



Cisco LAN Management Solution 2.5 導入ガイド

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com/en/US/products/netmgtsw/index.html>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



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。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン パーティションの一部として、UCB が開発したプログラムを最適化したものです。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。シスコシステムズおよびこれら各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、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、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のもので、「パートナー」という用語を使用している場合でも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0502R)

Cisco LAN Management Solution 2.5 導入ガイド

Copyright © 2005, Cisco Systems, Inc.

All rights reserved.



CHAPTER 1**Cisco LAN Management Solution 2.5 導入ガイド 1-1**

はじめに	1-1
LMS 2.5 に含まれるアプリケーション	1-1
LMS 2.5 のバージョン	1-2
LMS 2.x から LMS 2.5 へのアップグレード	1-2
LMS 2.5 のアーキテクチャ	1-3
Common Services と DCR	1-3
デバイスと LMS のワークフロー	1-4

CHAPTER 2**ネットワーク上のデバイスの設定 2-1**

デバイスの設定要素	2-1
システム名	2-1
ドメイン名	2-2
SNMP 設定	2-2
Cisco IOS デバイスでの SNMP v3 のイネーブル化	2-2
Catalyst OS デバイスでの SNMP v3 のイネーブル化	2-3
Cisco IOS デバイスでの SNMP v1 または v2c のイネーブル化	2-3
Cisco Catalyst OS デバイスでの SNMP v1 または v2c のイネーブル化	2-3
Catalyst OS デバイスでの特定のホストに送信されるトラップのイネーブル化	2-3
IOS デバイスでの SNMP v2c を使用する特定のホストに送信されるトラップのイネーブル化	2-4
システムのリロード	2-4
コマンドライン プロンプト	2-4
Telnet/SSH	2-4
Syslog メッセージ	2-5
プロトコルの設定	2-6
Cisco Discovery Protocol (CDP)	2-6
Cisco IOS デバイスでの CDP のイネーブル化またはディセーブル化	2-6
Cisco Catalyst OS デバイスでの CDP のイネーブル化またはディセーブル化	2-6
Remote Copy Protocol	2-7
Secure Copy Protocol (SCP)	2-7
HTTP サーバおよび HTTPS サーバ	2-8
Multiple Spanning-Tree の設定	2-9
Multiple Instance Spanning-Tree の設定	2-10

Per-VLAN Spanning Tree+ の設定	2-11
スパニング ツリー プロトコルの詳細情報	2-12
PVST+ 設定のデフォルト値	2-12
VTP の設定	2-13
ベスト プラクティスのための推奨事項	2-14
Catalyst スイッチ ポートでのトランキングのイネーブル化	2-14

CHAPTER 3

Cisco LAN Management Solution 2.5 のインストール要件 3-1

Solaris OS のインストール要件	3-1
推奨される Solaris ディスク レイアウト	3-1
バックアップに関する推奨事項	3-2
Windows OS のインストール要件	3-2
LMS アプリケーションのインストールの推奨順序	3-2
LMS アプリケーションで使用されるポート	3-3
ライセンスに関する用語とプロセス	3-4

CHAPTER 4

LAN Management Solution 2.5 サーバの初期設定 4-1

LMS アプリケーションでのアプリケーション モードの設定	4-1
プロトコル設定	4-2
構成管理	4-2
プロトコル順序の設定	4-3
ソフトウェア イメージ管理	4-3
セキュリティの設定	4-4
証明書の設定	4-4
システム ID ユーザの設定	4-4
ピア サーバアカウントの設定	4-4
LMS サーバでの HTTPS のイネーブル化	4-5
注	4-5
シングル サインオン	4-5
Cisco Secure Access Control Server の設定	4-6
LMS サーバと ACS の統合	4-6
LMS サーバでのシステム ID ユーザおよびピア サーバアカウント ユーザの設定	4-6
ACS サーバの設定	4-6
ACS サーバと通信するための LMS サーバの設定	4-7
ACS サーバでのシステム ID ユーザの設定	4-7
ロール マッピングのデフォルトの権限およびタスクを変更するための ACS サーバの設定 (任意)	4-8
ネットワーク デバイス グループ、ユーザ グループの作成と ACS サーバ でのネットワーク デバイス グループへのロールの割り当て	4-8
デバイスでタスクを実行するための権限の設定	4-9

CHAPTER 5

Cisco LAN Management Solution 2.5 でのデバイスの認識	5-1
Campus Manager のデバイス検出	5-1
Campus Manager でのシード デバイスの定義	5-2
Device and Credentials Repository へのバルク デバイス インポート	5-2
デバイス クレデンシャルの更新	5-3
デバイス管理	5-4
DCR から RME へのデバイスの追加	5-4
RME のコンフィギュレーション収集ステータスの表示	5-4
デバイスの起動および実行コンフィギュレーションの収集	5-4
LMS アプリケーションでのデバイス インポート ステータスの確認	5-5
Resource Manager Essentials	5-5
Campus Manager	5-5
Device Fault Manager	5-5

CHAPTER 6

Cisco LAN Management Solution 2.5 でのサーバ管理	6-1
Common Services	6-1
ユーザ定義グループの作成	6-2
LMS データのバックアップ	6-2
LMS データの復元	6-3
Campus Manager	6-3
Campus Manager のデバイス検出	6-3
ネットワーク検出の最適化	6-4
Campus Manager のデータ収集	6-4
データ収集の最適化	6-5
ユーザ追跡モジュール	6-5
UT メジャー検出の開始	6-5
削除ポリシー	6-6
Campus Manager 内の階層型グループ	6-6
Resource Manager Essentials	6-7
インベントリ収集とポーリング	6-7
ジョブ スケジュールのデフォルト設定の変更	6-7
コンフィギュレーション ファイルの収集とポーリング	6-7
コンフィギュレーションの収集とポーリングのタイミングおよび方法の指定	6-8
コンフィギュレーションの取得と適用に使用されるデフォルトの プロトコル	6-8
RME の削除ポリシー	6-8
コンフィギュレーション ファイルを削除するタイミングの指定	6-8
Syslog メッセージの定期的な削除	6-9
変更監査データの削除	6-9
Syslog メッセージ フィルタの定義	6-10

変更監査	6-10
インベントリ フィルタの設定	6-10
例外期間の定義	6-10
SWIM ベースライン収集	6-11
ソフトウェア リポジトリの同期	6-11
RME ジョブの管理	6-12
Internetwork Performance Monitor へのデバイスのインポート	6-13
Device Fault Manager	6-13
日常の削除スケジュール	6-14
SNMP トラップの転送	6-14
SNMP トラップの受信	6-14
デフォルトの SMTP サーバ	6-14
再検出	6-14
グループ管理	6-15
ポーリングおよびスレッシュホールド パラメータの設定	6-15
ビューの作成	6-15
CiscoView	6-15
Device Center	6-16
デバッグ ユーティリティの起動	6-16

CHAPTER 7

Cisco LAN Management Solution 2.5 でのネットワーク管理	7-1
障害モニタリング	7-1
設定作業	7-1
障害およびアラート通知サービス	7-2
障害履歴	7-3
アラートおよびアクティビティ	7-3
ベースライン設定	7-3
LMLS アプリケーションからのデータ抽出	7-3
Campus Data Extraction Engine	7-3
cmexport ユーティリティ	7-4
コア コマンド	7-4
アーカイブの場所	7-4
cmexport コマンドの使用可能な組み合わせ	7-5
Layer 2 Topology コマンドまたは Discrepancy コマンド	7-5
Data Extraction Engine への Servlet アクセス	7-6
Resource Manager Essentials の Data Extraction Engine	7-8
コマンドライン構文	7-9
データのアーカイブ場所	7-9
RME Servlet	7-10
Internetwork Performance Monitor でのエクスポート	7-11
IPM Export コマンド	7-11

DCR コマンドライン インターフェイス	7-12
ユーザ追跡レポート	7-13
デバイスでの Syslog の設定	7-13
VLAN に関する推奨設定	7-14
最小深度のスパニング ツリーに関する推奨設定の表示	7-14
イーサチャネルおよびトランクの構築	7-15
イーサチャネルの設定	7-15
トランクの設定	7-15
コンフィギュレーション ファイルの変更管理	7-16
RME Config Editor	7-16
NetConfig テンプレート	7-16
変更監査レポート	7-16



Cisco LAN Management Solution 2.5 導入ガイド

はじめに

今日のネットワークでは、企業がソリューションの導入および管理を行ううえで、ネットワーク管理が非常に重要です。生産性を向上させるためにネットワークへの依存度が高まるにつれて、企業はかつてない規模のネットワークの拡張に直面しています。このように、ネットワーク構成要素の数が増えるにつれて、ネットワーク管理者には課題が生じています。企業では、どうすればネットワーク デバイスを効率的に導入および保守できるでしょうか。

CiscoWorks LAN Management Solution (LMS) は、シスコのネットワークの設定、管理、モニタリング、およびトラブルシューティングを簡素化するために必要な、統合された管理ツールを提供します。CiscoWorks LMS は、管理アプリケーション間でのデバイス情報の共有、デバイス管理タスクの自動化、ネットワークの稼働状態および性能のチェック、ネットワーク障害の識別と原因の特定を行うための、統合されたシステムを IT 関連組織に提供します。CiscoWorks LMS は、共通の一元的なシステムとネットワーク インベントリに関する知識を使用することで、複数の分野にまたがる管理機能を備えた独自のプラットフォームを提供し、ネットワーク管理のオーバーヘッドを削減して、上位層のシステム統合を可能にします。

この導入ガイドでは、すべてのアプリケーションが 1 台のサーバにインストールされている構成例を想定し、サーバの設定に関するヒントおよび提案を示します。LMS 2.5 で取り入れられた複数サーバ構成に関連する概念についても説明します。

LMS 2.5 に含まれるアプリケーション

LMS 2.5 には、次のコンポーネントが含まれています。

- CiscoWorks Common Services 3.0

Common Services 3.0 は、すべての LMS アプリケーションで使用される共有アプリケーションサービスのセットです。Common Services 3.0 には、CiscoView 6.1 と Integration Utility 1.6 の両方が含まれます。

- CiscoView 6.1 には、シスコ製デバイスの「前面パネル」をグラフィカルに表示する機能があり、ユーザはデバイス コンポーネントに簡単にアクセスして、設定パラメータを変更したり統計情報をモニタしたりできます。
- Integration Utility 1.6 は、サードパーティ製のネットワーク管理システムをサポートする統合モジュールです。

- Resource Manager Essentials (RME) 4.0

ライフサイクル管理をサポートするために、RME は、デバイス インベントリと変更監査の管理、コンフィギュレーション ファイルの管理、ソフトウェア イメージの管理機能を提供します。また、Syslog 分析もサポートされます。

- Campus Manager (CM) 4.0

Campus Manager は、ネットワーク トポロジー図の視覚化、VLAN (仮想 LAN) の管理、ネットワーク 不一致の検出、レイヤ 2 およびレイヤ 3 データ、音声トレース、エンドホスト ユーザ情報を提供するための機能を備えています。

- Device Fault Manager (DFM) 2.0

Device Fault Manager は、デバイスの障害をリアルタイムでモニタし、デバイスレベルの障害状態を相互に関連付けることで、根本的原因を特定する機能を備えています。DFM は、電子メールまたはページャーを使用して、クリティカルなネットワーク状態に関して通知を発行できます。Fault History を使用すると、オペレータは、DFM によって検出および処理されたアラートおよび障害の履歴情報を保存したり、履歴情報にアクセスしたりできます。

- Internetwork Performance Monitor (IPM) 2.6

Internetwork Performance Monitor は、Cisco IOS IP SLA と呼ばれる Cisco IOS® ソフトウェア内の合成トラフィック生成テクノロジーに基づいて、ネットワーク パフォーマンスを測定します。

合成トラフィックを使用することによって、ネットワーク管理者は、ネットワーク パフォーマンスの測定対象となるネットワーク内のエンド ポイントを柔軟に選択できます。この柔軟性により、IPM は非常に効果的なパフォーマンストラブルシューティング ツールとなっています。

IPM は、Cisco IOS IP SLA テクノロジーを利用して、ルータ内にコレクタと呼ばれるネットワーク パフォーマンス エージェントを構築します。これらのコレクタは、コンフィギュレーションの一部として、ソース ルータ、ターゲット デバイス、およびオペレーション タイプなどを含んでいます。

LMS 2.5 のバージョン

ユーザは、次のいずれかのバージョンの LMS 2.5 を選択できます。

- 制限付きバージョン

LMS 2.5 の制限付きバージョンは、LMS 1.x 無制限バージョンまたは LMS 2.x から LMS 2.5 に移行するお客様を対象としています。このバージョンのデバイス制限は、300 デバイスです。

- 大企業バージョン

大企業バージョンは、LMS 1.x 無制限バージョンまたは LMS 2.x から LMS 2.5 に移行するお客様を対象としています。このバージョンには、サポートされるデバイス数に制限はありません。

LMS 2.x から LMS 2.5 へのアップグレード

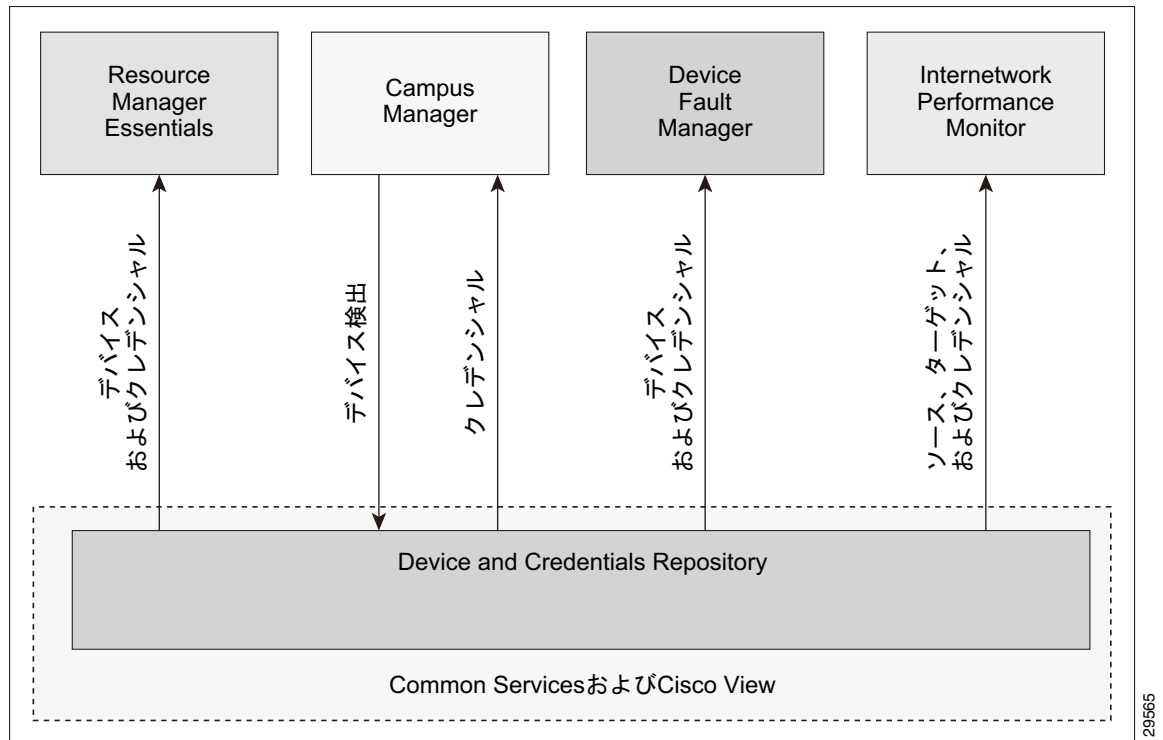
LMS 2.x から LMS 2.5 へのアップグレードの詳細については、次の URL から『LAN Management Solution 2.5 Data Migration Guidelines』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/dmgl_rm.htm

LMS 2.5 のアーキテクチャ

図 1-1 は、LMS 2.5 サーバのアーキテクチャと、1 台の LMS サーバにインストールされたアプリケーションが、デバイス情報を取得するために通信を行う様子を示しています。

図 1-1 LMS 2.5 のアーキテクチャ



Common Services と DCR

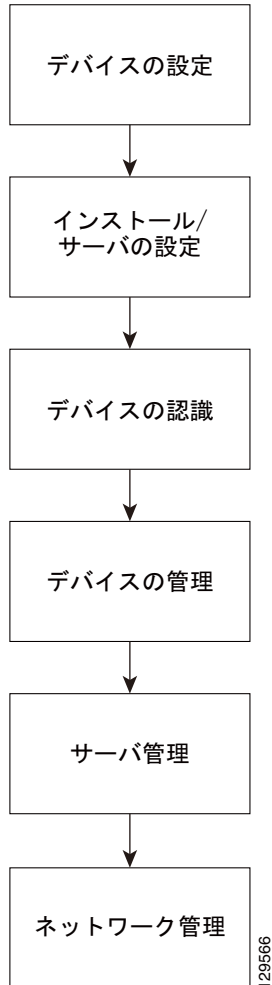
図 1-1 に示すように、LMS 2.5 アプリケーションは Common Services を使用します。Device and Credentials Repository (DCR) は、Common Services の一部であり、すべてのデバイスおよびクレデンシヤル情報のセキュアな中央リポジトリとして機能します。LMS 内のアプリケーションはすべて、DCR に対してデバイス クレデンシヤル情報を要求します。DCR は共有されているため、DCR に登録されたデバイスは別のアプリケーションでも自動的に登録されます (LMS アプリケーションで自動同期モードをイネーブルにする必要あり)。詳細については、「[LMS アプリケーションでのアプリケーションモードの設定](#)」(p.4-1) を参照してください。

DCR は、複数サーバの設定にも役立ちます。このマニュアルでは、複数サーバの設定の際に作成される基本的なコンフィギュレーションについて、一部だけを簡単に説明します。

デバイスと LMS のワークフロー

図 1-2 に、デバイスおよび LMS のセットアップのワークフローを示します。以降の章では、設定とワークフローのプロセスについて詳しく説明します。

図 1-2 デバイスおよび LMS のセットアップのワークフロー





ネットワーク上のデバイスの設定

LAN Management Solution (LMS) 2.5 は、ネットワーク上のシスコ製デバイスの管理に利用されます。ただし、LMS 2.5 が正しく機能するには、LMS 2.5 と双方向通信を行うネットワーク デバイスが、正しく設定されている必要があります。この章では、ネットワーク デバイスを正しく設定するために推奨される方法と手順について説明します。



(注) この章には、CiscoWorks LMS を使用してデバイスを管理するために必要な、さまざまなデバイス設定手順に関する情報が紹介されています。ただし、このマニュアルは、LMS 2.5 の包括的なコンフィギュレーションガイドとして使用する目的では書かれていません。設定の詳細については、可能であればシスコ認定ネットワーク技術者に問い合わせるか、*Cisco.com* で入手可能な適切な資料を参照してください。



ヒント LMS を導入する前に、Cisco IOS および Catalyst OS の場合、次のコマンドを使用して、コンフィギュレーションの変更をすべて NVRAM (不揮発性 RAM) に保存する必要があります。

