Cisco Prime Infrastructure 2.1 クイック スタート ガイド

改訂日：2014 年 5 月 9 日、OL-30962-01.

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO PRIME INFRASTRUCTURE

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

ADDITIONAL LICENSE RESTRICTIONS:

- Installation and Use. The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
  - Cisco Prime Infrastructure：お客様のネットワーク管理環境内にあるサーバにインストールできます。

  付与されているソフトウェア ライセンスごとに、お客様は、本ソフトウェアで提供されるライセンス ファイルまたはソフトウェア ライセンス権利証明書で指定された数のネットワーク デバイスおよびコーデックを管理するため、単一のサーバに本ソフトウェアをインストールし、実行できます。お客様の要件がネットワーク デバイスおよびコーデックの制限を超える場合、お客様は、アップグレード ライセンスまたは本ソフトウェアの追加コピーを購入する必要があります。ネットワーク デバイスおよびコーデックの制限は、ライセンス登録によって実施されます。
- Reproduction and Distribution. Customers may not reproduce nor distribute the Software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Refer to the Cisco Systems, Inc. End User License Agreement.

1 このマニュアルについて

このマニュアルでは、Prime Infrastructure 2.1 のインストール方法について説明します。

このマニュアルは、Prime Infrastructure の設定、モニタ、およびメンテナンスと、起こり得る問題のトラブルシューティングを担当する管理者を対象としています。これらの管理者は、VMware OVA アプリケーション、仮想化コンセプト、および仮想環境に精通している必要があります。

この製品の設定と管理の詳細については、『*Cisco Prime Infrastructure 2.1 Administrator Guide*』および『*Cisco Prime Infrastructure 2.1 User Guide*』を参照してください。

このマニュアルでは、お客様が用意したハードウェアに限定して、OVA として Prime Infrastructure をインストールする方法について説明します。Prime Infrastructure は、ハードウェア アプライアンスとして使用することもできます。アプライアンスのインストール方法については、『*Cisco Prime Infrastructure 2.1 Appliance Hardware Installation Guide*』を参照してください。

2 製品概要

Cisco Prime Infrastructure は、有線/ワイヤレス アクセス、キャンパス、ブランチ ネットワークの包括的なライフ サイクル管理、エンドユーザの接続性に対する豊富な可視性、およびアプリケーション パフォーマンスの保証問題のための単一の統合ソリューションを提供します。Cisco Prime Infrastructure は、企業 IT への「個人所有デバイスの持ち込み」（BYOD）の実現し、新しいサービスのロールアウト、モバイル デバイスのセキュアなアクセスと管理を加速します。アプリケーション パフォーマンスの可視性およびネットワーク制御とクライアントの認識とを緊密に結びつけることで、Cisco Prime Infrastructure は、エンドユーザに妥協のない品質のエクスペリエンスを保証します。Cisco Identity Services Engine（ISE）の機能を使用した緊密な統合によって、セキュリティとポリシー関連の問題を通してこの視覚化が拡張され、クライアントのアクセスの問題を解決するための明確な手順とともに、この問題の完璧な表示を提供します。

3 主な機能

手順は次のとおりです。

- Prime Infrastructure の機能と利点の概要については、最新のCisco Prime Infrastructure データ シートを参照してください。
- Prime Infrastructure2.1 での新機能の概要については、『*Release Notes for Cisco Prime Infrastructure 2.1* 』を参照してください。
- 最もよく使用される Prime Infrastructure の機能の詳細については、『*Cisco Prime Infrastructure 2.1 User Guide*』を参照してください。
- 管理者を対象とした Prime Infrastructure の機能の詳細については、『*Cisco Prime Infrastructure 2.1 Administrator Guide*』を参照してください。

4 Cisco Prime Infrastructure のライセンスについて

Prime Infrastructure 機能にアクセスするには Lifecycle ライセンスの購入、Prime Infrastructure の保証機能にアクセスするには Assurance ライセンスの購入が必要です。各ライセンスは、これらの機能を使用して管理できるデバイスの数を制御します。

Prime Infrastructure を初めてインストールした場合は、組み込まれている評価ライセンスを使用してライフサイクルおよび保証の管理機能にアクセスできます。デフォルトの評価ライセンスは 60 日間、最大 100 台のデバイスに対して有効です。次の場合、licensing@cisco.com に要求を送信します。

- 評価期間を延長する必要がある。
- デバイス数を増やす必要がある。
- すでに特定の機能のライセンスがあり、他の機能のライセンスを評価する必要がある。

Prime Infrastructure は物理アプライアンスまたは仮想アプライアンスを使用して展開されます。新しいライセンスを追加するには、標準ライセンス センター GUI を使用します。新しいライセンスは、物理アプライアンスの場合標準の Cisco Unique Device Identifier（UDI）、仮想アプライアンスの場合 Virtual Unique Device Identifier（VUDI）を使用してロックされます。この情報は、Prime Infrastructure Web インターフェイスで [Administration] > [Licenses] を選択して表示できます。

その他の参考資料は次のとおりです。

- Cisco Prime Infrastructure のライセンスの種類と注文方法については、『*Cisco Prime Infrastructure 2.1 Ordering and Licensing Guide*』を参照してください。
- 購入済みのライセンスを適用する方法については、『*Cisco Prime Infrastructure 2.1 User Guide*』を参照してください。

5 インストール前の作業

Prime Infrastructure をインストールする前に、次の項の作業を終了してください。

システム要件

サーバ要件

Prime Infrastructure は 3 つの異なるシステムサイズ オプションにあらかじめパッケージされています。表 1 で、各オプションの最小限のサーバ要件について説明します。

表 1　　Prime Infrastructure サーバの最小限の要件

要件	Express	Custom Express[1]	Standard	Pro
VMware バージョン	ESXi 4.1、5、または 5.1	ESXi 4.1、5、または 5.1	ESXi 5 または 5.1	ESXi 5 または 5.1
仮想 CPU	4	8	16	16
メモリ（DRAM）	12 GB	16 GB	16 GB	24 GB
HDD サイズ	300 GB	600 GB	900 GB	1200 GB
スループット（ディスク I/O）	200 MB/s	200 MB/s	200 MB/s	200 MB/s

1. Custom Express は、別の OVA ダウンロードとしては使用できません。代わりに、Express OVA をダウンロードしてから、Custom Express の要件に合わせてカスタマイズする必要があります。カスタマイズの詳細については、シスコの販売担当者にお問い合わせください。

3 種類の Prime Infrastructure オプションのどれも、ご使用のハードウェア上で Open Virtualization Archive（OVA）として、VMWare ESXi または ESX で実行できます。この実装を選択した場合、使用するサーバは、表に示す選択したオプションの要件を満たすか上回っている必要があります。

Prime Infrastructureは、Standard オプションの要件を満たすか上回る物理アプライアンスとして、シスコが提供するハードウェアにプレインストールされたものでも入手可能です。

*注記：

- Express オプションは、Prime Infrastructure の以前のバージョンで提供されていた Medium および Small オプションを置き換えます。
- Standard オプションは、Prime Infrastructure の以前のバージョンで提供されていた Large オプションを置き換えます。
- Pro オプションは、Prime Infrastructure の以前のバージョンで提供されていた Extra Large オプションを置き換えます。

Prime Infrastructure を OVA として選択したオプションに対する最小限の要件を満たすか超えているサーバにインストールする場合（またはインストール後に CPU、メモリまたはディスクを増設する場合）、追加のリソースを使用して製品パフォーマンスを向上させるように OVA を調整できます。「Improving Prime Infrastructure Performance」（『*Cisco Prime Infrastructure 2.1 Administrator Guide*』）を参照してください。

各オプションの最大管理容量については、「Prime Infrastructure の拡張」（P.5）を参照してください。

Web クライアントの要件

Prime Infrastructure ユーザは Web ブラウザ クライアントを使用して、製品にアクセスします。Web クライアントの要件は次のとおりです。

- ハードウェア：次のテスト済みサポート ブラウザのいずれかに対応している Mac または Windows のラップトップまたはデスクトップ。
  - Google Chrome 31 以降。
  - Microsoft Internet Explorer 8.0 または 9.0、Google Chrome Frame プラグインを使用（簡易 Lobby Ambassador インターフェイスにログインするユーザはプラグイン不要）。
  - Mozilla Firefox ESR 24。
  - Mozilla Firefox 24、25、または 26。
- 表示解像度：画面解像度を 1280 x 800 以上に設定することを推奨します。
- Adobe Flash Player：Prime Infrastructureの機能が適切に動作するには、Adobe Flash Player をクライアント マシンにインストールする必要があります。Adobe の Web サイトから、Adobe Flash Player の最新バージョンをダウンロードして、インストールすることを推奨します。

Prime Infrastructure の拡張

Prime Infrastructure にはさまざまなサーバ インストール オプションがあります（「システム要件」（P.4）を参照してください）。ネットワークの規模と複雑さに合ったオプションを選択したことを確認します。

表 2 に、各オプションのデバイス、クライアント、イベント、Netflow データ フローの最大数、およびその他のスケール パラメータを示します。

表 2　　Prime Infrastructure のインストール オプションの対応スケール（Assurance を含む）

パラメータ（最大数）	エクスプレス	Custom Express[1]	Standard	Pro
ユニファイド AP	300	2,500	5,000	20,000
自律 AP	300	500	3,000	3,000
有線デバイス	300	500	6,000	13,000
NAM	5	5	500	1,000
コントローラ	5	50	500	1,000
Wired Clients	6,000	50,000	50,000	50,000
Wireless Clients	4,000	30,000	75,000	200,000
変更クライアント	1,000	5,000	25,000	40,000
イベント継続レート（イベント数 / 秒）	100	100	300	1,000
NetFlow レート（フロー数 / 秒）	3,000	3,000	16,000	80,000
インターフェイス	12,000	50,000	250,000	350,000
有効 NAM データ ポーリング	5	5	20	40
キャンパスごとのサイト数	200	500	2,500	2,500
グループ：ユーザ定義 + アウト オブ ザ ボックス + デバイス グループ + ポート グループ	50	100	150	150
仮想ドメイン	100	600	1,200	1,200
同時使用 GUI クライアント	5	10	25	25
同時使用 API クライアント	2	2	5	5

