に表示されます。このレポートは 1 回限りのスタティックな情報で、収集データの平均値およびグラフが、レポート生成時のスナップショットとして作成されます。Top10 レポートは、Performance Manager の他のモニタリング テーブルおよびグラフと異なり、その他のデータが継続的に収集されるわけではなく、カラムによるソートもできません。Top10 レポートは、レポート生成時のスナップショット ビューであり、スタティックな情報です。これらは、レポート生成時のスナップショットとして、データ収集の平均およびグラフを生成する 1 回限りのレポートです。

ヒント　レポート名にタイムスタンプを指定しておくと、特定の日付または週のレポートを簡単に検索できます。

Top10 レポートは、Performance Manager の他のモニタリング テーブルおよびグラフと異なり、その他のデータが継続的に収集されるわけではなく、カラムによるソートもできません。Top10 レポートは、レポート生成時のスナップショット データです。

（注）　Top10 レポートの生成では、特定の時間範囲の既存データの分析が必要になるので、大型ファブリックの場合、数時間を要することがあります。

Top10 レポートの作成に関する詳細については、「カスタム レポート テンプレートの作成」（P.2-25）を参照してください。

スクリプトを使用した Top10 レポートの生成

次のコマンドを使用して、Top10 レポートを手動で生成できます。

- UNIX の場合、次のスクリプトを実行します。

  ```
  "/<user_directory>/.cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>"
  ```

- Windows の場合、次のスクリプトを実行します。

  ```
  "c:\Program Files\Cisco Systems\MDS 9000\bin\pm.bat display pm\pm.xml
  <output_directory>"
  ```

UNIX では、次の cron エントリを追加することによって、DCNM-SAN サーバ ホスト上で 1 時間に 1 度 Top10 レポートを自動生成することができます。

```
0 * * * * /<user_directory>/.cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>
```

crontab が自動的に実行されない場合、または Java に例 9-1 のような例外が表示される場合には、/<user_directory>/.cisco_mds9000/bin/pm.sh の JVMARGS コマンドに「-Djava.awt.headless=true」を追加する必要があります。

例 9-1　　Java 例外の例

```
in thread "main" java.lang.InternalError Can't connect to X11 window server using '0.0' as
the value of the DISPLAY variable.
```

Cisco Traffic Analyzer と併用するための Performance Manager の設定

Performance Manager と Cisco Traffic Analyzer を併用することによって、ファブリック上のトラフィックをモニタおよび管理できます。Cisco Traffic Analyzer と Performance Manager を併用するには、次のコンポーネントが必要です。

- ファイバ チャネル トラフィックを転送する設定済みのファイバ チャネル Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）Destination（SD）ポート。
- ファイバ チャネル トラフィックをイーサネット トラフィックに変換する Port Analyzer Adapter 2（PAA-2）。

- PAA-2 からのトラフィックを分析する Cisco Traffic Analyzer ソフトウェア。

Cisco Traffic Analyzer と併用するために Performance Manager を設定する手順は、次のとおりです。

ステップ 1　『*Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*』の手順に従って、Cisco Traffic Analyzer を設定します。

ステップ 2　次に示す 3 つの情報を取得します。

- Performance Manager および Cisco Traffic Analyzer が稼動している管理ワークステーションの IP アドレス。
- Cisco Traffic Analyzer がインストールされたディレクトリのパス。
- Cisco Traffic Analyzer が使用するポート（デフォルトは 3000）。

ステップ 3　Cisco Traffic Analyzer を起動します。

a. [Performance] > [Traffic Analyzer] > [Open] を選択します。

b. Cisco Traffic Analyzer の URL を次の形式で入力します。

```
http://<ip address>:<port number>
```

ip address は、Cisco Traffic Analyzer がインストールされている管理ワークステーションのアドレスです。

:*port number* は、Cisco Traffic Analyzer が使用するポートです（デフォルトは :3000）。

c. [OK] をクリックします。

d. [Performance] > [Traffic Analyzer] > [Start] を選択します。

e. Cisco Traffic Analyzer の場所を次の形式で入力します。

```
D:\<directory>\ntop.bat
```

D: は、Cisco Traffic Analyzer がインストールされているディスク ドライブのドライブ名です。

directory は、ntop.bat ファイルが格納されているディレクトリです。

f. [OK] をクリックします。

ステップ 4　Flow Configuration Wizard を使用して、Performance Manager でモニタするフローを作成します。「Performance Manager でのフローの作成」（P.9-2）を参照してください。

ステップ 5　Performance Manager Configuration Wizard を使用して、Performance Manager で収集するデータを定義します。「Performance Manager での収集の作成」（P.9-2）を参照してください。

a. 情報を収集する VSAN を選択するか、[All VSANs] を選択します。

b. 情報を収集する項目のタイプ（ホスト、ISL、ストレージ デバイス、およびフロー）を選択します。

c. Cisco Traffic Analyzer の URL を次の形式で入力します。

```
http://<ip address>/<directory>
```

それぞれの説明は次のとおりです。

ip address は、Cisco Traffic Analyzer がインストールされている管理ワークステーションのアドレスです。*directory* は、Cisco Traffic Analyzer がインストールされているディレクトリのパスです。

d. [Next] をクリックします。

e. このセクションおよび次のセクションに記載されたデータを確認して、このデータが目的のデータであることを確認します。

f. [Finish] をクリックして、データ収集を開始します。

（注）　JBOD または仮想ポートのデータは収集されません。データ収集中にデータ収集設定パラメータを変更した場合に、変更を有効にするには、収集プロセスを停止して再開する必要があります。

ステップ 6　[Performance] > [Reports] を選択して、レポートを生成します。Performance Manager Web Server が実行されている必要があります。Web Services が表示されます。[Custom] をクリックし、レポートのテンプレートを選択します。

（注）　レポートのデータ収集が開始されるまでに、最低 5 分かかります。収集の最初の 5 分間は、Performance Manager でレポートを生成しないでください。

ステップ 7　[Host] または [Storage] 詳細ページの最上部で [Cisco Traffic Analyzer] をクリックして Cisco Traffic Analyzer 情報を表示するか、または [Performance] > [Traffic Analyzer] > [Open] の順に選択します。ntop を開始していないと、Cisco Traffic Analyzer ページは開きません。

（注）　SPAN セッションの取り込み手順、および Cisco Traffic Analyzer セッションを開始して表示する手順については、『*Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*』を参照してください。

（注）　Performance Manager データの表示と解釈については、「Performance Manager でのフローの作成」（P.9-2）を参照してください。

Cisco Traffic Analyzer データの表示と解釈については、『*Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*』を参照してください。

より詳細な調査が必要な場合、Cisco Traffic Analyzer は Performance Manager のグラフのコンテキスト内で起動できます。ホスト、ストレージ デバイス、VSAN に対応するエイリアスが Cisco Traffic Analyzer に渡されるので、識別が容易になります。

収集データのエクスポート

ここでは、次の内容について説明します。

- 「収集データの XML ファイルへのエクスポート」（P.9-11）
- 「読み取り可能フォーマットでの収集データのエクスポート」（P.9-12）

収集データの XML ファイルへのエクスポート

Performance Manager で使用する RPD ファイルは、rrdtool というフリーウェア ツールにエクスポートできます。RRD ファイルは、DCNM-SAN サーバの pm/db に存在します。収集データを XML ファイルにエクスポートするには、オペレーティング システムのコマンドライン プロンプトに次のコマンドを入力します。

```
/bin/pm.bat xport xxx yyy
```

このコマンドで、*xxx* は RRD ファイル、*yyy* は生成する XML ファイルです。この XML ファイルは、次のコマンドを使用して rrdtool で読み込むことができるフォーマットになっています。

```
rrdtool restore filename.xml filename.rrd
```

XML ファイルをインポートするには、次のコマンドを使用します。

```
bin/pm.bat pm restore <xmlFile> <rrdFile>
```

このコマンドで読み込まれた XML エクスポート フォーマットは、次のコマンドを使用して rrdtool で書き出すことができます。

```
rrdtool xport filename.xml filename.rrd.
```

pm xport および **pm restore** コマンドは、DCNM-SAN サーバの bin\PM.bat（Windows プラットフォームの場合）または bin/PM.sh（UNIX プラットフォームの場合）にあります。rrdtool の詳細については、http://www.rrdtool.org を参照してください。

読み取り可能フォーマットでの収集データのエクスポート

Performance Manager で使用される RRD ファイルを、rrdtool と呼ばれるフリーウェア ツールにエクスポートし、収集データを XML ファイルにエクスポートできます。Cisco MDS SAN-OS Release 2.1(1a) では、カンマ区切り形式（CSV）で収集データをエクスポートできません。CSV 形式は、Microsoft Excel などの各種ツールにインポートできます。これらの読み取り可能な収集データは、DCNM-SAN Web Services のメニューからエクスポートするか、または Windows または UNIX のコマンド ラインからバッチ モードでエクスポートできます。DCNM-SAN Web Services を使用して、1 つのファイルをエクスポートできます。バッチ モードを使用すると、pm.xml ファイルの収集データをすべてエクスポートできます。

（注）　この機能を有効にするには、DCNM-SAN Web サーバが実行されている必要があります。

手順の詳細

DCNM-SAN Web サーバを使用して収集データを Microsoft Excel にエクスポートする手順は、次のとおりです。

ステップ 1　メイン ページで [Performance] タブをクリックします。

概要テーブルが表示されます。

ステップ 2　[Flows] サブタブをクリックします。

ステップ 3　エクスポートするエンティティの名前を右クリックし、[Export to Microsoft Excel] を選択します。

ポップアップ ウィンドウに、そのエンティティの Excel の図が表示されます。

コマンドラインのバッチ モードを使用して収集データをエクスポートする手順は、次のとおりです。

ステップ 1　ワークステーション上のインストレーション ディレクトリに移動し、さらに bin ディレクトリに移動します。

ステップ 2　Windows の場合、**.\pm.bat export C:¥Program Files¥Cisco Systems¥MDS 9000¥pm¥pm.xml** <*export directory*> を入力します。ワークステーションの *export directory* に csv ファイル（export.csv）が作成されます。

ステップ 3　UNIX の場合、**./pm.sh export /usr/local/cisco_mds9000/pm/pm.xml** <*export directory*> を入力します。ワークステーションの *export directory* に csv ファイル（export.csv）が作成されます。

このエクスポート ファイルを Microsoft Excel で開くと、次の情報が表示されます。

- エクスポートしたエンティティのタイトル、および情報の発信元スイッチのアドレス。
- このエンティティの接続リンク上の最大速度。
- VSAN ID および最大速度。
- タイムスタンプ、および送受信データのレート（バイト数/秒）。

SAN ヘルスの分析

SAN Health Advisor ツールは、パフォーマンスのモニタリングと統計情報の収集に使用するユーティリティです。このツールを使用して、次のタスクを実行できます。

- Performance Monitor を実行して I/O 統計情報を収集する。
- ファブリック インベントリ（スイッチやその他のデバイス）を収集する。
- ファブリック トポロジのグラフィック レイアウトを作成する。
- エラー状況と統計データのレポートを作成する。

任意の SAN 環境にこのツールをインストールすることで、特定期間（通常は 24 時間）の I/O 統計情報を収集し、ヘルス レポートを生成し、指定のシステム管理者に確認用として定期的にレポートを自動送信できます。

SAN Health Advisor ツールを起動すると、ウィザード モードが開始され、シード スイッチ クレデンシャル、データの送信先となるサーバの IP アドレス、およびソフトウェア設定に必要なすべての情報を入力するように求められます。ツールは、ファブリックが検出された時点でパフォーマンス データ、I/O 統計情報、およびエラー状況の取得を開始します。

収集データから生成されたレポートは、**$INSTALLDIR/dcm/fm/reports** ディレクトリに格納されます。これらのレポートは、指定の SAN 管理者に確認用として自動送信されます。ツールがデータ収集に失敗した場合、エラー メッセージまたは例外を示すレポートが生成されます。このレポートを送信した後、ツールは自動的にアンインストールし、ホスト マシンに確立されたすべてのプロセスを終了します。

SAN Health Advisor ツールによって生成されたレポートには、次の詳細が含まれます。

- イベント
- システム メッセージ
- 接続の分析
- ゾーンの不一致
- システム設定

- インターフェイス ステータス
- ドメイン情報
- セキュリティ設定

SAN Health Advisor ツールのインストール

SAN Health Advisor ツールは、Windows、UNIX、および Solaris プラットフォームにインストールし、実行できます。JRE バージョン 6.0 と一緒に .jar ファイルを含むパッケージをインストールします。

（注）　SAN Health ツールは、デフォルトでは DCNM-SAN ソフトウェアのインストール時にインストールされません。

Windows に SAN Health Advisor ツールをインストールする手順は、次のとおりです。

ステップ 1　SAN Health Advisor ツール インストーラをダブルクリックします。

SAN Health Advisor ツールのインストーラ ウィンドウが表示されます。

ステップ 2　ワークステーション上で、SAN Health Advisor 用のインストール フォルダを選択します。

Windows では、デフォルトのロケーションは **C:¥Program Files¥Cisco Systems¥** です。

ステップ 3　[Install] をクリックして、インストールを開始します。

インストールの進捗状況が表示されます。

[Fabric Options] ダイアログボックスが表示されます。

ステップ 4　[Seed Switch] テキスト ボックスにシード スイッチの IP アドレスを入力します。

ステップ 5　スイッチのユーザ名とパスワードを入力します。

ステップ 6　[Auth-Privacy] ドロップダウン リスト ボックスから認証プライバシー オプションを選択します。

ステップ 7　[Performance Collection] チェックボックスをオンにして、プロセスが 24 時間実行されるようにします。

ステップ 8　[Collect] をクリックして、パフォーマンス情報の収集を開始します。

収集ダイアログボックスが表示されます。

プロセスの途中で情報収集を停止する場合は、[Cancel] をクリックします。パフォーマンス収集が完了したことを示すメッセージが表示されます。

ステップ 9　SAN Health Advisor ソフトウェアを削除するには、[Uninstall] をクリックします。

CHAPTER 10

ソフトウェア イメージ

この章では、Cisco MDS ソフトウェア イメージのインストールおよびアップグレード方法について説明します。この章の内容は、次のとおりです。

- 「ソフトウェア イメージの概要」（P.10-1）
- 「ソフトウェア イメージのインストールの前提条件」（P.10-4）
- 「Software Install Wizard の使用方法」（P.10-8）
- 「ファブリックおよびモジュラ スイッチの中断がないアップグレードの実行」（P.10-11）
- 「スーパーバイザ モジュールのメンテナンス」（P.10-13）
- 「ジェネレーション 1 シャーシへのジェネレーション 2 モジュールの設置」（P.10-14）
- 「モジュールの交換」（P.10-15）

ソフトウェア イメージの概要

ここでは、次の内容について説明します。

- 「ソフトウェア アップグレード方法」（P.10-2）
- 「ソフトウェアの互換性の判別」（P.10-2）
- 「自動アップグレード」（P.10-3）
- 「Software Install Wizard を使用した場合の利点」（P.10-3）
- 「失敗するケースの特定」（P.10-4）

各スイッチは、Cisco MDS 9000 ファミリ スイッチ用の Cisco MDS NX-OS または SAN-OS オペレーティング システムが搭載されて出荷されます。Cisco MDS NX-OS は、キックスタート イメージとシステム イメージの 2 つのイメージで構成されます。スイッチを新しいイメージにアップグレードするには、スイッチをイメージに導く変数を指定する必要があります。

- キックスタート イメージを選択するには、KICKSTART 変数を使用します。
- システム イメージを選択するには、SYSTEM 変数を使用します。

イメージと変数は、インストールの手順で重要な要素となります。スイッチをアップグレードするには、変数とイメージを指定する必要があります。両方のイメージは、必ずしもそれぞれのインストールに必要とされるわけではありません。

（注）　明示的に指定されている場合を除き、この章のソフトウェアのインストール手順は、Cisco MDS 9000 ファミリのすべてのスイッチに適用します。

ソフトウェア アップグレード方法

ミッションクリティカルなハイ アベイラビリティ環境向けに設計された Cisco MDS NX-OS ソフトウェアを使用すると、中断なしにソフトウェアをアップグレードできます。Cisco MDS 9500 ディレクタの中断のないアップグレードの利点を活かすには、デュアル スーパーバイザ モジュールをインストールすることを強く推奨します。

Cisco MDS 9000 ファミリの任意のスイッチをアップグレードするには、次のいずれかの方法を使用します。

- 自動：Cisco MDS NX-OS スイッチの DCNM-SAN Software Install Wizard を使用できます（「Software Install Wizard の使用方法」（P.10-8）を参照）。
- 手動：手動によるアップグレードの詳細については、『*Cisco MDS 9020 Switch Configuration Guide and Command Reference*』を参照してください。

場合によっては、使用プロセスに関係なく、ソフトウェア アップグレードが中断されることがあります。そうした例外的なケースが発生するのは、次のような場合です。

- キックスタートまたはシステム イメージを持つシングル スーパーバイザ モジュール システムが変更される場合。
- 互換性のないシステム ソフトウェア イメージを持つデュアル スーパーバイザ モジュール システムの場合。

（注）　ハイ アベイラビリティを維持するには、同じネットワークまたは仮想 LAN にアクティブおよびスタンバイ両方のスーパーバイザのイーサネット ポートを接続する必要があります。アクティブ スーパーバイザは、これらのイーサネット接続が使用する 1 つの IP アドレスを所有しています。スイッチオーバーでは、新しくアクティブになったスーパーバイザがこの IP アドレスを継承します。

ソフトウェアの互換性の判別

稼動中のイメージとインストールするイメージに互換性がない場合は、非互換性がレポートされます。場合によっては、この設定を進めることができます。アクティブとスタンバイのスーパーバイザ モジュールが異なるバージョンのイメージを稼動する場合、両方のイメージが HA に互換性がある場合と、互換性がない場合があります。

互換性は、イメージと設定に基づいて確立されます。

- イメージの非互換性：稼動中のイメージとインストールするイメージに互換性がありません。
- 設定の非互換性：稼動中のイメージ内の特定の機能が、インストールするイメージでサポートされないために停止する場合は、互換性がありません。次のいずれかの記述に当てはまる場合、インストールするイメージが稼動中のイメージと互換性がないと見なされます。
  - 互換性のない機能が、インストールするイメージでイネーブルにされていて、稼動中のイメージでは利用できないために、スイッチが不整合な状態に移行する可能性がある場合。この場合、非互換性は *strict* です。

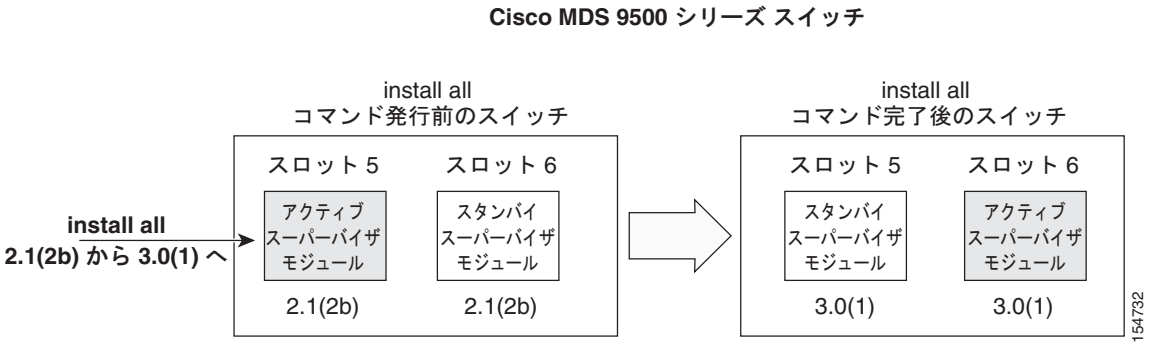
- 互換性のない機能が、インストールするイメージでイネーブルにされていて、稼動中のイメージでは利用できないが、スイッチが不整合な状態に移行する原因にならない場合。この場合、非互換性は *loose* です。

ヒント　**Software Install Wizard** は、インストールを継続する前に互換性を比較し、結果を示します。これらの変更を継続したくない場合は、終了できます。

自動アップグレード

Software Install Wizard は、Cisco MDS 9000 ファミリ スイッチのすべてのモジュールをアップグレードします。図 10-1 に、Software Install Wizard の使用前後のスイッチ ステータスの概要を示します。

図 10-1　Software Install Wizard の効果



Software Install Wizard は、スタンバイ スーパーバイザ モジュールが稼動しているか（存在する場合）自動確認します。稼動していない場合、モジュールをリロードし、**force download オプション**を使用して稼動するように強制します。

Software Install Wizard を使用した場合の利点

Software Install Wizard は、次の利点を提供します。

- 1 つの手順コマンドだけの使用でスイッチ全体をアップグレードできます。
- インストールを続行する前に、システムに加えようとしている変更についての説明を参照できます。
- 中断が最も少ない手順を使用して、スイッチ全体をアップグレードできます。
- このコマンドの経過表示を、コンソール、Telnet、および SSH 画面で確認できます。
  - 切り替えプロセス後は、両方のスーパーバイザ モジュールの経過表示を確認できます。
  - 切り替えプロセス前は、アクティブ スーパーバイザ モジュールの経過表示だけを確認できます。
- Software Install Wizard は、イメージの整合性を自動チェックします。これには、稼動中のキックスタートおよびシステム イメージが含まれます。

- Software Install Wizard はプラットフォームの有効性チェックを実行し、正しくないイメージが使用されていないかどうかを確認します。たとえば、不注意で MDS 9500 シリーズ イメージを使用して MDS 9200 シリーズ スイッチをアップグレードしていないかどうかを確認する場合などです。
- インストールを発行したあと、シーケンスの任意のステップが失敗すると、ウィザードは進行中のステップを終わらせ、終了します。

  たとえば、スイッチング モジュールが何らかの理由によって更新に失敗すると（たとえば、不安定なファブリックの状態）、コマンド シーケンスはモジュールを中断させながら更新し、終了します。このような場合、影響を受けたスイッチング モジュールの問題を確認し、その他のスイッチング モジュールをアップグレードできます。

失敗するケースの特定

次の状況が発生すると、インストールが終了します。

- スタンバイ スーパーバイザ モジュールの bootflash: ファイル システムに、更新されたイメージが入る十分なスペースがない。
- 指定したシステム イメージとキックスタート イメージに互いに互換性がない。
- アップグレードの進行中にファブリックまたはスイッチが設定された場合。
- アップグレードの進行中に、モジュールが削除される。
- アップグレードの進行中にスイッチの電源が停止した場合。
- リモート ロケーションへのパス全体が正確に指定されていない場合。
- アップグレード後のイメージに互換性がない。たとえば、スイッチング モジュールのイメージまたはキックスタート イメージがシステム イメージと互換性がない可能性があります。また、これは Software Install Wizard 互換性チェックによって特定されます。

注意　インストールが終了した場合、各段階でスイッチのステートを確認し、10 秒後にコマンドを再入力します。10 秒以内にインストールを再発行すると、インストールが現在進行中であることを示すエラー メッセージが表示されインストールが拒否されます。

ヒント　インストールがまだ終了していないときは、すべての設定が拒否されます。ただし、CFS アプリケーションを介した設定は受け入れられ、アップグレード手順に影響する場合があります。

ソフトウェア イメージのインストールの前提条件

ソフトウェア イメージのインストール手順は、次の要素によって異なります。

- ソフトウェア イメージ：Cisco MDS 9000 ファミリ スイッチ プロンプトからアクセスできるディレクトリまたはフォルダにキックスタートおよびシステム イメージ ファイルがあります。
- イメージ バージョン：各イメージ ファイルにはバージョンがあります。
- スイッチのフラッシュ ディスク：bootflash: はスーパーバイザ モジュール上にあり、CompactFlash ディスクは slot0: デバイスに挿入されています。

- スーパーバイザ モジュール：シングル スーパーバイザ モジュールまたはデュアル スーパーバイザ モジュールがあります。

Cisco MDS 9100 シリーズ スイッチの正しいソフトウェア イメージの選択

Cisco MDS 9100 シリーズ スイッチでサポートされているスーパーバイザ 1 およびスーパーバイザ 2 モジュールでは異なるシステム イメージとキックスタート イメージが必要です。表 10-1 と表 10-2 に示された命名規則により、スイッチで使用するイメージを判別できます。

表 10-1　MDS 9100 シリーズのスーパーバイザ モジュールのソフトウェア イメージ命名規則

Cisco MDS 9100 シリーズ スイッチのタイプ	スーパーバイザ モジュールのタイプ	命名規則
9124、9124e、9134、HP c-Class BladeSystem 用のシスコ ファブリック スイッチ、IBM BladeCenter 用のシスコ ファブリック スイッチ	スーパーバイザ 2 モジュール	ファイル名は m9100-s2ek9 で始まります。

表 10-2　MDS 9100 シリーズのソフトウェア イメージ命名規則

Cisco MDS 9100 シリーズ スイッチのタイプ	スーパーバイザ モジュールのタイプ	命名規則
Cisco MDS 9148 マルチレイヤ ファブリック スイッチ	スーパーバイザ 2 モジュール	ファイル名は m9100-s3ek9 で始まります。
Cisco MDS 9124 マルチレイヤ ファブリック スイッチ	スーパーバイザ 2 モジュール	ファイル名は m9100-s3ek9 で始まります。

Cisco MDS 9200 シリーズ スイッチの正しいソフトウェア イメージの選択

Cisco MDS 9200 シリーズ スイッチでサポートされているスーパーバイザ 1 およびスーパーバイザ 2 モジュールでは異なるシステム イメージとキックスタート イメージが必要です。表 10-3 に示された命名規則により、スイッチで使用するイメージを判別できます。

表 10-3　MDS 9200 シリーズのスーパーバイザ モジュールのソフトウェア イメージ命名規則

Cisco MDS 9200 シリーズ スイッチのタイプ	スーパーバイザ モジュールのタイプ	命名規則
9222i	スーパーバイザ 2 モジュール	ファイル名は m9200-s2ek9 で始まります。
9216、9216A、または 9216i	スーパーバイザ 1 モジュール	ファイル名は m9200-s1ek9 で始まります。

Cisco MDS 9500 ファミリ スイッチの正しいソフトウェア イメージの選択

Cisco MDS 9500 ファミリ スイッチでサポートされているスーパーバイザ 1 およびスーパーバイザ 2 モジュールでは異なるシステム イメージとキックスタート イメージが必要です。表 10-4 に示された命名規則により、スイッチで使用するイメージを判別できます。

表 10-4　MDS 9500 シリーズのスーパーバイザ モジュールのソフトウェア イメージ命名規則

Cisco MDS 9500 シリーズ スイッチのタイプ	スーパーバイザ モジュールのタイプ	命名規則
9513	スーパーバイザ 2 モジュール	ファイル名は m9500-sf2ek9 で始まります。
9506 または 9509	スーパーバイザ 2 モジュール	ファイル名は m9500-sf2ek9 で始まります。

不可欠なアップグレード要件

（注） Cisco SAN-OS 3.1(3) へのソフトウェア アップグレード中、CompactFlash CRC Checksum テストがバックグラウンドで自動的に実行されます。障害がある CompactFlash を実行しているモジュールがあると、オンラインのすべてのモジュールでテストが実行され、インストールが停止します。このような状況が発生した場合、この状況が訂正されるまでスイッチをアップグレードできません。システム メッセージはモジュールの情報を表示し、**system health cf-crc-check module** CLI コマンドを入力してトラブルシューティングを行う必要があることを示します。CompactFlash チェックサム機能でサポートされている新しいコマンドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

ソフトウェア イメージ バージョンを移行する前に、次の注意事項に従ってください。

- 購入した代理店

  ソフトウェアのアップグレードを実行する前に、ソフトウェアのアップグレード要件の確認と、現在の稼動環境に基づく推奨事項について、カスタマー サービス担当者に問い合わせます。

（注） シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接ご購入された場合は、次の URL にある Technical Assistance Center（TAC）にご連絡ください。
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

- スケジューリング

  ファブリックが一定して安定しているときに、アップグレードを予定します。スイッチまたはネットワークにアクセスできるすべての人がその時間にスイッチまたはネットワークを設定しないようにします。この時間帯は、すべての設定を禁止します。

- スペース

  イメージをコピーする場所に十分なスペースがあることを確認します。このロケーションは、アクティブおよびスタンバイ スーパーバイザ モジュール bootflash:（スイッチに内蔵）などです。

  - スタンバイ スーパーバイザ モジュールの bootflash: ファイル システム。
  - 内蔵 bootflash: には、約 200 MB のユーザ領域があります。

- ハードウェア

  インストール手順の際に、電源が停止しないようにします。このような問題は、ソフトウェア イメージを壊す可能性があります。

- 接続（リモート サーバからイメージを検索）
  - 10/100/1000 BASE-T イーサネット ポート接続の IPv4 アドレスまたは IPv6 アドレスを設定します（インターフェイス mgmt0）。

  （注）　Supervisor-2 モジュールでは 1000 BASE-T イーサネットのみを使用できます。

  - スイッチがリモート サーバへのルートを持つことを確認します。サブネット間でトラフィックをルーティングするルータがない場合は、スイッチおよびリモート サーバは同一のサブネットワーク上にある必要があります。
- イメージ
  - 指定したシステム イメージとキックスタート イメージに互いに互換性があることを確認します。
  - キックスタート イメージが指定されていない場合、スイッチは現在稼動中のキックスタート イメージを使用します。
  - 別のシステム イメージを指定する場合は、実行中のキックスタート イメージと互換性があることを確認します。
  - イメージは、次の 2 つの方法のいずれかで取得します。

    ローカル ファイル：イメージはスイッチでローカルに使用できます。

    リモート ファイル：イメージはリモート ロケーションにあり、ユーザはリモート サーバ パラメータとローカルに使用するファイル名を使用して宛先を指定します。
- 用語

  表 10-5 は、インストールとアップグレードのプロセスに特化した用語をまとめています。

表 10-5　特別な用語

用語		定義
bootable		イメージの互換性に基づいて、モジュールがブートできるかどうか。
impact		ソフトウェアのアップグレード メカニズムのタイプ（中断されるタイプ、または中断されないタイプ）。
install-type	reset	モジュールをリセットする。
	sw-reset	切り替え後すぐにモジュールをリセットする。
	rolling	各モジュールを順番にアップグレードする。
	copy-only	BIOS、ローダー、またはブート ROM のソフトウェアを更新する。

- ツール
  - DCNM-SAN の Software Install Wizard で [Verify Remote Server] をクリックして、リモート サーバへの接続を確認します。
  - Software Install Wizard を使用して空きディスク領域を確認し、イメージ ファイルをコピーするのに必要な領域があることを確認します。

- DCNM-SAN の Software Install Wizard を使用して、ソフトウェアをアップグレードすることを推奨します。このウィザードは、Cisco MDS 9000 ファミリ スイッチのすべてのモジュールをアップグレードします（「Software Install Wizard を使用した場合の利点」（P.10-3）を参照）。
- スイッチでは常に 1 つのインストールだけを実行します。
- インストールの実行中に別のコマンドを発行しないでください。
- スタンバイ スーパーバイザ モジュールではなく、アクティブ スーパーバイザ モジュールでインストールを実行します。

（注）　Cisco SAN-OS Release 3.0 よりも前のリリースでは、設定に FC ID を保存する場合、再起動される前に永続的 FC ID 機能がイネーブルであることを確認してください。この機能は、デフォルトでイネーブルにされています。以前のリリースでは、デフォルトでディセーブルでした。

（注）　Software Install Wizard は、Cisco MDS 9020 ファブリック スイッチまたは Cisco FabricWare のインストールとアップグレードをサポートします。正常なインストールとアップグレードは、Cisco MDS 9020 ファブリック スイッチが使用する TFTP サーバ アドレスを指定します。

（注）　このウィザードを使用する前に、スタンバイ スーパーバイザ管理ポートが接続されていることを確認してください。

デフォルト設定

表 10-6 に、すべての Cisco MDS 9000 ファミリ スイッチのイメージのデフォルト設定を示します。

表 10-6　イメージのデフォルト設定

パラメータ	デフォルト
キックスタート イメージ	イメージが指定されていない。
システム イメージ	イメージが指定されていない。

Software Install Wizard の使用方法

Software Install Wizard を使用して、サポート対象のスイッチに Cisco NX-OS イメージをインストールできます。

手順の詳細

Software Install Wizard を使用する手順は、次のとおりです。

ステップ 1　ツールバーで [Software Install Wizard] アイコンをクリックします。

デフォルトですべてのスイッチが選択された状態で [Select Switches] ダイアログボックスが表示されます。

ステップ 2　イメージをインストールしないスイッチのチェックボックスをオフにします。継続するには、少なくとも 1 つのスイッチを選択する必要があります。

ステップ 3　終了したら、[Next] をクリックします。

ステップ 4　（任意）[Skip Image Download] チェックボックスをオンにして、[Next] をクリックし、ダウンロード済みのイメージを使用します（ダウンロードされたファイルはブートフラッシュ上にあります）。ステップ 11 に進みます。

[Specify Software Image(s) by Model] ダイアログボックスが表示されます。

ステップ 5　[Use Saved Settings] チェックボックスをオンにして、指定した設定を保存します。[Next] をクリックすると、将来の使用に備えてこれらの設定が保存されます。

ステップ 6　次のいずれかのオプション ボタンをクリックします。

a.　ローカル コンピュータからファイルを転送するには、[Local FM TFTP] をクリックします。

b.　リモート コンピュータからファイルを転送するには、[Remote] をクリックします。

ステップ 7　[Local FM TFTP] を選択した場合は、ステップ 10 に進みます。

ステップ 8　[Remote] を選択した場合は、ファイルの転送方法としていずれかの [Copy Files Via] オプション ボタンをクリックします（[SFTP]、[SCP]、[FTP]）。

ステップ 9　サーバ名、ユーザ名、およびパスワードを入力します。

ステップ 10　バージョンとイメージ パスを入力してから、[Apply] をクリックします。

（注）　手順 6 で [Local FM TFTP] を選択した場合は、手動でファイル名を指定できます。これには、テーブルをダブルクリックして、[Open] ダイアログボックスからファイルを選択するか、システムの下のセルにファイル名を手動で入力できます。

バージョン文字列とイメージ パスを入力すると、DCNM-SAN がデフォルト ファイル名を取得し、イメージ ファイルの格納に必要なフラッシュ スペースを計算します。バージョン文字列は、インストールされている現在のバージョンにする必要があります。イメージ パスは、次の例に示すように、ソフトウェア イメージの場所を特定するためのパスです。

```
Image URI: /tftpboot/rel/qa/5_0_0_201/gdb/m9500-sf2ek9-mzg.5.0.0.201.bin.S2
Path - /tftpboot/rel/qa/5_0_0_201/gdb
Version String - 5.0.0.201.S2
```

ステップ 11　[System]、[Kickstart]、または [SSI] の各カラムの行をクリックして、イメージの URI を入力します。処理を進めるには、スイッチごとに少なくとも 1 つのイメージを指定する必要があります。

ステップ 12　[Verify Remote Server and Path] をクリックします。

DCNM-SAN は、ファイル パスとサーバ クレデンシャルを検証します。出力が表示されます。

ステップ 13　[Specify Software Images by Model] ダイアログボックスで [OK] をクリックし、次に [Next] をクリックします。

[Check Flash Free Space] ダイアログボックスが表示されます。このダイアログボックスに、各スイッチのアクティブ（および必要に応じてスタンバイ）ブートフラッシュの領域およびステータス（新規イメージを格納する十分な領域があるかどうか）が表示されます。スイッチに十分な領域がないと、継続できません。最初の画面に戻って、ブートフラッシュ サイズが十分でないスイッチのチェックボックスをオフにして、このスイッチの選択を解除します。

ステップ 14　[Next] をクリックします。

[Start Install] ダイアログボックスが表示されます。

（注）　アップグレードできるスイッチ数に制限はありません。

ステップ 15　次のいずれかのオプション ボタンをクリックします。

a.　スイッチを 1 台ずつアップグレードするには、[Serialized] をクリックします。

b.　複数のスイッチを同時にアップグレードするには、[Parallel] をクリックします。

ステップ 16　（任意）[Version Check Only] チェックボックスをオンにして、バージョン チェックをしてから、インストールを続行するための入力を求めるプロンプトが表示されるようにします。

ステップ 17　（任意）[Finish] をクリックして、インストールを開始します。

[Version Check Results] ダイアログボックスが表示されます。

ステップ 18　**（任意）**[Install without Version check Prompting] チェックボックスをオンにして、インストールを続行します。

（注）　バージョン チェックを実行すると、スイッチのモジュールごとにアップグレードの影響に関する情報が表示されます。また、生じる可能性のある非互換性も表示されます。このステージの最後のダイアログボックスが表示され、ここでこのチェックを実行する必要があるかどうかを確認します。バージョン チェック結果は省略しないことを推奨します。

注意　[Install without Version check Prompting] がオンの場合は、現在のスイッチ バージョンがインストール中のバージョンより新しい場合でも、アップグレードが進行します。

ステップ 19　[OK] をクリックしてウィザードを終了します。

ステップ 20　[Continue to install] をクリックしてインストールを開始します。

[Download and Install Status] ダイアログボックスが表示されます。

（注）　TFTP サーバを開始できないホストの場合は、警告が表示されます。既存の TFTP サーバが稼動しているか、または TFTP ポート 69 へのアクセスがセキュリティ上の理由から拒否されている場合（Linux のデフォルト設定）は、TFTP サーバを開始できないことがあります。このような場合は、ファイルをローカル ホストからスイッチに転送できません。

（注）　セッションを終了する前に、アップグレード プロセスが完了しているか確認してください。ウィザードを進めると、ステータスが随時表示されます。ウィザードの左下にステータス メッセージ [Upgrade Finished] が表示されることを確認します。ウィザードには最初にメッセージ **Success** が表示され、数秒後に InProgress Polling が表示されます。続いて、2 番めのメッセージ **Success** が表示されて、その後 Upgrade Finished が表示されます。

サービス モジュールのアップグレード

ファイバ チャネル スイッチング モジュールは、中断しないアップグレードをサポートしています。14/2 ポート マルチプロトコル サービス（MPS-14/2）モジュールは、ファイバ チャネル ポートの中断しないアップグレードをサポートします。このモジュールの 2 つのギガビット イーサネット ポートにおけるソフトウェア アップグレードは、中断を伴います。

Caching Services Module（CSM）と IP Storage Services（IPS）モジュールのソフトウェア アップグレードは、中断を伴います。

CSM および IPS モジュールは rolling アップグレード インストール メカニズムを使用するので、スイッチの各モジュールの安定した状態を保証します。

- スイッチの各 IPS モジュールは、次の IPS モジュールのアップグレードまで 5 分間の遅延を必要とします。
- 各 CSM モジュールは、次の CSM モジュールのアップグレードまで 30 分間の遅延を必要とします。CSM の詳細については、『*Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*』を参照してください。

ファブリックおよびモジュラ スイッチの中断がないアップグレードの実行

ここでは、次のシスコ ファブリック スイッチで中断がないアップグレードを実行する手順について説明します。

- Cisco MDS 9124 マルチレイヤ ファブリック スイッチ
- Cisco MDS 9134 マルチレイヤ ファブリック スイッチ
- Cisco MDS 9222i マルチサービス モジュラ スイッチ
- HP c-Class BladeSystem 用の Cisco ファブリック スイッチ
- IBM BladeCenter 用のシスコ ファブリック スイッチ

ここでは、次の内容について説明します。

- 「ファブリックおよびモジュラ スイッチの中断のないアップグレードの準備」（P.10-11）
- 「ファブリック スイッチでの中断がないアップグレードの実行」（P.10-12）

ファブリックおよびモジュラ スイッチの中断のないアップグレードの準備

システム ソフトウェア イメージ に対して Software Install Wizard を使用して、次のスイッチで中断なしでソフトウェアをアップグレードできます。

- Cisco MDS 9124 マルチレイヤ ファブリック スイッチ
- Cisco MDS 9134 マルチレイヤ ファブリック スイッチ
- Cisco MDS 9222i マルチサービス モジュラ スイッチ
- HP c-Class BladeSystem 用の Cisco ファブリック スイッチ
- IBM BladeCenter 用のシスコ ファブリック スイッチ

完了すると、スーパーバイザ キックスタート イメージ、スーパーバイザ システム イメージ、ライン カード イメージ、およびシステム BIOS のすべてが更新されます。

これらのファブリック スイッチの中断のないアップグレードは、コントロール プレーンを多くて 80 秒ダウンさせます。アップグレードが正常に停止しないポイントまで進行した場合、または障害が発生した場合などは、ソフトウェア アップグレードが中断する可能性があります。

（注）　アップグレード中、コントロール プレーンはダウン状態ですが、データ プレーンはアップ状態を維持します。そのため新しいデバイスはコントロール プレーンを介してファブリックにログインできませんが、既存のデバイスはデータ プレーンを介した場合に、トラフィックが中断されません。

これらのファブリック スイッチでソフトウェア イメージをアップグレードする前に、次の注意事項に従ってください。

- アップグレード中、ファブリックは安定している必要があります。次の設定アクティビティは、すべて許可されません。
  - ゾーンの変更
  - Telnet セッション
  - スケジュールの変更
  - スイッチのケーブル接続
  - 物理デバイスの追加または取り外し
- FSPF タイマーをデフォルト値（20 秒）に設定します。
- ファブリック内で CFS コミットが保留中であると、アップグレードが中断します。
- ゾーン サーバが進行中にマージすると、アップグレードが中断します。
- Software Install Wizard を使用して新しいイメージをロードするのに十分な領域がシステムにあることを確認します。この時点で、アップグレードを中断するか、中断を伴うアップグレードを継続する必要があります。
- Cisco MDS 18/4 ポート マルチサービス モジュールでは、ハイブリッド スーパーバイザ 18/4 ライン カードの 4 ギガビット イーサネット ポートのアップグレードは中断が伴います。

ファブリック スイッチでの中断がないアップグレードの実行

Software Install Wizard を使用して、Cisco MDS 9124 ファブリック スイッチで中断のないアップグレードを実行できます。Software Install Wizard の使用方法の詳細については、「Software Install Wizard の使用方法」（P.10-8）を参照してください。

注意　ファブリック スイッチの管理インターフェイスが接続される Catalyst スイッチのイーサネット インターフェイス上の Port Fast をイネーブルにすることを推奨します。これは、Catalyst スイッチのスパニングツリーのコンバージェンス時間を防ぎ、中断のないアップグレード中に、ファブリック スイッチからのパケットはただちに転送するためです。

（注）　アップグレード中にイメージを選択する場合、Cisco MDS 9124 スイッチおよび Cisco MDS 9134 マルチレイヤ ファブリック スイッチで ASM-SFN および SSI がサポートされません。

スーパーバイザ モジュールのメンテナンス

ここでは、スーパーバイザ モジュールの効率的な交換方法および使用方法に関する概要を説明します。

ここでは、次の内容について説明します。

- 「スーパーバイザ モジュールの交換」（P.10-13）
- 「スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールへの移行」（P.10-13）
- 「スタンバイ スーパーバイザ モジュールのブート変数バージョンの設定」（P.10-14）
- 「スタンバイ スーパーバイザ モジュールのブートフラッシュ メモリの設定」（P.10-14）
- 「スタンバイ スーパーバイザ モジュールのブート アラート」（P.10-14）

スーパーバイザ モジュールの交換

Cisco MDS 9500 シリーズ ディレクタからスーパーバイザ モジュールを取り外す際のパケット ロスを防ぐには、スーパーバイザ モジュールを取り外す前にスーパーバイザ モジュールをアウトオブサービスにします。

（注）　スーパーバイザ モジュールを取り外して再挿入または交換して、使用可能にする必要があります。

スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールへの移行

Cisco MDS NX-OS Release 4.1(1a) では、アクティブおよびスタンバイの両方のスーパーバイザ 2 モジュールが Cisco MDS 9509 および 9506 ディレクタ上に必要です。MDS NX-OS Release 4.1(1a) 以降にアップグレードする前に、Cisco MDS SAN-OS Release 3.3(1c) 以前を使用して、スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールにアップグレードする必要があります。

スーパーバイザ 1 モジュールとスーパーバイザ 2 モジュールは、移行を目的とした場合を除き、同じスイッチで使用できません。アクティブとスタンバイのスーパーバイザ モジュールは、両方とも同じタイプ（スーパーバイザ 1 モジュールまたはスーパーバイザ 2 モジュール）である必要があります。Cisco MDS 9513 ディレクタの場合、両方のスーパーバイザ モジュールがスーパーバイザ 2 モジュールである必要があります。

注意　スーパーバイザ モジュールの移行は、中断を伴う操作です。スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールへの移行が行われると、コールド スイッチオーバーが実行され、両方のモジュールがリロードされます。スーパーバイザ 1 がスタンバイとして起動を試行するとき、スーパーバイザ 2 がアクティブ スーパーバイザであれば、スタンバイは起動しません。

スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールへの移行についてのステップバイステップの説明については、『*Cisco MDS 9000 Family NX-OS and SAN-OS Software Upgrade and Downgrade Guide*』を参照してください。

（注）　スーパーバイザ 2 モジュールからスーパーバイザ 1 モジュールへの移行はサポートされていません。

スタンバイ スーパーバイザ モジュールのブート変数バージョンの設定

スタンバイ スーパーバイザ モジュールのブート変数イメージが、アクティブ スーパーバイザ モジュールで稼動するイメージと*同一*のバージョンでない場合、ソフトウェアでは、スタンバイ スーパーバイザ モジュールがアクティブ スーパーバイザ モジュールと同一のバージョンを実行するように強制します。

スタンバイ スーパーバイザ モジュールのブート変数を別のバージョンに特別に設定して、スタンバイ スーパーバイザ モジュールを再起動する場合、同一のバージョンがアクティブ スーパーバイザ モジュールで稼動していると、スタンバイ スーパーバイザ モジュールは指定されたブート変数だけをロードします。この時点で、スタンバイ スーパーバイザ モジュールは、ブート変数に設定されたイメージを稼動して*いません*。

スタンバイ スーパーバイザ モジュールのブートフラッシュ メモリの設定

スタンバイ スーパーバイザ モジュールのソフトウェア イメージを更新する場合は、イメージ用に十分な領域があることを確認します。古いバージョンの Cisco MDS NX-OS イメージおよびキックスタート イメージは削除します。

手順の詳細

Device Manager を使用してスタンバイ スーパーバイザの領域を確認する手順は、次のとおりです。

ステップ 1　[Admin] > [Flash Files] をクリックします。

ステップ 2　[Partition] ドロップダウン リストからスタンバイ スーパーバイザを選択します。

[Flash Files] ダイアログボックスの下部に、使用されている領域と空き領域が表示されます。

スタンバイ スーパーバイザ モジュールのブート アラート

スタンバイ スーパーバイザ モジュールが起動に失敗する場合、アクティブ スーパーバイザ モジュールがその状態を検出して Call Home イベントおよびシステム メッセージを生成し、スタンバイ スーパーバイザ モジュールが **loader>** プロンプトに移動した約 3 ～ 6 分後にスタンバイ スーパーバイザ モジュールを再起動します。

次のシステム メッセージが発行されます。

```
%DAEMON-2-SYSTEM_MSG:Standby supervisor failed to boot up.
```

このエラー メッセージは、次の状況のいずれかに該当する場合も生成されます。

- 長期間 loader> プロンプトに留まる場合。
- 適切にブート変数を設定していない場合。

ジェネレーション 1 シャーシへのジェネレーション 2 モジュールの設置

ジェネレーション 2 モジュールには次の設置制限事項があります。

- スーパーバイザ 2 モジュールはすべての Cisco MDS 9500 シリーズ ディレクタに設置できます。

（注）　Cisco MDS 9513 ディレクタはスーパーバイザ 1 モジュールをサポートしていません。

- ジェネレーション 2 スイッチング モジュールは、Cisco MDS 9216 スイッチを除くすべての Cisco MDS 9000 ファミリ スイッチに設置できます。
- ジェネレーション 1 モジュールは Cisco MDS 9000 ファミリ スイッチと一緒に使用できます。ただし、ジェネレーション 1 モジュールをジェネレーション 2 スイッチング モジュールと同じシャーシに設置すると、ジェネレーション 2 スイッチング モジュールの機能が低減します。
- ジェネレーション 1 およびジェネレーション 2 スイッチング モジュールは、スーパーバイザ 1 モジュールまたはスーパーバイザ 2 モジュールのどちらかを搭載した Cisco MDS 9500 ファミリ スイッチに設置できます。

モジュールの交換

モジュール（スーパーバイザ モジュール、スイッチング モジュール、またはサービス モジュール）を交換する場合、新しいモジュールがスイッチの他のモジュールと同一のソフトウェア バージョンを稼動していることを確認する必要があります。

Caching Services Module（CSM）交換の設定手順については、『*Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*』を参照してください。

（注）　スペアのスタンバイ スーパーバイザ モジュールが挿入されている場合、アクティブ スーパーバイザ モジュールと同一のイメージを使用します。Cisco NX-OS ソフトウェア イメージは、スタンバイ フラッシュ デバイスに自動的にコピーされません。

ヒント　Software Install Wizard を使用して、Cisco NX-OS ソフトウェア イメージをスタンバイ スーパーバイザ モジュールのブートフラッシュ デバイスにコピーします。

モジュールを交換したあとに Software Install Wizard を使用することによって、次の動作を確認します。

- 適切なシステムおよびキックスタート イメージがスタンバイ bootflash: ファイル システムにコピーされている。
- 適切なブート変数が設定されている。
- ローダーおよび BIOS がアクティブ スーパーバイザ モジュールで使用されている同一のバージョンにアップグレードされている。

手順の詳細

Cisco MDS 9200 シリーズまたは 9500 シリーズの任意のスイッチでモジュールを交換する手順は、次のとおりです。

ステップ 1　[Admin] > [Copy Configuration] をクリックし、[runningConfig] を [startupConfig] に選択して、必要に応じて既存のコンフィギュレーション ファイルのバックアップを作成します。

ステップ 2　『*Cisco MDS 9200 Series Hardware Installation Guide*』または『*Cisco MDS 9500 Series Hardware Installation Guide*』に指定されているように必要なモジュールを交換します。

ステップ 3　[Admin] > [Flash Files] をクリックし、[sup-standby] を選択して、スタンバイ スーパーバイザ モジュールのブートフラッシュに十分な領域があることを確認します。古いバージョンの Cisco MDS NX-OS イメージおよびキックスタート イメージは削除します。

ステップ 4　Software Install Wizard を使用して、新しいモジュールがスイッチの他のモジュールと同一のソフトウェアを稼動していることを確認します。

ステップ 5　新しいモジュールがオンライン状態になるのを待ってから、Device Manager で [Physical] > [Modules] をクリックして、交換が正常に行われたかどうかを確認します。

CHAPTER 11

管理ソフトウェアの FAQ

この章では、Cisco DCNM-SAN および Device Manager に関する主な FAQ について回答します。この章は、次の内容で構成されています。

- 「インストールの問題」（P.11-3）
  - 「Windows から Cisco DCNM-SAN をインストールするときに、インストールをクリックできません」（P.11-3）
  - 「Solaris で Cisco DCNM-SAN を起動できません」（P.11-3）
  - 「ブラウザ上に JNLP ファイルの保存を促すプロンプトが表示されます」（P.11-4）
  - 「[Java Web Start not detected] エラーが表示されます」（P.11-4）
  - 「Cisco DCNM-SAN または Device Manager を新しいバージョンにアップグレードする方法を教えてください」（P.11-4）
  - 「Cisco DCNM-SAN または Device Manager をダウングレードする方法を教えてください」（P.11-4）
  - 「アップグレードできません」（P.11-5）
  - 「ダウンロード ダイアログで Java Web Start が停止します」（P.11-5）
  - 「Java Web Start を手動で設定する方法を教えてください」（P.11-5）
  - 「Java Web Start をコマンドラインから実行する方法を教えてください」（P.11-6）
  - 「Java Web Start のキャッシュをクリアする方法を教えてください」（P.11-6）
  - 「Cisco DCNM-SAN または Device Manager にログインできません」（P.11-6）
  - 「pcAnyWhere の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません」（P.11-7）
  - 「[Services] メニューで、Cisco DCNM-SAN または Performance Manager サービスが [disabled] と表示されます」（P.11-7）
  - 「McAfee Internet Suite 6.0 Professional の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません」（P.11-7）
- 「全般」（P.11-7）
  - 「面グラフのモニタ中にエラーが表示されます。」（P.11-7）
  - 「[gen error] メッセージが表示されます。」（P.11-7）
  - 「Device Manager Summary View にディスク イメージが表示されません」（P.11-8）
  - 「Device Manager に D_S_TOV および E_D_TOV タイマーを同時に設定できません」（P.11-8）
  - 「Device Manager テーブルのカラムを大きくする方法を教えてください」（P.11-8）

  - 「ファブリックの変更がマップに伝播されません（リンクが消えないなど）」（P.11-8）
  - 「PortChannel の作成ダイアログボックスを何度か使用したら小さくなってしまいました」（P.11-8）
  - 「IPFC を設定するとエラーが表示されます」（P.11-8）
  - 「Cisco DCNM-SAN または Device Manager で正しいネットワーク インターフェイスが使用されません」（P.11-9）
  - 「Cisco DCNM-SAN または Device Manager の画面が正常に表示されません」（P.11-9）
  - 「編集ゾーン内のアクティブ ゾーン セットが（正しくアクティブ化した場合でも）太字で表示されます」（P.11-9）
  - 「プレフィクスが IVRZ のゾーンまたは nozonset という名前のゾーン セットを作成できますか」（P.11-10）
  - 「ワンクリック ライセンス インストールが実行されず、シスコの Web サイトにもアクセスできません」（P.11-10）
  - 「Cisco DCNM-SAN クライアントでログ ウィンドウのサイズを拡大する方法を教えてください」（P.11-10）
  - 「Cisco DCNM-SAN クライアントでログ ウィンドウのサイズを拡大する方法を教えてください」（P.11-10）
  - 「FM Server Database が起動できません。またはファイル ロック エラーが発生します」（P.11-10）
- 「Windows の問題」（P.11-11）
  - 「表示されたテキスト フィールドが小さすぎてデータを入力できません」（P.11-11）
  - 「印刷するとアプリケーションがクラッシュします」（P.11-11）
  - 「Windows XP が停止しました（ブルー画面になりました）」（P.11-11）
  - 「Cisco DCNM-SAN および Device Manager のアイコンが表示されません」（P.11-11）
  - 「Windows XP で Device Manager または Cisco DCNM-SAN ウィンドウの内容が表示されません」（P.11-12）
  - 「ファイルをローカル マシンからスイッチにコピーすると SCP/SFTP にエラーが発生します」（P.11-12）
- 「UNIX の問題」（P.11-12）
  - 「親メニューが表示されません」（P.11-12）
  - 「Web サーバは稼動しているのにブラウザで検出できません」（P.11-12）
  - 「[too many open files] エラーへの対処方法を教えてください」（P.11-12）
- 「その他」（P.11-13）
  - 「Cisco DCNM-SAN の再起動後もマップ レイアウトを保持する方法を教えてください」（P.11-13）
  - 「スイッチは 1 台しかないのにマップには 2 つ表示されます」（P.11-13）
  - 「スイッチ内のレッド/オレンジ/点線の意味を教えてください。」（P.11-14）
  - 「マップ設定を保持したままアップグレードする方法を教えてください」（P.11-19）
  - 「Cisco DCNM-SAN サーバを新規ホストに移行するときに履歴データを保持する方法を教えてください」（P.11-20）
  - 「FCIP 上で Cisco DCNM-SAN を使用するときの制限はありますか」（P.11-20）

– 「[Please insure that FM server is running on localhost] メッセージへの対処法を教えてください」（P.11-20）
– 「複数のインターフェイスを使用して Cisco DCNM-SAN を実行する方法を教えてください」（P.11-21）
– 「HTTP プロキシ サーバの設定方法を教えてください」（P.11-22）
– 「トポロジ マップをクリアする方法を教えてください」（P.11-23）
– 「ソフトウェアの混在環境で Cisco DCNM-SAN を使用する方法を教えてください」（P.11-23）
– 「Cisco DCNM-SAN 起動時に「corrupted jar file」エラーが表示されます。対処方法を教えてください」（P.11-23）
– 「ファブリック内のデバイスの検索方法を教えてください」（P.11-24）
– 「複数のファブリックの管理方法を教えてください」（P.11-25）
– 「ライセンス期限が切れるとスイッチに表示されるオレンジの X をクリアする方法を教えてください」（P.11-25）

インストールの問題

Windows から Cisco DCNM-SAN をインストールするときに、インストールをクリックできません

Java Web Start が正しくインストールされていることを確認してください。確認する手順は、次のとおりです。

ステップ 1　[Programs] メニューを開き、Java Web Start が表示されているかどうかを確認します。

ステップ 2　**Java Web Start** プログラムを起動して、Java Runtime のインストールに問題がないか確認します。

ステップ 3　[Preferences] タブをクリックし、Web Start のプロキシ設定が適切かどうかを確認します。

ステップ 4　JNLP 設定を適切に処理するようにブラウザが設定されているか確認します（「Java Web Start を手動で設定する方法を教えてください」（P.11-5）を参照）。

旧バージョンのアプリケーションを実行し、（エラーの詳細に）JNLP ファイルを開くことができないことを示すエラー ポップアップ ウィンドウが表示された場合、Java Web Start のキャッシュが破損している可能性があります。この問題を解決するには、キャッシュをクリアして、再試行してください。キャッシュをクリアする手順については、「Java Web Start のキャッシュをクリアする方法を教えてください」（P.11-6）を参照してください。

Solaris で Cisco DCNM-SAN を起動できません

Solaris 2.8 を使用し、ルートとしてログインしているユーザが、Netscape Navigator 6 を使用している場合は、MIME タイプを登録できません。正規ユーザが Netscape Navigator 6 に MIME タイプを登録するには、手動で追加する必要があります。Netscape 4.x は、すべてのユーザに対して適切に機能します。

ブラウザ上に JNLP ファイルの保存を促すプロンプトが表示されます

JNLP MIME タイプに対応した Java Web Start を起動するようにブラウザが設定されていない可能性があります。Java Web Start が適切にインストールされていないか、適切に設定されていません（「Java Web Start を手動で設定する方法を教えてください」（P.11-5）を参照）。

[Java Web Start not detected] エラーが表示されます

Java Web Start をインストールしたにもかかわらず、スイッチのホーム ページに「Java Web Start not detected...」というエラー メッセージが（赤色で）表示される場合は、単純な JavaScript エラーの可能性があります。Java Web Start インストールを検出するために、Internet Explorer および Mozilla（新しいバージョン）でテストされた JavaScript コードが実行されています。一部のブラウザ（Netscape 6.0 や Opera など）では、リンクが機能していても、このコードが正しく機能しないことがあります。

- まず、インストール リンクをクリックしてください。
- リンクが機能しない場合は、ブラウザのヘルパー アプリケーションが正しく設定されているかどうかを確認してください（Netscape 6.0 の場合は [Edit] > [Preferences] > [Navigator] > [Helper Applications] をクリックします）。「Java Web Start を手動で設定する方法を教えてください」（P.11-5）を参照してください。

Cisco DCNM-SAN または Device Manager を新しいバージョンにアップグレードする方法を教えてください

Cisco DCNM-SAN または Device Manager を新しいバージョンにアップグレードする手順は、次のとおりです。

ステップ 1　実行中のすべての Cisco DCNM-SAN または Device Manager のインスタンスを終了します。

ステップ 2　新規バージョンが稼動しているスイッチをブラウザで指定して、該当するインストール リンクをクリックします。このスイッチで新規バージョンが稼動している場合は、Cisco DCNM-SAN または Device Manager よりアップグレードを求めるプロンプトが表示されます。

インストーラがローカル コピーを調べて、新しいソフトウェア バージョンに更新します。

Cisco DCNM-SAN または Device Manager をダウングレードする方法を教えてください

Cisco MDS NX-OS Release 4.xCisco MDS 以降、インストーラでは、ダウングレードをサポートしません。Cisco DCNM-SAN または Device Manager を旧リリースにダウングレードするには、手動でアンインストールしてから、前のバージョンの Cisco DCNM-SAN または Device Manager をインストールする必要があります。

アップグレードできません

Cisco DCNM-SAN または Device Manager で、スイッチのバージョンの方が高いことを示すプロンプトが表示されたために、アップグレードを試みて失敗した場合は、デフォルト ブラウザ設定が正しくない可能性があります。最後のブラウザのアップグレードまたはインストール中に、何らかのエラーが発生しています。対処するには、ブラウザを単独で起動して、インストールをクリックします。

まれに、アップグレードしてもバージョンが変化しないことがあります。これは、HTTP がネットワークにキャッシュされているためです。アップグレード中に、スイッチのファイルに対する HTTP 要求がローカル マシンにキャッシュされます。スイッチのバージョンの方が高い場合でも、インストールされた管理ソフトウェアは古いバージョンのままです。対処するには、Fabric/Device Manager をアンインストールして、Java Web Start キャッシュをクリアしてから、新規にインストールします。

ダウンロード ダイアログで Java Web Start が停止します

ブラウザの設定と同様に Java Web Start がスイッチにアクセスするように設定されているかどうかを確認する手順は、次のとおりです。

ステップ 1　Java Web Start を起動します（**javaws.exe** または **javaws**）。Java Web Start Application Manager が表示されます。

ステップ 2　[File] > [Preferences] > [General] を選択し、プロキシが正しく設定されていることを確認します。たとえば、HTTP プロキシを使用している場合、ここで設定します。

ステップ 3　[Use Browser] を選択します。

ステップ 4　[OK] をクリックします。

Java Web Start を手動で設定する方法を教えてください

Opera、特定のバージョンの Mozilla、または Konqueror などのブラウザでは、JNLP ファイルのヘルパー アプリケーションとして Java Web Start を手動で登録する必要があります。このために必要なデータは、次のとおりです。

- 記述 = Java Web Start
- ファイル拡張子 = jnlp
- MIME タイプ = application/x-java-jnlp-file
- アプリケーション = javaws のパス（/usr/local/javaws/javaws など）

この設定の完了後、ブラウザを再起動する必要があります。[Java Web Start not detected] という警告が表示されても、無視してかまいません。これらの警告は JavaScript に基づいています。すべてのブラウザが JavaScript と適切に連携するわけではありません。インストール リンクをクリックして、Cisco DCNM-SAN または Device Manager をインストールしてください。

（注）　Windows ユーザの場合、*.jnlp ファイルに Java Web Start を設定するには、[Windows Explorer] > [Tools] > [Folder Options] > [File Types] を選択します。javaws.exe によって *.jnlp ファイルが開かれるように、JNLP の既存設定を変更するか、または設定を追加します。この実行ファイルは Program Files\Java Web Start 内にあります。

Java Web Start をコマンドラインから実行する方法を教えてください

ブラウザから Java Web Start を実行できない場合でも、コマンド ラインから Java Web Start（javaws.exe または javaws）を実行できます。そのためには、スイッチ上の Cisco DCNM-SAN または Device Manager の URL を引数として指定します。たとえば、スイッチの IP アドレスが 10.0.0.1 である場合は、次のコマンドを使用して、Cisco DCNM-SAN および Device Manager を起動します。

```
javaws http://10.0.0.1/cgi-bin/fabric-manager.jnlp
javaws http://10.0.0.1/cgi-bin/element-manager.jnlp
```

Java Web Start のキャッシュをクリアする方法を教えてください

Java Web Start のキャッシュをクリアする手順は、次のとおりです。

ステップ 1　Java Web Start Application Manager（**javaws.exe** または **javaws**）を起動します。

ステップ 2　[File] > [Preferences] > [Advanced] を選択し、アプリケーション フォルダまたはキャッシュをクリアします。.javaws またはキャッシュ ディレクトリは手動で削除できます。Windows の場合、このディレクトリは [Documents and Settings] 内にあります。UNIX の場合は、$HOME 内にあります。

Cisco DCNM-SAN のアップグレード中、ショートカットを作成するプロンプトが表示されません

この章の「*Java Web Start のキャッシュをクリアする方法を教えてください*」の手順に従って Java Web Start のキャッシュをクリアします。

Cisco DCNM-SAN または Device Manager にログインできません

スイッチ上で初期設定ルーチンが実行されているかどうかを確認します。

簡単に確認する手順は、次のとおりです。

- スイッチの管理インターフェイスが起動しているかどうかを確認します（**show interface mgmt0**）。
- 管理インターフェイスに接続できるかどうかを調べます（**ping**）。
- ユーザ名が有効かどうかを確認します（**show snmp user**）。CLI（コマンドライン インターフェイス）からユーザを追加/編集することもできます。
- ネットワーク インターフェイスが複数存在する場合は、「Cisco DCNM-SAN または Device Manager で正しいネットワーク インターフェイスが使用されません」（P.11-9）を参照してください。

pcAnyWhere の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません

pcAnyWhere サービスを停止して Cisco DCNM-SAN または Device Manager をインストールするか、または DirectX をインストール/更新してください。詳細については、www.oracle.com の Web サイトを参照してください。

[Services] メニューで、Cisco DCNM-SAN または Performance Manager サービスが [disabled] と表示されます

この状況は、次の場合に発生することがあります。

- アンインストール/アップグレード中に、Cisco DCNM-SAN または Performance Manager の [Services] メニューが開いていた場合。
- アンインストール/アップグレード中に、Cisco DCNM-SAN クライアントまたは Device Manager を実行していた場合。

このエラーは、Windows がサービスを完全に削除できない場合に発生します。ホストを再起動すると、問題が解決されます。

McAfee Internet Suite 6.0 Professional の実行中に Cisco DCNM-SAN または Device Manager をインストールできません。または Java を実行できません

McAfee Internet Suite にはウィルス スキャナ、ファイアウォール、アンチスパム、およびプライバシー管理機能が搭載されています。プライバシー管理は、Cisco DCNM-SAN のサーバとクライアントの対話に干渉する可能性があります。対処するには、プライバシー サービスを停止する必要があります。

全般

面グラフのモニタ中にエラーが表示されます。

モニタ ウィンドウから面グラフを表示する場合、最初のデータが戻される前に面グラフ上でマウスを移動すると、JChart getX() からのメッセージログに、java.lang.ArrayIndexOutOfBoundsException エラーが表示されます。これは、JChart がまだ存在しない値の検索を試みたことが原因です。この問題は、今後の JChart バージョンで修正される予定です。

[gen error] メッセージが表示されます。

通常、[gen error] は、SNMP（簡易ネットワーク管理プロトコル）要求の処理プロセスで、スイッチの SNMP エージェントに予期せぬエラーが発生したことを意味します。ただし、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）接続または任意の種類の Network Address Translation（NAT; ネットワーク アドレス変換）方式を介してスイッチにアクセスしている場合は、すべてのエ

ラーが [gen error] として報告されます。これは既知の問題であり、今後のリリースで修正される予定です。これが [gen error] の原因であるかどうかを調べるには、NAT が設定されていない環境でこのエラーを再生成します（スイッチと同じネットワークで作業します）。

Device Manager Summary View にディスク イメージが表示されません

Device Manager の Summary View テーブルに、Fx ポートに接続されたディスクのアイコンが表示されないことがあります。これは、このポートに FC4 機能が設定されていないためです。LUN 検出を発行して、FC4 タイプが登録されていないホスト/ディスクに関する情報を検出する必要があります。Device Manager で、[FC] > [Advanced] > [LUNs] をクリックしてください。

Device Manager に D_S_TOV および E_D_TOV タイマーを同時に設定できません

E_D_TOV と D_S_TOV を両方同時に変更した場合、新しい D_S_TOV 値が古い E_D_TOV 値よりも大きいと、WrongValue エラーが表示されます。対処するには、これらの値を個別に変更する必要があります。

Device Manager テーブルのカラムを大きくする方法を教えてください

Device Manager が大型テーブルの表示を試みたとき、スイッチの実行が遅いと、テーブルが表示されたときにタブが非表示になります。対処するには、データが表示されるようにウィンドウのサイズを変更する必要があります。

ファブリックの変更がマップに伝播されません（リンクが消えないなど）

Cisco DCNM-SAN では、ダウンしているデバイスまたはポート上にレッドの十字が表示されます。ただし、Cisco DCNM-SAN はすでに検出されている情報を削除しません。マップを正しく更新するには、再検出する必要があります。

PortChannel の作成ダイアログボックスを何度か使用したら小さくなってしまいました

MemberList TextBox（PortChannel の [Create] ウィンドウ内）を何度か使用すると、正しく表示されなくなります。ポート選択用のコンボ ボックスが付いた長いテキスト ボックスが、小さな正方形のテキスト ボックスに変わり、小さすぎてポートを選択できなくなります。これは既知の問題であり、今後のリリースで修正される予定です。この問題に対処するには、Cisco DCNM-SAN または Device Manager を停止して再起動します。

IPFC を設定するとエラーが表示されます

IPFC および帯域外管理が設定されていると、IPFC アドレスを使用した場合に、Device Manager と SNMPv3 が正しく動作しなくなることがあります。対処するには、管理インターフェイス（mgmt0）アドレスを使用するか、または IPFC 上で SNMPv1/v2c を使用します。

Cisco DCNM-SAN または Device Manager で正しいネットワーク インターフェイスが使用されません

この問題の原因は、ローカル インターフェイスが基本的な Java ライブラリによって任意に選択されることです。対処するには、コマンドライン引数を指定してから、Fabric/Device Manager を起動します。デスクトップ ショートカットまたはシェル スクリプト、あるいはバッチ ファイルにパラメータ「-Device Managerds.nmsAddress=」を追加します。