`write memory` または `copy running-config startup-config`

この2つのコマンドは、**LMS 導入前のコンフィギュレーションの変更**を保存するために使用します。LMS を導入後は、コンフィギュレーションの変更は適切な場所に自動的に保存されるため、ユーザが作業を行う必要はありません。新しいバージョンの Catalyst OS デバイスでは、実行および起動用に個別のコンフィギュレーションが用いられます。

デバイスの設定要素

この項では、デバイス設定の際、注意が必要な要素について個々に説明します。

システム名

すべてのデバイスを検出するために、ネットワーク内の各 Cisco IOS デバイスには一意のシステム名 (sysName) が必要です。システム名は、Cisco Discovery Protocol (CDP) テーブルにも登録されます。ネットワーク上に重複するシステム名がある場合、LMS はネットワーク上の1つの名前に対して、1つのデバイスのみを検出します。Cisco IOS デバイスでは、ドメイン名もシステム名に影響します。

システム名は、次のコマンドを使用して設定できます。

Cisco IOS デバイス

```
hostname <name>
```

Cisco Catalyst OS デバイス

```
set system name <name>
```

ドメイン名

Cisco IOS または Catalyst OS デバイスでは、ドメイン名を設定できます。

ドメイン名は、次のコマンドを使用して設定します。

Cisco IOS デバイス

```
ip domain-name <name>
```

Cisco Catalyst OS デバイス

```
set system name <name with domain name>
```

SNMP 設定

LMS は、SNMP（簡易ネットワーク管理プロトコル）コミュニティ ストリングを使用して、デバイスに対して情報の読み書きを行います。



(注) LMS は、SNMP v3 の SNMP AuthNoPriv モードをサポートします。

Cisco IOS デバイスでの SNMP v3 のイネーブル化

Cisco IOS デバイスで SNMP v3 をイネーブルにする手順は、次のとおりです。

-
- ステップ 1** ビューを作成します。
- ```
snmp view campus 1.3.6.1 included nonvolatile
```
- ステップ 2** セキュリティ モデルを設定します。
- ```
snmp access cmtest security-model v3 authentication read campus write campus nonvolatile
```
- ステップ 3** ユーザを作成して、使用する認証プロトコルを指定します。
- ```
snmp user cmtester authentication md5 cisco123
```
- ステップ 4** グループを作成して、ユーザを関連付けます。
- ```
snmp group cmtest user cmtester security-model v3 nonvolatile
```
-

Catalyst OS デバイスでの SNMP v3 のイネーブル化

Catalyst OS デバイスで SNMP v3 をイネーブルにする手順は、次のとおりです。

-
- ステップ 1** ビューを作成します。
- ```
set snmp view campus 1.3.6.1 included nonvolatile
```
- ステップ 2** セキュリティ モデルを設定します。
- ```
set snmp access cmtest security-model v3 authentication read campus write campus nonvolatile
```
- ステップ 3** ユーザを作成して、使用する認証プロトコルを指定します。
- ```
set snmp user cmtester authentication md5 cisco123
```
- ステップ 4** グループを作成して、ユーザを関連付けます。
- ```
set snmp group cmtest user cmtester security-model v3 nonvolatile
```
-

Cisco IOS デバイスでの SNMP v1 または v2c のイネーブル化

Cisco IOS デバイスで SNMP v1 または v2 をイネーブルにする手順は、次のとおりです。

-
- ステップ 1** `snmp-server community <read-community-string> ro`
- ステップ 2** `snmp-server community <write-community-string> rw`
-

Cisco Catalyst OS デバイスでの SNMP v1 または v2c のイネーブル化

Cisco Catalyst OS デバイスで SNMP v1 または v2c をイネーブルにするには、次のように設定します。

-
- ステップ 1** `set snmp community read-only <read-community-string>`
- ステップ 2** `set snmp community read-write <write-community-string>`
-

デバイスで設定されたコミュニティ スtring は、LMS の Device Credential Repository (DCR) コンポーネントに登録されたコミュニティ スtring と一致している必要があります。

Catalyst OS デバイスでの特定のホストに送信されるトラップのイネーブル化

Catalyst OS デバイスで、特定のホストに送信されるトラップをイネーブルにするには、次のコマンドを使用します。

```
set snmp trap 192.168.124.24 public
```

IOS デバイスでの SNMP v2c を使用する特定のホストに送信されるトラップのイネーブル化

IOS デバイスで、SNMP v2c を使用する特定のホストに送信されるトラップをイネーブルにするには、次のコマンドを使用します。

```
snmp-server host 192.168.124.24 traps version 2c public
```

ここで挙げたトラップのイネーブル化の例では、**public** コミュニティストリングを用いて、トラップの受信側でトラップの選択処理が行われています。

システムのリロード

Resource Manager Essentials (RME) によってソフトウェア イメージの配布作業が完了されると、イメージ配布ジョブで指定されている場合、RME はデバイスをリロードします。SNMP マネージャ (この場合は RME) がエージェントのリセットを許可されている場合のみ、RME はデバイス (IOS または Catalyst OS) をリロードできます。

Cisco IOS デバイスでは、次のコマンドが必要です。

```
snmp-server system-shutdown
```

コマンドライン プロンプト

NetConfig 機能を利用してデバイスの変更に関するバッチ処理を実行するためには、シスコ製デバイスのコマンドラインプロンプトが、この項で説明する要件を満たしている必要があります。



(注)

カスタマイズされたプロンプトも、これらの要件を満たしている必要があります。

Cisco IOS デバイス

- ログインプロンプトは、次の例のように、かぎカッコ (>) で終了する必要があります。
Cisco>
- イネーブルプロンプトは、次の例のように、シャープ記号 (#) で終了する必要があります。
Cisco#

Cisco Catalyst OS デバイス

イネーブルプロンプトは、次の例のように、「(enable)」で終了する必要があります。

```
Cisco(enable)
```

Telnet/SSH

Telnet は、構成管理のために RME で使用できるプロトコルの 1 つです。次のコマンドを使用して、Telnet をイネーブルにできます。

Cisco IOS デバイスおよび Catalyst OS デバイスで Telnet をイネーブルにするには、次のようにコマンドを入力します。

```
line vty 0 4
password <password>
login
exec-timeout 0 0
```



(注) ログインでは4本以上のVTY回線を選択できます。

VTY回線ごとに異なる認証はサポートされていません。

SSH (セキュアシェル) によって、デバイスとの安全な通信が可能です。

Cisco IOS

次に、Cisco IOS が稼働するルータでSSH制御パラメータを設定する例を示します。

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

Catalyst OS

次に、Catalyst OS でSSHの設定を行う例を示します。

```
(enable) set crypto key rsa 1024
(enable) set ipNote:
```



(注) より充実したアクセス制御およびロギング機能を利用するには、TACACS を使用します。

SSHの設定を行うには、ドメイン名を設定する必要があります。

Syslog メッセージ

LMS の機能をさらに活用し、特に RME を利用するために、シスコ製デバイスでは Syslog メッセージをイネーブルにできます。

Cisco IOS デバイス

グローバルコンフィギュレーションモードから、Cisco IOS デバイスで Syslog メッセージをイネーブルにします。

```
logging on
logging <server-ip-address>
logging trap <logging-level>
```



(注) syslog サーバに送信されるメッセージ数を制限するには、上記のロギングトラップコンフィギュレーションコマンドを使用します。

Catalyst OS デバイス

Catalyst OS デバイスで Syslog メッセージをイネーブルにするには、次のコマンドを使用します。

```
set logging server enable
set logging server <server-ip-address>
set logging level all <logging-level> default
```



ヒント <server-ip-address> パラメータは、LMS サーバの IP アドレスです。サーバが複数ある場合、ここに入力するサーバの IP アドレスは、RME サーバのアドレスになります。リモートの Syslog Analyzer およびコレクタを使用している場合、このパラメータは、リモートの Syslog Analyzer およびコレクタの IP アドレスになります。

プロトコルの設定

この項では、以下のプロトコルの基本的な設定手順について説明します。

- Cisco Discovery Protocol (CDP)
- Remote Copy Protocol (RCP)
- Secure Copy Protocol (SCP)
- HTTP プロトコルおよび HTTPS プロトコル
- Multiple Spanning-Tree Protocol (MST)
- Multiple Instance Spanning-Tree Protocol (MIST)
- Per-VLAN Spanning Tree Protocol (PVST+)
- VLAN Trunk Protocol (VTP; VLAN トランク プロトコル)

Cisco Discovery Protocol (CDP)

Cisco Campus Manager は、CDP を使用してネットワーク上のシスコ製デバイスを検出します。CDP は、メディアやプロトコルに依存しないシスコ独自のレイヤ 2 プロトコルで、シスコが製造したすべての機器で機能します。CDP を使用可能なシスコ製デバイスは、ネイバーから認識されるために定期的にインターフェイスの更新情報をマルチキャスト アドレスに送信します。CDP はレイヤ 2 プロトコルのため、これらのパケット (フレーム) はルーティングされません。Campus Manager は例外として、LANE/ATM ネットワークでは ILMI プロトコルを、Stratacom フレーム リレー ネットワークでは ELMI プロトコルを使用します。

デバイスで CDP をイネーブルにすると、Campus Manager は近接するデバイスに関する情報を取得して、そのデバイスに SNMP クエリを送信できます。Campus Manager は、そのデバイスで CDP がイネーブルになっている場合のみ、ネットワーク トポロジ进行检测できます。

Cisco IOS デバイスでの CDP のイネーブル化またはディセーブル化

Cisco IOS デバイスでは、デフォルトで CDP がイネーブルになっています。IOS デバイスで CDP 機能をイネーブルにするには、以下のコマンドを使用します。

- CDP をグローバルにイネーブルにするには、次のコマンドを使用します。
`cdp run`
- 特定のインターフェイスでのみ CDP をイネーブルにするには、次のコマンドを使用します。
`cdp enable`
- Cisco IOS デバイスで CDP 機能をディセーブルにするには、`no` コマンドを使用します。

Cisco Catalyst OS デバイスでの CDP のイネーブル化またはディセーブル化

Cisco Catalyst OS デバイスでは、デフォルトで CDP がイネーブルになっています。Catalyst OS デバイスで CDP 機能をイネーブルにするには、以下のコマンドを使用します。

- CDP をグローバルにイネーブルにするには、次のコマンドを使用します。
`set cdp enable`
- 特定のポートでのみ CDP をイネーブルにするには、次のコマンドを使用します。
`set cdp enable [mod/port]`
- Catalyst OS デバイスで CDP をディセーブルにするには、`set cdp disable` コマンドを使用します。



ヒント Campus Manager で検出する必要がないリンク上では、CDP を実行しないでください。たとえば、インターネットへの接続や、アクセス スイッチ上のエンドホスト接続ポートとの接続などです。CDP DoS 攻撃から保護するために、シスコ以外の製品に接続されたリンクでは CDP をイネーブルにしないでください。



(注) シスコ製品以外にも、CDP がサポートされるデバイスがあります。シスコ製以外のデバイスに接続されたシスコ製デバイスで CDP をイネーブルにすると、Campus マップに表示されます。

関連情報については、次の URL を参照してください。

- Catalyst 6500 シリーズ スイッチでの CDP の設定

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801a5b18.html

Remote Copy Protocol

RCP は、構成管理とソフトウェア イメージ管理を行うために、RNE で使用できるプロトコルの 1 つです。LMS で RCP を使用して、構成およびソフトウェア管理を実行できるようにするには、ネットワーク デバイス上で RCP をイネーブルにする必要があります。RCP は、次のコマンドの例で示すように、Cisco IOS が稼働するデバイス上でのみイネーブルにできます。

```
username cwuser password 7 000C1C0A05
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
```



(注) デバイスで入力される <remote-username> および <local-username> の値は、LMS サーバで指定された RCP User 値と一致している必要があります。デフォルト値は **cwuser** です。この値は、LMS サーバ上のユーザ インターフェイス リンク (CWHP > Common Services > Server > Admin > System Preferences) から変更できます。

Secure Copy Protocol (SCP)

Secure Copy 機能は、Cisco IOS 12.2(2)T で導入されました。

SCP サーバ機能をイネーブルにし、シスコ ルータの設定を行う手順は、次のとおりです。

	コマンド	説明
ステップ 1	Router> enable	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Router# configure terminal	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	Router (config)# aaa new-model	ログイン時に AAA (認証、許可、アカウントिंग) 認証を設定します。
ステップ 4	Router (config)# aaa authentication login default group tacacs+	AAA アクセス制御システムをイネーブルにします。完全な構文は次のとおりです。 aaa authentication login {default list-name} method1 [method2...]

	コマンド	説明
ステップ 5	Router (config)# aaa authorization exec default group tacacs+	ネットワークへのユーザアクセスを制限するパラメータを設定します。 exec キーワードは、ユーザが Exec シェルを実行できるかどうかを判断するための許可を実行します。したがって、SCP を設定するときにこのキーワードを使用する必要があります。構文は以下のとおりです。 aaa authorization {network exec commands level reverse-access configuration} {default list-name} [method1 [method2...]]
ステップ 6	Router (config)# username superuser privilege 2 password 0 superpassword	ユーザ名ベースの認証システムを確立します。 (注) ネットワークベースの認証メカニズム (TACACS+ または RADIUS など) がすでに設定されている場合、このステップを省略することもできます。 構文は以下のとおりです。 username name [privilege level] {password encryption-type encrypted-password}
ステップ 7	Router (config)# ip scp server enable	SCP サーバ機能をイネーブルにします。

HTTP サーバおよび HTTPS サーバ

Cisco IOS HTTP サーバは、クライアントの接続に対して認証は行いますが、暗号化は行いません。クライアントおよびサーバが相互に送信するデータは暗号化されていません。このため、クライアントとサーバ間の通信は、妨害および攻撃に対しての脆弱性を持っています。

http モードのイネーブル化

http モードをイネーブルにするには、次のコマンドを使用します。

```
ip http server
```

Secure HTTP (HTTPS) 機能を使用すると、Cisco IOS HTTPS サーバに安全に接続できるようになります。HTTPS は Secure Sockets Layer (SSL) および Transport Layer Security (TLS) を使用して、デバイス認証とデータ暗号化を行います。



(注) LMS 2.5 のリリース時点では、HTTPS モードは Cisco VPN 3000 シリーズ コンセントレータでのみサポートされています。

VPN 3000 コンセントレータで HTTPS モードをイネーブルにする方法については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a008015ce28.html#999607

Multiple Spanning-Tree の設定

Multiple Spanning-Tree (MST) (802.1s) を設定する手順は、次のとおりです。

ステップ 1 シスコ製スイッチで MST をイネーブルにします。

スイッチでスパニング ツリー モードを MST に設定するには、`set spantree mode mst` コマンドを使用します。



(注) MST をディセーブルにする前に、Per-VLAN Spanning-Tree + (PVST+) など、他のスパニング ツリー プロトコルを設定しておく必要があります。

ステップ 2 VLAN (仮想 LAN) とインスタンス間のマッピングを定義します。

VLAN をインスタンスへマッピングするには、次のコマンドを使用します。

```
set spantree MST instance vlan <vlans>
```

たとえば、VLAN の 1～10 と 20 をインスタンス 10 にマッピングするには、次のように入力します。

```
set spantree MST 10 vlan 1-10,20
```

デフォルトでは、すべての VLAN がインスタンスにマッピングされます。



(注) VLAN をインスタンスにマッピングしても、設定がコミットされるまで有効になりません。

ステップ 3 MST コンフィギュレーション名とリビジョン番号を定義します。

コンフィギュレーション名とリビジョン番号を設定するには、次のコマンドを使用します。

- `set spantree MST configuration name <name>`
- `set spantree MST configuration revision <revision-number>`

インスタンス 1～15 は、MST リージョン内でのみ動作します。

MST リージョンの境界では、MST はポート状態を IST からコピーします。IST は、PVST+、Common Spanning-Tree (CST) などのその他のスパニング ツリー プロトコルや、その他の MST リージョンなどと通信して、ループフリー トポロジを形成します。

MST がイネーブルになっているスイッチは、対応する VLAN と IST 間のマッピング、MST コンフィギュレーション名、および MST リビジョン番号がある場合のみ MST リージョンを形成します。この 3 つのいずれかが欠けた場合、ポートには境界ポートとしてフラグが設定されます。

ステップ 4 MST コンフィギュレーションをコミットして、スイッチに適用します。次のコマンドを使用します。

```
set spantree MST config commit
```

- 最後のコミット以降に行った編集をすべて破棄する必要がある場合は、`set spantree MST rollback` コマンドを使用します。
- 別のセッションを使用して他のユーザが行った MST コンフィギュレーションの変更を消去するには、`set spantree MST rollback force` コマンドを使用します。

コンフィギュレーションの関連情報については、次の URL を参照してください。

<http://www.cisco.com/warp/public/473/123.html>

Multiple Instance Spanning-Tree の設定

Multiple Instance Spanning-Tree (MISTP) を設定する手順は、次のとおりです。

-
- ステップ 1** スイッチで MISTP をイネーブルにします。
スイッチでスパンニング ツリー モードを MISTP に設定するには、次のコマンドを使用します。
`set spantree mode mistp`
- ステップ 2** MISTP のブリッジ ID プライオリティを設定します。
スイッチが MISTP または MISTP-PVST+ モードの場合、MISTP インスタンスのブリッジ ID プライオリティを設定できます。
ブリッジ プライオリティ値は、ブリッジ ID プライオリティを作成するために、拡張システム ID (MISTP インスタンスの ID) と組み合わせて使われます。
使用可能なブリッジ プライオリティ値は 16 個あります。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。
ブリッジ ID プライオリティを設定するには、次のコマンドを使用します。
`set spantree priority 8192 mistpinstance 1`
- ステップ 3** MISTP ポート コストを設定します。
スイッチ ポートにはポート コストを設定できます。ポート コストが低いポートは、フレーム転送用として優先的に選択されます。高速のメディア (全二重など) に接続されたポートには小さい数値を割り当て、低速のメディアに接続されたポートには大きい数値を割り当てます。デフォルトのコスト値は、メディアごとに異なります。
 - ポート コストの計算に short 方式を使用する場合、可能なコスト値の範囲は 1 ~ 65535 です。
 - ポート コストの計算に long 方式を使用する場合、可能なポート コスト値の範囲は 1 ~ 200000000 です。ポート コストを設定するには、次のコマンドを使用します。
`set spantree portcost 2/12 22222222`
- ステップ 4** MISTP ポート プライオリティを設定します。
スイッチ ポートにはポート プライオリティを設定できます。プライオリティ値が最も小さいポートは、すべての VLAN に対してフレームを転送します。使用可能なポート プライオリティ値の範囲は 0 ~ 63 です。デフォルトは 32 です。すべてのポートに同じプライオリティ値が設定されている場合、ポート番号が最も小さいポートがフレームを転送します。
ポート プライオリティを設定するには、次のコマンドを使用します。
`set spantree portpri 2/12 40`
-

Per-VLAN Spanning Tree+ の設定

Per VLAN Spanning Tree Plus (PVST+) は、ネットワーク上に構築された VLAN ごとに Spanning Tree インスタンスを保持します。VLAN トランクでは各 VLAN に応じて、転送とブロックを同時に行うことができます。PVST+ は各 VLAN を個別のネットワークとみなすため、Spanning Tree ループを発生させることなく、VLAN の転送ごとに別のトランクを使用して、レイヤ 2 トラフィックのロードバランスを実行できます。PVST+ では、ISL よりも 802.1Q トランッキングテクノロジーが多く使用されます。PVST+ は 802.1Q の仕様を拡張したものであり、シスコ以外の製品ではサポートされていません。

