Prime Infrastructure サーバのセットアップ

ここでは、次の内容について説明します。

サーバのセットアップ タスク

タスク	参照先
バックアップ設定の確認	自動アプリケーション バックアップのセットアップ
必要な製品ライセンスおよびソフトウェア アップデートのインストール	ライセンスおよびソフトウェア アップデート
Cisco.com へのログオンに使用するために保管されている Cisco.com クレデンシャル（ユーザ名とパスワード）を変更し、次の操作を行います。 • 製品アップデートの確認 • デバイス ソフトウェア イメージ アップデートの確認 • シスコ サポート ケースの登録または確認	保存されている Cisco.com クレデンシャルの設定

タスク	参照先
ソフトウェア アップデートの場合： • 製品ソフトウェア アップデート（重大な修正、デバイス サポート、アドオン）の通知を有効にする • Prime Infrastructure がソフトウェア アップデートを確認する際に、クレデンシャルを Cisco.com に保存するかどうかを指定する。保存する場合、更新の確認時にユーザにクレデンシャルについてのプロンプトを表示するかどうかを指定する	ソフトウェア アップデートに関する通知の有効化または無効化
サーバとブラウザベースの GUI クライアントの間のやり取りを保護するためにサーバ上で HTTPS を設定する（HTTP も使用できますが、HTTPS が推奨されています）	Prime Infrastructure サーバの接続の保護
ハイ アベイラビリティの設定	ハイ アベイラビリティの仕組み
データの保持および消去の調整	データ収集とバックグラウンド タスク
システムの問題を通知するサーバ関連のトラップでは、しきい値設定と重大度をカスタマイズし、設定した受信者に SNMP トラップ通知としてトラップを転送する	サーバの内部 SNMP トラップのカスタマイズおよびトラップの転送 アラーム通知先の設定
時間をサーバとネットワーク デバイスとの間で同期するための NTP（Network Time Protocol）のセットアップ	サーバでの NTP の設定
サーバとネットワーク デバイス間のファイル転送のためのサーバにおける FTP/TFTP の設定	サーバでの FTP/TFTP/SFTP サービスの有効化
Prime Infrastructure サーバのプロキシの設定	Prime Infrastructure プロキシ サーバの設定
電子メール サーバの設定	SMTP 電子メール サーバの設定
管理対象ネットワーク要素のグローバル SNMP ポーリング パラメータの設定	ネットワーク要素との通信に適用するグローバル SNMP の設定
コンプライアンス機能を有効にする（デバイス設定からの逸脱を識別するためにこの設定を使用する場合）	コンプライアンス監査の有効化および無効化
シスコ製品の向上に寄与する製品フィードバックの設定	シスコサポート リクエストのデフォルトの設定
シスコ製品の向上に寄与する製品フィードバックの設定	シスコ製品フィードバックの設定

ユーザ管理セットアップ タスク

タスク	参照先
管理権限を持つ Web GUI ユーザを作成し、Web GUI root アカウントを無効にします。	管理者権限を持つ Web GUI ユーザの作成 Web GUI ルート ユーザの無効化および有効化
ユーザ監査のセットアップ	設定アーカイブとソフトウェア画像管理の変更を監査する（変更監査ダッシュボード）
ユーザ認証および許可のセットアップ	外部認証の設定 ローカル認証の設定
ユーザ アカウントとユーザ グループの作成	ユーザが実行できるタスクの制御（ユーザ グループ）
ユーザ セキュリティ設定の調整（ローカル認証のパスワード規則、アイドル時間のログアウト設定）	ローカル認証のためのグローバル パスワード ポリシーの設定 アイドル ユーザ用のグローバル タイムアウトを設定する
ジョブを許可できるユーザの指定	ジョブ承認者を設定してジョブを承認する
仮想ドメインを作成してデバイス アクセスを制御する	デバイスへのユーザ アクセスを制御するための仮想ドメインの作成
ユーザが GUI クライアントにログインしたときに表示されるメッセージの作成	ログイン バナー（ログインの免責事項）の作成