たとえば、Windows では、「.javaw.exe -Device Managerds.nmsAddress=X.X.X.X -cp .」という行になります。

デスクトップ ショートカットでは、この長さが許容されている最大文字数を超える可能性があります。その場合は、-Dsun.java2d.ddoffscreen=false の部分を削除して、必要な文字数を確保します。リリース 1.2 以降では、優先するネットワーク インターフェイスを選択できます。

Cisco DCNM-SAN または Device Manager の画面が正常に表示されません

Cisco DCNM-SAN または Device Manager のサブメニューがメニューから切り離されて表示されたり、Cisco DCNM-SAN マップでマウスの動きに対するマウス ポインタの反応が遅くなったり、誤ったツールチップが表示されたりする場合、これらは、Cisco DCNM-SAN または Device Manager の問題ではなく、画面の異常です。

一部の古いビデオ カードでは、こうした画面の異常が発生する場合があります。この問題を解決するには、まずビデオ ドライバを更新します。それでも問題が解決しない場合は、ビデオ カードを交換します。

[Physical Attributes] カテゴリがほとんど表示されなくなりました

拡張機能がオフになっています。Cisco DCNM-SAN 画面の右上にある [Advanced Features] チェック ボックスを確認してください。チェック ボックスをオンにします。

[Information] ペインが表示されません

通常、[Information] ペインは Cisco DCNM-SAN のマップの上半分に表示されます。マップが重なっている可能性があります。マップ ウィンドウの端を下方向にドラッグするか、黒の三角をクリックして画面を再表示します。

編集ゾーン内のアクティブ ゾーン セットが（正しくアクティブ化した場合でも）太字で表示されます

VSAN のメンバーが IVR ゾーニングに参加しています。アクティブ ゾーンに IVR ゾーンが追加されたため、アクティブ ゾーン セットの設定が同名のローカル ゾーン セットの設定と異なります。この場合、ゾーン セット名が常に太字になります。

プレフィクスが IVRZ のゾーンまたは nozonset という名前のゾーン セットを作成できますか

これらの特殊な名前は使用しないでください。これらの名前は、IVR ゾーンを識別するためにシステムで使用されます。

ワンクリック ライセンス インストールが実行されず、シスコの Web サイトにもアクセスできません

ワンクリック ライセンス インストールでは、シスコ Web サイトへの HTTP 接続を開こうとします。ブラウザで HTTP プロキシを使用している場合には、Cisco DCNM-SAN クライアントのスクリプトに次のコマンドライン変数を追加する必要があります。

```
-Dhttps.proxyHost and -Dhttps.proxyPort.
```

ワンクリック インストールの URL が「https://」ではなく「http://」から開始する場合、変数は次のようになります。

```
-Dhttp.proxyHost and -Dhttp.proxyPort.
```

たとえば、Windows の場合、MDS 9000\bin\FabricManager.bat ファイルを編集し、JVMARGS に「-Dhttps.proxyHost=HOSTADDRESS -Dhttps.proxyPort=HOSTPORT」を追加します。

Cisco DCNM-SAN クライアントでログ ウィンドウのサイズを拡大する方法を教えてください

FM Client によるメモリ消費を制限するために、ログ ウィンドウはデフォルトで 500 行に制限されています。このサイズを拡大するには、*<install directory>*/db/*<user>* ディレクトリの sm.properties を編集し、LogBufferSize を変更します。

FM Server Database が起動できません。またはファイル ロック エラーが発生します

データベース ログ（FMPersist.log）に [The database is already in use by another process] というエラーメッセージが表示されます。HsqlDB 1.7.1 バージョンにこの問題があります。ファイル ロックはたまに発生しますが、db サーバをシャットダウンして再起動すると解決できます。Windows の場合は FMPersist サービスを停止して起動します。Unix の場合は FMPersist.sh スクリプトの引数を restart にして実行します。

Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバを再同期化する方法を教えてください

Cisco DCNM-SAN クライアントが Cisco DCNM-SAN サーバと同期していない場合、クライアントとサーバの再同期化が必要になる場合があります。Fabric Manager Client を Cisco DCNM-SAN サーバと再同期化するには、[File] メニューで [Resync All Open Fabrics] をクリックします。

現在のファブリックを再検出する方法を教えてください

Cisco DCNM-SAN サーバがファブリックのスイッチと非同期の場合、オンデマンド検出を実行してファブリックのスイッチの変更を Cisco DCNM-SAN クライアントで最新の状態にする必要があります。ファブリック スイッチを再検出するには、[File] メニューから [Rediscover] をクリックします。

SCSI ターゲットを再検出する方法を教えてください

Cisco DCNM-SAN サーバがファブリックの SCSI ターゲット スイッチと非同期の場合、オンデマンド検出を実行してファブリックの SCSI ターゲット スイッチの変更を Cisco DCNM-SAN クライアントで最新の状態にする必要があります。ファブリック スイッチを再検出するには、[File] メニューから [Rediscover SCSI Targets] をクリックします。

Windows の問題

表示されたテキスト フィールドが小さすぎてデータを入力できません

Reflection X を実行している場合、Cisco DCNM-SAN および Device Manager の特定のテキスト フィールドが完全な幅で表示されません。フィールドを適切に表示できるように、ダイアログボックスのサイズを変更してください。

印刷するとアプリケーションがクラッシュします

Windows NT には、既知の Sun JVM バグがあります（印刷サービスを実行すると VM がクラッシュします）。Sun が提案するソリューションは、NT を SP 6 に更新することです。詳細については、次の URL を参照してください。
http://developer.java.sun.com/developer/bugParade/bugs/4530428.html

Windows XP が停止しました（ブルー画面になりました）

Windows XP と ATI Radeon AGP グラフィック カードを併用している場合、Java アプリケーションを終了すると、フリーズ（停止）します。ATI の新しいドライバを使用すると、この問題が解決されるようです。その他の対応策は、「-Dsun.java2d.noddraw=true」を指定してアプリケーションを実行することです。ショートカットおよびシェル スクリプトの作成時に、現在この方法が使用されています。詳細については、次の URL を参照してください。
http://developer.java.sun.com/developer/bugParade/bugs/4713003.html

Cisco DCNM-SAN および Device Manager のアイコンが表示されません

Windows のバージョンによっては、特定のイメージが表示されません。これは Java のバグです。対応策（DirectDraw アクセラレーションのディセーブル化）を講じていますが、それでもこの問題が発生する場合があります。詳細については、次の URL を参照してください。
http://developer.java.sun.com/developer/bugParade/bugs/4664818.html

Windows XP で Device Manager または Cisco DCNM-SAN ウィンドウの内容が表示されません

Windows XP で Device Manager または Cisco DCNM-SAN のメイン ウィンドウの内容が表示されないのは、Java のバグが原因です。次の Web サイトを参照してください。
http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4919780

ウィンドウの内容を復元するには、ウィンドウを最小化または最大化してから標準サイズに戻します。<*FM-install-dir*>/bin/FabricManager.bat および DeviceManager.bat の JVMARGS に「-Dsun.java2d.noddraw=true」を追加し、Direct Draw をディセーブルにしても、この問題を防ぐことができます。

ファイルをローカル マシンからスイッチにコピーすると SCP/SFTP にエラーが発生します

ファイル パスにスペースが含まれていると、Windows の SCP/SFTP にエラーが発生します。スイッチから copyDeviceBusy エラーが返されます。License Wizard などのツールでは、tftp コピーが実行可能であることを確認するか、またはスペースを含まないファイル名を選択します。

UNIX の問題

親メニューが表示されません

サブメニューを表示すると、親メニューが表示されなくなることがあります。このバグの詳細については、次の URL を参照してください。
http://developer.java.sun.com/developer/bugParade/bugs/4470374.html

Web サーバは稼動しているのにブラウザで検出できません

ブラウザでプロキシ サーバを使用しているときに発生します。ブラウザでプロキシ サーバを使用しているかどうかを確認するには、Internet Explorer の場合は、メニューから [Tools] を選択し、[Internet Options]、[Connection] サブパネルの順に指定して [Lan Setting] をクリックします。ダイアログボックスが表示されます。プロキシの設定を確認します。

[too many open files] エラーへの対処方法を教えてください

Linux で Java Virtual Machine（JVM）が稼動していて、Java がインストールされたドライブまたはホーム ディレクトリが NFS マウントの場合、ファイル ロックの取得エラーに関する Sun JDK の既知のバグがあります。Cisco DCNM-SAN の症状として、Device Manager の起動またはファイルの保存/オープンに失敗し、「too many open files」という I/O またはソケット例外が表示されます。JVM は常に NFS マウント ドライブ上のファイルを開こうとして、失敗し、1024 のファイル記述子制限に達するまで試行し続けます。対応策は次のとおりです（/tmp はローカル ディスクです。実際の tmp 領域と置き換えてください）。

- システム設定

ローカル ディスクに、システム レベル設定が格納されていることを確認します。システム設定は $JAVA_HOME/.systemPrefs に格納されています（JAVA_HOME は JDK のインストール先）。このディレクトリが NFS マウントである場合は、次のコマンドを実行します。

```
$ rm -rf $JAVA_HOME/.systemPrefs<
$ mkdir /tmp/.systemPrefs
$ ln -s /tmp/.systemPrefs $JAVA_HOME/.systemPrefs
```

この対応策の問題点は、$JAVA_HOME を使用しているボックスごとに、/tmp/.systemPrefs が存在することを確認する必要がある点です。JVM をルートとして、ローカル ディスクにインストールすることを推奨します。

- ユーザ設定

  ホーム ディレクトリが NFS マウントの場合に、この問題が発生するときは、次の手順に従います。

```
$ rm -rf $HOME/.java
$ mkdir /tmp/.java.$USER
$ ln -s /tmp/.java.$USER $HOME/.java
```

詳細については、次の URL を参照してください。
http://developer.java.sun.com/developer/bugParade/bugs/4673298.html
http://developer.java.sun.com/developer/bugParade/bugs/4635353.html

その他

Cisco DCNM-SAN の再起動後もマップ レイアウトを保持する方法を教えてください

好みに合わせてマップを編成したあとにマップを「固定」して、Cisco DCNM-SAN を停止して再起動したあとにもオブジェクトが引き続き表示されるように設定する場合は、次の手順を実行します。

ステップ 1　マップ内のブランク領域で右クリックします。メニューが表示されます。

ステップ 2　メニューで [Layout] > [Fix All Nodes] を選択します。

スイッチは 1 台しかないのにマップには 2 つ表示されます

スイッチが 1 台しかない場合に、マップにスイッチが 2 つ表示されるときは、隣接していない VSAN（仮想 SAN）内の 2 つのスイッチに同じドメイン ID が設定されている可能性があります。Cisco DCNM-SAN は <vsanId><domainId> を使用してスイッチを検索するため、ファブリック検出時に、これらのスイッチ間にリンクが正しく割り当てられないことがあります。

この問題を回避するには、物理的に接続されたファブリック内の同じ VSAN 内のすべてのスイッチで、一意のドメイン ID が使用されているか確認します。（この作業には、ファブリック コンフィギュレーション チェッカを使用します）。

スイッチ内のレッド/オレンジ/点線の意味を教えてください。

スイッチ内にレッドの線が表示される場合、Fabric Manger はスイッチに関して問題点を検出しています。[Physical Attributes] ペインで [Switches] を選択して、[Information] ペインのステータス レポートを表示します。モジュール、ファン、電源装置に障害があるか、または装着されているにもかかわらずオフライン状態です。

スイッチ内にオレンジの点線が表示される場合は、スイッチに関するマイナー ステータス警告を示しています。通常、モジュールのいずれかに問題が発生しています。問題の原因はツールチップに表示されます。マウスをしばらくスイッチ上に置くと、ツールチップが表示されます。

次の表に、Cisco DCNM-SAN および Device Manager のカラーの設定とツールチップの定義を示します。

表 11-1　Cisco DCNM-SAN クライアントと Device Manager のカラーの定義

Cisco DCNM-SAN のカラー	定義
レッドのスラッシュ	SNMP を通してスイッチと通信できません。
レッドの X	ファブリック スイッチの Domain Manager/Fabric Configuration Server リスト内のスイッチと通信したり、このスイッチを表示することができません。
Device Manager のカラー	**定義**
モード（FICON の場合は F、T、TE、U/I など）の付いたグリーンの正方形	ポートが起動しています。
モードの付いたオレンジの正方形	トランクが不完全です。
オレンジの十字	OLS および NOS が受信されています。
ブラウンの正方形	ポートは管理上のダウン状態です。
ライト グレーの正方形	ポートを管理できません。
レッドの十字	ハードウェア障害/ループバック診断障害/リンク障害です。
レッドの正方形	その他の設定障害です。
正方形なし、またはブラックの正方形	ポートが未設定です。

表 11-2　Device Manager ツールチップの定義

ツールチップ	定義
adminDown	ポートが管理上のダウン状態です。
bitErrRTThresExceeded	ビット エラー レートが高すぎます。
bundleMisCfg	PortChannel メンバーシップで設定エラーが検出されました。
channelAdminDown	このポートは PortChannel のメンバーであり、この PortChannel が管理上のダウン状態です。
channelConfigurationInProgress	このポートは PortChannel の設定中です。
channelOperSuspended	このポートは PortChannel のメンバーであり、動作パラメータは PortChannel パラメータと互換性がありません。

表 11-2　Device Manager ツールチップの定義 （続き）

ツールチップ	定義
deniedDueToPortBinding	ポート バインディングにより中断中です。
domainAddrAssignFailureIsolation	選択された主要スイッチがドメイン アドレス マネージャ機能を実行できないため、Nx_port のトラフィックをスイッチ間で転送できません。したがって、スイッチ内のすべての Interconnect_Ports が隔離されます。
domainInvalidRCFReceived	無効な Reconfigure Fabric（RCF）が受信されました。
domainManagerDisabled	ドメイン マネージャがディセーブルです。
domainMaxReTxFailure	再試行を最大限に行っても、ドメイン マネージャに障害が発生します。
domainOtherSideEportIsolation	ピア E ポートが隔離されています。
domainOverlapIsolation	2 つの既存ファブリックを接続する際に、ドメインが重複しています。
elpFailureClassFParamErr	クラス F パラメータ エラーによる ELP 障害のために隔離されています。
elpFailureClassNParamErr	クラス N パラメータ エラーによる ELP 障害のために隔離されています。
elpFailureInvalidFlowCTLParam	無効なフロー制御パラメータによる ELP 障害のために隔離されています。
elpFailureInvalidPayloadSize	無効なペイロード サイズによる ELP 障害のために隔離されています。
elpFailureInvalidPortName	無効なポート名による ELP 障害のために隔離されています。
elpFailureInvalidSwitchName	無効なスイッチ名による ELP 障害のために隔離されています。
elpFailureInvalidTxBBCredit	無効な B2B クレジットの伝送による ELP 障害のために隔離されています。
elpFailureIsolation	ポート初期化中に、想定される Interconnect_Ports に互換性のないリンク パラメータが見つかりました。
elpFailureLoopbackDetected	検出されたループバックによる ELP 障害のために隔離されています。
elpFailureRatovEdtovMismatch	R_A_TOV または E_D_TOV の不一致による ELP 障害のために隔離されています。
elpFailureRevMismatch	リビジョンの不一致による ELP 障害のために隔離されています。
elpFailureUnknownFlowCTLCode	無効なフロー制御コードによる ELP 障害のために隔離されています。
ePortProhibited	E/TE ポートに FICON 禁止マスクが設定されているために、ポートがダウンしています。
eppFailure	再試行を最大限に行っても、トランク ネゴシエーション プロトコルに障害が発生します。

表 11-2　Device Manager ツールチップの定義 （続き）

ツールチップ	定義
errorDisabled	管理上の対応が必要なエラー条件により、ポートが動作していません。
escFailureIsolation	Exchange Switch Capabilities（ESC）の結果、ポート初期化中に、想定される Interconnect_Ports が初期化を継続できません。
fabricBindingDBMismatch	ファブリック バインディング アクティブ データベースがピアと一致しません。
fabricBindingDomainInvalid	ファブリック バインディング アクティブ データベース内のピア ドメイン ID が無効です。
fabricBindingNoRspFromPeer	ファブリック バインディングがピアからの応答を受信しません。
fabricBindingSWWNNotFound	ファブリック バインディング アクティブ データベース内に、ピアのスイッチ WWN が見つかりません。
fcipPortAdminCfgChange	設定変更により、FCIP ポートがダウンしました。
fcipPortKeepAliveTimerExpire	TCP キープアライブ タイマーの期限切れにより、FCIP ポートがダウンしました。
fcipPortMaxReTx	TCP 再送信回数が設定された制限値に到達したため、FCIP ポートがダウンしました。
fcipPortPersistTimerExpire	TCP 持続タイマーの期限切れにより、FCIP ポートがダウンしました。
fcipPortSrcAdminDown	発信元イーサネット リンクが管理上のシャットダウンになったために、FCIP ポートがダウンしました。
fcipPortSrcLinkDown	イーサネット リンクのダウンにより、FCIP ポートがダウンしました。
fcipSrcModuleNotOnline	発信元モジュールがオンラインでないため、FCIP ポートがダウンしました。
fcipSrcPortRemoved	送信元ポートが削除されたため、FCIP ポートがダウンしました。
fcotChksumErr	FSP SPROM チェックサム エラーが発生しました。
fcotNotPresent	SFP（GBIC）が搭載されていません。
fcotVendorNotSupported	FSP（GBIC）ベンダーがサポートされていません。
fcspAuthenfailure	ファイバ チャネル セキュリティ プロトコル認証に失敗しました。
ficonBeingEnabled	FICON がイネーブル化中です。
ficonNoPortnumber	FICON ポート番号が設定されていません。
ficonNotEnabled	FICON がイネーブル化されていません。
ficonVsanDown	FICON VSAN がダウンしています。

表 11-2　Device Manager ツールチップの定義 （続き）

ツールチップ	定義
firstPortNotUp	加入過多型ライン カードで、グループ内の他のポートが起動している場合に、先頭ポートを E モードで起動することができません。
firstPortUpAsEport	加入過多型ライン カードで、グループ内の先頭ポートが E モードで起動している場合に、このグループ内の他のポートを起動できません。
hwFailure	ハードウェア障害です。
incomAdminRxBBCreditPerBuf	管理ポート rxbbcredit、パフォーマンス バッファに互換性がないために、ディセーブルです。
incompatibleAdminMode	ポート管理モードとポート機能に互換性がありません。
incompatibleAdminRxBBCredit	受信 BB クレジットに互換性がありません。
incompatibleAdminRxBufferSize	受信バッファ サイズに互換性がありません。
incompatibleadminSpeed	ポート速度とポート機能に互換性がありません。
initializing	ポートが初期化中です。
interfaceRemoved	インターフェイスの削除中です。
invalidAttachment	接続が無効です。
invalidConfig	このポートのポート チャネル設定ミスです。
invalidFabricBindExh	ファブリック バインディング交換が無効です。
linkFailCreditLoss	過剰なクレジット損失が示されたため、リンクに障害が発生しました。
linkFailCreditLossB2B	キューが空でないため、Link Reset（LR）動作に失敗したときに、リンク障害が発生しました。
linkFailDebounceTimeout	再ネゴシエーションに失敗したために、リンク障害が発生しました。
linkFailLineCardPortShutdown	ポートがシャットダウンしたために、リンク障害が発生しました。
linkFailLinkReset	リンクがリセットされたために、リンク障害が発生しました。
linkFailLIPF8Rcvd	F8 LIP が受信されたために、リンク障害が発生しました。
linkFailLIPRcvdB2B	受信キューが空でないため、Loop Initialization（LIP）動作に失敗したときに、リンク障害が発生しました。
linkFailLossOfSignal	Loss of Signal（LOS; 信号消失）により、リンク障害が発生しました。
linkFailLossOfSync	同期ずれにより、リンク障害が発生しました。
linkFailLRRcvdB2B	受信キューが空でないため、LR 動作に失敗したときに、リンク障害が発生しました。
linkFailNOSRcvd	動作しないシーケンスが受信されたため、リンクに障害が発生しました。

表 11-2　Device Manager ツールチップの定義 （続き）

ツールチップ	定義
linkFailOLSRcvd	オフライン シーケンスが受信されたために、リンク障害が発生しました。
linkFailOPNyRETB2B	受信キューが空でない場合に、オープンな基本信号が戻されたため、リンク障害が発生しました。
linkFailOPNyTMOB2B	受信キューが空でない場合に、オープンな基本信号がタイムアウトになったため、リンク障害が発生しました。
linkFailPortInitFail	ポートの初期化に失敗したために、リンク障害が発生しました。
linkFailPortUnusable	ポートが使用不能なために、リンク障害が発生しました。
linkFailRxQOverFlow	受信キューのオーバーフローにより、リンク障害が発生しました。
linkFailTooManyINTR	ポート中断が過度に発生したために、リンク障害が発生しました。
linkFailure	物理的なリンク障害が発生しました。
loopbackDiagFailure	ループバック診断障害が発生しました。
loopbackIsolation	ポートが同じスイッチ内の別のポートに接続されています。
noCommonVsanIsolation	ピアに対して共通の VSAN が存在しないため、トランクが隔離されています。
none	障害は発生していません。
nonParticipating	ループ初期化中に、ポートがループ動作に参加できません。
offline	物理リンクがオフライン ステート（FC-FS 標準で定義済み）です。
ohmsExtLBTest	外部ループバック診断障害により、リンクが中断しました。
other	原因が定義されていません。
parentDown	このインターフェイスがバインドされている物理ポートがダウンしています。
peerFCIPPortClosedConnection	ピア FCIP ポートによって TCP 接続が閉じられたため、ポートがダウンしました。
peerFCIPPortResetConnection	ピア FCIP ポートによって TCP 接続がリセットされたため、ポートがダウンしました。
portBindFailure	ポート バインド障害が発生したために、ポートが隔離されました。
portBlocked	FICON により、ポートがブロックされました。
portChannelMembersDown	動作中のメンバーがありません。
portFabricBindFailure	ファブリック バインド障害が発生したために、ポートが隔離されました。
portGracefulShutdown	ポートが正常にシャットダウンしました。

表 11-2　Device Manager ツールチップの定義 （続き）

ツールチップ	定義
portVsanMismatchIsolation	異なるポート VSAN を持つ非トランキング ポートを使用して、2 つのスイッチを接続しようとしました。
rcfInProgres	隔離された xE_port が、隔離されていない単一ファブリックを構築するために RCF を送信し、中断的再設定を要求しています。隔離できるのは Interconnect_Ports だけです。
srcPortNotBound	このインターフェイスに対して送信元ポートが指定されていません。
suspendedByMode	動作モードに互換性がないために、ポート チャネルに属するポートが中断しています。
suspendedBySpeed	動作速度に互換性がないために、ポート チャネルに属するポートが中断しています。
suspendedByWWN	リモート sWWN に互換性がないために、ポート チャネルに属するポートが中断しています。
swFailure	ソフトウェア障害です。
tooManyInvalidFLOGIs	無効な FLOGI が多すぎるために中断しました。
tovMismatch	TOV の不一致により、リンクが隔離されました。
trunkNotFullyActive	ピアと共通の VSAN の一部が起動していません。
upgradeInProgress	ライン カード アップグレードが進行中です。
vsanInactive	ポート VSAN が非アクティブです。ポート VSAN をアクティブにすると、ポートが再び動作可能になります。
vsanMismatchIsolation	トランク ポートの両側にこの VSAN が設定されていません。
zoneMergeFailureIsolation	2 つの Interconnect_Ports が、ゾーニングのマージ要求を交換したあとに、ゾーニング設定をマージできません。
zoneRemoteNoRespIsolation	リモート ゾーン サーバが応答していないために、隔離されました。

マップ設定を保持したままアップグレードする方法を教えてください

Cisco DCNM-SAN のバージョンをアップグレードする場合に、マップ設定（ラック名、マップ上の位置など）を保持できます。

MDS 9000/db ディレクトリには、各ユーザのサブフォルダ（1 つは fmserver 用）が格納されています。これらのサブフォルダには、検出されたすべてのファブリック（*.dat）およびマップ（*.map）に関するファイルが格納されています。これらはバージョン間でアップグレード可能です。ファブリック キャッシュをクリアする必要がある場合は、まずラックをファイルにエクスポートし、これらが失われないようにします。ラック以外のすべてのもの、およびマップ座標は、スイッチに格納されます。初期設定、前回開いたときの設定、および site_ouis.txt フォーマットには、リリースによる違いがありません。

Cisco DCNM-SAN サーバを新規ホストに移行するときに履歴データを保持する方法を教えてください

Cisco DCNM-SAN サーバを新規ホストに移行するときにデータを保持する手順は、次のとおりです。

ステップ 1　ラックをファイルにエクスポートします。

ステップ 2　Cisco DCNM-SAN を再インストールします（新規ホストにインストールする場合は、Cisco DCNM-SAN をインストールします）。

ステップ 3　インストールが完了したら、Cisco DCNM-SAN サーバを停止します。

ステップ 4　元のホストから新規ホストに RRD ファイルをコピーします。このファイルをデータベース ディレクトリに格納します（Windows PC では、このディレクトリのデフォルトのインストール場所は C:¥Program Files¥Cisco Systems¥DCM¥fm¥pm¥db です）。

ステップ 5　新規ホストの $INSTALLDIR\dcm\fm\bin フォルダから **PM.bat sync** を実行します。これにより、ファイルと新規ディレクトリ構造が作成されます。データを収集したスイッチごとに、ディレクトリが存在します。

ステップ 6　特定のスイッチでデータ収集を継続するには、該当スイッチのフォルダ内の db サブフォルダを pm フォルダにコピーします。

ステップ 7　Cisco DCNM-SAN サーバを再起動します。

ステップ 8　Performance Manager の収集にファブリックを追加します。

ステップ 9　ラックの新規ホストを再度インポートします。

ステップ 10　古いホストの元のサービスは必ずオフにします。

FCIP 上で Cisco DCNM-SAN を使用するときの制限はありますか

FCIP トンネルが起動しているかぎり、Cisco DCNM-SAN はこのトンネル上で制限なく機能します。ただし、Cisco DCNM-SAN はファブリック内にある Cisco SN5428 の管理 IP アドレスを自動検出できません。このスイッチの場合は、タイムアウト エラーが発生するため、FCIP デバイスにレッドのスラッシュが表示されます。ただし、ネーム サーバまたは FSPF 内にターゲット、発信側、および Cisco SN5428（または他の任意のスイッチ）に接続された ISL（スイッチ間リンク）が表示されているかぎり、このスイッチはこれらをすべて認識します。

この問題を解決するには、[Switches] テーブルに IP アドレスを手動で入力し、[Apply] をクリックします。コミュニティ ストリングが正しい場合、レッド スラッシュは消えます。コミュニティ ストリングが正しくない場合でも、Cisco SN5428 をダブルクリックすると、Web ツールが起動します。

[Please insure that FM server is running on localhost] メッセージへの対処法を教えてください

このエラー メッセージは、ファブリックに接続できない場合、および PC に複数のネットワーク インターフェイス カードが搭載されている場合に、表示されることがあります。問題として考えられるのは、Cisco DCNM-SAN が不正なインターフェイスを通して通信を試みていることです（このことを確認するには、FMServer.log ファイルを調べます）。

通常は、起動時にインターフェイスを自動的に選択する方法が最適です。上記エラーが表示される場合は、不正な設定が含まれている可能性があります。

Cisco DCNM-SAN をリセットして、次回の起動時にインターフェイスを自動的に選択する手順は、次のとおりです。

ステップ 1　Cisco DCNM-SAN インストール ディレクトリにある server.properties ファイルを開きます。Windows プラットフォームの場合、このファイルはデフォルトで C:\Program Files\Cisco Systems\dcm 内にあります。

ステップ 2　snmp.localaddress 行をコメント化します。

ステップ 3　ファイルを保存して、終了します。

ステップ 4　Cisco DCNM-SAN サーバを再起動します。

（注）　場合によってはこの方法を使用せずに、Cisco DCNM-SAN が使用するインターフェイスを手動で選択する必要があります。詳細については、「複数のインターフェイスを使用して Cisco DCNM-SAN を実行する方法を教えてください」（P.11-21）を参照してください。

複数のインターフェイスを使用して Cisco DCNM-SAN を実行する方法を教えてください

ご使用の PC に複数のインターフェイス（NIC）が装備されている場合は、4 つの Cisco DCNM-SAN アプリケーションによってこれらのインターフェイスが自動的に検出されます（ループバック インターフェイスは無視されます）。Cisco DCNM-SAN クライアントおよび Device Manager は、起動するたびに PC 上のすべてのインターフェイスを検出し、ユーザはその中の 1 つを選択できます。Cisco DCNM-SAN サーバおよび Performance Manager は、初回インストール時に検出し、ユーザはその中の 1 つを選択できます。これらの 2 つのアプリケーションでは、インターフェイスの選択を求めるプロンプトは再表示されません。

使用しているインターフェイスを変更しなければならない場合があります。たとえば、次の場合です。

- Cisco DCNM-SAN サーバまたは Performance Manager をインストールしたあとに、インターフェイスを追加する場合
- 最初に選択したインターフェイスと異なるインターフェイスを使用する場合
- 何らかの理由により、いずれかの Cisco DCNM-SAN アプリケーションが複数のインターフェイスを検出しなかった場合

インターフェイスを認識するアプリケーションに応じて、次のセクションを参照してください。

- 「手動による Cisco DCNM-SAN サーバ用インターフェイスの指定」（P.11-21）
- 「手動による Cisco DCNM-SAN クライアントまたは Device Manager 用インターフェイスの指定」（P.11-22）

手動による Cisco DCNM-SAN サーバ用インターフェイスの指定

Cisco DCNM-SAN サーバ（Performance Manager および Cisco DCNM-SAN Web Services を含む）にインターフェイスを指定する手順は、次のとおりです。

ステップ 1　MDS 9000 フォルダに移動します。Windows プラットフォームの場合、このフォルダはデフォルトで C:¥Program Files¥Cisco Systems¥MDS 9000 内にあります。

ステップ 2　テキスト エディタを使用して server.properties ファイルを編集します。

ステップ 3　snmp.localaddress 行が表示されるまでスクロールします。

ステップ 4　この行がコメント化されている場合は、コメント文字を削除します。

ステップ 5　使用する NIC の IP アドレスまたはインターフェイス名にローカル アドレス値を設定します。

ステップ 6　ファイルを保存します。

ステップ 7　Cisco DCNM-SAN サーバを停止し、再起動します。

手動による Cisco DCNM-SAN クライアントまたは Device Manager 用インターフェイスの指定

Cisco DCNM-SAN クライアントまたは Device Manager にインターフェイスを指定する手順は、次のとおりです。

ステップ 1　MDS 9000/bin フォルダに移動します。Windows プラットフォームの場合、このフォルダはデフォルトで C:¥Program Files¥Cisco Systems¥MDS 9000 内にあります。

ステップ 2　DeviceManager.bat ファイルまたは FabricManager.bat ファイルを編集します。

ステップ 3　set JVMARGS= で開始する行にスクロールします。

ステップ 4　パラメータ -Device Managerds.nmsaddress= *ADDRESS* を追加します。*ADDRESS* は使用する NIC の IP アドレスまたはインターフェイス名です。

ステップ 5　ファイルを保存し、Cisco DCNM-SAN クライアントまたは Device Manager を再起動します。

HTTP プロキシ サーバの設定方法を教えてください

ネットワークでプロキシ サーバを使用して HTTP 要求を処理する場合は、Java Web Start Application Manager にプロキシ サーバの IP アドレスが正しく設定されているか確認してください。

Java Web Start Application Manager にプロキシ サーバを設定する手順は、次のとおりです。

ステップ 1　Java Web Start アプリケーションを起動します。

ステップ 2　Java Web Start Application Manager で [File] > [Preferences] を選択します。

ステップ 3　[Manual] オプション ボタンを選択し、[HTTP Proxy] フィールドにプロキシ サーバの IP アドレスを入力します。

ステップ 4　[HTTP Port] フィールドに、プロキシ サービスで使用する HTTP ポート番号を入力します。

ステップ 5　[OK] をクリックします。

トポロジ マップをクリアする方法を教えてください

ファブリックから削除されたスイッチがある場合は、スイッチのアイコンに赤色の X が表示されます。スイッチを再起動しなくても、Cisco DCNM-SAN クライアントまたは Cisco DCNM-SAN サーバからこの情報をクリアすることができます（Cisco DCNM-SAN サーバの場合は、すべてのクライアントの情報がクリアされます）。

Cisco DCNM-SAN を使用してトポロジ マップから情報をクリアする手順は、次のとおりです。

ステップ 1　[Fabric] ペインの [Refresh Map] アイコンをクリックします。

クライアントから情報がクリアされます。

ステップ 2　[Server] メニューの [Purge Down Elements] をクリックします。

サーバから情報がクリアされます。

注意　現在アクセスできないすべてのデバイス（オフラインの可能性がある）が除去されます。

ソフトウェアの混在環境で Cisco DCNM-SAN を使用する方法を教えてください

Cisco DCNM-SAN バージョン 2.0(x) を使用すると、Cisco MDS 9000 スイッチが混在しているファブリックを管理できます。これらの機能をサポートしないソフトウェア バージョンが稼動するスイッチでは、特定の 2.0 機能タブには何も表示されません。

Cisco DCNM-SAN 起動時に「corrupted jar file」エラーが表示されます。対処方法を教えてください

次のエラーが表示される場合：

```
An error occurred while launching the application Cisco DCNM-SAN.

download error:corrupted jar file at <ipaddress>\Device Managerboot.jar
```

（<*ipaddress*> はスイッチの IP アドレス）

表示されるエラー メッセージは、Java Web Start キャッシュが破損していることを示します。まず、Java Web Start キャッシュをクリアしてください。キャッシュをクリアするには、（[Programs] メニューから）Java Web Start を実行し、[preferences] で [clear cache] を選択します。または、すべての Cisco DCNM-SAN または Device Manager インスタンスが閉じていることを確認してから、.javaws/cache を削除して、手動でキャッシュをクリアします。新しい JRE では、このディレクトリは Documents and Settings\USERNAME 内に、古い JRE では Program Files\Java Web Start 内に作成されます。

キャッシュ フォルダ内を参照して、問題となる IPAddress フォルダ（cache/http/D10.0.0.1 など）を削除することもできます。

同様に、ホストでウィルス チェッカ /Java ブロック機能が稼動していないか確認してください。

アンインストール プログラムを実行してから、.cisco_mds ディレクトリを削除することもできます。その後、Cisco DCNM-SAN を再インストールします。

ファブリック内のデバイスの検索方法を教えてください

Cisco DCNM-SAN では、pWWN などの複数の属性を使用して、1 つまたは複数のデバイスを検索できます。

Cisco DCNM-SAN で検索を実行する手順は、次のとおりです。

ステップ 1　マップを右クリックし、ドロップダウン メニューで [Find Elements] を選択します。

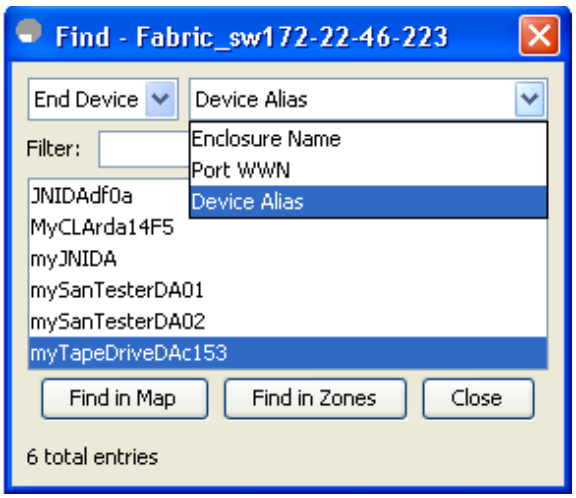
[Find Fabric] ダイアログボックスが表示されます（図 11-1 を参照）。

ステップ 2　左側のドロップダウン リストで [End Device] を選択します。

ステップ 3　右側のドロップダウン リストで [Port WWN] を選択します。

WWN の一部を入力してワイルドカード（*）を使用することもできます（たとえば、***fb*f8** と入力できます）。

図 11-1　エンド デバイスと Port WWN を選択した状態でファブリック ダイアログボックスを検索



ステップ 4　[Find in Map] をクリックします。

ゾーン内でデバイスを検索するには、[Find in Zones] をクリックします。[Fabric] ペイン内でデバイスがハイライト表示されます。任意のデバイスを右クリックすると、そのデバイスの属性が表示されます。これらのデバイスに接続されたリンクを選択して、リンクの属性を表示することもできます。

テーブルの検索方法を教えてください

Cisco DCNM-SAN では、1 つ以上の属性が割り当てられたデバイスを検索できます。[Find] ダイアログボックスに検索ストリングを入力し、[Next] および [Previous] ボタンを使用して結果を移動します。

Cisco DCNM-SAN のテーブル内で検索を実行する手順は、次のとおりです。

ステップ 1　ツールバーの [Find] アイコンをクリックします。

[Find] ダイアログボックスが表示されます。

ステップ 2　[Find] テキストボックスに検索ストリングを入力します。

ステップ 3　選択した行内を検索する場合は [Selection] をクリックします。

ステップ 4　大文字と小文字を区別しない場合は [Ignore Case] をオンにします。

ステップ 5　検索ストリングに完全一致するデータ値を検索する場合は [Exact Match] をオンにします。

ステップ 6　[Next] をクリックして検索を実行します。

ステップ 7　[Cancel] をクリックしてダイアログボックスを閉じます。

複数のファブリックの管理方法を教えてください

複数のファブリックをモニタして管理するには、1 つまたは複数のファブリックを保持する必要があります。このためには、[Server] > [Admin] ダイアログボックスの [Fabric] タブで [Persist] チェックボックスをオンにします。SAN-OS Release 1.3.x 以降が稼動するスイッチを両方のファブリックで使用し、これらで同じユーザ/パスワードを使用する必要もあります。両方のファブリックを物理的に接続しないでください。

ライセンス期限が切れるとスイッチに表示されるオレンジの X をクリアする方法を教えてください

ライセンス付き機能を使用している場合に、ライセンス期限が切れると、Cisco DCNM-SAN はライセンス違反であることを示し、Cisco DCNM-SAN マップ上のスイッチにオレンジの X を付加します。

ライセンス違反メッセージおよびオレンジの X をクリアするには、ホスト上で Cisco DCNM-SAN サービスを停止し、再起動します。

PART 3

Cisco DCNM for LAN

CHAPTER 12

DCNM-LAN の概要

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）の概要について説明します。

DCNM-LAN でサポートされる特定の Cisco Nexus 製品の詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

この章の内容は、次のとおりです。

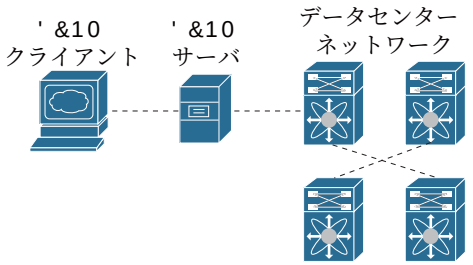
- 「DCNM-LAN クライアントおよびサーバ」（P.12-1）
- 「Cisco DCNM-LAN Release 5.2 の機能」（P.12-2）
- 「DCNM-LAN の関連資料」（P.12-3）

DCNM-LAN クライアントおよびサーバ

DCNM-LAN は、Java ベースのクライアント/サーバ アプリケーションです。Java、サーバ システムおよびクライアント システムの要件については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

図 12-1 に、DCNM-LAN クライアント/サーバ環境を示します。DCNM-LAN クライアントが通信するのは DCNM-LAN サーバだけです。管理対象の Cisco NX-OS デバイスと直接通信することはありません。DCNM-LAN サーバは、Cisco NX-OS デバイスの XML 管理インターフェイスを使用して、Cisco NX-OS デバイスを管理および監視します。XML 管理インターフェイスは、コマンドライン インターフェイス（CLI）機能を補完する NETCONF プロトコルに基づくプログラマチック方式です。詳細については、『*Cisco NX-OS XML Interface User Guide*』を参照してください。

図 12-1　DCNM-LAN クライアント/サーバ環境



Cisco DCNM-LAN Release 5.2 の機能

Cisco DCNM-LAN Release 5.2 は、次の Cisco NX-OS 機能の設定およびモニタリングをサポートしています。

- イーサネット スイッチング
  - 物理ポートと仮想ポート
  - ポート チャネルと Virtual Port Channel（vPC; 仮想ポートチャネル）
  - ループバック インターフェイスと管理インターフェイス
  - VLAN ネットワーク インターフェイス（Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）とも言う）
  - VLAN およびプライベート VLAN（PVLAN）
  - 高速スパニング ツリー（RST）およびマルチ スパニング ツリー プロトコル（MST）を含む、スパニング ツリー プロトコル
  - ファブリック エクステンダ
  - リンクステート トラッキング
  - Serial Over LAN
  - シャーシ内部ネットワーク
  - Fibre-Channel-over-Ethernet Initiation Protocol（FIP）スヌーピング
  - ポート プロファイル
- Ethernet ルーティング
  - Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、オブジェクト トラッキング、キーチェーン管理
  - ホット スタンバイ ルータ プロトコル（HSRP）
- ネットワーク セキュリティ
  - アクセス コントロール リスト
  - IEEE 802.1x
  - 認証、許可、アカウンティング（AAA）
  - ロールベース アクセス コントロール
  - ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング
  - ダイナミック アドレス解決プロトコル（ARP）インスペクション
  - IP ソース ガード
  - トラフィック ストーム制御
  - ポート セキュリティ
- 全般
  - 仮想デバイス コンテキスト
  - Ternary Content Addressable Memory（TCAM）統計情報によるハードウェア リソースの活用
  - スイッチド ポート アナライザ（SPAN）

DCNM-LAN は、ネットワーク管理を支援する次の機能を備えています。

- トポロジ ビューア

- ネットワーク サーバ
- デバイス グループ
- イベント ブラウザ
- コンフィギュレーション配信管理
- コンフィギュレーション変更管理
- デバイス OS 管理
- ハードウェアおよび仮想スイッチ コンポーネント

DCNM-LAN は、次の管理機能を備えています。

- DCNM-LAN サーバ ユーザ アカウント
- デバイス ディスカバリ
- 検出デバイスの自動同期
- 統計データ収集管理
- DCNM-LAN サーバとクライアントのロギング
- DCNM-LAN サーバ クラスタの管理

プラットフォーム サポート

DCNM-LAN は次のプラットフォームをサポートします。

- Cisco Nexus 1000V スイッチ
- Cisco Nexus 2000 Fabric Extender
- Cisco Nexus 3000 シリーズ スイッチ
- Cisco Nexus 4000 シリーズ スイッチ
- Cisco Nexus 5000 シリーズ スイッチ
- Catalyst 6500

  DCNM-LAN は、従来の IOS バージョン 12.2(33)SXI 以降が動作する Catalyst 6500 シリーズ スイッチに対して限定的なサポートを提供します。

  - DCNM-LAN は、デバイスの現在の設定属性の表示をサポートします。
  - DCNM-LAN は、デバイスの設定変更をサポートしません。
  - DCNM-LAN は、Catalyst 6500 シリーズ スイッチに対してファイアウォール サービス モジュール（FWSM）バージョン 4.0 以降をサポートしません。
- Cisco Nexus 7000 シリーズ スイッチ

DCNM-LAN の関連資料

DCNM-LAN のマニュアルには、複数のコンフィギュレーション ガイドおよびその他の資料が含まれています。DCNM-LAN マニュアルの詳細については、「マニュアルの入手方法およびテクニカル サポート」（P.lxviii）を参照してください。

CHAPTER 13

Cisco DCNM-LAN クライアントのインストールおよび起動

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）クライアントをインストールおよび起動する方法について説明します。

この章の内容は、次のとおりです。

- 「DCNM-LAN クライアントのインストールおよび起動の概要」（P.13-1）
- 「DCNM-LAN クライアントのインストールおよび起動の前提条件」（P.13-2）
- 「セキュアなクライアント通信」（P.13-2）
- 「デフォルトの管理者クレデンシャル」（P.13-3）
- 「DCNM-LAN クライアントのダウンロードおよび起動」（P.13-3）
- 「DCNM-LAN クライアントの再起動」（P.13-7）
- 「DCNM-LAN クライアントへのログイン」（P.13-7）
- 「DCNM-LAN クライアントのアンインストール」（P.13-9）
- 「その他の関連資料」（P.13-9）
- 「DCNM-LAN クライアントのインストールおよび起動の機能の履歴」（P.13-10）

DCNM-LAN クライアントのインストールおよび起動の概要

DCNM-LAN クライアントは Java アプリケーションです。DCNM-LAN クライアントのシステムへのインストールが完了した後、DCNM-LAN クライアントは自動的に起動されます。DCNM-LAN クライアントのインストール後はいつでも DCNM-LAN クライアントの再起動が必要なときに、システム上にある DCNM-LAN クライアント ソフトウェア イメージを使用して、すぐに起動できます。DCNM-LAN クライアントのバージョンが更新され入手可能になると、システム上に新バージョンの DCNM-LAN クライアントが自動的にダウンロードされます。

DCNM-LAN クライアントのインストールおよび起動の前提条件

DCNM-LAN クライアントのインストールおよび使用には、次の前提条件があります。

- DCNM-LAN クライアント ソフトウェアをインストールおよび使用するには、サポートされているオペレーティング システムをシステム上で実行している必要があります。クライアントのシステム要件については、次のサイトにある『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

  http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

- インストレーション プロセスでは、Java バージョン 1.6.0_21 を使用します。このバージョンの Java がシステムに存在しない場合は、インストレーション プロセスによりシステム上にインストールされます。

  DCNM-LAN クライアント インストーラでは、Java バージョン 1.6.0_21 JRE をダウンロードするためにインターネット アクセスが必要です。システムがインターネットにアクセスできない場合、別のシステムを使用して Java インストーラをダウンロードし、DCNM-LAN クライアントをインストールするシステムにコピーします。Java バージョン 1.6.0_21 JRE は、Oracle Technology Network Web サイトからダウンロードできます。

  ネットワーク環境で Java インストーラのダウンロードを許可させるプロキシ接続が必要な場合は、コントロール パネルからアクセスできるインターネット オプションでプロキシが設定されていることを確認します。

- 一部の DCNM-LAN 機能はライセンスが必要です。ライセンス対象機能を使用するには、事前に DCNM-LAN ライセンスをインストールします。ライセンス対象機能の詳細やライセンス インストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

セキュアなクライアント通信

デフォルトでは、DCNM-LAN のクライアント/サーバ間の通信は暗号化されませんが、クライアント サーバ通信を保護する Secure Sockets Layer（SSL）暗号化をイネーブルに設定できます。SSL 暗号化をイネーブルにしても、ユーザが行う DCNM-LAN クライアントのダウンロード、インストール、ログインの方法に影響はありません。

セキュアなクライアント通信のイネーブル化については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デフォルトの管理者クレデンシャル

DCNM-LAN をインストールする場合、DCNM-LAN ローカル ユーザである、デフォルトの管理者アカウントを指定します。RADIUS または TACACS+ の認証サーバを使用して DCNM-LAN クライアントへのアクセスを制御する場合は、デフォルトの管理者アカウントを使用すると、現在の認証モードで到達可能な認証サーバがない場合でもアクセスできるようになります。

DCNM-LAN への管理アクセス権を持つユーザがいない場合は、DCNM-LAN サーバ ソフトウェアを再インストールすることにより、ローカル管理者アカウントをリセットするか、DCNM-LAN サーバ認証設定を変更できます。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN クライアントのダウンロードおよび起動

DCNM-LAN クライアントは、DCNM-LAN サーバ上に存在する Web サーバから取得できます。DCNM-LAN クライアントは、Web ブラウザまたはコマンド プロンプトのいずれかを使用して、ダウンロードおよび起動できます。

DCNM-LAN クライアントをダウンロードおよび起動すると、自動的に、ローカル システム上にソフトウェアのイメージが保存され、DCNM-LAN クライアントが起動されます。以降、DCNM-LAN クライアントを起動するときは、ローカル システム上のイメージを使用して、すぐに起動できます。

ここでは、次の内容について説明します。

- 「Web ブラウザを使用して DCNM-LAN クライアントをダウンロードおよび起動する」（P.13-3）
- 「コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する」（P.13-5）
- 「コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する（Java Web Start Launcher を使用しない場合）」（P.13-6）

Web ブラウザを使用して DCNM-LAN クライアントをダウンロードおよび起動する

Web ブラウザを使用して、DCNM-LAN クライアントをダウンロードおよび起動できます。

はじめる前に

DCNM-LAN クライアントを実行するコンピュータには、Java バージョン 1.6.0_21 JRE がインストールされている必要があります。

DCNM-LAN クライアントを実行するコンピュータは、クライアントのシステム要件を満たしている必要があります。クライアントのシステム要件については、次のサイトにある『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

手順の詳細

ステップ 1　DCNM-LAN クライアントを使用するコンピュータ上で Web ブラウザを開き、次のアドレスにアクセスします。

http://*server_IP_address_or_DNS_name*:*web_server_port*/dcnm-client/index.html

たとえば、DCNM-LAN サーバの IP アドレスが 172.0.2.1 で、Web サーバ ポートが 8080 の場合は、次のアドレスを使用します。

```
http://172.0.2.1:8080/dcnm-client/index.html
```

ブラウザに DCNM-LAN クライアントのページが表示されます。

ステップ 2　[Launch DCNM Client] をクリックします。

DCNM-LAN サーバがブラウザに dcnm.jnlp ファイルを送信します。このファイルは、Java Web Start Launcher によってオープンされる必要があります。

ステップ 3　ブラウザから指示される場合は、dcnm.jnlp ファイルを開くようにします。ファイルを保存する必要はありません。

DCNM-LAN クライアント インストーラは、システム上にすでに Java がインストールされているかどうかを確認します。コンピュータ上にサポートされているバージョンの Java がインストーラで見つからなかった場合は、Java バージョン 1.6.0_21 をインストールするようにインストーラから指示されます。

（注）　Cisco DCNM クライアント インストーラでは、Java バージョン 1.6.0_21 JRE をダウンロードするためにインターネット アクセスが必要です。システムでインターネットにアクセスできない場合は、別のシステムを使用して Java インストーラをダウンロードし、Cisco DCNM クライアントをインストールするシステムにコピーして Java をインストールしてから、Cisco DCNM クライアントのインストレーションを再開します。Java バージョン 1.6.0_21 JRE は、Oracle Technology Network Web サイトからダウンロードできます。

ネットワーク環境で Java インストーラのダウンロードを許可させるプロキシ接続が必要な場合は、コントロール パネルからアクセスできるインターネット オプションでプロキシが設定されていることを確認します。

ステップ 4　Java バージョン 1.6.0_21 をインストールするようにインストーラから指示される場合の手順は、次のとおりです。

a.　[OK] をクリックして、サポートされているバージョンの Java のインストールを開始します。

b.　Java インストーラが期限切れのクレデンシャルでデジタル署名されているというセキュリティの警告が通知されたら、[Run] をクリックしてインストールを続行します。

c.　Java インストレーション ウィザードを実行します。

ヒント　サポートされているバージョンの Java を、コンピュータにインストール済みのブラウザで使用されるデフォルトのバージョンにするかどうかを指定する場合は、[License Agreement] ダイアログボックスの [Custom setup] を選択します。Java インストレーションの後半、[Browser Registration] ダイアログボックスで、DCNM-LAN でサポートされている Java バージョンを使用させるブラウザを指定できます。

DCNM-LAN クライアントがコンピュータにインストールされます。

（注）　インストーラによるソフトウェアのインストールが完了するまで、1 分以上かかることがあります。

DCNM-LAN クライアントのログイン ウィンドウが開きます。

ログインの手順については、「DCNM-LAN クライアントへのログイン」（P.13-7）を参照してください。

コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する

コマンド プロンプトを使用して、DCNM-LAN クライアントをダウンロードおよび起動できます。

はじめる前に

DCNM-LAN クライアントを実行するコンピュータには、Java バージョン 1.6.0_21 JRE がインストールされている必要があります。

DCNM-LAN クライアントを実行するコンピュータは、クライアントのシステム要件を満たしている必要があります。クライアントのシステム要件については、次のサイトにある『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

手順の詳細

ステップ 1　DCNM-LAN クライアントを使用するコンピュータで、コマンド プロンプトにアクセスします。

ステップ 2　次のように **cd** コマンドを使用して、ディレクトリを Java バージョン 1.6.0_21 インストレーション ディレクトリにある bin ディレクトリに変更します。

cd *path*

ここで、*path* は、bin ディレクトリへの相対パスまたは絶対パスです。たとえば、Microsoft Windows の場合、Java バージョン 1.6.0_21 の bin ディレクトリのデフォルト パスは、C:¥Program Files¥dcm¥Java¥jre1.6.0_21¥bin です。

ステップ 3　次のように該当するコマンドを入力します。

- Microsoft Windows の場合
  javaws.exe *server_IP_address_or_DNS_name*:*web_server_port*/**dcnm-client/dcnm.jnlp**
- RHEL の場合
  ./javaws *server_IP_address_or_DNS_name*:*web_server_port*/**dcnm-client/dcnm.jnlp**

Java Web Start Launcher は、DCNM-LAN サーバから dcnm.jnlp ファイルを取得し、DCNM-LAN クライアントをコンピュータにインストールします。

（注）　インストーラによるソフトウェアのインストールが完了するまで、1 分以上かかることがあります。

DCNM-LAN クライアントのログイン ウィンドウが開きます。

ログインの手順については、「DCNM-LAN クライアントへのログイン」（P.13-7）を参照してください。

コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する（Java Web Start Launcher を使用しない場合）

コマンド プロンプトを使用した DCNM-LAN クライアントのダウンロードおよび起動は、Java Web Start Launcher を使用せずにスタンドアロン モードで行うこともできます。

はじめる前に

DCNM-LAN クライアントを実行するコンピュータには、Java バージョン 1.6.0_21 JRE がインストールされている必要があります。

DCNM-LAN クライアントを実行するコンピュータは、クライアントのシステム要件を満たしている必要があります。クライアントのシステム要件については、次のサイトにある『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

（注）　DCNM-LAN クライアントがスタンドアロン モードでインストールされている場合、Cisco DCNM-SAN 相互起動機能はサポートされません。（スタンドアロン モードの DCNM-LAN クライアントは、Java Web Start アプリケーションではありません）。

手順の詳細

ステップ 1　DCNM-LAN サーバがインストールされているコンピュータ上でコマンド プロンプトにアクセスし、DCNM-LAN サーバがインストールされているディレクトリに移動します。

- Windows DCNM-LAN サーバの場合、DCNM-LAN サーバは <DCNM_INSTALL_LOCATION>\dcm\dcnm\ui-client ディレクトリにインストールされています。
  <DCNM_INSTALL_LOCATION> のデフォルトは、C:\Program Files\Cisco Systems です。
- RHEL DCNM-LAN サーバの場合、DCNM-LAN サーバは <DCNM_INSTALL_LOCATION>/dcm/dcnm/ui-client ディレクトリにインストールされています。
  <DCNM_INSTALL_LOCATION> のデフォルトは、/usr/cisco です。

ステップ 2　ui-client ディレクトリ内で、construct_DCNM_LAN_SA_Client スクリプトを探し、実行します。

- Windows DCNM-LAN サーバの場合、construct_DCNM_LAN_SA_Client.bat を実行します。
- RHEL DCNM-LAN サーバの場合、construct_DCNM_LAN_SA_Client.sh を実行します。

ステップ 3　ui-client ディレクトリを、DCNM-LAN クライアントを実行するコンピュータにコピーします。

ステップ 4　DCNM-LAN クライアントの準備を行うコンピュータ上で、コマンド プロンプトにアクセスし、Java JRE がインストールされている場所を JAVA_HOME に設定します。
次に例を示します。

- Microsoft Windows の場合
  set JAVA_HOME=C:\Program Files\Java\jre1.6.0_21
- RHEL の場合
  export JAVA_HOME=/usr/java/jre1.6.0_21

ステップ 5　DCNM-LAN クライアントの準備を行うコンピュータ上で、DCNM-LAN サーバからコピーされた ui-client ディレクトリに移動します。

ステップ 6　ui-client ディレクトリ内で、dcnm-client-sa スクリプトを探し、実行して、DCNM-LAN クライアントを起動します。

- Windows DCNM-LAN サーバの場合、dcnm-client-sa.bat を実行します。
- RHEL DCNM-LAN サーバの場合、dcnm-client-sa.sh を実行します。

DCNM-LAN クライアントのログイン ウィンドウが開きます。

ログインの手順については、「DCNM-LAN クライアントへのログイン」（P.13-7）を参照してください。

DCNM-LAN クライアントの再起動

これまでに DCNM-LAN クライアントをコンピュータにダウンロードおよび起動したことがある場合は、インストーラによってコンピュータに追加されたショートカットの 1 つを使用して、後で DCNM-LAN クライアントを起動できます。

DCNM-LAN クライアントを起動すると、DCNM-LAN クライアントは DCNM-LAN サーバに接続し、DCNM-LAN サーバ上で使用可能な DCNM-LAN クライアントが、ローカルにインストールされている DCNM-LAN クライアントよりも新しいバージョンであるかどうかをチェックします。DCNM-LAN クライアントの起動方法は、次のように、バージョンのチェック結果によって異なります。

- ローカルにインストールされている DCNM-LAN クライアントが、DCNM-LAN サーバ上で使用可能な DCNM-LAN クライアントと同じバージョンである場合、DCNM-LAN クライアント ウィンドウがすぐに開きます。
- ローカルにインストールされている DCNM-LAN クライアントが、DCNM-LAN サーバ上で使用可能な DCNM-LAN クライアントよりも古いバージョンである場合、DCNM-LAN サーバから DCNM-LAN クライアントが自動的にダウンロードされ、ローカルにインストールされている DCNM-LAN クライアントを置き換えた後、DCNM-LAN クライアント ウィンドウが開きます。

ログインの手順については、「DCNM-LAN クライアントへのログイン」（P.13-7）を参照してください。

DCNM-LAN クライアントへのログイン

DCNM-LAN クライアントにログインする場合は、有効な DCNM-LAN ユーザ アカウントを指定する必要があります。

はじめる前に

DCNM-LAN クライアントにログインする前に、次の情報を用意しておく必要があります。

- 有効な DCNM-LAN ユーザ名およびパスワード。
- DCNM-LAN サーバの IP アドレスまたは DNS 名。クラスタ サーバの配置では、これをマスター サーバの IP アドレスまたは DNS 名にする必要があります。
- DCNM-LAN サーバ ポート番号。デフォルトでは、サーバ ポート番号は 1099 です。
- プロキシ サーバ アドレス、HTTP ポート番号、Socks ポート番号（ネットワーク環境でプロキシ サーバが必要な場合）。

手順の詳細

ステップ 1　DCNM-LAN クライアントを起動します。これまでに DCNM-LAN クライアントをコンピュータにダウンロードおよび起動したことがある場合は、クライアント インストーラによってコンピュータに追加されたショートカットの 1 つを使用して、クライアントを起動できます。クライアントのダウンロードおよび起動の詳細については、次のいずれかを参照してください。

- 「Web ブラウザを使用して DCNM-LAN クライアントをダウンロードおよび起動する」（P.13-3）
- 「コマンド プロンプトを使用して DCNM-LAN クライアントをダウンロードおよび起動する」（P.13-5）

DCNM-LAN クライアントのログイン ウィンドウが開きます。

ステップ 2　[DCNM-LAN Server] フィールドに、DCNM-LAN サーバの DNS 名または IP アドレスを入力します。デフォルトで、このフィールドには、クライアントが前回サーバにログインしたときに指定したアドレスまたは名前が表示されます。クライアントのダウンロード後にログインしている場合、このフィールドには、クライアントをダウンロードしたサーバのアドレスが表示されます。

（注）　クラスタ サーバ環境に DCNM-LAN を配置している場合は、マスター DCNM-LAN サーバの DNS 名または IP アドレスを入力します。

ステップ 3　[Username] フィールドに、DCNM-LAN ユーザ名を入力します。サーバのインストール後初めて DCNM-LAN にログインしている場合は、サーバのインストレーション時に指定したローカル管理者名を入力します。詳細については、「デフォルトの管理者クレデンシャル」（P.13-3）を参照してください。

ステップ 4　[Password] フィールドに、指定した DCNM-LAN ユーザ名のパスワードを入力します。

ステップ 5　（任意）DCNM-LAN サーバ ポートを変更する必要がある場合は、次の手順を実行します。

a. [Port] フィールドが表示されていない場合は、[More >>] をクリックします。

b. [Port] フィールドに、ポート番号を入力します。

デフォルトの DCNM-LAN サーバ ポート番号は 1099 ですが、DCNM-LAN サーバのインストール時または再インストール時に別のポート番号を指定できます。

ステップ 6　（任意）DCNM-LAN サーバへの接続にプロキシ サーバを使用する必要がある場合は、次の手順を実行します。

a. [Connect to the DCNM-LAN server with a proxy server] チェックボックスが表示されていない場合は、[More >>] をクリックします。

b. [Connect to the DCNM-LAN server with a proxy server] をオンにします。

チェックボックスの下に [Proxy Server] 領域が表示されます。

c. [Address] フィールドに、プロキシ サーバの IP アドレスを入力します。

d. [HTTP Port] フィールドおよび [Socks Port] フィールドに、プロキシ サーバが HTTP 接続および Socks 接続を受け入れるポート番号を入力します。

e. （任意）プロキシ サーバで認証が必要な場合は、[Authentication] をオンにし、表示されるフィールドに有効なユーザ名とパスワードを入力します。

ステップ 7　[Login] をクリックします。

DCNM-LAN クライアントが開きます。DCNM-LAN クライアントの使用方法の詳細については、第 14 章「Cisco DCNM-LAN クライアントの使用方法」を参照してください。

DCNM-LAN クライアントのアンインストール

DCNM-LAN クライアントをコンピュータからアンインストールできます。

手順の詳細

ステップ 1　[Start] > [Control Panel] > [Java] の順にクリックします。

[Java Control Panel] ダイアログボックスが開きます。

ステップ 2　[General] タブの [Temporary Internet Files] で、[Settings] をクリックします。

[Temporary File Settings] ダイアログボックスが表示されます。

ステップ 3　[View Applications] をクリックします。

[Java Application Cache Viewer] ダイアログボックスが開きます。

ステップ 4　DCNM-LAN クライアント アプリケーションを選択し、[Remove Selected Application] をクリックします。

コンピュータから DCNM-LAN クライアント イメージが Java によってアンインストールされます。

ステップ 5　[Java Application Cache Viewer] を閉じます。

ステップ 6　[Temporary File Settings] ダイアログボックスで、[OK] をクリックします。

ステップ 7　[Java Control Panel] ダイアログボックスで、[OK] をクリックします。

ステップ 8　DCNM-LAN クライアントを再インストールする場合は、「DCNM-LAN クライアントのダウンロードおよび起動」（P.13-3）を参照してください。

その他の関連資料

DCNM-LAN クライアントのインストールおよび起動に関する追加情報については、次を参照してください。

- 「関連資料」（P.13-9）
- 「標準」（P.13-10）

関連資料

関連項目	参照先
DCNM-LAN クライアントの使用方法	第 14 章「Cisco DCNM-LAN クライアントの使用方法」
DCNM-LAN サーバの起動または停止	第 28 章「Cisco DCNM-LAN サーバの起動と停止」
組織での DCNM-LAN の導入プロセス	『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』
DCNM-LAN サーバのインストール	『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN クライアントのインストールおよび起動の機能の履歴

表 13-1 は、この機能のリリースの履歴です。

表 13-1　DCNM-LAN クライアントのインストールおよび起動の機能の履歴

機能名	リリース	機能情報
クライアントをダウンロードするためのコマンド プロンプトの使用。	5.0(2)	この機能のサポートが追加されました。
DCNM-LAN クライアントのプロキシのサポート。	5.0(2)	この機能のサポートが追加されました。

CHAPTER 14

Cisco DCNM-LAN クライアントの使用方法

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）クライアントのユーザ インターフェイス、および一般的な機能の使用方法について説明します。

この章の内容は、次のとおりです。

- 「DCNM-LAN クライアントの概要」（P.14-1）
- 「DCNM-LAN クライアントの起動」（P.14-8）
- 「DCNM-LAN クライアントの終了」（P.14-10）
- 「変更の配置」（P.14-10）
- 「統計情報および図の作業」（P.14-11）
- 「グローバル プリファレンスの設定」（P.14-16）
- 「オンライン ヘルプの使用方法」（P.14-18）
- 「その他の関連資料」（P.14-19）
- 「DCNM-LAN クライアントの使用の機能履歴」（P.14-20）

DCNM-LAN クライアントの概要

ここでは、DCNM-LAN クライアントとその内容について説明します。

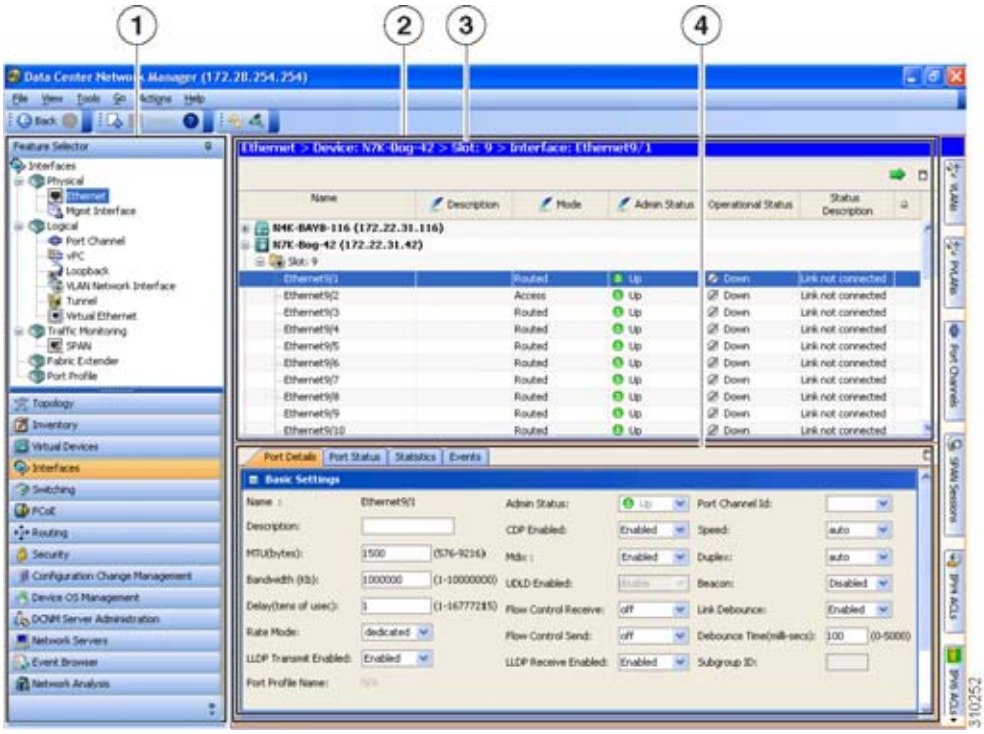
ここでは、次の内容について説明します。

- 「ユーザ インターフェイス」（P.14-2）
- 「[Feature Selector] ペイン」（P.14-2）
- 「[Contents] ペイン」（P.14-3）
- 「[Summary] ペイン」（P.14-3）
- 「[Details] ペイン」（P.14-3）
- 「[Association] ペイン」（P.14-4）
- 「メニュー」（P.14-5）
- 「ツールバー」（P.14-7）
- 「キーボード コマンド」（P.14-7）
- 「複数プラットフォームのサポート」（P.14-7）

ユーザ インターフェイス

DCNM-LAN クライアントのユーザ インターフェイス（図 14-1 を参照）には、デバイスのステータス情報が表示され、デバイスを管理する設定ツールが提供されています。この画面は、いくつかのペインに分割されています（図 14-1 を参照）。管理対象デバイスの特定のオブジェクトの情報を表示する場合、または設定タスクを実行する場合は、図 14-1 に示す順序でペインを使用します。

図 14-1　DCNM-LAN クライアントのユーザ インターフェイス



1	[Feature Selector] ペイン	**3**	[Summary] ペイン
2	[Contents] ペイン	**4**	[Details] ペイン

[Feature Selector] ペイン

[Feature Selector] ペイン（図 14-1 を参照）には、カテゴリ別にグループ化された機能が表示され、使用または設定する機能を選択できます。[Feature Selector] ペインの下部セクションには、機能カテゴリのボタンが表示されます。カテゴリを選択すると、[Feature Selector] ペインの上部セクションに、選択したカテゴリの機能ツリーが表示されます。

図 14-1 では、[Interfaces] カテゴリが選択されているため、ツリーには管理対象デバイスのインターフェイスを設定する機能が表示されています。

DCNM-LAN のマニュアルおよびオンライン ヘルプには、[Feature Selector] ペインから対応する機能を選択して開始する、多数の手順が含まれています。たとえば、イーサネット インターフェイスを設定する手順は、次のように開始します。

[Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] の順に選択します。

ツリーで機能を選択すると、[Contents] ペインに、その機能の情報が表示されます。

[Contents] ペイン

[Contents] ペイン（図 14-1 を参照）には、現在選択されている機能の情報が表示され、その機能を設定するためのフィールドがあります。[Contents] ペインには、さらに小さい [Summary] ペインと [Details] ペインがあります。