1. Custom Express は、別の OVA ダウンロードとしては使用できません。代わりに、Express OVA をダウンロードしてから、Custom Express の要件に合わせてカスタマイズする必要があります。カスタマイズの詳細については、シスコの販売担当者にお問い合わせください。

プレインストールされたシスコ提供のハードウェア アプライアンスの拡張限度は、Standard オプションと同じです。

プラグ アンド プレイ ゲートウェイの拡張

Prime Infrastructure のプラグ アンド プレイ ゲートウェイには、イベント ポート（11011 ～ 110XX）で使用できる最大デバイス接続数に管理上の上限があります。その上限数は、統合したサーバとスタンドアロン サーバで異なります。表 3 に、プラグ アンド プレイ ゲートウェイのインストールごとの、最大デバイス接続数とポート数を示します。開かれたイベント ポートごとに最大 1,000 台のデバイス接続をサポートできます。同時に 100 ～ 200 台のデバイスに対してプラグ アンド プレイをアクティブにできます。

表 3　　プラグ アンド プレイ ゲートウェイでの最大デバイス接続数

PnP のインストール	最大デバイス数	全ポート数	注
統合	2,000	2	ポート数は固定：SSL 用に開いた ポートを 1 つ、プレーン テキスト用に 1 つ。
スタンドアロン	1,000	10	SSL とプレーン テキストでのポート数はセットアップ時に設定可能。ただし、設定するポートの合計数は 10 が上限。

Prime Infrastructure と Assurance で使用されるポート

表 4 に、Prime Infrastructure と Assurance で使用されるポートの一覧を示します。これらのポートをファイアウォールで開く必要があります。

表 4　　Prime Infrastructure と Assurance で使用されるポート

ポート	プロトコル	方向	用途
7	TCP/UDP	サーバからエンド ポイントへ	エンド ポイントは ICMP によって検出
20、21	TCP	二方向サーバ / デバイス	デバイス間でのファイルの FTP 転送
		サーバから Cisco.com へ	Cisco.com からのファイルの FTP ダウンロード
22	TCP	サーバからエンド ポイントへ	トラブルシューティング プロセス時にエンドポイントへの SSH 接続を開始する。
		クライアントからサーバへ	Prime Infrastructure サーバに接続する。
23	TCP	サーバからデバイスへ	デバイスとの Telnet 通信
25	TCP	サーバから SMTP サーバへ	SMTP 電子メールのルーティング
49	TCP/UDP	サーバから TACACS サーバへ	TACACS を使用してユーザを認証
53	TCP/UDP	サーバから DNS サーバへ	DNS
69	UDP	デバイスからサーバへ	TFTP
161	UDP	サーバからデバイスへ	SNMP ポーリング
162	TCP/UDP	エンド ポイントからサーバへ	SNMP トラップ レシーバ ポート
443	TCP	クライアントからサーバへ	HTTPS を介した Prime Infrastructure へのブラウザ アクセス（デフォルトでは有効）。このポートは、Prime Infrastructure サーバと cisco.com との間でのソフトウェア更新の確認にも使用されます。
514	UDP	デバイスからサーバへ	Syslog サーバ
1099	TCP/UDP	AAA サーバからサーバへ	RMI レジストリ
1315 ～ 1319	TCP/UDP	プライマリ サーバからセカンダリ サーバ、セカンダリ サーバからプライマリ サーバ	プライマリおよびセカンダリの Prime Infrastructure 間の高可用性データベース接続を設定するため。
1522	TCP/UDP	プライマリ サーバからセカンダリ サーバ、セカンダリ サーバからプライマリ サーバ	プライマリおよびセカンダリの Prime Infrastructure 間の高可用性データベース接続を設定するため。
1645	UDP	サーバから RAS へ	RADIUS リモート アクセス サーバで Prime Infrastructure ユーザを認証
1646		RAS からサーバ	
1812		サーバから RAS へ	
1813		RAS からサーバ	
4444	TCP	AAA サーバからサーバへ	RMI サーバ
8080	TCP	クライアントからサーバへ	HTTP を使用した Prime Infrastructure へのブラウザ アクセス（デフォルトでは無効）
8082	TCP	サーバからクライアントへ	Health Monitor web インターフェイス、Apache/Tomcat JSP エンジン
8087			セカンダリ サーバが同期モードの場合のセカンダリ サーバ Software Update ページ

表 4　　Prime Infrastructure と Assurance で使用されるポート （続き）

ポート	プロトコル	方向	用途
8443[1]	TCP	サーバからコール プロセッサへ	RTMT と Cisco Unified CM 登録用の HTTPS 接続
		クライアントからサーバへ	HTTPS を使用した Prime Infrastructure へのブラウザ アクセス（デフォルトでは有効）
9991[1]	UDP	デバイスからサーバへ	NetFlow および NAM データ レシーバ
10022 ～ 10041	TCP	デバイスからサーバへ	パッシブ FTP ファイル転送に使用するポート範囲（コントローラ バックアップ、デバイス設定、レポート検索など）
11011[2]	TCP	エンド ポイントからサーバへ	プラグ アンド プレイ ゲートウェイのプレーン テキスト ディスパッチャ ポート
11012			プラグ アンド プレイ ゲートウェイの SSL ディスパッチャ ポート
11013			プレーン テキスト プラグ アンド プレイ ポート
11014			プラグ アンド プレイ ゲートウェイの SSL ポート
16113	TCP	コントローラからロケーション サーバへ、LS からコントローラへ	シスコのネットワーク モビリティ サービス プロトコルのメッセージング
20514[1]	UDP	エンド ポイントからサーバへ	syslog レシーバ
61617[3]	TCP	サーバからエンド ポイントへ	Java Message Service 接続用の SSL ポート

1. 保証付き Prime Infrastructure によってのみ使用。
2. プラグ アンド プレイ ゲートウェイを Prime Infrastructure サーバと統合する場合に使用します。
3. Prime Infrastructure プラグ アンド プレイ ゲートウェイでのみ使用されます。

スタンドアロン サーバ上のプラグ アンド プレイ ゲートウェイで使用されるポート

表 5 に、スタンドアロン サーバにインストールする際に、プラグ アンド プレイ ゲートウェイで使用されるポートの一覧を示します。

表 5　　プラグ アンド プレイ ゲートウェイで使用されるポート

ポート	プロトコル	方向	用途
21	FTP	ゲートウェイへのエンドポイント	内部プラグ アンド プレイ ゲートウェイの FTP サービス ポート
22	SSH	—	管理ユーザがログインしプラグ アンド プレイ ゲートウェイをモニタするポート。
69	TFTP	—	Prime Infrastructure からプラグ アンド プレイ ゲートウェイにイメージと設定をダウンロードする際に使用
80	HTTP	ゲートウェイへのエンドポイント	プラグ アンド プレイ ゲートウェイの HTTP サービス ポート
443	HTTPS	ゲートウェイへのエンドポイント	プラグ アンド プレイ ゲートウェイの HTTP サービス ポート
11012	TCP	デバイスからサーバへ	プラグ アンド プレイ ゲートウェイの SSL ディスパッチャ ポート
11014			プラグ アンド プレイ ゲートウェイの SSL イベント ポート
11016			
11018			
11020			
11022			

表 5　　プラグ アンド プレイ ゲートウェイで使用されるポート （続き）

ポート	プロトコル	方向	用途
11011	TCP	デバイスからサーバへ	プラグ アンド プレイ ゲートウェイのプレーン テキスト ディスパッチャ ポート
11013			プラグ アンド プレイ ゲートウェイのプレーン テキスト イベント ポート
11015			
11017			
11019			
11021			
62616	SSL	—	プラグ アンド プレイ ゲートウェイ内部メッセージ サーバ ポート
61617	SSH	—	Prime Infrastructure に接続するプラグ アンド プレイ ゲートウェイ ポート

Prime Infrastructure に対するデバイスの設定

インストールする前に、SNMP 通知などの必要となるデータを Prime Infrastructure に提供できるようにデバイスを設定します。

必要なソフトウェア バージョンおよび設定

Prime Infrastructure と共に動作させるには、サポートされているデバイスの一覧に示されている最低要件のソフトウェア バージョンを、お使いのデバイスで実行させておく必要があります。Prime Infrastructure のユーザ インターフェイスを使用し、[Help] > [Supported Devices List] を選択すれば、この一覧にアクセスできます。

また、次の項で説明されたように、デバイスが SNMP トラップおよび syslog と、ネットワーク タイム プロトコル（NTP）をサポートするよう設定する必要があります。

SNMP の設定

Prime Infrastructure が SNMP デバイスを照会し、それらからトラップと通知を受信できるようにするには、次の作業を行う必要があります。

- Prime Infrastructure を使用して管理する各デバイス上で SNMP クレデンシャル（コミュニティ ストリング）を設定します。
- 同じそれらのデバイスで、SNMP 通知を Prime Infrastructure サーバに送信するように設定します。

次の IOS コンフィギュレーション コマンドを使用して、読み取り/書き込みおよび読み取り専用のコミュニティ ストリングを SNMP デバイス上で設定します。

`admin(config)#` **snmp-server community** *private* **RW**

`admin(config)#` **snmp-server community** *public* **RW**

ここで、*private* と *public* は、設定するコミュニティ ストリングです。

コミュニティ ストリングの設定後に、各 SNMP デバイスで次の IOS グローバル コンフィギュレーション コマンドを使用して、デバイス通知をトラップとして Prime Infrastructure サーバに送信するよう指定できます。

`admin (config)#` **snmp-server host** *Host* **traps** *version community notification-type*

値は次のとおりです。

- *Host* は、Prime Infrastructure サーバの IP アドレスです。
- *version* は、トラップの送信に使用される SNMP のバージョンです。
- *community* は、通知動作でサーバに送信されるコミュニティ ストリングです。
- *notification-type* は、送信されるトラップのタイプです。

帯域幅の使用と、追加コマンドを使用して Prime Infrastructure サーバに送信されるトラップ情報の量を制御する必要がある場合があります。

SNMP の設定については、次を参照してください。

- 『IOS Command Reference』の「snmp-server community」および「snmp-server host」の項。
- 『Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2』の「Configuring SNMP Support」の項および「list of notification-type values」。