Per-VLAN Spanning Tree+ を設定する手順は、次のとおりです。

-
- ステップ 1** スイッチで PVST+ をイネーブルにします。
- Spanning Tree モードを `pvst+` に設定するには、次のコマンドを使用します。
- ```
set spantree mode pvst+
```
- ステップ 2** PVST+ のブリッジ ID プライオリティを設定します。
- ブリッジ ID プライオリティは、スイッチが PVST+ モードのときに適用される VLAN のプライオリティです。
- MAC アドレスリダクションがイネーブルになっていない状態でスイッチが PVST+ モードになると、0 ~ 65535 のブリッジプライオリティ値を入力できます。以降、VLAN のブリッジ ID プライオリティがその値に設定されます。
- MAC アドレスリダクションがイネーブルになっている状態でスイッチが PVST+ モードになると、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、または 61440 の 16 個のブリッジプライオリティ値のいずれかを入力できます。
- ブリッジプライオリティは、VLAN のブリッジ ID プライオリティを作成するために、拡張システム ID (VLAN の ID) と組み合わせて使われます。
- ブリッジ ID プライオリティを設定するには、次のようにコマンドを入力します。
- ```
set spantree priority 30000 1
```
- ステップ 3** PVST+ ポート コストを設定します。
- スイッチポートにはポート コストを設定できます。ポート コストが低いポートは、フレーム転送用として優先的に選択されます。高速のメディア (全二重など) に接続されたポートには小さい数値を割り当て、低速のメディアに接続されたポートには大きい数値を割り当てます。デフォルトのコスト値は、メディアごとに異なります。
- ポート コストの計算に `short` 方式を使用する場合、可能なポート コスト値は 1 ~ 65535 です。
 - ポート コストの計算に `long` 方式を使用する場合、可能なポート コストは値 1 ~ 2000000000 です。
- ポート コストを設定するには、次のコマンドを使用します。
- ```
set spantree portcost 2/3 12
```
- ステップ 4** PVST+ ポート プライオリティを設定します。
- PVST+ モードのスイッチポートにはポート プライオリティを設定できます。プライオリティ値が最も小さいポートは、すべての VLAN に対してフレームを転送します。使用可能なポート プライオリティ値は 0 ~ 63 です。デフォルトは 32 です。すべてのポートに同じプライオリティ値が設定されている場合、ポート番号が最も小さいポートがフレームを転送します。
- ポート プライオリティを設定するには、次のコマンドを使用します。
- ```
set spantree portpri 2/3 16
```
-

スパニング ツリー プロトコルの詳細情報

スパニング ツリー プロトコルの設定および推奨事項については、以下のリンクから詳細情報を参照してください。

- STP および IEEE 802.1s MST の設定
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spanntree.htm
- スパニング ツリー プロトコルの問題と関連する設計上の考慮事項
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800951ac.shtml
- FDDI 802.10 トランクの設定
http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007eeeb.html
- アベイラビリティ向上のための財務サービスの設計
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a008015a8ad.shtml
- Cisco Catalyst スイッチでのスパニング ツリーブリッジの設定
http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a00801ee706.html#71577

PVST+ 設定のデフォルト値

表 2-1 に、Cisco Catalyst 6000 デバイスでの PVST+ コンフィギュレーションのデフォルト値を示します。

表 2-1 Catalyst 6000 スイッチの PVST+ コンフィギュレーションのデフォルト値

機能	デフォルト値
VLAN 1	VLAN 1 に割り当てられたすべてのポート
イネーブル ステート	PVST+ はすべての VLAN に対してイネーブル
MAC アドレス リダクション	ディセーブル
ブリッジ プライオリティ	32768
ブリッジ ID プライオリティ	32769 (ブリッジ プライオリティに VLAN 1 の拡張システム ID を加算)
ポート プライオリティ	32
ポート コスト	<ul style="list-style-type: none"> • ギガビット イーサネット : 4 • ファスト イーサネット : 191 • FDDI/CDDI : 10 • イーサネット : 1002
デフォルトのスパニング ツリー ポート コスト モード	Short (802.1D)
ポート VLAN プライオリティ	ポート プライオリティと同じ。ただし PVST+ では VLAN ごとに設定可能
ポート VLAN コスト	ポート コストと同じ。ただし PVST+ では VLAN ごとに設定可能
最大エージング タイム	20 秒
ハロー タイム	2 秒
転送遅延時間	15 秒

VTP の設定

VTP を使用すると、スイッチド ネットワークでの管理作業が軽減されます。1 台の VTP サーバで新しい VLAN を構築する場合、その VLAN の情報は、ドメイン内のすべてのスイッチに配布されます。これにより、同じ VLAN をすべての場所で設定する必要がなくなります。VTP は、ほとんどの Cisco Catalyst ファミリー製品で使用できる、シスコ独自のプロトコルです。

VTP は、VLAN の設定を行い、その内容を複数のスイッチに対して配信するために使用されます。Campus Manager を介して VLAN を管理するためには、すべてのスイッチで VTP の設定を行う必要があります。VTP ドメインが設定され、各デバイスで VTP モードが定義される必要があります。

また、Campus Manager がドメインに VLAN を作成するためには、各 VTP ドメインの少なくとも 1 つのスイッチが、VTP サーバとして定義される必要があります。VTP トランスペアレント モードを使用するスイッチで確立された VLAN の検出は、Campus Manager 3.1 からサポートされています (VLAN を識別するために VTP ドメインに少なくとも 1 台のサーバを必要とする、旧バージョンでの制限は削除されました)。Campus Manager を使用すると、コマンドラインではなく、トポロジー サービス アプリケーションを介して VLAN を表示、作成、変更、および削除できます。



(注)

このプロトコルは、ネットワーク設計全体の一部としてイネーブル化および設定される必要があります。この項は、あくまでも参考としてお読みください。

Cisco Catalyst スイッチで VTP ドメインおよび VTP モードを設定するには、次のコマンドを使用します。各スイッチは、1 つの VTP ドメインにのみ対応します。

```
set vtp domain <name>
set vtp mode <client | server | transparent>
set vtp v2 <enable | disable>
```



(注)

set vtp v2 コマンドは、トークンリング ネットワークにおいて必要となります。VTP v2 は、トークンリング ネットワーク上で使用する必要があります。VTP バージョン 1 と 2 には互換性がないため、両方を同じドメインで実行することはできません。

各モードの説明は、次のとおりです。

- **サーバモード** : スイッチは、VLAN 設定を保持し、その内容を VTP ドメイン内のその他の全スイッチに対して配信します。
- **クライアントモード** : スイッチは VTP サーバから受信したアドバタイズと VLAN コンフィギュレーションを同期して、アドバタイズをネイバーに転送します。
- **トランスペアレントモード** : スイッチは、サーバからアドバタイズされる VLAN を共有しませんが、アドバタイズをネイバーに転送します。トランスペアレント スイッチ上に構築された VLAN は、そのスイッチに対してのみ有効になります。

ベスト プラクティスのための推奨事項

キャンパスのベスト プラクティスのために、キャンパスの安定性と予測可能性（特に STP などのプロトコルに対する）の重視を推奨します。慎重なアプローチを望まれる企業では、一般的な VTP サーバ / クライアント モデルではなく、VTP トランスペアレント モードを使用するか、または VTP をオフ（Catalyst OS 7.x）にすることを推奨します。

複数のスイッチにわたって同一の VLAN を作成できるという VTP の主な利点は、裏を返せばドメイン内のすべてのスイッチに対し、VLAN が自動的に拡張するのを助長するという点でもあり、必ずしも有益であるとは言えません。このため、実行されていない STP と、それに関する通知が複数のスイッチ間で交錯するというリスクが発生します。スパンニング ツリーが、プロトコルとして劣っているわけではありません。プロトコルが元々備えている機能が、望ましくないということなのです。

VTP クライアント / サーバ モデルのもう一つの主なリスクは、新しいサーバのバージョン機能によって、既存の VTP サーバが無効になり、そのドメイン内のすべてのスイッチから、新しいマスタ サーバにとって未知の VLAN が削除されてしまう可能性があることです。これらのリスクの一部は、VTP 認証、トランク クリア、およびトランク プルーニングによって軽減できますが、複雑性が増す分、あまり意義があるとは言えません。

Catalyst スイッチ ポートでのトランキングのイネーブル化

このプロトコルは、ネットワーク設計全体の一部としてイネーブル化および設定される必要があります。この項は、あくまでも参考としてお読みください。

トランキングは、複数の VLAN について、同一リンク（2 つのスイッチ間またはスイッチとルータ間）を介してトラフィックを転送する方法であり、これによって VLAN がネットワーク全体へと拡張されることとなります。トランキングを実行するために、リンクの両端のポートをトランク ポートとして設定して、ISL（スイッチ間リンク）または IEEE 802.1Q プロトコルをイネーブルにする必要があります。

ISL は、複数の VLAN からのトラフィックを 1 つのリンクに集約するために使用される、シスコ独自のプロトコルです。IEEE 802.1Q は、同様の機能を実行するための業界標準のプロトコルです。

トークン リング ネットワークでは、IEEE 802.1Q を使用する必要があります。

Catalyst スイッチ ポートでトランキングをイネーブルにするには、次のコマンドを使用します。

```
set trunk <module/port> on [vlans]
```

これにより、指定したモジュールまたはポートがトランク ポートとして確立され、ISL プロトコルがイネーブルになります。

オプションの **vlans** パラメータを使用すると、トランク内で許可される特定の VLAN の範囲を指定できます（有効な範囲は 1 ~ 1005）。

以下に例を示します。

```
set trunk 2/1 on 2-10
```

詳細については以下の URL にアクセスし、『Understanding and Configuring VLAN Trunk Protocol (VTP)』を参照してください。

<http://www.cisco.com/warp/public/473/21.html>



Cisco LAN Management Solution 2.5 のインストール要件

Cisco LAN Management Solution (LMS) のインストールは、Windows および Solaris OS (オペレーティングシステム) の米国版および日本語版でサポートされています。

Solaris OS のインストール要件

この項では、Solaris OS で LMS をインストールするための要件について説明します。

表 3-1 LMS Solaris Server の最少インストール要件

コンポーネント	最少要件
ハードウェア	1 GHz の Sun UltraSPARC IIIi
ソフトウェア	UltraSPARC IIIi : Solaris 2.8 または 2.9
使用可能なメモリ	UltraSPARC IIIi : <ul style="list-style-type: none">• 企業用ライセンスの場合 : 2 GB 以上の RAM• 大企業用ライセンスの場合 : 4 GB 以上の RAM
使用可能なディスク領域	<ul style="list-style-type: none">• UltraSPARC IIIi (ワークステーションおよびサーバ) : 80 GB• Unix ファイルシステムを推奨

推奨される Solaris ディスクレイアウト

Solaris ディスクでは、次のレイアウトを推奨します。

- /opt/CSCOPx パーティション

このパーティションでは、アプリケーションの実行ファイル、ライブラリ、およびデータベース ファイルを保持します。デバイス数、有効なデータの量、および syslog メッセージの数に比例してサイズが大きくなります。

- /var/adm/CSCOPx パーティション

このパーティションでは、ログ ファイル、デバイス コンフィギュレーション、ソフトウェア イメージ、およびエクスポートされたレポートを保持します。パーティションの拡大は、アーカイブされたコンフィギュレーションの数、デバッグの量、およびソフトウェア イメージの数によって異なります。

- /tftpboot パーティション

このパーティションでは、デバイスからダウンロード、またはデバイスにアップロードされたコンフィギュレーションおよびソフトウェア イメージを保持します。このパーティションは、最大の SWIM ジョブを処理できるサイズにする必要があります。

バックアップに関する推奨事項

シスコでは、バックアップ ファイルの保存には別のパーティション、または、できれば別のディスクを用いることを推奨します。バックアップ用のパーティションは、すべてのアプリケーション データベース (RME、ANI、DFM など) や、デバイス コンフィギュレーション、ソフトウェア イメージ、およびユーザ アカウントを保存するのに十分なサイズが必要です。バックアップ用のパーティションは、複数のリビジョンを許可する必要があります。また、必要時に備えて、すべてのバックアップ ファイルを検証することを推奨します。

Windows OS のインストール要件

この項では、Windows OS に LMS をインストールするための要件について説明します。

表 3-2 LMS Windows Server の最少インストール要件

コンポーネント	最少要件
ハードウェア	2.4 GHz または Pentium III プロセッサを搭載した IBM PC 互換機
ソフトウェア	次のいずれかが必要です。 <ul style="list-style-type: none"> • Service Pack 4 を適用した Windows 2000 Professional • Service Pack 4 を適用した Windows 2000 Server • Service Pack 4 を適用した Windows 2000 Advanced Server • Windows 2003 Standard Edition および Enterprise Edition
使用可能なメモリ	<ul style="list-style-type: none"> • 企業用ライセンスの場合：2 GB 以上の RAM • 大企業用ライセンスの場合：4 GB 以上の RAM
使用可能なディスク領域	<ul style="list-style-type: none"> • 80 GB 以上 • 仮想メモリ：4 GB • 大企業用ライセンスの場合：8 GB

LMS アプリケーションのインストールの推奨順序

LMS アプリケーションのインストールの推奨順序は、次のとおりです。

1. CiscoWorks Common Services 3.0 (CiscoView 6.1 を含む)
2. Resource Manager Essentials (RME) 4.0
3. Campus Manager (CM) 4.0
4. Device Fault Manager (DFM) 2.0
5. Internetwork Performance Monitor (IPM) 2.6



ヒント 唯一の要件は、CiscoWorks Common Services 3.0 をその他のアプリケーションをインストールする前にインストールすることです。CiscoWorks マシンに 1 つのアプリケーションのみをインストールする場合は、上記の推奨順序に従う必要はありません。

LMS アプリケーションで使用されるポート

LMS アプリケーションで使用されるポートの完全なリストについては、以下の URL にアクセスし、『Quick Start Guide for LAN Management Solution 2.5』の表 8 「LAN Management Solution Port Usage」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/lms25qsg.htm#wp65566

表 3-3 LMS アプリケーションで使用されるポート

プロトコル	ポート	サービス名	アプリケーション	接続の方向
ICMP		Ping	RME、CM、および DFM	サーバからデバイス
TCP	22	Secure Shell (SSH; セキュアシェル)	CiscoWorks Common Services および RME	サーバからデバイス
TCP	23	Telnet	Common Services	サーバからデバイス
TCP	49	TACACS+ および ACS	Common Services、RME、CM、および DFM	サーバから ACS、デバイスから ACS
TCP	80	HTTP	Common Services および CiscoView	クライアントからサーバ
TCP	514	Remote Copy Protocol (RCP)	Common Services	CiscoWorks サーバからデバイス
TCP	514	rsh デーモン	RME	サーバからデバイス
TCP	1683	Internet Inter-ORB Protocol (IIOP)	Common Services および CM	クライアントからサーバ
TCP	1684	IIOP	Common Services および CM	サーバからクライアント
TCP	1741	CiscoWorks HTTP プロトコル	Common Services、CiscoView、および RME	クライアントからサーバ
TCP	1742	SSL/HTTP ポート	Common Services	クライアントからサーバ
TCP	1783	IPM ゲートキーパの IIOP	IPM	クライアントからサーバ
TCP	1784	IPM ゲートキーパの IIOP	IPM	サーバからクライアント
TCP	8088	HIOP	Common Services	サーバからクライアント およびクライアントからサーバ
TCP	9002	DynamID 認証 (DFM ブローカ)	DFM	クライアントからサーバ
TCP	9088	IPM ゲートキーパの HIOP ポート	IPM	サーバからクライアント およびクライアントからサーバ
TCP	42352	ESS HTTP (代替ポートは 44352/tcp)	Common Services	クライアントからサーバ
TCP	44342	IPM ネームサーバ(OSAGENT)	IPM	クライアントからサーバ

表 3-3 LMS アプリケーションで使用されるポート (続き)

プロトコル	ポート	サービス名	アプリケーション	接続の方向
UDP	69	Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル)	Common Services および RME	サーバからデバイスおよびデバイスからサーバ
UDP	161	SNMP	Common Services、Cisco View、RME、CM、および DFM	サーバからデバイス
UDP	162	SNMP トラップ (標準ポート)	Common Services および DFM	デバイスからサーバ
UDP	514	Syslog	Common Services および RME	デバイスからサーバ
UDP	9000	CSlistener (ポート 162 が使用中の場合は DFM サーバ)	DFM	クライアントからサーバ
UDP	16236	UT ホスト 取得	CM	デバイスからサーバ

ライセンスに関する用語とプロセス

この項では、LMS 2.5 のソフトウェアベースの製品登録と、ライセンス キーのアクティベーションに関する用語およびテクノロジーについて説明します。

表 3-4 ライセンスに関する用語

ライセンス用語	説明
Product Identification Number (PIN)	PIN は、ソフトウェア使用許諾書に印刷されています。LMS のインストールプログラムでは、インストール時に PIN の入力を要求されます。インストール時に認証済みのライセンスを取得できない場合は、PIN を使用してインストールを続行します。PIN のみを入力した場合、LMS は正常に動作しますが、ライセンス登録を完了するよう、定期的にメッセージが表示されます。
Product Authorization Key (PAK)	PAK は、ソフトウェア使用許諾書に印刷されています。Cisco.com からライセンスを取得するには、PAK を使用します。製品のインストール時に限らず、LMS の使用中にはいつでも、ライセンス キーを取得して登録できます。
ライセンス ファイル	<p>Cisco.com の製品ライセンス エリアで LMS の購入を登録すると、ライセンス ファイルが提供されます。ライセンス ファイルを入手するには、PAK を入力する必要があります。</p> <p>Cisco.com の登録ユーザの場合は、次の URL にアクセスしてライセンス ファイルを入手してください。</p> <ul style="list-style-type: none"> http://www.cisco.com/go/license <p>Cisco.com の登録ユーザではない場合は、次のサイトにアクセスしてライセンス ファイルを入手してください。</p> <ul style="list-style-type: none"> http://www.cisco.com/go/license/public

ライセンスに関する注意事項

- CiscoWorks Common Services 3.0 を初めてインストールする場合、インストールプロセスでは PIN または PAK の登録は要求されません。
- 最初にインストールする LMS アプリケーションのインストール実行中に、LMS ライセンス情報を入力するように要求されます。LMS インストールプログラムでは、ライセンス ファイル、または PIN および PAK を登録するように要求されます。LMS の 1 つめのアプリケーションをインストールするときにライセンス情報を入力した場合、以降のアプリケーションのインストール時には入力する必要はありません。
- LMS の評価版をお使いの場合、90 日の評価期間中は製品を登録する必要はありません。

■ ライセンスに関する用語とプロセス



LAN Management Solution 2.5 サーバの初期設定

この章では、LAN Management Solution (LMS) サーバの初期設定について順を追って説明します。また、アプリケーションのデフォルト設定や、LMS サーバのすべてのデバイスを簡単に管理するための、アプリケーション設定の更新方法について説明します。

