Cisco Prime Infrastructure 3.10 管理者ガイド

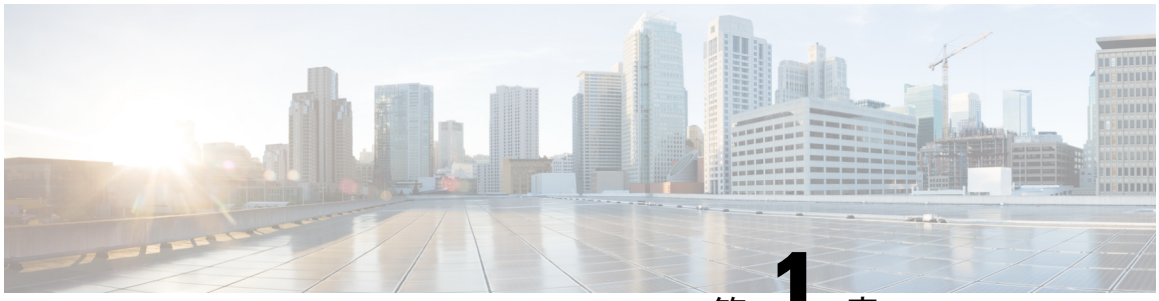
初版：2021 年 9 月 24 日

最終更新：2021 年 10 月 5 日

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/

【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。

目 次



第 1 章

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 （204 ページ）
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 （204 ページ）
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 （248 ページ）
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 （246 ページ）
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 （251 ページ）
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 （114 ページ）

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 （294 ページ）
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（295 ページ）
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 （295 ページ）
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（295 ページ）
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 （298 ページ）
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 （127 ページ）

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 （37 ページ）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 （236 ページ）

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 （264 ページ）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 （356 ページ）

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 （147 ページ）」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 （147 ページ）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）。

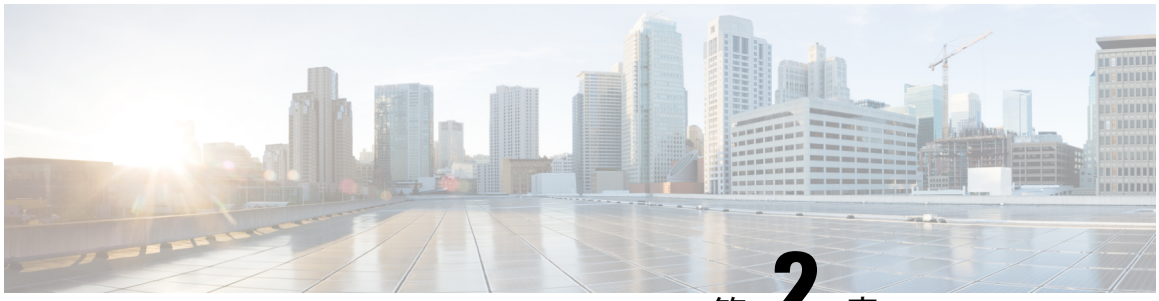
ステップ 4 パッチをインストールするには、次を実行します。

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



第 2 章

ライセンスおよびソフトウェアアップデート

ここでは、次の内容について説明します。

Prime Infrastructure ライセンス

ライセンスは、ネットワークの管理に必要な Prime Infrastructure の機能にアクセスするために購入します。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。

[管理（Administration）]>[ライ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）] ページを使用して、従来の Cisco Prime Infrastructure、ワイヤレス LAN コントローラ、および Mobility Services Engine（MSE）のライセンスを管理できます。

Prime Infrastructure および MSE のライセンスは [管理（Administration）]>[ライ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）] ページから完全に管理できますが、Cisco Wireless LAN Controller（WLC）は表示することしかできません。Cisco WLC のライセンスを管理するには、Cisco WLC または Cisco License Manager（CLM）を使用する必要があります。

[管理（Administration）]>[ライ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）] ページでは、スマート ライセンスの管理ができます。

基本ライセンスのほかに、それぞれの Prime Infrastructure 機能を使用して特定の数のデバイスを管理するために、その機能へのフルアクセスを提供する機能ライセンス（保証ライセンスなど）が必要です。

初めて Prime Infrastructure をインストールする場合はデフォルトで使用できる組み込みの評価ライセンスを使用してライフサイクルと保証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 100 台のデバイスで 60 日間有効です。次の場合に、ask-prime-infrastructure@cisco.com にリクエストを送信できます。

- 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

評価ライセンスの期限が切れる前に、基本ライセンスを注文し、対応する機能ライセンスを購入する必要があります。購入するライセンスは、以下の条件を満たす必要があります。

- ネットワークを管理するために使用する、すべての Prime Infrastructure 機能にアクセスできること。
- Prime Infrastructure を使用して管理するネットワー内のすべてのデバイスが対象であること。

これらの条件を満たすライセンスを入手するためには、以下のようにしてください。

1. 利用可能なライセンス パッケージのタイプと、それぞれの要件を理解します。
2. 既存のライセンスを確認します。ライセンスの注文およびダウンロードの方法については、ヘルプを参照してください。
3. 必要な機能のパッケージと、管理する必要があるデバイス数の両方に基づいて、必要となるライセンス数を計算します。
4. 新しいライセンスを追加します。
5. 既存のライセンスを削除します。

（注） Prime Infrastructure はノード固定型ライセンスのアプローチを現在はサポートしていないため、ライセンスの生成に必要な UDI 情報は、次に示すように、標準構文に制限されています。

- PID = PRIME-NCS-APL（物理アプライアンスの場合）

  PID = PRIME-NCS-VAPL（仮想アプライアンス/仮想マシンの場合）
- SN = ANY:ANY

新しいライセンスを生成するには、前述の形式で細かく区別して指定する必要があります。

詳細については、『Cisco Prime Infrastructure Ordering and Licensing Guide』を参照してください。

関連トピック

ライセンスの詳細の確認 （23 ページ）
ライセンスの追加 （23 ページ）
ライセンスの削除 （24 ページ）

Prime Infrastructure ライセンスの購入

Prime Infrastructure ライセンスは、ユーザーが使用可能な機能と、それらの機能を使用して管理可能なデバイスの数を制御します。Prime Infrastructure のライセンス タイプの詳細と注文方法については、使用する Prime Infrastructure のバージョンの『Cisco Prime Infrastructure Ordering and Licensing Guide』を参照してください。

[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）] 領域に表示される「基本ライセンスが見つかりません（Base license is missing）」や「複数の基本ライセンスが存在します。1つのみ使用してください（Multiple base licenses present, use only one）」などの警告メッセージは、無視して構いません。

ライセンスの詳細の確認

新しいライセンスを購入する前に、既存のライセンスに関する詳細を確認することをお勧めします。たとえば、システムで管理するデバイス数など。

ライセンスの詳細を確認するには、**[管理（Administration）]>[ライ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）]** を選択します。

関連トピック

Prime Infrastructure ライセンス （21 ページ）
コントローラ ライセンス （27 ページ）
MSE ライセンス （29 ページ）
保証ライセンス （35 ページ）

ライセンスの追加

以下の場合には、新しいライセンスを追加する必要があります。

- 新しい Prime Infrastructure ライセンスを購入した場合。
- すでに Prime Infrastructure を使用していて、追加のライセンスを購入した場合。

ステップ 1 **[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。

ステップ 2 [概要（Summary）] フォルダで [ファイル（Files）] をクリックし、次に [ライセンス ファイル（License Files）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ライセンス ファイルの場所を参照し、[OK] をクリックします。

関連トピック

ライセンスの削除 （24 ページ）
ライセンスのトラブルシューティング （24 ページ）

MSE ライセンスの構成マトリックス （29 ページ）
保証ライセンスの詳細の確認 （35 ページ）

ライセンスの削除

ライセンスを Prime Infrastructure から削除すると、すべてのライセンス情報がサーバーから削除されます。後で追加しなければならなくなった場合に備え、元のライセンス ファイルのコピーを作成してください。以下のような場合に、ライセンスを削除する必要があります。

- 一時ライセンスをインストールした場合。この場合、永続ライセンスを適用する前に、一時ライセンスを削除する必要があります。
- 別のサーバーにライセンスを移動する必要がある場合。この場合、元のサーバーからライセンスを削除してから、licensing@cisco.com 宛にライセンスの再ホストを要請する E メールを送信する必要があります。その後、再ホストされたライセンスを新しいサーバーに適用できます。

ステップ 1 [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。

ステップ 2 [ファイル（Files）] > [ライセンス ファイル（License Files）] の順にクリックします。

ステップ 3 削除するライセンス ファイルを選択し、[削除（Delete）] をクリックします。

関連トピック

ライセンスの追加 （23 ページ）
ライセンスのトラブルシューティング （24 ページ）
MSE ライセンスの構成マトリックス （29 ページ）
保証ライセンスの詳細の確認 （35 ページ）

ライセンスのトラブルシューティング

ライセンスのトラブルシューティングを行うには、システムにインストールされているライセンスの詳細を取得する必要があります。次のように操作します。

- 現在のライセンスの一覧を表示するには、[ヘルプ（Help）] > [Prime infrastructure について（About Prime Infrastructure）] の順にクリックします。
- ライセンスの詳細を取得するには、[管理（Administration）] > [ライ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）] の順に選択します。

ライセンスのトラブルシューティングを行う際は、Prime Infrastructure に次の 6 種類のライセンスがあることに留意することが重要です。

- **基本（Base）**：すべての Prime Infrastructure インストールに必要です。要件は主に、購入済みの Prime Infrastructure インスタンスの数を把握して正確なロイヤリティ アカウンティ

ングを実行するためのニーズによって決まります。基本ライセンスは、Prime Infrastructure インスタンスごとに必要であり、他のすべてのライセンス タイプの前提条件です。

- **ライフサイクル（Lifecycle）**：Prime Infrastructure の管理下にあるデバイスの総数を規定します。ライフサイクル ライセンスは、Prime Infrastructure の管理 VDC でのみ消費されます。子 VDC はライセンスを消費しません。管理者によって自動追加されるか、または個別に追加されます。
- **保証（Assurance）**：Prime Infrastructure の管理下にある NetFlow デバイスの総数を規定します。
- **コレクタ（Collector）**：Prime Infrastructure が処理できる 1 秒あたりの NetFlow データ フローの総数を規定します。

ライフサイクルライセンスと保証ライセンスは評価版または永久版のいずれかで提供されます（基本ライセンスまたはコレクタライセンスには明確な評価版はありません）。

- **評価（Evaluation）**：このライセンスは、事前に設定された期間の Prime Infrastructure へのアクセスを許可または拡張します。タイプごとに 1 つずつの評価ライセンスしか適用できません（つまり、ライフサイクル評価ライセンスが 1 つだけ、保証評価ライセンスが 1 つだけといった具合です）。同じライセンスの永久ライセンスに対して評価ライセンスを適用することはできません。
- **永久ライセンス（Permanent License）**：このライセンスは、規定どおりに Prime Infrastructure 機能へのアクセスを許可します。時間制限はありません。永久ライセンスは、評価ライセンスに適用することができます。また、段階的に適用することもできます（つまり、複数の永久保証ライセンスを所有するといったことが可能です）。

Prime Infrastructure は、次の基本ライセンス チェックを実行します。

- ライフサイクル ライセンスは保証ライセンスに不可欠な前提条件です。
- 保証のライセンスは収集装置ライセンスに不可欠な前提条件です。

次のことにも注意してください。

- Prime Infrastructure リリース 3.0 以降では、すべてのライセンスに対してアラームを生成するしきい値限度をユーザーが設定できます。ライセンスのしきい値限度を設定するには、関連項目の「通知の設定」を参照してください。
- Prime Infrastructure は、保証ライセンスが適用されるまで、保証関連の機能、メニュー オプション、およびリンクを非表示にします。保証ライセンスを購入しても、それを適用するまで、これらの機能は非表示のままです。
- 保証ライセンスを適用すると、1 つの Prime Infrastructure インスタンスで 1 秒あたり最大 20,000 件の NetFlow データ フローの処理を許可するコレクタ ライセンスが自動的に適用されます。1 秒あたり 80,000 フローを許可する収集装置ライセンスは、このデータ レートに課されるハードディスク要件によって、専門的構成または同等の構成でしか適用できません。
- ライフサイクルおよび保証の永久ライセンスは段階的に追加できます。ただし、収集装置 80K ライセンスは 1 つしか追加できず、専門的構成または同等の構成でしか追加できません。

次の表に、トラブルシューティングに関するいくつかのシナリオとヒントを示します。

表 2: トラブルシューティング シナリオ

シナリオ	考えられる原因	解像度
Prime Infrastructure は、ライセンス エラーを報告します。	ライセンス ファイルが破損して使用できない可能性があります。この現象は、何者かがライセンス ファイルを変更しようとしたときに発生する可能性があります。	1. 既存のライセンスを削除します。 2. 新しいライセンスをダウンロードしてインストールします。
新しいライセンスを追加できない。	一部のライセンス タイプは正しい順序で追加する必要があります。基本ライセンスは、ライフサイクル ライセンスを追加するための前提条件です。保証ライセンスを追加するには、ライフサイクルライセンスが必要です。保証ライセンスは、収集装置ライセンスを追加するための前提条件です（収集装置ライセンスは、自動的に、保証ライセンスと一緒に追加されます）。	1. 基本ライセンスを追加します。 2. ライフサイクル ライセンスを追加します。 3. 保証ライセンスを追加します。 4. データ センター ライセンスを追加します。 5. 収集装置ライセンスを追加します。
デバイスの状態が、非管理対象に変更されている。	デバイスの制限は、ライフサイクル ライセンスの制限以下でなければなりません。デバイスを追加または削除すると、インベントリ対象のデバイスの状態が管理対象外に変更されます。	1. 追加デバイスを削除します。 2. 24 時間同期の後、デバイスの状態が管理対象に変更されます。 インベントリ対象のデバイスの状態が管理対象に変更されたことを確認するには、次の手順に従ってください。 1. [モニター（Monitor）] > [ネットワーク デバイス（Network Devices）] の順に選択します。 2. 目的のデバイスが列挙されている行の [インベントリ収集ステータス（Inventory Collection Status）]列をチェックします。これにより、そのデバイスの現在の収集ステータス結果のサマリーを確認できます。 3. 収集ステータスの詳細を確認するには、[インベントリ収集ステータス（Inventory Collection Status）] 列の十字アイコンの上にマウス カーソルを移動します。

関連トピック

通知の設定 （471 ページ）
ライセンスの追加 （23 ページ）
ライセンスの削除 （24 ページ）
MSE ライセンスの構成マトリックス （29 ページ）
保証ライセンスの詳細の確認 （35 ページ）

コントローラ ライセンス

コントローラ ライセンスを表示するには、[管理（Administration）] > [ライ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）] の順に選択し、左側のサイドバー メニューから [ファイル（Files）]>[コントローラ ファイル（Controller Files）] の順に選択します。

（注） Prime Infrastructure は、コントローラ ライセンスを直接管理するのではなく、単にこのライセンスをモニターします。ライセンスは、コマンドライン インターフェイス（CLI）コマンド、Web UI、Cisco License Manager（CLM）、または Cisco Smart Software Manager（CSSM）を使用して管理できます。

このページには、次のパラメータが表示されます。

- [コントローラ名（Controller Name）]
- コントローラの IP（Controller IP）：コントローラの IP アドレス。
- [機能（Feature）]：ライセンス機能には、wplus-ap-count、wplus、base-ap-count、および base が含まれます。

インストールされているすべての物理ライセンスについて、コントローラに機能レベル ライセンスと ap-count ライセンスの 2 個のライセンス ファイルが表示されます。たとえば「WPlus 500」ライセンスをコントローラにインストールすると、「wplus」および「wplus-ap-count」機能が表示されます。組み合わせによって機能レベル（WPlus または Base）および AP カウントを有効にするために、常時、このうち 2 個の機能がアクティブになっています。

WPlus と基本の両方のライセンスを保持できますが、特定の時期にアクティブにできるのは 1 つのみです。

- AP 制限値

  [AP 制限（AP Limit）]：アクセス ポイントでこのコントローラを接続できる最大容量。
- [EULA ステータス（EULA status）]：[承諾（Accepted）] または [未承諾（Not Accepted）] のいずれかで、エンド ユーザー ライセンス契約書のステータスが表示されます。
- 説明

  コメント（Comments）：ライセンスをインストールするときにユーザーが入力したコメント。
- タイプ（Type）

  タイプ（Type）：次の 4 種類のライセンスがあります。

  - 永続的

    [無制限（Permanent）]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコ ライセンス ポータルによって発行されるライセン

スであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。

- [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンドユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。アクティブ ライセンスの残日数が最少の評価ライセンスについて、残日数が表示されます。
- [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコ ライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。
- [Grace Period]：ライセンスはノードロックされており、定量の対象です。これは、ライセンスをリホストするための許可チケットの一部として、シスコ ライセンス ポータルによって発行されるライセンスです。これらのライセンスは、リホスト操作の一環としてデバイス上にインストールされます。リホスト操作の一環としてEULAを受け入れる必要があります。

[無制限（Permanent）]以外のタイプでは、ライセンスが期限切れになるまでの残日数が表示されます。現在使用中でないライセンスのカウントは、「In Use」になるまで減算されません。

- Status（ステータス）
  - [In Use]：このライセンス レベルおよびライセンスは使用中です。
  - [Inactive]：このライセンス レベルは使用中ですが、このライセンスは使用中ではありません。
  - [Not In Use]：このライセンス レベルは使用中でなく、このライセンスは現在認識されていません。
  - [Expired In Use]：このライセンスは使用中ですが期限切れであり、次回のリブートで使用されなくなります。
  - [Expired Not In Use]：ライセンスは期限切れであり、もう使用できません。
  - [制限数使用済み（Count Consumed）]：この ap-count ライセンスは使用中です。

ライセンス ファイルのリストをフィルタする必要がある場合は、コントローラ名、機能、またはタイプを入力して [実行（Go）] をクリックします。

MSE ライセンス

MSE には、次のような関連サービス エンジンとアプリケーション プロセスとともに、ネットワーク トポロジ、NMSP などの設計、ネットワーク リポジトリに関連する複数の製品機能が付属しています。

- Context-Aware サービス
- ワイヤレス侵入防御システム（WIPS）

MSE とそのサービスをスムーズに管理できるように、各種ライセンスが提供されています。

MSE とその関連サービスを使用するには、Cisco Prime Infrastructure ライセンスが必要です。

関連トピック

MSE ライセンスの構成マトリックス （29 ページ）
MSE ライセンス ファイルのサンプル （30 ページ）
MSE ライセンスの取り消しと再使用 （30 ページ）
MSE サービスの共存 （31 ページ）
MSE ライセンスの管理 （32 ページ）

MSE ライセンスの構成マトリックス

次の表 に、MSE、ロケーション サービス、SCM、wIPS および MIR について、ハイエンド、ローエンド、評価のライセンス間でのライセンスの区別を示します。

表 *3 : MSE* ライセンスの構成マトリックス

	ハイエンド	ローエンド	評価
MSE プラットフォーム	Cisco 3350 および 3355 モビリティ サービス エンジンなどのハイエンド アプライアンスおよびインフラストラクチャ プラットフォーム	Cisco 3310 Mobility Services Engine などのローエンドアプライアンスおよびインフラストラクチャ プラットフォーム	—
コンテキスト認識型サービス	25,000 タグ	2000 タグ	60 日間有効、100 タグおよび 100 要素
	25,000 要素	2000 要素	
wIPS	3000 アクセス ポイント	2000 アクセス ポイント	60 日間有効、20 アクセス ポイント

関連トピック

MSE ライセンス ファイルのサンプル （30 ページ）
MSE ライセンスの取り消しと再使用 （30 ページ）
MSE サービスの共存 （31 ページ）

MSE ライセンスの管理 （32 ページ）

MSE ライセンス ファイルのサンプル

次に、MSE ライセンス ファイルのサンプルを示します。

FEATURE MSE cisco 1.0 permanent uncounted \

VENDOR_STRING=UDI=udi,COUNT=1 \

HOST ID=ANY \

NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \

<PAK>dummyPak</PAK>" \

SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \

45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \

1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"

このサンプル ファイルには、ライセンス エントリが 5 つあります。どのライセンス エントリでも最初の行の先頭の語は、どのタイプのライセンスであるかを示します。これは、Feature または Increment ライセンスのいずれかになります。Feature（機能）ライセンスは、ライセンス付与する唯一の固定アイテムです。MSE で実行しているサービス エンジンは複数ある場合があります。Increment（増分）ライセンスは、追加型のライセンスです。MSE では、個々のサービス エンジンが増分ライセンスとして扱われます。

最初の行の 2 番めの語は、ライセンス付与する特定のコンポーネントを定義します。たとえば、MSE、LOCATION_TAG などです。3 番めの語はライセンスのベンダーを示します。たとえば、Cisco などです。4 番めの語はライセンスのバージョンを示します。たとえば、1.0 などです。5つ目の単語は有効期限を示します。これは、期限のないライセンスの場合はpermanent、それ以外の場合は dd-mm-yyyy の形式の日付になります。最後の語は、このライセンスをカウントするかどうかを定義します。

関連トピック

MSE ライセンスの構成マトリックス （29 ページ）
MSE ライセンスの取り消しと再使用 （30 ページ）
MSE サービスの共存 （31 ページ）
MSE ライセンスの管理 （32 ページ）

MSE ライセンスの取り消しと再使用

MSE アプリケーション ライセンスをあるシステムから取り消し、別のシステムで再使用できます。ライセンスを取り消すと、ライセンス ファイルはシステムから削除されます。ライセンスを別のシステムで再使用する場合は、ライセンスをリホストする必要があります。

別のシステムでアップグレード最小在庫管理単位（SKU）を使用してライセンスを再使用する場合は、対応する Base ライセンス SKU を、アップグレード SKU を再使用するシステムにイ

ンストールする必要があります。対応する Base ライセンス SKU がシステムから削除された場合、そのシステムではアップグレード ライセンス SKU を再使用できません。

ライセンスを取り消すと、ライセンスに対して変更を反映するため、MSE により個別のサービス エンジンが再起動されます。次に、サービス エンジンは、起動時に MSE から更新された容量を受け取ります。

関連トピック

MSE ライセンスの構成マトリックス （29 ページ）
MSE ライセンス ファイルのサンプル （30 ページ）
MSE サービスの共存 （31 ページ）
MSE ライセンスの管理 （32 ページ）

MSE サービスの共存

MSE 6.0 以上では、複数のサービス（コンテキスト認識型および wIPS）を同時に実行できます。6.0 よりも前のバージョンでは、Mobility Services Engine では一度に 1 つのアクティブ サービスだけがサポートされていました。

複数サービスを共存させる場合には、以下の点を考慮してください。

- サービスの共存は、ライセンス執行の影響を受けることがあります。ライセンスが有効期限内である限り、複数サービスを有効にできます。

（注） サービスごとに制限事項が異なります。たとえば、ローエンド Mobility Services Engine（MSE-3310）は合計で 2,000 の CAS 要素を追跡し、ハイエンド Mobility Services Engine（MSE-3350）は合計で 25,000 の CAS 要素を追跡します。ローエンド Mobility Services Engine の wIPS 要素の上限は 2000 で、ハイエンド Mobility Services Engine の wIPS 要素の上限は 3000 です。

- 有効期限切れの評価ライセンスがあると、サービスが起動できません。
- CAS ライセンスを追加または削除すると、Mobility Services Engine のすべてのサービス（wIPS を含む）が再起動されます。wIPS ライセンスを追加または削除しても CAS には影響しません。wIPS が再起動するだけです。
- 最大数の要素の永久ライセンスが適用されている場合でも、その他のサービスを評価モードで有効にできます。

サービスの 1 つが最大数のライセンスで実行可能になっている場合は常に、別のサービスを並行して実行することはできません。これは、両方のサービスに同時に対応できる十分なキャパシティが MSE にないためです。たとえば、MSE-3310 に 2000 の wIPS ライセンスをインストールしている場合、CAS を同時に実行することはできません。ただし、評価ライセンスはこの制限の対象外です。

関連トピック

MSE ライセンスの構成マトリックス （29 ページ）
MSE ライセンス ファイルのサンプル （30 ページ）

MSE ライセンスの取り消しと再使用 （30 ページ）
MSE ライセンスの管理 （32 ページ）

MSE ライセンスの管理

Mobility Services Engine（MSE）ライセンスを表示するには、[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、左側のサイドバー メニューから [ファイル（Files）] > [MSE ファイル（MSE Files）] の順に選択します。

このページには、見つかった MSE と以下の情報が表示されます。

- [MSE License File]：MSE ライセンスを示します。
- [MSE]：MSE 名を示します。
- [Type]：Mobility Services Engine のタイプ（クライアント要素、ワイヤレス IPS ローカル モード、またはワイヤレス IPS モニタ モード アクセス ポイント）を示します。
- [Limit]：Mobility Services Engine 全体でのライセンスを持つクライアント要素またはワイヤレス IPS モニタ モード アクセス ポイントの総数が表示されます。
- [License Type]：このページに表示されるライセンスの種類は永久ライセンスだけです。永久ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコ ライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。

パートナー エンジンを使用してタグが追跡される場合、タグ ライセンスをインストールするには、AeroScout System Manager を使用します。その他の場合、タグは CAS 要素ライセンスとまとめてカウントされます。タグ ライセンスは、該当のベンダー アプリケーションを使用して追加および管理されるため、タグ ライセンスはこのページに表示されません。詳細については、「関連項目」の AeroScout Support Page を参照してください。評価（デモ）ライセンスも表示されません。

詳細については、AeroScout サポート ページを参照してください。

関連トピック

製品認証キーの登録 （32 ページ）
クライアント ライセンス ファイルおよび wIPS ライセンス ファイルのインストール （34 ページ）
Mobility Services Engine ライセンス ファイルの削除 （34 ページ）

製品認証キーの登録

クライアント、ワイヤレス IPS、またはタグのライセンスをシスコに注文すると、製品認証キー（PAK）が配布されます。Mobility Services Engine 上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。PAK の登録に成功すると、ライセンス ファイルが E メールで送信されます。

クライアントおよびワイヤレス IPS の PAK は、シスコに登録します。

タグ PAK は AeroScout に登録されます。タグ PAK を登録するには、「関連項目」の AeroScout Support Page に移動してしてください。

製品認証キー（PAK）を登録して、インストールするライセンス ファイルを入手するには、次の手順に従ってください。

ステップ 1 ブラウザでシスコ製品ライセンス登録ポータル（「関連項目」を参照）を開きます。

このサイトへは、Prime Infrastructure の [ライセンス センター（License Center）] ページにある [製品ライセンス登録（Product License Registration）] リンクをクリックすることによってもアクセスできます。

ステップ 2 PAK を入力し、[送信（SUBMIT）] をクリックします。

ステップ 3 ライセンスの購入内容を確認します。正しい場合は [続行（Continue）] をクリックします。ライセンス入力ページが表示されます。

ライセンスが正しくない場合は、[TAC Service Request Tool] リンクをクリックして問題をレポートしてください。

ステップ 4 [ライセンス取得者の指定（Designate Licensee）] ページで、[ホスト ID（host ID）] テキスト ボックスに Mobility Services Engine の UDI を入力します。これは、ライセンスがインストールされる Mobility Services Engine です。

Mobility Services Engine の UDI 情報は、[サービス（Services）] > [Mobility Services Engine] > [デバイス名（Device Name）] > [システム（System）] の [一般プロパティ（General Properties）] 領域に表示されます。

ステップ 5 [同意（Agreement）] チェックボックスをオンにします。チェックボックスの下に登録者情報が表示されます。

必要に応じて情報を変更します。

登録者およびエンドユーザの電話番号に、文字が含まれていないことを確認します。たとえば408.555.1212や 408-555-1212 ではなく 408 555 1212 と入力します。

ステップ 6 登録者とエンド ユーザーが異なる場合は、登録者情報の下の [ライセンス（エンドユーザー）（License (End-User)）] チェックボックスをオンにしてエンド ユーザー情報を入力します。

ステップ 7 [続行（Continue）] をクリックします。

ステップ 8 [完了（Finish）] と [送信（Submit）] ページで登録者とエンド ユーザーのデータを確認します。必要な場合には [設定を編集（Edit Details）] をクリックして情報を修正してから、[送信（Submit）] をクリックします。詳細については、『AeroScout Support Page』および『Cisco Product License Registration Portal』を参照してください。

関連トピック

クライアント ライセンス ファイルおよび wIPS ライセンス ファイルのインストール （34 ページ）

Mobility Services Engine ライセンス ファイルの削除 （34 ページ）

クライアント ライセンス ファイルおよび wIPS ライセンス ファイルのインストール

Prime Infrastructure から CAS 要素ライセンスおよび wIPS ライセンスをインストールできます。

タグ ライセンスをインストールするには、AeroScout System Manager を使用します。AeroScout サポート ページを参照してください。

PAK の登録後にクライアント ライセンスまたは wIPS ライセンスを Prime Infrastructure に追加するには、次の手順に従います。

ステップ 1 [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。

ステップ 2 左側のサイドバーのメニューから [ファイル（Files）] > [MSE ファイル（MSE Files）] の順に選択します。

ステップ 3 [追加（Add）] をクリックして、[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を開きます。

ステップ 4 [MSE 名（MSE Name）] ドロップダウン リストから、ライセンス ファイルの追加先となる Mobility Services Engine を選択します。

（注） 選択されている Mobility Services Engine の UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5 [ライセンス ファイル（License File）] テキスト ボックスにライセンス ファイルを入力するか、該当するライセンス ファイルをブラウズして選択します。

ステップ 6 [ライセンス ファイル（License File）] テキスト ボックスに表示されたら、[アップロード（Upload）] をクリックします。新しく追加されたライセンスが Mobility Services Engine ライセンス ファイル リストに表示されます。

（注）
- クライアント ライセンスまたはタグ ライセンスをインストールすると、Context Aware Service（CAS）が再起動されます。ワイヤレス IPS ライセンスをインストールすると、ワイヤレス IPS サービスが再起動されます。
- 別のライセンスの追加または削除を試行するには、その前にサービスが開始されている必要があります。

関連トピック

Mobility Services Engine ライセンス ファイルの削除 （34 ページ）

Mobility Services Engine ライセンス ファイルの削除

ステップ 1 [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、左側のサイドバー メニューから [ファイル（Files）] > [MSE ファイル（MSE Files）] の順に選択します。

ステップ 2 削除するモビリティ サービス エンジン ライセンス ファイルのチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックし、[OK] をクリックして削除を確認します。

関連トピック

製品認証キーの登録 （32 ページ）
クライアント ライセンス ファイルおよび wIPS ライセンス ファイルのインストール （34 ページ）

保証ライセンス

「Prime Infrastructure ライセンスの購入」（「関連項目」を参照）で説明しているように、保証機能のライセンスは、ネットワーク内の NetFlow モニター対象のデバイス数と、Network Analysis Module（NAM）のデータ収集対応デバイス数に基づきます。保証ライセンスの管理、確認、トラブルシューティングは、「ライセンスの追加」、「ライセンスの削除」、および「ライセンスのトラブルシューティング」で説明している他の機能ライセンスと同じように行うことができます。

これらの機能に加えて、Prime Infrastructure では、保証機能を使用して管理する NetFlow および NAM デバイスを選択することもできます。たとえば、保証機能ライセンスの数が 50 しかなく、50 台を超える NetFlow および NAM デバイスがある場合、最も重要なデバイスを選択して管理することができます。後で保証ライセンスを追加で購入すると、管理対象外だったデバイスにもライセンスを追加で適用できます。

関連トピック

Prime Infrastructure ライセンスの購入 （23 ページ）
保証ライセンスの詳細の確認 （35 ページ）
ライセンスの追加 （23 ページ）
ライセンスの削除 （24 ページ）
ライセンスのトラブルシューティング （24 ページ）

保証ライセンスの詳細の確認

新しい保証ライセンスを購入する前に、既存の保証ライセンスに関する詳細とその使用法を確認することをお勧めします。保証ライセンス情報を確認するには、以下の表のリソースを使用してください。

表 *4*: 保証ライセンス情報の確認

確認内容	Choose
保証管理下にあるネットワーク内の NetFlow 対応デバイス（所有している保証ラインセンスの合計数のパーセンテージとして表示）	[Administration] > [Licenses and Software Updates] > [Licenses] > [Summary]

確認内容	Choose
所有している保証ライセンスの合計数および関連付けられているファイル	[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）]>[ファイル（Files）]
NetFlow または NAM ポーリング データを Prime Infrastructure に送信するデバイスのリスト	[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）]>[保証ライセンス（Assurance Licenses）]（リンクはページ右上）
使用中の保証ライセンスの数	
利用可能な保証ライセンスの最大数	

デフォルトでは、保証ライセンスを追加または削除するたびに、[保証ライセンス（Assurance License）]、[概要（Summary）]、および [ファイル（Files）]>[ライセンス ファイル（License Files）] の各ページに表示される保証ライセンスの合計数が更新されます。これらの追加または削除された保証ライセンスでカバーされるデバイスの追加または削除は、システム定義ジョブ（12 時間ごとに自動的に実行）の一部として実行されます。追加または削除されたデバイスが表示されるまでに、最大で 12 時間かかる場合があります。

[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）]>[保証ライセンス（Assurance Licenses）] ページは、[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）]>[概要（Summary）] ページおよび [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）]>[ファイル（Files）] ページの右上にある [保証ライセンス（Assurance Licenses）] リンクから常にアクセスできます。

関連トピック

クライアント ライセンス ファイルおよび wIPS ライセンス ファイルのインストール （34 ページ）
Mobility Services Engine ライセンス ファイルの削除 （34 ページ）

NetFlow および NAM デバイスに対するライセンス サポートの追加

以下の場合に、NetFlow または NAM デバイスに対するライセンス サポートを追加することをお勧めします。

- 新規または追加の保証ライセンスを購入した場合。
- 保証管理のライセンスが付与されていない NetFlow および NAM デバイスがある場合。

ステップ 1 [Administration]>[Licenses and Software Updates]>[Licenses]>[Assurance Licenses] を選択します（[Assurance Licenses] リンクはページ右上）。

ステップ 2 現在保証管理の対象となっているデバイスのリストの上にある [デバイスの追加（Add Device）] をクリックします。

ステップ 3 保証管理の対象にする各デバイスの隣にあるチェックボックスをオンにしてから、[ライセンスの追加（Add License）] をクリックします。Prime Infrastructure により、デバイスがただちに追加されます。

ステップ 4 完了したら、[キャンセル（Cancel）] をクリックします。

関連トピック

NetFlow および NAM デバイスに対するライセンス サポートの削除 （37 ページ）

NetFlow および NAM デバイスに対するライセンス サポートの削除

以下の場合には、NetFlow または NAM デバイスに対するライセンス サポートを削除することをお勧めします。

- 所有している保証ライセンス数に対して NetFlow および NAM デバイスの数が多すぎる場合。
- 1 つ以上の NetFlow および NAM デバイスで保証管理機能の使用を停止する場合。

ステップ 1 [管理（Administration）] > [ライ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）] > [保証ライセンス（Assurance Licenses）] を選択します（[保証ライセンス（Assurance Licenses）] リンクはページ右上）。

Prime Infrastructure により、現在保証管理の対象となっているデバイスのリストが表示されます。また、所有している保証ライセンスの合計数、保証管理対象となっているデバイスの合計数も表示されます。

ステップ 2 保証管理から削除する各デバイスの隣にあるチェックボックスをオンにしてから、[デバイスの削除（Remove Device）] をクリックします。

関連トピック

NetFlow および NAM デバイスに対するライセンス サポートの追加 （36 ページ）

スマートライセンス

スマート ライセンス機能では、ユーザー エクスペリエンスを簡素化するための標準化されたライセンス プラットフォームを使用できます。スマート ライセンスを最初に有効化した時点では、Prime Infrastructure を Smart Software Manager（シスコの中央集約型 Web サイトにあります）で登録するまで Prime Infrastructure は評価モードになります。

現在、従来のライセンスを使用している場合は、スマート ライセンスへの移行が推奨されます。2 種類のライセンスの違いについては、Cisco.com で紹介している Cisco Smart Licensing の概要を参照してください。

スマート ライセンス機能の目的は、ユーザーが次の作業をできるようにして、ライセンス関連の複雑な作業を軽減することです。

- 追加ライセンスを購入して、自動的に情報を更新する。
- 現在の購入と権限を監視する（ユニットの長さと数）。

- 現在の使用状況に関する情報やトレンド情報を監視する。
- 適切な数のライセンスが購入されているか簡単に追跡する。
- 企業間でライセンスを転送できるようにして、時間を節約する。

（注） Cisco Prime Infrastructure リリース 3.5 以降、オペレーション センターでスマート ライセンスがサポートされています。

スマート ライセンス機能の制限事項は次のとおりです。

- HA（ハイ アベイラビリティ）では、HA プライマリ サーバーでスマート ライセンス関連の処理（有効化、登録、無効化）を行うことはできますが、これらの処理を HA セカンダリ サーバーで行うことはできません。
- バックアップおよび復元操作を実行すると、バックアップ中にサポートされていたライセンスが復元されます。スマート ライセンス登録状態を別のサーバーで復元することはできません。この場合、復元後の設定時に再度登録する必要があります。
- 旧バージョンからのアップグレードを実行する場合、旧バージョンでサポートされていたライセンスは、デフォルトでは新しいバージョンでも有効になります。

関連トピック

Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定 （39 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
スマート ソフトウェア ライセンスの選択 （43 ページ）
Prime Infrastructure ライセンス ダッシュボードのライセンスしきい値の設定 （43 ページ）
追加アクションの実行 （45 ページ）
ライセンス ダッシュボードの表示 （44 ページ）
参考：製品の登録とライセンス認証ステータス （46 ページ）

Prime Infrastructure での Cisco Smart Licensing の設定

以下の手順に従って、Cisco Smart Licensing を設定します。現在、従来のライセンスを使用している場合は、同じ手順で Cisco Smart Licensing に移行してください。

	手順	参照先：
1.	Cisco Systems でスマート アカウントを作成します。	「Smart Account Request」に移動し、Web サイトの指示に従います。
2.	Prime Infrastructure と Cisco.com の Cisco Smart Software Manager（CSSM）の間の通信を設定します。	Prime Infrastructure と Cisco Smart Software Manager 間のトランスポート モードの設定

	手順	参照先：
3.	Prime Infrastructure でスマート ライセンスを有効にします（Web GUI を再起動する必要があります）。	Prime Infrastructure のスマート ライセンスの有効化
4.	Prime Infrastructure を Cisco.com の CSSM に登録し、ライセンス トークンを Prime Infrastructure の Web GUI に入力します（Web GUI を再起動する必要があります）。	Cisco Smart Software Manager への Prime Infrastructure の登録
5.	Prime Infrastructure で使用するライセンスを選択します。	スマート ソフトウェア ライセンスの選択
6.	ライセンスが不足している場合に通知するスマート ライセンス ダッシュボードを設定します。	Prime Infrastructure ライセンス ダッシュボードのライセンスのしきい値の設定

Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [アカウント クレデンシャル（Account Credentials）]** の順に選択して、[スマート ライセンス トランスポート（Smart Licensing Transport）] タブを選択します。

または、[スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページのリンクをクリックして [スマート ライセンス トランスポート（Smart Licensing Transport）] タブに移動し、トランスポート設定を指定します。

ステップ 2 次の 3 つのモードのいずれかを選択します。

- [ダイレクト モード（Direct mode）]：シスコ クラウドにデータを直接送信する場合は、このオプションを選択します。Smart Call Home サーバーの URL は読み取り専用であり、変更できません。
- [トランスポート ゲートウェイ（Transport Gateway）]：Cisco Call Home トランスポート ゲートウェイまたはシスコ スマート ソフトウェア ライセンシング サテライトを使用します（シスコ スマート ソフトウェア ライセンシング サテライトは、顧客の構内に設置され、CSSM 機能の一部を提供します。サテライトの詳細については、Cisco.com を参照してください）。それぞれのスマート ソフトウェア マネージャ サテライトまたは Smart Software Manager に適切な DNS マッピングされた URL を指定します。詳細については『Smart Software Manager User Guide』を参照してください。
- [HTTP プロキシ（HTTP Proxy）]：Prime Infrastructure とシスコ クラウドのの間の中間 HTTP/HTTPS プロキシを使用する場合は、このオプションを選択します。このオプションを有効にするには、まず [プロキシ（Proxy）] タブでプロキシ設定を指定する必要があります。

ステップ 3 [接続のテスト（Test Connectivity）] をクリックして、接続ステータスをテストします。[保存（Save）] をクリックして、スマート ライセンス トランスポート モードを更新します。

ステップ 4 Prime Infrastructure のスマート ライセンスの有効化に進みます。

関連トピック

スマートライセンス （37 ページ）
Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
追加アクションの実行 （45 ページ）
ライセンス ダッシュボードの表示 （44 ページ）
参考：製品の登録とライセンス認証ステータス （46 ページ）

Prime Infrastructure のスマート ライセンスの有効化

スマート ライセンスを有効にするには、次の手順に従ってください。

始める前に

トランスポート モードが設定されていることを確認してください。「関連項目」の「Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定」を参照してください。

ステップ 1 [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。

ステップ 2 [ライセンス設定（Licensing Settings）] タブで、[スマート ソフトウェア ライセンシング（Smart Software Licensing）] を選択します。

ステップ 3 [製品名（Product Name）] ドロップダウン リストから [Prime Infrastructure] を選択します。

ステップ 4 [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。Prime Infrastructure にダイアログボックスが表示され、設定手順に進む前に Prime Infrastructure からログアウトして再度ログインする必要があることが通知されます。

ステップ 5 ダイアログ ボックスで [OK] をクリックします。

スマート ライセンスが有効になっていて、登録が済んでいない場合、本製品は 90 日間**評価モード**になり、任意の数のデバイスを管理できるようになります。

ステップ 6 次のいずれかを実行します。

1. Cisco.com で CSSM にまだ登録していない場合は、Cisco Smart Software Manager で [Prime Infrastructure の登録（Registering Prime Infrastructure）] に進みます。
2. CSSM にすでに登録している場合は、「スマート ソフトウェア ライセンスの選択」に進みます。

（注） 従来のライセンスを使用する場合は、[ライセンス設定（Licensing Settings）] タブで [従来のライセンス（Traditional Licensing）] を [ライセンス モード（Licensing Mode）] として選択し、[登録（Register）] をクリックします。[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）] ページが表示されます。

関連トピック

Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定 （39 ページ）
追加アクションの実行 （45 ページ）
ライセンス ダッシュボードの表示 （44 ページ）
スマート ライセンスの無効化 （45 ページ）
参考：製品の登録とライセンス認証ステータス （46 ページ）

Cisco Smart Software Manager への Prime Infrastructure の登録

この手順では、製品インスタンスをCSSMに登録するために使用するトークンを作成します。CSSM の使用方法の詳細については、『Cisco Smart Software Manager User Guide』を参照してください。

（注） CSSM で実行できるその他の操作については、『Cisco Smart Software Manager User Guide』を参照してください。たとえば、ライセンス登録やライセンス認証の更新、Cisco Smart Licensing での製品の登録解除などがあげられます。

関連トピック

トークン ID の生成 （41 ページ）
製品インスタンスの登録 （42 ページ）

トークン ID の生成

新規にインストールする（従来のライセンスから移行しない）場合は、以下の手順に従います。

始める前に

組織にスマート アカウントがない場合は、software.cisco.com で [スマート アカウントの申請（Request a Smart Account）] を選択し、指示に従ってアカウントを作成します。従来のライセンスから移行する場合は、「従来のライセンスから移行」を参照してください。

ステップ 1 Cisco Software Central の Web サイト（software.cisco.com）に移動します。

ステップ 2 Cisco Software Central で、[ライセンス（License）] > [スマート ソフトェア ライセンシング（Smart Software Licensing）] を選択します。

ステップ 3 適切な仮想アカウントを選択します（仮想アカウントはスマート アカウントの作成時に自動的に作成されます）。

ステップ 4 [全般（General）] タブをクリックし、[新規トークン（New Token）] をクリックします。

ステップ 5 指示に従って名前、期間、輸出コンプライアンスの適用性を入力してから、諸条件や責任について同意してください。

ステップ 6 [トークンの作成（Create Token）] をクリックします。

ステップ 7 トークン ID をクリップボードにコピーし、「製品インスタンスの登録」に進みます。

従来のライセンスからの移行

従来のライセンスから移行する場合は、以下の手順に従います。

ステップ 1 Cisco Software Central の Web サイト（software.cisco.com）に移動します。

ステップ 2 Cisco Software Central で、[ライセンス（License）] > [従来のライセンス（Traditional Licensing）] を選択します。

ステップ 3 [製品ライセンスの登録を続行（Continue to Product License Registration）] をクリックします。

ステップ 4 [製品ライセンス登録（Product License Registration）] ページの [管理（Manage）] 領域で [PAK/トークン（PAKs/Tokens）] タブをクリックして、移行する権限を選択します。

ステップ 5 [アクション（Actions）] ドロップダウン メニューで、[スマート権限に変換する（Convert to Smart Entitlements）] をクリックします。

ステップ 6 トークン ID をクリップボードにコピーし、「製品インスタンスの登録」に進みます。

製品インスタンスの登録

トークン ID を Prime Infrastructure の Web GUI に入力し、製品を登録します。

ステップ 1 **[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。

ステップ 2 [ライセンス設定（Licensing Settings）] タブの [登録トークン（Registration Token）] フィールドにトークンを貼り付けます。

ステップ 3 [登録（Register）] をクリックします。

ステップ 4 Prime Infrastructure からログアウトして、再度ログインします。

ステップ 5 続けて、スマート ソフトウェア ライセンスの選択を行います。

関連トピック

Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
スマート ソフトウェア ライセンスの選択 （43 ページ）
スマートライセンス （37 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定（39 ページ）
追加アクションの実行 （45 ページ）
ライセンス ダッシュボードの表示 （44 ページ）
参考：製品の登録とライセンス認証ステータス （46 ページ）

スマート ソフトウェア ライセンスの選択

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 [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。

ステップ 5 [Prime Infrastructure ライセンスのライセンスしきい値の設定（Configuring License Thresholds for the Prime Infrastructure License）] ダッシュボードに進みます。

Prime Infrastructure ライセンス ダッシュボードのライセンスしきい値の設定

ライセンスをより効率的に管理するため、ライセンスの残り数が少なくなったら通知するようライセンス ダッシュボードを設定します。ここでの設定はシステム全体に適用されます。

ステップ 1 [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、[ライセンス ダッシュボードの設定（License Dashboard Settings）] タブをクリックします。

ステップ 2 [ライセンス タイプ（License Type）] ドロップダウン リストからライセンスを選択します。

ステップ 3 [しきい値（Threshold Value）] フィールドに、値を入力します。

ステップ 4 [保存（Save）] をクリックします。

しきい値は [ライセンスの要約（License Summary）] と [ライセンスのデバイス ディストリビューション（Device Distribution for License）] のグラフ表示の直線として表されます。

関連トピック

ライセンス ダッシュボードの表示 （44 ページ）
スマート ソフトウェア ライセンスの選択 （43 ページ）
Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
スマート ライセンスの無効化 （45 ページ）
参考：製品の登録とライセンス認証ステータス （46 ページ）

ライセンス ダッシュボードの表示

このダッシュボードを開くには、次のいずれかを実行します。

- **[管理（Administration）]>[ダッシュボード（Dashboards）]>[ライセンス ダッシュボード（Licensing Dashboard）]** を選択します。
- [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページの右上にある [ライセンス ダッシュボード（Licensing Dashboard）] リンクをクリックします。

ダッシュボードに表示される情報は、有効になっているライセンス モードによって異なります。スマート ソフトウェア ライセンシングが現在有効になっている場合は、次のダッシュレットが表示されます。

- [ライセンスの要約（License Summary）] ダッシュレット：特定の期間に各ライセンス タイプで使用されるライセンスの棒グラフが表示されます。追加情報を表示するには、グラフの上にカーソルを置きます。
- [ライセンスのデバイス ディストリビューション（Device Distribution for License）] ダッシュレット：特定のライセンスのデバイス ディストリビューション グラフを表示するには、[ライセンスの要約（License Summary）] ダッシュレットに表示されたグラフの上部にあるリンクをクリックします。追加情報を表示するには、グラフの上にカーソルを置きます。

（注） [ライセンス ダッシュボード（License Dashboard）] に表示される情報は、SmartLicense ジョブが午前2時（事前設定されている実行時間）に実行された後、毎日更新されます。[ジョブ ダッシュボード（Job Dashboard）] にこのジョブを表示するには、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

スマート ライセンスの無効化

ステップ 1 スマート ライセンスを無効にします。

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

b) ウィンドウの下部で [スマート ライセンスの無効化（Disable Smart Licensing）] をクリックして、選択内容を確定します。

ステップ 2 従来のライセンスを有効にします。（この処理は [スマート ライセンスの設定（Smart License Settings）] ページで行います）

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）] > [ライセンス（Licenses）] の順に選択します。

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。

d) [ライセンス モード（Licensing Mode）] で [従来のライセンス（Traditional Licensing）] を選択します。

e) [登録（Register）] をクリックします。

関連トピック

Prime Infrastructure ライセンス ダッシュボードのライセンスしきい値の設定 （43 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
追加アクションの実行 （45 ページ）

追加アクションの実行

[アクション（Actions）] ドロップダウン リストから、次のいずれかのアクションを選択します。ライセンスと製品登録のステータスの詳細については、「参考：製品の登録とライセンス認証ステータス」を参照してください。

- [認証を今すぐ更新（Renew Authorization Now）]：[認証を今すぐ更新（Renew Authorization Now）] をクリックすると、CSSM での認証が更新され、Prime Infrastructure のコンプライアンスが維持されます。デフォルトでは、認証期間は 30 日ごとに更新されます。

- [登録を今すぐ更新（Renew Registration Now）]：[登録を今すぐ更新（Renew Registration Now）]をクリックすると、ID証明書が更新されます。このID証明書は、Prime Infrastructureの登録を継続するため毎年更新する必要があります。
- [登録解除（Deregister）]：Prime Infrastructureがスマート ソフトウェア ライセンシングから登録解除され、評価モードに戻ります。
- [スマート ソフトウェア ライセンシングの無効化（Disable Smart Software Licensing）]：Prime Infrastructureがスマート ライセンスから登録解除され、ライセンスがなくなります。無効になると、ログインしても[管理（Administration）]メニューしか使用できなくなります。「スマート ライセンスの無効化」を参照してください。

関連トピック

参考：製品の登録とライセンス認証ステータス （46 ページ）
Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
ライセンス ダッシュボードの表示 （44 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定 （39 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
スマート ライセンスの無効化 （45 ページ）

参考：製品の登録とライセンス認証ステータス

製品登録ステータス

製品登録ステータスは、製品がCisco.comのシスコ スマート ソフトウェア ライセンシングに正常に登録されているかどうかを表します。

製品登録ステータス	説明
未登録	スマート ソフトウェア ライセンスはPrime Infrastructureで有効になっていますが、Prime InfrastructureはCSSMに登録されていません。
登録済み	Prime InfrastructureはCSSMに登録されています。Prime InfrastructureはID証明書を受信しています。このID証明書は、将来シスコのライセンス担当者との通信に使用されます。
この登録通知の有効期限が切れました	Prime Infrastructureは有効期限までに正常に登録を更新できず、CSSMから削除されています。

ライセンス認証ステータス

ライセンス認証ステータスは、購入したライセンスに対する使用状況、およびCisco Smart Licensingに準拠しているかどうかを表しています。購入したライセンス数を超えると、コンプライアンス違反となります。

ライセンス認証ステータス	説明
評価モード	Prime Infrastructure は評価期間（90 日間）が終了するまで評価モードで稼働します。
承認済み（Authorized）	Prime Infrastructure に有効なスマート アカウントがあり、登録されています。製品が要求するすべてのライセンスの使用が承認されています。
コンプライアンス違反	Prime Infrastructure が購入したライセンス数を超えています。製品インスタンスがある仮想アカウントで、使用されているライセンス タイプのうち 1 つ以上が不足しています。
評価期限切れ	評価期間が終了し、Prime Infrastructure はライセンスなしの状態になります。
認証が期限切れ	Prime Infrastructure は、認証の有効期限前に、ライセンス認証を正常に更新できませんでした。

関連トピック

スマートライセンス （37 ページ）
Prime Infrastructure のスマート ライセンスの有効化 （40 ページ）
Prime Infrastructure での Cisco Smart Licensing の設定 （38 ページ）
Cisco Smart Software Manager への Prime Infrastructure の登録 （41 ページ）
追加アクションの実行 （45 ページ）

ソフトウェア アップデートの管理

ソフトウェア アップデートとは

シスコでは、ソフトウェアに対するアップデートを定期的に提供しています。これらのアップデートは、次のカテゴリに分類されます。

- 重要修正：ソフトウェアの重要な修正を提供します。これらのアップデートが利用可能になったら、ただちにこれらのすべてをダウンロードして適用することが強く推奨されます。
- デバイス サポート：がリリース時点でサポートしていなかったデバイスを管理するサポートを追加します。

- アドオン：現在使用中の バージョンを補完するための新しい機能を提供します（新しい GUI 画面や機能が含まれることもあります）。これには、 のメンテナンス パックとメンテナンス パック ポイント パッチが含まれます。

に表示されるアップデート通知は、管理者によって指定された通知設定によって異なります。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 （49 ページ）を参照してください。すべてのソフトウェア アップデートが .ubf ファイルにパッケージ化されます。大容量のアップデートには、インストールするものを選択可能な個別の小容量のアップデートが含まれている場合があります。アップデートをインストールすると、 が次の処理を実行します。

- ファイルの発行者が Cisco Systems であり、ファイルが改ざんされていないことを確認する
- 必要な他のアップデートを自動的にインストールする

http://www.cisco.com に接続できる場合は、Cisco.com から直接アップデートをダウンロードしてインストールできます。インターネット接続がない場合は、必要な接続を備えたサーバーからアップデートをコピーして、そこからインストールします。

インストール済み製品ソフトウェアのバージョンの表示

次のいずれかの方法で 製品バージョンを確認します。

CLI を使用するには、サーバーとの SSH セッションの確立 （109 ページ）を参照してください。

インストール済みのソフトウェア アップデートの表示

Web GUI にログインしていない場合は、ログイン ページから [インストール済みアップデートの表示（View Installed Updates）] をクリックすると、ソフトウェア アップデートを一覧表示するポップアップ ウィンドウを表示できます。

Web GUI にログインしている場合は、次の 2 つの方法でソフトウェア アップデートを表示できます。

- [ページで、ページの右上にある設定アイコンをクリックし、をクリックしてから、[インストール済みアップデートの表示（View Installed Updates）] をクリックします。（[インストール済みアップデートの表示（View Installed Updates）] リンクは、ログイン ページにもあります）。
- **[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択します（この方法を使用すると、最も詳細な情報が表示されます）。

[ソフトウェアアップデート（Software Update）] ページに 2 つのタブが表示されます。

- インストール済みの更新プログラム（Installed Updates）： で現在使用されているアップデート。

- アップロード済みアップデートファイル（Uploaded Update Files）：サーバーにアップロードされているアップデートファイル（使用されていないファイルを含む）。[対応するアップデート（Corresponding Updates）] フィールドには、アップロード済みの前提条件のアップデートも一覧表示されます。

  アップデートファイルがまだインストールされていない場合は、削除できます。ファイルを選択し、[削除（Delete）] ボタンをクリックします。

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

デフォルトでは、 は [ソフトウェアアップデート（Software Updates）] ページに有効なすべてのアップデートに関する情報を表示します。このリストはかなり長くなる場合があるため、表示する内容と通知対象とするアップデートを調整することをお勧めします。また、すべての通知を無効にして、後で再び有効にすることもできます。

ステップ 1 が有効なアップレードに関する情報を取得できるよう、デフォルトの Cisco.com クレデンシャルを設定します。

a) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

b) [Cisco.com クレデンシャル（Cisco.com Credentials）] タブをクリックし、クレデンシャルを入力してから [保存（Save）] をクリックします。

ステップ 2 ソフトウェア アップデートの通知を設定します。

a) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（Genera）] > [ソフトウェア アップデート（Software Update）]** を選択します。

b) [通知設定（Notification Settings）] で、アップデートのカテゴリをオンまたはオフにします。すべての通知を無効にするには、カテゴリが 1 つもオンになっていない状態にします。カテゴリの説明については、次を参照してください。 ソフトウェア アップデートとは （47 ページ）

c) [Save] をクリックします。

イメージ（ISO と OVA）をインストールする前に検証する

ソフトウェアをインストールする前に、イメージが署名されていることを確認することにより、発行者の信頼性を検証する必要があります。これにより、イメージが Cisco Systems 製であり、改ざんされていないことが保証されます。

ソフトウェアは、次の形式で提供されます。

- ソフトウェア アップデート Web GUI 機能を使用してダウンロードしてインストール可能な .ubf ファイル
- 主要な製品リリースと更新プログラムで提供される ISO または OVA イメージ

ソフトウェア アップデート機能を使用してダウンロードした UBF パッケージは手動で検証する必要がありません。これは、 がソフトウェア アップデート インストール プロセス中に自動的に .ubf ファイルを検証するためです。ファイルが署名されていない場合は、 がエラー メッセージを生成し、.ubf ファイルをインストールしません。この問題が発生した場合は、シスコの担当者にお問い合わせください。

ISO イメージと OVA イメージは手動で検証する必要があります。インストールする前に、次の手順を使用して検証します。

ステップ 1 **openssl** がインストールされていない場合は、それをダウンロードしてインストールします（http://www.openssl.org を参照）。

ステップ 2 一時ディレクトリに次のファイルを配置します。

- 検証する製品ファイル（***.iso** または ***.ova**）。
- 製品ファイルに同梱されている署名ファイル（***.signature**）。
- 証明書ファイル（***.pem**）OVA イメージと ISO イメージの検証には同じ証明書が使用されます。

ステップ 3 一時ディレクトリに移動し、Linux CLI ルート ユーザーとして次のコマンドを実行します（Linux CLI ルート ユーザーとしてのログインおよびログアウト （202 ページ）を参照）。

```
openssl dgst -sha512 -verify cert-file -signature sig-file content-file
```

ここで、

- *cert-file* は 証明書ファイル
- *sig-file* は 署名ファイル
- *content-file* は検証する ISO ファイルまたは OVA イメージ

ステップ 4 結果が [検証 OK（Verified OK）] の場合：

- ISO ファイルの場合は、インストールに進みます（この検証手順内の手順をこれ以上実行する必要はありません）。
- OVA パッケージの場合は、次のステップに進みます。

ステップ 5 （OVA パッケージのみ）Cisco Systems が発行者であることを確認します。

a) VMware vSphere クライアントで、**[ファイル（File）] > [OVF テンプレートの展開（Deploy OVF Template）]** を選択します。
b) OVA ファイル（*.ova）を参照して、それを選択し、[次へ（Next）] をクリックします。
c) [OVFテンプレートの詳細（OVF Template Details）] ウィンドウの [パブリッシャ（Publisher）] フィールドに、緑色のチェック マーク付きで [Cisco Systems, Inc.] が表示されていることを確認します。次のステップに進みます。

（注） [ベンダー（Vendor）] フィールドを使用してイメージを検証しないでください。このフィールドは Cisco Systems を発行者として認証しません。

（注） [パブリッシャ（Publisher）] フィールドに「**No certificate present**」と表示されている場合は、先に進まないでください。これは、イメージが署名されておらず、Cisco Systems 製ではない、または、改ざんされていることを示しています。

ステップ 6 証明書チェーンをチェックします。

a) [OVFテンプレートの詳細（OVF Template Details）] ウィンドウの [パブリッシャ（Publisher）] フィールドで、[Cisco Systems, Inc.] ハイパーリンクをクリックします。
b) [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブをクリックします。
c) [認証パス（Certification Path）] タブ（証明書チェーンが一覧表示されている）で、[認証パス（Certification Path）] 領域に [Cisco Systems, Inc.] が、[認証ステータス（Certification Status）] 領域に [この証明書は正常です（The certificate is OK）] が表示されていることを確認します。

Cisco.com からのソフトウェア アップデートのダウンロードとインストール

次の手順で、cisco.com からソフトウェア アップデートをダウンロードして サーバーにインストールする方法を示します。

高可用性を使用している場合は、を参照してください。

始める前に

Cisco.com にアカウントがあることを確認します。

ステップ 1 データをバックアップする。手動バックアップの実行 （68 ページ）を参照してください。

ステップ 2 ファイルをローカル マシンにダウンロードし、ローカル マシンから サーバーにそれをアップロードします。

a) cisco.com にログインし、 ソフトウェア ダウンロード サイトに移動します。
b) ダウンロードする .ubf ファイルを見つけて、ローカル マシンにダウンロードします。

ステップ 3 クライアント マシンから サーバーへのファイルのコピー （52 ページ）の説明に従って、ローカル マシンから サーバーにファイルをコピーします。

ステップ 4 管理者権限を持つユーザーとして Web GUI にログインします。

ステップ 5 サーバーにファイルをアップロードします。

a) **[管理（Administration）] > [ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）]** を選択します。
b) ページの上部にある [アップロード（Upload）] をクリックします。
c) [参照（Browse）] をクリックし、ファイルまで移動して [OK] をクリックします。アップロードが成功すると、[ファイル（Files）] タブの下にソフトウェアが表示されます。

ステップ 6 ソフトウェア アップデートを選択して [インストール（Install）] をクリックし、確認ポップアップ ウィンドウで [はい（Yes）] をクリックします。

（注） .ubfファイルが未署名の場合、またはCisco.comからダウンロードした後に変更された場合は、がインストールを中止します。Cisco の担当者にお問い合わせください。

が自動的に再起動し、Web GUI にしばらくアクセスできなくなります。（自動的に再起動しない場合は、の停止と再起動 （114 ページ）の手順に従って再起動してください。）

ステップ 7 Web GUI にアクセス可能になったら、ログインして [ソフトウェアアップデート（Software Update）] ページでバージョンを確認します。

a) **[管理（Administration）] > [ライセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）]** を選択します。

b) [更新（Updates）] タブで情報を確認します。

次のタスク

Web GUI を開く前にブラウザのキャッシュをクリアするよう、すべてのユーザーに指示してください。

クライアント マシンから サーバーへのファイルのコピー

次の SCP コマンドを使用してクライアント マシンからファイルを取得し、 サーバーのデフォルト ローカル リポジトリ（/localdisk/defaultRepo）にコピーします。このコマンドは、Linux CLI ルート ユーザーとして実行する必要があります（Linux CLI ルート ユーザーとしてのログインおよびログアウト （202 ページ） を参照）。

scp *clientUsername*@*clientIP*:/*fullpath-to-file* **/localdisk/defaultRepo**

ここで、

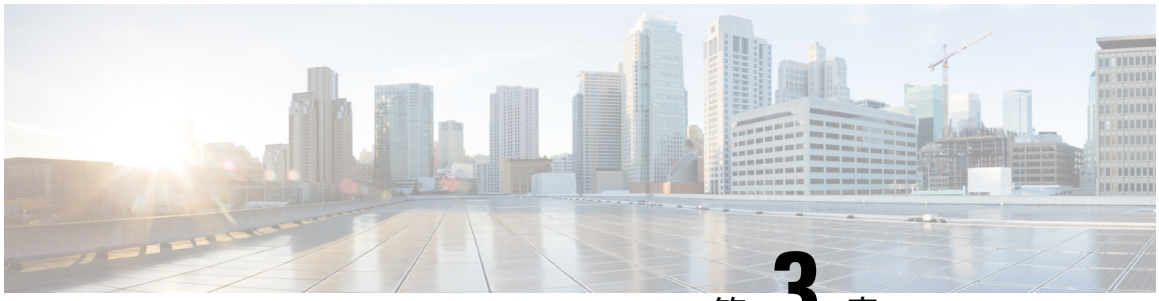
- *clientUsername* は、クライアント マシンのユーザー名です
- *clientIP* は、ファイルが存在しているクライアント マシンの IP アドレスです
- *fullpath-to-file* は、クライアント マシン上のファイルのフル パス名です

次に例を示します。

```
scp jsmith@123.456.789.101:/temp/myfile.tar.gz /localdisk/defaultRepo
```

始める前に

クライアント マシンで SCP が有効になっていること、および必要なポートが開いていることを確認します（『』を参照）。



第 3 章

バックアップと復元

バックアップと復元の概念

バックアップ タイプ：アプリケーションとアプライアンス

は次の 2 種類のバックアップをサポートしています。

- アプリケーション バックアップ：これには、 アプリケーション データが含まれますが、プラットフォーム データ（サーバーのホスト名や IP アドレスなどのホスト固有の設定）は含まれません。アプリケーション データのみを移動し、プラットフォーム/ホスト固有の設定は移動しない場合は、 のアップグレード時にアプリケーション バックアップを使用する必要があります。

- アプライアンスバックアップ：すべてのアプリケーションデータとプラットフォームデータ（ホスト名、IP アドレス、サブネット マスク、デフォルト ゲートウェイなどのホスト固有の設定）が含まれます。障害回復（またはプラットフォームのハードウェアまたはソフトウェア障害からの回復）の場合はアプライアンス バックアップを使用する必要があります。たとえば、ディスクまたはファイルシステムの障害から回復するには、標準の回復プロセスでは を再インストールしてからアプライアンスのバックアップを復元し、すべてのデータとプラットフォーム固有の設定を復元します。その後、アプライアンスのバックアップに含まれていない HA の設定を手動で再構築する必要があります。

（注） 何をアプリケーション データと見なすか、何をプラットフォーム データと見なすかの詳細については、バックアップされる情報を参照してください。

アプリケーションとアプライアンス バックアップについては、次の点に注意してください。

- ハードウェアとソフトウェアの構成が元のホストでの構成と同じであれば、アプリケーションおよびアプライアンスバックアップは、バックアップを作成した同じホストまたは新しいホストのどちらに復元することもできます。
- アプライアンスのバックアップは、バックアップを作成した元のサーバーと同じバージョンの サーバー ソフトウェアを実行しているホストにのみ復元できます。
- それ以降のバージョンの にアップグレードする場合、アプリケーションのバックアップと復元は、アップグレードパスがサポートされている限り異なるリリース間で実行できます。
- アプライアンスの復元コマンドを使用してアプリケーションのバックアップを復元することはできません。アプリケーションの復元コマンドを使用してアプライアンスのバックアップを復元することもできません。

次のベスト プラクティスを推奨します。

- を評価中の場合、ローカル リポジトリへのデフォルトの自動アプリケーション バックアップを使用します。
- 仮想アプライアンスとして実稼働環境で を実行中の場合は、アプリケーション バックアップを定期的に実行してリモート バックアップ サーバーに保管します。アプリケーション バックアップは、サーバー ハードウェアの完全な故障を除くすべての障害に対してサーバーを復元するために使用できます。

バックアップのスケジューリング

は自動で定期的にアプリケーション バックアップを実行します。この機能はデフォルトで有効になっていて毎日 1 つのアプリケーション バックアップ ファイルをデフォルトのローカル バックアップ リポジトリに作成します。

必要に応じてこのスケジュールを変更できます。また、随時、Web GUI から自動アプリケーション バックアップを実行できます。アプライアンス バックアップは、コマンド ラインからしか実行できません。

自動アプリケーション バックアップは、バックアップ リポジトリが サーバーに対してローカルな場合に保存スペースの問題を引き起こす可能性があります。このことはテスト実装ではあまり問題になりませんが、実稼働環境のリモート サーバーに対する定期バックアップの代用として使用することはできません。

実稼働環境では、次のことをお勧めします。

- バックアップ ファイルを保管するようにリモート リポジトリをセットアップする。
- 自動定期アプリケーション バックアップを使用して、定期的にリモート リポジトリ上でバックアップを作成する。

スケジュールされたバックアップを使用している場合でも、コマンドラインを使用してアプリケーションまたはアプライアンスのバックアップをいつでも作成できます。

（注） デフォルトでは、ジョブ作成のジョブ実行時間に 2 分が追加されます。

バックアップ リポジトリ

自動アプリケーション バックアップ機能は、デフォルトで、ローカル バックアップ リポジトリの **/localdisk/defaultRepo** にバックアップ ファイルを保存します。Web GUI を使用して新しいローカル バックアップ リポジトリを作成しておき、自動アプリケーション バックアップを設定するときにそれを選択できます。リモート リポジトリも指定できますが、まず、リポジトリのセットアップと管理 （59 ページ）の説明に従ってリポジトリを作成しておく必要があります。

コマンド ラインを使用してアプリケーションまたはアプライアンス バックアップを作成する場合、バックアップを保存するローカルまたはリモート リポジトリを指定する必要があります。実稼働環境では、通常、NFS、SFTP、または FTP でアクセスするリモート リポジトリです。NFS は通常は他のプロトコルより高速で信頼性が高いので、NFS を使用することを推奨します。

アプリケーション バックアップは、コマンド ラインと Web GUI のどちらから実行しても違いはありません。どちらの操作によっても、同じバックアップ ファイルが作成されます。

NFS を使用してバックアップの作成やリモート バックアップからのデータの復元を行う場合は、バックアップや復元の操作中、マウントされた NFS サーバーが、常にアクティブになるようにしてください。プロセスのいずれかの時点でNFS サーバーがシャットダウンした場合、バックアップや復元の操作は、警告やエラー メッセージなしで異常終了します。

バックアップ ファイル名

Web GUI から開始されるアプリケーション バックアップ：自動または手動のいずれかで次の形式のファイル名が割り当てられます。

*host-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

CLI から開始されるアプリケーション バックアップでは、同じ形式が使用されますが、ファイルがサーバー名ではなくユーザーの指定したファイル名から始まる点が異なります。

filename-*yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

CLI から開始されるアプライアンス バックアップのファイルもユーザーの指定したファイル名から始まりますが、形式は APP ではなく SYS です。

filename-*yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_**SYS**_CK*checksum*.tar.gpg

次の表に、バックアップ ファイルで使用される変数の説明を示します。

変数	説明
host	バックアップが作成されたサーバーのホスト名（Web GUI から開始されるアプリケーション バックアップの場合）
filename	コマンドラインでユーザーが指定したファイル名（CLI から開始されるアプリケーション バックアップおよびアプライアンス バックアップの場合）
yymmdd-hhmm	バックアップが作成された日時
ver	内部バージョン
size	バックアップの合計サイズ
cpus	バックアップが作成されたサーバーの CPU の総数
target	バックアップが作成されたサーバーのシステム メモリの合計量
ram	バックアップが作成されたサーバーの RAM の合計量
swap	バックアップが作成されたサーバーのスワップ ディスクの合計サイズ
checksum	バックアップ ファイルのチェックサム

バックアップ検証プロセス

は次の処理を行って、バックアップ ファイルを検証します。

1. バックアップ プロセスを開始する前に、ディスク サイズ、高速リカバリ領域、制御ファイルを検証します。
2. 復元可能であることを確認するために、作成されたバックアップ データベースを検証します。

3. バックアップされたファイルに対して、圧縮されたアプリケーション データを検証します。
4. TAR ファイルを検証して、ファイルが正しく完全であることを確認します。
5. GPG ファイルを検証して、ファイルが正しいことを確認します。

バックアップ ファイルを手動で転送する場合やバックアップ ファイルの転送が完了したことを検証する場合は、ファイルの md5CheckSum とファイル サイズを参照してください。

バックアップを検査するもう1つのベストプラクティスは、それを のスタンドアロンの「test」インストール環境に復元することです。

バックアップされる情報

次の表に、バックアップ ファイルに含まれる情報に関する説明を示します。この情報は、バックアップからサーバーに復元されます。

バックアップ メカニズムによって保存されないデータに関する詳細については、バックアップされない情報 （59 ページ）を参照してください。

（注） /opt/CSCOlumos/conf/Migration.xml ファイルには、バックアップされたすべてのコンフィギュレーション ファイルとレポートが含まれています。このファイルがバックアップに含まれており、復元されます。

データ タイプ	機能	保存および復元される情報

アプリケーションデータ	バックグラウンドジョブの設定	データベース内のデータ
	設定アーカイブ（デバイスコンフィギュレーション ファイル）	データベース内のデータ
	構成テンプレート	• /opt/CSCOlumos 内のファイル： • /conf/ootb • /xmp_inventory/dar/customized-feature-parts/CONFIGURATION • データベース内のデータ
	資格情報	データベース内のデータ
	デバイスインベントリ データ	データベース内のデータ
	ライセンス	/opt/CSCOlumos/licenses 内のファイル
	マップ（Maps）	• /opt/CSCOlumos/domainmaps 内のファイル • データベース内のデータ
	レポート	• /localdisk/ftp 内のファイル： • /reports • /reportsOnDemand • データベース内のデータ
	管理対象デバイスのソフトウェアイメージ ファイル	データベース内のデータ
	システム設定	データベース内のデータ
	ユーザー設定	• /opt/CSCOlumos/conf/wap/datastore/webacs/xml/prefs 内のファイル • データベース内のデータ
	ユーザー、グループ、およびロール	データベース内のデータ
	仮想ドメイン	データベース内のデータ

プラットフォーム データ	CLI 設定	すべての CLI 情報と設定が保持されます。これには、バックアップ リポジトリのリスト、FTP ユーザー名、CLI を使用して作成したユーザー、CLI 経由で指定した AAA 情報、その他の CLI 設定（端末タイムアウトなど）が含まれます。
	資格情報	Linux OS クレデンシャル ファイル
	ネットワーク設定（Network settings）	/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml 内のファイル
	Linux ユーザー プリファレンス	Linux データ構造
	Linux ユーザー、グループ、およびロール	Linux データ構造

バックアップされない情報

バックアップを実行する前に、次の情報を手動でメモする必要があります。これは、これらの情報がバックアップ プロセスの一部として保存されないためです。データの復元後にこれらの設定を再構成する必要があります。

- ハイ アベイラビリティ設定
- ローカル カスタマイズ（レポート ヒープ サイズなど）
- パッチ履歴情報
- 証明書

  Web証明書を使用してサーバーを構成し、クライアント証明書を使用してクライアントを認証するようにサーバーを設定した場合は、バックアップと復元の手順を完了した後、新しいサーバーで同じ構成を再度繰り返す必要があります。

バックアップされる情報のリストについては、バックアップされる情報 （57 ページ）を参照してください。

リポジトリのセットアップと管理

は次のリポジトリ タイプをサポートしています。

-
- リモートリポジトリ：NFS、FTP、SFTP および TFTP

これら異なるタイプのリポジトリをセットアップおよび管理する方法については、以降のトピックを参照してください。

ローカル バックアップ リポジトリの作成

は、デフォルトのローカル バックアップ リポジトリ **/localdisk/defaultRepo** にバックアップ ファイルを自動的に保存します。必要に応じて、別のローカル バックアップ リポジトリを作成して、それを使用することができます。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（nfrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] 一覧で、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックして、[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスを開きます。

ステップ 5 [ジョブ プロパティの編集（Edit Job properties）] ダイアログボックスを使用して、新しいローカル リポジトリを作成します。

1. [作成（Create）] をクリックします。[バックアップ リポジトリの作成（Create Backup Repository）] ダイアログボックスが開きます。
2. 作成するローカル リポジトリの名前を入力します。
3. バックアップをパスワードで保護する場合は、パスワードを入力します。

   （注） バックアップを復元するには、パスワードを覚えておく必要があることに注意してください。

4. FTP リポジトリの場合は、[FTP] チェックボックスをオンにし、場所とクレデンシャルを入力します。
5. [送信（Submit）] をクリックします。新しいリポジトリが、[ジョブ プロパティの編集（Edit Job properties）] ダイアログボックスの [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストに追加されます。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 今後の自動アプリケーション バックアップにリポジトリを使用する場合は、自動バックアップ用のバックアップ リポジトリの指定 （67 ページ）の説明に従ってそれを指定します。

リモート バックアップ リポジトリの使用

実稼働環境では、ネットワーク管理データがハードウェアやサイトの障害から保護されるように、バックアップにリモート リポジトリを使用することをお勧めします。ほとんどの場合、これは次のことを行う必要があることを意味します。

1. バックアップ ファイルを保持するための 1 つ以上のリモート リポジトリを作成します。組織でまだリモート バックアップ サーバーを使用していない場合は、独自にセットアップする必要があります。

2. 自動アプリケーション バックアップの保存先としてリモート リポジトリを指定します。
3. 必要な場合、自動アプリケーションバックアップの間隔とその実行時刻を指定します。リモート リポジトリに保存された自動アプリケーション バックアップをモニターして、手動でアーカイブする必要があります（[保持する最大バックアップ数（Max backups to keep）] の設定はリモート リポジトリには適用されないため）。
4. CLI バックアップ コマンドを使用してアプリケーションまたはアプライアンス バックアップを実行する場合は、バックアップ先としてリモート リポジトリを指定します。

リモート アクセスを計画しているリソースと同様に、セットアップ時に正しいサーバー IP アドレスとログイン クレデンシャルを指定することが、リモート バックアップ リポジトリと の使用を成功させる秘訣です。

リモート NFS バックアップ リポジトリの使用

これらのトピックでは、リモート NFS バックアップ リポジトリを使用する方法について説明します。

NFS バックアップ設定をセットアップする前に

- バックアップをステージングして保存する NFS サーバーの IP アドレスを知っていること。ステージング フォルダと保存フォルダは、同じ NFS サーバーに配置することも、別々の NFS サーバーに配置することもできます。ステージングと保存を別々の NFS サーバー上で計画している場合は、両方のサーバーの IP アドレスが必要です。
- NFS サーバー上のステージング フォルダと保存フォルダのパス名を知っていること。同じ NFS サーバ上でステージングおよび保存することを選択した場合は、ステージング フォルダと保存フォルダを違う名前にする必要があります。

リモート NFS サーバー上でバックアップリポジトリを作成し、それらのリポジトリを使用するように Cisco Prime Infrastructure サーバーを設定できます。バックアップをホストする NFS サーバーは、次の要件を満たしていれば、ネットワーク上のどこにでもセットアップできます。

UI の [Backup Repository] ドロップダウンリストに NFS サーバーの詳細を表示するには、CLI を使用して NFS サーバーを設定する必要があります。NFS サーバーは、CLI を使用してのみ設定できます。

手順の概要

1. Cisco Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法（147 ページ） を参照）。
2. コンフィギュレーション モードを開始します。
3. リモート NFS サーバーへのシンボリックリンクを設定します。
4. シンボリック リンクの作成を確認します。
5. コマンド ラインからバックアップを実行する場合は、新しいリポジトリを backup コマンド内にリポジトリ名として指定します。次に例を示します。

手順の詳細

ステップ 1 Cisco Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 2 コンフィギュレーション モードを開始します。

PIServer/admin# **configure terminal**

ステップ 3 リモート NFS サーバーへのシンボリックリンクを設定します。

pi-system-116/admin# conf t

pi-system-116/admin(config)# backup-staging-url nfs:// RemoteServerIP:/mnt/stagingfolder

pi-system-116/admin(config)# repository repositoryName

pi-system-116/admin(config-Repository)# url nfs:// RemoteServerIP:/mnt/sharefolder

pi-system-116/admin(config-Repository)# user userName password plain userPassword

pi-system-116/admin(config-Repository)# end

- RepositoryName は、リポジトリの名前です（MyRepo や PrimeInfrastructure など）。
- RemoteServerIP は、ステージングバックアップおよび共有バックアップフォルダをホストする NFS サーバーの IP アドレスです。上の例は、共有フォルダへの絶対パスを指定していることに注意してください。

共有フォルダへの相対パスを指定するには、URL で 1 本のスラッシュだけを使用します。例：
`nfs://RemoteServerIP/sharedfolder`

- Stagingfolder は、NFS サーバー上のステージング バックアップ フォルダの名前です。このフォルダには、後でファイルを tar するための初期データが一時的に転送されます。
- Sharedfolder は、バックアップが保存される NFS サーバー上の共有バックアップフォルダの名前です。
- UserName は、NFS サーバー上のリポジトリへの書き込み権限を持っているユーザーの名前です。
- UserPassword は、そのユーザーの対応するパスワードです。

ステップ 4 シンボリック リンクの作成を確認します。

```
PIServer/admin# show repository repositoryName
```

ステップ 5 コマンドラインからバックアップを実行する場合は、新しいリポジトリを backup コマンド内にリポジトリ名として指定します。次に例を示します。

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```

バックアップを自動的に実行する場合は、作成したリポジトリ名を Prime Infrastructure の Web インターフェイスでリポジトリ名として選択します。

リモート SFTP バックアップリポジトリの使用方法

リモート SFTP サーバー上でバックアップリポジトリを作成し、それを使用するように Prime Infrastructure サーバーを設定できます。

バックアップをホストする SFTP サーバーは、次の要件を満たしていれば、ネットワーク上のどこにでもセットアップできます。

- Prime Infrastructure サーバーからアクセスできる IP アドレスがある。
- ユーザーが SFTP サーバー ディスクへの書き込みアクセス権を持っている。
- バックアップが保存されるローカル共有フォルダが存在する。

これらの要件以外に、SFTP バックアップ サーバー上で必要な設定はありません。

リモート NFS リポジトリを使用することを推奨します。

SFTP サーバの詳細が UI の [Backup Repository] ドロップ ダウン リストに表示されるように、CLI を使用して SFTP サーバを設定する必要があります。SFTP サーバーは、CLI を使用してのみ設定できます。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 2 コンフィギュレーション モードを開始します。

PIServer/admin# **configure terminal**

ステップ 3 リモート SFTP サーバーへのシンボリック リンクを設定します。

PIServer/admin(config)# **repository** *repositoryName*

PIServer/admin(config-Repository)# **url sftp://RemoteServerIP//sharedfolder**

PIServer/admin(config-Repository)# **user** *userName* **password plain** *userPassword*

PIServer/admin(config-Repository)# **exit**

PIServer/admin(config)# **exit**

ここで、

- repositoryName は、リポジトリの名前です（たとえば、MyRepo や PrimeInfrastructure など）。
- RemoteServerIP は、共有バックアップ フォルダをホストする SFTP サーバーの IP アドレスです。上の例は、共有フォルダへの絶対パスを指定していることに注意してください。共有フォルダへの相対パスを指定するには、URL で 1 本のスラッシュだけを使用します。例：**url sftp://RemoteServerIP//sharedfolder**
- sharedfolder は、SFTP サーバー上の共有バックアップ フォルダの名前です。
- userName は、SFTP サーバー上のリポジトリへの書き込み権限を持っているユーザーの名前です。
- userPassword は、そのユーザーの対応するパスワードです。