NTP の設定

ネットワーク タイム プロトコル（NTP）同期は、ネットワーク内のすべてのデバイスと Prime Infrastructureサーバで設定する必要があります。サーバのインストール時に NTP サーバを指定する必要があります（参照「サーバのインストール」(P.20)）。

NTP は Prime Infrastructure 関連サーバのすべてで設定と同期がなされている必要があり、これにはバックアップ用のリモート FTP サーバ、セカンダリ Prime Infrastructure ハイ アベイラビリティ サーバ、プラグ アンド プレイ ゲートウェイ、VMware vCenter および ESX 仮想マシンなどが含まれます。ネットワーク全体の時刻の同期に問題がある場合、Prime Infrastructure の結果に異常が発生するおそれがあります。

保証付き Prime Infrastructure のデータ ソースの設定

保証ライセンスの場合、お使いのネットワーク インターフェイスとサービスを Assurance がモニタできるように事前インストール タスクを完了しておく必要があります。これらのタスクについては、「サポートされる保証のデータ ソース」を参照してください。これらのタスクは追加で「Prime Infrastructure に対するデバイスの設定」（P.8）で説明されています。

サポートされる保証のデータ ソース

保証付き Prime Infrastructure では、エクスポートされたデータ ソース（表 6 参照）を使用してネットワーク デバイスからのデータを収集する必要があります。この表には、各ソースについて、その形式のエクスポートをサポートするデバイスと、データをエクスポートするためにデバイス上で動作していなければならない IOS またはその他のソフトウェアの最小バージョンが示されています。

表 6 を使用して、ネットワーク デバイスとそれらのソフトウェアが、Prime Infrastructure で使用されるデータ ソースのタイプに対応していることを確認します。必要に応じて、ハードウェアやソフトウェアをアップグレードします。なお、示されている各ソフトウェア バージョンは、*最小*であることに注意してください。同じソフトウェアまたは IOS のリリース トレイン内であれば以降の任意のバージョンをデバイス上で実行できます。

さらに、Prime Infrastructure が SNMP を使用してデータを収集できるように、変更が必要になる場合もあります。「SNMP の設定」の説明を参照してください。

保証データ ソースの設定

インストールを行う前に、表 6 に示されているサポート対象のデバイスが、障害データ、アプリケーション データ、およびパフォーマンス データを Prime Infrastructure に提供できるようにする必要があります。また、ネットワーク全体にわたって時刻と日付の情報を一致させる必要があります。以降のトピックでは、この作業を行う方法のガイドラインを示します。

表 6　Prime Infrastructure Assurance：サポートされているデータ ソース、デバイスおよびソフトウェア バージョン

デバイス タイプ	NetFlow をサポートする Cisco IOS リリース	サポートされる NetFlow エクスポート タイプ	NetFlow の設定
Catalyst 3750-X/3560-X	15.0(1)SE IP ベースまたは IP サービス フィーチャ セット、およびネットワーク サービス モジュールを装備。	TCP および UDP トラフィック	『*Cisco Prime Infrastructure 2.1 User Guide*』の「Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches」の項を参照してください。
Catalyst 3850	15.0(1)EX	TCP および UDP トラフィック、音声とビデオ	TCP および UDP トラフィックを設定するには、『*Cisco Prime Infrastructure 2.1 User Guide*』の「Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches」の項を参照してください。 音声とビデオを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Medianet - PerfMon]**
Catalyst 4500	15.0(1)XO および 15.0(2)	TCP および UDP トラフィック、音声とビデオ	TCP および UDP トラフィックを設定するには、『*Cisco Prime Infrastructure 2.1 User Guide*』の「Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches」の項を参照してください。 音声とビデオを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Medianet - PerfMon]**
Catalyst 6500	SG 15.1(1) SY	TCP および UDP トラフィック、音声とビデオ	TCP および UDP トラフィックを設定するには、『*Cisco Prime Infrastructure 2.1 User Guide*』の「Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches」の項を参照してください。 音声とビデオを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Medianet - PerfMon]**
ISR	15.1(3) T	TCP および UDP トラフィック、音声とビデオ	TCP および UDP トラフィックを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Collecting Traffic Statistics]** 音声とビデオを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Medianet - PerfMon]**
ISR G2	15.2(1) T および 15.1(4)M	TCP および UDP トラフィック、アプリケーション応答時間、音声とビデオ	TCP、UDP、ART を設定するには、『Cisco Prime InfrastructureUser Guide』の「Configuring NetFlow on ISR Devices」の項を参照してください。 音声とビデオを設定するには、この CLI テンプレートを使用します。 **[Design] > [Feature Design] > [CLI Templates] > [System Templates - CLI] > [Medianet - PerfMon]**

表 6　Prime Infrastructure Assurance：サポートされているデータ ソース、デバイスおよびソフトウェア バージョン　（続き）

デバイス タイプ	NetFlow をサポートする Cisco IOS リリース	サポートされる NetFlow エクスポート タイプ	NetFlow の設定
ISR G2	15.2(4) M2 以降、15.3(1)T 以降	TCP および UDP トラフィック、アプリケーション応答時間、音声とビデオ	TCP、UDP、ART を設定するには、『*Cisco Prime Infrastructure 2.1 User Guide*』の「Configuring Application Visibility」の項を参照してください。
ASR	15.3(1)S1 以降	TCP および UDP トラフィック、アプリケーション応答時間、音声とビデオ、HTTP URL 可視性	
ISR G3	15.3(2)S 以降		

Medianet NetFlow のイネーブル化

Cisco Prime Infrastructure で Medianet データを利用できるようにするには、ネットワーク デバイスで次の作業を行う必要があります。

- Prime Infrastructure でサポートされている基本的な統計情報について Medianet NetFlow データ エクスポートをイネーブルにします。
- Medianet NetFlow データを Prime Infrastructure サーバおよびポートにエクスポートします。

次の例のような設定を使用して、Prime Infrastructure が、必要な Medianet データを取得するようにします。

```
flow record type performance-monitor PerfMonRecord
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect application media bytes counter
  collect application media bytes rate
  collect application media packets counter
  collect application media packets rate
  collect application media event
  collect interface input
  collect interface output
  collect counter bytes
  collect counter packets
  collect routing forwarding-status
  collect transport packets expected counter
  collect transport packets lost counter
  collect transport packets lost rate
  collect transport round-trip-time
  collect transport event packet-loss counter
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect timestamp interval
  collect ipv4 dscp
  collect ipv4 ttl
  collect ipv4 source mask
  collect ipv4 destination mask
  collect monitor event
flow monitor type performance-monitor PerfMon
  record PerfMonRecord
  exporter PerfMonExporter
flow exporter PerfMonExporter
  destination PrInIP
  source Loopback0
  transport udp PiInPort
```

```
policy-map type performance-monitor PerfMonPolicy
  class class-default
!Enter flow monitor configuration mode.
flow monitor PerfMon
!Enter RTP monitor metric configuration mode.
monitor metric rtp
!Specifies the minimum number of sequential packets required to identify a stream as being an RTP flow.
min-sequential 2
!Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring metrics.
max-dropout 2
!Specifies the maximum number of reorders allowed when sampling RTP video-monitoring metrics.
max-reorder 4
!Enter IP-CBR monitor metric configuration mode
  monitor metric ip-cbr
!Rate for monitoring the metrics (1 packet per sec)
  rate layer3 packet 1
interface interfacename
  service-policy type performance-monitor input PerfMonPolicy
  service-policy type performance-monitor output PerfMonPolicy
```

この設定例では、次の変数が使用されています。

- *PrInIP* は、Prime Infrastructure サーバの IP アドレスです。
- *PiInPort* は、Prime Infrastructure サーバが Medianet データをリッスンしている UDP ポートです（デフォルトは 9991）。
- *interfaceName* は、Medianet NetFlow データを指定の *PrInIP* に送信しているインターフェイスの名前です（GigabitEthernet0/0 や fastethernet 0/1 など）。

Medianet 設定の詳細については、『*Medianet Reference Guide*』を参照してください。

NetFlow と Flexible NetFlow のイネーブル化

Prime Infrastructure で NetFlow データを利用できるようにするには、ネットワーク デバイスで次の作業を行う必要があります。

- モニタするインターフェイス上で NetFlow をイネーブルにします。
- NetFlow データを Prime Infrastructure サーバおよびポートにエクスポートします。

バージョン 2.1 では、Prime Infrastructure は Flexible NetFlow のバージョン 5 と 9 をサポートします。NetFlow は、Prime Infrastructure のデータ収集対象となる各*物理*インターフェイス上でそれぞれイネーブルにする必要があります。通常、これらは、イーサネット インターフェイスか WAN インターフェイスです。これは、物理インターフェイスにのみ適用されます。VLAN およびトンネルに対しては NetFlow をイネーブルにする必要はありません。物理インターフェイス上で NetFlow をイネーブルにすれば、それらも自動的に含められます。

次のコマンドを使用して、Cisco IOS デバイス上で NetFlow をイネーブルにします。

Device(config)# **interface** *interfaceName*

Device(config)# **ip route-cache flow**

ここで、*interfaceName* は、NetFlow を有効にするインターフェイスの名前です（fastethernet や fastethernet0/1 など）。

NetFlow をデバイスでイネーブルにした後、エクスポータを設定して NetFlow データを Prime Infrastructure にエクスポートする必要があります。エクスポータは次のコマンドで設定できます。

Device(config)# **ip flow-export version 5**

Device(config)# **ip flow-export destination** *PrInIP PiInPort*

Device(config)# **ip flow-export source** *interfaceName*

値は次のとおりです。

- *PrInIP* は Prime Infrastructure サーバの IP アドレス
- *PiInPort* は、Prime Infrastructure サーバが NetFlow データをリッスンしている UDP ポート（デフォルトは 9991）
- *interfaceName* は、NetFlow データを指定の *PrInIP* に送信しているインターフェイスの名前。これにより、NetFlow エクスポート データグラムの一部として、送信元インターフェイスの IP アドレスが Cisco Prime Infrastructure に送信されます。