LMS アプリケーションでのアプリケーション モードの設定

LMS アプリケーションでアプリケーション モードの設定を行うと、Device Credential and Repository (DCR) からアプリケーションへの、デバイスおよびクレデンシャル情報のフロー制御に利用できるようになります。



(注) アプリケーションのユーザ インターフェイスごとに、アプリケーション モードを指定する必要があります。

LMS アプリケーション モードには、次の 2 つがあります。

- 手動モード
- 自動同期モード

手動モードでは、LMS アプリケーション (Campus Manager、Device Fault Manager、Resource Manager Essentials、および Internetwork Performance Monitor) は、DCR からデバイスの更新情報 (デバイスの追加、削除、およびクレデンシャルの更新) を自動的に取得しません。

自動同期モードでは、LMS アプリケーションは、DCR からデバイスの更新情報 (デバイスの追加、削除、およびクレデンシャルの更新) を自動的に取得します。デバイスの更新に応じて、各アプリケーションではデータ収集、パフォーマンスのモニタリング、および変更されたデバイスの障害のモニタリングが実行されることがあります。

- **Campus Manager (CM)** : デフォルトでは、CM は自動同期モードに設定されています。CM では、このアプリケーション モードをディセーブルにすることはできません。したがって、DCR に追加されたデバイスはすべて、アプリケーション モードを無効にするフィルタ (IP アドレス範囲、VTP ドメインなど) が設定されていないかぎり、自動的に CM で管理されるようになります。
- **Device Fault Manager (DFM)** : デフォルトでは、DFM も自動同期モードに設定されています。DCR に追加されたデバイスはすべて、自動的に DFM で管理されるようになります。DFM で自動同期モードをディセーブルにする手順は、次のとおりです。

■ プロトコル設定

- a. DFM のメニューから **Device Management > Device Selector** を選択します。
- b. **Synchronize with Device Credential Repository** オプションの選択を解除します。
 - Resource Manager Essentials (RME) : デフォルトでは、RME は自動同期モードに設定されています。DCR にインポートされたデバイスは、RME に自動的に追加されます。
RME で自動同期モードをディセーブルにする手順は、次のとおりです。
- a. RME のメニューから **Administration > Device Management** を選択します。
- b. **Automatically Manage Devices from Credential Repository** オプションの選択を解除します。
 - Internetwork Performance Monitor (IPM) : DCR からデータをインポートしたあと、IPM ソースおよびデータ コレクタを設定できます。手順については、「[Internetwork Performance Monitor へのデバイスのインポート](#)」(p.6-13) を参照してください。



ヒント

すべての LMS アプリケーションでのデバイス管理を簡単にするために、自動同期モードをイネーブルにしておくことを推奨します。

複数の CiscoWorks サーバが設置され、CiscoWorks サーバ間で多数のデバイスを管理する場合、手動モードをイネーブルにする必要があります。

DCR からデバイス情報を取得するために RME の自動同期モードがイネーブルになっている場合、2 台の異なるサーバにインストールされている RME の 2 つのインスタンスは、同じデバイスのグループを管理できます。このような 2 台の RME サーバから、異なるデバイスのグループを管理するには、ユーザの手作業による選択が必要です。

プロトコル設定

RME は、コンフィギュレーションおよびソフトウェア管理のために、さまざまなプロトコルも使用します。ネットワーク管理者は、構成管理およびソフトウェア管理のために RME で使用されるプロトコルを割り当てることができます。

構成管理

コンフィギュレーションのダウンロードおよび取得のために、Archive Management、Config Editor、NetConfig ジョブなどの構成管理アプリケーションに対してプロトコルと順序を設定できます。

使用可能なプロトコルは、次のとおりです。

- Telnet
- Trivial File Transport Protocol (TFTP; 簡易ファイル転送プロトコル)
- Remote Copy Protocol (RCP)
- Secure Shell (SSH; セキュア シェル)
- Secure Copy Protocol (SCP)
- Hyper Text Transfer Protocol Secured (HTTPS)

プロトコル順序の設定

Archive Management、Config Editor、および NetConfig の各コンフィギュレーション アプリケーションには、プロトコルの順序を設定できます。Config Management でプロトコルの順序を設定する手順は、次のとおりです。

-
- ステップ 1 RME のメニューから **Administration > Config Management** を選択します。
 - ステップ 2 **Application Name** ドロップダウン リストから目的のアプリケーションを選択します。
 - ステップ 3 **Add** または **Remove** をクリックしてプロトコル順序を選択したあと、**Apply** をクリックします。
-



ヒント サーバとデバイス間でセキュアな通信を行うには、SSH を使用します。

Software Management プロトコルの順序を指定する手順は、次のとおりです。

-
- ステップ 1 **Software Mgmt** をクリックします。
 - ステップ 2 コンテンツ テーブルから **View/Edit Preferences** を選択します。
 - ステップ 3 **Add** および **Remove** ボタンを使用して、プロトコル順序を選択します。
-

ソフトウェア イメージ管理

Software Management は、指定したプロトコル順序に基づいてソフトウェア イメージをダウンロードします。イメージをダウンロードする間、Software Management はリストの最初のプロトコルを使用します。リストの最初のプロトコルでのダウンロードが失敗した場合、Software Management がイメージをダウンロードするための伝送プロトコルを確立するまで、これらのジョブでは 2 番め以降のプロトコルを順に使用します。

サポートされているプロトコルは、RCP、TFTP、SCP、および HTTP です。

ソフトウェア イメージをダウンロードするために Software Management が使用するプロトコル順序を定義する手順は、次のとおりです。

-
- ステップ 1 RME のメニューから **Administration > Software Mgmt > View/Edit Preferences** を選択します。
 - ステップ 2 View/Edit Preferences ダイアログ ボックスで、プロトコル順序を定義します。
 - ステップ 3 **Add** および **Remove** ボタンを使用して、プロトコル順序を選択します。
-

セキュリティの設定

Cisco Secure ACS サーバと統合することで、LMS 2.5 は次のセキュリティ機能を提供します。

- デバイスへのユーザ アクセスを保護します。
- クライアントとしてのブラウザとサーバの通信を保護します。

証明書の設定

すべての CiscoWorks サーバでは、ユーザによって開始されないバックグラウンド タスクの実行の際に使用する、システム プロセスに対してのシステム ID ユーザを作成する必要があります。システム ID ユーザの作成は、CiscoWorks サーバのインストール時にデフォルトで行われます。

システム ID ユーザの設定

システム ID ユーザのデフォルト設定を確認したり、またはデフォルト設定を変更する手順は、次のとおりです。

-
- ステップ 1** CWHP > Common Services > Server > Security > Multi-Server Trust Management の順にメニューを選択します。
 - ステップ 2** System Identity Setup へのリンクを選択します。
 - ステップ 3** 必要な詳細情報を編集します。
-

ピア サーバ アカウントの設定

CiscoWorks サーバが、その他の CiscoWorks サーバと情報（デバイス クレデンシャルなど）を交換する必要がある場合、すべての CiscoWorks サーバに対してピア サーバ アカウントを設定する必要があります。ピア サーバ アカウントには、その他の CiscoWorks サーバのシステム ID ユーザ情報が必要です。

ピア サーバ アカウントは、サードパーティ製アプリケーションに CiscoWorks サーバへのアクセス権を与え、認証および許可を行う際にも使用します。ここで説明するとおりにピア サーバ アカウントを作成して、サードパーティ ユーザにクレデンシャル情報を付与します。

ピア サーバ アカウントを設定する手順は、次のとおりです。

-
- ステップ 1** 前の項で説明したように、システム ID ユーザを作成します。
 - ステップ 2** CWHP > Common Services > Server > Security > Multi-Server Trust Management の順にメニューを選択します。
 - ステップ 3** Peer Server Account Setup へのリンクを選択します。
 - ステップ 4** その他の CiscoWorks サーバのシステム ID ユーザが作成されたことを確認します。
-

LMS サーバでの HTTPS のイネーブル化

LMS サーバで HTTPS をイネーブルにすると、サーバとクライアント間のセキュアな通信を実行できます。

-
- ステップ 1** **Common Services > Server > Security > Ingle-Server Management** の順にメニューを選択して、サーバで SSL をイネーブルにします。
- ステップ 2** **Browser-Server Security Mode Setup** を選択します。
- ステップ 3** **Enable** を選択します。
-

注

- HTTPS 通信は、LMS サーバを再起動したあとから機能します。
- リンクまたはアプリケーション (あるいはその両方) の登録は、CiscoWorks セキュリティ モードを **http** から **https** に変更したあとから機能します。
- LMS サーバを再起動する手順は、次のとおりです。
 - Windowsサーバを使用している場合は、**net stop crmdmgtd** コマンドまたは **net start crmdmgtd** コマンドを実行します。
 - Solarisサーバを使用している場合は、**/etc/init.d/dmgtd stop** コマンドまたは **/etc/init.d/dmgtd start** コマンドを実行します。
- LMS サーバには、**https://server-url:1742** からアクセスします。

シングルサインオン

シングルサインオンは、1回の作業で複数のサーバにログインする機能で、パスワードの入力も1回で済みます。これは特に、多数の異なるサーバにアクセスする必要がある LAN または WAN 上のユーザなどにとって便利な機能です。

SSO モードでは、CiscoWorks サーバの1つが SSO 認証サーバまたはマスターとして機能し、その他の CiscoWorks サーバはすべてスレーブまたは通常の SSO サーバとして機能します。スレーブまたはマスターサーバにアクセスする場合、すべての認証はマスターサーバによって行われます。

このタスクはオプションであり、複数の CiscoWorks サーバ設定にのみ適用されます。

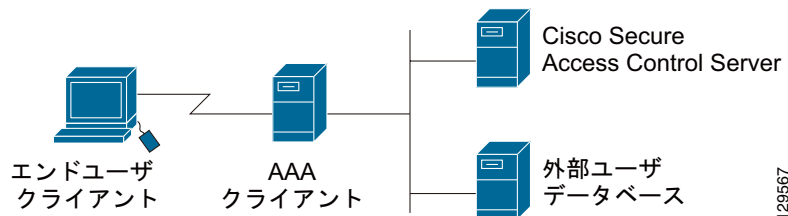
シングルサインオンを設定する手順は、次のとおりです。

-
- ステップ 1** 「**証明書の設定**」(p.4-4) を完了します。
- ステップ 2** CiscoWorks サーバの1つを認証サーバとして設定します。**CWHP > Common Services > Server > Security > Multi Server Trust Management** の順にメニューを選択します。
- ステップ 3** **Single Sign-on Setup** へのリンクを選択します。
- ステップ 4** **Master (SSO Authentication Server)** モードを選択します。
同じリンクを使用して、その他の CiscoWorks サーバをスレーブとして設定できます。
-

Cisco Secure Access Control Server の設定

Cisco Secure Access Control Server (ACS) は、ネットワーク アクセス サーバ、PIX セキュリティ アプライアンス、ルータなど、Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントティング) クライアントとして機能するネットワーク デバイスに AAA サービスを提供します。図 4-1 に AAA クライアント モデルを示します。

図 4-1 AAA クライアント モデル



LMS は ACS サーバと統合して、デバイスへのユーザ アクセスを制限するために AAA 機能を利用します。Common Services によって、冗長性をサポートするために、セカンダリおよび 3 次 ACS サーバを設定できるようになります。

LMS サーバと ACS の統合

LMS サーバと ACS を統合する手順は、次のとおりです。

LMS サーバでのシステム ID ユーザおよびピア サーバアカウント ユーザの設定

システム ID ユーザが設定されていることを確認する手順は、次のとおりです。

-
- ステップ 1** CWHP > Common Services > Server > Security > Multi-Server Trust Management の順にメニューを選択します。
 - ステップ 2** System Identity Setup へのリンクを選択します。
 - ステップ 3** LMS サーバと併用しているサードパーティ製のアプリケーションがある場合は、このときピア サーバアカウントを作成します。これは、サードパーティ製のアプリケーションには、システム ID 設定に関するクレデンシャルを認識させる必要がないためです。
-

ACS サーバの設定

ACS サーバを設定する手順は、次のとおりです。

-
- ステップ 1** ACS サーバにログインします。
 - ステップ 2** CiscoWorks LMSサーバをACSサーバのAAAクライアントとして追加するには、Network Configuration メニューから **Add Entry** を選択します。
 - ステップ 3** 設定する CiscoWorks LMS サーバの IP アドレスおよびホスト名を指定します。
 - ステップ 4** 秘密鍵を指定します。
 - ステップ 5** 認証方法として **TACACS+** を選択します。
 - ステップ 6** CiscoWorks LMS サーバを新しい NDG グループに割り当てます。

ステップ 7 新しいNDGグループを作成するには、Network Configurationメニューから **Add Entry** を選択します。

ステップ 8 ACS サーバの登録ユーザとしてシステム ID ユーザを追加します。

- a. **User Setup** を開きます。
- b. ユーザ名を入力して、**Add/Edit** をクリックします。
- c. **User Setup** セクションで、ユーザのパスワードを入力します。



(注) ユーザ登録で、LMS サーバに指定されたパスワードと同じパスワードが使用されていることを確認してください。

ステップ 9 グループを **Default Group** に追加して、下部フレームにある **Submit** をクリックします。



(注) その他のピアサーバユーザ名（特にサードパーティ製アプリケーションに対して作成されたユーザ）を ACS サーバに追加するには、同じ手順を実行する必要があります。

ACS サーバと通信するための LMS サーバの設定

ACS サーバと通信できるように LMS サーバを設定する手順は、次のとおりです。

ステップ 1 LMS サーバにログインします。

ステップ 2 CiscoWorks ホーム ページの Common Services Panel を開きます。

ステップ 3 Common Services が ACS ログイン モードになるように設定するには、**Server > Security > AAA Mode Setup > Select ACS Type** の順にメニューを選択します。

ステップ 4 プライマリ ACS サーバの IP アドレス、ACS 管理ユーザ名とパスワード、および共有秘密鍵を入力します。



(注) これらの各フィールドの値は、ACS サーバに登録された値と同じである必要があります。

ステップ 5 LMS サーバを再起動します。

- Windows サーバを使用している場合は、**net stop crmdmgtd** コマンドまたは **net start crmdmgtd** コマンドを実行します。
- Solaris サーバを使用している場合は、**/etc/init.d/dmgtd stop** コマンドまたは **/etc/init.d/dmgtd start** コマンドを実行します。

ACS サーバでのシステム ID ユーザの設定

この項では、LMS サーバが割り当てられているデバイスグループで、システム管理者権限をユーザグループに付与する手順について説明します。



(注) システム ID ユーザは特別な権限を持つユーザであり、ACS サーバで作成されるその他のユーザとは異なります。この設定とピアサーバユーザ設定の違いは、ピアサーバユーザ名には、NDG グループへの管理者権限を割り当てる必要がないという点だけです。

ACS サーバでシステム ID ユーザを設定する手順は、次のとおりです。

-
- ステップ 1 **Group Setup** を開きます。
 - ステップ 2 **User Group** を選択します。
 - ステップ 3 **Edit Settings** をクリックします。
 - ステップ 4 アプリケーション (CiscoWorks、CiscoView、RME、DFM、および CiscoWorks CM) の設定を閲覧して、LMS サーバを含むデバイス グループにシステム管理者権限を付与します。
-

ロール マッピングのデフォルト の権限およびタスクを変更するための ACS サーバの設定 (任意)

CiscoWorks で定義されているデフォルトのロールは、次の 5 つです。

- システム管理者
- ネットワーク管理者
- ネットワーク オペレータ
- アプルーバ
- ヘルプ デスク

これらのロールにはデフォルトで、CiscoWorks のさまざまなタスクへの権限が割り当てられています。ACS ユーザは、必要に応じてロール マッピングのタスクを変更できます。

-
- ステップ 1 ACS サーバにログインします。
 - ステップ 2 ロール マッピングのタスクを変更するには、左側のナビゲーション バーにある **Shared Profile Components** をクリックします。
 - ステップ 3 ロール マッピングのタスクを設定する必要があるアプリケーションを選択します。
たとえば、**CiscoWorks Common Services** をクリックして、続いてユーザ ロールをクリックし、そのロールに割り当てられたタスクを変更します。
-

ネットワーク デバイス グループ、ユーザ グループの作成と ACS サーバでのネットワーク デバイス グループへのロールの割り当て

ネットワーク デバイス グループおよびユーザ グループを作成して、そのグループにロールを割り当てる手順は、次のとおりです。

-
- ステップ 1 ACS サーバにログインします。
 - ステップ 2 ネットワーク デバイス グループを作成するには、左側のナビゲーション バーにある **Network Configuration** をクリックします。
 - ステップ 3 デバイスをネットワーク デバイス グループに追加します。
 - ステップ 4 ユーザをユーザ グループに追加するには、**Group Setup** をクリックしてから **Users in Group** をクリックします。
 - ステップ 5 さまざまなネットワーク デバイスに対してユーザ グループ権限 (システム管理者、ネットワーク管理者など) を割り当てるには、**Group Setup** をクリックしてから **Edit Settings** をクリックします。
-

デバイスでタスクを実行するための権限の設定

セキュリティ管理者が、LMS サーバのデバイスに対して、ユーザが特定のタスクのセット（この例では、タスク t1、t2、t3）だけを実行できるように制限する手順は、次のとおりです。

-
- ステップ 1** LMS サーバを ACS セキュリティ モードにします。
 - ステップ 2** 「Cisco Secure Access Control Server の設定」(p.4-6) の説明に従って、Cisco Secure ACS サーバを設定します。
 - ステップ 3** ACS サーバにログインします。
 - ステップ 4** ロール（ここでは、ネットワーク管理者）が有効になっており、制限されたタスクのリストのみに実行権限を持っていることを確認します。
 - ステップ 5** **Shared Profile Components** をクリックして、タスク t1、t2、および t3 が存在するアプリケーションを選択します。
 - ステップ 6** **Network Administrator** をクリックして、このロールに対してタスク t1、t2、および t3 のみをイネーブルにします。
 - ステップ 7** **Group Setup** をクリックして、ユーザを割り当てるユーザグループを選択します。
 - ステップ 8** **Edit Settings** をクリックして、タスク t1、t2、および t3 が存在するアプリケーション設定を開き、前のステップで選択したユーザに **Network Administrator** ロールを割り当てます。
-

■ デバイスでタスクを実行するための権限の設定



Cisco LAN Management Solution 2.5 でのデバイスの認識

第 4 章「LAN Management Solution 2.5 サーバの初期設定」で説明したタスクによって、LAN Management Solution (LMS) サーバの初期設定は完了されているとします。次に、LMS への管理用デバイスのインポートを行います。

次の 3 つのタスクのいずれかを使用して、LMS サーバでデバイスを認識できます。

- [Campus Manager のデバイス検出 \(p.5-1\)](#)
- [Device and Credentials Repository へのバルク デバイス インポート \(p.5-2\)](#)
- [デバイス クレデンシャルの更新 \(p.5-3\)](#)

Campus Manager のデバイス検出

Campus Manager には、Cisco Discovery Protocol (CDP) を使用して、ネットワーク内のシスコ製デバイスを検出する機能があります。したがって、Campus Manager を使用してデバイス検出を実行するには、ネットワークで CDP をイネーブルにする必要があります。ネットワークで CDP がイネーブルになっている場合、Campus Manager に 1 つまたは複数のシード デバイスを入力できます。



(注)