[Summary] ペイン

[Summary] ペイン（図 14-1 を参照）には、情報を表示したり、処理を実行したりできるオブジェクトが整理されて表示されます。表示されるオブジェクトのタイプは、選択した機能によって異なります。

たとえば、[Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] を選択すると、[Summary] ペインにデバイスのテーブルが表示されます。管理対象デバイスを展開すると、ネットワーク インターフェイス カードが搭載されたスロットが表示されます。スロットを展開すると、搭載されているインターフェイスと、ポート モード、管理ステータス、運用ステータスなど、インターフェイスの主要なステータス情報が表示されます。ほとんどの機能では、[Summary] ペインのタイトル バーに選択内容が表示されます。

表示または設定するオブジェクトを選択すると、[Details] ペインに、イーサネット インターフェイスなどの選択したオブジェクトの情報が表示されます。

[Summary] ペインのエクスポート

[Summary] ペインに表示されているデータを、Microsoft Excel 97-2003 形式のスプレッドシートにエクスポートできます。そのためには、[Summary] ペインの右上の隅にある緑色の矢印をクリックし、スプレッドシートのファイル名と場所を指定します。

[Summary] ペインのフィルタリング

多くの機能で、[Summary] ペインに表示するオブジェクトをフィルタリングできます。選択した機能がフィルタリングをサポートしていれば、メニュー バーで [View] > [Filter] を選択することにより、フィルタリングをイネーブルに設定できます。[Summary] ペインで、オブジェクトをフィルタリングできるカラムは、ドロップダウン リストになります。[Summary] ペインの表示をフィルタリングするには、カラムのドロップダウン リストで表示するオブジェクトを限定します。

[Details] ペイン

[Details] ペイン（図 14-1 を参照）には、[Summary] ペインで選択したオブジェクト固有の情報フィールドおよび設定フィールドが表示されます。[Details] タブには通常、いくつかのサブ タブが含まれています。タブをクリックすると、そのタブの内容が表示されます。

ここでは、次の内容について説明します。

- 「タブ」（P.14-3）
- 「セクション」（P.14-4）

タブ

関連フィールドおよび情報は、タブによって構成されています。たとえば、図 14-1 のようにイーサネット インターフェイスを選択した場合は、[Details] ペインに、[Port Details] タブなどの 4 つのタブが表示されます。

[Summary] ペインから選択する多数のオブジェクト タイプの場合、通常、次の 2 つの特殊タブが [Details] ペインに表示されます。

- [Statistics]：このタブを使用して、選択したオブジェクトに関する統計情報や図を操作できます。詳細については、「統計情報および図の作業」（P.14-11）を参照してください。
- [Events]：このタブを使用して、選択したオブジェクトに関する機能固有のイベントを表示できます。詳細については、『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

セクション

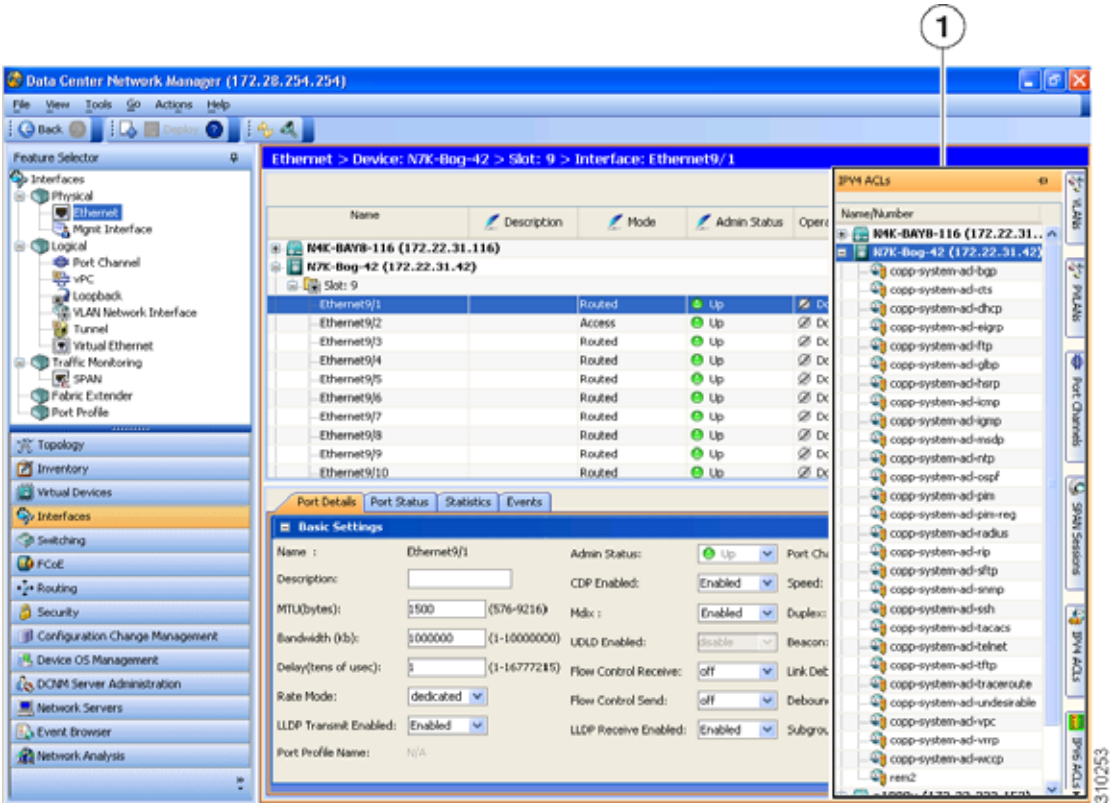
セクションには、関連フィールドおよび情報の、より詳細な構成が表示されます。DCNM-LAN クライアントでは、セクションを展開表示したり閉じたりできるため、必要に応じてフィールドおよび情報の表示と非表示を切り換えることができます。たとえば、図 14-1 の [Port Details] タブでは、[Basic Settings] セクションは展開表示されていますが、[Port Mode Settings] セクションは閉じています。

[Association] ペイン

DCNM-LAN クライアントには、現在選択中の機能に関連付けられた機能で設定したオブジェクトにアクセスできる、[Association] ペインも含まれています。図 14-2 に、[Association] ペインを示します。

[Association] ペインは、DCNM-LAN クライアントの右側に表示されているタブをクリックすると表示されます。たとえば、図 14-2 では、イーサネット インターフェイスの設定中に、[Association] ペインを使用して IPv4 ACL にアクセスし、インターフェイスに適用できます。[Association] ペインの IPv4 ACL を右クリックすると、インターフェイスにその ACL を適用したり、IPv4 ACL 機能に移動して ACL を設定したりできます。

図 14-2　[Association] ペイン



1	[Association] ペイン

メニュー

DCNM-LAN クライアントのメニュー バーには、次の標準的なメニューが含まれています。

[File] メニュー

- [New]：新しいオブジェクトを作成します。作成できるオブジェクトのタイプは、現在選択されている機能によって異なります。[Summary] ペインで選択したオブジェクトによって、作成できる内容が異なることもあります。
- [Deploy]：DCNM-LAN サーバに変更を保存し、管理対象デバイスに設定の変更を適用します。
- [Exit]：DCNM-LAN クライアントを閉じます。

[View] メニュー

- [Toolbars]：現在選択されている機能で使用できるツールバーの表示と非表示を切り換えます。詳細については、「ツールバー」（P.14-7）を参照してください。
- [Refresh]：DCNM-LAN クライアントで、DCNM-LAN サーバからのアップデート情報を強制的に取得します。
- [Filter]：[Summary] ペインのフィルタリング オプションをイネーブルまたはディセーブルにします。

[Tools] メニュー

- [Preferences] : [Global Preferences] ダイアログボックスを開きます。詳細については、「グローバル プリファレンスの設定」（P.14-16）を参照してください。
- [Debug] : DCNM-LAN クライアントのログ レベルを設定できる [DCNM-LAN Client Logging] ダイアログボックスが開きます。

（注）　特定の問題をトラブルシューティングする場合、またはシスコ テクニカル サポートからクライアントのログ レベルを変更するように要求された場合を除き、デフォルトのクライアント ログ レベルを使用することを推奨します。

[Go] メニュー

- [Topology] : [Feature Selector] ペインの [Topology] ボタンが選択されます。
- [Inventory] : [Feature Selector] ペインの [Inventory] ボタンが選択されます。
- [Virtual Devices] : [Feature Selector] ペインの [Virtual Devices] ボタンが選択されます。
- [Interfaces] : [Feature Selector] ペインの [Interfaces] ボタンが選択されます。
- [Switching] : [Feature Selector] ペインの [Switching] ボタンが選択されます。
- [FCoE] : [Feature Selector] ペインの [FCoE] ボタンが選択されます。
- [Routing] : [Feature Selector] ペインの [Routing] ボタンが選択されます。
- [Security] : [Feature Selector] ペインの [Security] ボタンが選択されます。
- [Configuration Change Management] : [Feature Selector] ペインの [Configuration Change Management] ボタンが選択されます。
- [Device OS Management] : [Feature Selector] ペインの [Device OS Management] ボタンが選択されます。
- [Configuration Delivery Management] : [Feature Selector] ペインの [Configuration Delivery Management] ボタンが選択されます。
- [DCNM-LAN Server Administration] : [Feature Selector] ペインの [DCNM-LAN Server Administration] ボタンが選択されます。
- [Network Servers] : [Feature Selector] ペインの [Network Servers] ボタンが選択されます。
- [Event Browser] : [Feature Selector] ペインの [Event Browser] ボタンが選択されます。

[Actions] メニュー

[Actions] メニュー上の項目には、使用している機能や [Summary] ペインで選択されているオブジェクトに応じて実行可能な操作が反映されます。[Inventory] など一部の機能では、[Actions] メニューがメニュー バーに表示されません。

[Help] メニュー

- [Help Contents] : オンライン ヘルプ システムの Welcome ページが開きます。
- [Context Help] : オンライン ヘルプ システムで、現在 [Feature Selector] ペインで選択されている機能に該当するページが開きます。

- [Show DCNM-LAN Instance ID]：DCNM-LAN サーバのライセンス ID が表示されたダイアログボックスが開きます。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
- [View Licenses]：ダイアログボックスが開き、DCNM-LAN サーバに現在インストールされているライセンス ファイルの情報が表示されます。
- [About Data Center Network Manager]：ダイアログボックスが開き、ソフトウェア バージョンや実装バージョンなど、DCNM-LAN サーバに関する情報が表示されます。

ツールバー

DCNM-LAN クライアントには、いくつかの標準的なツールバーに加え、該当する機能を選択したときにだけ使用可能な、追加の機能固有のツールバーが備わっています。次の表に、ツールバーを設定するために実行できる操作の一覧を示します。

アクション	方法
ツールバーの表示/非表示	ツールバー領域を右クリックして、表示または非表示にするツールバーを選択します。
ツールバーの再配置	移動するツールバーの左端をクリックして、移動先までドラッグします。
ツールバーの分離	分離するツールバーの左端をクリックし、ツールバー領域の外側までドラッグします。
ツールバーの非表示、再配置、分離の制御	ツールバー領域を右クリックして、制御するオプションを選択します。

キーボード コマンド

メニュー項目またはツールバーから実行できるコマンドの多くは、キーボードを使用して実行できます。メニューには、メニュー項目に対応するキーボード操作が表示されます。次に、よく使用するメニュー項目と、対応するキーボード コマンドを示します。

- Deploy（配置）：Ctrl+S
- Refresh（リフレッシュ）：F5
- Filter（フィルタ）：Ctrl+F
- Online help (オンライン ヘルプ) : F1
- Ext（終了）：Ctrl+Q

複数プラットフォームのサポート

DCNM-LAN は、いくつかの種類の Cisco Nexus プラットフォームをサポートしていますが、DCNM-LAN でサポートされている機能のいくつかは、一部のプラットフォームでサポートされていないか該当しません。ここでは、DCNM-LAN のユーザ インターフェイスで未サポートの機能が扱われる方法について説明します。

- サポートされていない機能：プラットフォームで特定の機能がサポートされていない場合、その機能に対してプラットフォームが表示されません。

たとえば、[Feature Selector] ペインで [Security] > [Access Control] > [Time-range] の順に選択した場合、[Summary] ペインに時間範囲機能をサポートするプラットフォーム タイプだけが表示されます。この例では、Cisco Nexus 1000V はこの機能をサポートしていないため、管理対象の Cisco Nexus 1000V プラットフォームが [Summary] ペインに表示されません。同様に、[Time-range association] ペインには Cisco Nexus 1000V プラットフォームが含まれません。

- サポートされていない属性：プラットフォームで機能がサポートされていても、その機能の特定の属性がサポートされていない場合があります。その場合には、属性が灰色で表示されるか値 N/A（非該当）がフィールドまたはセルに表示されます。

  特定のセクションにグループ化されたすべての属性がサポートされていない場合は、セクション タイトルに「N/A」が追加され、DCNM-LAN でそのセクションを展開できなくなります。

  特定のプラットフォームでタブ内のすべての属性がサポートされていない場合、タブは表示されますが、タブをクリックしても、属性がサポートされていないことを示すメッセージが表示されます。
- サポートされていない図：プラットフォームで図の中の一部の属性がサポートされていない場合、DCNM-LAN でそれらの属性が灰色で表示されます。プラットフォームが図の中のいずれかの属性をサポートしていない場合、図を選択すると、DCNM-LAN により図がサポートされていないことを示すメッセージが表示されます。
- サポートされていないオプション：プラットフォームがオプションをサポートしていない場合、そのオプションはドロップダウン リストなどに表示されません。
- サポートされない操作：プラットフォームで、コンテキスト メニューまたはツールバー メニュー上の特定の操作に対するオプションがサポートされていない場合、そのオプションは灰色表示されます。

DCNM-LAN クライアントの起動

使用するコンピュータ上に DCNM-LAN クライアントをインストールすれば、DCNM-LAN クライアントを起動できます。

はじめる前に

使用するコンピュータ上に、DCNM-LAN クライアントをインストールします。DCNM-LAN クライアントのインストールの詳細については、第 13 章「Cisco DCNM-LAN クライアントのインストールおよび起動」を参照してください。

手順の詳細

ステップ 1　スタート メニューから、[All Programs] > [Cisco DCNM Client] > [Cisco DCNM LAN] の順に選択します。

（注）　[All Programs] メニューに DCNM-LAN クライアントが表示されない場合は、DCNM-LAN サーバの Web サイトから DCNM-LAN クライアントを起動できます。詳細については、第 13 章「Cisco DCNM-LAN クライアントのインストールおよび起動」を参照してください。

ダイアログボックスにログイン フィールドが表示されます。

ステップ 2　[DCNM Server] フィールドに、DCNM-LAN サーバの IP アドレスまたはホスト名を入力します。ホスト名を使用できるのは、DNS サーバに DCNM-LAN サーバ ホスト名のエントリがある場合だけです。現在のクライアントで以前にサーバにログインしている場合は、ドロップダウン リストから IP アドレスまたはホスト名を選択することもできます。

（注）　クラスタ サーバ環境に DCNM-LAN を配置している場合は、マスター DCNM-LAN サーバの DNS 名または IP アドレスを入力します。

ステップ 3　[Username] フィールドに、DCNM-LAN クライアントへのアクセスに使用する DCNM-LAN サーバ ユーザ アカウントの名前を入力します。

ステップ 4　[Password] フィールドに、指定したユーザ アカウントのパスワードを入力します。

ステップ 5　（任意）DCNM-LAN サーバ ポートを変更する必要がある場合は、次の手順を実行します。

a.　[Port] フィールドが表示されていない場合は、[More >>] をクリックします。

b.　[Port] フィールドに、ポート番号を入力します。

デフォルトの DCNM-LAN サーバ ポート番号は 1099 ですが、DCNM-LAN サーバのインストール時または再インストール時に別のポート番号を指定できます。

ステップ 6　（任意）DCNM-LAN サーバへの接続にプロキシ サーバを使用する必要がある場合は、次の手順を実行します。

a.　[Connect to the DCNM-LAN server with a proxy server] チェックボックスが表示されていない場合は、[More >>] をクリックします。

b.　[Connect to the DCNM server with a proxy server] をオンにします。

チェックボックスの下に [Proxy Server] 領域が表示されます。

c.　[Address] フィールドに、プロキシ サーバの IP アドレスを入力します。

d.　[HTTP Port] フィールドおよび [Socks Port] フィールドに、プロキシ サーバが HTTP 接続および Socks 接続を受け入れるポート番号を入力します。

e.　（任意）プロキシ サーバで認証が必要な場合は、[Authentication] をオンにし、表示されるフィールドに有効なユーザ名とパスワードを入力します。

ステップ 7　[Login] をクリックします。

DCNM-LAN クライアントのユーザ インターフェイスが表示されます。

ダイアログボックスにデバイス クレデンシャルに関するメッセージが表示された場合、指定したユーザ アカウントに対してデバイス クレデンシャルが設定されていません。

ステップ 8　デバイス クレデンシャルが設定されていないというメッセージが表示されたら、次のいずれかを行います。

- デバイス クレデンシャルをすぐに設定する場合は、[Yes] をクリックします。
- デバイス クレデンシャルをすぐに設定しない場合は、[No] をクリックします。

（注）　デバイス クレデンシャルの設定の詳細については、「デバイスとクレデンシャルの管理」（P.17-1）を参照してください。

DCNM-LAN クライアントの終了

作業が完了したら、DCNM-LAN クライアントを終了します。

手順の詳細

ステップ 1　メニュー バーで、[File] > [Exit] を選択します。

ダイアログボックスに、確認メッセージが表示されます。

ステップ 2　（任意）変更を配置していない場合は、次のいずれかを行います。

- 変更を保存して、管理対象デバイスに設定の変更を適用するには、[Save pending changes] をオンにします。
- 変更を取り消すには、[Save pending changes] をオフにします。

ステップ 3　[Yes] をクリックします。

DCNM-LAN クライアント セッション中に何らかの統計データ収集プロセスを開始した場合、ダイアログボックスに収集プロセスが表示されます。

ステップ 4　開始した統計データ収集プロセスが表示されている場合は、次の作業を行います。

a. 停止する統計情報収集プロセスを判別します。

（注） DCNM-LAN クライアントからログアウトするときは、不要な統計収集プロセスを停止することをお勧めします。

b. 停止する統計情報収集プロセスにチェックマークを付けます。すべての収集プロセスを停止する場合は、[Select All] をクリックします。

c. [OK] をクリックします。

変更の配置

Cisco DCNM-LAN クライアントを使用して管理対象デバイスまたは Cisco DCNM-LAN サーバの設定を変更する場合、変更内容に応じて、変更の配置が必要になることがあります。また、DCNM-LAN クライアントによって自動的に変更が配置されることもあります。

- 自動的な配置：DCNM-LAN クライアントによって自動的に変更が配置される場合、「Deploying configuration」メッセージが短い時間表示されます。たとえば、ACL からアクセス ルールを削除した場合、DCNM-LAN クライアントによって、ACL がある管理対象デバイスにこの設定変更が配置されます。
- 手動配置：DCNM-LAN クライアントが設定変更を保存している場合、ツールバーで [Deploy] ボタンを使用できます。たとえば、ACL のアクセス ルールのシーケンス番号を変更すると、ACL がある管理対象デバイスに手動でこの設定変更を配置するまで、DCNM-LAN クライアントによってこの設定変更が保存されます。

  DCNM-LAN クライアントが保存している変更を配置する必要があることをユーザに知らせるために、DCNM-LAN マニュアル セット内の手順には配置手順が含まれています。

サーバの変更を配置すると、DCNM-LAN サーバ上に変更が保存されます。たとえば、DCNM-LAN サーバ ユーザ アカウントを追加した場合、変更を配置すると DCNM-LAN サーバにユーザ アカウントが追加されますが、管理対象デバイスには影響がありません。

管理対象デバイスに対して設定変更を配置すると、DCNM-LAN サーバによりデバイスの実行コンフィギュレーションがアップデートされます。

（注）　DCNM-LAN では、管理対象デバイスのスタートアップ コンフィギュレーションはアップデートされません。管理対象デバイスのスタートアップ コンフィギュレーションを実行コンフィギュレーションと置換する場合は、デバイスのコマンドライン インターフェイスにログインして、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コピーします。

DCNM-LAN クライアントの終了時に変更を配置していなかった場合は、DCNM-LAN クライアントの終了プロセスを取り消さなくても、変更を配置できます。詳細については、「DCNM-LAN クライアントの終了」（P.14-10）を参照してください。

統計情報および図の作業

ここでは、[Statistics] タブで使用できる統計図の使用方法について説明します。

ここでは、次の内容について説明します。

- 「統計情報および図の概要」（P.14-11）
- 「統計情報および図のライセンス要件」（P.14-11）
- 「図の表示」（P.14-12）
- 「図の統計モニタリングの開始」（P.14-12）
- 「図の統計モニタリングの停止」（P.14-13）
- 「図の使用方法」（P.14-13）
- 「概要図の使用方法」（P.14-14）
- 「図のエクスポート」（P.14-15）

統計情報および図の概要

[Statistics] タブを使用してオブジェクトの統計情報のモニタリングを開始および停止し、選択したオブジェクトに関する統計図を利用できます。各図には、履歴の傾向を調べ、標準図の時間範囲を制御できる概要図も表示されます。

新しい図のモニタリングを開始すると、DCNM-LAN により新しい統計情報収集プロセスが作成され、統計データ収集機能に表示されます。詳細については、「統計データ収集の管理」（P.25-1）を参照してください。

統計情報および図のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	リアルタイム モニタリングには、ライセンスは不要です。 Cisco DCNM-LAN の次の機能には、LAN エンタープライズ ライセンスが必要です。 • 統計データの履歴の保持 • 概要図の使用 Cisco DCNM-LAN LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

図の表示

任意の図を表示できます。特定の [Statistics] タブで使用できる図の内容は、機能および選択したオブジェクトによって異なります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、統計図を使用する機能を選択します。

たとえば、[Interfaces] > [Physical] > [Ethernet] の順に選択します。

ステップ 2　[Summary] ペインで、オブジェクトを選択します。

[Details] ペインに、[Statistics] タブが表示されます。

（注）　[Statistics] タブが表示されない場合、選択したオブジェクトには統計図が存在しません。

ステップ 3　[Statistics] タブをクリックします。

[Statistics] タブに、1 つ以上の図が表示されます。

（注）　[Summary] ペインで選択したオブジェクトに対して DCNM-LAN が実行している統計コレクションの図を表示するかどうかを確認するダイアログボックスが表示されます。詳細については、「モニタリング プリファレンスの設定」（P.14-16）を参照してください。

ステップ 4　監視する統計図が表示されない場合は、ツールバーで [New Chart] を選択し、該当する図を選択します。

ステップ 5　使用する図のタイトル バーをクリックします。

図のペインの左下隅に、図のステータスが表示されます。図がアクティブではない場合、図を使用するには、その図の統計モニタリングを開始する必要があります。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。

図の統計モニタリングの開始

統計モニタリングをサポートしている任意のデバイス コンフィギュレーション機能について、[Statistics] タブの図の統計モニタリングを開始できます。

（注）　新しい図のモニタリングを開始するごとに、DCNM-LAN により新しい統計情報収集プロセスが作成され、統計データ収集機能に表示されます。

手順の詳細

ステップ 1　統計モニタリングを開始する図を表示します。詳細については、「図の表示」（P.14-12）を参照してください。

ステップ 2　図のペインで、[Select Parameters] をクリックし、図に表示する最低 1 つの統計パラメータをオンにし、[Select Parameters] を再びクリックします。

ステップ 3　[Monitor] ツールバーで、 アイコンを選択し、収集プロセスを開始します。

ステップ 4　選択したパラメータの図が表示されます。

（注）　開始した統計情報収集プロセスを停止せずに DCNM-LAN クライアントを終了しようとすると、統計情報収集を停止するか続行するかを問い合わせるダイアログボックスが表示されます。DCNM-LAN クライアントからログアウトするときは、不要な統計収集プロセスを停止することをお勧めします。

図の統計モニタリングの停止

[Statistics] タブの図の統計モニタリングは、停止できます。

（注）　図のモニタリングを停止すると、統計データ収集機能に表示されている対応する統計情報収集プロセスが停止します。

手順の詳細

ステップ 1　統計モニタリングを停止する図を表示します。詳細については、「図の表示」（P.14-12）を参照してください。

ステップ 2　[Monitor] ツールバーで、 アイコンを選択します。

（注）　停止する図が表示されない場合は、統計データ収集機能を使用して、収集プロセスを停止してください。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。

図の使用方法

DCNM-LAN クライアントでは、図に対して、次の作業を行うことができます。

- パラメータの変更

- 図の更新頻度の設定
- 図データの拡大表示の制御
- しきい値の線の表示、移動、非表示
- DCNM-LAN クライアント ウィンドウからの図の分離

ここでは、各作業の基本的な手順について説明します。

（注）　概要図の使用方法については、「概要図の使用方法」（P.14-14）を参照してください。

手順の詳細

ステップ 1　使用する図を表示します。詳細については、「図の表示」（P.14-12）を参照してください。

ステップ 2　図がアクティブではない場合、図を使用するには、その図の統計モニタリングを開始する必要があります。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。

ステップ 3　（任意）パラメータを変更するには、[Select Parameters] をクリックし、収集する統計パラメータをオンにして、[Select Parameters] を再びクリックします。

ステップ 4　（任意）選択したオブジェクトの統計データの更新頻度を設定するには、[Monitor] ツールバーの [Select Frequency] ドロップダウン リストから、新しい頻度を選択します。

ステップ 5　（任意）図の拡大表示を制御するには、次のいずれかを行います。

- 図の一部の領域を拡大表示するには、その領域の一端にマウス ポインタを置き、マウスの左ボタンを押したまま、マウス ポインタを対角方向にドラッグして領域を選択し、マウス ボタンを放します。
- 図の一部の領域を拡大表示するには、その領域の一端にマウス ポインタを置き、マウス ポインタをクリックして、対角方向の端までドラッグします。
- 1 つ前のズームに戻すには、 アイコンをクリックします。
- 次のズームに変更するには、 アイコンをクリックします。
- デフォルトの拡大表示にリセットするには、 アイコンをクリックします。

ステップ 6　（任意）しきい値の線を表示、移動、または非表示にするには、次のいずれかを行います。

- しきい値の線の表示と非表示を切り換えるには、[Monitor] ツールバーの アイコンをクリックします。
- 上限しきい値の線を移動するには、 アイコンをクリックしてドラッグします。
- 上限しきい値の線を移動するには、 アイコンをクリックしてドラッグします。

ステップ 7　（任意）図を DCNM-LAN クライアント ウィンドウから分離するには、図のタイトルの下に表示されている赤い線をクリックします。

概要図の使用方法

概要図を使用して、現在の図の統計データの履歴傾向を表示し、標準図の時間範囲を設定することができます。

はじめる前に

概要図に表示するデータのあるすべてのデバイスが、DCNM-LAN ライセンス デバイスのリストに含まれていることを確認します。詳細については、「統計情報および図のライセンス要件」（P.14-11）を参照してください。

手順の詳細

ステップ 1　使用する概要図が含まれている図を表示します。詳細については、「図の表示」（P.14-12）を参照してください。

ステップ 2　図がアクティブではない場合、図の概要図を使用するには、その図の統計モニタリングを開始する必要があります。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。

ステップ 3　[Show Overview Chart] をクリックします。

新しいウィンドウに、統計データの履歴傾向を示す概要図が表示されます。

ステップ 4　図の時間範囲を設定するには、概要図のウィンドウの下で、設定する時間範囲のボタンをクリックします。時間範囲のボタンは、次のとおりです。

- [RT]：リアルタイム
- [1d]：1 日間
- [2d]：2 日間
- [5d]：5 日間
- [15d]：15 日間
- [1m]：1 ヶ月間
- [3m]：3 ヶ月間

ステップ 5　概要図を閉じるには、[Show Overview Chart] を再びクリックします。

図のエクスポート

図を、JPG イメージまたはカンマ区切り形式（CSV）ファイルとしてエクスポートできます。

図を JPG イメージとしてエクスポートすると、図の画像がそのままエクスポートされます。

図を CSV ファイルとしてエクスポートすると、図の統計収集の全データがファイルに含まれます。

手順の詳細

ステップ 1　使用する図を表示します。詳細については、「図の表示」（P.14-12）を参照してください。

ステップ 2　図がアクティブではない場合、図のイメージをエクスポートするには、その図の統計モニタリングを開始する必要があります。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。

ステップ 3　イメージをエクスポートする前に、図に表示するデータを設定します。詳細については、「図の使用方法」（P.14-13）を参照してください。

ステップ 4　図を右クリックします。

ステップ 5　次のいずれかを選択します。

- Export as CSV
- Export as JPG

ステップ 6　出力先とファイル名を指定し、[Save] をクリックします。

指定したファイル形式で、図がエクスポートされます。

グローバル プリファレンスの設定

[Global Preferences] ダイアログボックスを使用して、DCNM-LAN クライアントでのデータとフィールドの表示方法について、いくつかのプリファレンスを設定できます。[Global Preferences] ダイアログボックスには、次のセクションがあります。

- [Monitoring]：管理対象デバイスからのデフォルトの統計データ取得頻度と、統計図を自動的に開くかどうかを制御します。詳細については、「モニタリング プリファレンスの設定」（P.14-16）を参照してください。
- [Events]：DCNM-LAN クライアントの起動時に、DCNM-LAN サーバから取得するイベントの最大経過時間を制御します。詳細については、「サーバから取得するイベントの最大経過時間の設定」（P.14-17）を参照してください。
- [Pre Provision]：DCNM-LAN クライアントに、設定内容に応じて一部の設定だけを表示するか、常時すべての設定を表示するかを制御します。詳細については、「事前プロビジョニングの設定」（P.14-17）を参照してください。

モニタリング プリファレンスの設定

管理対象デバイスから統計データを取得するデフォルトの頻度を設定できます。デフォルトの統計データ取得頻度は、30 秒です。新しい図では、このデータ取得頻度が初期設定されます。図に特定の設定を変更することにより、デフォルトの頻度を無効にすることができます。

また、DCNM-LAN で統計データをすでに収集してあるオブジェクトの [Statistics] タブにアクセスしたときに、DCNM-LAN クライアントで統計図を自動的に開くかどうかも設定できます。

はじめる前に

DCNM-LAN が統計データを取得するデフォルトの頻度を確認します。図のデータについて、更新頻度の重要性を考慮してください。最新データの取得がきわめて重要であれば、データが頻繁に更新されるように、短い取得頻度を設定します。

手順の詳細

ステップ 1　メニュー バーで、[Tools] > [Preferences] を選択します。

[Global Preferences] ダイアログボックスが表示されます。[Monitoring] セクションの [Default Monitoring Frequency] ドロップダウン リストに、現在の統計データ取得頻度が表示されます。

デフォルトのポーリング頻度は、30 秒です。

ステップ 2　デフォルトの統計データ取得頻度を設定する場合は、[Default Monitoring Frequency] ドロップダウン リストから、新しいデータ取得頻度を選択します。

ステップ 3　また、DCNM-LAN で統計データをすでに収集してあるオブジェクトの [Statistics] タブにアクセスしたときのデフォルトの動作を設定するには、次のいずれかの手順を実行します。

- 確認を求めることなく図を表示するには、[Load history charts by default] チェックボックスをオンにします。
- 統計図を開く前に確認を求めるようにするには、[Load history charts by default] チェックボックスをオフにします。

ステップ 4　[OK] をクリックします。

サーバから取得するイベントの最大経過時間の設定

DCNM-LAN クライアントの起動時に、DCNM-LAN サーバから取得するイベントの最大経過時間を設定できます。この設定により、DCNM-LAN クライアントのイベント ブラウザおよび機能に固有の [Events] タブに表示されるイベントの経過時間が決まります。デフォルトでは、DCNM-LAN クライアントの起動時に、1 時間前までに発生したイベントが取得されます。DCNM-LAN クライアントの設定を変更すれば、最大 24 時間前までのイベントを取得できます。

手順の詳細

ステップ 1　メニュー バーで、[Tools] > [Preferences] を選択します。

[Global Preferences] ダイアログボックスが表示されます。[Events] セクションの [Fetch events before] ドロップダウン リストに、現在のイベント最大経過時間が表示されます。

ステップ 2　[Fetch events before] ドロップダウン リストから、新しいイベント最大経過時間を選択します。

（注）　DCNM-LAN クライアントで過去のイベントをまったく取得しない場合は、イベント最大経過時間としてゼロ（0）を選択します。ゼロを選択すると、DCNM-LAN クライアントの起動後に DCNM-LAN サーバが受信したイベントだけが表示されます。

ステップ 3　[OK] をクリックします。

事前プロビジョニングの設定

事前プロビジョニングとは、管理対象デバイスに、イネーブルではないモードまたはプロトコルを設定することを意味します。事前プロビジョニングのプリファレンスは、DCNM-LAN クライアント インターフェイスの次のセクションに影響します。

- [Interfaces] > [Physical] > [Ethernet] > [Device] > [Slot] > [Interface]、[Port Details] タブ、[Port Mode Settings] セクション

  事前プロビジョニングをイネーブルにすると、[Mode] ドロップダウン リストの設定に関係なく、DCNM-LAN クライアントにすべてのポート モード フィールドが表示されます。事前プロビジョニングをディセーブルにすると、現在選択されているポート モードに関連するポート モード設定だけが表示されます。たとえば、事前プロビジョニングがディセーブルの場合、[Mode] ドロップダウン リストから [Trunk] を選択すると、トランク設定だけが表示され、[Access]、[PVLAN Host]、および [PVLAN Promiscuous] のフィールドは表示されません。

また、[Access VLAN] フィールドおよび [Native VLAN] フィールドを設定するダイアログボックスには、[Create in the Device] チェックボックスが含まれています。事前プロビジョニングをイネーブルにして、このチェックボックスをオフにすることにより、デバイスが現在設定されていない VLAN を参照するように、DCNM-LAN を設定できます。事前プロビジョニングがディセーブルの場合、このチェックボックスは必ずチェックされた状態になるため、指定した VLAN が存在しない場合、DCNM-LAN により、その VLAN が作成されます。

- [Switching] > [Spanning Tree] > [Device]、[Configuration] タブ、[Global Settings] セクション

  事前プロビジョニングをイネーブルにすると、[Protocol] ドロップダウン リストの設定に関係なく、DCNM-LAN クライアントに MST 設定が表示されます。事前プロビジョニングをディセーブルにすると、[Protocol] ドロップダウン リストから MST を選択しない限り、[MST Setting] フィールドは表示されません。

手順の詳細

ステップ 1　メニュー バーで、[Tools] > [Preferences] を選択します。

[Global Preferences] ダイアログボックスが表示されます。[Pre Provision] セクションに、[Pre Provision] チェックボックスが表示されます。

ステップ 2　次のどちらかを実行します。

- 事前プロビジョニングをイネーブルにするには、[Pre Provision] チェックボックスをオンにします。
- 事前プロビジョニングをディセーブルにするには、[Pre Provision] チェックボックスをオフにします。

ステップ 3　[OK] をクリックします。

オンライン ヘルプの使用方法

オンライン ヘルプには、次の機能があります。

- [Contents] : オンライン ヘルプ ウィンドウの [Contents] タブに、DCNM-LAN オンライン ヘルプの構成が表示されます。トピックにサブトピックがある場合は、目次のトピックの左側に本のアイコンが表示されます。

  目次のトピックごとに、内容を展開表示したり、閉じたりすることができます。全トピックを展開表示したり、閉じたりすることもできます。

- [Index] : DCNM-LAN オンライン ヘルプには索引が含まれています。アルファベット順で項目を検索し、索引から直接、関連トピックを表示できます。
- [Favorites] : DCNM-LAN オンライン ヘルプでは、[Favorites] タブに特定のトピックを追加できます。お気に入りの内容は、オンライン ヘルプにアクセスするコンピュータ上にローカルで保存されます。

オンライン ヘルプの Welcome ページにアクセスするには、メニュー バーで、[Help] > [Help Contents] を選択します。

DCNM-LAN オンライン ヘルプには、状況依存ヘルプが含まれています。

機能の状況依存ヘルプにアクセスする手順は、次のとおりです。

ステップ 1　DCNM-LAN クライアントの [Feature Selector] ペインで、特定の機能を選択します。たとえば、[Security] > [Access Control] > [IPv4 ACL] と選択します。

ステップ 2　次のどちらかを実行します。

- F1 を押します。
- ツールバーで、疑問符のアイコンをクリックします。

ブラウザ ウィンドウに、選択した機能のオンライン ヘルプが表示されます。DCNM-LAN クライアントを実行しているコンピュータ上のデフォルトのブラウザ アプリケーションが使用されます。

その他の関連資料

DCNM-LAN クライアントの使用に関する追加情報については、次を参照してください。

- 「関連資料」（P.14-19）
- 「標準」（P.14-19）

関連資料

関連項目	参照先
DCNM-LAN クライアントのインストールおよび起動	第 13 章「Cisco DCNM-LAN クライアントのインストールおよび起動」
DCNM-LAN の特定の機能の使用方法	「マニュアルの入手方法およびテクニカル サポート」（P.lxviii）

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN クライアントの使用の機能履歴

表 14-1 は、この機能のリリースの履歴です。

表 14-1　DCNM-LAN クライアントのインストールおよび起動の機能の履歴

機能名	リリース	機能情報
グローバル プリファレンス	5.0(2)	[Load history charts by default] チェックボックスのサポートが追加されました。
複数プラットフォームのサポート	5.0(2)	DCNM-LAN クライアントで異なる Cisco NX-OS デバイス タイプの管理をサポートする方法についての情報が追加されました。

CHAPTER 15

DCNM-LAN 認証設定の管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）の認証設定を管理する方法について説明します。

この章の内容は、次のとおりです。

- 「DCNM-LAN 認証設定の管理の概要」（P.15-1）
- 「DCNM-LAN 認証設定を管理するためのライセンス要件」（P.15-4）
- 「DCNM-LAN 認証設定を管理するための前提条件」（P.15-4）
- 「DCNM-LAN 認証設定の管理に関する注意事項と制約事項」（P.15-5）
- 「DCNM-LAN 認証の設定」（P.15-5）
- 「DCNM-LAN ローカル ユーザの表示」（P.15-12）
- 「認証サーバ設定の確認」（P.15-12）
- 「DCNM-LAN 認証設定のフィールドの説明」（P.15-13）
- 「その他の関連資料」（P.15-14）
- 「DCNM-LAN 認証設定の機能の履歴」（P.15-15）

DCNM-LAN 認証設定の管理の概要

DCNM-LAN 認証設定は、DCNM-LAN クライアントを使用してサーバにアクセスを試みるユーザを DCNM-LAN サーバが認証する方法を決定します。また、ユーザのユーザ ロールを決定します。これは、DCNM-LAN クライアントでユーザが設定できる内容に影響を与えます。

ここでは、次の内容について説明します。

- 「ユーザとユーザ ロール」（P.15-2）
- 「ローカル認証と DCNM-LAN ローカル ユーザ」（P.15-2）
- 「RADIUS および TACACS+ 認証」（P.15-2）
- 「RADIUS および TACACS+ によるユーザ ロールの割り当て」（P.15-3）
- 「ローカル認証へのフォールバック」（P.15-3）
- 「パスワード回復」（P.15-3）
- 「ユーザとデバイス クレデンシャル」（P.15-4）
- 「仮想化のサポート」（P.15-4）

ユーザとユーザ ロール

DCNM-LAN には、DCNM-LAN クライアントを使用して DCNM-LAN サーバにアクセスできるユーザを制御できるユーザベースのアクセスが実装されています。ユーザ アクセスはパスワードで保護されます。DCNM-LAN は強力なパスワードをサポートしています。

DCNM-LAN にアクセスするそれぞれの人が一意のユーザ アカウントを持つようにすることで、ユーザベースのアクセスにより、各ユーザが実行できる操作を決定できます。

また、DCNM-LAN では、各ユーザにロールを割り当てることができます。ロールは、DCNM-LAN クライアントでユーザが実行できる操作を決定します。表 15-1 に示すとおり、DCNM-LAN では 2 つのユーザ ロールがサポートされています。

表 15-1　DCNM-LAN のユーザ ロール

DCNM-LAN ロール	説明
User	• DCNM-LAN 認証モードを変更できません • DCNM-LAN ローカル ユーザ アカウントを追加または削除できません • 自身のローカル ユーザ アカウントの詳細を変更できます • その他の機能もすべて使用できます
Administrator	• DCNM-LAN 認証設定を完全に制御できます • その他の機能もすべて使用できます

ローカル認証と DCNM-LAN ローカル ユーザ

DCNM-LAN データベースには、作成するすべての DCNM-LAN ローカル ユーザが格納されます。

（注） DCNM-LAN サーバのユーザは、DCNM-LAN サーバにローカルです。DCNM-LAN サーバ ユーザを作成、変更、削除しても、管理対象デバイス上のユーザ アカウントには影響がありません。

DCNM-LAN サーバは、次の場合にローカル ユーザを使用してアクセスを許可します。

- 認証モードがローカルである場合
- 現在の認証モードの認証サーバに到達できない場合。

ローカル認証を第一の認証モードとして使用できます。RADIUS または TACACS+ を第一の認証モードとして指定し、現在の認証モードの認証サーバに到達できない場合、DCNM-LAN サーバはローカル認証にフォールバックします。

RADIUS および TACACS+ 認証

DCNM-LAN を、RADIUS または TACACS+ AAA プロトコルを使用してユーザを認証するように設定できます。

DCNM-LAN では、RADIUS と TACACS+ に対して、プライマリ、セカンダリ、およびターシャリ認証サーバがサポートされています。必須なのはプライマリ サーバだけです。各認証サーバに対し、サーバが認証要求を待ち受けるポート番号を指定できます。

認証の際、現在の認証モードのプライマリ サーバが認証要求に応答しない場合、DCNM-LAN サーバは認証要求をセカンダリ サーバに送信します。セカンダリ サーバが応答しない場合、DCNM-LAN は認証要求をターシャリ サーバに送信します。

現在の認証モードに対して設定されているサーバのどれも認証要求に応答しない場合、DCNM-LAN サーバはローカル認証にフォールバックします。

RADIUS および TACACS+ によるユーザ ロールの割り当て

DCNM-LAN は、RADIUS または TACACS+ サーバによるユーザ ロールの割り当てをサポートしています。ユーザ ロールは、DCNM-LAN クライアントにユーザ アクセスを許可します。ユーザに割り当てられるユーザ ロールは、DCNM-LAN クライアントの現在のセッションだけに影響を与えます。

DCNM-LAN ユーザ ロールを RADIUS によって割り当てるには、RADIUS のベンダー固有属性 26/9/1（Cisco-AV-Pair 属性）を返すように RADIUS サーバを設定します。DCNM-LAN ユーザ ロールを TACACS+ によって割り当てるには、TACACS+ サーバから cisco-av-pair の属性と値のペアが返される必要があります。認証応答でユーザ ロールが割り当てられない場合、DCNM-LAN によってユーザ ロールが割り当てられます。表 15-2 に、各 DCNM-LAN ユーザ ロールに対してサポートされる属性と値のペアの値を示します。

表 15-2　DCNM-LAN ユーザ ロールの割り当て値

DCNM-LAN ロール	RADIUS Cisco-AV-Pair の値	TACACS+ Shell Cisco 属性と値（AV）のペアの値
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

ローカル認証へのフォールバック

ローカル認証は、常に RADIUS および TACACS+ 認証モードのフォールバック手段になります。現在の認証モードに対して設定されているサーバのどれも使用できない場合、DCNM-LAN サーバは、ローカル データベースを使用してログイン要求を認証します。この動作により、DCNM-LAN からの意図しないロックアウトを回避できます。

フォールバック サポートが必要なユーザに対して、そのローカル ユーザ アカウントのユーザ名は、認証サーバのユーザ名と同じである必要があります。また、透過的なフォールバックのサポートを実現するために、ローカル ユーザ アカウントのパスワードも認証サーバ上のパスワードと同じにすることをお勧めします。ユーザは、認証サーバとローカル データベースのどちらで認証サービスが提供されているかを判断できないため、認証サーバとローカル データベースで異なるユーザ名とパスワードを使用すると、ユーザはどのユーザ名とパスワードを指定すべきかわからなくなります。

パスワード回復

DCNM-LAN クライアントに誰も DCNM-LAN Administrator ロールを持つユーザとしてログインできない場合、次のいずれかのスクリプトを使用してパスワードをリセットできます。

- Microsoft Windows の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.bat を使用します（デフォルトでは、*dcnm_root_directory* は c:¥Program Files¥Cisco Systems¥dcm¥dcnm¥bin です）。
- Linux の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.sh を使用します（デフォルトでは、*dcnm_root_directory* は /usr/local/cisco です）。

パスワードをリセットするには、使用しているオペレーティング システム用のスクリプトを実行し、リセットするユーザ ID とそのユーザ ID で使用するパスワードを入力します。

または、DCNM-LAN サーバを再インストールすることで、Administrator ロールに割り当てるローカル ユーザ アカウントのユーザ名とパスワードを指定できます。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

ユーザとデバイス クレデンシャル

ユーザがローカル ユーザ アカウントを使用して認証されるか、RADIUS または TACACS+ サーバ上のアカウントを使用して認証されるかにかかわらず、DCNM-LAN サーバの各ユーザには一意のデバイス クレデンシャルがあります。この機能により、DCNM-LAN サーバの各ユーザの操作が反映されたアカウンティング ログを管理対象デバイス上に保持できます。詳細については、「デバイスとクレデンシャルの概要」（P.17-1）を参照してください。

仮想化のサポート

Cisco NX-OS による仮想デバイス コンテキストのサポートは、DCNM-LAN サーバ ユーザに影響を及ぼしません。

DCNM-LAN サーバ ユーザは任意の管理対象デバイスを設定できます。

DCNM-LAN 認証設定を管理するためのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	Cisco DCNM-LAN 認証設定を管理するためにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM-LAN LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN 認証設定を管理するための前提条件

DCNM-LAN 認証設定の管理には次の前提条件があります。

- DCNM-LAN とともに使用するすべての認証サーバが、DCNM-LAN サーバからの認証要求を受け付けるように設定する必要があります。DCNM-LAN をクラスタ サーバ環境に展開している場合には、すべての認証サーバが、クラスタ内の各 DCNM-LAN サーバからの要求を受け付けるように設定します。
- DCNM-LAN ローカル ユーザを追加、削除、変更するには、DCNM-LAN の Administrator ロールに割り当てられたユーザ アカウントを使用して DCNM-LAN クライアントにログインする必要があります。

DCNM-LAN 認証設定の管理に関する注意事項と制約事項

DCNM-LAN 認証設定の管理における注意事項と制約事項は次のとおりです。

- DCNM-LAN クライアントを使用するユーザごとに DCNM-LAN ユーザ アカウントを作成します。複数の人でユーザ アカウントを共有しないようにします。
- 使用していない DCNM-LAN ユーザ アカウントは削除します。
- 管理者ユーザ アカウントは、DCNM-LAN クライアントで管理タスクを行う必要があるユーザだけに与えます。
- 強力なパスワードの使用を推奨します。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

DCNM-LAN 認証の設定

ここでは、次の内容について説明します。

- 「認証モードの設定」（P.15-5）
- 「DCNM-LAN ローカル ユーザの追加」（P.15-6）
- 「DCNM-LAN ローカル ユーザのパスワードの変更」（P.15-7）
- 「DCNM-LAN ローカル ユーザのフルネーム、ロール、説明の変更」（P.15-8）
- 「DCNM-LAN サーバ ユーザの削除」（P.15-8）
- 「認証サーバの追加」（P.15-9）
- 「認証サーバ設定の変更」（P.15-10）
- 「認証サーバの削除」（P.15-11）

認証モードの設定

DCNM-LAN サーバが DCNM-LAN クライアント ユーザを認証するために使用するモードを設定できます。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

RADIUS または TACACS+ 認証モードをイネーブルにする場合は、目的とする認証モードに対して認証サーバを 1 台以上設定する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Mode] セクションを展開します。

ステップ 3　認証モードを選択します。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

ステップ 5　DCNM-LAN サーバを再起動します。詳細については、第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。

DCNM-LAN ローカル ユーザの追加

DCNM-LAN ローカル ユーザ アカウントを追加できます。

（注）　DCNM-LAN ローカル ユーザ アカウントを追加しても、Cisco NX-OS デバイス上のユーザ アカウント設定は影響を受けません。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

新規の DCNM-LAN ローカル ユーザ アカウントのユーザ名とパスワードを決定します。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [Cisco DCNM Local Users] セクションに表示されます。

ステップ 3　メニュー バーで、[Actions] > [Add User] の順に選択します。

ユーザ リストの一番下に新規の行が表示されます。デフォルトでは、新規の行のすべてのフィールドは空白になっています。

ステップ 4　新規行の [DCNM User Name] 列にユーザ名を入力します。ユーザ名は 1 ～ 198 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 5　（任意）[Full Name] 列で、エントリをダブルクリックして、名前を追加します。たとえば、DCNM-LAN ローカル ユーザ アカウントを使用するユーザの本名を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 6　[DCNM Role] 列で、エントリをダブルクリックして、ロールを選択します。デフォルトのロールは「ユーザ」です。

ステップ 7　[Password] 列で、エントリをダブルクリックして、下矢印ボタンをクリックします。

ステップ 8　[New Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。パスワードは 1 ～ 255 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 9　[OK] をクリックします。

ステップ 10　（任意）[Description] 列で、エントリをダブルクリックして、ユーザ アカウントの説明を追加します。たとえば、この DCNM-LAN サーバ ユーザ アカウントを使用するユーザの電子メールや電話番号など、連絡先の詳細を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 11　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザのパスワードの変更

DCNM-LAN ローカル ユーザのパスワードを変更できます。

はじめる前に

自分が DCNM-LAN クライアントにログインするときに使用するアカウント以外のローカル ユーザ アカウントのパスワードを変更する場合は、Administrator ロールが必要です。ユーザ アカウントがローカル ユーザ アカウントで、User ロールが割り当てられている場合、自身のアカウントのパスワードだけを変更できます。

新規のパスワードを決定してください。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Server Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、変更するユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　[Password] 列で、エントリをダブルクリックして、下矢印ボタンをクリックします。

ステップ 5　[New Password] フィールドと [Confirm Password] フィールドに、新規のパスワードを入力します。パスワードは 1 ～ 255 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 6　[OK] をクリックします。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザのフルネーム、ロール、説明の変更

DCNM-LAN ローカル ユーザのフルネーム、ロール、説明を変更できます。

（注）　ユーザ名は変更できません。代わりに、使用するユーザ名を持つローカル ユーザ アカウントを追加して、使用しないユーザ名を持つローカル ユーザ アカウントを削除します。

はじめる前に

新しいフルネームまたは説明を決定してください。

自分が DCNM-LAN クライアントにログインするときに使用するローカル ユーザ アカウント以外のローカル ユーザ アカウントのフルネーム、ロール、または説明を変更する場合は、Administrator ロールが必要です。ユーザ アカウントがローカル ユーザ アカウントで、User ロールが割り当てられている場合、自身のアカウントのフルネームと説明だけを変更できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [Cisco DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、変更するローカル ユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　（任意）[Full Name] 列で、エントリをダブルクリックして新しい名前を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 5　（任意）[DCNM Role] 列で、エントリをダブルクリックして、新規ロールを選択します。「管理者」または「ユーザ」を選択できます。

ステップ 6　（任意）[Description] 列で、エントリをダブルクリックして、ユーザ アカウントの説明を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN サーバ ユーザの削除

DCNM-LAN ローカル ユーザ アカウントを削除できます。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

削除しようとしている DCNM-LAN ローカル ユーザ アカウントが正しいことを確認してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、削除するユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　メニュー バーで、[Actions] > [Delete User] の順に選択します。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバの追加

RADIUS および TACACS+ サーバを DCNM-LAN 認証設定に追加できます。

はじめる前に

（注）　DCNM-LAN とともに使用するすべての認証サーバが、DCNM-LAN サーバからの認証要求を受け付けるように設定する必要があります。DCNM-LAN をクラスタ サーバ環境に展開している場合には、すべての認証サーバが、クラスタ内の各 DCNM-LAN サーバからの要求を受け付けるように設定します。

追加する各認証サーバについて次の情報を入手してあることを確認します。

- AAA プロトコル：RADIUS または TACACS+
- サーバの IPv4 アドレスまたは DCNM-LAN サーバが解決できる DNS 名。
- 秘密キー。
- サーバが認証要求を受け付けるポート番号。
- （RADIUS 限定）サーバがアカウンティング メッセージを受け付けるポート番号。
- 認証プロトコル：PAP、CHAP、MSCHAP、ASCII。
- （任意）サーバ確認用の、サーバ上の有効なユーザ アカウントのユーザ名とパスワード。

サーバをプライマリ、セカンダリ、ターシャリ サーバのどれにするかを決定します。これは、認証サーバのフェールオーバー戦略に依存します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　追加する各認証サーバに対し、次の手順を実行します。

a. サーバを追加する行を選択します。

（注） プライマリ サーバを追加しないとセカンダリ サーバを追加できません。また、セカンダリ サーバを追加しないとターシャリ サーバを追加できません。

b. [Server Name] フィールドをダブルクリックし、サーバの IPv4 アドレスまたは DNS ホスト名を入力します。

（注） DCNM-LAN サーバが解決できないホスト名を入力すると、[Server Name] フィールドが赤く強調表示されます。

c. [Secret Key] フィールドをダブルクリックし、認証サーバの秘密キー（共有秘密キーとも呼びます）を入力します。

d. （任意）デフォルトの [Authentication Port] または [Accounting Port]（RADIUS 限定）を変更する必要がある場合は、該当するポート フィールドをダブルクリックし、新しいポート番号を入力します。

e. [Authentication Method] フィールドをダブルクリックし、DCNM-LAN から認証サーバに認証要求を送信するときに使用する認証プロトコルを選択します。

ステップ 5　（任意）DCNM-LAN サーバが新しい認証サーバを使用してユーザを認証できることを確認するには、次の手順を実行します。

a. 確認する認証サーバの行の右にある [Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

b. 認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

c. [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバ設定の変更

DCNM-LAN クライアントで設定済みの認証サーバの設定を変更できます。複数の RADIUS または TACACS+ サーバがある場合、どのサーバをプライマリ、セカンダリ、ターシャリにするかを変更できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　（任意）認証サーバの設定を変更する場合は、変更する各フィールドをダブルクリックし、変更内容を入力します。

ステップ 5　（任意）RADIUS または TACACS+ サーバの順序を変更する場合は、サーバを右クリックし、[Move Up] または [Move Down] のいずれかを選択します。

ステップ 6　（任意）DCNM-LAN サーバが認証サーバを使用してユーザを認証できることを確認するには、次の手順を実行します。

a. 確認する認証サーバの行の右にある [Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

b. 認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

c. [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバの削除

RADIUS または TACACS+ の認証サーバを DCNM-LAN 認証設定から削除できます。

はじめる前に

現在の認証モードのすべての認証サーバの削除はできません。代わりに、まず認証モードを変更し、次にすべての認証サーバを削除します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　削除する認証サーバを右クリックし、[Remove Server] を選択します。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザの表示

DCNM-LAN サーバのユーザ アカウントを表示するには、[Feature Selector] ペインで [DCNM Server Administration] > [DCNM Authentication Settings] の順に選択し、必要に応じて [Cisco DCNM Local Users] セクションを展開します。

[Contents] ペインに、DCNM-LAN サーバ ユーザ アカウント（ユーザ名と説明を含む）が表示されます。パスワードはセキュリティ保護のためマスクされて表示されます。表示される各フィールドの詳細については、「DCNM-LAN 認証設定のフィールドの説明」（P.15-13）を参照してください。

認証サーバ設定の確認

設定した特定の認証サーバを使用して、DCNM-LAN サーバがユーザを認証できることを確認できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　[Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

ステップ 4　認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

ステップ 5　確認する認証サーバの行の右にある [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

DCNM-LAN 認証設定のフィールドの説明

ここでは、DCNM-LAN 認証設定機能における次の各フィールドについて説明します。

- 「[Authentication Mode] セクション」（P.15-13）
- 「[DCNM-LAN Local Users] セクション」（P.15-13）
- 「[Authentication Servers] セクション」（P.15-14）

[Authentication Mode] セクション

表 15-3　[Authentication Mode] セクション

フィールド	説明
Local	DCNM-LAN がローカル ユーザ データベースだけを使用してユーザを認証するかどうか。
RADIUS	DCNM-LAN が RADIUS サーバを使用してユーザを認証するかどうか。設定されている RADIUS サーバが到達不能な場合、DCNM-LAN はローカル データベースを使用したユーザ認証にフォールバックします。
TACACS+	DCNM-LAN が TACACS+ サーバを使用してユーザを認証するかどうか。設定されている TACACS+ サーバが到達不能な場合、DCNM-LAN はローカル データベースを使用したユーザ認証にフォールバックします。

[DCNM-LAN Local Users] セクション

表 15-4　[DCNM-LAN Local Users] セクション

フィールド	説明
DCNM-LAN User Name	*表示のみ*。DCNM-LAN サーバ ユーザ アカウントの名前。この名前は、認証モードがローカルの場合か、現在の認証モードの認証サーバが到達不能である場合に、DCNM-LAN クライアントにログインするために使用できます。大文字と小文字は区別されます。すべての数字、記号、文字を使用できます。最小長は 1 文字、最大長は 198 文字です。
Full Name	ユーザ アカウントの他の名前（DCNM-LAN サーバ ユーザ アカウントを使用するユーザの名前など）。この名前は、DCNM-LAN クライアントにログインするときには使用できません。すべての数字、記号、文字を使用できます。最大長は 255 文字です。デフォルトでは、このフィールドはブランクです。
DCNM-LAN Role	ユーザ アカウントのロール。「ユーザ」または「管理者」のいずれかを指定できます。詳細については、表 15-1 を参照してください。デフォルトでは、DCNM-LAN サーバ ユーザ アカウントに User ロールが割り当てられます。
Password	DCNM-LAN サーバ ユーザのパスワード。このフィールドはセキュリティ保護のため、常にマスクされます。大文字と小文字は区別されます。すべての数字、記号、文字を使用できます。最小長は 1 文字、最大長は 255 文字です。

表 15-4　[DCNM-LAN Local Users] セクション （続き）

フィールド	説明
Description	DCNM-LAN サーバ ユーザの説明。すべての数字、記号、文字を使用できます。最大長は 255 文字です。デフォルトでは、このフィールドはブランクです。

[Authentication Servers] セクション

表 15-5　[Authentication Servers] セクション

フィールド	説明
Server Name	認証サーバの DNS 名または IPv4 アドレス。 • DNS 名：DNS 名を指定した場合、DCNM-LAN サーバがサーバの IP アドレスを解決できる必要があります。有効な DNS 名の文字は英数字です。 • IPv4 アドレス：IP アドレスを指定する場合、有効なエントリはドット付き 10 進表記です。
Secret Key	認証サーバの共有秘密キー。有効なエントリは、文字（大文字と小文字を区別）、数字、記号です。
Authentication Port	認証サーバが認証要求を待ち受ける TCP または UDP ポート番号。デフォルトでは、RADIUS サーバの認証ポートは UDP ポート 1812、TACACS+ サーバの認証ポートは TCP ポート 49 です。
Accounting Port	RADIUS 認証サーバが認証要求を待ち受ける UDP ポート番号。デフォルトでは、RADIUS サーバのアカウンティング ポートは UDP ポート 1813 です。
Authentication Method	DCNM-LAN サーバが、認証サーバへの認証要求で使用する認証プロトコル。サポートされる認証方式は次のとおりです。 • PAP • CHAP • MSCHAP • ASCII

その他の関連資料

DCNM-LAN 認証設定の管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.15-15）
- 「標準」（P.15-15）

関連資料

関連項目	参照先
DCNM-LAN クライアントへのログイン	*「DCNM-LAN クライアントの起動」（P.14-8）*

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN 認証設定の機能の履歴

表 15-6 は、この機能のリリースの履歴です。

表 15-6　DCNM-LAN サーバ ユーザの機能の履歴

機能名	リリース	機能情報
DCNM-LAN 認証設定	5.0(2)	リリース 4.2 からの変更はありません。

CHAPTER 16

デバイス ディスカバリの管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）のデバイス ディスカバリ機能の管理方法について説明します。

この章の内容は、次のとおりです。

- 「デバイス ディスカバリの概要」（P.16-1）
- 「デバイス ディスカバリのライセンス要件」（P.16-5）
- 「デバイス ディスカバリの前提条件」（P.16-6）
- 「デバイス ディスカバリの注意事項と制約事項」（P.16-6）
- 「デバイス ディスカバリの実行」（P.16-7）
- 「デバイス ディスカバリ タスクのステータスの表示」（P.16-11）
- 「関連情報」（P.16-12）
- 「デバイス ディスカバリのフィールドの説明」（P.16-12）
- 「デバイス システム メッセージのログ レベルの参考情報」（P.16-13）
- 「デバイス ディスカバリに関するその他の関連資料」（P.16-17）
- 「デバイス ディスカバリ機能の履歴」（P.16-18）

デバイス ディスカバリの概要

ここでは、次の内容について説明します。

- 「デバイス ディスカバリ」（P.16-2）
- 「ディスカバリ プロトコル」（P.16-2）
- 「クレデンシャルとディスカバリ」（P.16-3）
- 「ディスカバリ プロセス」（P.16-3）
- 「Cisco NX-OS システム メッセージのロギング要件」（P.16-3）
- 「ログ レベル自動設定のサポート」（P.16-4）
- 「VDC のサポート」（P.16-5）

デバイス ディスカバリ

デバイス ディスカバリ機能では、Cisco NX-OS デバイスに接続し、実行コンフィギュレーションなどのデータをデバイスから取得して、DCNM-LAN にデバイスを作成します。DCNM-LAN は、最初のデバイスのネイバーである Cisco NX-OS デバイスおよびネットワーク サーバも検出します。これらのデバイスは*シード デバイス*と呼ばれています。

デバイスが仮想デバイス コンテキスト（VDC）をサポートしている場合、DCNM-LAN は物理デバイスに設定された各 VDC の実行コンフィギュレーションを取得します。DCNM-LAN は、各 VDC（デフォルトの VDC を含む）をデバイスとして表示します。Cisco NX-OS デバイスにデフォルトの VDC しか存在しない場合は、デバイス ディスカバリによって DCNM-LAN にデバイスが 1 つだけ作成されます。

デバイスに接続してその設定を取得する際、DCNM-LAN は XML 管理インターフェイスを使用します。このインターフェイスでは、セキュア シェル（SSH）上で動作する XML ベースの Network Configuration Protocol（NETCONF）を使用します。詳細については、『*Cisco NX-OS XML Interface User Guide*』を参照してください。

ディスカバリ プロトコル

DCNM-LAN はさまざまなプロトコルを使用して、データセンター ネットワーク内のデバイスおよびサーバを検出します。ここでは、次の内容について説明します。

- 「Cisco Discovery Protocol」（P.16-2）
- 「リンク層検出プロトコル」（P.16-2）
- 「ファイバ チャネル」（P.16-3）

Cisco Discovery Protocol

デバイス ディスカバリでは、ディスカバリ プロセスで Cisco Discovery Protocol（CDP）を使用して、初期デバイスに接続するデバイスを検索します。CDP では、データリンク層を介して隣接デバイス間で情報を交換します。こうして交換された情報によって、ネットワーク トポロジ、および論理レイヤまたは IP レイヤの下層にある物理コンフィギュレーションが確認されます。

CDP を使用すると、DCNM-LAN のディスカバリ プロセスで、シード デバイスから 1 ホップ以上離れたデバイスを検出できます。デバイス ディスカバリ機能を使用してディスカバリ プロセスを開始する際には、ディスカバリ プロセスで探索するホップ カウントを制限できます。

DCNM-LAN は、CDP を使用して Cisco NX-OS デバイスを検出したあと、そのデバイスに接続して、デバイスの実行コンフィギュレーションなどの情報を取得します。収集した情報を使用して、DCNM-LAN はそのデバイスを管理できます。

DCNM-LAN は、Cisco IOS ソフトウェアを実行している一部の Cisco スイッチ上で CDP ホップをサポートしています。DCNM-LAN ではこれらのデバイスを管理できませんが、トポロジ機能を使用することで、管理対象外のデバイス、および管理対象外デバイスと管理対象デバイス間の CDP リンクを確認できます。

リンク層検出プロトコル

デバイス ディスカバリは、Link Layer Discovery Protocol（LLDP）を使用して、Cisco NX-OS デバイスに接続されているサーバのネットワーク アダプタを検出します。詳細については、第 20 章「ネットワーク サーバの設定」を参照してください。

ファイバ チャネル

DCNM-LAN は、ストレージ エリア ネットワーク（SAN）内のネットワーク エレメントの検出にファイバ チャネルを使用します。DCNM-LAN は、SAN のスイッチ、サーバ、およびストレージ アレイを検出できます。

クレデンシャルとディスカバリ

デバイス ディスカバリを実行するには、シード デバイスのユーザ アカウントで使用されているユーザ名とパスワードを入力する必要があります。Cisco NX-OS デバイスの検出を正常に行うには、指定したユーザ アカウントが、network-admin ロールまたは vdc-admin ロールのいずれかに割り当てられている必要があります。

シード デバイスから 1 ホップ以上離れたデバイスを検出する場合は、ホップ経路上のすべてのデバイスに、同じユーザ名とパスワードを使用したユーザ アカウントを設定しておく必要があります。ホップ経路上のすべての Cisco NX-OS デバイスでは、そのユーザ アカウントを、network-admin ロールまたは vdc-admin ロールに割り当てる必要があります。

ディスカバリ プロセス

DCNM-LAN は、次のように、いくつかのフェーズを経てデバイスを検出します。

1. CDP ネイバー探索：シード デバイスから順に、ディスカバリ開始時に指定した CDP ホップ カウント分離れたデバイスまで、相互接続されたデバイスのトポロジを検出します。
2. サポート対象デバイスの選択：検出されたデバイスのうち、DCNM-LAN でサポートされているデバイスを判別します。サポートされているデバイスに対してだけディスカバリが続行されます。
3. コンポーネント ディスカバリ：前フェーズで選択したデバイスのコンポーネントを検出します。たとえば、デバイスが Cisco Nexus 7000 シリーズ スイッチの場合、コンポーネント ディスカバリでは、スーパーバイザ モジュール、I/O モジュール、電源装置、ファンが見つかります。デバイスが Cisco Nexus 1000V スイッチの場合、コンポーネント ディスカバリでは、仮想スーパーバイザ モジュールおよび仮想イーサネット モジュールが見つかります。
4. デバイス コンフィギュレーション ディスカバリ：インターフェイス、アクセス コントロール リスト、VLAN など、各デバイス上の機能設定の詳細情報を検出します。
5. ネットワーク ディスカバリ：前フェーズで検出したデバイス コンフィギュレーションの詳細情報とネットワーク機能を関連付けます。

Cisco NX-OS システム メッセージのロギング要件

DCNM-LAN は、デバイスを監視および管理するために、管理対象デバイスから取得するシステム メッセージを部分的に使用します。ここでは、DCNM-LAN で Cisco NX-OS デバイスを管理および監視するために、すべての Cisco NX-OS デバイスが事前に満たすべきシステム メッセージの要件について説明します。

ここでは、次の内容について説明します。

- 「インターフェイス リンク ステータス イベントのロギング要件」（P.16-4）
- 「ログファイルの要件」（P.16-4）
- 「ロギング重大度レベルの要件」（P.16-4）

インターフェイス リンク ステータス イベントのロギング要件

インターフェイス リンク ステータス変更イベントに関するシステム メッセージをロギングするように、デバイスを設定する必要があります。この要件は、DCNM-LAN がインターフェイス リンク ステータスの変更情報を確実に受信できるようにするためのものです。デバイス上の実行コンフィギュレーションに、次の 2 つのコマンドが設定されている必要があります。

- **logging event link-status enable**
- **logging event link status default**

これらのコマンドをデバイス上に確実に設定するには、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）の手順を実行します。

ログファイルの要件

重大度レベル 6 以下のシステム メッセージがログ ファイルに保存されるように、デバイスを設定する必要があります。

ログ ファイルには任意の名前を指定できますが、ログ ファイル名は変更しないことを推奨します。ログ ファイル名を変更すると、以前のシステム メッセージは消去されます。ログ ファイルのデフォルト名は「messages」です。

デフォルトのログ ファイル名を使用する場合は、デバイスの実行コンフィギュレーションに次のコマンドを設定する必要があります。

logging logfile messages 6

このコマンドをデバイス上に確実に設定するには、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）の手順を実行します。

ロギング重大度レベルの要件

DCNM-LAN では、一部の Cisco NX-OS ロギング ファシリティに対し、重大度レベルの最小要件が設定されています。Cisco NX-OS 上でイネーブルにされた機能はすべて、デフォルトのログ レベルが設定されます。DCNM-LAN に必要なログ レベルはロギング ファシリティによって異なりますが、多くの場合、Cisco NX-OS のデフォルトのログ レベルよりも高くなります。詳細については、「ログ レベル自動設定のサポート」（P.16-4）を参照してください。

ログ レベル自動設定のサポート

DCNM-LAN は、サポートされているすべての Cisco NX-OS リリースに対し、ログ レベル自動設定をサポートします（Cisco Nexus 7000 シリーズ スイッチ上だけで使用可能な Cisco NX-OS Release 4.0 を除く）。ここでは、DCNM-LAN によるログ レベル自動設定のサポート方法について説明します。Cisco NX-OS Release 4.0 のログ レベルの手動設定については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