障害管理セットアップ タスク

タスク	参照先
アラームとイベントを電子メール形式で他の受信者に転送する	アラーム通知先の設定
アラームとイベントを SNMP トラップ形式で他の受信者に転送する	アラーム通知先の設定

タスク	参照先
アラームとイベントの表示と検索用のグローバル設定を構成する • アラーム テーブルとイベント テーブルで確認済み、割り当て済み、およびクリア済みのアラームを非表示にする • 確認済みと割り当て済みのアラームを検索結果に含める • デバイス名をアラーム メッセージに含める	確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する
特定のイベントの重大度をカスタマイズする	アラーム重大度レベルの変更
アラームに関連付けられたトラブルシューティングテキストをカスタマイズする	アラームのトラブルシューティングテキストのカスタマイズ
特定のアラームの自動クリア間隔をカスタマイズする	アラームの自動クリア間隔の変更
アラームの [障害ソース（Failure Source）] フィールド内のテキストをユーザにわかりやすくする	アラーム重大度レベルの変更
一般イベント処理を制御する	汎用トラップ処理を有効または無効にする
ユーザがシスコ サポート要求を作成できるかどうかとその方法を制御する	シスコサポート リクエストのデフォルトの設定

管理者セットアップ タスク

オペレーション センターのセットアップ

Prime Infrastructure オペレーション センターは、 Prime Infrastructure の複数のインスタンスを単一のインスタンスから管理できるようにするライセンス機能です。オペレーションセンターを使用する前に、以下の作業を実行する必要があります。

1. オペレーション センターをホストする Prime Infrastructure サーバでオペレーション センターのライセンスをアクティブ化します。ライセンスを適用すると、オペレーションセンターが、管理対象の Prime Infrastructure インスタンスのクラスタの SSO サーバとして有効になります。
2. 管理対象の Prime Infrastructure インスタンスをオペレーション センターに追加します。各インスタンスはオペレーション センターへの追加時に SSO クライアントとして設定することができます

3. （省略可能）オペレーション センターに関するパーソナルおよびグローバルなアイドル ユーザ タイムアウトおよびその管理インスタンスのすべてを無効化します。
4. （省略可能）TACACS+ または RADIUS サーバを使用し、オペレーション センターに対応したリモート AAA 、およびその管理インスタンスのすべてを設定します。

これらの作業の実行方法については、「関連項目」を参照してください。

関連トピック

オペレーション センターへの Cisco Prime Infrastructure インスタンスの追加 （6 ページ）
オペレーション センターのアイドル ユーザ タイムアウトを無効にする （7 ページ）

オペレーション センター ライセンスのアクティブ化

オペレーション センターをセットアップする前に、次の処理を実施する必要があります。

- オペレーション センターをホストする Prime Infrastructure サーバの DNS エントリがそのサーバで設定されたホスト名と一致することを確認します。たとえば、オペレーションセンターをホストする Prime Infrastructure サーバで **nslookup** *ipaddress* コマンドと **hostname** コマンドを実行した場合、同じ出力が生成される必要があります。
- オペレーション センターを使用してネットワーク情報にアクセスするすべてのユーザが NBI Read と NBI Write の両方のアクセス権を持っていることを確認します。これは、これらのユーザ プロファイルを編集して、「NBI Read」ユーザ グループと「NBI Write」ユーザ グループのメンバーにすることで実施できます（「関連項目」の「ユーザ グループ メンバーシップの変更」を参照）。
- デフォルトでは、オペレーション センター ユーザー 1 人あたりの SSO ログイン セッションの最大数は 5 つです。これは、インスタンス数にも該当します。したがって、アクティブ SSO セッションの数が 5 を超えないようにする必要があります。そうでない場合は、管理インスタンスが「到達不能」の状態になります。
- オペレーション センターでリモート AAA を使用する場合：始める前に RADIUS または TACACS+ AAA サーバを設定します（「関連項目」の「オペレーションセンター用の AAA を有効にする」を参照）。