シード デバイスは通常、コア デバイスである必要があります。すべてのコア スイッチは、シード デバイスである必要があります。コア スイッチには多数の CDP ネイバーが接続されるため、検出プロセスが迅速化されます。

LMS 2.5 では、Campus Manager の処理は 2 つのプロセスに分けられます。1 つは**デバイス検出**、もう 1 つは**キャンパス データ収集**です。

Campus Manager のデバイス検出では CDP を使用して、シード デバイスを通じてネットワークを検出します。デバイス検出プロセスでは、Campus Manager は、ネットワークで検出されたデバイスのリストを Device and Credentials Repository (DCR) に登録します。デバイスに関する情報は、データ収集プロセスでのみ Campus Manager によって取得されます。

デバイスのリストを収集するには、まずデバイス検出プロセスを開始する必要があります。

Campus Manager でのシード デバイスの定義

Campus Manager でシード デバイスを定義する手順は、次のとおりです。

ステップ 1 **Administration** を選択します。

ステップ 2 リンクの **SNMP Settings** を選択します。



(注) SNMP 設定のページには、リード (read) コミュニティストリングのみを入力する必要があります。ネットワークで設定されたコミュニティストリングの数によって、**Add** または **Edit** をクリックしてリード コミュニティストリングの追加と編集を行います。デフォルトでは、*SNMPv2* リードストリングのみが登録されます。

ステップ 3 SNMPv3 を登録するには、**SNMPV3** ラジオ ボタンを選択します。

ステップ 4 SNMP ストリングを編集したあと、SNMP 設定画面で **Apply** をクリックします。

ステップ 5 シード デバイスを入力するには、TOC の下のリンク、**Discovery Settings** をクリックします。

ステップ 6 シード デバイスを設定して **Apply** をクリックします。

このアクションにより、デバイス検出プロセスがただちに開始されます。

アドレスフィルタを使用すると、特定のネットワーク内のデバイスを検出または検出しないように指定できます。

ステップ 7 アドレスフィルタを設定するには、**IP Address Range** をクリックします。



(注) デバイス検出がスケジュール化されている場合、LMS 内のデバイスは、Campus Manager のデバイス検出が行われたあとから認識されます。

ステップ 8 デバイス検出ステータスを確認するには、リンクの **Go to Campus Administration** をクリックします。

ステップ 9 ページの再読み込みをしてデバイス検出ステータスを更新し、アイドル状態のときに検出されたデバイスの数を確認します。

Campus Manager によって検出されたデバイスはすべて、この時点で DCR に登録されています。

Device and Credentials Repository へのバルク デバイス インポート

LMS では、DCR へのバルク インポートもサポートされています。

バルク デバイス インポートを実行するには、**CWHP > Common Services > Device Management > Bulk Import** の順にリンクを選択します。

DCR へのバルク インポートは、次の 3 つの形式のいずれかを使用して実行できます。

- **ファイル インポート**

File オプションを選択し、CSV または XML ファイルからデバイスをインポートします。

入力ファイルの形式は、オンライン ヘルプで指定された形式である必要があります。この方法では、デバイス名および IP アドレスとともに、すべてのデバイス クレデンシャルがインポートされます。

インポートされたデバイスにデバイス タイプが関連付けられていない場合は、グループ `/CS@server-name/ System Defined Groups/Unknown Device Type` に追加されます。

Device Management 画面でデバイスを選択して **Edit** をクリックすると、デバイスにデバイス タイプを割り当てることができます。

- ローカル NMS

CiscoWorks サーバと同じマシンにインストールされている HP OpenView Network Node Manager 6.x または IBM Tivoli NetView 7.x からデバイスをインポートするには、**Local NMS** オプションを選択します。HP OpenView NNM 6.x または IBM Tivoli NetView 7.x のインストール場所を指定する必要があります。

- リモート NMS

CiscoWorks サーバと異なるマシンにインストールされている HP OpenView Network Node Manager 6.x または IBM Tivoli NetView 7.x からデバイスをインポートするには、**Remote NMS** オプションを選択します。



(注)

LMS 2.5 では、デバイスのインポートは、RSH プロトコルをサポートするリモートの Unix NMS サーバまたはリモートの Windows NMS サーバからのみ実行できます。

インポートされたデバイス クレデンシャルの編集

Local NMS または **Remote NMS** オプションを使用してデバイスがインポートされたあと、該当するデバイスが属するグループを選択し、Device Management 画面から **Edit** をクリックして、これらのデバイスのクレデンシャルを編集できます。



ヒント

ネットワークで CDP が有効になっている場合は、Campus Manager のデバイス検出を使用して、シスコ製デバイスを認識させることを推奨します。

デバイス クレデンシャルの更新

LMS のすべての機能を利用するには、SNMP 読み取り用クレデンシャル以外のデバイス クレデンシャルを DCR に登録する必要があります。

DCR でクレデンシャルの更新を実行する手順は、次のとおりです。

ステップ 1 **CWHP > Common Services > Device and Credentials > Device Management** の順にリンクを選択します。

ステップ 2 **CS@server-name** グループにチェックをして CS グループのすべてのデバイスを選択し、**Edit** をクリックします。



ヒント

後続の画面のデバイスは選択しないでください。

ステップ 3 **Next** をクリックします。デフォルトでは、すべてのデバイスが選択されます。

ステップ 4 デバイス クレデンシャルを入力して、**Finish** をクリックします。

ステップ 5 デバイスの **ユーザ フィールド** に入力する必要がある場合は、**Next** をクリックして、最大 4 つまでユーザ定義フィールドを入力します。

すべてのデバイスで同じクレデンシャルを使用する場合は、上記の手順を使用してクレデンシャルを編集します。ユーザ定義フィールドを追加することもできます。

ステップ 6 ただし、デバイスに異なるクレデンシャルがある場合は、**CWHP > Common Services > Groups** の順にリンクを選択して、同じクレデンシャルを使用するデバイスのグループを作成します。

ステップ 7 **CS@server-name/User Defined Groups** グループの下にグループを作成します。

デバイス管理

デバイス検出機能は、LMS にデバイスを認識させるだけです。ネットワーク上のコンフィギュレーション ファイル、ソフトウェア イメージなど、デバイスに関する追加情報は別途追加する必要があります。LMS 内のすべてのアプリケーションでは、インポートされたデバイスが登録されます。

DCR から RME へのデバイスの追加

RME が自動同期モードに設定されていない場合、次の手順のいずれかを使用すると、DCR から RME にデバイスを追加できます。

- DCR に追加されたすべてのデバイスを RME で管理する場合は、RME の自動同期オプションをイネーブルにする必要があります。

次のいずれかの方法で、自動同期をイネーブルにします。

- a. CiscoWorks ホーム ページを開き、**RME > Administration > Device Management > Device Management Settings** の順にリンクを選択します。
- b. **Automatically Manage Devices from Credential Repository** をチェックします。

- DCR に登録されたデバイスの一部だけを RME で管理する場合は、自動同期オプションをオフのままにしておきます。

デバイスが Campus Manager のデバイス検出またはサードパーティ製の NMS によって認識され、RME の自動同期オプションがイネーブルになっている場合、コンフィギュレーションの収集に必要なクレデンシャル (SNMP 書き込み、Telnet/SSH) を LMS で使用できないため、最初のデバイスのコンフィギュレーション収集は失敗します。

RME のコンフィギュレーション収集ステータスの表示

RME のコンフィギュレーション収集ステータスを表示する手順は、次のとおりです。

1. **CWHP > Resource Manager Essentials > Config Management > Archive Management** の順にリンクを選択します。
2. アーカイブ処理に失敗したデバイスのリストを表示するには、リンクの **Number of Failed Devices** をクリックします。

LMS でクレデンシャルが更新されているため、同期操作を行ってから、管理対象デバイスのコンフィギュレーション ファイルを収集しなければならない場合があります。

デバイスの起動および実行コンフィギュレーションの収集

デバイスの起動および実行コンフィギュレーションを収集する手順は、次のとおりです。

-
- ステップ 1** TOC > Sync Archive に移動します。
- ステップ 2** 同期アーカイブ ジョブをスケジューリングする必要があります。これを実行するには、**RME@server-name** グループに属するデバイスを選択します。
- ステップ 3** **Fetch Startup Config** をチェックします。
- これは、最初の同期アーカイブ処理に失敗したデバイスに対してのみ実行できます。
-

これらの手順を実行すると、サーバでは管理対象のデバイスが認識されます。アプリケーションが正しく動作していることを確認するには、次の項で説明する確認プロセスを実行します。

LMS アプリケーションでのデバイス インポート ステータスの確認

この項では、Resource Manager Essentials (RME)、Campus Manager、および Device Fault Manager (DFM) でのデバイス インポート手順の確認について説明します。

Resource Manager Essentials

この項では、次の RME デバイス確認タスクについて説明します。

コンフィギュレーション ファイル収集の確認

コンフィギュレーション ファイルが収集されたかどうかを確認する手順は、次のとおりです。

1. ジョブ ステータスを確認するには、**Config Management** を開き、リンクの **Archive Management** を選択します。
 2. アーカイブ収集ステータスまたはジョブの詳細を表示するには、画面を更新します。
-

デバイス クレデンシャルの確認

デバイス クレデンシャルを確認する手順は、次のとおりです。

1. **Resource Manager Essentials > Devices > Device Management > Device Credential Verification** の順にリンクを選択して、デバイス クレデンシャルを確認します。
 2. チェックするデバイス クレデンシャルの種類を確認するには、**Check Device Credential** をクリックします。
 3. レポートを表示して、デバイス クレデンシャルが正しいかどうかを確認するには、**View Credential Verification Report** をクリックします。
 4. デバイスのクレデンシャルを変更する必要がある場合は、**Edit Device Credentials** をクリックします。
-

Campus Manager

Campus Manager でデバイスの現在のステータスを取得する手順は、次のとおりです。

CWHP > Campus Manager > Administration の順にリンクを選択します。

- **Device Discovery** の下に、デバイスの検出ステータスが表示されます。
- **Data Collection** の下に、デバイスのデータ収集ステータスが表示されます。

Device Fault Manager

DFM でデバイスの現在のステータスを取得する手順は、次のとおりです。

CWHP > Device Fault Manager > Device Management > Discovery Status に移動します。

- デバイスのステータスは**既知**である必要があります。
- DFM 処理は**アクティブ**である必要があります。



Cisco LAN Management Solution 2.5 でのサーバ管理

この章では、サーバのリソースを最適に利用するために、既存のネットワークトポロジーの状態を維持しつつ、サーバ管理とコンフィギュレーション設定を行う方法について説明します。

Common Services

Common Services は、CiscoWorks アプリケーションがデータとシステム リソースを共有するための運用基盤を提供します。また、CiscoWorks アプリケーションを起動するための共通のデスクトップや同時ログイン、ユーザ ロール定義、およびアクセス権限を利用できるようになります。CiscoWorks Common Services 3.0 の定期的な更新ファイルは、ダウンロードによって入手できます。インストールガイドおよびユーザガイドについては、以下のマニュアルを参照してください。

- Solaris 用『Installation and Setup Guide for CiscoWorks Common Services 3.0』(CiscoView を含む)
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00801e8b87.html
- Windows 用『Installation and Setup Guide for CiscoWorks Common Services 3.0』(CiscoView を含む)
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00801e8b8a.html
- 『User Guide for CiscoWorks Common Services 3.0』
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a00801e8b82.html

ユーザ定義グループの作成

Common Services のデバイスのグループ化作業では、Device and Credentials Repository (DCR) によって定義されるデバイスの **User Defined** フィールドに基づいて、ユーザ定義グループを作成します。このグループを Resource Manager Essentials (RME)、Campus Manager、Device Fault Manager (DFM)、または Internetwork Performance Monitor (IPM) で使用し、そのアプリケーションに関連するツールを起動できます (同様に、LAN Management Solution [LMS] 2.5 の各アプリケーションでもユーザ定義グループを作成できます)。

ユーザ定義グループを作成する手順は、次のとおりです。

-
- ステップ 1** CWHP > Common Services > Groups の順にリンクを選択します。
 - ステップ 2** リンクの **Group Admin** を選択します。
 - ステップ 3** Group Administration ウィンドウで、グループ セレクタから **/CS@server-name/User Defined Groups** を選択して、**Create** をクリックします。
 - ステップ 4** グループ名を入力して **Next** をクリックします。
 - ステップ 5** **Variable** ドロップダウン ボックスを選択します。
Variable フィールドの値は、**user_defined_field_0**、**user_defined_field_1**、**user_defined_field_2**、および **user_defined_field_3** の 4 つのいずれかです。
 - ステップ 6** オペレータおよび DCR のデバイスの値と一致する値を選択して、**Add Rule Expression**、**Next** の順にクリックします。
基準に一致するすべてのデバイスが右側のパネルに表示されます。
 - ステップ 7** **Next** をクリックします。
 - ステップ 8** **/CS@server-name/User Defined Groups** の下に新しいグループを作成するには、**Finish** をクリックします。
この新しく作成されたグループには、LMSのどのアプリケーション画面からでもアクセスできます。
-

LMS データのバックアップ

シスコでは、バックアップ データは、LMS がインストールされているディレクトリ (デフォルトでは Windows または Solaris の NMSROOT ディレクトリ) に保存しないことを推奨します。DCR マスター / スレーブ モードもバックアップされることに注意します。

LMS データをバックアップする手順は、次のとおりです。

-
- ステップ 1** CWHP > Common Services > Admin の順にリンクを選択します。
 - ステップ 2** リンクの **Backup** を選択します。
 - ステップ 3** バックアップ ディレクトリ名は指定できます。
バックアップ ジョブは、ただちに実行するか、スケジューリングして実行するかを選択できます。
-

LMS データの復元

LMS データの復元は、コマンドライン インターフェイスからのみ実行できます。LMS データのバックアップおよび復元手順の詳細については、以下の URL にアクセスして『LAN Management Solution Data Migration Guidelines』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/dmgl_rm.htm

-
- ステップ 1** LMS サーバにログインします。
- ステップ 2** デーモン マネージャをシャットダウンします。
- Windows サーバの場合：**net stop crmdmgtd** コマンドを実行します。
 - Solaris サーバの場合：**/etc/init.d/dmgtd stop** コマンドを実行します。
- ステップ 3** ディレクトリを **NMSROOT/bin** に変更します。
- ステップ 4** スクリプト **restorebackup.pl** を実行します。
-

Campus Manager

Campus Manager 4.0 では、検出メカニズムは次の 3 つに分類されます。

- デバイス検出
- データ収集
- ユーザ追跡メジャー収集

Campus Manager のデバイス検出

デバイス検出は、あらかじめ決められたスケジュールで実行するか、オペレータの操作によって開始できます。



(注) デバイスの検出を行っただけでは、Campus Manager ではデバイスは管理されません。

以下に、デバイス検出に関する主なポイントを示します。

- デバイス検出機能では、検出メカニズムとして Cisco Discovery Protocol を使用して、ネットワーク検出を実行します。
- デバイス検出機能では、デバイスの管理 IP アドレスを決定します。
- デバイス検出プロセスでは、DCR 内のデバイスと、ユーザが Campus Manager から設定したシード デバイスが使用されます。検出された次の情報が DCR に登録されます。
 - ホスト名
 - ドメイン名
 - 管理 IP アドレス
 - 表示名
 - sysObjectID
 - SNMP クレデンシャル

ネットワーク検出の最適化

ネットワークの検出を最適化するには、次のタスクを実行します。

IP フィルタの設定

特定のサブネットのみを検出する必要がある場合は、IP フィルタを設定します。IP アドレス フィルタは、検出する必要があるデバイス内の IP アドレスの範囲を決定するために利用できます。通常、この IP アドレスの範囲は同じサブネット内にあります。

IP フィルタを設定する手順は、次のとおりです。

1. **Campus Manager Administration > Admin > Device Discovery > Discovery Settings** の順にリンクを選択します。
 2. **IP Address Range** の下にある、**Configure** をクリックします。
-

DNS 参照のディセーブル化

DNS 参照によってデバイス検出が遅くなる可能性があるため、DNS 参照はディセーブルにできません。

DNS 参照をディセーブルにする手順は、次のとおりです。

1. **Campus Manager Administration > Admin > Device Discovery > Discovery Settings** の順にリンクを選択します。
 2. **DNS Lookup** チェックボックスの選択を解除します。
-

デバイス検出のトラブルシューティング

デバイス検出のトラブルシューティングを行う手順は、次のとおりです。

1. **CWHP > Campus Manager Administration > Reports > Discovery Reports** の順にリンクを選択し、**Campus Manager Panel** を開きます。
 2. 正常に検出されたデバイスで、SNMP 設定が正しいかどうかを確認します。
 3. ログ ファイル内に SNMP タイムアウトによる例外がある場合、**SNMP Timeout** および **Retry** の値を増やすことができます。
-

Campus Manager のデータ収集

データ収集は、あらかじめ決められたスケジュール、またはオペレータのアクションによって実行できます。

以下に、Campus Manager のデータ収集に関する主なポイントを示します。

データ収集には、DCR 内のデバイスのリストおよび対応するクレデンシャルが使用されます。

DCR に登録されているデバイスのみが管理対象となります。デバイスが DCR に登録されていない場合、Campus Manager で管理することはできません。

フィルタリング メカニズムを適用すると、DCR 内のデバイスの一部だけを管理できます。フィルタリングは、IP アドレスまたは VTP (VLAN トランク プロトコル) ドメインに基づいて実行されます。

データ収集の最適化

ネットワーク内のデバイスのデータ収集を最適化するには、次のタスクを実行します。

IP アドレスまたは VTP ドメイン フィルタの設定

IP アドレスまたは VTP ドメイン フィルタを設定できます。

Campus Manager Administration > Admin > Campus Data Collection > Data Collection Filters の順にリンクを選択します。

デバイス数に基づく最適化

- 5,000 を超えるデバイスについてデータ収集が行われる場合、ANIServer プロセス (Java ベース) のスレッシュホールドは 1,024 MB に達します。
- 5,000 近くのデバイスについてデータ収集が行われる場合、シスコでは ANIServer のヒープ サイズを **-Xmx1024m** から **-Xmx1280** に増やすことを推奨します。

ヒープ サイズを変更します。ANIServer のヒープ サイズを変更するには、**NMSROOT/objects/dmgt/dmgt.conf** ファイルを編集します。

このファイルには、ANIServer プロセスを開始するためのエントリがあります。このエントリには、文字列 **-Xmx1024m** が含まれています。この文字列を **-Xmx1280m** に変更します。



(注) **dmgt.conf** ファイルの編集は、LMS サーバをシャットダウンしたあとに実行できます。**dmgt.conf** ファイルの編集が完了したあと、LMS サーバを再起動する必要があります。

ユーザ追跡モジュール

Campus Manager のデータ収集機能以外に、Campus Manager のユーザ追跡モジュールでも、ネットワーク内のエンド ホスト、IP フォン、およびサブネットに関するデータを収集できます。ユーザ追跡での収集は、主に 2 つのタイプがあります。

- メジャー収集**：ネットワーク内のエンド ホスト、Cisco IP Phone、およびサブネットに関するデータを収集します。
- マイナー収集**：エンド ホストおよび IP フォンをポーリングして、ユーザ追跡のデータを最新の状態に保ちます。