デバイス ディスカバリ実行時

デバイス ディスカバリの実行中、検出したデバイスのログ レベルがそのロギング ファシリティのログ レベル最小要件よりも低いことがわかると、DCNM-LAN は最小要件を満たすためにログ レベルを引き上げます。ログ レベルが要件以上の場合、DCNM-LAN がディスカバリの実行中にログ レベルを変更することはありません。

DCNM-LAN クライアントでの機能のイネーブル化時

ユーザが DCNM-LAN クライアントを使用してデバイスの機能をイネーブルにし、その機能のデフォルトのログ レベルが最小要件を満たしていない場合、DCNM-LAN クライアントは警告を発行して、要件を満たすためにデバイスのログ レベルを設定することを通知します。ユーザがログ レベルの変更を拒否すると、DCNM-LAN は機能をイネーブル化しません。

管理対象デバイスとの自動同期化時

コマンドライン インターフェイス（CLI）などの他の手段を使用して管理対象デバイスの機能をイネーブルにし、その機能のデフォルトのログ レベルが最小要件を満たしていない場合、DCNM-LAN は機能がイネーブルになったことを検出したあと、要件を満たすためにログ レベルを自動的に設定します。

CLI または他の方法を使用してログ レベルを DCNM-LAN の最小要件よりも低くした場合、DCNM-LAN はログ レベルの変更を検出したあと、そのデバイスの状態を「Unmanaged」に変更します。この状態になった場合は、デバイスとクレデンシャル機能により、ログ レベルが原因でデバイスが管理対象外になっていることが表示されます。デバイスとクレデンシャル機能を使用して、デバイスを再検出できます。再検出時に、DCNM-LAN は最小要件よりも低いログ レベルを設定します。

VDC のサポート

DCNM-LAN は、VDC をサポートする Cisco NX-OS デバイスを検出すると、Cisco NX-OS デバイス上の VDC の数を調べます。DCNM-LAN では、各 VDC を個別のデバイスとして扱います。各 VDC のステータスは別々に追跡されるため、同じ Cisco NX-OS デバイス上の VDC はそれぞれ、他の VDC とは独立させて設定できます。

デフォルト以外の VDC が存在する Cisco Nexus 7000 シリーズ デバイスを検出するには、各 VDC がディスカバリの前提条件を満たしていることを事前に確認しておきます。詳細については、「デバイス ディスカバリの前提条件」（P.16-6）を参照してください。

デバイス ディスカバリのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM-LAN	デバイス ディスカバリ機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイス ディスカバリの前提条件

デバイス ディスカバリを実行する前に、次の機能について理解しておく必要があります。

- VDC（Cisco Nexus 7000 シリーズのデバイス ディスカバリを実行する場合）。
- CDP

デバイス ディスカバリ機能には次の前提条件があります。

- DCNM-LAN サーバが検出対象のデバイスに接続できること。
- Cisco NX-OS デバイスが、Cisco NX-OS のサポートされているリリースを実行していること。Cisco NX-OS のサポートされているリリースの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
- Cisco NX-OS デバイスが、デバイス ディスカバリを正常に完了するために必要な最小構成を備えていること。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。
- Cisco Nexus 7000 シリーズ デバイスの場合、検出する各 VDC に管理インターフェイスが設定されている必要があります。DCNM-LAN は、管理インターフェイスである mgmt0 インターフェイス（アウトオブバンドの仮想インターフェイス）、または VDC に割り当てられたインバンドのイーサネット インターフェイスが設定されている VDC の検出をサポートしています。
- CDP ネイバーであるデバイスを DCNM-LAN で検出できるようにするには、CDP を各デバイスでグローバルにイネーブルにし、さらに、デバイス ディスカバリに使用するデバイス インターフェイスでも CDP を明示的にイネーブルにする必要があります。Cisco Nexus 7000 シリーズ デバイスの場合、各 VDC、および各 VDC に使用するように設定された管理インターフェイス上で、CDP をグローバルにイネーブルにする必要があります。
- ネットワーク サーバのディスカバリでは、ネットワーク サーバに接続されたデバイス上でグローバルに LLDP をイネーブルにし、さらに、ネットワーク サーバのネットワーク アダプタに接続されたデバイス インターフェイス上で明示的に LLDP をイネーブルにする必要があります。

デバイス ディスカバリの注意事項と制約事項

デバイス ディスカバリ機能における設定時の注意事項と制約事項は次のとおりです。

- 検出対象の Cisco NX-OS デバイスが検出用に準備されていることを確認します。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。
- DCNM-LAN は、Cisco NX-OS を実行しているデバイスだけを管理できます。サポート対象デバイスのオペレーティング システムおよびサポート対象デバイスのハードウェアについては、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
- CDP ベースのデバイス ディスカバリを行うには、CDP ホップ経路上のすべてのデバイスが、シード デバイスで指定したものと同じユーザ名とパスワードを使用している必要があります。セキュリティ上の方針で、各デバイスに同じユーザ名とパスワードを使用できない場合は、それぞれのデバイスに対して個別にデバイス ディスカバリを実行できます。
- CDP ホップ上に存在するが、Cisco IOS ソフトウェアを実行していないデバイスは、トポロジ機能には表示されますが、DCNM-LAN で管理することはできません。

デバイス ディスカバリの実行

ここでは、次の内容について説明します。

- 「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）
- 「デバイスの検出」（P.16-9）
- 「デバイスの再検出」（P.16-10）

Cisco NX-OS デバイスのディスカバリ準備状態の確認

DCNM-LAN でデバイス ディスカバリを実行する前に、DCNM-LAN で管理および監視する各 Cisco NX-OS デバイス上で、次の手順を実行する必要があります。この手順により、デバイス ディスカバリを正常に実行し、DCNM-LAN で効率的にデバイスを管理および監視できるようになります。

（注） 仮想デバイス コンテキスト（VDC）をサポートする物理デバイスを準備している場合は、DCNM-LAN が各 VDC をそれぞれ 1 台のデバイスと見なすことに留意してください。DCNM-LAN で管理および監視する各 VDC について、ディスカバリの準備状態を確認する必要があります。

手順の詳細

ステップ 1　Cisco NX-OS デバイスの CLI にログインします。

ステップ 2　**configure terminal** コマンドを使用して、グローバル コンフィギュレーション モードを開始します。

ステップ 3　セキュア シェル（SSH）接続が成功するように、RSA キーまたは DSA キーが存在することを確認します。この確認には、**show ssh key rsa** コマンドまたは **show ssh key dsa** コマンドを使用します。

キーを生成する必要がある場合は、**ssh key** コマンドを使用します。

（注） キーを生成するには、事前に SSH サーバをディセーブルにする必要があります。これを実行するには、**no feature ssh** コマンドを使用します。

ステップ 4　SSH サーバがイネーブルであることを確認します。この確認には、**show ssh server** コマンドを使用します。

SSH サーバがイネーブルではない場合は、**feature ssh** コマンドを使用してイネーブルにします。

ステップ 5　CDP がグローバルにイネーブル化されていること、および DCNM-LAN がデバイスへの接続に使用するインターフェイス上でも CDP がイネーブルであることを確認します。CDP がイネーブルかどうかを確認するには、**show run cdp all** コマンドを使用します。

ステップ 6　**logging event link-status default** および **logging event link-status enable** コマンドが設定されていることを確認します。

```
switch(config)# show running-config all | include "logging event link-status"
logging event link-status default
logging event link-status enable
```

設定されていない場合は、いずれかのコマンドを入力して、実行コンフィギュレーションに追加します。

（注）　デフォルトの Cisco NX-OS コンフィギュレーションには、**logging event link-status enable** コマンドが含まれています。**show running-config** コマンドでは、**all** キーワードを使用した場合だけ、デフォルト設定が表示されます。

ステップ 7　デバイスに、重大度 6 以下のシステム メッセージのロギングが設定されていることを確認します。

（注）　ログ ファイルのデフォルト名は「messages」ですが、デバイスに現在設定されているログ ファイル名を使用することを推奨します。ログ ファイル名を変更すると、以前のシステム メッセージは消去されます。

```
switch(config)# show running-config all | include logfile
logging logfile logfile-name 6
```

logging logfile コマンドが出力されない場合、または重大度レベルが 6 より小さい場合は、**logging logfile** コマンドを設定します。

```
switch(config)# logging logfile logfile-name 6
```

ステップ 8　デバイスが Cisco NX-OS Release 4.0 を実行している Cisco Nexus 7000 シリーズ スイッチの場合は、デバイスのログ レベル設定が DCNM-LAN ログ レベルの要件を満たしていることを手動で確認する必要があります。これには、次の手順を実行します。

a.　デバイス上でイネーブルに設定されているデフォルト以外の機能を特定します。

```
switch(config)# show running-config | include feature
feature feature1
feature feature2
feature feature3
.
.
.
```

b.　デバイスに現在設定されているログ レベルを表示します。**show logging level** コマンドでは、イネーブルに設定されている機能のログ レベルだけが表示されます。[Current Session Severity] 列に現在のログ レベルが一覧表示されます。

```
switch(config)# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       5
aclmgr                  3                       3
.
.
.
```

（注）　単一のロギング ファシリティのログ レベルを確認する場合は、**show logging level aaa** のように、ファシリティ名を指定して **show logging level** コマンドを使用できます。

c.　どのデバイスのログ レベルが DCNM-LAN ログ レベルの最小要件よりも低く設定されているかを判別します。これを実行するには、（P.16-8）で表示されたログ レベルと、表 16-2 に示した DCNM-LAN ログ レベルの最小要件を比較します。

d.　ログ レベルが DCNM-LAN ログ レベルの最小要件よりも低く設定されている各ロギング ファシリティについて、ログ レベルが DCNM-LAN の要件以上になるようにデバイスを設定します。

```
switch(config)# logging level facility severity-level
```

facility 引数には、表 16-2 の対応するロギング ファシリティ キーワードを指定し、*severity-level* 引数には、対応する DCNM-LAN ログ レベルの最小要件以上の値（最大 7）を指定します。

