クイック スタート ガイド

# Cisco Prime Assurance Manager 1.1

# クイック スタート ガイド

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

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

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

改訂日： 2012 年 7 月 5 日、OL-26374-01-J

**シスコ ネットワーク管理ソフトウェア用使用許諾契約補則：CISCO PRIME ASSURANCE**

**重要：よくお読みください**：この追加ライセンス契約（"SLA"）では、お客様とシスコとの間で締結されるエンド ユーザ ライセンス契約の下でお客様に提供される本ソフトウェアのライセンスに関する追加の制限事項を規定します。この SLA 内で大文字で示された用語は、ここで特に定義されていない限り、エンド ユーザ ライセンス契約で定義されたとおりの意味になります。本ソフトウェアに適用される条件のいずれかに矛盾がある場合は、本 SLA に記載する条件を優先するものとします。

本ソフトウェアのインストール、ダウンロード、本ソフトウェアへのアクセス、またはそれ以外の方法で本ソフトウェアを使用した時点で、お客様は、本 SLA の条件に同意したことになります。お客様は、この SLA の条項に同意しない場合、本ソフトウェアをインストール、ダウンロード、またはその他の方法で使用することはできません。

追加のライセンス制限事項：

- インストールと使用：ソフトウェア コンポーネントは、インストール、アップデート、補足、または適用されている既存のネットワーク管理ソフトウェア製品との交換の目的でのみお客様に提供されます。お客様は、次のソフトウェア コンポーネントをインストールし、使用することができます。
  - Cisco Prime Assurance Manager：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。
- 複製と配布：お客様による本ソフトウェアの複製および配布は禁止されています。

その他の権利および制限条項の説明

シスコのエンド ユーザ ライセンス契約を参照してください。

# 1 このマニュアルについて

このマニュアルでは、Cisco Prime Assurance Manager 1.1（Prime AM 1.1）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、Cisco Prime Assurance Manager 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 アプリケーションに精通していなければなりません。また、仮想化の概念と仮想化環境についても理解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 Assurance Manager 1.1 User Guide*』を参照してください。

# 2 製品概要

Cisco Prime Assurance Manager は Web ベースのユーザ アプリケーションで、アプリケーション対応ネットワーク サービスの保証とパフォーマンス管理を実行します。次の 2 種類のコンポーネントで構成されます。

- データ コレクタ：Cisco NAM、NetFlow、SNMP ポーリング、トラップ、syslog などといったプロトコルやメカニズムを使用してパフォーマンスおよびパフォーマンス系の障害データをネットワーク内のデバイスから収集します。収集されたデータは集約され、しきい値と比較されます。
- Cisco Prime Assurance Manager サーバ：収集されたデータを利用して、Prime AM は、次の機能をエンド ユーザに提供します。
  - 中央集中型のパフォーマンス モニタリング：Prime AM は、パフォーマンス データをさまざまな粒度および集約度（空間ベースと時間ベースの両方）で表示するダッシュボードとレポートを提供します。
  - サービス保証：Prime AM は、実行中のアプリケーションとネットワーク サービスを自動的に識別し、それらのサービスをパフォーマンス データと障害データに関連付けます。
  - トラブルシューティング：パフォーマンス イベントの発生に応じて、パケットのキャプチャとデコーディングを実行できます。これらは、ネットワーク パフォーマンスの問題や障害のトラブルシューティングに利用できます。