オペレーション センターを個別にインストールする必要はありません。その代わり、他の Prime Infrastructure インスタンスを管理するために使用する Prime Infrastructure サーバを選択またはインストールし、そのサーバでオペレーションセンターのライセンスをアクティブにすることができます。

ライセンスを有効する際に、オペレーション センターは SSO サーバとして自動的に構成されます Prime Infrastructure。

オペレーション センターを使用して管理できる Prime Infrastructure インスタンスの数は、購入したライセンスによって異なります。詳細については、『Cisco Prime Infrastructure Ordering and Licensing Guide』を参照してください。

手順

ステップ 1 [管理（Administration）]>[ランセンスおよびソフトウェア アップデート（Licenses and Software Updates）]>[ライセンス（Licenses）]>[ファイル（Files）]>[ライセンス ファイル（License Files）] の順に選択します。[ライセンス ファイル（License Files）] ページが表示されます。

ステップ 2 [追加（Add）] をクリックします。[ライセンス ファイルの追加（Add a License File）] ダイアログボックスが表示されます。

ステップ 3 [ファイルの選択（Choose File）] をクリックします。

ステップ 4 ライセンス ファイルに移動し、ファイルを選択して、[開く（Open）] をクリックします。

ステップ 5 [OK] をクリックします。 Prime Infrastructure は、オペレーション センターのライセンスが追加されたことを確認します。

ステップ 6 SSO がセットアップされていないことを通知された場合は、次の手順を実行します。

- この新しいオペレーション センターを自動的に SSO サーバとして設定するには、[はい（Yes）] をクリックします。
- SSO を DNS 名で設定するには、[いいえ（No）] をクリックします。シームレス SSO が SSO サーバを DNS 名で追加します。

ステップ 7 ログアウトするよう指示があった場合：[OK] をクリックします。新しくアクティブになったライセンスが [ライセンス（Licenses）]>[ライセンス ファイル（License Files）] ページに表示されます。

ステップ 8 Prime Infrastructure からログアウトしてから、ログインし直します。表示されたログイン ページに [Cisco Prime Infrastructureオペレーションセンター[SSO]（Cisco Prime Infrastructure Operations Center [SSO]）] と表示され、ライセンスが適用されたことがわかります。

関連トピック

オペレーション センターのセットアップ （4 ページ）
オペレーション センター用の AAA の有効化 （8 ページ）
ユーザ グループ メンバーシップの変更

オペレーション センターへの Cisco Prime Infrastructure インスタンスの追加

オペレーション センターのライセンスを有効にしたら、オペレーション センターを使用して管理する Prime Infrastructure サーバ インスタンスをそれぞれオペレーション センターに追加する必要があります。

オペレーション センターを使用して管理するそれぞれの Prime Infrastructure サーバ インスタンスを、オペレーション センター サーバの SSO クライアントとして有効にする必要があります。この操作は事前に行うことができます。その場合、オペレーションセンターを管理対象インスタンスの SSO サーバとして追加します（「関連項目」の「SSO サーバの追加」を参照）。また、 Prime Infrastructure サーバをオペレーション センターに追加する際にオペレーション センターがこの操作を行うようにすることもできます（ Prime Infrastructure サーバ インスタンスの root ユーザのパスワードが必要です）。

手順

ステップ 1 Prime Infrastructure オペレーション センターにログインします。

ステップ 2 [モニタ（Monitor）] > [サーバの管理およびモニタ（Manage and Monitor Servers）] を選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 オペレーション センターを使用して管理する Prime Infrastructure サーバ インスタンスの IP アドレス/FQDN を入力します。サーバのエイリアスまたはホスト名も入力できます。