UT メジャー検出の開始

- CWHP > Campus Manager > User Tracking > Admin > Acquisition** の順にリンクを選択します。
- UT Major Discovery** を開始します。

次に、メジャー収集の際に選択できる重要なオプションのリストを示します。

- Enable User Tracking for DHCP environment**：IP アドレスが変更された場合にエンド ホストを追跡します。
- Use DNS to resolve host names**：ホスト名を解決します。
- IP phone acquisition on dot1q trunks for IOS switches**：Voice VLAN の設定中に、スイッチに接続されているエンド ホストを取得します。

メジャー収集のスケジュールの設定

メジャー収集を実行するスケジュールを設定する手順は、次のとおりです。

1. **Campus Manager > User Tracking > Admin > Acquisition** の順にリンクを選択します。
2. リンクの **Schedule Acquisition** を選択します。

サブネット内の IP アドレスでの ping スイープ

メジャー収集を開始する前に、サブネット内のすべての IP アドレスで ping スイープをイネーブルにできます。ping スイープから特定のサブネットを除外するオプションもあります。

削除ポリシー

必要に応じて、またはメジャー収集後指定された間隔で、ユーザ追跡からエンド ホストおよび IP フォンを削除できます。以下のリンクから、削除を実行します。

CWHP > Campus Manager > User Tracking > Admin > Acquisition > Delete Interval

特定の日付より古いアーカイブまたはジョブを削除することもできます。以下のリンクから、削除を実行します。

CWHP > Campus Manager > User Tracking > Admin > Reports > User Tracking Purge Policy

Campus Manager 内の階層型グループ

階層型グループを使用すると、ユーザは、ユーザ定義グループに実装されたトポロジーを視覚化できます。階層型グループは、トポロジー グループの一番上に作成されます。

-
- ステップ 1** **CWHP > Campus Manager** の順にリンクを選択します。
 - ステップ 2** リンクの **Topology Services** を選択します。
 - ステップ 3** 表示されたウィンドウで **Topology Groups** を選択して、**/Campus@server-name/System Defined Groups** を右クリックします。
 - ステップ 4** **Display View** オプションを選択します。
- 近接した 3 つのサブグループがマップとして表示されます。マップをクリックすると、2 つのマップ間の集約リンクを表示できます。このビューには、対象となる 2 つのマップ内に含まれるすべてのデバイス間の集約リンクが表示されます。
-

Resource Manager Essentials

この項では、RME の LMS サーバ管理タスクについて説明します。

インベントリ収集とポーリング

RME をインストールすると、インベントリ収集とポーリングの両方に対してシステム ジョブが作成され、それぞれデフォルトのスケジュールで実行されるようになります。定期的なインベントリ収集ジョブは、All Devices グループ内のすべてのデバイスからインベントリ データを収集し、インベントリ データベースを更新します。定期的なポーリングは、インベントリ内の変更を確認するためにすべてのデバイスをポーリングし、変更があった場合にのみインベントリ データベースを更新します。

デフォルトでは、インベントリ収集ジョブの周期は週に 1 回、ポーリング ジョブの周期は 1 日に 1 回です。



ヒント ポーラーは全デバイスのほぼすべての変更について、ネットワークと LMS サーバにはほとんど影響を与えずに検出を実行します。

ジョブ スケジュールのデフォルト 設定の変更

デフォルト設定を変更する手順は、次のとおりです。

- ステップ 1** **Resource Manager Essentials > Administration > Inventory > System Job Schedule** の順にリンクを選択します。
System Job Schedule ダイアログ ボックスに、現在の収集またはポーリング スケジュールが表示されます。
- ステップ 2** 必要に応じて値を変更して、**Apply** をクリックします。

コンフィギュレーション ファイルの収集とポーリング

コンフィギュレーション アーカイブは、定期的なコンフィギュレーションの収集（コンフィギュレーションのポーリングあり、またはなし）によってコンフィギュレーションの変更に対する更新を行います。

定期的なコンフィギュレーション アーカイブをイネーブルにする手順は、次のとおりです。

Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Collection Settings の順にリンクを選択します。



(注) デフォルトでは、定期的な収集とポーリングはディセーブルになっています。これは、お客様のネットワークでトラフィックのバーストが散発して、ネットワーク管理操作のために既存の帯域幅を使用できない場合があるためです。定期的な収集とポーリングを適用することを推奨します。

コンフィギュレーションの収集とポーリングのタイミングおよび方法の指定

次のオプションのどちらか一方、または両方を選択すると、コンフィギュレーション アーカイブにコンフィギュレーション ファイルを取り込む方法とタイミングを変更できます。

- **定期的なポーリング**

コンフィギュレーション アーカイブはデバイスで SNMP クエリを実行し、デバイスで検出されたコンフィギュレーションに変更がない場合、コンフィギュレーションは取得されません。

- **定期的な収集**

変更を確認せずにコンフィギュレーションが取得されます。

定期的なポーリング、定期的な収集、またはその両方を指定する手順は、次のとおりです。

1. **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Collection Settings** の順にリンクを選択します。
2. これらのオプションの 1 つまたは両方を選択します。

コンフィギュレーションの取得と適用に使用されるデフォルトの Protokol

コンフィギュレーションの取得と適用には、さまざまな Protokol が使用されます。システムでは、コンフィギュレーション ファイルを取得または適用するためにデバイスで使用される Protokol が、あらかじめ規定されています。使用する Protokol の順序は変更でき、Protokol の順序がネットワークに適していない場合は、リストから一部の Protokol を削除したりできます。

使用される Protokol のデフォルトのリストにアクセスして変更する手順は、次のとおりです。

ステップ 1 **Resource Manager Essentials > Administration** の順にリンクを選択します。

ステップ 2 リンクの **Config Mgmt** を選択します。

RME の削除ポリシー

この項では、構成管理、Syslog メッセージ、および変更監査データに関する RME の削除ポリシーについて説明します。

コンフィギュレーション ファイルを削除するタイミングの指定

アーカイブされたコンフィギュレーションを削除するタイミングを指定できます。これにより、ディスク領域が解放され、アーカイブを管理しやすいサイズに保つことができます (デフォルトでは、削除ジョブはディセーブルになっています)。コンフィギュレーション ファイルは、次の 2 つの基準に基づいて削除できます。

- **期間** : 指定した日数より古い設定が削除されます。
- **保存対象の各コンフィギュレーションの最大バージョン数** :

最大数に達した時点で最も古いコンフィギュレーション ファイルが削除されます。たとえば、最大保存バージョン数を 10 に設定すると、11 番目のバージョンのコンフィギュレーションがアーカイブされた時点で最初のバージョンが削除され、アーカイブされたバージョンの合計数を 10 に保ちます。

ステップ 1 **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Purge Settings** の順にリンクを選択します。

Archive Purge Setup ダイアログ ボックスが表示されます。

ステップ 2 **Enable** を選択します。

ステップ 3 削除ジョブをスケジューリングするには、**Change** をクリックします。

ステップ 4 アーカイブからコンフィギュレーション ファイルを削除するタイミングを指定するには、次のオプションの一方または両方を選択します。

- **Maximum Versions** : 保持するコンフィギュレーション ファイルの数を入力します。
- **Purge Versions Older Than** : 数値を入力して、日数、週数、または月数を選択します。
- **Purge Labeled Files** : ラベル付きのコンフィギュレーション ファイルを削除します。

Maximum versions to retain と **Purge versions older than** の両方に値が入力されている場合のみ、ラベル付きファイルが削除されます。



ヒント コンフィギュレーション ファイルの削除オプションについては、最大バージョン数と最大期間（日数、週数、または月数）の両方の値を指定することを推奨します。

ステップ 5 **Apply** をクリックします。

Syslog メッセージの定期的な削除

Syslog メッセージを定期的に削除するために、デフォルトのポリシーを指定できます。

Syslog メッセージのデフォルトの削除ポリシーを指定する手順は、次のとおりです。

ステップ 1 **Resource Manager Essentials > Administration > Syslog > Set Purge Policy** の順にリンクを選択します。

ステップ 2 **Purge records older than** フィールドに日数を指定します。

ここで指定した日数より古いレコードのみが削除されます。デフォルト値は 7 日です。

変更監査データの削除

変更監査データの定期的な削除または強制削除をスケジューリングできます。これによりディスク領域が解放され、変更監査データを管理しやすいサイズに保つことができます。

ステップ 1 **Resource Manager Essentials > Administration > ChangeAudit > Set Purge Policy** の順にリンクを選択します。

ステップ 2 各フィールドに値を入力します。

ステップ 3 指定した削除ポリシーを保存するには、**Save** をクリックします。

Syslog メッセージ フィルタの定義

フィルタを作成すると、Syslog Analyzer からメッセージを除外できます。メッセージを除外する手順は、次のとおりです。

- ステップ 1** **Resource Manager Essentials > Tools > Syslog > Message Filters** を選択します。
ダイアログ ボックスにすべてのメッセージ フィルタのリストが表示され、各フィルタの名前、ステータス (**Enabled** または **Disabled**) が表示されます。
- ステップ 2** **Drop** または **Keep** を選択して、フィルタが Syslog メッセージを廃棄するか、Syslog メッセージを保存するかを指定します。



(注) **Drop** または **Keep** オプションは、フィルタごとではなく、すべてのメッセージ フィルタに適用されます。

- **Drop** オプションを選択した場合、Common Syslog Collector は、その後の処理から Drop フィルタに一致する syslog を廃棄します。
- **Keep** オプションを選択した場合、Common Syslog Collector は、その後の処理から Keep フィルタに一致する syslog のみを許可します。

変更監査

この項では、RME の変更監査機能の 2 つの側面、つまりインベントリ フィルタの設定と例外期間の定義について説明します。

インベントリ フィルタの設定

インベントリ属性の中には、頻繁に変更され、収集が行われるたびに変更点に関するログが作成されるものがあります。このため、多数の変更監査メッセージが、極めて短期間に蓄積される可能性があります。これを回避するために、インベントリ変更フィルタで、こうした属性の変更監査が追跡されないように設定できます。

インベントリ フィルタを設定するには、以下の順にリンクを選択します。

Resource Manager Essentials > Administration > Inventory > Inventory Change Filter

例外期間の定義

例外期間とは、ネットワークの変更が行われない期間として、ユーザが指定する期間です。

例外期間を設定する手順は、次のとおりです。

- ステップ 1** **Resource Manager Essentials > Tools > Change Audit > Exception Period Definition** の順にリンクを選択します。
- ステップ 2** Day ドロップダウン リストから **Days of the week** を選択します。
- ステップ 3** Start Time および End Time ドロップダウン リストから、開始時刻と終了時刻を選択します。
- ステップ 4** **Add** をクリックします。

SWIM ベースライン収集

RME Software Image Manager (SWIM) は、ほとんどのシスコ製品のソフトウェア管理とアップグレードに非常に役立つツールです。

ネットワークで稼働するすべてのソフトウェア イメージのベースラインを最初にインポートすることを推奨します。

ベースラインは、ネットワークで稼働する一意のソフトウェア イメージのコピーをインポートします (複数のデバイスで同じイメージが稼働している場合には、ソフトウェア ライブラリには1回だけインポートされます)。デバイスに障害が発生して新しいソフトウェア イメージが必要になった場合、またはアップグレード中にエラーが発生した場合に、イメージはバックアップ ファイルとして機能します。ソフトウェア リポジトリにないソフトウェア イメージを実行しているデバイスの場合、これらのデバイスについて同期レポートを生成できます。

ソフトウェア リポジトリの同期

RME ソフトウェア リポジトリの同期を行う手順は、次のとおりです。

-
- ステップ 1 **Resource Manager Essentials > Software Mgmt > Software Repository** の順にリンクを選択します。
 - ステップ 2 **Software Repository Synchronization** を選択します。
 - ステップ 3 **Schedule** をクリックします。
 - ステップ 4 スケジューリング情報を入力して、**Submit** をクリックします。
 - ステップ 5 すべてのソフトウェア イメージのベースラインをインポートします。
ソフトウェア リポジトリの同期ジョブが正常に完了すると、次の手順により、ネットワーク上のすべてのソフトウェア イメージをインポートするジョブを作成できます。
 - ステップ 6 **Resource Manager Essentials > Software Mgmt > Software Repository** の順にリンクを選択します。
 - ステップ 7 **Add** をクリックします。
 - ステップ 8 **Network** を選択します。
 - ステップ 9 **Use Generated Out-of-Sync Report** を選択して、**Next** をクリックします。



(注) **Use Generated Out-of-Sync Report** オプションを選択しないと、ソフトウェア イメージ選択ダイアログ ボックスが表示されるまで時間がかかります。

ソフトウェア リポジトリに登録されていない実行中のイメージがすべて表示されます。

- ステップ 10 **Next** をクリックして、ジョブ制御情報を入力します。
 - ステップ 11 **Next** をクリックして、**Finish** をクリックします。
-

RME ジョブの管理

アーカイブ管理の実行、コンフィギュレーションファイルの編集、コンフィギュレーションのダウンロード、およびデバイスの IOS/Catalyst OS イメージを管理するために、ジョブを作成する必要があります。RME には、さまざまな目的で作成されたジョブを一覧表示できる集合ロケーションがあります。

RME で作成されたすべてのジョブを表示する手順は、次のとおりです。

1. **CWHP > Resource Manager Essentials > Job Mgmt** の順にリンクを選択します。
2. リンクの **RME Jobs** を選択します。

ジョブのステータス、タイプなどの基準を用いて、すべてのジョブを検索できます。

RME では、ジョブを実行する前に承認を行うよう設定できます。

ジョブの承認を行うよう設定する手順は、次のとおりです。

ステップ 1 **CWHP > Resource Manager Essentials > Administration > Approval** の順にリンクを選択します。

ステップ 2 リンクの **Approver Details** を選択します。



(注)

ここで作成したユーザには、システム（ローカル セキュリティ モード、ACS セキュリティ モードなど）のアプリューバロールが必要です。

ジョブ アプリューバ リストの作成

ユーザはアプリューバのリストを作成する必要があります。リストには名前を付けて、アプリューバを割り当てなくてはなりません。

ステップ 3 **CWHP > Resource Manager Essentials > Administration > Approval** の順にリンクを選択します。

ステップ 4 **Create/Edit Approver Lists** を選択します。

ステップ 5 左上のテキスト フィールドにアプリューバ名を入力して、**Add** をクリックします。

ステップ 6 **Available Users** フィールドのリストからユーザを選択して、中央の **Add** をクリックします。

ステップ 7 承認リストのコンフィギュレーションを保存します。

ジョブ承認が必要なアプリケーションの指定

ステップ 8 NetConfig、Config Editor、Archive Management、Software Management など、さまざまな機能に承認リストを割り当てます。

ステップ 9 NetConfig、Config Editor、Archive Management、Software Management など、さまざまな機能で承認リストをイネーブルにします。

これにより、NetConfig、Config Editor、Archive Management、および Software Management に対して作成されたすべてのジョブを実行する前に、承認が必要になります。

承認を保留しているジョブの表示

ステップ 10 **CWHP > Resource Manager Essentials > Job Mgmt** の順にリンクを選択すると、承認を保留しているすべてのジョブを表示できます。

ステップ 11 リンクの **Job Approval** を選択します。

アプリューバは、ジョブを承認または拒否できます。ジョブが拒否された場合、ジョブを作成したユーザに対して、ジョブのステータス更新が報告されます。

Internetwork Performance Monitor へのデバイスのインポート

デバイスが DCR に追加されると、DCR から IPM にデバイスをインポートできます。IPM はこのリポジトリから、デバイス リスト、デバイス属性、およびデバイス クレデンシャルを取得します。



(注)

DCR からデバイスをインポートする前に、リポジトリ内にデバイスが登録されていることを確認してください。また、選択したデバイスのみを DCR から IPM にインポートする機能はありません。DCR 内のすべてのデバイスが IPM にインポートされます。IPM ソースにならない DCR 内のデバイスは追加されず、インポート ログ ファイルにはそのデバイスに対してエラー メッセージが残されます。

デバイスのインポート形式は、以下のとおりです。

- ソース

デバイスをソースとしてインポートする場合、IPM はデバイスに接続し、対象となるデバイスで IP SLA 機能を使用して IOS イメージが実行され、リード/ライト (read/write) コミュニティストリングが指定されている場合のみ、そのデバイスを追加します。

- ターゲット IP SLA レスポンダ

デバイスがターゲット IP SLA レスポンダとしてインポートされる場合、デバイスにリード コミュニティストリングが設定されていると、IPM はそのターゲットで IP SLA レスポンダがイネーブルになっているかどうかを確認します。リード コミュニティストリングが設定されていない場合、ターゲットの IP SLA レスポンダ ステータスは確認されません。

- ターゲット IP デバイス

デバイスをターゲット IP デバイスとしてインポートする場合、IPM は、デバイスへの接続または確認を行わずにデバイスを追加します。

DCR からデバイスをインポートするときに、デバイスがすでに IPM に存在する場合、デバイスの情報が更新されます。

インポート ステータス ログ ファイル : IPM は、DCR のインポート ステータスについて個別のログ ファイルを作成します。ログ ファイルは、*IPMROOT/etc/source* or *IPMROOT/etc/target* にあります。

デバイスのインポート結果の表示 : **View Import Source Log** または **View Import Target Log** をクリックすると、CiscoWorks ホーム ページにデバイスのインポート結果を表示できます。

Device Fault Manager

DFM サーバの管理は、次の項目に分類できます。

- 日常の削除スケジュール
- SNMP トラップの転送
- SNMP トラップの受信
- デフォルトの SMTP サーバ
- 再検出
- グループ管理
- ポーリングおよびスレッシュホールド管理
- ビュー管理

日常の削除スケジュール

DFM の障害履歴情報について、日常的な削除スケジュールを設定する必要があります。削除スケジュールを設定する手順は、次のとおりです。

Device Fault Manager パネルを開き、**Configuration > Other Configuration > Daily Purging Schedule** の順にリンクを選択します。

SNMP トラップの転送

このコンフィギュレーションにより、DFM のトラップレシーバーで受信されるトラップをブライインド転送できます。この機能は、ネットワーク内のデバイスから受信されるトラップに対して有効です。トラップ転送を設定する手順は、次のとおりです。

Device Fault Manager パネルを開き、**Configuration > Other Configuration > SNMP Trap Forwarding** の順にリンクを選択します。



(注) HP Open View などのアプリケーションの NB トラップ生成とは異なります。

SNMP トラップの受信

このコンフィギュレーションにより、DFM でトラップを受信するためのグローバルポートが設定されます。トラップ受信に使用されるポートを設定する手順は、次のとおりです。

Device Fault Manager パネルを開き、**Configuration > Other Configuration > SNMP Trap Receiving** の順にリンクを選択します。

デフォルトの SMTP サーバ

DFM には電子メール通知サービス機能があり、アラートまたはイベントが生成されたときに電子メールを送信できます。この電子メール通知サービスには、電子メールを転送するための SMTP サーバ情報が必要です。

電子メールを送信するために SMTP サーバ情報を設定する手順は、次のとおりです。

Device Fault Manager パネルを開き、**Configuration > Other Configuration > SNMP Default Server** の順にリンクを選択します。

再検出

再検出は、DFM で認識済みのデバイスのリストに対してのみ使用できます。複数の再検出をスケジューリングできます。

再検出をスケジューリングする手順は、次のとおりです。

Configuration > Other Configuration の順に選択して、続いてリンクの **Rediscovery Schedule** を選択します。