- トラフィック分析：容量計画と最適化を行うために、さまざまなソースからデータを収集して、トラフィックを分析できます。

# 3 主な機能

次の表に、Cisco Prime Assurance Manager の主な機能の詳細を示します。

**表 1　　Cisco Prime Assurance Manager の主な機能**

| 機能 | 作用 | 利点 |
|---|---|---|
| **パフォーマンス モニタリング** | 音声ベース、ビデオ ベース、および TCP ベースのアプリケーション用の中央集中型パフォーマンス モニタリング | エンドユーザ エクスペリエンスを可視化し、サービス レベル目標に従ってビジネスに不可欠なアプリケーションを管理します。 |
| **トラフィック分析** | トラフィック分析データ取集、画面上のインジケータ、および WAN 最適化とデータフロー分析のレポート。 | WAN 最適化の機会を識別し、異常なトラフィック動作を検出し、ネットワークリソースの使用状況とスループットを分析し、過去の傾向を考慮することにより、アプリケーションのパフォーマンスを改善します |
| **パフォーマンス診断** | 問題の調査と分離 | リアルタイム表示とトラブルシューティングのために、パフォーマンス データを詳細なレベルまでドリルダウンします。 |
| **Multi-NAM 管理** | 自動化された NAM 検出、パケット キャプチャの中央管理、複数の NAM からの中央レポーティング、NAM 間で整合性を保つための中央集中型アプリケーション分類、WAN 最適化を可視化するための WAAS サーバ リストの中央プロビジョニング、より詳細に分析するための NAM UI へのコンテキスト依存の相互起動、中央集中型しきい値処理。 | グローバル ネットワーク全体にわたって一貫したアプリケーション エクスペリエンスを実現するために、迅速かつ簡単に複数 NAM デバイスの能力を活用します。 |
| **中央集中型レポーティング** | すぐに利用可能で、柔軟性があり、お客様によって生成され、スケジュールが作成され、エクスポート可能な、幹部向けのレポート | パフォーマンス データの表示にあらかじめパッケージ化されているセットやカスタム セットを使用して、生産性およびコミュニケーションを改善します。 |
| **中央集中型パフォーマンス データ収集** | 内部と外部の管理アプリケーションに対するパフォーマンス データ アクセス、抽象的な収集管理 | 検出、設定、収集、およびメンテナンスの自動化を利用して、シスコのインテリジェントな組み込み装置とプローブにお客様が簡単にアクセスできます。 |
| **ユーザビリティ** | ネットワーク デバイスからレポートされる現行の NAM、NetFlow、SNMP などのデータを使用して、すぐに使用可能な「ゼロ タッチ」モニタリングを提供します。 | 検出および自動化を活用することで、ほとんどまたはまったく設定しなくても意味のあるレポートを出力できます |

Prime AM の機能の詳細については、『*Cisco Prime Assurance Manager 1.1 User Guide*』を参照してください。

# 4 Cisco Prime Assurance Manager のライセンスについて

Cisco Prime Assurance Manager は、管理対象のネットワーク インターフェイスの数に基づいてライセンスされます。Prime AM を使用するには、次のいずれかのライセンスが必要です。

- 評価ライセンス：60 日間有効で、100 インターフェイスまで使用できます。評価ライセンスは、https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y で入手できます。
- 基本ライセンス：購入できる基本ライセンスのサイズは、50、100、500、1000、または 5000 インターフェイスです。Prime AM を既存の NCS（WAN）インストールのアドオンとして購入する場合を除き、Prime AM を使用するには、基本インターフェイス数を 1 つだけ購入する必要があります。すでに NCS（WAN）が基本ライセンスでインストールされている場合は、アドオン ライセンスを購入するだけで Prime AM を使用できます。基本ライセンスは、http://www.cisco.com/go/licensing において、注文時に提供された製品認証キー（PAK）と、インストールした Prime AM のインスタンスから取得される Virtual Unique Device Identifier（VUDI）を使用して入手できます。
- アドオン ライセンス：購入できるアドオン ライセンスのサイズは、50、100、500、1000、または 5000 インターフェイスです。アドオン ライセンスは、インターフェイス数の増加に応じて購入できます。アドオン ライセンスは、http://www.cisco.com/go/licensing において、PAK と VUDI を使用して入手できます。

Prime AM ライセンス ファイルは、Virtual Unique Device Identifier（VUDI）に基づいて仮想マシンにノードロックされます。VUDI は、製品 ID と一意に生成されたシリアル番号で構成されます。この情報は、Prime AM Web インターフェイスで [Administration] > [Licenses] を選択して表示できます。

Prime AM ライセンスの発注方法の詳細については、http://www.cisco.com/go/primeassurance にあるライセンス情報を参照してください。