オペレーション センターと、 Prime Infrastructure が管理するインスタンスとの間の HTTPS 通信用に、ポート番号 443 がプリセットされています。別のポートで HTTPS が設定されている場合を除き、この値は変更しないでください。

ステップ 5 OK をクリックします。

追加する Prime Infrastructure サーバ インスタンスが、すでにオペレーション センターを SSO サーバとして使用するよう設定されている場合、管理対象サーバインスタンスとして追加されます。

Prime Infrastructure サーバ インスタンスが SSO クライアントとして設定されていない場合は、以下の手順に従います。

a) [自動的にシングル サインオンを有効化（Enable Single-Sign-On Automatically）] を選択します。オペレーション センターで**ユーザ名**と**パスワード**を入力するよう要求されます。
b) 追加する Prime Infrastructure サーバ インスタンスで、root ユーザのユーザ名とパスワードを入力します。
c) もう一度 [OK] をクリックします。

ステップ 6 上記の手順を繰り返して、他の Prime Infrastructure サーバを追加します。ライセンスの限度まで追加できます。

関連トピック

オペレーション センターのセットアップ （4 ページ）
SSO サーバの追加

オペレーション センターのアイドル ユーザ タイムアウトを無効にする

デフォルトで、 Prime Infrastructure は、セッションが長時間にわたってアイドル状態になっているユーザをすべて自動的にサインアウトします。この機能は、デフォルトで有効化されており、ネットワーク帯域幅と Prime Infrastructure 処理サイクルを維持して積極的に活用できるようになっています。

この機能は、オペレーションセンターのユーザにとって不都合な場合があります。これは、一般にオペレーション センターのみならず、オペレーション センターが管理する Prime Infrastructure の複数のインスタンスとのセッションを開いたままにするユーザに当てはまります。これらのセッションの 1 つがアイドル状態になると、すべてのセッションに対してグロー

バル アイドルユーザ タイムアウトが適用され、警告なしに突然のログアウトという結果になります。

この不便さを回避する必要がある場合、 Prime Infrastructure 管理者は以下のようにします。

1. 『Cisco Prime Infrastructure User Guide』の「*Adjust Your GUI Idle Timeout and Other Settings*」の項の説明に従って、グローバル アイドル ユーザ タイムアウト機能を無効にします。ただし、管理者はこの機能を無効化する場合、オペレーション センターが管理する Prime Infrastructure 管理インスタンスのそれぞれに対して別々に行う必要があります。
2. オペレーション センターのユーザに、アクセス対象となる Prime Infrastructure 管理インスタンスのユーザ固有のアイドル ユーザ タイムアウト機能を無効にするように指示します（『Cisco Prime Infrastructure User Guide』の「*Changing Your Idle User Timeout*」の項を参照）。ただし、それぞれの Prime Infrastructure ユーザはこの機能を無効にする場合、アクセス対象となる Prime Infrastructure 管理インスタンスのそれぞれに対して、別々に行う必要があります。

関連トピック

オペレーション センターのセットアップ （4 ページ）

オペレーション センター用の AAA の有効化

オペレーション センターでは、ローカル認証のほかに、TACACS+ や RADIUS を使用した リモート AAA をサポートします。リモート AAA の使用はオプションですが、使用する場合はこのワークフローに従います。

1. リモート サーバの TACACS+ または RADIUS のセットアップを完了します。Cisco ACS と RADIUS または TACACS+ による外部認証 を参照するか、 Cisco ISE と RADIUS または TACACS+ による外部認証
2. オペレーション センターのサーバにログインし、**[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、およびAAA（Users, Roles & AAA）]** に移動します。
3. TACACS+ または RADIUS サーバをオペレーション センターに追加します。
4. [SSOサーバの設定（SSO Server Settings）] をクリックします。リモート サーバの認証に応じて、[SSOサーバAAA（SSO Server AAA）] モードで TACACS+ または RADIUS を選択します。
5. [ローカルへのフォールバックを有効にする（Enable Fall-back to Local）] チェック ボックスをクリックして、ドロップダウン リストから「認証の失敗時またはサーバからの応答がない場合（On Authentication Failure or No Response from Server）」を選択します。AAA サーバで構成されている共有シークレットが共有シークレットと一致する必要があることに注意してください。