同じルータに複数の NetFlow エクスポータを設定する場合、これらのうち 1 つだけが Prime Infrastructure サーバにエクスポートするようにします。同じ送信先にエクスポートするエクスポータが同じルータに複数ある場合は、データが破損する恐れがあります。

NetFlow がデバイスで動作していることを確認するには、次のコマンドを使用します。

```
Device# show ip flow export
Device# show ip cache flow
Device# show ip cache verbose flow
```

NetFlow 設定の詳細については、次を参照してください。

- *『Cisco IOS Switching Services Configuration Guide, Release 12.1』*
- *『Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T』*
- *『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』*
- *『Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting』*

Network Analysis Module（NAM）の導入

ネットワーク内で NAM を適切に設置する必要があります。詳細については、以下を参照してください。

- 『*Cisco Network Analysis Module Software 5.1 User Guide*』: 導入シナリオが掲載されており、ブランチ内での NAM の導入や WAN 最適化向けの NAM の導入など、さまざまなトピックを扱っています。
- 『*Cisco Network Analysis Module Deployment Guide*』:「Places in the Network Where NAMs Are Deployed」のトピックを参照してください。

NAM が適切に導入されれば、インストール前に必要な追加の作業はありません。Cisco Prime AM を使用して検出を実行する場合、各 NAM に対して HTTP アクセス クレデンシャルを入力する必要があります。

Prime Infrastructure は、より効率的な REST インターフェイスを使用して NAM を照会します。そのため、NAM からの NetFlow データの直接エクスポートをサポートしていません。NetFlow データをエクスポートしているデバイスは、その NetFlow データを NAM 経由ではなく、Prime Infrastructure に直接エクスポートする必要があります。NAM から Cisco Prime Infrastructure に NetFlow データがエクスポートされると、データの重複が発生します。

Performance Agent のイネーブル化

Prime Infrastructure がアプリケーション パフォーマンス データを収集できるようにするには、IOS *mace*（測定、集約、相関エンジン）キーワードを使用して、ブランチ オフィスとデータセンターのルータ上に Performance Agent（PA）データ フロー ソースを設定します。

たとえば、IOS グローバル コンフィギュレーション モードで次のコマンドを使用して、PA フロー エクスポータをルータ上に設定します。

```
Router (config)# flow exporter mace-export
Router (config)# destination 172.30.104.128
Router (config)# transport udp 9991
```

次のようなコマンドを使用して、フローがルータを通過するアプリケーションのフロー レコードを設定します。

```
Router (config)# flow record type mace mace-record
Router (config)# collect application name
Router (config)# collect art all
```

ここで、*application name* は、フロー データの収集対象となるアプリケーションの名前です。

PA フロー モニタ タイプを設定するには、次のコマンドを使用します。

```
Router (config)# flow monitor type mace mace-monitor
Router (config)# record mace-record
Router (config)# exporter mace-export
```

対象となるトラフィックを収集するには、次のようなコマンドを使用します。

```
Router (config)# access-list 100 permit tcp any host 10.0.0.1 eq 80
```

```
Router (config)# class-map match-any mace-traffic
Router (config)# match access-group 100
```

PA ポリシー マップを設定し、PA トラフィックを正しいモニタに転送するには、次のコマンドを使用します。

```
Router (config)# policy-map type mace mace_global
Router (config)# class mace-traffic
Router (config)# flow monitor mace-monitor
```

最後に、WAN インターフェイス上で PA をイネーブルにします。

```
Router (config)# interface Serial0/0/0
Router (config)# mace enable
```

Performance Agent の設定の詳細については、『*Cisco Performance Agent Deployment Guide*』を参照してください。

6 Cisco Prime Infrastructure のアップグレード

次の Cisco Prime Infrastructure（およびそれ以前の）製品は Cisco Prime Infrastructure2.1 にアップグレードできます。

- Cisco Prime Infrastructure2.0.0.0.294
- Cisco Prime Infrastructure 1.3.0.20

1.3.0.20 以前のバージョンを使用している場合は、『*Cisco Prime Infrastructure 2.0 Quick Start Guide*』の手順を参照して、ソフトウェアをバージョン 2.0 にアップグレードしてください。現在、バージョン 1.4.x からバージョン 2.1 へのアップグレード パスはありません。

2.1 へのアップグレードを行う前に、まず『表 7』に一覧表示されている適切なパッチをダウンロードしてください。その後、「パッチのインストール」（P.15）の手順でパッチをインストールします。適切なパッチをインストールした後、システムの移行またはインライン アップグレードを実行する前に、新しいアプリケーションをバックアップする必要があります。

表 7　　重要なポイント パッチ

使用中のバージョン	アップグレードする前にインストールするパッチ
Prime Infrastructure 1.3.0.20（1.3.0.20-2 を含む）	PI_1_3_0_20-Update.4-16.tar.gz

パッチのインストール後に、次のいずれかの方法によって、これらのバージョンを 2.1 にアップグレードできます。

1. **システムの移行**：Cisco Prime Infrastructure 2.1 を新しいシステムとして新しいホストにインストールし、新しいホストに既存のシステムのデータを復元します。次に、古いホストを解放できます。このオプションは、より大規模な OVA に移行する、大規模なネットワークが存在する、またはサービスのダウンタイムを見過ごすことができないといった場合に優先されます。詳細については、「新システムへの移行」（P.16）を参照してください。
2. **インライン アップグレード**：既存のシステムをバージョン 2.1 にアップグレードします。既存のすべてのデータが保持され、アップグレードの完了後も同じサイズの OVA を使用します。既存の製品はアップグレードが完了するまで使用できません。このオプションは、同じサイズの OVA を維持する場合や、アップグレード中のサービスのダウンタイムが許容できる場合に優先されます。詳細については、「インライン アップグレードの実行」（P.17）を参照してください。

Prime Infrastructure のアプリケーション バックアップにはライセンス データが含まれます。*最新のアプリケーション バックアップを使用して、以前のシステムからアップグレードしたシステムにライセンス データを復元する*のであれば、新しいシステムや仮想マシンに再インストールしても、ライセンスを再ホストする必要はありません。その他の場合は、licensing@cisco.com に要求を電子メールで送信し、ライセンスを再ホストする必要があります。要求には、ライセンスを含む VUDI の詳細や既存のライセンスの詳細を含める必要があります。

パッチのインストール

アップグレードがサポートされているレベルまで Prime Infrastructure のバージョンを上げるために、パッチのインストールが必要になる場合があります。たとえば、バージョン 1.3.0 の Cisco Prime Infrastructure を現在実行している場合、アップグレードを行う前に PI_1_3_0_20-Update.4-16 のパッチをインストールする必要があります。動作中の Prime Infrastructure のバージョンとパッチ バージョンは、**show version** と **show application** の CLI コマンドで確認できます。

Prime Infrastructure およびその以前の製品の各バージョンについて、異なるポイント パッチ ファイルが提供されます。既存のシステムのバージョンに対応させるために必要なパッチ ファイルをダウンロードしてインストールします。これは新しいバージョンにアップグレードする前に必要です。適切なパッチを見つけるには、ブラウザで Cisco Download Software navigator を開きます。

パッチをインストールする前に、Prime Infrastructure サーバのデフォルト リポジトリにパッチ ファイルをコピーする必要があります。多くのユーザは、パッチ ファイルをまずローカル FTP サーバにダウンロードし、それからリポジトリにコピーするのが楽だと感じています。また、次のいずれかの方法でも、デフォルトのリポジトリにパッチ ファイルをコピーできます。

- cdrom：ローカルの CD-ROM ドライブ（読み取り専用）
- disk：ローカルのハード ディスク領域
- ftp：FTP サーバを使用している URL
- http：HTTP サーバを使用している URL（読み取り専用）
- https：HTTPS サーバを使用している URL（読み取り専用）
- nfs：NFS サーバを使用している URL
- sftp：SFTP サーバを使用している URL
- tftp：TFTP サーバを使用している URL

ステップ 1 ご使用の環境内のローカル リソースに、適切なポイント パッチをダウンロードします。

a. ブラウザに Cisco Download Software navigator を表示し、[Products] > [Cloud and Systems Management] > [Routing and Switching Management] > [Network Management Solutions] > [Cisco Prime Infrastructure] と選択します。

b. 現在使用しているものに最も近い Cisco Prime Infrastructure のバージョンを選択します（例：**Cisco Prime Infrastructure 1.2**）。

c. [Prime Infrastructure Patches] をクリックして、製品のそのバージョンに適用可能なパッチのリストを表示します。

d. 必要な各パッチの横で [Download] をクリックし、プロンプトに従ってファイルをダウンロードします。

ステップ 2 Prime Infrastructure サーバでコマンドライン インターフェイス セッションを開きます（『*Cisco Prime Infrastructure 2.1 Administrator Guide*』の「Connecting Via CLI」を参照）。

ステップ 3 ダウンロードしたパッチ ファイルをデフォルトのローカル リポジトリにコピーします。次に例を示します。

```
admin# copy source path/defaultRepo
```

それぞれの説明は次のとおりです。

- *source* は、ダウンロードしたパッチ ファイルの場所と名前です（例：`ftp://MyFTPServer/pi_9.3.1.0_update.tar.gz`）。
- *path* は、デフォルトのローカル バックアップ リポジトリ（defaultRepo）への完全パスです。

ステップ 4 パッチをインストールするには、次を実行します。

```
admin# patch install patchFile defaultRepo
```

ここで、*patchFile* は、defaultRepo にコピーしたパッチ ファイルの名前です。

プラグ アンド プレイ ゲートウェイ パッチのインストール

プラグ アンド プレイ ゲートウェイのスタンドアロン サーバ パッチは pnp-gateway-patch-2.0.0.28.tar.gz ファイルから使用できます。

パッチ アップグレード手順では、パッチ ファイルを含む FTP または TFTP サーバが必要です。Cisco Prime Infrastructure 1.2 プラグ アンド プレイ ゲートウェイ スタンドアロン サーバからサーバにアクセスできます。