# 5 インストール前の作業

Cisco Prime Assurance Manager をインストールする前に、次の各項に示された要件を満たし、作業を実行します。

## システム要件

VMware ESX Server または ESXi Server の 4.1.x 以降のソフトウェアがサーバ上に必要です。

表 2 に、Cisco Prime AM OVA の各オプションに対する最小サーバ要件を示します。この表の「フロー レコード」には、NAM ポーリングによって生成される NetFlows およびフロー レコードが含まれます。

**表 2　　仮想アプライアンスを導入するための最小サーバ要件**

| OVA サイズ | 最大フロー レコード | 最大 NAM | 最小要件 |
|---|---|---|---|
| **小** | <1,000 レコード/秒 | 10（うち 5 個のポーリングがイネーブル） | RAM：8 GB<br>ディスク領域：200 GB<br>プロセッサ：4 × 2.93 GHz 以上の仮想 CPU |
| **大** | <15,000 レコード/秒 | 80（うち 25 個のポーリングがイネーブル） | RAM：16 GB<br>ディスク領域：400 GB<br>プロセッサ：8 × 仮想 CPU（2.93 GHz 以上） |
| **特大** | <80,000 レコード/秒 | 400（うち 40 個のポーリングがイネーブル） | RAM：24 GB<br>ディスク領域：1.2 TB<br>プロセッサ：8 × 仮想 CPU（2.93 GHz 以上） |

### Web クライアントの要件

ハードウェア：次のサポート 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。

- Flash プラグインと Chrome プラグインをインストールした Internet Explorer 8.0
- Mozilla Firefox 7.0

ディスプレイ解像度：画面解像度を 1024 × 768 以上に設定することを推奨します。

Adobe Flash Player：Cisco Prime Assurance Manager の機能が正しく動作するには、Web クライアントに Adobe Flash Player バージョン 10.x 以降がインストールされている必要があります。Adobe の Web サイトからダウンロードし、インストールすることを推奨します。

## 使用ポート

表 3 に、Cisco Prime Assurance Manager で使用されるポートを示します。インストール前に、これらのポートを開いておく必要があります。

**表 3　　使用ポート**

| ポート | プロトコル | 方向 | 用途 |
|---|---|---|---|
| 7 | ICMP | サーバからエンドポイントへ。 | エンドポイントの検出。 |
| 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。 | Cisco Prime Assurance Manager サーバに接続する。 |
| 25 | TCP | サーバから SMTP サーバへ | SMTP |
| 53 | TCP | サーバから DNS サーバへ | DNS |
| 161 | UDP | サーバからネットワーク デバイスへ。 | SNMP MIB ポーリング |
| 162 | UDP | エンドポイントからサーバへ。 | トラップ レシーバ ポート。 |
| 443 | TCP | サーバからインターフェイスへ。 | トラブルシューティング時のインターフェイスへの HTTPS 接続。 |
| 8080 | TCP | クライアントからサーバへ | Cisco Prime Assurance Manager サーバへのブラウザ アクセス（HTTP 経由）。 |
| 8443 | 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。 | Cisco Prime Assurance Manager サーバへのセキュアなブラウザ アクセス（HTTPS 経由）。 |
| 9991 | UDP | ネットワーク デバイスからサーバへ | NetFlow データ レシーバ |
| 20514 | UDP | エンドポイントからサーバへ。 | syslog レシーバ |

## サポートされるデータ ソース

ネットワーク インターフェイスとサービスをモニタするには、Prime AM が、エクスポートされたデータ ソース（表 4）を使用してそれ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。

この表を使用して、ネットワーク デバイスとそれらのソフトウェアが、Prime AM 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 AM でこのデータを収集するために変更が必要になる場合があります。「データ ソースの設定」の説明を参照してください。