（注） **[管理 （Administration）] > [ユーザ（Users）] > [ユーザ、ロール、およびAAA（Users, Roles & AAA）] > [AAAモードの設定（AAA Mode Setting）]** で、AAA 設定を変更しないことを確認してください。SSO モードのみにする必要があります。

6. Prime Infrastructure サーバでインスタンスを管理するため、手順に従います。

（注） Prime Infrastructure 管理インスタンス、SSO サーバに到達できない場合や応答しない場合に TACACS+ または RADIUS にフォールバックのみします。

次の作業

セットアップ作業を完了すると、オペレーション センターの使用が可能になります。

オペレーションセンターインスタンスでハイアベイラビリティ（HA）を使用できるようにすることができます。HA では、リンクされて同期された Prime Infrastructure サーバのペアを使用して、いずれかのサーバで発生する可能性のあるアプリケーション障害またはハードウェア障害による影響を最小限に、あるいは完全に排除します。詳細については、「関連項目」の「オペレーション センター用の HA の有効化」を参照してください。

関連トピック

オペレーション センターのセットアップ （4 ページ）
オペレーション センター用の HA の有効化

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。この一覧には、 Prime Infrastructure のユーザ インターフェイスを使用してアクセスできます。[ヘルプ（Help）]>[サポートされるデバイス（Supported Devices）] を選択してください。

また、関連項目の説明に従って、デバイスが SNMP トラップおよび Syslog と、Network Time Protocol（NTP）をサポートするよう設定する必要があります。

関連トピック

SNMP の設定 （9 ページ）
NTP の設定 （10 ページ）

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 Cisco 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**

引数の説明

- *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 Cisco 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*

引数の説明

- *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。

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

使用するデバイスと Prime Infrastructure サーバ間で IPSec トンネリングの実装を計画している場合、IPSec は自由形式の Syslog をサポートしないので、IPSec トンネリングの実装後には、それらのデバイスから Prime Infrastructure サーバに送信される Syslog を受信しなくなることに注意してください。ただし、IPSec は SNMP トラップをサポートします。これらのタイプのデバイスから SNMP 通知を引き続き取得するには、 Prime Infrastructure サーバに SNMP トラップを送信するようにデバイスを設定する必要があります。

NTP の設定

Network Time Protocol（**NTP**）は、ネットワーク内のすべてのデバイスと Prime Infrastructure サーバで正しく同期される必要があります。この中には Prime Infrastructure 関連のすべてのサーバが含まれます。たとえば、 Prime Infrastructure のバックアップに使用するリモート FTP サーバ、セカンダリ Prime Infrastructure ハイ アベイラビリティ サーバ、 Prime Infrastructure プラグ アンド プレイ ゲートウェイ、VMware vCenter と ESX の仮想マシンなどがあります。

Prime Infrastructure サーバのインストール時にデフォルトおよびセカンダリの NTP サーバを指定します。また、 Prime Infrastructure の **ntp server** コマンドを使用して、インストール後に NTP

サーバのリストを追加または変更することもできます。詳細については、「CLI から接続する方法」および『Command Reference Guide』の **ntp server** コマンドに関する項を参照してください。 Prime Infrastructure を NTP サーバとして設定することはできません（NTP クライアントとしてのみ機能します）。

ネットワーク全体の NTP 同期の管理で障害が発生した場合、 Prime Infrastructure で異常な結果が発生する可能性があります。ネットワーク時刻精度の管理は組織のネットワーク アーキテクチャを含む広範囲の問題であり、このガイドの範囲外です。このトピックの詳細については、シスコ ホワイト ペーパー『Network Time Protocol: Best Practices』などを参照してください。