ステップ 4 シンボリック リンクの作成を確認します。

PIServer/admin# s **how repository** *repositoryName*

ステップ 5 コマンドラインからバックアップを実行する場合は、新しいリポジトリを backup コマンド内にリポジトリ名として指定します。次に例を示します。

PIServer/admin# backup MyBackupFileName repository MyRepo application NCS

バックアップを自動的に実行する場合は、作成したリポジトリ名を Prime Infrastructure の Web インターフェイスでリポジトリ名として選択します。

関連トピック

リモート NFS バックアップ リポジトリの使用 （61 ページ）
CLI を使用した即時アプリケーション バックアップの実行 （69 ページ）
CLI を使用した即時アプライアンス バックアップの実行 （68 ページ）
自動バックアップ用のバックアップ リポジトリの指定 （67 ページ）

リモート FTP バックアップリポジトリの使用方法

リモート FTP サーバー上でバックアップリポジトリを作成し、それを使用するように Prime Infrastructure サーバーを設定できます。

バックアップをホストする SFTP サーバーは、FTP サーバーが次の要件を満たしていれば、ネットワーク上のどこにでもセットアップできます。

- Prime Infrastructure サーバーからアクセスできる IP アドレスがある。
- ユーザー（FTP ユーザー）が FTP サーバー ディスクへの書き込みアクセス権を持っている。
- Prime Infrastructure サーバー上で指定されたリポジトリ名と一致するローカル サブディレクトリが存在する。
- パスワードが 15 文字以下である。

これらの要件以外に、FTP バックアップ サーバー上で必要な設定はありません。

リモート NFS リポジトリを使用することを推奨します。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 2 コンフィギュレーション モードを開始します。

PIServer/admin# **configure terminal**

ステップ 3 リモート FTP サーバーへのシンボリック リンクを設定します。

PIServer/admin(config)# **repository** *repositoryName*

PIServer/admin(config-Repository)# url **ftp://RemoteServerIP/sharedfolder**

PIServer/admin(config-Repository)# **user** *userName* **password plain** *userPassword*

PIServer/admin(config-Repository)# **exit**

PIServer/admin(config)# **exit**

ここで、

- repositoryName は、リポジトリの名前です（たとえば、MyRepo や PrimeInfrastructure など）。
- RemoteServerIP は、共有バックアップ フォルダをホストする FTP サーバーの IP アドレスです。
- sharedfolder は、FTP サーバー上の共有バックアップ フォルダの名前です。
- userName は、FTP サーバー上のリポジトリへの書き込み権限を持っているユーザーの名前です。
- userPassword は、そのユーザーの対応するパスワードです。このパスワードは 15 文字以下にする必要があります。

ステップ 4 シンボリック リンクの作成を確認します。

PIServer/admin# s **how repository** *repositoryName*

ステップ 5 コマンドラインからバックアップを実行する場合は、新しい FTP リポジトリを backup コマンド内にリポジトリ名として指定します。次に例を示します。

PIServer/admin# backup MyBackupFileName repository MyRepo application NCS

バックアップを自動的に実行する場合は、作成したリポジトリ名を Prime Infrastructure の Web インターフェイスでリポジトリ名として選択します。

関連トピック

リモート NFS バックアップ リポジトリの使用 （61 ページ）
CLI を使用した即時アプリケーション バックアップの実行 （69 ページ）
CLI を使用した即時アプライアンス バックアップの実行 （68 ページ）
自動バックアップ用のバックアップ リポジトリの指定 （67 ページ）

ローカル バックアップ リポジトリの削除

ローカル バックアップ リポジトリを削除するには、以下の手順に従います。この手順に従うことにより、管理インターフェイスで確実に更新済みの情報が使用されるようになります。

ステップ 1 CLI 管理ユーザーとしてサーバーにログインします（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 2 ローカル アプリケーション バックアップ リポジトリを一覧表示し、削除するリポジトリを特定します。

```
show running-config | begin repository
```

ステップ 3 コンフィギュレーション モードを開始して、リポジトリを削除します。

```
configure terminal
(config)# no repository repositoryName
```

ステップ 4 ステップ 2 を繰り返して、リポジトリが削除されたことを確認します。

自動アプリケーション バックアップのセットアップ

インストール後、自動アプリケーションバックアップはデフォルトで有効になっています。スケジュールをカスタマイズしたり、別のバックアップリポジトリを指定したり、あるいは保存されるバックアップの数を調整したりできます。

どのデータがバックアップメカニズムによって保存されるかを確認する（およびバックアップされないデータを手動で保存する必要があるかどうかを確認する）には、以下のトピックを参照してください。

- バックアップされる情報 （57 ページ）
- バックアップされない情報 （59 ページ）

自動アプリケーション バックアップのスケジューリング

自動アプリケーション バックアップはデフォルトで有効になっていますが、これらのバックアップを実行する日付および間隔を調整できます。バックアップの実行は、リソースを消費するため、サーバーのパフォーマンスに影響します。トラフィックがピークの時間帯に自動バックアップが発生するスケジューリングは避けてください。

自動バックアップ アプリケーションが失敗すると、からバックアップ失敗アラームが（メジャーなシビラティ（重大度）で）発生します。これらのアラームは他のアラームと同様に表示できます。

（注） 自動アプリケーション バックアップに失敗すると、それ以降、ログインしようとするたびにポップアップ メッセージが表示されます。このメッセージは、該当のアラームに対する確認応答をするまで、表示され続けます。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（nfrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] リストで、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにして、[スケジュールの編集（Edit Schedule）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが開きます。

ステップ 4 [スケジュール（Schedule）] ダイアログボックスで、開始日、繰り返し間隔、およびオプションの終了時間を選択します。

ステップ 5 [送信（Submit）] をクリックします。これらの設定が、今後の自動アプリケーション バックアップに使用されます。

自動バックアップ用のバックアップ リポジトリの指定

インターフェイスを使用して、自動アプリケーション バックアップ用の別のバックアップ リポジトリを指定できます。バックアップ リポジトリは、ローカルまたはリモートにすることができます。このインターフェイスを使用すれば、まだ存在しない新しいローカルバックアップ リポジトリを作成することもできます。

始める前に

自動バックアップ用のリモート リポジトリを使用するには、最初にリポジトリを作成する必要があります。ローカル リポジトリのみが、この手順を使用して作成できます。リポジトリのセットアップと管理 （59 ページ）を参照してください。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（nfrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] のリストで、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックします。[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスが開きます。

ステップ 5 [バックアップ リポジトリ（Backup Repository）] ドロップダウン リストからリポジトリを選択し、[保存（Save）] をクリックします。 は、次の自動アプリケーション バックアップを実行するときに新しいリポジトリを使用します。

保存する自動アプリケーション バックアップ数の変更

ローカル リポジトリに保存する自動アプリケーション バックアップの数を調整するには、この手順に従います。バックアップの数がこの手順で指定する数を超えると、 は最も古いバックアップをリポジトリから削除します。

自動アプリケーション バックアップにリモート リポジトリが使用されている場合は、[保持する最大 UI バックアップ数（Max UI backups to keep）] 設定が適用されません。独自の方法を使用して、リモート リポジトリ上の古いバックアップをモニターし、アーカイブまたは削除する必要があります。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）] > [インフラストラクチャ（nfrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] 一覧で、[サーバーのバックアップ（Server Backup）] チェックボックスをオンにします。

ステップ 4 [編集（Edit）]（鉛筆アイコン）をクリックして、[ジョブ プロパティの編集（Edit Job Properties）] ダイアログボックスを開きます。

ステップ 5 [保持する最大 UI バックアップ数（Max UI backups to keep）] フィールドに値を入力してから、[保存（Save）] をクリックします。 は、この設定を次のバックアップから適用します。

手動バックアップの実行

この項のトピックでは、手動アプリケーション バックアップまたは手動アプライアンス バックアップを実行する方法について説明します。

どのデータがバックアップ メカニズムによって保存されるかを確認する（およびバックアップされないデータを手動で保存する必要があるかどうかを確認する）には、以下のトピックを参照してください。

- バックアップされる情報 （57 ページ）
- バックアップされない情報 （59 ページ）

CLI を使用した即時アプライアンス バックアップの実行

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 2 アプライアンス バックアップのリストを表示します。

```
PIServer/(admin)#show repository repositoryName
```

ここで、*repositoryName* は、アプライアンス バックアップを保存するリポジトリです。

ステップ 3 アプライアンスをバックアップします。

```
PIServer/(admin)#backup filename repository repositoryName
```

filename は、アプライアンス バックアップ ファイルに指定する名前です（例：myBackup）。ファイル名の長さは 26 文字です。その他の情報はファイル名に自動的に付加されます。次を参照： バックアップ ファイル名 （56 ページ）

Web GUI を使用した即時アプリケーション バックアップの実行

Web GUI を使用して即時アプリケーション バックアップをトリガーするには、次の手順に従います。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）]** > **[インフラストラクチャ（nfrastructure）]** を選択します。

ステップ 3 [ジョブ（Jobs）] リストで [サーバーのバックアップ（Server Backup）] チェックボックスをオンにし、[実行（Run）] をクリックします。

ステップ 4 バックアップ ステータスを確認するには、テーブル上部までスクロールし、新しいジョブを見つけ、そのステータスと結果を確認します。

CLI を使用した即時アプリケーション バックアップの実行

CLI を使用して即時アプリケーション バックアップをトリガーするには、次の手順に従います。

ステップ 1 CLI admin ユーザーとしてサーバーにログインします（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 2 バックアップのリストを表示します。ここで *repositoryName* はバックアップ リポジトリの名前です。

```
show repository repositoryName
```

ステップ 3 リモート バックアップを開始します。

```
backup filename repository repositoryName application NCS
```

ここで、filename は、アプリケーション バックアップ ファイルに付ける名前です（myBackup など）。ファイル名の長さは 26 文字です。その他の情報はファイル名に自動的に付加されます。バックアップ ファイル名 （56 ページ）を参照。

手動アプライアンス バックアップの実行

リモート リポジトリへのアプライアンスのバックアップを実行するには、次の手順に従います。

ステップ 1 リモート ホストが使用可能であることを確認します。

ステップ 2 admin として サーバーにログインします（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 3 リモート バックアップを開始します。

```
(admin)# backup filename repository repositoryName
```

ステップ 4 バックアップ転送が完了していることを確認するため、md5CheckSum とファイル サイズを確認します。

データの復元

復元操作はすべて、CLIを使用して実行します。バックアップが実行されたホスト（ローカルホスト）またはリモートホストにデータを復元できます。バックアップは全体の復元のみが可能です（バックアップの一部のみを復元することはできません）。

詳細については、次のトピックを参照してください。

- アプリケーション バックアップの復元 （70 ページ）
- アプライアンス バックアップの復元 （71 ページ）

アプリケーション バックアップの復元

（注） アプライアンスのバックアップを復元するには、「アプライアンス バックアップの復元 （71 ページ）」の手順に従います。

始める前に

高可用性を使用している場合、データを復元する前に「 」のガイドラインを参照してください。

ステップ 1 CLI admin ユーザーとしてサーバーにログインします（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 2 以前の復元の試行に失敗した場合、データベースが破損している可能性があります。次のコマンドを実行して、データベースを再作成します。

```
ncs run reset db
```

ステップ 3 保存済みのアプリケーションバックアップを一覧し、復元するバックアップを特定します。*repositoryName* は、バックアップ ファイルを格納しているリポジトリです。

```
show repository repositoryName
```

ステップ 4 vmWare vSphere クライアント（OVA）または Cisco IMC サーバー（ベア メタル）からデータを復元します。

```
restore backupFileName repository repositoryName application NCS
```

ステップ 5 Cisco Smart Licensing を使用している場合は、Cisco.com で Cisco Smart Software Manager（CSSM）に を再登録します。を参照してください。

アプライアンス バックアップの復元

（注） アプリケーション バックアップを復元するには、アプリケーション バックアップの復元 （70 ページ） の手順を使用します。

始める前に

ハイ アベイラビリティを使用している場合は、データを復元する前に の情報を参照してください。

ステップ 1 CLI admin ユーザーとしてサーバーにログインします（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 2 以前の復元の試行に失敗した場合、データベースが破損している可能性があります。外部リポジトリに保存されているバックアップで、同じリリースを使用してセットアップを再インストールし、復元をやり直します。

ステップ 3 保存されているアプライアンス バックアップをリストし、復元するバックアップを指定します。*repositoryName* は、バックアップ ファイルを格納しているリポジトリです。

```
show repository repositoryName
```

ステップ 4 vmWare vSphere クライアント（OVA）または Cisco IMC サーバー（ベア メタル）からデータを復元します。

```
restore backupFileName repository repositoryName
```

ステップ 5 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを変更するかどうかを決定します。

a) インストール環境が次の条件に該当するかどうかを確認します。

- 復元したホストが古いホストと同じサブネット上に存在し、古いホストがまだアクティブのままである。
- 復元したホストが古いホストとは別のサブネット上に存在する。

該当する場合は、次のステップを実行します。

b) 復元したサーバーで、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、およびオプションでホスト名を変更します。

c) サーバーの実行コンフィギュレーションに変更を書き込み、 サービスを再起動します。次に例を示します。

```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
(config)# exit
(admin)# write mem
(admin)# ncs stop
```

```
(admin)# ncs start
(admin)# exit
```

ステップ 6 Cisco Smart Licensing を使用している場合は、Cisco.com で Cisco Smart Software Manager（CSSM）に を再登録します。を参照してください。

失敗した復元からの回復

復元が完了しなかったり、エラーが報告されたりすることがあります。復元が失敗した場合は、常に、データベース破損のリスクが伴い、それ以上の復元または再インストールができなくなることがあります。別の復元または再インストールを試行する前に、破損したデータベースを復元するには次の手順を実行します。

ステップ 1 サーバーとの CLI セッションを開きます（サーバーとの SSH セッションの確立 （109 ページ）を参照）。

ステップ 2 次のコマンドを入力して、破損したデータベースをリセットします。

```
ncs run reset db
```

バックアップおよび復元中のディスク容量の問題の管理方法

バックアップまたは復元中にディスク領域の問題が発生した場合、次のいずれか行うことを推奨します。

- VMware の**設定の編集**機能を使用して、仮想マシンに割り当てるディスク容量のサイズを拡大します（「VMware vSphere クライアントを使用した VM のリソース割り当ての変更」を参照）。

VMware ESXi 5.5 以降を使用する場合は、この設定を調整するために vSphere Web Client を使用してください（『Modify VM Resource Allocation Using VMware vSphere Client』を参照）。

- バックアップと復元を使用した別の仮想アプライアンスへの移行 （73 ページ）（またはバックアップと復元を使用した別の物理アプライアンスへの移行 （73 ページ））に記載されている方法を使用して、十分なディスク容量を持つサーバーにインストールを移動します。

既存のシステムを復元した後に、バックアップを作成できない場合は、「Prime Infrastructure データベースの圧縮」の手順に従ってディスク容量を解放し、正常なバックアップを作成してください。

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、バックアップ用にリモートリポジトリを（FTP、SFTP、または NFS を使用して）セットアップして使用してください（「リモート バックアップ リポジトリの使用」を参照）。

関連トピック

VMware vSphere クライアントを使用した VM のリソース割り当ての変更 （134 ページ）
バックアップと復元を使用した別の物理アプライアンスへの移行 （73 ページ）
バックアップと復元を使用した別の仮想アプライアンスへの移行 （73 ページ）
Prime Infrastructure データベースの圧縮 （136 ページ）
リモート バックアップ リポジトリの使用 （60 ページ）
ディスク容量の問題を管理する方法 （167 ページ）

バックアップと復元を使用した別の仮想アプライアンスへの移行

以下の場合のように、既存の仮想アプライアンス（OVA サーバー インストール構成）から新しいインストール構成に データを移行する必要が生じることがあります。

- 致命的なハードウェア障害が発生した場合などは、古いサーバーを丸ごと交換します。この場合は、古いインストール メディアを使用して交換用サーバー上で新しいホストを作成し直してから、古いホストから新しいホストにアプリケーションデータを移行することができます。
- を使用してネットワークをさらに管理できるように、より大規模なまたはより強力なサーバーに移行します。この場合、OVA インストール ファイルが存在すること、および、より大きなサーバーにインストールできる機能を使用して、そのファイルを新しいサーバーにインストールできることを確認してから、古く小さいサーバーを取り外すことができます。その後で、古いホストからアプリケーション データを移行できます。

いずれの場合も、古いホストから作成したアプライアンスバックアップまたはアプリケーションバックアップを新しいホストに復元することによって、比較的簡単に古いデータを新しい仮想アプライアンスに移行できます。

ステップ 1 まだ実行していない場合は、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（リモート バックアップ リポジトリの使用 （60 ページ）を参照）。

ステップ 2 古いホストのアプリケーションバックアップを実行し、リモートリポジトリにバックアップを保存します（CLI を使用した即時アプリケーション バックアップの実行 （69 ページ）を参照）。

ステップ 3 新しいホストをインストールします

ステップ 4 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に新しいホストを設定します（リモート バックアップ リポジトリの使用 （60 ページ）を参照）。

ステップ 5 リモートリポジトリ上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（アプリケーション バックアップの復元 （70 ページ）を参照）。

バックアップと復元を使用した別の物理アプライアンスへの移行

次の操作を行う場合には必ず、既存の物理アプライアンスから新しいアプライアンスに Prime Infrastructure データを移行する必要があります。

- 致命的なハードウェア障害が発生した場合などは、古いアプライアンスを丸ごと交換します。この場合は、交換用アプライアンスを発注してから、古いアプライアンスから新しいアプライアンスにデータを移行できます。
- 新しくインストールしたアプライアンスに移行します。

いずれの場合も、古いホストから作成したアプライアンス バックアップまたはアプリケーション バックアップを新しいアプライアンスに復元することによって、比較的簡単に古いデータを新しいアプライアンスに移行できます。

ステップ 1 古いアプライアンスがまだ機能している場合：

a) まだ実行していない場合は、古いアプライアンスのリモート バックアップ リポジトリをセットアップします（「関連項目」の「リモート バックアップ リポジトリの使用」を参照）。

b) リモート リポジトリ上で古いアプライアンスのアプライアンス バックアップまたはアプリケーション バックアップを実行します（それぞれ「アプライアンス バックアップの実行」または「アプリケーション バックアップの実行」を参照）。

ステップ 2 古いアプライアンスと同じリモート バックアップ リポジトリを使用するように新しいアプライアンスを設定します（「リモート バックアップ リポジトリの使用」を参照）。

ステップ 3 リモート リポジトリのアプライアンス バックアップまたはアプリケーション バックアップを新しいアプライアンスに復元します（それぞれ「アプライアンス バックアップからの復元」または「アプリケーション バックアップからの復元」を参照）。復元するバックアップの種類に適した手順に従うようにしてください。たとえば、古いアプライアンスからアプリケーション バックアップを作成した場合は、アプライアンス バックアップではなくアプリケーション バックアップを復元する手順を使用して、それを復元する必要があります。

関連トピック

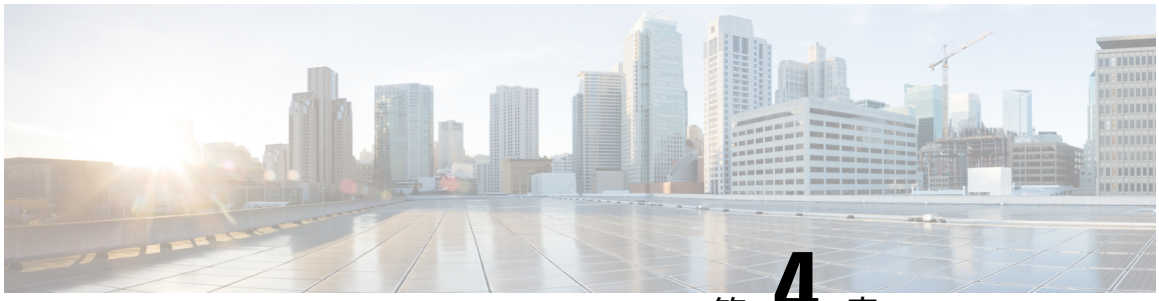
リモート バックアップ リポジトリの使用 （60 ページ）
CLI を使用した即時アプリケーション バックアップの実行 （69 ページ）
CLI を使用した即時アプライアンス バックアップの実行 （68 ページ）
アプライアンス バックアップの復元 （71 ページ）
アプリケーション バックアップの復元 （70 ページ）

Operations Center でのバックアップと復元の使用

オペレーションセンターおよびオペレーションセンターのサーバー上で実行されている Cisco Prime Infrastructure インスタンスは、CLI を使用して、バージョン 3.7.x、3.8.x、および 3.9.x から作成されたアプリケーション バックアップの復元をサポートできます。

Operations Center 上で実行されている Prime Infrastructure インスタンスからの自動アプリケーション バックアップをスケジュール設定することはできません。

詳細については、「リモート バックアップ リポジトリの使用」および「アプリケーション バックアップの復元」を参照してください。



第 4 章

Prime Infrastructure サーバーを設定する

サーバーの構成の表示

現在のサーバー時間、カーネル バージョン、オペレーティング システム、ハードウェア情報などの サーバーの構成情報を表示するには、以下の手順を使用します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム監視ダッシュボード（System Monitoring Dashboard）]** を選択します。

ステップ 2 [概要（Overview）] タブをクリックします。

ステップ 3 ダッシュボードの左上にある [システム情報（System Information）] をクリックして、[システム情報（System Information）] フィールドを展開します。

使用可能なシステム設定

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] メニューには、Cisco Prime Infrastructure 設定値を設定または変更するためのオプションが含まれています。これらの設定値の多くは、最初に Prime Infrastructure を実装する際にカスタマイズできますが、実稼働に移した後に変更することは、ほとんどありません。

次の表に、[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] メニューから設定または変更できる設定値のタイプを一覧表示します。

表 *5 :* 使用可能な *Prime Infrastructure* システム設定オプション

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
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（ユーザー名とパスワード）を変更し、次の操作を行います。 • シスコ ソフトウェア イメージ アップデートの有無の確認 • シスコ サポート ケースの登録または確認 このページへは、[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ソフトウェア更新（Software Update）] ページのリンクからもアクセスできます。	[一般（General）] > [アカウント クレデンシャル（Account Credentials）]	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure サーバーとそのローカル認証サーバーのプロキシを設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [プロキシ（Proxy）] 「プロキシ サーバーの設定」を参照してください。	N/A
テクニカル サポート リクエストを作成するための設定値を設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [サポート リクエスト（Support Request）] 「シスコサポート リクエストのデフォルトの設定」を参照してください。	有線およびワイヤレス デバイス
スマート ライセンスが有効な状態で、Smart Call Home Transport Gateway を使用してインターネット経由で情報を送信するように Transport Gateway のモードを設定します。	[一般（General）] > [アカウント クレデンシャル（Account credentials）] > [スマート ライセンス トランスポート（Smart Licensing Transport）] 「Prime Infrastructure と Cisco Smart Software Manager との間のトランスポート モードの設定」を参照してください。	Prime Infrastructure アプライアンス
特定のデータ タイプ（傾向、デバイス ヘルス、パフォーマンス、ネットワーク監査、システム ヘルス）の保存期間を設定します。	**[一般（General）] > [データ保存（Data Retention）]** 履歴データの保持について （170 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
ゲストアカウント設定値を設定して、有効期限が終了したすべてのゲストアカウントをグローバルに削除します。デフォルトでは、Prime Infrastructure ロビーアンバサダーは作成者に関係なく、すべてのゲストアカウントにアクセスできます。[この Lobby Ambassador が作成したゲストのみを検索して表示（Search and List only guest accounts created by this lobby ambassador）] チェックボックスをオンにした場合、Lobby Ambassador は本人が作成したゲストアカウントのみにアクセスできます。	**[一般（General）] > [ゲスト アカウント（Guest Account）]** ゲスト アカウントの設定 （239 ページ）を参照してください。	ワイヤレス デバイスのみ
シスコ製品の向上のために、Prime Infrastructure は製品フィードバック データを収集してシスコに送信します。	[一般（General）] > [改善にご協力ください（Help Us Improve）] シスコ製品フィードバックの設定 （128 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
ジョブ承認を有効にして、実行する前に管理者の承認を必要とするジョブを指定します。	**[一般（General）] > [ジョブ承認（Job Approval）]** ジョブ承認者を設定してジョブを承認する （246 ページ）を参照してください。	有線およびワイヤレス デバイス
すべてのユーザに対してログインページに表示される免責事項テキストを変更します。	**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** ログイン バナー（ログインの免責事項）の作成 （114 ページ）を参照してください。	Prime Infrastructure アプライアンス
定期レポートの保存先パス、およびレポートの保存期間を設定します。	**[一般（General）] > [レポート（Report）]** レポートの保存と保持の制御 （177 ページ）を参照してください。	有線およびワイヤレス デバイス
• FTP、TFTP、および HTTP/HTTPS サーバープロキシを有効または無効にし、これらのプロキシが通信に使用するポートを指定します。 • Prime Infrastructure に対して現在設定されているローカル タイムゾーンと NTP サーバー名を確認します。	**[一般（General）] > [サーバー（Server）]** サーバー ポートおよびグローバル タイムアウトの設定 （111 ページ）を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
• Prime Infrastructure が Cisco.com でシスコ ソフトウェア イメージ アップデートを確認するときに、cisco.com に保管されているクレデンシャルを使用しないことを指定します。 • 通知を受信する Prime Infrastructure ソフトウェア アップデートの種類（重要な修正、新しいデバイス サポート、Prime Add-On 製品など）を選択します。	**[一般（General）] > [ソフトウェア更新（Software Update）]**	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
インベントリ、サイトグループ、ユーザー定義の CLI や複合テンプレート、関連するサイトマップ、および CMX データを Cisco Prime Infrastructure から Cisco DNA Center に移行します。	**[Mega] メニュー > [Cisco DNA Center coexistence]** Cisco Prime Infrastructure と Cisco Digital Network Architecture Center の共存ガイド [英語] を参照	Prime Infrastructure から Cisco DNA Center への移行
[監査ログのパージ設定（Audit Log Purge Settings）] チェックボックスをオンにして、変更監査 JMS 通知を有効にします。	**[メールおよび通知（Mail and Notification）] > [監査通知の変更（Change Audit Notification）]** 変更監査通知の有効化および syslog レシーバの設定 （304 ページ）を参照してください。	有線およびワイヤレス デバイス
ユーザージョブごとにジョブ通知メールを送信します。	**[メールと通知（Mail and Notification）] > [ジョブ通知メール（Job Notification Mail）]** 「ユーザ ジョブ用のジョブ通知メールを設定する」を参照	有線およびワイヤレス デバイス
レポートおよびアラーム通知の電子メール配信を有効にします。	**[メールおよび通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** 電子メール サーバー設定の構成 （472 ページ）を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• コントローラおよび自律 AP CLI セッションに使用するプロトコルを設定します。 • 検出時の自律 AP 移行分析を有効にします。	**[ネットワークおよびデバイス（Network and Device）] > [CLI セッション（CLI Session）]** を参照してください。	ワイヤレス デバイスのみ
ワイヤレス コントローラのアップグレード後の自動更新を有効にし、save config トラップを処理します。	**[ネットワークおよびデバイス（Network and Device）] > [コントローダ アップグレード（Controller Upgrade）]** アップグレード後のコントローラの更新 （325 ページ）を参照してください。	ワイヤレス デバイスのみ
Cisco Prime Infrastructure での Unified AP の ping 機能設定を有効にします。	**[ネットワークとデバイス（Network and Device）] > [Unified AP への Ping 確認（Unified AP Ping Reachability）]**	ワイヤレス デバイスのみ
プラグ アンド プレイの設定を変更します。	**[ネットワークおよびデバイス（Network and Device）] > [プラグ アンド プレイ（Plug & Play）]**	有線デバイスのみ

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
	[ネットワークおよびデバイス（Network and Device）] > [SNMP] グローバル SNMP の設定 （115 ページ）を参照してください。	ワイヤレス デバイスのみ

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
トレース表示値、到達可能性パラメータ、バックオフアルゴリズムを含め、グローバル SNMP ポーリングパラメータを設定します。 バックオフアルゴリズムに [Exponential] を選択した場合は、SNMP 初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。[一定タイムアウト（Constant Timeout）] を選択した場合は、すべての SNMP 試行に対して同じ待機時間（指定したタイムアウト値）が適用されます。到達可能性パラメータを使用することを選択した場合は、Prime Infrastructure はデフォルトで、ユーザーが設定したグローバルな [到達可能性の再試行回数		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
（Reachability Retries）]および[タイムアウト（Timeout）] を使用します。チェックボックスがオフにされている場合、Prime Infrastructure は常に、指定されたタイムアウトと再試行を使用します。		
不正 AP を設定し、Prime Infrastructure がネットワーク内で不正アクセスポイントの接続先となっているスイッチポートを自動的に追跡できるようにします。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）]** 不正 AP トレース用の SNMP クレデンシャルの設定 （331 ページ）を参照してください。	ワイヤレス デバイスのみ
不正 AP スイッチ ポートのトレースで使用する SNMP クレデンシャルとトレースパラメータを設定します。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）]** 不正 AP トレース用の SNMP クレデンシャルの設定 （331 ページ）を参照してください。	ワイヤレス デバイスのみ
スイッチポートトレースの基本パラメータと拡張パラメータを設定します。	**[ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）]** スイッチ ポート トレースを設定する （326 ページ）を参照してください。	有線デバイスのみ

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure で使用可能なイーサネット MAC アドレスの表示、追加、削除を行います。この一覧に複数のイーサネット MAC アドレスを追加すると、自動スイッチポート トレースで、これらのポートでの不正 AP のスキャンが行われなくなります。	**[ネットワークとデバイス（Network and Device）] > [ポート トレースのスイッチ（SPT）（Switch Port Trace (SPT)）] > [認識済みのイーサネット MAC アドレス（Known Ethernet MAC Address）]**	Prime Infrastructure アプライアンス
デバイス設定の導入時に使用する基本制御パラメータ（実行コンフィギュレーションのバックアップの有効化、ロールバック、キャッシュからの **show** コマンド出力の取得、使用する CLI スレッド プールの数など）を設定します。	**[インベントリ（Inventory）] > [設定（Configuration）]** テンプレート導入前のデバイス設定のアーカイブ （178 ページ）を参照してください。	有線およびワイヤレス デバイス
設定アーカイブの基本パラメータ（プロトコルや保存する設定バージョン数など）を設定します。	**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** WLC 設定をいつどのようにアーカイブするかの指定 （178 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
IPv4 または IPv6 アドレスの優先設定を指定します。	**[インベントリ（Inventory）] > [Discovery]**	有線およびワイヤレス デバイス
メンバーまたは子が関連付けられていないグループを表示するかどうかを設定します。	**[インベントリ（Inventory）] > [グループ化（Grouping）]**	有線およびワイヤレス デバイス
ソフトウェアイメージのダウンロード、配布、および推奨用のグローバルプリファレンスパラメータを設定します。	**[インベントリ（Inventory）] > [ソフトウェアイメージの管理（Software Image Management）]** ソフトウェアイメージの管理の詳細については、『Cisco Prime Infrastructure User Guide』を参照してください。	有線およびワイヤレス デバイス
インベントリ収集を有効にして、Prime Infrastructure がデバイスに関する syslog イベントを受信した場合にインベントリを収集できるようにします。	**[インベントリ（Inventory）] > [インベントリ（Inventory）]** イベント受信後のインベントリ収集の指定 （177 ページ）を参照してください。	有線およびワイヤレス デバイス
デバイスに関する追加情報を保存します。	**[インベントリ（Inventory）] > [ユーザー定義フィールド（User Defined Fields）]** ユーザー定義フィールドにデバイス情報を追加する （123 ページ）を参照してください。	有線デバイスのみ

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• 削除するアラーム、イベント、syslog と、削除する頻度を変更します。 • 電子メール通知の送信対象とするアラームのタイプ、および送信する頻度を設定します。 • [Alarm Summary] ビューに表示するアラームのタイプを設定します。 • 電子メールで送信するアラーム通知の内容を変更します。 • 障害の原因の表示方式を変更します。	**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** アラーム クリーンアップ、表示、および電子メール オプションの指定 （291 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure から通知を受信するリモートイベントおよびアラームの受信者を設定します。 アラートおよびイベントは SNMPv2 通知として、設定された通知宛先に送信されます。通知タイプ UDP の通知宛先を追加する場合、その追加する宛先はそれが設定されている同じポート上で UDP をリッスンしている必要があります。デフォルトでは、選択されたカテゴリに対する INFO レベルのイベントのみが処理されます。ノースバウンド通知では、SNMPV2 トラップのみが考慮されます。	**[メールと通知（Mail and Notification）] > [通知宛先（Notification Destination）]** アラーム通知先の設定 （285 ページ）を参照してください。 **[アラームおよびイベント（Alarms and Events）] > [アラーム通知ポリシー（Alarm Notification Policies）]** アラーム通知ポリシーのカスタマイズ （287 ページ）を参照してください。	有線およびワイヤレス デバイス
生成される任意のアラームのシビラティ（重大度）を設定します。	**[アラームおよびイベント（Alarms and Events）] > [アラームのシビラティ（重大度）および自動クリア（Alarm Severity and Auto Clear）]** シビラティ（重大度）レベルの変更 （295 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
Prime Infrastructure ハードウェアアプライアンスについて生成される SNMP トラップとイベントを設定します。	**[アラームおよびイベント（Alarms and Events）] > [システム イベント設定（System Event Configuration）]** 内部 SNMP トラップの生成 （453 ページ）を参照してください。	Prime Infrastructure アプライアンス

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
	[クライアントおよびユーザー（Client and User）] > [クライアント（Client）] クライアント パフォーマンスの設定 （136 ページ）を参照してください。	有線およびワイヤレス デバイス

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• 診断チャネルでクライアントの自動トラブルシューティングを有効にします。 • DNS サーバからのクライアントホスト名のルックアップを有効にし、ホスト名をキャッシュに保持する期間を設定します。 • 関連付けが解除されたクライアントとそのセッションデータを保持する期間を設定します。 • 有線クライアントをポーリングし、トラップまたは syslog を受信した場合にのみセッションを識別します。 （注） これ		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
は、ワイヤレスクライアントが多数あるネットワークで使用することが推奨されるオプションではあり		

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
ません。 • [拡張クライアント トラップからクライアントを検出する（Discover Clients from enhanced client traps）] を有効にすると、互換性のある Cisco WLC から受信した拡張トラップからのクライアントおよびセッション情報が検出できるようになります。 次の CLI コマンドを使用して、トラップを送信するように WLC を設定する必要があります。		

手順は次のとおりです。	**[Administration] > [Settings] > [System Settings]** から選択する項目	適用対象
• config trapflags client • config trapflags client • config trapflags client • config trapflags client		

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
• [トランクポート上の有線クライアントを検出（Discover wired clients on trunk ports）] を有効にすると、トランク ポートに接続されている、スイッチとルータ以外の管理対象外エンティティを検出できるようになります。 • イベントとしてのクライアント関連付けおよび関連付け解除のトラップと syslog の保存を無効にします。 • イベントとしてのクライアント認証失敗トラップの保存、および失敗トラップの間でイベントを保		

手順は次のとおりです。	[Administration] > [Settings] > [System Settings] から選択する項目	適用対象
存する期間を有効にします。		
ベンダーの組織固有識別子（OUI）マッピング XML ファイルを追加します。	**[クライアントおよびユーザー（Client and User）] > [ユーザー定義 OUI（User Defined OUI）]** 「新しいベンダー OUI マッピングの追加」を参照してください。	有線およびワイヤレス デバイス
更新されたベンダー OUI マッピング XML ファイルをアップロードします。	**[クライアントおよびユーザー（Client and User）] > [OUI のアップロード（Upload OUI）]** 「更新されたベンダー OUI マッピング ファイルのアップロード」を参照してください。	有線およびワイヤレス デバイス
Cisco Prime Infrastructure に Cisco WAAS Central Manager の IP アドレスを設定します。	**[サービス（Services）] > [サービス コンテナの管理（Service Container Management）]** 『Cisco WAAS Central Manager Integration』（ユーザー ガイド）を参照してください。	有線デバイスのみ

サーバーの接続の保護

データ セキュリティのため、は、標準の公開キー暗号化方式と Public Key Infrastructure（PKI）を使用して送信中のデータを暗号化します。インターネット上で、これらのテクノロジーに関する詳細情報を得ることができます。 は、次の接続間で交換されるデータを暗号化します。

- Web サーバーと Web クライアント間
- CLI クライアントと CLI シェル インターフェイス間（SSH で処理）
- 、AAA のようなシステム、および外部ストレージ間

Web サーバーと Web クライアント間の通信を保護するには、HTTPS メカニズムの一部として組み込まれる公開キー暗号化サービスを使用します。そのためには、Web サーバーの公開キーを生成し、それをサーバーに保存して、Web クライアントと共有する必要があります。これは、標準 PKI 証明書のメカニズムを使用して実現できます。このメカニズムを使用することによって、Web サーバーの公開キーを Web クライアントと共有するだけでなく、アクセスする Web サーバー（URL）に公開キーが必ず属することが保証されます。これにより、第三者が

Web サーバーと見せかけて、Web クライアントが Web サーバーに送信する機密情報を収集することを防ぎます。

以下のトピックでは、Web サーバーを保護するために実行できるその他の手順について説明します。

- シスコでは、 Web サーバーは証明書ベースの認証を使用して、Web クライアントを認証するようお勧めします。
- CLI クライアントと CLI インターフェイスの間の接続を保護するには、のセキュリティを強化する手順を参照してください。
- 、AAA などのシステム、および外部ストレージの間の接続を保護するには、の推奨事項を参照してください。

Prime Infrastructure への HTTPS アクセスをセットアップする

Prime Infrastructure では、セキュア HTTPS クライアント アクセスがサポートされます。HTTPS アクセスを使用するには、秘密キーと対応する証明書ファイルを Prime Infrastructure サーバーに適用し、これらの証明書を信頼するようにユーザーが各自のクライアント ブラウザを更新する必要があります。

このためには、次のいずれかの証明書ファイルを使用できます。

- 自己署名。「関連項目」の「自己署名証明書の生成および適用」の手順に従って、自己署名証明書の生成および適用ができます。
- 認証局（CA）によるデジタル署名。CA とは、識別情報を検証して証明書を発行する組織（Cisco や VeriSign など）です。CA が発行した証明書は、証明書に指定されているエンティティ（サービスやデバイスなど）の名前に公開キーをバインドします。関連項目の「CA 署名付きホスト証明書のインポート」の手順に従って、サードパーティ CA から CA 証明書を取得し、Prime Infrastructure サーバーに適用できます。

（注） インストール時に、秘密キー、およびデフォルトのパラメータを持つ自己署名証明書が生成されます。

関連トピック

自己署名証明書の生成および適用 （99 ページ）
CA 署名付きホスト証明書のインポート （100 ページ）
秘密キーのインポート （103 ページ）
秘密キーのエクスポート （103 ページ）

自己署名証明書の生成および適用

Prime Infrastructure を使用して、自己署名証明書を生成および適用します。

ステップ 1 Prime Infrastructure との CLI セッションを開始します（CLI から接続する方法 （147 ページ）を参照）。「configure terminal」モードにしないでください。

ステップ 2 ドメイン情報を使用して新しいRSAキーと自己署名証明書を作成するには、次のコマンドを入力してください。

PIServer/admin# **ncs key genkey –newdn**

証明書の [識別名（DN）（Distinguished Name (DN)）] フィールドへの入力が求められます。Prime Infrastructure にアクセスするために使用するドメイン名として、サーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。

ステップ 3 証明書を有効にするため、Prime Infrastructure を再起動します（CLI を使用した Prime Infrastructure の再起動 （149 ページ）を参照）。

ログインの問題を防ぐため、Prime Infrastructure ログイン ページに次回アクセスするときにブラウザの信頼ストアに自己署名証明書を追加するようにユーザーに指示します。

CA 署名付きホスト証明書のインポート

Prime Infrastructure を使用して、証明書署名要求（CSR）ファイルを生成し、検証のために認証局（CA）に送信します。CA に CSR ファイルを送信する方法は、CA によって異なります。

証明書の CSR ファイルを生成して送信した後は、同じ Prime Infrastructure サーバーで再び新しいキーを生成するために **genkey** コマンドを再度使用しないでください。コマンドを再度使用すると、インポートされる CA 署名付き証明書のキーとサーバー上のファイルのキーが一致しなくなります。

署名付きサーバー証明書はホスト固有であることに注意してください。つまり、Prime Infrastructure バックアップで保持されますが、復元されるのはバックアップ サーバーとリストア サーバーのホスト名が同一である場合だけです。

（注） ハイ アベイラビリティ仮想 IP は、サーバー管理の簡素化を目的として設計されています。署名付きサーバー証明書の設定は、Prime Infrastructure の HA 仮想 IP 展開では機能しません。

ステップ 1 「管理」クレデンシャルを使用して Prime Infrastructure との CLI セッションを開始し、既存の信頼できる証明書を確認します（「CLI 経由の接続方法」を参照）。「configure terminal」モードにしないでください。

PIServer/admin# **ncs key listcacerts**

ここで、**listcacerts** は既存の信頼できる証明書をリストするコマンドです。

ステップ 2 PI サーバーの場所（**/opt/CSCOncs/migrate/restore**）に移動し、「ルート」CLI クレデンシャルを使用してインポートされた証明書を確認します。

ステップ 3 証明書が見つかったら、「管理」CLI クレデンシャルを使用して証明書を削除します（「CA 署名付き証明書の削除」を参照）。証明書が見つからなければ、ステップ 4 に進みます。

PIServer/admin# pi/admin# **ncs key deletecacert** <*certificate name*>

証明書を削除した後、Prime Infrastructure サーバーを再起動します。

ステップ 4 以下のコマンドを入力して、デフォルトのバックアップ リポジトリに CSR ファイルを生成します。

PIServer/admin# **ncs key genkey -newdn -csr <csrfilename> repository <repositoryname>**

-newdn：ドメイン情報を使用して新しい RSA キーと自己署名証明書を生成します。

-csr：新しい CSR 証明書を生成します。

Csrfilename：CSR ファイル名。これは任意の名前です（例：MyCertificate.csr）。

repositoryname：ファイルの場所。ファイルの名前には、最大 80 文字の英数字を使用できます。

例：

PIServer/admin# ncs key genkey -newdn -csr CSRFile.csr repository <*repositoryname*>

The NCS server is running. Changes will take effect on the next server restart

サーバーの完全修飾ドメイン名を入力します：**<FQDN>**

組織単位の名前を入力します：**<organization>**

組織の名前を入力します：**<organization>**

市区町村の名前を入力します：**<city>**

都道府県の名前を入力します：**<state>**

2 文字の国コードを入力します：**<country code>**

サブジェクト代替名を指定します。

指定しない場合は、CN が使用されます。

カンマ区切りのリストを使用します（DNS:<name>,IP:）<address>

DNS:<FQDN>,IP:<IPADDRESS>

公開キー アルゴリズム [rsa/ec] を指定します：**rsa**

RSA キー サイズ [2048/4096/8192] を指定します：**4096**

署名アルゴリズム [sha256/sha512] を指定します：**sha256**

キーと CSR/証明書が以下の詳細で生成されます。

サブジェクト：/C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=DNS:<FQDN>

サブジェクト代替名：DNS:<FQDN>,IP:<IPADDRESS>

公開キー アルゴリズム：4096

署名アルゴリズム：sha256

続行 [yes]：yes

生成しています。

完了しました。変更は次回のサーバーの再起動時に反映されます。

（注） 「サブジェクト代替名」を指定しない場合、このマシンにのみ CA 証明書をインポートできます。

「サブジェクト代替名」を指定した場合、CA から受け取った CA 証明書を、指定の FQDN を持つ任意のサーバーにインポートできます。SAN 指定のサーバーに CA 証明書をインポートするには、CSR を生成したサーバーから秘密キーをエクスポートし、その秘密キーを署名付き証明書とともに他の指定サーバーにインポートする必要があります。

SAN リストに、現在のサーバーの FQDN を追加する必要があります。

ステップ 5 任意の認証局（CA）に CSR ファイルを送信します。

CA は、署名付きサーバー証明書と 1 つ以上の CA 証明書ファイルを送信することで応答します。CA の応答は、ファイルが次のいずれであるかを示します。

- 署名付きサーバー証明書。通常、証明書の適用対象サーバーのホスト名がそのファイル名に反映されています。
- CA 証明書。通常は CA の名前を反映したファイル名が付いています。

すべての証明書を連結して 1 つのファイルにまとめます。ファイルの先頭がホスト証明書で、その後にチェーンと同じ順序で CA 証明書を配置する必要があります。

たとえば Linux の場合、次のコマンドを使用してファイルを結合できます。

cat host.pem subca.pem rootca.pem > servercert.pem

（注） 証明書は PEM 形式である必要があります。

ステップ 6 次のコマンドを入力して、Prime Infrastructure サーバーに署名付きサーバー証明書ファイルをインポートします。

PIServer/admin# **ncs key importcacert tomcat** <*certificate_name*> **repository** <*repositoryname*>

ステップ 7 次のコマンドを入力して、Prime Infrastructure サーバーに署名付き証明書ファイルをインポートします。

PIServer/admin# **ncs key importsignedcert <certificate_name> repository <repositoryname>**

ステップ 8 CA 署名付き証明書を有効にするために、Prime Infrastructure を再起動します（「Prime Infrastructure の再起動」を参照）。

証明書に署名した CA が組織内で信頼される CA ではない場合は、ユーザーに対し、Prime Infrastructure ログイン ページに次回アクセスするときに、CA 署名付き証明書を各自のブラウザの信頼ストアに追加するように指示してください。

（注） CA 証明書をインポートして、PI と外部デバイス/サーバーの間にセキュアな接続を確立するには、以下のコマンドを使用します。

PIServer/admin# **ncs key importcacert truststore {system | devicemgmt}alias <alias_name> <CA_certifcate_name> repository <repository_name>**

詳細については、CLI から接続する方法 （147 ページ）およびCLI を使用した Prime Infrastructure の再起動（149 ページ）を参照してください。

秘密キーのインポート

秘密キーと署名付き証明書を外部で生成できます。外部で生成する場合は、次のコマンドを使用してキーと証明書の両方をインポートできます。

ncs key importkey <private_key_filename> <certificate_filename> repository <repository_name>

秘密キーのエクスポート

秘密キーをエクスポートするコマンドを次に示します。

ncs key exportkey <private_key_filename> <certificate_filename> repository <repository_name>

上記のコマンドを実行すると、秘密キーが生成され、リポジトリの指定されたファイルの場所に配置されます。

証明書の検証設定

TLS/HTTPS 接続のようなセキュアなトランザクション時のユーザー認証（証明書ベースの認証が有効になっている場合）では、Prime Infrastructure は外部エンティティから証明書を受信します。Prime Infrastructure はこれらの証明書を検証して証明書の整合性と証明書の所有者のアイデンティティを確認する必要があります。証明書の検証機能により、ユーザーは他のエンティティから受信した証明書を検証する方法を制御できます。

証明書の検証が適用されると、他のエンティティから受信した証明書は、その証明書が Prime Infrastructure によって信頼されている認証局（CA）が署名している場合にのみ、Prime Infrastructure によって受け入れられます。信頼ストアは、ユーザーが信頼できる CA 証明書を維持できる場所です。署名付き証明書チェーンが信頼ストア内のいずれかの CA 証明書がルートでない場合、検証は失敗します。

信頼ストアの管理

ユーザーは信頼ストア内の信頼できる CA を管理できます。Prime Infrastructure は、さまざまな信頼ストア、つまり、pubnet、system、devicemgmt、および user を提供します。

- pubnet：パブリックネットワーク内のサーバーに接続したときにリモートホストから受信した証明書の検証中に使用されます。
- system：ネットワーク内のシステムに接続したときにリモートシステムから受信した証明書の検証中に使用されます。
- devicemgmt：管理対象デバイスから受信した証明書の検証中に使用されます。
- user：ユーザー証明書の検証に使用されます（証明書ベースの認証が有効になっている場合）。

信頼ストアを管理する *CLI*

次に、信頼ストアを管理するために使用される CLI を示します。

- 信頼ストアへの CA 証明書のインポート （104 ページ）
- 信頼ストアでの CA 証明書の表示 （104 ページ）
- 信頼ストアからの CA 証明書の削除 （104 ページ）

信頼ストアへの CA 証明書のインポート

次に、信頼ストアに CA 証明書をインポートするコマンドを示します。

- ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}

信頼ストアでの CA 証明書の表示

次に、信頼ストアで CA 証明書を表示するコマンドを示します。

- ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt | pubnet | system | user}

信頼ストアからの CA 証明書の削除

次に、信頼ストアから CA 証明書を削除するコマンドを示します。

- ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore {devicemgmt | pubnet | system | user}

証明書の検証の設定

ユーザーは、次のカテゴリに対して証明書の検証を設定できます。

- 証明書の検証の有効化
- 証明書の検証の無効化
- TOFU（ゼロトラスト）：信頼ストアは使用されず、リモートホストから受信した証明書が接続が最初に確立された時点で信頼されます。リモートホストが後続の任意の接続に対して別の証明書を送信すると、接続は拒否されます。

証明書の検証の有効化

次に、証明書の検証を有効にするコマンドを示します。

- ncs certvalidation certificate-check trust-on-first-use trustzone {devicemgmt | pubnet | system | user}

証明書検証リストの表示

次に、証明書検証リストを表示するコマンドを示します。

- ncs certvalidation tofu-certs listcerts

証明書の検証の削除

次に、証明書の検証を削除するコマンドを示します。

- ncs certvalidation tofu-certs deletecert host <host>

CA リストの自動更新

シスコは、シスコが推奨する CA 証明書の標準セットを随時リリースしています。これらの信頼ストアは、ソフトウェアアップデート時にシスコの信頼できる CA バンドルを使用して CA リストを更新するように自動的に設定できます。

次に、CA リストの自動更新を設定するコマンドを示します。

- ncs certvalidation trusted-ca-store auto-ca-update enable truststore {devicemgmt | pubnet | system | user}

[Certificate Validation] ページへのアクセス

証明書は、UI で利用可能な [Certificate Validation] ページから生成可能になったため、管理 CLI コマンドを使用せずに CSR を直接生成して、インポートまたはエクスポートできます。

[Certificate Validation] ページにアクセスするには、次のメニューに移動します。

[Administration] > [Settings] > [Certificate] メニューには、Cisco Prime Infrastructure で証明書を作成、インポート、およびエクスポートするためのオプションがあります。

信頼できる CA と設定：

インポートされた証明書とカテゴリがここにリストされます。

- [System]：システムレベルで PI と他のサーバーとの間で発生する通信を有効にできます。
- [Pubnet]：pubnet レベルで PI と他のサーバーとの間で発生する通信を有効にできます。
- [Device management]：PI と他のサーバー間のデバイス管理通信を有効にできます。
- [User]：PI と他のサーバー間のユーザー通信を有効にできます。

[Certificate Validation]：証明書をインポートまたはエクスポートするときに使用される検証の詳細を選択できます。

ピン留めされた *TOFU* 証明書

PI サーバーと通信する他のサーバーの全 TOFU 証明書が一覧表示されます。

カスタム OCSP レスポンダ

発行日や有効期限などの検証の詳細が提供されます。

MIB と Prime Infrastructure アラート/イベントのマッピング

次の表に、CISCO_WIRELESS_NOTIFICATION_MIB フィールドおよび OID から Prime Infrastructure アラート/イベントへのマッピングの要約を示します。

表 *6 : CISCO_WIRELESS_NOTIFICATION_MIB* から *Prime Infrastructure* アラート/イベントへのマッピング

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationTimestamp	DateAndTime	createTime：NmsAlert eventTime：NmsEvent	アラーム/イベントの作成時刻。
cWNotificationUpdatedTimestamp	DateAndTime	modTime：NmsAlert	アラームの修正時刻。 イベントには修正時刻がありません。
cWNotificationKey	SnmpAdminString	objectId：NmsEvent entityString：NmsAlert	文字列形式の一意のアラーム/イベント ID。

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cwNotificationCategory	CWirelessNotificationCategory	該当なし	イベント/アラームのカテゴリ。値は次のとおりです。 unknown accessPoints adhocRogue clients controllers coverageHole interference contextAwareNotifications meshLinks mobilityService performance rogueAP rrm security wcs switch ncs
cWNotificationSubCategory	OCTET STRING	アラートの Type フィールドおよびイベントの eventType。	このオブジェクトはアラートのサブカテゴリを表します。
cWNotificationServerAddress	InetAddress	該当なし	Prime Infrastructure の IP アドレス。

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationManagedObjectAddressType	InetAddressType	該当なし	管理対象オブジェクトに到達可能なインターネットアドレスの種類。有効値： 0：不明 1：IPv4 2：IPv6 3：IPv4z 4：IPv6z 16：DNS Prime Infrastructure は IPv4 アドレスのみをサポートしているため、常に「1」に設定されます。
cWNotificationManagedObjectAddress	InetAddress	getNode() 値を使用（存在する場合）	getNode はイベントおよび一部のアラートに対して設定されます。ヌルでない場合は、このフィールドに使用されます。
cWNotificationSourceDisplayName	オクテット文字列	アラート/イベントの sourceDisplayName フィールド。	このオブジェクトは、通知の送信元の表示名を表します。
cWNotificationDescription	OCTET STRING	Text：NmsEvent Message：NmsAlert	アラームの説明を示す文字列。
cWNotificationSeverity	INTEGER	severity：NmsEvent、NmsAlert	アラート/イベントのシビラティ（重大度）は以下のとおりです。 cleared(1) critical(3) major(4) minor(5) warning(6) info(7)

フィールド名およびオブジェクト ID	データ タイプ	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationSpecialAttributes	OCTET STRING	基本アラート/イベント クラス以外のすべてのアラート/イベントの属性。	このオブジェクトは、アラート専用の属性（APAssociated、APDisassociated、RogueAPAlert、CoverageHoleAlert など）を表します。文字列は CSV 形式で「プロパティ=値」のペアで表されます。
cWNotificationVirtualDomains	OCTET STRING	該当なし	アラームを発生させたオブジェクトの仮想ドメイン。現行リリースの場合、このフィールドは空です。

サーバーとの SSH セッションの確立

サーバーに接続するときには、admin ユーザーとして SSH を使用してログインします。（詳細については、ユーザー インターフェイス、ユーザー タイプ、およびそれらの間の遷移 （199 ページ）を参照してください）。

ステップ 1 SSH セッションを開き、 admin ユーザーとしてログインします。

- コマンド ラインから次のように入力します。*server-ip* は です。

```
ssh admin server-ip
```

- SSH クライアントを開き、**admin** としてログインします。

（注） ユーザーは、SSH または PuTTY に接続する新しいアルゴリズムを作成してカスタマイズできるようになりました。

ステップ 2 admin パスワードを入力します。プロンプトが次のように変化します。

```
(admin)
```

管理ユーザーが実行できる操作のリストを表示するには、プロンプトで **?** と入力します。

admin コンフィギュレーション モードを開始するには、次のコマンドを入力します（プロンプトの変化に注意してください）。

```
(admin) configure terminal
(config)
```

サーバーでの 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。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。これには、 バックアップに使用する任意のリモート FTP サーバー、セカンダリ 高可用性サーバーなど、すべての 関連サーバーが含まれます。

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。

（注） は NTP サーバーとして設定できません。NTP クライアントとしてだけ機能します。最大で 3 台までの NTP サーバーが使用できます。

ステップ 1 サーバーに管理者ユーザーとしてログインし、コンフィギュレーションモードを開始します。サーバーとの SSH セッションの確立 （109 ページ）を参照してください。

ステップ 2 次の方法のいずれかのコマンドを使用して、NTP サーバーを設定します。

認証されていない NTP サーバーのセットアップの場合：

ntp server *ntp-server-IP*

認証済み NTP サーバーのセットアップの場合：

ntp server *ntp-server-IP ntp-key-id ntp-type password*

ここで、

- *ntp server IP* は、 サーバーにクロック同期を提供するサーバーの IP アドレスまたはホスト名です
- *ntp-key-id* は、認証済み NTP サーバーの MD5 キー ID MD5 キーです。
- *ntp-type* は、プレーンまたはハッシュのいずれかにすることができます。
- *password* は NTPv4 サーバーの MD5 プレーン テキスト パスワードです。

プロキシ サーバーの設定

サーバーのプロキシと、そのローカル認証サーバー（設定されている場合）のプロキシを設定するには、次の手順に従います。ネットワークとインターネットの間のセキュリティ バリアとしてプロキシ サーバーを使用する場合、次の手順に従ってプロキシを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [プロキシ（Proxy）] タブをクリックします。

ステップ 3 [プロキシの有効化（Enable Proxy）] チェックボックスをオンにし、Cisco.com に接続してプロキシとして機能するサーバーに関する必須情報を入力します。

ステップ 4 [認証プロキシ（Authentication Proxy）] チェックボックスをオンにし、プロキシ サーバーのユーザー名とパスワードを入力します。

ステップ 5 [接続のテスト（Test Connectivity）] をクリックして、プロキシ サーバーに接続できることを確認します。

ステップ 6 [Save] をクリックします。

サーバー ポートおよびグローバル タイムアウトの設定

[サーバー（Server）] ページでは、Prime Infrastructure の FTP、TFT、HTTP/HTTPS の各サービスの有効化または無効化ができます。

通常、FTP および TFTP サービスはデフォルトで有効です。HTTP サービスはデフォルトで無効になっています。プラグ アンド プレイ機能を使用し、デバイスが HTTP を使用してブートストラップ設定の初期設定を取得するように設定されている場合は、HTTP サービスを有効にする必要があります。

詳細については、最新の『Prime Infrastructure Quick Start Guide』を参照してください。

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[一般（General）]>[サーバー（Server）] の順に選択します。

ステップ 2 インストール時に確立された FTP、TFTP、または HTTP サービスのステータスとポートを変更するには、変更するポート番号（または必要に応じてポート番号およびルート）を入力し、[有効（Enable）] または [無効（Disable）] をクリックします。

[グローバル アイドル タイムアウト（Global Idle Timeout）] はデフォルトで有効になっており、10 分に設定されています。[グローバル アイドル タイムアウト（Global Idle Timeout）] 設定は、[自分の環境設定（My Preferences）] ページの [ユーザー アイドル タイムアウト（User Idle Timeout）] 設定より優先されます。管理者権限を持つユーザーのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の値を無効化したり、そのタイムリミットを変更できます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 変更を適用するにはサーバーを再起動する必要があります（CLI を使用した Prime Infrastructure の再起動（149 ページ）を参照）。

SMTP 電子メール サーバーの設定

で（アラーム、ジョブ、レポートなどの）電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メールサーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[メールと通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** を選択します。

ステップ 2 [プライマリ SMTP サーバー（Primary SMTP Server）] で、 が使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力し、プライマリ SMTP サーバーのホスト名を入力します。

（注） 仮想 IP アドレスを [ホスト名/IP（Hostname/IP）] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 3 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。SMTP サーバーのユーザー名とパスワード。

ステップ 4 [送信者および受信者（Sender and Receivers）] で、 の正当なメール アドレスを入力します。

ステップ 5 完了したら、[保存（Save）] をクリックします。

サーバーでの FTP/TFTP/SFTP サービスの有効化

FTP/TFTP/SFTP は、デバイス設定およびソフトウェアイメージファイルの管理のために、サーバーとデバイスの間でファイルを転送する目的で使用されます。また、これらのプロトコルは、高可用性導入環境において、セカンダリ サーバーにファイルを転送するためにも使用されます。これらのサービスは、通常はデフォルトで有効になっています。FIPS モードで をインストールした場合、これらはデフォルトで無効になります。このページを使用してこれらのサービスを有効にすると、 は FIPS に準拠しなくなります。

SFTP は、セキュリティで保護されたバージョンのファイル転送サービスです。デフォルトでこれが使用されます。FTP は、セキュリティで保護されていないファイル転送サービス バージョンです。TFTP は、セキュリティで保護されていない、単純なサービス バージョンです。FTP または TFTP のいずれかを使用するには、サーバーの追加後にサービスを有効化する必要があります。

ステップ 1 FTP、TFTP、または SFTP サーバーを使用するように を設定します。

a) **[管理（Administration）] > [サーバー（Servers）] > [TFTP/FTP/SFTP サーバー（TFTP/FTP/SFTP Servers）]** を選択します。

b) [コマンドの選択（Select a command）] ドロップダウン リストから、[TFTP/FTP/SFTP サーバーの追加（Add TFTP/FTP/SFTP Server）] を選択し、[移動（Go）] をクリックします。

- **[サーバータイプ（Server Type）]** ドロップダウンリストから、**[FTP]**、**[TFTP]**、**[SFTP]**、または **[すべて（All）]** を選択します。
- サーバーのユーザー定義名を入力します。
- サーバーの IP アドレスを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 FTP または TFTP を使用する場合には、 サーバーでそれを有効化します。

a) **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。

b) [FTP] または [TFTP] エリアに移動します。

c) [有効（Enable）] をクリックします。

d) **[保存（Save）]** をクリックします。

ステップ 3 を再起動し、変更を適用します。 の停止と再起動 （114 ページ）を参照してください。

保存されている Cisco.com クレデンシャルの設定

では、次のタスクの実行時に Cisco.com にログインするためのユーザー名のみが保存され、パスワードは保存されません。

- 製品ソフトウェア アップデートの有無の確認
- デバイス ソフトウェア イメージ アップデートの有無の確認

アップデートをダウンロードし、サポート ケースを開いたり確認したりするには、パスワードを入力する必要があります。

これらが設定されていない場合、ではユーザーがこれらのタスクを行うと、ユーザーに対してクレデンシャルの入力を求めます。グローバル Cisco.com ユーザー名とパスワードを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [Cisco.com クレデンシャル（Cisco.com Credentials）] タブでユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ログイン バナー（ログインの免責事項）の作成

すべてのユーザーに対してログイン前に表示するメッセージがある場合は、ログインの免責事項を作成します。テキストは GUI クライアント ログイン ページのログイン フィールドとパスワード フィールドの下に表示されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [ログインの免責事項（Login Disclaimer）]** を選択します。

ステップ 2 ログインの免責事項テキストを入力（または編集）します。

（注） 改行文字は無視されます。

変更はすぐに反映されます。

の停止と再起動

製品ソフトウェアのアップグレード、ログファイルの設定変更、セキュアポート設定のハンギング、レポートファイルの圧縮、サービス検出設定の変更、LDAP 設定の構成の後などに、再起動が必要です。 サーバーを停止すると、すべてのユーザー セッションが終了します。

サーバーを停止するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs stop
```

サーバーを再起動するには、サーバーとの CLI セッションを開いて、以下を入力します。

```
ncs start
```

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

[SNMP の設定（SNMP Settings）] ページは、サーバーが SNMP を使用してデバイスにアクセスおよびモニターする方法を制御します。これらの設定によって、デバイスが到達不能であると判断される条件が決まります。このページで行う変更はグローバルに適用され、再起動されても、バックアップと復旧が行われても保存された状態に維持されます。

（注） デフォルトのネットワーク アドレスは 0.0.0.0 です。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[ネットワークとデバイス（Network and Device）] > [SNMP]** を選択します。

ステップ 2 （任意）SNMP を使用して取得されたメディエーション トレース レベル ログのデータ値を表示するには、[トレース表示値（Trace Display Values）] チェックボックスをオンにします。

ステップ 3 [バックオフ アルゴリズム（Backoff Algorithm）] ドロップダウン リストからアルゴリズムを選択します。

- [指数（Exponential）]：SNMP の初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。
- [一定（Constant）]：SNMP の試行時に、毎回同じ待機時間（タイムアウト）が適用されます。このオプションは、必要な再試行回数が多い、不安定なネットワークで役立ちます。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 4 デバイスで指定されているタイムアウトと再試行を使用しない場合は、次のパラメータを設定します。

（注） スイッチ ポート トレースが完了するまでに長い時間がかかる場合は、[到達可能性再試行回数（Reachability Retries）] の値を小さくします。

- [到達可能性再試行回数（Reachability Retries）]：グローバルに適用する再試行回数を入力します。
- [到達可能性タイムアウト（Reachability Timeout）]：グローバルに適用するタイムアウト値を入力します。

ステップ 5 [PDU取得ごとの最大変数バインド（Maximum VarBinds per Get PDU）] フィールドおよび [PDU設定ごとの最大変数バインド（Maximum VarBinds per Set PDU）] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。これらのフィールドを使用することで、SNMP に関連した障害が発生したときに、必要な変更を加えることができます。ネットワークでの PDU フラグメンテーションに問題がある場合は、この数を 50 に減らすと、通常はフラグメンテーションが解消されます。

ステップ 6 必要に応じて [テーブルごとの最大行数（Maximum Rows per Table）] の値を調整します。

ステップ 7 [Save] をクリックします。

グローバル SNMP の設定

[SNMP の設定（SNMP Settings）] ページでは、グローバル SNMP 設定を Prime Infrastructure 用に構成することができます。

このページで行った変更は Prime Infrastructure 全体に影響します。変更は、再起動をまたがって有効であり、バックアップと復元をまたがって有効です。

デフォルトのネットワーク アドレスは 0.0.0.0 です。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 1 [Administration] > [Settings]> [System Settings] > [Network and Device] > [SNMP] の順に選択します。

ステップ 2 （オプション）SNMP を使用しているコントローラから取得したメディエーション トレース レベル ログのデータ値を表示するには、[Trace Display Values] チェック ボックスをオンにします。オフにした場合は、これらの値は表示されません。

ステップ 3 [Backoff Algorithm] から、[Exponential] または [Constant Timeout] を選択します。[指数（Exponential）] を選択した場合、SNMP の初回試行時には指定したタイムアウト値が使用され、2 回目からは、前回の試行時の 2 倍の待機時間が適用されます。[Constant Timeout] を選択した場合は、すべての SNMP 試行に対して同じ待機時間（指定したタイムアウト値）が適用されます。

ネットワークの信頼性が低く、再試行回数が多くなる可能性がある場合（衛星ネットワークなど）は、通常 [Constant Timeout] を使用します。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 4 到達可能性に関するパラメータを使用するかどうかを決定します。オンにした場合は、Prime Infrastructure がデフォルトで、構成されたグローバルな [到達可能性の再試行回数（Reachability Retries）] および [到達可能性のタイムアウト（Reachability Timeout）] に設定されます。オフにした場合は、Prime Infrastructure ではコントローラごと、または IOS アクセス ポイントごとに指定したタイムアウトと再試行が常に使用されます。

スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

ステップ 5 [到達可能性の再試行回数（Reachability Retries）] に、デバイスの到達可能性を判別するためのグローバルな再試行回数を入力します。このフィールドは、[到達可能性パラメータの使用（Use Reachability Parameters）] チェック ボックスをオンにした場合だけ使用できます。

スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

（注） [到達可能性のタイムアウト（Reachability Timeout）] の値は編集できません。デフォルト値は 2 秒です。

ステップ 6 [PDU あたりの最大変数バインド数（Maximum VarBinds per PDU）] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。

この [Maximum VarBinds per PDU] フィールドを使用することで、関連した障害が発生したときに、必要な SNMP の変更を実施できます。

ネットワークでの PDU フラグメンテーションに問題がある場合は、この数を 50 に減らすとフラグメンテーションが解消されます。

テーブルのフィールドごとの最大行数を設定できます。設定した値は、Prime Infrastructure を新しいバージョンにアップグレードしても保持されます。

ステップ 7 [保存（Save）] をクリックして、これらの設定を保存します。

関連トピック

SNMP クレデンシャルの詳細表示 （117 ページ）
SNMP クレデンシャルの追加 （118 ページ）
SNMP クレデンシャルのインポート （119 ページ）

SNMP クレデンシャルの詳細表示

このページに表示される SNMP クレデンシャルは、不正 AP スイッチ ポート トレースにのみ使用されます。

ステップ 1 [Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] の順に選択します。

ステップ 2 [Network Address] リンクをクリックすると、[SNMP Credential Details] ページが表示されます。このページには、次の情報が表示されます。

- General Parameters
  - [フォーマット タイプの追加（Add Format Type）]：表示のみ。詳細については、「関連項目」の「SNMP クレデンシャルの追加」を参照してください。
  - ネットワーク アドレス（Network Address）
  - Network Mask
- [SNMP Parameters]：SNMP パラメータの該当するバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。
- 書き込みアクセスに対応する SNMP パラメータ（存在する場合）を入力します。表示専用のアクセス パラメータでは、スイッチが追加されますが、その設定を Prime Infrastructure では変更できません。デバイス接続テストでは、SNMP 再試行およびタイムアウト パラメータが使用されます。
- [再試行（Retries）]：スイッチの検出を試行する回数。
- [Timeout]：セッション タイムアウト値（秒数）。これは、クライアントに再認証を強制するまでの最大許容時間を指定します。
- [SNMP v1 Parameters or v2 Parameters]：選択した場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters]：選択した場合は、次のパラメータを設定します。
  - ユーザ名
  - Auth. タイプ
  - Auth. パスワード
  - Privacy タイプ

- プライバシー パスワード（Privacy Password）

デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプを使用する、デフォルト ユーザーなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 3 [OK] をクリックして変更を保存します。

関連トピック

グローバル SNMP の設定 （115 ページ）
SNMP クレデンシャルの追加 （118 ページ）
SNMP クレデンシャルのインポート （119 ページ）

SNMP クレデンシャルの追加

Prime Infrastructure がネットワーク デバイスのポーリングやそれらの構成のバックアップおよび変更を実行するには、デバイスの SNMP クレデンシャルが必要です。SNMP クレデンシャルは手動で追加できます。また、それらを一括してインポートすることもできます（詳細については、「関連項目」の「SNMP クレデンシャルのインポート」を参照）。

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します。

ステップ 3 [フォーマット タイプの追加（Add Format Type）] ドロップダウン リストで、[SNMP クレデンシャル情報（SNMP Credential Info）] を選択します。

ステップ 4 追加するスイッチの IP アドレスを入力します。複数のスイッチを追加する場合は、各 IP アドレスの間にカンマを使用します。

ステップ 5 [再試行（Retries）] フィールドに、スイッチの検出を試行する回数を入力します。

ステップ 6 セッション タイムアウト値を秒単位で入力します。この値により、クライアントの再認証が強制されるまでの最大時間が決定されます。

ステップ 7 SNMP パラメータの該当するバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。

- [SNMP v1 Parameters or v2 Parameters] が選択されている場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters] が選択されている場合は、次のパラメータを設定します。
- ユーザ名
- Auth. タイプ
- Auth. パスワード

- Privacy タイプ
- プライバシー パスワード（Privacy Password）

デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプを使用する、デフォルト ユーザーなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 8 [OK] をクリックします。

リストされている SNMP クレデンシャルを使用して Prime Infrastructure がスイッチにアクセスできる場合は、今後使用できるようにスイッチが追加され、[ネットワーク デバイス（Network Devices）] ページに表示されます。このページは、[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] からアクセスできます。[ネットワーク デバイス（Network Devices）] ページから手動でスイッチを追加する場合、スイッチ ポートのトレースではこのページのクレデンシャルが使用され、[SNMP クレデンシャル（SNMP Credentials）] ページにリストされているクレデンシャルは使用されません。手動で追加したスイッチ クレデンシャルが変更されている場合は、[ネットワーク デバイス（Network Devices）] ページを使用してこれらのクレデンシャルを更新する必要があります。

関連トピック

グローバル SNMP の設定 （115 ページ）
SNMP クレデンシャルの詳細表示 （117 ページ）
SNMP クレデンシャルのインポート （119 ページ）

SNMP クレデンシャルのインポート

Prime Infrastructure がネットワーク デバイスのポーリングやそれらの構成のバックアップおよび変更を実行するには、デバイスの SNMP クレデンシャルが必要です。SNMP クレデンシャルは、CSV ファイルからインポートすることで、一括インポートができます。また、それらを手動で追加することもできます（「関連項目」の「SNMP クレデンシャルの追加」を参照）。

CSV ファイルが適切なフォーマットで作成されており、Prime Infrastructure のアクセスに使用するクライアント マシン上のフォルダからアップロード可能であることを確認してください。以下に、インポート用の SNMP クレデンシャル CSV ファイル例を示します。

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,
snmpv3_privacy_type,snmpv3_privacy_password,network_mask 1.1.1.0,v2,private,user1,HMAC-MD5,
12345,DES,12345,255.255.255.0 2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,
255.255.255.0 10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

ファイルの最初の行は、列配置を説明するための必須行です。IP アドレス列も必須です。CSV ファイルには、次のフィールドを含めることができます。

- ip_address：IP アドレス
- snmp_version：SNMP バージョン
- network_mask：ネットワーク マスク
- snmp_community：SNMP V1/V2 コミュニティ

- snmpv3_user_name：SNMP V3 ユーザ名
- snmpv3_auth_type：SNMP V3 認証タイプ。None または HMAC-MD5 または HMAC-SHA を選択できます
- snmpv3_auth_password：SNMP V3 認証パスワード
- snmpv3_privacy_type：SNMP V3 プライバシー タイプ。None または DES または CFB-AES-128 を選択できます
- snmpv3_privacy_password：SNMP V3 プライバシー パスワード
- snmp_retries：SNMP リトライ
- snmp_timeout：SNMP タイムアウト

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します。

ステップ 3 [フォーマット タイプの追加（Add Format Type）] ドロップダウン リストで、[ファイル（File）] を選択します。

ステップ 4 [参照（Browse）] をクリックして、インポートする CSV ファイルに移動し、それを選択します。

ステップ 5 [OK] をクリックしてファイルをインポートします。

リストされている SNMP クレデンシャルを使用して Prime Infrastructure がスイッチにアクセスできる場合は、今後使用できるようにスイッチが追加され、[ネットワーク デバイス（Network Devices）] ページに表示されます。このページは、[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] からアクセスできます。[ネットワーク デバイス（Network Devices）] ページから手動でスイッチを追加する場合、スイッチ ポートのトレースではこのページのクレデンシャルが使用され、[SNMP クレデンシャル（SNMP Credentials）] ページにリストされているクレデンシャルは使用されません。手動で追加したスイッチ クレデンシャルが変更されている場合は、[ネットワーク デバイス（Network Devices）] ページを使用してこれらのクレデンシャルを更新する必要があります。

関連トピック

グローバル SNMP の設定 （115 ページ）
SNMP クレデンシャルの詳細表示 （117 ページ）
SNMP クレデンシャルの追加 （118 ページ）

コンプライアンス サービスの有効化

コンプライアンス サービスにより、Prime Infrastructure ユーザーが Cisco PSIRT セキュリティ レポートおよび EOX 廃止デバイス コンプライアンス レポートを実行できるようになります。

また、この機能により、ベースラインデバイス設定標準の確立、これらの標準に照らした監査領域の設定、非準拠のデバイスおよびそれらの設定の標準からの逸脱状況の特定もユーザが実施可能になります。

コンプライアンス サービスは、デフォルトで無効化されています。これらを使用するには、Prime Infrastructure 管理者が機能を有効化する必要があります。また、サーバーのデバイス インベントリの再同期も必要になります。また、[設定（Configuration）] > [コンプライアンス（Compliance）] メニュー オプションを表示する場合、すべてのユーザーは、ログアウトした後にログインし直す必要があります。

コンプライアンス サービスは、次の Prime Infrastructure サーバー オプションのみで使用可能です。

- Professional 仮想アプライアンス。詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Virtual Appliance Options」および「Understanding System Requirements」のセクションを参照してください。
- Cisco Unified Computing System（UCS）Gen 2 物理アプライアンス。詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Virtual Appliance Options」および「Understand System Requirements」のセクションを参照してください。
- 標準 Prime Infrastructure 仮想アプライアンス詳細については、最新の『Cisco Prime Infrastructure Quick Start Guide』の「Prime Infrastructure Minimum Server Requirements」のセクションを参照してください。

Express、Express-Plus 上でコンプライアンス サービスを有効化しないでください。その場合、機能そのものが動作しません。また、有効化した後、新規にインストールした Professional や Gen 2 UCS アプライアンスにデータを移行すると、元の Express または Express-Plus から移行したデータの設定により、ターゲットのアプライアンス上でコンプライアンス サービスが動作しません。この問題は、Express または Express-Plus 上ではコンプライアンス サービス機能を無効化したままにして、Professional または Gen2 UCS アプライアンスにデータを移行するだけで回避できます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [サーバー（Server）] の順に選択します。

ステップ 2 [Compliance Services] の横にある [Enable] をクリックします。

ステップ 3 [Save] をクリックします。

ステップ 4 Prime Infrastructure のデバイス インベントリを再同期します。手順としては、[Inventory] > [Network Devices] の順に選択し、[All Devices] を選択した後、[Sync] アイコンをクリックします。

ステップ 5 現在 Prime Infrastructure にログインしているユーザにログアウトするよう求めます。再度ログインすると、[設定（Configuration）] > [コンプライアンス（Compliance）] の新しいメニュー オプションが表示されます。

詳細については、「Virtual Appliance Options」と「Physical Appliance Options」を参照してください。

ISE サーバーの設定

ステップ 1 [管理（Administration）] > [サーバー（Servers）] > [ISE サーバー（ISE Servers）] を選択します。
ステップ 2 [Select a command] > [Add ISE Server] を選択し、[Go] をクリックします。
ステップ 3 ISE サーバの IP アドレス、ユーザ名、およびパスワードを設定します。
ステップ 4 ISE サーバのパスワードを確認入力します。
ステップ 5 [Save] をクリックします。

ソフトウェア イメージ管理サーバーを設定する

イメージの配布のため、最大 3 台のソフトウェア イメージ管理サーバーを追加できます。

ステップ 1 [管理（Administration）] > [サーバー（Servers）] > [ソフトウェア イメージ（Software Image）] をクリックします。
ステップ 2 [追加（Add）] アイコンをクリックし、次のフィールドに値を入力します。

- サーバー名（Server Name）
- [IPアドレス（IP Address）]
- 対象サイト（Sites Served）
- 説明

ステップ 3 [保存（Save）] をクリックします。
ステップ 4 [プロトコルの管理（Manage Protocols）] をクリックしてプロトコルを追加します。
ステップ 5 [追加（Add）] アイコンをクリックし、次のフィールドに値を入力します。

- プロトコル
- [ユーザ名（Username）]
- パスワード
- プロトコル ディレクトリ（Protocol Directory）

（注） TFTP プロトコルを選択した場合は、[プロトコル ディレクトリ（Protocol Directory）] フィールドに、先頭にスラッシュを付けずに相対パスを入力します。[プロトコルディレクトリ（Protocol Directory）] フィールドを空にした場合は、イメージ転送で外部サーバーのデフォルトのホームディレクトリが使用されます。

ステップ 6 [Save] をクリックします。

ユーザー定義フィールドにデバイス情報を追加する

ユーザー定義フィールド（UDF）は、デバイスのロケーション属性（たとえば、エリア、施設、フロア）など、デバイスに関する追加情報を格納するために使用されます。新しいデバイスの追加、インポート、またはエクスポートが行われるたびに、UDF 属性が使用されます。

ステップ 1 [Administration] > [System Settings] > [Inventory] > [User Defined Field] の順に選択します。

ステップ 2 UDF を追加するには、[行の追加（Add Row）] をクリックします。

ステップ 3 フィールド ラベルおよび説明を対応するフィールドに入力します。

ステップ 4 [保存（Save）] をクリックして UDF を追加します。

OUI を管理する

Prime Infrastructure では、IEEE 組織固有識別子（OUI）データベースを使用してクライアントベンダー名マッピングが識別されます。Prime Infrastructure では、ベンダー OUI マッピングは、vendorMacs.xml という名前の XML ファイルに保存されます。このファイルは、Prime Infrastructure のリリースごとに更新されます。OUI 更新を使用すると、既存の OUI のベンダー表示名を変更したり、新しい OUI を Prime Infrastructure に追加したり、新しいベンダー OUI マッピングで vendorMacs.xml ファイルを更新し、Prime Infrastructure にアップロードしたりできます。

関連トピック

新しいベンダー OUI マッピングの追加 （123 ページ）
更新されたベンダー OUI マッピング ファイルのアップロード （124 ページ）

新しいベンダー OUI マッピングの追加

[ユーザー定義 OUI リスト（User Defined OUI List）] ページに、作成したベンダー OUI マッピングのリストが表示されます。このページで、新しいベンダー OUI マッピングの追加、OUI エントリの削除、および vendorMacs.xml ファイルに存在する OUI のベンダー名の更新を実行できます。

OUI を追加すると、Prime Infrastructure は vendorMacs.xml ファイルを調べて OUI があるかどうかを確認します。OUI がある場合、Prime Infrastructure は OUI のベンダー名を更新します。OUI がない場合、Prime Infrastructure はベンダー OUI マッピングに新しい OUI エントリを追加します。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントおよびユーザー（Client and User）] > [ユーザー定義 OUI（User Defined OUI）] の順に選択します。[ユーザー定義 OUI（User Defined OUI）] ページが表示されます。

ステップ 2 [Select a Command] ドロップダウン リストから [Add OUI Entries] を選択し、[Go] をクリックします。

ステップ 3 [OUI] フィールドに有効な OUI を入力します。形式は aa:bb:cc です。

ステップ 4 [Check] をクリックして、OUI がベンダー OUI マッピングに存在するかどうかを確認します。

ステップ 5 [Name] フィールドに、OUI のベンダーの表示名を入力します。

ステップ 6 [ベンダー名の変更（Change Vendor Name）] チェックボックスをオンにしてから [OK] をクリックし、OUI がベンダー OUI マッピングに存在する場合にはベンダーの表示名が更新されるようにします。

更新されたベンダー OUI マッピング ファイルのアップロード

Prime Infrastructure を使用すると、IEEE 登録局データベースからオンラインで OUI アップデートを取得できます（「関連項目」の RA データベースのリンク参照）。Prime Infrastructure が IEEE データベースに到達できない場合、メッセージが表示され、ファイルを保存して Prime Infrastructure サーバーにアップロードするよう指示されます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントおよびユーザー（Client and User）] > [OUI のアップロード（Upload OUI）] の順に選択します。[Upload OUI From File] ページが表示されます。

ステップ 2 [IEEE からオンラインでアップロード（Update online from IEEE）] をクリックして、IEEE 登録局データベースから OUI アップデートを取得します（「関連項目」の RA データベースのリンク参照）。Prime Infrastructure が IEEE データベースに到達できない場合、メッセージが表示され、ファイルを保存してアップロードするよう指示されます。

ステップ 3 アップデートが正常に終了したら、[OK] をクリックします。

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [OUI のアップロード（Upload OUI）] ページで vendorMacs.xml ファイルをアップロードした後、[一意のクライアントとユーザーの概要（Unique Clients and Users Summary）] レポートで既存の不明ベンダー クライアントにベンダー名が反映されていない場合は、*updateUnknownClient.sh* スクリプトを実行します。このスクリプトは、/opt/CSCOlumos/bin フォルダにあります。

詳細については、「IEEE Registration Authority database」を参照してください。

ノースバウンド SNMP レシーバのログ ファイル例

以下の出力例に、Prime Infrastructure によって生成された *ncs_nb.log* ファイルを示します。このログ ファイルは、Prime Infrastructure サーバーのログ ファイル ディレクトリ（/opt/CSCOlumos/logs）にあります。ログ出力は、アラームを North Bound SNMP レシーバで受信していない場合のトラブルシューティングに役立ちます。