**表 4　　Prime AM でサポートされるデータ ソース、デバイス、ソフトウェア バージョン**

| デバイス データ ソース | サポートされるデバイス | 最小ソフトウェア バージョン |
|---|---|---|
| Medianet NetFlow | Cisco Catalyst 3750 シリーズ スイッチ、Cisco Catalyst 3560 シリーズ スイッチ | IOS 12.2(58)SE |
| | Cisco Catalyst 6500 および Catalyst 6500-E シリーズ スイッチ | IOS 15.0(1)SY |
| | Cisco 880、890、1900、2900、および 3900 シリーズ サービス統合型ルータ | IOS 15.1(3)T |
| NetFlow（NF）および Flexible NetFlow（FNF） | ほとんどすべてのシスコ デバイス | IOS 11.1（NF の場合のみ）または IOS 12.2(31)SB2（FNF の場合） |
| Network Analysis Module（NAM） | 任意の NAM 互換製品（Cisco Catalyst 6500 シリーズ Network Analysis Module（NAM-1/NAM-2/NAM-3）、Cisco 7600 シリーズ Network Analysis Module（NAM-1/NAM-2/NAM-3）、Cisco NAM 2200 シリーズ アプライアンス、Cisco Network Analysis Module Software、Cisco Prime NAM for ISR G2 SRE、Cisco Prime NAM for Nexus 1010、Cisco Prime NAM for WAAS Virtual Blade（VB）など）。 | Cisco Prime Network Analysis Module Software 5.1（2-patch4） |
| Performance Agent（PA） | Cisco 880、890、1900、2900、および 3900 サービス統合型ルータ（PA は、「E」モデルと 3925 ではサポートされません） | IOS 15.1(4)M |
| 簡易ネットワーク管理プロトコル（SNMP） | All | 該当なし |

# データ ソースの設定

インストールを行う前に、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 AM 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。

## Medianet NetFlow のイネーブル化

Cisco Prime Assurance Manager 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。

- Cisco Prime Assurance Manager 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 Cisco Prime Assurance Manager 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、Cisco Prime Assurance Manager 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
  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 PAMIP
  source Loopback0
  transport udp PAMPort
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 sequental 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。

- *PAMIP* は、Prime AM サーバの IP アドレスです。
- *PAMPort* は、Prime AM 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 *PAMIP* 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 AM 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 AM サーバおよびポートにエクスポートします。

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。

```
interface interfaceName
ip route-cache flow
```

ここで、*interfaceName* は、NetFlow をイネーブルにするインターフェイスの名前です（「fastethernet」や「fastethernet0/1」など）。

NetFlow は、Prime AM 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、NetFlow がデバイス上で動作していることを確認します。

```
show ip flow export
show ip cache flow
show ip cache verbose flow
```

NetFlow をイネーブルにした後、次の IOS コンフィギュレーションモード コマンドを使用して、デバイスが NetFlow データを Prime AM にエクスポートするように設定できます。

```
ip flow-export version 5
ip flow-export destination PAMIP PAMPort
ip flow-export source interfaceName
```

ここで、

- *PAMIP* は Prime AM サーバの IP アドレス
- *PAMPort* は、Prime AM 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 *PAMIP* に送信しているインターフェイスの名前。これにより、送信元インターフェイスの IP アドレスが、Cisco Prime Assurance Manager に送信される NetFlow エクスポート データグラムに含められます。

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、次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。

**（注）** Prime AM 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 AM に直接エクスポートする必要があります。NAM から Cisco Prime Assurance Manager 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 AM 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。

```
flow exporter mace-export
destination 172.30.104.128
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。

```
flow record type mace mace-record
collect application name
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。

```
flow monitor type mace mace-monitor
record mace-record
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。

```
access-list 100 permit tcp any host 10.0.0.1 eq 80
class-map match-any mace-traffic
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。

```
policy-map type mace mace_global
class mace-traffic
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。

```
interface Serial0/0/0
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。

## SNMP の設定

Cisco Prime Assurance Manager 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。

- Cisco Prime Assurance Manager 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 Cisco Prime Assurance Manager 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。

```
snmp-server community private RW
snmp-server community public RO
```

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 ストリングの設定が完了したら、各 SNMP デバイス上で次の 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、デバイス通知がトラップとして Cisco Prime Assurance Manager サーバに送信されることを指定できます。

```
snmp-server host PAMHost traps version community notification-type
```