ステップ 1 管理ユーザとしてプラグ アンド プレイ ゲートウェイ スタンドアロン サーバにログインします。

ステップ 2 リポジトリをコンフィギュレーション モードで作成し、リポジトリの名前およびその他の詳細を提供して repository コマンドを実行します。

ステップ 3 patch install コマンドを使用してプラグ アンド プレイ ゲートウェイ スタンドアロン パッチ pnp-gateway-patch-2.0.0.28.tar.gz をインストールします。

ステップ 4 **pnp setup** コマンドを実行してプラグ アンド プレイ スタンドアロン サーバを再設定し、プラグ アンド プレイ プロセスを開始します。次に例を示します。

```
pnp-server login: admin
Password:
pnp-server/admin# configure
Enter configuration commands, one per line.End with CNTL/Z.
pnp-server/admin(config)# repository <repository_name>
pnp-server/admin(config-Repository)# url ftp://<SERVER_HOST_NAME>/<FOLDER_LOCATION>
pnp-server/admin(config-Repository)# user <USER_ID> password <OPTION> <PASSWORD>
pnp-server/admin(config-Repository)# exit
pnp-server/admin(config)# exit
pnp-server/admin#
pnp-server/admin# patch install pnp-gateway-patch-2.0.0.28.tar.gz
pnp-patching-<VERSION>.tar.gz <repository_name>
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Patch installation...
Patch successfully installed
pnp-server/admin#
pnp-server/admin# pnp setup
```

新システムへの移行

システムの移行は、製品インストールのほとんどのアップグレードで優先される選択肢です。ほとんどの場合、移行を完了するために新しいサーバ ハードウェアを用意する必要があります。

この方法を使用する場合、「Cisco Prime Infrastructure のアップグレード」（P.14）の一覧にあるリリース レベルから移行すること、さらに 表 7（P.14）の一覧にある必要なバックアップと復元のパッチをインストールしてあることが必要となることに注意してください。

ステップ 1 開始する前に、プライマリおよびセカンダリの Prime Infrastructure サーバから、既存のハイ アベイラビリティ設定を削除します。これは、次の選択肢のいずれかを使用して実行できます。

- Prime Infrastructure を起動し、**[Administration] > [High Availability] > [HA Configuration]** と選択し、**[Remove]** をクリックします。
- Prime Infrastructure サーバでコマンドライン インターフェイス セッションを開き（『*Cisco Prime Infrastructure 2.1 Administrator Guide*』の「Connecting Via CLI」を参照）、**ncs ha remove** コマンドを実行します。

ステップ 2 まだしていなかった場合、古いホストのリモート バックアップ リポジトリをセット アップします。詳細については、*Cisco Prime Infrastructure 2.1 Administrator Guide*の「Using Remote Backup Repositories」を参照してください。

ステップ 3 リモート リポジトリの古いホストのアプリケーション バックアップを作成します。詳細については、『*Cisco Prime Infrastructure 2.1 Administrator Guide*』の「Taking Application Backups」を参照してください。

ステップ 4 「Cisco Prime Infrastructure のインストール」（P.19）の説明に従って、新しいホストをインストールします。

ステップ 5 古いホストと同じリモート バックアップ リポジトリを使用するよう、新しいホストを設定します。

ステップ 6 *Cisco Prime Infrastructure 2.1 Administrator Guide*の「Restoring From Application Backups」で説明されているように、リモート リポジトリのアプリケーション バックアップを新しいホストに復元します。

ステップ 7 アップグレード完了後：

- ユーザに対して、アップグレードされた Prime Infrastructure サーバに接続を試行する前に、Prime Infrastructure の古いバージョンにアクセスしたすべてのクライアント マシンのブラウザでキャッシュをクリアするように指示します。
- このリリースへのアップグレード後にバックアップ作成で問題が発生した場合は、『「Prime Infrastructure サーバのディスク領域問題の管理」（P.18）』を参照してください。
- アップグレードの前に外部 AAA（RADIUS または TACACS）を使用している場合は、「AAA 設定の更新」（P.18）を参照してください。
- Prime Infrastructure を使用して Cisco Wireless LAN Controllers を管理している場合は、『「WLC 設定の再同期」（P.18）』を参照してください。

インライン アップグレードの実行

インライン アップグレードはシステムの移行より簡単で、新しいハードウェアも必要ではありません。

ステップ 1 開始する前に、プライマリおよびセカンダリの Prime Infrastructure サーバから、既存のハイ アベイラビリティ設定を削除します。これは、次の選択肢のいずれかを使用して実行できます。

- Prime Infrastructure を起動し、**[Administration] > [High Availability] > [HA Configuration]** と選択し、[Remove] をクリックします。
- Prime Infrastructure サーバでコマンドライン インターフェイス セッションを開き（*Cisco Prime Infrastructure 2.1 Administrator Guide*の「Connecting Via CLI」を参照）、**ncs ha remove** コマンドを実行します。

ステップ 2 まだしていなかった場合、サーバで CLI セッションを開き、cisco.com からダウンロードしたアップグレード ファイルをデフォルトのバックアップ リポジトリにコピーします。

`admin#` **copy** *source path:***/defaultRepo**

それぞれの説明は次のとおりです。

- *source* は、アプリケーションのアップグレード ファイルの URL、パス、およびファイル名です（例：`FTP://<YourFTPServer>/PI-upgrade-bundle-#.#.tar.gz`）。
- *path* は、デフォルトのローカル バックアップ リポジトリ（defaultRepo）への完全パスです。

ステップ 3 **`ncs stop`** コマンドを入力して、Prime Infrastructure サーバを停止します。

ステップ 4 アプリケーション アップグレードの実行:

`admin#` **application upgrade PI-upgrade-bundle-2.1.0.0.87.tar.gz defaultRepo**

この手順は、アプリケーション データベースのサイズによっては、完了するまでに 30 分以上かかる場合があります。

ステップ 5 アップグレード完了後：

- CLI セッションを開き、**ncs status** コマンドを入力して、アプリケーションが実行中であることを確認します。
- ユーザに対して、アップグレードされた Prime Infrastructure サーバに接続を試行する前に、Prime Infrastructure の古いバージョンにアクセスしたすべてのクライアント マシンのブラウザでキャッシュをクリアするように指示します。
- バージョン 2.1 へのアップグレード後にバックアップ作成で問題が発生した場合は、「Prime Infrastructure サーバのディスク領域問題の管理」（P.18）を参照してください。
- アップグレードの前に外部 AAA（RADIUS または TACACS）を使用している場合は、「AAA 設定の更新」（P.18）を参照してください。
- Prime Infrastructure を使用して Cisco Wireless LAN Controllers を管理している場合は、「WLC 設定の再同期」（P.18）を参照してください。

Prime Infrastructure サーバのディスク領域問題の管理

アップグレード *中に*ディスクディスク領域についての問題が発生した場合、次のいずれかの方法を提案します。

- VMware の**設定編集**機能を使用して、OVA に割り当てられたディスク領域を増加させます。
- 「新システムへの移行」（P.16）に説明されているアップグレード方法を使用して、十分なディスク領域を持つサーバにインストールを移動します。

既存のシステムをアップグレードした *後に*、バックアップを作成できない場合は、以下の手順に従ってディスク領域を解放し、正常なバックアップを作成します。`ncs cleanup` コマンド使用後にもバックアップを作成できない場合、Cisco Prime Infrastructure 2.1 Administrator Guideの「Using Remote Backup Repositories」の説明に従って、バックアップ用にリモート FTP リポジトリをセットアップして使用します。

ステップ 1 Prime Infrastructure サーバでコマンドライン インターフェイスを開き（『Connecting Via CLI』を参照）、管理者 ID を使用してサーバにログインします。

ステップ 2 アプリケーション データベースを圧縮するために、コマンド ラインで次のコマンドを入力します。

```
admin# ncs cleanup
```

ステップ 3 プロンプトが表示されたら、[deep cleanup] オプションに「**Yes**」と答えます。操作が完了すると、別のバックアップを実行できるようになります。

AAA 設定の更新

アップグレードする前に、外部 RADIUS または TACACS+ ユーザ認証を使用していた場合、AAA サーバに拡大 Prime Infrastructure 2.1 ユーザのタスク リストを転送する必要があります。Prime Infrastructure をアップグレードした後、TACACS+ または RADIUS サーバに権限を再度追加し、Prime Infrastructure サーバからのタスクで TACACS サーバのロールを更新する必要があります。詳細については、『*Cisco Prime Infrastructure 2.1 Administrator Guide*』の「Setting the AAA Mode」を参照してください。

アップグレード プロセス中に Prime Infrastructure サーバの IP アドレスを変更した場合は、他のユーザがログインする前に、「root」ユーザとして Prime Infrastructure にログインし、「Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes」で示される手順に従う必要があります。

WLC 設定の再同期

アップグレードすると、Cisco Wireless LAN Controller の設定である Prime Infrastructure サーバの記録は、これらのデバイスに保存された設定と同期しないようになります。続ける前に、次の手順でこれらを再同期します。

ステップ 1 Prime Infrastructure にログインし、[Classic] ビューに切り替えます。

ステップ 2 **[Configure] > [Controllers]** を選択します。Prime Infrastructure は、あらゆる Cisco WLC を含む、管理対象のすべてのコントローラの一覧を表示します。

ステップ 3 いずれかの WLC を詳細表示している行で、[Audit Status] 列に示されているステータス リンクをクリックします。Prime Infrastructure は、選択した WLC の監査レポートを表示します。そこには、見つかった **Config Discrepancies** が一覧表示されています。

ステップ 4 **[Audit Now]** をクリックし、続いて [**Refresh Config from Controller**] をクリックします。

ステップ 5 プロンプトが表示されたら、**[Use the configuration on the controller currently]** を選択し、続いて **[Go]** をクリックします。

プロセスが完了すると、「成功」のステータス値で更新設定レポートが表示されます。

ステップ 6 他のすべての WLC に対して、ステップ 3 ～ 5 繰り返します。

7 Cisco Prime Infrastructure のインストール

現在 Cisco Prime Network Control System（NCS）、NCS（WAN）または Prime Assurance Manager の以前のバージョンを実行している場合、インストールするのではなく、アップグレードする必要があります。「Cisco Prime Infrastructure のアップグレード」（P.14）を参照してください。