(注) 再検出は Campus Manager に記録されるため、デバイスは DCR には追加されません。

グループ管理

グループ管理とは、DFM に含まれるグループを作成、編集、または削除する機能です。これらのグループは、他のアプリケーションと共有できます。

DFM でグループを作成する手順は、次のとおりです。

Configuration > Other Configuration の順にリンクを選択して、次にリンクの **Group Administration** を選択します。

ポーリングおよびスレッシュホールド パラメータの設定

DFM で障害とイベントの発生について検知するために、ポーリング パラメータおよびスレッシュホールド パラメータを設定する必要があります。

- DFM サーバは、**ポーリング パラメータ**を使用して、指定された間隔でさまざまなグループ内のデバイスに対してポーリングを行います。
- **スレッシュホールド パラメータ**は、さまざまなデバイスのスレッシュホールドを決定します。さまざまなデバイス タイプについてこれらのスレッシュホールドの設定値を超えると、DFM サーバでアラートが発生します。

ポーリングおよびスレッシュホールド パラメータを設定する手順は、次のとおりです。

CWHP > Device Fault Manager > Configuration の順にリンクを選択して、続いてリンクの **Polling and Threshold** を選択します。

ビューの作成

ビュー管理を使用すると、オペレータはデバイスのグループのアラートおよびアクティビティを確認できます。グループのリストに対してビューを作成すると、このビューは、DFM の Alerts and Activities ウィンドウに表示されます。

ビューを作成する手順は、次のとおりです。

Configuration > Other Configuration の順にリンクを選択して、続いてリンクの **Alerts and Activities Defaults** を選択します。

CiscoView

CiscoView は、Web ベースのデバイス管理アプリケーションで、広範囲なシスコのインターネットワーキング製品に対し、動的ステータス、モニタリング、およびコンフィギュレーション情報を提供します。CiscoView では、デバイス シャーシの物理的なビューが表示され、モジュールとポートの色分け表示によって、ステータスが一目でわかります。モニタリング機能により、パフォーマンスおよびその他の統計情報が表示されます。コンフィギュレーション機能を使用すると、必要なセキュリティ権限を付与されたユーザは、デバイス設定の一括変更を行うことができます。

CiscoView は、動作の軽い HTML ベースのクライアントを提供します。また、IPv6 機能を持ちながら、IPv4 アドレスの管理にも対応しています。

CiscoView を起動するには、**CWHP > CiscoView > Chassis View** の順にリンクを選択します。

Device Center

Device Center は LMS ソリューション内のポータルで、特定のデバイスに関する情報を収集してデバッグする機能を提供します。Device Center のサマリーでは、次の情報が得られます。

- デバイスの IP アドレス
- デバイスのタイプ
- 24 時間の変更監査のサマリー
- インベントリ収集およびコンフィギュレーション収集が最後に行われた時刻
- Syslog サマリー
- デバイスおよび近接するデバイスの障害に関連するアラート

Device Center は、デバッグの支援、デバイスに関するレポート、およびクレデンシャルの変更などの管理タスクを実行する一連の機能も提供します。

Device Center は、Common Services の一部としてインストールされます。Device Center を起動する手順は、次のとおりです。

CWHP > Device Troubleshooting > Device Center の順にリンクを選択します。



(注) Device Center に読み込まれる情報は、LMS サーバにインストールされているアプリケーションによって異なります。

デバッグ ユーティリティの起動

特定のデバイスでデバッグ ユーティリティを起動する手順は、次のとおりです。

-
- ステップ 1** グループ階層を閲覧してデバイスを選択するか、グループ セレクタの上にある検索ユーティリティに名前を入力して、特定のデバイスを検索します。
- ステップ 2** デバイス名を選択した後、デバイス名のリンクをクリックします。
これにより、デバイスのサマリーおよびツール ページが表示されます。
右フレームの上半分には、デバイスに関する 24 時間のレポートが表示され、右フレームの下半分にツールが起動されます。
-

一連の推奨ツールを実行する手順は、次のとおりです。このリストは完全ではありませんが、Device Center でどのようなツールを利用できるのかを理解するのに役立ちます。

- **Ping** : デバイスの接続試験を実行して、LMS サーバからアクセスできるかどうかを確認します。
- **Credential Verification Report** : Credential Verification Report を起動して、不足しているクレデンシャルがないかどうかを確認します。
- クレデンシャルが不足している場合は、Edit Device Credentials ツールを起動して、クレデンシャルを編集します。
- **Edit Device Credentials ツール** : デバイスで Detailed Device Report を起動して、メモリ、フラッシュ、イメージ、および IP アドレスに関する情報を表示します。
- **Fault History Report** : Fault History Report を起動して、過去 24 時間または 31 日以内に発生した障害を表示します。
- **CiscoView ツール** : 障害が見つかった場合は、CiscoView ツールを開き、シャーンシを表示して、インターフェイスまたはポートに必要な変更を行います。

- **Switch Port Usage レポート** : デバイスがスイッチの場合、稼働中のポート、停止中のポート、または未使用のポートの最新のサマリーを表示する、Switch Port Usage レポートを起動できます。
- **アーカイブおよびイメージ管理** : アーカイブの同期、以前のコンフィギュレーションのアーカイブのダウンロード、またはソフトウェア イメージのアップグレードを実行できます。



Cisco LAN Management Solution 2.5 でのネットワーク管理

この章では、Device Fault Manager (DFM)、Resource Manager Essentials (RME)、Campus Manager、Internetwork Performance Monitor (IPM)、および Common Services のすべてのアプリケーションに関する、LMS のネットワーク管理タスクについて詳しく説明します。



(注)

この章には、LMS アプリケーション スイートに関するネットワーク管理の例の一部が記載されています。この章は、LMS を使ったネットワーク管理の包括的なマニュアルではないことに注意してください。

障害モニタリング

DFM には、障害をモニタリングする方法として、次の 3 つの異なるオプションがあります。

- 障害履歴を使用して、過去の障害データを確認できます。
- 電子メール、トラップ メッセージ、または Syslog メッセージによる通知を選択できます。
- アラートおよびアクティビティ ウィンドウで、現在の障害をリアルタイムで確認できます。

設定作業

DFM で障害モニタリングをイネーブルにする前に、次の作業を行う必要があります。

DCR からのデバイス リストの追加

Device and Credentials Repository (DCR) から DFM に、デバイスのリストをインポートする必要があります。

CWHP > Device Fault Manager > Device Management の順にリンクを選択し、**Device Selector** ツールを開きます。

デバイスのステータスの確認

すべてのデバイスのステータスは**既知**である必要があります。

Device Fault Manager > Device Management > Device Summary の順に選択します。

ポーリングおよびスレッシュホールドの設定

デフォルトのポーリング設定を使用してデバイスに対してポーリングが実行されているため、すべてのデバイスについて障害およびイベントの発生が自動的に検知されます。

ポーリングおよびスレッシュホールド パラメータを設定する手順は、次のとおりです。

1. **CWHP > Device Fault Manager > Configuration** の順にリンクを選択します。
2. リンクの **Polling and Threshold** を選択します。

この **Polling and Threshold** リンクでは、デフォルトのポーリングおよびスレッシュホールド設定を変更するか、ユーザ定義のデバイス インターフェイスとポート グループについて新しいポーリングおよびスレッシュホールド設定を行うかを選択できます。

DFM サーバは、ポーリング パラメータを使用して、指定された間隔でさまざまなグループ内のデバイスに対してポーリングを行います。

スレッシュホールド パラメータは、各デバイスのスレッシュホールドを決定します。これらのスレッシュホールドの設定値を超えると、DFM サーバでアラートが発生します。

障害およびアラート通知サービス

DFM では、デバイスで発生した障害またはアラートを通知するために、さまざまな通知サービスを利用できます。

-
- ステップ 1** **CWHP > Device Fault Manager** の順にリンクを選択します。
 - ステップ 2** リンクの **Notification Services** を選択します。
 - ステップ 3** リンクの **Notification Groups** をクリックして、通知グループを作成します。
 - ステップ 4** グループ セレクタからグループを選択して、次のいずれかを選択します。
 - アラート 重大度
 - イベント 重大度
 - アラート ステータス
 - 通知を送信するグループ内のデバイスに対する イベント ステータス
 - ステップ 5** **Next** をクリックします。
 - ステップ 6** 通知グループ名を指定して、**Next** をクリックします。
 - ステップ 7** **Finish** をクリックすると、通知グループが作成されます。
 - ステップ 8** 通知グループごとに通知を送信する必要がある場合、HP Open View Network Node Manager のような NB アプリケーションにトラップを送信するには、リンクの **SNMP Trap Notification** をクリックします。
 - ステップ 9** 通知グループごとに通知を送信する必要がある場合、ユーザに電子メールによる通知を送信するには、リンクの **E-Mail Notification** をクリックします。
 - ステップ 10** 通知グループごとに通知を送信する必要がある場合、別のマシンに syslog メッセージを送信するには、リンクの **Syslog Notification** をクリックします。
-

障害履歴

障害履歴機能の利用には、設定を行う必要はありません。デバイス内の障害はすべて自動的に蓄積され、以下の手順で表示できます。

Device Fault Manager を開き、リンクの **Fault History** を選択します。

1つのデバイス、デバイスのグループ、障害 ID、またはイベント ID から検索して、障害を表示できます。

アラートおよびアクティビティ

Alerts and Activities ウィンドウには、デバイスまたはビューの障害がリアルタイムで表示されます。

Alerts and Activities ウィンドウを起動する手順は、次のとおりです。

CWHP > Device Fault Manager の順にリンクを選択して、リンクの **Alerts and Activities** をクリックします。

関連情報については、「[ビューの作成](#)」(p.6-15) を参照してください。

ベースライン設定

すべての企業では、ネットワーク内のすべてのデバイスに対して何らかの標準ポリシーを適用する必要があります。エンタープライズ ネットワークは、定期的にポリシー監査を行い、ポリシーに違反するデバイスが見つかった場合、強制的にポリシーを適用する必要があります。

RME Baseline テンプレートおよび適合性チェックによって、次の機能を利用できます。

まず、一連のデバイスで実行する、標準化されたポリシーベースのコマンドのセットを特定します。次に、特定されたコマンドのセットを使用して、**Baseline** テンプレートを作成します。ベースライン テンプレートを作成したあと、次のタスクを実行できます。

- デバイスのコンフィギュレーションを比較して、ベースライン テンプレートに準拠していないすべてのデバイスをリストアップしたレポートを生成します。
- ベースライン テンプレートを、ネットワーク内の同じカテゴリのデバイスに適用します。
- 適合性チェック ジョブをスケジューリングして、ベースライン テンプレートをデバイスに適用します。

LMLS アプリケーションからのデータ抽出

この項では、Campus Data Extraction Engine および RME Data Extraction Engine について説明します。

Campus Data Extraction Engine

Campus Manager には、次のデータを抽出するためのデータ抽出エンジンがあります。

- ユーザ追跡データ
- レイヤ2トポロジー
- ネットワーク設定の不一致

データ抽出は、コマンドライン インターフェイスまたは Servlet アクセスによって実行できます。

cmexport ユーティリティ

`NMSROOT/campus/bin` ディレクトリを開くと、コマンドライン インターフェイス ユーティリティ `cmexport` にアクセスできます。

トップレベルの `Help` は、次の情報を提供します。

```
cmexport <-h | -v | commands> <arguments>
```

コア コマンド

表 7-1 に、コア データ抽出コマンドを示します。

`cmexport` コマンドは、表 7-1 に示されたコア コマンドの 1 つとともに実行する必要があります。コア コマンドを指定しないと、`cmexport` は `-v` または `-h` オプションだけを実行します。

表 7-1 コアコマンド : Campus Manager のデータ抽出

コア コマンド	説明
<code>ut</code>	ユーザ追跡データを XML 形式で生成します。
<code>l2topology</code>	レイヤ 2 トポロジー データを XML 形式で生成します。
<code>discrepancy</code>	不一致データを XML 形式で生成します。
<code>-f</code>	Data Extraction Engine の出力を格納するために、ファイル名およびディレクトリを指定します。
<code>-h</code>	(Null オプション) このユーティリティの使用に関するヘルプ情報を表示します。
<code>-v</code>	<code>cmexport</code> ユーティリティのバージョンを表示します。

アーカイブの場所

`cmexport` コマンドライン インターフェイスによって生成されたデータは、デフォルトでは次の場所にアーカイブされます。

- ユーザ追跡データ :
`PX_DATADIR/cmexport/ut/timestamput.xml`
- レイヤ 2 トポロジー データ :
`PX_DATADIR/cmexport/L2Topology/timestampL2Topology.xml`
- 不一致データ :
`PX_DATADIR/cmexport/Discrepancy/timestampDiscrepancy.xml`

ディレクトリの場所

- `PX_DATADIR` ディレクトリの場所は、次のとおりです。
 - Windows : `%NMSROOT%\files` フォルダ
 - Solaris : `/var/adm/CSCOPx/files`
- `NMSROOT` は、Campus Manager をインストールしたディレクトリです。
- `timestamp` は、ログが次の形式で書き込まれた時刻です。
YearMonthDateHourOfDayMinuteSecond 形式

このユーティリティには、アーカイブに作成されたファイルを削除する機能はありません。これらのファイルは、必要に応じてユーザ自身が削除する必要があります。ただし、同じファイル名とディレクトリを 2 回使用すると、前のファイルが上書きされます。

cmexport コマンドの使用可能な組み合わせ

ユーザ追跡

表 7-2 ユーザ追跡の cmexport パラメータ

パラメータ	説明
-layout	ユーザ追跡のホスト データは、 layoutname で指定されたレイアウトに対して、XML 形式でエクスポートされます。レイアウトは、ユーザ追跡でユーザが定義したカスタム レイアウトです。このパラメータは、 -host が選択されている場合のみ適用できます。
-layoutPhone	ユーザ通話追跡データは、 layoutPhone で指定されたレイアウトに対して、XML 形式でエクスポートされます。このパラメータは、 -phone が選択されている場合のみ適用できます。
-query	ユーザ追跡のホスト データは、 queryname で指定されたクエリに対して、XML 形式でエクスポートされます。このパラメータは、 -host が選択されている場合のみ適用できます。
-queryPhone	ユーザ通話追跡データは、 phonequeryname で指定されたクエリに対して、XML 形式でエクスポートされます。このパラメータは、 -phone が選択されている場合のみ適用できます。
-view	ユーザ追跡 XML データが表示される形式を指定します。現在、2つのオプションがサポートされています。 <ul style="list-style-type: none"> • switch : ユーザ追跡データは、スイッチに基づいて表示されます。 • subnet : ユーザ追跡データは、所属するサブネットに基づいて表示されます。

コマンド例

```
cmexport ut -u admin -p admin -host
cmexport ut -u admin -p admin -phone
cmexport ut -u admin -p admin -host -query dupMAC -layout all
cmexport ut -u admin -p admin -host -query dupMAC -layout <name>
cmexport ut -u admin -p admin -phone -queryPhone <name> -layoutPhone <name>
cmexport ut -u admin -p admin -host -f ut.xml
cmexport ut -u admin -view switch -host
```

Layer 2 Topology コマンドまたは Discrepancy コマンド

```
cmexport L2Topology|Discrepancy -u admin -p admin
cmexport L2Topology|Discrepancy -u admin -p admin -f 013104L2.xml
```

Data Extraction Engine への Servlet アクセス

Campus Manager Data Extraction Engine への Servlet アクセスについて説明します。

Servlet はユーザ要求を受け入れ、Common Services 認証メカニズムを使用して、要求側のユーザの ID を認証します。ユーザ追跡、トポロジー、および不一致をエクスポートするコマンドは、HTTP または HTTPS 要求として送信できます。

Servlet では、ユーザのクレデンシャルの詳細、実行するコマンド、ログおよびデバッグ オプションなどのオプションの詳細を含む、XML 方式の入力用ペイロード ファイルが必要です。Servlet は、XML にエンコードされたペイロード ファイルを解析して処理を実行し、結果を XML 形式で返します。通常、Servlet アクセスは、クライアント システムからデータを抽出するために使用されます。Servlet によってデータが生成される間、クライアント端末に出力が表示されます。

入力 XML ファイルには、ユーザ名、パスワード、コア コマンドなどのさまざまなタグと、オプション タグが含まれます。

Servlet からのエクスポート ファイルの抽出

Servlet からエクスポート ファイルを抽出する手順は、次のとおりです。

-
- ステップ 1** 目的のデータを使用して、必要となるペイロード XML ファイルを生成します。
 - ステップ 2** スクリプトを使用して、生成したペイロード ファイルを適用した Servlet に POST 操作を実行します。Servlet は、以下の場所にあります。
http://Campus-Server:1741/CSCOnm/campus/servlet/CMExportServlet
 Servlet の HTTP 応答には、ペイロード ファイルで指定されたパラメータを使用し、サーバで **cmexport** コマンドを実行することで生成された、XML ファイルが含まれています。
 - ステップ 3** HTTP 応答の内容から XML ファイルを抽出して、ローカルファイルとして保存します。
-

ペイロードの例

```
<payload>
<!--The following element specifies the username (valid CiscoWorks or ACS user ID) of the
person initiating this DEE call -->
  <username>username</username>
<!-- The following element specifies the valid password of the user ID -->
  <password>password</password>
<!--The following element specifies the DEE command used for extracting User Tracking host,
phone, discrepancy and L2 topology information -->
  <command>ut_host</command>
<!--The following element specifies the logfile where all logs need to be output -->
  <logfile>filename</logfile>
<!--The following element specifies the debug level at which the log is output. -->
  <debug>1</debug>
<!--The following element specifies the custom report name created in the User Tracking
user interface by navigating to CWHP > Campus Manager > User Tracking > Reports > Custom
Reports.>
  <view></view>
</payload>
```

Servlet にアクセスするための Perl スクリプトの例



(注) スクリプト例は、Campus Manager Data Extraction Engine のオンライン ヘルプで入手できます。

```
#!/opt/CSCOPx/bin/perl
use LWP::UserAgent;
$| = 1;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
if ( -f $fname ) {
open (FILE,$fname) || die "File open Failed $!";
while ( <FILE> )
{
    $str .= $_ ;
}
close(FILE);
}
url_call($temp);
#-- Activate a CGI:
sub url_call {
    my ($url) = @_ ;
    my $ua = new LWP::UserAgent;
    $ua->timeout(5000);
    my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
    my $req = new HTTP::Request ('GET', $url, $hdr);
    $req->content($str);
    my $res = $ua->request($req);
    my $result;
    if ($res->is_error)
    {
        print "ERROR :", $res->code, " :", $res->message, "\n";
        $result = '';
    }
    else
    {
        $result = $res->content;
        if($result =~ /Authorization error/)
        {
            print "Authorization error\n";
        }
        else
        {
            print $result ;
        }
    }
}
```

上記の Perl スクリプトは、`payload.xml` ファイルを使用して Servlet を起動します。コマンドは、HTTP モードおよび HTTPS モードの次のコマンドに似ています。

- HTTP モード
`./perl script.pl http://server:1741/campus/servlet/CMExportServlet payload.xml`
- HTTPS モード
`./perl script.pl https://server/campus/servlet/CMExportServlet payload.xml`