```
2013-12-02 17:11:53,868 [main] INFO  services - Queue type is order
2013-12-02 17:11:53,870 [main] INFO  services - Starting the notification thread..
2013-12-02 17:11:53,871 [NBNotifier] INFO  services - Fetching the head of the queue
```

```
2013-12-02 17:11:53,871 [NBNotifier] INFO  services - The Queue is empty
2013-12-02 17:11:53,871 [main] INFO  notification - Setting the NB process flag
2013-12-02 17:41:50,839 [Task Scheduler Worker-10] ERROR notification - Unable to get
OSS list
2013-12-03 08:22:39,227 [main] INFO  services - Queue type is order
2013-12-03 08:22:39,229 [main] INFO  services - Starting the notification thread..
2013-12-03 08:22:39,231 [NBNotifier] INFO  services - Fetching the head of the queue
2013-12-03 08:22:39,231 [NBNotifier] INFO  services - The Queue is empty
2013-12-03 08:22:39,231 [main] INFO  notification - Setting the NB process flag
2013-12-03 08:44:40,287 [main] INFO  services - Queue type is order
2013-12-03 08:44:40,289 [main] INFO  services - Starting the notification thread..
2013-12-03 08:44:40,290 [NBNotifier] INFO  services - Fetching the head of the queue
2013-12-03 08:44:40,290 [NBNotifier] INFO  services - The Queue is empty
2013-12-03 08:44:40,290 [main] INFO  notification - Setting the NB process flag
2013-12-03 08:56:18,864 [Task Scheduler Worker-8] ERROR notification - Unable to get OSS
 list
```

システムの問題を示すサーバー内部 SNMP トラップの使用

は、システム コンポーネントに関する潜在的な問題を示す内部 SNMP トラップを生成します。これには、ハードウェア コンポーネントの障害、ハイ アベイラビリティ状態の変化、バックアップ ステータスなどが含まれます。障害トラップは、障害または状態の変化が検出されるとすぐに生成され、クリアリング トラップは、障害が修正されると生成されます。TCA（CPU、メモリ、ディスクの高い使用率に関するトラップなど）では、しきい値を超えるとトラップが生成されます。

サーバーの内部 SNMP トラップの完全なリストについては、『』に記載されています。 は通知宛先のポート 162 にトラップを送信します。このポートは現時点ではカスタマイズできません。

以下のトピックの説明に従って、これらのトラップをカスタマイズしたり、管理したりできます。

- サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送 （125 ページ）
- サーバー内部 SNMP トラップをトラブルシュートする （126 ページ）

サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送

トラップのシビラティ（重大度）または（TCA の場合）しきい値を調整することで、サーバの内部 SNMP トラップをカスタマイズできます。また、トラップを無効化/有効化することもできます。サーバーの内部 SNMP トラップは、「*Cisco Evolved Programmable Network* でサポートされているアラーム」で確認できます。

（注） は SNMPv2 通知も SNMPv3 通知も送信しません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）] > [システム イベントの設定（System Event Configuration）]** を選択します。

ステップ 2 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントのシビラティ（重大度）（Event Severity）] を [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、およびメモリの使用率や、その他のハードウェアのトラップに対しては、[しきい値値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。（しきい値設定が NA と表示されるイベントのしきい値は設定できません）。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) バックアップしきい値と証明書の有効期日（重要）に対しては、[しきい値値（Threshold）] に日数（*x* ～ *y*）を入力します。ここで、*x* は最小の日数、*y* は最大の日数です。

e) トラップを生成するかどうかを制御するには、[イベントステータス（Event Status）] を設定します。

ステップ 3 **[その他の設定（Other Settings）]** で、**[アラーム反復の作成とクリア（Create and Clear Alarm Iteration）]** に必要な値を入力します。

ステップ 4 トラップの変更内容を保存するには、（テーブルの下にある）[保存（Save）] をクリックします。

ステップ 5 サーバーの内部 SNMP トラップの受信者を設定するには、情報を電子メールで送信するか、トラップ通知として送信するかに応じて、以下のトピックで説明している手順を参照してください）。

サーバー内部 SNMP トラップをトラブルシュートする

「」では、サーバーの内部 SNMP トラップの完全なリスト、その推定原因、および問題を解決するための推奨処置が提供されています。必要な情報がこのドキュメントに記載されていない場合は、次の手順に従って、サーバーの問題をトラブルシュートし、詳細情報を入手してください。

ステップ 1 サーバーから通知に ping を実行し、 と管理アプリケーション間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して にログインします。**Administration > Logging** を選択してログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

- ncs_nbi.log：これは が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これはその他の最新の アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。

- hm-#-#.log：これはすべてのヘルス モニター アクティビティのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポート ケースを開き、疑わしいログ ファイルをケースに添付してください。シスコ サポート ケースの登録（300 ページ）を参照してください。

シスコサポート リクエストのデフォルトの設定

デフォルトでは、 GUI のさまざまな部分からシスコサポート リクエストを作成できます。必要に応じて、送信者の電子メールアドレスやその他の電子メールの特性を設定できます。これらを設定しない場合、ユーザーがケースを登録するときに情報を入力できます。

ユーザーが GUI クライアントからリクエストを作成できないようにするには、その機能を無効にします。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [サポート リクエスト（Supporte Request）] タブをクリックします。

ステップ 3 必要なインタラクション タイプを選択します。

- [サーバーから直接インタラクションを有効にしてください（Enable interactions directly from the server）]：サーバーから直接サポート ケースを作成する場合は、このオプションを指定します。サポート プロバイダーへの電子メールは、 サーバーに関連付けられているメール アドレス、または指定したメール アドレスから送信されます。
- [クライアントシステムを介したインタラクションのみ（Interactions via client system only）]：サポート ケースに必要な情報をクライアント マシンにダウンロードする場合は、このオプションを指定します。この場合、ダウンロードしたサポート ケースの詳細および情報をサポート プロバイダーに電子メールで送信する必要があります。

ステップ 4 テクニカル サポート プロバイダーを選択します。

- [Cisco] をクリックし、シスコ テクニカル サポートにサポート ケースを登録し、各自の Cisco.com クレデンシャルを入力し、[接続のテスト（Test Connectivity）] をクリックして次のサーバーへの接続を確認します。
  - メール サーバー
  - シスコ サポート サーバー
  - フォーラム サーバー

- [サードパーティ サポート プロバイダー（Third-party Support Provider）] をクリックして、サードパーティ サポート プロバイダーへのサービス要求を作成します。プロバイダーの電子メールアドレス、件名、Web サイト URL を入力します。

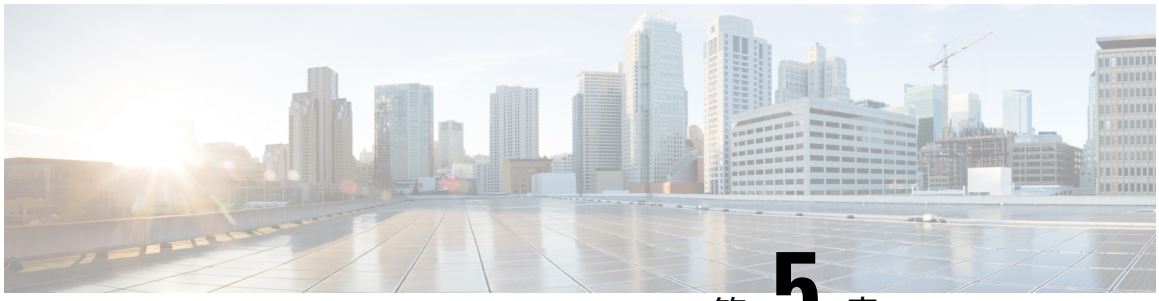
シスコ製品フィードバックの設定

シスコ製品の向上のために、 は以下のデータを収集してシスコに送信します。

- 製品情報：製品タイプ、ソフトウェア バージョン、インストール済みライセンス。
- システム情報：サーバーのオペレーティング システムおよび利用可能なメモリ。
- ネットワーク情報：ネットワーク上のデバイスの数とタイプ。

この機能はデフォルトでイネーブルになっています。データは日単位、週単位、または月単位で収集され、HTTPS を使用してシスコ クラウドの REST URL に送信されます。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（General）] > [改善にご協力ください（Help Us Improve）]** を選択します。

- シスコが収集するデータの種類を確認するには、[シスコが収集するデータについて（What data is Cisco collecting?）] をクリックします。
- この機能を無効にするには、[今回は協力しない（Not at this time, thank you）] を選択し、[保存（Save）] をクリックします。



第 5 章

Prime Infrastructure サーバーの状態の維持

概要ダッシュボード

次の表は、[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム モニタリング ダッシュボード（System Monitoring Dashboard）] > [概要（Overview）] ダッシュボードに表示される情報の内容です。

表 7 : [管理（*Administration*）] > [ダッシュボード（*Dashboards*）] > [システム モニタリング ダッシュボード（*System Monitoring Dashboard*）] > [概要（*Overview*）] の情報

表示する情報	使用するダッシュレット
PI サーバーのハードウェアおよびソフトウェア サーバーの詳細。	システム情報（System Information）
CPU/メモリ/ディスクの使用率における経時変化	ライブ トレンド情報（Live Trend Information）
選択された期間のデータ クリーンアップ ジョブのステータス。	データのクリーンアップ（Data Cleanup）
バックアップ ジョブのステータス、使用可能なサーバー バックアップ、および選択された期間のサーバー バックアップに関するアラーム。	バックアップ情報（Backup Information）

表示する情報	使用するダッシュレット
設定しきい値限界を示す合計メモリとスワップ メモリ使用率。また、しきい値を超えると、メモリを使用しているスレッドに関する情報が表示されます。	メモリ使用率（Memory Utilization）
CPU 使用率と、設定されているしきい値の限度。また、しきい値を超えると CPU の消費量が増える、Prime Infrastructure 内で動作中のプロセスとジョブに関する情報を提供します。	CPU 使用率（CPU Utilization）
ディスク使用率と、設定されているしきい値の限度。また、しきい値を超えると、ディスクを使用しているファイルとテーブルスペースに関する情報が表示されます。	ディスク使用率（Disk Utilization）
[仮想ドメインの概要（Virtual Domain Summary）]：概要アイコンをクリックすると、仮想ドメインとユーザーの関連付けが表示されます。仮想ドメインと関連付けのないメンバーも表示されます。これにより、それぞれの関連付けの一覧をエクスポートできます。	仮想ドメインの概要（Virtual Domain Summary）
使用可能なディスク スペース。	ディスク統計（Disk Statistics）
選択された期間の成功復元情報、バックアップ名、および復元時間。	情報の復元（Restore Information）

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [システム イベント設定（System Event Configuration）] を選択して、CPU/ディスク/メモリ使用率のしきい値の限度を設定し、アラーム生成およびクリアランス モニターを設定します。

関連トピック

パフォーマンス ダッシュボード （130 ページ）
管理ダッシュボード （131 ページ）

パフォーマンス ダッシュボード

次の表に、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [システム モニタリング ダッシュボード（System Monitoring Dashboard）] > [パフォーマンス（Performance）]** ダッシュボードに表示される情報を示します。

表 *8 :[*管理（*Administration***）*]>[*ダッシュボード（***Dashboards***）*]>[*システム モニタリング ダッシュボード（***System Monitoring Dashboard***）*]>[*パフォーマンス（***Performance***）*]* の情報**

表示する情報	使用するダッシュレット
設定した収集時間内に受信した Syslog。	Syslog
設定した収集時間内に受信したトラップ。	トラップ

表示する情報	使用するダッシュレット
設定した収集時間内のディスクの読み書き。	システム ディスク スループット（System Disk Throughput）
サーバーに発行された1秒あたりの読み取り/書き込み要求の数。	システム ディスクス IOP（System Disk IOPS）
サーバー キューで待機している要求の数。	システム ディスク未処理 I/O（System Disk Outstanding I/O）
eth0、eth1、I/O インターフェイスなどの使用可能なネットワーク インターフェイスを通過しているトラフィックに基づいた、現在のデータの転送速度。	ネットワーク インターフェイス トラフィック（Network Interface Traffic）
CPU 使用率、ディスク使用率、およびメモリ使用量の集合的な情報。	複合ビュー（Composite View）

管理ダッシュボード

次の表に、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[システム監視ダッシュボード（System Monitoring Dashboard）]** > **[管理（Admin）]** ダッシュボードに表示される情報の説明を示します。

表 *9: [*管理ダッシュボード（*Administration Dashboards*）*][*システム監視ダッシュボード（*System Monitoring Dashboard*）*][*管理情報（*Admin Information*）*]*

表示する情報	選択するタブ	参照するダッシュレット
Prime Infrastructure サーバ自体に発行されたアラームとイベント。イベントのリスト、イベントの発生日時、およびシビラティ（重大度）を含む。	ヘルス（Health）	システム アラーム（System Alarms）
スケジュールされたジョブ数や実行中のジョブ数などの Prime Infrastructure サーバーの一般的なヘルス統計情報、サポートされている MIB 変数の数、サーバーのポーリングの実行時間、およびログインしているユーザー数。		システム情報（System Information）
デバイス インベントリ（「ライフサイクル クライアント（Lifecycle Clients）」）の検出時にデータが取得される Prime Infrastructure サーバー データベースの相対的割合、現在のステータスとパフォーマンス データ（「ライフサイクル統計（Lifecycle Statistics）」）、およびサーバー独自のシステム データ（「インフラストラクチャ（Infrastructure）」と「DB-Index」）。		DB 使用状況（DB Usage Distribution）

表示する情報	選択するタブ	参照するダッシュレット
Prime Infrastructure サーバーが、デバイスの到達可能性、アラーム、イベントなどの情報に対するユーザー サービス要求に応答する速度。クライアント サービスの基礎となる API ごとの最大、最小、および平均応答時間を示します。	API Health	API の応答時間の概要（API Response Time Summary）
Prime Infrastructure サーバーがユーザー サービス要求に応答する速度の一定期間の傾向。	サービスの詳細	API の応答時間の傾向（API Response Time Trend）
発行されたサービス要求数で測定される、ログインした Prime Infrastructure ユーザーごとの活動レベル。		クライアントあたりの API 呼び出しチャート（API Calls Per Client Chart）
ログインしたクライアントが発行したサービス要求数の合計の一定期間の傾向。		API リクエスト カウントの傾向（API Request Count Trend）

OVA サイズとシステム リソースの評価方法

Prime Infrastructure システム実装は、『Cisco Prime Infrastructure Quick Start Guide』の「System Requirements」の項に記載されている適切な OVA サイズに関する推奨事項に従う必要があります（「関連項目」を参照）。

『*Quick Start Guide*』に記載されているデバイス、インターフェイス、およびフロー レコードの制限値はすべて最大値であることに注意してください。特定のサイズの OVA は、このデバイス数、インターフェイス数、および秒単位のフロー数を超えないように調整されています。また、RAM、ディスク領域、およびプロセッサに関するシステム要件がすべて最小値であることにも注意してください。これらのリソースのいずれかを増やすことによって、より多くのデータをより長い期間保存したり、より迅速に入力フローを処理したりできます。

ネットワークが拡大するにつれて、OVA に関するデバイス/インターフェイス/フローの最大指標に近付きます。この変化はときどきチェックする必要があります。これは、「Prime Infrastructure ヘルスのモニタリング」にも記載されているように、Admin ダッシュボードで入手可能な情報を使用することによってチェックできます。

Prime Infrastructure が、システム リソースの 80 % 以上を使用している、または、インストールされた OVA のサイズに関する推奨デバイス/インターフェイス/フロー数を消費していることが判明した場合は、必要に応じて次のアプローチのいずれかを使用してこれに対処することをお勧めします。

- 「Prime Infrastructure データベースの圧縮」の手順に従って、できるだけ多くの既存のディスク領域を回復します。
- ディスク領域を追加します。VMware OVA テクノロジーを使用すれば、簡単に既存のサーバーのディスク領域を増やすことができます。物理ディスク領域を拡張する場合は、先に Prime Infrastructure サーバーをシャット ダウンし、VMware から提供される手順に従う必要があります（「関連項目」の「VMware vSphere documentation」を参照）。仮想アプライ

アンスを再起動すると、Prime Infrastructure が、自動的に、追加されたディスク領域を使用します。

- 収集を制限します。Prime Infrastructure によって収集可能なすべてのデータが役に立つわけではありません。たとえば、無線パフォーマンス統計情報の報告システムを使用していない場合は、そのデータを収集または保存する必要がないため、Radio Performance 収集タスクを無効にできます。また、集約後の Radio Performance データだけが必要な場合は、未加工のパフォーマンスデータの保持を無効にできます。この方法の詳細については、「カテゴリ別のデータ保持の指定」を参照してください。
- 保持期間を短縮します。Prime Infrastructure は、デフォルトで、維持するすべてのデータと生成するレポートにとって十分な保持期間を設定します。これらの一部が必要以上の期間であることが判明して、悪影響が出ないようにそれらを短縮できる場合があります。この方法の詳細については、「レポートの保存および保持の制御」、「カテゴリ別のデータ保持の指定」、「データベース テーブル別のデータ保持の指定」を参照してください。
- バックアップとレポートの負荷を軽減します。レポートとバックアップをリモート サーバーに保存することによって、Prime Infrastructure サーバー上のスペースを節約できます。詳細については、「リモート バックアップ リポジトリの使用」を参照してください。
- 新しいサーバに移行します。現在よりも 1 つ上のレベルの物理または仮想アプライアンスの RAM、ディスク領域、およびプロセッサの最小要件を満たす新しいサーバをセットアップします。既存のシステムをバックアップして、より高いレベルのサーバー上の仮想マシンに復元します。詳細については、「バックアップと復元を使用した別の OVA への移行」を参照してください。

詳細については、「System Requirements」、『Cisco Prime Infrastructure Quick Start Guide』、および『VMware vSphere Documentation』を参照してください。

関連トピック

概要ダッシュボード （129 ページ）
Prime Infrastructure データベースの圧縮 （136 ページ）
データ保持設定が Web GUI データに及ぼす影響 （169 ページ）
データベース テーブル別のデータ保持の指定 （174 ページ）
レポートの保存と保持の制御 （177 ページ）
リモート バックアップ リポジトリの使用 （60 ページ）
バックアップと復元を使用した別の仮想アプライアンスへの移行 （73 ページ）

Prime Infrastructure が管理しているデバイスの数の表示

Prime Infrastructure が管理しているデバイスとインターフェイスの総数を確認するには、**[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）]** を選択します。

システムのディスク容量の総使用量を確認するには、**[管理（Administration）] > [設定（Settings）] > [アプライアンス（Appliance）]** を選択してから、[アプライアンス ステータス（Appliance Status）] タブをクリックします。次に、[インベントリ（Inventory）] の下の [ディスク使用率（Disk Usage）] を展開します。

関連トピック

OVA サイズとシステム リソースの評価方法 （132 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

Prime Infrastructure のパフォーマンスを向上させる方法

Prime Infrastructure の速度と拡張性は、いくつかの手法で向上できます。

関連トピック

サーバーの調整 （134 ページ）
Prime Infrastructure データベースの圧縮 （136 ページ）
クライアント パフォーマンスの設定 （136 ページ）
保証処理のメモリ最適化 （141 ページ）
保証メモリ割り当てと需要のモニタリング （142 ページ）

サーバーの調整

Prime Infrastructure サーバーとその仮想マシン（または VM）に割り当てる RAM、CPU、およびディスク領域の量を増やすことによって、Prime Infrastructure のパフォーマンスと拡張性を向上させることができます。

サーバーを適切に調整するには、次のワークフローを実行する必要があります。

1. VM の変更には失敗のリスクが伴います。VM に変更を加える前にアプリケーション バックアップを作成してください（詳細については、「関連項目」の「Web GUI を使用した即時アプリケーション バックアップの実行」を参照）。
2. VM でリソース変更を実行してから、VM とサーバーを再起動します（「VMware vSphere クライアントを使用して VM のリソース割り当てを変更する」を参照）。

関連トピック

VMware vSphere クライアントを使用した VM のリソース割り当ての変更 （134 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）
Web GUI を使用した即時アプリケーション バックアップの実行 （68 ページ）

VMware vSphere クライアントを使用した VM のリソース割り当ての変更

次の手順を使用して、仮想アプライアンスの RAM、CPU、またはディスク領域リソースの割り当てを変更します。

この種の変更を試みる前に、Prime Infrastructure サーバーのバックアップを実行してください（「関連項目」の「Prime Infrastructure のバックアップおよび復元」を参照）。

インストール後に RAM、CPU、またはディスク領域リソースの割り当てを拡張した場合、コンプライアンス サービス機能は動作しない点に注意してください。

ヒント　パフォーマンスを向上させるために：Prime Infrastructure を実行する仮想マシンの RAM および CPU リソースの割り当てを使用する際、同じハードウェアで実行する仮想マシンが複数ある場合は、vSphere クライアントの [リソース割り当て（Resource Allocation）] タブを使用して、RAM および CPU リソース予約も変更することを推奨します。詳細については、「関連項目」の「VMware vSphere documentation」を参照してください。

ステップ 1　Prime Infrastructure サーバーとの CLI セッションを開きます（「CLI 経由の接続」を参照）。

ステップ 2　**ncs stop** コマンドを使用して Prime Infrastructure を停止します（「Prime Infrastructure の停止」を参照）。

ステップ 3　VMware 仮想アプライアンスを停止します。

PIServer/admin# **halt**

ステップ 4　vSphere クライアントを起動して、仮想アプライアンスを右クリックしてから、[設定の編集（Edit Settings）] をクリックします。

ステップ 5　RAM の割り当てを変更するには、[Memory] を選択し、必要に応じて、[Memory Size] を変更します。次に [OK] をクリックします。

ステップ 6　CPU の割り当てを変更するには、[CPUs] を選択して、ドロップダウン リストから [Number of Virtual Processors] を選択します。次に [OK] をクリックします。

ステップ 7　新しいディスクを追加するには、次の手順を実行します（既存ディスクの領域を拡張することはできません）。

a) [Add] をクリックします。
b) [Hard Disk] を選択して、[Next] をクリックします。
c) [Create a new virtual disk] をオンにしてから、[Next] をクリックします。
d) 必要な [Disk Size] を入力して、新しい仮想ディスクの [Location] を指定し、[Next] をクリックします。
e) [詳細オプション（Advanced Options）] が表示されたら、[次へ（Next）] をクリックして、[完了（Finish）] をクリックします。

ステップ 8　仮想アプライアンスの電源をオンにします（「Prime Infrastructure の再起動」を参照）。

詳細については、「Prime Infrastructure のバックアップおよび復元」および「VMware vSphere Documentation」を参照してください。

（注） Cisco Prime Infrastructure は、1 Gbps ポートのみを使用してインストールされます。10 Gbps ポートを無効にし、1 Gbps ポートを使用して Prime Infrastructure をインストールするには、次の手順を実行します。

1. **CIMC コンソール**にログインします。
2. [コンピューティング（Compute）] > [BIOS] > [BIOSの設定（Configure BIOS）] > [詳細設定（Advanced）] > [LOMおよびPCIeスロットの設定（LOM and PCIe Slots Configuration）] に移動します。
3. [PCIeスロット：MLOMオプションROM（PCIe Slot:MLOM OptionROM）] および [PCIeスロット：MLOMリンク速度] ドロップダウンリストから [無効（Disabled）] オプションを選択します。
4. [保存（Save）] ボタンをクリックします。
5. [ホストの電源（Host Power）] に移動し、マシンの電源を再投入してオンにします。

関連トピック

CLI から接続する方法 （147 ページ）
Prime Infrastructure の停止 （149 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

Prime Infrastructure データベースの圧縮

Prime Infrastructure データベースを圧縮することによって、ディスク領域を再利用できます。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（「関連項目」の「CLI 経由の接続」を参照）。

ステップ 2 次のコマンドを入力して、アプリケーション データベースを圧縮します。

PIServer/admin# **ncs cleanup**

ステップ 3 プロンプトが表示されたら、ディープ クリーンアップ オプションに対し [はい（Yes）] を選択します。

関連トピック

CLI から接続する方法 （147 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

クライアント パフォーマンスの設定

多くのクライアント プロセスを設定することで、Prime Infrastructure のパフォーマンスと拡張性を向上させることができます（「関連項目」を参照）。

関連トピック

自動クライアント トラブルシューティングの有効化 （137 ページ）
DNS ホスト名ルックアップの有効化 （138 ページ）
クライアント アソシエーション履歴データの保持期間の指定 （138 ページ）
クライアント トラップ/Syslog 受信中のクライアントのポーリング （139 ページ）
イベントとしてのクライアント トラップの保存 （139 ページ）
802.1x および 802.11 クライアント トラップのイベントとしての保存 （140 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

自動クライアント トラブルシューティングの有効化

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントとユーザー（Client and User）] > [クライアント（Client）] ページでは、Cisco Compatible Extensions（CCX）を実行しているサードパーティ製ワイヤレス クライアントに対して、診断チャネルによる自動クライアント トラブルシューティングを有効にできます。

この機能が有効になっている場合、Prime Infrastructure は client ccx test-association トラップを処理し、それによって各 CCX クライアントに対して一連のテストが呼び出されます。すべてのタスクが完了した時点でクライアントが更新され、自動トラブルシューティング レポートが生成されます（dist/acs/win/webnms/logs に配置されます）。テストが完了するたびに、クライアント詳細情報ページ、V5 または V6 タブ、および [Automated Troubleshooting Report] エリアでテスト ログの場所が更新されます。ログをエクスポートするには、[エクスポート（Export）] をクリックします。

この機能が有効になっていない場合、Prime Infrastructure はトラップを処理しますが、自動トラブルシューティングは開始されません。

自動クライアント トラブルシューティングは、CCX バージョン 5 または 6 を実行しているクライアントのみ使用できます。CCX 認定パートナー メーカーと CCX クライアント デバイスのリストについては、下記の「関連項目」のリンクから「Cisco Compatible Extensions クライアントデバイス」のページを参照してください。

ステップ 1 [Administration] > [Settings] > [System Settings] > [Client and User] > [Client] の順に選択します。[クライアント（Client）] ページが表示されます。

ステップ 2 [プロセス診断トラップ（Process Diagnostic Trap）] エリアで、[診断チャネルのクライアントを自動的にトラブルシューティング（Automatically troubleshoot client on diagnostic channel）] チェックボックスをオンにして、[保存（Save）] をクリックします。詳細については、「Cisco Compatible Extensions クライアント デバイス」のページを参照してください。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

DNS ホスト名ルックアップの有効化

DNS ルックアップには膨大な時間がかかるため、Prime Infrastructure ではデフォルトでこの機能が無効になっています。

クライアント ホスト名の DNS ルックアップを有効または無効にしたり、Prime Infrastructure が以前の DNS ルックアップの結果をキャッシュに保持する期間を変更したりできます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントとユーザー（Client and User）] > [クライアント（Client）] の順に選択します。

ステップ 2 [DNS サーバーからのクライアント ホスト名のルックアップ（Lookup client host names from DNS server）] チェックボックスをオンにします。

ステップ 3 ホスト名をキャッシュに保持しておく日数を入力して、[保存（Save）] をクリックします。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

クライアント アソシエーション履歴データの保持期間の指定

クライアントアソシエーション履歴は、多くのデータベース領域およびディスク領域を使用する場合があります。これは、データベースのバックアップおよび復元機能において、問題となる場合があります。クライアントアソシエーション履歴の保持期間を設定して、この潜在的な問題を管理しやすくすることができます。

ステップ 1 [Administration] > [Settings] > [System Settings] > [Client and User] > [Client] の順に選択します。

ステップ 2 [データ保存（Data Retention）] で、必要に応じて次のパラメータを変更します。

- [関連付けが解除されたクライアント（Dissociated Clients）]：Prime Infrastructure でデータを保持する日数を入力します。有効な範囲は 1 ～ 30 日です。
- [クライアント セッション履歴（Client session history）]：Prime Infrastructure でデータを保持する日数を入力します。有効な範囲は 7 ～ 365 日です。
- [維持する行数（Number of Rows To Keep）]：維持するクライアント セッション レコードの最大数を入力します。デフォルトは 8,000,000 です。

ステップ 3 **[保存（Save）]** をクリックします。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

クライアント トラップ/Syslog 受信中のクライアントのポーリング

通常の環境で、Prime Infrastructure は、数分単位で定期的にクライアントをポーリングして、その間のセッション情報を特定します。また、Prime Infrastructure に、トラップや Syslog の受信直後にクライアントをポーリングするように指示することもできます。これは、新しいクライアントとそのセッションを迅速に検出するのに役立ちます。

このオプションは、Prime Infrastructure のパフォーマンスに影響を与える可能性があるため、デフォルトで無効になっています。複数のクライアントからなる高負荷ネットワークでは、クライアントがローミングとアソシエーション/ディスアソシエーションを頻繁に繰り返すピーク時には大量のトラップおよびSyslogが発生する可能性が特に高まります。この場合、トラップやSyslogを受け取るたびにクライアントをポーリングすると、不要な処理負荷が発生する可能性があります。

[クライアント トラップ/Syslog受信中のクライアントのワイヤレス ポーリング（Wireless Polling Clients when Receiving Client Traps/Syslogs）] オプションを有効にすると、Prime Infrastructure では、以前 WLC のトラップを無効にした場合でも WLC のクライアント認証、クライアント認証解除、クライアント関連付け解除のトラップが有効になります。Prime Infrastructure によって WLC 同期操作がトリガーされ、WLC のクライアント トラップが有効になります。

ステップ 1 **[管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[クライアント（Client）]** の順に選択します。

ステップ 2 [クライアント トラップ/syslog 受信中のクライアントのポーリング（Poll clients when client traps/syslogs received）] チェックボックスをオンにします。Prime Infrastructure は、トラップまたはSyslogを受信した直後にクライアントをポーリングして、クライアント セッションを特定します。

ステップ 3 **[保存（Save）]** をクリックします。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

イベントとしてのクライアント トラップの保存

導入環境によっては、Prime Infrastructure は大量のクライアント アソシエーション トラップおよびディスアソシエーション トラップを受信する場合があります。これらのトラップをイベントとして保存すると、サーバーのパフォーマンスが低下する可能性があります。また、保存するトラップ量が多すぎて、他の有益なイベントが予想よりも早く期限切れになる可能性があります。

Prime Infrastructure がクライアント アソシエーションおよびディスアソシエーション トラップをイベントとして保存しないようにするには、次の手順を実行します。

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[クライアント（Client）] の順に選択します。

ステップ 2 [イベントとしてのクライアント アソシエーションおよびディスアソシエーション トラップの保存（Save client association and disassociation traps as events）] チェックボックスをオフにします。

ステップ 3 [保存（Save）] をクリックして、この設定の変更を確定します。このオプションはデフォルトでは無効になっています。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

802.1x および 802.11 クライアント トラップのイベントとしての保存

デバッグ用に、[802.1x および 802.11 クライアント認証失敗トラップのイベントとしての保存（Save 802.1x and 802.11 client authentication failed traps as events）] を有効にする必要があります。

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[クライアント（Client）] の順に選択します。

ステップ 2 [802.1x および 802.11 クライアント認証失敗トラップのイベントとしての保存（Save 802.1x and 802.11 client authentication failed traps as events）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックして、この設定の変更を確定します。

関連トピック

クライアント パフォーマンスの設定 （136 ページ）
Prime Infrastructure のパフォーマンスを向上させる方法 （134 ページ）

拡張クライアント トラップの有効化

拡張クライアント トラップを有効にするには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントとユーザー（Client and User）] > [クライアント（Client）]** の順に選択します。

ステップ 2 [拡張クライアント トラップからクライアントを検出する（Discover Clients from enhanced client traps）] チェックボックスをオンにします。

ステップ 3 Prime Infrastructure サーバーが、Cisco WLC でクライアント トラップを受信するトラップ レシーバとして登録されていることを確認します。拡張クライアント トラップが機能するには、次のトラップ フラグがデバイスで有効になっている必要があります。

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

ステップ 4 Prime Infrastructure 側の入力拡張クライアント トラップを記録するには、SSH から root シェルを経由してクライアント トラップのロギングを有効にします。これにより、/opt/CSCOlumos/logs 内に clientTraps.log ファイルが生成されます。

- /opt/CSCOlumos/bin/setLogLevel.sh com.cisco.client.traps TRACE

（注） Prime Infrastructure からの拡張クライアント トラップは、WLC バージョン 8.0 以降でサポートされています。

保証処理のメモリ最適化

Prime Infrastructure の保証機能は、NAM などのデバイスによって Prime Infrastructure サーバーに転送される大量の NetFlow データに大きく依存します。Prime Infrastructure は NetFlow データを保存する前に常に集約するため、適切なデータによって保証機能をサポートすることはメモリインテンシブ プロセスです。

集約時に NetFlow データを保持するための作業メモリを増やすことにより、Prime Infrastructure はこのジョブをより迅速かつ効率的に行うことができます。これは、組織が保証機能のライセンスを取得し、それらを多用する場合、重要なパフォーマンス向上につながる可能性があります。

Prime Infrastructure は次の処理に関する支援機能を提供します。

- 現在、保証関連データ処理に割り当てられているメモリ量、および完全に個別の保証機能がそのメモリ プールをどのように使用しているかを識別する。
- 保証関連データを処理するために使用されるメモリのデフォルト プールを増やす。
- 個々の保証機能に割り当てられるメモリのバランスを取り、メモリを最も必要としている機能に必要なメモリが割り当てられるようにする。

これらの機能を使用して得られるパフォーマンス向上の量は、利用可能なメモリと保証機能の使用法によって異なりますが、相当なものになる可能性があります。例：推奨される最小ハードウェア Prime Infrastructure に実装される Prime Infrastructure Professional が単一の 5 分の集約周期で最大 414,000 の NetFlow ホスト レコードを処理できるとします。保証メモリ最適化により、同じタイプのデータの最大処理量はサイクルごとに 800,000 レコード近くになります。

保証メモリ割り当てのバランスを取らずに保証メモリ プールを拡張することも、その逆も可能です。ただし、これら 2 つの最適化オプションをともに使用することは、保証機能を使用した場合の Prime Infrastructure のパフォーマンスを向上する最善の方法です。

関連トピック

保証メモリ割り当てと需要のモニタリング （142 ページ）
CLI 経由の保証メモリ プールの増加 （142 ページ）
保証メモリ割り当てのロード バランシング方法 （143 ページ）
保証メモリ割り当てのリセット （143 ページ）
保証メモリ プールのリセット （143 ページ）

保証メモリ割り当てと需要のモニタリング

Prime Infrastructure の現在の保証関連のメモリ割り当てと使用率をすぐに確認できます。

ステップ 1 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データソース（Data Sources）] の順に選択します。

ステップ 2 [保証メモリ統計情報（Assurance Memory Statistics）] テキストリンク（ページの右上）を選択します。Prime Infrastructure に次の情報が表示されます。

- 主要な保証機能カテゴリ（トラフィック、パフォーマンスルーティング、アプリケーション、音声/ビデオ データ、デバイス ヘルス、Lync およびその他のデータなど）各部に対する、現在のメモリ割り当て量（メガバイト単位）。
- 過去24時間の各エリアのメモリ使用割り当ての使用率。この割合は該当期間中のピーク時のメモリ使用率を表します（つまり、過去 24 時間のいずれかの時点でメモリ割り当ての 100 % が使用されている場合、表示される使用率パーセンテージは 100 % になります）。

関連トピック

保証処理のメモリ最適化 （141 ページ）
CLI 経由の保証メモリ プールの増加 （142 ページ）
保証メモリ割り当てのロード バランシング方法 （143 ページ）

CLI 経由の保証メモリ プールの増加

Prime Infrastructure コマンド ラインを使用して、すべてのタイプの保証関連データ処理に、より多くのメモリを割り当てることができます。**ncs tune-resources assurance** コマンドを使用すると、サーバーの再起動が必要になることに注意してください。再起動後、サーバーはすべての保証関連データ処理に割り当てられたメモリの合計プールを増やします。

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力します。

PIServer/admin# **ncs tune-resources assurance**

ステップ 3 Prime Infrastructure サーバーを再起動します（「Prime Infrastructure の再起動」を参照）。

関連トピック

CLI から接続する方法 （147 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
保証処理のメモリ最適化 （141 ページ）

保証メモリ割り当てのロード バランシング方法

Prime Infrastructure インターフェイスを使用して、保証関連のデータ処理の各カテゴリに対する合計保証メモリ プールのバランスを自動的に調整し、メモリを最も必要とする保証機能に割り当てることができます。

ステップ 1 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ ソース（Data Sources）] の順に選択します。

ステップ 2 [保証メモリ統計情報（Assurance Memory Statistics）] テキスト リンク（[データ ソース（Data Sources）] ページの右上）を選択します。

ステップ 3 [再調整（Rebalance）] をクリックします。

Prime Infrastructure は必要に応じて、個々の機能に対する保証メモリ割り当てを変更し、あまり使用されていない機能への割り当てを減らし、過去 24 時間の使用率が 100 % または 100 % に近い機能への割り当てを増やします。

関連トピック

保証処理のメモリ最適化 （141 ページ）

保証メモリ割り当てのリセット

Prime Infrastructure インターフェイスを使用して、保証メモリ バランス調整をキャンセルし、各保証関連機能の割り当てをデフォルト値に戻すことができます。

ステップ 1 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ ソース（Data Sources）] の順に選択します。

ステップ 2 [保証メモリ統計情報（Assurance Memory Statistics）] テキスト リンク（[データ ソース（Data Sources）] ページの右上）を選択します。

ステップ 3 [リセット（Reset）] をクリックします。

関連トピック

保証処理のメモリ最適化 （141 ページ）

保証メモリ プールのリセット

Prime Infrastructure コマンド ラインを使用して、保証メモリ プールをデフォルトの割り当てに戻すことができます。この際は、「CLI 経由の保証メモリ プールの増加」の説明に従って **ncs tune-resources assurance** コマンドを使用し、作成したすべての変更を無効化します。

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力します。

PIServer/admin# **ncs tune-resources default**

ステップ 3 Prime Infrastructure サーバーを再起動します（「Prime Infrastructure の再起動」を参照）。

関連トピック

CLI 経由の保証メモリ プールの増加 （142 ページ）
CLI から接続する方法 （147 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
保証処理のメモリ最適化 （141 ページ）

データ ソースを管理する

Prime Infrastructure は、デバイス、パフォーマンス、保証データを正確に収集およびレポート作成するうえで、さまざまなソースに依存しています。これらのソースとしては、NAM などの専門モニタリング デバイスのほか、Cisco Medianet、NetFlow、Network Based Application Recognition（NBAR）、Performance Monitoring（PerfMon）、Performance Agent などの通常デバイス上で実行されるプロトコルなどもあります。

アクティブなソースから正確なデータのみが収集されるようにするには、これらのソースの管理が必要となります。[Data Sources] ページを使用すれば、現在のデータ ソースを確認し、無効になったデータ ソースを削除することができます。

ダッシュレットで使用されるデータ ソースの詳細については、「関連項目」の「高度なモニタリング」を参照してください。個々のデータ ソースのセットアップの詳細については、同じく「関連項目」の「管理者の設定タスク」のデータ ソース設定に関するセクションを参照してください。

関連トピック

現在のデータ ソースの表示 （144 ページ）
データ ソースの削除 （145 ページ）
高度なモニタリング
管理者セットアップ タスク （3 ページ）
保証付き のデータ ソースの設定 （11 ページ）
Medianet NetFlow の有効化 （14 ページ）
NetFlow と Flexible NetFlow の有効化 （16 ページ）
ネットワーク解析モジュール（NAM）を展開する （17 ページ）
Performance Agent の有効化 （18 ページ）

現在のデータ ソースの表示

[データ ソース（Data Sources）] ページを使用することにより、Prime Infrastructure の現在のデータ ソースを表示できます。このページにアクセスするには、管理者権限が必要です。

[Services] > [Application Visibility & Control] > [Data Sources] の順に選択します。Prime Infrastructure は、各デバイス データ ソースの一覧を示すサマリ ページを表示します。

- **Device Name**：データ ソースの名前
- **Data Source**：データ ソースの IP アドレス
- **Type**：このソースが Prime Infrastructure に送信しているデータのタイプ（“Netflow” など）
- **Exporting Device**：データを Prime Infrastructure にエクスポートするデバイスの IP アドレス
- **Last 5 min Flow Read Rate**：過去 5 分間に Prime Infrastructure がこのソースから受け取ったデータの量
- **Last Active Time**：Prime Infrastructure がこのソースから最後にデータを受け取った日付と時刻

  ページには、Cisco NAM データ コレクター ソースごとに、次の項目が一覧表示されます。

  - **Name**：NAM のホスト名。
  - **Type**：NAM が収集して Prime Infrastructure に送信するデータのタイプ（「Cisco Branch Routers Series Network Analysis Module」など）。
  - **Host IP Address**：NAM の IP アドレス。
  - **Data Usage in System**：この NAM によって転送されたデータについて、Prime Infrastructure での使用が有効化されたかどうか。
  - [最終アクティブ時刻（Last Active Time）]：Prime Infrastructure がこの NAM から最後にデータを受け取った日付と時刻

関連トピック

特別な管理タスク （146 ページ）
データ ソースの削除 （145 ページ）

データ ソースの削除

[データ ソース（Data Sources）] ページを使用することにより、Prime Infrastructure の無効なデータ ソースを削除できます。このページにアクセスするには、管理者権限が必要です。

NetFlow データ ソースは、そこから最後にデータを受け取った日から丸 7 日が経過するまでは削除できません。この時間差により、NetFlow データ ソースが廃棄済みであることをネットワーク オペレータが確認する時間（丸 1 週間）が確保されるため、NetFlow データ（ソースに従って Prime Infrastructure が識別および集約するデータ）の整合性保護が可能になります。その期間中にソースがアクティブであり続け、かつ Prime Infrastructure にデータを送信する場合、そこからのデータは、同一ソース（新しいソースとしては識別されない）からの別のデータと共に、引き続き正しく識別および集約されます。

ステップ 1 [Services] > [Application Visibility & Control] > [Data Sources] の順に選択します。
ステップ 2 削除する無効データ ソースの隣にあるチェックボックスをオンにします。
ステップ 3 [Delete] をクリックします。
ステップ 4 [OK] をクリックして、削除を実行します。

関連トピック

特別な管理タスク （146 ページ）
現在のデータ ソースの表示 （144 ページ）

特別な管理タスク

Prime Infrastructure は、管理者に、次のような頻度の低いさまざまなタスクを実行するための特別なアクセス権を提供しています。

- SSH コマンド ライン インターフェイス（CLI）セッション経由のサーバーへの接続。
- サーバーのハードウェア セットアップとリソース割り当ての変更。
- Prime Infrastructure サービスの開始、停止、およびステータス チェック。
- CLI 経由でのみアクセス可能な Prime Infrastructure プロセスの実行。
- 特別なタスクを行うユーザー ID のパスワードの変更などのアクセス権限の管理。
- Prime Infrastructure の削除またはリセット。

関連トピック

CLI から接続する方法 （147 ページ）
Prime Infrastructure の起動 （148 ページ）
Prime Infrastructure サーバーのステータスの確認 （148 ページ）
Prime Infrastructure のバージョンとパッチ ステータスの確認 （149 ページ）
Prime Infrastructure の停止 （149 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
Prime Infrastructure の削除方法 （150 ページ）
Prime Infrastructure のデフォルトへのリセット （151 ページ）
Prime Infrastructure ホスト名の変更 （151 ページ）
FTP ユーザーの有効化 （152 ページ）
root ユーザー パスワードの変更 （153 ページ）
仮想アプライアンスの管理者パスワードの回復方法 （154 ページ）
物理アプライアンスの管理者パスワードの回復方法 （155 ページ）
インストール ISO イメージの取得方法 （158 ページ）
ハイ アベイラビリティ ステータスの確認 （366 ページ）

CLI から接続する方法

管理者は、コマンド ライン インターフェイス（CLI）経由で Prime Infrastructure サーバーに接続できます。CLI アクセスは、Prime Infrastructure CLI 経由でのみアクセス可能なコマンドとプロセスを実行しなければならない場合に必要です。これらには、サーバーの起動および停止、ステータスの確認などを行うコマンドが含まれます。

（注） SSH レガシー暗号を無効にすると、レガシー SSH クライアントを利用する Prime Infrastructure との関連付けに影響する可能性があります。

始める前に

手順を開始する前に、次の点を確認してください。

- そのサーバーまたはアプライアンスへの CLI アクセス権を持っている管理ユーザーのユーザー ID とパスワードがわかっていること。明示的に禁止されていない限り、すべての管理ユーザーには CLI アクセス権が与えられます。
- Prime Infrastructure サーバーの IP アドレスまたはホスト名がわかっていること。

ステップ 1 SSH クライアントを起動し、ローカル マシンのコマンド ラインから SSH セッションを開始するか、Prime Infrastructure の物理アプライアンスあるいは仮想アプライアンス上で専用コンソールの接続をします。

ステップ 2 該当する方法でログインします。GUI クラアントを使用している場は：CLI アクセス権を持つアクティブな管理者の ID と Prime Infrastructure サーバーの IP アドレスまたはホスト名を入力します。その後で、接続を開始します。コマンドライン クライアントまたはセッションを使用している場合：[localhost]# ssh username@IPHost のようなコマンドを使用してログインします。username はサーバーへの CLI アクセス権を持つ Prime Infrastructure 管理者のユーザー ID で、IPHost は、Prime Infrastructure サーバーまたはアプライアンスの IP アドレスかホスト名です。コンソールを使用している場合：管理者ユーザー名を入力するためのプロンプトが表示されます。ユーザー名を入力します。

その後、Prime Infrastructure から、入力された管理者 ID のパスワードの入力が要求されます。

ステップ 3 管理 ID パスワードを入力します。Prime Infrastructure に PIServer/admin# のようなコマンド プロンプトが表示されます。

ステップ 4 入力する必要があるコマンドによって、「configure terminal」モードに入ることが必須である場合、プロンプトで次のコマンドを入力します。

PIServer/admin# configure terminal

プロンプトが PIServer/admin# から PIServer/admin/conf# に変わります。

関連トピック

特別な管理タスク （146 ページ）

Prime Infrastructure の起動

以下の手順で Prime Infrastructure を起動します。

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力して、Prime Infrastructure サーバーまたはアプライアンスを起動します。

PIServer/admin# **ncs start**

関連トピック

CLI から接続する方法 （147 ページ）
Prime Infrastructure の停止 （149 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
特別な管理タスク （146 ページ）

Prime Infrastructure サーバーのステータスの確認

すべての Prime Infrastructure サーバーまたはアプライアンス プロセスのステータスはサーバーを停止せずにいつでも確認できます。テクニカル サポート担当者が、Prime Infrastructure に関する問題をトラブルシューティングするときにこのタスクの実行を要請する場合があります。

Admin Dashboard 上のダッシュレットを使用して、サーバーの現在のヘルスをチェックすることもできます（「Prime Infrastructure ヘルスのモニタリング」を参照）。

ncs ha status コマンドを使用して、サーバーで有効になっているハイ アベイラビリティ オプションのステータスを確認できます（「ハイ アベイラビリティ ステータスの確認」を参照）。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（「CLI 経由の接続」を参照）。

ステップ 2 次のコマンドを入力して、Prime Infrastructure のプロセスとサービスの現在のステータスを表示します。

PIServer/admin# **ncs status**

詳細については、「ハイ アベイラビリティ ステータスの確認」を参照してください。

関連トピック

CLI から接続する方法 （147 ページ）
概要ダッシュボード （129 ページ）
特別な管理タスク （146 ページ）

Prime Infrastructure のバージョンとパッチ ステータスの確認

Prime Infrastructure サーバーのバージョンと適用されているパッチは、サーバーを停止せずにいつでも確認できます。通常この確認は、サーバー ソフトウェアをアップグレードまたはパッチ適用するときに必要になります。

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力して、Prime Infrastructure のプロセスとサービスの現在のステータスを表示します。

PIServer/admin# **show version**

関連トピック

CLI から接続する方法 （147 ページ）
特別な管理タスク （146 ページ）

Prime Infrastructure の停止

コマンド ライン インターフェイスを使用して、Prime Infrastructure サーバーまたはアプライアンスをいつでも停止できます。Prime Infrastructure の停止時にログインしていたすべてのユーザーのセッションが機能を停止します。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（「CLI 経由の接続方法」を参照）。

ステップ 2 次のコマンドを入力して、Prime Infrastructure サーバーまたはアプライアンスを停止します。

PIServer/admin# **ncs stop**

関連トピック

CLI から接続する方法 （147 ページ）
特別な管理タスク （146 ページ）

CLI を使用した Prime Infrastructure の再起動

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力して、Prime Infrastructure サーバーまたはアプライアンスを停止します。

PIServer/admin# **ncs stop**

ステップ 3 上記のコマンドが完了するまで待機します。

ステップ 4 次のコマンドを入力して、Prime Infrastructure サーバーまたはアプライアンスを再起動します。

PIServer/admin# **ncs start**

関連トピック

CLI から接続する方法 （147 ページ）
特別な管理タスク （146 ページ）
GUI を使用した Prime Infrastructure の再起動 （150 ページ）

GUI を使用した Prime Infrastructure の再起動

サーバーの GUI から サーバーを起動するには、次の手順に従います。

始める前に

GUI を使用して サーバーを再起動するには、ルート ユーザー権限またはスーパー ユーザー権限が必要です。

ステップ 1 [管理（Administration）] > [システム設定（System Settings）] > [サーバー（Server）] の順に選択します。

ステップ 2 [Prime Infrastructure の再起動（Restart Prime Infrastructure）] をクリックします。

ステップ 3 ポップアップ ウィンドウの [再起動の確認（Restart acknowledgment）] チェックボックスをオンにして、[再起動（Restart）] をクリックします。

関連トピック

CLI を使用した Prime Infrastructure の再起動 （149 ページ）

Prime Infrastructure の削除方法

クリーンな「ゼロから」の再インストールを準備するために、Prime Infrastructure を削除する必要が生じることがあります。これは次の手順で実行できます。

この手順によって、すべてのサーバー設定およびローカルバックアップなど、サーバー上の既存のデータがすべて削除されることに注意してください。リモートバックアップを持っていない場合、またはディスク レベルのデータ リカバリ方法を使用できない場合、データを復元できません。

ステップ 1 サーバーを停止します（「Prime Infrastructure の停止」を参照）。

ステップ 2 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 3 仮想アプライアンスの電源を切ります。

ステップ 4 電源をオフにした仮想アプライアンスを右クリックし、[ディスクから削除（Delete from Disk）] オプションを選択します。

関連トピック

Prime Infrastructure の停止 （149 ページ）
特別な管理タスク （146 ページ）

Prime Infrastructure のデフォルトへのリセット

Prime Infrastructure サーバーを出荷時の初期状態にリセットし、すべてのユーザー データとカスタマイズを削除する一方で、インストール環境自体は維持する必要が生じることがあります。これは次の手順で実行できます。

この手順により、Prime Infrastructure に付属するデフォルトの設定を除いて、サーバー ホスト上の既存のデータがすべて削除されることに注意してください。リモート バックアップを持っていない場合、またはディスク レベルのデータ リカバリ方法を使用できない場合、データを復元できません。

ステップ 1 サーバーを停止します（「Prime Infrastructure の停止」を参照）。

ステップ 2 インストールされている Prime Infrastructure 仮想または物理アプライアンス サーバー ソフトウェアのバージョンに該当するインストール ISO イメージをダウンロードして、DVD に書き込みます（「インストール ISO イメージの取得方法」を参照）。

ステップ 3 仮想アプライアンスの電源を切ります。

ステップ 4 DVD からホストをブートすることによって、アプライアンスまたは OVA を再インストールします。

関連トピック

Prime Infrastructure の停止 （149 ページ）
インストール ISO イメージの取得方法 （158 ページ）
特別な管理タスク （146 ページ）

Prime Infrastructure ホスト名の変更

Prime Infrastructure では、サーバーのインストール時にホスト名の入力が求められます。さまざまな理由で、Prime Infrastructure サーバー上のホスト名と別の場所にあるホスト名との間で不一致が発生することがあります。その場合、サーバー上のホスト名を変更することによって、再インストールせずに回復できます。

（注） **hostnamectl** を使用してホスト名を設定すると、大文字が小文字に変更されます。Redhat 7 および CentOS 7 には、ホスト名を永続的に設定する **hostnamectl** が用意されていますが、ユーザーが大文字を指定しても実際のホスト名は小文字のみになります。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（「CLI から接続する方法」を参照）。必ず「端末設定」モードにしてください。

ステップ 2 次のコマンドを入力します。

PIServer/admin(config)# **hostname** *newHostName*

ここで *newHostName* は、Prime Infrastructure サーバーに割り当てる新しいホスト名です。

ステップ 3 「Prime Infrastructure の再起動」の説明に従い、**ncs stop** コマンドと **ncs start** コマンドを使用して Prime Infrastructure サーバーを再起動します。

関連トピック

CLI から接続する方法 （147 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
特別な管理タスク （146 ページ）

FTP ユーザーの有効化

ファイル転送およびソフトウェア イメージ管理用の FTP サーバーとして Prime Infrastructure を使用する場合、管理者は FTP アカウントを設定する必要があります。アカウントを有効化して、パスワードを設定するには、次の手順を実行します。

ftp-user を有効にすると、スタンドアロン サーバーまたはハイ アベイラビリティ プライマリ サーバー（設定されている場合）の /localdisk/ftp フォルダとの間でのみファイルの FTP 転送ができるようになります。ftp-user では、ディレクトリ変更（cd）およびディレクトリ一覧表示（ls）機能は使用できません。

ステップ 1 Prime Infrastructure サーバーとの CLI 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 2 次のコマンドを入力します。

PIServer/admin#**ncs password ftpuser ftp-user password password**

ここで、

- **ftp-user** は、FTP 操作に使用するユーザー名です。
- **password** は、**ftp-user** のログイン パスワードです。

（注） FTP のユーザー名は、**ftp-user** でなければなりません。

次に例を示します。