はじめる前に

仮想マシンで Prime Infrastructure をインストールする前に、次のことを確認する必要があります。

- Prime Infrastructure で動作するように、ネットワーク内のデバイスとデータ ソースをセットアップしている（「インストール前の作業」（P.4）を参照）。
- Prime Infrastructure サーバとして使用する予定のマシン上に VMware ESX/ESXi がインストールされ、設定されている。VMware ホストのセットアップと設定については、VMware のマニュアルを参照してください。
- インストールされた VMware ESX/ESXi ホストが到達可能である。
- VMware vSphere Client が Windows ホスト（またはラップトップ）にインストールされている。VMware vSphere Client をインストールする方法は、VMware のマニュアルを参照してください。ネットワークで仮想ホストが使用可能になった後、その IP アドレスを参照して、VMware vSphere Client のインストールが可能な Web ベース インターフェイスを表示できます。

  VMware vSphere クライアントは Windows ベースのため、Windows PC を使用してクライアントをダウンロードしてインストールします。
- Prime InfrastructureOVA が、vSphere クライアントのインストール先と同じマシンに保存されています。シスコとの取り決めに従って、OVA ファイルを Cisco.com からダウンロードするか、シスコが提供するインストール メディアを使用します。

VMware vSphere Client からの OVA の導入

OVA を導入する前に、システム要件をすべて満たしていることを確認します。「システム要件」（P.4）および 「はじめる前に」（P.19）の項を確認します。

ステップ 1 VMware vSphere Client を起動します。

ステップ 2 **[File] > [Deploy OVF Template]** を選択します。

[Deploy OVF Template] ウィンドウが表示されます。

ステップ 3 **[Deploy from file]** オプション ボタンをクリックします。

ステップ 4 **[Browse]** をクリックして、OVA ファイルを保存した場所にアクセスします。

ステップ 5 **[Next]** をクリックします。

[OVF Template Details] ウィンドウに、OVF テンプレートの詳細が表示されます。

ステップ 6 製品名、バージョン、およびサイズを含む OVA ファイルの詳細を確認して、[Next] をクリックします。

[Name and Location] ウィンドウが表示されます。

ステップ 7 導入するテンプレートの名前と場所を指定します。名前はインベントリ フォルダ内で固有である必要があり、最大 80 文字で構成できます。

ステップ 8 **[Next]** をクリックします。

[Ready to Complete] ウィンドウが表示されます。このウィンドウには、OVA ファイルの詳細、仮想アプライアンスの名前、サイズ、ホスト、およびストレージの詳細が表示されます。

ステップ 9 オプションを確認したら、**[Finish]** をクリックして導入を開始します。

このタスクが完了するまで数分かかる場合があります。[Deploying Virtual Application] ウィンドウの経過表示バーをチェックして、タスクのステータスをモニタします。

導入タスクが正常に完了すると、確認ウィンドウが表示されます。

ステップ 10 **[Close]** をクリックします。

導入した仮想アプライアンスが、vSphere クライアントの左側のペインで、ホストの下に表示されます。

サーバのインストール

Prime Infrastructure OVA の導入後に、Prime Infrastructure をインストールおよび起動するために仮想アプライアンスを設定する必要があります。

ステップ 1 VMware vSphere Client で、導入済みの仮想アプライアンスを右クリックし、[Power] > [Power On] を選択します。

ステップ 2 [Console] タブをクリックします。ローカルホスト ログイン プロンプトで、**setup** と入力します。

ステップ 3 コンソールから次のパラメータの入力を求められます。

- [hostname]：仮想アプライアンスのホスト名。
- [IP Address]：仮想アプライアンスの IP アドレス。
- [IP default netmask]：IP アドレスのデフォルト サブネット マスク。
- [IP default gateway]：デフォルト ゲートウェイの IP アドレス。
- [Default DNS domain]：デフォルトのドメイン名。
- [Primary nameserver]：プライマリ ネーム サーバの IP アドレス。
- [Secondary name servers]：セカンダリ ネーム サーバの IP アドレス（存在する場合）。最大 3 台のセカンダリ ネーム サーバを追加できます。
- [Primary NTP server]：ユーザが使用するプライマリ ネットワーク タイム プロトコル サーバの IP アドレスまたはホスト名。（`time.nist.gov` がデフォルトです）。
- [Secondary NTP servers]：セカンダリ NTP サーバの IP アドレスを入力します。
- [System Time Zone]：ユーザが使用する時間帯コード。
- [Clock time]：サーバの時間帯に基づいた時刻。
- [Username]：最初の管理ユーザの名前（「admin」）。これは、SSH または Telnet を使用してサーバへのログインに使用する管理者アカウントです。デフォルトの `admin` を受け入れることができます。
- [Password]：管理ユーザ パスワードを入力し、確認します。デフォルトは `admin` です。

ステップ 4 これらの値の入力が完了すると、入力したネットワーク設定パラメータがインストール用アプリケーションによってテストされます。テストに成功すると、Prime Infrastructure のインストールが開始されます。

ステップ 5 アプリケーションのインストールが完了すると、次のインストール後パラメータの入力を促されます:

- [High Availability Role Selection]：ハイ アベイラビリティ実装のフォール バックのセカンダリ サーバとしてこのインストールされたサーバを使用する場合は、プロンプトで `yes` を入力します。ハイ アベイラビリティの登録キーを提供するように促されます。プロンプトに対して `no` と入力した場合、サーバはプライマリ サーバ（スタンドアロン）として動作し、インストールでは次のプロンプトが処理されます。
- [Root Password]：デフォルトの `root` 管理者に使用するパスワードを入力し、確認します。これは、Prime Infrastructure ユーザ インターフェイスにログインし、別のユーザ アカウントを設定するために使用するルート アカウントです。
- [FTP password]：FTP パスワードを入力し、パスワードを確認します。

ステップ 6 インストールが完了すると、仮想アプライアンスがリブートし、ログイン プロンプトが表示されます。

ステップ 7 ステップ 3 で指定した「admin」ユーザ名とパスワードを使用して仮想アプライアンスにログインします。

Prime Infrastructure ユーザ インターフェイスへのログイン

Web ブラウザを介して Prime Infrastructure ユーザ インターフェイスにログインする手順は、次のとおりです。

ステップ 1 Prime Infrastructure をインストールし、起動したものとは別のコンピュータ上で、いずれかのサポート ブラウザ（「システム要件」（P.4）を参照）を起動します。

ステップ 2 ブラウザのアドレス行に、**https:**//*ipaddress* と入力します。ここで、*ipaddress* は、Prime Infrastructure をインストールしたサーバの IP アドレスです。Prime Infrastructure ユーザ インターフェイスに [Login] ウィンドウが表示されます。

初めて Prime Infrastructure にアクセスしたとき、一部のブラウザでは、サイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、Prime Infrastructure サーバから自己署名証明書をダウンロードします。この手順の完了後に、ブラウザは将来のすべてのログイン試行で Prime Infrastructure を信頼できるサイトとして受け入れます。

ステップ 3 「サーバのインストール」（P.20）で指定した管理者のユーザ名とパスワードを *root* と入力します。

ライセンスの問題が発生した場合は、アラート ボックスにメッセージが表示されます。評価ライセンスがある場合は、ライセンスの有効期限までの日数が表示されます。また、期限切れになったライセンスに対するアラートも表示されます。これらの問題に対処するために、**[Administration] > [Licenses]** ページに直接移動することができます。

ステップ 4 [Login] をクリックして Prime Infrastructure にログインします。ユーザ インターフェイスは、この時点でアクティブになり、使用可能になります。ホームページが表示されます。

システムのセキュリティを確保するには、**[Administration] > [Users, Roles & AAA] > [Change Password]** を選択して、*root* 管理者のパスワードを変更します。

ユーザ インターフェイスを終了するには、ブラウザのページを閉じるか、そのページの右上隅の **[Logout]** をクリックします。Prime Infrastructureユーザ インターフェイス セッションを終了しても、サーバ上では Prime Infrastructureはシャットダウンされません。

Prime Infrastructure のセッション中にシステム管理者が Prime Infrastructure サーバを停止すると、セッションが終了し、ブラウザに「The page cannot be displayed.」というメッセージが表示されます。サーバが再起動される際に、セッションは Prime Infrastructure に再び関連付けられません。新しい Prime Infrastructure セッションを開始する必要があります。

8 使用する前に

Prime Infrastructure をインストールした後、ネットワークの管理を開始するために、追加の作業を実行する必要があります。これらのタスクは、すべて『*Cisco Prime Infrastructure 2.1 User Guide*』の「Getting Started」の章に示されています。これらのタスクの完了後に、ネットワークのモニタと設定を開始できます。

9 スタンドアロン サーバ上のプラグ アンド プレイ ゲートウェイのインストール

Prime Infrastructure プラグ アンド プレイ ゲートウェイをインストールして開始するには、OVA を導入し、仮想アプライアンスを設定します。

リリース 1.2 以降の Prime Infrastructure では、プラグ アンド プレイ サーバは Prime Infrastructure サーバと統合されます。プラグ アンド プレイ ゲートウェイは Prime Infrastructure サーバと共に自動的に起動し、同じクレデンシャルと証明書を使用します。この項では、ネットワーク DMZ の拡張などのシナリオで使用するために、プラグ アンド プレイ ゲートウェイをインストールし、スタンドアロン アクセス サーバとして使用する方法について説明します。

Prime Infrastructure プラグ アンド プレイ サーバ要件

Cisco Prime Infrastructure プラグ アンド プレイ ゲートウェイ OVA のサーバ要件は次のとおりです。

- VMware ESXi 4.1.0 またはバージョン 5.0 が必須です。バージョン 5.0 が優先されます。Prime Infrastructure 2.1 は、バージョン 5.0 以降の VMware ESXi サーバではテストされていません。
- RAM：4GB
- ディスク領域：100 GB（SAN 使用に推奨）
- プロセッサ：4 個の 2.93 GHz 以上の仮想 CPU

Prime Infrastructure プラグ アンド プレイ ゲートウェイ OVA の導入

OVA を導入する前に、システム要件をすべて満たしていることを確認します。「Prime Infrastructure プラグ アンド プレイ サーバ要件」（P.21）および「はじめる前に」（P.19）の項を参照してください。