保証付き Cisco Prime Infrastructure のデータ ソースの設定

Prime Infrastructure Assurance 機能のライセンスを取得する場合は、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。

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 1 : Prime Infrastructure Assurance：サポートされるデータ ソース、デバイス、およびソフトウェア バージョン 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 Cisco 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 1 : Prime Infrastructure Assurance：サポートされるデータ ソース、デバイス、およびソフトウェア バージョン 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 Cisco 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、「SNMP の設定」で説明されているように、 Prime Infrastructure が SNMP を使用してデータを収集できるよう変更する必要がある場合もあります。

保証データ ソースの設定

Prime Infrastructure をインストールする前に、次の表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。次の表に、この作業を行う方法のガイドラインを示します。

表 *1*：*Prime Infrastructure Assurance*：サポートされるデータ 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（Device Type）	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 User Guide』の「*Configure 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 User Guide』の「*Configure 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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（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 User Guide』の「*Configure 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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（System Templates - CLI）] > [Medianet - PerfMon]**

デバイスタイプ（**Device Type**）	**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 6500	SG15.1(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 User Guide』の「*Configure 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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（System Templates - CLI）] > [トラフィック統計情報の収集（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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（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所要時間、音声とビデオ	TCP、UDP、および ART を設定するには、『Cisco Prime Infrastructure User Guide』の「*Configure 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。 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート - CLI（System Templates - CLI）] > [Medianet - PerfMon]**

デバイスタイプ（Device Type）	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、および ART を設定するには、『Cisco Prime Infrastructure User Guide』の「*Improve Application Performance With Application Visibility and Control*」の章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 の有効化

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 エクスポートを有効にします。
- 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
- 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 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
- transport udp PiInPort
- 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
- 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 の有効化

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有効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を有効にする必要はありません。物理インターフェイス上でNetFlowを有効にすれば、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 ここで、
- *PrInIP* は、 Prime Infrastructure サーバの IP アドレスです。
- *PiInPort* は、 Prime Infrastructure サーバが NetFlow データをリッスンしている UDP ポートです。（デフォルトは 9991 です）。
- *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です。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 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 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 12.2
- 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

ネットワーク解析モジュール（NAM）を展開する

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」の項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 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 の有効化

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、Cisco 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パフォーマンス エージェント（PA）データ フロー ソースを設定します。

たとえば、Cisco 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、収集するフロー データを持つ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：

- 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 を有効にします。

- 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。

Cisco Prime Infrastructure 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。動作中の Prime Infrastructure のバージョンとパッチ バージョンは、CLI コマンド **show version** と **show application** 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し、新しいバージョンにアップグレードする前に必要なパッチ ファイルのみをダウンロードしてインストールします。適切なパッチを見つけるには、ブラウザで Cisco Download Software ナビゲータを開きます。

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

手順

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) ブラウザで Cisco Download Software ナビゲータを表示し、[製品（Products）] > [クラウドシステム管理（Cloud and Systems Management）] > [ルーティングおよびスイッチ管理（Routing and Switching Management）] > [ネットワーク管理ソリューション（Network Management Solutions）] > [Prime Infrastructure] を選択します。
b) 現在使用しているものに最も近いバージョンの Prime Infrastructure を選択します。
c) [Prime Infrastructure パッチ（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 [ダウンロード（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 サーバとのコマンドライン インターフェイス セッションを開きます（CLI から接続する方法を参照）。

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**

ここで、

- *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。
- *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（例：/localdisk）。

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 Repositoryname*

ここで、

- *patchFile* は、/localdisk/defaultRepo にコピーしたパッチ ファイルの名前です。
- *Repositoryname* はリポジトリの名前です。

例：admin# patch install test.tar.gz defaultRepo