```
pi-system-999/admin# ncs password ftpuser root password MyPassword
Updating FTP password.
Saving FTP account password in credential store
Syncing FTP account password to database store - location-ftp-user
Syncing FTP account password to system store
Completed FTP password update
```

pi-system-999/admin#

関連トピック

CLI から接続する方法 （147 ページ）
特別な管理タスク （146 ページ）

root ユーザー パスワードの変更

管理ユーザーは、この特別な管理 ID に関連付けられたパスワードを変更できます。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（「関連項目」の「CLI 経由の接続」を参照）。

ステップ 2 次のコマンドを入力します。

PIServer/admin# **ncs password root password** *password*

ここで、*password* は root ユーザーのログイン パスワードです。80 文字までのパスワードを入力できます。

次に例を示します。

PIServer/admin# ncs password root password #password#

pi-system-198/admin# ncs password root password #password#

Password updated for web root user

pi-system-198/admin#

関連トピック

CLI から接続する方法 （147 ページ）
特別な管理タスク （146 ページ）

CLI を使用した管理者パスワードの変更

新しい CLI コマンド「change-password」が導入されました。このユーザーを使用すると、自身のパスワードを変更できます。このコマンドは、すべてのロールで使用できます。

次の CLI ユーザーロールが適用されます。

- Super-user（admin）：初期設定時に作成されるスーパーユーザーは 1 つだけです。
- Security-admin：スーパーユーザーの後に最も高い権限が与えられます。
- Network-admin：ネットワーク関連の設定を実行する権限があります。
- User：読み取り専用アクセス権の権限があります。

ステップ 1 Prime Infrastructure との CLI セッションを開きます。

ステップ 2 次のコマンドを入力します。

pi-cluster-54/admin# change-password

ユーザー管理者のパスワードの変更

管理者のパスワードを変更します。

（現在）UNIX パスワード

仮想アプライアンスの管理者パスワードの回復方法

独自のハードウェアにインストールされた Prime Infrastructure 仮想マシン（別名 OVA）上で管理者パスワードを回復（つまりリセット）することができます。

始める前に

次の条件が満たされていることを確認します。

- Prime Infrastructure サーバーに物理的にアクセスできること。
- ソフトウェアのバージョンに適切なインストール ISO イメージのコピー。「関連項目」の「インストール ISO イメージの取得方法」を参照してください。
- VMware vSphere クライアントへのアクセスと、vSphere インベントリ、データストア、およびオブジェクトの各機能へのアクセス。このようなアクセスがない場合は、VMware 管理者にお問い合わせください。vSphere クライアントから直接 ESX にアクセスしないようにしてください。

ステップ 1 VMware vSphere Client を起動し、ESXi ホストまたは vCenter サーバーに接続します。

ステップ 2 次のように、OVA 仮想マシン上のデータストアにインストール ISO イメージをアップロードします。

a) vSphere サーバーで、[インベントリ（Inventory）] > [概要（Summary）] > [データストア（Datastores）] をクリックします。
b) [オブジェクト（Objects）] タブで、ファイルをアップロードするデータストアを選択します。
c) [Navigate to the datastore file browser] アイコンをクリックします。
d) 必要に応じて、[Create a new folder] アイコンをクリックして、新しいフォルダを作成します。
e) 作成したフォルダを選択するか、既存のフォルダを選択して、[Upload a File] アイコンをクリックします。

   [Client Integration Access Control] ダイアログ ボックスが表示されたら、[Allow] をクリックして、プラグインからオペレーティング システムにアクセスできるようにし、ファイルのアップロードに進みます。

f) ローカル コンピュータで、ISO ファイルを検索して、そのファイルをアップロードします。
g) データストア ファイル ブラウザを更新して、アップロードされたファイルを一覧表示します。

ステップ 3 ISO イメージがデータストアにアップロードされたら、次のように、それをデフォルトのブート イメージにします。

a) VMware vSphere クライアントを使用して、導入済みの OVA を右クリックして、[電源（Power）] > [電源オフ（Power Off）] の順に選択します。
b) [設定の編集（Edit Settings）] > [ハードウェア（Hardware）] の順に選択して、[CD/DVD ドライブ 1（CD/DVD drive 1）] を選択します。
c) [Device Type] で、[Datastore ISO File] を選択してから、[Browse] ボタンを使用して、データストアにアップロードした ISO イメージ ファイルを選択します。
d) [Device Status] で、[Connect at power on] を選択します。
e) [Options] タブをクリックして、[Boot Options] を選択します。[Force BIOS Setup] で、[Next time VM boots, force entry into BIOS setup Screen] を選択します。これにより、仮想マシンを再起動すると、仮想マシンの BIOS からブートが開始されます。
f) [OK] をクリックします。
g) VMware vSphere クライアントで、導入済みの OVA を右クリックして、[Power] > [Power On] の順に選択します。
h) BIOS セットアップ メニューで、デバイスのブート順序を制御するオプションを探して、[DVD/CDROM] を一番上に移動します。

ステップ 4 次の手順に従って、サーバー管理者パスワードをリセットします。

a) BIOS 設定を保存して、BIOS セットアップ メニューを終了します。仮想マシンが ISO イメージからブートし、ブート オプションのリストが表示されます。
b) キーボードとモニターを使用して OVA にアクセスしている場合は「**3**」を、コマンド ラインまたはコンソール経由でアクセスしている場合は「**4**」を入力します。vSphere クライアントに、管理者ユーザー名のリストが表示されます。
c) パスワードをリセットする管理者ユーザー名の横に表示された番号を入力します。
d) 新しいパスワードを入力し、2 回目の入力でそれを確認します。
e) vSphere クライアントを使用して変更を確認する前に、必ず ISO イメージを切断します。
f) CD アイコンをクリックし、ISO の切断イメージを選択します。
g) 「**Y**」と入力して、変更を保存し、リブートします。

ステップ 5 新しい管理者パスワードを使用してログインします。

関連トピック

インストール ISO イメージの取得方法 （158 ページ）
特別な管理タスク （146 ページ）

物理アプライアンスの管理者パスワードの回復方法

Prime Infrastructure の物理アプライアンス上で管理者パスワードを回復（リセット）することができます。

はじめる前に

次の条件が満たされていることを確認します。

- Prime Infrastructure アプライアンスに物理的にアクセスできること。
- 出荷されたアプライアンスに同梱されているアプライアンス リカバリ CD のコピー。

アプライアンス リカバリ CD を紛失した場合は、「インストール ISO イメージの取得方法」に記載されているように、ISO イメージのコピーをダウンロードして、DVD に書き込みます。その後、その DVD を使用して、アプライアンス上で管理者パスワードをリセットすることができます（詳細な手順については「仮想アプライアンスの管理者パスワードの回復方法」を参照）。

次の方法でパスワードをリセットできます。

- **コンソール**：KVM コンソール（この他のコンソール オプションには、VGA コンソール、シリアル コンソール/Serial Over LAN（SOL）があります）
- **DVD マウント オプション**：KVM がマッピングされた DVD（他のマウント オプションには、CIMC がマッピングされた DVD と外付けの物理 DVD があります）

詳細については、『Cisco Prime Infrastructure Hardware Installation Guide』を参照してください。

KVM コンソールを使用してパスワードを回復するには、次の手順を実行します。

ステップ 1 Cisco Integrated Management Controller を起動します。

ステップ 2 左側のナビゲーション ペインから [サーバー（Server）] > [概要（Summary）] を選択します。

ステップ 3 [アクション（Actions）] で、[KVM コンソールの起動（Launch KVM Console）] を選択します。

ステップ 4 コンソールで、[仮想メディア（Virtual Media）] > [仮想デバイスの有効化（Activate Virtual Devices）] を選択します。

ステップ 5 [セッションを承認（Accept the session）] ラジオ ボタンを選択してから [適用（Apply）] をクリックします。

ステップ 6 コンソールで、[仮想メディア（Virtual Media）] > [CD/DVD のマッピング（Map CD/DVD）] を選択します。

ステップ 7 Prime Infrastructure ISO イメージの場所を参照して、[デバイスのマッピング（Map Devices）] をクリックします。

ステップ 8 コンソールで、[電源（Power）] > [システムのリセット（ウォーム ブート）（Reset System(warm boot)）] を選択します。

ステップ 9 確認メッセージが表示されます。[はい（Yes）] をクリックします。

ステップ 10 マシンが再起動し、F6 を押してブート オプションを表示するよう要求されます。ファンクション キー **F6** を押します。

画面に [ブート選択メニューを表示（Enter boot selection menu...）] が出るまでに F6 を複数回押すことが必要となる場合があります。ブート デバイス オプションが表示されるまで数分間かかります。

ステップ 11 DVD マウント オプションを選択します。この例では、[Cisco vKVM-Mapped vDVD1.22] を選択する必要があります。

ステップ 12 vSphere クライアントに、ブート オプションのリストが表示されます。「**3**」と入力して、[管理者パスワードの回復（キーボード/モニター）（Recover Administrator Password (Keyboard/Monitor)）] ブート オプションを選択します。

（注） パスワードを回復するためにシリアル コンソールを使用している場合、「**4**」と入力して、[管理者パスワードの回復（キーボード/モニター）（Recover Administrator Password (Keyboard/Monitor)）] ブート オプションを選択します。

ステップ 13 vSphereクライアントに、管理者ユーザー名のリストが表示されます。パスワードを回復（リセット）する管理者ユーザー名の横に表示された番号を入力し、**Enter** キーを押します。

ステップ 14 新しいパスワードを入力し、2 回目の入力でそれを確認します。

ステップ 15 「**Y**」と入力して、変更を保存し、システムをリブートします。

ステップ 16 新しい管理者パスワードで管理 CLI にログインします。

（注） 同じ手順に従って、VGA コンソールとシリアル コンソールを使用してパスワードを回復することができます。

Hyper-V 仮想アプライアンスでの管理者パスワードの回復方法

Prime Infrastructure Hyper-V 仮想アプライアンスで管理者パスワードを回復（リセット）できます。

はじめる前に

次の条件が満たされていることを確認します。

- Prime Infrastructure アプライアンスに物理的にアクセスできること。
- ソフトウェアのバージョンに適切なインストール ISO イメージのコピー。インストール ISO イメージの取得方法（158 ページ）を参照してください。
- Hyper-V マシンおよび Hyper-V Manager へのアクセス権限。アクセス権限がない場合は、Hyper-V 管理者に支援してもらいます。

ステップ 1 Hyper-V マシンを起動し、Hyper-V マシン内で ISO イメージを使用できることを確認します。

ステップ 2 Hyper-V Manager に接続します。

a) パスワードをリセットする仮想マシンを右クリックし、[接続（Connect）] を選択します。[仮想マシンの接続（Virtual Machine Connection）] ウィンドウが開きます。

b) [メディア（Media）] > [DVD ドライブ（DVD Drive）] > [ディスクの挿入（Insert Disk）] の順に選択します。

c) [参照（Browse）] をクリックし、ISO イメージを選択します。

d) 次の手順に従って、仮想マシンの電源をオフにしてから仮想マシンを起動します。

- [アクション（Action）] > [電源オフ（Turn Off）] の順に選択します。

- [マシンの電源オフ（Turn Off Machine）] ポップアップで [電源オフ（Turn Off）] をクリックします。
- [アクション（Action）] > [起動（Start）] の順に選択します。

ステップ 3 仮想マシンが ISO イメージからブートし、ブート オプションのリストが表示されます。

a) 「3」（管理者パスワードを回復するためのオプション）と入力します。
b) パスワードをリセットする管理者ユーザー名に表示された番号を入力します。
c) 新しいパスワードを入力し、2 回目の入力でそれを確認します。
d) 「Y」と入力して、変更を保存し、リブートします。
e) マシンがリブートするまで待ちます。

ステップ 4 新しい管理者パスワードを使用してログインします。

インストール ISO イメージの取得方法

Prime Infrastructure のインストール ISO イメージのコピーは、管理者パスワードのリセットなどの特別なメンテナンス作業で必要です。

Prime Infrastructure の ISO イメージ ファイルの形式は、PI-APL-**version**-K9.iso です。**version** は製品のバージョン番号です。バージョン番号に製品のパッチ レベルを示す拡張番号が含まれている場合があります。例：Prime Infrastructure 3.10 の完全更新バージョンを使用している場合は、Cisco.com から PI-APL-3.10.0.0.205-1-K9.iso をダウンロードする必要があります。

ISO イメージのコピーを入手していない場合は、次の手順で Cisco.com からダウンロードできます。

ステップ 1 インターネット アクセス可能なブラウザで、Cisco ソフトウェア ダウンロード ナビゲータにリンクします（「関連項目」を参照）。

ステップ 2 [検索（Find）] ボックスを使用して、「Cisco Prime Infrastructure」を検索します。

ステップ 3 結果の一覧から、使用しているソフトウェアのバージョンを選択します。

ステップ 4 [Prime Infrastructure ソフトウェア（Prime Infrastructure Software）] を選択して、そのソフトウェア バージョンの ISO と他のダウンロード可能イメージ ファイルのリストを表示します。

ステップ 5 そのページから ISO イメージをダウンロードします。

ステップ 6 ダウンロードが完了したら、ダウンロードしたファイルの MD5 チェックサムと Cisco.com ダウンロード ページでそのファイルに関して表示されたチェックサムが一致していることを確認します。チェックサムが一致していない場合は、ファイルが破損しているため、Cisco.com からダウンロードし直す必要があります。

ステップ 7 ディスク上の ISO イメージが必要な場合：DVD オーサリング ソフトウェアを使用して、ISO イメージを 2 層 DVD に書き込みます。信頼できる結果を得るために、書き込みは 1 倍速（1X）で行い、[検証（Verify）] オプションをオンにします。

詳細については、https://software.cisco.com/download/navigator.htmlおよび『Cisco Prime Infrastructure Appliance Hardware Installation Guide』[英語] を参照してください。

関連トピック

特別な管理タスク （146 ページ）

最新のソフトウェア アップデートで Prime Infrastructure を更新する方法

シスコでは、Prime Infrastructure ソフトウェアのアップデートを定期的に提供しています。これらのアップデートは、以下のカテゴリに分類されます。

- 重要修正：ソフトウェアの重要な修正を提供します。これらのアップデートが利用可能になったら、ただちにこれらのすべてをダウンロードして適用することが強く推奨されます。
- デバイス サポート：Prime Infrastructure がリリース時点でサポートしていなかったデバイスを管理するサポートを追加します。これらのアップデートは毎月発行されます。
- アドオン：現在使用中の Prime Infrastructure バージョンを補完するための新しい機能を提供します（新しい GUI 画面や機能が含まれることもあります）。

これらのアップデートを検索する方法、およびこれらのリリース時に通知を受け取る方法に関する詳細は、「関連項目」の「インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示」を参照してください。

Prime Infrastructure が表示するアップデート通知は、[管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[ソフトウェア アップデート（Software Update）] で指定された通知設定に基づいています。詳細については、「ソフトウェア アップデート通知の設定」を参照してください。

これらのアップデートのインストールの詳細については、「ソフトウェアアップデートのインストール」を参照してください。

Cisco.com アカウントを使用したソフトウェア アップデート通知およびインストールの簡素化の詳細については、「Prime Infrastructure での Cisco.com アカウント クレデンシャルの使用方法」を参照してください。

関連トピック

インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
ソフトウェア アップデート通知の設定 （161 ページ）
ソフトウェア アップデートのインストール （162 ページ）
Prime Infrastructure での Cisco.com アカウント クレデンシャルの使用方法 （165 ページ）

インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示

Prime Infrastructure を使用して次のことができます。

- 新しいソフトウェア アップデートが利用可能になったときに通知を受け取る。
- 新しいソフトウェアアップデートが利用可能になったときの通知方法とタイミングを変更する。
- それぞれのアップデートの詳細を表示する。
- どのソフトウェア アップデートがインストール済みかを確認する。

これらの作業の実行方法について、以降の項目で説明します。

関連トピック

ソフトウェア アップデート通知の設定方法 （160 ページ）
ソフトウェア アップデート通知の設定 （161 ページ）
インストール済みのソフトウェア アップデートの詳細の表示 （161 ページ）
ログイン ページからのインストール済みアップデートの表示 （162 ページ）
[バージョン情報（About）]ページからのインストール済みアップデートの表示 （162 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

ソフトウェア アップデート通知の設定方法

正しく設定されている場合、Prime Infrastructure は新しいソフトウェア アップデートが利用可能になると自動的に通知を送信します。

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[アカウント設定（Account Settings）] の順に選択します。

ステップ 2 有効な Cisco.com ユーザー名とパスワードを入力します。

ステップ 3 [Save] をクリックします。

ステップ 4 [Administration] > [Settings] > [System Settings] > [General] > [Software Update] の順に選択します。

ステップ 5 [Notification Settings] で、[Administration] > [Software Update] ページにアップデートを表示するカテゴリを選択します。

ステップ 6 [Save] をクリックします。

通知を確認するには、右上のアラーム アイコンの隣にある通知アイコンをクリックします。

関連トピック

ソフトウェア アップデート通知の設定 （161 ページ）
インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
Prime Infrastructure での Cisco.com アカウント クレデンシャルの使用方法 （165 ページ）

最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

ソフトウェア アップデート通知の設定

Prime Infrastructur が表示するアップデート通知は、[管理（Administration）] > [ソフトウェア アップデート（Software Update）] ページで変更できます。たとえば、Prime Infrastructur へのアップデートのインストールを一切希望しない場合、すべての通知を無効にして、Prime Infrastructur で使用可能なアップデートの通知を行わないようにすることができます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [ソフトウェア アップデート（Software Update）] の順に選択します。

ステップ 2 [Notification Settings] で、[Administration] > [Software Update] ページにアップデートを表示するカテゴリを選択します。

ステップ 3 [保存（Save）] をクリックします。

関連トピック

インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
ソフトウェア アップデート通知の設定方法 （160 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

インストール済みのソフトウェア アップデートの詳細の表示

ステップ 1 [管理設定（Administration settings）]>[ランセンスおよびソフトウェア アップデート（Licenses and Software Updates）] > [ソフトウェア アップデート（Software Update）] の順に選択します。

ステップ 2 [更新（Updates）] タブをクリックすると、インストール済みの各ソフトウェア アップデートの名前、タイプ、バージョン、ステータス、日付が表示されます。

この一覧をフィルタリングするには、[アップデート（Updates）] タブの右側にある [フィルタ（Filter）] アイコンをクリックし、表示したいインストール済みアップデートのカテゴリを選択します。

ステップ 3 [Files] タブをクリックすると、インストール済みの UBF ファイル、およびダウンロード済みでまだインストールされていない UBF ファイルの一覧が表示されます。

まだインストールされていないソフトウェア アップデートを削除するには、ファイルを選択して [削除（Delete）] をクリックします。

関連トピック

インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
ログイン ページからのインストール済みアップデートの表示 （162 ページ）
[バージョン情報（About）] ページからのインストール済みアップデートの表示 （162 ページ）

最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

ログイン ページからのインストール済みアップデートの表示

ステップ 1 Prime Infrastructure の起動またはログアウトを行います。ログイン ページが表示されます。

ステップ 2 [View installed updates] をクリックします。Prime Infrastructure は、すべてのインストール済みソフトウェア アップデートについて、名前とバージョンのポップアップ リストを表示します。

ステップ 3 ポップアップ リストを閉じるには、[閉じる（Close）] ボタンをクリックします。

関連トピック

[バージョン情報（About）]ページからのインストール済みアップデートの表示 （162 ページ）
インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

[バージョン情報（About）] ページからのインストール済みアップデートの表示

ステップ 1 任意の [Prime Infrastructure] ページの右上にある [設定（settings）] アイコンをクリックします。

ステップ 2 [Prime infrastructure バージョン情報（About Prime infrastructure）] をクリックします。バージョン情報ページが表示され、製品のバージョンおよびその他の詳細が一覧表示されます。

ステップ 3 [インストール済みアップデートの表示（View installed updates）] をクリックします。Prime Infrastructure は、すべてのインストール済みソフトウェア アップデートについて、名前とバージョンのポップアップ リストを表示します。

ステップ 4 ポップアップ リストを閉じるには、[閉じる（Close）] ボタンをクリックします。

関連トピック

ログイン ページからのインストール済みアップデートの表示 （162 ページ）
インストール済みのソフトウェア アップデートと利用可能なソフトウェア アップデートの表示 （160 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

ソフトウェア アップデートのインストール

Prime Infrastructure は、[管理（Administration）]>[ソフトウェア アップデート（Software Update）] を選択することによりダウンロードとインストールが可能な、重要修正、デバイス サポート、およびアドオン アップデートを定期的に提供します。接続と設定に応じて、次の方法でソフトウェア アップデートをインストールできます。

- cisco.com からアップデートを Prime Infrastructure に直接ダウンロードします。

この方法の場合、Prime Infrastructure サーバーが外部から Cisco.com に接続できることが必要です。詳細については、「関連項目」の「Cisco.com からのソフトウェア アップデートのインストール」を参照してください。

- 外部接続のあるクライアントまたはサーバーにソフトウェアの更新ファイルをダウンロードし、

  それらをアップロードして Prime Infrastructure サーバーにインストールします。詳細については、「関連項目」の「ダウンロードしたソフトウェアのアップロードとインストール」を参照してください。

関連トピック

Cisco.com からのソフトウェア アップデートのインストール （163 ページ）
ダウンロードしたソフトウェアのアップロードとインストール （164 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

Cisco.com からのソフトウェア アップデートのインストール

次の手順では、ソフトウェア アップデートを Cisco.com から直接インストール方法について説明します。この手順では、Prime Infrastructure が Cisco.com に外部から接続可能であり、アップデートを Cisco.com から直接ダウンロードすることを前提としています。

ステップ 1 [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）]>[ソフトウェア アップデート（Software Update）] の順に選択します。

ステップ 2 ページの上部にある [ダウンロード（download）] リンクをクリックして、最新のアップデートを Cisco.com から取得します。

ステップ 3 Cisco.com のログイン クレデンシャルを入力します。Prime Infrastructure により、使用可能なアップデートがリストされます。

Cisco.com への接続に問題があることを示すエラーが発生した場合は、[管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[一般（General）]>[アカウント設定（Account Settings）]>[プロキシ（Proxy）] を選択して、プロキシ設定を確認します。プロキシ設定が機能していない場合、[プロキシの有効化（Enable Proxy）] の選択を解除し、[保存（Save）] をクリックします。

ステップ 4 [詳細の表示（Show Details）] をクリックして、アップデートの詳細を確認します。

ステップ 5 インストールするアップデートの横にある [ダウンロード（Download）] をクリックします。

ステップ 6 更新プログラムをダウンロードしたら、[インストール（Install）] をクリックします。

ステップ 7 ポップアップ メッセージで [はい（Yes）] をクリックします。サーバーが自動的に再起動します。

ステップ 8 再起動が完了したら、[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）]>[ソフトウェア アップデート（Software Update）] を選択します。[更新（Updates）] テーブルでは更新プログラムの状態が [インストール済み（Installed）] と表示されます。

関連トピック

ソフトウェア アップデートのインストール （162 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）

最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

ダウンロードしたソフトウェアのアップロードとインストール

次の手順は、ソフトウェアアップデートのアップロードおよびインストールの方法を示しています。この手順は、Prime Infrastructure サーバーが外部接続を持たない場合やファイルを別のサーバーにダウンロードする場合に便利です。

ステップ 1 [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）] > [ソフトウェア アップデート（Software Update）] の順に選択します。

ステップ 2 ページ上部の [upload] リンクをクリックします。

ステップ 3 [Upload Update] ウィンドウの [Cisco Download] をクリックします。すると、Cisco.com の [Download Software] ページが表示されます。

ステップ 4 [製品（Products）] > [クラウドおよびシステム管理（Cloud and Systems Management）] > [ルーティングおよびスイッチ管理（Routing and Switch 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。

ステップ 5 正しいバージョンの Prime Infrastructure を選択します。

ステップ 6 アップデート ソフトウェアのタイプ（「Prime Infrastructure Device Packs」など）を選択します。

ステップ 7 表示されたページから、目的のアップデートが含まれるファイルの隣にある [Download] をクリックします。ファイルには、UBF ファイル名の拡張子が付けられます。

Cisco.com クレデンシャルをまだ保存していない場合（「関連項目」の「Prime Infrastructure での Cisco.com アカウントクレデンシャルの保存」を参照）、アップデートファイルをダウンロードする前に Cisco.com にログインして、シスコとのアクティブなライセンス契約に同意することを求められます。

必ず、Prime Infrastructure のバージョンと一致するソフトウェアアップデートをダウンロードしてください。

ステップ 8 アップデートファイルをクライアント マシンにダウンロードしたら、[Prime Infrastructure] タブに戻り、[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）] > [ソフトウェア アップデート（Software Update）] を選択します。

ステップ 9 [アップロード（Upload）]をクリックし、ダウンロード済みのアップデートファイルの場所を特定して、それを選択します。

ステップ 10 [インストール（Install）] をクリックします。

ステップ 11 ポップアップ メッセージで [はい（Yes）] をクリックします。サーバーが自動的に再起動します。

ステップ 12 再起動が完了したら、[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）] > [ソフトウェア アップデート（Software Update）] を選択します。[更新（Updates）] テーブルでは更新プログラムの状態が [インストール済み（Installed）] と表示されます。

関連トピック

ソフトウェア アップデートのインストール （162 ページ）
Prime Infrastructure への Cisco.com アカウント クレデンシャルの保存 （165 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）

最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

Prime Infrastructure での Cisco.com アカウント クレデンシャルの使用方法

Cisco.com アカウントのユーザー名とパスワードを Prime Infrastructure に保存できます。すると、ソフトウェアアップデートのダウンロードおよびインストールが簡素化され、アップデートの自動確認と通知の高速化が可能になります。

Prime Infrastructure は、一度に 1 セットの Cisco.com クレデンシャルのみを保存します。パスワードは、安全に暗号化された形式で保存されます。この保存済みのユーザー名とパスワードは、すべてのソフトウェアアップデート通知の確認に使用されます。これらは、別のユーザーが保存済みクレデンシャルを削除（「関連項目」の「Cisco.com アカウントクレデンシャルの削除」の説明参照）するか、新しい Cisco.com ユーザー名とパスワードを入力して上書きするまで有効です。

関連トピック

Prime Infrastructure への Cisco.com アカウント クレデンシャルの保存 （165 ページ）
Cisco.com アカウント クレデンシャルの削除 （165 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

Prime Infrastructure への Cisco.com アカウント クレデンシャルの保存

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[アカウント設定（Account Settings）] の順に選択します。

ステップ 2 有効な Cisco.com ユーザー名とパスワードを入力します。

ステップ 3 [保存（Save）] をクリックします。

関連トピック

Cisco.com からのソフトウェア アップデートのインストール （163 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

Cisco.com アカウント クレデンシャルの削除

ステップ 1 [管理（Administration）]>[設定（Settings）]>[システム設定（System Settings）]>[アカウント設定（Account Settings）] の順に選択します。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 削除を確定するには、[はい（Yes）] をクリックします。

関連トピック

ソフトウェア アップデートのインストール （162 ページ）
CLI を使用した Prime Infrastructure の再起動 （149 ページ）
最新のソフトウェア アップデートで Prime Infrastructure を更新する方法 （159 ページ）

サポート要求の設定方法

[サポート リクエストの設定（Support Request Settings）] ページで、一般的なサポートおよびテクニカル サポート情報を設定できます。

ステップ 1 [Administration] > [Settings] > [System Settings] > [Support Request] の順に選択します。[サポート リクエストの設定（Support Request Settings）] ページが表示されます。

ステップ 2 次のパラメータを設定します。

- 一般的なサポートの設定:
  - [Enable interactions directly from the server]：サーバからの直接的なサポート要求の対話を許可するには、このチェック ボックスをオンにします。
  - [Sender E mail Address]：サポート要求送信者のメール アドレスを入力します。
  - [Interactions via client system only]：クライアント システムを通じてのみサポート要求に関する対話を許可する場合は、このチェックボックスをオンにします。
- テクニカル サポート プロバイダーの情報:
  - [Cisco]：テクニカルサポートプロバイダーがシスコの場合、このチェックボックスをオンにします。
  - [Default Cisco.com Username]：Cisco.com にログインするためのデフォルト ユーザ名を入力します。メール サーバ、Cisco サポート サーバ、およびフォーラム サーバへの接続をテストするには、[Test Connectivity] をクリックします。
  - [Third-Party Support Provider]：テクニカル サポート プロバイダーが Cisco.com 以外のサードパーティの場合は、このチェック ボックスをオンにします。メールアドレス、電子メールの件名の形式、サポート プロバイダーの Web サイトの URL を入力します。

ステップ 3 [設定の保存（Save Settings）] をクリックします。

関連トピック

シスコ サポート ケースの登録 （300 ページ）
シスコ サポート コミュニティへの参加 （301 ページ）

ディスク容量の問題を管理する方法

Prime Infrastructure サーバーの物理または仮想サーバーのディスク領域が 90 パーセントに達すると、サーバーのディスク領域が少ないことを示す主要アラートがトリガーされます。

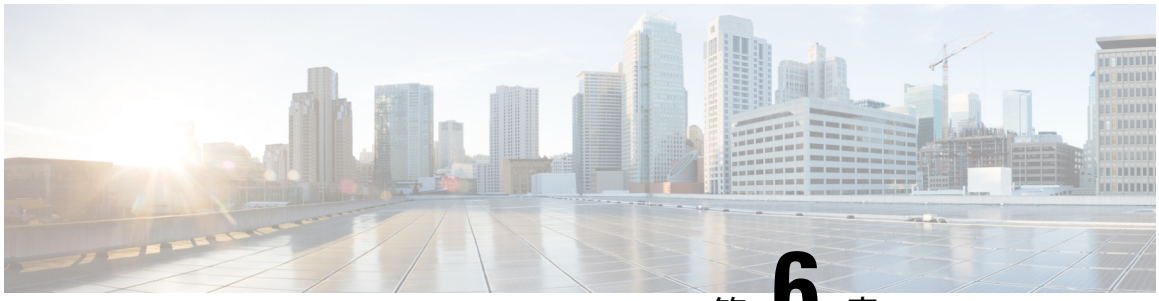
これらのアラームのしきい値超過は、Prime Infrastructure optvol および localdiskvol パーティションの使用率のみに基づいて計算されます。optvol パーティションは Prime Infrastructure のすべてのインベントリおよびネットワーク データを保存するための Oracle データベースを含むのに対して、localdiskvol はローカル アプリケーション バックアップ、WLC および MSE バックアップ、およびレポートを保存します。アラームをトリガーする設定は、Prime Infrastructure サーバーの /opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging フォルダにある PackagingResources.properties ファイルで定義されます。

管理者は、主要アラートの受信後すぐに、ディスク領域の増加アクションを取ることを推奨します。これを行うために、次のいずれかの方法を組み合わせて使用できます。

- 「Prime Infrastructure データベースの圧縮」の手順に従って、既存のデータベース領域を解放します。
- 「リモート バックアップ リポジトリの使用」の手順に従って、リモート バックアップ リポジトリのセットアップと使用により、localdiskvol パーティションのストレージ ロードを減らします。
- インベントリおよびネットワーク データを保持する量と保管期間を減らして、optvol パーティションのストレージ ロードを減らします。
  - 「クライアント アソシエーション履歴データの保持期間の指定」および「イベントとしてのクライアント トラップの保存」の手順に従って、クライアント アソシエーション データおよび関連イベントを保存する時間を短縮します。
  - 「レポートの保存および保持の制御」の手順に従って、レポートを保存する時間を短縮します。
  - 「カテゴリ別のデータ保持の指定」および「DNS ホスト名ルックアップの有効化」の手順に従って、ネットワーク インベントリ、パフォーマンス、その他のデータ クラスの保存期間を短縮します。
- 「VMware vSphere クライアントを使用した VM のリソース割り当ての変更」の手順に従って、Prime Infrastructure に割り当てられた既存の仮想ディスク領域の容量を増やします。VMware ESXi 5.5 以降を使用する場合、vSphere Web クライアントを使用してディスク領域割り当てを調整します（「関連項目」の「VMware vSphere documentation」を参照）。追加の物理ディスク ストレージをインストールし、VMware 編集設定または vSphere Web クライアントを使用して、追加ストレージを Prime Infrastructure に割り当てることもできます。
- 「バックアップと復元を使用した別の OVA への移行」および「バックアップと復元を使用した別のアプライアンスへの移行」の手順に従って、Prime Infrastructure サーバー インストール構成を、適切なディスク領域を持つサーバーに移行します。詳細については、「VMware vSphere Documentation」を参照してください。

関連トピック

Prime Infrastructure データベースの圧縮 （136 ページ）
リモート バックアップ リポジトリの使用 （60 ページ）
クライアント アソシエーション履歴データの保持期間の指定 （138 ページ）
イベントとしてのクライアント トラップの保存 （139 ページ）
データ保持設定が Web GUI データに及ぼす影響 （169 ページ）
データベース テーブル別のデータ保持の指定 （174 ページ）
DNS ホスト名ルックアップの有効化 （138 ページ）
VMware vSphere クライアントを使用した VM のリソース割り当ての変更 （134 ページ）
バックアップと復元を使用した別の仮想アプライアンスへの移行 （73 ページ）
バックアップと復元を使用した別の物理アプライアンスへの移行 （73 ページ）



第 6 章

データ収集とバックグラウンド タスク

ここでは、次の内容について説明します。

データ収集ジョブの制御

すべてのデータ収集タスク（およびデータ消去タスク）がジョブ ダッシュボードから制御されます。「」を参照してください。データ収集ジョブは、「 」に一覧表示されています。

データ保持設定が Web GUI データに及ぼす影響

[データの保持（Data Retention）]ページで加えた変更に従って、Web GUI に表示される情報が決まります。[データの保持（Data Retention）]ページを開くには、**[管理（Administration）]**>**[設定（Settings）]**>**[システム設定（System Settings）]** を選択し、さらに **[一般（General）]**>**[データの保持（Data Retention）]** を選択します。

たとえば、7 日より前の古い履歴パフォーマンス データが不要な場合、パフォーマンス データ保持の値を次のように変更できます。

- [短期データ保持期間（Short-term Data Retention Period）]：1 日

- [中期データ保持期間（Medium-term Data Retain Period）]：3 日
- [長期データ保持期間（Long-term Data Retain Period）]：7 日

このような設定に変更すると、パフォーマンス レポートおよびパフォーマンス ダッシュボードに表示されるすべてのデータは、過去7日間のみが対象になります。パフォーマンス レポートを作成すると、過去 7 日間より長いレポート期間を選択した場合でも、レポートには過去 7 日間のデータのみが含まれます（これは、保持するように選択したデータが7日間分であるためです）。

同様に、パフォーマンス ダッシュボードを表示して1週間を超える時間枠を選択しても、ダッシュボードには過去 7 日間の日付のみが含まれます。

インターフェイスのモニタリング ポリシーを作成する際に、15分ごと、5分ごと、または1分ごとのポーリング間隔を定義できます。選択したポーリング間隔に基づいてデバイスデータがポーリングされ、Oracle データベースに保存されます。データは 1 時間ごとに AHxxx テーブルに集約されます。また、1/5/15分に設定されたポーリング間隔に関係なく、ADxxxテーブルへの集約が 1 日に 1 回行われます。

[インターフェイスヘルスポリシー（Interface Health Policy）] タブでは、頻度が 5 分に設定されている場合は、1 時間あたり 12 個のサンプルを表示できます。1 時間ごとにデータが集約テーブルに移動されてインターフェイス統計の平均値が算出され、1 時間ごとの集約テーブルに 1 つのエントリが表示されます。ポーリング間隔に関係なく、集約はすべてのポリシーで同一です。

データ保持の詳細とデータストレージの期間、イベント時間（ミリ秒単位）、および各データベースのエンティティ ID とイベント時間を表示できます。パフォーマンスデータと集約データは、[パフォーマンス ダッシュレット（Performance Dashlet）] > [インターフェイス（Interfaces）] > [トラフィック使用率（Traffic Utilization）] タブに表示されます。

履歴データの保持について

Prime Infrastructure は次の 2 種類の履歴データを保存します。

1. 非集約履歴データ：まとめて収集または集約できない数値データ。クライアント アソシエーション履歴は、非集約履歴データの 1 つの例です。

（注） 非集約データ収集タスクごとの保存期間（およびその他の設定）を定義できます。たとえば、**[Administration]** > **[Settings]** > **[System Settings]** > **[Client]**で、クライアント関連付け履歴の保持期間を定義できます。デフォルトで、すべての非集約履歴データの保存期間は 31 日または 1,000,000 レコードです。この保持期間は 365 日まで増やすことができます。

1. 集約履歴データ：全体として収集し、最小、最大、および平均として集約することが可能な数値データ。クライアント数は、集約履歴データの 1 つの例です。

集約履歴データのタイプは次のとおりです。

- 傾向：これには、クライアント履歴、AP履歴、AP使用率、クライアント統計情報などの無線関連の履歴情報が含まれます。
- デバイス ヘルス：これには、デバイスのアベイラビリティ、CPU、メモリ、およびインターフェイスの使用率、QoSなどの有線デバイスと無線デバイスに関するSNMPポーリング データが含まれます。
- ネットワーク監査レコード：これには、ユーザーがトリガーした設定変更に関する監査レコードなどが含まれます。
- パフォーマンス：これには、トラフィック統計情報、アプリケーションメトリック、音声メトリックなどの保証データが含まれます。
- システム ヘルス レコード：これには、Prime Infrastructure 管理者ダッシュボードに表示されるほとんどのデータが含まれます。

これらの集約タイプの保持期間はデフォルト値、最小値、および最大値として定義されます（下記の表参照）。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [データの保持（Data Retention）]** ページを使用して、集約データの保持期間を定義します。集約タイプには、時間単位、日単位、および週単位があります。

表 *10 :* 集約履歴データの保持期間

傾向データの保存期間			
期間	**デフォルト**	**最小**	**最大**
時単位	7 日間	1 日間	31 日
日単位	90 日間	7 日間	365 日
週単位	54 週間	2 週間	108 週間
デバイス ヘルス データの保存期間			
時単位	15 日間	1 日	31 日
日単位	90 日間	7 日間	365 日間
週単位	54 週間	2 週間	108 週間
パフォーマンス データの保存期間			
短期データ	7 日間	1 日	31 日
中期データ	31 日	7 日間	365 日
長期データ	378 日間	2 日間	756 日間
ネットワーク監査データの保存期間			

すべての監査データ	7 日間	7 週間	365 日
システム ヘルス データの保存期間			
時単位	7 日間	1 日	31 日
日単位	31 日	7 日間	365 日
週単位	54 週間	7 週間	365 日間
ユーザージョブデータの保持期間			
週 1 回	7 日間	2 日間	365 日

パフォーマンス データは次のように集約されます。

- 短期データは 5 分ごとに集約されます。
- 中期データは 1 時間ごとに集約されます。
- 長期データは 1 日ごとに集約されます。

パフォーマンスおよびシステムのヘルス データ保持

（注） デフォルト設定はインタラクティブ グラフから最も役立つ情報を取得するように最適化されているため、トレンド、デバイス ヘルス、システム ヘルス、およびパフォーマンス データの保持期間を変更しないことをお勧めします。

次の表に、[データの保持（Data Retention）] ページに表示される情報を示します。

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
傾向データの保持期間（Trend Data Retain Periods）	デバイス関連の履歴情報。トレンド データは全体として収集され、最小、最大、または平均として要約されます。	毎時データの保持期間：15（日） 日次データの保持期間：90（日） 週次データの保持期間：54（週）	時間単位のデータ：1 ～ 31（日） 日単位のデータ：7 ～ 365（日） 週単位のデータ：2 ～ 108（週）

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
デバイスヘルスデータの保持期間（Device Health Data Retain Periods）	デバイスの到達可能性などの SNMP ポーリングされたデバイスデータ、およびCPU、メモリ、インターフェイスの使用率。	毎時データの保持期間：15（日） 日次データの保持期間：90（日） 週次データの保持期間：54（週）	時間単位のデータ：1 ー 31（日） 日単位のデータ：7 ー 365（日） 週単位のデータ：2 ～ 108（週）
パフォーマンスデータの保持期間（Performance Data Retain Periods）	トラフィック統計などの保証データ。 • 短期データは 5 分ごとに集約されます。 • 中期データは 1 時間ごとに集約されます。 • 長期データは 1 日ごとに集約されます。 （注） **[詳細設定（Advanced Settings）]** をクリックして、使用可能な属性の **[経過時間（日）（Age (In days)）]** と **[最大レコード数（Max Records）]** を設定できます。	短期データの保持期間：7（日） 中期データの保持期間：31（日） 長期データの保持期間：378（日）	短期の範囲：1 ー 31（日） 中期の範囲：7 ー 365（日） 長期の範囲：2 ー 756（日）
ユーザージョブデータ保持期間	完了状態のユーザージョブのすべてのレコード。	ユーザージョブデータ保持期間：7（日）	2 ～ 365（日）

データのタイプ	説明	デフォルトの保持設定	保持設定範囲
システムヘルスデータの保持期間（System Health Data Retain Periods）	管理ダッシュボードに表示されるほとんどのデータが含まれます。	毎時データの保持期間：1（日） 日次データの保持期間：7（日） 週次データの保持期間：54（週）	時間単位のデータ範囲：1 ー 31（日） 日単位のデータ範囲：7 ー 365（日） 週単位のデータ範囲：2 ー 108（週）

データベース テーブル別のデータ保持の指定

管理者は、[データの保持（Data Retention）] ページの [その他のデータ保持条件（Other Data Retention Criteria）] セクションを使用して、特定の Prime Infrastructure データベース テーブルの保持期間を設定できます。次の属性を使用して保持期間を指定できます。

- **Age (in hours)**：データベース内のすべてのレコードの最大データ保持期間を時間の単位で指定します。
- **Max Records**：特定のデータベースに保持するレコードの最大数を指定します。[最大レコード数（Max Records）] の値が「NA」の場合、考慮される保持条件が [経過時間（Age）] 属性のみであることを意味します。

セクションは、複数のサブセクションに分類されます。それぞれのサブセクションには、各データベース テーブル名と現在の Age および Max Records の値が一覧表示されます。これらの値によって、テーブル内の個々のレコードが保持されるか破棄されるかが決定されます。このページには、テーブル内のデータの期間経過を計算するために使用される [経過時間（Age）] 属性テーブルも一覧表示されます。オプティカル デバイスのカテゴリは、Prime Infrastructure の適用対象外です。

このセクションのいずれかのテーブルの値を変更するときは、事前に Cisco Technical Assistance Center に相談することを強くお勧めします。支援なしに変更すると、システム パフォーマンスに悪影響を与える可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）]l > [データの保持（Data Retention）]** の順に選択します。

ステップ 2 [その他のデータ保存基準（Other Data Retention Criteria）] セクションを展開します。

ステップ 3 Age および Max Records の値を指定するデータベース テーブル サブセクションを展開します。

ステップ 4 一覧表示しているデータベース テーブルをクリックし、必要に応じて新しい値を入力します。

ステップ 5 [保存（Save）] をクリックします。

クライアント データの収集と保存の指定

管理者は、Prime Infrastructure の [クライアント（Client）] ページを使用して、次のようなネットワーク クライアント上のデータの保存に影響するパラメータを設定できます。

- アソシエーション解除されたクライアントに関するデータ。デフォルトは 7 日間で、これはクライアントが再度アソシエートを試みるかどうかに関係なく適用されます。
- クライアント セッション履歴に関するデータ。Prime Infrastructure データベース内の行数として、維持するセッション エントリの最大数を指定することもできます。
- DNS サーバーから取得してキャッシュされたクライアント ホスト名。

これらのデータ保存オプションに加えて、このページでは次のオプションを有効または無効にすることができます。

- クライアントからトラップが受信されたときに、自動的に診断チャネルを使用してそのクライアントを修復します。
- 自動的に DNS サーバからクライアント ホスト名を取得します。
- クライアントからトラップまたは syslog が受信されたときに、そのクライアントをポーリングします。
- 拡張クライアント トラップからクライアントを検出します。
- トランク ポートで有線クライアントを検出します。
- ルーチン クライアント アソシエーションおよびアソシエーション解除トラップおよび syslog を Prime Infrastructure イベントとして保存します。このオプションは、この種のトラップや syslog が膨大な数になる期間（ネットワーク セットアップなど）の大規模ネットワーク上の Prime Infrastructure のパフォーマンス問題を回避するために、デフォルトで無効になっています。それ以外の期間は、このオプションを有効にすることができます。
- すべての 802.1x および 802.11 クライアント認証失敗トラップを Prime Infrastructure イベントとして保存します。このオプションは、この種のトラップや syslog が膨大な数になる期間（ネットワーク セットアップなど）の大規模ネットワーク上の Prime Infrastructure のパフォーマンス問題を回避するために、デフォルトで無効になっています。ネットワークが安定している場合は、このオプションを有効にすることができます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [クライアントとユーザー（Client and User）] > [クライアント（Client）]** の順に選択します。

ステップ 2 [データの保持（Data Retention）] で、必要に応じて値を変更します。

ステップ 3 [保存（Save）] をクリックします。

データ重複排除の有効化

データ重複除去を使用すれば、次のクラスのアプリケーションデータごとに権限のあるソースを特定することができます。

- TCP アプリケーションのアプリケーション応答時間データ
- すべてのアプリケーションのトラフィック分析データ
- RTP アプリケーションの音声/ビデオデータ

Prime Infrastructure は、ネットワークの要素とプロトコルに関するすべての受信データを保存します。これには、複数のソースから受信した重複データも含まれます。信頼できるデータ ソースを指定した場合は、特定の場所やサイトを開いたときに、指定したソースからのデータだけが表示されます。

[データ重複除去（Data Deduplication）]ページを使用すれば、特定の場所にある信頼できるデータ ソースを 1 つまたは複数指定できます。たとえば、ブランチ オフィスのネットワーク解析モジュール（NAM）に加えて、同じブランチから送信された NetFlow データもある場合は、その場所の NAM または NetFlow データだけを Prime Infrastructure で表示するように選択できます。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ重複排除（Data Deduplication）]** を選択します。

ステップ 2 [データ重複除去の有効化（Enable Data Deduplication）] チェックボックスをオンにして、[適用（Apply）] をクリックします。[Data Deduplicatio] ページに定義済みの場所グループが一覧表示されます。

ステップ 3 すべての場所にある信頼できるソースを自動的に検出するには、[自動検出（Auto-Detect）] をクリックします。これにより特定されると、アプリケーション データの各クラスのソースを一覧表示する列の下にあるリスト ボックスに、信頼できるソースのアドレスが Prime Infrastructure によって入力されます。

ステップ 4 特定の場所にあるアプリケーション データのクラスの信頼できるソースを指定するには、次のように操作します。

a) 場所グループ名をクリックします。
b) 信頼できるソースを指定するアプリケーション データのクラスの下にあるドロップダウン リスト ボックスをクリックします（例えば、[Application Response Time] の下にあるリスト ボックスをクリック）。
c) ドロップダウン リストから、その場所およびアプリケーション データのタイプに関して信頼できるソースとして指定するデータ ソースを選択します。次に [OK] をクリックします。
d) [Save] をクリックして選択内容を保存します。

信頼できるデータ ソースを指定する対象となる場所およびアプリケーション データのタイプのそれぞれに対し、必要に応じてこの手順を繰り返します。

ステップ 5 終了したら、[適用（Apply）] をクリックして変更内容を保存します。

レポートの保存と保持の制御

すべての定期レポートが定期レポートリポジトリに格納されます。定期レポートは、妥当な期間だけリポジトリ内に保持しておいて、定期的に削除する必要があると考えられます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）]l > [レポート（Report）]** の順に選択します。[レポート（Report）] ページが表示されます。

ステップ 2 [リポジトリ パス（Repository Path）] で、Prime Infrastructure サーバー上のレポート リポジトリ パスを指定します。

ステップ 3 [ファイルの保持期間（File Retain Period）] で、レポートを保持する最大日数を指定します。

ステップ 4 [Save] をクリックします。

イベント受信後のインベントリ収集の指定

[インベントリ（Inventory）] ページで、デバイスの syslog イベントが受信された場合に、Prime Infrastructure でインベントリを収集するかどうかを指定できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）]** の順に選択します。[インベントリ（Inventory）] ページが表示されます。

ステップ 2 [イベント ベースのインベントリ収集の有効化（Enable event based inventory collection）] チェックボックスをオンにして、Prime Infrastructure がデバイスの syslog イベントを受信した場合にインベントリを収集できるようにします。

ステップ 3 Prime Infrastructure が新しく追加されたデバイスに関する syslog 通知とトラップ通知を有効にできるようにする場合は、[デバイスに関する syslog とトラップを有効にする（Enable Syslog and Traps on device）] チェックボックスをオンにします。

（注） この機能は、Cisco Nexus ではサポートされません。

ステップ 4 [Save] をクリックします。

設定導入動作の制御

管理者は、Prime Infrastructure ユーザーが新しいデバイス設定テンプレートを導入するたびに、デバイス設定をバックアップまたはロールバックするかどうかを選択できます。また、Cisco WLC 設定のアーカイブ方法も制御できます（下記の「関連項目」を参照）。

関連トピック

テンプレート導入前のデバイス設定のアーカイブ （178 ページ）
テンプレート導入失敗時のデバイス設定のロールバック （178 ページ）
WLC 設定をいつどのようにアーカイブするかの指定 （178 ページ）

テンプレート導入前のデバイス設定のアーカイブ

[デバイス設定のバックアップ（Backup Device Configuration）] が有効になっている場合は、新しい設定テンプレートが導入される前に、Prime Infrastructure が自動的にすべてのデバイスの実行コンフィギュレーションとスタートアップ コンフィギュレーションをバックアップします。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [設定（Configuration）]** を選択します。

ステップ 2 [Backup Device Configuration] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。

関連トピック

テンプレート導入失敗時のデバイス設定のロールバック （178 ページ）

テンプレート導入失敗時のデバイス設定のロールバック

[ロールバック設定（Rollback Configuration）] が有効になっている場合は、新しい設定テンプレートのデバイスへの導入に失敗した場合に、Prime Infrastructure が自動的に最後にアーカイブされた実行コンフィギュレーションとスタートアップ コンフィギュレーションに各デバイスをロールバックします。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [設定（Configuration）] の順に選択します。

ステップ 2 [Rollback Configuration] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。

WLC 設定をいつどのようにアーカイブするかの指定

デフォルトで、Prime Infrastructure は、次の場合にいつでも、Cisco Wireless LAN Controller（WLC）ソフトウェアを実行している各デバイスのスタートアップ コンフィギュレーションのバックアップ アーカイブを維持します。

- これらのデバイスの初期インベントリを収集した場合
- これらのデバイスの設定変更イベントの通知を受信した場合

Prime Infrastructure は、Cisco WLC ソフトウェアを実行しているデバイスのコンフィギュレーション アーカイブ サポートを提供します。コンフィギュレーション アーカイブには、スタートアップ コンフィギュレーションのみが含まれています。実行コンフィギュレーションはコンフィギュレーション アーカイブから除外されます。

次のような、Cisco WLC 設定アーカイブを制御するさまざまな基本パラメータを変更できます。

- すべての Cisco WLC 設定操作（フェッチ、アーカイブ、またはロールバック）の最大タイムアウト。
- Cisco WLC 設定アーカイブ サマリー情報の更新を待機する最大時間。
- 初期インベントリ収集時、各インベントリの同期後、および設定変更イベントの受信時に設定をアーカイブするかどうか。
- アーカイブした設定をファイルにエクスポートするときにセキュリティ情報をマスクするかどうか。
- 各デバイスのアーカイブした設定の最大数とそれらを保持する最大日数。
- アーカイブ操作に使用するスレッド プールの最大数。デフォルトを増やすと、1,000 を超えるデバイスが関係する変更をアーカイブする間の Prime Infrastructure のパフォーマンスに役立つ可能性があります。

また、アーカイブの目的で、特定のファミリ、タイプ、またはモデルのデバイス上で指定したコマンドが関係するすべての変更を無視するように Prime Infrastructure に指示することもできます。これは、1 つ以上のデバイスの一部のパラメータの重要でない変更または定常的に発生する変更を無視する場合に便利です。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [設定アーカイブ（Configuration Archive）]** の順に選択します。

ステップ 2 [基本（Basic）] タブで、必要に応じて基本的なアーカイブ パラメータを変更します。

（注） エクスポート中にセキュリティ コンテンツをマスキングするオプションが、[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[設定アーカイブ（Configuration Archive）] ページに表示されます。詳細については、Download Configuration Filesを参照してください。

ステップ 3 アーカイブする設定から除外するデバイスと設定コマンドを指定するには、次の手順を実行します。

a) [Advanced] タブをクリックします。

b) [Product Family] リストで、除外する設定コマンドを指定するデバイスを選択します。

リスト/ツリー ビュー ドロップダウンを使用するか、>アイコンをクリックして、除外コマンドを指定する個別の製品タイプとモデルにドリルダウンします。

c) [コマンド除外リスト（Command Exclude List）] で、現在選択されているファミリ、タイプ、またはモデルから除外する設定コマンドを（カンマで区切って）入力します。

選択したデバイスに設定変更がされていても、その変更が除外リストで指定されたコマンドの 1 つであることを Prime Infrastructure が検出した場合、Prime Infrastructure はその変更を含む設定のアーカイブ バージョンを作成しません。

d) [保存（Save）] をクリックします。

e) デバイス ファミリ、タイプ、またはモデルに対して指定された一連のコマンド除外を削除するには、[製品ファミリ（Product Family）] リストでデバイスを選択して、[リセット（Reset）] をクリックします。

アラーム、イベント、および Syslog の消去

（注） これらのデフォルトの消去設定は、最適なパフォーマンスを保証するために用意されています。これらの設定を調整するときには、特に が非常に大規模なネットワーク（これらの設定値を大きくすると悪影響が生じる可能性がある）を管理している場合に注意が必要です。

は、最大 8000000 個のイベントと 2000000 個の syslog をデータベースに格納します。

システム パフォーマンスを保護するため、 は次の表の設定に従ってアラーム、イベント、およびsyslogを消去します。これらの設定はすべてデフォルトで有効化されます。データは毎日削除されます。アラームテーブルは毎時チェックされ、アラームテーブルが300,000の上限を超えた場合、 は、アラーム テーブルのサイズが制限内に収まるまで、最も古いクリア済みアラームを削除します。

データ タイプ	削除されるまでの日数：	デフォルト設定
アラーム：クリア済みのセキュリティ アラーム	30日間	[有効（Enabled）]
アラーム：クリア済みの非セキュリティ アラーム	7 日	[有効（Enabled）]
イベント	60 日	[有効（Enabled）]
Syslogs	30日間	[有効（Enabled）]
アラーム	30日間	無効

設定を変更するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択して、**[アラームおよびイベント（Alarms and Events）]** > **[アラームおよびイベント（Alarms and Events）]** を選択し、[アラームおよびイベントのクリーンアップ オプション（Alarm and Event Cleanup Options）] エリアの設定を変更します。

ログの消去

ログの消去設定を調整するには、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択します。ログは最大サイズに達するまで保存されます。最大サイズに達した時点で、ログファイルに番号が追加され、新しいログが開始されます。ログの数が最大数を超えると、最も古いログが削除されます。

次の表に、一般ログと SNMP ログのデフォルトの消去値をリストします。

ログ タイプ	ログのサイズ	ログの数	設定を変更する場合の参照先：

一般	10 MB	10	一般的なログ ファイルの設定とデフォルト サイズの調整 （307 ページ）
SNMP	10 MB	5	一般的なシステム ログを表示して管理する（307 ページ）

レポートの消去

デフォルトでは、レポートは/localdisk/ftp/reports という名前のリポジトリに保管され、31 日が経過するとこのディレクトリから削除されます。フィルタ ページで設定したレポート フィルタはデータベースに保存され、消去されることはありません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[一般（Genera）] > [レポート（Reports）]** を選択します。

ステップ 2 必要に応じて、サーバー上のレポート リポジトリの場所を変更します。リポジトリは、FTP ルート パーティションの下になければなりません。

ステップ 3 デフォルトの消去までの経過期間を変更する場合は、[ファイルの保持期間（File Retain Period）] フィールドに新しい値を入力します。

ステップ 4 [保存（Save）] をクリックします。

バックアップの消去

デフォルトで、2つのバックアップがローカル リポジトリに保存されます。リモート リポジトリを使用している場合は、自動バックアップ消去メカニズムがありません。古いバックアップを手動で削除する必要があります。保存する自動アプリケーション バックアップ数の変更 （67 ページ）を参照してください。

デバイス コンフィギュレーション ファイルの消去

デバイスごとに、5つのコンフィギュレーション ファイルが設定アーカイブに保存されます。30 日より前のファイルは消去されます。デバイス コンフィギュレーション ファイルは手動で削除することができません。。

ソフトウェア イメージ ファイルの消去

デバイス ソフトウェア イメージ ファイルは、データベースから自動的には消去されません。このファイルは、GUI クライアントを使用して手動で削除する必要があります。

システム ジョブの制御

Prime Infrastructure では、スケジュール設定されたデータ収集ジョブを定期的に実行します。各ジョブのスケジュールを変更したり、ジョブを一時停止、再開、または即時実行できます。

これらのシステム ジョブを無効化または制限すると、Prime Infrastructure の使用、特にレポート作成に直接影響する可能性があります。このような影響を考慮するには、そのデータが使用されるレポートに注目してください。

関連トピック

データ収集ジョブのスケジューリング （182 ページ）
データ収集ジョブの再開 （182 ページ）
データ収集ジョブの即時実行 （183 ページ）
システム ジョブについて （183 ページ）

データ収集ジョブのスケジューリング

システム ジョブは、「システム ジョブについて」で説明しているとおり、デフォルトの定期スケジュールで実行されます。必要に応じてこれらのスケジュールを再設定できます。

ステップ 1 **[管理（Administration）]>[ダッシュボード（Dashboard）]>[ジョブ ダッシュボード（Job Dashboard）]>[システム ジョブ（System Jobs）]** の順に選択します。

ステップ 2 スケジュールを再設定するデータ収集ジョブのカテゴリ（たとえば[APIC-EM 統合（APIC-EM Integration）]、[保証とヘルスの要約（Assurance and Health Summary）]、[インフラストラクチャ（Infrastructure）]、[インベントリとディスカバリ（Inventory and Discovery）]、[ステータスとワイヤレスのモニタリング（Status and Wireless Monitoring）] など）を選択します。

ステップ 3 スケジュールを再設定するシステム ジョブの横にあるチェックボックスをクリックします。

ステップ 4 [Edit Schedule] をクリックし、ジョブの実行スケジュールを指定します。

ジョブが実行される日付と時刻を指定できます。ジョブの繰り返しとして、1 分に 1 回、1 時間に 1 回、週 1 回、月 1 回、年 1 回を選択できます。デフォルトでは終了時刻は指定されていません。

ステップ 5 終了したら、[送信（Submit）] をクリックします。

データ収集ジョブの再開

スケジュール設定されたデータ収集ジョブの一時停止や、すでに一時停止されたジョブの再開ができます。

ステップ 1 **[管理（Administration）]>[ダッシュボード（Dashboard）]>[ジョブ ダッシュボード（Job Dashboard）]>[システム ジョブ（System Jobs）]** の順に選択します。

ステップ 2 停止または再開するデータ収集ジョブのカテゴリ（たとえば [APIC-EM 統合（APIC-EM Integration）]、[保証とヘルスの要約（Assurance and Health Summary）]、[インフラストラクチャ（Infrastructure）]、[インベントリとディスカバリ（Inventory and Discovery）]、[ステータスとワイヤレスのモニタリング（Status and Wireless Monitoring）] など）を選択します。

ステップ 3 目的のシステム ジョブの横にあるチェックボックスをクリックします。

ステップ 4 [Pause Series] をクリックすると、ジョブの実行が停止します。

ジョブがすでに一時停止されている場合は、[シリーズの再開（Resume Series）] をクリックすると、現在のスケジュールに基づいて実行が再開されます。

データ収集ジョブの即時実行

下記の手順に加え、ジョブのスケジュールを再設定して、実行時刻として [今すぐ（Now）] を選択して送信すると、ジョブを即時に実行できます。その後、このジョブを選択し、[実行（Run）] をクリックします。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboard）]** > **[ジョブ ダッシュボード（Job Dashboard）]** > **[システム ジョブ（System Jobs）]** の順に選択します。

ステップ 2 実行するデータ収集ジョブのカテゴリ（たとえば [APIC-EM 統合（APIC-EM Integration）]、[保証とヘルスの要約（Assurance and Health Summary）]、[インフラストラクチャ（Infrastructure）]、[インベントリとディスカバリ（Inventory and Discovery）]、[ステータスとワイヤレスのモニタリング（Status and Wireless Monitoring）] など）を選択します。

ステップ 3 即時実行するシステム ジョブの横にあるチェックボックスをクリックします。

ステップ 4 [Run] をクリックします。

システム ジョブについて

次の表に、Prime Infrastructure が実行するバックグラウンド データ収集ジョブの説明を示します。

（注） インフラストラクチャジョブとインベントリジョブはI/O高集約型の操作を行うことからPrime Infrastructure のパフォーマンスに一定期間影響を与えるため、これらジョブの頻度を増やす場合は注意が必要があります。

表 *11* : インベントリ データ収集ジョブ

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
APIC EM 統合ジョブ			

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
APIC-EM サイトの同期（APIC-EM Site Sync）	6 時間	APIC-EM と Prime Infrastructure の間でのサイトとデバイスの同期をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
APIC サーバーのステータス定期確認（APIC Server Status Periodic）	5 分	APIC-EM サーバーが到達可能であるか確認する作業をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ネットワークデバイスへの ping の送信	5 分	ICMP ping の到達可能性をスケジュールし、デバイスの到達可能性ステータスと遅延時間を更新します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
PnP の一括インポート（PnP Bulk Import）	5 分	APIC-EM から Prime Infrastructure へのデバイスプロファイルの一括インポートをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
PnP ステータスのポーリング（PnP Status Polling）	5 分	APIC-EM で作成した PnP デバイスのステータスを追跡し、正常であればそのデバイスを Prime インベントリに追加します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ポスト PnP ジョブ（Post PnP Job）		デバイス上でのポスト PnP 設定の検証をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
保証とヘルスの要約ジョブ			

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
AGGREGATION_HEALTH_SUMMARY	無効	デバイス メトリック（ルータ、スイッチ、アクセスポイントなど）のヘルス スコアを集計します。	編集不可
保証のデータ ソースの更新（Assurance DataSource Update）	無効	PI の異なる 2 つのプロセスの間でデータ ソースの一覧を同期します。	編集不可
保証のライセンスの更新（Assurance License Update）	無効	12 時間ごとに、デバイスとそれに関連付けられている AP を取得します。	編集不可
保証の Lync の集計（Assurance Lync Aggregation）	無効	Lync の通話統計情報を計算します。	編集不可
BASELINE_DAILY	無効	時間単位の基準値を集計して、アプリケーション データの日単位の値を算出します。	編集不可
BASELINE_HOURLY	無効	アプリケーション データの時間単位の基準データ ポイントを計算します。	編集不可
DAHealth_SITE	無効	PI の異なる 2 つのプロセスの間でサイト ルールを同期します。	編集不可
HEALTH_SUMMARY_5MIN	無効	アプリケーションのヘルス スコアを計算します。	編集不可
PushCollectionPlanToDA	無効	コレクション プランを DA にプッシュします。	編集不可
WUserSyncJob_USER	無効	ステーション キャッシュから現在のクライアントの一覧を取得し、NetFlow ユーザー キャッシュを更新します。	編集不可
インフラストラクチャ ジョブ			

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
一括再計算 RF 予測（Bulk Recompute RF Prediction）	15 日	一括再計算 RF 予測のステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
接続先のモビリティ到達可能性ステータス（Connected Mobility Reachability Status）	5 分	接続先のモビリティ到達可能性のステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
コントローラ設定のバックアップ（Controller Configuration Backup）	1 日	コントローラ設定のバックアップ アクティビティが表示されます。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
データのクリーンアップ（Data Cleanup）	2 時間	日単位のデータ ファイルのクリーンアップをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。 s

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
デバイス設定の外部バックアップ（Device Config Backup-External）	15 分	デバイス設定を定期的に外部リポジトリに転送します。リポジトリの設定や作成は CLI コマンドで行うことができます。サポートされているリポジトリは FTP、SSH FTP（SFTP）、ネットワーク ファイル システム（NFS）です。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。 [編集（Edit）] アイコンをクリックし、[最新の設定のみをエクスポートする（Export only Latest Configuration）] チェックボックスをオンにすると、最新の設定のみが転送されます。 ロールベース アクセス コントロール（RBAC）で設定されたユーザー権限に基づいて、ジョブのプロパティを編集することができます。
ゲスト アカウントの同期（Guest Accounts Sync）	1 日	ゲスト アカウントのポーリングと同期をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
インデックス検索エンティティ（Index serach Entities）	3 時間	インデックス検索エンティティのジョブをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
モビリティサービスのバックアップ（Mobility Service Backup）	7 日	モビリティ サービスの自動バックアップをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
モビリティ サービスのステータス（Mobility Service Status）	5 分	モビリティ サービスのステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
モビリティ サービスの同期（Mobility Service Synchronization）	1 時間	モビリティ サービスの同期をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
オン デマンド レポート クリーンアップ（On Demand Reports Cleanup）	6 時間	レポートのクリーンアップをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
サーバーのバックアップ（Server Backup）	1 日	Prime Infrastructure サーバーの自動バックアップをスケジュールします。作成されるバックアップは、アプリケーション バックアップです。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。 （注） サーバーバックアップジョブは、1時間ごとではなく、1日1回スケジュールすることをお勧めします。
スマート ライセンスのコンプライアンス ステータス（Smart License Compliance Status）	無効	スマート ライセンスに対してデフォルトのスケジュールで実行されます。	編集不可。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
wIPS アラームの同期（wIPS Alarm Sync）	2 時間	wIPS アラームの同期をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
インベントリおよびディスカバリ ジョブ			
自律 AP インベントリ（Autonomous AP Inventory）	1 日	自律 AP のインベントリ情報を収集します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
スイッチインベントリ（Switch Inventory）	1 日	スイッチに関するインベントリ情報を収集します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ワイヤレス コントローラ インベントリ（Wireless Controller Inventory）	1 日	ワイヤレス コントローラに関するインベントリ情報を収集します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ステータス ジョブ			

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
アプライアンス ステータス（Appliance Status）	5 分	アプライアンスのポーリングをスケジュールします。このタスクでは、[管理（Administration）] > [アプライアンス（Appliance）] > [アプライアンス ステータス（Appliance Status）] ページからアプライアンスのポーリングの詳細が読み込まれます。また、アプライアンスがパフォーマンスや障害を確認できるかどうかに関する情報なども読み込まれます。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
自律型クライアントのステータス（Autonomous Client Status）	5 分	自律 AP クライアントのステータス ポーリングをスケジュールできるようにします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
自律型 AP の動作ステータス（Autonomous AP Operational Status）	5 分	自律型ワイヤレス アクセス ポイントのステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
コントローラの動作ステータス（Controller Operational Status）	5 分	コントローラの動作ステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
デバイス データ コレクター（Device Data Collector）	30 分	設定した時間間隔で指定したコマンドラインインターフェイス（CLI）コマンドに基づいてデータ収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Identity Services Engine ステータス（Identity Services Engine Status）	15 分	Identity Services Engine のポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
干渉（Interferers）	15 分	干渉の情報収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
Unified AP ping 機能の学習（Learn Unified AP Ping Capability）	このジョブは、一時停止状態で、オンデマンドで動作します。	Unified AP ping 機能情報の収集をスケジュールします。	編集不可。
ライセンス ステータス（License Status）	4 時間	ライセンス ステータス情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
Lightweight AP のイーサネット インターフェイスのステータス（Lightweight AP Ethernet Interface Status）	1 分	Lightweight AP のイーサネット インターフェイスのステータス情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
Lightweight AP の動作ステータス（Lightweight AP Operational Status）	5 分	Lightweight AP の動作ステータス情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
Lightweight クライアントのステータス（Lightweight Client Status）	5 分	ネットワークからの Lightweight AP クライアントの情報収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
モビリティ サービスのパフォーマンス（Mobility Service Performance）	15 分	モビリティ サービスのパフォーマンスのステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
モビリティ ステータス タスク（ Mobility Status Task）	15 分	Mobility Services Engine のステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
OSS サーバー ステータス（OSS Server Status）	5 分	OSS サーバーのステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
冗長ステータス（Redundancy Status）	1 時間	プライマリおよびセカンダリ コントローラの冗長性ステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
スイッチのNSMPおよびロケーション ステータス（Switch NMSP and Location Status）	4 時間	スイッチ ネットワーク モビリティ サービス プロトコル（NMSP）およびシビック ロケーション ステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
スイッチの動作ステータス（Switch Operational Status）	5 分	スイッチの動作ステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
サードパーティ アクセス ポイントの動作ステータス（Third party Access Point Operational Status）	3 時間	サードパーティ AP の動作ステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
サードパーティ コントローラの動作ステータス（Third party Controller Operational Status）	3 時間	サードパーティ コントローラの動作ステータス ポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
管理対象外 AP（Unmanaged APs）	15 分	管理対象外アクセス ポイントに関するポーリング情報を収集します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
有線クライアント ステータス（Wired Client Status）	2 時間	ワイヤレス クライアントのステータスのポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ワイヤレス AP 検出（Wireless AP Discovery）	5 分	ワイヤレス AP 検出をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ワイヤレス設定の監査（Wireless Configuration Audit）	1 日	ワイヤレス設定エージェント監査情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
無線モニタリング ジョブ			

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
AP イーサネット統計（AP Ethernet Statistics）	15 分	APイーサネット統計の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
AP イメージの事前ダウンロードのステータス（AP Image Pre-Download Status）	15 分	コントローラの関連 AP のイメージ プレダウンロード ステータスを確認できます。アクセス ポイントのステータスを表示するには、コントローラにソフトウェアをダウンロードしている間に [AP へのソフトウェアの事前ダウンロード（Pre-download software to APs）] チェックボックスをオンにする必要があります。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
自律型 AP CPU とメモリの使用率（Autonomous AP CPU and Memory Utilization）	15 分	自律 AP のメモリおよび CPU 使用率に関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
自律 AP の無線パフォーマンス（Autonomous AP Radio Performance）	15 分	無線パフォーマンスに関する情報や、自律 AP の無線アップまたはダウン ステータスの収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
自律 AP Tx の電力とチャネルの使用率（Autonomous AP Tx Power and Channel Utilization）	15 分	自律 AP の無線パフォーマンスに関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
CCX クライアントの統計情報（CCX Client Statistics）	1 時間	CCX バージョン 5 およびバージョン 6 クライアントの Dot11 およびセキュリティ統計情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
CleanAir 電波品質（CleanAir Air Quality）	15 分	CleanAir の電波品質に関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
クライアント統計情報（Client Statistics）	15 分	自律および軽量クライアント用の統計情報の取得をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
マップ情報ポーリング ジョブ（Map Info Polling Job）	1 分		[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
メディア ストリーム クライアント（Media Stream Clients）	15 分	メディア ストリーム クライアントに関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
メッシュ リンクのステータス（Mesh Link Status）	5 分	メッシュ リンクのステータスの収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
メッシュ リンクのパフォーマンス（Mesh link Performance）	10 分	メッシュ リンクのパフォーマンスに関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
無線パフォーマンス（Radio Performance）	15 分	ワイヤレス無線からの統計情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
無線音声パフォーマンス（Radio Voice Performance）	15 分	ワイヤレス無線からの音声統計情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
不正 AP（Rogue AP）	2 時間	不正アクセス ポイントに関する情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
スイッチの CPU とメモリのポーリング（Switch CPU and Memory Poll）	30 分	スイッチの CPU とメモリの情報のポーリングをスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
トラフィック ストリーム メトリック（Traffic Stream Metrics）	8 分	クライアントのトラフィック ストリーム メトリックを取得します。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
ワイヤレス コントローラのパフォーマンス（Wireless Controller Performance）	30 分	ワイヤレス コントローラのパフォーマンス統計情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。
ワイヤレス QoS 統計（Wireless QoS Statistics）	15 分	ワイヤレス コントローラの QoS 統計情報の収集をスケジュールします。	[スケジュールの編集（Edit Schedule）] > [繰り返し（Recurrencce）] の順に選択し、ジョブをスケジュールするための適切な設定を選択します。

Cisco Prime LMS から Cisco Prime Infrastructure へのデータの移行

Prime Infrastructure は、すべてのプラットフォーム上で Cisco Prime LAN Management Solution（LMS）バージョン 4.2.5 からのデータ移行をサポートしています。次の LMS データを CAR CLI を使用して Prime Infrastructure にインポートできます。

- Device Credential and Repository（DCR）デバイス
- Static Groups
- Dynamic Groups
- Software Image Management Repository Images
- User Defined Templates（Netconfig）
- LMS Local Users
- MIB

LMS からインポートできるのは、次の属性を使用したルールを含む Dynamic Groups だけです。

- PI attribute Name—LMS attribute name
- Contact—System.Contact
- Description—System.Description
- Location— System.Location
- Management_Address—Device.ManagementIpAddress
- Name—System.Name
- Product_Family—Device.Category
- Product_Series—Device.Series
- Product_Type—Device.Model
- Software_Type—System.OStype
- Software_Version：Image.Version

LMS データを Prime Infrastructure に移行するには、次の手順を実行します。

ステップ 1 LMS バックアップ データが格納されているサーバーを特定します。

ステップ 2 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 3 次のコマンドを入力して、バックアップの場所を設定します。

admin# **configure terminal**

admin(config)# **repository carsapps**

admin(config-Repository)# **url** *location*

admin(config-Repository)# **user root password plain** *password*

admin(config-Repository)# **end**

引数の説明

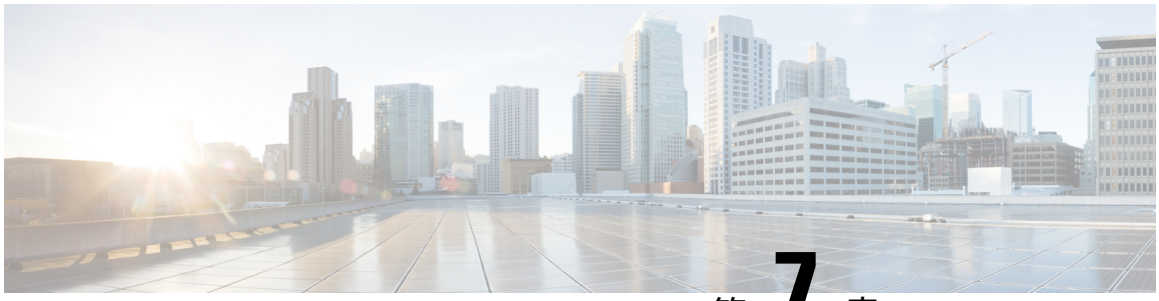
1. *location* は、LMS バックアップ データの場所の、アクセス プロトコルを含む完全修飾 URL です。例：ftp://10.77.213.137/opt/lms、sftp://10.77.213.137/opt/lms、または fdisk:foldername。
2. *password* は root ユーザー パスワードです。

ステップ 4 次のコマンドを使用して LMS バックアップを Prime Infrastructure にインポートします。

admin# **lms migrate repository carsapps**

ステップ 5 CLI セッションを終了して、Prime Infrastructure ユーザー インターフェイスにログインし直し、LMS データが正常にインポートされたことを確認します。次の表に、Prime Infrastructure でインポートした LMS データを確認する場所を示します。

LMS データ	**Prime Infrastructure での場所**
DCR デバイス	[Inventory] > [Network Devices]
Static Group	[Inventory] > [Network Devices] > [User Defined Group]
Dynamic Group	[Inventory] > [Network Devices] > [User Defined Group]
Software Image Management Repository Images	[Inventory] > [Software Images]
User Defined Templates（Netconfig）	[Configuration] > [Templates] > [Features & Technologies]
LMS Local Users	[Administration] > [Users, Roles & AAA] > [Users]
MIB	[Monitor] > [Monitoring Policies] メニューで、[追加（Add）] をクリックしてから、[ポリシー タイプ（Policy Types）] > [カスタム MIB ポーリング（Custom MIB Polling）] の順に選択します。



第 7 章

ユーザー権限とデバイス アクセス

ユーザーインターフェイス、ユーザータイプ、およびそれらの間の遷移

これらのトピックでは、 で使用される GUI と CLI インターフェイス、および と Linux CLI インターフェイス間の遷移について説明します。

ユーザー インターフェイスとユーザー タイプ

次の表に、 によって採用されたユーザー インターフェイスと、各インターフェイスにアクセス可能なユーザーのタイプの説明を示します。

ユーザー インターフェイス	インターフェイスの説明	ユーザー タイプ
Web GUI	Web GUI を使用して日常業務と管理業務を容易にする Web インターフェイス。これらのユーザーは、さまざまなレベルの権限を持つことができ、ロールベース アクセス コントロール（RBAC）クラスとサブクラスに分類されます。 このインターフェイスは、 の CLI 管理ユーザーと CLI構成ユーザーによって提供される操作のサブセットを提供します。	[Web GUI通常ユーザー（Cisco EPN Manager web GUI everyday users）]：Web GUI のルートユーザーによって作成されます。このユーザーは、さまざまなレベルの権限を持ち、ユーザー グループ（管理者、スーパー ユーザー、構成マネージャなど）と呼ばれるロールベース アクセス コントロール（RBAC）クラスとサブクラスに分類されます。ユーザー グループについては、ユーザー グループのタイプ （205 ページ）を参照してください。 Web GUI ルート ユーザー：インストール時に作成され、Web GUI への 1 回目のログインと他のユーザー アカウントの作成に使用されます。このアカウントは、管理者権限を持つ少なくとも 1 人の Web GUI ユーザー、つまり、管理者ユーザーまたはスーパー ユーザー ユーザー グループに属している Web GUI ユーザーの作成後に無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （204 ページ）を参照してください。 （注） Web GUI ルート ユーザーは、Linux CLI ルート ユーザーと同じではなく、CLI管理者ユーザーとも異なります。

ユーザー インターフェイス	インターフェイスの説明	ユーザー タイプ
管理者 CLI	システムへのセキュアで限定的なアクセスを提供するシスコ独自のシェル（Linux シェルと比較した場合）。この管理者シェルと CLI は、高度な管理タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、 CLI 管理者ユーザー アクセス権を持っている必要があります。SSHを使用してリモート コンピュータからこのシェルにアクセスできます。	**CLI 管理者ユーザー**：インストール時に作成され、アプリケーションの停止と再起動やリモートバックアップリポジトリの作成などの管理操作に使用されます（この管理操作のサブセットは、Web GUI で使用できます）。 このユーザーが実行可能な操作のリストを表示するには、プロンプトで **?** と入力します。 一部のタスクは、コンフィギュレーション モードで実行する必要があります。コンフィギュレーション モードに移行するには、 管理 CLI と 構成 CLI の切り替え （202 ページ）内の手順を使用します。 管理者 CLI ユーザーは、次のコマンドを使用して、さまざまな理由で他の CLI ユーザーを作成できます。 `(config) username username password role {admin|user} password`
構成 CLI	Linux シェルよりセキュアで限定されたシスコ独自のシェル。この構成シェルと CLI は、 システム設定タスク用のコマンドを提供します。これらのコマンドについては、このガイドを通して説明します。この CLI を使用するには、管理者レベルのユーザー アクセス権を持っている必要があります（この表の [ユーザー タイプ（User Types）]列内の情報を参照）。管理者 CLI シェルでこのシェルにアクセスできます。	
Linux CLI	すべての Linux コマンドを提供する Linux シェル。Linux シェルは、シスコ テクニカル サポート担当者のみが使用できます。標準のシステム管理者は、Linux シェルを使用しないでください。SSH を使用してリモート コンピュータからこのシェルに到達することはできません。到達するには、管理者シェルと CLI を経由する必要があります。	**Linux CLI 管理ユーザー**：インストール時に作成され、Linux レベルの管理目的に使用されます。 この管理者ユーザーは、Linux CLI ルート ユーザーとしてのログインおよびログアウト （202 ページ）に記載されている手順に従って、ルートレベル権限を取得できます。ルート レベル権限が必要なタスクは、シスコ サポート チームだけが製品に関連した動作上の問題をデバッグするために実行する必要があります。セキュリティの目的で、Linux CLI 管理者ユーザーとルートユーザーは無効にする必要があります。での Linux CLI ユーザーの無効化および有効化 （203 ページ）を参照してください。

で CLI ユーザー インターフェイスを切り替える方法

次の図に、 を実行している展開上で と Linux の CLI ユーザー インターフェイスを切り替える方法を示します。

管理 CLI と 構成 CLI の切り替え

管理 CLI から 構成 CLI に移行するには、admin プロンプトで **config** と入力します。

```
(admin)# config
(config)#
```

構成 CLI から管理 CLI に戻るには、config プロンプトで **exit** または **end** と入力します。

```
(config)# exit
(admin)#
```

Linux CLI ルート ユーザーとしてのログインおよびログアウト

Linux CLI のシェル ユーザーは、管理アクセス権を持つユーザー（Linux CLI 管理者ユーザー）と、ルート アクセス権を持つユーザー（Linux CLI ルート ユーザー）の 2 つです。で CLI ユーザー インターフェイスを切り替える方法（202 ページ）に、さまざまな CLI ユーザーとしてログインおよびログアウトするためのフロー図を示しています。

Linux CLI ルート ユーザーとしてログインするには、 CLI 管理者ユーザーから Linux CLI 管理者ユーザーに移行し、さらに Linux CLI ルート ユーザーに移行する必要があります。次に、実行する必要がある具体的な手順を示します。

始める前に

Linux CLI ユーザーが無効になっている場合は、再度有効にします。での Linux CLI ユーザーの無効化および有効化 （203 ページ）を参照してください。

ステップ 1 Linux CLI ルート ユーザーとしてログインするには、次の手順を実行します。

a) サーバーで SSH セッションを開始して、 CLI 管理者ユーザーとしてログインします。

b) CLI 管理者ユーザーが Linux CLI 管理者ユーザーとしてログインします。

```
shell
Enter shell access password:  password
```

c) Linux CLI ルート ユーザーとしてログインします。

```
sudo -i
```

デフォルトでは、Linux CLI のシェル プロンプトは Linux CLI 管理者およびルート ユーザーに対するものと同じです。**whoami** コマンドを使用して、現在のユーザーを確認できます。

ステップ 2 終了するには、次の手順を実行します。

a) Linux CLI ルート ユーザーとしてログアウトします。

```
exit
```

b) Linux CLI 管理者ユーザーとしてログアウトします。

```
exit
```

これで CLI 管理者ユーザーとしてログインしていることになります。

次のタスク

セキュリティ上の理由から、Linux CLI ユーザーを無効にします。での Linux CLI ユーザーの無効化および有効化 （203 ページ）を参照してください。

Linux CLI および Web GUI のルートへのアクセスの有効化および無効化

インストール、で CLI ユーザー インターフェイスを切り替える方法 （202 ページ）の説明に従って管理者権限またはスーパーユーザー権限を持つ他の Web GUI ユーザーを 1 人以上作成したら、 Web GUI **root** ユーザーを無効にする必要があります。Web GUI ルート ユーザーの無効化および有効化 （204 ページ）を参照してください。

Linux CLI ルート ユーザーは、インストール後に無効になります。再度有効にする必要がある場合は、での Linux CLI ユーザーの無効化および有効化 （203 ページ）の手順に従います。

での Linux CLI ユーザーの無効化および有効化

この手順では、 で稼働している展開環境で Linux CLI 管理シェルを無効化および有効化する方法を説明します。シェルを無効にすると、Linux CLI 管理ユーザーまたはルート ユーザーとしてログインできなくなります。シェルが有効にされている場合、ユーザーはで CLI ユーザー インターフェイスを切り替える方法 （202 ページ）で説明している手順に従ってログインできます。

始める前に

Linux CLI 管理ユーザーのパスワードが必要です。

ステップ 1 CLI 管理ユーザーとして にログインします。サーバーとの SSH セッションの確立 （109 ページ）を参照してください。

ステップ 2 Linux CLI 管理シェルを無効にするには（Linux CLI 管理ユーザーおよびルート ユーザーが無効になります）、次のコマンドを実行します。

```
shell disable
Enter shell access password: passwd
shell access is disabled
```

ステップ 3 Linux CLI管理シェルを再び有効にするには、次のコマンドを実行します（このコマンドは、CLI管理ユーザーとして実行する必要があります）。

```
shell
Shell access password is not set
Configure password for shell access

Password: passwd
Password again: passwd

Shell access password is set
Run the command again to enter shell
```

Web GUI ルート ユーザーの無効化および有効化

ステップ 1 ルートとして Web GUI にログインし、ルート権限を持つ別の Web GUI ユーザー（つまり、管理ユーザー グループまたはスーパー ユーザー グループに属する Web GUI ユーザー）を作成します。上記のステップが完了すると、Web GUI **root** アカウントを無効化できるようになります。

ステップ 2 次のコマンドを実行して Web GUI ルート ユーザー アカウントを無効化します（Web GUI 管理アカウントはアクティブな状態に維持されるので、必要なすべての CLI 関数を実行できます）。