e. **show logging level** コマンドを使用して、設定の変更を確認します。

ステップ 9　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コピーし、変更を保存します。

```
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

デバイスの検出

1 つ以上のデバイスを検出できます。ディスカバリ タスクが正常に終了すると、DCNM-LAN は検出された Cisco NX-OS デバイスの実行コンフィギュレーションとステータス情報を取得します。

ここで示す手順（デバイスの検出）は、次の目的に使用してください。

- 現在 DCNM-LAN によって管理されていないデバイスを検出する場合。たとえば、新規インストールのあとなど、DCNM-LAN がデバイスを 1 台も検出していない場合には、この手順を実行する必要があります。
- DCNM-LAN ですでに検出済みのデバイスは再検出せずに、ネットワークに新しく追加したデバイスだけを検出する場合。
- CDP リンクが変更されたとき、DCNM-LAN ですでに検出済みのデバイスは再検出せずに、トポロジを再検出する場合。

（注）　DCNM-LAN を使用して Cisco NX-OS デバイスを設定するには、事前にその Cisco NX-OS デバイスを正常に検出しておく必要があります。

はじめる前に

DCNM-LAN サーバが Cisco NX-OS デバイスに接続して正常に検出できるように、Cisco NX-OS デバイスが設定されていることを確認します。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

ディスカバリ タスクを開始したとき、DCNM-LAN を最初に接続するデバイスの IPv4 アドレスを確認します。このデバイスが、そのディスカバリのシード デバイスになります。

シード デバイスの CDP ネイバーを検出するかどうかを確認します。検出する場合は、ディスカバリ プロセスによる探索の対象となる、シード デバイスからの最大ホップ カウントを決定してください。

（注）　ネイバー デバイスにシード デバイスと同じクレデンシャルが設定されている場合だけ、ディスカバリ プロセスはネイバーを完全に検出できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Discovery] の順に選択します。

[Contents] ペインの [Discovery Tasks] 領域にディスカバリ タスクが表示されます。

ステップ 2　[Seed Device] フィールドに、ディスカバリ タスクを開始したときに DCNM-LAN を最初に接続するデバイスの IPv4 アドレスを入力します。ドット付き 10 進形式で入力します。

ステップ 3　[User Name] フィールドに、デバイスに定義されているユーザ アカウントのユーザ名を入力します。入力するユーザ アカウントは、network-admin または vdc-admin のいずれかのロールに割り当てられている必要があります。

ステップ 4　[Password] フィールドに、[User Name] フィールドに、入力したユーザ アカウントのパスワードを入力します。

Catalyst 6500 デバイスの場合は、IOS 特権 EXEC モード コマンドを実行できるように、[Enable Password] フィールドにイネーブル パスワードを入力します。

ステップ 5　（任意）DCNM-LAN でシード デバイスの CDP ネイバーを検出する場合は、[Maximum Hops of Neighbors to Discover] フィールドに、使用する最大ホップ カウントを入力します。デフォルトの最大ホップ カウントは 0（ゼロ）です。

ステップ 6　[Rediscover Configuration and Status for Existing Devices] チェックボックスがオフになっていることを確認します。デフォルトでは、このチェックボックスはオフになっています。

このチェックボックスをオフにしておくと、デバイスの実行コンフィギュレーションとステータス情報を取得しなくても、CDP ホップとして以前検出されたデバイスを DCNM-LAN でそのまま使用できます。

ステップ 7　[Start Discovery] をクリックします。

少し経つと、[Discovery Tasks] 領域のタスク一覧の最下部にディスカバリ タスクが表示されます。タスクのステータスは定期的に更新されます。

ステップ 8　タスクのステータスが「Successful（成功）」になるまで待ちます。この処理は数分かかることがあります。

ステータスが「Successful」になったら、DCNM-LAN を使用して、検出されたデバイスを設定および監視できます。

変更内容を保存する必要はありません。

デバイスの再検出

1 つ以上のデバイスを再検出できます。

（注）　再検出を行うと、DCNM-LAN が保持している Cisco NX-OS デバイスのコンフィギュレーション データが、再検出によって取得されたコンフィギュレーション データで置換されます。すでに検出済みのデバイスのコンフィギュレーションおよびステータス情報を取得せずに、1 つ以上のデバイスを検出する必要がある場合は、「デバイスの検出」（P.16-9）を参照してください。

DCNM-LAN を使用して Cisco NX-OS デバイスを設定するには、事前にその Cisco NX-OS デバイスを正常に検出しておく必要があります。

はじめる前に

DCNM-LAN サーバが接続できるように、Cisco NX-OS デバイスが設定されていることを確認します。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Discovery] の順に選択します。

[Contents] ペインの [Discovery Tasks] 領域にディスカバリ タスクとそのステータスが表示されます。

ステップ 2　[Seed Device] フィールドに、ディスカバリ タスクを開始したときに DCNM-LAN を最初に接続するデバイスの IPv4 アドレスを入力します。ドット付き 10 進形式で入力します。

ステップ 3　[User Name] フィールドに、デバイスに定義されているユーザ アカウントのユーザ名を入力します。入力するユーザ アカウントは、network-admin または vdc-admin のいずれかのロールに割り当てられている必要があります。

ステップ 4　[Password] フィールドに、[User Name] フィールドに、入力したユーザ アカウントのパスワードを入力します。

Catalyst 6500 デバイスの場合は、IOS 特権 EXEC モード コマンドを実行できるように、[Enable Password] フィールドにイネーブル パスワードを入力します。

ステップ 5　（任意）DCNM-LAN でシード デバイスの CDP ネイバーを再検出する場合は、[Maximum Hops of Neighbors to Discover] フィールドに、使用する最大ホップ カウントを入力します。デフォルトの最大ホップ カウントは 0（ゼロ）です。

ステップ 6　[Rediscover Configuration and Status for Existing Devices] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

このチェックボックスをオンにすると、DCNM-LAN は、以前に検出したデバイスに関して保持しているすべてのコンフィギュレーションおよびステータス情報を、デバイスから取得した実行コンフィギュレーションおよびステータス情報で置換します。

ステップ 7　[Start Discovery] をクリックします。

少し経つと、[Discovery Tasks] 領域のタスク一覧の最下部にディスカバリ タスクが表示されます。タスクのステータスは定期的に更新されます。

ステップ 8　タスクのステータスが「Successful（成功）」になるまで待ちます。この処理は数分かかることがあります。

ステータスが「Successful」になったら、DCNM-LAN を使用して、検出されたデバイスを設定および監視できます。

変更内容を保存する必要はありません。

デバイス ディスカバリ タスクのステータスの表示

デバイス ディスカバリ タスクのステータスを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [Device Discovery] の順に選択します。

[Contents] ペインの [Discovery Tasks] 領域に、タスクとタスク ステータスが表示されます。表示される各フィールドの詳細については、「デバイス ディスカバリのフィールドの説明」（P.16-12）を参照してください。

関連情報

検出されたデバイスを表示し、必要に応じて、一意なデバイス クレデンシャルを設定します。詳細については、「デバイスとクレデンシャルの管理」（P.17-1）を参照してください。

デバイス ディスカバリのフィールドの説明

ここでは、デバイス ディスカバリ機能の次の各フィールドについて説明します。

- 「デバイス ディスカバリの [Contents] ペイン」（P.16-12）
- 「関連フィールド」（P.16-13）

デバイス ディスカバリの [Contents] ペイン

表 16-1　デバイス ディスカバリの [Contents] ペイン

フィールド	説明
Discovery Setting	
Seed Device	検出する最初のデバイスの IPv4 アドレス。ドット付き 10 進形式で入力します。デフォルトでは、このフィールドは空白です。
User Name	DCNM-LAN サーバがデバイスへのアクセスに使用するデバイス ユーザ アカウントの名前。入力するユーザ アカウントは、デバイスの network-admin または vdc-admin のいずれかの権限を保持している必要があります。デフォルトでは、このフィールドは空白です。
Password	[User Name] フィールドに、指定したデバイス ユーザ アカウントのパスワード。デフォルトでは、このフィールドは空白です。
Enable Password	Catalyst 6500 デバイスのイネーブル パスワード。IOS 特権 EXEC モード コマンドの実行を可能にします。
Maximum Hops of Neighbors to Discover	DCNM-LAN サーバとデバイス間で許容される最大 CDP ホップ カウント。サーバがデバイスに接続していてもこのホップ カウントを超えると、ディスカバリは失敗します。デフォルトの設定は 0（つまり、ネイバー デバイスのディスカバリはディセーブル）です。
Rediscover Configuration and Status for Existing Devices	設定中のディスカバリ タスクで、完了済みの既存のデバイス ディスカバリを置換するかどうかを指定します。デフォルトでは、このチェックボックスはオフになっています。
Discovery Tasks	
Task ID	*表示のみ。*ディスカバリ タスクに割り当てられる番号。タスク ID は、ディスカバリ タスクが起動される順序を示します。
Owner	*表示のみ。*ディスカバリ タスクを開始するときに使用する DCNM-LAN サーバのユーザ アカウント。
Seed Device IP Address	*表示のみ。*シード デバイスの IPv4 アドレス。
Discovered Time	*表示のみ。*[Status] フィールドの最終更新日時。
Reason	*表示のみ。*ディスカバリ タスクが作成された理由。

表 16-1　デバイス ディスカバリの [Contents] ペイン （続き）

フィールド	説明
Status	*表示のみ*。ディスカバリ タスクの状態。有効な値は、次のとおりです。 • [In progress]：ディスカバリ タスクが継続中。 • [Successful]：ディスカバリ タスクが正常に終了。 • [Failed]：ディスカバリ タスクでエラーが発生。

関連フィールド

デバイスを設定するための各フィールドの詳細については、「デバイスとクレデンシャルの管理」（P.17-1）を参照してください。

デバイス システム メッセージのログ レベルの参考情報

ここでは、DCNM-LAN のデバイス ログ レベルの最小要件ついて説明します。DCNM-LAN では、サポートされているデバイスのロギング ファシリティのサブセットに対してだけ、ログ レベルの要件が設定されています。Cisco NX-OS のロギング ファシリティがここで明記されていない場合、DCNM-LAN にはそのロギング ファシリティに対する要件はありません。

（注）　DCNM-LAN は自動デバイス ログ レベルをサポートしています。詳細については、「ログ レベル自動設定のサポート」（P.16-4）を参照してください。

次のトピックでは、サポートされているデバイス タイプごとに DCNM-LAN ログ レベルの最小要件を説明します。

- 「DCNM-LAN 機能別 Cisco Nexus 7000 NX-OS ログ レベル」（P.16-14）
- 「DCNM-LAN 機能別 Cisco Nexus 5000 NX-OS ログ レベル」（P.16-15）
- 「DCNM-LAN 機能別 Cisco Nexus 4000 NX-OS ログ レベル」（P.16-16）
- 「DCNM-LAN 機能別 Cisco Nexus 1000V NX-OS ログ レベル」（P.16-17）

DCNM-LAN 機能別 Cisco Nexus 7000 NX-OS ログ レベル

表 16-2　Cisco DCNM-LAN 機能別 Cisco Nexus 7000 NX-OS ログ レベル

Cisco DCNM-LAN 機能	Cisco Nexus 7000 NX-OS ロギング ファシリティ	デフォルトのイネーブル設定	ロギング ファシリティ キーワード	Cisco NX-OS デフォルト ログ レベル	Cisco DCNM-LAN ログ レベルの最小要件[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
トポロジ	LLDP	No	lldp	2	**5**
DHCP スヌーピング	DHCP スヌーピング	No	dhcp	2	**6**
ダイナミック ARP インスペクション					
IP ソース ガード					
Dot1X	802.1X	No	dot1x	2	**5**
イーサネット インターフェイス	イーサネット ポート マネージャ	Yes	ethpm	5	5
トラフィック ストーム制御					
Gateway Load Balancing Protocol（GLBP）	GLBP	No	glbp	3	**6**
ホット スタンバイ ルータ プロトコル（HSRP）	HSRP エンジン	No	hsrp	3	**6**
インベントリ	モジュール	Yes	module	5	5
	プラットフォーム	Yes	platform	5	5
	システム マネージャ	Yes	sysmgr	3	3
オブジェクト トラッキング	オブジェクト トラッキング	Yes	track	3	**6**
ポートチャネル インターフェイス	ポートチャネル インターフェイス	Yes	port-channel	5	**6**
ポート セキュリティ	ポート セキュリティ	No	port-security	2	**5**
SPAN	SPAN	Yes	monitor	3	**6**
スパニング ツリー	スパニング ツリー	Yes	spanning-tree	3	**6**
Unidirectional Link Detection（UDLD; 単一方向リンク検出）	UDLD	No	udld	5	5
仮想デバイス コンテキスト（VDC）	VDC マネージャ	Yes	vdc_mgr	6	6
Virtual Port Channel（vPC; 仮想ポートチャネル）	VPC	No	vpc	2	**6**
VLAN ネットワーク インターフェイス	インターフェイス VLAN	No	interface-vlan	2	**5**

1. Cisco Nexus 7000 NX-OS ロギング ファシリティのデフォルトのログ レベルが極端に低い場合、Cisco DCNM-LAN の最小ログ レベルは**太字**で表記されています。

DCNM-LAN 機能別 Cisco Nexus 5000 NX-OS ログ レベル

表 16-3　Cisco DCNM-LAN 機能別 Cisco Nexus 5000 NX-OS ログ レベル

Cisco DCNM-LAN 機能	Cisco Nexus 5000 NX-OS ロギング ファシリティ	デフォルトのイネーブル設定	ロギング ファシリティ キーワード	Cisco NX-OS デフォルト ログ レベル	Cisco DCNM-LAN ログ レベルの最小要件[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
トポロジ	LLDP	No	lldp	2	**5**
イーサネット インターフェイス	イーサネット ポート マネージャ	Yes	ethpm	5	5
トラフィック ストーム制御					
ファブリック エクステンダ	FEX	Yes	fex	5	5
インベントリ	システム マネージャ	Yes	sysmgr	3	3
	プラットフォーム	Yes	pfm	5	5
	NOHMS	Yes	nohms	2	2
ポートチャネル インターフェイス	ポートチャネル インターフェイス	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
スパニング ツリー	スパニング ツリー	Yes	spanning-tree	3	**6**
Unidirectional Link Detection（UDLD; 単一方向リンク検出）	UDLD	No	udld	5	5
仮想ポート チャネル	VPC	No	vpc	2	**6**
VLAN ネットワーク インターフェイス	インターフェイス VLAN	No	interface-vlan	2	**5**

1. Cisco Nexus 5000 NX-OS ロギング ファシリティのデフォルトのログ レベルが極端に低い場合、Cisco DCNM-LAN の最小ログ レベルは**太字**で表記されています。

DCNM-LAN 機能別 Cisco Nexus 4000 NX-OS ログ レベル

表 16-4　Cisco DCNM-LAN 機能別 Cisco Nexus 4000 NX-OS ログ レベル

Cisco DCNM-LAN 機能	Cisco Nexus 4000 NX-OS ロギング ファシリティ	デフォルトのイネーブル設定	ロギング ファシリティ キーワード	Cisco NX-OS デフォルト ログ レベル	Cisco DCNM-LAN ログ レベルの最小要件[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
トポロジ					
イーサネット インターフェイス	イーサネット ポート マネージャ	Yes	ethpm	5	5
トラフィック ストーム制御					
FIP スヌーピング	FIPSM	Yes	fip-snooping	2	**5**
インベントリ	システム マネージャ	Yes	sysmgr	3	3
リンクステート トラッキング	LST	No	lstsvc	2	**4**
ポートチャネル インターフェイス	ポートチャネル インターフェイス	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
スパニング ツリー	スパニング ツリー	Yes	spanning-tree	3	**6**
Unidirectional Link Detection（UDLD; 単一方向リンク検出）	UDLD	No	udld	5	5
VLAN ネットワーク インターフェイス	インターフェイス VLAN	No	interface-vlan	2	**5**

1. Cisco Nexus 4000 NX-OS ロギング ファシリティのデフォルトのログ レベルが極端に低い場合、Cisco DCNM-LAN の最小ログ レベルは**太字**で表記されています。

DCNM-LAN 機能別 Cisco Nexus 1000V NX-OS ログ レベル

表 16-5　Cisco DCNM-LAN 機能別 Cisco Nexus 1000V NX-OS ログ レベル

Cisco DCNM-LAN 機能	Cisco Nexus 1000V NX-OS ロギング ファシリティ	デフォルトのイネーブル設定	ロギング ファシリティ キーワード	Cisco NX-OS デフォルト ログ レベル	Cisco DCNM-LAN ログ レベルの最小要件[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery トポロジ	CDP	Yes	cdp	2	**6**
イーサネット インターフェイス	イーサネット ポート マネージャ	Yes	ethpm	5	5
仮想イーサネット インターフェイス	Ifmgr	Yes	ifmgr	5	5
	VIM	Yes	vim	5	5
インベントリ	モジュール	Yes	module	5	5
	プラットフォーム	Yes	platform	5	5
	システム マネージャ	Yes	sysmgr	3	3
仮想スイッチ	MSP	Yes	msp	5	5
ポートチャネル インターフェイス	ポートチャネル インターフェイス	Yes	port-channel	5	**6**
ポート プロファイル	ポート プロファイル	Yes	port-profile	5	5
	VMS	Yes	vms	5	5
SPAN	SPAN	Yes	monitor	3	**6**

1. Cisco Nexus 1000V NX-OS ロギング ファシリティのデフォルトのログ レベルが極端に低い場合、Cisco DCNM-LAN の最小ログ レベルは**太字**で表記されています。

デバイス ディスカバリに関するその他の関連資料

デバイス ディスカバリに関連する追加情報については、次を参照してください。

- 「関連資料」（P.16-17）
- 「標準」（P.16-18）

関連資料

関連項目	参照先
デバイスとクレデンシャル	第 17 章「デバイスとクレデンシャルの管理」

関連項目	参照先
ネットワーク サーバ	第 20 章「ネットワーク サーバの設定」
Cisco NX-OS XML 管理インターフェイス	『*Cisco NX-OS XML Interface User Guide*』

標準

標準	タイトル
Secure Shell（SSH; セキュア シェル）上の NETCONF プロトコル	RFC 4742

デバイス ディスカバリ機能の履歴

表 16-6 は、この機能のリリースの履歴です。

表 16-6　デバイス ディスカバリ機能の履歴

機能名	リリース	機能情報
LLDP ディスカバリ	5.0(2)	この機能のサポートが追加されました。
ファイバ チャネル ディスカバリ	5.0(2)	この機能のサポートが追加されました。
ログ レベル自動設定のサポート	5.0(2)	この機能のサポートが追加されました。

CHAPTER 17

デバイスとクレデンシャルの管理

この章では、Cisco NX-OS デバイス、および Cisco Data Center Network Manager for LAN（DCNM-LAN）サーバが各デバイスに対して自己認証するために使用するクレデンシャルの管理方法について説明します。

この章の内容は、次のとおりです。

- 「デバイスとクレデンシャルの概要」（P.17-1）
- 「デバイスとクレデンシャル機能のライセンス要件」（P.17-3）
- 「デバイスとクレデンシャル機能を管理するための前提条件」（P.17-3）
- 「デバイスとクレデンシャル機能の注意事項と制約事項」（P.17-3）
- 「デバイスとクレデンシャル機能の設定」（P.17-3）
- 「デバイス クレデンシャルとステータスの表示」（P.17-9）
- 「デバイスとクレデンシャル機能の各フィールドの説明」（P.17-11）
- 「デバイスとクレデンシャル機能のその他の関連資料」（P.17-11）
- 「デバイスとクレデンシャル機能の履歴」（P.17-12）

デバイスとクレデンシャルの概要

ここでは、次の内容について説明します。

- 「デバイス」（P.17-1）
- 「クレデンシャル」（P.17-2）
- 「デバイスのステータス」（P.17-2）
- 「VDC のサポート」（P.17-2）

デバイス

デバイスとクレデンシャル機能により、デバイスの管理状態を管理できます。管理対象の物理デバイスが仮想デバイス コンテキスト（VDC）をサポートする場合、DCNM-LAN は、各 VDC をデバイスとして表します。複数の VDC を持つ物理デバイス上の単一 VDC の実行コンフィギュレーションおよびステータス情報を取得する必要がある場合は、物理デバイス上のすべての VDC に対してデバイス ディスカバリを実行する代わりに、デバイスとクレデンシャル機能を使用して、変更された VDC を表す単一のデバイスを再検出できます。

クレデンシャル

デバイスとクレデンシャル機能では、管理対象の各デバイスを異なるクレデンシャルで保護する機能をサポートしています。DCNM-LAN では、検出したデバイスごとに一意なクレデンシャルを設定できます。また、デバイスに一意なクレデンシャルを設定しない場合にデフォルトのクレデンシャルを使用することもできます。一部の管理対象デバイスだけが同じクレデンシャルを共有している場合は、一部のデバイスに一意なクレデンシャルを設定し、一部の管理対象デバイスで共有されているクレデンシャルをデフォルトのクレデンシャルとして設定します。

デバイスとクレデンシャル機能は、一意のデバイス クレデンシャル セットを各 DCNM-LAN サーバ ユーザに関連付けます。これにより、管理対象デバイス上のアカウンティング ログに各 DCNM-LAN サーバ ユーザの操作が反映されます。デバイス クレデンシャルが設定されていないユーザとして DCNM-LAN クライアントにログインすると、そのユーザ アカウント用のデバイス クレデンシャルを設定するように DCNM-LAN クライアントから要求されます。

アカウント機能のサポートを重視していない組織でも、DCNM-LAN サーバの各ユーザにはデバイス クレデンシャルを設定する必要があります。その際、各ユーザに指定するクレデンシャルは同じでもかまいません。

デバイスのステータス

デバイスとクレデンシャル機能では、各デバイスのステータスが表示されます。表示されるステータスは次のとおりです。

- Managed（管理対象）：DCNM-LAN はセキュア シェル（SSH）を使用してデバイスに接続して、デバイスの実行コンフィギュレーションを設定し、デバイスからログなどのデータを取得できます。このステータスが表示されるのは、Cisco NX-OS のサポートされているリリースを実行しており、DCNM-LAN によるディスカバリをサポートするように正しく設定されているデバイスだけです。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。
- Unmanaged（管理対象外）：DCNM はデバイスの管理、またはデバイスのステータスの監視を行いません。
- Unreachable（到達不能）：DCNM からデバイス（到達不能になる前に管理対象だったデバイス）に接続できません。このステータスには次の原因が考えられます。
  - ネットワーク障害のため、DCNM-LAN サーバがデバイスにアクセスできない。
  - SSH がデバイス上でディセーブルになっている。
  - デバイス上のすべての端末ラインが使用中である。

VDC のサポート

VDC をサポートするデバイスの場合、DCNM-LAN は、物理デバイス上の各 VDC を個別のデバイスとして扱います。これにより、デバイス上の各 VDC に一意なクレデンシャルを用意できます。また、DCNM-LAN は各 VDC のステータスも個別に追跡します。

デバイスとクレデンシャル機能のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	デバイスとクレデンシャル機能にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイスとクレデンシャル機能を管理するための前提条件

デバイスとクレデンシャル機能でデバイス ディスカバリを実行するには、次の前提条件を満たしている必要があります。

- DCNM-LAN サーバが検出対象のデバイスに接続できること。
- Cisco NX-OS デバイスが、Cisco NX-OS のサポートされているリリースを実行していること。Cisco NX-OS のサポートされているリリースの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
- Cisco NX-OS デバイスが、デバイス ディスカバリを正常に完了するために必要な最小構成を備えていること。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

デバイスとクレデンシャル機能の注意事項と制約事項

デバイスとクレデンシャル機能における設定上の注意事項と制約事項は次のとおりです。

- デバイスとクレデンシャル機能を使用したデバイス ディスカバリでは、CDP ベースのネイバー ディスカバリはサポートされていません。CDP ベースのディスカバリを使用する方法については、「デバイス ディスカバリの管理」（P.16-1）を参照してください。
- デフォルトのクレデンシャルやデバイス固有のクレデンシャルを変更する場合は慎重に行ってください。クレデンシャルが間違っていると、DCNM-LAN がデバイスを管理できなくなります。

デバイスとクレデンシャル機能の設定

ここでは、次の内容について説明します。

- 「デバイスの追加」（P.17-4）
- 「デバイスの検出」（P.17-4）
- 「デバイスの非管理対象化」（P.17-5）
- 「デバイスの削除」（P.17-6）
- 「デフォルトのデバイス クレデンシャルの設定」（P.17-6）
- 「デフォルトのデバイス クレデンシャルの消去」（P.17-7）
- 「デバイスの一意なクレデンシャルの設定」（P.17-8）

- 「デバイスの一意なクレデンシャルの消去」（P.17-9）

デバイスの追加

デバイスを追加できます。デバイスを追加した後、デバイスを検出できます。詳細については、「デバイスの検出」（P.17-4）を参照してください。

はじめる前に

デバイスの IPv4 アドレスを確認します。

DCNM-LAN がデフォルトのデバイス クレデンシャルを使用しているデバイスと通信できるかどうか、または DCNM-LAN にデバイスを追加するとき一意なデバイス クレデンシャルを追加する必要があるかどうかを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　メニュー バーで、[Actions] > [New Device] の順に選択します。

[Contents] ペインの [Devices] 領域に空白行が表示されます。

ステップ 3　新規デバイスの [IP Address] 列に、DCNM-LAN がそのデバイスに接続するときに使用する必要のある IPv4 アドレスを入力します。

ステップ 4　Enter を押します。

ステップ 5　（任意）一意なデバイス クレデンシャルを追加する必要がある場合は、[User Credentials] 列で、追加したデバイスのエントリをダブルクリックし、下矢印ボタンをクリックして、一意なデバイス クレデンシャルを設定します。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

新規デバイスのステータスは「Unmanaged」です。

デバイスの検出

デバイスを検出できます。

管理対象外のデバイスを検出すると、ステータスが「Managed」に変わります。検出中、DCNM-LAN はデバイスの実行コンフィギュレーションを取得します。

デバイスを再検出すると、DCNM-LAN が取得するコンフィギュレーション データで、デバイスの既存のコンフィギュレーション データが置換されます。DCNM-LAN が保持しているデバイスのコンフィギュレーション データが正しくない場合は（たとえば、デバイス管理者がコマンドライン インターフェイスを使用して実行コンフィギュレーションを変更した場合など）、この手順を使用して、DCNM-LAN が保持しているデバイスのコンフィギュレーション データを更新できます。

（注）　デバイスを検出しても、そのデバイスの実行コンフィギュレーションは影響を受けません。

はじめる前に

一意のデバイス クレデンシャルを使用してデバイス エントリを設定していること、または DCNM-LAN がデフォルトのデバイス クレデンシャルを使用してデバイスに接続できることを確認してください。詳細については、「デフォルトのデバイス クレデンシャルの設定」（P.17-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　検出するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Discover] の順に選択します。

デバイス ディスカバリが開始されます。デバイスのステータスが「Discovering（検出中）」に変わります。

ステップ 4　ステータスが「Managed」に変わるまで待ちます。

通常は、5 分未満でデバイス ディスカバリが行われます。ステータスが「Managed」に変わったら、DCNM-LAN を使用してデバイスを設定できます。

変更内容を保存する必要はありません。

デバイスの非管理対象化

デバイスのステータスを「Unmanaged」にすることができます。

はじめる前に

ステータスを変更するデバイスを正しく選択していることを確認してください。DCNM-LAN は管理対象外デバイスの実行コンフィギュレーションを制御できません。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　ステータスを「Unmanaged」に変更するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Unmanage] の順に選択します。

少し経つと、デバイスのステータスが「Unmanaged」に変わります。

変更内容を保存する必要はありません。

デバイスの削除

デバイスを削除できます。デバイスを削除すると、そのデバイスに関するすべてのコンフィギュレーション データが DCNM-LAN から削除されます。

DCNM-LAN で管理するつもりのないデバイスは削除することを検討する必要があります。また、VDC をサポートするデバイスのネットワーク管理者がデバイスのコマンドライン インターフェイスを使用して VDC を削除する場合は、その VDC を表しているデバイスを DCNM-LAN から削除する必要があります。

（注）　デバイスを削除しても、そのデバイスの実行コンフィギュレーションは影響を受けません。

はじめる前に

削除対象のデバイスを正しく選択していることを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　削除するデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Delete] の順に選択します。

[Devices] 領域からデバイスが消去されます。

変更内容を保存する必要はありません。

デフォルトのデバイス クレデンシャルの設定

デフォルトのクレデンシャルを設定できます。デフォルトのクレデンシャルは、検出された Cisco NX-OS デバイスに対して接続するとき、DCNM-LAN がデバイスに対して自身を認証するために使用します。DCNM-LAN は、一意なデバイス クレデンシャルが設定されていない検出済みの各デバイスと通信するとき、デフォルトのデバイス クレデンシャルを使用します。

（注）　デバイス クレデンシャルは、DCNM-LAN サーバのユーザごとに一意です。

はじめる前に

デフォルトのデバイス クレデンシャルの内容を確認します。DCNM-LAN がデフォルトのクレデンシャルを使用して通信するすべての Cisco NX-OS デバイスには、DCNM-LAN に設定するデフォルトのクレデンシャルと同じユーザ名とパスワードが設定されたネットワーク管理者アカウントを定義しておく必要があります。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペイン内の [Devices] 領域の上の [Default Credentials] 領域に、検出済みのデバイスの一覧が表示されます。

ステップ 2　[User Name] フィールドに、デフォルトのクレデンシャルのユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 28 文字のユーザ名をサポートしています。

ステップ 3　[Password] フィールドの右側にある下矢印ボタンをクリックします。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、デフォルトのクレデンシャルのパスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 64 文字のパスワードをサポートしています。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デフォルトのデバイス クレデンシャルの消去

デフォルトのデバイス クレデンシャルを消去できます。

（注）　デフォルトのデバイス クレデンシャルを消去すると、各管理対象デバイスに一意なクレデンシャルを設定していない限り、DCNM-LAN は検出済みのデバイスに接続できなくなります。

はじめる前に

デフォルトのデバイス クレデンシャルなしで DCNM-LAN を使用する場合は、次の手順を実行する前に、検出済みの各デバイスに一意なデバイス クレデンシャルが設定されていることを確認する必要があります。詳細については、「デバイスの一意なクレデンシャルの設定」（P.17-8）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペイン内の [Devices] 領域の上の [Default Credentials] 領域に、検出済みのデバイスの一覧が表示されます。

ステップ 2　[Default Credentials] 領域で、[Clear] をクリックします。

[User Name] フィールドと [Password] フィールドが消去されます。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイスの一意なクレデンシャルの設定

検出済みのデバイスに一意なクレデンシャルを設定できます。検出済みのデバイスに一意なクレデンシャルが存在する場合、DCNM-LAN は、デフォルトのデバイス クレデンシャルではなく一意なクレデンシャルを使用してそのデバイスに接続します。

（注）　デバイス クレデンシャルは、DCNM-LAN サーバのユーザごとに一意です。

はじめる前に

検出済みのデバイスに設定されているネットワーク管理者用ユーザ アカウントのユーザ名とパスワードを確認します。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　デバイスの [User Credentials] 列で、入力値をダブルクリックして、下矢印ボタンをクリックします。

ステップ 3　[User Name] フィールドに、ユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 28 文字のユーザ名をサポートしています。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

（注）　Cisco NX-OS では、最大 64 文字のパスワードをサポートしています。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイスの一意なクレデンシャルの消去

検出済みデバイスの一意なクレデンシャルを消去できます。

（注）　検出済みデバイスの一意なクレデンシャルを消去すると、DCNM-LAN はデフォルトのクレデンシャルを使用してデバイスに接続するようになります。

はじめる前に

一意なデバイス クレデンシャルなしで DCNM-LAN を運用する場合は、次の手順を実行する前に、DCNM-LAN にデフォルトのデバイス クレデンシャルが設定されていることを確認する必要があります。詳細については、「デフォルトのデバイス クレデンシャルの設定」（P.17-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Devices] 領域に検出済みのデバイスが表示されます。

ステップ 2　デバイスの [User Credentials] 列で、入力値をダブルクリックして、下矢印ボタンをクリックします。

ステップ 3　[User Name] フィールドのテキストをすべて削除します。

ステップ 4　[Password] フィールドのテキストをすべて削除します。

ステップ 5　[Confirm Password] フィールドのテキストをすべて削除します。

ステップ 6　[OK] をクリックします。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デバイス クレデンシャルとステータスの表示

デバイスのステータス、およびデバイスにクレデンシャルが設定されているかどうかを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [Devices and Credentials] の順に選択します。

[Contents] ペインの [Default Credentials] 領域に、デフォルトのクレデンシャルが表示されます。クレデンシャルとステータスなど、デバイスに関する情報は、[Contents] ペインの [Devices] 領域に表示されます。

[Reason] フィールドに、デバイスのステータスを解説する簡単なメッセージが表示されます。次の表に、メッセージによって示される問題の解決方法に関する情報を示します。

理由	解決方法
Success	該当なし。DCNM-LAN がデバイスを管理しています。
Authentication failure（認証失敗）	デバイスのクレデンシャルが正しいことを確認します。DCNM-LAN がデバイスに到達可能であることを確認します。
Unsupported platform（サポート対象外のプラットフォーム）	デバイスがサポートされているプラットフォームであること、そのプラットフォームでサポートされているリリースの Cisco NX-OS を実行していることを確認します。サポートされているプラットフォームおよび Cisco NX-OS リリースの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。
Device sync up failure（デバイスの同期化失敗）	Cisco Nexus 7000 シリーズ デバイス用。アカウント機能およびシステム メッセージのログ メッセージの連番の形式が適切ではありません。デバイス上のログ ファイルを消去し、デバイスを再検出します。
Unmanaged manually（手動による非管理対象化）	DCNM-LAN ユーザがデバイスのステータスを「Unmanaged」に変更しました。デバイスを再検出します。
Error when executing database query（データベース クエリー実行時のエラー）	デバイスを再検出します。エラーが再度発生する場合は、DCNM-LAN データベースをクリーンアップします。データベースのクリーンアップの詳細については、第 29 章「Cisco DCNM-LAN データベースのメンテナンス」を参照してください。
Auto synchronization for device is disabled by user（ユーザによるデバイスの自動同期化のディセーブル化）	デバイスを再検出します。
Logging levels required by DCNM-LAN are not configured on the device（DCNM-LAN に必要なログ レベルがデバイスに設定されていない）	デバイスを再検出します。詳細については、「ログ レベル自動設定のサポート」（P.16-4）を参照してください。
Error in SSH connection（SSH 接続のエラー）	デバイスで SSH がイネーブルになっていること、SSH が適切に機能していることを確認します。デバイスを再検出します。
Unreachable（到達不能）	デバイスの正しい IP アドレスを指定していることを確認します。DCNM-LAN がデバイスにアクセスできることを確認します。デバイスを再検出します。
Discovery failed because server node stopped/crashed（サーバ ノードの停止またはクラッシュによるディスカバリの失敗）	デバイスを再検出します。
Syslog messages logging disabled on device（デバイスでの Syslog メッセージ ロギングのディセーブル化）	デバイスを再検出します。

表示される各フィールドの詳細については、「デバイスとクレデンシャル機能の各フィールドの説明」（P.17-11）を参照してください。

デバイスとクレデンシャル機能の各フィールドの説明

ここでは、デバイスとクレデンシャルの次の各フィールドについて説明します。

- 「デバイスとクレデンシャルの [Contents] ペイン」（P.17-11）

デバイスとクレデンシャルの [Contents] ペイン

表 17-1　デバイスとクレデンシャルの [Contents] ペイン

フィールド	説明
Default Credentials	
User Name	DCNM-LAN サーバが検出または管理しているデバイスへのアクセスに使用する Cisco NX-OS デバイス ユーザ アカウントの名前。デバイス上でこのユーザ アカウントに、network-admin ロールまたは vdc-admin ロールが割り当てられている必要があります。デフォルトでは、このフィールドは空白です。 **（注）** [Default Credentials] セクションの情報は、[Devices] 領域の [User Credentials] フィールド内の情報によって上書きされます。
Password	[User Name] フィールドに、指定した Cisco NX-OS デバイス ユーザ アカウントのパスワード。デフォルトでは、このフィールドは空白です。
Devices	
IP Address	*表示のみ。*Cisco NX-OS デバイスの IPv4 アドレス。
Name	*表示のみ。*Cisco NX-OS デバイスの名前。
User Credentials	DCNM-LAN が Cisco NX-OS デバイスに接続するときに使用する Cisco NX-OS ユーザ アカウント。 **（注）** このフィールドを設定すると、DCNM-LAN は、デバイスに接続するとき、指定したユーザ アカウントを使用します。このフィールドが空白の場合、DCNM-LAN は、[Default Credentials] 領域に指定されたユーザ アカウントを使用します。デフォルトでは、このフィールドは空白です。
Status	*表示のみ。*DCNM-LAN サーバがデバイスに対して接続および設定できるかどうかを示します。有効な値は、次のとおりです。 • [Managed] : DCNM-LAN サーバはデバイスを設定できます。 • [Unmanaged] : DCNM-LAN サーバはデバイスを設定できません。 • [Unreachable] : DCNM-LAN サーバはデバイスに到達できません。
Reason	*表示のみ。*デバイスのステータスに関する簡単な説明が表示されます。詳細については、「デバイス クレデンシャルとステータスの表示」（P.17-9）を参照してください。

デバイスとクレデンシャル機能のその他の関連資料

デバイスとクレデンシャル機能に関する追加情報については、次のセクションを参照してください。

- 「関連資料」（P.17-12）

- 「標準」（P.17-12）

関連資料

関連項目	参照先
Cisco NX-OS XML 管理インターフェイス	『*Cisco NX-OS XML Interface User Guide*』

標準

標準	タイトル
Secure Shell（SSH; セキュア シェル）上の NETCONF プロトコル	RFC 4742

デバイスとクレデンシャル機能の履歴

表 17-2 は、この機能のリリースの履歴です。

表 17-2　デバイスとクレデンシャル機能の履歴

機能名	リリース	機能情報
[Reason] フィールド	5.0(2)	デバイスとクレデンシャル機能に [Reason] フィールドが追加されました。

CHAPTER 18

DCNM-LAN ライセンス デバイスの管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）ライセンス デバイス機能を使用する方法について説明します。

この章の内容は、次のとおりです。

- 「DCNM-LAN ライセンス デバイスの概要」（P.18-1）
- 「DCNM-LAN ライセンス デバイス管理のライセンス要件」（P.18-2）
- 「DCNM-LAN ライセンス デバイス管理の前提条件」（P.18-2）
- 「DCNM-LAN ライセンス デバイス管理の注意事項と制約事項」（P.18-2）
- 「DCNM-LAN ライセンス デバイスの設定」（P.18-2）
- 「DCNM-LAN ライセンス デバイスの表示」（P.18-4）
- 「DCNM-LAN ライセンス デバイスのフィールドの説明」（P.18-4）
- 「その他の関連資料」（P.18-5）
- 「DCNM-LAN ライセンス デバイスの機能の履歴」（P.18-6）

DCNM-LAN ライセンス デバイスの概要

DCNM-LAN ライセンス デバイス機能を使用すると、ライセンス済み DCNM-LAN 機能を使用して管理できる物理デバイスを制御できます。この機能では、ライセンス済みデバイス リストを保持します。デバイスがこのリストに含まれていれば、そのデバイス上でライセンス済み DCNM-LAN 機能を管理できます。

ライセンスには、ライセンスでサポートされている数までデバイスを追加できます。たとえば、2 つの LAN エンタープライズ ライセンスをインストールした場合、それぞれが 5 つのデバイスをサポートしていれば、ライセンス済みデバイス リストに合計 10 のデバイスを追加できます。

ライセンス済みデバイス リストからデバイスを削除して、別のデバイスで置換することもできます。

ライセンス済みデバイス リストに追加されていないデバイスを DCNM-LAN ライセンス済み機能を使用して設定しようとしても、DCNM-LAN クライアントでは、その機能を使用してライセンスされていないデバイスを設定できません。

DCNM-LAN ライセンス デバイス管理のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	DCNM-LAN ライセンス デバイスには Enterprise LAN ライセンスが必要です。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN ライセンス デバイス管理の前提条件

DCNM-LAN ライセンス デバイスを管理するには、次の前提条件を満たしている必要があります。

- 1 つ以上の LAN エンタープライズ ライセンスがインストールされていること。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
- DCNM-LAN ライセンス デバイスのリストに追加するデバイスが検出されていること。詳細については、「デバイスの検出」（P.16-9）を参照してください。

DCNM-LAN ライセンス デバイス管理の注意事項と制約事項

DCNM-LAN ライセンス デバイス管理における設定時の注意事項と制約事項は次のとおりです。

- ライセンス済みデバイス リストに追加できるのは管理対象デバイスだけです。
- ライセンス済みデバイス リストには、インストールされているすべての LAN エンタープライズ ライセンスによって許可されている合計数までデバイスを追加できます。
- ライセンス済みデバイス リストからデバイスを削除すると、そのデバイスは DCNM-LAN から削除されます。その物理デバイスが仮想デバイス コンテキスト（VDC）をサポートする場合、デバイス上のすべての VDC が DCNM-LAN から削除されます。削除したデバイスの管理を再開するには、そのデバイスを検出する必要があります。詳細については、「デバイスの検出」（P.16-9）を参照してください。

DCNM-LAN ライセンス デバイスの設定

ここでは、次の内容について説明します。

- 「ライセンス済みデバイス リストへのデバイスの追加」（P.18-3）
- 「ライセンス済みデバイス リストからのデバイスの削除」（P.18-3）

ライセンス済みデバイス リストへのデバイスの追加

管理対象デバイスは、DCNM-LAN ライセンス済みデバイス リストに追加できます。

はじめる前に

少なくとも 1 つの Cisco DCNM Enterprise LAN ライセンスをインストールしておく必要があります。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

すでに、手持ちのライセンスで許可されているデバイス数の上限までデバイスを追加している場合、新しいデバイスをリストに追加するには、まずライセンス済みデバイス リストから 1 つ以上のデバイスを削除する必要があります。詳細については、「ライセンス済みデバイス リストからのデバイスの削除」（P.18-3）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Licensed Devices] の順に選択します。

[Contents] ペインにライセンス済みデバイス リストが表示されます。

ステップ 2　メニュー バーで、[Actions] > [New] の順に選択します。

DCNM-LAN クライアントによってリストに 1 行追加され、[Available Devices] ダイアログボックスに選択された使用可能な物理デバイスが一覧表示されます。

ステップ 3　[Available Devices] リストで、ライセンスに追加する物理デバイスを選択して、[Add] をクリックします。

ステップ 4　[OK] をクリックします。

追加したデバイスを含むライセンス済みデバイス リストが [Contents] ペインに表示されます。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

追加したデバイスを管理するとき、ライセンス済み DCNM-LAN 機能を使用できるようになります。

ライセンス済みデバイス リストからのデバイスの削除

ライセンス済み DCNM-LAN 機能を使用してデバイスを管理する必要がなくなったら、DCNM-LAN ライセンス デバイス リストから 1 つ以上の物理デバイスを削除できます。

（注）　ライセンス済みデバイス リストから物理デバイスを削除すると、そのデバイスとデバイスに含まれるすべての VDC が DCNM-LAN から削除されます。削除したデバイスの管理を再開するには、そのデバイスを検出する必要があります。詳細については、「デバイスの検出」（P.16-9）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Licensed Devices] の順に選択します。

[Contents] ペインにライセンス済みデバイス リストが表示されます。

ステップ 2　ライセンス済みデバイス リストから削除する各デバイスについて、次の手順を実行します。

a. ライセンス済みデバイス リストから削除するデバイスを選択します。

b. メニュー バーで、[Actions] > [Delete] の順に選択します。

確認のダイアログボックスが表示されます。

c. [Yes] をクリックします。

ライセンス済みデバイス リストからデバイスが削除されます。

（注） ライセンス済みデバイス リストから削除したデバイスは、DCNM-LAN によって管理されなくなります。

ステップ 3　（任意）ライセンス済みデバイス リストから削除したデバイスの管理を再開する場合は、そのデバイスを検出します。詳細については、「デバイスの検出」（P.16-9）を参照してください。

DCNM-LAN ライセンス デバイスの表示

DCNM-LAN ライセンス デバイス リストを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Licensed Devices] の順に選択します。

[Contents] ペインに、DCNM-LAN ライセンス デバイス リストが表示されます。表示される各フィールドの詳細については、「DCNM-LAN ライセンス デバイスのフィールドの説明」（P.18-4）を参照してください。

DCNM-LAN ライセンス デバイスのフィールドの説明

ここでは、DCNM-LAN ライセンス デバイスの次の各フィールドについて説明します。

- 「DCNM-LAN ライセンス デバイスの [Contents] ペイン」（P.18-4）

DCNM-LAN ライセンス デバイスの [Contents] ペイン

表 18-1　DCNM-LAN ライセンス デバイスの [Contents] ペイン

フィールド	説明
Total License Count	*表示のみ。*インストール済みのすべての Cisco DCNM Enterprise LAN ライセンスによってライセンスされているデバイス数の合計。たとえば、5 デバイスをサポートしているライセンスを 2 つインストールした場合、このフィールドの表示は 10 になります。
Total N7K Permanent License Count	*表示のみ。*インストール済みのすべての Cisco DCNM Enterprise LAN ライセンスによってライセンスされている Nexus 7000 デバイスの合計台数（永久ライセンス）。
Total N7K Trial License Count	*表示のみ。*インストール済みのすべての Cisco DCNM Enterprise LAN ライセンスによってライセンスされている Nexus 7000 デバイスの合計台数（トライアル ライセンス）。

表 18-1　DCNM-LAN ライセンス デバイスの [Contents] ペイン （続き）

フィールド	説明
Total N5K, N4K, N3K, N1K License Count	*表示のみ。*インストール済みのすべての Cisco DCNM Enterprise LAN ライセンスによってライセンスされている Nexus 5000、Nexus 4000、Nexus 3000、および Nexus 1000 デバイスの合計台数。
Total Remaining License Count	*表示のみ。*残っているライセンスの合計数
Total Remaining N7K License Count	*表示のみ。*残っている Nexus 7000 デバイス ライセンスの合計数。
Total Remaining N5K, N4K, N3K, N1K License Count	*表示のみ。*残っている Nexus 5000、Nexus 4000、Nexus 3000、および Nexus 1000 デバイス ライセンスの合計数。
Switch Name	*表示のみ。*ライセンス済み物理デバイスの名前。このデバイス上では、ライセンス済み DCNM-LAN 機能を使用できます。
Virtual Devices	*表示のみ。*物理デバイス上に設定された各 Virtual Device Context（VDC; 仮想デバイス コンテキスト）。物理デバイスで VDC がサポートされない場合、このフィールドには何も表示されません。

その他の関連資料

DCNM-LAN ライセンス デバイスの管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.18-5）
- 「標準」（P.18-5）

関連資料

関連項目	参照先
Cisco DCNM Enterprise LAN ライセンスのインストール	『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN ライセンス デバイスの機能の履歴

表 18-2 は、この機能のリリースの履歴です。

表 18-2　DCNM-LAN ライセンス デバイスの機能の履歴

機能名	リリース	機能情報
DCNM-LAN ライセンス デバイス	5.0(2)	リリース 4.2 からの変更はありません

CHAPTER 19

トポロジの作業

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）のトポロジ機能の使用方法について説明します。

この章の内容は、次のとおりです。

- 「トポロジの概要」（P.19-1）
- 「トポロジのライセンス要件」（P.19-8）
- 「トポロジ機能の前提条件」（P.19-8）
- 「注意事項と制限」（P.19-8）
- 「トポロジ機能の使用方法」（P.19-8）
- 「関連資料」（P.19-30）
- 「トポロジの機能履歴」（P.19-30）

トポロジの概要

トポロジ機能では、サポートされている Cisco NX-OS デバイスのトポロジ マップが表示されます。トポロジ マップには、Catalyst 6500 シリーズ スイッチなど、Cisco IOS ソフトウェアが動作するスイッチも表示されます。Nexus 7000 シリーズ デバイスの場合、マップに Virtual Device Context（VDC; 仮想デバイス コンテキスト）の詳細が表示されます。

Cisco Data Center Network Manager for LAN（DCNM-LAN）は、新しい情報を受信すると、DCNM-LAN クライアントのマップをダイナミックにアップデートします。デフォルトでは、1 分間に 1 回、アップデートが実行されます。リンク ダウン、または VDC の作成、削除、変更など、リンクおよびデバイスのステータスの変更を確認できます。

マップには最新情報が表示されるため、この情報を使用して、進行中のネットワーク管理の問題についてトラブルシューティングを行うことができます。

デバイス アイコンのレイアウトは、変更および保存できます。また、マップを使用して、管理対象デバイスの機能を迅速に設定することもできます。

ここでは、次の内容について説明します。

- 「マップのビュー」（P.19-2）
- 「レイアウト」（P.19-5）
- 「vPC のサポート」（P.19-6）
- 「DCNM-SAN のサポート」（P.19-6）
- 「FabricPath のサポート」（P.19-7）

- 「デバイス グループ」（P.19-7）
- 「ネットワーク サーバ」（P.19-7）

マップのビュー

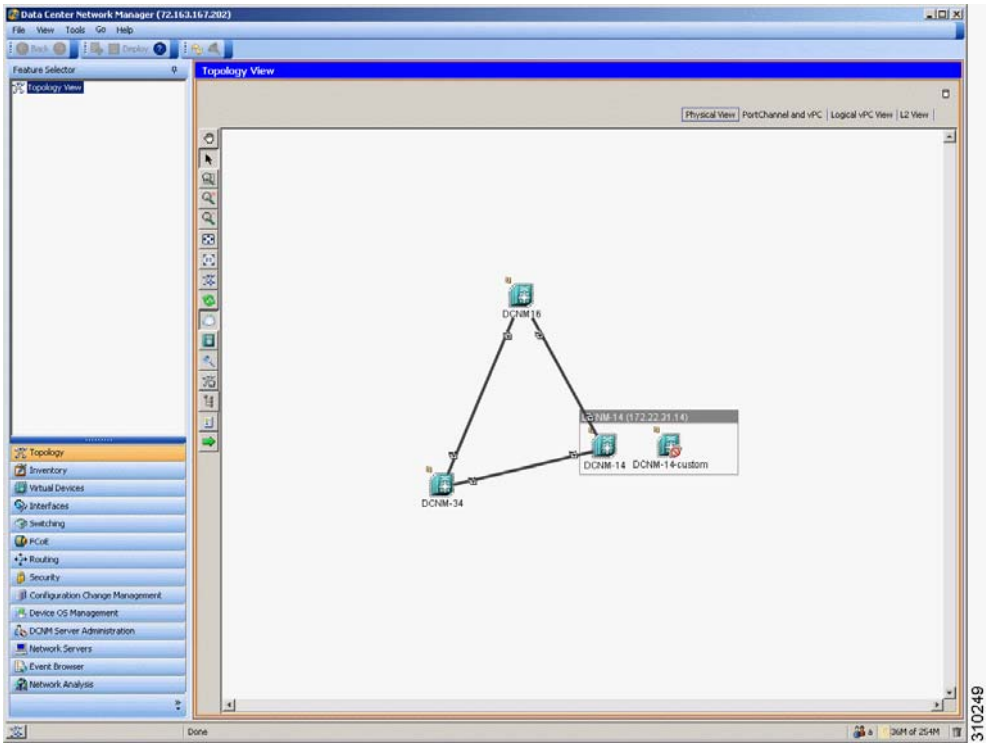
トポロジ マップには、次で説明するように、トポロジの 4 つのビューが含まれています。

- 「Physical View」（P.19-2）
- 「PortChannel and vPC」（P.19-3）
- 「Logical vPC View」（P.19-4）
- 「L2 View」（P.19-5）

Physical View

[Physical View]（図 19-1 を参照）には、検出したデバイス間の物理的な接続が表示されます。これはデフォルトのトポロジ ビューです。

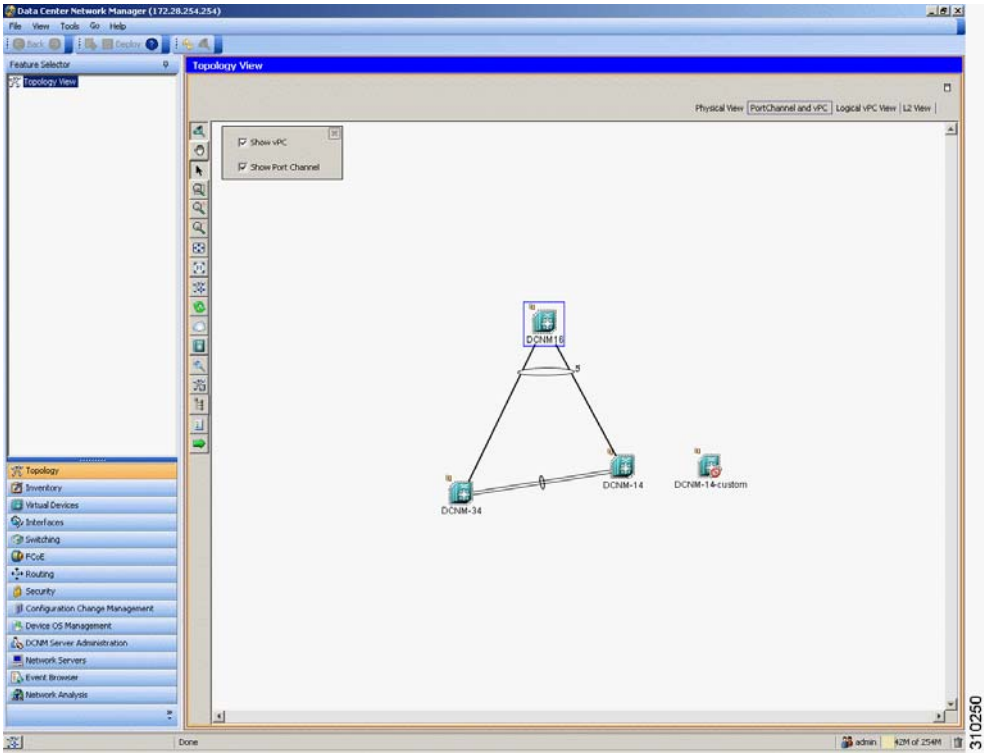
図 19-1　トポロジ マップの [Physical View]



PortChannel and vPC

[PortChannel and vPC] ビュー（図 19-2 を参照）には、検出したデバイス間のすべての物理接続とすべての論理接続が表示されます。これには、ポート チャネル リンク、virtual Port Channel（vPC）リンク、vPC ピア リンクが含まれます。このビューでは、物理リンクは灰色で表示されます。

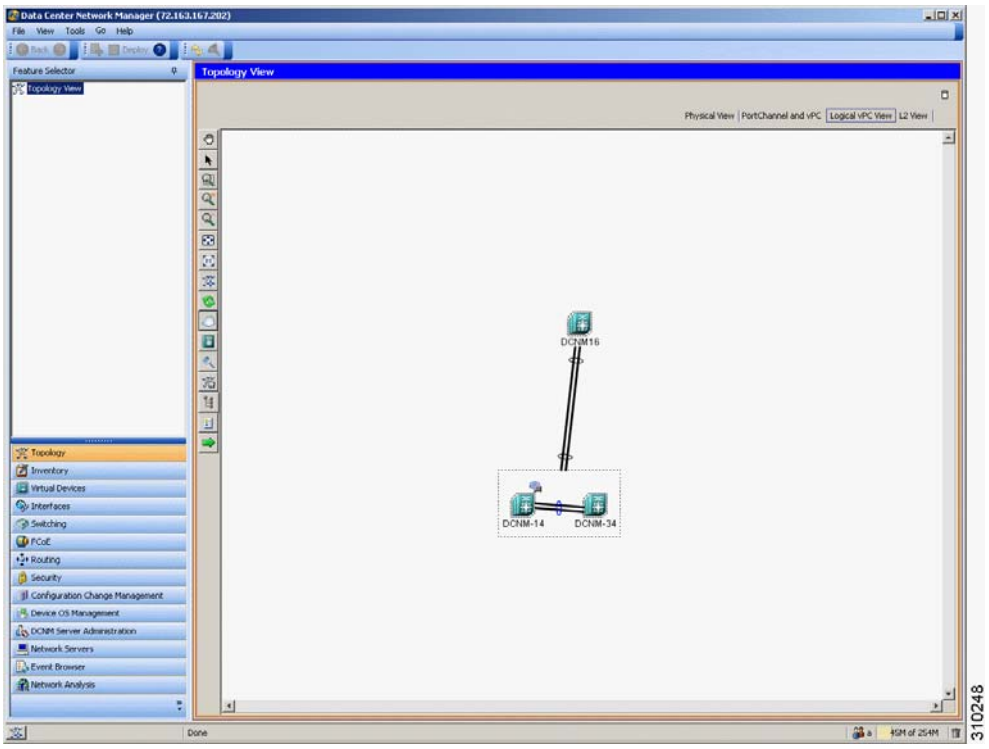
図 19-2　トポロジ マップの [PortChannel and vPC] ビュー



Logical vPC View

[Logical vPC View]（図 19-3 を参照）には、検出したデバイス間の vPC リンクと vPC ピア リンクが表示されますが、物理接続は表示されません。

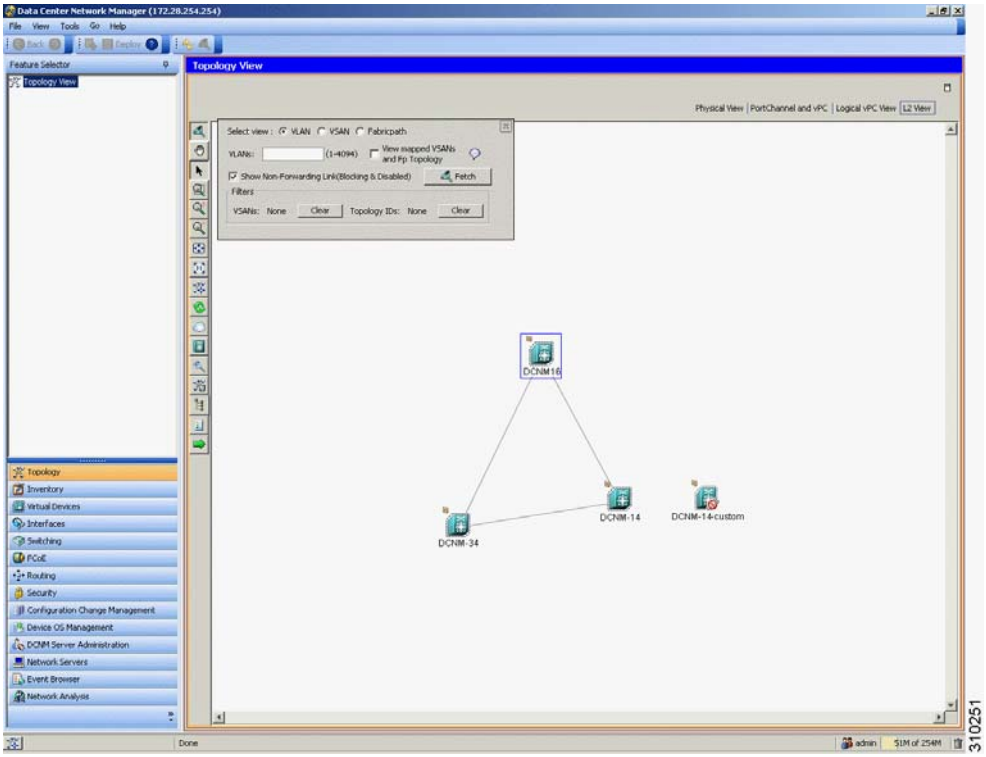
図 19-3　トポロジ マップの [Logical vPC View]



L2 View

[L2 View]（図 19-4 を参照）には、検出したデバイス間で設定されている VLAN が表示されます。Cisco DCNM-LAN Release 5.1 から、VSAN オーバーレイが L2 ビューの一部になりました。VSAN オーバーレイ機能を使用すると、特定の VSAN または一連の VSAN に対してアクティブなファイバ チャネル（FC）および Fibre Channel over Ethernet（FCoE）リンクを表示できます。また、設定された VLAN について、データセンター ネットワークにある Cisco Nexus デバイス間の転送および非転送リンクも視覚的に表示されます。

図 19-4　　トポロジ マップの [L2 View]



レイアウト

トポロジ マップでは、目的の場所にデバイスを移動できます。レイアウトを保存しておくと、次回トポロジ マップを使用するときにデバイスがその場所に表示されます。DCNM-LAN クライアントは、DCNM-LAN クライアントを実行しているコンピュータ上のローカル ユーザ データとしてトポロジ レイアウトを保存します。DCNM-LAN クライアントを使用する場合は、他のコンピュータ上に保存したトポロジ レイアウトや、別のユーザ名でログインして保存したトポロジ レイアウトにはアクセスできません。

[Physical View] を使用しているときは、レイアウトを保存するのに加えて、次のいずれかのレイアウトをロードできます。

- スプリング：接続に重みを付けることで決定される位置にデバイスが表示されます。多くの場合、接続の交差が最小限か交差のないレイアウトが生成されます。

- ツリー：デバイス間で接続がループしていない限り、デバイスがツリーに表示されます。ループしている場合、デバイスはスパニング ツリー（接続のほとんどがグリッド レイアウトに従うグリッド）に表示されます。

vPC のサポート

トポロジ マップには、vPC 固有の次の機能があります。

- vPC の作成：[PortChannel and vPC] ビューから [vPC Creation Wizard] を起動できます。「vPC ウィザードの起動」（P.19-27）を参照してください。
- vPC 機能へのクイック アクセス：特定の vPC の設定に [PortChannel and vPC] ビューまたは [Logical vPC View] ビューからアクセスできます。「vPC の管理」（P.19-28）を参照してください。
- vPC の設定の不一致：設定が矛盾している vPC リンクと vPC ピア リンクを確認できます。トポロジ マップから [Resolve Configuration Consistency] ダイアログボックスを開くことができます。「vPC 設定の不一致の検索と解決」（P.19-28）を参照してください。

DCNM-SAN のサポート

DCNM-LAN トポロジ マップでは、次に説明する機能を提供することで、Cisco Data Center Network Manager for SAN（DCNM-SAN）がサポートされています。

- 「共通のトポロジ」（P.19-6）
- 「DCNM-SAN 機能へのアクセス」（P.19-6）

共通のトポロジ

トポロジ マップには、イーサネット LAN 接続とデバイスに加えて、ストレージ エリア ネットワーク（SAN）接続とデバイスが表示できます。DCNM-LAN のトポロジ マップを使用して、データセンター ネットワーク全体を表示できます。

DCNM-SAN 機能へのアクセス

Cisco MDS 9000 ファミリ マルチレイヤ スイッチなどの SAN デバイスが DCNM-LAN クライアントのトポロジ マップに表示される場合、トポロジ マップを使用して Cisco DCNM-SAN クライアントを起動し、SAN デバイスを設定できます。

Cisco DCNM-SAN がサーバ モードでインストールされている場合、Cisco DCNM-SAN 相互起動機能は DCNM-LAN クライアントだけでサポートされます。Cisco DCNM-SAN がスタンドアロン モードでインストールされている場合、DCNM-LAN クライアントで相互起動はサポートされません。また、DCNM-LAN クライアントがスタンドアロン モードの場合は、相互起動はサポートされません。

スタンドアロン モードでの DCNM-LAN クライアントのインストールについては、第 13 章「Cisco DCNM-LAN クライアントのインストールおよび起動」を参照してください。

Cisco DCNM-SAN と DCNM-LAN を同じサーバ システムにインストールする方法については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

FabricPath のサポート

L2MP-ISIS プロトコルを実行する L2MP 対応デバイスに対する FabricPath のサポートは、[Topology] ドロワーの [L2 View] で提供されています。[L2 View] には、表示されるグラフのタイプを選択できるダイアログボックスがあります。ダイアログボックスで [Fabricpath] ビューを選択すると、次のタイプのグラフを表示できます。

- 複数宛先

  複数宛先またはブロードキャスト グラフには、トポロジ内のブロードキャスト トラフィックおよび不明なユニキャスト トラフィックが表示されます。

- 到達可能性

  L2MP-ISIS により、ネットワーク内の各ノードのスイッチ ID 到達可能性が自動的に計算されます。

- ユニキャスト

  ユニキャスト グラフには、ネットワーク内のノード間の等コスト ルートが表示されます。

- マルチキャスト

  マルチキャスト グラフには、指定したデバイスから特定の IGMP グループをリッスンしているすべてのホストへのマルチキャスト トラフィックが表示されます。

また、[L2 View] から FabricPath Topology Wizard を起動することもできます。FabricPath Topology Wizard を使用すると、FabricPath トポロジの追加、インベントリの表示、エンド デバイスの表示など、多くの操作を実行できます。

（注）　Cisco NX-OS Release 5.1(1) では、FabricPath Topology Wizard はサポートされません。

ウィザードを起動するには、複数のデバイスを選択し、右クリックして使用可能な操作を示すコンテキスト メニューを表示する必要があります。Shift キーを押した状態で、グラフに表示される適切なデバイスをクリックすることにより、複数のデバイスを選択できます。または、マウスの左ボタンを押した状態で、適切なデバイス上をドラッグすることもできます。

デバイス グループ

デバイス グループを使用するとトポロジ マップ中でデバイスのグループ間の相互接続を簡単に視覚化できます。定義したデバイス グループにデバイスを分類することで、トポロジを表示する際に、限られた数のデバイスに焦点を絞ることができます。

デバイス グループはトポロジ マップを使用して管理できるため、グループの作成、グループの削除、グループ間でのデバイスの移動が可能です。デバイス グループ機能は、複数のデバイスをグループに簡単に割り当てるために特に便利です。

デバイス グループの詳細については、第 21 章「デバイス グループの設定」を参照してください。

ネットワーク サーバ

トポロジ マップにはネットワーク サーバを表示できます。ネットワーク サーバ機能を使うと、DCNM-LAN が Link Layer Discovery Protocol（LLDP）を介して検出したホスト バス アダプタ（HBA）とイーサネット ネットワーク アダプタをネットワーク サーバに関連付けることができます。

詳細については、第 20 章「ネットワーク サーバの設定」を参照してください。

トポロジのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	トポロジ機能にライセンスは不要です。ただし、トポロジ マップの [Logical vPC View] ビューには、LAN エンタープライズ ライセンスが必要です。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

トポロジ機能の前提条件

トポロジ機能の前提条件は、次のとおりです。

- トポロジ マップには、DCNM-LAN によって検出されたデバイスだけが表示されます。
- トポロジ マップを完全にサポートするためには、検出されたデバイスで該当する検出プロトコルがグローバルとアクティブ インターフェイスの両方でイネーブルになっている必要があります。DCNM-LAN が使用する検出プロトコルの詳細については、第 16 章「デバイス ディスカバリの管理」を参照してください。

注意事項と制限

トポロジ機能には、次の構成に関する注意事項と制約事項があります。

- トポロジ機能はライセンスが不要な機能ですが、トポロジに表示される Cisco Nexus 7000 シリーズ スイッチのデフォルト以外の VDC を管理するには、LAN エンタープライズ ライセンスが必要です。
- トポロジ機能によるトポロジ変更は、アカウンティングおよびシステム ログのポーリング頻度で実行されます。デフォルトのポーリング頻度は、1 分です。詳細については、「デバイスとの自動同期化の概要」（P.23-1）を参照してください。

トポロジ機能の使用方法

ここでは、次の内容について説明します。

- 「トポロジ マップを開く」（P.19-9）
- 「デバイス アイコンとリンクの説明」（P.19-10）
- 「表示ツールの使用」（P.19-11）
- 「[Details] ペインの表示、非表示、使用」（P.19-12）
- 「トポロジ マップ上のデバイスの移動」（P.19-13）
- 「レイアウトのロード」（P.19-14）
- 「以前保存したレイアウトの再ロード」（P.19-15）
- 「仮想シャーシまたは物理シャーシの表示」（P.19-16）

- 「ネットワーク サーバの表示または非表示」（P.19-16）
- 「ネットワーク サーバの管理」（P.19-16）
- 「デバイス グループの表示または非表示」（P.19-17）
- 「デバイス グループの展開と折りたたみ」（P.19-18）
- 「デバイス グループの作成」（P.19-18）
- 「デバイス グループ間でのデバイスの移動」（P.19-19）
- 「デバイス グループからのデバイスの削除」（P.19-20）
- 「実行コンフィギュレーションのスタートアップ コンフィギュレーションへのコピー」（P.19-20）
- 「デバイス グループの削除」（P.19-21）
- 「JPG イメージでのトポロジのエクスポート」（P.19-22）
- 「トポロジ マップからの DCNM-LAN 機能へのアクセス」（P.19-22）
- 「トポロジ マップからの Cisco DCNM-SAN 機能へのアクセス」（P.19-23）
- 「トポロジ マップからの Cisco FabricPath 機能へのアクセス」（P.19-24）
- 「vPC ウィザードの起動」（P.19-27）
- 「vPC の管理」（P.19-28）
- 「vPC 設定の不一致の検索と解決」（P.19-28）
- 「トポロジ マップからのリモート接続された CNA へのアクセス」（P.19-29）
- 「VSAN オーバーレイの使用方法」（P.19-29）

トポロジ マップを開く

トポロジ マップを開いて検出したデバイスのトポロジを表示できます。

（注） FabricPath を使用する場合は、検出の前に、コマンドライン インターフェイス（CLI）を使用して次のことを行う必要があります。

- 拡張レイヤ 2 ライセンスをデバイスにインストールします。このライセンスのインストールの詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。
- FabricPath フィーチャ セットをデバイスにインストールします。フィーチャ セットのインストールの詳細については、『*Cisco Configuring Feature Set for FabricPath Guide*』を参照してください。
- カスタム VDC でイネーブルにできるように FabricPath フィーチャ セットを設定します。フィーチャ セットの設定の詳細については、『*Cisco Configuring Feature Set for FabricPath Guide*』を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。使用可能な各トポロジ ビューのボタンがトポロジ マップの上に表示されます。

ステップ 2　（任意）トポロジ ビューを変更する場合は、トポロジ ビュー名をクリックします。

トポロジ マップに、選択したトポロジのビューが表示されます。

ステップ 3　（任意）ビュー固有のオプションを使用する場合は、次の表を参照してください。

ビュー機能	使用できるビュー	使用方法
すべての VDC の表示と非表示	• Physical View	マップを右クリックし、[Show All VDCs] または [Hide All VDCs] を選択します。 すべての VDC を表示すると、Cisco Nexus 7000 シリーズ デバイスが灰色のボックスとして表示され、その中に Cisco Nexus 7000 シリーズ デバイスで設定されている各 VDC のデバイス アイコンが表示されます。
エンド デバイスの表示と非表示	• Physical View • L2 View	マップを右クリックし、[Show End Devices] または [Hide End Devices] を選択します。
VLAN のフィルタ	• L2 View	1. VLAN ボックスがマップに表示されない場合は、トポロジ ツールバーの [Filter] アイコンをクリックします。 2. VLAN ID のリストを入力します。単一の VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます。 3. [Filter] をクリックします。
非転送リンクの表示と非表示	• L2 View	1. マップ上で VLAN ボックスを探します。 2. [Show Non-Forwarding Link (Blocking & Disabled)] をオンまたはオフにします。
vPC またはポート チャネルの表示と非表示	• PortChannel and vPC	1. マップ上で、[Show vPC] チェックボックスと [Show Port Channel] チェックボックスが含まれる灰色のボックスを探します。灰色のボックスを見つけるには、マップのスクロールやズーム アウトが必要な場合があります。 2. チェックボックスをオンまたはオフにします。

デバイス アイコンとリンクの説明

トポロジ マップに表示されるデバイス アイコンとリンクについて理解するために、凡例を開くことができます。凡例には、現在選択されているトポロジ ビューに表示されているデバイス アイコンとリンクに関する情報が表示されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。使用可能な各トポロジ ビューのボタンがトポロジ マップの上に表示されます。

ステップ 2　（任意）トポロジ ビューを変更する場合は、トポロジ ビュー名をクリックします。

トポロジ マップに、選択したトポロジのビューが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

ステップ 3　トポロジ ツールバーで、アイコンをクリックします。

[Legend] ダイアログボックスに、現在選択されているトポロジ ビューに表示されているデバイス アイコンとリンクに関する説明が表示されます。

表示ツールの使用

パン、選択、ズーム、検索ツールを使用してトポロジ マップを表示できます。

次の表に、トポロジ マップの左側にあるトポロジ ツールバー上の表示ツールの説明を示します。

表示ツールのアイコンと名前	使用方法
Pan	マップを移動（パン）します。 1. アイコンをクリックします。 2. トポロジ マップの任意の場所をクリックし、マウス ボタンを押したままにします。 3. マップを任意の方向にドラッグします。 4. マウス ボタンを放します。
Select	デバイス、リンク、ポート アイコンのいずれかを選択できます。 1. アイコンをクリックします。 2. 操作するデバイス、リンク、またはポート アイコンをクリックします。 バルーンに、クリックしたアイコンに関する情報が表示されます。
Zoom in Rect	マップの特定の部分をズームします。 1. アイコンをクリックします。 2. マップをクリックし、表示する領域の上に矩形をドラッグし、マウス ボタンを放します。
Zoom In	拡大します。アイコンをクリックします。
Zoom Out	縮小します。アイコンをクリックします。
Fit to View	検出したデバイスのトポロジ全体をトポロジ マップに合わせて表示します。アイコンをクリックします。
Reset Zoom	デフォルトの倍率にズームをリセットします。アイコンをクリックします。
Load Layout	レイアウトをロードします。
Reload Layout	最後に保存したレイアウトをロードします。「以前保存したレイアウトの再ロード」（P.19-15）を参照してください。

表示ツールのアイコンと名前	使用方法
Show Device Groups	デバイス グループを表示または非表示にします。「デバイス グループの表示または非表示」（P.19-17）を参照してください。
Search	デバイスを名前で検索するためのデバイス検索ツールを使用できます。 1. マップに [Search] ツールを表示するには、アイコンをクリックします。 2. [Device] ボックスに、検索するデバイスの名前の全体または一部を入力し、アイコンをクリックします。 3. 検索ツールを非表示にするには、再度アイコンをクリックします。 **ヒント** トポロジ マップ上で検索ツールを移動するには、選択ツールがイネーブルな状態で検索ツールをクリックしてドラッグします。
Save Layout	デバイス アイコン レイアウトに対して行った変更を保存します。「トポロジ マップ上のデバイスの移動」（P.19-13）を参照してください。
Hide/Show Details	詳細ペインを表示および非表示にします。「[Details] ペインの表示、非表示、使用」（P.19-12）を参照してください。
Legend	[Legend] ダイアログボックスを開きます。「デバイス アイコンとリンクの説明」（P.19-10）を参照してください。
Export as JPG	トポロジ マップを JPG イメージ ファイルとして保存します。「JPG イメージでのトポロジのエクスポート」（P.19-22）を参照してください。

[Details] ペインの表示、非表示、使用

トポロジ マップ内の [Details] ペインを表示または非表示にできます。[Details] ペインを表示するとき、[Details] ペイン内のセクションを使用して、トポロジ内のデバイスと接続について理解することができます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

ヒント　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　詳細を表示または非表示にするには、アイコンをクリックします。

詳細を表示するとき、[Details] ペインがトポロジ ツーバーとトポロジ マップの間に表示されます。

ヒント　選択ツールが選択されていることを確認します。選択ツールを選ぶには、アイコンをクリックします。

ステップ 3　[Details] ペインのセクションを使用するには、次の表を参照してください。

セクション	使用可能な場所	使用方法
VDC View	• Physical View • L2 View	[VDC View] ツリーの中を参照し、VDC が含まれている Cisco Nexus 7000 シリーズ デバイスを確認します。デバイスに関する詳細を参照するには、デバイスをクリックして [Properties] セクションを確認します。
vPC	• PortChannel and vPC • Logical vPC	vPC ツリーの中を参照し、トポロジ マップ内のすべての論理接続を分類したリストを表示します。vPC、vPC ピア リンク、ポート チャネルの詳細を参照するには、対象をクリックして [Properties] セクションを確認します。
Overview	• すべてのビュー	**ヒント** [Overview] セクションを参照するには、[Properties] セクションの [Overview] タブをクリックする必要があります。[Overview] セクションと [Properties] セクションは、同じセクション タイトル バーを共有します。 [Overview] セクションには、トポロジ全体のサムネイル ビューが表示されます。青い矩形は、現在マップに表示されているトポロジの部分を示しています。 • マップに表示するトポロジの部分を変更するには、概要で、マップに表示する部分をクリックします。 • 拡大または縮小するには、青い矩形の角をクリックし、マップが目的の大きさに拡大または縮小されるまでドラッグします。
Properties	• すべてのビュー	**ヒント** [Properties] セクションを表示するには、[Overview] セクションで [Properties] タブをクリックする必要があります。[Overview] セクションと [Properties] セクションは、同じセクション タイトル バーを共有します。 **1.** 次のどちらかを実行します。 – [VDC View] セクションで、物理デバイスまたは仮想デバイスをクリックします。 – vPC セクションで、論理接続をクリックします。 – トポロジ マップで、デバイス、リンク、またはポートをクリックします。 **2.** [Properties] セクションで、選択したオブジェクトのプロパティを表示します。

トポロジ マップ上のデバイスの移動

トポロジ マップに表示されているデバイス アイコンを移動できます。デバイスの位置は、すべてのトポロジ ビューと共有されています。つまり、デバイスを移動して別のトポロジ ビューに切り替えると、デバイスは移動先に表示されたままになります。

また、レイアウトを保存しておいて、以降リロードして変更したり、最後に保存したレイアウトに戻したりすることができます。

詳細については、「以前保存したレイアウトの再ロード」（P.19-15）を参照してください。

保存したレイアウトは、DCNM-LAN クライアントの起動時にトポロジ マップに表示されるデフォルトのレイアウトになります。

（注）　DCNM-LAN クライアントは、DCNM-LAN クライアントを実行しているコンピュータ上のローカル ユーザ データとしてトポロジ レイアウトを保存します。DCNM-LAN クライアントを使用する場合は、他のコンピュータ上に保存したトポロジ レイアウトや、別のユーザ名でログインして保存したトポロジ レイアウトにはアクセスできません。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　トポロジ ツールバーで、アイコンを選択します。

ステップ 3　必要に応じて、デバイス アイコンを検索して、移動します。アイコンを移動するには、デバイス アイコン上をクリックし、マウス ボタンを押しながら、アイコンを移動先までドラッグして、マウス ボタンを放します。

必要に応じて、ズームおよびパン操作を使用して、アイコンを検索できます。

詳細については、「表示ツールの使用」（P.19-11）を参照してください。

ステップ 4　（任意）デバイス アイコンのレイアウト変更を保存する場合は、アイコンをクリックします。

レイアウトのロード

[Physical View] を使用している場合、レイアウトのロード を選択できます。デバイスの位置はすべてのトポロジ ビューで共有されています。この動作により、[Physical View] でレイアウトをロードし、別のビューで選択することで、すべてのビューで任意のレイアウトを使用できます。

（注）　[Physical View] 以外のビューを使用している場合、トポロジ ツールバー上のアイコンはアイコンと同様に振る舞います。アイコンの使用方法については、「以前保存したレイアウトの再ロード」（P.19-15）を参照してください。

はじめる前に

コア スイッチとして指定する物理デバイスを決定します。保存したレイアウト以外のレイアウトをロードすると、コア スイッチがトポロジ マップの上部に表示され、コア スイッチから 1 CDP ホップ離れたデバイスがそのすぐ下に表示されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　（任意）レイアウトの上部に表示する各物理デバイスに対し、デバイス アイコンを右クリックして [Make as Core Switch] を選択します。

ステップ 3　トポロジ ツールバーで、 アイコンをクリックします。

[Layout] ドロップダウン リストが表示されます。

ステップ 4　[Layout] ドロップダウン リストから、ロードするレイアウトを選択します。

トポロジ マップの [Physical View] が、選択したレイアウトに変わります。コア スイッチとして指定した任意のデバイスがマップの上部に表示され、コア スイッチから 1 CDP ホップ離れたデバイスがそのすぐ下に表示されます。

以前保存したレイアウトの再ロード

最後に保存したレイアウトをロードできます。この機能により、レイアウトの最後の保存後に行ったデバイス配置の変更を取り消すことができます。

（注）　DCNM-LAN クライアントは、DCNM-LAN クライアントを実行しているコンピュータ上のローカル ユーザ データとしてトポロジ レイアウトを保存します。DCNM-LAN クライアントを使用する場合は、他のコンピュータ上に保存したトポロジ レイアウトや、別のユーザ名でログインして保存したトポロジ レイアウトにはアクセスできません。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　トポロジ ツールバーで、 アイコンを選択します。

トポロジ マップが変更され、最後に保存したレイアウトに戻ります。

仮想シャーシまたは物理シャーシの表示

Cisco Nexus 1000V デバイスでは、トポロジ マップにデバイスの仮想シャーシと物理シャーシのどちらを表示するかを指定できます。デフォルトでは、トポロジ マップに仮想シャーシが表示されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

ステップ 2　Cisco Nexus 1000V デバイスのアイコンを探します。

トポロジ マップには、仮想シャーシと物理シャーシのいずれかが表示されます。

ステップ 3　デバイス アイコンを右クリックし、いずれかの適切なオプションを選択します。

- **Show Virtual Chassis**
- **Show Physical Chassis**

ネットワーク サーバの表示または非表示

特定のデバイスに接続されているネットワーク サーバを表示または非表示にできます。デフォルトでは、ネットワーク サーバはトポロジ マップで非表示になっています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

ステップ 2　表示または非表示にするネットワーク サーバに接続されているデバイスを探します。

ステップ 3　デバイスを右クリックし、次のいずれかを選択します。

- 接続されているネットワーク サーバを表示するには、[Show End Devices] を選択します。
- 接続されているネットワーク サーバを非表示にするには、[Hide End Devices] を選択します。

ネットワーク サーバの管理

トポロジ マップを使用して、マップ上に表示されているネットワーク サーバのネットワーク サーバ機能にアクセスできます。

はじめる前に

トポロジ マップにネットワーク サーバが表示されている必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　ネットワーク サーバ機能で管理するネットワーク サーバを探します。

ヒント　ネットワーク サーバがマップに表示されていない場合は、接続されているデバイスを右クリックし、[Show End Devices] を選択します。

ステップ 3　サーバを右クリックし、[Manage Server] を選択します。

DCNM-LAN クライアントでネットワーク サーバ機能が開きます。選択したサーバが管理対象サーバまたは検出されたサーバ上のイーサネット アダプタを表している場合、クライアントで [Servers] コンテンツ ペインが開きます。選択したサーバが、サーバに関連付けられていないかバインドされていないホスト バス アダプタ（HBA）を表している場合、クライアントで [Static Server-Adapter Mapping] コンテンツ ペインが開きます。

デバイス グループの表示または非表示

デバイス グループを表示または非表示にできます。デバイス グループが非表示の場合、トポロジ マップに検出されたすべてのデバイスと接続が表示されます。デバイス グループが表示されている場合、個別のデバイス グループまたはすべてのデバイス グループを展開または折りたたむことができます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

トポロジ ツールバーの アイコンは、デバイス グループをトポロジ マップに表示するかどうかを制御します。アイコンが押し込まれて表示されている場合、トポロジ マップにデバイス グループが表示されます。アイコンが押し込まれて表示されていない場合、トポロジ マップにデバイス グループが表示されません。

ステップ 2　デバイス グループの表示と非表示を切り替えるには、 アイコンをクリックします。

デバイス グループの展開と折りたたみ

個別のデバイス グループまたはすべてのデバイス グループを展開および折りたたむことができます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　デバイス グループがトポロジ マップに表示されていない場合は、トポロジ ツールバーの アイコンをクリックします。

ステップ 3　次のどちらかを実行します。

- 単一のデバイス グループを展開するには、デバイス グループ アイコンを右クリックし、[Expand Device Group] を選択します。
- すべてのデバイス グループを展開するには、マップの空白部分を右クリックし、[Expand all Device Groups] を選択します。
- 単一のデバイス グループを折りたたむには、デバイス グループのタイトルを右クリックし、[Collapse Device Group] を選択します。
- すべてのデバイス グループを折りたたむには、マップの空白部分を右クリックし、[Collapse all Device Groups] を選択します。

デバイス グループの作成

トポロジ マップ上にカスタム デバイス グループを作成できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　マップの空白部分を右クリックし、[New Device Group] を選択します。

ダイアログボックスが表示され、新しいデバイス グループの名前を指定するためのフィールドが表示されます。

ステップ 3　デバイス グループの名前を入力し、[OK] をクリックします。

新しいデバイス グループがトポロジ マップに表示されます。

デバイス グループ間でのデバイスの移動

トポロジ マップ上のデバイス グループ間でデバイスを移動できます。

（注） グループからデバイスを移動した後でデバイス グループが空になる場合は、デバイス グループが削除されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注） トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　デバイス グループがトポロジ マップに表示されていない場合は、トポロジ ツールバーの アイコンをクリックします。

ステップ 3　デバイスの移動元のデバイス グループを探します。

ステップ 4　デバイス グループが折りたたまれている場合は、デバイス グループをダブルクリックして展開します。

ステップ 5　グループから移動するデバイスを右クリックし、[Cut] を選択します。

ステップ 6　デバイスの移動先のデバイス グループを探します。

ヒント デバイスをデバイス グループに移動する前にそのグループを展開しておく必要はありません。

ステップ 7　デバイス グループを右クリックし、[Paste] を選択します。

ヒント デバイス グループが展開されている場合は、デバイス グループのタイトルをクリックする必要があります。

デバイス グループを移動することを確認する警告ダイアログボックスが表示されます。

ステップ 8　[Yes] をクリックします。

デバイスが 2 番目に指定したデバイス グループに追加され、最初に指定したデバイス グループから削除されます。デバイスを移動した後に最初に指定したデバイス グループが空になる場合は、そのデバイス グループが削除されます。

デバイス グループからのデバイスの削除

カスタム デバイス グループからデバイスを削除できます。カスタム グループから削除したすべてのデバイスはデフォルト デバイス グループに追加されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　デバイス グループがトポロジ マップに表示されていない場合は、トポロジ ツールバーのアイコンをクリックします。

ステップ 3　削除するデバイスが含まれているデバイス グループを探します。

ステップ 4　デバイス グループが折りたたまれている場合は、デバイス グループをダブルクリックして展開します。

ステップ 5　グループから削除するデバイスを右クリックし、[Remove from Group] を選択します。

グループに 1 つしかないデバイスを削除する場合、デバイス グループを削除することを確認するダイアログボックスが表示されます。

ステップ 6　警告が表示されたら、[Yes] をクリックします。

デバイスがカスタム デバイス グループから削除され、デフォルト デバイス グループに追加されます。

実行コンフィギュレーションのスタートアップ コンフィギュレーションへのコピー

[Physical View] で、実行コンフィギュレーションを、選択した 1 つ以上のデバイスのスタートアップ コンフィギュレーションにコピーできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　デバイス グループがトポロジ マップに表示されていない場合は、トポロジ ツールバーのアイコンをクリックします。

ステップ 3　トポロジ マップの上部にある [Physical View] を選択します。

ステップ 4　実行コンフィギュレーションのコピー元のデバイスを選択します。

ステップ 5　デバイス グループが折りたたまれている場合は、デバイス グループをダブルクリックして展開します。

ステップ 6　実行コンフィギュレーションのコピー元のデバイスを右クリックします。

- 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コピーする場合は、[Copy Run to Start] を選択します。

  実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
- 実行コンフィギュレーションをブートフラッシュ ディレクトリのファイルにコピーする場合は、[Copy Run to File in Bootflash] を選択します。表示されたダイアログボックスで、コピー先のファイルの名前を入力し、[OK] をクリックして操作を完了します。

  実行コンフィギュレーションが指定したファイルにコピーされます。

デバイス グループの削除

トポロジ マップからカスタム デバイス グループを削除できます。

削除したカスタム デバイス グループに属しているデバイスは、自動的にデフォルト デバイス グループのメンバーになります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　デバイス グループがトポロジ マップに表示されていない場合は、トポロジ ツールバーのアイコンをクリックします。

ステップ 3　削除するデバイス グループを探します。

ステップ 4　デバイス グループを右クリックし、[Delete Group] を選択します。

トポロジ マップからデバイス グループが削除されます。削除したデバイス グループに属していたデバイスは、デフォルト デバイス グループのメンバーになります。

（注）　デバイス グループを削除した後でカスタム デバイス グループがない場合、すべてのデバイスがデフォルト デバイス グループに属するため、トポロジ マップ上のデバイス グループは自動的に非表示になります。

JPG イメージでのトポロジのエクスポート

トポロジ マップの JPG イメージをエクスポートまたは保存できます。トポロジ マップ全体またはトポロジ マップの表示されている部分だけをエクスポートできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　トポロジ マップを、保存する状態で表示します。

詳細については、「表示ツールの使用」（P.19-11）を参照してください。

ステップ 3　必要に応じて、デバイス アイコンを配置します。

詳細については、「トポロジ マップ上のデバイスの移動」（P.19-13）を参照してください。

ステップ 4　トポロジ ツールバーで、 アイコンをクリックします。

ダイアログボックスが開き、トポロジ マップ全体をエクスポートするか、マップの表示されている部分だけをエクスポートするかを選択するよう求められます。

ステップ 5　次のどちらかを実行します。

- トポロジ マップ全体を JPG イメージとしてエクスポートするには、[Yes] をクリックします。
- トポロジ マップの表示されている部分だけをエクスポートするには、[No] をクリックします。

ステップ 6　JPG イメージの保存先とファイル名を指定して、[Save] をクリックします。

トポロジ マップの表示部分が、JPG イメージとして保存されます。

トポロジ マップからの DCNM-LAN 機能へのアクセス

トポロジ マップを使用して、管理対象デバイスの他の DCNM-LAN 機能にアクセスできます。トポロジ マップから、次の [Feature Selector] ドロワーにある機能にアクセスできます。

- Inventory
- Virtual Devices
- Interfaces
- Routing
- Switching
- Security

また、トポロジ マップを使用してデバイス ディスカバリ機能にアクセスすることもできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　特定の管理対象デバイス用の DCNM-LAN 機能にアクセスするには、次の手順を実行します。

a.　トポロジ マップでデバイスを検索します。

b.　デバイスを右クリックして、設定する機能を選択します。

[Contents] ペインに、選択した機能が表示されます。トポロジ マップで選択したデバイスが、[Summary] テーブルの機能で選択されます。

ステップ 3　デバイス ディスカバリ機能にアクセスするには、マップ上の空白部分を右クリックして、[Discover Device] を選択します。

[Contents] ペインに、デバイス ディスカバリ機能が表示されます。

トポロジ マップからの Cisco DCNM-SAN 機能へのアクセス