ここで、

- *PAMHost* は、Cisco Prime Assurance Manager 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。帯域幅の使用量と Cisco Prime Assurance Manager サーバに送信されるトラップ情報の量は、このパラメータを使用して制御しなければならない場合があります。

帯域幅の使用量と Cisco Prime Assurance Manager サーバに送信されるトラップ情報の量は、追加のコマンドを使用して制御しなければならない場合があります。

Prime AM で利用可能な SNMP 情報の種類は、デバイスにインストールされている MIB によって異なります。たとえば、Prime AM でデバイスまたはデバイス グループの environmentTemperature 変数をモニタする場合は、それらのデバイスに CISCO-ENVMON-MIB と CISCO-ENTITY-SENSOR-MIB がインストールされていることを確認する必要があります。

SNMP の設定の詳細については、『*Cisco IOS Network Management Command Reference*』の「snmp-server community」と「snmp-server host」を参照してください。さらに、『*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*』の「Configuring SNMP Notifications」と、通知タイプ値のリストも参照してください。

### NTP の設定

ネットワーク タイム プロトコルの同期は、Prime AM サーバ上はもとより、ネットワーク内のすべてのデバイスと NAM 上で設定する必要があります。NTP サーバは、Prime AM OVA を導入するときに指定できます。また後から、イストール済みの製品内で選択することにより、NTP サーバを変更することもできます。NAM と他のデバイス上のタイムスタンプを協調させることは、組織のネットワーク設計者にとって重要な問題です。ネットワーク全体の時刻の同期化に失敗すれば、Prime AM で異常な結果が発生する可能性があります。

# 6 Cisco Prime Assurance Manager のインストール

## はじめる前に

「インストール前の作業」（P.4）に説明されている事前準備の要件を満たしている必要があります。

Cisco Prime Assurance Manager を仮想ホストにインストールする前に、次のことも確認する必要があります。

- Cisco Prime Assurance Manager サーバのホストとして使用する予定のマシン上に VMware ESX または ESXi がインストールされ、設定されている。ホスト マシン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。
- インストールされている VMware ESX または ESXi ホストがネットワーク経由で到達可能である。
- VMware vSphere Client が同じホスト上にインストールされている。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 をインストールできる Web ベースのインターフェイスを表示できます。

  （注） VMware vSphere Client は Windows ベースです。このクライアントは Windows PC からダウンロードし、インストールする必要があります。

  VMware vSphere Client をインストールしたら、このクライアントを実行して、仮想ホストのホスト名または IP アドレス、ルート ログイン ID、および設定したパスワードを使用して仮想ホストにログインできます。vCenter を介して管理する場合は、ホストを vCenter に追加できます。詳細については、VMware vSphere のマニュアルを参照してください。
- Prime AM OVA が、vSphere Client のインストール先と同じマシンに保存されている。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ストール メディアから入手できます。

# 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）と「はじめる前に」（P.10）を確認してください。

**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。

# サーバのインストール

Cisco Prime Assurance Manager OVA を導入した後、Cisco Prime AM のインストールおよび起動を行うために、仮想アプリケーション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。

- [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。このネームサーバは、追加または編集できます。複数のネーム サーバまたは NTP サーバを設定するには、**y** と入力します。
- [Primary NTP server] : デフォルトは time.nist.gov です。

- [Username]：最初の管理ユーザの名前。デフォルトの admin を受け入れることができます。
- [Password]：パスワードを入力して、確認します。デフォルトは **admin** です。パスワードは取得もリセットもできないので、入力したパスワードは書き留めておくことを推奨します。

**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 vSphere Client によってテストされます。テストに成功すると、Cisco Prime Assurance Manager のインストールが開始されます。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、システムが初期化されます。初期化が完了すると、ログイン プロンプトが表示されます（初期化中はコンソールがほぼ使用できない、もしくはまったく使用できない状態になりますので、しばらくお待ちください）。

**ステップ 5** 指定した管理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。

# Cisco Prime Assurance Manager へのログイン

Web ブラウザを介して Cisco Prime Assurance Manager 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 AM をインストールし、起動した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* を入力します。**ここで、*IPaddress* は Prime AM をインストールしたサーバの IP アドレスです。Prime AM 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。