```
ncs webroot disable
```

ステップ 3 アカウントを再び有効にするには、次のコマンドを実行します。

```
ncs webroot enable
```

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

Web インターフェイス ユーザーの場合、 では、ユーザー認証はユーザーグループを使用して実装されます。ユーザー グループには、ユーザーがアクセスできる の部分およびユーザーがその部分で実行できるタスクを制御するタスクの一覧が含まれています。

ユーザー グループはユーザーの操作を制御しますが、仮想ドメインはユーザーがこれらのタスクを実行できるデバイスを制御します。仮想ドメインの詳細については、「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 （251 ページ）」を参照してください。

では、いくつかのユーザー グループが事前定義されています。ユーザーがユーザー グループに属している場合、ユーザーはそのグループのすべての認証設定を継承します。ユーザーは通常、アカウントが作成されるときにユーザー グループに追加されます。

ユーザー グループのタイプ

は、次の事前定義のユーザー グループを提供します。

- ユーザ グループ：Web UI （205 ページ）
- ユーザ グループ - NBI （206 ページ）

CLIユーザーについては、ユーザー インターフェイスとユーザー タイプ （200 ページ）を参照してください）。

ユーザ グループ：Web UI

は、次の表にリストされているデフォルトのWeb GUIユーザーグループを提供します。Monitor Liteユーザーグループに属するユーザーを除き、ユーザーを複数のグループに割り当てることができます（Monitor Lite は、権限が制限されているユーザー向けであるためです）。

ユーザー グループ	グループ タスク フォーカス
Root	すべての操作。このグループの権限は編集できません。インストール後に、root Web UI ユーザーが使用可能になります。ユーザー インターフェイスとユーザー タイプ （200 ページ）を参照してください。Web GUI ルート ユーザーの無効化および有効化 （204 ページ）に説明されているとおり、Admin または Super Users 権限で別のユーザーを作成し、root Web UI ユーザーを無効にすることをお勧めします。
スーパーユーザー	すべての操作（rootに似ています）。このグループの権限は編集できます。
Admin	システムとサーバーを管理します。モニタリングや設定に関する操作を実行できます。このグループの権限は編集できます。
Config Managers	ネットワークを設定およびモニターします（管理タスクは行いません）。このグループに割り当てられる権限は、編集可能です。
System Monitoring	ネットワークをモニターします（設定タスクは行いません）。このグループの権限は編集できます。
Help Desk Admin	ヘルプデスクとユーザー設定関連のページにしかアクセスできません。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。これは、ユーザー インターフェイスへのアクセスがない特殊なグループです。

ユーザー グループ	グループ タスク フォーカス
Lobby Ambassador	ゲスト ユーザーのみのユーザー管理。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
User–Defined 1 ～ 50	これらはブランクのグループで、必要に応じて編集したり、カスタマイズしたりできます。
Monitor Lite	ネットワーク トポロジおよびユーザー タグを表示します。このグループの権限は編集できません。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
North Bound API	SOAP API にアクセスします。
User Assistant	ローカル ネット ユーザー管理のみ。このユーザー グループのメンバーは、他のユーザー グループのメンバーを兼ねることはできません。
mDNS Policy Admin	mDNS ポリシー管理機能。

ユーザ グループ - NBI

は、次の表に記載されているデフォルトの NBI ユーザーグループを提供します。これらのグループ内の権限は編集できません。

ユーザー グループ	アクセス対象：
NBI Read	
NBI Write	

ユーザーが実行できるタスクの表示と変更

ユーザーが実行できるタスクは、ユーザーが所属するユーザー グループによって制御されます。ユーザーが所属するグループと、ユーザーが実行する権限を持つタスクを確認するには、次の手順を実行します。

（注） ユーザーがアクセスできるデバイスを確認する場合は、ユーザーへの仮想ドメインの割り当て（257 ページ）を参照してください。

ステップ 1 **[管理（Administrration）]>[ユーザー（Users）]>[ユーザー、ロール、およびAAA（Users, Roles & AAA）]** を選択し、ユーザー名を見つけます。

ステップ 2 ユーザー名を見つけて、[以下のメンバー（Member of）] の列をチェックして、ユーザーが所属するユーザー グループを見つけます。

ステップ 3 ユーザー グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウで、グループのメンバーが実行できるタスクと実行できないタスクのリストを表示します。

- チェックが付けられているチェックボックスは、グループ メンバーがそのタスクを実行する権限を持っていることを意味します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。たとえば、 では、Monitor Lite ユーザー グループの [タグの表示（View tags）] タスクを削除できません。これは、そのユーザー グループにとって不可欠なタスクであるためです。
- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザー グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 4 権限を変更するには、次の選択肢があります。

（注） この操作は慎重に行ってください。[グループ詳細（Group Detail）] ウィンドウでタスクのチェックボックスをオンまたはオフにすると、すべてのグループ メンバーに変更が適用されます。

- すべてのユーザー グループのメンバーの権限を変更します。グループで実行できるタスクを表示および変更する （233 ページ）を参照してください。
- 別のユーザー グループにユーザーを追加します。事前定義されたユーザー グループについては、ユーザ グループ：Web UI （205 ページ） とユーザ グループ - NBI （206 ページ） で説明します。これらのトピックでは、グループの制限についても説明します。たとえば、ユーザーが事前定義済みの Monitor Lite ユーザー グループに属している場合、そのユーザーは他のグループに所属することはできません。
- このグループからユーザーを削除します。ユーザーが属しているグループを表示して変更する （207 ページ）を参照してください。
- カスタマイズされたユーザー グループを使用し、ユーザーをそのグループに追加します。既存のカスタマイズされたグループを確認するには、グループで実行できるタスクを表示および変更する （233 ページ）を参照してください。新たにカスタマイズされたグループを作成するには、カスタム ユーザー グループの作成 （232 ページ）を参照してください。

ユーザーが属しているグループを表示して変更する

ユーザーが実行可能なタスクは、そのユーザーが属しているユーザー グループににによって決定されます。通常は、ユーザーアカウントの作成時に設定されます（ユーザーの追加および削除（237 ページ）を参照）。ユーザー グループについては、ユーザー グループのタイプ （205 ページ）で説明します。

この手順では、ユーザーが属しているグループを表示し、必要に応じて、ユーザーのグループ メンバーシップを変更する方法について説明します。

ステップ 1 >[管理（Administration）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）] を選択してから、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー名（User Name）] 列で、ユーザー名のハイパーリンクを探してクリックし、[ユーザーの詳細（User Details）] ウィンドウを開きます。すべてのユーザー グループが [一般（General）] タブの下に一覧表示されます。

- オンになっているチェックボックスは、ユーザーがそのグループに属していることを意味します。オンになっているボックスが灰色表示されている場合は、そのグループからユーザーを削除できないことを意味します。たとえば、 では、ルート ユーザー グループから **root** という名前のユーザーを削除できません。
- オフになっているチェックボックスは、ユーザーがそのグループに属していないことを意味します。オフになっているチェックボックスが灰色表示されている場合は、そのグループにユーザーを追加できないことを意味します

（グループが実行可能なタスクをチェックするには、左側のサイドバー メニューで、[ユーザー グループ（User Groups）] を選択し、グループ名をクリックします）。

ステップ 3 ユーザーが属しているグループを変更するには、[ユーザーの詳細（User Details）] ウィンドウで該当するグループを選択して選択解除してから、[保存（Save）] をクリックします。

ユーザー グループとそのメンバーの表示

ユーザーは、Monitoring Lite などの非常に制限されたグループに属していない限り、複数のグループに所属できます。この手順では、既存のユーザー グループとそのメンバーを表示する方法を説明します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー グループ（User Groups）] をクリックします。

[ユーザー グループ（User Groups）] ページには、既存のすべてのユーザー グループとそのメンバーの短いリストが表示されます。これらのグループの詳細については、ユーザー グループのタイプ （205 ページ）を参照してください。

ステップ 2 グループのすべてのメンバーを表示するには、グループのハイパーリンクをクリックして[グループの詳細（Group Details）] ウィンドウを開き、[メンバー（Members）] タブをクリックします。

ステップ 3 これらのグループを変更する場合は、以下を参照してください。

- グループで実行できるタスクを表示および変更する （233 ページ）
- ユーザーが属しているグループを表示して変更する （207 ページ）

ユーザーグループの権限とタスクの説明

次の表に、ユーザーグループの権限とタスクの説明を示します。

表 *12 :* ユーザーグループの権限とタスクの説明

タスクグループ名	タスク名	説明
APIC-EM コントローラ	APIC コントローラの読み取りアクセス（Apic Controller Read Access）	ユーザーは APIC-EM コントローラの詳細を読み取ることができます。
	APIC コントローラの書き込みアクセス（Apic Controller Write Access）	ユーザーは APIC-EM コントローラの詳細を作成または更新できます。
	APIC グローバル PnP の読み取りアクセス（Apic Global PnP Read Access）	ユーザーは APIC グローバル PnP/Ztd の設定を読み取ることができます。
	APIC グローバル PnP の書き込みアクセス（Apic Global PnP Write Access）	ユーザーは APIC グローバル PnP/Ztd の設定を作成または更新できます。
アクティブ セッション（Active Sessions）	アクセスの強制ログアウト（Force Logout Access）	ユーザーは、アクティブなセッションからその他のユーザーを強制的にログアウトさせることができます。

タスクグループ名	タスク名	説明
Administrative Operations	アプライアンス	ユーザーは [管理（Administration）] > [設定（Settings）] > [アプライアンス（Appliance）] メニューにアクセスできます。
	アプリケーションサーバーの管理アクセス（Application Server Management Access）	ユーザーは NAM サーバーリストを管理できます。
	アプリケーションおよびサービスへのアクセス（Application and Services Access）	ユーザーはカスタムのアプリケーションとサービスを作成、変更、削除できます。
	データの移行	
	設計エンドポイントサイトの関連付けアクセス（Design Endpoint Site Association Access）	ユーザーは保証サイトの分類ルールを作成できます。
	デバイス詳細 UDF（Device Detail UDF）	ユーザーはデバイス詳細 UDF にアクセスできます。
	監査ログのエクスポート（Export Audit Logs Access）	ユーザーは [管理メガ（Admin Mega）] メニューから [インポートポリシーの更新（Import Policy Update）] にアクセスできます。
	ヘルスモニターの詳細（Health Monitor Details）	ユーザーはサイトのヘルススコア定義を変更できます。
	ハイ アベイラビリティ設定	ユーザーはプライマリサーバーとセカンダリサーバーのペアリングに [ハイアベイラビリティ（High Availability）] を設定できます。
	インポートポリシーの更新（Import Policy Update）	ユーザーはポリシーの更新を手動でダウンロードし、コンプライアンスおよび監査マネージャエンジンにインポートできます。
	ライセンスセンター/スマートライセンス（License Center/Smart License）	

タスクグループ名	タスク名	説明
		ユーザーはライセンスセンター/スマートライセンスにアクセスできます。
	ログ	ユーザーは製品のログレベルを設定できるメニュー項目にアクセスできます。
	スケジュールされたタスクとデータコレクション（Scheduled Tasks and Data Collection）	バックグラウンドタスクを表示する画面へのアクセスを制御します。
	システム設定（System Settings）	[管理（Administration）] > [システム設定（System Settings）] メニューへのアクセスを制御します。
	ツール	ユーザーは [管理（Administration）] > [システム設定（System Settings）] メニューにアクセスできます。
	ユーザー設定	[管理（Administration）] > [ユーザー設定（User Preference）] メニューへのアクセスを制御します。
	監査ログの表示へのアクセス（View Audit Logs Access）	ユーザーは [ネットワーク（Network）] および [システム監査（System audits）] を表示できます。

タスクグループ名	タスク名	説明
Alerts and Events	ACK アラートおよびUNACK アラート（Ack and Unack Alerts）	ユーザーは既存のアラームの確認応答または確認応答解除を実行できます。
	アラームポリシー（Alarm Policies）	ユーザーはアラームポリシーにアクセスできます。
	アラームポリシーの編集アクセス（Alarm Policies Edit Access）	ユーザーはアラームポリシーを編集できます。
	アラートの削除およびクリア（Delete and Clear Alerts）	ユーザーはアクティブアラームをクリアおよび削除できます。
	通知ポリシーの読み取りアクセス（Notification Policies Read Access）	ユーザーはアラーム通知ポリシーを表示できます。
	通知ポリシーの読み取り/書き込みアクセス（Notification Policies Read-Write Access）	ユーザーはアラーム通知ポリシーを設定できます。
	アラートの選択および選択解除（Pick and Unpick Alerts）	ユーザーはアラートを選択および選択解除できます。
	Syslog ポリシー	[Syslog ポリシー（Syslog Policies）]ページへのアクセス権を付与します。
	Syslog ポリシーの編集へのアクセス（Syslog Policies Edit Access）	Syslog ポリシーを作成、変更、削除できます。
	トラブルシューティング	ユーザーはアラームで traceroute や ping などの基本的なトラブルシューティングを実行できます。
	アラート状態の表示（View Alert Condition）	ユーザーはアラート条件を表示できます。
	アラートとイベントの表示（View Alerts and Events）	ユーザーはイベントおよびアラームのリストを表示できます。

タスクグループ名	タスク名	説明
設定アーカイブ（Configuration Archive）	設定アーカイブの読み取り専用タスク（figuration Archive Read-Only Task）	ユーザーはアーカイブされた設定の表示と、設定のアーカイブ収集ジョブのスケジュールができます。
	設定アーカイブの読み取り/書き込みタスク（Configuration Archive Read-Write Task）	ユーザーはすべての設定アーカイブ操作を実行できます。
診断タスク（Diagnostic Tasks）	診断情報（Diagnostic Information）	[診断（Diagnostic）] ページへのアクセスを制御します。
フィードバックタスクとサポートのタスク	自動フィードバック（Automated Feedback）	自動フィードバックにアクセスできます。
	TAC ケース管理ツール（TAC Case Management Tool）	ユーザーは TAC ケースを開くことができます。
グローバル変数の設定（Global Variable Configuration）	グローバル変数へのアクセス（Global Variable Access）	ユーザーはグローバル変数にアクセスできます。
グループ管理（Groups Management）	グループメンバーの追加（Add Group Members）	ユーザーはデバイスやポートなどのエンティティをグループに追加できます。
	グループの追加（Add Groups）	ユーザーはグループを作成できます。
	グループメンバーの削除（Delete Group Members）	ユーザーはグループからメンバーを削除できます。
	グループの削除	ユーザーはグループを削除できます。
	グループのエクスポート（Export Groups）	ユーザーはグループをエクスポートできます。
	グループのインポート（Import Groups）	ユーザーはグループをエクスポートできます。
	グループの変更（Modify Groups）	ユーザーは名前、親、ルールなどのグループ属性を編集できます。

タスクグループ名	タスク名	説明
ジョブ管理	ジョブの承認（Approve Job）	ユーザーは別のユーザーに承認を得るためにジョブを送信できます。
	ジョブのキャンセル（Cancel Job）	ユーザーは実行中のジョブをキャンセルできます。
	[ジョブの削除（Delete Job）]	ユーザーは [ジョブ（Jobs）] ダッシュボードからジョブを削除できます。
	[ジョブの編集（Edit Job）]	ユーザーは [ジョブ（Jobs）] ダッシュボードからジョブを編集できます。
	ジョブの一時停止（Pause Job）	ユーザーは実行中のジョブとシステムジョブを一時停止できます。
	ジョブのスケジュール（Schedule Job）	ユーザーはジョブをスケジュールできます。
	ジョブの表示（Schedule Job）	ユーザーはジョブをスケジュールできます。
	編集ジョブの展開の設定（Config Deploy Edit Job）	ユーザーは展開済みのジョブの設定を編集できます。
	デバイス設定バックアップジョブの編集アクセス（Device Config Backup Job Edit Access）	ユーザーはリポジトリやファイル暗号化パスワードなどの外部バックアップ設定を変更できます。
	ジョブ通知メール（Job Notification Mail）	ユーザーはさまざまなジョブタイプに関して通知メールを設定できます。
	ジョブの実行（Run Job）	ユーザーは一時停止されたジョブとスケジュール済みのジョブを実行できます。
	[システムジョブ（System Jobs）] タブへのアクセス	ユーザーはシステムジョブを表示できます。

タスクグループ名	タスク名	説明
マップ（Maps）	クライアント ロケーション	ユーザーは地図上にクライアントの場所を表示できます。
	地図の読み取り専用（Maps Read Only）	ユーザーは地図を読み取り専用モードで表示できます。
	地図の読み取り/書き込み（Maps Read Write）	ユーザーは AP 配置などの地図内の要素を表示し、操作することもできます。
	プランニング モード（Planning Mode）	ユーザーはプランニングモードツールを起動できます。
	不正位置	ユーザーは地図上に不正な AP の場所を表示できます。
モビリティ サービス	モビリティサービス管理（Mobility Service Management）	ユーザーはモビリティサービスエンジンのプロパティとパラメータを編集し、セッションとトラップの宛先を表示し、ユーザーとグループアカウントを管理し、ステータス情報を管理できます。
	CAS の通知のみの表示（View CAS Notifications Only）	ユーザーは CAS の通知を表示できます。

タスクグループ名	タスク名	説明
ネットワーク構成	デバイスの追加アクセス（Add Device Access）	ユーザーは Prime Infrastructure にデバイスを追加できます。
	管理テンプレートへの書き込みアクセス（Admin Templates Write Access）	ユーザー定義ロールの管理テンプレートへの書き込みアクセスを有効にするには、このチェックボックスをオンにします。
	自動プロビジョニング（Auto Provisioning）	自動プロビジョニングにアクセスできます。
	コンプライアンス監査の修正アクセス（Compliance Audit Fix Access）	ユーザーはコンプライアンス修正ジョブおよびレポートを表示、スケジュール、エクスポートできます。
	コンプライアンス監査PASへのアクセス（Compliance Audit PAS Access）	ユーザーは「PSIRT」および「EOX」のジョブおよびレポートを表示、スケジュール、エクスポートできます。
	コンプライアンス監査ポリシーへのアクセス（Compliance Audit Policy Access）	ユーザーはコンプライアンスポリシーを作成、変更、削除、インポート、エクスポートできます。
	コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）	ユーザーはコンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます。
	コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）	ユーザーはコンプライアンスプロファイルについては作成、変更、削除でき、コンプライアンス監査ジョブまたはレポートについては表示、スケジュール、エクスポートでき、違反概要については表示およびダウンロードできます。

タスクグループ名	タスク名	説明
	設定テンプレートへの読み取りアクセス（Configuration Templates Read Access）	読み取り専用モードで設定テンプレートにアクセスできます。
	ACS View Server の設定（Configure ACS View Servers）	ACS View Server にアクセスして管理できます。
	アクセスポイントの設定	ユーザーはアクセスポイントを設定できます。
	Autonomous アクセス ポイント テンプレートの設定（Configure Autonomous Access Point Templates）	Prime Infrastructure の 自律型 APテンプレートにアクセスして設定できます。
	チョークポイントの設定（Configure Choke Points）	ユーザーはチョークポイントにアクセスして設定できます。
	設定グループの設定（Configure Config Groups）	設定グループにアクセスできます。
	コントローラの設定	ユーザーはワイヤレスコントローラの機能を設定できます。
	イーサネットスイッチポートの設定（Configure Ethernet Switch Ports）	DWC でデバイスのイーサネットの詳細を表示するときの設定機能へのアクセスを制御します。
	イーサネットスイッチの設定（Configure Ethernet Switches）	DWC でデバイスのイーサネットの詳細を表示するときの設定機能へのアクセスを制御します。
	ISE サーバーの設定	ユーザーは Prime Infrastructure で ISE サーバーを管理できます。
	Lightweight アクセス ポイント テンプレートの設定（Configure Lightweight Access Point Templates）	Prime Infrastructure の Lightweight アクセス ポイント テンプレートを設定できます。
	モビリティデバイスの設定（Configure Mobility Devices）	

タスクグループ名	タスク名	説明
		ユーザーはCAS、WIPS、モバイル コンシェルジュ サービス、ロケーション分析サービスを設定してモビリティ手順を示すことができます。
	Spectrum Expert の設定（Configure Spectrum Experts）	ユーザーは Spectrum Expert を設定できます。
	スイッチ位置設定テンプレートの設定（Configure Switch Location Configuration Templates）	ユーザーは設定テンプレートを変更できます。
	テンプレートの設定（Configure Templates）	ユーザーは DWC で機能テンプレートの CRUD 操作を実行してテンプレートを設定できます。
	サードパーティ製コントローラおよびアクセスポイントの設定（Configure Third Party Controllers and Access Point）	ユーザーは Prime Infrastructure でサードパーティ製コントローラとアクセスポイントを設定できます。
	WIPSプロファイルの設定（Configure WIPS Profiles）	ユーザーは WIPS プロファイルにアクセスできます。
	WiFi TDoA レシーバの設定（Configure WiFi TDOA Receivers）	ユーザーは WiFi TDoA レシーバを設定できます。
	クレデンシャルプロファイルの Add_Edit へのアクセス（Credential Profile Add_Edit Access）	ユーザーはクレデンシャルプロファイルを追加および編集できます。
	クレデンシャルプロファイルの削除アクセス（Credential Profile Delete Access）	ユーザーはクレデンシャルプロファイルを削除できます。
	クレデンシャルプロファイルの表示アクセス（Credential Profile View Access）	ユーザーはクレデンシャルプロファイルを表示できます。
	デバイスアクセスの削除（Delete Device Access）	ユーザーは Prime Infrastructure からデバイスを削除できます。
	アクセス設定の展開（Deploy Configuring Access）	ユーザーは設定と IWAN テンプレートを展開できます。

タスクグループ名	タスク名	説明
	設計設定テンプレートへのアクセス（Design Configuration Template Access）	ユーザーは、[設定（Configuration）] から共有ポリシー オブジェクト テンプレートや設定グループテンプレートを作成できます。
	デバイス一括インポートアクセス（Device Bulk Import Access）	ユーザーはCSV ファイルからデバイスの一括インポートを実行できます。
	デバイス表示設定アクセス（Device View configuration Access）	ユーザーはデバイスワークセンターでデバイスを設定できます。
	デバイスアクセスの編集（Edit Device Access）	ユーザーはデバイスクレデンシャルやデバイスのその他の詳細情報を編集できます。
	デバイスアクセスのエクスポート（Export Device Access）	ユーザーはクレデンシャルなどのデバイスのリストを CSV ファイルとしてエクスポートできます。
	グローバル SSID グループ（Global SSID Groups）	ユーザーはグローバル SSID グループを設定できます。
	移行テンプレート（Migration Templates）	ユーザーは自律型 AP の移行テンプレートを作成できます。
	[ネットワーク デバイス（Network Devices）]	ユーザーはネットワークデバイスにアクセスできます。
	ネットワークトポロジの編集（Network Topology Edit）	ユーザーはトポロジマップでデバイス、リンク、ネットワークを作成でき、手動で作成したリンクを編集して、インターフェイスを割り当てることができます。
	スケジュール済みの設定タスク（Scheduled Configuration Tasks）	ユーザーは設定テンプレート、設定グループ、ソフトウェア ダウンロード タスクおよびテンプレートを作成してスケジュールできます。

タスクグループ名	タスク名	説明
	TrustSec 準備状況評価（TrustSec Readiness Assessment）	ユーザーがネットワーク内の TrustSec を設定できる TrustSec メニューにアクセスできます。
	コンピューティングデバイスの表示	データセンターのコンピューティングサーバーと、Prime Infrastructure で管理されているホストや仮想マシンなどの仮想要素にアクセスします。
	WIPS サービス（WIPS Service）	ユーザーは WIPS サービスを設定できます。
	ワイヤレス セキュリティ	ユーザーは、ワイヤレスセキュリティ設定ウィザードを使用して不正ポリシー、不正ルール、WIPSプロファイルを設定できます。

タスクグループ名	タスク名	説明
ネットワーク モニタリング	セキュリティインデックスの問題のACKおよびUNACK（Ack and Unack Security Index Issues）	ユーザーはセキュリティインデックス侵害を確認応答または確認応答解除できます。
	管理ダッシュボードへのアクセス（Admin Dashboard Access）	ユーザーは管理ダッシュボードにアクセスできます。
	設定監査ダッシュボード（Config Audit Dashboard）	ユーザーは設定監査ダッシュボードにアクセスできます。
	データ収集管理アクセス（Data Collection Management Access）	ユーザーは[保証データソース（Assurance Data Sources）]ページにアクセスできます。
	詳細ダッシュボードへのアクセス（Details Dashboard Access）	ユーザーは詳細ダッシュボードにアクセスできます。
	クライアントの無効化（Disable Clients）	ユーザーは[無効なクライアント（Disabled Clients）]ページにアクセスできます。
	不明ユーザーの識別（Identify Unknown Users）	ユーザーは[不明ユーザーの識別（Identify Unknown Users）]ページにアクセスできます。
	インシデントアラームイベントへのアクセス（Incidents Alarms Events Access）	ユーザーはインシデントアラームイベントにアクセスできます。
	最新の設定監査レポート（Latest Config Audit Report）	ユーザーは最新の設定監査レポートを表示できます。
	Lync モニタリングアクセス（Lync Monitoring Access）	ユーザーは [Lync モニタリング（Lync monitoring）] ページにアクセスして表示できます。
	モニター アクセス ポイント	ユーザーは[アクセスポイントのモニター（Monitor Access Points）] ページを表示できます。
	チョークポイントのモニター	ユーザーは[チョークポイントのモニター（Monitor Chokepoints）]ページにアクセスできます。

タスクグループ名	タスク名	説明
	クライアントのモニター（Monitor Clients）	ユーザーは[クライアントのモニター（Monitor Clients）] ページにアクセスできます。
	イーサネットスイッチのモニター（Monitor Ethernet Switches）	ユーザーはイーサネットインターフェイス、VLAN スイッチポート、およびイーサネットスイッチの VLAN トランクをモニターできます。
	干渉源のモニター（Monitor Interferers）	ユーザーは[干渉源のモニター（Monitor Interferers）] ページにアクセスできます。
	[モニター（Monitor）] [メディアストリーム（Media Streams）]	ユーザーは名前、開始アドレスと終了アドレス、最大帯域幅、動作ステータス、平均パケットサイズ、RRC の更新、優先度、違反など、メディアストリームの設定情報をモニターできます。
	モバイルデバイスのモニター（Monitor Mobility Devices）	ユーザーはモビリティ統計情報、モビリティレスポンダの統計情報、モビリティイニシエータの統計情報などのモビリティグループのイベントをモニターできます。
	モニターのセキュリティ	ユーザーは RADIUS 認証、RADIUS アカウンティング、管理フレーム保護、不正 AP ルール、ゲストユーザーなど、コントローラのセキュリティ情報をモニターできます。
	Spectrum Expert のモニター（Monitor Spectrum Experts）	ユーザーは Spectrum Expert をモニターできます。
	タグのモニター	ユーザーはタグをモニターできます。

タスクグループ名	タスク名	説明
	サードパーティ製コントローラおよびアクセスポイントのモニター（Monitor Third Party Controllers and Access Point）	ユーザーは[サードパーティ製コントローラとアクセスポイントのモニター（Monitor Third Party Controllers and Access Point）]ページにアクセスできます。
	WiFi TDOA レシーバのモニター	ユーザーは[WiFi TDoAレシーバのモニター（Monitor WiFi TDOA Receivers）]ページにアクセスできます。
	モニタリング ポリシー	ユーザーは最も使用されたルールを特定し、特定のルールをトラブルシューティングして、選択したルールのヒットを確認できます。
	ネットワーク トポロジ（Network Topology）	ユーザーはネットワークトポロジマップを起動し、マップ内のデバイスとリンクを表示できます。
	パケットキャプチャアクセス（Packet Capture Access）	ユーザーはNAMおよびサポートされているルータのパケットキャプチャを開始できます。
	パフォーマンス ダッシュボードへのアクセス（Performance Dashboard Access）	ユーザーはパフォーマンスダッシュボードにアクセスできます。
	PfR モニタリングアクセス（PfR Monitoring Access）	ユーザーは[PfR モニタリング（PfR Monitoring）]ページにアクセスして表示できます。
	RRM ダッシュボード	ユーザーはRRMダッシュボードページにアクセスできます。
	クライアントの削除（Remove Clients）	ユーザーは[クライアントの削除（Remove Clients）]ページにアクセスできます。
	サービス状態へのアクセス（Service Health Access）	

タスクグループ名	タスク名	説明
		ユーザーは [サービスの状態（Service Health Access）] ページにアクセスして表示できます。
	サイト可視性へのアクセス（Site Visibility Access）	ユーザーはサイトの可視性にアクセスできます。
	クライアントの追跡（Track Clients）	ユーザーは[クライアントの追跡（Track Clients）] ページにアクセスできます。
	セキュリティインデックスの問題の表示（View Security Index Issues）	ユーザーは[セキュリティインデックスの問題（Security Index Issues）] ページにアクセスできます。
	音声診断（Voice Diagnostics）	ユーザーは音声診断情報にアクセスできます。
	ワイヤレスダッシュボードへのアクセス（Wireless Dashboard Access）	ユーザーはワイヤレスダッシュボードを表示できます。
オペレーションセンタータスク（Operations Center Tasks）	[サーバーの管理とモニター（Manage and Monitor Servers）] ページでの管理者権限（Administrative privileges under Manage and Monitor Servers page）	M&M ページでサーバーの追加/削除/編集/アクティブ化/非アクティブ化などの管理タスクを実行できます。
	NBI 読み取りアクセス権だけを持つユーザーがレポートおよびダッシュレットを使用できます。	レポートを生成し、すべてのダッシュレットに入力できるよう、NBI 読み取りアクセス権を持つユーザー向けにこのオプションを有効にします。
	[サーバーの管理とモニター（Manage and Monitor Servers）] ページへのアクセス（Manage and Monitor Servers Page Access）	[サーバーの管理とモニター（Manage & Monitor Servers）] ページにアクセスできます。

タスクグループ名	タスク名	説明
プラグアンドプレイの設定（Plug n Play Configuration）	PnP 展開履歴への読み取りアクセス（PnP Deploy History Read Access）	ユーザーはプロビジョニング済みのデバイスのステータスを読み取ることができます。
	PnP 展開履歴への読み取り/書き込みアクセス（PnP Deploy History Read-Write Access）	ユーザーはプロビジョニング済みデバイスで操作の読み取りおよび削除を実行できます。
	PnP ユーザー設定への読み取りアクセス	ユーザーはプラグアンドプレイのユーザー設定を表示できます。
	PnP ユーザー設定への読み取り/書き込みアクセス（PnP Preferences Read-Write Access）	ユーザーはプラグアンドプレイのユーザー設定を編集できます。
	PnP プロファイル展開への読み取りアクセス（PnP Profile Deploy Read Access）	ユーザーはプラグアンドプレイのプロビジョニング プロファイルを表示できます。
	PnP プロファイル展開への読み取り/書き込みアクセス（PnP Profile Deploy Read-Write Access）	ユーザーはプラグアンドプレイのプロビジョニング プロファイルを作成、変更、削除できます。
	PnP プロファイルへの読み取りアクセス（PnP Profile Read Access）	ユーザーはプラグアンドプレイのプロファイルを表示できます。
	PnP プロファイルへの読み取り/書き込みアクセス（PnP Profile Read-Write Access）	ユーザーはプラグアンドプレイのプロファイルを作成、削除、変更できます。
	WorkflowsReadWriteAccess	ユーザーはシスコの IOS スイッチおよびアクセスデバイスを設定できます。
製品使用状況レポート	製品のフィードバック	ユーザーは [フィードバック（Help Us Improve）] ページにアクセスできます。

タスクグループ名	タスク名	説明
レポート	Autonomous AP レポート	ユーザーは新しい自律型 AP レポートを作成できます。
	読み取り専用自律型 AP レポート（Autonomous AP Reports Read Only）	ユーザーは自律型 AP レポートを表示できます。
	CleanAir レポート	ユーザーは新しい CleanAir レポートを作成できます。
	読み取り専用 CleanAir レポート（CleanAir Reports Read Only）	ユーザーは CleanAir レポートを表示できます。
	クライアント レポート	ユーザーはクライアントレポートを作成できます
	読み取り専用クライアントレポート（Client Reports Read Only）	ユーザーはクライアントレポートを表示できます。
	コンプライアンス レポート	ユーザーは設定監査、ネットワーク一の不一致、PCI DSS 詳細レポートおよび PCI DSS サマリーレポート、PSIRT 詳細レポートおよび PSIRT サマリーレポートをカスタマイズできます。
	読み取り専用コンプライアンスレポート（Compliance Reports Read Only）	ユーザーは設定監査、ネットワーク一の不一致、PCI DSS 詳細レポートおよび PCI DSS サマリーレポート、PSIRT 詳細レポートおよび PSIRT サマリーレポートを表示できます。
	コンテキスト認識型レポート（Context Aware Reports）	ユーザーはコンテキスト認識型/ロケーション固有のレポートを実行できます。
	読み取り専用コンテキスト認識型レポート（Context Aware Reports Read Only）	ユーザーはコンテキスト認識型/ロケーション固有のレポートを実行できます。
	カスタムコンポジットレポート（Custom Composite Report）	

タスクグループ名	タスク名	説明
		ユーザーは 2 つ以上（最大 5 つのレポート）の既存のレポートテンプレートを使用して「カスタム」レポートを単一レポートに作成できます。
	カスタム NetFlow レポート（Custom NetFlow Reports）	ユーザーは NetFlow カスタムレポートにアクセスできます。
	読み取り専用 NetFlow カスタムレポート	ユーザーは NetFlow カスタムレポートを表示できます。
	デバイス レポート	ユーザーはデバイスに関連する特定のレポートのモニタリングに固有のレポートを実行できます。
	読み取り専用デバイスレポート（Device Reports Read Only）	ユーザーは生成されたデバイスレポートを読むことができます。
	ゲスト レポート	ユーザーはゲストレポートを作成できます。
	読み取り専用ゲストレポート（Guest Reports Read Only）	ユーザーはゲストレポートを表示できます。
	MSAP レポート	ユーザーはモバイルコンシェルジュのレポートを実行できます。
	読み取り専用 MSAP レポート（MSAP Reports Read Only）	ユーザーはモバイルコンシェルジュのレポートを実行できます。
	メッシュレポート（Mesh Reports）	ユーザーはメッシュレポートを作成できます。
	読み取り専用メッシュレポート（Mesh Reports Read Only）	ユーザーはメッシュレポートを表示できます。
	Network Summary レポート	ユーザーはネットワーク サマリー レポートを作成および実行できます。

タスクグループ名	タスク名	説明
	読み取り専用ネットワーク サマリー レポート（Network Summary Reports Read Only）	ユーザーはすべてのサマリー レポートを表示できます。
	パフォーマンス レポート	ユーザーはパフォーマンス レポートを作成できます。
	読み取り専用パフォーマンスレポート（Performance Reports Read Only）	ユーザーはパフォーマンス レポートを表示できます。
	Raw NetFlow レポート	ユーザーは NetFlow レポートを表示できます。
	読み取り専用 Raw NetFlow レポート（Raw NetFlow Reports Read Only）	ユーザーは Raw NetFlow レポートを表示できます。
	レポート ラウンチ パッド	ユーザーは [レポート（Report）] ページにアクセスできます。
	レポート実行履歴（Report Run History）	ユーザーはレポート履歴を表示できます。
	レポートリストの実行（Run Reports List）	ユーザーはレポートを実行できます。
	保存済みレポートリスト（Saved Reports List）	ユーザーはレポートを保存できます。
	読み取り専用保存済みレポートリスト（Saved Reports List Read Only）	ユーザーは保存済みレポートを表示できます。
	セキュリティ レポート	ユーザーはセキュリティ レポートを作成できます。
	読み取り専用セキュリティレポート（Security Reports Read Only）	ユーザーは不正な AP、WIPS などに関連するワイヤレス セキュリティ レポートを表示できます。
	仮想ドメインリスト（Virtual Domains List）	ユーザーは仮想ドメインの関連のレポートを作成できます。
	音声監査レポート（Voice Audit Report）	ユーザーは仮想ドメインの関連のレポートを作成できます。

タスクグループ名	タスク名	説明
ソフトウェア イメージの管理	ソフトウェアイメージ管理サーバーの追加（Add Software Image Management Servers）	ユーザーはソフトウェアイメージ管理サーバーを追加できます。
	ソフトウェアイメージのアクセス権限（Software Image Access Privilege）	ユーザーは [インベントリ（Inventory）]>[ソフトウェアイメージ（Software Images）] にアクセスできます。
	ソフトウェアイメージの有効化（Software Image Activation）	ユーザーはネットワーク内のデバイスを管理するソフトウェアバージョンをアップグレードおよびダウングレードできます。
	ソフトウェアイメージの収集（Software Image Collection）	ユーザーは、デバイス、Cisco.com、またはURLなど、さまざまな場所からイメージを収集できます。
	ソフトウェアイメージの削除（Software Image Delete）	ユーザーはプラグアンドプレイのプロファイルに含まれるイメージを除き、[ソフトウェアイメージ（Software Images）]ページからイメージを削除できます。
	ソフトウェアイメージの詳細の表示（Software Image Details View）	ユーザーはイメージの詳細を表示できます。
	ソフトウェアイメージの配布（Software Image Distribution）	ユーザーはネットワーク内の管理対象デバイスにソフトウェアバージョンを配布できます。
	ソフトウェアイメージ情報の更新（Software Image Info Update）	ユーザーは最小 RAM、最小 FLASH、最小ブート ROM のバージョンなど、イメージのプロパティを編集して保存できます。
	ソフトウェアイメージ管理サーバー管理プロトコル（Software Image Management Server-Manage Protocols）	ユーザーはプロトコルを管理できます。

タスクグループ名	タスク名	説明
	ソフトウェアイメージのユーザー設定の保存（Software Image Preference Save）	ユーザーは [ソフトウェアイメージ（Software Images）] ページでユーザー設定のオプションを保存できます。
	推奨ソフトウェアイメージ（Software Image Recommendation）	ユーザーは Cisco.com およびローカルリポジトリからイメージを推奨できます。
	ソフトウェアイメージのアップグレード分析（Software Image Upgrade Analysis）	ユーザーはソフトウェアイメージを分析して、ソフトウェアのアップグレードを実行する前に、ハードウェアのアップグレード（該当する場合はブートROM、フラッシュメモリ、RAM、ブートフラッシュ）が必要かどうかを判断できます。

タスクグループ名	タスク名	説明
ユーザー管理	監査証跡	ユーザーはユーザーのログインおよびログアウトに関する[監査証跡（Audit trails）] にアクセスできます。
	RADIUS サーバー	ユーザーは [RADIUSサーバー（RADIUS Servers）] メニューにアクセスできます。
	SSO サーバー AAA モード（SSO Server AAA Mode）	ユーザーは [AAA] メニューにアクセスできます。
	SSO サーバー	ユーザーは [SSO] メニューにアクセスできます。
	TACACS+ サーバー	ユーザーは [TACACS+サーバー（TACACS+ Servers）] メニューにアクセスできます。
	ユーザーとグループ	ユーザーは[ユーザーとグループ（Users and Groups）] メニューにアクセスできます。
	仮想ドメイン管理（Virtual Domain Management）	ユーザーは[仮想ドメイン管理（Virtual Domain Management）] メニューにアクセスできます。
	[仮想要素（Virtual Elements）] タブへのアクセス（Virtual Elements Tab Access）	仮想ドメインを作成、またはメンバーを仮想ドメインにメンバーを追加する場合、ユーザーは [仮想要素（Virtual Elements）] タブにアクセスすることができ、仮想要素（データセンター、クラスタ、ホスト）を仮想ドメインに追加できます。
オンラインヘルプの表示（View Online Help）	OnlineHelp	ユーザーは Prime Infrastructure のオンラインヘルプにアクセスできます。

カスタム ユーザー グループの作成

に用意されている一連の定義済みユーザー グループを利用してユーザーの権限を制御できます。これらの定義済みグループ（ユーザー グループのタイプ （205 ページ）を参照）に含まれているユーザー定義グループをカスタマイズすることで、展開に固有のユーザー グループを作成できます。次の手順で、4 つの定義済みユーザー定義グループ テンプレートのうちの 1 つを使用してカスタム グループを作成する方法を説明します。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザー グループ（User Groups）] を選択します。

ステップ 2 メンバーがないユーザー定義グループを見つけて、そのグループ名のハイパーリンクをクリックします。

ステップ 3 [グループの詳細（Group Detail）] ウィンドウでタスクをオンまたはオフにして、グループ アクセス権限をカスタマイズします。タスクが灰色で表示されている場合、その設定を調整することはできません。グループ名は変更できません任意.

ステップ 4 [保存（Save）] をクリックして設定を保存します。

ステップ 5 グループにメンバーを追加するには、該当するユーザー アカウントを編集して、そのユーザーを新しいグループに追加します。ユーザー アカウントの調整の詳細については、ユーザーの追加および削除 （237 ページ）を参照してください。

ワイヤレス ペルソナを使用したユーザーの追加

ワイヤレス ペルソナを使用してローカル ユーザーを追加することで、ユーザーにワイヤレス関連のナビゲーション メニュー項目だけが表示されるようにすることができます。

（注） ワイヤレス ペルソナを使用して AAA ユーザーまたはリモート ユーザーを追加することはできません。

ステップ 1 Cisco Prime Infrastructure に管理者としてログインします。

ステップ 2 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザー（Users）] を選択します。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、[ユーザーの追加（Add User）] を選択し、[実行（Go）] をクリックします。

ステップ 4 ユーザー アカウントを設定します。

a) ユーザー名とパスワードを入力します。

b) ユーザーが実行できるアクションを制御するために、1 つ以上のユーザー グループを選択します。ユーザー グループについては、ユーザー グループとそのメンバーの表示 （208 ページ）を参照してください。

c) ユーザーがアクセスできるデバイスを制御するために、[仮想ドメイン（Virtual Domains）] タブをクリックし、ドメインをユーザーに割り当てます。詳細については、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 （251 ページ）を参照してください。

ステップ 5 [ペルソナ（Persona）] ペインで、[ワイヤレス（Wireless）] チェックボックスをオンにします。マウスのカーソルをヘルプ テキストの疑問符の上に重ねて、ナビゲーションから削除されるメニュー項目を確認します。

ステップ 6 [保存（Save）] をクリックします。

（注） 次のユーザー グループはワイヤレス ペルソナ ベースのメニューをサポートしていません。

1. Root
2. Lobby Ambassador
3. Lobby Ambassador + NBI Credential
4. Lobby Ambassador + NBI Read
5. Lobby Ambassador + NBI Write
6. Lobby Ambassador + (NBI Credential + NBI Read)
7. Lobby Ambassador + (NBI Read + NBI Write)
8. Lobby Ambassador + (NBI Credential + NBI Write)
9. Lobby Ambassador + (NBI Credential + NBI Read +NBI Write)
10. Help Desk Admin
11. Help Desk Admin + NBI Credential
12. Help Desk Admin + NBI Read
13. Help Desk Admin + NBI Writer
14. Help Desk Admin + (NBI Credential + NBI Read)
15. Help Desk Admin + (NBI Read + NBI Write)
16. Help Desk Admin + (NBI Credential + NBI Write)
17. Help Desk Admin + (NBI Credential + NBI Read +NBI Write)
18. mDNS Policy Admin

グループで実行できるタスクを表示および変更する

既存のユーザー グループに関する情報と、グループ メンバーが実行できるタスクに関する情報を入手するには、次の手順に従ってください。事前定義されているユーザー グループの詳細

については、「ユーザー グループとそのメンバーの表示 （208 ページ）」を参照してください。

（注） デバイス アクセスを変更する場合は、「ユーザーへの仮想ドメインの割り当て （257ページ）」を参照してください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー グループ（User Groups）] を選択します。

[ユーザー グループ（User Groups）] ページには、既存のすべてのユーザー グループが一覧表示されます。

ステップ 2 ユーザー グループのハイパーリンクをクリックします。[グループの詳細（Group Detail）] ウィンドウに、グループのアクセス許可が一覧表示されます。

- チェックマークの付いているタスクは、グループ メンバーがそのタスクを実行する権限を持っていることを示します。チェックボックスがグレー表示されている場合は、タスクを無効にできません。
- チェックボックスがオフの場合は、グループ メンバーがそのタスクを実行できないことを示します。オフのチェックボックスがグレー表示されている場合は、そのユーザー グループに対してタスクを有効にすることができません。

Web GUI ルートと Monitor Lite グループ、および NBI グループは編集できません。

ステップ 3 すべてのグループ メンバーに影響するグループの権限を変更する場合は、タスクのチェックボックスをオンまたはオフにして、[保存（Save）] をクリックします。

RADIUS および TACACS+ での ユーザー グループの使用

に存在するユーザー グループを認識するように、RADIUS または TACACS+ サーバーを設定する必要があります。RADIUS および TACACS+ の ユーザ グループとロール属性のエクスポート （234 ページ）の手順に従って、これを実行できます。

RADIUS および TACACS+ の ユーザ グループとロール属性のエクスポート

RADIUS または TACACS+ を使用している場合は、すべての ユーザー グループおよびロール情報を Cisco Access Control Server（ACS）または Cisco Identity Services Engine（ISE）サーバーにコピーする必要があります。これを行うには、 Web GUI にある [タスク リスト（Task List）] ダイアログボックスを使用します。データを Cisco ACS または Cisco ISE サーバーにエクスポートしない場合、 は、ユーザーに割り当てられたタスクの実行を許可しません。

次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメインおよびロールの情報が必要です（タスクは自動的に追加されます）。
- RADIUS：仮想ドメインおよび権限の情報が必要です（タスクは自動的に追加されます）。

[タスク リスト（Task List）] ダイアログの情報は、Cisco ACS サーバー用に事前に書式設定されています。

（注） 外部サーバーにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザーで必須です。

始める前に

「」の説明に従い、AAA サーバーを追加し、AAA モードを設定していることを確認してください。

ステップ 1 で、次の手順を実行します。

a) **[管理（Administration）] > [ユーザー（Users）] > [ユーザーグループ（User Groups）]** を選択します。

b) [ユーザーグループ（User Groups）] テーブルで、ユーザー グループ行の末尾にある [タスクリスト（Task List）] ハイパーリンクをクリックして、各ユーザー グループのロールをコピーします。

- RADIUS を使用している場合は、[RADIUSカスタム属性（RADIUS Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。
- TACACS+ を使用している場合は、[TACACS+カスタム属性（TACACS+ Custom Attributes）] フィールドの role0 行を右クリックして、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバーに情報を貼り付けます。次の手順は、Cisco ACS の既存のユーザー グループに情報を追加する方法を示しています。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ を使用した外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証 （264 ページ）

a) [ユーザー設定（User Setup）] または [グループ設定（Group Setup）] に移動します。

b) 該当するユーザーまたはグループの [設定の編集（Edit Settings）] をクリックします。

c) 該当するテキスト ボックスに属性一覧を貼り付けます。

d) これらの属性を有効にするチェックボックスをオンにしてから、[送信して再起動（Submit + Restart）] をクリックします。

ユーザの追加およびユーザ アカウントの管理

- ユーザーのパスワードを変更する （239 ページ）

ユーザー グループ メンバーシップの変更

ユーザーが属しているユーザー グループを変更することによって、Prime Infrastructure 内のユーザーの権限を簡単に変更できます。

仮想ドメインからアクセス可能なサイトまたはデバイスを割り当てることもできます。詳細については、「関連項目」の「デバイスへのユーザーアクセスを制御するための仮想ドメインの作成」を参照してください。

Prime Infrastructure では、許可されないユーザー グループ メンバーシップの特定の組み合わせがあります。たとえば、ユーザーは「Root」ユーザー グループと「Lobby Ambassador」ユーザー グループに同時に属することはできません（詳細については、「ユーザーが実行できるタスクの制御（ユーザー グループ）」の表を参照してください）。Prime Infrastructure ユーザーの認証に RADIUS を使用している場合、RADIUS ユーザー属性/値ペアに無効なユーザー グループ メンバーシップの組み合わせを挿入しないようにしてください。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles, & AAA）] > [ユーザー（Users）] の順に選択します。

ステップ 3 メンバーシップを変更するユーザーのユーザー名をクリックします。[ユーザー詳細（User Details）] ページが表示されます。

ステップ 4 [一般（General）] タブの [このユーザーに割り当てられたグループ（Groups Assigned to This User）] で、以下を行います。

- そのユーザーを追加する各ユーザー グループの横にあるチェックボックスをオンにします。
- そのユーザーを削除する各ユーザー グループの横にあるチェックボックスをオフにします。

ステップ 5 完了したら、[保存（Save）] をクリックします。

関連トピック

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 （204 ページ）
グループで実行できるタスクを表示および変更する （233 ページ）
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 （251 ページ）

管理者権限を持つ Web GUI ユーザーの作成

インストール後、には **root** という名前の GUI ルート アカウントが作成されています。このアカウントは、サーバーに初めてログインして次のものを作成するために使用されます。

- 製品および機能を管理する、管理者権限を持つ Web GUI ユーザー
- その他すべてのユーザー アカウント

通常の操作には Web GUI root アカウントを使用しないでください。セキュリティ上の理由から、管理者権限（およびすべてのデバイスへのアクセス権）を持つ新しい Web GUI ユーザーを作成した後には Web GUI root アカウントを無効にしてください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザー名（Username）] テキストボックスにユーザー名を入力します。

ステップ 3 パスワードを入力します。新しいパスワードは、パスワードポリシーで指定された条件を満たす必要があります。[?] アイコンをクリックして、パスワードポリシーを表示します。

（オプション）**[新しいパスワードを生成（Generate New Password）]** ボタンをクリックして、システムによって生成されるセキュアなパスワードを設定します。このボタンをクリックすると、新しいパスワードが隣のテキストボックスに表示されます。**[新しいパスワード（New password）]** および **[パスワードの確認（Confirm password）]** テキストボックスにも同じものが表示されます。目のアイコンをクリックするとパスワードの表示/非表示が切り替わります。**[コピー（Copy）]** ボタンをクリックして、パスワードをクリップボードにコピーすることもできます。

ダイアログボックス内の値をクリアするには、[リセット（Reset）] ボタンをクリックします。

ステップ 4 （オプション）ユーザーの [名（First Name）]、[姓（Last Name）]、および [説明（Description）] を入力します。

ステップ 5 [電子メールアドレス（Email Address）] テキストボックスに電子メールアドレスを入力します。

ステップ 6 [一般（General）] タブの [このユーザーに割り当てられているグループ（Groups Assigned to This User）] で、[管理（Admin）] をクリックします。

ステップ 7 [仮想ドメイン（Virtual Domains）] タブをクリックして、ユーザーがアクセスできるデバイスを指定します。すべてのデバイスへのアクセス権を持つ管理者 Web GUI ユーザー（ROOT-DOMAIN）を 1 つ以上作成する必要があります。仮想ドメインの詳細については、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 （251 ページ）を参照してください。

（注） 親仮想ドメインを選択すると、その下の子（従属）仮想ドメインも選択されます。

ステップ 8 [保存（Save）] をクリックします。

（注） Cisco Prime Infrastructure は、Spring Security の SHA-256 エンコーダを使用します。

次のタスク

まだ行っていない場合は、セキュリティ上の理由から、Web GUI ルート ユーザーの無効化および有効化 （204 ページ）の説明に従って Web GUI root アカウントを無効にしてください。

ユーザーの追加および削除

ユーザー アカウントを作成する前に、デバイス アクセスを制御するための仮想ドメインを作成し、アカウントの作成時にそれらの仮想ドメインを適用できるようにします。この作業を行

わないと、ユーザー アカウントを編集してドメイン アクセスを追加しなければならなくなります。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（251 ページ）を参照してください。

アカウントを（削除するのではなく）一時的に無効にするには、ユーザーアカウントの無効化（ロック）（238 ページ）を参照してください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[ユーザー（Users）] を選択します。

ステップ 2 [ユーザーの追加（Add User）] をクリックします。

ステップ 3 ユーザー アカウントを設定します。

a) ユーザー名とパスワードを入力します。

b) ユーザーの名、姓、説明を入力します。

c) ユーザーが実行できるアクションを制御するために、1 つ以上のユーザー グループを選択します。ユーザー グループについては、ユーザー グループとそのメンバーの表示（208 ページ）を参照してください。

d) ユーザーがアクセスできるデバイスを制御するために、[仮想ドメイン（Virtual Domains）] タブをクリックし、ドメインをユーザーに割り当てます。（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（251 ページ）を参照）。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 ユーザーを削除するには、ユーザーを選択して

ユーザー アカウントの無効化（ロック）

一時的にユーザーが GUI にログインできないようにするには、ユーザー アカウントを無効にします。ユーザーが一時的にジョブ機能を変更する場合にこのように設定することがあります。ユーザーがログインしようとすると、では、アカウントがロックされているためにログインが失敗したことを伝えるメッセージが表示されます。ユーザーを再作成することなく、後でアカウントをアンロックできます。ユーザーアカウントを削除する場合は、ユーザーの追加および削除（237 ページ）を参照してください。

期限失効前にパスワードを変更しなかった場合は、自動的にユーザーアカウントが無効になります。この場合、パスワードをリセットできるのは管理者だけです。ユーザーのパスワードを変更する（239 ページ）および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（248 ページ）を参照してください。

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、次に [ユーザー（Users）] をクリックします。

ステップ 2 アクセスを無効または有効にするユーザーを選択します。

ステップ 3 [ユーザーのロック（Lock User(s)）]（または [ユーザーのロック解除（Unlock User(s)）] をクリックします。

ユーザーのパスワードを変更する

パスワードルールを使用して、ユーザーにパスワードを定期的に変更するように義務付けることができます（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（248 ページ）を参照）。ユーザーは、自分のパスワードを変更できます。ユーザーのパスワードをすぐに変更する必要がある場合は、次の手順を使用します。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[ユーザー（Users）] をクリックします。

ステップ 2 ユーザー名のハイパーリンクをクリックします。

ステップ 3 新しいパスワードをパスワード フィールドに入力してから、[保存（Save）] をクリックします。

ゲスト アカウントの設定

Prime Infrastructure 管理者は次の選択ができます。

- 期限切れのゲスト アカウントをすべて強制的に自動削除する。
- Lobby Ambassador のゲスト アカウントに対する制御を、その Lobby Ambassador が作成したアカウントのみに制限する。

これらの選択肢はいずれも、Lobby ambassador がこれらの一時ゲスト アカウントの管理する必要がある範囲に制限を加えることになります。Lobby ambassador の使用に関する詳細については、「関連項目」の「Lobby Ambassador を使用したゲスト ユーザー アカウントの管理」を参照してください。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [ゲスト アカウント（Guest Account）] の順に選択します。

ステップ 3 次のように、オプション ボタンの選択を変更します。

- [期限切れのゲスト アカウントを自動削除する（Automatically remove expired guest accounts）] を選択して、ライフタイムが終了したゲスト アカウントが [期限切れ（Expired）] 状態に移行されるようにします。[期限切れ（Expired）] 状態のゲスト アカウントは Prime Infrastructure から自動的に削除されます。
- [この Lobby Ambassador が作成したゲスト アカウントのみを検索して一覧表示（Search and List only guest accounts created by this lobby ambassador）] を選択して、作成したゲスト アカウントしか変更でき

ないように Lobby Ambassador を制限します。デフォルトでは、Lobby Ambassador は、どのユーザーが作成したかに関係なく、任意のゲスト アカウントを変更または削除できます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

Lobby Ambassadors を使用したゲスト ユーザー アカウントの管理 （240 ページ）
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 （204 ページ）
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 （251 ページ）

Lobby Ambassadors を使用したゲスト ユーザー アカウントの管理

Lobby Ambassador アカウントは、特殊な Prime Infrastructure 管理アカウントであり、一時ゲスト ユーザー アカウントの追加、管理、廃棄に使用されます。Lobby Ambassador アカウントは、Lobby Ambassador プロファイルで規定されるきわめて限定的なネットワーク設定権限を持ち、ゲスト アカウントの管理に使用される Prime Infrastructure 機能のみにアクセスできます。

通常、企業によって提供されるゲスト ネットワークは、企業のホストを危険にさらすことなく、ゲストがインターネットにアクセスできるようにします。Web 認証は専用クライアントなしで提供されるのが普通であるため、大半のゲストはそれらの目的の宛先への VPN トンネルを開始する必要があります。

Prime Infrastructure では、有線および無線の両方のゲスト ユーザ アクセスを許可しています。有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスまたは会議室の特定のポート経由で利用可能にすることもできます。無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。

Lobby Ambassador では、次の種類のゲスト ユーザ アカウントを作成できます。

- ライフタイムの期限があるゲスト ユーザ アカウント。指定した時間が経過すると、ゲスト ユーザ アカウントは自動的に失効します。
- ライフタイムの期限がないゲスト ユーザ アカウント。このアカウントには有効期限がありません。
- 事前に定義された将来の時刻にアクティブ化されるゲスト ユーザ アカウント。Lobby Ambassador では、有効期間の開始と終了が定義されています。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ゲスト ユーザー アカウントの管理：ワークフロー

Lobby Ambassadorは、次のワークフローに従ってゲストユーザーアカウントを管理できます。

1. ゲスト ユーザ アカウントの作成：Lobby Ambassador としてログインし、ゲスト ユーザ アカウントを必要に応じて作成します。
2. ゲスト ユーザ アカウントのスケジュール設定：Lobby Ambassador としてログインし、ゲスト ユーザ アカウントの自動作成のスケジュールを設定します。
3. ゲストユーザ詳細の印刷または電子メール送信：Lobby Ambassadorとしてログインし、ゲスト ユーザ アカウントの詳細を印刷したり、ゲストを受け入れるホストや個人にこの情報を電子メールで送信します。

フル アクセスが可能な Prime Infrastructure 管理者は、次のワークフローを使用して、Lobby Ambassador とそれらの作業を管理できます。

1. Lobby Ambassador アカウントの作成：Prime Infrastructure 管理者としてログインし、Lobby Ambassador アカウントを必要に応じて作成します。
2. Lobby Ambassadorアクティビティの表示：Prime Infrastructure管理者としてログインし、ログを使って Lobby Ambassador のアクティビティを管理します。

Lobby Ambassador アカウントの作成 （241 ページ）
ロビー アンバサダーとしてのゲスト ユーザー アカウントの作成 （242 ページ）
ゲスト ユーザー アカウントのスケジュール設定 （243 ページ）
ゲスト ユーザーの詳細の印刷または電子メールでの送信 （243 ページ）
Lobby Ambassador アクティビティの表示 （244 ページ）

Lobby Ambassador アカウントの作成

Lobby Ambassadorアカウントの作成を開始する前に、デバイスで正しく時間設定が行われていることを確認する必要があります（正しくない場合、ゲスト ユーザー アカウントが検出された後のアカウント ライフタイムに誤りが生じます）。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [ユーザー（Users）] の順に選択します。

ステップ 3 [コマンドの選択（Select a command）] > [ユーザーの追加（Add User）] > [実行（Go）] の順に選択します。

ステップ 4 次のように必須フィールドに入力します。

a) [このユーザーに割り当てられたグループ（Groups Assigned to this User）] セクションで、[Lobby Ambassador] チェックボックスをオンにすると、[Lobby Ambassador のデフォルト（Lobby Ambassador Defaults）] タブが表示されます。

b) [Lobby Ambassador のデフォルト設定（Lobby Ambassador Defaults）] タブの必須フィールドに入力します。

c) [Virtual Domains] タブをクリックし、この Lobby Ambassador アカウントの仮想ドメインを割り当てます。

d) [使用可能な仮想ドメイン（Available Virtual Domains）] リストで、このユーザーにアクセスを許可する仮想ドメインをクリックしてハイライト表示します。続いて [追加（Add）] をクリックして、これを [選択済みの仮想ドメイン（Selected Virtual Domains）] リストに追加します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ロビー アンバサダーとしてログインする

Prime Infrastructure ユーザー インターフェイスにログインするには、Lobby Ambassador のユーザー名とパスワードを使用する必要があります。Lobby Ambassador としてログインすると、[ゲスト ユーザー（Guest User）] ページが開き、作成済みのすべてのゲスト ユーザーのサマリが表示されます。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ロビー アンバサダーとしてのゲスト ユーザー アカウントの作成

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [コマンドの選択（Select a command）] > [ユーザー グループの追加（Add User Group）] > [実行（Go）] の順に選択します。

ステップ 3 [一般（General）] タブおよび [詳細設定（Advanced）] タブの必須フィールドに入力します。

フィールドの説明については、リファレンス ガイドを参照してください。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ゲスト ユーザー アカウントのスケジュール設定

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [コマンドの選択（Select a command）] > [ゲストユーザーのスケジュール（Schedule Guest User）] > [実行（Go）] の順に選択します。

ステップ 3 **必須**パラメータを設定します。

[各スケジュールで新規パスワードを生成します（Generate new password on every schedule）] および [どの曜日にも生成しない（No days of the week）] チェックボックスがオンの場合、ユーザーはアカウントが有効な期間全体に対して 1 つのパスワードを使用します。

[各スケジュールで新規パスワードを生成します（Generate new password on every schedule）] および [どの曜日にも生成する（Any days of the week）] チェックボックスがオンの場合、ユーザーは毎日新しいパスワードを使用します。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ゲスト ユーザーの詳細の印刷または電子メールでの送信

Lobby Ambassador では、ゲスト ユーザー アカウントの詳細を印刷したり、ゲストを受け入れるホストや個人にこの情報を電子メールで送信できます。電子メールや印刷済みシートには、次のアカウント詳細が示されます。

- ゲスト ユーザー アカウント名。
- ゲスト ユーザ アカウントのパスワード。
- ゲスト ユーザ アカウントが有効化される日付と時刻。
- ゲスト ユーザ アカウントが期限切れになって終了する日付と時刻。
- ゲスト ユーザに割り当てられるプロファイル ID。使用する Profile ID については管理者に問い合わせてください。
- ゲスト ユーザに関する免責事項情報。

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [Guest User] ページで、アカウント詳細を送信するユーザ名の横にあるチェックボックスをオンにします。

ステップ 3 [Select a command] > [Print/E-mail User Details] > [Go] の順に選択します。次のように続けます。

- 印刷する場合は、[印刷（Print）] **をクリックします。[印刷（Print）]** ページで、プリンタを選択して [印刷（Print）] をクリックします。

- 電子メールを送信する場合は、[電子メール（Email）]をクリックします。[電子メール（Email）]ページで、件名行に入力し、受信者の電子メールアドレスを入力して、[送信（Send）]をクリックします。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

Lobby Ambassador アクティビティの表示

Prime Infrastructure 管理者は、監査証跡機能を使用して Lobby Ambassador を管理できます。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [Administration] > [Users] > [Users, Roles, & AAA] > [User Groups] の順に選択します。

ステップ 3 表示する Lobby Ambassador アカウントの [監査証跡（Audit Trail）] アイコンをクリックします。Lobby Ambassador の [Audit Trail] ページが表示されます。このページで、Lobby Ambassador アクティビティ一覧を時系列表示できます。

- ユーザのログイン名
- 監査された操作の種類
- 操作が監査された時刻
- ログインの成功または失敗
- ログイン失敗の理由（無効なパスワードなど）を示します。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ゲスト アカウントのデバイスへの保存

ステップ 1 Lobby Ambassador として Prime Infrastructure にログインします。

ステップ 2 [ゲスト ユーザー（Guest User）] ページの [デバイスにゲストアカウントを保存（Save Guest Accounts on Device）] チェックボックスをオンにして、ゲスト アカウントを Cisco Wireless LAN Controller（WLC）フラッシュに保存すると、WLC リブート時にもアカウントを保持できます。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト ユーザーのクレデンシャルの編集 （245 ページ）

ゲスト ユーザーのクレデンシャルの編集

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles, & AAA）] > [ユーザー（Users）] の順に選択します。

ステップ 3 クレデンシャルを編集するユーザー名をクリックします。

ステップ 4 対象のクレデンシャルに変更を加えます。

編集の際、[プロファイル（Profile）] の選択が削除されている場合（[プロファイルの選択（Select a profile）] に変更されている場合）、この Lobby Ambassador のデフォルト値は削除されています。デフォルト値を再び有効にするには、設定し直す必要があります。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

ゲスト ユーザー アカウントの管理：ワークフロー （241 ページ）
ゲスト アカウントのデバイスへの保存 （244 ページ）

現在ログイン中のユーザーの確認

現在 サーバーにログインしているユーザーを確認するには、この手順に従います。また、現在の Web GUI セッションおよび過去のセッションでユーザーが実行した操作の履歴リストを参照することもできます。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）]** を選択し、[アクティブなセッション（Active Sessions）] をクリックします。 により、 サーバに現在ログインしているすべてのユーザと、各ユーザのクライアントマシンの IP アドレスがリストされます。ユーザーが管理対象デバイスに対して何らかのアクションを実行すると（ユーザーが新しいデバイスを に追加する場合など）、デバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列にリストされます。

ステップ 2 このユーザーが実行したすべてのアクションの履歴リストを表示するには、ユーザー名に対応する監査証跡アイコンをクリックします。

ユーザーが実行するタスクを表示する（監査証跡）

は、アクティブな Web GUI セッションおよび過去の Web GUI セッションでユーザーが実行したすべてのアクションの履歴を保持します。特定のユーザーまたは特定のユーザー グループのすべてのメンバーが実行したタスクの履歴を一覧表示するには、次の手順に従ってください。監査情報には、タスクの説明、ユーザーがタスクを実行したクライアントの IP アドレス、およびタスクが実行された時刻が含まれます。タスクが管理対象デバイスに影響した場合（ユーザーが新しいデバイスを追加した場合など）は、影響を受けたデバイスの IP アドレスが [デバイスの IP アドレス（Device IP Address）] 列に表示されます。複数のデバイスが変更された場合（たとえば、ユーザーが構成テンプレートを 10 個のスイッチに展開した場合）は、 によって、各スイッチの監査エントリが表示されます。

Web GUI に現在ログインしているユーザーを確認するには、「現在ログイン中のユーザーの確認 （245 ページ）」を参照してください。

ユーザー固有ではない監査を表示するには、次のトピックを参照してください。

- GUI から実行されたアクションを監査する（システムの監査） （306 ページ）
- ユーザーによって行われる変更の監査（変更の監査） （303 ページ）

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択します。

ステップ 2 特定のユーザーが実行するタスクを表示するには：

1. [ユーザー（Users）] を選択します。
2. ユーザー名を見つけて、そのユーザーに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ステップ 3 ユーザー グループのすべてのメンバーが実行したタスクの履歴リストを表示するには、次の手順に従ってください。

1. [ユーザー グループ（User Groups）] を選択します。
2. ユーザー グループ名を見つけて、そのグループに対応する [監査証跡（Audit Trail）] アイコンをクリックします。

ジョブ承認者を設定してジョブを承認する

ネットワークに大きな影響を与える可能性があるジョブを制御するには、ジョブ承認を使用します。ジョブを承認する必要がある場合は、がに電子メールを送信し、彼らの誰かが承認する

までジョブを実行しません。ジョブが承認者によって拒否された場合は、そのジョブがデータベースから削除されます。デフォルトでは、どのジョブでも承認は不要です。

ジョブ承認がすでに有効になっており、承認が必要なジョブを表示したり、ジョブを承認したり、ジョブを拒否したりする場合は、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブダッシュボード（Job Dashboard）]** を選択してから、[ジョブ承認（Job Approval）] リンクをクリックします。

ジョブ承認を有効にし、実行する前に承認が必要なジョブを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[一般（General）]** > **[ジョブ承認（Job Approval）]** を選択します。

ステップ 2 [ジョブ承認の有効化（Enable Job Approval）] チェックボックスをオンにします。

ステップ 3 承認用に設定するジョブを探して、それらを左側のフィールドから右側のフィールドに移動します。

ステップ 4 [Save] をクリックします。

ユーザ ジョブ用のジョブ通知メールを設定する

Last_Run_Status に次のステータスが表示される場合は、すべてのユーザージョブにジョブ通知メールを送信するように Cisco Prime Infrastructure を設定できます。[Failure]、[Partial Success]、[Success] [Failure]、[Success]、[Canceled]、 [Scheduled] 、または [Expired-Before-Approval]。

ユーザー ジョブに関するジョブ通知メールの設定を構成するには、次の手順を使用します。

ステップ 1 **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択してから、**[メールと通知（Mail and Notification）]** > **[ジョブ通知メール（Job Notification Mail）]** を選択します。

ステップ 2 [ジョブ通知メールの有効化（Enable Job Notification Mail）] チェックボックスをオンにして、通知を有効にします。

ステップ 3 [宛先（To）] テキスト ボックスに、電子メール アドレスを入力します。デフォルトで、[メール サーバー設定（Mail Server Configuration）] で設定された電子メール アドレスまたは事前に設定された電子メール アドレスが [宛先（To）] テキスト ボックスに表示されます。で説明されている手順を実行することによって、電子メールサーバーを設定できます。 電子メール サーバー設定の構成 （472 ページ）

ステップ 4 [件名（Subject）] テキスト ボックスに、ジョブ通知メールの件名を入力します。件名は、自動的にジョブ名が付加されます。

ステップ 5 [ジョブステータス（Job Status）] を選択します。[成功（Success）]、[一部成功（Partial Success）]、または [失敗（Failure）] のステータスオプションのいずれかか、または両方のオプションを選択して、受信者のアドレスを指定できます。

（注） 目的のジョブタイプを選択し、[Job Success/Job Partial] や [Job Failure] の下にあるチェックボックスをクリックします。ジョブ通知メールは、選択したジョブステータスのオプションに対してトリガーされます。

ステップ 6 [コンプライアンス監査ジョブ（Compliance Audit Job）] チェックボックスと [コンプライアンス修正ジョブ（Compliance Fix Job）] チェックボックスをオンにします。ジョブ通知メールは、選択したジョブに対してトリガーされます。

ステップ 7 [保存（Save）] をクリックします。ジョブ通知メールは、選択したジョブステータスに対してのみトリガーされ、ジョブの完了後にのみ送信されます。設定されたメールサーバーに指定されているサイズをファイルサイズが超えた場合、ジョブ通知メールは受信されません。

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

ローカル認証（ の認証メカニズム）を使用している場合、Web GUI からグローバル パスワード ポリシーを制御します。外部認証を使用して ユーザーを認証している場合、ポリシーは、外部アプリケーションによって制御されます（を参照）。

デフォルトでは、ユーザーは、任意の期間の経過後にパスワードの変更が強制されることはありません。パスワード変更を強制し、他のパスワード ルールを設定するには、**[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択し、[ローカル パスワード ポリシー（Local Password Policy）] を選択します。

（注） 新しいユーザーが への初回ログイン時にデフォルトのパスワードを変更するように要求するには、[パスワードの変更（Change password）] を選択する必要があります。このチェックボックスをオフにすると、ログイン時に [ホームダッシュボード（Home Dashboard）] ページが開きます。

アイドルユーザー用のグローバルタイムアウトを設定する

には、アイドルユーザーを自動的にログアウトするタイミングと方法を制御する、以下の2つの設定があります。

- [ユーザー アイドル タイムアウト（User Idle Timeout）]：タイムアウトになったときにユーザーセッションを自動的に終了するこの設定を無効にするか設定することができます。この設定はデフォルトで有効になっており、15 分に設定されています。
- [グローバル アイドル タイムアウト（Global Idle Timeout）]：[ユーザー アイドル タイムアウト（User Idle Timeout）] 設定よりも優先されます。[グローバルアイドルタイムアウト（Global Idle Timeout）] はデフォルトで有効になっており、15 分に設定されています。管理者権限を持つユーザーのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を無効化したり、そのタイムリミットを変更できます。

デフォルトで、クライアント セッションは無効になっており、ユーザーは 15 分間非アクティブだった場合に自動的にログアウトされます。これは、すべてのユーザーに適用されるグローバル設定です。セキュリティ上の理由から、このメカニズムは無効にしないでください。ただし、次の手順を使用して、タイムアウト値を調整できます。アイドルユーザーのタイムアウトを無効にするか変更するには、アイドルユーザーのタイムアウトの無効化（249 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[一般（General）] > [サーバー（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] 領域で、[すべてのアイドル ユーザーをログアウトする（Logout all idle users）] チェックボックスがオンになっていること確認します（これは、メカニズムが有効になっていることを意味します）。

ステップ 3 [後にすべてのアイドル ユーザーをログアウトする（Logout all idle users after）] ドロップダウン リストで、値を選択することによって、タイムアウトを設定します。

ステップ 4 [Save（保存）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

アイドル ユーザーのタイムアウトの無効化

デフォルトでは、一定の期間にわたって何も行われないと、クライアントセッションが無効になりユーザーは自動的にログアウトされます。これはすべてのユーザーに適用されるグローバル設定です。インストール中にログアウトしないようにするには、次の手順に従って、システム設定でアイドル ユーザーの自動ログアウトを無効にすることを推奨します。

（注） [グローバル アイドル タイムアウト（Global Idle Timeout）] 設定は、[ユーザー アイドル タイムアウト（User Idle Timeout）] 設定より優先されます。[グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を行うには、を参照してください。

顧客がシステム設定で [すべてのアイドルユーザーをログアウト（Logout all idle users）] を無効にするか、またはルートユーザーのマイプリファレンス設定で [アイドルユーザーをログアウト（Logout idle user）] を無効にするか、あるいはその両方で無効にするかに関係なく、Web サーバーのセッションタイムアウトに到達すると、セッションは最終的にタイムアウトします。これは、基本的にセキュリティポスチャを維持するためです。セッションタイムアウトの増減に関するガイドラインについては、https://owasp.org/www-community/Session_Timeout を参照してください。

（注） セッションは非アクティブな場合にのみタイムアウトしますが、アクティブなユーザーセッションはタイムアウトしません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバー（Server）]** を選択します。

ステップ 2 [グローバル アイドル タイムアウト（Global Idle Timeout）] エリアで、[すべてのアイドル ユーザーをログアウトする（Logout all idle users）] チェックボックスをオフにし、[保存（Save）] をクリックします。

ステップ 3 Web GUI ウィンドウの右上にある ⚙ をクリックし、[マイ プリファレンス（My Preferences）] を選択します。

ステップ 4 [ユーザー アイドル タイムアウト（User Idle Timeout）] エリアで [アイドル状態ユーザーのログアウト（Logout idle user）] チェックボックスをオフにし、[保存（Save）] をクリックします。

アイドルタイムアウトの値を変更する必要がある場合は、[アイドル状態ユーザーのログアウト（Logout idle user）]チェックボックスをオンにし、[アイドルユーザーをログアウトするまでの時間（Logout idle user after）] ドロップダウンリストから、アイドルタイムアウト制限を 1 つ選択します。（ただし、この値は [グローバル アイドル タイムアウト（Global Idle Timeout）] に設定されている値を超えることはできません。）

ステップ 5 [Save（保存）] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

ユーザー当たりの最大セッション数の設定

Web GUI を使用してユーザーあたりの最大セッション数を設定するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [サーバー（Server）]** の順に選択します。

ステップ 2 ユーザーあたりの最大セッション数を設定するには、[最大セッション数（Max Sessions）] テキスト ボックスに値を入力します。入力可能な値は 1 ～ 50 で、デフォルト値は 5 です。

ステップ 3 完了したら、[保存（Save）] をクリックします。

ステップ 4 サーバーを再起動して、変更を適用します。

（注） このセッション制限は、ローカル サーバー、RADIUS サーバー、および TACACS+ サーバーにのみ適用されます。このセッション制限は HA モードおよび SSO モードには適用されません。

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

仮想ドメインとは

仮想ドメインは、デバイス、サイト、およびその他の NE の論理グループで、それらの NE にアクセスできるユーザーを制御するために使用されます。仮想ドメインに含める要素とその仮想ドメインへのアクセス権を付与するユーザーを選択します。仮想ドメインは、物理サイト、デバイス タイプ、ユーザー コミュニティ、または選択するあらゆる指定項目に基づいて設定できます。すべてのデバイスはROOT-DOMAINに属します。ROOT-DOMAINはすべての新しい仮想ドメインの親ドメインです。

仮想ドメインは、ユーザー グループと連携します。仮想ドメインは、ユーザーがアクセスできるデバイスを制御しますが、ユーザー グループは、ユーザーがそれらのデバイスで実行できるアクションを決定します。仮想ドメインへのアクセス権を持つユーザーは、ユーザーの権限に応じて、デバイスを設定したり、アラームを表示したり、仮想ドメインの NE に関するレポートを生成したりできます。

デバイスを に追加したら、仮想ドメインを作成できます。各仮想ドメインには名前が必要です。オプションで説明、電子メール アドレス、およびタイム ゾーンを設定できます。 は、指定されたタイム ゾーンと電子メール アドレスを使用して、ドメイン固有のレポートをスケジュールして電子メール送信します。

ユーザーは、一度に 1 つの仮想ドメインで作業します。ユーザーは、[仮想ドメイン（Virtual Domain）] ドロップダウン リストから別の仮想ドメインを選択することによって、現在の仮想ドメインを変更できます。

仮想ドメインをセットアップする前に、ネットワークの特定の領域を管理するユーザーを決定します。次に、ニーズに応じて（たとえば、地域ごと、デバイス タイプごと、ネットワークが機能するユーザー コミュニティごと）仮想ドメインを編成します。

仮想ドメインが 機能に及ぼす影響

仮想ドメインは、階層構造で編成されています。ROOT-DOMAIN ドメインには、すべての仮想ドメインが含まれています。

ネットワーク要素は階層的に管理されるため、デバイス（および一部の関連する機能とコンポーネント）のユーザー ビューがユーザーの仮想ドメインの影響を受けます。次のトピックでは、これらの機能に対する仮想ドメインの影響について説明します。

レポートと仮想ドメイン

レポートには、アクティブ仮想ドメインに属しているコンポーネントのみが含まれています。親仮想ドメインは、その子ドメインからのレポートは表示できません。新しいコンポーネントは、その追加後に生成されたレポートにのみ反映されます。

検索と仮想ドメイン

検索結果には、アクティブ ドメインに属しているコンポーネントのみが含まれます。検索が実行され保存されたドメインと同じドメインに位置している場合にのみ保存した検索結果が表示されます。親ドメインで作業する場合、子ドメインで実行した検索結果は表示されません。

アラームと仮想ドメイン

コンポーネントが仮想ドメインに追加された場合、そのコンポーネントの以前のアラームは、該当する仮想ドメインに表示されません。新しいアラームだけが表示されます。たとえば、ネットワーク要素が に追加され、追加の前後でそのネットワーク要素がアラームを生成した場合は、追加後に生成されたアラームのみがアラーム履歴に記録されます。

（注） アラーム電子メール通知の場合は、ROOT-DOMAIN 仮想ドメインだけがロケーション通知、ロケーション サーバー、および 電子メール通知を有効にできます。

マップおよび仮想ドメイン

マップには、アクティブな仮想ドメインのメンバーであるネットワーク要素のみが表示されます。

設定テンプレートと仮想ドメイン

仮想ドメインで作成または検出した設定テンプレートは、その仮想ドメイン内のネットワーク要素にのみ適用できます。テンプレートをデバイスに適用してから、そのデバイスを子ドメインに追加した場合は、その子ドメイン内の同じデバイスでもテンプレートを使用できるようになります。

（注） 子ドメインを作成してから、設定テンプレートを仮想ドメイン内の両方のネットワーク要素に適用した場合は、テンプレートが適用されたパーティションの数が に正しく反映されない場合があります。

グループおよび仮想ドメインの設定

親ドメインは、子ドメインの設定グループ内のネットワーク要素を表示できます。親ドメインは、子ドメインの設定グループを編集することもできます。

電子メール通知と仮想ドメイン

仮想ドメインごとに電子メール通知を設定できます。

アラーム電子メール通知の場合は、ROOT-DOMAIN だけがロケーション通知、ロケーション サーバー、および電子メール通知を有効にできます。

新しい仮想ドメインの作成

新しい仮想ドメインを作成するには、仮想ドメインの目的の階層に応じて、次のいずれかの手順を実行します。

新しい仮想ドメイン（***new-domain***）の作成場所：	手順の参照先：
ROOT-DOMAIN > ***new-domain***	ROOT-DOMAIN 直下での仮想ドメインの作成 （254 ページ）
ROOT-DOMAIN > *existing-domain* > ***new-domain***	子仮想ドメイン（サブドメイン）の作成 （254 ページ）
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
（その他）	

ROOT-DOMAIN 直下での仮想ドメインの作成

ROOT-DOMAIN の下に空の仮想ドメインを作成する手順を次に示します。また、複数の仮想ドメインを一括に作成するには、仮想ドメインのリストのインポート（256ページ）の手順を使用します。

ROOT-DOMAIN の下に仮想ドメインがすでに存在しており、その仮想ドメインの下に新しいドメイン（子ドメイン）を作成するには、子仮想ドメイン（サブドメイン）の作成（254ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで [+] アイコン（[新規ドメインの追加（Add New Domain）]）をクリックします。

ステップ 3 [名前（Name）] テキスト ボックスに名前を入力します。これは必須です。

ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）] をクリックして、新しく作成された仮想ドメインの概要を表示します。

次のタスク

仮想ドメインへのネットワーク デバイスの追加（256ページ）の説明に従って、仮想ドメインにデバイスを追加します。

子仮想ドメイン（サブドメイン）の作成

次の手順を実行すると、仮想子ドメイン（サブドメインともいう）が作成されます。子仮想ドメインはROOT-DOMAINの直下にあるドメインではなく、ROOT-DOMAIN直下のドメインの下にあるドメインです。

ROOT-DOMAIN の直下に新しい仮想ドメインを表示させるには、この手順を使用しないでください。その場合には、ROOT-DOMAIN直下での仮想ドメインの作成（254ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** を選択します。

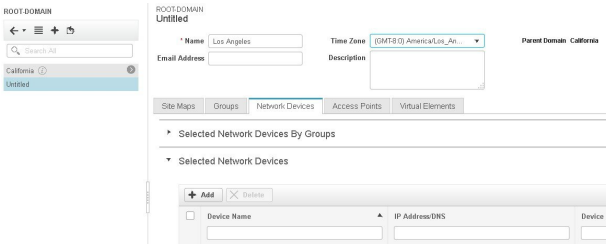
ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、次の手順を実行します。

a) その下に新しい子ドメインを作成するドメインを見つけます。（これは親ドメインと呼ばれます。）この例では、親ドメインは **California** です。

b) ドメイン名の隣にある情報（[i]）アイコンをクリックします。データ ポップアップ ウィンドウが開きます。

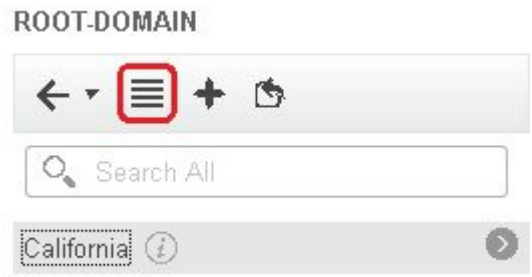
c) ポップアップ ウィンドウで、[サブドメインの作成（Create Sub Domain）] をクリックします。ナビゲーション ペインがリスト ビューに切り替わり、親ドメイン [California] が [無題（Untitled）] の上に表示されます。

ステップ 3 [名前（Name）]テキストボックスに名前を入力します。これは必須です。この例では、新しい子ドメインに **Los Angeles** という名前を付けます。（ナビゲーション ペインに表示される名前は、新しい子ドメインを保存するまでは、[無題（Untitled）] から [Los Angeles] に変更されません。）

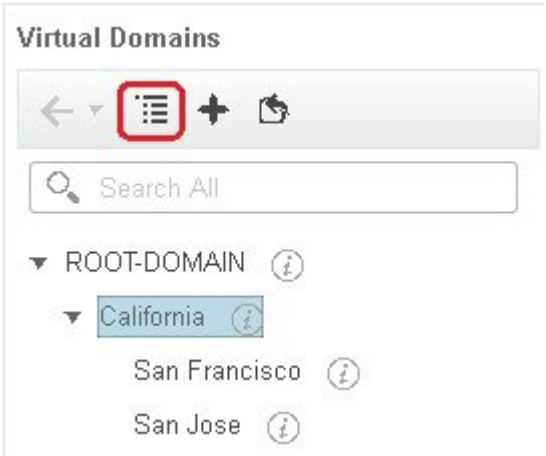


ステップ 4 （オプション）新しいドメインのタイム ゾーン、電子メール アドレス、および説明を入力します。

ステップ 5 [送信（Submit）]をクリックし、新しい子ドメインを作成することを確認します。階層ビューに戻るには、ナビゲーション ペイの上部にある表示トグル ボタンをクリックします。



表示が階層ビューに戻ります。



次のタスク

仮想ドメインへのネットワーク デバイスの追加 （256ページ）の説明に従って、仮想ドメインにデバイスを追加します。

仮想ドメインのリストのインポート

複数の仮想ドメインを作成する予定の場合、またはドメインを複雑な階層にする場合は、より簡単な方法として、それらを正しくフォーマットされた CSV ファイルで指定して、そのファイルをインポートできます。CSV フォーマットを使用すれば、作成した仮想ドメインだけでなく、その親ドメインの名前、説明、タイム ゾーン、および電子メール アドレスも指定できます。仮想ドメインへのネットワーク要素の追加は、別途行う必要があります。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [ドメインのインポート（Import Domain(s)）] アイコンをクリックし、ポップアップに表示されるリンクからサンプル CSV ファイルをダウンロードして CSV ファイルを用意します。

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

ステップ 4 [インポート（Import）] をクリックして、CSV ファイルをインポートし、指定した仮想ドメインを作成します。

次のタスク

仮想ドメインにデバイスを追加します（仮想ドメインへのネットワーク デバイスの追加（256 ページ）を参照）。

仮想ドメインへのネットワーク デバイスの追加

ネットワーク デバイスを仮想ドメインに追加するには、次の手順に従います。新しいネットワーク デバイスを既存の仮想ドメインに追加すると、そのドメインへのアクセス権を持つユーザーに対し、追加されたネットワーク デバイスがただちにアクセス可能になります（Web GUI を再起動する必要はありません）。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、ネットワーク デバイスを追加する仮想ドメインをクリックします。

ステップ 3 [送信（Submit）] をクリックして、仮想ドメインの内容を表示します。

ステップ 4 [保存（Save）] をクリックして変更を確定します。

次のタスク

ユーザーへの仮想ドメインの割り当て（257 ページ）で説明されている手順に従って、仮想ドメインへのアクセス権をユーザーに付与します。

仮想ドメインへのグループの追加

デバイス グループを仮想ドメインに追加するには、次の手順に従います。

ステップ 1 Prime Infrastructure に管理者としてログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）] の順に選択します。

ステップ 3 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、ロケーション グループを追加する仮想ドメインをクリックします。

ステップ 4 [グループ（Group）] タブで [追加（Add）] をクリックして、使用可能なロケーションとユーザー定義グループのリストを表示します。

[グループの追加（Add Group）] ウィンドウが表示されます。

ステップ 5 [グループの追加（Add Group）] ウィンドウには、自分に該当するグループのみが表示されます。これらのグループは仮想ドメインに追加できます。[すべてのロケーション（All Locations）] で必要なグループのチェック ボックスを選択し、[選択（Select）] をクリックして、デバイスを [選択されたグループ（Selected Groups）] テーブルに追加します。

（注） 選択したグループが親グループの場合、そのすべての子グループが自動的に仮想ドメインに追加されます。

ステップ 6 [送信（Submit）] をクリックして、仮想ドメインのサマリーを表示します。

ステップ 7 [保存（Save）] をクリックして、変更を確定します。

[グループ（Groups）] タブから追加されたこれらのグループには、作成、読み取り、更新、削除の各権限が設定されます。

ステップ 8 ユーザー アカウントの作成に進みます。

ユーザーへの仮想ドメインの割り当て

仮想ドメインをユーザー アカウントに割り当てると、そのユーザーが表示して操作を実行できるデバイスは、ユーザーに割り当てられたドメイン内のデバイスに制限されます。

（注） 外部 AAA を使用しているときは、外部 AAA サーバーの該当するユーザーまたはグループ設定に仮想ドメインのカスタム属性を追加してください。RADIUS と TACACS+ で仮想ドメインを使用する （259 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [ユーザー（Users）]** の順に選択します。

ステップ 2 デバイス アクセス権を付与するユーザーを選択します。

ステップ 3 [仮想ドメイン（Virtual Domains）] タブをクリックします。

ステップ 4 [追加（Add）] ボタンと [削除（Remove）] ボタンを使用して割り当てを変更してから、[保存（Save）] をクリックします。

仮想ドメインの編集

仮想ドメインを調節するには、左側のサイドバー メニューの [仮想ドメイン階層（Virtual Domain Hierarchy）] から仮想ドメインを選択し、このドメインに割り当てられているネットワーク デバイスを表示または編集します。ROOT-DOMAIN の設定はすべて編集できません。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、編集する仮想ドメインをクリックします。

ステップ 3 名前、電子メール アドレス、タイム ゾーン、説明を調整するには、テキスト ボックスに変更内容を入力します。

ステップ 4 デバイス メンバーを調整するには、次の手順を実行します。

- デバイスを追加するには、[追加（Add）] をクリックし、仮想ドメインへのネットワーク デバイスの追加 （256 ページ）の手順に従います。
- デバイスを削除するには、デバイスのチェックボックスを使用してデバイスを選択し、[削除（Delete）] をクリックします。

ステップ 5 [送信（Submit）] をクリックし、変更内容のサマリーを確認します。

ステップ 6 [保存（Save）] をクリックして編集内容を適用、保存します。

仮想ドメインの削除

仮想ドメインを から削除するには、以下の手順に従います。この手順では、仮想ドメインだけが削除され、ネットワーク要素は から削除されません（ネットワーク要素は引き続き で管理されます）。

始める前に

仮想ドメインを削除できるのは、以下の場合に限られます。

- 仮想ドメインにネットワーク要素も子ドメインも一切含まれていない場合。
- ユーザーがアクセスできる唯一のドメインではない場合。つまり、ユーザーがそのドメインにしかアクセスできない場合、ドメインを削除することはできません。
- ドメインにログインしているユーザーがいない場合。

ステップ 1 **[管理（Administration）] > [ユーザー（Users）] > [仮想ドメイン（Virtual Domains）]** の順に選択します。

ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューで、仮想ドメイン名の横にある情報（[i]）アイコンをクリックします。これにより、データ ポップアップ ウィンドウが開きます。

ステップ 3 ポップアップ ウィンドウで [削除（Delete）] をクリックします。

ステップ 4 [OK] をクリックして、仮想ドメインの削除を確認します。

RADIUS と TACACS+ で 仮想ドメインを使用する

RADIUS または TACACS+ サーバーは、内に存在する仮想ドメインを認識するように設定する必要があります。これを実行するは、「」の手順を使用します。

RADIUS または TACACS+ サーバーにユーザー向けの仮想ドメイン情報が保存されていない場合は、 で設定された仮想ドメインの数に応じて、以下が発生します。

- に 1 つの仮想ドメイン（ROOT-DOMAIN）しか割り当てられていない場合は、デフォルトで ROOT-DOMAIN がユーザーに割り当てられます。
- に複数の仮想ドメインが割り当てられている場合は、ユーザーがログインできなくなります。

RADIUS と TACACS+ の Prime Infrastructure 仮想ドメイン属性のエクスポート

RADIUS または TACACS+ を使用する場合は、 Cisco Prime Infrastructure 仮想ドメインの情報をすべて Cisco ACS サーバーまたは Cisco ISE サーバーにコピーする必要があります。Web GUI に表示される [Cisco Prime Infrastructure 仮想ドメインのカスタム属性（Prime Infrastructure Virtual Domains Custom Attributes）] ダイアログボックスを使用して、この操作を実行できます。Cisco ACS サーバーまたは Cisco ISE サーバーにデータをエクスポートしなかった場合、Cisco Prime Infrastructure はユーザーのログインを許可しなくなります。

使用するプロトコルに応じて、次の情報をエクスポートする必要があります。

- TACACS+：仮想ドメイン、権限、およびタスク情報が必要です。
- RADIUS：仮想ドメインとロールの情報が必要です（タスクは自動的に追加されます）。

既存の仮想ドメインの子ドメインを作成すると、親仮想ドメインで RADIUS/TACACS+ カスタム属性のシーケンス番号も更新されます。これらのシーケンス番号は表示専用で、AAA 統合には影響しません。

[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログボックスの情報は、Cisco ACS サーバーで使用できるように事前にフォーマットされています。

（注） 外部サーバーにタスクを追加するときには、[ホーム メニュー アクセス（Home Menu Access）] タスクを必ず追加してください。これはすべてのユーザーで必須です。

始める前に

「外部認証の設定」の説明に従い、AAA サーバーを追加し、AAA モードを設定していることを確認してください。

ステップ 1 Cisco Prime Infrastructure で次の手順を実行します。

a) **[管理（Administration）]** > **[ユーザー（Users）]** > **[仮想ドメイン（Virtual Domains）]** を選択します。

b) ウィンドウ右上の [カスタム属性のエクスポート（Export Custom Attributes）] をクリックします。これにより、[仮想ドメイン カスタム属性（Virtual Domains Custom Attributes）] ダイアログが表示されます。

c) 属性リストをコピーします。

- RADIUS を使用する場合は、[RADIUS カスタム属性（RADIUS Custom Attributes）] フィールドのすべてのテキストを選択して右クリックし、[コピー（Copy）] を選択します。
- TACACS+ を使用している場合は、[TACACS+ カスタム属性（TACACS+ Custom Attributes）] フィールドですべてのテキストを右クリックして、[コピー（Copy）] を選択します。

ステップ 2 Cisco ACS または Cisco ISE サーバーに情報を貼り付けます。この情報をまだ Cisco ACS または Cisco ISE に追加していない場合は、次を参照してください。

- Cisco ACS と RADIUS または TACACS+ による外部認証
- Cisco ISE と RADIUS または TACACS+ による外部認証

ローカル認証の設定

はデフォルトでローカル認証を使用します。つまり、ユーザー パスワードが データベースに保管されて、データベース内のパスワードが検証されます。使用中の認証モードを確認するには、**[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、**[AAA モードの設定（AAA Mode Settings）]** を選択します。これにより、[AAA モードの設定（AAA Mode Settings）] ページが表示されます。ローカル認証を使用する場合、必ず強力なパスワードポリシーを設定する必要があります。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 （248 ページ）を参照してください。

ローカル認証で SSO を使用するには、ローカル認証での SSO の使用 （260 ページ）を参照してください。

ローカル認証での SSO の使用

ローカル認証で SSO を使用するには、SSO サーバーを追加し、ローカル モードで SSO を使用するように を設定する必要があります。

は、SSO サインイン ページでのローカライズをサポートしていません。

以下のトピックでは、外部認証用に SSO を設定する方法について説明していますが、同じ手順を使用して、ローカル認証用に SSO を設定することもできます。唯一の違いは、 サーバーで SSO モードを設定するときに、[ローカル（Local）] モード（RADIUS や TACACS+ ではない）を選択することです。

•

外部認証の設定

Web GUI のルートユーザーまたはスーパーユーザーの権限を持つユーザーは、外部認証、認可、およびアカウンティング（AAA）のために外部 RADIUS、TACACS+、SSO サーバーと通信するように Cisco Prime Infrastructure を設定できます。外部認証を設定することを選択した場合、ユーザーグループ、ユーザー、認証プロファイル、認証ポリシー、およびポリシールールが、Cisco Prime Infrastructure へのすべてのアクセス要求がルーティングされる外部サーバーで作成済みである必要があります。

最大 3 つの AAA サーバーを使用できます。ユーザーは、最初のサーバーが到達不能であるかネットワークに問題がある場合にのみ、2 番目のサーバーで認証されます。

CLI から外部認証を設定するには、「CLI からの外部 AAA の設定」を参照してください。

詳細については、次のトピックを参照してください。

- 外部認証での RADIUS または TACACS+ の使用
- Cisco ISE と RADIUS または TACACS+ による外部認証
- Cisco ACS と RADIUS または TACACS+ による外部認証
- SSO による外部認証

と LDAP サーバーの統合

では、LDAP サーバーを使用した外部認証がサポートされています。この設定に興味がある場合は、シスコ担当者までお問い合わせください。

外部認証での RADIUS または TACACS+ の使用

このトピックでは、RADIUS サーバーまたは TACACS+ サーバーを使用するように設定する方法について説明します。

- Cisco Prime Infrastructure への RADIUS サーバーまたは TACACS+ サーバーの追加

Prime Infrastructure への RADIUS または TACACS+ サーバーの追加

TACACS は、3 ウェイ ハンドシェイク パケットのアプローチを使用して、ログイン クレデンシャルの認証と許可を行います。TACACS+ RFC 標準規格の規定では、PAP モードでは 2 つの

認証パケット/1 つの許可パケットを使用し、CHAP モードでは 1 つの認証パケット/1 つの許可パケットを使用することになっています。

Cisco Prime Infrastructure に RADIUS または TACACS+ サーバーを追加するには、次の手順を実行します。

ステップ 1 **[管理（Administration）]**>**[ユーザー（Users）]**>**[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[RADIUS サーバー（RADIUS Servers）] を選択します。

ステップ 2 追加するサーバーのタイプを選択します。

- RADIUS の場合は、[RADIUS サーバー（RADIUS Servers）] を選択し、[RADIUS サーバーの追加（Add RADIUS Server）] をクリックします。
- TACACS+ の場合は、[TACACS+ サーバー（TACACS+ Servers）] を選択し、[TACACS+ サーバーの追加（Add TACACS+ Server）] をクリックします。

（注） [上へ移動（Move Up）] および [下へ移動（Move Down）] 矢印を使用して、使用可能な IP アドレスの順序を並べ替えることができます。

ステップ 3 必要な情報（IP アドレス、DNS 名など）を入力します。Cisco Prime Infrastructure が外部認証サーバーと通信するためには、このページで入力する共有秘密が RADIUS また TACACS+ サーバーに設定された共有秘密と一致している必要があります。サードパーティ製の TACACS+ または RADIUS サーバー用の共有秘密キーを入力するときに、'（一重引用符）と "（二重引用符）を除く、アルファベット、数字、および特殊文字を使用できます。

ステップ 4 認証タイプを選択します。

- PAP：パスワード ベースの認証は、2 つのエンティティが 1 つのパスワードを事前に共有し、そのパスワードを認証の基準に使用するプロトコルです。
- CHAP：チャレンジ ハンドシェイク認証プロトコルでは、クライアントとサーバーの両方がプレーンテキストの秘密キーを認識しており、その秘密キーは絶対にネットワーク上に送信されないことが必要になります。CHAP は、パスワード認証プロトコル（PAP）より優れたセキュリティを提供します。

ステップ 5 高可用性機能を有効にして、[ローカル インターフェイス IP（Local Interface IP）] に仮想 IP アドレスを設定した場合、プライマリ サーバーの仮想 IP アドレスまたは物理 IP アドレスのいずれかを選択します。『Cisco Prime Infrastructure Quick Start Guide』を参照してください。

（注） 外部認証サーバーに設定された IP アドレスは、[ローカル インターフェイス IP（Local Interface IP）] の値と一致していなければなりません。

ステップ 6 [テスト（Test）] をクリックして、AAA サーバーの接続を確認します。接続テストは、入力したポート、認証タイプ、および共有キーが TACACS または RADIUS サーバーと一致する場合にのみ合格します。

（注） RADIUS サーバーに対しては、サーバーの到達可能性のみがテストされます。

ステップ 7 **[保存 (Save)]** をクリックします。

（注） ヘッダーの下にある検索フィールドでサーバーを検索できます。

（注） 追加したサーバーを削除するには、リストから削除するサーバーを選択し、次をクリックします。

- RADIUS サーバーを削除するには、[RADIUS サーバーの削除（Delete RADIUS Server）] を選択します。
- [TACACS サーバーの削除（Delete TACACS Sever）]：TACACS サーバーを削除します。

サーバー上で RADIUS または TACACS+ モードを設定する

ステップ 1 **[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）]** を選択してから、[AAA モード（AAA Mode）] を選択します。

ステップ 2 [TACACS+] または [RADIUS] を選択します。

ステップ 3 [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] チェックボックスをオンにすると、外部 AAA サーバーがダウンした場合にローカル データベースの使用が有効になります。

ステップ 4 外部 RADIUS または TACACS+ サーバーがダウンした場合にローカル認証に戻すには、次の手順を実行します。

a) [ローカルへのフォールバックを有効にする（Enable Fallback to Local）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

Prime Infrastructure の IP アドレス変更後の必須 TACACS+/RADIUS 設定

TACACS+ または RADIUS サーバーを追加した後で、Prime Infrastructure サーバーの IP アドレスを変更した場合は、手動で、Prime Infrastructure サーバーの新しい IP アドレスで TACACS+ または RADIUS サーバーを設定する必要があります。Prime Infrastructure は RADIUS または TACACS+ 要求が送信されるローカル インターフェイスをキャッシュに保存するため、Prime Infrastructure の IP アドレスが確実に更新されるように RADIUS または TACACS+ サーバーの設定を手動で編集する必要があります。

関連トピック

Prime Infrastructure への RADIUS または TACACS+ サーバーの追加
新しい Prime Infrastructure バージョンのインストール後の AAA 設定の更新 （263 ページ）

新しい Prime Infrastructure バージョンのインストール後の AAA 設定の更新

既存のデータを Prime Infrastructure の新しいバージョンに移行する前に、外部 RADIUS または TACACS+ ユーザー認証を使用していた場合は、拡張した Prime Infrastructure ユーザー タスク リストを AAA サーバーに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 サーバーに権限を再度追加し、Prime Infrastructure サーバーからのタスクで TACACS サーバーのロールを更新する必要があります。

関連トピック

Prime Infrastructure への RADIUS または TACACS+ サーバーの追加
Prime Infrastructure の IP アドレス変更後の必須 TACACS+/RADIUS 設定 （263 ページ）

Cisco ISE と RADIUS または TACACS+ による外部認証

Cisco Identity Services Engine（ISE）は、認証、認可、およびアカウンティング（AAA）に RADIUS または TACACS+ プロトコルを使用します。Cisco ISE に を統合し、RADIUS または TACACS+プロトコルを使用して ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー グループ、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ISE データベースから保存および確認する必要があります。

Cisco ISE で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ISE を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ISE のサポートされるバージョンを使用していることを確認します。	でサポートされる Cisco ISE のバージョン （265 ページ）
Cisco ISE で を AAA クライアントとして追加します。	Cisco ISE にクライアントとして を追加する （265 ページ）
Cisco ISE でユーザー グループを作成します。	Cisco ISE でのユーザー グループの作成 （265 ページ）
Cisco ISE でユーザーを作成し、そのユーザーを Cisco ISE で作成したユーザー グループに追加します。	Cisco ISE でのユーザーの作成およびユーザー グループへのユーザーの追加 （266ページ）
（RADIUS を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、で作成したユーザー ロールと仮想ドメインを使用して RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ISE での RADIUS の認証プロファイルの作成 （266ページ）
（TACACS+ を使用する場合）Cisco ISE でネットワーク アクセスの認証プロファイルを作成し、で作成したユーザー ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 （注） TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	

Cisco ISE で認証ポリシーを作成し、Cisco ISE で作成したユーザー グループと認証プロファイルにポリシーを関連付けます	Cisco ISE での認可ポリシーを設定する （268 ページ）
認証ポリシーを作成して、Cisco ISE が と通信するために使用する必要があるプロトコルと に対してユーザーを認証するために使用するアイデンティティ ソースを定義します。	Cisco ISE での認証ポリシーの作成 （269 ページ）
で RADIUS または TACACS+ サーバーとして Cisco ISE を追加します。	
サーバで RADIUS または TACACS+ モードを設定します。	サーバー上で RADIUS または TACACS+ モードを設定する （263 ページ）

でサポートされる Cisco ISE のバージョン

。

Cisco ISE にクライアントとして を追加する

ステップ 1 admin ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [追加（Add）] をクリックします。

ステップ 4 サーバーのデバイス名と IP アドレスを入力します。

ステップ 5 [認証設定（Authentication Settings）] チェックボックスをオンにして、共有秘密を入力します。

（注） この共有秘密は、 で Cisco ISE サーバーを RADIUS サーバーとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 [送信（Submit）] をクリックします。

Cisco ISE でのユーザー グループの作成

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）]** > **[ID管理（Identity Management）]** > **[グループ（Groups）]** を選択します。

ステップ 3 [ユーザー アイデンティティ グループ（User Identity Groups）] ページで、[追加（Add）] をクリックします。

ステップ 4 [アイデンティティ グループ（Identity Group）] ページで、ユーザー グループの名前と説明を入力します。

ステップ 5 [送信（Submit）] をクリックします。

Cisco ISE でのユーザーの作成およびユーザー グループへのユーザーの追加

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）]** を選択します。

ステップ 3 [ネットワーク アクセス ユーザー（Network Access Users）] ページで [追加（Add）] をクリックします。

ステップ 4 [項目の選択（Select an item）] ドロップダウン リストから、ユーザーを割り当てるユーザー グループを選択します。

ステップ 5 [送信（Submit）] をクリックします。

Cisco ISE での RADIUS の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、内に作成したユーザー ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザー ロールの属性を追加できます。タスクはユーザー ロールによって自動的に追加されます。

Cisco ISE の認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーとプロファイルの管理に関する情報を参照してください。

Cisco ISE で RADIUS の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示すRADIUSのすべての カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ISE に追加する必要があります。

- ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の ユーザ グループとロール属性のエクスポート （234 ページ）

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）]** を選択します。

ステップ 3 左側のサイドバーのメニューから **[認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 4 [標準認証プロファイル（Standard Authorization Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [認証プロファイル（Authorization Profile）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 6 [アクセス タイプ（Access Type）] ドロップダウンリストから、[ACCESS_ACCEPT] を選択します。

ステップ 7 [詳細な属性設定（Advanced Attributes Settings）] エリアで、次のアイテムのずべての RADIUS カスタム属性のリストを貼り付けます。

- ユーザー ロール
- 仮想ドメイン

（注） ユーザータスクを追加する場合は、必ずホーム メニューアクセスタスクを追加してください。これは必須です。

ステップ 8 [送信（Submit）] をクリックします。

Cisco ISE での TACACS+ 用の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、 で作成されたユーザー ロールおよび仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

（注）

- TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。
- リリース 8.5.135.0 では、認可サーバーの作成は廃止されています。認可サーバを作成するには、認証サーバを作成して、認可サーバとして複製する必要があります。この機能変更により、Cisco Prime Infrastructure 3.2 では次のようなアラームが生成されます。