トポロジ マップを使用して、管理対象 SAN デバイスの Cisco DCNM-SAN クライアントの機能にアクセスできます。Cisco DCNM-SAN がデバイスを検出していない場合、トポロジ マップを通じて Cisco DCNM-SAN クライアントにアクセスすると、Cisco DCNM-SAN によって SAN デバイスが検出されます。

アクセスできる Cisco DCNM-SAN の機能には、次のものがあります。

- ゾーン、ゾーン セット、ゾーン セットのメンバーシップ
- ポート チャネル インターフェイス
- ファイバ チャネル物理および論理インターフェイス
- IP トンネル上のファイバ チャネル
- イベント

（注）　Cisco DCNM-SAN がサーバ モードでインストールされている場合、Cisco DCNM-SAN 相互起動機能は DCNM-LAN クライアントだけでサポートされます。Cisco DCNM-SAN がスタンドアロン モードでインストールされている場合、DCNM-LAN クライアントで相互起動はサポートされません。また、DCNM-LAN クライアントがスタンドアロン モードの場合は、相互起動はサポートされません。

はじめる前に

DCNM-LAN クライアントが動作するコンピュータに Cisco DCNM-SAN クライアントがインストールされている必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　トポロジ マップで SAN デバイスを探します。

ステップ 3　デバイスを右クリックして、設定する機能を選択します。

Cisco DCNM-SAN クライアントで選択した機能が開きます。

トポロジ マップからの Cisco FabricPath 機能へのアクセス

トポロジ マップを使用して、Cisco FabricPath の機能にアクセスできます。

ここでは、次の内容について説明します。

- 「複数宛先」（P.19-24）
- 「デバイスの到達可能性」（P.19-25）
- 「ユニキャスト」（P.19-25）
- 「マルチキャスト」（P.19-26）

複数宛先

複数宛先またはブロードキャスト グラフには、トポロジ内のブロードキャスト トラフィックおよび不明なユニキャスト トラフィックが表示されます。特定のトポロジの複数宛先情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　マップの上部にある [L2 View] をクリックします。

[Contents] ペインにダイアログボックスが表示されます。

ステップ 3　ダイアログボックスで [Fabricpath] ビューを選択します。

ステップ 4　トポロジ ID を入力し、[Fetch] をクリックします。表示されるグラフは、トポロジ ID に基づいてフィルタリングされます。

ステップ 5　[Select type of graph] をオンにして複数宛先グラフの選択をイネーブルにします。

ステップ 6　[Multi-destination] オプションをオンにします。

ステップ 7　[Anchor] ドロップダウン リストからデバイスを選択します。選択したデバイスは、グラフのエントリ ポイントです。

ステップ 8　[Graph ID] ドロップダウン リストから ID を選択します。グラフ ID は、グラフの転送タグです。

ステップ 9　[Fetch] をクリックしてグラフを表示します。

デバイスの到達可能性

L2MP-ISIS により、ネットワーク内の各ノードのスイッチ ID 到達可能性が自動的に計算されます。特定のトポロジの到達可能性情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　マップの上部にある [L2 View] をクリックします。

[Contents] ペインにダイアログボックスが表示されます。

ステップ 3　ダイアログボックスで [Fabricpath] ビューを選択します。

ステップ 4　トポロジ ID を入力します。表示されるグラフは、トポロジ ID に基づいてフィルタリングされます。

ステップ 5　[Select type of graph] をオンにして到達可能性グラフの選択をイネーブルにします。

ステップ 6　[Reachability] オプションをオンにします。

ステップ 7　[Anchor] ドロップダウン リストからデバイスを選択します。選択したデバイスは、グラフのエントリ ポイントです。

ステップ 8　[Fetch] をクリックしてグラフを表示します。

（注）　グラフ内で赤色のアイコンとして表示されるデバイスは、選択したトポロジではそのデバイスが到達不能であることを示します。

ユニキャスト

ユニキャスト グラフには、ネットワーク内のノード間の等コスト ルートが表示されます。特定のトポロジのユニキャスト情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　マップの上部にある [L2 View] をクリックします。

[Contents] ペインにダイアログボックスが表示されます。

ステップ 3　ダイアログボックスで [Fabricpath] ビューを選択します。

ステップ 4　トポロジ ID を入力します。表示されるグラフは、トポロジ ID に基づいてフィルタリングされます。

ステップ 5　[Select type of graph] をオンにしてユニキャスト グラフの選択をイネーブルにします。

ステップ 6　[Unicast] オプションをオンにします。

ステップ 7　[Anchor] ドロップダウン リストからデバイスを選択します。選択したデバイスは、グラフのエントリポイントです。

ステップ 8　[Destination] ドロップダウン リストからデバイスを選択します。選択したデバイスは、グラフの宛先です。

ステップ 9　[Fetch] をクリックしてグラフを表示します。

（注）　結果として得られたグラフに送信元から宛先へのパスがトレースされていない場合は、次のいずれかが原因となっている可能性があります。

- L2MP クラウド内のアイランド。
- DCNM-LAN で中間デバイスが管理されていない。

マルチキャスト

マルチキャスト グラフには、指定したデバイスから特定の IGMP グループをリッスンしているすべてのホストへのマルチキャスト トラフィックが表示されます。特定のトポロジのマルチキャスト情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

（注）　トポロジ ツールバーのアイコンの名前を表示するには、マウス ポインタをアイコンに移動します。しばらくすると、アイコンの名前が表示されます。

ステップ 2　マップの上部にある [L2 View] をクリックします。

[Contents] ペインにダイアログボックスが表示されます。

ステップ 3　ダイアログボックスで [Fabricpath] ビューを選択します。

ステップ 4　トポロジ ID を入力します。表示されるグラフは、トポロジ ID に基づいてフィルタリングされます。

ステップ 5　[Select type of graph] をオンにしてマルチキャスト グラフの選択をイネーブルにします。

ステップ 6　[Multicast] オプションをオンにします。

ステップ 7　[Anchor] ドロップダウン リストからデバイスを選択します。選択したデバイスは、グラフのエントリ ポイントです。

ステップ 8　[Graph ID] ドロップダウン リストから ID を選択します。グラフ ID は、グラフの転送タグです。

ステップ 9　[Source] フィールドに、マルチキャストの発信元デバイスを入力します。マルチキャストの発信元デバイスは IP アドレスまたは「*」（ワイルドカード）として指定されます。

ステップ 10　[IGMP] フィールドに、IGMP グループ アドレスを入力します。

ステップ 11　[VLAN] フィールドに、マルチキャスト関連の VLAN 情報を入力します。

ステップ 12　[Fetch] をクリックしてグラフを表示します。

vPC ウィザードの起動

トポロジ マップから vPC ウィザードを起動して vPC を作成できます。

はじめる前に

vPC ピア スイッチとして使用する 2 台のデバイスを決定します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。

ステップ 2　マップの上で、[PortChannel and vPC] をクリックします。

マップにトポロジの [PortChannel and vPC] ビューが表示されます。

ステップ 3　トポロジ ツールバーで、アイコンを選択します。

ステップ 4　vPC ピア スイッチとして使用する 1 台のデバイスをクリックします。

ステップ 5　**Shift** キーを押したままにします。

ステップ 6　vPC ピア スイッチとして使用するデバイスをクリックします。

ステップ 7　いずれかのデバイスを右クリックし、[Launch vPC Wizard] を選択します。

[vPC Creation Wizard] ダイアログボックスが表示されます。

このウィザードの使用方法の詳細については、『*Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

vPC の管理

トポロジ マップから、特定の vPC リンクの vPC 機能にアクセスできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。

ステップ 2　マップの上で次のいずれかのビューをクリックします。

- **PortChannel and vPC**
- **Logical vPC View**

ステップ 3　管理する vPC の vPC リンクを探します。

ステップ 4　選択したビュー応じて次の該当する手順を実行します。

- [PortChannel and vPC] : vPC リンク上の楕円を右クリックし、[Manage vPC] を選択します。
- [Logical vPC View] : vPC リンクを右クリックし、[Manage vPC] を選択します。

vPC 機能が表示されます。管理する vPC が要約テーブルで選択されます。

vPC 機能の詳細については、『*Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

vPC 設定の不一致の検索と解決

トポロジ マップを使用して、設定上の不一致がある vPC を検索し、[Resolve Configuration Inconsistency] ダイアログボックスを開くことができます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。

ステップ 2　マップの上で次のいずれかのビューをクリックします。

- **PortChannel and vPC**
- **Logical vPC View**

ステップ 3　設定上の不一致を解決する vPC を探します。

vPC リンクに設定上の不一致がある場合、リンク上に赤い楕円が表示されます。[PortChannel and vPC] ビューを使用する場合、設定上の不一致がある vPC ピア リンクにも赤い楕円が表示されます。

ステップ 4　（任意）設定上の不一致をすぐに解決する場合には、次のいずれかを行います。

- vPC リンク*および*vPC ピア リンクの設定上の不一致を解決するには、vPC リンク上の赤い楕円を右クリックし、[Launch Configuration Consistency] を選択します。
- vPC ピア リンクの設定上の不一致だけを解決するには、vPC リンク上の赤い楕円を右クリックし、[Launch Configuration Consistency] を選択します。

[Resolve Configuration Inconsistency] ダイアログボックスが表示されます。

[Resolve Configuration Inconsistencies] ダイアログボックスの使用方法の詳細については、『*Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

トポロジ マップからのリモート接続された CNA へのアクセス

トポロジ マップを使用して、Cisco Nexus 4000 シリーズ スイッチに接続されたサーバにアクセスできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。トポロジ マップの左側には、トポロジ ツールバーが表示されます。

ステップ 2　スイッチを右クリックして、[Show End Devices] を選択します。

[Contents] ペインに、スイッチに接続されているすべてのサーバが表示されます。IP アドレスが FIP スヌーピングの enode 情報の一部として使用できないため、サーバの pWWN だけが表示されます。

VSAN オーバーレイの使用方法

トポロジ マップから VSAN オーバーレイ機能にアクセスするには、次の手順を実行します。

ステップ 1　[Feature Selector] ペインで、[Topology] > [Topology View] を選択します。

[Contents] ペインに、トポロジ マップが表示されます。

ステップ 2　マップの上部にある [L2 View] をクリックします。

[Contents] ペインにダイアログボックスが表示されます。

ステップ 3　ダイアログボックスで [VSAN] をクリックします。

ステップ 4　検索の範囲を入力します（有効な値は 1 ～ 4094 です）。

ステップ 5　[View mapped VLANs] をオンにして VLAN を表示します。

ステップ 6　[Fetch] をクリックします。

関連資料

トポロジ マップに関する追加情報については、次のセクションを参照してください。

関連項目	参照先
VDC	『*Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
vPC	『*Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
管理対象デバイス上での LLDP の設定	『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」
デバイス グループ	第 21 章「デバイス グループの設定」
ネットワーク サーバ	第 20 章「ネットワーク サーバの設定」

トポロジの機能履歴

表 19-1 は、この機能のリリースの履歴です。

表 19-1　トポロジの機能履歴

機能名	リリース	機能情報
共通のトポロジ	5.0(2)	SAN デバイスと接続に対するサポートが追加されました。
ネットワーク サーバ	5.0(2)	ネットワーク サーバを表示するためのサポートが追加されました。
DCNM-SAN のサポート	5.0(2)	Cisco DCNM-SAN クライアントの起動のサポートが追加されました。
デバイス グループ	5.0(2)	デバイス グループのサポートが追加されました。
VSAN オーバーレイ	5.1(0)	VSAN オーバーレイのサポートが L2 ビューの一部として追加されました。
CNA を介して Cisco Nexus 5000 シリーズ スイッチに接続されたサーバの検出	5.1(0)	Cisco Nexus 5000 シリーズ スイッチまたは CNA に直接接続されたサーバの検出のサポート。
FabricPath のサポート	5.1(0)	FabricPath のサポートが追加されました。

CHAPTER 20

ネットワーク サーバの設定

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）のネットワーク サーバ機能を設定する方法について説明します。

この章の内容は、次のとおりです。

- 「ネットワーク サーバの概要」（P.20-1）
- 「ネットワーク サーバのライセンス要件」（P.20-2）
- 「ネットワーク サーバの前提条件」（P.20-3）
- 「ネットワーク サーバに関する注意事項および制約事項」（P.20-3）
- 「ネットワーク サーバの設定」（P.20-3）
- 「サーバ接続情報の表示」（P.20-11）
- 「ネットワーク サーバのフィールドの説明」（P.20-11）
- 「その他の関連資料」（P.20-14）
- 「ネットワーク サーバの機能の履歴」（P.20-15）

ネットワーク サーバの概要

DCNM-LAN では、デバイス ディスカバリの際に、ネットワークの Cisco NX-OS デバイスに接続されているネットワーク サーバについてホスト バス アダプタ（HBA）とイーサネット ネットワーク アダプタを検出できます。DCNM-LAN は、リンク層検出プロトコル（LLDP）を使ってネットワーク サーバからイーサネット ネットワーク アダプタに関する情報を取得します。ただし、LLDP によって取得される情報は、検出されたネットワーク アダプタが同じネットワーク サーバに含まれるかどうかを DCNM-LAN が判別するには適していません。

DCNM-LAN Release 5.1 以降では、DCNM-LAN を使用して、次のシナリオのサーバを検出できます。

- Cisco Nexus 5000 シリーズ スイッチに直接接続されている統合型ネットワーク アダプタ（CNA）を搭載しているサーバ。
- Nexus 2000 経由で Nexus 5000 シリーズ スイッチに接続されている CNA を搭載しているサーバ。
- Nexus 7000 シリーズ スイッチに直接接続されている CNA を搭載しているサーバ。

（注） Nexus 7000 シリーズ スイッチに接続された Nexus 2000 シリーズ スイッチ上では LLDP がサポートされないため、Nexus 2000 シリーズ スイッチ経由で Nexus 7000 シリーズ スイッチに接続された CNA を搭載しているサーバは、Cisco DCNM-LAN で検出できません。

検出された CNA アダプタは [Static Server-Adapter Mapping] 機能ペインで確認できます。DCNM-LAN では、CNA 経由で Cisco Nexus 5000 シリーズ スイッチに接続されているアダプタを自動で関連付けることはできません。ただし、ネットワーク サーバに属する CNA アダプタを手動で関連付けることはできます。検出プロセスの詳細については、第 16 章「デバイス ディスカバリの管理」を参照してください。

ネットワーク サーバ機能を使うと、DCNM-LAN が LLDP を介して検出した HBA およびイーサネット ネットワーク アダプタをサーバに関連付けることができます。定義するネットワーク サーバをトポロジ マップで表示できます。

（注）　DCNM-LAN で検出および管理できるのは、VMware ESX サーバ（ESX サーバ上にホストされている仮想マシンを含む）、Linux サーバ、および Windows 2008 サーバだけです。

また、ネットワーク サーバ機能を使うと、サーバの接続情報を表示することもできます。

アダプタとサーバの自動関連付け

ネットワーク サーバへログインできる有効なユーザ名およびパスワードを DCNM-LAN に設定すると、DCNM-LAN は、ネットワーク サーバのネットワーク アダプタを自動的に関連付けることができます。これにより、DCNM-LAN は、検出されたどのアダプタが同じネットワーク サーバに属しているか判定するのに必要な情報をネットワーク サーバから取得できるようになります。DCNM-LAN のトポロジ ビューでは、アダプタとサーバの間の関連付けがグラフィック表示されます。

DCNM-LAN がネットワーク サーバに正常にログインして接続情報を取得できる場合、そのサーバは管理されていると見なされます。

ネットワーク サーバの管理を簡略化するために、DCNM-LAN サーバ関連付け機能を使用して、ログイン クレデンシャルを複数のサーバに設定できます。複数のサーバを、同じクレデンシャルまたはサーバごとに一意なクレデンシャルを使用するように設定できます。

アダプタとサーバの手動関連付け

ネットワーク サーバにログインするためのクレデンシャルを DCNM-LAN に指定できない場合は、アダプタとネットワーク サーバを手動で関連付け（バインド）できます。

ネットワーク サーバのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	ネットワーク サーバにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

ネットワーク サーバの前提条件

ネットワーク サーバ機能の前提条件は、次のとおりです。

- LLDP がネットワーク サーバでイネーブルになっている必要があります。
- ネットワーク サーバ機能を使ってアダプタとサーバを自動的に関連付ける、または手動でバインドするには、前もって DCNM-LAN によってサーバのネットワーク アダプタが検出されていることが必要です。

ネットワーク サーバに関する注意事項および制約事項

ネットワーク サーバ機能に関する設定時の注意事項および制約事項は、次のとおりです。

- DCNM-LAN は、Linux オペレーティング システムが動作しているネットワーク サーバを検出できます。
- DCNM-LAN は、Emulex 製または Qlogic 製の HBA ポートの場合にのみ、ネットワーク サーバを自動的に関連付けできます。
- DCNM-LAN は、Linux オペレーティング システム サーバ上と ESX サーバ上のアダプタのみを自動的に関連付けできます。
- DCNM-LAN がサポートする CNA は、Emulex 製と Qlogic 製のみです。
- CNA はサーバの IP アドレスをアドバタイズしないため、最初の 1 つを手動で関連付けておく必要があります。それ以降のエントリに対しては自動関連付けを実行することができます。

ネットワーク サーバの設定

ここでは、次の内容について説明します。

- 「デフォルトのサーバ クレデンシャルの設定」（P.20-3）
- 「デフォルトのサーバ クレデンシャルの消去」（P.20-4）
- 「サーバの一意なクレデンシャルの設定」（P.20-5）
- 「サーバの一意なクレデンシャルの消去」（P.20-6）
- 「サーバの関連付け」（P.20-6）
- 「サーバとアダプタの自動関連付け」（P.20-9）
- 「アダプタとサーバの手動バインド」（P.20-10）
- 「アダプタとサーバのアンバインド」（P.20-10）

デフォルトのサーバ クレデンシャルの設定

デフォルトのサーバ クレデンシャルを設定できます。DCNM-LAN が、新たに検出されたサーバに接続するときにこの情報を使って認証します。一意なサーバ クレデンシャルをまだ設定していない検出済みサーバそれぞれと通信するとき、DCNM-LAN はデフォルトのサーバ クレデンシャルを使用します。

（注）　サーバ クレデンシャルは DCNM-LAN ユーザごとに一意です。

はじめる前に

デフォルトのサーバ クレデンシャルの内容を決めます。DCNM-LAN がデフォルトのサーバ クレデンシャルを使って通信するすべてのサーバには、DCNM-LAN に設定するデフォルト サーバ クレデンシャルと同じユーザ名とパスワードのユーザ アカウントが必要です。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Server Credentials] の順に選択します。

[Contents] ペイン内の [Servers] 領域の上の [Server Credentials] 領域に、検出済みのサーバの一覧が表示されます。

ステップ 2　[User Name] フィールドに、デフォルトのサーバ クレデンシャルのユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 3　[Password] フィールドの右側にある下矢印ボタンをクリックします。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、デフォルトのクレデンシャルのパスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、デフォルトのクレデンシャルを保存します。

デフォルトのサーバ クレデンシャルの消去

デフォルトのサーバ クレデンシャルを消去できます。

（注）　デフォルトのサーバ クレデンシャルを消去すると、各管理対象サーバに一意なクレデンシャルを設定していない限り、DCNM-LAN は検出済みのサーバに接続できなくなります。

はじめる前に

デフォルトのサーバ クレデンシャルを使わずに DCNM-LAN を使用する予定であれば、この手順を実行する前に、検出済みの各サーバに対する一意なサーバ クレデンシャルを DCNM-LAN に設定してください。

詳細については、「サーバの一意なクレデンシャルの設定」（P.20-5）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Server Credentials] の順に選択します。

[Contents] ペイン内の [Servers] 領域の上の [Server Credentials] 領域に、検出済みのサーバの一覧が表示されます。

ステップ 2　[Default Credentials] 領域で、[Clear] をクリックします。

[User Name] フィールドと [Password] フィールドが消去されます。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

サーバの一意なクレデンシャルの設定

検出済みのサーバに一意なクレデンシャルを設定できます。検出済みのサーバに一意なクレデンシャルが存在する場合、DCNM-LAN は、デフォルトのサーバ クレデンシャルではなく一意なクレデンシャルを使用してそのサーバに接続します。

（注）　サーバ クレデンシャルは DCNM-LAN ユーザごとに一意です。

はじめる前に

検出済みのサーバに設定されているユーザ アカウントのユーザ名とパスワードを確認してください。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Server Credentials] の順に選択します。

[Contents] ペインの [Servers] 領域に検出済みのサーバが表示されます。

ステップ 2　サーバの [User Credentials] 列で、入力値をダブルクリックして、下矢印ボタンをクリックします。

ステップ 3　[User Name] フィールドに、ユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 5　[OK] をクリックします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、DCNM-LAN サーバにサーバ クレデンシャルを保存します。

サーバの一意なクレデンシャルの消去

検出済みサーバの一意なクレデンシャルを消去できます。

（注）　検出済みサーバの一意なクレデンシャルを消去すると、DCNM-LAN はデフォルトのクレデンシャルを使用してサーバに接続するようになります。

はじめる前に

一意なサーバ クレデンシャルなしで DCNM-LAN を運用する場合は、次の手順を実行する前に、DCNM-LAN にデフォルトのサーバ クレデンシャルが設定されていることを確認してください。

詳細については、「デフォルトのサーバ クレデンシャルの設定」（P.20-3）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Server Credentials] の順に選択します。

[Contents] ペインの [Servers] 領域に検出済みのサーバが表示されます。

ステップ 2　[Servers] 領域で、クレデンシャルを消去するサーバをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Clear Credentials] の順に選択します。

確認用のダイアログボックスが表示されます。

ステップ 4　[Yes] をクリックします。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

サーバの関連付け

サーバの関連付けは、サーバの範囲を管理するのに役立ちます。サーバの範囲に対して 1 つの操作が実行されると、その範囲内のすべてのサーバに対してその操作が適用されます。

はじめる前に

該当するプラットフォームについて次の内容を確認および設定しておく必要があります。

- Windows Server 2003 の場合
  - Windows Server 2003 R2（5.2.3970 以降のバージョン）のみがサポートされている。
  - WinRM システム ユーティリティがインストールされている。
    （Windows Server インストレーション CD または Microsoft Support サイトから入手可能）。
  - Telnet サービスがイネーブルになっていて、動作している。
  - ユーザ レベル権限がイネーブルになっている。
  - NIC が識別されている。
    NIC が識別されていることを確認するには、**iponfig /all** CLI コマンドを使用できます。
  - HBA が識別されている。
    HBA が識別されていることを確認するには、**winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI コマンドを使用できます。

（注）　HBA がサーバに搭載されていないと、コマンド出力にエラーが表示される場合があります。これは予想どおりの結果です。このエラーは無視してください。

- Windows Server 2008 の場合
  - Windows Server 2008 Standard、Enterprise、および R2（6.0.6001 以降のバージョン）がサポートされている。
  - WinRM システム ユーティリティがインストールされている。
  - Telnet サービスがイネーブルになっていて、動作している。
  - ユーザ レベル権限がイネーブルになっている。
  - NIC が識別されている。
    NIC が識別されていることを確認するには、**iponfig /all** CLI コマンドを使用できます。
  - HBA が識別されている。
    HBA が識別されていることを確認するには、**winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI コマンドを使用できます。

（注）　HBA がサーバに搭載されていないと、コマンド出力にエラーが表示される場合があります。これは予想どおりの結果です。このエラーは無視してください。

- RHEL の場合
  - RHEL 4.5 がサポートされている。
  - SSH がイネーブルになっている。
  - ユーザ レベル権限がイネーブルになっている。
  - NIC が識別されている。
    NIC が識別されていることを確認するには、**ifconfig -a** CLI コマンドを使用できます。
  - HBA が識別されている。

    Qlogic HBA が識別されていることを確認するには、
    grep adapter-port /proc/scsi/qla2xxx/* CLI コマンドを使用できます。

    Emulex HBA が識別されていることを確認するには、**find /sys/class/scsi_host/ -name port_name** CLI コマンドと **find /sys/class/fc_host/ -name port_name** CLI コマンドを使用できます。

    情報をまとめて表示するには、結果として得られたファイルに「cat」を使用します。
- VMware ESX の場合
  - ESX 3.5 以降のバージョンがサポートされている。
  - SSH がイネーブルになっている。
  - NIC が識別されている。
    NIC が識別されていることを確認するには、**esxcfg-nics -l** CLI コマンドを使用できます。
  - HBA が識別されている。
    HBA が識別されていることを確認するには、**esxcfg-scsidevs -a** CLI コマンドを使用できます。
  - Qlogic 製と Emulex 製の HBA および CNA がテスト済みであり、サポートされている。

（注）　仮想マシンの場合、HBA 情報は仮想マシン内で表示されません。仮想マシン表示では、SAN の詳細が仮想マシンに対してディセーブルになっています。HBA 情報は、ESX 内で表示されます。

- デバイスのバージョン サポート
  - Nexus 7000 の場合、5.0 以降で LLDP がサポートされている。
  - Nexus 5000 の場合、4.2(1)N1(1) 以降で LLDP がサポートされている。
  - Nexus 5000 の場合、すべてのバージョンで FC がサポートされている。
  - MDS の場合、3.3(2) 以降でサポートされている。

表 20-1 に、プラットフォームごとのサポートの要約を示します。

表 20-1　要約

	Windows Server 2003	Windows Server 2008	RHEL	ESX
サポートされる NIC	すべて	すべて	すべて	すべて
サポートされる HBA	Qlogic、Emulex	Qlogic、Emulex	Qlogic、Emulex	Qlogic、Emulex
サポートされる CNA	Qlogic、Emulex	Qlogic、Emulex	Qlogic、Emulex	Qlogic、Emulex
オペレーティング システム	R2（すべてのエディション） 32 ビットと 64 ビット	すべてのエディション 32 ビットと 64 ビット	RHEL 4.5	ESX 3.5
必要なサービス	Telnet/SSH WinRM	Telnet/SSH WinRM	SSH/Telnet	SSH/Telnet
権限	ユーザ レベル権限	ユーザ レベル権限	ユーザ レベル権限	ユーザ レベル権限

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Server Credentials] の順に選択します。
[Contents] ペインの [Servers] 領域に検出済みのサーバが表示されます。

ステップ 2　[Servers] ペイン内で右クリックして、コンテキスト メニューにアクセスします。

ステップ 3　コンテキスト メニュー内の [New Server] を選択します。
新しいサーバ用の行が表示されます。

ステップ 4　[IP Address] フィールドに、サーバの範囲の IP アドレスを入力します。
IP アドレスは、カンマまたはハイフンで区切ります。
IP アドレスが入力された後、それらのアドレスはシステムによって検証されます。枠が赤色の場合はエラー状態です。枠が黄色の場合は有効なエントリです。

ステップ 5　[User Credentials] フィールドをダブルクリックして、[Set User Credentials] ダイアログボックスを表示します。

ステップ 6　[User Name] フィールドに、ユーザ名を入力します。有効なユーザ名は 1 ～ 32 文字です。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 7　[Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。数字、記号、文字（大文字小文字を区別）を使用できます。

ステップ 8　[OK] をクリックします。

ステップ 9　メニュー バーで、[File] > [Deploy] の順に選択して、設定を DCNM-LAN サーバに保存します。

ステップ 10　サーバ関連付けを開始するには、対象の行またはその範囲内の 1 台のサーバを右クリックして、コンテキスト メニューにアクセスします。

ステップ 11　コンテキスト メニュー内の [Correlate] を選択します。

この操作により、各サーバのステータスが [Discovering] に変化します。操作が完了すると、アダプタがサーバにバインドされます。操作が失敗すると、サーバのステータスが [Unreachable] になり、メッセージが表示されます。

サーバとアダプタの自動関連付け

DCNM-LAN は、Linux オペレーティング システムを実行するサーバにログインし、そこで取得するネットワーク接続情報を使用して、検出した HBA ネットワーク アダプタを Linux サーバに関連付けることができます。

はじめる前に

DCNM-LAN で HBA アダプタを自動的に関連付けるサーバに、有効なサーバ クレデンシャルを設定する必要があります。サーバに対して一意なクレデンシャルを設定するか、そのクレデンシャルが他のサーバに対しても有効な場合は、デフォルトのサーバ クレデンシャルを設定できます。

（注）　サーバ クレデンシャルを使用できない場合は、アダプタとサーバを手動でバインドできます。詳細については、「アダプタとサーバの手動バインド」（P.20-10）を参照してください。

DCNM-LAN によって、1 つ以上の HBA ネットワーク アダプタと 1 台のネットワーク サーバがすでに検出されていることが必要です。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Servers] の順に選択します。

[Summary] ペインの [Servers] 領域に検出済みのサーバが表示されます。

ステップ 2　[Server] 列で、アダプタと自動的に関連付けるサーバをクリックします。

ヒント 一度に複数のサーバを関連付ける場合は、Ctrl キーを押した状態で、アダプタと関連付ける各サーバをクリックします。

ステップ 3　選択したサーバを右クリックして、[Correlate Server(s)] を選択します。

DCNM-LAN によって、選択したサーバからのネットワーク接続情報の検出が開始されます。

検出が完了すると、サーバに関連付けられているその他の接続が [Connected Switches] 列に表示されます。選択したサーバの右側に表示されるローカル トポロジも、サーバに関連付けられたその他の接続を表示するように更新されます。

アダプタとサーバの手動バインド

DCNM-LAN では、検出した HBA ネットワーク アダプタを検出済みのサーバに関連付けることができます。このプロセスは、DCNM-LAN がサーバにログインして情報を取得できるかどうかには関係ありません。

アダプタとサーバのバインドを正常に行うと、管理対象デバイスとサーバの接続がトポロジ マップに表示されます。

はじめる前に

DCNM-LAN によって、1 つ以上の HBA ネットワーク アダプタが検出されていることが必要です。

DCNM-LAN で、アダプタをバインドするサーバに IP アドレスまたは DNS 名を使って接続できることが必要です。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Static Server-Adapter Mapping] の順に選択します。

[Contents] ペインに、検出された HBA ネットワーク アダプタのリストが表示されます。

ステップ 2　Ctrl キーを押した状態で、サーバにバインドする各アダプタをクリックします。

ステップ 3　選択したアダプタのいずれかを右クリックし、[Bind to Server] を選択します。

[Enter Server Name] ダイアログボックスが表示されます。

ステップ 4　[Server Name] フィールドに、サーバの IP アドレスまたは DNS 名を入力して、[OK] をクリックします。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

トポロジ マップでは、アダプタと管理対象デバイス間の接続を表示できます（管理対象デバイスのエンド デバイスへの接続を表示するように選択したとき）。

アダプタとサーバのアンバインド

作成したサーバとアダプタのバインドを削除できます。このプロセスは、DCNM-LAN がサーバにログインして情報を取得できるかどうかには関係ありません。

はじめる前に

削除するサーバとアダプタのバインドが DCNM-LAN に存在する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Static Server-Adapter Mapping] の順に選択します。
[Contents] ペインに、検出された HBA ネットワーク アダプタのリストが表示されます。

ステップ 2　[Server Port] 列で、アンバインドするアダプタをクリックします。

ステップ 3　そのアダプタを右クリックして、[Unbind from Server] を選択します。
選択したアダプタの [Server Name] フィールドが消去されます。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。
トポロジ マップで、アダプタと管理対象デバイス間の接続が表示できなくなります。

サーバ接続情報の表示

DCNM-LAN サーバの接続情報を表示できます。

ステップ 1　[Feature Selector] ペインで、[Network Servers] > [Servers] の順に選択します。
[Summary] ペインに検出済みサーバのリストが表示されます。

ステップ 2　[Summary] ペインで、ネットワーク接続情報を表示するサーバをクリックします。
そのサーバのローカル トポロジが [Summary] ペインの右側に表示されます。

ステップ 3　（任意）サーバに関してイーサネット ネットワークまたはストレージ エリア ネットワークの接続を [Server Details] タブに表示する場合は、必要に応じて [LAN Connectivity] セクションまたは [SAN Connectivity] を展開します。

ネットワーク サーバのフィールドの説明

ここでは、ネットワーク サーバ機能における次の各フィールドについて説明します。

- 「サーバのフィールドの説明」（P.20-11）
- 「[Servers Summary] ペイン」（P.20-12）
- 「[Server Credentials] のフィールドの説明」（P.20-13）

サーバのフィールドの説明

ここでは、次の各フィールドについて説明します。

- 「[Servers Summary] ペイン」（P.20-12）
- 「[Server] : [Server Details] : [LAN Connectivity] セクション」（P.20-12）

- 「[Server]：[Server Details]：[LAN Connectivity] セクション」（P.20-12）

[Servers Summary] ペイン

表 20-2　[Servers Summary] ペイン

フィールド	説明
Server	*表示のみ。*サーバの DNS 名または IP アドレス。DCNM-LAN によってサーバの DNS 名が判別できなかった場合は、IP アドレスが表示されます。
Connected Switches	*表示のみ。*サーバに接続している各検出済みデバイスの名前と IP アドレス。
Status	*表示のみ。*DCNM-LAN サーバがサーバに接続してログインできるかどうかを示します。有効な値は、次のとおりです。 • [Managed]：DCNM-LAN がサーバ アダプタの自動関連付けの際に、サーバに正常にログインしました。 • [Unmanaged]：DCNM-LAN はまだサーバへのログインを試行していません。デフォルトでは、検出済みサーバは、アダプタの自動関連付けを試行するまでは管理対象外です。 • [Unreachable]：サーバ アダプタの自動関連付けの際に、DCNM-LAN がサーバに接続できませんでした。または、認証に失敗しました。メッセージによってこのステータスの理由が示されます。

[Server]：[Server Details]：[LAN Connectivity] セクション

表 20-3　[Server]：[Server Details]：[LAN Connectivity] セクション

フィールド	説明
Switch	
Name	*表示のみ。*サーバがイーサネット接続で接続しているデバイスの名前と IP アドレス。
Port Name	*表示のみ。*デバイスのイーサネット インターフェイスの名前（Ethernet1/2 など）。
Server	
MAC Address	*表示のみ。*デバイスに接続しているサーバのイーサネット アダプタの MAC アドレス。
Port Name	*表示のみ。*サーバのインターフェイスの名前。

[Server]：[Server Details]：[SAN Connectivity] セクション

表 20-4　[Server]：[Server Details]：[SAN Connectivity] セクション

フィールド	説明
Switch	
Name	*表示のみ。*サーバがファイバ チャネル接続で接続しているデバイスの名前と IP アドレス。

表 20-4　[Server] : [Server Details] : [SAN Connectivity] セクション （続き）

フィールド	説明
FC Port WWN	*表示のみ。*デバイスのファイバ チャネル インターフェイスの World Wide Name（WWN）。
Port Name	*表示のみ。*デバイスのファイバ チャネル インターフェイスの名前（Fc1/4 など）。
Server	
FC Port WWN	*表示のみ。*サーバの HBA インターフェイスの World Wide Name。

[Static Server-Adapter Mapping] のフィールドの説明

表 20-5　[Static Server-Adapter Mapping] の [Contents] ペイン

フィールド	説明
Server Port	*表示のみ。*アダプタのタイプに応じて、次のようにサーバ アダプタが示されます。 • HBA アダプタの場合、アダプタに割り当てられた WWN がこのフィールドに表示されます。 • イーサネット アダプタの場合、アダプタの MAC アドレスがこのフィールドに表示されます。イーサネット アダプタが [Static Server-Adapter Mapping] の [Contents] ペインに表示されるのは、LLDP でサーバがアダプタの IP アドレスをアドバタイズしないときです。
Server Name	アダプタがバインドされるネットワーク サーバの DNS 名または IP アドレス。
Vendor	*表示のみ。*アダプタの製造元の名前。
Switch Port	*表示のみ。*接続しているデバイスのファイバ チャネル インターフェイスの名前と WWN。
Switch Name	*表示のみ。*接続しているデバイスの名前と IP アドレス。

[Server Credentials] のフィールドの説明

表 20-6　[Server Credentials] の [Contents] ペイン

フィールド	説明
Default Credentials	
User Name	サーバ ユーザ アカウントの名前。DCNM-LAN サーバが検出または管理するサーバにアクセスするときに、このアカウントを使用します。サーバにおいて、このユーザ アカウントは、サーバ ネットワーク アダプタの情報を取得するために適切な権限を含む必要があります。 **（注）** [Default Credentials] セクションの情報は、[Servers] 領域の [User Credentials] フィールド内の情報によって上書きされます。
Password	[User Name] フィールドに、指定したサーバ ユーザ アカウントのパスワード。デフォルトでは、このフィールドは空白です。

表 20-6　[Server Credentials] の [Contents] ペイン （続き）

フィールド	説明
Servers	
IP Address	*表示のみ*。サーバの IPv4 アドレス。
Name	*表示のみ*。サーバの名前。DCNM-LAN によってサーバ名が判別できない場合は、サーバの IP アドレスが表示されます。
User Credentials	DCNM-LAN がサーバに接続するために使うサーバ ユーザ アカウント。 **（注）** このフィールドを設定すると、DCNM-LAN は、サーバに接続するときにこのユーザ アカウントを使用します。このフィールドが空白の場合、DCNM-LAN は、[Default Credentials] 領域に指定されたユーザ アカウントを使用します。デフォルトでは、このフィールドは空白です。
Status	*表示のみ*。DCNM-LAN サーバがサーバに接続してログインできるかどうかを示します。有効な値は、次のとおりです。 • [Managed] : DCNM-LAN がサーバ アダプタの自動関連付けの際に、サーバに正常にログインしました。 • [Unmanaged] : DCNM-LAN はまだサーバへのログインを試行していません。デフォルトでは、検出済みサーバは、アダプタの自動関連付けを試行するまでは管理対象外です。 • [Unreachable] : サーバ アダプタの自動関連付けの際に、DCNM-LAN がサーバに接続できませんでした。または、認証に失敗しました。メッセージによってこのステータスの理由が示されます。

その他の関連資料

ネットワーク サーバの管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.20-14）
- 「標準」（P.20-15）

関連資料

関連項目	参照先
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」
トポロジ マップ	第 19 章「トポロジの作業」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

ネットワーク サーバの機能の履歴

表 20-7 は、この機能のリリースの履歴です。

表 20-7　ネットワーク サーバの機能の履歴

機能名	リリース	機能情報
ネットワーク サーバ	5.0(2)	サポートが追加されました。

CHAPTER 21

デバイス グループの設定

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）のデバイス グループ機能の設定方法について説明します。

この章の内容は、次のとおりです。

- 「デバイス グループの概要」（P.21-1）
- 「デバイス グループのライセンス要件」（P.21-2）
- 「デバイス グループの前提条件」（P.21-2）
- 「デバイス グループの注意事項と制約事項」（P.21-2）
- 「デバイス グループの設定」（P.21-2）
- 「関連情報」（P.21-6）
- 「デバイス グループのフィールドの説明」（P.21-6）
- 「その他の関連資料」（P.21-7）
- 「デバイス グループ機能の履歴」（P.21-8）

デバイス グループの概要

デバイス グループを使用すると、トポロジ機能でデバイスのグループ間の相互接続を簡単に視覚化できます。定義したデバイス グループにデバイスを分類することで、トポロジを表示する際に、限られた数のデバイスに焦点を絞ることができます。デバイス グループを使用することで、DCNM-LAN によるデータセンターの管理をより効率的に行うことができます。

たとえば、次のいずれかの基準を用いて、デバイスのグループを作成できます。

- 場所：都市、あるいはデータセンターの指定ラックというような具体的な物理的場所に基づいてデバイスをグループ化できます。
- 管理者：デバイスを管理する DCNM-LAN ユーザに基づいてデバイスをグループ化できます。
- データセンター アーキテクチャ：アグリゲーション、アクセス、ストレージのレイヤなど、データセンターのネットワーク アーキテクチャのレイヤに基づいてデバイスをグループ化できます。
- デバイス タイプ：Cisco Nexus 7000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチなど、デバイスのタイプに基づいてデバイスをグループ化できます。

1 台のデバイスがメンバーになれるグループは 1 つだけです。

デフォルトのデバイス グループは、カスタム デバイス グループに割り当てていないすべてのデバイスを含みます。新しく検出されたデバイスはいずれも、デフォルトのグループに入ります。

デバイス グループのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	デバイス グループにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイス グループの前提条件

デバイス グループ機能には次の前提条件があります。

- デバイスをデバイス グループに割り当てるには、事前にデバイスが検出されている必要があります。

デバイス グループの注意事項と制約事項

デバイス グループ機能における設定時の注意事項と制約事項は次のとおりです。

- デフォルトでは、検出されたすべてのデバイスはデフォルトのデバイス グループに属します。
- 1 台のデバイスがメンバーになれるグループは 1 つだけです。
- Virtual Device Context（VDC; 仮想デバイス コンテキスト）をサポートする物理デバイスの場合は、同じ物理デバイス上に存在する VDC を別のデバイス グループに割り当てることができます。
- ご使用のネットワーク トポロジが最も簡素化されるような、デバイス グループへのデバイスの分類方法を選択します。

デバイス グループの設定

ここでは、次の内容について説明します。

- 「デバイス グループの作成」（P.21-2）
- 「グループへのデバイスの追加」（P.21-4）
- 「グループからのデバイスの削除」（P.21-5）
- 「デバイス グループの削除」（P.21-5）

デバイス グループの作成

デバイス グループを作成し、1 つ以上のデバイスを追加できます。

デフォルトのグループは 1 つだけ存在します。他のすべてのグループは、カスタム デバイス グループです。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Groups] の順に選択します。

[Summary] ペインにカスタム デバイス グループがあれば一覧表示されます。デフォルト グループは表示されません。

[Details] ペインにグループ名、説明、グループ内のデバイス一覧が表示されます。

ステップ 2　メニュー バーで、[Actions] > [Create Device Group] の順に選択します。

[Summary] テーブルに空白の行が表示されます。

ステップ 3　空白行の [Device Group Name] にグループの名前を入力します。

ステップ 4　（任意）[Description] にグループについてわかりやすい説明を入力します。

ステップ 5　必要に応じて、[Details] ペインの [Membership Details] セクションを展開します。

ステップ 6　デバイスをグループに追加する手順は、次のとおりです。

a. [Membership Details] セクションの列名の下を右クリックし、[Add Device] を選択します。

[Device Selection] ダイアログボックスが表示されます。

b. （任意）[Select Search Criteria] ドロップダウン リストを使用して、[Available Devices] リストに表示されているデバイスをフィルタします。次のいずれかの方法でデバイスをフィルタできます。

- All devices：検出されたデバイスをすべて表示します。
- Device type：検出されたデバイスのうち、Cisco Nexus 7000 シリーズ スイッチなど、選択したタイプのデバイスだけを表示します。
- Unsupported devices：DCNM-LAN で管理および監視できない検出済みデバイスを表示します。
- Connected devices：IP アドレスで指定するシード デバイスまで、指定するホップ カウント以内で接続された検出済みデバイスを表示します。
- Subnet devices：サブネットおよびサブネット マスクの IP アドレスで指定するサブネット内の IP アドレスを持つ検出済みデバイスを表示します。

c. 1 台以上のデバイスを [Available Devices] リストから [Selected Devices] リストに移動します。

デバイスを 1 台移動するには、デバイスをクリックしてから [Add] をクリックします。

複数のデバイスを移動するには、Ctrl キーを押しながら各デバイスをクリックし、[Add] をクリックします。

d. [OK] をクリックします。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択してデバイス グループの設定を保存します。

新しいグループはトポロジ マップで使用できます。

新しいデバイス グループに追加した各デバイスは、以前のグループから削除されます。以前から存在しているデフォルト以外のデバイス グループが、そのデバイスをすべて新しいデバイス グループに移動したことで空になった場合、DCNM-LAN は空になったデバイス グループを自動的に削除します。

グループへのデバイスの追加

既存のデバイス グループにデバイスを追加できます。

すべてのデバイスはいずれかのグループに属します。属すグループは 1 つだけです。カスタム デバイス グループのメンバーではないデバイスは、デフォルトのデバイス グループに自動的に属します。

グループにデバイスを追加すると、そのデバイスは以前属していたグループから自動的に削除されます。

はじめる前に

デバイスを追加するデバイス グループが存在することを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Groups] の順に選択します。

[Summary] ペインにカスタム デバイス グループが一覧表示されます。デフォルト グループは表示されません。

[Details] ペインにグループ名、説明、グループ内のデバイス一覧が表示されます。

ステップ 2　1 台以上のデバイスを追加するデバイス グループをクリックします。

ステップ 3　必要に応じて、[Details] ペインの [Membership Details] セクションを展開します。

ステップ 4　デバイスをグループに追加する手順は、次のとおりです。

a. [Membership Details] セクションの列名の下を右クリックし、[Add Device] を選択します。

[Device Selection] ダイアログボックスが表示されます。

b. （任意）[Select Search Criteria] ドロップダウン リストを使用して、[Available Devices] リストに表示されているデバイスをフィルタします。次のいずれかの方法でデバイスをフィルタできます。

- All devices：検出されたデバイスをすべて表示します。
- Device type：検出されたデバイスのうち、Cisco Nexus 7000 シリーズ スイッチなど、選択したタイプのデバイスだけを表示します。
- Unsupported devices：DCNM-LAN で管理および監視できない検出済みデバイスを表示します。
- Connected devices：IP アドレスで指定するシード デバイスまで、指定するホップ カウント以内で接続された検出済みデバイスを表示します。
- Subnet devices：サブネットおよびサブネット マスクの IP アドレスで指定するサブネット内の IP アドレスを持つ検出済みデバイスを表示します。

c. 1 台以上のデバイスを [Available Devices] リストから [Selected Devices] リストに移動します。

デバイスを 1 台移動するには、デバイスをクリックしてから [Add] をクリックします。

複数のデバイスを移動するには、Ctrl キーを押しながら各デバイスをクリックし、[Add] をクリックします。

d. [OK] をクリックします。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択してデバイス グループの設定を保存します。

トポロジ マップ上のデバイス グループに、追加したデバイスが表示されます。

デバイス グループに追加した各デバイスは、以前のグループから削除されます。以前から存在しているデフォルト以外のデバイス グループが、そのデバイスをすべて新しいデバイス グループに移動したことで空になった場合、DCNM-LAN は空になったデバイス グループを自動的に削除します。

グループからのデバイスの削除

カスタム デバイス グループからデバイスを削除できます。カスタム グループから削除したすべてのデバイスはデフォルト デバイス グループに追加されます。

ヒント　あるグループから別のグループにデバイスを移動する場合は、デバイスを他のグループに追加します。デバイスを他のグループに追加すると、DCNM-LAN はデバイスを元のグループから自動的に削除します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Groups] の順に選択します。

[Summary] ペインにカスタム デバイス グループが一覧表示されます。デフォルト グループは表示されません。

[Details] ペインにグループ名、説明、グループ内のデバイス一覧が表示されます。

ステップ 2　1 台以上のデバイスを削除するデバイス グループをクリックします。

ステップ 3　必要に応じて、[Details] ペインの [Membership Details] セクションを展開します。

ステップ 4　[Membership Details] セクションで、削除するデバイスを選択します。

単一のデバイスを選択する場合は、デバイスをクリックします。

2 台以上のデバイスを選択する場合は、Ctrl キーを押したまま、各デバイスをクリックします。

ステップ 5　選択したいずれかのデバイスを右クリックし、[Delete] を選択します。

DCNM-LAN は、選択されたデバイスをデバイス グループから削除します。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択してデバイス グループの設定を保存します。

トポロジ マップ上のデフォルトのデバイス グループに、カスタム デバイス グループから削除したデバイスが表示されます。

カスタム デバイス グループから削除した各デバイスは、デフォルトのデバイス グループに追加されます。カスタム デバイス グループが、そのすべてのデバイスを削除したことで空になった場合、DCNM-LAN は空になったデバイス グループを自動的に削除します。

デバイス グループの削除

カスタム デバイス グループを削除できます。

削除したカスタム デバイス グループに属しているデバイスは、自動的にデフォルト デバイス グループのメンバーになります。

ヒント　カスタム デバイス グループのすべてのデバイスを他のカスタム デバイス グループに追加した場合、DCNM-LAN は空になったデバイス グループを自動的に削除します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Device Groups] の順に選択します。

[Summary] ペインにカスタム デバイス グループが一覧表示されます。デフォルト グループは表示されません。

[Details] ペインにグループ名、説明、グループ内のデバイス一覧が表示されます。

ステップ 2　削除するデバイス グループをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Delete Device Group] の順に選択します。

DCNM-LAN は、[Summary] ペインからデバイス グループを削除します。削除したデバイス グループに属していたデバイスは、デフォルト デバイス グループのメンバーになります。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択してデバイス グループの設定を保存します。

トポロジ マップ上のデフォルトのデバイス グループに、削除したデバイス グループに存在していたデバイスが表示されます。

関連情報

トポロジ機能におけるデバイス グループの使用方法については、第 19 章「トポロジの作業」を参照してください。

デバイス グループのフィールドの説明

ここでは、デバイス グループ機能における次の各フィールドについて説明します。

- 「[Summary] ペイン」（P.21-6）
- 「[Device Group] : [Details] : [Global Settings] セクション」（P.21-7）
- 「[Device Group] : [Details] : [Membership Details] セクション」（P.21-7）

[Summary] ペイン

表 21-1　デバイス グループの [Summary] ペイン

フィールド	説明
Device Group Name	*表示のみ。*デバイス グループに割り当てた名前。デバイス グループを作成した後、名前を編集することはできません。デバイス グループ名は文字で始まり、最大 30 文字の英数字を使用できます。
Description	デバイス グループについて説明するテキスト。説明に使用できる文字数は最大 80 文字です。

[Device Group]：[Details]：[Global Settings] セクション

表 21-2　[Device Group]：[Details]：[Global Settings] セクション

フィールド	説明
Device Group Name	*表示のみ。*デバイス グループに割り当てた名前。
Description	デバイス グループについて説明するテキスト。説明に使用できる文字数は最大 80 文字です。

[Device Group]：[Details]：[Membership Details] セクション

表 21-3　[Device Group]：[Details]：[Membership Details] セクション

フィールド	説明
Switch Name	*表示のみ。*デバイス グループに割り当てたデバイスの名前。
Platform	*表示のみ。*「Cisco Nexus 1000V シリーズ」、「Cisco Nexus 7000 シリーズ」など、物理デバイスまたは仮想デバイスのタイプの名前。

その他の関連資料

デバイス グループの管理に関連する追加情報については、次を参照してください。

- 「関連資料」（P.21-7）
- 「標準」（P.21-7）

関連資料

関連項目	参照先
トポロジ	第 19 章「トポロジの作業」
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

デバイス グループ機能の履歴

表 21-4 は、この機能のリリースの履歴です。

表 21-4　デバイス グループ機能の履歴

機能名	リリース	機能情報
デバイス グループ	5.0(2)	サポートが追加されました。

CHAPTER 22

クラスタ管理の作業

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）のクラスタ管理機能の使用方法について説明します。

この章の内容は、次のとおりです。

- 「クラスタ管理の概要」（P.22-1）
- 「クラスタ管理のライセンス要件」（P.22-3）
- 「クラスタ管理の前提条件」（P.22-4）
- 「クラスタ管理の注意事項と制約事項」（P.22-4）
- 「サーバ情報の表示」（P.22-4）
- 「クラスタ管理のフィールドの説明」（P.22-4）
- 「その他の関連資料」（P.22-5）
- 「クラスタ管理機能の履歴」（P.22-6）

クラスタ管理の概要

ここでは、次の内容について説明します。

- 「クラスタ管理」（P.22-1）
- 「クラスタ サーバ環境」（P.22-2）
- 「マスター サーバ ロール」（P.22-2）
- 「分散サーバ タスク」（P.22-2）
- 「サーバ タスク分散におけるクラスタ変更の影響」（P.22-3）

クラスタ管理

クラスタ管理を使用すると、サーバ クラスタで動作するように設定された DCNM-LAN サーバに関する情報を表示できます。クラスタで動作するように DCNM-LAN サーバが設定されていない場合、クラスタ管理機能では単一サーバに関する情報を表示できます。

クラスタ管理の要約ペインに表示される各サーバについて、DCNM-LAN のリリース番号、Java バージョン、オペレーティング システム、システム スレッド、メモリ利用状況、IP アドレス、ディスク ドライブの使用状況などの情報を表示できます。

クラスタ サーバ環境

サーバ クラスタに DCNM-LAN を配置できます。1 つのクラスタには最大 5 つの DCNM-LAN サーバを配置できます。1 つのクラスタ内にある複数の DCNM-LAN サーバは、マルチキャスト IP メッセージを使用して通信します。クラスタ型サーバ配置の主な利点は、DCNM-LAN で実行するデバイス管理タスクの処理性能が向上することです。クラスタ型のサーバ配置により、DCNM-LAN サーバのアベイラビリティも確保できます。DCNM-LAN は、クラスタ内のすべてのサーバ間でタスクを分散させます。クラスタ内のサーバは常にアクティブであり、スタンバイ モードになることはありません。

クラスタ サーバの配置に関するサーバ システムとネットワークの要件、およびサーバ クラスタのインストール手順の詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

マスター サーバ ロール

DCNM-LAN サーバ クラスタ内の 1 つのサーバがマスター サーバです。マスター サーバの役割は、自身を含め、サーバ クラスタ内のすべてのサーバにタスクを割り当てることです。タスクは DCNM-LAN データベースに保存されます。マスター サーバに障害が発生した場合、マスター サーバ ロールを担うサーバがデータベース内のタスクにアクセスできます。

ユーザは DCNM-LAN クライアントへのログイン時に、マスター サーバの IP アドレスまたは DNS 名を指定する必要があります。マスター サーバに要求を送信すると、マスター サーバは必要に応じてタスクを分散させます。

DCNM-LAN は、サーバの開始時間が早い順にどのサーバがマスター サーバであるかを判断します。最初に開始された DCNM-LAN サーバが、常にサーバ クラスタのマスター サーバになります。マスター サーバに障害が発生した場合、その次に開始時間の早い DCNM-LAN サーバがマスター サーバ ロールを担います。クラスタ内でサーバを開始する順序を制御することにより、マスター サーバにするサーバを制御できます。

分散サーバ タスク

マスター サーバは、管理対象デバイスをサーバ クラスタ内のサーバに割り当てることで、タスクを分散させます。たとえば、4 つのサーバから成るクラスタで、DCNM-LAN が 20 台のデバイスを管理している場合、マスター サーバは自身を含めて 5 台の管理対象デバイスを各サーバに割り当てます。

マスター サーバがサーバにデバイスを割り当てた後、サーバはそのデバイスに対して次のタスクを実行します。

- デバイスとの自動同期化：システム メッセージ ログ ファイルをデバイスから定期的に取得します。自動同期化の詳細については、第 23 章「デバイスとの自動同期化の管理」を参照してください。
- 統計データ収集：仮想ポート チャネル（vPC）の統計情報を除き、デバイスの統計データ コレクタを実行します。マスター サーバは常に、vPC 統計情報の統計データ コレクタを実行します。統計データ収集の詳細については、第 25 章「統計データ収集の管理」を参照してください。
- デバイス ディスカバリ：デバイスに対してデバイス コンフィギュレーション ディスカバリを実行しますが、デバイス ディスカバリの残りのフェーズはマスター サーバが実行します。デバイス ディスカバリのフェーズについては、「ディスカバリ プロセス」（P.16-3）を参照してください。

たとえば、DC-NEXUS-7010-3 というスイッチのデバイス ディスカバリを開始した場合、マスター サーバはデバイス ディスカバリの初期フェーズを実行します。次に、DC-NEXUS-7010-3 のデバイス コンフィギュレーション ディスカバリ フェーズをクラスタ内のいずれかのサーバに割り当て、ディスカバリ タスクが均等に分散されるようにします。ディスカバリが完了すると、マスター サーバは DC-NEXUS-7010-3 を、管理しているデバイス数が最も少ないサーバに割り当てます。マスター サーバは、DC-NEXUS-7010-3 の自動同期化を実行するように、割り当てたサーバに指示します。DCNM-LAN クライアント ユーザが DC-NEXUS-7010-3 で管理される機能の統計図を開始すると、マスター サーバは割り当てられたサーバに対し、図の統計データ コレクタを実行するように指示します。

サーバ タスク分散におけるクラスタ変更の影響

サーバがクラスタに参加する、またはクラスタから脱退するとき、マスター サーバは常に、サーバに対する管理対象デバイスの割り当てを、クラスタ内のサーバ間で均等になるように分散させます。表 22-1 で、具体的なイベントに対する DCNM-LAN サーバ クラスタの動作を説明します。

表 22-1　クラスタ変更イベントと動作

クラスタ変更イベント	クラスタの動作
マスター サーバの停止または障害の発生時	最も開始時間の早いサーバがマスター サーバになり、クラスタ内に残っているサーバ間で均等になるように管理対象デバイスの割り当てを分散させます。クラスタ サイズが減少するため、各サーバに割り当たるデバイス数は増加します。
サーバの停止または障害の発生時	マスター サーバは、クラスタ内に残っているサーバ間で均等になるように管理対象デバイスの割り当てを分散させます。クラスタ サイズが減少するため、各サーバに割り当たるデバイス数は増加します。
ユーザによって開始されたデバイス コンフィギュレーションの展開を実行中にサーバに障害が発生した場合	メンバーのサーバに障害が発生し、ユーザによって開始されたデバイス コンフィギュレーションの展開が完了しなかった場合、展開に失敗し、デバイス コンフィギュレーションを展開するサーバ タスクは消失します。 展開の消失から復旧するには、設定手順を繰り返し、設定を再度展開する必要があります。失敗の結果、デバイスが「Unmanaged」になることもあり、この場合は、デバイスを再検出してから設定手順を繰り返す必要があります。 マスター サーバは、クラスタ内に残っているサーバ間で均等になるように管理対象デバイスの割り当てを分散させます。クラスタ サイズが減少するため、各サーバに割り当たるデバイス数は増加します。
サーバの開始時	マスター サーバは、クラスタ内に残っているサーバ間で均等になるように管理対象デバイスの割り当てを分散させます。クラスタ サイズが増加するため、各サーバに割り当たるデバイス数は減少します。

クラスタ管理のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM-LAN	クラスタ管理にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

クラスタ管理の前提条件

クラスタ管理機能には次の前提条件があります。

- クラスタ内のサーバは、クラスタ サーバの要件を満たしている必要があります。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

クラスタ管理の注意事項と制約事項

クラスタ管理機能には次の制約事項があります。

- クラスタ管理機能では、実行中のサーバに関する情報だけを表示します。クラスタ内のサーバの停止または障害が発生すると、そのサーバはクラスタから脱退しているように見え、クラスタ管理機能ではそのサーバの情報は表示されません。

サーバ情報の表示

サーバ クラスタとして動作するように設定された DCNM-LAN サーバに関する情報を表示できます。サーバ クラスタのメンバーとして動作するように設定されていない単一サーバを使用している場合は、クラスタ管理機能を使用して、そのサーバに関する情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Cluster Administration] の順に選択します。

[Summary] ペインに、インストール中にクラスタに割り当てられたパーティション名でクラスタが表示されます。単一サーバ環境では、インストール中に割り当てられたパーティション名を維持します。

ステップ 2　クラスタを展開します。

[Summary] ペインに、サーバに関する情報とともに、クラスタ内の各 DCNM-LAN サーバが一覧表示されます。

ヒント　サーバ情報を更新するには、ツールバーで [View] > [Refresh] の順に選択します。

ステップ 3　（任意）ディスク使用状況の情報を表示する場合は、[Details] タブで [Logical Disk(s)] セクションを展開します。

クラスタ管理のフィールドの説明

ここでは、クラスタ管理機能における次の各フィールドについて説明します。

- 「[Summary] ペイン」（P.22-5）
- 「[Server] : [Details] タブ」（P.22-5）

[Summary] ペイン

表 22-2　クラスタ管理の [Summary] ペイン

フィールド	説明
Cluster partition name	*表示のみ。*サーバ ソフトウェアのインストール時に DCNM-LAN サーバ パーティションに割り当てた名前。 **（注）** [Summary] ペインの残りのフィールドは、クラスタ内の特定のサーバに関するものです。
IP Address	*表示のみ。*DCNM-LAN サーバの IPv4 アドレス。現在、このサーバがサーバ クラスタ内のマスター サーバである場合、[IP Address] フィールドでも、そのサーバがマスター サーバであることが表示されます。
DCNM-LAN Version	*表示のみ。*サーバが実行している DCNM-LAN のリリース番号。
Java Version	*表示のみ。*CNM-LAN サーバが使用中の Java バージョン。
Total Threads	*表示のみ。*サーバ システム上の DCNM-LAN ソフトウェアが使用している処理中スレッド数。
Memory Utilization (Percentage)	*表示のみ。*サーバ システム上の DCNM-LAN ソフトウェアで使用しているシステム メモリのパーセンテージ。
Last Local Refresh Time	*表示のみ。*クライアントが最後に更新情報を受信したときの DCNM-LAN サーバのローカル日時。

[Server] : [Details] タブ

表 22-3　[Server] : [Details] タブ

フィールド	説明
General	
このセクションのフィールドには、[Summary] ペインの同じ名前のフィールドと同じ情報が表示されます。	
Logical Disk(s)	
Name	*表示のみ。*デバイスの名前。
Size (MB)	*表示のみ。*ドライブの合計容量（MB 単位）。
Free Space (MB)	*表示のみ。*ドライブ上で使用可能な MB 単位の数値。

その他の関連資料

クラスタ管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.22-6）
- 「標準」（P.22-6）

関連資料

関連項目	参照先
イベント	『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」
デバイスとの自動同期化	第 23 章「デバイスとの自動同期化の管理」
統計データ収集	第 25 章「統計データ収集の管理」
サーバの停止	第 28 章「Cisco DCNM-LAN サーバの起動と停止」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

クラスタ管理機能の履歴

表 22-4 は、この機能のリリースの履歴です。

表 22-4　クラスタ管理機能の履歴

機能名	リリース	機能情報
クラスタ管理	5.0(2)	サポートが追加されました。

CHAPTER 23

デバイスとの自動同期化の管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）でデバイスとの自動同期化機能を管理する方法について説明します。

この章の内容は、次のとおりです。

- 「デバイスとの自動同期化の概要」（P.23-1）
- 「デバイスとの自動同期化のライセンス要件」（P.23-2）
- 「デバイスとの自動同期化の前提条件」（P.23-2）
- 「デバイスとの自動同期化の注意事項と制約事項」（P.23-3）
- 「デバイスとの自動同期化の設定」（P.23-3）
- 「自動同期化ポーラーのステータスの表示」（P.23-8）
- 「デバイスとの自動同期化のフィールドの説明」（P.23-8）
- 「その他の関連資料」（P.23-10）
- 「デバイスとの自動同期化機能の履歴」（P.23-11）

デバイスとの自動同期化の概要

デバイスとの自動同期化機能によって、Cisco Data Center Network Manager for LAN（DCNM-LAN）サーバは、管理対象デバイスの最新のコンフィギュレーションおよびステータス情報を確実に保持できます。DCNM-LAN サーバは、この機能に必要なシステム ログおよびアカウンティング ログを取得するために、デバイスごとにポーラー プロセスを 1 つずつ作成します。

[Feature Selector] ペインで [Auto Synchronization with Devices] を選択すると、[Contents] ペインに各ポーラー プロセスに関する情報が表示され、それらを管理することができます。

DCNM-LAN が次にデバイスをポーリングするまでの時間間隔を設定できます。DCNM-LAN では、管理対象の各デバイスに対してデフォルトのポーリング間隔が設定されます。デフォルト値はデバイスのタイプによって異なります。デバイスの [Polling Interval] フィールドの編集を開始すると、ポーリング間隔の値の範囲が表示されます。詳細については、「ポーリング間隔の設定」（P.23-4）を参照してください。

DCNM-LAN はデバイスを並列にポーリングしますが、すべてのデバイスを同時にポーリングするのを避けるために、デバイス名のアルファベット順にポーリングを開始し、各ポーリング プロセスの開始を、ランダムに決められたごく短い時間だけ遅らせます。

ここでは、次の内容について説明します。

- 「イベント データの自動消去および手動消去」（P.23-2）
- 「仮想化のサポート」（P.23-2）

イベント データの自動消去および手動消去

デバイスとの自動同期化機能を使用して、不要なイベント データを削除できます。DCNM-LAN は、イベント データの自動消去をサポートしています。イベント データの自動消去について次の側面を設定できます。

- 自動消去を行う曜日と時刻。
- DCNM-LAN が消去するイベント データを、経過日数またはデータベース エントリの最大数のどちらで判別するか。
- イベントの重大度レベル。

イベント データは手動でも消去できます。

仮想化のサポート

DCNM-LAN では、Cisco NX-OS デバイス上の各仮想デバイス コンテキスト（VDC）が個別のデバイスとして扱われます。DCNM-LAN は、デバイスごとにポーラー プロセスを 1 つずつ作成します。

デバイスとの自動同期化のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM-LAN	デバイスとの自動同期化にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイスとの自動同期化の前提条件

デバイスとの自動同期化機能を使用するには、次の前提条件を満たしている必要があります。

- DCNM-LAN サーバが各デバイスに接続できること。
- Cisco NX-OS デバイスが、Cisco NX-OS のサポートされているバージョンを実行していること。
- Cisco NX-OS デバイスが、デバイス ディスカバリを正常に完了するために必要な最小構成を備えていること。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

デバイスとの自動同期化の注意事項と制約事項

デバイスとの自動同期化機能における設定時の注意事項と制約事項は次のとおりです。

- デバイスからの応答が遅い、あるいは管理するデバイスが多いため同期化処理に問題が発生する場合を除き、デフォルトのデバイス ポーリング間隔を使用することをお勧めします。詳細については、「ポーリング間隔の設定」（P.23-4）を参照してください。
- DCNM-LAN クライアントの [Summary] ペインに表示される情報のうち、デバイスとの自動同期化機能については自動的に更新されません。最新の情報を表示するには、メニュー バーで、[View] > [Refresh] の順に選択してください。
- DCNM-LAN データベースのサイズが大きくなりすぎないように、イベント データの自動消去を設定することを推奨します。

デバイスとの自動同期化の設定

ここでは、次の内容について説明します。

- 「ポーラーの開始と停止」（P.23-3）
- 「ポーリング間隔の設定」（P.23-4）
- 「デバイスとの同期化」（P.23-4）
- 「イベント データベースからのデータの削除」（P.23-5）
- 「自動イベント消去のイネーブル化およびディセーブル化」（P.23-6）
- 「自動イベント消去の設定」（P.23-6）
- 「イベントをすぐに消去する」（P.23-7）

ポーラーの開始と停止

デバイスに対してポーラーを開始および停止できます。ポーラーを停止すると、デバイスとの自動同期化が行われなくなります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Contents] ペインに、ポーラーの一覧表が表示されます。各行は、そのデバイスのポーラーに対応しています。デバイスはアルファベット順に表示されます。[Poller Status] フィールドに、ポーラーが実行中か停止しているかを示すメッセージが表示されます。

ステップ 2　開始または停止するポーラーをクリックします。

ステップ 3　次のどちらかを実行します。

- ポーラーを開始する場合は、メニュー バーで、[Actions] > [Start Poller] の順に選択します。[Poller Status] フィールドの表示が「Running」に変わります。
- ポーラーを停止する場合は、メニュー バーで、[Actions] > [Stop Poller] の順に選択します。[Poller Status] フィールドの表示が「Stopped」に変わります。

変更内容を保存する必要はありません。

ポーリング間隔の設定

DCNM-LAN サーバが管理対象デバイスと同期化する頻度を設定できます。同期化の実行中、DCNM-LAN サーバは、管理対象デバイスからアカウント ログおよびシステム ログを取得します。この設定は、DCNM-LAN クライアントの機能が管理対象デバイスに関する更新情報を受信する頻度に影響します。

はじめる前に

DCNM-LAN が管理対象デバイスとの自動同期化を実行する頻度を決定します。次の点に注意してください。

- DCNM-LAN 以外の方法（デバイスのコマンドライン インターフェイスを使用するなど）でデバイス コンフィギュレーションを変更する頻度。DCNM-LAN 以外の方法による変更が頻繁に行われる場合は、ポーリング間隔を短くすることを検討します。
- 管理対象デバイスのコンフィギュレーションに合わせて DCNM-LAN を最新に保つことの重要度。最新の設定情報を保持することが重要な場合は、ポーリング間隔を短くすることを検討します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

すべてのデバイスのポーリング間隔が、ポーラー テーブルの下の [Poller Setting] タブに表示されます。

ステップ 2　操作するデバイスを [Platform] カラムで選択します。

ステップ 3　[Polling Interval] フィールドに、選択したデバイスで自動同期化を実行する間隔を秒数で入力します。デバイスの [Polling Interval] フィールドの編集を開始すると、ポーリング間隔の値の範囲が表示されます。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択してポーリング間隔を保存します。

デバイスとの同期化

次回の自動同期化が実行されるまで待てない場合、DCNM-LAN とデバイスとの同期化を手動で実行できます。

（注）　前回の同期化が正常に終了してからデバイスに多くの設定変更を行った場合は、同期化ではなくデバイス ディスカバリを実行することを検討してください。詳細については、「デバイスの検出」（P.17-4）を参照してください。

はじめる前に

一意のデバイス クレデンシャルを使用してデバイス エントリを設定していること、または DCNM-LAN がデフォルトのデバイス クレデンシャルを使用してデバイスに接続できることを確認してください。詳細については、「デフォルトのデバイス クレデンシャルの設定」（P.17-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Contents] ペインに、ポーラーの一覧表が表示されます。各行は、そのデバイスのポーラーに対応しています。デバイスはアルファベット順に表示されます。

ステップ 2　DCNM-LAN と同期させるデバイスをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Synchronize with Device] の順に選択します。

同期化が開始されます。

同期化が終了したかどうかを確認するには、[Last Sync Status] 列を監視してください。通常、デバイスとの同期は 5 分未満で終了します。

変更内容を保存する必要はありません。

イベント データベースからのデータの削除

正確なイベントの経過時間に基づいてイベント データベースからデータを削除できます。削除するイベントは、イベント ブラウザまたは機能固有の [Events] タブに表示されなくなります。

ヒント　データベース内のイベント数に基づいてイベントを削除する場合は、「イベントをすぐに消去する」（P.23-7）を参照してください。

はじめる前に

削除対象となる最も新しいイベント データの日時を確認します。この手順に従って作業を行うと、指定した日時よりも古いイベントは DCNM-LAN によってすべて削除されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Details] ペインのポーラー一覧表の下に [Events Database Administration] タブが表示されます。

ステップ 2　[Delete events older than] ドロップダウン リストで、削除対象となる最も新しいイベントの日時を選択し、[OK] をクリックします。

ステップ 3　[Delete] をクリックします。

指定した日時よりも古いイベントが DCNM-LAN によってすべて削除されます。

自動イベント消去のイネーブル化およびディセーブル化

DCNM-LAN イベント データベースからのイベントの自動消去をイネーブルまたはディセーブルに設定できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Details] ペインのポーラー一覧表の下に [Events Database Administration] タブが表示されます。

ステップ 2　[Auto Purge Settings] で、次のいずれかを行います。

- 自動イベント消去をイネーブルにする場合は、[Enable Auto Purge] をオンにします。
- 自動イベント消去をディセーブルにする場合は、[Enable Auto Purge] をオフにします。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

自動イベント消去の設定

自動イベント消去を実行するタイミングと、DCNM-LAN が消去するイベントの判別に使用する基準を設定できます。

はじめる前に

自動イベント消去を実行するタイミングを確認します。自動イベント消去は DCNM-LAN の使用率が低いときに実行することを推奨します。

DCNM-LAN データベースのバックアップを実行する場合は、すべてのイベントのレコードが保持されるように、データベースのバックアップの実行後に自動イベント消去をスケジューリングすることを検討します。

DCNM-LAN が消去するイベントの判別に使用する基準を決定します。使用できる基準は、次のとおりです。

- イベントの経過時間：DCNM は、特定の日数、週数、または月数を経過した古いイベントをすべて消去できます。
- データベース内のイベント数：データベース内のイベント数がユーザの指定した最大数を超えた場合、DCNM-LAN は最大数以下になるまで最も古いイベントから順に消去できます。
- イベントの重大度：DCNM は、イベントの重大度レベルに基づいてイベントを消去できます。

両方の基準をイネーブルにした場合、DCNM-LAN はそれらを相互に独立させて適用します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Details] ペインのポーラー一覧表の下に [Events Database Administration] タブが表示されます。

ステップ 2　[Purge Threshold] で、DCNM-LAN が消去するイベントの判別に使用する基準を設定します。次の表の基準を任意に設定できます。

消去基準	設定方法
イベントの経過時間	1. [Data older than] をオンにします。 2. 最初のドロップダウン リストから、日数、週数、または月数を選択します。 3. 2 番めのドロップダウン リストから、必要に応じて [Days]、[Weeks]、または [Months] を選択します。
データベース内のイベント数	1. [Total Entries Exceed(0-2147483647)] をオンにします。 2. ボックスに、イベント データベースで許容するエントリの最大数を入力します。
イベントの重大度	1. [Severity] をオンにします。8 段階の重大度レベルのリストが使用できるようになります。 2. DCNM-LAN がイベントを消去するかどうかの判別に使用するそれぞれの重大度レベルについて、重大度のレベルを確認します。

ステップ 3　[Auto Purge Settings] で、次の手順に従って自動消去を実行するタイミングを設定します。

a. 自動消去の実行を曜日で指定する場合は、[days-of-the-week] チェックボックスをオンにします。

b. 自動イベント消去を指定した日時に実行するように設定する場合は、[Run at] ボックスを使用します。

ステップ 4　（任意）自動イベント消去をイネーブルにする場合は、[Enable Auto Purge] をオンにします。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

イベントをすぐに消去する

自動イベント消去設定を使用して消去するイベントを判別し、イベント データをオンデマンドで削除できます。削除するイベントは、イベント ブラウザまたは機能固有の [Events] タブに表示されなくなります。

ヒント　イベントの正確な経過時間に基づいて、イベントをオンデマンドで削除する場合は、「イベント データベースからのデータの削除」（P.23-5）を参照してください。

はじめる前に

必要に応じて、自動イベント消去が設定されていることを確認します。詳細については、「自動イベント消去の設定」（P.23-6）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Details] ペインのポーラー一覧表の下に [Events Database Administration] タブが表示されます。

ステップ 2　[Purge] で、[Purge Now] をクリックします。

DCNM-LAN は、自動イベント消去の設定を使用して消去対象のイベントを判別し、イベントを削除します。

自動同期化ポーラーのステータスの表示

自動同期化ポーラーのステータスを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [Auto Synchronization with Devices] の順に選択します。

[Contents] ペインの [Pollers] 領域に、ポーラーのステータスおよび同期化の時刻とステータスに関する情報が表示されます。

表 23-1　自動同期化ポーラー情報

フィールド	説明
Pollers	
Last Refresh Time	*表示のみ。*[Contents] ペインに表示されている情報を DCNM-LAN クライアントが更新した日時。
Device	*表示のみ。*対応するポーラーのデバイスの名前と IP アドレス。
Poller Status	*表示のみ。*ポーラーが実行中か停止しているかを示します。実行中のポーラーは、[Device Polling Interval] フィールドに、指定した頻度で、対応するデバイスのコンフィギュレーションおよびステータス情報の同期化を実行します。
Last Sync Time	*表示のみ。*前回ポーラーがデバイスからシステム ログおよびアカウント ログのデータを取得した日時。
Last Sync Status	*表示のみ。*前回の同期化が成功したか失敗したかを示します。同期化が失敗した場合は、DCNM-LAN がデバイスに接続できなかった理由を特定します。必要なら、デバイスを再検出します。

デバイスとの自動同期化のフィールドの説明

ここでは、デバイスとの自動同期化機能の次の各フィールドについて説明します。

- 「[Poller Setting] タブ」（P.23-9）
- 「[Events Database Administration] タブ」（P.23-9）

[Poller Setting] タブ

表 23-2　デバイスとの自動同期化の [Poller Setting] タブ

フィールド	説明
Pollers	
Polling Interval	デバイスとの同期化の次回試行まですべてのポーラーが待機する間隔（秒）。デバイスの [Polling Interval] フィールドの編集を開始すると、ポーリング間隔の値の範囲が表示されます。
Device	*表示のみ*。対応するポーラーのデバイスの名前と IP アドレス。

[Events Database Administration] タブ

表 23-3　[Events Database Administration] タブ

フィールド	説明
Delete events older than	イベント データベースから削除する最も新しいイベントの日時。このフィールドにデフォルト値はありません。
Purge Threshold	
Data older than	イベントの自動消去中に、DCNM-LAN がこのチェックボックスの右側にあるドロップダウン リストに指定された経過時間よりも古いイベントを削除するかどうかを示します。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオンにすると、デフォルトの経過時間は 1 日になります。
Total Entries Exceed	イベントの自動消去中に、DCNM-LAN が、このチェックボックスの右側にあるボックスの値とイベント数が等しくなるまで、古いイベントを削除するかどうかを示します。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオンにすると、デフォルトのイベント数は 25,000 になります。
Severity	イベントの自動消去中に、DCNM-LAN が重大度レベルのリストから選択された重大度レベルが設定されているイベントを削除するかどうかを示します。デフォルトでは、このチェックボックスはディセーブルになっています。

表 23-3　[Events Database Administration] タブ （続き）

フィールド	説明
Severity Levels	イベントの自動消去中に DCNM-LAN が削除するイベントの重大度レベル。重大度レベルは、[Severity] チェックボックスがオンになっているときだけ使用できます。デフォルトでは、すべての重大度レベルがディセーブルになっています。重大度レベルは次のとおりです。 • Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
Auto Purge Settings	
Enable Auto Purge	イベント データの自動消去をイネーブルにするかどうかを示します。デフォルトでは、このチェックボックスはディセーブルになっています。
Run on	イベント データの自動消去を実行する曜日。デフォルトでは、どのチェックボックスもオンになっていません。[Daily] チェックボックスをオンにすると、個別の曜日を指定するためのチェックボックスが選択できなくなります。
Run at	自動消去がイネーブルになっている曜日に、イベント データの自動消去を実行する時刻。

その他の関連資料

デバイスとの自動同期化の管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.23-10）
- 「標準」（P.23-11）

関連資料

関連項目	参照先
イベント	『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

デバイスとの自動同期化機能の履歴

表 23-4 は、この機能のリリースの履歴です。

表 23-4　デバイスとの自動同期化機能の履歴

機能名	リリース	機能情報
デバイスとの自動同期化	5.0(2)	リリース 4.2 からの変更はありません。

CHAPTER 24

しきい値ルールの作業

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）を使用してしきい値ルールを設定する方法について説明します。

この章の内容は、次のとおりです。

- 「しきい値ルールに関する情報」（P.24-1）
- 「しきい値ルールのライセンス要件」（P.24-4）
- 「しきい値ルールの設定」（P.24-4）
- 「その他の関連資料」（P.24-8）
- 「しきい値ルールの機能履歴」（P.24-9）

しきい値ルールに関する情報

ここでは、次の内容について説明します。

- 「しきい値ルールの概要」（P.24-1）
- 「しきい値ルールの例」（P.24-2）

しきい値ルールの概要

DCNM-LAN は、収集済み統計データのサンプル変数に、上昇または下限しきい値ルールを設定できる機能を提供します。ルールの定義に基づいて、DCNM-LAN によって一連のアクションが実行されます。[Threshold Rules] ページでしきい値ルールを定義し、既存の図にしきい値ルールを適用します。

ここでは、次の内容について説明します。

- 「上昇しきい値」（P.24-1）
- 「下降しきい値」（P.24-2）
- 「しきい値ルールのプロパティ」（P.24-2）
- 「しきい値ルールのアクション」（P.24-2）

上昇しきい値

上昇しきい値は、サンプル変数の上限しきい値です。現在のサンプル変数が指定されたしきい値以上になると、一連のアクションが実行されます。

下降しきい値

下降しきい値は、サンプル変数の下限しきい値です。現在のサンプル変数が指定されたしきい値以下になると、一連のアクションが実行されます。

（注）　1 つのサンプル変数に指定できる上昇しきい値と下限しきい値は、それぞれ 1 つだけです。

しきい値ルールのプロパティ

しきい値ルールのプロパティは、次のとおりです。

- 名前：しきい値ルールの名前を指定します。
- 頻度：アクションがトリガーされるまでにサンプル変数がしきい値を超える必要のある回数を指定します。
- 期間：頻度がモニタされる間隔を指定します。
- 繰り返し：期間内で、アクションのトリガー後にタイマーがリセットされないようにします。
- トレンド：上昇または下限しきい値を指定します。

しきい値ルールのアクション

しきい値ルールのアクションは、次のとおりです。

- メール サーバに電子メールまたは SMS を送信する、または SMS ゲートウェイにメール送信する。
