Prime Infrastructure サーバーのセットアップ

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

サーバーのパーティションデータのスクラビング

サーバーからすべてのパーティションデータをスクラブまたは消去する必要がある場合があります。欠陥のあるアプライアンスからデータを消去して、インストール用のデータを上書きできます。

インストールの問題を回避するために、次の手順を使用してサーバーからすべてのパーティションデータを消去します。

.

始める前に

Red Hat Enterprise Linux 6.4 の完全な DVD ISO をダウンロードしてください。

ステップ 1 CLI 管理者ユーザーとしてサーバーにログインします。

ステップ 2 RHEL インストール DVD ISO からシステムを起動してレスキューモードに入ります。

ステップ 3 レスキュー環境での起動が完了したら、使用する言語を選択します。

ステップ 4 画面にプロンプトが表示されたら使用するキーボードレイアウトを選択します。

ステップ 5 レスキュー環境では、システムの現在の Red Hat Enterprise Linux インストールが検索され、次のオプションが表示されます。

a) [Continue] を押してシェルモードに入り、レスキューモードから次のスクリプトを実行します。

```
# fdisk -l | egrep "Disk /dev/v|Disk /dev/s|Disk /dev/h|Disk /dev/dasd|Disk /dev/cciss" | cut -d'
' -f1-2 | sed 's/Disk/dd if=\/dev\/zero/g' | sed 's/dd if=\/dev\/zero /dd if=\/dev\/zero of=/g' |
sed 's/:/ bs=1M count=2048/g' > /tmp/wipeout.sh # cat /tmp/wipeout.sh # sh /tmp/wipeout.sh
```

ステップ 6 ワイプアウト操作を確認するには、次のコマンドを実行して、使用可能なパーティションデータを確認します。

```
# fdisk -l
```

ユーザー管理セットアップ タスク

タスク	参照先
管理権限を持つ Web GUI ユーザーを作成し、Web GUI root アカウントを無効にします。	Web GUI ルート ユーザーの無効化および有効化
ユーザー認証および許可のセットアップ	
ユーザー アカウントとユーザー グループの作成	ユーザーが実行できるタスク Web インターフェイスの制御
ユーザー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
ジョブを許可できるユーザーの指定	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
ユーザーが 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	

タスク	参照先
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
特定のイベントのシビラティ（重大度）をカスタマイズする	シビラティ（重大度）レベルの変更
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ーにわかりやすくする	シビラティ（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
ユーザーがシスコ 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

オペレーション センターは、 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 サーバーでオペレーション 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 インスタンスのクラスタのSSOサーバーとして有効になります。

（注） スマート ライセンス機能を使用して、オペレーション センターをホストする Prime Infrastructure サーバーでオペレーション センター ライセンスをアクティブ化することもできます。また、スマート ライセンスを適用すると、オペレーション センターが、自身が管理する Prime Infrastructure インスタンスのクラスタの SSO サーバーとして自動的に有効になります。スマート ライセンスの詳細については、スマートライセンスを参照してください。

2. 管理対象の 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 ユーザー 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 サーバーを使用し、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 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 ユーザー 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 サーバーの DNS エントリがそのサーバー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 サーバーで **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ーが 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、これらのユーザー プロファイルを編集して、「NBI Read」ユーザー グループと「NBI Write」ユーザー 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「ユーザー 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 サーバーを設定します（「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 インスタンスを管理するために使用する サーバーを選択またはインストールし、そのサーバーでオペレーション 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。

（注） オペレーション センター ライセンスを有効にすると、同じサーバーインスタンスがデバイスを直接モニターできなくなります。デバイスは別のインスタンスに追加されます。

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 サーバーとして自動的に構成されます。

オペレーション センターを使用して管理できる 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。

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。 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 サーバー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 サーバーを 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 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 （3 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）
ユーザー 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のスマート ソフトウェア ライセンスの有効化

ステップ 1 これが初回の場合、スマート ライセンスを選択します。

a) [管理（Administration）] > [ライセンスとソフトウェア アップデート（Licenses and Software Updates）] > [ライセンス（Licenses）] の順に選択します。

しばらくすると、Prime Infrastructure にダイアログボックスが表示され、従来のライセンスを使用していないためページにアクセスできないことが通知されます。これは正常です。

b) ダイアログ ボックスで、[スマート ライセンスの設定（Smart License Settings）] をクリックします。

c) [ライセンス設定（Licensing Settings）] タブをクリックします。

ステップ 2 すでにスマート ライセンスを使用している場合は、以下の手順に従います。

a) [管理（Administration）] > [ライセンスとソフトウェア アップデート（Licenses and Software Updates）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] の順に選択します。

b) [ライセンス設定（Licensing Settings）] タブをクリックします。

ステップ 3 [スマートソフトウェアライセンシング（Smart Software Licensing）] ラジオ ボタンをクリックします。

ステップ 4 [製品名（Product Name）] ドロップダウンリストから [Prime Infrastructure オペレーションセンター（Prime Infrastructure Operation Center）] を選択し、[スマート ソフトウェア ライセンシングの有効化（Enable Smart Software Licensing）] をクリックします。