  ```
  1.Successfully created Authentication server. 2.Failed to create
  authorization server:SNMP operation to Device failed: SetOperation
  not allowed for TACACS authorization server.1.Successfully
  createdAccounting server.
  ```

  Cisco Prime Infrastructure での回避策は、テンプレート上で認可サーバーをオフにすることです。詳細については、『CSCvm01415』を参照してください。

Cisco ISE 認証プロファイルの詳細については、『Cisco Identity Services Engine Administrator Guide』の認証ポリシーおよび認証プロファイルの管理に関する情報を参照してください。

Cisco ISE で TACACS+ 用の認証プロファイルを作成するには、次の手順に従います。

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）]** の順に選択します。

ステップ 3 左側のサイドバーから、[TACACS プロファイル（TACACS Profiles）] を選択します。

ステップ 4 [TACACS プロファイル（TACACS Profiles）] ページで、[追加（Add）] をクリックします。

ステップ 5 [TACACS プロファイル（TACACS Profiles）] ページで、認証プロファイルの名前と説明を入力します。

ステップ 6 [raw ビュー（Raw View）] 領域に、以下についての TACACS+ カスタム属性の完全なリストを貼り付けます。

- タスクを含むユーザー ロール
- 仮想ドメイン

ステップ 7 [送信（Submit）] をクリックします。

Cisco ISE で の認可ポリシーを設定する

認可ポリシーは、認可プロファイルで定義された特定の権限のセットを形成する、ユーザー定義のルールまたはルールのセットで構成されます。認可プロファイルに基づいて、 へのアクセス要求が処理されます。

設定可能な認可ポリシーには、次の 2 つのタイプがあります。

- 標準：標準ポリシーは、安定化を目的としており、長期間にわたって効果を発揮し、より大きなユーザーのグループ、デバイス、または権限の共通セットを共有するグループに適用するために作成します。
- 例外：例外ポリシーは、限定数のユーザー、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザーまたはユーザーのサブセットに合わせて調整された、ID グループ、条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。

認可ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authorization Policies and Profiles」の章を参照してください。

Cisco ISE で認可ポリシーを作成するには、次の手順を実行します。

ステップ 1 管理者ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [許可（Authorization）]** を選択します。

ステップ 3 [標準（Standard）] 領域で、右端にある下矢印をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のどちらかを選択します。

ステップ 4 ルール名を入力して、認可ポリシーの ID グループ、条件、属性、および権限を選択します。

たとえば、ユーザーグループを -System Monitoring-Group として定義して、そのグループを [アイデンティティグループ（Identity Groups）] ドロップダウンリストから選択することができます。同様に、認証プロファイルを -System Monitoring-authorization プロファイルとして定義し、[権限（Permissions）] ドロップダウンリストからこのプロファイルを選択します。これで、システムモニタリングアイデンティティ グループに属しているすべてのユーザーに、システム モニタリングのカスタム属性が定義された適切な認証ポリシーが適用されます。

ステップ 5 [完了（Done）] をクリックしてから、[保存（Save）] をクリックします。

Cisco ISE での TACACS 認証ポリシーの設定

Cisco ISE で TACACS 認証ポリシーを作成するには、次の手順に従います。

ステップ 1 管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[デバイス ワーク センター（Device Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** の順に選択します。

ステップ 3 左側のペインで [デフォルト（Default）] を選択します。

ステップ 4 [認証ポリシー（Authorization Policy）] 領域で、右端にある下矢印をクリックし、[新規ルールを上に挿入（Insert New Rule Above）] または [新規ルールを下に挿入（Insert New Rule Below）] のどちらかを選択します。

ステップ 5 ルール名を入力し、アイデンティティ グループ、条件、認証ポリシーのシェル プロファイルを選択します。

たとえば、ユーザー グループを -SystemMonitoring-Group として定義して、そのグループを [アイデンティティ グループ（Identity Groups）] ドロップダウン リストから選択することができます。同様に、認可プロファイルを -SystemMonitoring-authorization プロファイルとして定義し、[権限（Permissions）] ドロップダウン リストからそのプロファイルを選択します。これで、 システム モニタリング アイデンティティ グループに属しているすべてのユーザーに、システム モニタリングのカスタム属性が定義された適切な認証ポリシーが適用されます。

ステップ 6 [Save] をクリックします。

Cisco ISE での認証ポリシーの作成

認証ポリシーは、Cisco ISE が と通信するために使用するプロトコルを定義します。また、 に対するユーザーの認証に使用するアイデンティティ ソースを特定します。アイデンティティ ソースは、ユーザー情報が格納されている内部または外部データベースです。

Cisco ISE で作成できる認証ポリシーには、次の 2 つのタイプがあります。

- シンプルな認証ポリシー：このタイプのポリシーでは、ユーザーの認証に使用できるプロトコルとアイデンティティ ソースを選択できます。
- ルールベースの認証ポリシー：このタイプのポリシーでは、許可するプロトコルとアイデンティティ ソースを Cisco ISE に動的に選択させるための条件を定義できます。

認証ポリシーの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Manage Authentication Policies」の章を参照してください。

Cisco ISE で認証ポリシーを作成するには、次の手順に従います。

ステップ 1 上級管理ユーザーまたはシステム管理ユーザーとして Cisco ISE にログインします。

ステップ 2 **[ポリシー（Policy）] > [認証（Authentication）]** の順に選択します。

ステップ 3 必要な認証ポリシーを作成するために、[ポリシー タイプ（Policy Type）] として [シンプル（Simple）] または [ルールベース（Rule-Based）] を選択します。

ステップ 4 選択したポリシー タイプに基づいて、必要な情報を入力します。

ステップ 5 [Save] をクリックします。

Cisco ACS と RADIUS または TACACS+ による外部認証

Cisco Secure Access Control System（ACS）は、認証、許可、およびアカウンティング（AAA）に RADIUS および TACACS+ プロトコルを使用します。Cisco ACS に Cisco Prime Infrastructure を統合し、RADIUS または TACACS+ プロトコルを使用して Cisco Prime Infrastructure ユーザーを認証できます。外部認証を使用する場合は、ユーザー、ユーザー ロール、パスワード、認証プロファイル、認証ポリシー、ポリシー規則などの AAA に必要な詳細を Cisco ACS データベースから保存および確認する必要があります。

Cisco ACS で外部認証に RADIUS または TACACS+ プロトコルを使用するには、次のタスクを実行します。

外部認証に Cisco ACS を使用するために実行するタスク	詳細については、次を参照してください。
Cisco ACS のサポートされるバージョンを使用していることを確認します。	でサポートされる Cisco ACS のバージョン
Cisco ACS での AAA クライアントとしての Cisco Prime Infrastructure の追加	Cisco ACS にクライアントとして を追加する
Cisco ACS でユーザー グループを作成します。	Cisco ACS でのユーザー グループの作成
Cisco ACS でユーザーを作成し、そのユーザーを Cisco ACS のユーザー グループに追加します。	Cisco ACS でのユーザーの作成とユーザー グループへのユーザーの追加
（RADIUS を使用する場合）Cisco ACS でネットワーク アクセスの認証プロファイルを作成し、Cisco Prime Infrastructure で作成したユーザー ロールと仮想ドメインの RADIUS カスタム属性を追加します。 （注） RADIUS では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ACS での RADIUS 用の認証プロファイルの作成

（TACACS+ を使用する場合）Cisco ACS でデバイス管理の認証プロファイルを作成し、Cisco Prime Infrastructure で作成したユーザー ロールおよび仮想ドメインを使用した TACACS+ カスタム属性を追加します。 （注） TACACS+ では、ユーザー タスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。	Cisco ACS での TACACS+ の認証プロファイルの作成
Cisco ACS でアクセス サービスを作成し、アクセス サービスのポリシー構造を定義します。	Cisco ACS での 用アクセス サービスの作成
Cisco ACS で認証ポリシー規則を作成し、アクセス タイプ（ネットワーク アクセスまたはデバイス管理）に基づいて認証またはシェル プロファイルをマッピングします。	Cisco ACS での認証ポリシー ルールの作成
Cisco ACS でサービス選択ポリシーを設定し、着信要求にアクセス サービスを割り当てます。	Cisco ACS でのサービス セレクション ポリシーの設定
Cisco Prime Infrastructure で RADIUS または TACACS+ サーバーとして Cisco ACS を追加します。	
Cisco Prime Infrastructure で RADIUS モードまたは TACACS+ モードを設定します。	サーバー上で RADIUS または TACACS+ モードを設定する

でサポートされる Cisco ACS のバージョン

は Cisco ACS 5.*x* リリースをサポートしています。

Cisco ACS にクライアントとして を追加する

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** > **[ネットワーク デバイスおよび AAA クライアント（Network Devices and AAA Clients）]** の順に選択します。

ステップ 3 [ネットワーク デバイス（Network Devices）] ページで [作成（Create）] をクリックします。

ステップ 4 サーバーのデバイス名と IP アドレスを入力します。

ステップ 5 認証オプションで [RADIUS] または [TACACS+] を選択し、共有秘密を入力します。

（注） この共有秘密は、 で Cisco ACS サーバーを RADIUS または TACACS+ サーバーとして追加したときに入力した共有秘密と必ず一致するようにします。

ステップ 6 [送信（Submit）] をクリックします。

Cisco ACS でのユーザー グループの作成

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザーと ID ストア（Users and Identity Stores）]** > **[アイデンティティ グループ（Identity Groups）]** の順に選択します。

ステップ 3 [アイデンティティグループ（Identity Groups）] ページで [作成（Create）] をクリックします。

ステップ 4 グループの名前と説明を入力します。

ステップ 5 ユーザー グループの親ネットワーク デバイス グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

Cisco ACS でのユーザーの作成とユーザー グループへのユーザーの追加

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ユーザーとIDストア（Users and Identity Stores）]** > **[内部IDストア（Internal Identity Stores）]** > **[ユーザー（Users）]** の順に選択します。

ステップ 3 [内部ユーザー（Internal Users）] ページで [作成（Create）] をクリックします。

ステップ 4 次の必須詳細情報を入力します。

ステップ 5 [アイデンティティ グループ（Identity Group）] フィールドで [選択（Select）] を選択して、ユーザーを割り当てるユーザー グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

Cisco ACS での RADIUS 用の認証プロファイルの作成

許可プロファイルを作成して、さまざまなタイプのユーザーにネットワークへのアクセスを認可する方法を定義します。たとえば、VPN 接続を介してネットワークへのアクセスを試みるユーザーには、有線接続を介してネットワークへのアクセスを試みるユーザーよりも厳しく取り扱うことを定義できます。

デバイス管理用の認証プロファイルを作成するには、内に作成したユーザー ロール、タスク、仮想ドメインに関連付けられている RADIUS カスタム属性を追加する必要があります。

（注） RADIUS の場合、タスクの属性を追加せずにユーザー ロールの属性を追加できます。タスクはユーザー ロールによって自動的に追加されます。

Cisco ACS 認証プロファイルおよびポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素およびアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で RADIUS 用の認証プロファイルを作成するには、次の手順に従います。

始める前に

RADIUS用の次の カスタム属性を完全に網羅したリストを用意しておきます。次の手順では、この情報を Cisco ACS に追加する必要があります。

- ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の ユーザ グループとロール属性のエクスポート （234 ページ）

ステップ 1 管理ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）] > [認証と許可（Authorizations and Permissions）] > [ネットワーク アクセス（Network Access）] > [認証プロファイル（Authorization Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [RADIUS 属性（RADIUS Attributes）] タブをクリックし、以下についての RADIUS カスタム属性の完全なリストを貼り付けます。

- ユーザー ロール
- 仮想ドメイン

（注） ユーザータスクを追加する場合は、必ずホーム メニューアクセスタスクを追加してください。これは必須です。

ステップ 6 [送信（Submit）] をクリックします。

Cisco ACS での TACACS+ の認証プロファイルの作成

デバイス管理用の認証プロファイルを作成するには、 で作成されたユーザー ロールおよび仮想ドメインに関連付けられている TACACS+ カスタム属性を追加する必要があります。

（注） TACACS+では、ユーザータスクの属性を追加する必要はありません。これらはユーザー ロールに基づいて自動的に追加されます。

Cisco ACS認証プロファイルとポリシーの詳細については、『User Guide for Cisco Secure Access Control System』のポリシー要素とアクセス ポリシーの管理に関する章を参照してください。

Cisco ACS で TACACS+ の認証プロファイルを作成するには、次の手順を実行します。

始める前に

次に示すすべての カスタム属性のリストがあることを確認します。次の手順では、この情報を Cisco ACS に追加する必要があります。

- ユーザー ロールとタスク：を参照してください。RADIUS および TACACS+ の ユーザ グループとロール属性のエクスポート （234 ページ）

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[ポリシー要素（Policy Elements）]** > **[認証と許可（Authorizations and Permissions）]** > **[デバイス管理（Device Administration）]** > **[シェル プロファイル（Shell Profiles）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 [一般（General）] タブで、認証プロファイルの名前と説明を入力します。

ステップ 5 [カスタム属性（Custom Attributes）] タブをクリックし、次のアイテムのずべての TACACS+ カスタム属性のリストを貼り付けます。

- タスクを含むユーザー ロール
- 仮想ドメイン

ステップ 6 [送信（Submit）] をクリックします。

Cisco ACS での 用アクセス サービスの作成

アクセス サービスには、アクセス要求の認証および認可ポリシーが含まれています。使用事例（デバイス管理（TACACS+）やネットワーク アクセス（RADIUS）など）ごとに異なるアクセス サービスを作成できます。

Cisco ACS でアクセス サービスを作成するときに、サービスに含まれるポリシーのタイプとポリシー構造を定義します。たとえば、デバイス管理やネットワーク アクセス用のポリシーがあります。

（注） サービス選択ルールを定義する前に、アクセス サービスを作成する必要がありますが、サービスにポリシーを定義する必要はありません。

の要求用にアクセス サービスを作成するには、次の手順を実行します。

ステップ 1 管理ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）]** > **[アクセス サービス（ Access Services）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 アクセス サービスの名前と説明を入力します。

ステップ 5 アクセス サービスのポリシー構造を定義するために、次のいずれかのオプションを選択します。

- [サービス テンプレート ベース（Based on service template）]：定義済みテンプレートに基づいたポリシーを含むアクセス サービスを作成します。

- [既存のサービス ベース（Based on existing service）]：既存のアクセス サービスに基づいたポリシーを含むアクセス サービスを作成します。ただし、新しいアクセス サービスには既存のサービスのポリシー ルールは含まれません。
- [ユーザー選択のサービス タイプ（User selected service type）]：ユーザーがアクセス サービスのタイプを選択できます。選択可能なオプションには、ネットワーク アクセス（RADIUS）、デバイス管理（TACACS+）、外部プロキシ（外部 RADIUS または TACACS+ サーバー）があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サービス アクセスに使用できる認証プロトコルを選択します。

ステップ 8 [終了（Finish）] をクリックします。

Cisco ACS での認証ポリシー ルールの作成

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセスポリシー（Access Policies）]** > **[アクセスサービス（Access Services）]** > **[サービス（service）]** > **[認証（Authorization）]** の順に選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 ルールの必須条件を設定します。

たとえば、ロケーション、デバイス タイプ、または作成したユーザー グループに基づいてルールを作成できます。

ステップ 6 ネットワーク アクセス（RADIUS）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須認証プロファイルを選択します。

あるいは、デバイス管理（TACACS+）の認証ポリシー ルールを作成する場合は、認証ポリシー ルールにマッピングする必須シェル プロファイルを選択します。

（注） 複数の認証プロファイルまたはシェル プロファイルを使用する場合は、優先順位の高い順に並べる必要があります。

ステップ 7 [OK] をクリックします。

Cisco ACS でのサービス セレクション ポリシーの設定

サービス セレクション ポリシーでは、着信要求に適用するアクセス サービスを決定します。たとえば、TACACS+ プロトコルを使用するアクセス要求にデバイス管理アクセス サービスを適用するサービス セレクション ポリシーを設定できます。

次の 2 種類のサービス セレクション ポリシーを設定できます。

- 単純なサービス セレクション ポリシー：すべての要求に同じアクセス サービスを適用します。

- ルール ベースのサービス セレクション ポリシー：1 つ以上の条件とその結果（着信要求に適用されるアクセス サービス）が設定されています。

サービス セレクション ポリシーを設定するには、次の手順を実行します。

ステップ 1 admin ユーザーとして Cisco ACS にログインします。

ステップ 2 左側のサイドバーから、**[アクセス ポリシー（Access Policies）]** > **[アクセス サービス（Access Services）]** > **[サービス セレクション ルール（Service Selection Rules）]** の順に選択します。

ステップ 3 単純なサービス セレクション ポリシーを設定するには、[単一結果の選択（Single result selection）] オプション ボタンをクリックし、すべての要求に適用するアクセス サービスを選択します。

または、ルールベースのサービスセレクションポリシーを設定するには、[ルールベースの結果選択（Rule based result selection）] オプション ボタンをオンにし、[作成（Create）] をクリックします。

ステップ 4 ルール名を入力し、ルール ステータスを選択します。

ステップ 5 サービス セレクション ポリシーのプロトコルとして [RADIUS] または [TACACS+] を選択します。

ステップ 6 必要な複合条件を設定し、着信要求に適用するアクセス サービスを選択します。

ステップ 7 [OK] をクリックし、[変更の保存（Save Changes）] をクリックします。

SSO による外部認証

（RADIUS または TACACS+ サーバーの有無にかかわらず）SSO をセットアップおよび使用するには、これらのトピックを参照してください。

では、SSO サインイン ページのローカリゼーションをサポートしていません。

SSO サーバの追加

Cisco Prime Infrastructure には最大 3 つの AAA サーバーを設定できます。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** の順に選択し、[SSO サーバー（SSO Servers）] を選択します。

ステップ 2 [SSO サーバーの追加（Add SSO Servers）] をクリックします。

ステップ 3 SSO 情報を入力します。

SSO サーバー認証要求のサーバー再試行回数は最大 3 回です。

ステップ 4 [保存（Save）] をクリックします。

（注） ヘッダーの下の検索フィールドにサーバーの詳細を入力すると、サーバーを検索できます。

（注） 追加したサーバーを削除する場合は、リストから削除するサーバーを選択し、[SSO サーバーの削除（Delete SSO Server(s)）] をクリックします。

（注） [SOO サーバーとして自身を追加（Add self as SSO Server）] ボタンを使用して、自身をサーバーとして追加することもできます。

Prime Infrastructure サーバーで SSO モードを設定する

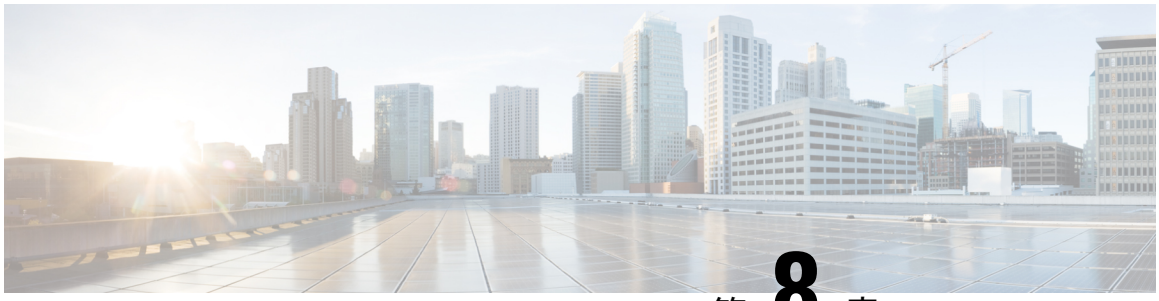
シングルサインオン（SSO）認証は、マルチユーザー、マルチリポジトリ環境でのユーザーの認証および管理に使用されます。SSO サーバーは、異種のシステムへのログインに使用されるクレデンシャルの保存および取得を行います。 の他のインスタンス用の SSO サーバーとしてをセットアップできます。

（注） 次の手順を使用して SSO を設定するが、ローカル認証を使用する場合は、ステップ 2 で [ローカル（Local）] を選択します。

ステップ 1 **[管理（Administration）]** > **[ユーザー（Users）]** > **[ユーザー、ロール、および AAA（Users, Roles & AAA）]** > **[SSO サーバーの設定（SSO Server Settings）]** を選択します。

ステップ 2 使用する SSO サーバー AAA モードを選択します。オプションは次のとおりです。[ローカル（Local）]、[RADIUS]、または [TACACS+]。

ステップ 3 [Save] をクリックします。



第 8 章

障害管理タスク

ここでは、次の内容について説明します。

イベントの受信、転送、および通知

は、デバイスから受信した syslog と SNMPv1、v2、および v3 トラップを処理します。サーバーは、自動的に UDP ポート 162 でこれらのイベントをリッスンします。サーバー上でイベント リスニング設定を実行する必要はありませんが、適切なポート上で にトラップと syslog を転送するようにデバイスを設定する必要があります。

通知は、SNMPv2 または SNMPv3 形式で転送されます。対応する通知ポリシーがセットアップされている場合は、電子メール受信者にも通知が転送されます。通知タイプ UDP の通知を追加する場合、その追加するはそれが設定されている同じポート上で UDP をリッスンしている必要があります。INFO レベル イベントだけが、選択されたカテゴリに対して処理され、アラームはクリティカル、メジャー、マイナー、および警告レベルで処理されます。

（注） SNMPv3 形式を使用する通知受信者には、一意のユーザー名が必要です。2 つ以上の通知受信者が同じユーザー名でパスワードが異なる場合、そのうちの 1 つが機能しません。

は、受信した syslog、トラップ、および TL/1 アラームを処理することによって発生したアラームとイベントをノースバウンド通知のに転送できます。

また、SNMP トラップ通知メカニズムを使用して、サーバーの問題を示す SNMP トラップを転送することもできます。

アラートおよびイベントは SNMPv2 として送信されます。

アラーム通知設定を構成するためのユーザー ロールとアクセス権限

次の表に、通知先を設定して、カスタマイズされた通知ポリシーを作成するためのユーザー ロールとアクセス権限の説明を示します。

（注） 通知先と通知ポリシーを表示、作成、および編集するには、次のユーザー ロール用のタスク権限が有効になっていることを確認します。

- [アラートとイベント（Alerts and Events）] の通知ポリシーの読み取り/書き込みアクセス
- 仮想ドメイン リスト（[レポート（Reports）]）

詳細については、ユーザーが実行できるタスクの表示と変更（206 ページ）を参照してください。

ユーザー ロール	アクセス権限
ルート ドメインを持つルート ユーザー	通知先と通知ポリシーを表示、作成、削除、および編集します。
非ルート ドメインを持つルート ユーザー	通知先と通知ポリシーを表示します。
ルート ドメインを持つ管理者ユーザー	通知先と通知ポリシーを表示、作成、削除、および編集します。
ルート ドメインを持つスーパー ユーザー	通知先とアラーム通知ポリシーを表示、作成、削除、および編集します。
ルート ドメインを持つシステム モニタリング ユーザー	通知先と通知ポリシーを表示します。
ルート ドメインを持つ構成マネージャ	通知先と通知ポリシーを表示します。

ユーザー ロール	アクセス権限
非ルート ドメインを持つ管理者ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルート ドメインを持つスーパー ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルートドメインを持つシステム モニタリング ユーザー	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。
非ルート ドメインを持つ構成マネージャ	それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。

新しい通知ポリシーを追加する場合の注意事項

次の表に、新しい通知ポリシーを追加する場合に覚えておかなければならないいくつかのポイントの説明を示します。

通知ポリシー ページで選択されたカテゴリ	注意事項
E メール	• 各仮想ドメインには、一意の連絡先名と電子メール アドレス（電子メール受信者）を割り当てる必要があります。 • 電子メール受信者は、ROOT-DOMAIN からのみ、追加、変更、および削除できます。 • 1 つの電子メール アドレスを複数の仮想ドメインに関連付けることができます。 • Prime Infrastructure は、アラーム通知を送信するために、電話番号、携帯番号、および郵便先住所の詳細を使用しません。

通知ポリシー ページで選択されたカテゴリ	注意事項
トラップ受信者	• 連絡先名は、トラップ受信者ごとに一意です。 • トラップ受信者は、ROOT-DOMAINからしか追加、変更、および削除することができません。トラップ受信者はROOT-DOMAIN でのみ適用可能です。 • ノースバウンド トラップ受信者だけが、通知ポリシー エンジンから転送されたアラーム/イベントを受信できます。 • ゲストアクセストラップ受信者は、ゲスト クライアントに関係するアラームだけを受信します。

通知ポリシー ページで選択されたカテゴリ	注意事項
通知ポリシー	

通知ポリシー ページで選択されたカテゴリ	注意事項
	• 各通知ポリシーは、アラーム カテゴリ、アラームシビラティ（重大度）、アラーム タイプ、デバイス グループ、通知先、および時間範囲という条件で構成されます。 • 通知ポリシーはそれぞれ一意の仮想ドメインに関連付けられます。 • 必要な条件を選択するときに、ツリー ビュー ドロップダウン リストをドリルダウンして、個別のカテゴリ（スイッチやルータなど）とシビラティ（重大度）（メジャーなど）を選択できます。さらに、特定のアラーム タイプ（リンク ダウンなど）を選択できます。 • ポリシー内の条件と一致したアラームがそれぞれの通知先に転送されます。 • アラームが同じ仮想ドメイン内の複数のポリシーと一致し、それらのポリシーに同じ宛先が設定されている場合は、1つの通知だけがそれぞれの宛先に送信されます。 • 通知ポリシーに関連付けられた仮想ドメインを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。 • ポリシーで指定された 1 つ以上のデバイス グループを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。 • 既存のアラーム ポリシーによって抑制されているアラームは、通知先に転送され

通知ポリシー ページで選択されたカテゴリ	注意事項
	ません。 • ルール条件にシステム カテゴリ アラームと非システム カテゴリ アラームの両方が含まれている通知ポリシーの場合は、非システム カテゴリ アラーム用のデバイス グループを選択する必要があります。 • 指定された期間に発生したアラームだけが通知先に送信されます。たとえば、期間を 8:00 ～ 17:00 に指定した場合は、午前 8 時 00 分から午後 5 時 00 分の間のアラームのみが通知されます。

アラーム通知先の設定

Prime Infrastructure によって生成されたアラームを通知するために、電子メール通知およびノースバウンド トラップの受信者を設定できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールと通知（Mail and Notification）] > [通知先（Notification Destination）]** の順に選択します。

ステップ 2 [追加（Add）] アイコンをクリックして、新しい通知先を作成します。

ステップ 3 電子メールの宛先を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] ドロップダウン リストから [電子メール（Email）] を選択します。

b) [連絡先の名前（Contact Name）] テキスト ボックスに連絡先の名前を入力します。

c) [メール宛先（Email To）] テキスト ボックスに有効な電子メール ID を入力します。
電子メールは [メール宛先（Email To）] フィールドに入力した電子メール ID に送信されます。

d) [連絡先の氏名（Contact Full Name）] に連絡先の氏名を入力します。

e) [仮想ドメイン（Virtual Domain）] ドロップダウン リストから仮想ドメインを選択します。

f) [電話番号（Telephone Number）]、[携帯電話の番号（Mobile Number）]、[郵便先住所（Postal Address）] の各フィールドに値を入力します。

g) [保存（Save）] をクリックします。

ステップ 4 IP アドレスを使用してノースバウンド トラップの受信者を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] から [ノースバウンド トラップの受信者（Northbound Trap Receiver）] を選択します。

b) [IP アドレス（IP Address）] オプション ボタンを選択し、[IP アドレス（IP Address）] および [サーバー名（Server Name）] に値を入力します。

c) [受信者のタイプ（Receiver Type）] および [通知タイプ（Notification Type）] で必要なタイプを選択します。

d) [ポート番号（Port Number）] に値を入力し、[SMNP バージョン（SMNP Version）] を選択します。
e) [SMNP バージョン（SMNP Version）] として [v2c] を選択する場合、必要に応じて [コミュニティ（Community）] 設定に値を入力します。
f) [SMNP バージョン（SMNP Version）] として [v3] を選択する場合、[ユーザー名（Username）]、[モード（Mode）]、[認証タイプ（Auth.Type）]、[認証パスワード（Auth.Password）]、[認証パスワードの確認（Confirm Auth.Password）]、[プライバシー タイプ（Privacy Type）]、[プライバシー パスワード（Privacy Password）]、[プライバシー パスワードの確認（Confirm Privacy Password）] の各フィールドに値を入力します。
g) [保存（Save）] をクリックします。

ステップ 5 DNS を使用してノースバウンド トラップの受信者を設定するには、次の手順を実行します。

a) [連絡先のタイプの選択（Select Contact Type）] から [ノースバウンド トラップの受信者（Northbound Trap Receiver）] を選択します。
b) [DNS] オプション ボタンを選択し、[DNS 名（DNS Name）] に値を入力します。
c) [受信者のタイプ（Receiver Type）] および [通知タイプ（Notification Type）] で必要なタイプを選択します。
d) [ポート番号（Port Number）] に値を入力し、[SMNP バージョン（SMNP Version）] を選択します。
e) [SMNP バージョン（SMNP Version）] として [v2c] を選択する場合、必要に応じて [コミュニティ（Community）] 設定に値を入力します。
f) [SMNP バージョン（SMNP Version）] として [v3] を選択する場合、[ユーザー名（Username）]、[モード（Mode）]、[認証タイプ（Auth.Type）]、[認証パスワード（Auth.Password）]、[認証パスワードの確認（Confirm Auth.Password）]、[プライバシー タイプ（Privacy Type）]、[プライバシー パスワード（Privacy Password）]、[プライバシー パスワードの確認（Confirm Privacy Password）] の各フィールドに値を入力します。
g) [保存（Save）] をクリックします。

（注）
- [受信者のタイプ（Receiver Type）] として [ゲスト アクセス（Guest Access）] を選択すると、 は通知ポリシーに従ってノースバウンド トラップの受信者にアラームを転送することはしません。ゲスト アクセス受信者は、ゲスト クライアント関連のイベントだけを受信します。通知ポリシーで使用するのは、ノースバウンド トラップの受信者のみです。外部 SNMPv3 トラップの受信者を設定する際は、必ず同じエンジン ID と同じ認証パスワードおよびプライバシー パスワードを使用してください。
- 通知の宛先トラップの受信者を更新中、動作状態には、次のポーリングによって状態が更新されるまで以前のトラップの受信者が表示されます。
- [通知ポリシー（Notification Policies）] ページには、[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [通知ポリシー（Notification Policies）] [モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラーム通知ポリシー（Alarm Notification Policies）]の順に選択して移動することもできます。
- 受信者の電子メール ID が複数の通知ポリシーで設定されていると、条件が一致した場合、アラームはその電子メール ID に一度だけ転送されます。
- 通知ポリシーに関連付けられている通知先を削除することはできません。

アラーム通知ポリシーのカスタマイズ

新しいアラーム通知ポリシーを追加するか、または既存のアラーム通知ポリシーを編集して、特定のデバイス グループで生成される特定のアラームに関する通知を、特定の受信者（電子メール受信者またはノースバウンド トラップ受信者のいずれかまたは両方）宛てに送信するようにできます。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [通知ポリシー（Notification Policies）] [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [アラーム通知ポリシー（Alarm Notification Policies）]を選択します。新しいアラーム通知ポリシーを追加するには、次の手順に従います。

a) [追加（Add）] アイコンをクリックし、[仮想ドメインの選択（Select a Virtual Domain）] ポップアップ ウィンドウで必要な仮想ドメインを選択します。

Cisco Prime Infrastructure により、仮想ドメインのデバイスから受信したアラームが、同じ仮想ドメインの通知ポリシーと照合されます。Prime Infrastructure により生成されるシステム カテゴリ アラームは、すべてのアラーム通知ポリシーと照合できます。

（注） 非ルート ドメインの場合、デバイスから送信されたアラームが転送されるのは、仮想ドメイン ページの [ネットワーク デバイス（Network Devices）] タブでそのデバイスまたはデバイスを含むデバイス グループが追加または選択されている場合だけです。

b) [OK] をクリックします。
[通知ポリシー（Notification Policies）] ウィザードが表示されます。

c) 通知をトリガーする必要があるシビラティ（重大度）、カテゴリ、およびイベント状態を選択します。デフォルトでは、すべてのシビラティ（重大度）タイプ、カテゴリ、および状態が選択されています。

d) [次へ（Next）] をクリックし、アラーム通知をトリガーするデバイス グループを選択します。

アラーム通知は、選択したデバイスグループに対してのみトリガーされます。

たとえば、デバイスグループのタイプに [ユーザー定義（User Defined）] を選択すると、設定されているユーザー定義のすべてのデバイスグループに対してアラーム通知がトリガーされます。同様に、デバイスグループのタイプに [ユーザー定義（User Defined）] と [場所（Locations）] の両方を選択した場合は、設定されているユーザー定義と場所のすべてのデバイスグループに対してアラーム通知がトリガーされます。

デバイスグループタイプを選択して、他のデバイスグループからの重要でないアラーム通知の受信を抑制します。

前のステップでシステム カテゴリ アラームだけを選択した場合は、[デバイス グループ（Device Group）] タブに「『システム』ベースのアラームだけが選択されている場合、デバイス グループは選択できません（Device Groups are not applicable when only 'System' based alarms are selected）」というメッセージが表示されます。ただし非システム カテゴリ アラームを選択した場合は、1 つ以上のデバイス グループを選択する必要があります。

e) [次へ（Next）] をクリックし、[通知の宛先（Notification Destination）] ページで必要な宛先を選択します。
ステップ 1-a でルート ドメインを選択した場合、Prime Infrastructure で作成されたすべての電子メールおよびノースバウンド トラップの受信者の宛先が [通知宛先（Notification Destination）] ページに表示されます。非ルート ドメインを選択している場合、特定のドメインで作成された電子メールの宛先が [通知宛先（Notification Destination）] ページに表示されます。アラーム通知先の設定 （285 ページ）を参照してください

f) あるいは、追加アイコンのドロップダウンリストで [電子メール（Email）] または [ノースバウンド トラップの受信者（Northbound Trap Receiver）] オプションを選択し、必要なフィールドに情報を入力します。

g) 通知の宛先を選択したら、[期間の変更（Change Duration）] をクリックします。

h) [期間の設定（Set Duration）] ポップアップ ウィンドウで [開始（From）] と [終了（To）] のタイミングを選択し、[OK] をクリックします。
指定した期間内に生成されるアラームだけが、通知宛先に送信されます。

i) [次へ（Next）] をクリックし、[サマリー（Summary）] ページでアラーム通知ポリシーの [名前（Name）] と [説明（Description）] を入力します。

j) **[保存（Save）]** をクリックします。

（注） 「インターフェイス」は予約語であるため、アラーム通知ポリシーの名前として使用しないでください。

ステップ 2 アラーム通知ポリシーを編集するには、次の手順を実行します。

a) ポリシーを選択し、編集アイコンをクリックします。
[通知ポリシー（Notification Policies）] ウィザードが表示されます。

b) ステップ 1 の説明に従い、[状態（Conditions）]、[デバイス グループ（Device Groups）]、および [宛先（Destination）] を選択します。
c) **[保存 (Save)]** をクリックします。

（注） [モニター（Monitor）]>[モニタリング ツール（Monitoring Tools）]>[アラム ポリシー（IAlarm Policies）] でアラーム タイプのシビラティ（重大度）を変更する場合は、ノースバウンド トラップの受信者の電子メール受信者には通知が送信されません。

関連トピック

アラーム通知先の設定 （285 ページ）

古い電子メールとトラップ通知データを新しいアラーム通知ポリシーに変換する

を以前のリリースから最新のバージョンへアップグレードまたは移行すると、の以前のリリースで作成された電子メールとトラップ通知データが新しいアラーム通知ポリシーに変換されます。

移行されたアラーム通知ポリシーは、[アラームおよびイベント通知ポリシー（Alarms and Events Notification Policies）] ページで確認できます。

では、次のアラームカテゴリがサポートされます。

- 変更監査
- 汎用
- システム
- アプリケーション パフォーマンス
- コンピューティング サーバー
- Nexus VPC スイッチ
- スイッチとルータ
- AP
- アドホック不正
- Clients
- コンテキスト認識型通知
- コントローラ
- カバレッジ ホール
- メッシュ リンク
- モビリティ サービス
- パフォーマンス
- RRM
- 不正 AP

- SE で検出された干渉源
- セキュリティ
- サードパーティ AP
- サードパーティ コントローラ

リリース 3.6 では、次のアラーム カテゴリはサポートされません。

- 自律 AP
- Cisco UCS シリーズ
- ルータ
- スイッチおよびハブ
- ワイヤレス コントローラ

移行されたアラーム通知ポリシーを編集するには、「アラーム通知ポリシーのカスタマイズ」を参照してください。

電子メール通知のデフォルト設定

メールサーバーを設定していない場合は、「SMTP電子メールサーバーの設定（112ページ）」に記載の手順を実行してください。この手順を実行しないと、通知は送信されません。

すべてのアラームおよびイベントのメール通知に適用される特定のデフォルト設定を設定できます。これらの設定は、ユーザーが個別の通知と受信者を設定するときに、上書きできます。

デフォルトでは、電子メールの件名にアラームのシビラティ（重大度）とカテゴリが含まれます。次の設定も使用できますが、デフォルトでは無効になっています。

- [件名（Subject line）]：より重要なアラームシビラティ（重大度）を含めるか、カスタム テキストを追加します。また、件名全体をカスタム テキストに置き換えることもできます。
- [電子メールの本文（Body of the email）]：カスタム テキスト、アラーム条件、およびアラームの詳細ページへのリンクを含めます。
- [セキュアなメッセージ モード（Secure message mode）]：このモードを有効にすると、IP アドレスとコントローラ名がマスクされます。

これらの設定を有効化、無効化、または調整するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** を選択し、さらに **[アラームおよびイベント（Alarms and Events）]** > **[アラームおよびイベント（Alarms and Events）]** を選択します。[アラーム電子メール オプション（Alarm Email Options）] エリアで変更を加えます。

アラームクリーンアップ、表示、および電子メールオプションの指定

[Administration] > [System Settings] > [Alarms and Events] ページでは、アラームのクリーンアップ、表示、電子メール送信のタイミングと方法を指定できます。

ステップ 1 [Administration > [Settings] > [System Settings] > [Alarms and Events] > [Alarms and Events] を選択します。

ステップ 2 [アラームおよびイベントのクリーンアップ オプション（Alarm and Event Cleanup Options）] を次のように変更します。

- [アクティブおよびクリアされたアラームを次の後で削除（Delete active and cleared alarms after）]：アクティブなアラームまたはクリアされたアラームが削除されるまでの日数を入力します。
- [Delete cleared security alarms after]：セキュリティ アラーム、不正 AP アラーム、およびアドホック不正アラームが削除されるまでの日数を入力します。
- [Delete cleared non-security alarms after]：セキュリティ アラーム以外のアラームが削除されるまでの日数を入力します。セキュリティ アラーム以外のアラームには、[Security]、[Rogue AP]、または [Adhoc Rogue] カテゴリに属するアラーム以外のすべてのアラームが含まれます。
- [Delete all events after]：すべてのイベントを削除するまでの日数を入力します。
- [最大保持イベント数（Max Number of Events to Keep）]：データベースで保持する必要があるイベントの数を入力します。

Cisco Prime Infrastructure ではデフォルトで、通常のデータ クリーンアップ タスクの一部として古いアラームとイベントが削除され、2 時間ごとにデータベース アラーム テーブルのストレージ サイズが確認されます。アラーム テーブルが 300,000 の上限を超えた場合、Prime Infrastructure はアラーム テーブルのサイズが制限内に収まるまで、クリアされたアラームを最も古いものから削除します。クリアされたアラームを 7 日より長く保持する必要がある場合は、アラーム テーブルのサイズが上限に達しない範囲で、[クリアされた非セキュリティアラームを次の後で削除（Delete cleared non-security alarms after）] テキスト ボックスに 7 日を超える値を指定できます。

ステップ 3 [syslog クリーンアップ オプション（Syslog Cleanup Options）] を次のように変更します。

- [すべての syslog を次の後で削除（Delete all Syslogs after）]：すべての古い syslog について、削除するまでの日数を入力します。
- [最大保持 syslog 数（Max Number of Syslog to Keep）]：データベースで保持する必要がある syslog の数を入力します。

ステップ 4 必要に応じて、[アラーム表示オプション（Alarm Display Options）] を変更します。

- [Hide acknowledged alarms]：このチェック ボックスをオンにすると、承認済みのアラームは [Alarm] ページに表示されません。このオプションは、デフォルトで有効です。シビラティ（重大度）の変化に関係なく、確認応答済みのアラームに対して電子メールは生成されません。
- [Hide assigned alarms]：このチェックボックスをオンにすると、割り当て済みのアラームは [Alarm] ページに表示されません。

- [クリア済みのアラームを非表示（Hide cleared alarms）]：このチェックボックスをオンにすると、クリアされたアラームは [アラームのまとめ（Alarm Summary）] ページに表示されません。このオプションは、デフォルトで有効です。
- [Add device name to alarm messages]：このチェックボックスをオンにすると、デバイスの名前がアラーム メッセージに追加されます。

これらのオプションの変更は、[Alarm] ページにのみ適用されます。エンティティに対するアラームのクイック検索は、アラームの状態に関係なく、そのエンティティのすべてのアラームを表示します。

ステップ 5 アラームの [障害ソース パターン（Failure Source Pattern）] を次のように変更します。

- カスタマイズするカテゴリを選択し、[Edit] をクリックします。
- 利用可能な選択肢から障害ソース パターンを選択し、[OK] をクリックします。
- セパレータをカスタマイズするカテゴリを選択し、[セパレータの編集（Edit Separator）] をクリックします。使用可能なオプションの 1 つを選択し、[OK] をクリックします。

選択したカテゴリに対して生成されるアラームには、ユーザーが設定するカスタム パターンが使用されます。たとえば、[クライアント（Clients）] カテゴリを選択し、セパレータが # になるように編集するとします。サポートされるクライアント アラームが生成されたときにユーザーが [モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択すると、そのアラームの [障害のソース（Failure Source）] 列は *MAC* アドレス#名前となります。

（注） 障害のソースは、カスタム トラップ、syslog 生成イベント、およびカスタム syslog 変換ではサポートされません。

ステップ 6 [電子メールオプションのアラーム（Alarm Email Options）] を次のように変更します。

- [電子メール通知に Prime Infrastructure アドレスを追加（Add Prime Infrastructure address to email notifications）]：このチェックボックスをオンにすると、電子メール通知に Prime Infrastructure アドレスが追加されます。
- [Include alarm severity in the email subject line]：このチェック ボックスをオンにすると、電子メールの件名にアラームシビラティ（重大度）が含まれるようになります。このオプションは、デフォルトで有効です。
- [Include alarm Category in the email subject line]：このチェック ボックスをオンにすると、電子メールの件名にアラームのカテゴリが含まれるようになります。このオプションは、デフォルトで有効です。
- [Include prior alarm severity in the email subject line]：このチェック ボックスをオンにすると、電子メールの件名に事前アラームシビラティ（重大度）が含まれるようになります。
- [Include custom text in the email subject line]：このチェック ボックスをオンにすると、電子メールの件名にカスタム テキストが追加されます。[Replace the e-mail subject line with custom text] チェック ボックスをオンにして、電子メールの件名をカスタム テキストに置き換えることもできます。
- [Include custom text in body of email]：このチェック ボックスをオンにすると、電子メールの本文にカスタム テキストが追加されます。
- [Include alarm condition in body of email]：このチェック ボックスをオンにすると、電子メールの本文にアラーム状態が含まれるようになります。
- [電子メールの本文にアラーム アプリケーション カテゴリ データを含める（Include alarm application category data in body of email）]：このチェックボックスをオンにすると、電子メールの本文にアラーム カテゴリが含まれるようになります。

- [Add link to Alarm detail page in body of email]：このチェック ボックスをオンにすると、電子メールの本文に [Alarm detail] ページへのリンクが追加されます。
- [Enable Secure Message Mode]：チェックボックスをオンにすると、セキュア メッセージ モードが有効になります。[Mask IP Address and Mask Controller Name] チェック ボックスをオンにした場合、アラーム電子メールはセキュア モードで送信され、すべての IP アドレスとコントローラ名はマスクされます。
- [電子メール送信間隔（Email Send Interval）]：電子メールの送信間隔を指定します。

（注） Prime Infrastructure はアラームの最初のインスタンスに関するアラーム通知電子メールを送信し、その後の通知はアラームシビラティ（重大度）が変更された場合にのみ送信されます。

- [Skip to send first alarm separately as email notification]：最初のアラームは、個別の電子メール通知として送信されます。

（注） このオプションを無効にすると、指定した [Email Send Interval] 期間における最初のアラームの直後に電子メール通知が送信されます。残りのアラームは2番目の電子メールにグループ化されます。このオプションを有効にすると、指定した [Email Send Interval] 期間に 1 通の電子メール通知のみが送信されます。最初の電子メールアラートは既存のリストにグループ化されます。

ステップ 7 [Alarm Other Options] を次のように変更します。

- [コントローラライセンス数のしきい値（Controller License Count Threshold -）]：しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラで使用可能なライセンスの指定レートに達すると、アラームがトリガーされます。たとえば、コントローラのアクセスポイントライセンスが 100、しきい値が 80% で設定されている場合、コントローラに接続されているアクセスポイントの数が 80 を超えると、アラームがトリガーされます。
- [コントローラ アクセスポイント数のしきい値（Controller Access Point Count Threshold -）]：しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラでサポートされているアクセスポイントの最大数の指定レートに達すると、アラームがトリガーされます。たとえば、コントローラが最大6000アクセスポイントをサポートしており、しきい値が80%に設定されている場合、コントローラに接続されているアクセスポイントの数が 4800 を超えるとアラームがトリガーされます。
- [Unacknowledge and Unassign Alarm on Clear]：リストからクリアされた確認済みおよび割り当て済みのアラームを未確認のままにし、再発した場合に同じ所有者に対して割り当て解除する必要がある場合は、このチェックボックスをオフにします。確認済みまたは前の所有者に割り当てられたアラームをクリアするときに、アラームが未確認で割り当てられていない場合は、このチェックボックスをオンにします。

ステップ 8 [Save] をクリックします。

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

次の表に、確認済み、クリア済み、および割り当て済みのアラーム用の表示オプションの一部を示します。これらの設定は、個別のユーザーが（表示設定で）調整することができません。これは、非常に大規模なシステムの場合に、ユーザーがシステムパフォーマンスに影響を及ぼすような変更を加える可能性があるためです。

- アラーム、イベント、および Syslog の消去 （180 ページ）

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [表示オプションのアラーム（Alarm Display Options）] 領域で、必要に応じて、これらの設定を有効または無効にします。

アラーム表示オプション	説明	設定が検索結果にも影響するかどうか
確認済みのアラームを非表示（Hide acknowledged alarms）	[アラーム（Alarms）] リストに確認済みのアラームを表示しないか、それらを検索結果に含めません。	○
割り当て済みのアラームを非表示（Hide assigned alarms）	[アラーム（Alarms）] リストまたは検索結果に割り当て済みのアラームを表示しません。	○
クリア済みのアラームをアラームブラウザで非表示（Hide cleared alarms in alarm browser）	[アラーム（Alarms）] リストまたは検索結果にクリア済みのアラームを表示しません。	なし
アラームメッセージにデバイス名を追加（Add device name to alarm messages）	電子メール通知にデバイス名を追加します。	なし

ステップ 3 変更を適用するには、[アラームおよびイベント（Alarms and Events）] ウィンドウの下部にある [保存（Save）] をクリックします。

シビラティ（重大度）レベルの変更

の各アラームにはシビラティ（重大度）が設定されます。アラームのシビラティ（重大度）は、アラームに関連付けられている最も重大なイベントによって決定します。新たに生成されたイベントのシビラティ（重大度）を変更することにより、アラームのシビラティ（重大度）を調整できます。

（注） ハイ アベイラビリティなど のシステム管理に関連付けられたアラームについては、サーバーの内部 SNMP トラップのカスタマイズおよびトラップの転送（125 ページ）を参照してください。

- 特定のアラーム：このセクションの手順を使用します。

ステップ 1 **[管理（Administration）] > [システム設定（System Settings）]** を選択し、**[アラームおよびイベント（Alarms and Events）] > [アラームのシビラティ（重大度）および自動クリア（Alarm Severity and Auto Clear）]** の順に選択します。

ステップ 2 列で使用可能なカテゴリを拡張するか、または列見出しのすぐ下にある フィールドにイベントテキスト全体または一部を入力して必要な を検索します。

アラームの自動クリア間隔の変更

特定の期間が経つと自動的にアラームがクリアされるように設定できます。この設定は、クリアイベントがない場合などに役立ちます。アラームの自動クリアによって、アラームに関連するイベントの重大度が変更されることはありません。

（注）
- アラームの自動クリアを有効にしている場合、作成されたアラームのクリアに遅延が生じることがあります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[アラームおよびイベント（Alarms and Events）] > [アラームのシビラティ（重大度）および自動クリア（Alarm Severity and Auto Clear）]** を選択します。

ステップ 2 [イベントタイプ（Event Types）] 列の下に表示されているカテゴリを展開します。または、列ヘッダーの下にある [イベントタイプ（Event Types）] 検索フィールドにイベントのテキストの全部または一部を入力することにより、イベントタイプを検索します。

ステップ 3 自動クリアの期間を変更するには、次の手順を実行します。

- 単一のイベントの場合、チェックボックスをオンにしてイベントを選択し、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックするか、**または**、選択したイベントの [自動クリア期間（Auto Clear Duration）] 列の下のフィールドをダブルクリックします。新しい期間を入力します。
- 複数のイベントの場合、イベントまたはイベントのグループのチェックボックスをオンにし、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックして、新しい期間を入力します。

ステップ 4 [OK] または [保存（Save）] をクリックして、自動クリア期間を保存します。

アラームの失敗の原因に表示される情報を変更する

アラームが生成された場合は、失敗の原因に関する情報がそれに含まれています。情報は特定の形式を使用して表示されます。たとえば、パフォーマンスの失敗の場合は、*MACAddress*:*SlotID* という形式が使用されます。他のアラームの失敗の原因として、ホスト名、IP アドレス、またはその他のプロパティが含まれている場合があります。次の手順を使用して、アラームの失敗の原因に表示されるプロパティと区切り文字（コロン、ダッシュ、またはシャープ記号）を調整します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[アラームおよびイベント（Alarms and Events）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 2 [失敗の原因パターン（Failure Source Pattern）] 領域で、カスタマイズするアラーム カテゴリを選択します。

ステップ 3 次のように失敗の原因形式を調整します。

- 表示されるプロパティをカスタマイズするには、[編集（Edit）] をクリックして、プロパティを選択し、[OK] をクリックします。プロパティが灰色表示されている場合は、それを削除することができません。
- プロパティの間に表示される区切り文字をカスタマイズするには、[区切り文字の編集（Edit Separator）] をクリックします。

ステップ 4 変更を適用するには、[アラームおよびイベント（Alarms and Events）] 設定ウィンドウの下部にある [保存（Save）] をクリックします。

完全優先ベントの動作の変更

は、デバイスから設定変更イベントを受信すると、他の関連するイベントが送信される場合に備えて特定の時間待機してからインベントリ収集を開始します。これにより、複数の収集プロセスの同時実行が回避されます。これは、インベントリ収集保留時間と呼ばれ、デフォルトで 10 分に設定されています。この設定は、[インベントリ（Inventory）] システム設定ページ（**[管**

理（**Administration**）] > **[**設定（**Settings**）] > **[**システム設定（**System Settings**）] > **[**インベントリ（**Inventory**）]）で制御されています。

次のイベントは、デフォルトの時間間隔である 10 分以内に によって処理されます。

タイプ	サポートされるイベント
リンク	LINK-3-UPDOWN
カード保護	CARD_PROTECTION-4-PROTECTION CARD_PROTECTION-4-ACTIVE
VLAN	PORT_SECURITY-6-VLAN_REMOVED PORT_SECURITY-6-VLAN_FULL
ICCP SM	L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR INFRA-ICCP-5-ISOLATION INFRA-ICCP-5-ISOLATION_CLR INFRA-ICCP-5-NEIGHBOR_STATE_UP INFRA-ICCP-5-NEIGHBOR_STATE_DOWN INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN L2-BM-6-ACTIVE_CLEAR L2-BM-6-ACTIVE_PROBLEM L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR
衛星	PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR
クラスタ	PLATFORM-REDDRV-7-ROLE_CHANGE PLATFORM-CE_SWITCH-6-UPDN PLATFORM-CLUSTER_CLM-6-UPDN LINK_UP LINK_DOWN
Celeborn カード	UEA_SPA_MODE-6-UEA_SPA_MODE_CHG
コンフィギュレーション コミット syslog	MGBL-CONFIG-6-DB_COMMIT SYS-5-CONFIG_I

ただし、次の重大なイベントが発生した場合はすぐに、によってデバイスのフルディスカバリが実行されます。

SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
cefcFRURemoved
cefcFRUInserted

Web GUI に表示される汎用イベントのカスタマイズ

SNMP トラップおよび syslog によって生成される汎用イベントの説明とシビラティ（重大度）をカスタマイズすることができます。カスタマイズした内容は、SNMP トラップ イベントの [イベント（Events）] タブに表示されます。MIB モジュールがロードされていない場合は、手動でロードし、その MIB で提供される通知をカスタマイズすることができます。

これらの汎用イベントをカスタマイズする方法については、「SNMP トラップに基づく汎用イベントのカスタマイズ （299 ページ）」を参照してください。

汎用トラップおよび Syslog の処理の無効化および有効化

デフォルトでは、 は受信した syslog またはトラップを廃棄しません。 は、受信した syslog またはトラップについて が新規イベントを作成すべきかどうかを決定する（新規イベントを作成する場合は、アラームを作成するかどうかも決定する）イベント カタログを保持しています。 がイベントを作成しない場合、トラップまたは syslog は汎用イベントと見なされます。

デフォルトでは、 により次のことが実行されます。

- イベント一覧に汎用イベントが表示されます。

トラップの内容に関係なく、これらのすべてのイベントに MINOR シビラティ（重大度）が割り当てられ、アラーム カテゴリ [汎用（Generic）] に分類されます。

汎用トラップ処理を有効または無効にする

genericTrap.sh コマンドを使用して一般的な syslog を管理します。

操作の目的：	使用するコマンド：
汎用トラップ処理をオフにする	**/opt/CSCOlumos/bin/genericTrap.sh -l**
汎用トラップ処理をオンにする	**/opt/CSCOlumos/bin/genericTrap.sh -u**

汎用 syslog 処理の無効化および有効化

汎用 syslog を管理するには、genericSyslog.sh コマンドを使用します。

操作の目的：	使用するコマンド：
汎用 syslog 処理をオフにする	**/opt/CSCOlumos/bin/genericSyslog.sh -l**
汎用 syslog 処理をオンにする	**/opt/CSCOlumos/bin/genericSyslog.sh -u**

SNMP トラップに基づく汎用イベントのカスタマイズ

では、GUI での汎用イベントのカスタマイズ表現がサポートされています。管理対象オブジェクトは通常、SNMP トラップと通知を生成します。これらの通知には、SNMP トラップ オブジェクトの ID（SnmpTrapOID）と可変バインド オブジェクト ID（VarBindOIDs）が数値形式で含まれています。 は、カスタマイズされた MIB モジュールを使用して、SnmpTrapOID および VarBindOID の数値をわかりやすい名前に変換し、その後 Web GUI（イベント テーブル、[デバイス 360（Device 360）] ビューなど）に汎用イベントを表示します。

にパッケージされている SNMP MIB ファイルを使用して、各自の展開環境のテクノロジー要件に合わせて、定義されている MIB をカスタマイズできます。

次の表に、ObjectID の復号化方法と GUI での表示方法を示します。

表 *13 :* 例 : *ObjectID* 表現

復号化前の OID	復号化後の OID
snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1	mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1

次の手順に従い、カスタム汎用イベントを作成します。

ステップ 1 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** の順に選択します。

ステップ 2 [イベント（Events）] タブをクリックします。

ステップ 3 [カスタム トラップ イベント（Custom Trap Events）] をクリックし、次に [新しい MIB のアップロード（Upload New Mibs）] をクリックします。

ステップ 4 [MIB のアップロード（Upload Mib）] ウィンドウで、[新しい MIB のアップロード（Upload New MIB）] をクリックし、MIB ファイルをアップロードします。

ステップ 5 新しいMIBファイルをアップロードする場合は、ファイルのアップロードが完了するまで待機してから、[MIB の更新（Refresh MIBs）] をクリックします。新しく追加された MIB が [MIB] ドロップダウンリストに含まれるようになります。

ステップ 6 [OK] をクリックします。

は、指定されたトラップの新しいイベント タイプとアラーム条件を作成します。

障害処理エラーのトラブルシュート

導入環境で障害処理に問題が発生している場合、次の手順に従って障害ログを確認します。

ステップ 1 管理者権限を持つユーザー ID を使用して にログインします。

ステップ 2 **[管理（Administration）]>[設定（Settings）]> [ロギング（Logging）]** を選択し、[グローバル設定（Global Settings）] タブを選択します。

ステップ 3 [ダウンロード（Download）] をクリックしてすべてのサーバーのログファイルをダウンロードします。

ステップ 4 これらのログファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

console.log

ncs-x-x.log

decap.core.java.log

xmp_correlation.log

decap.processor.log

（注） [EPNMからのリセット（Reset from EPNM）] をクリックしてグローバル設定をリセットすることはできません。

次のタスク

シスコ サポート コミュニティからも援助を受けられます。サポート ケースを開く必要がある場合は、疑わしいログファイルをケースに添付します。シスコ サポート コミュニティとテクニカルアシスタンスセンター（TAC）から支援を受ける（300ページ）を参照してください。

シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける

シスコ サポート ケースの登録

Web GUI からサポート ケースを登録すると、 ではデバイスから取得できる情報が、このケースフォームに自動的に読み込まれます。これには、デバイスの技術的な詳細、デバイスでの設定変更、および過去24時間以内に発生したすべてのデバイスイベントなどがあります。また、ケースに各自のファイルを添付することもできます。

始める前に

次の状況では、Web GUI でサポート ケースを登録できます。

- 管理者により、ユーザーがこの作業を実行できるように が設定されている。
- サーバーがインターネットに直接接続しているか、またはプロキシサーバー経由で接続している。

- Cisco.com のユーザー名とパスワードがある。

ステップ 1 次のいずれかを実行します。

- **[モニター（Monitor）]**>**[モニタリング ツール（Monitoring Tools）]**>**[アラームおよびイベント（Alarms and Events）]** の順に選択します。アラームを 1 つクリックし、**[トラブルシュート（Troubleshoot）]**>**[サポート ケース（Support Case）]** を選択します。[トラブルシュート（Troubleshoot）] ボタンが表示されない場合は、ブラウザ ウィンドウを拡大します。
- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから [サポート リクエスト（Support Request）] を選択します。

ステップ 2 Cisco.com ユーザー名とパスワードを入力します。

ステップ 3 [作成（Create）] をクリックします。 は、デバイスから取得するデータをこのフォームに読み込みます。

ステップ 4 （オプション）組織のトラブル チケット システムに対応したトラッキング番号を入力します。

ステップ 5 [次へ（Next）] をクリックして、問題の説明を入力します。

では、デバイスから取得したデータがフォーム読み込まれ、必要なサポート ドキュメントが自動的に生成されます。

必要に応じて、ローカル マシンからファイルをアップロードします。

ステップ 6 [サービス リクエストの作成（Create Service Request）] をクリックします。

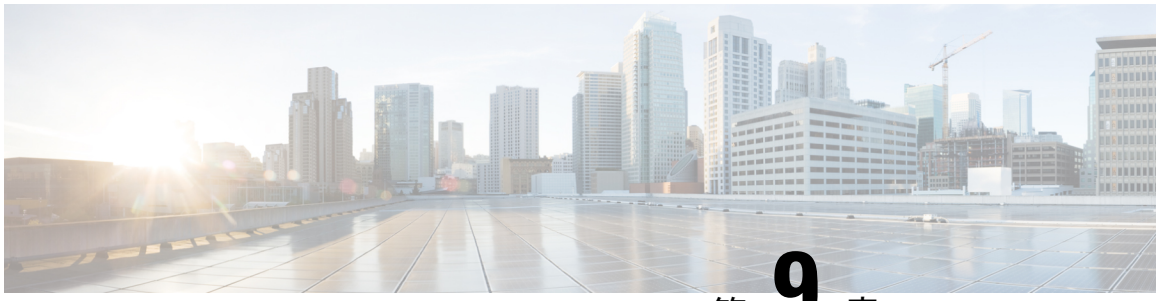
シスコ サポート コミュニティへの参加

オンライン シスコ サポート コミュニティ内のディスカッション フォーラムにアクセスして、参加できます。Cisco.com のユーザー名とパスワードが必要です。

ステップ 1 次のいずれかを実行します。

- **[Monitor] [>] [Monitoring Tools] [>] [Alarms and Events]** に移動します。いずれかのアラームをクリックし、**Troubleshoot > Support Forum** を選択します。**[Troubleshoot]** ボタンが表示されない場合は、ブラウザ ウィンドウの幅を広げてください。
- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから、[サポート コミュニティ（Support Community）] を選択します。

ステップ 2 シスコ サポート コミュニティ フォーラムのページで、必要な情報を見つけるための検索パラメータを入力します。



第 9 章

監査およびログ

ここでは、次の内容について説明します。

設定アーカイブとソフトウェア管理の変更を監査する（）

[ネットワーク監査（Network Audit）][変更監査ダッシュボード（Change Audit Dashboard）]ウィンドウに、設定アーカイブとソフトウェア管理機能を使用して行われたデバイスへの変更が表示されます。これらの変更を表示するには、 を選択します。 によって、最新のデバイスの変更が変更のタイプ（設定アーカイブ、ソフトウェア イメージ管理）とともに一覧表示されます。

また、デバイスの 360 度ビューの [最新の変更（Recent Changes）] タブで、デバイスの最新の変更を表示することもできます。

ユーザーによって行われる変更の監査（変更の監査）

では、以下の方法で、変更の監査データの管理がサポートされています。

変更監査レポートの生成

変更監査レポートには、ユーザーが の機能を使用して実行したアクションのリストが表示されます。次の表に、変更監査レポートの表示内容の例を示します。

機能	例
デバイス管理	デバイス「209.165.202.159」が追加された
ユーザー管理	ユーザー「mmjones」が追加された

機能	例
管理	209.165.202.129 からのユーザー jlsmith のログアウトが成功 認証に失敗した209.165.202.125 からのユーザー fjclark のログインに失敗
コンフィギュレーションの変更	CLI コマンド：ip access-list standard testremark test
モニタリングポリシー	モニタリング テンプレート「IF Outbound Errors (Threshold)」が作成された
構成テンプレート	構成テンプレート「Add-Host-Name-IOS-Test」が作成された
ジョブ	[設定の展開 - 展開ビュー（Config Deploy - Deploy View）] タイプの「Show-Users-On-Device-IOS_1」ジョブがスケジュールされた
インベントリ	論理ファイル「/bootflash/tracelogs/inst_cleanup_R0-0.log.19999.20150126210302」が削除された

変更監査レポートを定期的に実行するようにスケジュールできます。また、必要に応じて から結果を電子メールで送信することもできます。さらに、この情報を変更監査通知で転送することもできます（変更監査通知の有効化および syslog レシーバの設定 （304 ページ）を参照）。

ステップ 1 **[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）]** を選択し、**[コンプライアンス（Compliance）] > [監査の変更（Change Audit）]** を選択します。

ステップ 2 [新規（New）] をクリックして新しいレポートを生成します。

ステップ 3 [設定（Settings）] エリアに、レポート条件（期間、レポートの開始時点など）を入力します。

ステップ 4 後で実行するようにレポートをスケジュールするには、[スケジュール（Schedule）]エリアに設定を入力します。また、レポートの送信先となる電子メール アドレスを指定することもできます。

ステップ 5 レポートをすぐに実行するには、ウィンドウの下部にある [実行（Run）] をクリックします。

[レポートの実行結果（Report Run Result）] に、すべてのユーザーおよび指定された期間内に行われた変更がリストされます。

変更監査通知の有効化および syslog レシーバの設定

必要に応じて、システムに変更が加えられると が変更監査通知を送信するように設定できます。これらの変更には、デバイスインベントリと設定の変更、設定テンプレートおよびモニタリング テンプレートの操作、ユーザー操作（ログイン、ログアウト、ユーザー アカウントの変更など）が含まれます。

次の動作を行うように を設定できます。

- 変更監査通知として変更を Java メッセージ サーバー（JMS）に転送する
- これらのメッセージを特定の syslog レシーバに送信する

syslog レシーバを設定しても syslog を受信しない場合は、宛先 syslog レシーバでのウイルス対策またはファイアウォールの設定を変更して、syslog メッセージの受信を許可するようにしなければならない可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[メールと通知（Mail and Notification）] > [監査通知の変更（Change Audit Notification）]** を選択します。

ステップ 2 [監査の変更通知の有効化（Enable Change Audit Notification）] チェックボックスをオンにして通知を有効にします。

ステップ 3 メッセージを特定の syslog レシーバに送信するには、次の手順に従います。

a) [追加（Add）] ボタン（+）をクリックして、Syslog レシーバを指定します。

b) [syslogレシーバ（Syslog Receiver）] 領域で、syslog レシーバの IP アドレス、プロトコル、およびポート番号を入力します。

さらに追加の syslog レシーバを指定するには、必要に応じてこの手順を繰り返します。

ステップ 4 [保存（Save）] をクリックします。

（注） レコードをセキュアな tls ログに反映するために サーバーの再起動をお勧めします。

監査の変更の詳細表示

ステップ 1 管理者として にログインします。

ステップ 2 **[モニター（Monitor）] > [ツール（Tools）] > [監査の変更ダッシュボード（Change Audit Dashboard）]** を選択します。

[監査の変更ダッシュボード（Change Audit Dashboard）] では、ネットワークの監査ログを表示し、デバイス管理、ユーザー管理、構成テンプレート管理、デバイス コミュニティとクレデンシャルの変更、およびデバイスのインベントリ変更に関する監査データを変更します。[監査レポートの変更（Change Audit report）] と [監査の変更（Change Audit）] ダッシュボードには、ログインしている仮想ドメインに関係なく詳細が表示されます。

[監査ダッシュボードの変更（Change Audit Dashboard）] 画面には、IP アドレス、監査の説明、監査名、クライアント IP アドレスなどの細かな項目とは別に、デバイス名が表示されるようになりました。さらに、IP アドレスの他に [i] アイコンをクリックすると、デバイス 360 の詳細を表示できます。

GUI から実行されたアクションを監査する（システムの監査）

（注） は、すべての監査変更通知を XML 形式でトピック **ChangeAudit.All** に送信します。通知を受信するためには、**ChangeAudit.All** に登録する必要があります。

[システムの監査（System Audit）] ウィンドウに、ユーザーがアクセスしたすべての GUI ページが一覧表示されます。[システムの監査（System Audit）] を表示するには、**[管理（Administration）] > [設定（Settings）] > [システムの監査（System Audit）]** を選択します。

次の表に、クイック フィルタを使用して [システムの監査（System Audit）] ページで見つかる情報の一部を示します。クイック フィルタを有効にするには、[表示（Show）] ドロップダウン リストから [クイック フィルタ（Quick Filter）] を選択します。

実行されたアクションの検索対象：	次の手順を実行します。
特定のユーザー	[ユーザー名（Username）] クイック フィルタ フィールドにユーザー名を入力します。
ユーザー グループ内のすべてのユーザー	[ユーザー グループ（User Group）] クイック フィルタ フィールドにグループ名を入力します
特定の仮想ドメイン内のデバイス	[アクティブ仮想ドメイン（Active Virtual Domain）] クイック フィルタ フィールドに仮想ドメイン名を入力します。
Web GUI ルート ユーザー	[表示（Show）] ドロップダウン リストから、[ルート ユーザー ログ（Root User Logs）] を選択します。
特定のデバイス	[IP アドレス（IP Address）] クイック フィルタ フィールドに IP アドレスを入力します。
特定の日付	[監査時間（Audit Time）] クイック フィルタ フィールドに日付を入力します（*yyyy–mmm–dd* の形式）。

システム ログ

は、**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** を選択して制御される 3 つのクラスのログを提供しています。

ログの種類	説明	次を参照してください。
一般	システムでのアクションに関する情報を取得します。	一般的なシステム ログを表示して管理する （307 ページ）
SNMP	管理対象デバイスとの対話を取得します。	SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整 （321 ページ）
Syslog	監査ログを（syslog として）他の受信者に転送します。	Syslog としてのシステム監査ログの転送 （320 ページ）

一般的なシステム ログを表示して管理する

システム ログは、ローカル サーバーにダウンロード後に表示することができます。

特定のジョブのログを表示する

ステップ 1 **[管理（Administration）]>[ダッシュボード（Dashboards）]>[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

ステップ 2 [ジョブ（Jobs）]ペインからジョブタイプを選択し、[ジョブ（Jobs）] ウィンドウからジョブインスタンス リンクをクリックします。

ステップ 3 [ジョブインスタンス（Job instance）] ウィンドウの左上にある [ログファイル（Log file）] を見つけ、[ダウンロード（Download）] をクリックします。

（注） 設定アーカイブソフトウェア、設定ロールバック、設定上書き、設定展開のジョブタイプのログのみをダウンロードできます。

ステップ 4 必要に応じてファイルを開くか保存します。

一般的なログ ファイルの設定とデフォルト サイズの調整

デフォルトでは、は、すべての管理対象デバイスで生成されたすべてのエラー、情報、およびトレース メッセージをログに記録します。

操作の目的：	**[管理（Administration）]>[設定（Settings）]>[ロギング（Logging）]での操作：**
ログのサイズ、保存するログの数、ファイル圧縮のオプションを変更する	ログ ファイルの設定を調整します。 （注） システムへの影響を避けるため、これらの設定は慎重に変更してください。 Log4j MaxBackupIndex ごとに、メインファイルが 1 つ存在し、バックアップファイルのセット数が伴います。たとえば、ログファイルの数が 3 に設定されている場合は、1 つのメインファイル（.log）と 3 つのバックアップファイル（.log.1、.log.2、.log.3）が存在します。 [ファイルの数（Number of files）] を以前に設定した値よりも小さい値に変更した場合、ログファイルの設定は新しく生成されたファイルにのみ適用されます。たとえば、設定済みの値が 5 の場合、ここで 2 に変更すると、設定は .log ファイル .log.1 および .log.2 にのみ適用されます。files.log.3、.log.4、および .log.5 に変更はありません。 **[圧縮（Zip）（Compression (Zip)）]** オプションを選択すると、ログファイルが圧縮され、プロセスの フォルダにアーカイブされます。圧縮されたログファイルの保持は、次の基準に従います。 • [ストレージ（MB）（Storage (MB)）]：フォルダの最大サイズ（MB） • [日数（Number of Days）]：ログファイルの最大経過時間 いずれかの条件が満たされると、消去が開始されます。 必要に応じて、[外部ロケーションへのバックアップ（Backup to external location）] が有効になっている場合、クリーンアップ対象としてマークされたログファイルは、削除前に指定された外部リポジトリにコピーされます。 （注） [外部ロケーションへのバックアップ（Backup to external location）] を選択した場合は、ログが失われないように、[グローバル設定（Global Settings）] タブでパラメータが定義されていることを確認してください。

操作の目的：	**[管理（Administration）]>[設定（Settings）]>[ロギング（Logging）]での操作：**
特定のモジュールのログ レベルを変更する	[一般的なログ設定（General Log Settings）] で、ファイルと必要なレベルを選択して **[Save]** をクリックします。たとえば、[メッセージレベル（Message Level）] ドロップダウンリストから、現在のログ レベルとして次のいずれかを選択します。 • [エラー（Error）]：システム上のエラー ログをキャプチャします。 • [情報（Information）]：システム上の情報ログをキャプチャします。 • [トレース（Trace）]：詳細情報をログに記録するために、システムで管理対象デバイスの問題を再現します。 • [デバッグ（Debug）]：システムのデバッグログをキャプチャします。 変更を有効にするには、 を再起動する必要があります。

トラブルシューティングのためのログ ファイルのダウンロードとメール送信

（注） この手順では、ログ メッセージ レベルを [トレース（Trace）] に設定します。システム パフォーマンスに影響しないように、ログ メッセージ レベルを必ず元の設定に戻してください。

ステップ 1 **[管理（Administration）]**>**[設定（Settings）]**>**[ロギング（Logging）]** を選択し、[ログファイル設定（Log File Settings）] を選択します。

ステップ 2 後でリセットする必要があるため、[メッセージ レベル（Message Level）] ドロップダウンリストの設定をメモします。

ステップ 3 [ログモジュールの有効化（Enable Log Modules）] 領域で、目的の [ログモジュール（Log Modules）] を選択します。

ログモジュール	説明
AAA	このログモジュールは、ncs-0-0.log ファイル、nms_sys_error.log ファイル、usermgmt.log ファイル、および XmpUserMgmtRbac.log ファイルを有効にします。ユーザーがログインするとログが印刷されます。ローカル、TACACS、RADIUS、および SSO モードの変更など、 AAA モードの変更が実行されます。
アクセスワークフロー	このログモジュールは、ifm_access_workflow.log ファイルを有効にします。

ログモジュール	説明
アクションフレームワーク	このログモジュールは、nms-actions.log ファイルを有効にします。
admin	このログモジュールは、ファイルサイズ、メッセージレベルなどをキャプチャする admin.log ファイルを有効にします。
Alertcache	このログモジュールは、alertcache.log ファイルと alertcache_error.log ファイルを有効にします。
APIC	このログモジュールは、PNP プロファイルが APIC と同期したときに発生するログをキャプチャする ifm_apic.log ファイルを有効にします。
APICPIIntegration	このログモジュールは、プロファイルがサイトとして APICEM で同期されたときにログをキャプチャする apic_pi_integration.log ファイルを有効にします。
AppNav	このログモジュールは、テンプレートに ACL 設定を保存し、テンプレートから ACL を削除し、WAAS インターフェイスを作成および更新するとき、およびサービスノードグループとコントローラグループを作成、更新、削除するときに、ログをキャプチャするために appNav.log ファイルを有効にします。
アシュアランス AppClassifier（Assurance AppClassifier）	このログモジュールは、着信 AVC/ワイヤレス NetFlow データでの NBAR 分類に関連する情報をキャプチャする assurance_appclassifier.log ファイルを有効にします。これは、 での NetFlow 処理の一環として、フローレコードのアプリケーションの分類または識別を行うためのものです。
アシュアランス NetFlow（Assurance Netflow）	このログモジュールは、さまざまな NetFlow デバイスから へ送信する着信 NetFlow データの処理に関する情報をキャプチャする assurance_netflow.log ファイルを有効にします。UDP ポート 9991 で受信したフローエクスポートで実行された NetFlow 処理に関連する情報をログに記録します。
アシュアランス PfR（Assurance PfR）	このログモジュールは、PfRMonitoring プロセスに関連する情報をキャプチャする assurance_pfr.log ファイルを有効にします。
アシュアランス WirelessUser（Assurance WirelessUser）	このログモジュールは、WirelessUser ジョブを実行してユーザーデータを読み取り、そのデータを WIRELESS_ASSURANCE トリガーによって追加さ

ログモジュール	説明
	れたメモリキャッシュに挿入したときの情報をキャプチャする assurance_wirelessuser.log ファイルを有効にします。
アシュアランス WSA（Assurance WSA）	このログモジュールは、WLC がデバイスから へのデータを処理している間に情報をキャプチャする wsa_collector.log、access_log、assurance_wsa.log、および error_log の各ファイルを有効にします。ログは、ワイヤレスコントローラのデータ収集の一環として生成されます。
AVC ユーティリティ（AVC Utilities）	このログモジュールは、aems_avc_utils.log ファイルを有効にします。AVC設定機能に固有のユーティリティフローのログは、このコンポーネントの一部として生成されます。
CIDS デバイスのログ（CIDS Device Logs）	このログモジュールは、XDEに移行されないデバイスのデバイスパック操作に関連する情報をキャプチャします。
回線/VCトレース	このログモジュールは、nms-multilayer.log ファイルを有効にします。
cluster_core	このログモジュールは、cluster.core.log ファイルを有効にします。
収集（Collection）	このログモジュールは、デバイスの準備状況を確認するために起動されるダッシュレットの情報をキャプチャします。
共通ヘルパー（Common Helper）	このログモジュールは、XMP共通の関連情報をキャプチャします。
コンプライアンス	このログモジュールは、ifm_compliance.log ファイルを有効にします。
設定（Configuration）	このログモジュールは、CLI、複合、MBC などのテンプレートがデバイスに展開されている場合に、ifm_config.log ファイルを有効にします。サービスビジネスロジックの実行デバッグログがキャプチャされます。
設定アーカイブ（Configuration Archive）	このログモジュールは、ifm_config_archive.log ファイルと ifm_config_archive_core.log ファイルを有効にします。ログはGUIで選択されたログレベルに基づいてキャプチャされ、設定アーカイブの収集、設定

ログモジュール	説明
	アーカイブの上書き、設定アーカイブのロールバック、設定アーカイブの展開など、設定アーカイブモジュールがサポートするすべての動作に対してログが記録されます。
設定アーカイブコア（Configuration Archive Core）	このログモジュールは、設定アーカイブの収集、設定アーカイブの上書き、設定アーカイブのロールバック、設定アーカイブの展開のような操作の実行中にサービスレイヤとデバイスパック間でのやり取りでの情報をキャプチャする ifm_config_archive_core.log ファイルを有効にします。
設定テンプレート（Configuration Templates）	このログモジュールは、ifm_config.log ファイルと ifm_template.log ファイルを有効にします。これらのファイルは、システムテンプレート、カスタム CLI テンプレート、複合テンプレート、または機能テンプレートがデバイスにデプロイされ、デプロイジョブが作成されたときにログに記録されます。GUI で選択したログレベル（INFO、DEBUG、TRACE）に基づいてログがキャプチャされ、デバイスに展開された設定テンプレートに対してログが記録されます。
コンテナ管理（Container Management）	このログモジュールは、ifm_container.log ファイルのログを有効にします。このファイルは、コンテナ管理が仮想アプライアンスのライフサイクル操作（インストール、アクティブ化、アンインストール、および非アクティブ化）を実行するときにログに記録されます。
Config	このログモジュールは、ノードレベルの設定、テンプレートの展開、サービスのプロビジョニングなどで構成される config.log を有効にします。
クレデンシャル管理（Credential Management）	このログモジュールは、NMS_SysOut.log ファイルからのログを有効にします。
クレデンシャルプロファイル（Credential Profile）	このログモジュールは、プロファイルの作成、削除、およびプロファイル更新の情報をキャプチャする ifm_credential_profile.log ファイルを有効にします。
DA	このログモジュールは、ifm_da.log ファイルと da_daemon.log ファイルを有効にし、SNMP ポーリン

ログモジュール	説明
	グ、NAM ポーリング、パケットキャプチャのワークフローなどの情報をキャプチャします。
データベース（Database）	このログモジュールは、rman.log ファイルと db_migration.log ファイルを有効にします。
データセンター（Data center）	このログモジュールは、datacenterevent.log ファイルと ifm_datacenter.log ファイルを有効にします。デバイス（検索ソース、UCS、Nexus）の追加、編集、および削除すると同時に、これらのファイルにはデバッグ情報が含まれています。また、インベントリモジュールのログには、データセンターのデバイスに関するデバッグ情報も含まれています。
デバイス クレデンシャルの検証（Device Credential Verification）	このログモジュールは、XDE.log ファイルを有効にします。
検出（Discovery）	このログモジュールは、ディスカバリ設定またはディスカバリジョブの作成、編集、および削除とディスカバリジョブの実行中にログをキャプチャする ifm_discovery.log ファイルと existenceDiscovery.log ファイルを有効にします。
分散キャッシュ	このログモジュールは、distributed-cache.log ファイルを有効にします。
DSM	このログモジュールは、仮想インベントリ ディスカバリ ソース マネージャに関連する情報をキャプチャします。
ems_assurance	このログモジュールは、ems-assurance.log ファイルを有効にします。
epnm_lcm	このログモジュールは、Life Cycle Manager（LCM）コンポーネントで使用される epnm-lcm.log ファイルを有効にします。
epnm_mcn	このログモジュールは、Model Changes Notifier（MCN）コンポーネントで使用される epnm-mcn.log ファイルを有効にします。
epnm_remote	このログモジュールは、epnm-remote.log ファイルを有効にします。
イベント処理	このログモジュールは、assurance_fault_error.log ファイルと assurance_fault.log ファイルを有効にします。

ログモジュール	説明
障害管理（Fault Management）	このログモジュールは、ifm_fault.log、xmp_correlation.log、および xmp_syslog.log の各ファイルを有効にします。
障害（Fault）	このログモジュールは、ifm_fault.log、xmp_correlation.log、および xmp_syslog.log の各ファイルを有効にします。
ファイアウォールと AVC の設定（Firewall and AVC Configuration）	このログモジュールは、AVC、ZBFW、QoS、およびNAT設定の詳細をキャプチャする aems_config.log ファイルを有効にします。
ファイアウォールと AVC のインベントリ（Firewall and AVC Inventory）	このログモジュールは、AVC、ZBFW、QoS、およびNAT の設定を読み取ったデバイスインベントリ時間をキャプチャする aems_zbfw_ice_post_processors.log ファイルを有効にします。
ファイアウォールと AVC の REST API（Firewall and AVC REST API）	このモジュールは、AVC、ZBFW、QoS、NAT、およびPPM の機能の REST API コールの詳細をキャプチャする aems_config_access_layer.log ファイルを有効にします。
ファイアウォールとAVCのユーティリティ（Firewall and AVC Utilities）	このログモジュールは、AVC/ZBFW/QoS、NAT、およびPPM の機能で共通のユーティリティコールをキャプチャする aems_utils.log ファイルを有効にします。
ファイアウォールのユーティリティ（Firewall Utilities）	このログモジュールは、ZBFW ユーティリティコールをキャプチャする aems_zbfw_utils.log ファイルを有効にします。
一般	このログモジュールは、ifm_common.log ファイルを有効にします。
Geo サーバ	このログモジュールは、nms-geoserver.log ファイルを有効にします。
グループ化（Grouping）	このログモジュールは、ifm_grouping.log ファイルと grouping-spring.log ファイルを有効にします。グループの追加、編集、削除、ならびにメンバーの追加および削除の間にデータをキャプチャします。また、CSV形式でグループをインポートまたはエクスポートしたり、ポートグループの作成、編集、およびポートグループの削除のときにもログをキャプチャします。

ログモジュール	説明
gui	このログモジュールは、xmp-wap.log ファイルを有効にします。
IFMCommon	このログモジュールは、ifm_common.log ファイルと ifm_common_helper.log ファイルを有効にします。
インベントリ（Inventory）	このログモジュールは、inventory.log、ifm_inventory.log、existenceInventory.log、および xde.log の各ファイルを有効にします。デバイスを追加、編集、および削除し、インベントリ収集を実行しているときに、データをキャプチャします。
キー証明書の管理	このログモジュールは、key_admin_web.log ファイルを有効にします。
MBC UI フレームワーク	このログモジュールは、mbcui_fw.log ファイルを有効にします。
モビリティ（Mobility）	このログモジュールは、サーバーに追加されたモビリティアンカーデバイスに関連する情報をキャプチャします。
モニター（Monitor）	このログモジュールは、上位 N のメモリと上位 N の CPU などのモニターダッシュレットの起動中に表示される API に関連する情報をキャプチャします。
MSAP	このログモジュールは、ncs.log ファイルを有効にします。これは、プロキシ設定や BBX 設定などの MSE ハイアベイラビリティのアクションに関連するデータをキャプチャします。
MSE	このログモジュールは、ncs.log ファイルを有効にします。MSE の追加、編集、および削除と、SiteMap と MSE の同期などのモビリティサービスエンジンに関連するデータをキャプチャします。
NBIFW	このログモジュールでは、NBI API フレームワークのログレベルを変更できます。この情報は、xmpNbiFw.log ファイルに表示できます。