ステップ 1 VMware vSphere Client を起動します。

ステップ 2 **[File] > [Deploy OVF Template]** を選択します。

[Deploy OVF Template] ウィンドウが表示されます。

ステップ 3 **[Deploy from file]** オプション ボタンをクリックします。

ステップ 4 **[Browse]** をクリックして、OVA ファイルを保存した場所にアクセスします。

ステップ 5 **[Next]** をクリックします。[OVF Template Details] ウィンドウに、OVF テンプレートの詳細が表示されます。

ステップ 6 製品名、バージョン、およびサイズを含む OVA ファイルの詳細を確認して、[Next] をクリックします。[Name and Location] ウィンドウが表示されます。

ステップ 7 導入するテンプレートの名前と場所を指定します。名前はインベントリ フォルダ内で固有である必要があり、最大 80 文字で構成できます。

ステップ 8 **[Next]** をクリックします。[Ready to Complete] ウィンドウが表示されます。このウィンドウには、OVA ファイルの詳細、仮想アプライアンスの名前、サイズ、ホスト、およびストレージの詳細が表示されます。

ステップ 9 オプションを確認したら、**[Finish]** をクリックして導入を開始します。

このタスクが完了するまで数分かかる場合があります。[Deploying Virtual Application] ウィンドウの経過表示バーをチェックして、タスクのステータスをモニタします。導入タスクが正常に完了すると、確認ウィンドウが表示されます。

ステップ 10 **[Close]** をクリックします。導入した仮想アプライアンスが、vSphere クライアントの左側のペインで、ホストの下に表示されます。

Cisco Prime Infrastructure プラグ アンド プレイ ゲートウェイのスタンドアロンとしてのインストール

Cisco Prime Infrastructure プラグ アンド プレイ ゲートウェイの OVA を導入した後、Cisco Prime Infrastructure プラグ アンド プレイ ゲートウェイをインストールして起動する仮想アプライアンスを設定する必要があります。

ステップ 1 VMware vSphere Client で、導入済みの仮想アプライアンスを右クリックし、**[Power] > [Power On]** を選択します。

ステップ 2 「サーバのインストール」（P.20）のステップ 2 とステップ 3 を繰り返します。

ステップ 3 値を入力したあと、ネットワーク設定パラメータがテストされます。テストが成功した場合、Cisco Prime Infrastructure プラグ アンド プレイ ゲートウェイのインストールが開始します。

ステップ 4 インストールが完了すると、仮想アプライアンスがリブートされ、ログイン プロンプトが表示されます。

ステップ 5 管理者のユーザ名とパスワードを使用して、仮想アプライアンスにログインします。

プラグ アンド プレイ ゲートウェイ用の CA 署名付き証明書の生成

デフォルトでは、プラグ アンド プレイ ゲートウェイは自己署名証明書を生成するように設定できます。証明書は、SSL 通信用にデバイスでトラストポイントを作成する際に使用できます。プラグ アンド プレイ ゲートウェイとデバイスの両方に対して、1 つの CA によって署名された SSL 証明書を使用することを推奨します。

プラグ アンド プレイ ゲートウェイとデバイス間で、CA 署名付き証明書による SSL 通信が必要な場合にのみ、証明書を生成するようにします。

ステップ 1 CNS がサポートする K9 デバイスにログインし、**show version** コマンドを使用して、ソフトウェア イメージのバージョンを確認します。CNS がサポートする K9 デバイスにロードされるイメージは、暗号化イメージである必要があります。

ステップ 2 次のコマンドを使用して CA からサーバ証明書を取得します。

```
Generate RSA keys and certificate signing request:
$cd /root
$openssl genrsa -out server.key 1024 // generate an RSA Keypair and a Certificate Signing Request:
$chown root:root server.key
$chmod 400 server.key
$openssl req -new -key server.key -out server.csr

You can enter a period (.) in case you do not want to enter any information.But remember to enter CE
server name as
(Ex: myCEserver.example.com) when asked for Common Name (e.g., YOUR name) []:
```

server.key と server.csr ファイルがルート ディレクトリに作成されます。

（注） .csr ファイルを使用して、署名された CA 証明書を取得することを確認します。CA から .crt ファイルを 3 つ受信することになります。

ステップ 3 プラグ アンド プレイ セットアップを実行し、CA 証明書をコピーします。プラグ アンド プレイ セットアップの詳細については、「Prime Infrastructure プラグ アンド プレイ ゲートウェイの設定」（P.25）を参照してください。

エンドポイント デバイスの CA 証明書のアクティベート

CNS のサポートする K9 デバイスでサーバ証明書をアクティベートするには、次の手順を実行します。

ステップ 1 CNS のサポートする K9 デバイスにログインし、時刻のタイミングを確認します。エンドポイント デバイスとプラグ アンド プレイ ゲートウェイ サーバとに、同じタイムスタンプが必要です。

```
Router#show clock
02:04:40.065 PST Fri Feb 20 2009
The certificate begins to be valid starting at 19:30 GMT,
which is 3:30pm Eastern Time, which is 12:30 Pacific Time.
Hence make sure the clock on router is set correctly.

Router#clock set 01:08:10 20 FEBRUARY 2009
Router#show clock
.01:08:14.082 PST Fri Feb 20 2009
```

ステップ 2 必要なトラスト ポイントに証明書がすでにインストールされていることを確認します。インストールされている場合、次の設定コマンドを使用して古い証明書を無効にします。

```
Router# conf terminal
```

```
Router(config)# no crypto ca trustpoint example.com
```

証明書を破棄することを尋ねられたら、「Yes」と応答します。次に例を示します。

```
% Removing an enrolled trustpoint will destroy all certificates
 received from the related Certificate Authority.
Are you sure you want to do this? [yes/no]: yes
```

ステップ 3 トラスト ポイントを定義するには、次のコマンドを実行します。

```
Router(config)# ip host hostname address
Router(config)# ip host hostname.example.com address
Router(config)# ip domain-lookup
Router(config)# crypto ca trustpoint myCEServer.example.com
Router(ca-trustpoint)# enrollment mode ra
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# usage ssl-client
Router(ca-trustpoint)#  exit
```

ステップ 4 トラスト ポイントを認証します。

```
Router(config)#  crypto ca authenticate hostname.example.com
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
Copy the entire content of server.crt here and press enter as below.

Router(config)# crypto ca authenticate myCEServer.example.com
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDFTCCAf2gAwIBAgIKMt87mwABAAABrjANBgkqhkiG9w0BAQUFADAuMRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtURVNULVNTTC1DQTAeFw0wOTAx
MTYxMDU0NDJaFw0xMDAxMTYxMTA0NDJaMDAxDjAMBgNVBAoTBUNpc2NvMR4wHAYD
VQQDExVpbWd3LXRlc3QxMC5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAPAdsaSPKMpGOny05TDuZG3t9Dwlc1VGk2ZfPpp7oX1eQNK4ub3Lr3o5
fb83nmwzzb6hXgDvO3ElX+Xjh+j4LZDDWb30db5jxJvYVz9MyrnChBD7kyLuUaOc
uxLNxPUwnWTzd28n+Wg5uSptH8b/ofxx5WBessCY20448hjTROq5AgMBAAGjgbYw
gbMwHQYDVR0OBBYEFClHMwLRjIfWNvv3FrMLNO/ILJz5MB8GA1UdIwQYMBaAFI7J
Ti5oRslwv2B3MmERGbPKKUsSMFwGA1UdIARVMFMwUQYKKwYBBAEJFQEBADBDMEEG
CCsGAQUFBwIBFjVodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvcG9s
aWNpZXMvaW5kZXguaHRtbDATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0B
AQUFAAOCAQEAXP9iMHWVGRucbda++UUR8PFSzaSChmQyWti5+oWe+WCUBU/HtonM
XACZBxwA4HTT7eqhPfs4HhNUUHT/l/ChZLksaWJNTO7Wa2X80vvJJUoWHVZod1Pm
vUJFgvZCBVBj54wvFaH+ijADzJ3ASVPOMxxdKdJzpYspNE4W0s0ghyIQxXF1Ht/B
n+DBipuG4hx5dK9px5f/nzCYNh5zxPnriaFe7WYiWUxg47WWT1nBMiVED8Z48WwB
gSX2K9+87Jg+lJ8EpQ1Avkf2X7vWsCW1vx9YicLw+RFS6o+4Za+NrwSmF/Y0pGJg
rCJlwLn2n0ZI64atJFa/FdAujr9W9KWrmw==
-----END CERTIFICATE-----quit

Trustpoint 'myCEServer.example.com' is a subordinate CA and holds a non self signed cert
Trustpoint 'myCEServer.example.com' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: C7C7BFB5 CD3DDB95 987B0899 0385282E
      Fingerprint SHA1: 82721218 56C6C4FE 855C8B43 AA653F63 786D63BF

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

ステップ 5 CNS のサポートする K9 デバイスで、次の CNS 設定を実行します。

```
Router#sh run | i cns
        cns trusted-server all-agents myCEServer
        cns trusted-server all-agents myCEServer.example.com
        cns id string Router
        cns id string Router event
        cns id string Router image
```

```
         cns event myCEServer.example.com encrypt 11012 keepalive 60 3
         cns config partial myCEServer.example.com encrypt 443
cns image server https://imgw-test35:443/cns/HttpMsgDispatcher status
https://imgw-test35:443/cns/HttpMsgDispatcher

         cns inventory
         cns exec encrypt 443
```

ステップ 6 CNS のサポートする K9 デバイスと Prime Infrastructure との間の接続が確立されているかどうか確認します。

```
Router# sh cns event conn
```

接続が確立されると、次のような出力が表示されます。

```
The currently configured primary event gateway:
        hostname is imgw-test10.example.com.
        port number is 11012.
        encryption is enabled.
Event-Id is Router
Keepalive setting:
        keepalive timeout is 60.
        keepalive retry count is 3.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.
The currently connected event gateway:
        hostname is imgw-test10.example.com.
        port number is 11012.
        encryption is enabled.
```

Prime Infrastructure プラグ アンド プレイ ゲートウェイの設定

Cisco Prime プラグ アンド プレイ ゲートウェイの OVA を設定するには、次の手順を実行します。

ステップ 1 管理ユーザ名とパスワードを使用して、Cisco Prime プラグ アンド プレイ ゲートウェイ サーバにログインします。

ステップ 2 コマンド プロンプトで、**pnp setup** コマンドを入力し、Enter キーを押します。

ステップ 3 次のパラメータのコンソール プロンプトは、次のように表示されます。

- IP Address：プラグ アンド プレイ ゲートウェイ サーバが使用する IP アドレス。
- SSL Server Certificate：プラグ アンド プレイ ゲートウェイの自己署名/CA 署名済みサーバ証明書。
- CNS Event：ダイナミック ロケーションのデバイスに導入されている CNS イベント設定。

ステップ 4 コンソールには次のように表示されます。

```
bgl-pnp-dev1-ovf/admin# pnp setup

        ######################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ######################################################################

Enter Prime Infrastructure IP Address: [10.104.105.168]
Enable self certificate for server bgl-pnp-dev1-ovf (y/n) [y]
Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for server 10.104.105.168 (y/n) [y] n
Enter absolute pathname of Prime Infrastructure server certificate file:
[/var/KickStart/install/ncs_server_certificate.crt]

        The maximum number of Event Gateways allowed is '10' for both plain text
        and ssl combined.The Event Gateway ports 11011 and 11012 are reserved for port
```

```
        automatic allocation.These ports are not counted while taking the maximum number of ports.