（注） オペレーションセンターの SSO を有効にするには、**[IP/DNS] ダイアログボックスを使用して同じサーバーに SSO を追加する場合は、**[はい（Yes）] をクリックします。

ステップ 5 [使用可能なライセンス（Available Licenses）] ダイアログ ボックスでライセンスを選択してから、[保存（Save）] をクリックします。

オペレーション センターへの 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 サーバー 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 サーバー インスタンスを、オペレーション センター サーバーの 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 サーバーとして追加します（「関連項目」の「SSO サーバーの追加」を参照）。また、サーバーをオペレーション 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（ サーバー インスタンスの root ユーザーのパスワードが必要です）。

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 [モニタリング（Monitor）] > [サーバーの管理およびモニタリング（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 サーバー インスタンスの IP アドレス/FQDN を入力します。サーバー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、 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 サーバー インスタンスが、すでにオペレーション センターを SSO サーバーとして使用するよう設定されている場合、管理対象サーバー インスタンスとして追加されます。

サーバー 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**ユーザー名**と**パスワード**を入力するよう要求されます。

b) 追加する サーバー インスタンスで、root ユーザーのユーザー名とパスワードを入力します。

（注） SSO 認証ユーザーとしてログインして API クエリを実行する場合は、SSO は API が要求する基本認証をサポートしていないため、その特定のインスタンスにローカル ユーザーとしてログインしていることを確認してください。

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 サーバーを追加します。ライセンスの限度まで追加できます。

（注） Prime Operations Center で追加した後でマネージドインスタンスの高可用性を構成する場合は、**[モニター] > [管理対象要素] > [サーバーの管理と監視] に移動して、プライマリ サーバーとセカンダリ サーバーの詳細が正しく表示されていることを確認します。**.

関連トピック

オペレーション センターのセットアップ （3 ページ）
SSO サーバーの追加

オペレーション センターのアイドル ユーザー タイムアウトを無効にする

デフォルトで、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ー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 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ー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 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ーに当てはまります。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 ユーザー 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、 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 ユーザー 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 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ーに、アクセス対象となる 管理インスタンスのユーザー固有のアイドルユーザー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 ユーザーはこの機能を無効にする場合、アクセス対象となる 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 （3 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 サーバーの 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」またはCisco ISE と RADIUS または TACACS+ による外部認証を参照してください。
2. オペレーション センターのサーバーにログインし、**[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、およびAAA（Users, Roles & AAA）]** に移動します。
3. TACACS+ または RADIUS サーバーをオペレーション センターに追加します。
4. [SSOサーバーの設定（SSO Server Settings）] をクリックします。リモート サーバーの認証に応じて、[SSOサーバー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ー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 サーバー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）] > [ユーザー（Users）] > [ユーザー、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 サーバーでインスタンスを管理するため、手順に従います。

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

次の作業

セットアップ タスクを完了すると、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 サーバーのペアを使用して、いずれかのサーバー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 （3 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

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、のユーザー 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

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。

- 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 サーバー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

- 設定するコミュニティ文字列は *private* と *public* 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 サーバー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 サーバーの 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、通知動作でサーバー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 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 サーバー間で 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 サーバーに送信される 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、 サーバーに 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 サーバーで正しく同期される必要があります。この中には 関連のすべてのサーバーが含まれます。たとえば、のバックアップに使用するリモート FTP サーバー、セカンダリ ハイ アベイラビリティ サーバー、 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。

サーバーのインストール時にデフォルトおよびセカンダリの NTP サーバーを指定します。また、 の **ntp server** コマンドを使用して、インストール後に NTP サーバー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。 を NTP サーバー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、 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 のデータ ソースの設定

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 がモニター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 では、エクスポートされたデータ ソース（表 1 : 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 : 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、 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、 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

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 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*: *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。 **[設定（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。 **[設定（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	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 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。 **[設定（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。 **[設定（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。 **[設定（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。 **[設定（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 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。

- 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 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、 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、 サーバの IP アドレスです。
- *PiInPort* は、 サーバーが 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

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。

- モニター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 サーバー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、 は Flexible NetFlow のバージョン 5 と 9 をサポートします。NetFlow は、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 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、 サーバーの IP アドレスです。
- *PiInPort* は、 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 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 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
- 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。

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、 に直接エクスポートする必要があります。NAM から 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

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 モニター 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ーに転送するには、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。

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 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 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。

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、サーバーのデフォルト 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）] 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 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 サーバー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

翻訳について
このドキュメントは、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。