ncs_nbi	このログモジュールでは、統計情報 NBI サービスのログレベルを変更できます。ncs_nbi.log ファイルで情報を閲覧することができます。

ログモジュール	説明
ネットワークテクノロジーオーバーレイ	このログモジュールは、technology-overlay.log ファイルと synce-technology-overlay.log ファイルを有効にします。
ネットワーク テクノロジー オーバーレイ プロバイダー	このログモジュールは、technology-overlay.log ファイルを有効にします。
ネットワーク トポロジ（Network Topology）	このログモジュールは、nms-topology.log ファイルおよびxmptopology.log ファイルを有効にします。このログモジュールは、[マップ（Maps）]>[ネットワークトポロジ（Network Topology）] ページに関連するログをキャプチャします。デバイス間のリンクの追加や削除などの情報がキャプチャされます。
NFVOS	このログモジュールは、esa dna 統合プロセスを追跡するために使用されます。
ナイス値（Nice）	このログモジュールは、デバイスを追加した後に、トポロジ関連の情報をキャプチャします。
NMS アシュアランス永続性ロガー	このログモジュールは、nms-assurance-persistence.log ファイルを有効にします。
NMS 共通トレース	このログモジュールは、nms-common.log ファイルを有効にします。
nms_assurance	このログモジュールは、nms-assurance.log ファイルを有効にします。
通知（Notifications）	このログモジュールは、ncs-0-0.log、ncs_nb.log、および alarm_notification_policy.log の各ファイルからの情報をキャプチャします。
Optical	このログモジュールは、nms-optical.log、nms-optical-fault.log、 nms-optical-event.log、および nms-optical-cerberus.log ファイルを有効にします。
PA	このログモジュールは、ifm_sam.log ファイルと sam_daemon.log ファイルを有効にします。アプリケーションやサービスなどの情報、ダッシュボードやダッシュレットサービスの API コール、NAM 設定、NAM ポーリング、およびパケットキャプチャ機能のワークフローがキャプチャされます。
参加回線サービス	このログモジュールは、nms-paticipating-circuit.log ファイルを有効にします。

ログモジュール	説明
Ping	このログモジュールは、ネットワークデバイスのポーリング間隔ジョブに関連する情報をキャプチャします。ジョブが完了すると、システム内の各デバイスは ping を受信します。
PKI	このログモジュールは、pki.log ファイルを有効にします。
プラグ アンド プレイ（Plug and Play）	このモジュールを有効にすると、PNP プロファイルの作成およびプロビジョニング、ブートストラップの初期設定、APIC EM の同期のタイムフレームに関連する情報をキャプチャできます。これらのログは、ifm_pnp.log ファイルと ifm_apic.log ファイルにキャプチャされます。
pnpgateway	このログモジュールは、pnp_gateway_cns.log、pnp_gateway_image.log、および pnp_gateway.log ファイルを有効にします。
プロトコルパック管理（Protocol Pack Management）	このモジュールは、aems_ppm_service.log、ifm_container.log、jobManager.log、および ifm_jobscheduler.log の各ファイルを有効にします。これにより、プロトコルパックのインポート、プロトコルパックの配布、およびジョブの詳細に関連する情報がログに記録されます。
QoS	クラスマップやポリシーマップなどの QoS ポリシーの作成、デバイスへの展開、インターフェイスとの関連付けまたは関連付け解除が行われると、このログモジュールは qos_config.log ファイルを有効にします。
レポート（Reports）	このモジュールを有効にすると、レポートに関連するクエリ、メモリ消費量、およびレポート生成のタイムフレームを表示できます。
REST サービス	このログモジュールは、nms-rest-service.log ファイルを有効にします。
RTTS	このログモジュールは、ifm_RTTS.log ファイルを有効にします。
サービス ディスカバリ	このログモジュールは、サービスで使用される nms-service-discovery.log ファイルと nms-service-discovery-distributed.log ファイルを有効にします。

ログモジュール	説明
サービス履歴	このログモジュールは、nms-service-history.log ファイルを有効にします。
サービスへの影響の分析	このログモジュールは、障害が発生したサービス影響分析機能で使用される sia.log ファイルを有効にします。
サービスマルチレイヤ	このログモジュールは、nms-service-multilayer.log ファイルを有効にします。
サービスプロビジョニング UI	このログモジュールは、provisioning-ui.log ファイルを有効にします。
スマートライセンス（Smart Licensing）	このログモジュールは、ifm_smartagent.log ファイルと smart_call_home.log ファイルを有効にします。ifm_smartagent.log ファイルにはスマートライセンシングに関連するライセンスのログが含まれており、smart_call_home.log にはCSSM（Cisco Smart Software Manager）に送信された情報をキャプチャする Call Home のログが含まれています。これらのログは、定期的なイベントとユーザーアクションベースのイベントでキャプチャされます。
SNMP	このログモジュールは、snmp.log ファイルと mibLibrary.log ファイルを有効にします。
特定の	このログモジュールは、ifm_app.log ファイルを有効にします。
SWIM	このモジュールを有効にすると、ifm_swim.log ファイルにソフトウェアイメージ管理モジュールのログを記録できます。これらのログは、GUI で選択されているログレベルに従ってキャプチャされます。ソフトウェアイメージの推奨事項、ソフトウェアイメージのアップグレード分析、ソフトウェアイメージのインポート、ソフトウェアイメージのアクティブ化、およびソフトウェアイメージのコミットのようなソフトウェアイメージの管理操作に関連する情報をログに記録します。
システム（System）	このログモジュールは、jobManager.log、lockManager.log、preference.log、grouping-spring.log、updates.log、poller.log、xmptopology.log、audit.log、connmanager.log、dpl_rest.log、datacenterevent.log、xmp-syslog.log、および webcontainer_filters.log ファイルを有効にします。

ログモジュール	説明
システムモニタリング（System Monitoring）	このログモジュールは、ifm_sysmon.log ファイルを有効にします。これにより、ルールの開始時刻および終了時刻とともに、その間に実行された操作に関する情報がログに記録されます。
テクノロジーコレクション	このログモジュールは、technology_collection.log ファイルを有効にします。
ThreadManager	このログモジュールは、hybernate 関連情報をキャプチャする xmp _threadmanager.log ファイルを有効にします。
しきい値（Threshold）	このモジュールを有効にすると、しきい値モニターによって処理されるイベントの詳細を表示できます。
TrustSec	このモジュールを有効にすると、TrustSec 準備状況デバイス、適用可能なデバイス、デバイス分類、および対応デバイスの情報をキャプチャできます。このリストは、サービス TrustSec の準備状況で表示されます。ログは ifm_trustsec.log ファイルに表示できます。
WLAN AVC 設定（WLAN AVC Configuration）	このログモジュールは、aems_config_wlan.log ファイルを有効にして、WLAN設定のワークフロー関連情報を表示します。
XDE	このログモジュールは、xde.log ファイルを有効にします。
XMLMED	このモジュールを有効にすると、SOAP 要求と応答をキャプチャできます。これらのログは、ncs.log ファイルにも表示できます。

ステップ 4 [メッセージ レベル（Message Level）] ドロップダウンリストから [トレース（Trace）] を選択します。

ステップ 5 詳細情報をログに記録するため、システムで問題を再現します。

ステップ 6 [ログ ファイルのダウンロード（Download Log File）] エリアで、[ダウンロード（Download）] をクリックします。ダウンロード zip ファイルの名前は次のようになります。

NCS-*hostname*-logs-*yy-mm-dd-hh-mm-ss*。

このファイルには、zip ファイルに含まれているすべてのファイルをリストした HTML ファイルがあります。

ifm_da.log ファイルと ifm_sam.log ファイルでキャプチャされた情報は、付属するクラスに分割されるようになりました。

- assurance_wirelessuser.log
- assurance_pfr.log
- assurance_netflow.log
- assurance_appclassifier.log

ifm_da.log ファイルには、 に Netflow デバイスが追加された後、デバイスとそれぞれの pcap に関連する情報が記録されます。assurance_wirelessuser.log ファイルには、WirelessUser ジョブを実行し、ユーザー データを読み取って WIRELESS_ASSURANCE によって追加されたメモリ キャッシュに格納する際に取得した情報が記録されます。assurance_pfr.log ファイルには、PfR モニタリング関連の情報が格納されます。assurance_netflow.log ファイルには、さまざまな Netflow デバイスから に送信された着信 Netflow データの処理が記録されます。assurance_appclassifier.log ファイルには、着信 AVC/ワイヤレス NetFlow データでの NBAR 分類に関するログが格納されます。

ステップ 7 [電子メールでログ ファイルを送信（E-Mail Log File）] エリアで、電子メール ID をカンマで区切ったリストを入力します。

ステップ 8 [メッセージ レベル（Message Level）] ドロップダウンリストで元の設定に戻します。

Syslog としてのシステム監査ログの転送

始める前に

Syslog としてシステム監査ログを転送するには、ユーザーが監査の変更通知を有効化して syslog レシーバを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** の順に選択してから、**[Syslog]** タブを選択し、**[Syslog ロギングオプション（Syslog Logging Options）]** を表示します。

ステップ 2 システム ログの収集および処理を有効にするために、[Syslog の有効化（Enable Syslog）] チェックボックスをオンにします。

ステップ 3 [Syslog ホスト（Syslog Host）] フィールドに、メッセージ送信先の宛先サーバーの IP アドレスを入力します。

ステップ 4 [Syslog ファシリティ（Syslog Facility）] ドロップダウン リストから、8 つのローカル用途のファシリティのうち、Syslog メッセージを送信するために使用するファシリティを選択します。このローカル用途のファシリティは予約されておらず、一般的な用途で使用可能です。

ステップ 5 **[保存 (Save)]** をクリックします。

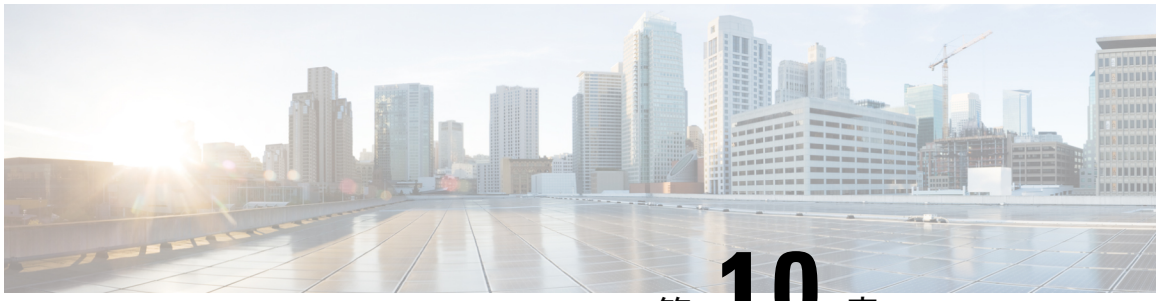
（注） 管理 CLI を使用してリモートサーバーへのシステムログ転送を有効にすると、ログは ade.log ファイルに登録されません。

SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整

SNMP トレースを有効にし、SNMP によって送受信されるパケットに関する詳細情報にアクセスします。これは、トラップのドロップ時など、トラブルシューティングの際に必要になることがあります。

次の変更を行うには、**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** を選択してから、**[SNMP ログ（SNMP Log）]** タブを選択します。

目的	次の手順を実行します。
特定のデバイスでの SNMP トレースの有効化	[SNMP ログ設定（SNMP Log Settings）] 領域で、次のようにします。 **1.** [SNMP トレースの有効化（Enable SNMP Trace）] チェックボックスと [値の表示（Display Values）] チェックボックスをオンにします。 **2.** トレースするデバイスの IP アドレスまたは DNS アドレス、あるいはその両方を入力し、[保存（Save）] をクリックします。
ログのサイズと保存されるログ番号の変更	[SNMP ログ ファイル設定（SNMP Log File Settings）] 領域で、次のようにします。 （注） これらの設定を変更するときは、（非常に多くのデータを保存するなどして）システムパフォーマンスに影響を与えないように注意してください。 **1.** ファイルの最大数とファイル サイズを調整します。 **2.** を再起動して、変更内容を有効にします。の停止と再起動（114 ページ）を参照してください。



第 10 章

コントローラと AP の設定を構成する

CLI セッションのプロトコル設定

多くの Prime Infrastructure のワイヤレス機能（自律アクセス ポイントおよびコントローラのコマンドライン インターフェイス（CLI）テンプレートや移行テンプレートなど）では、自律アクセス ポイントまたはコントローラに対して CLI コマンドを実行する必要があります。これらの CLI コマンドを入力するには、Telnet または SSH セッションを確立します。CLI セッション ページでは、セッション プロトコルを選択できます。

CLI テンプレートでは、質問に対する回答操作（コマンドに対して「はい（Yes）」または「いいえ（No）」で回答する、*Enter* キーを押して続行する、など）は不要です。これは Prime Infrastructure によって自動的に実行されます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [CLI セッション（CLI Session）]** の順に選択します。

ステップ 2 [コントローラ セッション プロトコル（Controller Session Protocol）] を選択します。[SSH] または [Telnet] を選択できます（[SSH] がデフォルト）。

ステップ 3 [Autonomous AP Session Protocol] を選択します。[SSH] または [Telnet] を選択できます（[SSH] がデフォルト）。

ステップ 4 デフォルトでは、[Run Autonomous AP Migration Analysis on discovery] オプション ボタンは [No] に設定されています。Autonomous AP を検出し、移行分析を実行する場合は、[Yes] を選択します。

ステップ 5 [Save] をクリックします。

Prime Infrastructure での Unified AP ping 到達可能性設定の有効化

Cisco Prime Infrastructure で Unified AP が検出されるたびに、Prime Infrastructure はその AP が ping に対応するかどうかを判別し、それに応じて Prime Infrastructure データベース内の ping 対応ステータスを更新します。

次の条件に応じて、さまざまなアラームが起動されます。

- Unified AP が関連付け解除された場合、その AP が FlexConnect モードであれば、Prime Infrastructure は AP に到達可能であるかどうかをチェックします。AP が ping に対応し、ping で到達可能である場合、Prime Infrastructure は低シビラティ（重大度）のアラームを起動します。AP が ping に対応しない場合、または ping で到達可能でない場合は、高シビラティ（重大度）のアラームを起動します。
- Unified AP が関連付け解除された場合、その AP が FlexConnect モードでなければ、Prime Infrastructure は高シビラティ（重大度）のアラームを起動します。

デフォルトでは、Unified AP の ping 到達可能性機能は、Prime Infrastructure バージョン 3.3 以降で有効です。ただし、3.2 以前のバージョンでは無効です。有効にするには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [Unified AP ping 到達可能性（Unified AP Ping Reachability）]** の順に選択します。

ステップ 2 [PrimeがAPの到達可能性を取得できるようにする（Allow Prime to learn about AP Reachability）] オプション ボタンを選択して、Cisco Prime Infrastructure が AP の到達可能性を取得できるようにします。これにより、バックグラウンド タスクがトリガーされ、各アクセス ポイントに対して ping が実行されて、その結果が Prime Infrastructure データベースに保存されます。

ステップ 3 ユーザーには、ping 到達可能性を取得するためにバックグラウンド ジョブがトリガーされることを伝えるアラートでプロンプトが出されます。[OK] をクリックして、先へ進みます。

AP の到達可能性を取得するために、Prime Infrastructure 内でバックグラウンド ジョブがトリガーされて、関連付けられているすべての API に対して実行されます。新しいジョブは、[ジョブ ダッシュボード（Job Dashboard）] で次の情報を使用して作成します。

ステップ 4 [Prime からすべてのアクセス ポイントに ping で到達可能（All access points are ping reachable from Prime）] オプション ボタンを選択すると、管理者はすべての Unified AP を ping 対応としてマークします。

ステップ 5 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [システム ジョブ（System Jobs）] > [ステータス（Status）]** を選択し、ジョブのステータスを表示します。

ステップ 6 ジョブの詳細を検索するには、[クイック フィルタ（Quick Filter）] オプションを使用して、[名前（Name）] 検索フィールドに **[Unified AP ping 機能の詳細（Learn Unified AP Ping Capability）]** を入力します。

結果は [ステータス（Status）] テーブルに表示されます。このテーブルには、次の情報が表示されます。

- ジョブ タイプ（**Job Type**）
- **Status**（ステータス）
- 最終実行ステータス（**Last Run Status**）
- 前回の開始時間（**Last Start Time**）
- デュレーション（**Duration**）
- 次回の開始時間（**Next Start Time**）
- 詳細を表示するには、[AP ping 到達可能性の詳細（Learn AP Ping Reachability）] リンクをクリックします。[AP ping 到達可能性の詳細（Learn AP Ping Reachability）] ページに、次の情報が表示されます。すべてのジョブ インスタンスの詳細を表示するには、[すべて表示（Show All）] をクリックします。
  - 定例（**Recurrence**）
  - インターバル（**Interval**
  - 実行 ID（**Run ID**）
  - **Status**（ステータス）
  - デュレーション（**Duration**）
  - 開始時刻（**Start Time**）
  - 完了時刻（**Completion Time**）

アップグレード後のコントローラの更新

[コントローラ アップグレード（Controller Upgrade）] ページでは、コントローラのアップグレード後に自動更新を行って、コントローライメージに変更があるたびに自動的に設定を復元することができます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [コントローラ アップグレード（Controller Upgrade）]** の順に選択します。

ステップ 2 [アップグレード後の自動更新（Auto refresh After Upgrade）] チェックボックスをオンにすると、コントローラのイメージに変更があるたびに設定は自動的に復元されます。

ステップ 3 [Save Config トラップで同期（Sync on Save Config Trap）] チェックボックスをオンにすると、Prime Infrastructure が Save Config トラップを受信するとコントローラで同期がトリガーされます。このチェックボックスをオンにすると、次のいずれかのオプションを選択できます。

- Prime Infrastructure データベースに設定を保持（Retain the configuration in the Prime Infrastructure database）
- [コントローラ上の現在の設定を使用（Use the configuration on the controller currently）]

ステップ 4 [Save] をクリックします。

不正 AP に接続したスイッチ ポートの追跡

は、不正なアクセス ポイントが接続されているネットワーク スイッチ ポートを自動的に識別できます。この機能は自動スイッチ ポート トレーシングに基づくものであり、その動作には Prime Infrastructure のフル ライセンスが要求されることに注意してください。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）]** の順に選択します。[自動 SPT（Auto SPT）] ページが表示されます。

ステップ 2 [自動スイッチ ポート トレースの有効化（Enable Auto Switch Port Tracing）] チェックボックスをオンにして、Prime Infrastructure が不正アクセス ポイントの接続先スイッチ ポートを自動的にトレースできるようにします。次に、以下を含む自動ポート トレース用のパラメータを指定します。

- 不正 API とポート間のトレースを実行する間隔（分）
- 有線で検出された不正 AP をトレースするかどうか
- 含めるシビラティ（重大度）（重大、メジャー、マイナー）

ステップ 3 [自動封じ込みの有効化（Enable Auto Containment）] チェックボックスをオンにして、Prime Infrastructure がシビラティ（重大度）に応じて自動的に不正 AP を封じ込めるようにします。次に、自動封じ込み用の以下のパラメータを指定します。

- ポート トレースによって有線で検出された不正 AP を除外するかどうか
- 封じ込み対象に含めるシビラティ（重大度）（重大、メジャー）
- 封じ込みレベル（最大 4 つの AP）

ステップ 4 [OK] をクリックします。

スイッチ ポート トレースを設定する

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方式では、Prime Infrastructure がコントローラから受信した情報を収集します。この機能拡張により、検出された不正アクセス ポイントに対応し、今後発生する攻撃を回避できま

す。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続しているスイッチ ポートを追跡します。危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

スイッチ ポート トレーシングで、v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。[Switch Port Trace] ページでは、回線上で検出された不正アクセス ポイントに対するトレースを実行できます。

適切にトレースして不正アクセス ポイントを封じ込めるには、以下の情報を正しく指定する必要があります。

- レポート AP：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- AP CDP ネイバー：シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル：トレース対象のすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。個々のスイッチだけを追加するのではなく、ネットワーク アドレスをベースに項目を追加できます。正しい write コミュニティ ストリングを指定して、スイッチ ポートを有効または無効にする必要があります。トレーシングの場合は、read コミュニティ ストリングで十分です。/32 サブネット マスクを使用したネットワーク アドレスは、グローバル SNMP クレデンシャルの設定ではサポートされていません。詳細なガイダンス情報については、「関連項目」の「不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問」を参照してください。
- スイッチ ポートの設定：トランキング スイッチ ポートを正しく設定する必要があります。スイッチのポート セキュリティを無効にする必要があります。
- スイッチ ポート トレーシングは、Cisco イーサネット スイッチおよび Catalyst スイッチ 2960、3560、3560-E、3750-E、3850、4500 シリーズのみでサポートされます。
- スイッチ VLAN 設定が適切に構成されている必要があります。Prime Infrastructure は、Cisco Discovery Protocol ネイバー情報を使用して、スイッチの IP アドレスを取得します。そのスイッチ内の VLAN 情報を使用して、スイッチの CAM テーブル エントリを読み取ります。スイッチ内の VLAN 情報が正しく設定されていないと、Prime Infrastructure は CAM テーブル エントリを読み取れません。したがって、スイッチの不正 AP をトレースすることができません。
- CDP プロトコルがすべてのスイッチ上で有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正なイーサネット スイッチ ポート情報を高い信頼性で検出する場合、不正アクセス ポイントとイーサネット スイッチ間のイーサネット MAC アドレスの差がおおむね 3 以上であれば、これらの間にトラフィックが存在するとみなします。

- 不正アクセス ポイントは、最大ホップ カウントの制限内でスイッチに接続される必要があります。
- SNMPv3 を選択している場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成します。

（注） ベンダー OUI の一致を効果的に使用して一致の誤検出を排除するには、スイッチ ポートにロケーション情報を設定しておく必要があります。設定されていないスイッチ ポートは、ロケーション別の削除の実行後も OUI の一致対象のままとなります。

関連トピック

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

SNMP クレデンシャルの設定

スイッチ ポート トレースの詳細を表示するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [ポート トレースのスイッチ（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）] の順に選択します。

ステップ 2 次の基本設定値を設定します。

- [MAC address +1/-1 search]：有効にするには、チェックボックスをオンにします。

この検索では、無線 MAC アドレスに 1 加算するか 1 減算することによって不正アクセス ポイントの有線側の MAC アドレスを得る、慣習的な MAC アドレス +1/-1 方式を使用します。

- [Rogue client MAC address search]：有効にするには、チェックボックスをオンにします。

不正クライアントが存在していると、検索可能な MAC アドレスのリストにクライアントの MAC アドレスが追加されます。

- [ベンダー（OUI）検索（Vendor (OUI) search）]：有効にするには、チェックボックスをオンにします。OUI は組織固有識別子の検索を意味し、MAC アドレスの先頭 3 バイトで検索します。
- [スイッチ トランク ポートの除外（Exclude switch trunk ports）]：スイッチ ポートのトレースからスイッチ トランク ポートを除外する場合に、このチェックボックスをオンにします。

（注） 特定の MAC アドレスについて複数ポートをトレースする場合は、精度を向上させるために、追加のチェックが実行されます。追加のチェックには、トランク ポートのチェック、ポート上にある AP でない CDP ネイバーのチェック、およびこの MAC アドレスがこのポート上の唯一のアドレスであるかどうかのチェックが含まれます。

- [デバイス リストの除外（Exclude device list）]：トレースから追加のデバイスを除外する場合に、このチェックボックスをオンにします。スイッチ ポート トレースから除外する各デバイスをデバイス リスト テキスト ボックスに入力します。各デバイス名をコンマで区切って入力してください。
- [最大ホップ数（Max hop count）]：このトレースに対するホップの最大数を入力します。ホップ カウントを大きくするほど、スイッチ ポート トレースの実行時間が長くなることに留意してください。

（注）　このホップ カウント値は自動 SPT に適用できません。

- [ベンダー リストの除外（Exclude vendor list）]：スイッチ ポート トレースから除外するすべてのベンダーをベンダー リスト テキスト ボックスに入力します。ベンダー名はカンマで区切ります。ベンダー リストでは、大文字と小文字が区別されません。

ステップ 3 次の詳細設定値を設定します。

- [不正 AP タスク最大スレッドのトレース（TraceRogueAP task max thread）]：スイッチ ポート トレーシングで、複数のスレッドを使用して不正アクセス ポイントをトレースします。このフィールドは、並列スレッドでトレースできる不正アクセス ポイントの最大数を示します。
- [不正 AP 最大キュー サイズのトレース（TraceRogueAP max queue size）]：スイッチ ポート トレーシングでは、キューを保持して、不正アクセス ポイントをトレースします。トレーシングする不正アクセス ポイントを選択すると、処理待ちのキューに入ります。このフィールドは、キューに保管できる項目の最大数を示します。
- [スイッチ タスク最大スレッド（SwitchTask max thread）]：スイッチ ポート トレーシングでは、複数のスレッドを使用して、スイッチ デバイスをクエリーします。このフィールドは、並列スレッドでクエリーできるスイッチ デバイスの最大数を示します。

これらのパラメータのデフォルト値は、通常の運用に適しています。これらのパラメータは、スイッチ ポート トレーシングと Prime Infrastructure のパフォーマンスに直接影響します。必要な場合を除き、これらのパラメータは変更しないことを推奨します。

- [CDP デバイス機能の選択（Select CDP device capabilities）]：有効にするには、チェックボックスをオンにします。

Prime Infrastructure では、トレーシング中にネイバーを検出するために CDP を使用します。ネイバーが検証されると、Prime Infrastructure では、[CDP 機能（CDP capabilities）] フィールドを使用して、ネイバー デバイスが有効なスイッチであるかどうかを判別します。ネイバー デバイスが有効なスイッチでない場合は、トレースされません。

ステップ 4 行った変更を保存するには [Save] をクリックします。ページを元の設定に戻すには、[Reset] をクリックします。出荷時の初期状態に設定を戻すには、[初期設定へのリセット（Factory Reset）] をクリックします。

スイッチポート トレースの詳細表示

スイッチ ポート トレースの詳細を表示するには、次の手順を実行します。

ステップ 1 [設定（Configure）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] ページを使用して、フル ライセンスを持つスイッチを追加します。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチポートトレース（SPT）（Switch Port Trace (SPT)）] > [自動 SPT（Auto SPT）] ページで自動スイッチポートトレースを有効にします。

ステップ 3 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] ページで、有線クライアント ステータス メジャー ポーリング バックグラウンド タスクを実行するようにスケジュール設定します。

ステップ 4 [不正 API の詳細（Rogue AP detail）] ページで、トレース スイッチ ポート アイコンをクリックします。新しいポップアップに、トレースされたスイッチ ポートの詳細が表示されます。詳細ステータスをクリックして、「起動済み/検出済み（started/Found）」などのトレース ステータスをチェックします。

（注） Prime Infrastructure にスイッチを追加しなくても、手動 SPT は機能します。しかし、[管理（Administration ）] > [設定（Settings ）] > [システム設定（System Settings）] > [ネットワークとデバイス（Network and Device）] > [スイッチポートトレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）] ページの SNMP クレデンシャルを正しく設定する必要があります。「プライベート」はデフォルトのクレデンシャルです。特に設定されていない場合、これが手動のスイッチポートトレース中に使用されます。

- [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークおよびデバイス（Network and Device）] の順に選択することによってスイッチが Prime Infrastructure に追加された場合、そのスイッチに対して入力された SNMP クレデンシャルは、ここで入力されたあらゆるスイッチ SNMP クレデンシャルより優先され、スイッチ ポート トレーシングに使用されます。[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークおよびデバイス（Network and Device）] ページで、スイッチの SNMP クレデンシャルを変更できます。Prime Infrastructure は、SPT を使用してスイッチを追加するためのライセンスを必要とせず、スイッチに接続された有線クライアントを表示しません。[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス グループ（Device Groups）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] ページには、SPT を使用して追加されたスイッチの詳細は表示されません。
- Prime Infrastructure には、スイッチを追加するためのフルライセンスが必要です。[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス グループ（Device Groups）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] ページには、フル ライセンスを使用して追加されたスイッチの詳細が表示されます。Prime Infrastructure には、スイッチに接続された有線クライアントも表示されます。スイッチの場所は MSE を使用して追跡されます。

スイッチ ポート トレーシングの確立

ステップ 1 [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] の順に選択します。

ステップ 2 [Malicious Rogue APs]、[Unclassified Rogue APs]、[Friendly Rogue APs]、[Custom Rogue APs]、および [Adhoc Rogues] ダッシュレットで、過去 1 時間または過去 24 時間に識別された不正 AP の数、またはアクティブ

な不正 AP の合計数を表す数値リンクをクリックします。[アラーム（Alarms）] ウィンドウが開き、不正の疑いがある AP に対してアラームが示されます。

ステップ 3 スイッチ ポート トラッキングをセットアップする対象の不正 AP の隣にあるチェックボックスをオンにして、その不正 AP を選択します。

ステップ 4 該当するアラームを展開し、アラーム詳細の [スイッチ ポート トレーシング（Switch Port Tracing）] サブセクションにある [スイッチ ポートのトレース（Trace Switch Port）] ボタンを手動で選択します。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正スイッチ ポートとして報告されます。

[スイッチ ポート トレースの詳細（Switch Port Tracing Details）] ダイアログボックスに関する追加情報については、スイッチ ポート トレースの詳細 （332 ページ）を参照してください。

不正 AP トレース用の SNMP クレデンシャルの設定

[SNMP クレデンシャル（SNMP Credentials）] ページでは、不正アクセス ポイントのトレースに使用するクレデンシャルを指定できます。番号ベースのエントリを使用しても特定のエントリを確認できない場合は、このオプションを使用します。スイッチ クレデンシャルが Cisco Prime Infrastructure に追加されていない場合は、このページの SNMP クレデンシャルを使用してスイッチに接続できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[ネットワークとデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [手動 SPT（Manual SPT）]** を選択します。[手動 SPT（Manual SPT）] ページが表示されます。

ステップ 2 現在の SNMP クレデンシャル エントリの詳細を表示または編集します。目的のエントリの [ネットワーク アドレス（Network Address）] リンクをクリックすることで操作できます。

この作業の詳細については、「関連項目」の「グローバル SNMP の設定」および「SNMP クレデンシャル詳細の表示」を参照してください。

デフォルト エントリは、ネットワーク 0.0.0.0 に対応します。これは、ネットワーク全体を意味します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。ネットワーク 0.0.0.0 に対して定義された SNMP クレデンシャルは、SNMP クレデンシャルのデフォルトです。これは、SNMP クレデンシャルが定義されていないときに使用されます。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 3 新しい SNMP エントリを追加するには、[コマンドの選択（Select a command）] > [SNMP エントリの追加（Add SNMP Entries）] > [実行（Go）] の順に選択します（「SNMP クレデンシャルの追加」を参照）。

関連トピック

グローバル SNMP の設定 （115 ページ）

SNMP クレデンシャルの詳細表示 （117 ページ）
SNMP クレデンシャルの追加 （118 ページ）

スイッチ ポート トレースの詳細

[スイッチ ポート トレースの詳細（Switch Port Tracing Details）] ダイアログボックスでは、スイッチ ポートの有効化および無効化、スイッチ ポートのトレース、およびアクセス ポイント スイッチ トレースの詳細ステータスの表示を行うことができます。

スイッチ ポート トレーシングの詳細については、以下の関連項目を参照してください。

[スイッチ ポート トレースの詳細（Switch Port tracing Details）] ダイアログボックスで、次のいずれかを実行します。

- [スイッチ ポートの有効化/無効化（Enable/Disable Switch Port(s)）] をクリック：選択した任意のポートを有効または無効にします。
- [スイッチ ポートのトレース（Trace Switch Port(s)）] をクリック：別のスイッチ ポート トレースを実行します。
- [詳細ステータスの表示（Show Detail Status）] をクリック：このアクセス ポイントのスイッチ ポート トレースに関する詳細を表示します。
- [閉じる（Close）] をクリックします。

関連トピック

スイッチ ポート トレースを設定する （326 ページ）
不正 AP トレース用の SNMP クレデンシャルの設定 （331 ページ）

スイッチ ポート トレースのトラブルシューティング

スイッチポートトレース（SPT）は、ベストエフォート方式で動作します。SPT では、適切にトレースして不正 AP を組み込むために、以下の情報を必要とします。

- レポート アクセス ポイント：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- アクセス ポイント CDP ネイバー：シード スイッチを判別するには、アクセス ポイント Cisco Discovery Protocol（CDP）ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル
  - トレースする必要のあるすべてのスイッチは管理IPアドレスを持つ必要があり、SNMP管理が有効にされている必要があります。
  - SNMPクレデンシャルが新しく変更される場合は、個々のスイッチをPrime Infrastructureに追加するのではなく、ネットワーク アドレスに基づき追加できます。
  - この新しい SNMP クレデンシャル機能は、read と write の両方についてデフォルトのコミュニティ ストリングを「private」とするデフォルトエントリ 0.0.0.0 を持ちます。
  - スイッチ ポートを有効または無効にするには、正しい write コミュニティ ストリングを指定する必要があります。トレーシングの場合には、read コミュニティ ストリングのみで十分です。

- スイッチ ポートの設定
  - トランキングされているスイッチ ポートは、トランク ポートとして正しく設定されている必要があります。
  - スイッチのポート セキュリティを無効にする必要があります。
- スイッチ ポート トレーシングは、Cisco イーサネット スイッチおよび Catalyst スイッチ 2960、3560、3560-E、3650、3750-E、3750-X、3850、4500 および 6500 シリーズのみでサポートされます。
- スイッチ VLAN 設定が適切に構成されている必要があります。
- すべてのスイッチについて CDP プロトコルが有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内で、スイッチに接続される必要があります。デフォルト ホップは 2 です。最大ホップは 10 です。
- SNMPv3 を使用する場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成してください。

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問

下記の「関連項目」では、Prime Infrastructure の不正 AP 検出およびスイッチ ポート トレーシング（SPT）に関するさまざまな質問の答えを提供しています。

関連トピック

自動 SPT の設定方法を教えてください （333 ページ）
自動 SPT と手動 SPT はどのように違いますか （334 ページ）
SPT の結果（手動および自動）はどこで確認できますか （335 ページ）
自動 SPT を円滑に実行するにはどうすればいいですか
自動 SPT の方が有線の不正の検出に時間がかかるのはなぜですか （335 ページ）
トランク ポート上の有線の不正を検出するにはどうすればいいですか （336 ページ）
自動 SPT の [ロケーション別の削除（Eliminate By Location）] 機能を使用するにはどうすればいいですか （338 ページ）
「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください（338 ページ）

自動 SPT の設定方法を教えてください

自動 SPT を設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network and Device] > [Network] を使用して、[License Level] が [Full] のスイッチを追加します。

ステップ 2 [Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Auto SPT] の順に選択し、[Enable Auto Switch Port Tracing] を選択します。[OK] をクリックします。

ステップ 3 [Administration] > [Settings] > [Background Tasks] > [Wired Client Status] の順に選択します。このタスクが有効化され、1 日に 2 回以上実行するようにスケジュール設定されていることを確認してください。

関連トピック

SPT の結果（手動および自動）はどこで確認できますか （335 ページ）
自動 SPT を円滑に実行するにはどうすればよいですか。
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

自動 SPT と手動 SPT はどのように違いますか

手動 SPT は、個別の不正 AP アラームに対して実行されます。不正 AP アラームの詳細ページで [Trace Switch Port] アイコンをクリックすることにより、この機能をトリガーする必要があります。

自動 SPT は、アラームのバッチに基づき、有線クライアント ステータス バックグラウンド タスクに対して定義されたスケジュールで自動的に実行されます。

手動 SPT のトリガーは、アクセス ポイントで有効化された CDP および適切な SNMP コミュニティ文字列を持つスイッチに依存する点に注意してください。手動 SPT およびその動作の詳細については、「関連項目」の「WCS Switch Port Trace Demonstration」リンクを参照してください。

自動および手動の SPT では、ライセンスおよびスイッチの「ライセンス レベル」の取り扱い方法にも違いがあります。スイッチの「ライセンス レベル」は、スイッチを追加する際に [Full] または [Switch Port Trace Only] のいずれかに設定できます。相違点を次の 3 つのケースで例示します。

- **「フル」ライセンス レベルのスイッチを追加する場合**：Prime Infrastructure は、追加されたフル ライセンス レベルのスイッチごとにライセンスを消費します。スイッチに接続されたすべての有線クライアントは、[モニター（Monitor）] > [管理対象デバイス（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）] の順に選択することで表示できます。また、MSE を使用してスイッチの場所を追跡することもできます。「フル」ライセンス レベルは、自動 STP の動作に必須です。
- **スイッチを追加しない場合**：スイッチを追加しなくても、手動 SPT は動作します。ただし、すべてのスイッチに対して SNMP クレデンシャルを適切に設定する必要があることに注意してください。設定には、[Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] を使用します。
- **「Switch Port Trace Only」ライセンス レベルのスイッチを追加する場合**：[Configuration] > [Network]> [Network Devices] > [Add Device] を使用してスイッチを Prime Infrastructure に追加し、[Switch Port Trace Only] ライセンス レベルを選択する場合、スイッチを追加する

ときに入力した SNMP クレデンシャルは、[Administration] > [Settings]> [System Settings] > [Network and Device] > [Switch Port Trace (SPT)] > [Manual SPT] を使用して入力された SNMP クレデンシャルより優先されます。入力した SNMP クレデンシャルは、スイッチ ポート トレーシングに使用されます。これが、スイッチを追加しない場合と、「スイッチ ポート トレース専用」のライセンス レベルのスイッチを追加する場合との主な違いです。Prime Infrastructure は、SPT 専用ライセンス レベルのスイッチに対してライセンスを消費せず、[モニター（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチとハブ（Switches and Hubs）] にこれらのスイッチは表示しません。また、これらのスイッチに接続された有線クライアントも表示しません。

詳細については、「WCS Switch Port Trace Demonstration」を参照してください。

関連トピック

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください（338 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

SPT の結果（手動および自動）はどこで確認できますか

ステップ 1 必要な不正 AP アラームの詳細を表示します。次に例を示します。

a) 任意の Prime Infrastructure ページの上部にある [Alarm Summary] アイコンをクリックします。アラーム カテゴリの一覧が表示されます。

b) リスト内の [不正 AP（Rogue AP）] リンクをクリックします。Prime Infrastructure が不正 AP アラームの一覧を表示します。

c) 詳細を表示する不正 AP アラームを展開します。そのアラームに関する詳細ページが表示されます。

ステップ 2 [Switch Port Tracing] ペインで、[Trace Switch Port] アイコンをクリックします。[Switch Port Trace] ウィンドウにトレースされたスイッチ ポートの詳細が表示されます。

SPT が実行されていない場合は、[Trace Switch Port(s)] をクリックしてトレースを開始します。[詳細ステータスの表示（Show Detail Status）] ボタンをクリックすると、進行中のトレースのステータスの詳細を取得できます。

関連トピック

不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

自動 SPT の方が有線の不正の検出に時間がかかるのはなぜですか

自動 SPT の方が手動 SPT より有線の不正の検出に比較的時間がかかる理由は、以下のとおりです。

1. 自動 SPTは、有線クライアント検出プロセスに依存しており、このプロセスは有線クライアント ステータス メジャー ポーリング バックグラウンド タスクが実行されているときだけに起動されます。デフォルトでは、このバックグラウンド タスクのメジャー ポーリン

グは、2 つのマイナー ポーリングごと、または 4 時間ごとのみに実行されるようにスケジュール設定されています。

2. 有線の不正 AP はスイッチに接続されますが、有線の不正 AP の状態が「関連付け状態」の場合、Prime Infrastructure は有線ポートのみを検出します。Prime Infrastructure は、有線クライアントのステータスが関連付け状態か関連付け解除状態かを常に確認しています。有線クライアントのステータスが関連付け解除状態の場合、Prime Infrastructure はこれをポート未接続として表示します。
3. 不正トレーシングはバッチで実行されます。特定の有線の不正検出に要する時間は、Prime Infrastructure が処理するバッチによって異なります。特定の不正が前回のバッチで処理されていた場合、そのトレースにはさらに時間がかかります。
4. 任意の有線の不正検出に要する時間は、Prime Infrastructure に存在する不正アラームの数と、有線クライアント ステータス メジャー ポーリングの間隔よって異なります。

関連トピック

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください（338 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問（333 ページ）

トランク ポート上の有線の不正を検出するにはどうすればいいですか

トランク ポート上の有線の不正は、次の手順で検出できます。

ただし、Cisco 2950 スイッチのトランク ポート上の不正を検出する場合は、先に Prime Infrastructure Device Pack 5.0 に含まれるアップデート版の 2950 サポートをインストールする必要があります。

ステップ 1 [管理（Administration）] > [設定（Settings）]> [システム設定（System Settings）] > [ネットワークおよびデバイス（Network and Device）] > [スイッチ ポート トレース（SPT）（Switch Port Trace (SPT)）] > [SPT 設定（SPT Configuration）] の順に選択します。

ステップ 2 [Exclude switch trunk ports] チェック ボックスをオフにして、[Save] をクリックします。

ステップ 3 [Administration] > [Settings] > [System Settings] > [Client and User] > [Client] の順に選択します。

ステップ 4 [Discover wired clients on trunk ports] チェック ボックスをオンにして、[Save] をクリックします。

スイッチは、有線クライアント ステータス バックグラウンド タスクによるメジャー ポーリングの次回実行時から、トランク ポート上の有線クライアントの検出を開始します。

関連トピック

自動 SPT の設定方法を教えてください（333 ページ）
「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください（338 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問（333 ページ）

どのようにスイッチ ポートの場所を設定しますか。

スイッチ ポートの場所を設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

ステップ 2 デバイス名をクリックします。デフォルトでは、[設定（Configuration）] タブが開きます。

ステップ 3 右上隅の [スイッチ ポートの場所（Switch Port Location）] をクリックします。

ステップ 4 場所を設定するポートを 1 つ以上選択し、ドロップダウン リストから [場所の設定（Configure Location）] を選択して [実行（Go）] をクリックします。

ステップ 5 [マップ ロケーション（Map Location）] グループで、次のように設定します。

- [キャンパス/サイト（Campus/Site）] ドロップダウン リストから、スイッチまたはスイッチ ポートのキャンパス マップを選択します。
- [建物（Building）] ドロップダウン リストから、スイッチまたはスイッチ ポートの建物マップ ロケーションを選択します。
- [フロア（Floor）] ドロップダウン リストから、フロア マップを選択します。
- [キャンパス/サイト（Campus/Site）]、[建物（Building）]、[フロア（Floor）] の詳細が設定されたファイルをすでに保存している場合は、[シビックのインポート（Import Civic）] をクリックします。これにより、Prime Infrastructure を使用して MSE のシビック情報がインポートされます。テキスト ファイル名を入力するか、ファイル名を参照して、[インポート（Import）] をクリックします。

ステップ 6 [ELIN とシビック ロケーション（ELIN and Civic Location）] グループ ボックスで、次のように設定できます。

- [ELIN] テキスト ボックスに緊急ロケーション ID 番号（ELIN）を入力します。ELIN は、自動ロケーション情報（ALI）データベースとも呼ばれるマスター データベースで発信者の地理的な位置を調べるために、公安応答局（PSAP）で使用される番号です。また、ELIN により、PSAP は、電話の接続が切断された場合、緊急の発信者に直接連絡することもできます。
- [住所（Civic Address）] および [詳細（Advanced）] タブの必須フィールドを入力します。
- ファイル内に ELIN およびシビック ロケーション情報が保存されている場合、[スイッチ ロケーションのインポート（Import Switch Location）] をクリックするとインポートできます。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

自動 SPT を円滑に実行するにはどうすればいいですか。
自動 SPT の設定方法を教えてください （333 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

自動 SPT の [ロケーション別の削除（Eliminate By Location）] 機能を使用するにはどうすればいいですか

[ロケーション別の削除（Eliminate By Location）] は、Prime Infrastructure が有線の不正を検出するために使用するアルゴリズムの 1 つです。このアルゴリズムでは、不正 AP の場所情報を使用して、関連付け状態のスイッチ ポートを検索します。このアルゴリズムは、検出 AP のフロア ID を使用した自動 SPT 処理中の誤検出削減に役立ち、有線の不正の追跡精度を向上させます。

「ロケーション別の削除（Eliminate by location）」を有効にすると、有線クライアント ステータス バックグラウンド タスクによって、管理スイッチのすべての有線クライアントが検出されます。次回の自動 SPT の実行時、「ロケーション別の削除（eliminate by location）」アルゴリズムに基づいてスイッチ ポートがフィルタリングされます。

「Eliminate by location」を有効にするには、次の手順を実行してください。

ステップ 1 Cisco Mobility Service Engine（MSE）を Prime Infrastructure と統合します。

ステップ 2 検出 AP が配置されたフロア定義領域と MSE が同期していることを確認します。MSE が不正を追跡できるはずです。

ステップ 3 すべてのスイッチを Prime Infrastructure に追加します。

ステップ 4 すべてのスイッチが PI に追加されており、管理対象状態にある場合は、使用するアルゴリズムのスイッチ ポートをすべて設定する必要があります。スイッチ ポートのすべてのスイッチが設定されていない場合、誤検出結果が生成されます。[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] から [デバイス名（Device Name）] をクリックし、右上隅で [スイッチ ポートの場所（Switch Port Location）] をクリックして設定できます。

ステップ 5 マップに検出アクセス ポイントをマッピングしてから、Cisco MSE が同期され、不正 AP がフロアで検出されることを確認します。

[ロケーション別の削除（Eliminate By Location）] アルゴリズムは、検出 AP のフロア ID を取得し、他のすべての ID を削除します。一部のスイッチ ポートが設定されていない場合、これらのポートの値はゼロに設定されて考慮されます。そのため、結果には誤検出が含まれる場合があり、正確なフロア ID と値がゼロのフロア ID が含まれます。

ステップ 6 必ずすべてのポートが正しいフロア領域に割り当てられるように、スイッチ ポートの場所を設定します。

関連トピック

どのようにスイッチ ポートの場所を設定しますか。（337 ページ）
自動 SPT の設定方法を教えてください（333 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問（333 ページ）

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください

自動 SPT 定義をトリガーする有線クライアント ステータス バックグラウンド タスクは次のとおりです。

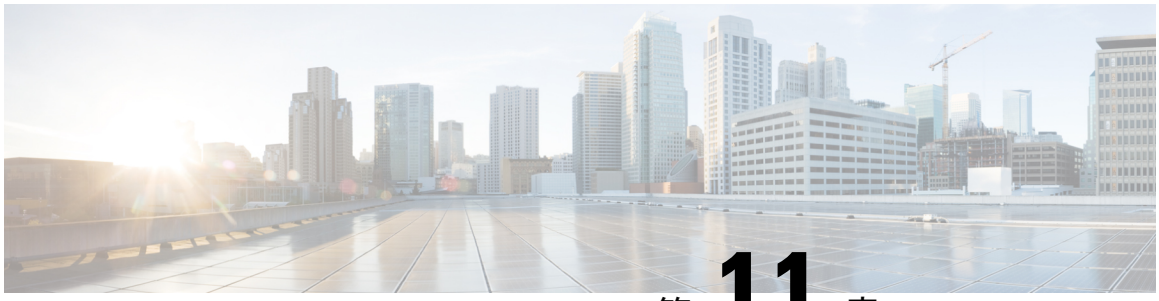
メジャー ポーリング：メジャー ポーリング中、Prime Infrastructure は、重要クライアント情報のすべてをデータベースと同期させることにより、すべての有線デバイス ポートでのクライアント検出をトリガーします。Prime Infrastructure 2.2 の場合、このポーリングの頻度は 1 日 2 回よりも少なくなっていました。現在は、完全に設定可能になっています。

マイナー ポーリング：マイナー ポーリング中、Prime Infrastructure は、最近アクティブになったデバイス インターフェイスおよびポート上のみのクライアント検出をトリガーします。Prime Infrastructure はインターフェイス稼働時間データを使用して、いずれかのクライアントによってポートやインターフェイスが追加または削除されたのがいつなのかを検出します。

関連トピック

自動 SPT と手動 SPT はどのように違いますか （334 ページ）
自動 SPT の方が有線の不正の検出に時間がかかるのはなぜですか （335 ページ）
不正およびスイッチ ポート トレーシングに関して頻繁に寄せられる質問 （333 ページ）

「メジャー ポーリング」と「マイナー ポーリング」の違いについて教えてください



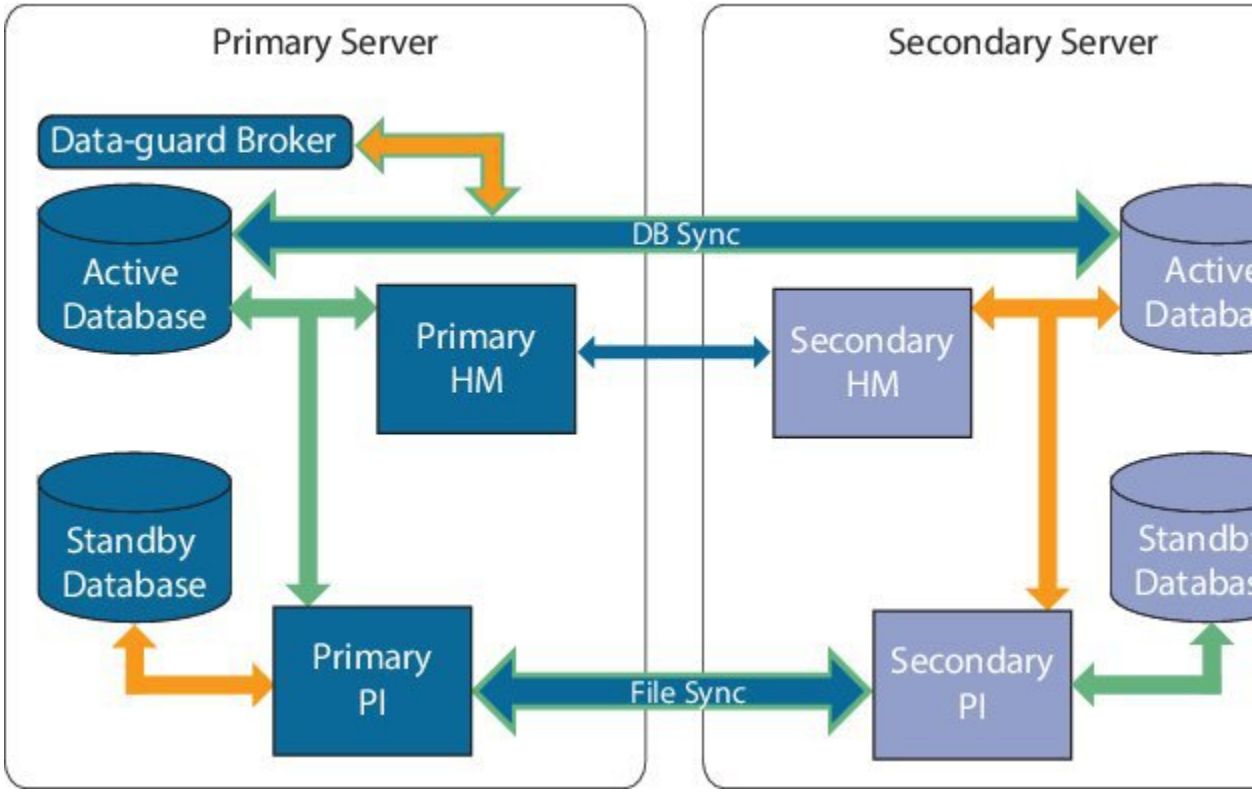
第 11 章

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

以下の図に、Prime Infrastructure ハイ アベイラビリティ（HA）をセットアップしてプライマリ サーバーをアクティブにするための主要コンポーネントとプロセス フローを示します。

図 *1 : HA* の導入



HA の導入には、2 台の Prime Infrastructure サーバー（プライマリとセカンダリ）が必要です。これらのサーバーのそれぞれに、アクティブ データベースとアクティブ データベースのスタンバイ バックアップ コピーがあります。通常状態では、プライマリ サーバーがアクティブです。つまり、プライマリ サーバーが自身のアクティブ データベースに接続されており、ネットワークを管理します。セカンダリ サーバーはパッシブ状態で、自身のスタンバイ データベースのみに接続されていますが、プライマリ サーバーとは継続的な通信状態にあります。

両方のサーバーで実行されているヘルス モニター プロセスにより、お互いのサーバーのステータスがモニターされています。両方のサーバー上で実行されている Oracle Recovery Manager（RMAN）は、アクティブ データベースおよびスタンバイ データベースを作成し、変更の発生時には、プライマリ サーバーで実行される Oracle Data Guard Broker の効果によりデータベースを同期します。

プライマリ サーバーに障害が発生すると、セカンダリが引き継ぎ、自身のアクティブ データベースに接続します。このデータベースは、アクティブ プライマリ データベースと同期されています。この切り替えは「フェールオーバー」と呼ばれ、手動（推奨）または自動でトリガーできます。その後は、プライマリ サーバーへのアクセスの復元作業をしながら、セカンダリ サーバーを使用してネットワークを管理します。プライマリ サーバーが再度使用可能になると、プライマリ サーバーに戻すための切り替え（「フェールバック」）を開始し、プライマリを使用してネットワーク管理を再開できます。

プライマリ サーバーとセカンダリ サーバーを同一 IP サブネットに導入する場合は、1 つの仮想 IP アドレスで Prime Infrastructure に通知を送信するようにデバイスを設定できます。ディザ

スタ リカバリの実施などの目的で、2 台のサーバーを地理的に離れた位置に分散する場合は、両方のサーバーに通知を送信するようにデバイスを設定する必要があります。

関連トピック

プライマリ サーバーとセカンダリ サーバーについて （343 ページ）
障害の原因 （343 ページ）
ファイルおよびデータベースの同期 （344 ページ）
HA サーバー通信 （344 ページ）
ヘルス モニター プロセス （345 ページ）
ヘルス モニター Web ページ （345 ページ）
HA での仮想 IP アドレッシングの使用 （348 ページ）
HA 環境で SSL 証明書を使用する方法 （349 ページ）
Web ブラウザへのクライアント証明書のインポート （349 ページ）

プライマリ サーバーとセカンダリ サーバーについて

すべての Prime Infrastructure HA 実装には、プライマリ サーバーの特定のインスタンスに対して専用のセカンダリ サーバーが 1 台のみ必要です。

通常、HA サーバーごとに独自の IP アドレスまたはホスト名が設定されています。同一サブネット上に配置されているサーバーは、仮想 IP を使用して同じ IP を共有できます。これにより、デバイスの設定が容易になります。Prime Infrastructure のプライマリおよびセカンダリ サーバーは、HA 実装時にネットワーク インターフェイス ethernet0（eth0）で有効にする必要があります。

HA をセットアップした後は、HA サーバーの IP アドレスやホスト名を変更しないください。変更すると、HA 設定が失われます（「関連項目」の「サーバーの IP アドレスまたはホスト名のリセット」を参照）。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
HA での仮想 IP アドレッシングの使用 （348 ページ）
HA サーバーの IP アドレスまたはホスト名のリセット （399 ページ）

障害の原因

Prime Infrastructure サーバーの障害は、以下の 1 つ以上の分野での問題が原因で発生する可能性があります。

- **アプリケーション プロセス**：NMS サーバー、MATLAB、TFTP、FTP を含め、1 つ以上の Prime Infrastructure サーバー プロセスが失敗した場合。各アプリケーション プロセスの動作ステータスを確認するには、管理コンソールから ncs status コマンドを実行します。
- **データベース サーバー**：1 つ以上のデータベース関連のプロセスがダウンした場合。データベース サーバーは、Prime Infrastructure 内のサービスとして実行されます。
- **ネットワーク**：ネットワーク アクセスの問題や、到達可能性の問題が発生した場合。

- **システム**：サーバーの物理ハードウェアまたはオペレーティング システムに関連する問題が発生した場合。
- **仮想マシン**（VM）：プライマリ サーバーとセカンダリ サーバーがインストールされている VM 環境に問題が発生した場合（HA が VM 環境で稼動している場合）。

詳細については、「ハイ アベイラビリティの仕組み」を参照してください。

ファイルおよびデータベースの同期

HA コンフィギュレーションが、プライマリ サーバーでの変更を判別すると、常にその変更がセカンダリ サーバーに同期されます。これらの変更には、次の 2 種類があります。

1. **データベース**：コンフィギュレーション、パフォーマンス、およびモニタリング データに関連するデータベースの更新などです。
2. **ファイル**：コンフィギュレーション ファイルに対する変更などです。

両方のサーバー上で実行されている Oracle Recovery Manager（RMAN）は、アクティブ データベースおよびスタンバイ データベースを作成し、変更の発生時には、プライマリ サーバーで実行される Oracle Data Guard Broker の効果によりデータベースを同期します。

ファイルの変更内容は、HTTPS プロトコルを使用して同期されます。ファイルの同期は、以下のいずれかの方法で行われます。

- **バッチ**：このカテゴリには、頻繁に更新されないファイル（ライセンス ファイルなど）が含まれます。これらのファイルは、500 秒間隔で同期されます。
- **ほぼリアルタイム**：頻繁に更新されるファイルは、このカテゴリに分類されます。これらのファイルは、11 秒間隔で同期されます。

デフォルトでは、HA フレームワークは、必要なすべての構成データをコピーするように設定されます。これらの構成データには、以下が含まれます。

- レポート設定
- コンフィギュレーション テンプレート
- TFTP ルート
- 管理設定
- ライセンス ファイル

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）

HA サーバー通信

プライマリおよびセカンダリ HA サーバーは、HA システムのヘルスを維持するために、次のメッセージを交換します。

- データベース同期：プライマリ サーバーとセカンダリ サーバー上のデータベースが稼働および同期するために必要なすべての情報が含まれます。

- ファイル同期：頻繁に更新されるコンフィギュレーション ファイルが含まれます。これらのファイルは11秒間隔で同期され、他の頻繁に更新されないコンフィギュレーション ファイルは 500 秒間隔で同期されます。
- プロセス同期：アプリケーションおよびデータベースに関連するプロセスの実行が継続されるようにします。これらのメッセージは、ハートビート カテゴリに分類されます。
- Health Monitor 同期：これらのメッセージは、以下の障害状態の有無を確認します。
  - ネットワーク障害
  - システム障害（サーバー ハードウェアとオペレーティング システムでの障害）
  - ヘルス モニター障害

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）

ヘルス モニター プロセス

Health Monitor（HM）とは、HA 操作を管理する主要コンポーネントです。プライマリ サーバーとセカンダリ サーバーでは、それぞれ別個の HM インスタンスがアプリケーション プロセスとして実行されます。HM は、以下の役割を果たします。

- HA に関連するデータベースおよび構成データを同期します（Oracle Data Guard を使用して別途同期されるデータベースは除きます）。
- プライマリ サーバーとセカンダリ サーバーの間で 5 秒間隔でハートビート メッセージを交換し、サーバー間の通信が維持されていることを確認します。
- 両方のサーバー上で使用可能なディスク容量を定期的に確認し、ストレージ容量が不足している場合にはイベントを生成します。
- リンクされた HA サーバー全体のヘルスを管理、制御、モニターします。プライマリ サーバーで障害が発生した場合にセカンダリ サーバーをアクティブ化するのは、Health Monitor の役目です。

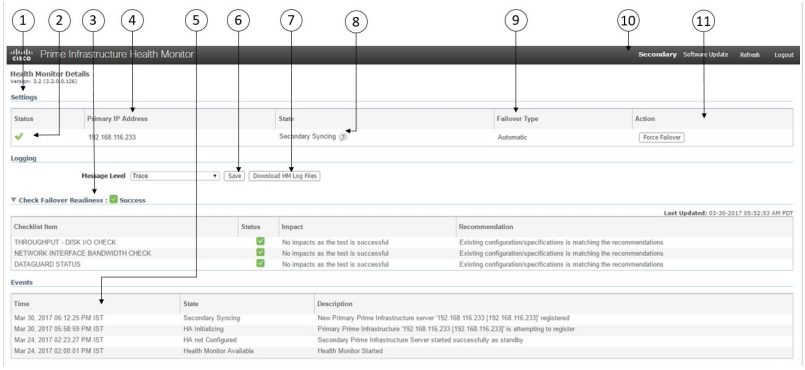
関連トピック

ハイ アベイラビリティの仕組み （341 ページ）

ヘルス モニター Web ページ

Health Monitor Web ページを使用して HA の動作を制御します。プライマリ サーバーまたはセカンダリ サーバーで実行される Health Monitor インスタンスごとに、専用の Web ページがあります。次の図に、「プライマリ アクティブ」状態と「セカンダリ同期中」状態にあるセカンダリ サーバーのヘルス モニター Web ページの例を示します。

図 *2:* ヘルス モニター *Web* ページ（セカンダリ サーバー）



1	[設定（Settings）] 領域に、ヘルス モニターの状態と設定の詳細情報を示す 5 つのセクションが表示されています。
2	[Status] は、HA セットアップの現在の機能ステータスを示します（緑色のチェック マークは、HA がオンであり機能していることを実行します）。
3	[フェールオーバーの準備状況の確認（Check Failover Readiness）] フィールドに、チェックリスト項目のシステム フェールバックの値とシステム フェールオーバーの詳細が表示されます。 詳細については、表の下の「フェールオーバーの準備状況の確認」を参照してください。
4	[プライマリ IP アドレス（Primary IP Address）] は、このセカンダリ サーバーのピア サーバーの IP を示します（プライマリ サーバーの場合、このフィールドには [セカンダリ IP アドレス（Secondary IP Address）] というラベルが付いています）。
5	[イベント（Events）] 表には、現在のすべての HA 関連イベントが最新のイベントを先頭に時系列順に表示されます。
6	[Message Level] フィールドでは、ログ レベル（[Error]、[Informational]、[Trace]）を変更できます。ログ レベルを変更するには、[保存（Save）] をクリックする必要があります。
7	[ロギング ダウンロード（Logging Download）] 領域では、ヘルス モニター ログ ファイルをダウンロードできます。
8	[状態（State）] は、この Health Monitoring インスタンスが実行されているサーバーの現在の HA の状態を示します。
9	[フェールオーバー タイプ（Failover Type）] は、設定されているフェールオーバー タイプ（[手動（Manual）] または [自動（Automatic）]）を示します。
10	表示している Health Monitor Web ページの対象 HA サーバーを示します。

11	[アクション（Actions）]は、実行できるアクション（フェールオーバーまたはフェールバック）を示します。[アクション（Actions）] のボタンは、HA 状態の変更が必要なアクションが Health Monitor により検出された場合にだけ有効になります。

[フェールオーバーの準備状況の確認（Check Failover Readiness）] セクションの説明：

チェックリスト名	説明
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバーとセカンダリ サーバーの両方でディスク IOPS を検証します。 必要な最小ディスク IOPS は 200 Mbps です。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	プライマリ サーバーとセカンダリ サーバーの両方で eth0 インターフェイス速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - ネットワーク帯域幅速度の確認（NETWORK - CHECK NETWORK BANDWIDTH SPEED）	プライマリ サーバーとセカンダリ サーバーの両方でネットワーク帯域幅速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバーの間でデータを送信することによってネットワーク帯域幅を測定します。 （注） Cisco Prime Infrastructure では、ネットワーク帯域幅の速度テストは Mbps でのみ計算されます。そのため、GBps、MBps、KBps、および Mbps は Mbps に変更され、速度テストへの入力として指定されます。
データベース - 同期ステータス（DATABASE - SYNC STATUS）	プライマリ データベースとセカンダリ データベースを同期する Oracle Data Guard Broker の設定を確認します。

フェールオーバー準備状況の確認に関する傾向グラフ：

- 傾向グラフの [ここをクリック（Click here）] リンクをクリックして、すべてのフェールオーバー準備状況の確認テストに関する傾向グラフを確認します。傾向グラフには、テストの履歴サマリーとシステム/ネットワークの安定性に関するステータスが示されます。
- [日付範囲の選択（Select Date Range）] をクリックして日付と時刻を変更し、[適用（Apply）] をクリックします。デフォルトでは、過去 6 時間の値が傾向グラフに表示されます。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
データベースの同期の問題を解決する方法 （391 ページ）

HA での仮想 IP アドレッシングの使用

通常の状況下では、Prime Infrastructure を使用して、管理対象デバイスがその syslog、SNMP トラップ、およびその他の情報を Prime Infrastructure サーバーの IP アドレスに送信するように設定します。HA を実装する場合、それぞれ異なる IP アドレスを持つ 2 台の Prime Infrastructure サーバーが導入されます。プライマリ サーバーと同様にセカンダリ サーバーにも通知を送信するようにデバイスを再設定しないと、セカンダリ Prime Infrastructure サーバーがアクティブモードになったときに、セカンダリ サーバーではすべての通信が受信されません。

管理対象デバイスすべてで2台の別個のサーバーに通知を送信するよう設定する場合、追加のデバイス設定作業が必要です。この追加のオーバーヘッドを回避するため、HA では両方のサーバーが管理アドレスとして共有できる仮想IPアドレスの使用がサポートされています。フェールオーバー プロセスとフェールバック プロセスの実行中に、この 2 台のサーバーは必要に応じて IP を切り替えます。仮想 IP アドレスは常に、正しい Prime Infrastructure サーバーを指し示します。

両方の HA サーバーのアドレスおよび仮想 IP がすべて同じサブネット上にない場合、仮想 IP アドレッシングを使用できないことに注意してください。これは、HA サーバー導入の選択方法に影響する可能性があります（「関連項目」の「HA の導入計画」および「ローカル モデルの使用」参照）。

また、仮想 IP アドレスを 2 つのサーバー IP アドレスの代わりとして使用することは一切意図されていないことに注意してください。仮想 IP は、syslog やトラップなど Prime Infrastructure サーバーに送信されるデバイス管理メッセージの宛先として使用されます。デバイスのポーリングは、2 つの Prime Infrastructure サーバー IP アドレスのうちの 1 つから常に実施されます。このことを考慮すると、仮想 IP アドレッシングを使用している場合、3 つすべてのアドレス（仮想 IP アドレスおよび 2 つの実際のサーバー IP）における着信および発信 TCP/IP 通信に対してファイアウォールを開く必要があります。

オペレーション センターでの HA の使用を計画している場合、仮想 IP アドレッシングを使用することもできます。オペレーション センターが有効になっている Prime Infrastructure インスタンスに仮想 IP を SSO として割り当てることができます。オペレーション センターを使用して管理されているインスタンスには、仮想 IP は必要ありません（「オペレーション センター用の HA の有効化」を参照）。

プライマリ サーバーでの HA の登録時に仮想 IP アドレッシングを有効にできます。そのためには、この機能を使用する旨を指定し、プライマリ サーバーとセカンダリ サーバーで共有する仮想 IPv4（必要な場合は IPv6）アドレスを入力します（「プライマリ サーバーでの HA の登録方法」を参照）。

仮想 IP アドレッシングを有効化した後に仮想 IP アドレッシングを削除するには、HA を完全に削除する必要があります（「GUI での HA の削除」を参照）。

関連トピック

仮想 IP アドレッシングを使用できない場合の対処 （354 ページ）
HA の導入計画 （350 ページ）
ローカル モデルの使用 （352 ページ）
オペレーション センター用の HA の有効化 （356 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
ハイ アベイラビリティの仕組み （341 ページ）
GUI での HA の削除 （396 ページ）

HA 環境で SSL 証明書を使用する方法

Prime Infrastructure サーバーとユーザー間の通信をセキュアなものにするために SSL 認証を使用することを決め、HA の実装も計画している場合、プライマリ HA サーバーとセカンダリ HA サーバー用に別々の証明書を生成する必要があります。

これらの証明書は、各サーバーの FQDN（完全修飾ドメイン名）を使用して生成する必要があります。つまり、プライマリ サーバーで使用する予定の証明書の生成にはプライマリ サーバーの FQDN を使用し、セカンダリ サーバーで使用する予定の証明書の生成にはセカンダリ サーバーの FQDN を使用する必要があります。

証明書を生成したら、各サーバーに署名付き証明書をインポートします。

仮想 IP アドレスを使用して SSL 証明書を生成しないでください。仮想 IP アドレス機能は、Prime Infrastructure とネットワーク デバイス間の通信を可能にするために使用します。

Cisco Prime Infrastructure の HTTPS アクセスを設定するには、「Prime Infrastructure への HTTPS アクセスをセットアップする」を参照してください。

Web ブラウザへのクライアント証明書のインポート

証明書認証が設定された Prime Infrastructure サーバーにアクセスするユーザーは、認証用にクライアント証明書をブラウザにインポートする必要があります。このプロセスは各種ブラウザで同様ですが、実際の詳細部分についてはブラウザによって異なります。以下の手順では、ユーザーが Prime Infrastructure 互換の Firefox を使用しているものとしています。

クライアント証明書をインポートするユーザーに関して、以下について確認する必要があります。

- クライアント マシンのローカル ストレージ リソースに証明書ファイルのコピーをダウンロード済みであること。
- 証明書ファイルが暗号化されている場合は、証明書ファイルの暗号化に使用されたパスワードを保有していること。

ステップ 1 Firefox を起動し、次の URL をロケーション バーに入力します：**about:preferences#advanced**

Firefox の [オプション（Options）] > [詳細設定（Advanced）] タブが表示されます。

ステップ 2 [証明書（Certificates）] > [証明書の表示（View Certificates）] > 自分の証明書の順に選択して [インポート...（Import...）] をクリックします。.

ステップ 3 ダウンロードした証明書ファイルに移動してそれらを選択し、[OK] または [開く（Open）] をクリックします。

ステップ 4 証明書ファイルが暗号化されている場合、証明書ファイルの暗号化に使用されたパスワードの入力が求められます。該当するパスワードを入力し、[OK] をクリックします。

これで証明書がブラウザにインストールされました。

ステップ 5 Ctrl+Shift+Del を押して、ブラウザのキャッシュをクリアします。

ステップ 6 証明書認証を使用してブラウザで Prime Infrastructure サーバーにアクセスします。

要求されたサーバー認証に応答するための証明書の選択が求められます。適切な証明書を選択し、[OK] をクリックします。

ホット スタンバイ動作

プライマリ サーバがアクティブ状態のとき、セカンダリ サーバは、プライマリ サーバと常時同期状態にあり、高速で切り替えができるように、すべての Prime Infrastructure プロセスを実行しています。プライマリ サーバに障害が発生すると、セカンダリ サーバがフェールオーバー後 2 ～ 3 分以内にアクティブなロールを素早く引き継ぎます。

プライマリ サーバでの問題が解消され、プライマリ サーバが実行状態に戻ると、プライマリ サーバがスタンバイ ロールになります。プライマリ サーバがスタンバイ ロールになると、ヘルス モニタの GUI には「Primary Syncing」状態が表示され、プライマリ サーバ上のデータベースおよびファイルとアクティブなセカンダリ サーバとの同期が開始されます。

プライマリ サーバが再度使用可能になり、フェールバックがトリガーされると、再度プライマリ サーバがアクティブ ロールを引き継ぎます。このようなプライマリ サーバーとセカンダリ サーバー間でのロールの切り替えは、2 ～ 3 分以内に実行されます。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）

HA の導入計画

Prime Infrastructure の HA 機能は、以下の導入モデルをサポートしています。

- **ローカル**：HA サーバーの両方を同じサブネットに配置します（サーバーにレイヤ 2 近接性を与えます）。通常は、両方のサーバーが同じデータ センター内に配置されます。
- **キャンパス**：HA サーバーのそれぞれを、LAN で接続された異なるサブネットに配置します。通常、これらのサーバーは同じ 1 つのキャンパスに導入されますが、キャンパス内で配置される場所は異なります。

- **リモート**：HA サーバーのそれぞれを、WAN で接続された異なるリモート サブネットに配置します。各サーバーが、異なる施設に配置されます。これらの施設は、国や大陸間にまたがり、地理的に分散されています。

以降の項で、各モデルの利点および欠点と、すべての導入モデルに影響する基本的な制約事項について説明します。

HA は、サポートされているいずれの導入モデルでも機能します。主な制約事項は、HA のパフォーマンスと信頼性に関して存在し、これらは帯域幅と遅延の基準によって異なります（「HA のネットワーク スループットに関する制限事項」参照）。これらのパラメータを正常に管理できる限り、使用可能な導入モデルのどれを選んで実装するかは、（コスト、企業の規模、地理、コンプライアンス標準などのビジネスパラメータに基づく）ビジネス上の意思決定です。

関連トピック

HA のネットワーク スループットに関する制限事項 （351 ページ）
ローカル モデルの使用 （352 ページ）
キャンパス モデルの使用 （353 ページ）
リモート モデルの使用 （354 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （354 ページ）
自動フェールオーバーと手動フェールオーバーの違い （355 ページ）
オペレーション センター用の HA の有効化 （356 ページ）

HA のネットワーク スループットに関する制限事項

Prime Infrastructure の HA パフォーマンスは、常に以下の制限要因の影響を受けます。

- すべての操作を処理するために Prime Infrastructure で利用できる正味の帯域幅。これらの操作には、HA 登録、データベース同期、ファイル同期、フェールバックのトリガーが含まれます（ただし、これらに限定されません）。
- プライマリ サーバーとセカンダリ サーバー間のリンク全体における正味のネットワーク遅延。この 2 台のサーバーの物理的な近接性にかかわらず、サーバー間のリンクで発生する遅延が大きい場合、Prime Infrastructure によるプライマリ サーバーとセカンダリ サーバー間のセッション維持状態に影響が及ぶ可能性があります。
- プライマリ サーバーとセカンダリ サーバーを接続するネットワークが提供できる正味のスループット。正味のスループットは正味の帯域幅と遅延によって異なり、これら 2 つの要因の関数と見なすことができます。

モデルによって問題の大きさが異なりますが、これらの制限は、少なくとも何らかのレベルであらゆる導入モデルに当てはまります。例えば、リモート導入モデルは、地理的な分散が大きいため、帯域幅と遅延の両方で問題が発生しがちです。一方、ローカル モデルとキャンパス モデルの場合も、正しく構成されていなければ、帯域幅の問題が発生する可能性が高くなります。これは、低帯域幅、高遅延、高ネットワーク使用率によって制限を受ける可能性があるためです。

スループットの問題がフェールバックやフェールオーバーに影響することはほとんどありません。2 つの HA サーバーがほとんど常に通信して、データベースの変更内容が即座に複製されるためです。ほとんどのフェールオーバーおよびフェールバックは、約 2 ～ 3 分を要します。

この原則の最大の例外は、データベースのフル コピー動作における遅延です。この種類のアクションは、プライマリ サーバーがデータ保持期間を超えてダウンした後、これを再度稼働させる場合にトリガーされます。Express、Express-Plus、Standard の各構成サーバーのデータ保持期間は 6 時間で、Professional および Gen 2 アプライアンス サーバーでは 12 時間です。

Prime Infrastructure はセカンダリ サーバーからプライマリ サーバーへのデータベースのフル コピー動作をトリガーします。この期間中のフェールバックはできませんが、[ヘルス モニター（Health Monitor）] ページには、データベースのコピー進行中に発生したすべてのイベントが表示されます。コピーが完了するとすぐに、プライマリ サーバーは「プライマリ同期中（Primary Synching）」状態に移行し、その後、フェールバックのトリガーが可能になります。データベースのフル コピーが行われている間は、プライマリ サーバーの再起動やネットワーク接続切断を行わないでください。

データベースのフル コピー動作中の正味スループットの変動は、データベースのサイズやその他の要因とは無関係に、データベースのフル コピー動作が 1 時間未満で正常に完了するケースと、まったく完了できないケースという違いを生じるぐらいの意味を持ちます。シスコでは、標準的なデータベース サイズである 105 GB ～ 156 GB の Prime Infrastructure を使用して、以下のリモート モデルの構成での HA 導入における正味スループットの影響をテストしてきました。これらのテストに基づき、シスコでは、125 GB の標準的なデータベース（10 GB のバックアップ ファイルを生成）に対して、以下のように推奨します。

- 最適な結果の場合：サブミリ秒の遅延と 977 Mbps の正味スループットにおいて、データベースのフル コピーの時間を 1 時間未満と想定。
- 良好な結果の場合：70 ミリ秒の遅延と 255 Mbps 以上の正味スループットにおいて、データベースのフル コピーの時間を 2 時間未満と想定。
- 許容可能な結果の場合：220 ミリ秒以下の遅延と 86 Mbps 以上の正味スループットにおいて、データベースのフル コピーの時間を 4.5 時間未満と想定。

遅延が 330ms 以上、スループットが 46Mbps 以下の場合、データベースのコピーが正常に完了しない危険があります。

関連トピック

HA の導入計画 （350 ページ）
リモート モデルの使用 （354 ページ）

ローカル モデルの使用

ローカル導入モデルの主要なメリットは、仮想 IP アドレスをシステムの単一管理ドレスとして使用することが許可される点です。ユーザーはこの仮想 IP アドレスを使用して Prime Infrastructure に接続し、デバイスではこの仮想 IP アドレスを SNMP トラップおよびその他の通知の宛先として使用できます。

仮想 IP アドレスを割り当てる際の唯一の制約は、仮想 IP アドレスが、プライマリ サーバーの IP アドレスおよびセカンダリ サーバーの IP アドレスと同じサブネット上のアドレスでなければならない点です。例：プライマリ サーバーとセカンダリ サーバーに対し、1 つのサブネット内の次の IP アドレスが割り当てられている場合、この両方のサーバーの仮想 IP アドレスは次のように割り当てることができます。

- サブネット マスク：255.255.255.224 (/27)
- プライマリ サーバーの IP アドレス：10.10.101.2
- セカンダリ サーバーの IP アドレス：10.10.101.3
- 仮想 IP アドレス：10.10.101.[4-30]（例：10.10.101.4）仮想 IP アドレスは、特定のサブネットマスクで有効かつ未使用のアドレス範囲内の任意のアドレスになることに注意してください。

この主な利点に加え、ローカル モデルには以下の利点もあります。

- 通常、高帯域幅と低遅延を実現します。
- 管理が簡素化されます。
- syslog および SNMP 通知を転送するようにデバイスを設定するのが、大幅に簡単になります。

ローカル モデルには、以下の欠点があります。

- 同じデータ センター内に配置されることから、停電や自然災害など、サイト全体の障害の危険にさらされます。
- 破壊的なサイト障害の危険が高くなることから、ビジネス継続性の計画が複雑になります。また、損害保険のコストも高くなる可能性があります。

関連トピック

HA の導入計画 （350 ページ）
キャンパス モデルの使用 （353 ページ）
リモート モデルの使用 （354 ページ）

キャンパス モデルの使用

キャンパス モデルでは、HA を導入する組織が、同じ都道府県の同じ市区町村内の 1 つ以上のロケーションを拠点にしていて、これらの複数ロケーションによって「キャンパス」を形成していることが前提となります。このモデルには、以下の利点があります。

- 通常、ローカル モデルに匹敵するか、それ以上の帯域幅と遅延を提供します。
- リモート モデルより簡単に管理できます。

キャンパス モデルには、以下の欠点があります。

- ローカル モデルより、管理が複雑になります。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。その場合は、多くのデバイス設定が必要となります（「関連項目」の「仮想 IP アドレッシングを使用できない場合の対処」参照）。
- ローカルモデルと比べると、帯域幅が小さくなり、遅延が大きくなる可能性があります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「関連項目」の「HA のネットワーク スループットに関する制限事項」参照）。
- 同じサイトに配置されてはいませんが、それでも都道府県全体、または市区町村全体の災害の危険にさらされます。そのため、ビジネス継続性の計画が複雑になり、災害復旧のコストが高くなる可能性があります。

関連トピック

HA の導入計画 （350 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）
ローカル モデルの使用 （352 ページ）
リモート モデルの使用 （354 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （354 ページ）

リモート モデルの使用

リモートモデルでは、導入する組織に複数のサイトまたはキャンパスがあること、そしてこれらのロケーション間では、地理的な境界を超えて WAN リンクで通信することが前提となります。このモデルには、以下の利点があります。

- 自然災害による影響を受ける可能性が最小限になります。ビジネス継続性および災害復旧という点では、通常、これが最も複雑でなく、コストのかからないモデルになります。
- 事業保険のコストを節約できる可能性があります。

リモート モデルには、以下の欠点があります。

- ローカルまたはキャンパス モデルより、管理が複雑です。
- 仮想 IP アドレスをシステムの単一管理アドレスとして使用することを許可しないでください。その場合は、多くのデバイス設定が必要となります（「関連項目」の「仮想 IP アドレッシングを使用できない場合の対処」参照）。
- 通常、他の2つのモデルよりも提供される帯域幅が低く、遅延が大きくなります。これは HA の信頼性に影響を与える可能性があり、是正するには管理者の介入が必要になる場合もあります（「関連項目」の「HA のネットワーク スループットに関する制限事項」参照）。

関連トピック

HA の導入計画 （350 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）
ローカル モデルの使用 （352 ページ）
キャンパス モデルの使用 （353 ページ）
仮想 IP アドレッシングを使用できない場合の対処 （354 ページ）

仮想 IP アドレッシングを使用できない場合の対処

選択する導入モデルによっては、仮想IPアドレスを設定しないでおくと、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが発生した場合に syslog と SNMP 通知がセカンダリ サーバーに転送されるようにするために、管理者が追加の作業を行わなければならない状況になることがあります。一般的な方法は、両方のサーバーにすべてのsyslogとトラップを転送するようにデバイスを設定することです。このためには通常、転送先をプライマリ サーバーとセカンダリ サーバーの両方を含む特定のサブネットまたは IP アドレス範囲に設定します。

この設定作業は、HA のセットアップと同時、つまりセカンダリ サーバーのインストール後からプライマリ サーバーでの HA の登録までの間に行う必要があります。これはフェールオーバーが発生する前に完了しておく必要があります。これにより、データが失われる可能性を解消または削減できます。仮想 IP アドレスを使用しない場合、セカンダリ サーバーのインストール手順は変更されません。ただし通常どおり、個別の IP アドレスを使用してプライマリ サーバーとセカンダリ サーバーをプロビジョニングする必要があります。

オペレーションセンターで HA を使用する場合、この回避策は使用できません。この場合、仮想 IP アドレスを有効にすることが必須条件となります（「オペレーション センター用の HA の有効化」を参照）。

関連トピック

HA での仮想 IP アドレッシングの使用 （348 ページ）
HA の導入計画 （350 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）
キャンパス モデルの使用 （353 ページ）
リモート モデルの使用 （354 ページ）
オペレーション センター用の HA の有効化 （356 ページ）

自動フェールオーバーと手動フェールオーバーの違い

自動フェールオーバーを行うように HA を設定すると、ネットワーク管理者による HA の管理の必要性が減少します。また、セカンダリ サーバーが自動的に起動されるため、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。

ただし、ほとんどの場合は、システムで手動フェールオーバーを設定することが推奨されます。この推奨に従うことで、断続的なネットワークの停止に伴い Prime Infrastructure がセカンダリ サーバーに頻繁にフェールオーバーすることがなくなります。この状況が発生する可能性が最も高いのは、リモートモデルを使用して HA を導入する場合です。このモデルは、特に帯域幅と遅延の急激な変化による影響を受けます（「関連項目」の「HA の導入計画」および「HA のネットワーク スループットに関する制限事項」参照）。

フェールオーバー タイプが [自動（Automatic）] に設定されている場合に、ネットワーク接続がダウンするか、またはプライマリ サーバーとセカンダリ サーバー間のネットワーク リンクが到達不能になると、プライマリ サーバーとセカンダリ サーバーの両方が同時にアクティブになる可能性がわずかながらあります。これは「スプリット ブレーン状況」と呼ばれます。

この状況を防ぐため、プライマリ サーバーはセカンダリ サーバーがアクティブかどうかを常に確認します。ネットワーク接続またはリンクが復元され、プライマリ サーバーからセカンダリ サーバーに再び到達可能になると、プライマリ サーバーはセカンダリ サーバーの状態を確認します。セカンダリ サーバーの状態がアクティブな場合、プライマリ サーバーは自らダウンします。続いてユーザーがプライマリ サーバーへの標準の手動フェールバックを実行できます。

この状況が発生するのは、プライマリ HA サーバーで自動フェールオーバーが設定されている場合だけであることに注意してください。プライマリ サーバーで手動フェールオーバーを設定

することで、この状況が発生する可能性が排除されます。これが、手動フェールオーバー設定を推奨するもう 1 つの理由です。

大企業では特に、自動フェールオーバーは不適切です。特定の HA 導入環境で自動フェールオーバーを実行することになった場合、管理者はプライマリ サーバーまたはセカンダリ サーバーに新規に追加されたデータのいずれかを選択しなければならないことがあります。つまり、スプリットブレーンの状況が発生するたびにデータが失われる可能性があります。この問題に対処するには、「関連項目」の「スプリット ブレイン シナリオからの回復方法」を参照してください。

HA が適切に管理されるために、Prime Infrastructure 管理者に推奨されるのは、フェールオーバーまたはフェールバックを開始する前に、常に以下を含む HA 導入の全体的な状態を確認することです。

- プライマリ サーバーの現在の状態。
- セカンダリ サーバーの現在の状態。
- 2 台のサーバー間の現在の接続状態。

関連トピック

HA の導入計画 （350 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）
フェールバックのトリガー方法 （378 ページ）
スプリット ブレイン シナリオからの回復方法 （390 ページ）
オペレーション センター用の HA の有効化 （356 ページ）

オペレーション センター用の HA の有効化

オペレーション センターには、Prime Infrastructure の高可用性（HA）フレームワークとの互換性があります。オペレーション センター用の HA は、プライマリおよびセカンダリオペレーション センター サーバーを設定すると簡単に有効化できます。この操作は、オペレーション センターを使用して管理する通常の Prime Infrastructure サーバー インスタンスに対して HA を実装する場合と同様です。

セカンダリ サーバーではオペレーション センターの追加ライセンスは必要ありません。オペレーションセンター用の HA は、手動および自動の両方のフェールオーバーをサポートしています。フェールオーバーの発生時には、セカンダリ オペレーション センター サーバーがアクティブになると、プライマリ オペレーション センター サーバーからから管理されているすべてのインスタンスが自動的にセカンダリ サーバーに継承されます。プライマリ オペレーション センター サーバーが新規であってもすでに稼働中のオペレーション センターであっても、プライマリで HA を有効化することができます。

オペレーション センター用の HA の有効化は必須ではありません。ただし、オペレーション センター用に HA を有効化するよう選択した場合、オペレーション センターでの HA 登録時に仮想 IP アドレッシングを有効にすることもできます。仮想 IP を使用するには、プライマリ サーバーとセカンダリ サーバーが同じサブネットにあることが必要です。

仮想 IP を使用してオペレーション センター用の HA をセットアップするには、次のワークフローに従ってください。

1. 両方のサーバーで使用する仮想 IP アドレスを決定します。詳細については、関連項目の「HA での仮想 IP アドレッシングの使用」と「ハイ アベイラビリティをセットアップする前に」を参照してください。
2. プライマリ オペレーション センター HA サーバーとして使用するサーバーに Prime Infrastructure をインストールします。

   オペレーション センターが有効な Prime Infrastructure サーバーがあり、このサーバーを HA を備えたプライマリ オペレーション センター サーバーとして使用する場合は、オペレーション センター インスタンスと、そのオペレーション センター サーバーが管理するすべての Prime Infrastructure インスタンスから、シングル サインオン（SSO）サーバーを削除します。この操作は **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [SSO サーバー（SSO Servers）]** を選択し、**[SSO サーバーを削除（Delete SSO Server(s)）]** コマンドを使用すると簡単にできます。
3. セカンダリ サーバーをインストールし、HA を使用できるよう設定します。詳細については、「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照してください。
4. プライマリでセカンダリ サーバーを登録します。このとき、仮想 IP を有効化するよう指定し、選択した仮想 IP アドレスを入力します。サーバーからログアウトし、仮想 IP アドレスでもう一度ログインます。詳細については、「関連項目」の「プライマリ サーバーでの HA の登録方法」を参照してください。
5. 新しいプライマリ HA サーバーの場合：オペレーション センター ライセンス ファイルをプライマリ サーバーに適用して、オペレーション センターに変換します。詳細については、「オペレーション センター ライセンスのアクティブ化」を参照してください。
6. プライマリ サーバーで仮想 IP アドレスを SSO サーバーとしてセットアップします。このとき、仮想 IP アドレスを SSO サーバーの IP アドレスとして指定します。詳細については、「関連項目」の「オペレーション センターの SSO を有効にする」を参照してください。

（注） 既定では、TOFU はプライマリ サーバーで有効になっており、プライマリまたはセカンダリに CA 証明書が展開されていない場合は、フェールオーバー後に PI インスタンスとセカンダリ サーバーから仮想 IP TOFU を削除します。フェールバック後、プライマリ サーバーで同じ操作を繰り返します。SSO（プライマリ）クライアントサーバーから仮想 IP の TOFU を削除するには、次の操作を行います。