        Each Event Gateway can serves up to a maximum of 1000 devices.

Enter number of Event Gateways that will be started with crypto operation: [5] 10
All the ports are configured for crypto operation.No plain text port is available.Is it the right
configuration y/n: [y]

        The CNS Event command configures how the managed devices should
        connect to this particular Plug and Play Gateway.The command entered in the following
        line should match what's configured on the devices WITHOUT the port
        number and keyword 'encrypt' if cryptographic is enabled.

        For example, if the following CLI is configured on devices
        "cns event bgl-pnp-dev1-ovf encrypt 11012 keepalive 120 2 reconnect 10",
        then `encrypt 11012` should be removed and the below line should be entered :
        "cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10"

        Another example, if this is a backup Plug and Play Gateway and the following CLI is
        configured on devices
        "cns event bgl-pnp-dev1-ovf 11011 source Vlan1 backup", then `11011`
        should be removed and the below line should be entered :
        "cns event bgl-pnp-dev1-ovf source Vlan1 backup"

        Unable to enter a correct CLI could cause the managed devices not
        be able to connect to this Plug and Play Gateway.For details, please refer to
        Installation and Configuration Guide.

Enter CNS Event command: [cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10]


Commit changes (y/n): y
```

（注） 高度な設定には、**pnp setup advanced** コマンドを使用します。詳細については、『Command Reference Guide for Cisco Prime Infrastructure2.1』を参照してください。

```
bgl-pnp-dev1-ovf/admin# pnp setup advanced

        ########################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ########################################################################

Enter IP Address of Plug and Play Gateway server [10.104.105.167]
 **** Setup abort!!!Exiting ***
```

ステップ 5 Prime Infrastructure プラグ アンド プレイ ゲートウェイ サーバの状態を調べるには、ゲートウェイ サーバにログインし、**pnp status** コマンドを実行するか、ブラウザに次の URL を入力します。https://<IP address or hostname>/cns/ResourceInit?name=port。ゲートウェイ サーバの状態が表示されます。

```
bgl-pnp-dev1-ovf/admin# pnp status


SERVICE                       |  MODE                |  STATUS        |  ADDITIONAL INFO
-------------------------------------------------------------------------------------------------
System                        |                      |  UP            |
-------------------------------------------------------------------------------------------------
Event Messaging Bus           |  PLAIN TEXT          |  UP            |  pid: 21161
CNS Gateway Dispatcher        |  PLAIN TEXT          |  UP            |  pid: 21520, port: 11011
CNS Gateway                   |  PLAIN TEXT          |  UP            |  pid: 21549, port: 11013
CNS Gateway                   |  PLAIN TEXT          |  UP            |  pid: 21583, port: 11015
CNS Gateway                   |  PLAIN TEXT          |  UP            |  pid: 21617, port: 11017
CNS Gateway                   |  PLAIN TEXT          |  UP            |  pid: 21656, port: 11019
CNS Gateway                   |  PLAIN TEXT          |  UP            |  pid: 21691, port: 11021
```

```
CNS Gateway Dispatcher          |  SSL              |  UP          |  pid: 21755, port: 11012
CNS Gateway                     |  SSL              |  UP          |  pid: 21987, port: 11014
CNS Gateway                     |  SSL              |  UP          |  pid: 22113, port: 11016
CNS Gateway                     |  SSL              |  UP          |  pid: 22194, port: 11018
CNS Gateway                     |  SSL              |  UP          |  pid: 22228, port: 11020
CNS Gateway                     |  SSL              |  UP          |  pid: 22287, port: 11022
HTTPD                           |                   |  UP          |
Image Web Service               |  SSL              |  UP          |
Config Web Service              |  SSL              |  UP          |
Resource Web Service            |  SSL              |  UP          |
Image Web Service               |  PLAIN TEXT       |  UP          |
Config Web Service              |  PLAIN TEXT       |  UP          |
Resource Web Service            |  PLAIN TEXT       |  UP          |
Prime Infrastructure Broker     |  SSL              |  UP          |  port: 61617, connection: 1


bgl-pnp-dev1-ovf/admin#
```

10 Prime Infrastructure 仮想アプライアンスの削除

次の方法を使用した Prime Infrastructure の削除では、サーバ設定およびローカル バックアップなどのサーバ上のすべてのデータが削除されます。リモート バックアップがない場合、データを復元できなくなります。削除の他の例については、『*Cisco Prime Infrastructure 2.1 Administrator Guide*』の「Removing Prime Infrastructure」を参照してください。

ステップ 1 VMware vSphere クライアントで、Prime Infrastructure 仮想アプライアンスを右クリックします。

ステップ 2 仮想アプライアンスの電源を切ります。

ステップ 3 [Delete from Disk] をクリックして、Prime Infrastructure 仮想アプライアンスを削除します。

11 ナビゲーションおよびマニュアルの参照先

この項では、Prime Infrastructure の機能にアクセスするためのナビゲーション パスの情報と、Prime Infrastructure のマニュアル内でそれらの機能を扱っている項目の詳細を示します。

表 8　　ナビゲーションおよびマニュアルの参照先

タスク	Cisco Prime Infrastructure 内のナビゲーション	Cisco Prime Infrastructure User Guide 内の項
ネットワークの検出	**[Operate] > [Discovery]**	使用する前に
ポート モニタリングのセットアップ	**[Design] > [Port Grouping]**	ネットワークの設計
仮想ドメインのセットアップ	**[Administration] > [Virtual Domains]**	使用する前に
モニタリング ダッシュボードの使用	**[Operate] > [Monitoring Dashboards]**	ネットワークの運用
テンプレートを使用した設定とモニタリング	**[Design] > [Feature Design]** または **[Design] > [Monitor Configuration]**	ネットワークの設計
ワイヤレス設定のテンプレートの使用	**[Design] > [Wireless Configuration]**	ワイヤレス コントローラ テンプレートの作成
アラームの表示	**[Operate] > [Alarms & Events]**	アラームのモニタリング
デバイス設定の検索と比較	**[Operate] > [Configuration Archive]**	デバイス コンフィギュレーションの操作

表 8　　ナビゲーションおよびマニュアルの参照先 （続き）

タスク	Cisco Prime Infrastructure 内のナビゲーション	Cisco Prime Infrastructure User Guide 内の項
デバイス設定のメンテナンス	**[Operate] > [Configuration Archive]**	デバイス コンフィギュレーション インベントリの保守
ユーザの管理	**[Administration] > [Users, Roles & AAA]**	ユーザ アクセスの制御
Prime Infrastructure に追加されたアクセス スイッチの設定	**[Workflows] > [Initial Device Setup]**	デバイスのセットアップと設定のヘルプの利用
ネットワークに今後追加されるデバイスの事前設定	**[Workflows] > [Plug and Play Setup]**	デバイスのセットアップと設定のヘルプの利用

12 物理アプライアンスでの Cisco Prime Infrastructure の再インストール

物理アプライアンスに Prime Infrastructure をインストールするには、root 権限が必要です。Prime Infrastructure を再インストールする前に、最新のバックアップを実行したことを確認します。再インストール後に、バックアップを使用してデータを復元できます。

物理アプライアンスに Prime Infrastructure を再インストールするには、次の手順を実行します。

ステップ 1　提供される Prime Infrastructure ソフトウェア イメージ DVD を挿入します。システムがブートし、次のコンソールが表示されます。

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005 H.Peter Anvin

                  Welcome to Cisco Prime Infrastructure

To boot from hard disk, press <Enter>.

Available boot options:

      [1] Prime Infrastructure Installation (Keyboard/Monitor)
      [2] Prime Infrastructure Installation (Serial Console)
      [3] Recover administrator password.(Keyboard/Monitor)
      [4] Recover administrator password.(Serial Console)
      <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

ステップ 2　Prime Infrastructure ソフトウェア イメージを再インストールするには、オプション 1 を選択します。システムがリブートし、[configure appliance] 画面が表示されます。

ステップ 3　初期設定パラメータを入力すると、システムが再度リブートします。DVD を取り出し、手順に従って Prime Infrastructure サーバを起動します。

13 関連資料

Cisco Prime Infrastructure 2.1 Documentation Overview に、Prime Infrastructure で利用できるマニュアルの一覧を示します。

（注）　元のドキュメントの発行後に、ドキュメントを更新することがあります。マニュアルのアップデートについては、Cisco.com で確認してください。

14 マニュアルの入手方法およびテクニカル サポート

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

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

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

米国本社
Cisco Systems, Inc.
San Jose, CA

アジア太平洋本部
Cisco Systems (USA) Pte.Ltd.
Singapore

ヨーロッパ地域本部
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in the USA on recycled paper containing 10% postconsumer waste.

OL-30962-01.