- サーバでスクリプトを実行する。
- 現在の DCNM JMS チャネルにイベントを送信する。

しきい値ルールの例

（注）　期間の粒度は、データ収集の最小間隔によって決定されます。したがって、期間はその間隔よりも長くなければなりません。

ここでは、次の内容について説明します。

- 「しきい値を超えるたびにアクションをトリガーする」（P.24-2）
- 「しきい値を超えたときに期間内で 1 回だけアクションをトリガーする」（P.24-3）
- 「しきい値を超えたときに期間内で 4 回ごとにアクションをトリガーする」（P.24-4）

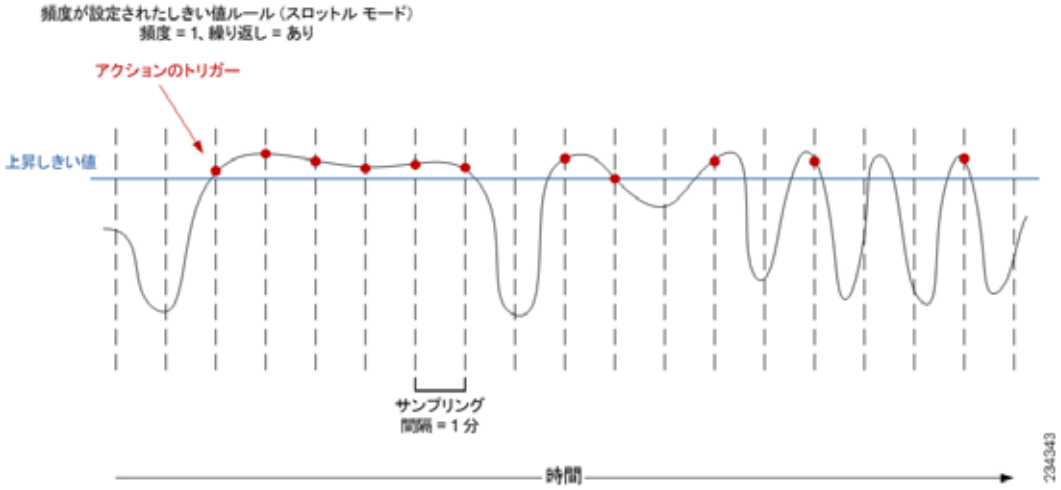
しきい値を超えるたびにアクションをトリガーする

しきい値を超えるたびにアクションをトリガーするには、次のようにプロパティを設定します。

- 頻度：**1**
- 繰り返し：**あり**

図 24-1 に、ルールのプロパティを上記の値に設定した場合のトリガー アクションを示します。

図 24-1　しきい値を超えるたびにアクションをトリガーする



サンプル変数がしきい値を超えた場合、初めてしきい値を超えたときにアクションが実行されます。その結果、しきい値を超えるたびにアクションが実行されます。

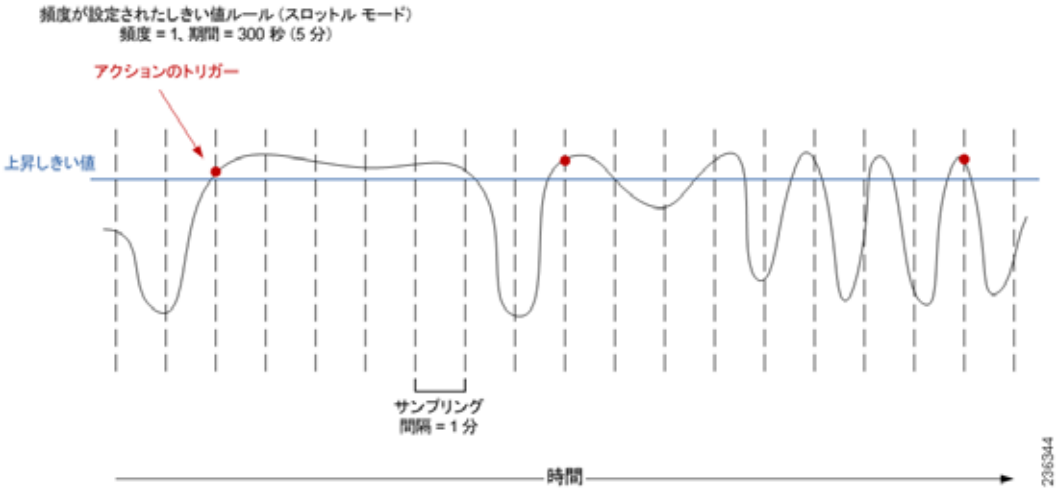
しきい値を超えたときに期間内で 1 回だけアクションをトリガーする

しきい値を超えたときに期間内で 1 回だけアクションをトリガーするには、次のようにプロパティを設定します。

- 頻度：**1**
- 期間：**300**
- 繰り返し：**なし**

図 24-2 に、ルールのプロパティを上記の値に設定した場合のトリガー アクションを示します。

図 24-2　期間内でしきい値を超えたときに 1 回だけアクションをトリガーする



サンプル変数がしきい値を超えた場合、初めてしきい値を超えたときにアクションが実行されます。残りの 5 分間には、アクションは実行されません。その結果、指定された期間中に 1 回だけアクションが実行されます。

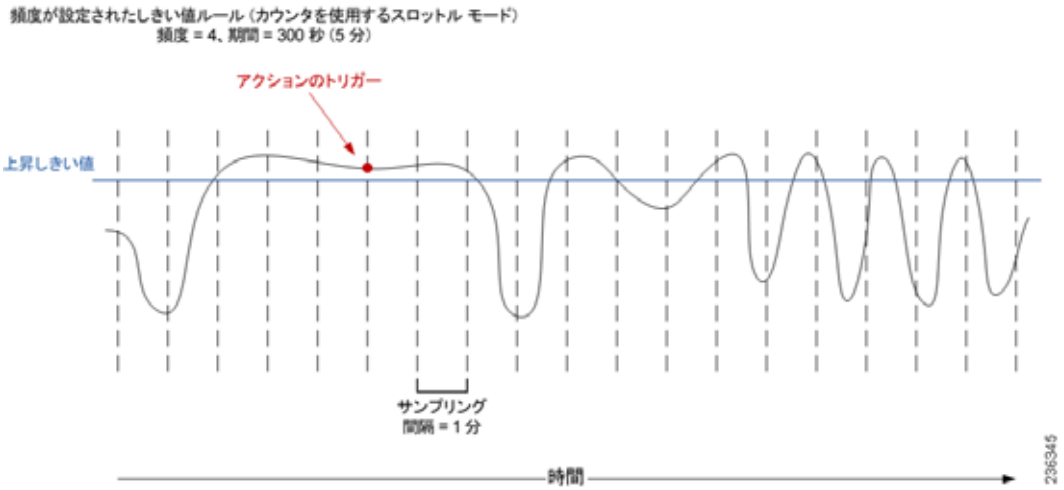
しきい値を超えたときに期間内で 4 回ごとにアクションをトリガーする

しきい値を超えたときに期間内で 4 回ごとにアクションをトリガーするには、次のようにプロパティを設定します。

- 頻度：**4**
- 期間：**300**
- 繰り返し：**なし**

図 24-3 に、ルールのプロパティを上記の値に設定した場合のトリガー アクションを示します。

図 24-3　　しきい値を超えたときに期間内で 4 回ごとにアクションをトリガーする



サンプル変数がしきい値を超えた場合、4 回目にしきい値を超えたときにアクションが実行されます。残りの 5 分間には、アクションは実行されません。その結果、指定された期間中に 1 回だけアクションが実行されます。

しきい値ルールのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	しきい値ルールにライセンスは必要ありません。

しきい値ルールの設定

この機能を使用して、ルールを作成、削除、編集、表示し、図に適用することができます。

ここでは、機能の詳細を説明します。

ここでは、次の内容について説明します。

- 「しきい値ルールの作成」（P.24-5）

- 「しきい値ルールの削除」（P.24-7）
- 「しきい値ルールの編集」（P.24-7）
- 「しきい値ルールの表示」（P.24-7）
- 「しきい値ルールの図への適用」（P.24-8）

しきい値ルールの作成

DCNM-LAN を使用して、しきい値ルールを作成できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Threshold Rules] の順に選択します。

ステップ 2　ツールバーで [New] を選択し、[New Threshold Rule] を選択します。

[Details] ペインに [Details] および [Threshold Bindings] タブが表示され、[Details] タブが開いた状態になります。

ステップ 3　次のように、しきい値ルールを作成します。

a. [Name] フィールドに、名前を入力します。

b. [Description] フィールドに、しきい値ルールの説明を入力します。

説明を入力すると、[Rising Threshold] チェックボックスが自動的にオンになり、[Settings] 領域の [Threshold] フィールドが赤色の枠で囲まれます。

（注）　枠が赤色のフィールドは、入力が必要であることを示します。枠が黄色のフィールドは、入力されていることを示します。

c. [Settings] 領域の [Threshold] フィールドに値を入力します。

値を入力すると、[Action] 領域の 3 つのオプションが赤色の枠で囲まれます。

d. [Action] 領域で、次のいずれかを実行します。

- 電子メール アドレス（カンマ区切り）を入力する
- [Sent Event] を選択してイベントを DCNM-LAN イベント ブラウザに転送する
- スクリプト名を入力する

スクリプトは、しきい値の超過に関するすべてのデータを受信します。スクリプトは、任意のプログラミング言語で記述し、システム パスのディレクトリのいずれかに保存できます。

表 24-1 に、使用可能なパラメータの説明を示します。

表 24-1　スクリプトに渡されるパラメータ

パラメータ	説明
$1	デバイス名
$2	しきい値名
$3	タイムスタンプ
$4	重大度

表 24-1　スクリプトに渡されるパラメータ （続き）

パラメータ	説明
$5	モニタされるメトリック（カウンタまたは非カウンタ）。 • カウンタとして使用される場合は、メトリック単位のレート（秒）を表します。 • 非カウンタとして使用される場合は、メトリック単位の絶対値を表します。
$6	モニタされるメトリック（カウンタまたは非カウンタ）のしきい値。 • カウンタとして使用される場合は、メトリック単位のレート（秒）を表します。 • 非カウンタとして使用される場合は、メトリック単位の絶対値を表します。
$7	トレンド タイプ 使用可能な値は次のとおりです。 • **rate** カウンタです。 • **absolute** 非カウンタです。
$8	しきい値タイプ 使用可能な値は次のとおりです。 • **rising** • **falling**
$9	統計クラス
$10	統計変数
$11	ソース オブジェクト

（注）　DCNM-LAN サーバに SMTP サーバが設定されていることを確認します。DCNM-LAN サーバの設定方法の詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

e. （任意）対応する [Settings] および [Action] 領域で、[Falling Threshold] を設定します。

f. （任意）[Threshold Bindings] タブをクリックしてバインディングを表示します。

g. [Deploy] をクリックします。

ルールが適用されます。

DCNM-LAN を終了し、警告ダイアログボックスで [Save Pending Changes] がオンになった場合は、[Yes] をクリックしてルールを保存します。

しきい値ルールの削除

DCNM-LAN を使用して、ルールを削除できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Threshold Rules] の順に選択します。
[Summary] ペインにルールが表示されます。

ステップ 2　[Summary] ペインで、適切なルールを右クリックします。

ステップ 3　ドロップダウン リストから [Delete Threshold Rule] を選択します。
警告ダイアログボックスが表示され、「Are you sure you want to delete?」と表示されます。

ステップ 4　[Yes] をクリックします。
ルールが削除されます。

しきい値ルールの編集

DCNM-LAN を使用して、しきい値ルールを表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Threshold Rules] の順に選択します。
[Summary] ペインにルールが表示されます。

ステップ 2　適切な領域を編集します。

（注）　[Name] フィールドは編集できません。

しきい値ルールの表示

DCNM-LAN を使用して、しきい値ルールを表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Threshold Rules] の順に選択します。
[Summary] ペインにルールが表示されます。

ステップ 2　表示するルールをクリックします。

しきい値ルールの図への適用

DCNM-LAN を使用して、しきい値ルールを適用できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、適切な機能を選択します。たとえば、イーサネット ポートの統計情報を確認する場合は、[Interfaces] > [Physical] > [Ethernet] の順に選択します。

[Summary] ペインに使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、適切なデバイスを選択します。

ステップ 3　[Statistics] タブをクリックします。

ステップ 4　ツールバーで [New Chart] をクリックし、ドロップダウン リストから表示する図を選択します。たとえば、トラフィックの統計情報を確認する場合は、[Traffic Statistics Chart] を選択します。

ステップ 5　図ツールバーで、[Launch Threshold Setting] をクリックします。

その他の関連資料

しきい値ルールの管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.24-8）
- 「標準」（P.24-8）

関連資料

関連項目	参照先
イベント	『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』
統計データ収集	第 25 章「統計データ収集の管理」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

しきい値ルールの機能履歴

表 24-2 は、この機能のリリースの履歴です。

表 24-2　しきい値ルールの機能履歴

機能名	リリース	機能情報
しきい値ルール	5.2(0)	—

CHAPTER 25

統計データ収集の管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）で統計データ収集を管理する方法について説明します。

この章の内容は、次のとおりです。

- 「統計データの収集の概要」（P.25-1）
- 「統計データ収集機能のライセンス要件」（P.25-2）
- 「統計データ収集の前提条件」（P.25-2）
- 「統計データ収集の注意事項と制約事項」（P.25-3）
- 「統計データ収集の設定」（P.25-3）
- 「統計データ コレクタのステータスの表示」（P.25-9）
- 「統計データ収集機能のフィールドの説明」（P.25-9）
- 「その他の関連資料」（P.25-11）
- 「統計データ収集の機能履歴」（P.25-11）

統計データの収集の概要

統計データ収集機能を使用して、統計をサポートする多数のデバイス コンフィギュレーション機能のうち、特定の機能のために作成した統計モニタリング プロセスを制御できます。

[Feature Selector] ペインで [Statistical Data Collection] を選択すると、[Contents] ペインに各統計収集に関する情報が表示され、それらを制御できます。この機能を使用して、統計データベースから古いデータ消去することもできます。

Cisco Data Center Network Manager for LAN（DCNM-LAN）がモニタリング中のデバイスから統計データを取得する間隔も設定できます。デフォルトでは、DCNM-LAN は、監視中のデバイスから 30 秒ごとに統計データを取得します。統計データの取得間隔は最大 4 分まで増やすことができます。詳細については、「モニタリング プリファレンスの設定」（P.14-16）を参照してください。

ここでは、次の内容について説明します。

- 「統計データの自動的な消去または手動での消去」（P.25-2）
- 「仮想化のサポート」（P.25-2）

統計データの自動的な消去または手動での消去

統計データ収集機能を使用して、不要な統計データを削除できます。DCNM-LAN では、統計データの自動的な消去がサポートされています。統計データの自動的な消去の次の項目を設定できます。

- 自動消去を行う曜日と時刻。
- DCNM-LAN で、データの経過時間と最大データベース エントリ数のどちらで消去すべき統計データを決定するか。
- 消去した統計データを削除するか、1 つのエントリに統合するか。

統計データは手動で消去することもできます。

仮想化のサポート

DCNM-LAN では、Cisco NX-OS デバイス上の各仮想デバイス コンテキスト（VDC）が個別のデバイスとして扱われます。収集された統計データには、各デバイスのオブジェクトの統計情報が含まれています。

統計データ収集機能のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	リアルタイム モニタリングには、ライセンスは不要です。 Cisco DCNM-LAN の次の機能には、LAN エンタープライズ ライセンスが必要です。 • 統計データの履歴の保持 • 概要図の使用 Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

統計データ収集の前提条件

統計データを収集するには、次の前提条件が満たされている必要があります。

- DCNM-LAN サーバが各デバイスに接続できること。
- DCNM-LAN サーバと DCNM-LAN クライアントのシステム クロックが同期されていること。システム クロックが同期されていないと、データ収集のスケジューリング タスクが誤った時刻に開始または終了する可能性があります。
- Cisco NX-OS デバイスが、Cisco NX-OS のサポートされているバージョンを実行していること。
- Cisco NX-OS デバイスが、デバイス ディスカバリを正常に完了するために必要な最小構成を備えていること。詳細については、「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。

統計データ収集の注意事項と制約事項

統計データ収集機能における設定時の注意事項と制約事項は次のとおりです。

- コレクションは、新しい図のためのモニタリングを開始することによって作成されます。詳細については、「図の統計モニタリングの開始」（P.14-12）を参照してください。
- 統計データ収集機能では、[Summary] ペインに表示される情報は DCNM-LAN クライアントによって自動的に更新されません。最新の情報を表示するには、メニュー バーで、[View] > [Refresh] の順に選択してください。
- 1 つ以上の図について統計モニタリングを開始して DCNM-LAN クライアントを閉じると、データの収集を停止するのか継続するのかの確認を求めるダイアログボックスが表示されます。DCNM-LAN クライアントからログアウトするときは、不要なデータ収集をすべて停止することをお勧めします。これにより、データベース領域が節約され、サーバの負荷も軽減されます。
- DCNM-LAN のデータベース サイズが大きくなりすぎないように、統計データの自動的な消去を設定することをお勧めします。

統計データ収集の設定

ここでは、次の内容について説明します。

- 「統計データ収集の開始と停止」（P.25-3）
- 「統計図でのモードの使用方法」（P.25-4）
- 「コレクションからの統計データの削除」（P.25-5）
- 「コレクションの削除」（P.25-5）
- 「統計データベースからのデータの削除」（P.25-6）
- 「統計データの自動的な消去のイネーブル化とディセーブル化」（P.25-6）
- 「統計データの自動的な消去の設定」（P.25-7）
- 「すぐに統計データを消去する」（P.25-8）

統計データ収集の開始と停止

統計データ収集機能を使用して、統計データ収集プロセスを開始および停止できます。各収集プロセスは、デバイス コンフィギュレーション機能のモニタリングを開始することによって作成される統計監視プロセスを表します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Contents] ペインに、統計データ コレクタの一覧が表示されます。各行は、そのデバイスのコレクタに対応しています。[Status] フィールドに、コレクタが実行中か停止しているかを示すメッセージが表示されます。

ステップ 2　開始または停止するコレクタをクリックします。

ステップ 3　次のどちらかを実行します。

- コレクタを開始するには、メニュー バーで、[Actions] > [Start Collection] の順に選択します。[Status] フィールドの表示が「Running」に変わります。
- コレクタを停止するには、メニュー バーで、[Actions] > [Stop Collection] の順に選択します。[Status] フィールドの表示が「Stopped」に変わります。

変更内容を保存する必要はありません。

統計図でのモードの使用方法

統計図を使用して、デルタ モードとレート モードの間を切り替えます。表 25-1 に、統計図およびデルタ モードとレート モードの切り替えボタンが含まれる機能を示します。

表 25-1　統計図およびデルタ モードとレート モードの切り替えボタンが含まれる機能

パス	機能
[Interfaces] > [Physical]	イーサネット インターフェイス
[Interfaces] > [Physical]	管理インターフェイス
[Interfaces] > [Logical]	ループバック インターフェイス
[Interfaces] > [Logical]	ポート チャネル
[Interfaces] > [Logical]	vPC
Switching	VLAN
[Switching] > [Spanning Tree]	Rapid PVST+
[Switching] > [Spanning Tree]	MST
[Switching] > [Fabricpath]	ISIS プロセス
[Switching] > [Layer 2 Security]	ポート セキュリティ
[Switching] > [Layer 2 Security]	ARP 検査
[Switching] > [Layer 2 Security]	DHCP スヌーピング
[Switching] > [Layer 2 Security]	トラフィック ストーム制御
[Switching] > [Layer 2 Security]	IGMP スヌーピング
Security	DOT1x
[Security] > [Access Control]	IPv4 ACL
[Security] > [Access Control]	IPv6 ACL
[Security] > [Access Control]	MAC ACL
[Security] > [AAA]	サーバ グループ
Inventory	仮想スイッチ

手順の詳細

ステップ 1　[Feature Selector] ペインで、適切な機能を選択します。たとえば、イーサネット機能の統計情報を確認する場合は、[Interfaces] > [Physical] > [Ethernet] の順に選択します。

[Summary] ペインに使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、デバイスをダブルクリックします。

ステップ 3　[Summary] ペインで、[Slots] をダブルクリックします。

ステップ 4　インターフェイスをクリックします。

ステップ 5　[Details] ペインで、[Statistics] タブを選択します。

ステップ 6　ツールバーで [New Chart] をクリックします。その後、メニュー バーのドロップダウン リストから、表示する図を選択します。たとえば、トラフィックの統計情報を確認する場合は、[Traffic Statistics Chart] を選択します。

ステップ 7　（任意）統計情報モードとレート モードの間を切り替えるには、[Select Frequency] ドロップダウン リストの右側にあるボタンをクリックします。

コレクションからの統計データの削除

特定のコレクションから統計データを削除できます。この機能により、他のコレクションのデータに影響を与えることなく、特定のコレクションからすべてのデータを削除できます。コレクション自体は削除されずに残されます。各収集プロセスは、デバイス コンフィギュレーション機能のモニタリングを開始することによって作成される統計監視プロセスを表します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Contents] ペインに、統計データ コレクタの一覧が表示されます。各行は、そのデバイスのコレクタに対応しています。デバイスはアルファベット順に表示されます。[Status] フィールドに、コレクタが実行中か停止しているかを示すメッセージが表示されます。

ステップ 2　特定のコレクションを右クリックします。

ステップ 3　メニュー バーで、[Actions] > [Delete Statistical Data] の順に選択します。

コレクションからすべての統計データが削除されます。

コレクションの削除

特定のデバイスから統計データのコレクションを削除できます。各収集プロセスは、デバイス コンフィギュレーション機能のモニタリングを開始することによって作成される統計監視プロセスを表します。

（注）　コレクション自体を削除するのではなく特定のコレクションのすべてのデータを削除する場合は、「コレクションからの統計データの削除」（P.25-5）に示した手順に従います。

はじめる前に

削除するデータ コレクションを確認してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Contents] ペインに、統計データ コレクタの一覧が表示されます。デバイスはアルファベット順に表示されます。各行は、そのデバイスの統計データ コレクションに対応しています。

ステップ 2　削除するデータ コレクションをクリックします。

ステップ 3　メニュー バーで、[Actions] > [Delete Collection] の順に選択します。

コレクションが削除されます。

変更内容を保存する必要はありません。

統計データベースからのデータの削除

統計データベースから統計データを削除できます。

（注）　すべてのコレクションから古いデータを削除するのではなく特定のコレクションのすべてのデータを削除する場合は、「コレクションの削除」（P.25-5）に示した手順に従います。

はじめる前に

削除する最も新しい統計データの日時を確認してください。この手順の作業を行うと、指定した日時よりも古い統計情報がすべて削除されます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Contents] ペインの統計データ コレクタ一覧の下に、統計データベース領域が表示されます。

ステップ 2　[Delete statistical data older than] ドロップダウン リストで、削除対象となる最も新しい統計情報の日時を選択し、[OK] をクリックします。

ステップ 3　[Delete] をクリックします。

指定した日時よりも古い統計情報がすべて削除されます。

統計データの自動的な消去のイネーブル化とディセーブル化

DCNM-LAN 統計データベースからの統計データの自動的な消去をイネーブルまたはディセーブルにできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Details] ペインの統計データ コレクタのテーブルの下に、[Statistical Database Administration] タブが表示されます。

ステップ 2　[Auto Purge Settings] で、次のいずれかを行います。

- 統計データの自動的な消去をイネーブルにするには、[Enable Auto Purge] をオンにします。
- 統計データの自動的な消去をディセーブルにするには、[Enable Auto Purge] をオフにします。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

統計データの自動的な消去の設定

統計データの自動的な消去を行うタイミングと、消去する統計データを決定するための基準を設定できます。

はじめる前に

統計データの自動的な消去を実行するタイミングを決定します。統計データの自動的な消去は、DCNM-LAN の使用率が低いときに行われるよう設定することをお勧めします。

DCNM-LAN データベースをバックアップするときは、すべての統計データのレコードが保持されるように、データベースをバックアップした後に統計データの自動的な消去を行うようスケジューリングすることを検討してください。

消去する統計データを決定するために使用する基準を決定します。使用できる基準は次の 2 つです。

- 統計データの経過時間：DCNM-LAN では、指定した日数、週の数、月数よりも古い統計データ エントリをすべて消去できます。
- データベース中の統計データ エントリの数：データベース中の統計データ エントリの数が指定した最大数を超えた場合、最大数を超えなくなるまで、最も古い統計データ エントリから順番に消去できます。

両方の基準をイネーブルにした場合、DCNM-LAN はそれらを相互に独立させて適用します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Details] ペインの統計データ コレクタのテーブルの下に、[Statistical Database Administration] タブが表示されます。

ステップ 2　[Purge Threshold] で、DCNM-LAN が消去する統計データの判別に使用する基準を設定します。表 25-2 の情報を使用して、いずれかまたは両方の基準を設定できます。

表 25-2　消去基準

消去基準	設定方法
統計データの経過時間	1. [Data older than] をオンにします。 2. 最初のドロップダウン リストから、日数、週数、または月数を選択します。 3. 2 番めのドロップダウン リストから、必要に応じて [Days]、[Weeks]、または [Months] を選択します。
データベース中の統計データ エントリの数	1. [Stats. Entries Exceed(0-2147483647)] をオンにします。 2. ボックスに、統計データベースへの格納を許可する最大エントリ数を入力します。

ステップ 3　消去基準を満たす統計データベース エントリに対して実行する操作を設定します。次のいずれかを選択できます。

- [Delete]：消去基準に一致するデータベース エントリを削除します。
- [Consolidate]：消去基準に一致するすべての統計データ エントリを 1 つのエントリにマージします。

ステップ 4　[Auto Purge Settings] で、次の手順に従って自動消去を実行するタイミングを設定します。

a. 自動消去の実行を曜日で指定する場合は、[days-of-the-week] チェックボックスをオンにします。

b. 指定した日のうち、統計データを自動的に消去する正確な時刻を設定するには、[Run at] ボックスを使用します。

ステップ 5　（任意）統計データの自動的な消去をイネーブルにするには、[Enable Auto Purge] をオンにします。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに保存します。

すぐに統計データを消去する

統計データの自動的な消去の設定を使用して消去する統計データを決定し、オンデマンドで統計データを消去できます。

ヒント　統計データ エントリの経過時間に基づいて統計データをオンデマンドで消去するには、「統計データベースからのデータの削除」（P.25-6）を参照してください。

はじめる前に

統計データの自動的な消去の設定が希望の内容に設定されていることを確認します。詳細については、「統計データの自動的な消去の設定」（P.25-7）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Details] ペインの統計データ コレクタのテーブルの下に、[Statistical Database Administration] タブが表示されます。

ステップ 2　[Purge] で、[Purge Now] をクリックします。

統計データの自動的な消去の設定を使用して消去する統計データ エントリが決定され、統計データが削除されます。

統計データ コレクタのステータスの表示

統計データ コレクタのステータスを表示するには、[Feature Selector] ペインで、[DCNM Server Administration] > [Statistical Data Collection] の順に選択します。

[Contents] ペインの [Statistical Data Collectors] 領域に、コレクタのステータスおよびその他の情報が表示されます。表示される各フィールドの詳細については、「統計データ収集機能のフィールドの説明」（P.25-9）を参照してください。

統計データ収集機能のフィールドの説明

ここでは、統計データ収集機能における次の各フィールドについて説明します。

- 「[Summary] ペイン」（P.25-9）
- 「[Statistical Database Administration] タブ」（P.25-10）

[Summary] ペイン

表 25-3　[Summary] ペイン

フィールド	説明
Statistical Data Collectors	
Last Refresh Time	*表示のみ。*[Contents] ペインに表示されている情報を DCNM-LAN クライアントが更新した日時。
Collector ID	*表示のみ。*対応するポーラーのデバイスの名前と IP アドレス。
Owner	*表示のみ。*コレクションに対応する図のためのモニタリングを開始した DCNM-LAN ユーザのユーザ名。
Device	*表示のみ。*コレクションの統計データを提供するデバイスの名前と IP アドレス。

表 25-3　[Summary] ペイン （続き）

フィールド	説明
Objects	*表示のみ。*コレクションの統計データを提供するデバイス上のエンティティの説明。 たとえば、コレクションがシーケンス番号 10 を割り当てられたルールの統計データを保持しており、acl-01 という名前の IPc4 ACL に登録されている場合、このフィールドには、「acl-01,seqNo=10」と表示されます。 コレクションが、Ethernet 1/5 ポートのデータを保持している場合、このフィールドには「Ethernet 1/5」と表示されます。
Collected Statistics	*表示のみ。*コレクション内の統計データのタイプ。たとえば、コレクションが IPv4 ACL のルールに従っているかどうかを示す統計データを保持している場合、このフィールドには「IpAclAceMatchStatistics」と表示されます。
Status	*表示のみ。*コレクタが実行中か停止しているか。
Statistics Database	
Delete statistical data older than	統計データベースから削除する最も新しい統計データの日時。このフィールドにデフォルト値はありません。

[Statistical Database Administration] タブ

表 25-4　[Statistical Database Administration] タブ

フィールド	説明
Delete statistical data older than	統計データベースから削除する最も新しい統計データの日時。このフィールドにデフォルト値はありません。
Purge	
Action	統計データの自動的な消去で、消去しきい値を超えた統計データ エントリを削除するか統合するか。集約では、消去しきい値を超えたすべての統計データ エントリが 1 つのエントリにマージされます。
Purge Threshold	
Data older than	統計データの自動的な消去の際に、このチェックボックスの右にあるドロップダウン リストで指定した経過時間よりも古い統計エントリを削除するかどうか。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオンにすると、デフォルトの経過時間は 1 日になります。
Stat.Entries Exceed	統計データの自動的な消去の際に、エントリの数が、このチェックボックスの右にあるボックスの数値に等しくなるまで古い統計エントリを削除するかどうか。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオンにすると、デフォルトのイベント数は 25,000 になります。
Auto Purge Settings	
Enable Auto Purge	統計データの自動的な消去をイネーブルにするかどうか。デフォルトでは、このチェックボックスはディセーブルになっています。

表 25-4　[Statistical Database Administration] タブ（続き）

フィールド	説明
Run on	統計データの自動的な消去を行う曜日。デフォルトでは、どのチェックボックスもオンになっていません。[Daily] チェックボックスをオンにすると、個別の曜日を指定するためのチェックボックスが選択できなくなります。
Run at	自動的な消去をイネーブルにした曜日に、統計データの自動的な消去を行う時刻。

その他の関連資料

統計データ収集の管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.25-11）
- 「標準」（P.25-11）

関連資料

関連項目	参照先
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

統計データ収集の機能履歴

表 25-5 は、この機能のリリースの履歴です。

表 25-5　統計データ収集の機能履歴

機能名	リリース	機能情報
統計データ収集	5.0(2)	リリース 4.2 からの変更はありません。

CHAPTER 26

ネットワーク分析の作業

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）でネットワーク分析（PONG）機能を使用する方法について説明します。

この章の内容は、次のとおりです。

- 「ネットワーク分析の概要」（P.26-1）
- 「ネットワーク分析のライセンス要件」（P.26-2）
- 「ネットワーク分析の前提条件」（P.26-2）
- 「ネットワーク分析に関する注意事項および制約事項」（P.26-2）
- 「ネットワーク分析機能の使用方法」（P.26-2）
- 「関連資料」（P.26-8）
- 「ネットワーク分析の機能の履歴」（P.26-8）

ネットワーク分析の概要

ネットワーク分析機能は、指定された 2 台のスイッチ間の遅延を、指定された時間間隔で追跡および監視するための情報を提供します。ネットワーク分析では、ネットワーク内に指定した 2 点間の遅延を調査することにより、ネットワークの健全性を確認できます。

ネットワーク分析機能には次の特徴があります。

- ユーザが指定した 2 つのデバイス間またはポート間のリアルタイムで経時的なネットワーク分析をサポートします。ユーザは、必要なモニタリング間隔を指定します。
- 次に関するネットワーク分析の経時的な測定結果のアーカイブをサポートします。
  - エンドツーエンドのラウンドトリップ時間。
  - 各ホップでのスイッチング遅延。
  - パスごとのホップ間のリンク遅延。
- 結果として得られた統計情報が図や要約テーブルとして含まれるレポートを提供します。

ネットワーク分析のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	ネットワーク分析機能にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

ネットワーク分析の前提条件

ネットワーク分析には次の前提条件があります。

- ネットワーク分析は、DCNM-LAN によって検出されているデバイスのみが対象となります。

ネットワーク分析に関する注意事項および制約事項

ネットワーク分析機能に関する設定時の注意事項および制約事項は、次のとおりです。

- 2 台のエンド ホスト間またはホストとサーバの間のネットワーク パスを監視するために、デバイスの IP アドレスを指定します。これにより、送信元が接続されているスイッチの入力ポートから、エンド ホストまたはサーバに接続されているターゲット スイッチの出力ポートまでを監視することが可能になります。
- スイッチ間のパスを監視するために、それらのスイッチの IP アドレス、VLAN、およびオプションのインターフェイス情報を指定します。
- パス遅延の結果の評価に利用する、ラウンドトリップ時間のしきい値レベルを指定します。

ネットワーク分析機能の使用方法

ここでは、次の内容について説明します。

- 「ネットワーク分析の使用方法」（P.26-2）
- 「New Path Latency Session ウィザードの使用方法」（P.26-4）
- 「セッション統計情報の表示」（P.26-8）

ネットワーク分析の使用方法

ネットワーク分析を使用して、分析の範囲を指定したり、分析に関する情報を表示したりできます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Analysis] > [Path Latency Monitoring (PONG)] の順に選択します。

[Contents] ペインに [Summary] ペインが表示されます。テーブル内の各行が 1 つのパス遅延セッションを表します。自分で作成したセッションはもとより、他のユーザが作成したセッションも表示できます。表 26-1 を参照してください。

管理者権限を持つユーザは、他のユーザのセッションを修正することができます。

表 26-1　[Summary] ペイン内の情報

カラム	説明
Session ID	ユーザによって作成されたセッションの一意な ID。この ID は、ユーザがセッションを導入した後に更新されます。
Session Name	パス遅延セッションに対してユーザが入力した一意な名前。
Source Switch	パス遅延の監視の起点となる送信元スイッチの IP アドレス。
Destination Switch	パス遅延の監視の終点となる宛先スイッチの IP アドレス。
VLAN	実際のトラフィックが流れる VLAN ID（1 ～ 4094）。
Class of Service (CoS)	トラフィック モニタリングをサービス クラス値に基づいてフィルタリングするために使用されるオプション値（0 ～ 7）。CoS 値については、表 26-2 を参照してください。
Round Trip Time (microseconds)	現時点までに算出されたすべてのラウンドトリップ時間遅延のなかで、最小、最大、平均、および最新の RTT の値（双方向パス：送信元 <-> 宛先）。
Forward Delay (microseconds)	現時点までに算出されたすべての順方向遅延のなかで、最小、最大、平均、および最新の順方向遅延の値（順方向パス：送信元 -> 宛先）。
Reverse Delay (microseconds)	現時点までに算出されたすべての逆方向遅延のなかで、最小、最大、平均、および最新の逆方向遅延の値（逆方向パス：宛先 -> 送信元）。
Owner	セッションの作成者。
Success Percentage	指定された時間間隔内での送信元から宛先までのパケット移動の成功率。
Scheduled At	モニタリングが開始された日時。
Status	次の状態を示すカラム。 • セッション作成 • モニタリング開始 • モニタリング停止

表 26-2　CoS 値および対応するトラフィック タイプ

ユーザ優先度	トラフィック タイプ
0	バックグラウンド
1	ベスト エフォート
2	エクセレント エフォート
3	クリティカル アプリケーション
4	ビデオ、100 ms 未満の遅延
5	音声、10 ms 未満の遅延
6	インターネットワーク制御
7	ネットワーク制御

ステップ 2　[Summary] ペインの上で、[Configure New Rule] リンクをクリックして、次のパラメータのいずれかについてしきい値規則を設定します。

- ラウンドトリップ時間
- 順方向遅延
- 逆方向遅延

（注）　[Configure New Rule] をクリックすると、DCNM-LAN サーバ管理機能のしきい値規則にリンクします。

ステップ 3　[Summary] ペインの上で、[Set Global Threshold] リンクをクリックして、次のパラメータのグローバルしきい値規則を設定します。

- ラウンドトリップ時間
- 順方向遅延
- 逆方向遅延

グローバルしきい値設定は、[Summary] テーブル内のすべてのセッションに適用されます。

ステップ 4　[Summary] ペインの上で、[VLAN-CoS] ボタンをクリックして、VLAN-CoS でグループ化されたセッションを表示します。

New Path Latency Session ウィザードの使用方法

New Path Latency Session ウィザードを使用して、新しいセッションを作成できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Analysis] > [Path Latency Monitoring (PONG)] の順に選択します。

[Contents] ペインに [Summary] ペインが表示されます。

ステップ 2　[Summary] ペイン内で右クリックし、コンテキスト メニュー内の [New Path Latency Session] を選択します。

New Path Latency Session ウィザードが表示されます。

ステップ 3　[Select Session Monitor Option of Interest] 画面で次を入力します。

- セッション名

  （長さ：1 ～ 256 文字）
- VLAN

  （値：1 ～ 4094）
- Class of Service（CoS）

表 26-3　CoS 値および対応するトラフィック タイプ

ユーザ優先度	トラフィック タイプ
0	バックグラウンド
1	ベスト エフォート
2	エクセレント エフォート
3	クリティカル アプリケーション
4	ビデオ、100 ms 未満の遅延
5	音声、10 ms 未満の遅延
6	インターネットワーク制御
7	ネットワーク制御

ステップ 4　[Select Option] セクションで、次のいずれかのオプションを選択します。

- Monitor latency between source VDC and destination VDC.
- Monitor latency between source and destination VDC including source switching delay.
- Monitor latency between source and destination VDC including destination switching delay.
- Monitor latency between source and destination VDC including both switching delays.

[Monitor latency between source VDC and destination VDC] オプションでは、ファブリック パス モード接続を持つスイッチ間の遅延を測定するように追加で選択することもできます。この遅延の測定値は、送信元スイッチと宛先スイッチの間で測定されますが、これら両方のエンド スイッチのスイッチング遅延は含まれていません。

（注）　クラシカル イーサネット クラウド内のスイッチの場合、このウィザードでは、後に続くウィザード画面でそれらのスイッチの VDC MAC アドレス /IP アドレス / ホスト名を選択できます。

[Next] をクリックして続行します。

ステップ 5　[Select Source and Destination Switch] 画面で、次の作業を実行します。

- 送信元スイッチを選択するために、[Select Source Switch] フィールドの隣にある楕円をクリックします。表示された画面内で対象デバイスを強調表示にし、[OK] をクリックしてその選択を入力します。

- 宛先スイッチを選択するために、[Select Destination Switch] フィールドの隣にある楕円をクリックします。表示された画面内で対象デバイスを強調表示にし、[OK] をクリックしてその選択を入力します。

表 26-4 に、[Select Source and Destination Switch] 画面で入力しなければならない必須およびオプションの情報を示します。これらの情報は、前述の [Select Option] セクション内で行った選択に応じて変化します。

表 26-4　必須およびオプションの情報

オプション	必須	任意
Monitor latency between source VDC and destination VDC	• 送信元と宛先	• 送信元からパケットが発信される出力/アウトバウンド インターフェイス。
Monitor latency between source and destination VDC including source switching delay	• 送信元と宛先 • 送信元スイッチからパケットが挿入される必要のある挿入/入力インターフェイス。このインターフェイスに関連付けられる送信元スタティック MAC アドレスも必要です。	• N/A
Monitor latency between source and destination VDC including destination switching delay	• 送信元と宛先 • 宛先スイッチでパケットが終端される出力/アウトバウンド インターフェイス。このインターフェイスに関連付けられる宛先スタティック MAC アドレスも必要です。	• 送信元からパケットが発信される出力/アウトバウンド インターフェイス。
Monitor latency between source and destination VDC including both switching delays	• 送信元と宛先 • 送信元スイッチからパケットが挿入される必要のある挿入/入力インターフェイス。このインターフェイスに関連付けられる送信元スタティック MAC アドレスも必要です。 • 宛先スイッチでパケットが終端される出力/アウトバウンド インターフェイス。このインターフェイスに関連付けられる宛先スタティック MAC アドレスも必要です。	• N/A

（注）　選択したインターフェイスを指し示す任意の一意なスタティック MAC アドレスを入力できます。新しいスタティック MAC アドレスを設定する場合は、グローバルに管理されている MAC アドレス（他のホスト/デバイスに関連付けられている）と競合することがないように、次の推奨アドレスのいずれかを使用します。

- X2XX.XXXX.XXXX
- X6XX.XXXX.XXXX
- XAXX.XXXX.XXXX
- XEXX.XXXX.XXXX

ここで、X は 16 進数値です。

[Next] をクリックして続行します。

ステップ 6　表示されたダイアログボックスで、[OK] をクリックして入力の検証を開始します。

[Input Verification] 画面が表示され、結果が表示されます。

入力の検証では、次の内容が検証されます。

- 指定されたデバイス間のパス遅延の測定。
- 指定されたデバイス間のパケットの移動。

検証に失敗した場合、ウィザードで前に入力した情報を指定する必要があります。

表 26-5 に、[Input Verification] ウィンドウで使用可能な追加の設定を示します。

表 26-5　[Input Verification] 設定

設定	説明	値
Monitor Interval	データ収集ポイント間の時間間隔。	0.5 ～ 5 分 （デフォルト：5 分）
End Time	セッション終了の時間	N/A
Calculate Jitter	パケット間の RTT 遅延の変動	デフォルト：オフ
No.of Packets to send	セッションで遅延を測定するために送信するパケット数。 ジッター（パケット間の遅延の変動）を計算するには、2 つ以上のパケットを送信する必要があります。	1 ～ 5 パケット （デフォルト：1 パケット）

検証に成功したら [Finish] をクリックして設定を入力します。

セッション統計情報の表示

[Summary] ペインからセッション統計情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Network Analysis] > [Path Latency Monitoring (PONG)] の順に選択します。

[Contents] ペインに [Summary] ペインが表示されます。

ステップ 2　セッションを右クリックし、コンテキスト メニュー内の [Go To Statistics] を選択します。

[Details] ペイン内に、セッションの統計情報が図とテーブルで詳細に表示されます。

ステップ 3　[Details] ペインで、[Path Latency] タブをクリックして各パスの RTT 情報を表示します。

ステップ 4　[Details] ペイン内で右クリックして、追加の統計情報表示のコンテキスト メニューを表示します。

- パス固有のスイッチング遅延：各パスで通過したすべてのスイッチのスイッチング遅延。
- パス固有のリンク遅延：各パスで通過した各ホップでのリンク遅延。
- セッション内で通過したさまざまなパスでの各スイッチのスイッチング遅延。
- セッション内で通過したさまざまなパスでの各リンクのリンク遅延。

ステップ 5　[Details] ペインで、[Session Report] タブをクリックしてセッションに関する総合的な統計情報を表示します。

これらの情報は、テーブルの上部付近にある [export] ボタンをクリックして、Excel の .xls ファイルとしてエクスポートできます。

関連資料

トポロジ マップに関する追加情報については、次のセクションを参照してください。

関連項目	参照先
デバイス ディスカバリ	第 16 章「デバイス ディスカバリの管理」
ネットワーク サーバ	第 20 章「ネットワーク サーバの設定」

ネットワーク分析の機能の履歴

表 26-6 は、この機能のリリースの履歴です。

表 26-6　トポロジの機能履歴

機能名	リリース	機能情報
ネットワーク分析サポート	5.2(0)	ネットワーク分析のサポートが追加されました。

CHAPTER 27

DCNM-LAN サーバ ログ設定の管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）で DCNM-LAN サーバ ログ設定機能を管理する方法について説明します。

この章で説明する内容は、次のとおりです。

- 「DCNM-LAN サーバ ログ設定の管理の概要」（P.27-1）
- 「DCNM-LAN サーバ ログ設定の管理のライセンス要件」（P.27-2）
- 「DCNM-LAN サーバ ログ設定の管理に関する前提条件」（P.27-2）
- 「DCNM-LAN サーバ ログ設定の管理に関する注意事項と制約事項」（P.27-3）
- 「DCNM-LAN サーバ ログの設定」（P.27-3）
- 「DCNM-LAN サーバ ログ設定の表示」（P.27-5）
- 「DCNM-LAN サーバ ログ設定のフィールドの説明」（P.27-5）
- 「その他の関連資料」（P.27-6）
- 「DCNM-LAN サーバ ログ設定の機能の履歴」（P.27-7）

DCNM-LAN サーバ ログ設定の管理の概要

DCNM-LAN サーバは、その動作を記録したログ ファイルを管理しています。このログ ファイルには、DCNM-LAN 機能とサーバ コンポーネントに関する情報が記録されます。

（注） DCNM-LAN サーバ ログ設定機能は、Cisco NX-OS デバイスのログ レベルには影響を与えません。DCNM-LAN では、デバイスのログ レベルを設定できません。

ここでは、次の内容について説明します。

- 「ログ レベル」（P.27-2）
- 「ログ ファイルとその存在場所」（P.27-2）
- 「仮想化のサポート」（P.27-2）

ログ レベル

DCNM-LAN サーバは、ログ メッセージの重大度で順序付けされたログ レベル階層をサポートしています。各レベルには、そのレベルのメッセージに加えて、より重大度の高いすべてのログ メッセージが含まれます。次のログ レベルがあります（重大度の高い順）。

- Fatal Errors
- Errors
- Warnings
- Information
- Debugging
- Verbose

ログ ファイルとその存在場所

DCNM-LAN サーバは、サーバ ログ メッセージを、次の場所にある sys.pipe ファイルに書き出します。

INSTALL_DIR\log

デフォルトでは、Microsoft Windows Server に DCNM-LAN サーバをインストールする場合、INSTALL_DIR は C:¥Program Files¥Cisco Systems¥dcnm になっています。

仮想化のサポート

DCNM-LAN サーバ ログには、Cisco NX-OS デバイスからのログ メッセージは記録されません。したがって、この機能は仮想化サポートには影響を与えません。

DCNM-LAN サーバ ログ設定の管理のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	DCNM-LAN サーバ ログ設定にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN サーバ ログ設定の管理に関する前提条件

DCNM-LAN サーバ ログの設定を管理するには、次の前提条件を満たしている必要があります。

- DCNM-LAN の機能に対してサーバ ログを設定するにはその機能の知識が必要です。

DCNM-LAN サーバ ログ設定の管理に関する注意事項と制約事項

DCNM-LAN サーバ ログ設定機能の管理における注意事項と制約事項は次のとおりです。

- ログ レベルの重大度を下げると、ログ ファイルに出力されるメッセージの数が増えます。
- トラブルシューティングを行っている場合を除き、デフォルトのログ設定を使用することを推奨します。
- トラブルシューティングを行っている場合は、関連する機能やサーバ コンポーネントのログ レベルの重大度を下げることを検討します。
- 問題が解決したら、関連する機能やサーバ コンポーネントのログ レベルの重大度を元に戻すことを検討します。

DCNM-LAN サーバ ログの設定

ここでは、次の内容について説明します。

- 「デフォルトのログ レベルの設定」（P.27-3）
- 「機能またはサーバ コンポーネントの一意なログ レベルの設定」（P.27-3）
- 「デフォルトのログ レベルを使用させるための機能またはサーバ コンポーネントの設定」（P.27-4）

デフォルトのログ レベルの設定

すべての DCNM-LAN 機能およびサーバ コンポーネントにはデフォルトのログ レベルを設定できます。

はじめる前に

目的のデフォルト ログ レベルを確認してください。詳細については、「ログ レベル」（P.27-2）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Server Log Settings] の順に選択します。

[Contents] ペインにログ設定が表示されます。

ステップ 2　[Default Logging Level] ドロップダウン リストで、ログ レベルを選択します。

ステップ 3　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

機能またはサーバ コンポーネントの一意なログ レベルの設定

デフォルトのログ レベルとは別に、機能またはサーバ コンポーネントにログ レベルを設定できます。

はじめる前に

機能またはサービスの目的のログ レベルを確認してください。詳細については、「ログ レベル」（P.27-2）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Server Log Settings] の順に選択します。

[Contents] ペインにログ設定が表示されます。

ステップ 2　一意なログ レベルを設定する機能またはサーバ コンポーネントを検索します。

ステップ 3　その機能またはサーバ コンポーネントの右側にある [Default] チェックボックスをオフにします。

機能またはサーバ コンポーネントの [Logging Level] ドロップダウン リストが使用できるようになります。

ステップ 4　[Logging Level] ドロップダウン リストで、ログ レベルを選択します。詳細については、「ログ レベル」（P.27-2）を参照してください。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

デフォルトのログ レベルを使用させるための機能またはサーバ コンポーネントの設定

デフォルトのログ レベルを使用するように機能またはサーバ コンポーネントを設定できます。

はじめる前に

対象となる機能またはサービスにとってデフォルトのログ レベルが適切であることを確認します。詳細については、「ログ レベル」（P.27-2）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Server Log Settings] の順に選択します。

[Contents] ペインにログ設定が表示されます。

ステップ 2　デフォルトのログ レベルを使用する機能またはサーバ コンポーネントを検索します。

ステップ 3　その機能またはサービスの右側にある [Default] チェックボックスをオンにします。

機能またはサーバ コンポーネントの [Logging Level] ドロップダウン リストが使用不可になります。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN サーバ ログ設定の表示

DCNM-LAN サーバ ユーザ アカウントを表示するには、[Feature Selector] ペインで [DCNM Server Administration] > [DCNM Server Log Settings] の順に選択します。

[Contents] ペインに、デフォルトのログ レベル、機能ログ設定、およびサーバ コンポーネント ログ設定が表示されます。表示される各フィールドの詳細については、「DCNM-LAN サーバ ログ設定のフィールドの説明」（P.27-5）を参照してください。

DCNM-LAN サーバ ログ設定のフィールドの説明

ここでは、DCNM-LAN サーバ ログ設定の次の各フィールドについて説明します。

- 「DCNM-LAN サーバ ログ設定の [Contents] ペイン」（P.27-5）

DCNM-LAN サーバ ログ設定の [Contents] ペイン

表 27-1　DCNM-LAN サーバ ログ設定の [Contents] ペイン

フィールド	説明
Default Logging Level	[Default] チェックボックスがオンになっている機能またはサーバ コンポーネントのログ レベル。このリストのデフォルト値は [Informational] です。ログ レベルの詳細については、「ログ レベル」（P.27-2）を参照してください。
DCNM-LAN の機能	
Default	対応する機能のロギングに、デフォルトのログ レベルまたは機能固有のログ レベルのどちらを使用するかを示します。[Default] チェックボックスをオンにすると、対応する機能のログ レベル リストが使用不可になります。デフォルトでは、このチェックボックスはオフになっています。
AAA	AAA 機能のログ レベル。
ACL	アクセス コントロール リスト機能のログ レベル。
Dot1X	802.1X 機能のログ レベル。
GLBP	ゲートウェイ ロード バランシング プロトコル機能のログ レベル。
Interfaces	インターフェイス機能のログ レベル。
Key Chain	キーチェーン管理機能のログ レベル。
Layer 2 Security	レイヤ 2 セキュリティ機能のログ レベル。次のいずれかを指定します。 • ダイナミック ARP インスペクション • ポート セキュリティ • DHCP スヌーピング • IP ソース ガード • トラフィック ストーム制御
Object Tracking	オブジェクト トラッキング機能のログ レベル。
Port Channel	ポート セキュリティ機能のログ レベル。
SPAN	SPAN 機能のログ レベル。

表 27-1　DCNM-LAN サーバ ログ設定の [Contents] ペイン （続き）

フィールド	説明
Spanning Tree	STP 機能のログ レベル。
Tunnel	トンネル インターフェイス管理機能のログ レベル。
Virtual Devices	仮想デバイス コンテキスト機能のログ レベル。
VLAN	VLAN 機能のログ レベル。
FabricExtender	Fabric Extender 機能のログ レベル。
VPC	vPC 機能のログ レベル。
HSRP	HSRP 機能のログ レベル。
DEVICE GROUP	デバイス グループ機能のログ レベル。
DCNM-LAN サーバ コンポーネント	
Default	対応するサーバ コンポーネントのロギングに、デフォルトのログ レベルまたはコンポーネント固有のログ レベルのどちらを使用するかを示します。[Default] チェックボックスをオンにすると、対応するコンポーネントのログ レベル リストが使用不可になります。デフォルトでは、このチェックボックスはオフになっています。
Event	イベント コンポーネントのログ レベル。イベント コンポーネントには、DCNM-LAN がシステムを処理する方法に関するメッセージ、DCNM-LAN がデバイスから取得するアカウンティング ログ、DCNM-LAN によって生成されるイベントなどが含まれます。
Statistics Collection	統計情報データ収集コンポーネントのログ レベル。
Config Archive	コンフィギュレーション変更管理機能によって使われる設定アーカイブ コンポーネントのログ レベル。
Device Connections	DCNM-LAN サーバをデバイスに接続するコンポーネントのログ レベル。
Device Discovery	デバイス ディスカバリを実行するコンポーネントのログ レベル。

その他の関連資料

DCNM-LAN サーバ ログ設定の管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.27-6）
- 「標準」（P.27-7）

関連資料

関連項目	参照先
DCNM-LAN のトラブルシューティング	第 30 章「DCNM-LAN のトラブルシューティング」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN サーバ ログ設定の機能の履歴

表 27-2 は、この機能のリリースの履歴です。

表 27-2　DCNM-LAN サーバ ログ設定の機能の履歴

機能名	リリース	機能情報
デバイス グループのロギング	5.0(2)	デバイス グループ機能のログ レベルを設定するためのサポートが追加されました。

CHAPTER 28

Cisco DCNM-LAN サーバの起動と停止

ここでは、Cisco Data Center Network Manager for LAN（DCNM-LAN）サーバを起動および停止する方法について説明します。

この章の内容は、次のとおりです。

- 「DCNM-LAN サーバの起動と停止の概要」（P.28-1）
- 「Cisco DCNM-LAN サーバの起動と停止のライセンス要件」（P.28-1）
- 「DCNM-LAN サーバの起動」（P.28-1）
- 「DCNM-LAN サーバの停止」（P.28-5）
- 「関連資料」（P.28-8）
- 「DCNM-LAN サーバの起動と停止の機能の履歴」（P.28-9）

DCNM-LAN サーバの起動と停止の概要

DCNM-LAN サーバの起動と停止は、データベースのバックアップ、クリーンアップ、復元などのサーバ メンテナンスで必要です。クラスタ サーバ配置では、DCNM-LAN サーバを起動する順序によって、どのサーバがマスター サーバになるかが決まります。ここでは、単一サーバ配置とクラスタ サーバ配置の両方について DCNM-LAN サーバの起動と停止の詳しい手順を説明します。

Cisco DCNM-LAN サーバの起動と停止のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	Cisco DCNM-LAN サーバの起動と停止にライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN サーバの起動

ここでは、次の内容について説明します。

- 「単一の DCNM-LAN サーバの起動」（P.28-2）
- 「DCNM-LAN サーバ クラスタの起動」（P.28-3）

単一の DCNM-LAN サーバの起動

単一の DCNM-LAN サーバを起動できます。単一の DCNM-LAN サーバを起動する手順は、システムで使用されるオペレーティング システムによって異なります。サポートされる Microsoft Windows Server オペレーティング システムと Red Hat Enterprise Linux（RHEL）オペレーティング システムについて次に説明します。

- 「単一の DCNM-LAN サーバ（Microsoft Windows Server）の起動」（P.28-2）
- 「単一の DCNM-LAN サーバ（RHEL）の起動」（P.28-2）

単一の DCNM-LAN サーバ（Microsoft Windows Server）の起動

Microsoft Windows Server を実行するサーバ システムでは、Windows サービスを介して、または [Start DCNM-LAN Server] アイコンをクリックして、DCNM-LAN サーバを起動できます。

はじめる前に

DCNM-LAN サーバをインストールしておく必要があります。

サーバ クラスタを起動している場合は、正しい順序でサーバを起動してください。詳細については、「DCNM-LAN サーバ クラスタの起動」（P.28-3）を参照してください。

手順の詳細

ステップ 1　[Control Panel] ウィンドウを開き、[Administrative Tools] > [Services] の順に選択します。

[Services] ウィンドウが開きます。

ステップ 2　[Cisco DCNM Server] を右クリックして、[Start] を選択します。

（注）　または、[Start] > [All Programs] > [Cisco DCNM Server] > [Start DCNM Server] の順に選択します。ただし、ショートカットの場所は、DCNM-LAN サーバをインストールしたときの選択内容によって異なります。

DCNM-LAN サーバが起動している間、スプラッシュ画面が開きます。DCNM-LAN サーバが実行されると、この画面は閉じます。

単一の DCNM-LAN サーバ（RHEL）の起動

RHEL を実行するサーバ システムでは、Start_DCNM_LAN_Server スクリプトで DCNM-LAN サーバを起動できます。このスクリプトはホーム フォルダ内か、Cisco DCNM-LAN のインストール時にリンク フォルダの設定で指定したフォルダ内にあります。

（注）　Start_DCNM_LAN_Server は、/usr/local/Cisco/dcm/dcnm/bin/startdcnm.sh を起動します。

はじめる前に

DCNM-LAN サーバをインストールする必要があります。

サーバ クラスタを起動している場合は、正しい順序でサーバを起動してください。詳細については、「DCNM-LAN サーバ クラスタの起動」（P.28-3）を参照してください。

手順の詳細

ステップ 1　**Start_DCNM_LAN_Server** スクリプトを使用して、RHEL オペレーティング システム上でサーバを起動します。

DCNM-LAN サーバのサーバ コンソール ウィンドウが開き、サーバ起動時に実行されるプロセスが表示されます。サーバが実行されると、「Started in *X*m:*XX*s:*XXX*ms」メッセージが表示されます。

DCNM-LAN サーバ クラスタの起動

セカンダリ サーバのオペレーティング システムに応じて、DCNM-LAN サーバの起動には、Windows GUI、CLI、または DCNM Install Manager ツールを使用できます。RHEL が動作しているセカンダリ サーバでは、CLI または DCNM Install Manager ツールを使用できます。Microsoft Windows が動作しているセカンダリ サーバの場合、DCNM-LAN サーバは Windows GUI で起動できます。

Windows GUI または RHEL CLI を使用した起動

DCNM-LAN サーバ クラスタを起動するときは、各サーバを 1 台ずつ起動する必要があり、サーバ起動の順序が重要です。起動時刻の最も古いサーバが、サーバ クラスタでマスター サーバ ロールを実行します。

はじめる前に

プライマリ インストール サーバをマスター サーバとして使用することを推奨します。クラスタ サーバ環境の配置の詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

クラスタ内で実行しているサーバがある場合は、そのサーバを停止してからクラスタを起動します。どのサーバをマスター サーバにするかを制御するには、他のサーバよりも先にマスター サーバを起動する必要があります。詳細については、「DCNM-LAN サーバの停止」（P.28-5）を参照してください。

手順の詳細

ステップ 1　クラスタのマスター サーバにするサーバを起動します。これは、該当するオペレーティング システムの単一の DCNM-LAN サーバを起動するための次の手順に従って行います。

- 「単一の DCNM-LAN サーバ（Microsoft Windows Server）の起動」（P.28-2）
- 「単一の DCNM-LAN サーバ（RHEL）の起動」（P.28-2）

ステップ 2　マスター サーバが起動を終了するまで待機します。

ステップ 3　クラスタ内の残りのサーバを 1 台ずつ起動します。1 台のサーバを起動したら、少なくとも 1 分間待ってから次のサーバを起動します。このように遅らせることで、サーバ クラスタが早く安定します。

サーバごとに、該当するオペレーティング システムの単一の DCNM-LAN サーバを起動する手順は、次のとおりです。

- 「単一の DCNM-LAN サーバ（Microsoft Windows Server）の起動」（P.28-2）
- 「単一の DCNM-LAN サーバ（RHEL）の起動」（P.28-2）

Install Manager を使用した起動

DCNM Install Manager は、Linux が動作するサーバ用の GUI ツールです。セカンダリ サーバ（リモート ノード）上でのサイレント モード操作の実行を支援するように設計されています。

（注）　DCNM Install Manager は、Windows サーバをサポートしていません。

手順の詳細

ステップ 1　Install Manager にアクセスするには、dcnm-install-manager.sh ファイルの場所（DCNM-LAN サーバがインストールされた bin フォルダ内）に移動します。

Linux が動作しているサーバの場合、デフォルトの bin フォルダは、/usr/local/Cisco/dcm/dcnm/bin です。

ステップ 2　**dcnm-install-manager.sh** ファイルをダブルクリックして、Install Manager を起動します。

ステップ 3　ツールバーで、Install Manager GUI の上部付近にある [New] アイコンをセカンダリ サーバの台数と同じ回数だけクリックします。

[New] アイコンがクリックされるたびに、[Server Nodes] のリスト内に新しい行が作成されます。

（注）　ツールバーで、[Delete] アイコンをクリックすると、[Server Nodes] のリスト内で選択されている行が削除されます。このステップでは、クラスタ サーバ環境からセカンダリ サーバは削除されません。

ステップ 4　[Server Nodes] のリスト内でそれぞれ 1 行で表されている各セカンダリ サーバについて、次を入力します。

- [Server Name/IP Address] フィールドに、サーバ名または IP アドレス。
- [Protocol] フィールドに、接続に使用されるプロトコル。

  このプロトコルは Telnet または SSH のいずれかです。
- [User Credentials] フィールドに、セカンダリ サーバへの接続に使用されるユーザ クレデンシャル（ユーザ ID とパスワード）。

  このユーザ クレデンシャルは、サーバへの SSH 接続に使用されます。サーバへの Telnet 接続には、ユーザ クレデンシャルは必要ありません。

  別の方法として、GUI の [Default Credentials] セクションでクレデンシャルを入力することにより、デフォルト ユーザ クレデンシャルを設定することもできます。このデフォルト クレデンシャルは、[User Credential] フィールドが空白のときに使用されます。
- （任意）[Comments] フィールドに、セカンダリ サーバを識別する際に役立つコメント。

[Server Nodes] のリスト内の [Last Action Status] 列には、最後に実行された操作の成功または失敗ステータスが示されます。[Last Action Status] の [+] アイコンをクリックすると、表示が展開され、サーバに対して実行された操作のログがすべて表示されます。

ステップ 5　[Server Nodes] のリスト内で、起動するセカンダリ サーバを選択します。

ステップ 6　ツールバーで、[Verify] アイコンをクリックして、選択したセカンダリ サーバへの接続を確認します。

接続に関する問題がある場合は、先に進む前に修正します。

ステップ 7　ツールバーで、[Start] アイコンをクリックして、選択したセカンダリ サーバを起動します。

（注）　Install Manager はスタンドアロン アプリケーションです。指定された設定は保存されず、永続的ではありません。Install Manager GUI を閉じると、設定は失われます。

DCNM-LAN サーバの停止

ここでは、次の内容について説明します。

- 「単一の DCNM-LAN サーバの停止」（P.28-5）
- 「DCNM-LAN サーバ クラスタの停止」（P.28-6）

単一の DCNM-LAN サーバの停止

単一の DCNM-LAN サーバを停止できます。

単一の DCNM-LAN サーバを停止する手順は、システムで使用されるオペレーティング システムによって異なります。サポートされる Microsoft Windows Server オペレーティング システムと RHEL オペレーティング システムについて次に説明します。

- 「単一の DCNM-LAN サーバ（Microsoft Windows Server）の停止」（P.28-5）
- 「単一の DCNM-LAN サーバ（RHEL）の停止」（P.28-6）

単一の DCNM-LAN サーバ（Microsoft Windows Server）の停止

Microsoft Windows Server を実行するサーバ システムでは、Windows サービスを介して、または [Stop DCNM Server] アイコンをクリックして、DCNM-LAN サーバを停止できます。

手順の詳細

ステップ 1　[Control Panel] ウィンドウを開き、[Administrative Tools] > [Services] の順に選択します。

ウィンドウが開き、Windows サービスのリストが表示されます。

ステップ 2　[Cisco DCNM Server] を右クリックして、[Stop] を選択します。

（注）　または、[Start] > [All Programs] > [Cisco DCNM Server] > [Stop DCNM Server] の順に選択します。ただし、ショートカットの場所は、DCNM-LAN サーバをインストールしたときの選択内容によって異なります。

DCNM-LAN サーバのシャットダウン中は、スプラッシュ画面が表示されます。DCNM-LAN サーバが停止すると、スプラッシュ画面は閉じます。

単一の DCNM-LAN サーバ（RHEL）の停止

RHEL を実行するサーバ システムでは、Stop_DCNM_LAN_Server スクリプトで DCNM-LAN サーバを停止できます。このスクリプトはホーム フォルダ内か、Cisco DCNM-LAN のインストール時にリンク フォルダの設定で指定したフォルダ内にあります。

（注）　Stop_DCNM_LAN_Server は、/usr/local/Cisco/dcm/dcnm/bin/stopdcnm.sh を起動します。

手順の詳細

ステップ 1　**Stop_DCNM_LAN_Server** スクリプトを使用して、RHEL オペレーティング システム上のサーバを停止します。

DCNM-LAN サーバのサーバ コンソール ウィンドウが開き、サーバ停止時に実行されるプロセスが表示されます。サーバが停止すると、「Stopped at *X*m:*XX*s:*XXX*ms」メッセージが表示されます。

DCNM-LAN サーバ クラスタの停止

セカンダリ サーバのオペレーティング システムに応じて、DCNM-LAN サーバの停止には、CLI または DCNM Install Manager ツールを使用できます。RHEL が動作しているセカンダリ サーバでは、CLI または DCNM Install Manager ツールを使用できます。Microsoft Windows が動作しているセカンダリ サーバの場合、DCNM-LAN サーバは CLI で停止できます。

CLI を使用した停止

クラスタ サーバ DCNM-LAN 配置の場合、stop-dcnm-cluster スクリプトを使用してクラスタ内のすべてのサーバを停止できます。

はじめる前に

DCNM-LAN サーバ クラスタ内でどのサーバが現在のマスター サーバであるかを確認してください。これはクラスタ管理機能を使って確認できます。詳細については、「サーバ情報の表示」（P.22-4）を参照してください。

手順の詳細

ステップ 1　マスター サーバで、コマンド プロンプトにアクセスします。

ステップ 2　次のように **cd** コマンドを使用して、ディレクトリを Cisco DCNM インストレーション ディレクトリにある bin ディレクトリに変更します。

cd *path*

ここで、*path* は、bin ディレクトリへの相対パスまたは絶対パスです。Microsoft Windows では、Cisco DCNM bin ディレクトリのデフォルト パスは C:¥Program Files¥Cisco Systems¥dcm¥dcnm¥bin です。RHEL の場合、bin ディレクトリへのデフォルト パスは /usr/local/cisco/dcm/dcnm/bin です。

ステップ 3　**stop-dcnm-cluster** スクリプトを実行します。スクリプト名は、次の表に示すようにサーバ オペレーティング システムによって異なります。

サーバ オペレーティング システム	DCNM クラスタ停止スクリプト
Microsoft Windows	stop-dcnm-cluster.bat
Linux	stop-dcnm-cluster.sh

このスクリプトにより、クラスタ内の各 DCNM-LAN サーバが停止を指示されます。

例

次の Microsoft Windows サーバの例は、DCNM-LAN サーバ クラスタを停止する方法を示しています。DCNM-LAN はデフォルト ディレクトリにインストールされています。

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>stop-dcnm-cluster.bat

C:\Program Files\Cisco Systems\dcm\dcnm\bin>set JAVA_HOME=C:\Program Files\Cisco Systems\
dcm\java\jre1.5

C:\Program Files\Cisco Systems\dcm\dcnm\bin>"C:\Program Files\Cisco Systems\dcm\
jboss-4.2.2.GA\bin\twiddle.bat" -s 172.28.254.254:1099 invoke
"com.cisco.dcbu.dcm:service=ClusterServerInfo" stopServerInstancesInCluster 10
Shutdown Triggered for all Servers Successfully
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

Install Manager を使用した停止

Cisco DCNM Install Manager は、Linux が動作するサーバ用の GUI ツールです。セカンダリ サーバ（リモート ノード）上でのサイレント モード操作の実行を支援するように設計されています。

（注）　Cisco DCNM Install Manager は、Windows サーバをサポートしていません。

手順の詳細

ステップ 1　Install Manager にアクセスするには、dcnm-install-manager.sh ファイルの場所（DCNM-LAN サーバがインストールされた bin フォルダ内）に移動します。

Linux が動作しているサーバの場合、デフォルトの bin フォルダは、/usr/local/Cisco/dcm/dcnm/bin です。

ステップ 2　**dcnm-install-manager.sh** ファイルをダブルクリックして、Install Manager を起動します。

ステップ 3　ツールバーで、Install Manager GUI の上部付近にある [New] アイコンをセカンダリ サーバの台数と同じ回数だけクリックします。

[New] アイコンがクリックされるたびに、[Server Nodes] のリスト内に新しい行が作成されます。

（注）　ツールバーで、[Delete] アイコンをクリックすると、[Server Nodes] のリスト内で選択されている行が削除されます。このステップでは、クラスタ サーバ環境からセカンダリ サーバは削除されません。

ステップ 4　[Server Nodes] のリスト内でそれぞれ 1 行で表されている各セカンダリ サーバについて、次を入力します。

- [Server Name/IP Address] フィールドに、サーバ名または IP アドレス。
- [Protocol] フィールドに、接続に使用されるプロトコル。

  このプロトコルは Telnet または SSH のいずれかです。
- [User Credentials] フィールドに、セカンダリ サーバへの接続に使用されるユーザ クレデンシャル（ユーザ ID とパスワード）。

  このユーザ クレデンシャルは、サーバへの SSH 接続に使用されます。サーバへの Telnet 接続には、ユーザ クレデンシャルは必要ありません。

  別の方法として、GUI の [Default Credentials] セクションでクレデンシャルを入力することにより、デフォルト ユーザ クレデンシャルを設定することもできます。このデフォルト クレデンシャルは、[User Credential] フィールドが空白のときに使用されます。
- （任意）[Comments] フィールドに、セカンダリ サーバを識別する際に役立つコメント。

[Server Nodes] のリスト内の [Last Action Status] 列には、最後に実行された操作の成功または失敗ステータスが示されます。[Last Action Status] の [+] アイコンをクリックすると、表示が展開され、サーバに対して実行された操作のログがすべて表示されます。

ステップ 5　[Server Nodes] のリスト内で、停止するセカンダリ サーバを選択します。

ステップ 6　ツールバーで、[Verify] アイコンをクリックして、選択したセカンダリ サーバへの接続を確認します。

接続に関する問題がある場合は、先に進む前に修正します。

ステップ 7　ツールバーで、[Stop] アイコンをクリックして、選択したセカンダリ サーバを停止します。

（注）　Install Manager はスタンドアロン アプリケーションです。指定された設定は保存されず、永続的ではありません。Install Manager GUI を終了すると、設定は失われます。

関連資料

関連項目	参照先
単一の DCNM-LAN サーバの配置と DCNM-LAN サーバ クラスタの配置	『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』
サーバ クラスタ情報の表示	第 22 章「クラスタ管理の作業」
DCNM-LAN データベースのバックアップ、クリーンアップ、および復元	第 29 章「Cisco DCNM-LAN データベースのメンテナンス」

DCNM-LAN サーバの起動と停止の機能の履歴

表 28-1 は、この機能のリリースの履歴です。

表 28-1　DCNM-LAN サーバの起動と停止の機能の履歴

機能名	リリース	機能情報
サーバ クラスタの起動と停止	5.0(2)	サーバ クラスタの起動と停止のサポートが導入されました。

CHAPTER 29

Cisco DCNM-LAN データベースのメンテナンス

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）データベースのメンテナンス方法について説明します。

この章の内容は、次のとおりです。

- 「データベース メンテナンスの概要」（P.29-1）
- 「データベース メンテナンスのライセンス要件」（P.29-3）
- 「データベース メンテナンスの前提条件」（P.29-3）
- 「データベース メンテナンスの注意事項と制約事項」（P.29-3）
- 「データベース メンテナンスの実行」（P.29-4）
- 「その他の関連資料」（P.29-9）
- 「DCNM-LAN データベース メンテナンス機能の履歴」（P.29-10）

データベース メンテナンスの概要

DCNM-LAN は PostgreSQL データベースまたは Oracle データベースを使用して、管理対象デバイスからの設定情報、管理対象デバイスから収集したイベントおよび統計データ、DCNM-LAN ユーザ情報など、すべてのデータを保存します。DCNM-LAN は、データベースのメンテナンスを行うように実行できるスクリプトのほか、不要になったイベントおよび統計データを削除できる機能を備えています。

ここでは、次の内容について説明します。

- 「データの自動消去および手動消去」（P.29-1）
- 「データベースのバックアップ」（P.29-2）
- 「データベースのクリーンアップ」（P.29-2）
- 「データベースの復元」（P.29-2）

データの自動消去および手動消去

デバイスとの自動同期化機能を使用して不要なイベント データを削除し、統計データ収集機能を使用して不要な統計データを削除できます。DCNM-LAN は、両方のデータ タイプの自動消去をサポートしています。自動データ消去について次の側面を設定できます。

- 自動消去を行う曜日と時刻。
- DCNM-LAN が消去するデータを、経過日数またはデータベース エントリの最大数のどちらで判別するか。
- イベント関連データの場合、DCNM-LAN が消去するイベントをイベントの重大度で判別するか。

DCNM-LAN データベースのサイズが大きくなりすぎないように、イベントおよび統計データの自動消去を設定することを推奨します。

イベントおよび統計データは手動でも消去できます。

詳細については、次の項を参照してください。

- 「イベント データの自動消去および手動消去」（P.23-2）
- 「統計データの自動的な消去または手動での消去」（P.25-2）

データベースのバックアップ

DCNM-LAN データベース バックアップ スクリプトを使用して、DCNM データベースのバックアップ ファイルを作成できます。

DCNM-LAN データベースを定期的にバックアップすること、およびバックアップ ファイルを DCNM-LAN サーバ システム以外の保護された場所にアーカイブすることを強く推奨します。バックアップ ファイルは、組織の基準によって要求される期間保持する必要があります。

データベースのクリーンアップ

Cisco DCNM データベース クリーンアップ スクリプトを使用して、DCNM-LAN データベースをクリーンアップできます。クリーンアップにより、データベースからすべての DCNM-LAN データが削除されます。DCNM-LAN データベースを復元する前に、クリーンアップを行う必要があります。データベースをクリーンアップすると、バックアップされていないデータベース レコードはすべて消失します。

バックアップからデータを復元せずに、すべてのデータを削除し、DCNM-LAN の実装を再構築する場合にも、データベースをクリーンアップできます。

データベースの復元

Cisco DCNM データベース復元スクリプトを使用して、バックアップ ファイルから DCNM-LAN データベースを復元できます。バックアップ ファイルは、データ復元先の DCNM-LAN と同じリリースに付属している DCNM-LAN データベース バックアップ スクリプトによって作成されている必要があります。たとえば、Cisco DCNM Release 5.0(2) を実行している場合、必ず Cisco DCNM Release 5.0(2) のバックアップからデータベースの復元を行う必要があります。

また、バックアップ ファイルは、データを復元している同じデータベース タイプおよび同じリリースから作成されている必要があります。たとえば、Oracle 11g データベースにデータを復元している場合、バックアップ ファイルは Oracle 11g データベースから作成されている必要があります。

DCNM-LAN データベースを復元する前に、データベースをクリーンアップする必要があります。データベースをクリーンアップせずにデータベースを復元すると、予期しない結果になる可能性があります。

データベース メンテナンスのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM-LAN	データベース メンテナンスにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

データベース メンテナンスの前提条件

データベース メンテナンスには次の前提条件があります。

- DCNM-LAN サーバが正常にインストールされている必要があります。
- DCNM-LAN データベースをクリーンアップする場合は、DCNM-LAN サーバを停止する必要があります。
- DCNM-LAN データベースの復元には次の要件があります。
  - バックアップ ファイルを使用して復元する DCNM-LAN と厳密に同じリリースの DCNM-LAN で作成されたバックアップ ファイルを用意する必要があります。
  - データ復元先のデータベースのタイプおよびリリースが厳密に同じデータベースから作成されたバックアップ ファイルを用意する必要があります。
  - 復元するデータベースと同じオペレーティング システムで実行されている DCNM-LAN データベースから作成されたバックアップ ファイルを用意する必要があります。たとえば、Microsoft Server 2003 で実行されているデータベースから作成されたバックアップ ファイルは、Microsoft Server 2003 で実行されている他の DCNM-LAN データベースを復元する場合のみ使用できます。

データベース メンテナンスの注意事項と制約事項

データベース メンテナンスには、次の設定上の注意事項および制約事項があります。

- DCNM-LAN データベースのサイズが大きくなりすぎないように、統計データおよびイベント データの自動消去を設定することを推奨します。
- 定期的なバックアップの実行を推奨します。組織で定められた基準に従って、バックアップを実行すべき頻度を決定します。
- DCNM-LAN データベースは、同じリリースの DCNM-LAN のバックアップからのみ復元できます。たとえば、Cisco DCNM Release 5.0(2) を実行している場合、必ず Cisco DCNM Release 5.0(2) のバックアップからデータベースの復元を行う必要があります。
- DCNM-LAN データベースは、現在のデータベースとタイプおよびリリースが同じデータベースのバックアップからのみ復元できます。たとえば、現在のデータベースが Oracle 11g データベースであれば、このデータベースを復元できるのは、Oracle 11g データベースから作成されたバックアップ ファイルを使用する場合だけです。

- DCNM-LAN データベースは、復元するデータベースと同じオペレーティング システムで実行されている DCNM-LAN データベースから作成されたバックアップ ファイルからのみ復元できます。たとえば、Microsoft Server 2003 で実行されているデータベースから作成されたバックアップ ファイルは、Microsoft Server 2003 で実行されている他の DCNM-LAN データベースを復元する場合のみ使用できます。

データベース メンテナンスの実行

ここでは、次の内容について説明します。

- 「DCNM-LAN データベースのバックアップ」（P.29-4）
- 「DCNM-LAN データベースのクリーンアップ」（P.29-5）
- 「バックアップ ファイルからの DCNM-LAN データベースの復元」（P.29-7）

DCNM-LAN データベースのバックアップ

バックアップ スクリプトを使用して DCNM-LAN データベースをバックアップできます。DCNM-LAN サーバ インストーラは、サーバのインストール時にユーザが指定したデータベース ユーザ名とデータベース名を使用してバックアップ スクリプトを設定します。

手順の詳細

ステップ 1　DCNM-LAN サーバ上で、コマンド プロンプトにアクセスします。

ステップ 2　次のように **cd** コマンドを使用して、ディレクトリを Cisco DCNM インストレーション ディレクトリにある bin ディレクトリに変更します。

cd *path*

ここで、*path* は、bin ディレクトリへの相対パスまたは絶対パスです。Microsoft Windows の場合、bin ディレクトリへのデフォルト パスは、C:¥Program Files¥dcm¥dcnm¥bin です。RHEL の場合、bin ディレクトリへのデフォルト パスは /usr/local/cisco/dcm/dcnm/bin です。

ステップ 3　Cisco DCNM データベース バックアップ スクリプトを実行します。スクリプト名は、次の表に示すように、サーバ オペレーティング システムおよびデータベース タイプによって異なります。

サーバ オペレーティング システム	データベース タイプ	バックアップ スクリプト名
Microsoft Windows	PostgreSQL	backup-pgsql-dcnm-db.bat
	Oracle	backup-oracle-dcnm-db.bat
Linux	PostgreSQL	backup-pgsql-dcnm-db.sh
	Oracle	backup-oracle-dcnm-db.sh

ステップ 4　作成しているバックアップのファイル名を入力します。

ステップ 5　確認のプロンプトで、**y** を入力してバックアップを続行します。

ステップ 6　指定したとおりバックアップ ファイルが作成されたこと、ファイル サイズがゼロより大きいことを確認します。

- Linux の場合、**ls -l** コマンドを使用します。

- Microsoft Windows の場合、**dir** コマンドを使用します。

ステップ 7　安全な場所にバックアップ ファイルを保存します。ハードウェアの壊滅的な故障の可能性からデータを保護するために、バックアップ ファイルは DCNM-LAN サーバ システムから離れた安全な場所にコピーすることを推奨します。

例

次の Windows サーバの例に、デフォルト値を使用してインストールされた PostgreSQL の DCNM-LAN データベースから masterbackup.bkp というバックアップを作成する方法を示します。

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>backup-pgsql-dcnm-db.bat
 ========================================================

  Database Postgres Environment

  PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

  DCNM Database Name : "dcmdb"

  DCNM Database User Name : "dcnmuser"

 ========================================================


Please enter the filename to be used for Database Backup:masterbackup.bkp
""
"Database Schema "dcnmuser" will be backed up in filename : masterbackup.bkp"
""
Continue y/n [n] : y
.
.
.
Database backup File: woobie1
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>dir masterbackup.bkp
 Volume in drive C has no label.
 Volume Serial Number is D415-F632

 Directory of C:\Program Files\PostgreSQL\8.2\bin

06/15/2009 01:53 PM           900,129 masterbackup.bkp
               1 File(s)        900,129 bytes
               0 Dir(s)  23,960,858,624 bytes free

C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

DCNM-LAN データベースのクリーンアップ

DCNM-LAN データベース クリーンアップ スクリプトを使用して、データベースをクリーンアップできます。DCNM-LAN データベース内のデータはすべて削除されます。データベースのクリーンアップは、次のような理由により実行されます。

- DCNM-LAN データベースをバックアップから復元する場合。

- バックアップからデータを復元せずに、すべてのデータを削除し、DCNM-LAN の実装を再構築する場合。

DCNM-LAN サーバ インストーラは、サーバのインストール時にユーザが指定したデータベース ユーザ名とデータベース名を使用してクリーンアップ スクリプトを設定します。

はじめる前に

DCNM-LAN データベースをバックアップします。バックアップで保存されていないデータはすべて、データベースのクリーンアップ時に消失します。

DCNM-LAN サーバを停止します。データベース クリーンアップ処理を完了するには、先に DCNM-LAN サーバを停止しておく必要があります。詳細については、「DCNM-LAN サーバの停止」（P.28-5）を参照してください。

手順の詳細

ステップ 1　DCNM-LAN サーバ上で、コマンド プロンプトにアクセスします。

ステップ 2　DCNM-LAN サーバをまだ停止していない場合は停止します。詳細については、「DCNM-LAN サーバの停止」（P.28-5）を参照してください。

ステップ 3　次のように **cd** コマンドを使用して、ディレクトリを Cisco DCNM インストレーション ディレクトリにある bin ディレクトリに変更します。

cd *path*

ここで、*path* は、bin ディレクトリへの相対パスまたは絶対パスです。Microsoft Windows の場合、bin ディレクトリへのデフォルト パスは、C:¥Program Files¥dcm¥dcnm¥bin です。RHEL の場合、bin ディレクトリへのデフォルト パスは /usr/local/cisco/dcm/dcnm/bin です。

ステップ 4　Cisco DCNM データベース クリーンアップ スクリプトを実行します。スクリプト名は、次の表に示すように、サーバ オペレーティング システムおよびデータベース タイプによって異なります。

サーバ オペレーティング システム	データベース タイプ	クリーンアップ スクリプト
Microsoft Windows	PostgreSQL	clean-pgsql-dcnm-db.bat
	Oracle	clean-oracle-dcnm-db.bat
Linux	PostgreSQL	clean-pgsql-dcnm-db.sh
	Oracle	clean-oracle-dcnm-db.sh

ステップ 5　確認のプロンプトで、**y** を入力してデータベースのクリーンアップを続行します。

ステップ 6　DCNM-LAN データベースをバックアップから復元する場合は、「バックアップ ファイルからの DCNM-LAN データベースの復元」（P.29-7）に進みます。DCNM-LAN サーバは起動しないでください。

DCNM-LAN データベースをバックアップから復元せずに、手動で DCNM-LAN の実装を再構築する場合は、DCNM-LAN サーバを起動します。「単一の DCNM-LAN サーバの起動」（P.28-2）を参照してください。

例

次の Windows サーバの例に、デフォルト値を使用してインストールされた PostgreSQL の DCNM-LAN データベースをクリーンアップする方法を示します。

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>clean-pgsql-dcnm-db.bat

 =======================================================

  Database Postgres Environment

  PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

  DCNM Database Name : "dcmdb"

  DCNM Database User Name : "dcnmuser"

  DCNM Database SuperUser Name : "cisco"
 =======================================================