**（注）** 初めて Cisco Prime Assurance Manager 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。その場合は、プロンプトに従って、セキュリティ例外を追加し、サーバから自己署名証明書をダウンロードします。この手順が完了した後のブラウザでは、ログイン時はいつも、そのサーバが信頼できるサイトとして受け入れられます。

**ステップ 3** デフォルトの管理者ユーザ名とパスワードを入力します。これらはそれぞれ *root* と *Public123* になります。

初めてログインするときにライセンスの問題が発生すると、アラート ボックスでメッセージが表示されます。評価ライセンスを使用している場合は、ライセンスの期限が切れるまでの日数が表示されます。また、期限切れのライセンスに対してもアラートが表示されます。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 Cisco Prime Assurance Manager にログインします。Prime AM のホーム 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 ページを閉じるか、ページの右上にあるユーザ名の下の [Logout] をクリックします。ユーザ インターフェイス セッションを終了しても、サーバ上の Prime AM はシャットダウンされません。

セッション中にシステム管理者によって Prime AM サーバが停止されると、そのセッションは終了し、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。サーバが再起動しても、そのセッションが再アソシエートされることはありません。現在のセッションを終了して、新しいセッションを開始する必要があります。

# 7 はじめに

Cisco Prime Assurance Manager 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。これらの作業については、『*Cisco Prime Assurance Manager 1.1 User Guide*』の「Getting Started」にすべて記載されています。これらの作業が完了すれば、エンドツーエンドのアプリケーション パフォーマンスをモニタしたり、問題をトラブルシューティングしたり、WAN のパフォーマンスを最適化したり、一貫性のあるネットワーク サービスの配信を保証したりできます。

# 8 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 AM 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 AM 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 5　　ナビゲーションおよびマニュアルの参照先**

| 作業 | Cisco Prime Assurance Manager 内のナビゲーション | 『Cisco Prime Assurance Manager User Guide』内の項 |
|---|---|---|
| ネットワークの検出 | [Operate] > [Discovery] | 「Setting Up」 |
| サイト プロファイルのセットアップ | [Operate] > [Site Profiles & Maps]<br>[Operate] > [Device Workcenter] | |
| ポート モニタリングのセットアップ | [Operate] > [Port Grouping] | |
| 仮想ドメインのセットアップ | [Administration] > [Virtual Domains] | |
| モニタリング ダッシュボードの使用 | [Operate] > [Monitoring Dashboards] | 「Operating the Network」 |
| テンプレートを使用した設定とモニタリング | [Design] > [Templates] | |
| アラームの表示 | [Operate] > [Alarms & Events] | 「Monitoring Alarms」 |
| デバイス設定の検索と比較 | [Operate] > [Configuration Archive] | 「Working with Device Configurations」 |
| デバイス設定のメンテナンス | [Operate] > [Configuration Archive] | 「Maintaining Device Configuration Inventory」 |
| ユーザの管理 | [Administration] > [Users, Roles & AAA] | 「Controlling User Access」 |

# 9 Cisco Prime Assurance Manager のアンインストール

ローカル サーバ上のデータ コレクタを含め、Cisco Prime Assurance Manager をアン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**　Cisco Prime Assurance Manager 仮想アプライアンスを右クリックします。

**ステップ 2**　[Remove from Disk] を選択します。

# 10 関連資料

Cisco.com の Cisco Prime Assurance Manager ページから、次の Cisco Prime Assurance Manager に関する追加ガイドにアクセスできます。

（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。

- 『*Cisco Prime Assurance Manager* 1.1 *クイック スタート ガイド*』（本マニュアル）
- 『*Cisco Prime Assurance Manager 1.1 User Guide*』
- 『*Open Source Used in Cisco Prime Assurance Manager 1.1*』
- 『*Cisco Prime Assurance 1.1 Release Notes*』

# 11 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。



シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00 ～ 12:00、13:00 ～ 17:00
http://www.cisco.com/jp/go/contactcenter/

OL-26374-01-J