Data Extraction Engine を使用するすべてのユーザには認証および許可が行われます。ユーザ名とパスワードは、コマンドライン インターフェイスおよび Servlet を呼び出す際に入力するか、パスワードをパスワード ファイルに入力し、Data Extraction Engine によって取得させます。許可されていないアクセスから保護するために、ファイルへのアクセス権限を設定できます。このオプションを使用する場合、クレデンシャルを含むファイルを指すように CMEXPORTFILE 環境変数を設定する必要があります。コマンドは、次の形式で入力する必要があります。

```
cmexport ut -u admin -host
```

この構文により、**cmexport** は、ユーザ名（この例ではユーザ名 **admin**）に関連付けられたパスワードを検索できます。

Resource Manager Essentials の Data Extraction Engine

Resource Manager Essentials には、次のデータを抽出するためのデータ抽出エンジンがあります。

- インベントリ
- 変更監査
- デバイスのコンフィギュレーションの詳細

データ抽出は、コマンドライン インターフェイスまたは Servlet アクセスを用いて実行できます。コマンドライン インターフェイス ユーティリティ **cwcli** にアクセスするには、**NMSROOT/bin** ディレクトリを開きます。

トップレベルの **Help** コマンド **cwcli -help** は、次の情報を提供します。

引数を使用してコマンドを実行するための一般的な構文は、次のとおりです。

```
cwcli <application/command> <arguments>
```

コマンドおよび引数の詳細なヘルプを表示するには、次のコマンドを実行します。

```
cwcli <application/command> -help
```

cwcli コマンドは、表 7-3 で示されたコア コマンドの 1 つとともに実行する必要があります。コア コマンドを指定しないと、**cwcli** は **-v** または **-help** オプションのみ実行できます。

表 7-3 コア コマンド : Resource Manager Essentials のデータ抽出

コア コマンド	説明
config	コンフィギュレーションのダウンロードと取得、2 つの異なるコンフィギュレーションの比較、アーカイブされたコンフィギュレーション ファイルの削除、およびデバイスのリロードを実行するために使用されるコマンドのセットを提供します。
export	インベントリ データ、コンフィギュレーション データ、変更監査データを、XML 形式にエクスポートします。
inventory	インベントリ収集ジョブを作成、削除、およびキャンセルするためのコマンドライン インターフェイス ツール。インベントリのデータを XML ファイルとしてインポートまたはエクスポートする場合にも利用できます。
invreport	すべてのカスタム レポートをリストアップして、特定のテンプレートについて CSV 形式のインベントリ レポートを生成します。
netconfig	NetConfig ジョブを作成、削除、およびキャンセルするためのコマンドライン インターフェイス ツール。ユーザ定義テンプレートの XML ファイルをインポートまたはエクスポートする場合にも利用できます。
-v	cwcli ユーティリティのバージョンを表示します。
-help	(Null オプション) このユーティリティの使用に関する情報を表示します。

コマンドライン構文

アプリケーションのコマンドライン構文の形式は、次のとおりです。

```
cwcli export command GlobalArguments AppSpecificArguments
```

- **cwcli export** は、インベントリ、コンフィギュレーション、および変更監査の詳細を XML 形式にエクスポートする CiscoWorks コマンドライン インターフェイスです。
- **Command** は、実行されるコア操作を指定します。
- **GlobalArguments** は、各コア コマンドに必要な追加パラメータです。
- **AppSpecificArguments** はオプションのパラメータで、特定の cwcli export コア コマンドの動作を変更します。

引数とオプションの順序は重要ではありません。ただし、コア コマンドは **cwcli export** の直後に入力する必要があります。

UNIX では、MANPATH を次のように設定すると、cwcli export の man ページが表示されます。

```
/opt/CSCOpX/man/man1
```

cwcli export コマンドについて表示する man ページは、**cwcli export** コマンドについて表示する **man cwcli-export** です。

- cwcli export changeaudit コマンドについて表示するコマンドは、次のとおりです。
man export-changeaudit
- cwcli export config コマンドについて表示するコマンドは、次のとおりです。
man export-config
- cwcli export inventory コマンドについて表示するコマンドは、次のとおりです。
man export-inventory

データのアーカイブ場所

cwcli export コマンドライン インターフェイスによって生成されたデータは、デフォルトでは次の場所にアーカイブされます。

- 変更監査
 - Solaris : `/var/adm/CSCOpX/files/rme/archive/YYYY-MM-DD-HH-MM-SS-changeaudit.xml`
 - Windows : `NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS-changeaudit.xml`
- コンフィギュレーション
 - Solaris :
`/var/adm/CSCOpX/files/rme/cwconfig/YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name.xml`
 - Windows :
`NMSROOT\files\rme\cwconfig\ YYYY-MM-DD-HH-MM-SSMSMSMS-Device_Display_Name.xml`
- インベントリ
 - Solaris : `/var/adm/CSCOpX/files/rme/archive/YYYY-MM-DD-HH-MM-SS-inventory.xml`
 - Windows : `NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS- inventory.xml`

RME Servlet

RME Data Extraction Engine への Servlet アクセスについて説明します。

Servlet の名前は `/rme/cwcli` です。次に、コマンドを実行するために起動される Servlet を示します。

POST 要求の場合

`http://<rme-server>:<rme-port>/rme/cwcli <payload XML file>`

GET 要求の場合

`http://<rme-server>:<rme-port>/rme/cwcli?command=cwcli config <commandname>-u <user> -p <Base64 encoded pwd> -args1 <arg1value>...`



(注)

引数がファイルの場合は、`<arg>` および `<argval>` タグを使用します。

ペイロード xml ファイルの内容は、次のとおりです。

```
<payload>
<command>
cwcli config export -u admin -p <Base64Encoded pwd> -device 1.1.1.1 -xml
</command>
<arg>
</arg>
<arg-val>
</arg-val>
</payload>
```

たとえば、`import` コマンド `payload.xml` は、次のようにして実行します。

```
<payload>
<command>
cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106
<arg>
-f
</arg>
<arg-val>
banner motd "Welcome, Sir"
</arg-val>
</command>
</payload>
```

Remote Access Servlet は、`import` コマンドの `arg-val` タグ間で指定された内容を使用して、一時ファイルを作成します。サーバでは、コマンドは `cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106 -f tempfile` として実行されます。

この例では、一時ファイルには `banner motd "Welcome, Sir"` という行があります。

以下の例を参照してください。

`Perl samplescript.pl http(s)://<rme-server>:<rme-port>/rme/cwcli <payload XML file>`



(注)

セキュアモード (HTTPS) の場合、ポート番号は 443 です。HTTP モードの CiscoWorks サーバのデフォルトポートは 1741 です。

Servlet を起動するスクリプトの例

```
#!/opt/CSCOpX/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{ $str .= $_ ;
}
print $str ;
url_call($temp);
#-- Activate a CGI:
sub url_call
{
my ($url) = @_ ;
my $ua = new LWP::UserAgent;
$ua->timeout(1000);
# you can set timeout value depending on number of devices
my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
my $req = new HTTP::Request ('POST', $url, $hdr);
$req->content($str);
my $res = $ua->request ($req);
my $result;
if ($res->is_error)
{
print "ERROR :", $res->code, " :", $res->message, "\n";      $result = '';
}

else {
$result = $res->content;
if($result =~ /Authorization error/)
{
print "Authorization error\n";
}
else {
print $result ;
}
}
}
}
```

Internetwork Performance Monitor でのエクスポート

IPM でのデータのエクスポート方法は、以前のバージョンと変更はありません。ipm export コマンドライン インターフェイスは、IPM エクスポートを実行するコマンドです。

IPM Export コマンド

次の例は、ipm export Help コマンドを使用するときに表示されるコマンド構文とヘルプを示しています。

ipm export コマンドを使用して IPM データをエクスポートするには、root ユーザ (Solaris) または administrator (Windows) としてログインする必要があります。

```
ipm export
[-q] [[-k <letter>] | -w] [-h]
[ ( -c | -s | -t | -o | -cs) [<CollectorName> ] ]
[ [ (-dh | -dd | -dw | -dm) <StartTime> <EndTime> [ <CollectorName> ] ] ]
| [ (-jh | -jd | -jw | -jm) <StartTime> <EndTime> [ <CollectorName> ] ] ]
| [ (-ph | -pd | -pw | -pm) <StartTime> <EndTime> [ <CollectorName> ] ] ]
| [ -r [<WhichDay>] ] ]
| [ -all [<StartDate>] [<EndDate>]] ]
```

一般的なオプション

[ipmRoot] /opt/CSCOipm などの、IPM のルートの場所。

- q 静的出力: 列見出しは表示されません。プレーン テキスト 出力形式の場合のみ適用されます。
- k デリミタ: フィールド デリミタを <letter> に設定します。デフォルトでは、これはカンマ「,」に設定されています。プレーン テキスト 出力形式の場合のみ適用されます。
- w HTML 出力: このコマンドの出力から Web ページが生成されます。
- h ヘルプ: この使用方法のヘルプを表示します。

形式:

時刻: <StartTime> および <EndTime> は次のように入力する必要があります。

MM/DD/YYYY-hh:mm:ss

日付: <WhichDay> は次のように入力する必要があります。

MM/DD/YYYY

<StartDate> および <EndDate> は次のように入力する必要があります。

MM/DD/YYYY

DCR コマンドライン インターフェイス

コマンドライン インターフェイスを使用すると、デバイスの追加、削除、変更、および DCR のモード変更を実行できます。DCR に格納される DCR 属性のリストを表示して、現在の DCR モードを確認することもできます。

起動する主なコマンドは、次の場所にあります。

NMSROOT/bin/dcrecli

コマンドを起動する手順は、次のとおりです。

ステップ 1 NMSROOT/bin/dcrecli -u **username** と入力します。

ステップ 2 ユーザ名に対応するパスワードを入力します。

ステップ 3 トップレベル コマンドの中から 1 つを選択します。

- **add**: デバイスを追加します。
 - **del**: デバイスを削除します。
 - **details**: デバイスの詳細を表示します。
 - **exp**: ファイルにエクスポートします。
 - **impFile**、**impNms**、**impRNms**、**impACS**: ファイル、ローカル NMS、リモート NMS、および ACS (AAA サーバ) からデバイス リストをインポートします。
 - **lsattr**: DCR に格納されている属性を表示します。
 - **lsmode**: マスター、スレーブ、またはスタンドアロンといった、DCR モードを表示します。
 - **mod**: デバイスを変更します。
 - **setmaster**、**setstand**、**setslave**: DCR をマスター、スタンドアロン、またはスレーブ モードに設定します。
-

ユーザ追跡レポート

UT (ユーザ追跡) レポートを生成するには、**CWHP > Campus Manager > User Tracking** の順にリンクを選択します。次に、リンクの **Reports** を選択します。

次のレポートを生成できます。

- エンド ホストおよび IP フォンに関するレポートを迅速に表示する機能を提供します。シンプルなクエリを入力するだけで、ユーザ追跡の対象内からエンド ホストまたは IP フォンのサブセットを表示できます。
- スイッチのスイッチ ポート使用状況に関する統計レポートを生成します。最近停止したポート、未使用の停止中のポート、および未使用の稼働中のポートについて、スイッチ ポート使用状況レポートを生成できます。
- レポートを生成するために定期的に行われるジョブをリストアップします。これらのジョブでは、エンド ホスト、IP フォン、重複するデバイス エントリ、およびスイッチ ポートの使用状況に関するレポートを生成します。

レポート ジョブのリストを表示するには、**User Tracking > Reports > Report Jobs** の順にリンクを選択します。

- グループを選択し、続いてグループに関するクエリを評価することでエンド ホストおよび IP フォンの数をサブセット化し、エンド ホストおよび IP フォンのカスタムレポートを生成します。

カスタム レポートを生成するには、**User Tracking > Reports > Custom Reports** の順にリンクを選択します。

生成したカスタム レポートは保存できます。

User Tracking > Reports > Report Generator の順にリンクを選択し、カスタム レポートを利用して、エンド ホストまたは IP フォンに関する詳細なレポートを生成できます。

デバイスでの Syslog の設定

LMS は、ネットワーク内のデバイスから受信した syslog メッセージを収集して分析できます。syslog メッセージの収集は、ネットワークをより効率的に管理するために利用できます。syslog メッセージをイネーブルにすると、以下のように多くの利点があります。

- LMS は、ネットワーク上のコンフィギュレーションおよびインベントリの変更を収集して更新します。
- 受信した syslog メッセージは分析に用いたり、別のアクションを自動発生させるためのトリガーとして使用することもできます。

NetConfig による Syslog のイネーブル化

NetConfig を使用して、デバイスで Syslog をイネーブルにできます。NetConfig には、Syslog をイネーブルにするテンプレートが組み込まれています。

Resource Manager Essentials > Config Mgmt > NetConfig からテンプレートにアクセスできます。

NetConfig ジョブの作成

TOC メニューから **NetConfig Jobs** をクリックして、NetConfig ジョブを作成します。

RME によってデバイス コンフィギュレーションが管理されるようになると、NetConfig によって syslog をイネーブルにできます。

RME 4.0 は、Cisco IOS および Catalyst OS を使用して、複数のデバイスに対して 1 つのジョブをスケジューリングできます。

VLAN に関する推奨設定

Campus Manager を使用すると、VLAN を表示して、スパニング ツリーに推奨設定を適用できます。推奨設定でサポートされているスパニング ツリーのタイプは、PVST、MIST、および 802.1s です。ほとんどのスイッチド トラフィックはルート ブリッジを介して送信されるため、適切なスイッチをルート ブリッジとして指定する必要があります。Campus Manager では、次の基準に基づいてルート ブリッジを選択できます。

1. 最小深度

最小深度方式を使用すると、ユーザは特定の VLAN について、ネットワーク内の各ノードからルートへの深度が最小になるようルート ブリッジを選択できます。この方法で作成されたスパニング ツリーは、深度が最小になります。

2. 最小コスト

最小コストに関する推奨設定は、スイッチ クラウド内のすべてのノードからのコストが最小になるように、ルート ブリッジに推奨設定を適用します。

3. トラフィック データ

Campus Manager はまた、ネットワーク内のトラフィックに基づいてルート ブリッジの推奨を行います。Campus Manager は、Cisco Network Analysis Module (NAM; ネットワーク解析モジュール) と NetFlow コレクタの 2 つのソースからトラフィック情報を受信します。

最小深度のスパニング ツリーに関する推奨設定の表示

最小深度のスパニング ツリーに関する推奨設定を表示する手順は、次のとおりです。

-
- ステップ 1** **Topology Services > Network Views > LAN Edge View** の順にリンクを選択します。
 - ステップ 2** 目的のスイッチ クラウドを選択します。
 - ステップ 3** **Display View** をクリックします。
 - ステップ 4** Switch Cloud ビューで、**Reports** を選択します。
 - ステップ 5** 最適なルートおよびインスタンス リダクションとインスタンス推奨設定レポートを実行するには、次のオプションのいずれかを選択します。
 - **Per VLAN STP Recommendations**
 - **Cisco MISTP Recommendations**
 - **IEEE 802.1s Recommendations**
-

イーサチャネルおよびトランクの構築

Campus Manager Topology Services Layer 2 ビューでは、イーサチャネルおよびトランクを設定することもできます。

イーサチャネルの設定

イーサチャネルを設定する手順は、次のとおりです。

-
- ステップ 1** Layer 2 ビューのリンクを選択します。
 - ステップ 2** 右クリックして **Configure Ether Channel** を選択します。
Ether Channel Configuration ウィンドウが表示されます。
 - ステップ 3** **Ether Channel protocol** に **PagP** を指定します。
 - ステップ 4** チャネル モードを **Desirable** に設定します。
 - ステップ 5** **distribution protocol** は、**ip**、**mac**、または **port** に設定します。
 - ステップ 6** **distribution address type** は、**source**、**destination**、または **both** に設定します。
Ether Channel Configuration ウィンドウには、イーサチャネルの構築を行う 2 つのデバイス間の、すべてのリンクが表示されます。
 - ステップ 7** イーサチャネルを構成するリンクを選択します。
コンフィギュレーション ウィンドウでは、実行用コンフィギュレーションを起動用コンフィギュレーションにコピーすることもできます。
-

トランクの設定

トランクを設定する手順は、次のとおりです。

-
- ステップ 1** 特定のリンクを右クリックして、**Create Trunk** を選択します。
 - ステップ 2** カプセル化のタイプを選択します。
 - 802.1Q
 - ISL
 - ネゴシエーション
 - ステップ 3** そのトランクで許可される VLAN および拒否される VLAN を入力します。
-

コンフィギュレーション ファイルの変更管理

この項では、コンフィギュレーション ファイルの変更管理を行うアプリケーションについて説明します。

RME Config Editor

RME Config Editor 機能を使用すると、コンフィギュレーション アーカイブに格納されたデバイス コンフィギュレーションを編集して、デバイスにダウンロードできます。Config Editor ツールを使用すると、すべてのバージョンのコンフィギュレーション ファイルの変更、変更の確認、およびデバイスへの変更のダウンロードを実行できます。

今回のバージョンでは、Config Editor を使って、複数のユーザがコンフィギュレーション ファイルを同時に編集できます。このコンフィギュレーション ファイルは、個人のワーク エリアに保存できます。

NetConfig テンプレート

NetConfig 機能は、複数のデバイスでデバイス コンフィギュレーションを同時に更新するために使用できる、コマンド テンプレートのセットを提供します。NetConfig ツールはウィザードベースのテンプレートを提供して、グローバルな変更をネットワーク デバイスに適用する作業を簡素化し、作業時間を短縮します。

このテンプレートを使用すると、複数のデバイスに対して1つ以上のコンフィギュレーション コマンドを同時に実行することもできます。たとえば、デバイスのセキュリティを向上させるために、SNMP コミュニティ スtring を定期的に変更するには、適切な SNMP テンプレートを使用して、同じジョブを使用するすべてのデバイスでコミュニティ スtring を更新します。更新されたコンフィギュレーションのコピーはすべて、自動的にコンフィギュレーション アーカイブに保存されます。

NetConfig には、必要なコマンドをすべて含んだ定義済みのテンプレートが付属しています。ユーザはコマンドのパラメータを指定するだけで、NetConfig により実際のコマンド構文へと変換されます。この定義済みのテンプレートには、対応するロールバック コマンドが含まれているため、デバイスでジョブが失敗すると、コンフィギュレーションは元の常態に戻ります。

変更監査レポート

LMS によってネットワーク上で行われた変更はすべて、変更監査の一部として記録されます。デバイスで syslog がイネーブになっている場合、デバイスで行われたアウトバンドの変更も、変更監査の一部として記録されます。

変更監査レポートを表示する手順は、次のとおりです。

ステップ 1 Resource Manager Essentials > Reports > Report Generator の順にリンクを選択します。

ステップ 2 アプリケーションとして **Change Audit** を選択します。

レポート タイプを選択します。

- 24 時間レポート
 - 標準レポート
 - 例外期間レポート
-

これらのレポートは、ネットワーク上の変更を管理するために利用できます。Resource Manager Essentials には**監査証跡**機能もあります。監査証跡機能によって、デバイスの追加または削除、クレンジョブの変更など、サーバで行われたすべての変更の証跡が得られます。