 ************************************************************************
 PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!
 ************************************************************************


DCNM database schema  "dcnmuser" will be deleted permanently...

Please Confirm y/n [n] : y
.
.
.
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

バックアップ ファイルからの DCNM-LAN データベースの復元

Cisco DCNM データベース復元スクリプトを使用して、バックアップ ファイルから DCNM-LAN データベースを復元できます。復元スクリプトは、データベースを復元する前に、データベースをクリーンアップします。

はじめる前に

DCNM-LAN データベースの復元に使用するバックアップ ファイルを探します。

データベースの復元に使用するバックアップ ファイルが、同じリリースの DCNM-LAN から作成されていることを確認します。たとえば、Cisco DCNM Release 5.0(2) データベースは、Cisco DCNM Release 5.0(2) データベースから作成されたバックアップ ファイルからだけ復元できます。

バックアップ ファイルが、現在のデータベースと同じデータベースのタイプおよびリリースから作成されていることを確認します。たとえば、Oracle 11g データベースは、Oracle 11g データベースから作成されたバックアップ ファイルからだけ復元できます。

バックアップ ファイルが、データベース復元先の DCNM-LAN サーバと同じオペレーティング システムで実行されている DCNM-LAN データベースから作成されていることを確認します。たとえば、Microsoft Server 2003 で実行されているデータベースから作成されたバックアップ ファイルは、Microsoft Server 2003 で実行されている他の DCNM-LAN データベースを復元する場合のみ使用できます。

データベースの復元中は、DCNM-LAN サーバを停止する必要があります。

手順の詳細

ステップ 1　DCNM-LAN サーバ上で、コマンド プロンプトにアクセスします。

ステップ 2　DCNM-LAN サーバをまだ停止していない場合は停止します。詳細については、「DCNM-LAN サーバの停止」（P.28-5）を参照してください。

ステップ 3　次のように **cd** コマンドを使用して、ディレクトリを Cisco DCNM インストレーション ディレクトリにある bin ディレクトリに変更します。

cd *path*

ここで、*path* は、bin ディレクトリへの相対パスまたは絶対パスです。Microsoft Windows の場合、bin ディレクトリへのデフォルト パスは、C:\Program Files\dcm\dcnm\bin です。RHEL の場合、bin ディレクトリへのデフォルト パスは /usr/local/cisco/dcm/dcnm/bin です。

ステップ 4　Cisco DCNM データベース復元スクリプトを実行します。スクリプト名は、次の表に示すように、サーバ オペレーティング システムおよびデータベース タイプによって異なります。

サーバ オペレーティング システム	データベース タイプ	復元スクリプト
Microsoft Windows	PostgreSQL	restore-pgsql-dcnm-db.bat
	Oracle	restore-oracle-dcnm-db.bat
Linux	PostgreSQL	restore-pgsql-dcnm-db.sh
	Oracle	restore-oracle-dcnm-db.sh

ステップ 5　DCNM-LAN データベースの復元に使用するバックアップ ファイルの名前を入力します。

ステップ 6　確認のプロンプトで、**y** を入力してデータベースの復元を続行します。

ステップ 7　DCNM-LAN の使用を再開するには、DCNM-LAN サーバを起動します。「単一の DCNM-LAN サーバの起動」（P.28-2）を参照してください。

例

次の Microsoft Windows サーバの例に、デフォルト値を使用してインストールされた DCNM-LAN の PostgreSQL データベースを、DCNM インストール ディレクトリの bin ディレクトリにある masterbackup.bkp というバックアップ ファイルを使用して復元する方法を示します。

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"


C:\Program Files\Cisco Systems\dcm\dcnm\bin>restore-pgsql-dcnm-db.bat
 ============================================================

  Database Postgres Environment
```

```
 PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

 DCNM Database Name : "dcmdb"

 DCNM Database User Name : "dcnmuser"

=========================================================


*******************************************************************************
PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!
*******************************************************************************



Please enter the filename to be used for Database Restore:masterbackup.bkp
""
"Database Schema "dcnmuser" will be Restore from filename : masterbackup.bkp"
""
Continue y/n [n] : y

"Cleaning the database...
.
.
.
"Done"
pg_restore: connecting to database for restore
.
.
.
Restored Database from : masterbackup.bkp
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

その他の関連資料

DCNM-LAN データベースのメンテナンスに関する追加情報については、次を参照してください。

- 「関連資料」（P.29-9）
- 「標準」（P.29-10）

関連資料

関連項目	参照先
イベント データの自動消去	第 23 章「デバイスとの自動同期化の管理」
統計データの自動消去	第 25 章「統計データ収集の管理」

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN データベース メンテナンス機能の履歴

表 29-1 は、この機能のリリースの履歴です。

表 29-1　DCNM-LAN データベース メンテナンス機能の履歴

機能名	リリース	機能情報
データベース メンテナンス スクリプト	5.0(2)	リリース 4.2(3) からの変更点はありません。

CHAPTER 30

DCNM-LAN のトラブルシューティング

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）の使用時に発生する可能性のある一般的な問題のトラブルシューティング方法について説明します。

（注） DCNM-LAN サーバのインストールに関する問題のトラブルシューティングについては、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

この章の内容は、次のとおりです。

- 「DCNM-LAN を使用するときのヒント」（P.30-1）
- 「DCNM-LAN サーバの起動に関する問題」（P.30-2）
- 「DCNM-LAN データベースに関する問題」（P.30-3）
- 「DCNM-LAN クライアントに関する問題」（P.30-6）
- 「デバイス ディスカバリまたはデバイス スタータスに関する問題」（P.30-11）
- 「デバイス管理に関する問題」（P.30-12）
- 「トポロジに関する問題」（P.30-12）
- 「デバイス OS 管理に関する問題」（P.30-13）
- 「イベント ブラウジングに関する問題」（P.30-13）

DCNM-LAN を使用するときのヒント

ここでは、次の内容について説明します。

- 「[Events] タブに表示されるイベント数がイベント ブラウザに表示されるイベント数よりも少ない」（P.30-1）
- 「イベント ブラウザの円グラフの表示が小さな数値に関して不正確である」（P.30-2）

[Events] タブに表示されるイベント数がイベント ブラウザに表示されるイベント数よりも少ない

イベント ブラウザ機能では DCNM-LAN が受信したすべてのメッセージが表示されます。これには、DCNM-LAN によってサポートされていない機能に属するメッセージも含まれます。

[Events] タブには、現在選択されている機能のステータスを反映するメッセージだけが表示されます。これは、一部の機能では、その機能に関して発生する可能性のあるメッセージのサブセットになります。

イベント ブラウザの円グラフの表示が小さな数値に関して不正確である

イベント ブラウザの円グラフでは、円全体の 5% に満たない扇形のサイズが正しく表示されないことがあります（数値は正しく表示されます）。

DCNM-LAN サーバの起動に関する問題

ここでは、次の内容について説明します。

- 「DCNM-LAN サーバを起動できない」（P.30-3）

DCNM-LAN サーバを起動できない

表 30-1 をチェックして、DCNM-LAN クライアントのダウンロードに関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-1　DCNM-LAN サーバを起動できない

現象	考えられる原因	ソリューション
DCNM-LAN サーバを起動できない。	Postgres データベースがインストールされていない。	DCNM-LAN サーバのインストールに関する問題のトラブルシューティングについては、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
	Postgres サービスが実行されていない。	Postgres サービスを起動します。 • Microsoft Windows Server では、[Start] > [All Programs] > [Postgres 8.2] > [Start Service] の順に選択します。 • RHEL では次のコマンドを使用します。 **/DCNM/db/bin/DB start**
	Postgres のユーザ クレデンシャルに誤りがある。	1. Postgres のユーザ クレデンシャルを修正します。詳細については、「pgAdmin III での DCNM-LAN データベース名とユーザ名の更新」（P.30-4）を参照してください。 2. DCNM-LAN サーバを起動します。詳細については、「DCNM-LAN サーバの起動」（P.28-1）を参照してください。
	サーバが使用するポートがすでに使用されている。	1. サーバ ログをチェックして、「Port *port-number* already in use」などのメッセージが出力されていないか確認します。サーバ ログは次のファイルです。 *Installation_directory*\jboss-4.2.2.GA\server\dcnm\log\server.log 2. 当該ポートを使用しているアプリケーションを調べて、アプリケーションを停止または再構成します。 3. DCNM-LAN サーバを再起動します。

DCNM-LAN データベースに関する問題

ここでは、次の内容について説明します。

- 「PostgreSQL データベースに関する問題」（P.30-4）
- 「Oracle データベースに関する問題」（P.30-5）

（注）　DCNM-LAN データベースに障害が発生した場合、または DCNM-LAN データベースとの通信に障害が発生した場合は、問題に対処する前に、DCNM-LAN サーバを停止するか、DCNM-LAN サーバ クラスタをシャットダウンする必要があります。DCNM-LAN サーバまたは DCNM-LAN サーバ クラスタを再起動する前に、必ず DCNM-LAN データベースおよび DCNM-LAN データベースとの通信が適切に機能していることを確認してください。

PostgreSQL データベースに関する問題

表 30-2 をチェックして、DCNM-LAN で使用する PostgreSQL データベースを管理するための pgAdmin III アプリケーションに関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-2　pgAdmin III のエラー

現象	考えられる原因	ソリューション
DCNM-LAN データベースが存在しないというエラー メッセージ表示される。	DCNM-LAN サーバ ソフトウェアをアップグレードまたは再インストールしたときに、DCNM-LAN データベース名が変更されている。	pgAdmin III アプリケーションで、「pgAdmin III での DCNM-LAN データベース名とユーザ名の更新」（P.30-4）の手順を実行します。
DCNM-LAN データベース ユーザ名のパスワード認証に失敗したというエラー メッセージが表示される。	DCNM-LAN サーバ ソフトウェアをアップグレードまたは再インストールしたときに、DCNM-LAN データベース ユーザ名が変更されている。	

pgAdmin III での DCNM-LAN データベース名とユーザ名の更新

pgAdmin III で、DCNM-LAN データベースおよびユーザ名を更新できます。

ステップ 1　pgAdmin III アプリケーションを開きます。

ステップ 2　[Object Browser] ペインの [Servers] で、[PostgreSQL Database Server 8.2] をクリックします。

右側のペインに、[Properties] タブと他のいくつかのタブが表示されます。

ステップ 3　[Properties] タブで、[Maintenance database] をダブルクリックします。

ダイアログボックスにサーバの [Properties] タブが表示されます。

ステップ 4　データベース名を変更する必要がある場合は、[Maintenance DB] フィールドをクリックし、正しい DCNM-LAN データベース名を入力します。

（注）　データベース名として、最後に DCNM-LAN サーバ ソフトウェアをアップグレードまたは再インストールしたときに指定した名前を指定する必要があります。

ステップ 5　データベース ユーザ名を変更する必要がある場合は、[Username] フィールドをクリックし、正しい DCNM-LAN データベース ユーザ名を入力します。

（注）　データベース ユーザ名としては、最後に DCNM-LAN サーバ ソフトウェアをアップグレードまたは再インストールしたときに指定したデータベース ユーザ名を指定する必要があります。

ステップ 6　[OK] をクリックします。

ステップ 7　[Object Browser] ペインで、[PostgreSQL Database Server 8.2] をダブルクリックします。

ステップ 5 でユーザ名を変更した場合、[Connect to Server] ダイアログボックスが表示されます。

ステップ 8　必要に応じて、ステップ 5 で指定したユーザ名のパスワードを入力し、[OK] をクリックします。

pgAdmin III アプリケーションは DCNM-LAN データベースに接続し、データベースとログイン ロールを表示します。

さらなる支援が必要な場合は、pgAdmin III アプリケーションの [Help] メニューか、次の URL にある pgAdmin の Web サイトを参照してください。

http://pgadmin.org/docs/1.6/index.html

Oracle データベースに関する問題

DCNM-LAN サーバに、Oracle データベースの使用に関する問題がある場合、エラー メッセージが次のファイルに出力されます。

Installation_directory\jboss-4.2.2.GA\server\dcnm\log\server.log

表 30-3 をチェックして、DCNM-LAN での Oracle データベースの使用に関する現象が生じていないか確認してください。各エラー メッセージに対し、考えられる原因を確認し、対応する解決策に従ってください。

表 30-3　DCNM-LAN server.log ファイルの Oracle データベースに関するエラー

現象	考えられる原因	ソリューション
server.log ファイルに次のエラーが出力される。 `java.sql.SQLException: ORA-01653: unable to extend table Cisco DCNMUSER.DCMRAWEVENTTABLE by 1024 in tablespace SYSTEM`	テーブルスペース SYSTEM が小さすぎる。	1. DCNM-LAN サーバを停止します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。 2. SYSTEM テーブルスペースを大きくします。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。 3. DCNM-LAN サーバを起動します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。

表 30-3　DCNM-LAN server.log ファイルの Oracle データベースに関するエラー （続き）

現象	考えられる原因	ソリューション

server.log ファイルに次のエラーが出力される。
`[org.hibernate.util.JDBCExceptionReporter] Could not create connection; - nested throwable:`
 	
`(java.sql.SQLException: Listener refused the connection with the following error: ORA-12519, TNS:no appropriate service handler found`
	使用可能なセッションとプロセスの数が適切でない。	1. DCNM-LAN サーバを停止します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。
		2. セッション数とプロセス数をそれぞれ 150 に増やします。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
		3. DCNM-LAN サーバを起動します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。

server.log ファイルに次のエラーが出力される。
`2009-04-08 15:53:47,125 ERROR [org.hibernate.util.JDBCExceptionReporter] ORA-00604: error occurred at recursive SQL level 1`
`ORA-01000: maximum open cursors exceeded`
	開いているカーソルの数が適切でない。	1. DCNM-LAN サーバを停止します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。
		2. 開いているカーソルの数を 1000 に増やします。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
		3. DCNM-LAN サーバを起動します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。

DCNM-LAN クライアントに関する問題

ここでは、次の内容について説明します。

- 「サーバから DCNM-LAN クライアントをダウンロードできない」（P.30-7）
- 「DCNM-LAN クライアントをインストールできない」（P.30-7）
- 「DCNM-LAN クライアントを起動できない」（P.30-8）
- 「DCNM-LAN クライアントにログインできない」（P.30-9）
- 「クライアントと DCNM-LAN サーバとの接続が失われる」（P.30-10）

サーバから DCNM-LAN クライアントをダウンロードできない

表 30-4 をチェックして、DCNM-LAN クライアントのダウンロードに関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-4　サーバから DCNM-LAN クライアントをダウンロードできない

現象	考えられる原因	ソリューション
サーバから DCNM-LAN クライアントをダウンロードできない。	URL または Web サーバ ポートが間違っている。	ポート番号も含め、正しい URL を使用していることを確認します。
	TCP ポートがゲートウェイ デバイスによってブロックされている。	ファイアウォール内の TCP ポートを開きます。DCNM-LAN によって使用されるポートについては、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
	サポートされていない Web ブラウザを使用している。	サポートされている Web ブラウザを使用します。サポートされている Web ブラウザの詳細については、『*Cisco DCNM Release Notes, Release 5.x*』を参照してください。

DCNM-LAN クライアントをインストールできない

表 30-4 をチェックして、DCNM-LAN クライアントのインストールに関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-5　DCNM-LAN クライアントをインストールできない

現象	考えられる原因	ソリューション
インストーラが Java バージョン 1.6.0_21 をインストールしようとして失敗する。	システムがインターネットにアクセスできない。	DCNM-LAN クライアント インストーラでは、Java バージョン 1.6.0_21 JRE をダウンロードするためにインターネット アクセスが必要です。システムでインターネットにアクセスできない場合は、別のシステムを使用して Java インストーラをダウンロードし、DCNM-LAN クライアントをインストールするシステムにコピーして Java をインストールしてから、DCNM-LAN クライアントのインストールを再開します。 Java バージョン 1.6.0_21 JRE は、Oracle Technology Network Web サイトからダウンロードできます。
	インターネットにアクセスするためにプロキシ接続が必要なネットワーク環境になっている。	ネットワーク環境で Java インストーラのダウンロードを許可させるプロキシ接続が必要な場合は、コントロール パネルからアクセスできるインターネット オプションでプロキシが設定されていることを確認します。

DCNM-LAN クライアントを起動できない

表 30-6 をチェックして、DCNM-LAN クライアントの起動に関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-6　DCNM-LAN クライアントを起動できない

現象	考えられる原因	ソリューション
DCNM-LAN クライアントを起動できない。	クライアントのインストールが壊れている。 正しくないバージョンの Java がインストールされている。	1. DCNM-LAN クライアントをアンインストールします。詳細については、「DCNM-LAN クライアントのアンインストール」（P.13-9）を参照してください。 2. DCNM-LAN クライアントを DCNM-LAN サーバからダウンロードしてインストールします。 クライアントのインストールの際、DCNM-LAN がサポートされているバージョンの Java をコンピュータにインストールするのを許可します。DCNM-LAN サーバからクライアントをダウンロードするとき、サポートされているバージョンの Java がコンピュータ上で検出されない場合、DCNM-LAN によってサポートされているバージョンの Java をインストールして良いか質問されます。 ブラウザから、Java インストーラが期限切れのクレデンシャルでデジタル署名されていることが通知される場合があります。続行するにはインストールを許可します。 詳細については、「DCNM-LAN クライアントのダウンロードおよび起動」（P.13-3）を参照してください。

DCNM-LAN クライアントにログインできない

表 30-7 をチェックして、DCNM-LAN クライアントのログインに関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-7　DCNM-LAN クライアントにログインできない

現象	考えられる原因	ソリューション
DCNM-LAN クライアントにログインできない。	パスワードを忘れた。	DCNM-LAN 管理者に、次のいずれかのスクリプトを使用してパスワードをリセットするよう依頼します。 • Microsoft Windows の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.bat を使用します（デフォルトでは、*dcnm_root_directory* は c:¥Program Files¥Cisco Systems¥dcm¥dcnm¥bin です）。 • Linux の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.sh を使用します（デフォルトでは、*dcnm_root_directory* は /usr/local/cisco です）。 パスワードをリセットするには、使用しているオペレーティング システムに適したスクリプトを実行し、リセットするユーザ ID とそのユーザ ID で使用するパスワードを入力します。 DCNM-LAN への管理アクセス権を持つユーザがいない場合は、DCNM-LAN サーバ ソフトウェアを再インストールすることにより、ローカル管理者アカウントをリセットするか、DCNM-LAN サーバ認証設定を変更できます。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
	認証サーバが、DCNM-LAN ユーザを認証するように設定されていない。	DCNM-LAN が認証サーバを使用するように設定されている場合は、DCNM-LAN で使用するように設定したすべての認証サーバで、DCNM-LAN サーバからの認証要求を受け付けるように設定されていることを確認します。DCNM-LAN をクラスタ サーバ環境に展開している場合には、すべての認証サーバが、クラスタ内の各 DCNM-LAN サーバからの要求を受け付けるように設定します。
	DCNM-LAN サーバがダウンしている。	DCNM-LAN サーバを再起動します。「単一の DCNM-LAN サーバの起動」（P.28-2）を参照してください。
	DCNM-LAN サーバに到達できない。	DCNM-LAN クライアントを実行しているコンピュータが、DCNM-LAN クライアントをリモートで使用するためのネットワーク要件を満たしていることを確認します。DCNM-LAN クライアントとサーバの間のすべてのゲートウェイ ネットワーク デバイスで、DCNM-LAN Web サーバと DCNM-LAN サーバへの接続を許可する必要があります。デフォルトでは、DCNM-LAN Web サーバはポート 8080 をリッスンし、DCNM-LAN サーバはポート 1099 をリッスンします。ただし、これらのポートは、DCNM-LAN サーバのインストール時に設定できます。いずれかのポートを変更する必要がある場合は、サーバを再インストールし、[Full Reinstall] オプションを選択します。DCNM-LAN によって使用されるポートについては、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
	サーバをインストールした後で DCNM-LAN サーバの IP アドレスが変更された。	次の手順に従います。 1. DCNM-LAN サーバの IP アドレスが静的に割り当てられていることを確認します。 2. DCNM-LAN サーバを再インストールし、[Full Reinstall] オプションを選択します。これにより、サーバの IP アドレスを指定できます。『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。 3. DCNM-LAN クライアントにログインし、DCNM-LAN サーバの新しい IP アドレスをログイン ダイアログボックスの [DCNM-LAN Server] フィールドに指定します。

表 30-7　DCNM-LAN クライアントにログインできない （続き）

現象	考えられる原因	ソリューション
DCNM-LAN クライアントにログインできない（続き）。	ログインで正しくない DCNM-LAN サーバ ポート番号を使用した。	DCNM-LAN クライアントのログイン ウィンドウで [More] をクリックし、[Port] フィールドで DCNM-LAN サーバが使用するポート番号を変更します。「DCNM-LAN クライアントの再起動」（P.13-7）を参照してください。 DCNM-LAN サーバがリッスンするポートを変更する場合は、DCNM-LAN サーバを再インストールし、[Full Reinstall] オプションを選択します。これにより、DCNM-LAN サーバ ポートを指定できます。『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。
DCNM-LAN クライアントにログインしようとすると、次のエラー メッセージが表示される。「Can not resolve DCNM-LAN server *hostname* via DNS. Make sure that DCNM-LAN server has a valid DNS entry.」	ログイン時にあるホスト名を使用して DCNM-LAN サーバを指定したが、その DCNM-LAN サーバのエントリが DNS に存在しない。	自社ネットワーク上の DNS に、DCNM-LAN サーバ ホスト名のエントリが存在することを確認してください。

クライアントと DCNM-LAN サーバとの接続が失われる

表 30-8 をチェックして、DCNM-LAN クライアントとサーバとの接続性の喪失に関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-8　クライアントと DCNM-LAN サーバとの接続が失われる

現象	考えられる原因	ソリューション
• クライアントとサーバとの接続が失われる。 • DCNM-LAN クライアント ウィンドウがピンク色になっている。	クライアントに障害がある。	DCNM-LAN クライアントを再起動します。
	DCNM-LAN サーバがダウンしている。	DCNM-LAN サーバを再起動します。第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。
	DCNM-LAN サーバに到達できない。	ネットワークを調査して、DCNM-LAN クライアントをリモートで使用するためのネットワーク要件が満たされているかどうか確認します。DCNM-LAN によって使用されるポートについては、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

デバイス ディスカバリまたはデバイス スタータスに関する問題

表 30-9 をチェックして、デバイス ディスカバリまたはデバイス ステータスの問題に関する現象が生じていないか確認します。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-9　デバイス ディスカバリまたはデバイス スタータスに関する問題

現象	考えられる原因	ソリューション
• デバイス ディスカバリ タスクでエラーが発生する。 • デバイス ステータスが「Unmanaged（管理対象外）」または「Unreachable（到達不能）」になる。	間違ったデバイス クレデンシャルが提出された。	ユーザ名とパスワードを再入力し、デバイスを再検出します。 シード デバイスの CDP ネイバーを検出する場合は、提出するクレデンシャルが検出対象のすべてのデバイスで有効であることを確認してください。
	SSH サーバがデバイス上でディセーブルになっている。	デバイス上の SSH サーバを再度イネーブル化して、デバイスを再検出します。
	デバイスがサポートしている SSH セッションの最大数に達した。	デバイス上のユーザ セッション数を確認します。少なくとも 1 つの接続を解放してから、デバイスを再検出します。
	CDP が、デバイス上、または DCNM-LAN サーバが接続するデバイス インターフェイス上でディセーブルになっている。	CDP が、デバイスでグローバルにイネーブルになっており、DCNM-LAN サーバが接続する特定のインターフェイス上でもイネーブルになっていることを確認します。
	DCNM-LAN サーバが接続するデバイス インターフェイスがシャットダウンされている。	DCNM-LAN サーバが接続するデバイス インターフェイスがアップ状態になっていることを確認します。
	ディスカバリが完了する前にデバイスが再起動またはシャットダウンされた。	デバイスが動作していることを確認し、デバイスを再検出します。
	DCNM-LAN サーバがデバイスに到達できない。	デバイス管理のためのネットワーク要件が満たされていることを確認します。「Cisco NX-OS デバイスのディスカバリ準備状態の確認」（P.16-7）を参照してください。
	システム ログ メッセージに矛盾がある。	clear logging logfile コマンドを使用してデバイスのシステム ログをクリアし、手動によるデバイスの検出を試みます。
	アカウンティング ログ メッセージに矛盾がある。	clear accounting log コマンドを使用してデバイスのアカウンティング ログ メッセージをクリアし、手動によるデバイスの検出を試みます。 **（注）** カスタム VDC を使用する場合は、デフォルトの VDC からのみ、アカウンティング ログ メッセージのクリアを行います。

デバイス管理に関する問題

表 30-6 をチェックして、デバイス管理に関する現象が生じていないか確認します。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-10　デバイス管理に関する問題

現象	考えられる原因	ソリューション
Cisco NX-OS デバイスでログ ファイルやアカウンティング ログをクリアしても、DCNM-LAN によってデバイスが自動的に再検出されない。	デバイスが、アカウンティング ログまたはログ ファイルのクリアに関するシステム メッセージを生成しない。この問題は、デバイスが、Cisco SAN-OS Release 3.1 以前のリリースが動作する Cisco MDS 9000 ファミリ マルチレイヤ スイッチである場合に特に発生する可能性が高くなります。	デバイスをもう一度検出します。詳細については、「デバイスの検出」（P.17-4）を参照してください。
DCNM-LAN クライアントに古いデバイス設定情報が表示される。	DCNM-LAN サーバがダウンした。	次のいずれかの操作を実行できます。 • デバイスをもう一度検出します。詳細については、「デバイスの検出」（P.17-4）を参照してください。 • DCNM-LAN サーバをクリーンなデータベースで再起動します。サーバが長期間にわたってダウンしていた場合は、この解決策を推奨します。 1. 「DCNM-LAN サーバの停止」（P.28-5） 2. 「DCNM-LAN データベースのクリーンアップ」（P.29-5） 3. 「DCNM-LAN サーバの起動」（P.28-1）

トポロジに関する問題

表 30-11 をチェックして、トポロジ機能の使用に関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-11　トポロジに関する問題

現象	考えられる原因	ソリューション
• Cisco MDS 9000 ファミリ マルチレイヤ スイッチ間のリンクが、そのリンクがダウンした後も引き続き表示される。	デバイスがギガビット イーサネット ポートまたはファスト イーサネット ポートによって接続され、Cisco SAN-OS Release 3.1 以前のリリースが動作している。	トポロジで誤ってリンクされていると表示されるデバイスを再検出します。

デバイス OS 管理に関する問題

表 30-12 をチェックして、デバイス OS 管理機能に関する現象が生じていないか確認してください。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-12　デバイス OS 管理に関する問題

現象	考えられる原因	ソリューション
• ソフトウェア インストール ジョブで、ファイル サーバとデバイスの間のソフトウェア イメージ ファイルの転送に時間がかかる。	ファイル サーバとデバイスの間の接続が低速である。	ソフトウェア インストール ジョブに含まれているデバイスと同じ LAN 上のファイル サーバを使用します。 使用可能なすべてのファイル サーバでソフトウェア イメージ ファイルの転送が遅い場合は、ソフトウェア インストール ジョブを作成する前に、ジョブに含めるデバイスに手動でファイルをコピーし、ファイル サーバではなく手動でコピーしたファイルを使用するようにジョブを設定します。 ソフトウェア インストール ジョブの設定については、『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

イベント ブラウジングに関する問題

表 30-13 をチェックして、イベント ブラウジングに関する現象が生じていないか確認します。問題を表す現象ごとに、考えられる原因として該当するものを特定し、対応する解決方法に従います。

表 30-13　イベント ブラウジングに関する問題

現象	考えられる原因	ソリューション
• デバイスのコマンドラインで使用可能なイベントが DCNM-LAN クライアントに表示されない。 • イベント ブラウザまたは [Events] タブに表示されるイベントの数が少なすぎる。	管理対象デバイスのログ レベルが正しく設定されていない。	管理対象デバイスのログ レベルの設定を確認します。「Cisco NX-OS システム メッセージのロギング要件」（P.16-3）を参照してください。
	DCNM-LAN クライアントが取得対象期間の古いイベントを取得していない。	DCNM-LAN クライアントのプリファレンスでイベント関連設定を確認します。詳細については、「サーバから取得するイベントの最大経過時間の設定」（P.14-17）を参照してください。

表 30-13　イベント ブラウジングに関する問題

現象	考えられる原因	ソリューション
イベント ブラウザまたは [Events] タブに表示されるイベントの数が多すぎる。	特定の管理対象デバイスで問題が発生し、多数のシステム ログ メッセージが生成されている。	問題が解決するまで当該デバイスを一時的に管理対象外にします。詳細については、「デバイスの非管理対象化」（P.17-5）を参照してください。
	管理対象デバイスのログ レベルが正しく設定されていない。	管理対象デバイスのログ レベルの設定を確認します。「Cisco NX-OS システム メッセージのロギング要件」（P.16-3）を参照してください。
イベント ブラウザには表示されるイベントが、特定の機能の [Events] タブに表示されない。	設計により、[Events] タブには現在選択されている機能に該当するメッセージだけが表示されます。このため、その機能に関して発生する可能性のあるメッセージのサブセットしか表示されないことがあります。詳細については、「[Events] タブに表示されるイベント数がイベント ブラウザに表示されるイベント数よりも少ない」（P.30-1）を参照してください。	イベント ブラウザを使用して、DCNM-LAN が受信したステータス関連のシステム メッセージを確認します。詳細については、『*System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

PART 4

付録

APPENDIX A

Cisco SAN-OS Release 3.2(1) 以前のリリースでの Fabric Manager の起動

この付録では、Cisco SAN-OS 3.2(1) 以前のリリースで Fabric Manager Client を起動する方法を説明します。

この付録の内容は、次のとおりです。

- 「Cisco SAN-OS Release 3.1(1) ～ 3.2(1) のシード スイッチの設定」（P.A-1）
- 「Cisco SAN-OS Release 3.1(1) 以前のリリースのシード スイッチの設定」（P.A-3）

Cisco SAN-OS Release 3.1(1) ～ 3.2(1) のシード スイッチの設定

（注） Cisco SAN-OS Release 3.1(1) 以降、Fabric Manager Client のログイン手順が変更されました。Cisco SAN-OS 3.1(1) 以前の Cisco SAN-OS を実行している場合は、「Cisco SAN-OS Release 3.1(1) 以前のリリースのシード スイッチの設定」（P.A-3）のログイン手順に従ってください。

Cisco SAN-OS Release 3.1(1) ～ Release 3.2(1) では、ファブリックを検出する前あるいはファブリックに接続する前に Fabric Manage Server にログインする必要があります。ファブリックには異なるユーザ クレデンシャルを設定できます。Web Server のスイッチごとに異なる SNMP（簡易ネットワーク管理プロトコル）コミュニティを指定できます。

（注） 初回ログイン時のデフォルトのユーザ名は **admin**、デフォルトのパスワードは **password** です。この情報はデータベースに保存されています。Fabric Manager Server と Web Server は同じユーザ クレデンシャル データベースを使用します。

Fabric Manager Server にログインしてファブリックに接続する手順は次のとおりです。

ステップ 1 ワークステーションの [Fabric Manager Client] アイコンをダブルクリックします。

[Fabric Manager Server Login] ダイアログボックスが表示されます。

ステップ 2 FM Server に、Fabric Manager Server がインストールされたマシンの IP アドレスを設定します。Fabric Manager Server をローカル ワークステーションにインストールした場合は、**localhost** を設定します。

パスワードを忘れた場合は、次のいずれかのスクリプトを実行します。

- **bin\webUserAdd.bat admin password** を実行すると、データベースにユーザ名とパスワードが追加されます。
- **bin\DBReset.bat** を実行すると、データベースを初期状態に戻して検出したファブリックを削除します。

どちらのスクリプトも UNIX の .sh ファイルとして保存されています。

ステップ 3　Fabric Manager Server のユーザ名とパスワードを入力します。

ステップ 4　Fabric Manager Client が TCP ベース プロキシ サーバを介して Fabric Manager Server と通信するように設定する場合は、[Use SNMP Proxy] チェックボックスをオンにします。

ステップ 5　[Login] をクリックします。Fabric Manager Server に正しくログインしたら、シード スイッチを設定してアクセス権があるファブリックを開きます。

[Discover New Fabric] ダイアログボックスが表示されます。

ステップ 6　Fabric Manager で使用する Cisco MDS 9000 ファミリ スイッチにファブリック シード スイッチを設定します。

ステップ 7　スイッチのユーザ名とパスワードを入力します。

ステップ 8　ログイン時には [Auth-Privacy] オプションで [MD5]（デフォルト）を選択します。

（注）　通常は [Accelerate Discovery] チェック ボックスはオンのままです。スイッチ IP アドレスを変更した場合にだけ、チェック ボックスをオフにします。このチェック ボックスをオフにして Fabric Manager で SAN ID を使用するとエラーが発生します。

ステップ 9　[Discover] をクリックします。

[Open Fabric] ダイアログボックスが表示されます。

ステップ 10　[Select] カラムで接続先ファブリックの隣にあるチェックボックスをオンにします。または [Discover] ボタンをクリックして新しいファブリックを追加します。

（注）　Cisco SAN-OS Release 3.1(1) 以降では、複数のファブリックに接続するにはライセンスが必要です。ライセンスがないファブリックに接続しようとすると、エラー メッセージが表示されます。

（注）　Cisco SAN-OS Release 3.1(2b) 以降、ライセンスには、永久ライセンス、評価ライセンス、ライセンスなし（すべての評価ライセンスが期限切れ）があります。

ステップ 11　[Open] をクリックして、ファブリックに接続します。

Cisco SAN-OS Release 3.1(1) 以前のリリースのシード スイッチの設定

（注）　Cisco SAN-OS Release 3.1(1) 以降、Fabric Manager Client のログイン手順が変更されました。Cisco SAN-OS Release 3.1(1) ～ 3.2(1) を実行している場合、「Cisco SAN-OS Release 3.1(1) ～ 3.2(1) のシード スイッチの設定」（P.A-1）のログイン手順を実行します。

Fabric Manager を実行する場合は、Fabric Manager のスイッチを選択してファブリックを検出します。Cisco SAN-OS Release 3.1(1) 以前のリリースでは、接続するファブリックごとに同じユーザ名とパスワードを使用し、Fabric Manager を使用する MDS 9000 ファミリ スイッチに直接ログインします。

Cisco SAN-OS Release 3.1(1) 以前の Cisco SAN-O を実行してシード スイッチを設定する手順は次のとおりです。

ステップ 1　ワークステーションの [Fabric Manager Client] アイコンをダブルクリックします。

[Fabric Manager Login] ダイアログボックスが表示されます。

ステップ 2　このダイアログボックスのオプション設定が必要な場合は、[Options] ボタンをクリックします。

ステップ 3　FM Server に、Fabric Manager Server がインストールされたマシンの IP アドレスを設定します。Fabric Manager Server をローカル ワークステーションにインストールした場合は、**localhost** を設定します。

ステップ 4　Fabric Manager で使用する MDS 9000 ファミリ スイッチにファブリック シード スイッチを設定します。

ステップ 5　スイッチのユーザ名とパスワードを入力します。

ステップ 6　Fabric Manager Client が TCP ベース プロキシ サーバを介して Fabric Manager Server と通信するように設定する場合は、[Use SNMP Proxy] チェックボックスをオンにします。

（注）　通常は [Accelerate Discovery] チェック ボックスはオンのままです。スイッチ IP アドレスを変更した場合にだけ、チェック ボックスをオフにします。このチェック ボックスをオフにして Fabric Manager で非同期 SAN ID を使用するとエラーが発生します。

ステップ 7　[Open] をクリックして、ファブリックに接続します。

APPENDIX B

Cisco Fabric Manager でサポートされない機能のリスト

ここでは、Cisco Fabric Manager または Device Manager によってサポートされない機能がリストにまとめられています。機能はサポートされている場合に記載箇所となる章の順に並べられています。（表 B-1 を参照）。

表 B-1　Cisco Fabric Manager または Device Manage でサポートされない機能

パート	章 / カテゴリ	手順
2 Cisco MDS NX-OS のインストールとスイッチ管理	ライセンスの入手とインストール	ライセンス ファイルのバックアップ スイッチ間のライセンスの移動
	初期設定	スイッチの起動（初期設定） コンソール設定の変更 COM1 およびモデム設定の変更 夏時間の調整 初期化ストリングの設定 基本的なスイッチ設定 端末の設定 ファイル システム コマンド ファイル内容の表示
	ソフトウェア イメージ	デュアル スーパーバイザ スイッチの手動アップグレード 破損したブートフラッシュの復旧

表 B-1　Cisco Fabric Manager または Device Manage でサポートされない機能 （続き）

パート	章 / カテゴリ	手順
	設定ファイルの取り扱い	外部コンパクト フラッシュのフォーマット
		ファイルの圧縮と解凍
		ファイルの最終行の表示
		スクリプトで指定されたコマンドの実行
		遅延時間の設定
		設定ファイルの表示
		スタートアップ コンフィギュレーション ファイルのロック解除
		リモート ファイル システムへのアクセス
	ハイ アベイラビリティの設定	スタンバイ スーパーバイザへのイメージのコピー
	システム ハードウェアの管理	クロック モジュール
	モジュールの管理	モジュールへの接続
		モジュール設定の保存
		モジュール設定の消去
		EPLD 設定
		SSI ブート イメージの設定
		SSM の管理
3 スイッチ設定	インターフェイスの設定	ALPA キャッシュ コンテンツの表示
		ALPA キャッシュの消去
	タスクのスケジューリング	スケジュール設定
4 ファブリック設定	VSAN 間ルーティングの設定	VSAN 間ルーティング（IVR）の FICON サポート
		IVR サービス グループ
6 IP サービス	FCIP の設定	ARP キャッシュの表示と削除
	SAN Extension Tuner の設定	チューナ設定
	IP ストレージの設定	IPS モジュールのコア ダンプ
8 ネットワークとスイッチのモニタリング	SPAN を使用したネットワーク トラフィックのモニタリング	リモート SPAN

表 B-1　Cisco Fabric Manager または Device Manage でサポートされない機能 （続き）

パート	章 / カテゴリ	手順
10 トラブルシューティング	ファブリックのトラブルシューティング	ループ モニタリング CIM の設定 FC タイマー用 CFS ローカル テキスト ベース キャプチャ FC Analyzer フレームのローカル キャプチャ キャプチャした FC Analyzer フレームをリモート IP アドレスに送信する 設定された FC Analyzer 情報の消去 リモート キャプチャに設定されたホスト リストの表示 ファブリック アナライザのディスプレイ フィルタの使用
	システム プロセスおよびログのモニタ	最後のコアをフラッシュに保存する カーネル コアのダンプ システム ヘルスの開始 ループバック テストの設定頻度 ハードウェア障害時の処理 特定モジュールのテスト 前回のエラー レポートのクリア オンライン ヘルス管理システム • OHMS のイネーブル化とディセーブル化 • ハードウェア障害時の処理のイネーブル化とディセーブル化 • オンボード障害ロギングの設定 • 前回のエラー レポートのクリア • 特定モジュールのテストの実行 • 自動ループバック テストの設定 • SERDES ループバック テストの実行

APPENDIX C

インターフェイスの非動作原因コード

インターフェイスの管理ステートが Up、動作ステートが Down の場合、原因コードは非動作原因コードによって異なります。表 C-1 に、非動作の原因コードの説明を示します。

表 C-1　　非動作ステートの原因コード

原因コード	説明	適用可能なモード
Link failure or not connected	物理層リンクが正常に動作していません。	すべて
SFP not present	小型フォーム ファクタ（SFP）ハードウェアが接続されていません。	
Initializing	物理層リンクが正常に動作しており、プロトコル初期化が進行中です。	
Reconfigure fabric in progress	ファブリックが現在再設定されています。	
Offline	Cisco MDS SAN-OS は指定された R_A_TOV 時間だけ待機してから、初期化を再試行します。	
Inactive	インターフェイス VSAN が削除されているか、suspended ステートにあります。 インターフェイスを正常に動作させるには、設定されたアクティブな VSAN にポートを割り当てます。	
Hardware failure	ハードウェア障害が検出されました。	
Error disabled	エラー条件は、管理上の注意を必要とします。さまざまな理由でインターフェイスがエラーディセーブルになることがあります。次に例を示します。 • 設定障害。 • 互換性のない BB_credit 設定。 インターフェイスを動作させるには、最初にこのステートの原因となるエラー条件を修正してから、インターフェイスを管理上のシャット ダウン状態またはイネーブル状態にします。	

表 C-1　非動作ステートの原因コード （続き）

原因コード	説明	適用可能なモード
Isolation due to ELP failure	ポートのネゴシエーションに失敗しました。	E ポートと TE ポートのみ
Isolation due to ESC failure	ポートのネゴシエーションに失敗しました。	
Isolation due to domain overlap	Fibre Channel Domain（fcdomain）のオーバーラップ。	
Isolation due to domain ID assignment failure	割り当てられたドメイン ID が無効です。	
Isolation due to other side E port isolated	リンクのもう一方の端の E ポートが分離しています。	
Isolation due to invalid fabric reconfiguration	ファブリックの再設定によりポートが分離されました。	
Isolation due to domain manager disabled	fcdomain 機能がディセーブルです。	
Isolation due to zone merge failure	ゾーン結合に失敗しました。	
Isolation due to VSAN mismatch	ISL の両端の VSAN が異なります。	
Nonparticipating	FL ポートがループ操作に参加できません。1 つのループ内に複数の FL ポートが存在する場合に発生します。この場合、FL ポート 1 つを除くすべてが自動的に非参加モードになります。	FL ポートおよび TL ポートだけ
PortChannel administratively down	PortChannel に所属するインターフェイスがダウンの状態です。	PortChannel インターフェイスだけ
Suspended due to incompatible speed	PortChannel に所属するインターフェイスに互換性のない速度が存在します。	
Suspended due to incompatible mode	PortChannel に所属するインターフェイスに互換性のないモードが存在します。	
Suspended due to incompatible remote switch WWN	不適切な接続が検出されました。PortChannel のすべてのインターフェイスが同じスイッチ ペアに接続されている必要があります。	

APPENDIX D

Cisco FabricWare の管理

MDS 9020 スイッチ上で実行される Cisco FabricWare ソフトウェアによってファイバ チャネル スイッチング サービスのパフォーマンスを最大限まで向上することができます。Cisco FabricWare にはゾーン分割、高度なセキュリティ、非中断ソフトウェア アップグレード、診断、Cisco IOS に類似した構文を備えた CLI、およびアプリケーションを管理する標準インターフェイスなどのネットワーキング機能が備えられています。

この付録の内容は、次のとおりです。

- 「ファイバ チャネル サポート」（P.D-1）
- 「ゾーン設定」（P.D-2）
- 「セキュリティ」（P.D-2）
- 「イベント」（P.D-2）
- 「Fabric Manager を使用した Cisco FabricWare メッセージ送信」（P.D-3）

ファイバ チャネル サポート

Cisco FabricWare では、最大 4-Gbps の帯域幅に対応した自動設定ファイバ チャネル ポートがサポートされます。Cisco FabricWare では次のポート タイプがサポートされます。

- E
- F
- FL
- Fx
- Auto

Cisco FabricWare では、ファイバ チャネル ファブリックで使用される標準パス選択プロトコルとして Fabric Shortest Path First（FSPF）がサポートされます。FSPF 機能は、どのファイバ チャネル スイッチでも、デフォルトでイネーブルになっています。特殊な考慮事項を必要とする設定を除き、FSPF サービスを設定する必要はありません。FSPF はファブリック内の任意の 2 つのスイッチ間の最適パスを自動的に計算します。

ゾーン設定

ゾーン分割により、ストレージ デバイス間またはユーザ グループ間のアクセス コントロールの設定が可能になります。ファブリックで管理者権限を持つユーザは、ゾーンを作成してネットワーク セキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。Cisco FabricWare では QoS、ブロードキャスト、LUN、または読み取り専用ゾーンはサポートされません。

Fabric Manager ゾーン設定ツールを使用して Cisco FabricWare が実行されているスイッチのゾーン セット、ゾーン、およびゾーン メンバシップを管理できます。Cisco FabricWare では pWWN 別にゾーン メンバシップをサポートしています。『*Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide*』を参照してください。

セキュリティ

Cisco FabricWare では次のセキュリティ機能がサポートされます。

- RADIUS
- SSH
- ユーザ ベース ロール
- IP アクセス コントロール リスト

Cisco FabricWare では、リモート AAA サーバとの通信に RADIUS プロトコルを使用できます。RADIUS はネットワークへの不正なアクセスを防ぐ分散型クライアント/サーバ プロトコルです。Cisco の実装では、RADIUS クライアントは Cisco MDS 9000 ファミリ スイッチで実行され、ユーザ認証およびネットワーク サービス アクセス情報がすべて含まれる RADIUS 中央サーバに認証要求が送信されます。

CLI にはコンソール（シリアル接続）、Telnet、またはセキュア シェル（SSH）を使用してアクセスできます。管理パス（コンソールまたは Telnet および SSH）にはそれぞれ [loca]、[remote（RADIUS）]、または [none] から 1 つ以上のセキュリティ プロトコルを設定できます。

このアクセス方法を使用すると、認証されたユーザがスイッチ アクセス時に付与されるロールを設定できます。Cisco FabricWare では、ネットワーク管理者とネットワーク オペレータの 2 種類の固定ロールがサポートされます。

IP アクセス リスト（IP-ACL）によって IP 経由の管理トラフィックが制御されます。これは、スイッチに許可または拒否されるトラフィック タイプを管理することで実現されます。IP-ACL は mgmt0 ポートでだけ設定できます。

Fabric Manager Server では、Cisco FabricWare との通信に SNMPv1 および SNMPv2 を使用します。

イベント

Cisco FabricWare スイッチのファブリックおよびスイッチのステータスを Syslog サーバまたは SNMP トラップ レシーバ経由で監視できます。

Syslog（システム メッセージ ロギング ソフトウェア）によってメッセージがログ ファイルに保存されるか、メッセージが他のデバイスにダイレクトされます。この機能には次の特徴があります。

- モニタリングおよびトラブルシューティングに使用するロギング情報を提供
- 取得したロギング情報のタイプが選択可能

- 取得したロギング情報を転送する宛先サーバが選択可能

デフォルトでは、標準的かつ重要なシステム メッセージがログ ファイルに記録され、システム コンソールに送信されます。ファシリティおよび重大度に基づいて保存するシステム メッセージを指定できます。ロギングされたシステム メッセージには CLI を使用してアクセスするか、適切に設定されたシステム メッセージ ロギング サーバに保存することができます。

Cisco MDS 9020 スイッチは特定のイベントが発生すると CLI を使用して SNMP マネージャに通知を送信するように設定できます。通知はトラップとして送信できます。

Fabric Manager を使用した Cisco FabricWare メッセージ送信

Fabric Manager では、Cisco FabricWare 上で実行されているスイッチをサポートします。

表 D-1 にサポートされている機能と機能に関する詳細が記載された資料を示します。

表 D-1　Fabric Manager の FabricWare 機能

機能	FabricWare の機能	ガイド
ゾーン	ゾーン設定 pWWN 別ゾーン メンバシップ Cisco FabricWare では QoS、ブロードキャスト、LUN、または読み取り専用ゾーンはサポートされません。	『*Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide*』を参照してください。
インターフェイス	1/2/4 ファイバ チャネル自動ネゴシエーション ポート	『*Cisco MDS 9000 Family Fabric Manager Interfaces Configuration Guide*』を参照してください。
SNMP	SNMPv1 および SNMPv2c	『*Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide*』を参照してください。
ソフトウェア イメージ	自動アップグレード 手動アップグレード	『*Cisco MDS 9000 Family Fabric Manager System Management Configuration Guide*』を参照してください。
FLOGI、ネーム サーバ、FDMI、および RSCN	FLOGI の詳細の表示 ネーム サーバ プロキシの登録 FDMI の表示 RSCN 統計情報	『*Cisco MDS 9020 Switch Configuration Guide and Command Reference*』を参照してください。
セキュリティ	RADIUS の設定 サーバ グループの設定 ロールベース認証の設定 ユーザ アカウントの設定 SSH サービスの設定	『*Cisco MDS 9000 Family Fabric Manager Security Configuration Guide*』を参照してください。

表 D-1　Fabric Manager の FabricWare 機能 （続き）

機能	FabricWare の機能	ガイド
ファイバ チャネル ルーティング	FSPF グローバル設定 FSPF インターフェイス設定	『*Cisco MDS 9020 Switch Configuration Guide and Command Reference*』を参照してください。
IP サービス	mgmt0 の IP アクセス コントロール リスト	『*Cisco MDS 9000 Family Fabric Manager Security Configuration Guide*』を参照してください。
システム メッセージ	システム メッセージ ロギング設定	『*Cisco MDS 9000 Family Fabric Manager Fundamentals Configuration Guide*』を参照してください。
詳細な設定	FC タイマー	『*Cisco MDS 9000 Family Fabric Manager Fabric Configuration Guide*』を参照してください。

INDEX

A

adminDown ツールチップ 11-14
Admin タブ
　説明 2-30
ALPA キャッシュ
　クリア B-2
　内容の表示 B-2
ARP キャッシュ
　クリア B-2
　表示 B-2

B

BB_credit
　理由コード C-1
bitErrRTThresExceeded ツールチップ 11-14
bootflash:
　スペース要件 10-6
　破損からの回復 B-1
　ファイル システム 10-4
Buffer-to-Buffer credit。「BB_credit」を参照
bundleMisCfg ツールチップ 11-14

C

CA
　DCNM-SAN Web サービス 2-5
channelAdminDown ツールチップ 11-14
channelConfigurationInProgress ツールチップ 11-14
channelOperSuspended ツールチップ 11-14
CIM
　設定 B-3
Cisco DCNM-LAN クライアント
　Java 13-2
　インストールの前提条件 13-2
　オペレーティング システム 13-2
　クライアントのアンインストール 13-9
　クライアントの再インストール 13-9
　ダウンロード 13-3
　パスワード、デフォルト 13-3
　ライセンス対象機能 13-2
Cisco DCNM-LAN サーバ
　起動 28-2
　停止 28-5
　ライセンスからのデバイスの削除 18-3
　ライセンスへのデバイスの追加 18-3
Cisco DCNM エンタープライズ LAN ライセンス
　ライセンスからのデバイスの削除 18-3
　ライセンスへのデバイスの追加 18-3
Cisco DCNM ライセンス
　「Cisco DCNM エンタープライズ LAN ライセンス」を参照
Cisco MDS SAN-OS
　ソフトウェア イメージ 10-1
Cisco NX-OS
　DCNM-LAN
　　ロギング要件 16-3
Cisco Traffic Analyzer
　Performance Manager と併用するための設定 9-9
CLI
　アクセス D-2
　ファイアウォール 4-2
COM1 ポート
　設定 B-1
CompactFlash

slot0: 10-4
Custom タブ
説明 2-24

D

DCNM-SAN
corrupted jar file エラー 11-23
FAQ 11-1
FCIP 11-20
[Information] ペインが見つからない 11-9
ISL 統計情報 9-5
アップグレード 11-4
アップグレードできない 11-5
インストール エラー 11-7
エラー回復 11-7
起動のトラブルシューティング 11-3
サービスがディセーブルと表示される 11-7
ソフトウェアの混在環境 11-23
ダウングレード 11-4
デバイスの検索 11-24
認証 4-1
ネットワークの検出 5-30
複数の NIC での実行 11-21
プリファレンスの設定 5-28
分離可能なテーブル 5-19
マップ変更に関する問題 11-8
ログイン エラー リカバリ 11-6
DCNM-SAN Web サーバ
RADIUS 認証の設定 4-4
TACACS+ 認証の設定 4-5
認証 4-4
DCNM-SAN Web サービス
SSL との併用 2-5
TCP ポート 2-5
印刷 2-5
起動 2-3
コミュニティの設定 2-35
説明 2-1
ナビゲート 2-4
パフォーマンス データのエクスポート 2-5
ユーザの設定 2-38
DCNM-SAN クライアント
[Information] ペイン 5-18
ウィザード 5-32
拡張モード 5-2
ステータス バー 5-24
説明 5-1
ツールバー アイコン（表） 5-12
トラブルシューティング ツール 5-33
フィルタリング 5-15
物理属性の表示 5-15
プリファレンスの設定 5-28
メイン メニュー 5-8
DCNM-SAN サーバ
Red Hat Linux サポート 3-1
Solaris サポート 3-1
Windows サポート 3-1
インストール 3-3
インストールの概要 3-2
管理タスクの実行 2-30
機能 3-1
設定タスクの実行 2-30
設定の修正 3-8
説明 3-1
全ファブリックの再検出 3-9
ディスク容量要件 3-1
データベースが起動しない 11-10
認証 4-2
パスワード 3-9
ファブリックの継続的なモニタリング 3-6
ファブリックの検出 4-3
プロパティ ファイル 3-7
ポーリング時間 3-9
ユーザ名 3-9
ローカル ホスト エラー メッセージ 11-20
ログの表示 2-36
DCNM-SAN 認証

Web サーバ サポート 4-4
検出のベスト プラクティス 4-3
説明 4-1
deniedDueToPortBinding ツールチップ 11-15
Device Manager
FAQ 11-1
アイコン 6-5
アップグレード 11-4
アップグレードできない 11-5
色の定義 6-6
インストール エラー 11-7
インターフェイスの使用法（図） 6-3
コンテキスト メニュー 6-7
スイッチ モジュールの表示 6-7
スーパーバイザ モジュールの表示 6-7
説明 6-1
ダウングレード 11-4
タブ 6-6
ディスク イメージが表示されない 11-8
トランキング 6-7
プリファレンス 6-9
プリファレンスの設定 6-9
ポート ステータスの表示 6-6
ポートチャネル 6-7
ポートの管理 6-7
ラベルの定義 6-6
ログイン エラー リカバリ 11-6
DirectX
インストール 11-7
domainAddrAssignFailureIsolation ツールチップ 11-15
domainInvalidRCFReceived ツールチップ 11-15
domainManagerDisabled ツールチップ 11-15
domainMaxReTxFailure ツールチップ 11-15
domainOtherSideEportIsolation ツールチップ 11-15
domainOverlapIsolation ツールチップ 11-15
DPVM
ウィザード 5-33
D_S_TOV
設定時のエラー 11-8

E

E_D_TOV
設定時のエラー 11-8
elpFailureClassFParamErr ツールチップ 11-15
elpFailureClassNParamErr ツールチップ 11-15
elpFailureInvalidFlowCTLParam ツールチップ 11-15
elpFailureInvalidPayloadSize ツールチップ 11-15
elpFailureInvalidPortName ツールチップ 11-15
elpFailureInvalidTxBBCredit ツールチップ 11-15
elpFailureIsolation ツールチップ 11-15
elpFailureLoopbackDetected ツールチップ 11-15
elpFailureRatovEdtovMismatch ツールチップ 11-15
elpFailureRevMismatch ツールチップ 11-15
elpFailureUnknownFlowCTLCode ツールチップ 11-15
ELP 障害
理由コード C-2
EPLD イメージ
設定 B-2
ePortProhibited ツールチップ 11-15
eppFailure ツールチップ 11-15
errorDisabled ツールチップ 11-16
escFailureIsolation ツールチップ 11-16
ESC 障害
理由コード C-2
[Events] タブ
DCNM-LAN
イベント最大経過時間の設定 14-17
Exchange Link Parameter 障害。「ELP 障害」を参照
E ポート
分離 C-2

F

fabricBindingDBMismatch ツールチップ 11-16
fabricBindingDomainInvalid ツールチップ 11-16
fabricBindingNoRspFromPeer ツールチップ 11-16
fabricBindingSWWNNotFound ツールチップ 11-16
Fabric Manager Client

Fabric ペイン 5-19
インターフェイスの使用法（図） 5-7
FabricPath 19-9
FabricWare
DCNM-SAN サポート（表） D-3
SNMP トラップ D-2
syslog トラップ D-2
イベント D-2
セキュリティ D-2
ゾーン分割のサポート D-2
ファイバ チャネル サポート D-1
ロール D-2
FAQ
DCNM-SAN 11-1
Device Manager 11-1
FC-GS-3 要求
デバイス グループ化のサポート 5-31
FCIP
制約事項 11-20
fcipPortAdminCfgChange ツールチップ 11-16
fcipPortKeepAliveTimerExpire ツールチップ 11-16
fcipPortMaxReTx ツールチップ 11-16
fcipPortPersistTimerExpire ツールチップ 11-16
fcipPortSrcAdminDown ツールチップ 11-16
fcipPortSrcLinkDown ツールチップ 11-16
fcipSrcModuleNotOnline ツールチップ 11-16
fcipSrcPortRemoved ツールチップ 11-16
FCoE
ウィザード 5-33
fcotChksumErr ツールチップ 11-16
fcotNotPresent ツールチップ 11-16
fcotVendorNotSupported ツールチップ 11-16
fcspAuthenfailure ツールチップ 11-16
fctimer
CFS の設定 B-3
FC エイリアス
DCNM-SAN での使用 3-10
FICON
DCNM-SAN クライアント サポート 5-2
ficonBeingEnabled ツールチップ 11-16
ficonNoPortnumber ツールチップ 11-16
ficonNotEnabled ツールチップ 11-16
ficonVsanDown ツールチップ 11-16
FICP
ウィザード 5-33
firstPortNotUp ツールチップ 11-17
firstPortUpAsEport ツールチップ 11-17
FL ポート
「Nonparticipating」コード C-2
FSPF
パス選択プロトコル D-1
フロー統計情報 7-3

H

Health タブ
説明 2-8
HTTP プロキシ サーバ
設定 11-22
hwFailure ツールチップ 11-17

I

incomAdminRxBBCreditPerBuf ツールチップ 11-17
incompatibleAdminMode ツールチップ 11-17
incompatibleAdminRxBBCredit ツールチップ 11-17
incompatibleAdminRxBufferSize ツールチップ 11-17
incompatibleadminSpeed ツールチップ 11-17
initializing ツールチップ 11-17
install all コマンド
失敗するケース 10-4
interfaceRemoved ツールチップ 11-17
invalidAttachment ツールチップ 11-17
invalidConfig ツールチップ 11-17
invalidFabricBindExh ツールチップ 11-17
Inventory タブ
説明 2-19
IP-ACL

ウィザード 5-33
「IPv4-ACL」「IPv6-ACL」も参照
IPFC
設定が原因のエラー 11-8
IPS モジュール
コア ダンプ B-2
IPv4-ACL
FabricWare のサポート D-2
iSCSI
DCNM-SAN クライアント サポート 5-2
ウィザード 5-33
ISL
詳細なインベントリ情報の表示 2-23
統計情報 9-5
パフォーマンス情報の表示 2-15
パフォーマンス統計情報 7-1
IVR
DCNM-SAN クライアント サポート 5-2
FICON のサポート B-2
ウィザード 5-33
サービス グループ B-2

J

Java
実行エラー 11-7
java.lang.ArrayIndexOutOfBoundsException errorArrayIndexOutOfBoundsException エラー 11-7
Java Web Start
*.jnlp ファイルに設定 11-5
not detected 11-4
インストールの確認 11-3
キャッシュのクリア 11-6
コマンドラインから実行 11-6
ダウンロード ダイアログで停止 11-5
JNLP
設定の確認 11-3

K

Konqueror
Java Web Start に対する設定 11-5

L

linkFailCreditLossB2B ツールチップ 11-17
linkFailCreditLoss ツールチップ 11-17
linkFailDebounceTimeout ツールチップ 11-17
linkFailLineCardPortShutdown ツールチップ 11-17
linkFailLinkReset ツールチップ 11-17
linkFailLIPF8Rcvd ツールチップ 11-17
linkFailLIPRcvdB2B ツールチップ 11-17
linkFailLossOfSignal ツールチップ 11-17
linkFailLossOfSync ツールチップ 11-17
linkFailLRRcvdB2B ツールチップ 11-17
linkFailNOSRcvd ツールチップ 11-17
linkFailOLSRcvd ツールチップ 11-18
linkFailOPNyRETB2B ツールチップ 11-18
linkFailOPNyTMOB2B ツールチップ 11-18
linkFailPortInitFail ツールチップ 11-18
linkFailPortUnusable ツールチップ 11-18
linkFailRxQOverFlow ツールチップ 11-18
linkFailTooManyINTR ツールチップ 11-18
linkFailure ツールチップ 11-18
loopbackDiagFailure ツールチップ 11-18
loopbackIsolation ツールチップ 11-18

M

McAfee Internet Suite 6.0 Professional
DCNM-SAN インストール エラー 11-7
Device Manager インストール エラー 11-7
Mozilla
Java Web Start に対する設定 11-5

N

NIC
DCNM-SAN クライアントに手動で指定 11-22
DCNM-SAN サーバに手動で指定 11-21
Device Manager に手動で指定 11-22
nonParticipating ツールチップ 11-18
NPV
ウィザード 5-33

O

offline ツールチップ 11-18
OHMS
設定 B-3
ohmsExtLBTest ツールチップ 11-18
Online Health Management System。「OHMS」を参照
Opera
Java Web Start に対する設定 11-5
other ツールチップ 11-18

P

parentDown ツールチップ 11-18
pcAnyWhere
DirectX で置き換え 11-7
停止 11-7
peerFCIPPortClosedConnection ツールチップ 11-18
peerFCIPPortResetConnection ツールチップ 11-18
Performance Manager
CSV 形式でエクスポート 9-12
Traffic Analyzer と併用するための設定 9-9
サービスがディセーブルと表示される 11-7
しきい値の使用法 7-2
収集の確認 3-6
収集の作成 9-2
設定ウィザード 9-6
データ収集 7-2
データ収集の設定 7-4
データ補間 7-2
認証 4-4
フローの作成 9-2
フローの設定 7-4
レポート 9-7
レポートの表示 9-7
Performance Manager レポート
XML 形式でエクスポート 9-11
イベントの表示 9-8
グラフの表示 9-8
サマリー レポートの表示 9-7
テーブルの表示 9-8
トップ 10 の生成 9-8
ホスト最適化ポート グループ パフォーマンスの表示 9-8
Performance タブ
説明 2-10
PONG、「ネットワーク分析」を参照
portBindFailure ツールチップ 11-18
portBlocked ツールチップ 11-18
portChannelMembersDown ツールチップ 11-18
portFabricBindFailure ツールチップ 11-18
portGracefulShutdown ツールチップ 11-18
portVsanMismatchIsolation ツールチップ 11-19

Q

QoS
ウィザード 5-33

R

RADIUS
FabricWare のサポート D-2
rcfInProgres ツールチップ 11-19
Red Hat Linux
DCNM-SAN サーバ 3-1
RRD
データベースの設定 2-41

RSPAN
設定 B-2

S

SAN オペレーティング システム。「Cisco MDS SAN-OS」を参照
SAN 拡張チューナー
設定 B-2
SFP
存在しない理由コード C-1
SNMPv1
FabricWare のサポート D-2
SNMPv2
FabricWare のサポート D-2
SNMP 設定
Enable Audible Alert when Event Received のデフォルト 5-29
Retry request 1 time(s) after 5 sec timeout のデフォルト 5-29
Trace SNMP packets in Log のデフォルト 5-29
Solaris
DCNM-SAN 3-1
srcPortNotBound ツールチップ 11-19
SSH
FabricWare のサポート D-2
SSI ブート イメージ
設定 B-2
SSL 証明書
DCNM-SAN Web サービスとの併用 2-5
SSM
管理 B-2
[Statistics] タブ
DCNM-LAN
モニタリングの停止と開始 14-12, 14-13
suspendedByMode ツールチップ 11-19
suspendedBySpeed ツールチップ 11-19
suspendedByWWN ツールチップ 11-19
swFailure ツールチップ 11-19
syslog
Events タブでの表示 2-8
情報の表示 2-9
登録情報の表示 2-37

T

tooManyInvalidFLOGIs ツールチップ 11-19
tovMismatch ツールチップ 11-19
trunkNotFullyActive ツールチップ 11-19

U

UNIX
DCNM-SAN Web サービスの起動 2-3
UNIX の問題
too many open files エラー 11-12
親メニューが表示されない 11-12
ブラウザで Web サーバを検出できない 11-12
upgradeInProgress ツールチップ 11-19

V

Visio 図
マップの保存 5-22
VSAN
ウィザード 5-33
不一致 C-2
フロー統計情報 7-3
vsanInactive ツールチップ 11-19
vsanMismatchIsolation ツールチップ 11-19

W

Windows
DCNM-SAN サーバ 3-1
Windows の問題
DCNM-SAN ウィンドウの内容が表示されない 11-12

Device Manager ウィンドウの内容が表示されない 11-12
SCP/SFTP に失敗 11-12
Windows XP の停止 11-11
アイコンがデスクトップに表示されない 11-11
印刷するとアプリケーションがクラッシュする 11-11
テキスト フィールドが小さすぎる 11-11
ブルー画面 11-11
WWN
中断された接続 C-2

Z

zoneMergeFailureIsolation ツールチップ 11-19
zoneRemoteNoRespIsolation ツールチップ 11-19

あ

アイコン
Device Manager 6-5
アカウンティング
リストの表示 2-9
アップグレード。「中断を伴うアップグレード」「中断のないアップグレード」「ソフトウェア アップグレード」を参照

い

イーサネット インターフェイス
パフォーマンス情報の表示 2-18
イベント
DCNM-SAN Web サービスを使用した表示 8-2
DCNM-SAN を使用した表示 8-2
Device Manager を使用した表示 8-2
表示 2-9
イベント ブラウザ
DCNM-LAN
イベント最大経過時間の設定 14-17
イメージ
Software Install Wizard 10-8
「キックスタート イメージ」「ソフトウェア イメージ」「システム イメージ」を参照
イメージ。「キックスタート イメージ」を参照
インストール
DCNM-LAN
前提条件 13-2
インターフェイス
動作不能理由コード C-1
理由コード C-1
インベントリ
ISL 情報の表示 2-23
VSAN の詳細の表示 2-19
管理 8-4
スイッチの詳細の表示 2-20
ゾーン情報の表示 2-23, 2-24
モジュールの詳細の表示 2-21

う

ウィザード
DPVM Wizard 5-33
FCIP Wizard 5-33
FCoE Wizard 5-33
IP ACL Wizard 5-33
iSCSI Wizard 5-33
IVR Zone Wizard 5-33
License Install Wizard 5-33
NPV Wizard 5-33
PortChannel Wizard 5-33
Port Security Wizard 5-33
QoS Wizard 5-33
Software Install Wizard 5-33
VSAN Wizard 5-33
Zone Edit Tool Wizard 5-33

え

エイリアス

FDCNM-SAN での使用 3-10
グローバル デバイス エイリアスと FC エイリアスの切り替え 3-10
ラック名としての使用 5-31, 5-32
エクスポート
CSV 形式の Performance Manager レポート 9-12
エラー メッセージ
gen エラー メッセージ 11-7
エラー レポート
以前のレポートの消去 B-3

か

カーネル コア ダンプ
設定 B-3
外部 CompactFlash
フォーマット B-2
カスタム レポート
テンプレートの作成 2-25
テンプレートの修正 2-29
管理
ロールベース 5-32
関連資料 i-lxiv

き

ギガビット イーサネット インターフェイス
パフォーマンス情報の表示 2-18
キックスタート イメージ
KICKSTART 変数 10-1
スーパーバイザ モジュールの選択 10-6
説明 10-4

く

クライアント
切断 2-40
表示 2-40
クラスタ管理
DCNM-LAN
説明 22-1
データの表示 22-4
グローバル プリファレンス
DCNM-LAN
イベント プリファレンス 14-17
概要 14-16
事前プロビジョニング プリファレンス 14-17
モニタリング プリファレンス 14-16
クロック モジュール
管理 B-2

こ

コア ダンプ
IPS モジュール B-2
コア ファイル
CompactFlash への保存 B-3
更新
スイッチ B-1
コマンド スクリプト
実行 B-2
コマンド スケジューラ
設定 B-2
コミュニティ
削除 2-35
追加 2-35
コンソール設定値
設定 B-1
コンフィギュレーション ファイル
表示 B-2

さ

サーバ ログ設定
DCNM-LAN
説明 27-1
デフォルト ログ レベルの設定 27-3
サービス

開始 2-31
再開 2-31
停止 2-31
サービス モジュール
交換 10-15
サマリー レポート
説明 2-2

し

時間遅延
設定 B-2
しきい値
パフォーマンスの基準 7-3
システム イメージ
SYSTEM 変数 10-1
スーパーバイザ モジュールの選択 10-6
説明 10-4
システム ヘルス
開始 B-3
システム メッセージ
DCNM-SAN Web サーバによる表示 8-4
Device Manager による表示 8-5
Events タブでの表示 2-8
表示 2-9
初期化文字列
設定 B-1

す

スイッチ
始動 B-1
デュアル スーパーバイザでの更新 B-1
ライセンス情報の表示 2-20
スイッチング モジュール
Device Manager による表示 6-7
交換 10-15
スーパーバイザ 1 モジュール
スーパーバイザ 2 モジュールからの移行（注意） 10-13
ソフトウェア イメージの選択 10-6
スーパーバイザ 2 モジュール
スーパーバイザ 1 モジュールからの移行 10-13
ソフトウェア イメージの選択 10-6
第 1 世代シャーシ 10-14
スーパーバイザ モジュール
Device Manager による表示 6-7
交換 10-13, 10-15
スーパーバイザ 2 モジュールへの移行 10-13
スタンバイ bootflash: の管理 10-14
スタンバイ スーパーバイザのブート変数バージョン 10-14
スタンバイのブート アラート 10-14
デュアル スーパーバイザ スイッチの更新 B-1
スケジューラ。「コマンド スケジューラ」を参照
スタートアップ コンフィギュレーション ファイル
ロック解除 B-2
スタンバイ スーパーバイザ モジュール
bootflash: の管理 10-14
イメージのコピー B-2
ブート アラート 10-14
ブート変数バージョン 10-14
ストレージ デバイス
パフォーマンス統計情報 7-1
ストレージ トラフィック
パフォーマンス情報の表示 2-16

せ

接続
トラブルシューティング ツール 5-33

そ

ゾーン
インベントリ情報の表示 2-23, 2-24
ウィザード 5-33

トラブルシューティング ツール 5-33
太字で表示 11-9
ゾーン分割
FabricWare のサポート D-2
ソフトウェア アップグレード
Software Install Wizard 10-8
中断 10-2
メカニズム 10-2
ソフトウェア イメージ
SAN-OS イメージのアップグレード 10-1
アップグレード要件 10-6
スーパーバイザ モジュールの選択 10-6
スペース要件 10-7
デフォルト設定 10-8
変数 10-1
ソフトウェア インストール
Software Install Wizard 10-8

た

第 2 世代スイッチング モジュール
第 1 世代シャーシへの設置 10-14
端末
設定値の設定 B-1

ち

中断のないアップグレード
方法 10-2

つ

通知
送信条件 2-42
転送の削除 2-38
転送の追加 2-37

て

データベース
DCNM-LAN
クリーンアップ 29-5
注意事項 29-3
バックアップ 29-4
復元 29-7
メンテナンス 29-1
データベース ファイル
ロック エラーの解決 2-30
テーブル
情報の検索 2-5
ナビゲート 2-4
フィルタリング 2-4
デバイス
DCNM-SAN での検索 11-24
グループの変更（手順） 5-31
検出 8-2
デバイス グループ
DCNM-LAN
グループからのデバイスの削除 21-5
グループへのデバイスの追加 21-4
説明 21-1
デバイス グループの作成 21-2
トポロジ内 19-18
デバイス ディスカバリ
DCNM-LAN
説明 16-1
デバイスの検出 16-9
デバイスの再検出 16-10
デバイスとクレデンシャル
DCNM-LAN
説明 17-1
デバイスの検出 17-4
デバイスの削除 17-6
デバイスの追加 17-4
デバイスの非管理対象化 17-5
デフォルト クレデンシャルの設定 17-6

デバイスとの自動同期化
DCNM-LAN
イベント データの削除 21-5, 23-5
説明 23-1
データの自動的な消去 23-6
データの即時消去 23-7
デバイスとの同期化 23-4
ポーラー間隔 14-16, 23-4
ポーラーの開始と停止 23-3
テンプレート
カスタム レポート テンプレートの修正 2-29
カスタム レポートの作成 2-25

と

統計データ収集
DCNM-LAN
[Statistics] タブ 14-12, 14-13
コレクションからのデータの削除 25-5
コレクションの削除 25-5
説明 25-1
データ収集の停止と開始 25-3
データの自動的な消去 25-6
データの即時消去 25-8
統計データベースからのデータの削除 25-6
トポロジ
DCNM-SAN へのアクセス 19-23
JPG イメージとしてエクスポート 19-22
vPC 設定の不一致 19-28
vPC の管理 19-28
アイコンおよびリンクの概要 19-10
スタートアップ コンフィギュレーションへの実行コンフィギュレーションのコピー 19-20
説明 19-1
デバイス グループからのデバイスの削除 19-20
デバイス グループ間でのデバイスの移動 19-19
デバイス グループの折りたたみ 19-18
デバイス グループの削除 19-21
デバイス グループの作成 19-18
デバイス グループの展開 19-18
デバイス グループの非表示 19-17
デバイス グループの表示 19-17
デバイスの移動 19-13
ネットワーク サーバの非表示 19-16
ネットワーク サーバの表示 19-16
凡例 19-10
ビュー 19-2
表示ツールの使用 19-11
ファブリック パスへのアクセス 19-24
他の機能へのアクセス 19-22
マッピング 8-3
マップのオープン 19-9
マップのクリア 11-23
レイアウト 19-5
レイアウトのロード 19-14, 19-15
トポロジ マップ
カスタム 8-3
カスタム レイアウトの保存（手順） 8-3
説明 8-3
複数ファブリックのマッピング 8-4
ラック 8-4
ドメイン
オーバーラップ分離 C-2
ドメイン ID
障害 C-2
重複によるエラーの発生 11-13
トラブルシューティング
DCNM-SAN ツール 5-33
トランキング
Device Manager による設定 6-7
ドリル ダウン レポート
説明 2-2

な

夏時間
調整 B-1

に

認証
- DCNM-SAN Web サービス 4-4

ね

ネットワーク オペレータのロール
- FabricWare D-2

ネットワーク管理者のロール
- FabricWare D-2

ネットワーク サーバ
- DCNM-LAN
  - 一意なクレデンシャルの消去 20-6
  - 一意なクレデンシャルの設定 20-5
  - サーバからのアダプタのアンバインド 20-10
  - サーバとアダプタの関連付け 20-9
  - サーバの関連付け 20-6
  - サーバへのアダプタのバインド 20-10
  - 説明 20-1
  - デフォルト クレデンシャルの消去 20-4
  - デフォルト クレデンシャルの設定 20-3

ネットワーク分析
- DCNM-LAN
  - PONG 26-2

ネットワーク モニタリング
- デバイスの検出 8-2
- トポロジのマッピング 8-3

は

ハードウェア
- リストの表示 2-9

ハードウェア障害
- アクションの設定 B-3

ハイ アベイラビリティ
- ソフトウェア アップグレード 10-2

パスワード
- DCNM-SAN を使用した割り当て 5-32

パフォーマンス
- Device Manager でのモニタリング（手順） 9-4
- ISL 統計情報（手順） 9-5
- イベント トリガー 7-2
- グラフ 9-8
- サマリーの表示 2-49
- サマリー レポート 9-7
- しきい値の使用法 7-2
- 収集の設定 2-40
- データ 7-4
- テーブル 9-8
- ポート単位のモニタリング（手順） 9-5
- ホスト最適化ポート グループ 9-8
- リアルタイム モニタリング 9-1
- 履歴のモニタリング 9-2
- レポートのカスタマイズ 2-24

パフォーマンスの収集
- 削除 2-41
- しきい値の設定 2-36, 2-42
- 追加 2-40

ふ

ファイバ チャネル アナライザ
- 設定した情報のクリア B-3
- フレームをリモート IP アドレスに送信 B-3
- フレームをローカルでキャプチャ B-3

ファイル
- 圧縮 B-2
- 圧縮解除 B-2
- 内容の表示 B-1
- 末尾の表示 B-2

ファブリック
- 検出 5-30
- モニタリング 3-6
- モニタリングの編集 2-32

ファブリック アナライザ
- ディスプレイ フィルタの使用 B-3

フィルタリング

エンド ポート グループ 5-23
スイッチ グループ 5-23
複数のファブリック 8-4
管理 11-25
プリファレンス
Confirm Deletion のデフォルト 5-29
DCNM-SAN クライアント 5-28
Device Manager 6-9
Export Tables with Format のデフォルト 5-29
Show CFS Warnings のデフォルト 5-29
Show End Device Using のデフォルト 5-28
Show Shortened iSCSI Names のデフォルト 5-28
Show Timestamps as Date/Time のデフォルト 5-28
Show WorldWideName（WWN）Vendor のデフォルト 5-28
Telnet Path のデフォルト 5-28
Use Secure Shell instead of Telnet のデフォルト 5-29
デフォルト 5-28
デフォルトの Show Device Name 5-28
フロー
パフォーマンス情報の表示 2-16
パフォーマンス統計情報 7-1

ほ

ポート
Device Manager によるイネーブル化 6-7
Device Manager によるディセーブル化 6-7
ポート グループ
ホスト最適化パフォーマンス 9-8
ポート セキュリティ
ウィザード 5-33
ポートチャネル
Device Manager による設定 6-7
ウィザード 5-33
互換性のない速度 C-2
互換性のないモード C-2
互換性のないリモート スイッチ C-2
作成ダイアログボックスの大きさ 11-8
ダウン状態 C-2
ポーリング時間
変更 3-9
ホスト
パフォーマンス統計情報 7-1

ま

マップ
1 つしかないスイッチが 2 つ表示される 11-13
Visio 図 5-22
アイコンの説明 5-19
色の定義 11-14
エンド デバイスのグループ化 5-31
大きい表示 5-21
オレンジの十字 11-14
強調表示 5-22
スイッチ内のレッドの線 11-14
正方形なし 11-14
タブの説明 5-21
デフォルト設定 5-29
トポロジのクリア 11-23
ブラウンの正方形 11-14
ブラックの正方形 11-14
保存 5-22
マップ設定を保持したままソフトウェアをアップグレード 11-19
モードの付いたオレンジの正方形 11-14
モードの付いたグリーンの正方形 11-14
モジュール警告 11-14
要素の消去 5-23
ライセンス オレンジ X のクリア 11-25
ライト グレーの正方形 11-14
リフレッシュ 5-23
レイアウト表示の保持 11-13
レッドの十字 11-14
レッドの正方形 11-14
マップ設定

Automatically Save Layout のデフォルト 5-29
Detach Overview Window のデフォルト 5-29
Display End Device Labels のデフォルト 5-29
Display End Devices のデフォルト 5-29
Display Unselected VSAN Members のデフォルト 5-29
Expand Loops のデフォルト 5-29
Expand Multiple Links のデフォルト 5-29
Layout New Devices Automatically のデフォルト 5-29
Open New Device Manager Each Time のデフォルト 5-29
Override Preferences for Non-default Layout のデフォルト 5-29
Select Switch or Link from Table のデフォルト 5-29
Use Quick Layout when Switch has >=30 End Devices のデフォルト 5-29
マップ モジュール エラーマップ
ファン エラーマップ
電源モジュール エラー 11-14
マニュアル
追加資料 i-lxiv

め

メッセージ
重大度の選択 2-37

も

モジュール
交換 10-15
接続 B-2
モジュール設定
維持 B-2
消去 B-2
モジュール テスト
設定 B-3
モデム
設定値の設定 B-1
モニタリング
停止と開始 14-13
DCNM-LAN 14-12

ゆ

ユーザ
DCNM-LAN
説明 15-1
ローカル ユーザの削除 15-8
ローカル ユーザの追加 15-6
ローカル ユーザ パスワードの変更 15-7
ロール 15-2
削除 2-39
追加 2-38
ユーザベースのロール
FabricWare のサポート D-2

よ

よくある質問。「FAQ」を参照

ら

ライセンス
「Cisco DCNM エンタープライズ LAN ライセンス」を参照 18-3
One-Click License Install が実行されない 11-10
ウィザード 5-33
サポートされていない機能 B-1
スイッチ間の移動 B-1
スイッチ情報の表示 2-20
ファイルのバック アップ B-1
ラック名
エイリアス 5-31, 5-32

り

リモート AAA サーバ
　認証の遅延　4-2
リモート SPAN
　設定　B-2
リモート ファイル システム
　アクセス　B-2
理由コード
　説明（表）　C-1
履歴データ
　維持　11-20
リンク障害
　理由コード　C-1

る

ループ
　モニタリング　B-3
ループバック テスト
　頻度の設定　B-3

ろ

ロール
　Web Service のロールの削除　2-40
　Web Service のロールの追加　2-39
　権限　5-32
ロールベースの管理
　アクセス コントロール　5-32
ログ
　DCNM-SAN Web サーバによる表示　8-4
　Device Manager による表示　8-5
　情報の表示　2-36
　ログ ウィンドウ サイズの拡大　11-10
ログイン
　エラー リカバリ　11-6