```
ncs certvalidation tofu-certs deletecert host <virtual ip>
```

7. プライマリ オペレーション センター サーバーが管理する Prime Infrastructure のすべてのインスタンスで、仮想 IP SSO サーバーの設定を繰り返します。古い SSO 構成が削除されていること確認し、PI サーバーを独自の IP で起動します。
8. すべての Prime Infrastructure インスタンスからログアウトしてから、仮想 IP アドレスをオペレーション センター IP として使用してオペレーション センター インスタンスにログインします。
9. 新しいプライマリ HA サーバーの場合：「関連項目」の「オペレーション センターに Cisco Prime Infrastructure インスタンスを追加する」の説明に従って、Prime Infrastructure インスタンスをオペレーション センター サーバーに追加します。

詳細については、「関連項目」の「オペレーションセンターライセンスのアクティブ化」を参照してください。

（注） 管理対象サーバーと SSO 設定の両方で、ホスト名または IP アドレスを統一して使用することを推奨します。IP アドレスとホスト名の両方を含めると、OPC から管理対象 PI への相互起動時に SSO で予期しない動作が発生する可能性があります。

仮想 IP を使用せずにオペレーション センター用の HA をセットアップするには、次のワークフローに従ってください。

1. プライマリ オペレーション センター HA サーバーとして使用するサーバーに Prime Infrastructure をインストールします。

   オペレーションセンターが有効な Prime Infrastructure サーバーがあり、このサーバーを HA を備えたプライマリ オペレーション センター サーバーとして使用する場合は、オペレーション センター インスタンスと、そのオペレーション センター サーバーが管理するすべての Prime Infrastructure インスタンスから、シングル サインオン（SSO）サーバーを削除します。この操作は **[管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [SSO サーバー（SSO Servers）]** を選択し、**[SSO サーバーを削除（Delete SSO Server(s)）]** コマンドを使用すると簡単にできます。

2. セカンダリ サーバーをインストールし、HA を使用できるよう設定します。詳細については、「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照してください。
3. プライマリ上でセカンダリ サーバーを登録します。
4. 新しいプライマリ HA サーバーの場合：オペレーション センター ライセンス ファイルをプライマリ サーバーに適用して、オペレーション センターに変換します。詳細については、「オペレーション センター ライセンスのアクティブ化」を参照してください。
5. プライマリ オペレーション センター サーバーによって管理される Prime Infrastructure のすべてのインスタンスに対して、プライマリ サーバー IP アドレスのセットアップを繰り返します。
6. すべての Prime Infrastructure インスタンスからログアウトして、プライマリ IP アドレスをオペレーション センター サーバー IP として使用してオペレーション センター インスタンスにログインします。
7. 新しいプライマリ HA サーバーの場合：「関連項目」の「オペレーションセンターに Cisco Prime Infrastructure インスタンスを追加する」の説明に従って、Prime Infrastructure インスタンスをオペレーション センター サーバーに追加します。

   詳細については、「関連項目」の「オペレーションセンターライセンスのアクティブ化」を参照してください。

関連トピック

HA での仮想 IP アドレッシングの使用 （348 ページ）
ハイ アベイラビリティをセットアップする前に （359 ページ）
HA セカンダリ サーバーのインストール方法 （361 ページ）

プライマリ サーバーでの HA の登録方法 （362 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 （4 ページ）
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）

ハイ アベイラビリティのセットアップ

Prime Infrastructure で HA 機能を使用するには、以下の作業を行う必要があります。

1. HA を有効にするために必要な情報と設定が揃っていることを確認します。詳細については、「関連項目」の「ハイ アベイラビリティをセットアップする前に」を参照してください。
2. 2 台目の Prime Infrastructure サーバーをインストールし、セカンダリ HA サーバーとして機能するように設定します。詳細については、「HA セカンダリ サーバーのインストール方法」を参照してください。
3. プライマリ サーバーでハイ アベイラビリティ モードを設定します。このとき、インストールしたセカンダリ サーバーを HA フォールバック サーバーとして指定します。詳細については、「プライマリ サーバー上での HA の登録方法」を参照してください。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
HA の導入計画 （350 ページ）
オペレーション センター用の HA の有効化 （356 ページ）
ハイ アベイラビリティをセットアップする前に （359 ページ）
HA セカンダリ サーバーのインストール方法 （361 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
HA 登録中の動作 （367 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法 （371 ページ）
ハイ アベイラビリティのモニター （376 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

ハイ アベイラビリティをセットアップする前に

セットアップの前に、以下のものが必要です。

- Prime Infrastructure インストール ソフトウェア。HA セカンダリ サーバーを作成するには、このソフトウェアを使用します。このソフトウェアのバージョンは、プライマリ サーバーにインストールされている Prime Infrastructure のバージョンと一致していなければなりません。プライマリ サーバー ソフトウェアの現在のバージョンを確認するには、CLI **show version** コマンドを使用します。
- プライマリ サーバーにパッチが適用されている場合は、セカンダリ サーバーにも同じレベルのパッチを適用する必要があります。[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）] > [ソフトウェア アップデート（Software Update）] を選択すると、プライマリ サーバーに適用されているパッチの一覧が表示されます。ハイ アベイラビリティのセットアップ後に「ペアリング済みハイ アベイラビリティ サーバーのパッチ適用方法」の手順に従い、セカンダリ サーバーにプライマリ サーバーと同じレベルのパッチを適用します。

- プライマリ サーバーの要件を満たすか、それを上回るハードウェアおよびソフトウェア仕様を備えたセカンダリ サーバー。たとえば、プライマリ サーバーが Prime Infrastructure の標準サイズの OVA としてインストールされている場合、セカンダリ サーバーも標準サーバーとしてインストールする必要があります。この場合、セカンダリ サーバーは、『Cisco Prime Infastructure Quick Start Guide』に記載されている標準サイズのサーバーのすべての要件を満たすか、それを上回っていなければなりません。
- セカンダリ サーバーの IP アドレスまたはホスト名。プライマリ サーバーで HA を設定する際に必要になります。
- 仮想 IP アドレッシングを使用する場合：両方の HA サーバーで仮想 IP として使用する仮想 IPv4 および IPv6 アドレス。仮想 IP 機能を使用する場合のみ必須となります（「関連項目」の「HA での仮想 IP アドレッシングの使用」を参照）。仮想 IP アドレッシングを使用するには、両方の HA サーバーが同一サブネット上にあることが必要です。オペレーション センターで HA を使用するには、仮想 IP アドレッシングを使用する必要があります（「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）。
- 任意の長さの認証キー。小文字の英字、大文字の英字、数字、および特殊文字のうち、少なくとも 3 種類の文字が含まれている必要があります。セカンダリ サーバーをインストールするときに、この認証キーを入力します。HA の実装では、このキーを使用して、プライマリ サーバーとセカンダリ サーバー間の通信を認証します。管理者は、プライマリ サーバーに HA を設定する際や、HA 実装のモニターおよび問題のトラブルシューティングを行うためにセカンダリ サーバーの Health Monitor ページにログオンする際にも、このキーを使用します。
- プライマリ サーバーに対して管理者権限を持つ Prime Infrastructure ユーザー ID。
- HA 状態変更の通知先として設定できる、有効なメール アドレス。Prime Infrastructure は、HA 登録、障害、フェールオーバーおよびフェールバックが発生すると、状態変更を通知する電子メールを送信します。
- 許容可能な結果の場合：プライマリ サーバーとセカンダリ サーバーの間のリンクにおいて、220 ミリ秒以下の遅延と 86 Mbps 以上の正味スループット。少なくともこのリンク品質を提供できなければ、データ レプリケーションの妨げとなり、HA 障害が発生する可能性があります。許容可能なパフォーマンス要件の範囲のアドバイスについては、「HA のネットワーク スループットに関する制限事項」を参照してください。
- プライマリ サーバーとセカンダリ サーバーの間にファイアウォールを設定する場合は、ファイアウォールが以下のポートで着信および発信 TCP/UDP を許可するようにしてください。
  - 8082：ヘルス モニター プロセスでハートビート メッセージを交換するために使用されます。
  - 1522：Oracle でデータを同期するために使用されます。

- 8085：ユーザーがハイ アベイラビリティの準備状況テストを実行すると、プライマリ サーバーとセカンダリ サーバー間のネットワーク帯域幅速度を確認するためにヘルス モニター プロセスで使用されます

- Prime Infrastructure の HA 実装とともにオペレーション センターを使用する予定がある場合：HA 対応の Prime Infrastructure サーバーのすべて（プライマリとセカンダリの両方）がホスト名を完全に解決していることを確認してください。

  詳細については、『Cisco Prime Infastructure Quick Start Guide』を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法（371 ページ）
HA での仮想 IP アドレッシングの使用 （348 ページ）
オペレーション センター用の HA の有効化 （356 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）

HA セカンダリ サーバーのインストール方法

プライマリ サーバーにパッチが適用されている場合は、セカンダリ サーバーのインストール後、プライマリ サーバーで HA を登録する前に、同じパッチをセカンダリ サーバーにも必ず適用してください。

手順を開始する前に、必ず認証キーを決定しておいてください（「関連項目」の「ハイ アベイラビリティをセットアップする前に」参照）。

ステップ 1 プライマリ サーバーの場合と同じように、セカンダリ サーバーへの Prime Infrastructure サーバー ソフトウェアのインストールを開始します。サーバーのインストール手順については、『Cisco Prime Infrastructure Quick Start Guide』を参照してください。

ステップ 2 インストール中に、以下のプロンプトが出されます。

Will this server be used as a secondary for HA? (yes/no)

プロンプトで **yes** と入力します。

ステップ 3 次に、以下のように HA 認証キーの入力を求めるプロンプトが出されます。

Enter Authentication Key:

プロンプトで認証キーを入力します。確認プロンプトでパスワードを再入力します。

ステップ 4 セカンダリ サーバーのインストールが完了したら、以下の作業を行います。

a) 両方のサーバーで CLI **show version** コマンドを使用して、バージョンおよびパッチ レベルが同じであることを確認します（「Prime Infrastructure のバージョンおよびパッチ ステータスの確認」を参照）。

b) ncs status コマンドを実行して、すべてのプロセスが起動され、セカンダリ サーバーで実行中であることを確認します（「Prime Infrastructure サーバー ステータスの確認」を参照）。

c) プライマリ サーバーで HA を登録します（「プライマリ サーバーでの HA の登録方法」を参照）。

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
ハイ アベイラビリティをセットアップする前に （359 ページ）
Prime Infrastructure のバージョンとパッチ ステータスの確認 （149 ページ）
Prime Infrastructure サーバーのステータスの確認 （148 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）

プライマリ サーバーでの HA の登録方法

HA を有効にするには、プライマリ サーバーに HA を登録する必要があります。プライマリ サーバーが HA コンフィギュレーションに参加するために、サーバーのインストール中に必要となる設定はありません。プライマリ サーバーで必要な情報は次の情報のみです。

- インストールと設定が完了しているセカンダリ HA サーバーの IP アドレスまたはホスト名（「関連項目」の「HA セカンダリ サーバーのインストール方法」を参照）。
- セカンダリ サーバーのインストール時に設定した認証キー。
- 通知の送信先となる 1 つ以上の電子メール アドレス。
- フェールオーバー タイプと自動フェールオーバー（「自動フェールオーバーと手動フェールオーバーの違い」を参照）。

仮想 IP アドレッシングを使用する場合（「HA での仮想 IP アドレッシングの使用」を参照）、次の作業も必要となります。

- [仮想 IP の有効化（Enable Virtual IP）] チェックボックスを選択します。
- プライマリおよびセカンダリ HA サーバーで共有する IPv4 仮想 IP アドレスを指定します。IPv6 仮想 IP アドレスも指定できますが、これは必須ではありません。

次の手順では、プライマリ サーバーに HA を登録する方法について説明します。HA を再登録する場合にも、以下と同じ手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Prime Infrastructure にログインします。

ステップ 2 メニューから、**[管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]** の順に選択します。Prime Infrastructure に [HA ステータス（HA status）] ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択し、次のフィールドに入力します。

1. [セカンダリ サーバー（Secondary Server）]：セカンダリ サーバーの IP アドレスまたはホスト名を入力します。
2. [認証キー（Authentication Key）]：セカンダリ サーバーのインストール中に設定したパスワードを認証キーとして入力します。

3. [電子メール アドレス（Email Address）]：HA の状態変更に関する通知の送信先アドレス（またはコンマで区切ったアドレスのリスト）を入力します。[メール サーバー設定（Mail Server Configuration）] ページで電子メール通知をすでに設定している場合（「電子メール サーバー設定の構成」参照）、ここに入力するメール アドレスは、メール サーバーですでに設定されているアドレスのリストに追加されます。
4. [フェールオーバー タイプ（Failover Type）]：[手動（Manual）] または [自動（Automatic）] を選択します。[手動（Manual）] を選択することが推奨されます。

ステップ 4 仮想 IP 機能を使用する場合：[仮想 IP の有効化（Enable Virtual IP）] チェックボックスをオンにし、追加フィールドに次のように入力します。

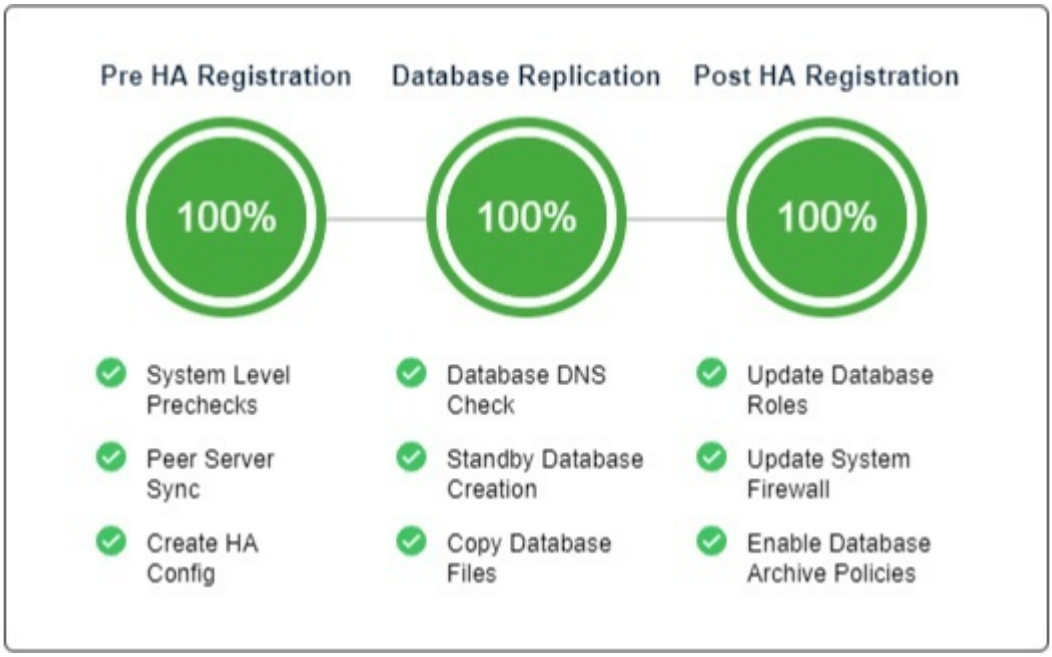
1. [IPV4 仮想 IP（IPV4 Virtual IP）]：両方の HA サーバーに使用する仮想 IPv4 アドレスを入力します。
2. [IPV6 Virtual IP]：（オプション）両方の HA サーバーに使用する仮想 IPv6 アドレスを入力します。

両方のサーバーが同一サブネット上にない場合は、仮想 IP アドレッシングは機能**しない**ことに注意してください。IPV6 アドレス ブロック fe80 は、リンクローカル ユニキャスト アドレッシング用に予約されているため使用しないでください。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックし、HA 関連の環境パラメータが設定を行える状態になっているか確認します。

詳細については、「HA 登録/設定の準備状況の確認」を参照してください。

ステップ 6 [登録（Register）] をクリックしてマイルストーン進行状況バーを表示し、以下に示すように、プレ HA 登録、データベース レプリケーション、およびポスト HA 登録が 100% 完了していることを確認します。Prime Infrastructure により HA 登録プロセスが開始されます。登録が正常に完了すると、[コンフィギュレーション モード（Configuration Mode）] に、[プライマリ アクティブ（Primary Active）] という値が表示されます。



詳細については、電子メール サーバー設定の構成 （472 ページ）を参照してください。

関連トピック

HA セカンダリ サーバーのインストール方法 （361 ページ）
自動フェールオーバーと手動フェールオーバーの違い （355 ページ）
HA での仮想 IP アドレッシングの使用 （348 ページ）
ハイ アベイラビリティをセットアップする前に （359 ページ）
HA 登録中の動作 （367 ページ）
ハイ アベイラビリティのセットアップ （359 ページ）
HA の登録/設定の準備状況の確認 （364 ページ）

HA の登録/設定の準備状況の確認

HA 登録時に、HA に関連する他の環境パラメータ（システム仕様、ネットワーク構成、サーバー間の帯域幅など）によって HA 設定が決定されます。

約 15 のチェックがシステム内で実行されて、エラーや障害が発生することなく HA 設定が完了したことが確認されます。準備状況の確認機能を実行すると、チェックリストの名前および対応するステータスが、該当する場合は推奨事項とともに表示されます。

HA 設定の準備状況を確認するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID とパスワードを使用して Prime Infrastructure にログインします。

ステップ 2 メニューから、**[管理（Administration）]**>**[設定（Settings）]**>**[ハイ アベイラビリティ（High Availability）]** の順に選択します。Prime Infrastructure に [HA ステータス（HA status）] ページが表示されます。

ステップ 3 [HA 設定（HA Configuration）] を選択します。

ステップ 4 [セカンダリ サーバー（Secondary Server）] フィールドにセカンダリ サーバーの IP アドレスを入力し、[認証キー（Authentication Key）] フィールドのセカンダリの認証キーを入力します。

ステップ 5 [準備状況の確認（Check Readiness）] をクリックします。

ポップアップ ウィンドウが開き、システム仕様およびその他のパラメータが表示されます。画面には、チェックリスト項目の名前、ステータス、影響、推奨事項の詳細が示されます。

その下に、準備状況の確認に使用されたチェックリストのテスト名と説明のリストが表示されます。

表 *14*：チェックリストの名前と説明

チェックリストのテスト名	テストの説明
システム - CPU 数の確認（SYSTEM - Check CPU Count）	プライマリサーバーとセカンダリサーバーの CPU 数を検証します。 プライマリ サーバーの CPU 数は、セカンダリ サーバーの CPU 数以下の場合があります。

データベース - リスナーのステータス（DATABASE - LISTENER STATUS）	データベースのリスナーがプライマリ サーバーとセカンダリ サーバーの両方で稼働中であるかどうかを確認します。 障害が発生した場合、テストが再起動されてステータスが報告されます。 wcs インスタンスのすべてが oracle「listener.ora」ファイル内にあるかどうかを確認します。このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
データベース - メモリターゲットの確認（DATABASE - CHECK MEMORY TARGET）	HA セットアップの「/dev/shm」データベースのメモリ ターゲット サイズを確認します。
データベース - リスナー設定ファイルの破損確認（DATABASE - CHECK LISTENER CONFIG CORRUPTION）	すべてのデータベース インスタンスがデータベース リスナー設定に存在することを確認します。 このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
システム - ヘルス モニターのステータス（SYSTEM - HEALTH MONITOR STATUS）	ヘルス モニター プロセスがプライマリ サーバーとセカンダリ サーバーの両方で実行されていることを確認します。
システム - ディスク IOPS の確認（SYSTEM - CHECK DISK IOPS）	プライマリ サーバーとセカンダリ サーバーの両方でディスク IOPS を検証します。 必要な最小ディスク IOPS は 200 Mbps です。
ネットワーク - データベース ポートの開閉についてファイアウォールの確認（NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY）	データベース ポート 1522 がシステム ファイアウォールでオープンになっていることを確認します。 このポートが無効になっていると、テストは iptables リストで 1522 の権限を付与します。
ネットワーク - ネットワーク インターフェイスの帯域幅確認（NETWORK - CHECK NETWORK INTERFACE BANDWIDTH）	プライマリ サーバーとセカンダリ サーバーの両方で eth0 インターフェイス速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバー間でのデータ送信によるネットワーク帯域幅の測定は行いません。
ネットワーク - ネットワーク帯域幅速度の確認（NETWORK - CHECK NETWORK BANDWIDTH SPEED）	プライマリ サーバーとセカンダリ サーバーの両方でネットワーク帯域幅速度が推奨速度の 100 Mbps と一致するかどうかを確認します。 このテストでは、プライマリ サーバーとセカンダリ サーバーの間でデータを送信することによってネットワーク帯域幅を測定します。

データベース - オンラインステータスの確認（DATABASE - CHECK ONLINE STATUS）	プライマリ サーバーとセカンダリ サーバーの両方でデータベース ファイルのステータスがオンラインでアクセス可能であることを確認します。
データベース - TNS 設定ファイルの破損確認（DATABASE - CHECK TNS CONFIG CORRUPTION）	プライマリ サーバーとセカンダリ サーバーの両方で tnsping が成功するかどうかを検証します。
データベース - TNS 到達可能性のステータス（DATABASE - TNS REACHABILITY STATUS）	wcs インスタンスのすべてが oracle「listener.ora」ファイル内にあるかどうかを確認します。 このテストはプライマリ サーバーとセカンダリ サーバーの両方で実行されます。
データベース - スタンバイデータベースインスタンスの検証（DATABASE - VALIDATE STANDBY DATABASE INSTANCE）	スタンバイ データベース インスタンス（stbywcs）がプライマリ サーバーとセカンダリ サーバーの両方で使用できるかどうかを検証します。
システム - RAM サイズの確認（SYSTEM - CHECK RAM SIZE）	プライマリ サーバーのディスク サイズがセカンダリ サーバーのディスク サイズ以下かどうかを確認します。
システム - サーバーへの ping 確認（SYSTEM - CHECK SERVER PING REACHABILITY）	プライマリ サーバーがリモート（セカンダリ）サーバーとの ping チェックを実行できることを確認します。

ステップ 6 すべてのパラメータのチェックが完了したら、パラメータのステータスを確認し、[クリア（Clear）] をクリックしてウィンドウを閉じます。

（注） 準備状況の確認中の検証フェールバックおよびフェールオーバー イベントは [アラームおよびイベント（Alarms and Events ）] ページに送信されますが、登録失敗イベントは [アラームおよびイベント（Alarms and Events ）] ページに表示されません。

ハイ アベイラビリティ ステータスの確認

Prime Infrastructure サーバー上で有効になっているハイ アベイラビリティのステータスを確認できます。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 2 次のコマンドを入力して、Prime Infrastructure HA プロセスの現在のステータスを表示します。

PIServer/admin# **ncs ha status**

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）

HA 登録中の動作

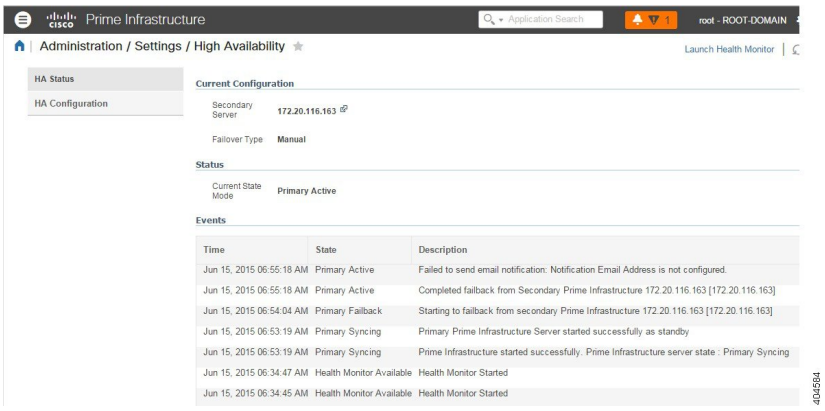
[HA 設定（HA Configuration）] ページで設定情報の入力を完了して [保存（Save）] をクリックすると、プライマリおよびセカンダリ HA サーバーが互いを登録し、プライマリ サーバーからセカンダリ サーバーにすべてのデータベースおよび構成データをコピーするプロセスが開始されます。

コピーが完了するまでの時間は、複製するデータベースおよび構成データの量と、2 台のサーバー間のネットワーク リンクで使用可能な帯域幅によって異なります。データの量が多かったり、リンクの速度が遅かったりすると、レプリケーションにもそれだけ時間がかかります。比較的新しいサーバー（数日しか稼動していないサーバー）の場合、デバイス数が 100 で、リンク速度が 1 Gbps だとすると、コピーには約 25 分かかります。

HA の登録中に、プライマリ サーバーとセカンダリ サーバーの状態は以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA not Configured	元の状態：HA not Configured
次の状態：HA Initializing	次の状態：HA Initializing
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

これらの状態変更は、プライマリ サーバーの [HA Status] ページまたは 2 台のサーバーのいずれかの Health Monitor Web ページで確認できます。[HA ステータス（HA Status）] ページを使用している場合は、[更新（Refresh）] をクリックすると、進行状況が表示されます。データが完全に同期すると、次の図に示すように、[HA ステータス（HA Status）] ページが更新され、現在の状態として [プライマリ アクティブ（Primary Active）] が表示されます。



登録が開始されると、Prime Infrastructure により、プライマリおよびセカンダリ HA サーバー間の同期が開始されます。同期によってユーザーアクティビティに影響が及ぶことはありませんが、同期が完了するまでは、ユーザーがシステム応答速度が低下したと感じる場合がありま

す。同期の所要時間は、データベースの合計サイズによって決まります。同期は、RMANおよびData Guard Brokerのプロセスによって Oracle データベース レベルで処理されます。同期中、ユーザーまたはシステム関連のアクティビティの実行への影響はありません。

登録時に、Prime Infrastructure はセカンダリ サーバーに完全なデータベースを複製します。セカンダリ サーバー上のすべてのプロセスが実行されますが、サーバー自体はパッシブ モードになります。セカンダリ サーバーが「セカンダリ同期中（Secondary Syncing）」状態のときに、Prime Infrastructure の CLI コマンド **ncs status** をセカンダリ サーバー上で実行すると、コマンド出力にはすべてのプロセスが実行中として表示されます。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
HA の導入計画 （350 ページ）
ハイ アベイラビリティのセットアップ （359 ページ）

HA サーバーにパッチを適用する方法

状況に応じて、次の方法のいずれかでHA サーバーの UBF パッチのダウンロードとインストールを行います。

- 現在ペアリングされていない HA サーバーにパッチをインストールします。Prime Infrastructure の HA が設定されていない場合は、この方法が推奨されます。
- 手動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。HA がすでに設定されている場合はこの方法が推奨されます。
- 自動フェールオーバーを使用して、ペアリングされている既存の HA サーバーにパッチをインストールします。

それぞれの方法の詳細については、「関連項目」を参照してください。

関連トピック

新しい HA サーバーへのパッチ適用方法 （368 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法（371 ページ）
自動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチを適用する方法 （373 ページ）

新しい HA サーバーへのパッチ適用方法

新しい Prime Infrastructure ハイ アベイラビリティ（HA）実装をセットアップするが、新しいサーバーが同一パッチ レベルではない場合には、次の手順に従って両方のサーバーにパッチをインストールし、同じパッチ レベルにします。

ステップ 1 パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[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）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
i) プライマリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 2 セカンダリ サーバーに同じパッチをインストールします。

a) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

（注） ユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

（注） HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

b) ユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。
c) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。
d) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

i) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 3 両方のサーバーのパッチ ステータスが同一であることを次のように確認します。

a) 上記のステップ 1 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

b) 上記のステップ 2 と同じ方法でセカンダリ サーバーのヘルス モニター Web ページにアクセスします。インストールされているすべてのパッチの [ステータス（Status）] 列で [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 サーバーを登録します。

詳細については、「Cisco Prime Infrastructure 用ソフトウェア パッチのリスト」、「CLI を使用した Prime Infrastructure の再起動」および「Prime Infrastructure サーバーのステータスの確認」を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
HA サーバーにパッチを適用する方法 （368 ページ）

ペアリング済み HA サーバーへのパッチ適用方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

ペアリング済み HA サーバーへのパッチの適用はサポートされていません。HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されます。そのため、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しい HA サーバーのパッチ適用方法」の手順に従ってパッチを適用します。
3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」の手順に従ってください。

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
ハイ アベイラビリティ ステータスの確認 （366 ページ）
GUI での HA の削除 （396 ページ）
新しい HA サーバーへのパッチ適用方法 （368 ページ）

手動フェールオーバー用に設定されているペアリング済みHAサーバーのパッチ適用方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

パッチのインストールは、[プライマリ アクティブ（Primary Active）] 状態のプライマリ サーバー、および[セカンダリ同期中（Secondary Syncing）] 状態のセカンダリ サーバーで開始する必要があります。

手動フェールオーバー用に設定されているプライマリおよびセカンダリ HA サーバーのパッチ適用は約 30 分かかります。フェールオーバーとフェールバックは必要ではありません。プライマリ HA サーバーとセカンダリ HA サーバーにパッチを適用するには、約 30 分かかります。プライマリ パッチのインストール再起動時のダウンタイムは 15 ～ 20 分です。

場合によっては、HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されることがあります。その場合、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。この場合、この手順のステップを使用できません。代わりに、次の手順に従います。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しい HA サーバーのパッチ適用方法」の手順に従ってパッチを適用します。

（注） HA が有効になっている場合は、ユーザー名と認証キーの入力が求められます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」の手順に従ってください。

ステップ 1 HA 実装が有効になっていて、更新できる状態であることを確認します。

a) 管理者特権を持つ ID を使用して、プライマリ サーバーにログインします。

b) [Administration] > [Settings] > [High Availability] を選択します。[HA Status] ページに表示されるプライマリ サーバーの状態が [Primary Active] になっているはずです。

c) [HA 設定（HA Configuration）] を選択します。現在の [Configuration Mode] が、[HA Enabled] になります。パッチのインストール中にフェールオーバー タイプを [manual] に設定することを推奨します。

d) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

e) HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

ステップ 2 HA を有効にしたときに入力したユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

ステップ 3 UBF パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[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）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（Upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
h) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
i) プライマリ サーバーの再起動が完了した後、[管理（Administration）] > [設定（Settings）] > [ハイ アベイラビリティ（High Availability）] を選択します。[HA ステータス（HA Status）] ページに表示されるプライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）] です。
j) [ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、パッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 4 プライマリ サーバーにパッチを適用したら、同じパッチをセカンダリ サーバーにもインストールします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。
b) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。
c) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。
d) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
e) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
f) パッチ ファイルを選択し、[インストール（Install）] をクリックします。
g) 警告ポップアップで、[はい（Yes）] をクリックします。インストールが完了すると、サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。
h) セカンダリ サーバーが再起動したら、セカンダリ HM ページ（https://serverIP:8082）にログインして、HM Web ページに表示されているセカンダリ サーバーの状態が「セカンダリ同期中（Secondary Syncing）」であることを確認します。

i) [ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、パッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

ステップ 5 サーバーが再起動したら、以下の手順でパッチのインストールを確認します。

a) 上記のステップ 2 と同じ方法でプライマリ サーバーにログインし、[ソフトウェアアップデート（Software Update）] ページにアクセスします。[Status of Updates] > [Update] タブの [Status] 列に、パッチのステータスが [Installed] と表示されている必要があります。

b) 上記のステップ 3 と同じ方法でセカンダリ サーバーの [Software Update] ページにアクセスします。[アップデートのステータス（Status of Updates）]>[アップデート（Updates）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

詳細については、次を参照してください。

- Cisco Prime Infrastructure のソフトウェア パッチのリスト。
- Prime Infrastructure の起動 （148 ページ）
- Prime Infrastructure の停止 （149 ページ）
- Prime Infrastructure サーバーのステータスの確認 （148 ページ）

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
ハイ アベイラビリティ ステータスの確認 （366 ページ）
GUI での HA の削除 （396 ページ）
新しい HA サーバーへのパッチ適用方法 （368 ページ）
自動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチを適用する方法 （373 ページ）

自動フェールオーバー用に設定されているペアリング済みHAサーバーのパッチを適用する方法

現在の Prime Infrastructure 実装に含まれているハイ アベイラビリティ サーバーのパッチ レベルが同一ではない場合、または両方の HA サーバーに適用する必要がある新しいパッチがある場合は、次の手順を実行します。

パッチのインストールは、[プライマリ アクティブ（Primary Active）] 状態のプライマリ サーバー、および [セカンダリ同期中（Secondary Syncing）] 状態のセカンダリ サーバーで開始する必要があります。

自動フェールオーバー用に設定されているプライマリおよびセカンダリ HA サーバーのパッチ適用は約 1 時間かかります。また、フェールオーバーとフェールバックの両方が必要です。フェールオーバーとフェイルバックによるダウンタイムは 10 ～ 15 分です。

場合によっては、HA が設定されている状態では Prime Infrastructure サーバーのアップデートが実行できないことを示すポップアップ エラー メッセージが表示されることがあります。その場合、パッチを適用する前に、まずプライマリおよびセカンダリ サーバーを接続解除しなければなりません。この場合、この手順のステップを使用できません。代わりに、次の手順に従います。

1. 「GUI での HA の削除」の手順（「関連項目」を参照）に従って、プライマリ サーバーとセカンダリ サーバーとの接続を切断します。
2. 「新しいHAサーバーへのパッチ適用方法」（「関連項目」を参照）の手順に従って、パッチを適用します。
3. HA の設定を復元するには、「ハイ アベイラビリティのセットアップ」（「関連項目」を参照）の手順に従ってください。

ステップ 1 HA 実装が有効になっていて、更新できる状態であることを確認します。

a) 管理者特権を持つ ID を使用して、プライマリ サーバーにログインします。
b) [Administration] > [Settings] > [High Availability] を選択します。[HA Status] ページに表示されるプライマリ サーバーの状態が [Primary Active] になっているはずです。
c) [HA 設定（HA Configuration）] を選択します。現在の [Configuration Mode] が、[HA Enabled] になります。
d) ブラウザで以下の URL にアクセスして、セカンダリ サーバーの Health Monitor（HM）Web ページを表示します。

https://*ServerIP***:8082**

ここで、*ServerIP* はセカンダリ サーバーの IP アドレスまたはホスト名です。

e) HA を有効にしたときに入力したユーザー名と認証キーの入力を求めるプロンプトが表示されます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。
f) HM Web ページに表示されるセカンダリ サーバーの状態が [セカンダリ同期中（Secondary Syncing）] となっていることを確認します。

ステップ 2 UBF パッチをダウンロードして、プライマリ サーバーにインストールします。

a) ブラウザで Cisco Prime Infrastructure 用ソフトウェア パッチのリストにアクセスします（「関連項目」を参照）。
b) インストールする必要があるパッチ ファイル（UBF ファイル拡張子で終わるファイル）に対応する [ダウンロード（Download）] ボタンをクリックし、そのファイルをローカルに保存します。
c) 管理者特権を持つ ID を使用してプライマリ サーバーにログインし、[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）] > [ソフトウェア アップデート（Software Update）] を選択します。
d) ページ上部の [アップロード（upload）] リンクをクリックし、パッチ ファイルの保存場所に移動します。
e) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。
f) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。
g) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

h) 警告ポップアップで、[はい（Yes）] をクリックします。フェールオーバーがトリガーされ、プライマリ サーバーが自動的に再起動します。フェールオーバーが完了するまでに 2 ～ 4 時間かかります。フェールオーバーが完了すると、セカンダリ サーバーは「セカンダリ アクティブ（Secondary Active）」状態になります。

i) プライマリ サーバーが再起動したら、**ncs status** コマンドを実行（「Prime Infrastructure サーバー ステータスの確認」を参照）して、プライマリ サーバーのプロセスが再開したことを確認します。続行する前に：プライマリ サーバーの HM Web ページにアクセスし、表示されたプライマリ サーバーの状態が「プライマリ同期中（Primary Synching）」であることを確認します。

ステップ 3 セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーにフェールバックします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。

b) [Failback] をクリックして、セカンダリ サーバーからプライマリ サーバーへのフェールバックを開始します。動作が完了するまで2～3分かかります。フェールバックが完了するとすぐに、セカンダリ サーバーは自動的にスタンバイ モードで再起動します。再起動が完了するまでに最大15分間かかります。そして、プライマリ サーバーと同期されます。

再起動の確認は、セカンダリ サーバーの HM Web ページにログインし、[Prime Infrastructure は正常に起動しました（Prime Infrastructure stopped successfully）]、および [Prime Infrastructure は正常に停止しました（Prime Infrastructure started successfully）] というメッセージを探すことで行えます。

フェールバックが完了した後、プライマリ サーバーの状態が「プライマリ アクティブ（Primary Active）」に変更されます。

c) 続行する前に：プライマリ サーバーとセカンダリ サーバーの両方で **ncs ha status** コマンドを実行します。プライマリ サーバーの状態が「プライマリ アクティブ（Primary Active）」に変わり、セカンダリ サーバーの状態が「セカンダリ同期中（Secondary Synching）」であることを確認します。

ステップ 4 フェールバックが完了したら、プライマリ サーバーに上記にログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスして、パッチのインストールを確認します（上記のステップ 2 と同様です）。[アップデートのステータス（Status of Updates）] > [アップデート（Update）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

ステップ 5 プライマリ サーバーにパッチを適用したら、同じパッチをセカンダリ サーバーにもインストールします。

a) セカンダリ サーバーの HM Web ページにアクセスし、必要に応じてログインします。

b) HM Web ページの [Software Update] リンクをクリックします。再び、認証キーの入力を求めるプロンプトが出されます。パスワードを入力し、[Login] を再びクリックします。

c) [アップデート ファイルのアップロード（Upload Update File）] をクリックし、パッチ ファイルを保存した場所を参照します。

d) UBF ファイルを選択し、[OK] をクリックしてファイルをアップロードします。

e) アップロードが完了したら、[ソフトウェア アップロード（Software Upload）] ページで、パッチ ファイルの名前、公開日と説明が正しいことを確認します。

f) パッチ ファイルを選択し、[インストール（Install）] をクリックします。

g) 警告ポップアップで、[はい（Yes）] をクリックします。サーバーが自動的に再起動します。再起動には通常 15 ～ 20 分かかります。

h) セカンダリ サーバーでのインストールが完了したら、[ソフトウェア アップデート（Software Update）] ページの [アップデートのステータス（Status of Updates）] 表で、このパッチのステータスが [インストール済み（Installed）] と表示されていることを確認します。

i) セカンダリ サーバーが再起動したら、セカンダリ HM ページにログインして、HM Web ページに表示されているセカンダリ サーバーの状態が「セカンダリ同期中（Secondary Syncing）」であることを確認します。

ステップ 6 サーバーが再起動したら、以下の手順でパッチのインストールを確認します。

a) 上記のステップ 2 と同じ方法でプライマリ サーバーにログインし、[ソフトウェア アップデート（Software Update）] ページにアクセスします。[Status of Updates] > [Update] タブの [Status] 列に、パッチのステータスが [Installed] と表示されている必要があります。

b) 上記のステップ 5 と同じ方法でセカンダリ サーバーの [ソフトウェア アップデート（Software Update）] ページにアクセスします。[アップデートのステータス（Status of Updates）]>[アップデート（Updates）] タブの [ステータス（Status）] 列に、パッチのステータスが [インストール済み（Installed）] と表示されている必要があります。

詳細にういては、「Cisco Prime Infrastructure 用ソフトウェア パッチのリスト」、「Prime Infrastructure の停止」、「Prime Infrastructure の起動」および「Prime Infrastructure サーバーのステータスの確認」を参照してください。

関連トピック

ハイ アベイラビリティのセットアップ （359 ページ）
ハイ アベイラビリティ ステータスの確認 （366 ページ）
GUI での HA の削除 （396 ページ）
新しい HA サーバーへのパッチ適用方法 （368 ページ）
手動フェールオーバー用に設定されているペアリング済み HA サーバーのパッチ適用方法 （371 ページ）

ハイ アベイラビリティのモニター

HA を設定し、それをプライマリ サーバー上で登録した後、HA とのやり取りでは、ほとんどの場合、サーバーの Health Monitor Web ページにアクセスし、フェールオーバーまたはフェールバックをトリガーして電子メールでの通知に応答することになります。これらのプロセスおよび複雑な応答を必要とする特別な状況について、次の「関連項目」で説明しています。

関連トピック

ヘルス モニター Web ページへのアクセス （377 ページ）
フェールオーバーのトリガー方法 （377 ページ）
フェールバックのトリガー方法 （378 ページ）
フェールオーバーの強制実行 （379 ページ）
その他の HA イベントに対する応答 （380 ページ）

ヘルス モニター Web ページへのアクセス

プライマリ サーバーとセカンダリ サーバーの Health Monitor Web ページにアクセスするには、ブラウザで次の URL を開きます。

https://**Server**:8082

ここで、**Server** は、Health Monitor Web ページを表示する対象のプライマリ サーバーまたはセカンダリ サーバーの IP アドレスまたはホスト名です。

（注） ユーザー名と認証キーの入力を求められます。ユーザー名を「root」として認証キーとともに入力し、[ログイン（Login）] をクリックします。

現在アクティブなサーバーのヘルス モニター Web ページにアクセスするには、Prime Infrastructure にログインして [管理（Administration）] > [設定（Settings）] > [ハイ アベイラビリティ（High Availability）] を選択し、[HA ステータス（HA Status）] ページの右上にある [ヘルス モニターの起動（Launch Health Monitor）] リンクをクリックします。

関連トピック

ハイ アベイラビリティのモニター （376 ページ）
フェールオーバーのトリガー方法 （377 ページ）
フェールバックのトリガー方法 （378 ページ）
フェールオーバーの強制実行 （379 ページ）

フェールオーバーのトリガー方法

フェールオーバーとは、プライマリ サーバーで検出された障害への対応として、セカンダリ サーバーをアクティブ化するプロセスのことです。

Health Monitor（HM）は、2 台のサーバー間で交換されるハートビート メッセージを使用して障害状態を検出します。プライマリ サーバーがセカンダリ サーバーから送信されるハートビート メッセージに 3 回連続して応答しない場合、プライマリ サーバーに障害が発生したと見なされます。ヘルス チェック中に、HM はアプリケーション プロセスのステータスおよびデータベースのヘルスもチェックします。これらのチェックに対して適切な応答がない場合は、アプリケーション プロセスやデータベースも障害が発生しているとして処理されます。

HA システムがプライマリ サーバーでのプロセス障害を検出してフェールオーバーを開始するまでには、約 10 秒から 15 秒かかります。ネットワークの問題によってセカンダリ サーバーがプライマリ サーバーに接続できない場合は、フェールオーバーを開始するまでに、さらに長い時間がかかることがあります。また、セカンダリ サーバーでのアプリケーション プロセスが完全に機能するようになるまでにも時間がかかることがあります。

HM は障害を検知するとすぐに、電子メールでの通知を送信します。この E メールには、障害ステータスに加え、セカンダリ サーバーの Health Monitor Web ページへのリンクも記載されます。

HA が自動フェールオーバーを行うよう設定されている場合は、セカンダリ サーバーが自動的にアクティブ化されるため、ユーザーが実行しなければならないアクションはありません。

HA が手動フェールオーバー用に設定されている場合は、以下の手順に従ってフェールオーバーをトリガーする必要があります。

フェールオーバーは、一時的なものであると見なす必要があります。障害が発生したプライマリ Prime Infrastructure インスタンスをできるだけ早く復旧して、フェールバックを再開する必要があります。

ステップ 1 電子メールでの通知に記載されている Web リンクを使用するか、または「Health Monitor Web ページへのアクセス」の手順に従って、セカンダリ サーバーの Health Monitor Web ページにアクセスします。

ステップ 2 [フェールオーバー（Failover）] ボタンをクリックしてフェールオーバーをトリガーします。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
フェールバックのトリガー方法 （378 ページ）
ハイ アベイラビリティのモニター （376 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）

フェールバックのトリガー方法

フェールバックとは、オンライン状態に戻ったプライマリ サーバーをアクティブ化するプロセスのことです。また、このプロセスでは、アクティブ ステータスをセカンダリ サーバーからプライマリ サーバーに移して、セカンダリ サーバーでのアクティブなネットワーク モニタリング プロセスを停止します。

フェールバック中は、プロセスがセカンダリ サーバー上で再開される期間を除き、セカンダリ サーバーを使用できます。両方のサーバーの Health Monitor Web ページにアクセスして、フェールバックの進行状態をモニターすることができます。さらに、ユーザーはセカンダリ サーバーに接続して、通常のすべての機能を使用することもできます。ただし、その場合は以下の注意事項があります。

- フェールバックの進行中は、設定またはプロビジョニングのアクティビティを開始しないでください。
- フェールバックが正常に完了すると、セカンダリ サーバーがパッシブ（「セカンダリ同期中（Secondary Syncing）」）モードに移行して、制御がプライマリ サーバーに切り替わることに注意してください。このプロセス中は、しばらくの間、ユーザーが Prime Infrastructure にアクセスできなくなります。

フェールバックは常に、手動でトリガーする必要があります。それには、以下の手順に従います。

ステップ 1 電子メールでの通知に記載されているリンクを使用するか、または「Health Monitor Web ページへのアクセス」の手順に従って、セカンダリ サーバーの Health Monitor Web ページにアクセスします。

ステップ 2 [Failback] ボタンをクリックしてフェールバックをトリガーします。

セカンダリ サーバーは、フェールバック後に自動的にスタンバイ モードで再起動され、自動的にプライマリ サーバーと同期されます。プライマリ サーバーが Prime Infrastructure サーバーとして利用可能になります。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
フェールオーバーのトリガー方法 （377 ページ）
フェールオーバーの強制実行 （379 ページ）
ハイ アベイラビリティのモニター （376 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）

フェールオーバーの強制実行

強制フェールオーバーは、プライマリ サーバーが稼働している間に、セカンダリ サーバーをアクティブにするプロセスです。このオプションは、たとえば、HA セットアップは完全に機能しているかどうかをテストする場合に使用します。

強制フェールオーバーを使用できるのは、プライマリがアクティブで、セカンダリが「セカンダリ同期中（Secondary Syncing）」状態であり、すべてのプロセスが両方のサーバーで実行中の場合に限られます。プライマリ サーバーがダウンしている場合、強制フェールオーバーは無効になります。この状況では、通常のフェールオーバーのみが有効です。

強制フェールオーバーが完了すると、セカンダリ サーバーがアクティブになり、プライマリ サーバーは自動的にスタンバイ状態で再起動します。通常のフェイルバックをトリガーすると、元の通りプライマリ サーバーがアクティブになり、セカンダリ サーバーがスタンバイ状態になります。

ステップ 1 「ヘルス モニター Web ページへのアクセス」の手順に従って、セカンダリ サーバーのヘルス モニター Web ページにアクセスします。

ステップ 2 [強制フェールオーバー（Force Failover）] ボタンをクリックして強制フェールオーバーをトリガーします。強制フェールオーバーは 2 ～ 3 分で完了します。

関連トピック

ハイ アベイラビリティの仕組み （341 ページ）
フェールオーバーのトリガー方法 （377 ページ）
フェールバックのトリガー方法 （378 ページ）
ハイ アベイラビリティのモニター （376 ページ）

プライマリ サーバーでの HA の登録方法 （362 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）

その他の HA イベントに対する応答

HA 関連のすべてのイベントは、[HA ステータス（HA Status）] ページ、ヘルス モニター Web ページ、および Prime Infrastructure の [アラームおよびイベント（Alarms and Events）] ページに表示されます。ほとんどのイベントには、オペレータの応答は不要ですが、フェールオーバーおよびフェールバックのトリガーは例外です。「関連項目」で説明するように、複雑なイベントもいくつかあります。

関連トピック

HA 登録が失敗した場合 （380 ページ）
ネットワークがダウンしている場合（自動フェールオーバー） （381 ページ）
ネットワークがダウンしている場合（手動フェールオーバー） （382 ページ）
プロセスをリスタートできない場合（手動フェールオーバー） （385 ページ）
同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー） （386 ページ）
同期中にセカンダリ サーバーが再起動した場合 （386 ページ）
HA サーバーが両方ともダウンしている場合 （387 ページ）
HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （388 ページ）
プライマリ MSE の交換 （418 ページ）
スプリット ブレイン シナリオからの回復方法 （390 ページ）

HA 登録が失敗した場合

HA 登録が失敗すると、サーバーごとの HA 状態が、（「HA 登録中の動作」で説明したように変更されるのではなく）以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA Initializing	元の状態：HA Initializing
次の状態：HA not Configured	次の状態：HA not Configured

HA 登録の失敗から回復するには、次の手順に従います。

ステップ 1 ping または他のツールを使用して、2 台の Prime Infrastructure サーバー間のネットワーク接続を確認します。プライマリ サーバーからセカンダリ サーバーに接続できること、その逆も可能であることを確認します。

ステップ 2 ゲートウェイ、サブネットマスク、仮想IPアドレス（設定されている場合）、サーバーのホスト名、DNS、NTP 設定がすべて正しいことを確認します。

ステップ 3 設定された DNS および NTP サーバーにプライマリ サーバーとセカンダリ サーバーから接続可能であること、そして DNS および NTP サーバーの両方が遅延や他のネットワーク固有の問題を伴うことなく応答していることを確認します。

ステップ 4 すべての Prime Infrastructure ライセンスが正しく設定されていることを確認します。

ステップ 5 接続または設定の問題を解決したら、関連トピックの「プライマリ サーバーでのハイ アベイラビリティの登録方法」の手順を再試行します。

関連トピック

その他の HA イベントに対する応答 （380 ページ）
HA 登録中の動作 （367 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）

ネットワークがダウンしている場合（自動フェールオーバー）

フェールオーバー タイプが [自動（Automatic）] に設定されている場合、2 台の Prime Infrastructure サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Lost Secondary	次の状態：Secondary Failover
次の状態：Primary Lost Secondary	次の状態：[セカンダリ アクティブ（Secondary Active）]

セカンダリ サーバーがアクティブであることを示す電子メール通知を受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出できるようになったら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Active
次の状態：Primary Failover	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （380 ページ）
フェールバックのトリガー方法 （378 ページ）

ネットワークがダウンしている場合（手動フェールオーバー）

フェールオーバー タイプが [手動（Manual）] に設定されている場合、2 台の Prime Infrastructure サーバー間のネットワーク接続が失われると、それぞれのサーバーの HA 状態が以下のように遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

各サーバーがもう一方のサーバーを失ったことを通知する電子メールを受信します。

ステップ 1 2 台のサーバー間のネットワーク接続を確認し、必要に応じて復元します。

ネットワーク接続が復元されると、次ように状態が遷移します。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Lost Primary
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は不要です。

ステップ 2 何らかの理由でネットワーク接続を復元できない場合は、セカンダリ サーバーの HM Web ページを使用して、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Lost Primary
次の状態：Primary Lost Secondary	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

セカンダリ サーバーがアクティブになったことを通知する電子メールを受信します。

ステップ 3 2台のサーバー間のネットワーク接続を確認し、復元します。ネットワーク接続が復旧し、セカンダリ サーバーがアクティブなことをプライマリ サーバーが検出したら、プライマリ サーバー上のすべてのサービスが自動的に再開し、パッシブ状態になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Lost Secondary	元の状態：Secondary Active
次の状態：Primary Failover	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 4 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。

以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （380 ページ）
フェールバックのトリガー方法 （378 ページ）

プロセスを再開できない場合（自動フェールオーバー）

Prime Infrastructure のヘルス モニター プロセスは、失敗した Prime Infrastructure サーバー プロセスのリスタートを試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。

HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。現在設定されているフェールオーバー タイプが [automatic] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Uncertain	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Failover	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

このプロセスが完了すると、セカンダリ サーバーがアクティブになったことを通知する電子メールでの通知を受信します。

ステップ 1 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、その状態は [Primary Syncing] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Failover	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Preparing for Failback	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 2 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （380 ページ）
フェールバックのトリガー方法 （378 ページ）

プロセスをリスタートできない場合（手動フェールオーバー）

Prime Infrastructure のヘルス モニター プロセスは、失敗した Prime Infrastructure サーバー プロセスのリスタートを試行します。通常、そのような障害が発生した時点でのプライマリ サーバーとセカンダリ サーバーの状態は、[プライマリ アクティブ（Primary Active）] および [セカンダリ同期中（Secondary Syncing）] となっているはずです。HM がプライマリ サーバーで重要なプロセスを再開できない場合は、プライマリ サーバーは障害が発生したものとみなされます。その場合、障害を通知する電子メールを受信します。現在設定されているフェールオーバー タイプが [Manual] の場合、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Uncertain	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]

ステップ 1 セカンダリ サーバーで、プライマリ サーバーからセカンダリ サーバーへのフェールオーバーをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Uncertain	元の状態：Secondary Syncing
次の状態：Primary Failover	次の状態：Secondary Failover
次の状態：Primary Failover	次の状態：Secondary Active

ステップ 2 プライマリ サーバーを再起動し、稼働していることを確認します。プライマリ サーバーが再起動すると、プライマリ サーバーの HA 状態は [Primary Syncing] になります。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Failover	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Preparing for Failback	次の状態：Secondary Active
次の状態：Primary Syncing	次の状態：Secondary Active

ステップ 3 セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーします。以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Syncing	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

その他の HA イベントに対する応答 （380 ページ）
フェールオーバーのトリガー方法 （377 ページ）
フェールバックのトリガー方法 （378 ページ）

同期中にプライマリ サーバーが再起動した場合（手動フェールオーバー）

セカンダリ サーバーとの同期中に Prime Infrastructure サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Alone	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

[Primary Alone] および [Primary Active] 状態への遷移は、プライマリ サーバーがオンライン状態に戻った直後に行われます。管理者による応答は必要ありません。

関連トピック

その他の HA イベントに対する応答 （380 ページ）

同期中にセカンダリ サーバーが再起動した場合

プライマリ サーバーとの同期中にセカンダリ Prime Infrastructure サーバーが再起動された場合は、以下の状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：Primary Active	元の状態：Secondary Syncing
次の状態：Primary Lost Secondary	元の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

管理者による応答は必要ありません。

関連トピック

その他の HA イベントに対する応答 （380 ページ）

HA サーバーが両方ともダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーが同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーおよびセカンダリ サーバー上で稼働する Prime Infrastructure のインスタンスを再起動します。何らかの理由でセカンダリ サーバーを再起動できなかった場合は、「関連項目」の「HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合」を参照してください。

ステップ 2 セカンダリ サーバーで Prime Infrastructure が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバーと、プライマリ サーバー上で稼働する Prime Infrastructure のインスタンスを再起動します。Prime Infrastructure がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （388 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）
その他の HA イベントに対する応答 （380 ページ）

両方の HA サーバーの電源がダウンしている場合

プライマリ サーバーおよびセカンダリ サーバーの電源が同時にダウンした場合、次の手順で説明するように正しい順序で稼働中の状態に戻すことで復旧できます。

ステップ 1 セカンダリ サーバーとその上で稼働する Prime Infrastructure のインスタンスの電源をオンにします。

この時点では、プライマリに到達できないため、セカンダリ HA の再起動に失敗します。ただし、セカンダリ ヘルス モニター プロセスは動作し、エラーが表示されます。

ステップ 2 セカンダリ サーバーで Prime Infrastructure が稼働中になったら、セカンダリ サーバーの Health Monitor Web ページにアクセスします。セカンダリ サーバーの状態が [セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）] に遷移します。

ステップ 3 プライマリ サーバと、プライマリ サーバ上で稼働する Prime Infrastructure のインスタンスの電源をオンにします。

ステップ 4 Prime Infrastructure がプライマリ サーバー上で稼働している場合、プライマリ サーバーは自動的にセカンダリ サーバーと同期します。これを確認するには、プライマリ サーバーの Health Monitor Web ページにアクセスします。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
次の状態：Primary Lost Secondary	次の状態：[セカンダリがプライマリとの接続を失いました（Secondary Lost Primary）]
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

ステップ 5 セカンダリ サーバーとその上で稼働する Prime Infrastructure のインスタンスを再起動します。この時点では、プロセスのすべてがセカンダリ サーバーで実行されているわけではないため、この操作が必要です。

何らかの理由でセカンダリ サーバを再起動できなかった場合は、「関連項目」の「HA サーバが両方ともダウンし、セカンダリ サーバが再起動しない場合」を参照してください。

ステップ 6 Prime Infrastructure がセカンダリ サーバーでの再起動を完了すると、すべてのプロセスが実行されているはずです。これを確認するには、ncs status コマンドを実行します（「関連項目」の「Prime Infrastructure サーバーのステータスの確認」を参照）。

関連トピック

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合 （388 ページ）
ヘルス モニター Web ページへのアクセス （377 ページ）
その他の HA イベントに対する応答 （380 ページ）
Prime Infrastructure サーバーのステータスの確認 （148 ページ）

HA サーバーが両方ともダウンし、セカンダリ サーバーが再起動しない場合

両方の HA サーバーが同時にダウンし、セカンダリ サーバーが再起動しない場合は、セカンダリ サーバーの交換または復元ができるまで、プライマリ サーバーをスタンドアロンとして使用するように、プライマリ サーバーから HA 設定を削除する必要があります。

以下の手順では、すでにセカンダリ サーバーの再起動を試み、再起動に失敗したものとしています。

ステップ 1 Prime Infrastructure のプライマリ インスタンスの再起動を試みます。少なくともプライマリ インスタンスの再起動が可能である場合は、HA 設定の削除が必要であることを示すエラー メッセージが表示されて再起動が中断されます。

ステップ 2 プライマリ Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。

ステップ 3 次のコマンドを入力して、プライマリ サーバーの HA 設定を削除します。

PIServer/admin# **ncs ha remove**

ステップ 4 HA 設定を削除するかどうかを確認するメッセージが表示されます。確認要求に対して **Y** と応答します。

今度は、エラー メッセージなしで Prime Infrastructure プライマリ インスタンスの再起動が可能になり、これをスタンドアロンとして使用できるようになるはずです。

セカンダリ サーバーの復元または交換ができたら、「関連項目」の「プライマリ サーバーでのハイ アベイラビリティの登録方法」の手順に従って続行してください。

関連トピック

ヘルス モニター Web ページへのアクセス （377 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
CLI での HA の削除 （397 ページ）
その他の HA イベントに対する応答 （380 ページ）

プライマリ サーバーの交換方法

通常の状況下では、プライマリ サーバーの状態は [プライマリ アクティブ（Primary Active）]、セカンダリ サーバーの状態は [セカンダリ同期中（Secondary Syncing）] です。プライマリ サーバで何らかの理由で障害が発生した場合、セカンダリ サーバへのフェールオーバーが自動または手動で行われます。

HA への完全なアクセスを復旧するには、新しいハードウェアを使用してプライマリ サーバをインストールする必要があることがあります。この場合、次の手順に従うことで、データを失うことなく新しいプライマリ サーバを起動できます。

ステップ 1 セカンダリ サーバーの状態が [セカンダリ アクティブ（Secondary Active）] であることを確認します。プライマリ サーバの [Failover Type] を [manual] に設定している場合は、セカンダリ サーバへのフェールオーバーを手動でトリガーします。

ステップ 2 交換する古いプライマリ サーバーがネットワークから切断していることを確認します。

ステップ 3 新しいプライマリ サーバーが使用可能な状態であることを確認します。これには、このプライマリ サーバがネットワークに接続されており、古いプライマリ サーバと同じサーバ IP、サブネット マスク、およびゲートウェイが割り当てられていることが含まれます。また、セカンダリ サーバーのインストール時に入力したものと同じ認証キーを入力する必要があります。

ステップ 4 プライマリサーバーとセカンダリサーバーが同じパッチ レベルであることを確認します。プライマリサーバーを置換する場合は、次の手順を実行する必要があります。

a) プライマリサーバーとセカンダリサーバーが TOFU モードであることを確認します。
b) セカンダリサーバー管理 CLI にログインします。
c) セカンダリサーバーの CLI で次のコマンドを実行します。
d) PIServer/admin# ncs certvalidation tofu-certs deletecert host <primaryserver's-hostname>

これは、プライマリサーバーとセカンダリサーバー間の通信を再確立するために必要です。

ステップ 5 セカンダリ サーバーから、新たにインストールしたプライマリ サーバーへのフェールバックをトリガーします。新しいプライマリ HA サーバーへのフェールバック中にはデータベースのフル コピーが実行されるため、使用可能な帯域幅とネットワーク遅延によってはこの処理の完了に時間がかかります（「関連項目」の「HA のネットワーク スループットに関する制限事項」を参照）。2 台のサーバーで、以下の一連の HA 状態遷移が行われます。

プライマリ HA の状態遷移	セカンダリ HA の状態遷移
元の状態：HA not configured	元の状態：[セカンダリ アクティブ（Secondary Active）]
次の状態：Primary Failback	次の状態：Secondary Failback
次の状態：Primary Failback	次の状態：Secondary Post Failback
次の状態：Primary Active	次の状態：[セカンダリ同期中（Secondary Syncing）]

関連トピック

フェールオーバーのトリガー方法 （377 ページ）
フェールバックのトリガー方法 （378 ページ）
その他の HA イベントに対する応答 （380 ページ）
HA のネットワーク スループットに関する制限事項 （351 ページ）

スプリット ブレイン シナリオからの回復方法

「自動フェールオーバーと手動フェールオーバーの違い」（「関連項目」参照）で説明されているように、「スプリットブレーン状況」が発生する稀な状況では、データが失われる可能性が常にあります。この場合、以下の手順に従い、新しく追加されたデータをセカンダリに保存し、追加されたデータをプライマリには保存しないようにすることができます。

ステップ 1 ネットワークが起動し、セカンダリ サーバーが起動すると、プライマリ サーバーはスタンバイ データベースを使用して自動的に再起動します。プライマリ サーバーの HA ステータスはまず「プライマリ フェールオーバー（Primary Failover）」になり、その後「プライマリ同期中（Primary Syncing）」に変わります。これを確認するには、プライマリ サーバーのヘルス モニター Web ページにログオンします。

ステップ 2 プライマリ サーバーのステータスが「プライマリ同期中（Primary Syncing）」になった後、Web ブラウザを使用して、ユーザーがセカンダリ サーバーの Prime Infrastructure ページ（たとえば、https://x.x.x.x:443）にログインできることを確認します。確認が済むまで、手順を進めないでください。

ステップ 3 セカンダリ サーバーにアクセスできることが確認できたら、セカンダリ サーバーのヘルス モニター Web ページから、フェールバックを開始します（フェールバックのトリガー方法 （378 ページ）を参照）。プライマリ サーバーへのスイッチオーバーが完了するまで、セカンダリ サーバーでモニタリング アクティビティを続行できます。

詳細については、CLI を使用した Prime Infrastructure の再起動 （149 ページ）を参照してください。

関連トピック

自動フェールオーバーと手動フェールオーバーの違い （355 ページ）
CLI での HA の削除 （397 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）

データベースの同期の問題を解決する方法

データベースの同期の問題を解決するには、プライマリ サーバーが「プライマリ アクティブ」状態で、セカンダリ サーバーが「セカンダリ同期」状態になっているときに、次の手順に従います。

ステップ 1 HA を削除します（CLI での HA の削除 （397 ページ）およびGUI での HA の削除 （396 ページ）を参照）。

ステップ 2 プライマリ サーバーとセカンダリ サーバーの両方が「HA 未設定」の状態になったら、HA を登録します。ハイ アベイラビリティのセットアップ （359 ページ） を参照してください

ハイ アベイラビリティの参照情報

以下の項に、HA に関する参照情報を記載します。

関連トピック

HA コンフィギュレーション モード リファレンス （392 ページ）
HA 状態リファレンス （392 ページ）
HA 状態遷移リファレンス （394 ページ）
ハイ アベイラビリティ CLI コマンド リファレンス （396 ページ）
HA 認証キーのリセット （396 ページ）
GUI での HA の削除 （396 ページ）
CLI での HA の削除 （397 ページ）
復元中の HA の削除 （397 ページ）
アップグレード中の HA の削除 （398 ページ）
HA エラー ロギングの使用 （399 ページ）

HA サーバーの IP アドレスまたはホスト名のリセット （399 ページ）

HA コンフィギュレーション モード リファレンス

次の表に、すべての可能な HA コンフィギュレーション モードを示します。

表 *15*：ハイ アベイラビリティ モード

モード	説明
HA 未設定（HA not configured）	HA は、この Prime Infrastructure サーバーに設定されていません。
HA 初期化中（HA initializing）	プライマリ サーバーとセカンダリ サーバー間の HA 登録プロセスが開始されました。
HA enabled	プライマリ サーバーとセカンダリ サーバー間で HA が有効になりました。
HA alone	プライマリ サーバーは単独で実行されています。HA は有効ですが、プライマリ サーバーがセカンダリ サーバーと同期していないか、セカンダリ サーバーがダウンしているか、またはセカンダリ サーバーに到達できません。

関連トピック

ハイ アベイラビリティの参照情報 （391 ページ）

HA 状態リファレンス

次の表に、ユーザーによる応答が必要ない状態も含め、すべての可能な HA 状態をリストします。

表 *16*：ハイ アベイラビリティ状態

状態	Server	説明
スタンドアロン（Stand Alone）	両方	HA は、この Prime Infrastructure サーバーに設定されていません。
プライマリ単独（Primary Alone）	プライマリ	プライマリ サーバーは、セカンダリ サーバーを失った後に再起動しました。Health Monitor のみがこの状態で稼働します。
HA 初期化中（HA Initializing）	両方	プライマリ サーバーとセカンダリ サーバー間の HA 登録プロセスが開始されました。
プライマリアクティブ（Primary Active）	プライマリ	プライマリ サーバーは現在アクティブであり、セカンダリ サーバーと同期中です。

状態	Server	説明
プライマリデータベースのコピー失敗（Primary Database Copy Failed）	プライマリ	再起動されるプライマリ サーバーは、自身が24時間以上ダウンしていたためにデータ ギャップが生じていないかを常に確認します。そして、このようなギャップを検出すると、自動的にアクティブなセカンダリ サーバーからのデータ コピーをトリガーします。まれに、このデータベースのコピーに失敗することがあります。そのような場合に、この遷移状態がプライマリ サーバーに設定されます。データベース コピーが正常に終了するまで、プライマリへのフェールバックの試行はすべてブロックされます。データベース コピーが正常に終了するとすぐに、プライマリ サーバーの状態が「プライマリ同期中（Primary Syncing）」に設定されます。
プライマリフェールオーバー（Primary Failover）	プライマリ	プライマリ サーバーで障害が検出されました。
プライマリフェールバック（Primary Failback）	プライマリ	ユーザーによってトリガーされたフェールバックが進行中です。
プライマリがセカンダリとの接続を喪失（Primary Lost Secondary）	プライマリ	プライマリ サーバーは、セカンダリ サーバーと通信できません。
プライマリがフェールバックの準備中（Primary Preparing for Failback）	プライマリ	セカンダリへのフェールオーバー後、プライマリ サーバーの起動時にこの状態が設定されます。この状態は、プライマリ サーバーがスタンバイ モード（セカンダリ サーバーがアクティブであるため）で起動し、フェールバックの準備ができていることを示します。プライマリ サーバーがフェールバックの準備ができると、その状態は「プライマリ同期中（Primary Syncing）」に設定されます。
プライマリ同期中（Primary Syncing）	プライマリ	プライマリ サーバーは、データベースおよびコンフィギュレーション ファイルを、アクティブなセカンダリ サーバーと同期しています。セカンダリ サーバーにフェールオーバーし、セカンダリ サーバーがアクティブ ロールを引き継いだ後、プライマリ プロセスが送り込まれてくるときに、プライマリ サーバーがこの状態に移行します。
プライマリの状態を確認不能（Primary Uncertain）	プライマリ	プライマリ サーバーのアプリケーション プロセスがデータベースに接続できません。
セカンダリ単独（Secondary Alone）	セカンダリ	プライマリ サーバーの再起動後、セカンダリ サーバーからプライマリ サーバーに接続できません。
セカンダリ同期中（Secondary Syncing）	セカンダリ	セカンダリ サーバーは、プライマリ サーバーとデータベースおよびコンフィギュレーション ファイルを同期しています。
セカンダリアクティブ（Secondary Active）	セカンダリ	プライマリ サーバーからセカンダリ サーバーへのフェールオーバーが正常に完了しました。

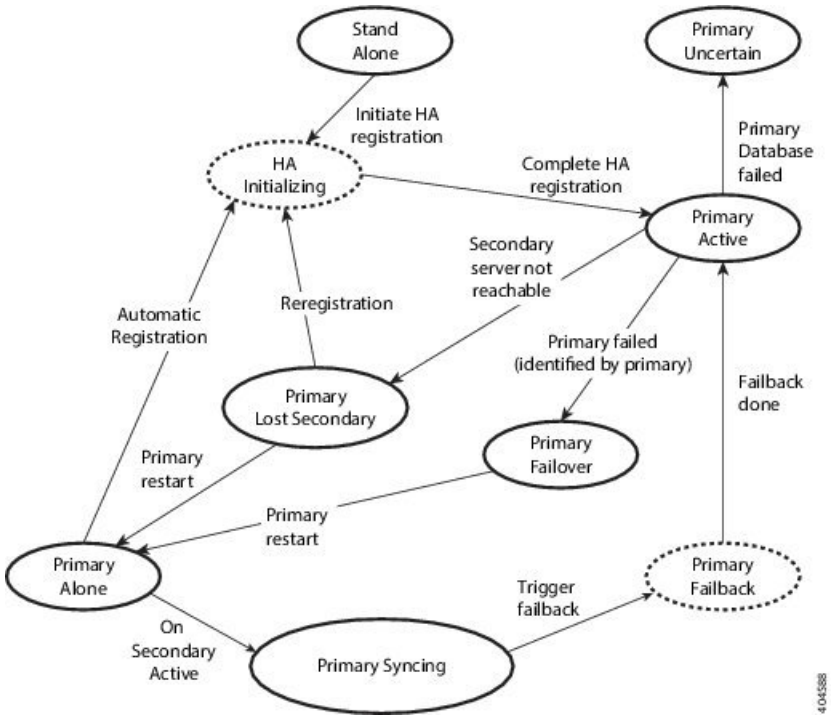
状態	Server	説明
セカンダリがプライマリとの接続を喪失（Secondary Lost Primary）	セカンダリ	セカンダリ サーバーがプライマリ サーバーに接続できません（この状態は、プライマリ サーバーで障害が発生した場合、またはネットワーク接続が失われた場合に発生します）。 この状態から自動フェールオーバーが行われる場合、セカンダリ サーバーは自動的に [Active] 状態に移ります。手動フェールオーバーの場合は、ユーザーがフェールオーバーをトリガーしてセカンダリ サーバーをアクティブにすることができます。
セカンダリフェールオーバー（Secondary Failover）	セカンダリ	フェールオーバーがトリガーされて進行中です。
セカンダリフェールバック（Secondary Failback）	セカンダリ	フェールバックがトリガーされて進行中です（データベースおよびファイル レプリケーションが進行中）。
セカンダリ ポスト フェールバック（Secondary Post Failback）	セカンダリ	この状態が発生するのは、フェールバックがトリガーされて、セカンダリ サーバーからプライマリ サーバーへのデータベースおよびコンフィギュレーション ファイルの複製が完了し、Health Monitor がセカンダリ サーバーの [Secondary Syncing] への状態遷移およびプライマリ サーバーの [Primary Active] への状態遷移を開始した場合です。この状態は、これらの状態変更および関連するプロセスの開始と停止が進行中であることを示します。
セカンダリの状態を確認不能（Secondary Uncertain）	セカンダリ	セカンダリ サーバーのアプリケーション プロセスが、セカンダリ サーバーのデータベースに接続できません。

関連トピック

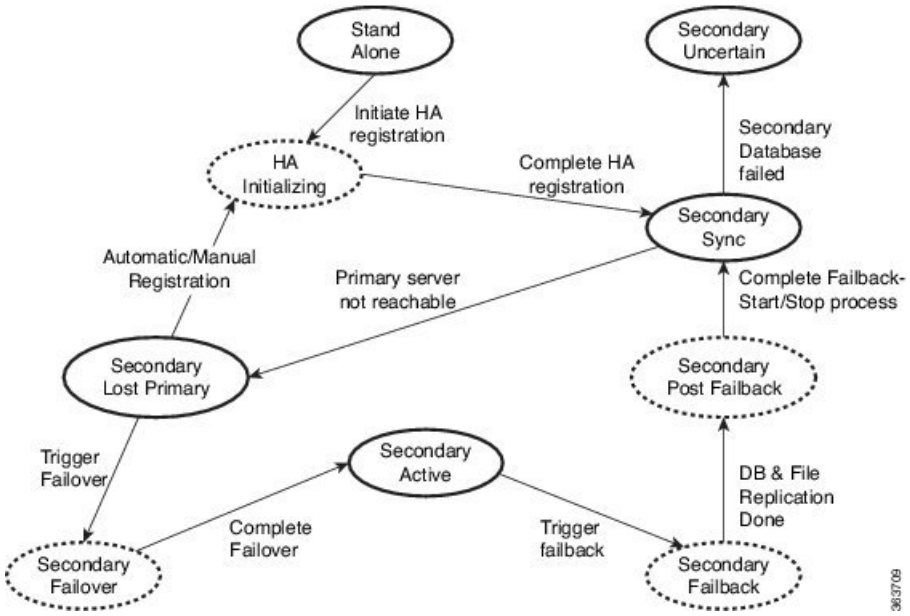
ハイ アベイラビリティの参照情報 （391 ページ）

HA 状態遷移リファレンス

次の図は、プライマリ サーバーのすべての可能な状態遷移を詳しく説明しています。



次の図は、セカンダリ サーバーのすべての可能な状態遷移を詳しく説明しています。



関連トピック

ハイ アベイラビリティの参照情報 （391 ページ）

ハイ アベイラビリティ CLI コマンド リファレンス

次の表に、HA 管理に使用できる CLI コマンドをリストします。これらのコマンドを実行するには、管理者としてプライマリ サーバーにログインします（「CLI から接続する方法 （147 ページ）」を参照）。

表 *17*：ハイ アベイラビリティ コマンド

コマンド	説明
ncs ha ?	ハイ アベイラビリティ CLI コマンドのヘルプを取得します。
ncs ha authkey authkey	ハイ アベイラビリティの認証キーを更新します。
ncs ha remove	ハイ アベイラビリティ構成を削除します。
ncs ha status	ハイ アベイラビリティの現在の状態を取得します。

関連トピック

ハイ アベイラビリティの参照情報 （391 ページ）

HA 認証キーのリセット

Prime Infrastructure 管理者は、**ncs ha authkey** コマンドを使用して HA 認証キーを変更できます。新しい認証キーがパスワード標準を満たすようにする必要があります。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha authkey** *MyNewAuthKey*

ここで、*MyNewAuthKey* は新しい認証キーです。詳細については、CLI から接続する方法 （147 ページ）を参照してください。

関連トピック

ハイ アベイラビリティをセットアップする前に （359 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

GUI での HA の削除

既存の HA 実装を削除するには、以下の手順で説明するように、GUI を使用するのが最も簡単な方法です。また、コマンド ラインから HA 設定を削除することもできます。

この方法を使用するには、プライマリ Prime Infrastructure サーバーの状態が「プライマリ アクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ

サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 管理者権限を持つユーザー ID を使用してプライマリ Prime Infrastructure サーバーにログインします。

ステップ 2 [管理（Administration）]>[設定（Settings）]>[ハイ アベイラビリティ（High Availability）]>[HA 設定（HA Configuration）] の順に選択します。

ステップ 3 [削除（Remove）] を選択します。HA 設定の削除には 3 ～ 4 分かかります。

削除が完了したら、ページに表示されている HA 設定モードが「HA 未設定（HA not Configured）」になっていることを確認します。

関連トピック

CLI での HA の削除 （397 ページ）
フェールバックのトリガー方法 （378 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

CLI での HA の削除

何らかの理由でプライマリ サーバー上の Prime Infrastructure GUI にアクセスできない場合、管理者は以下の手順に従い、コマンド ラインから HA 設定を削除することができます。

この方法を使用するには、プライマリ Prime Infrastructure サーバーの状態が「プライマリ アクティブ（Primary Active）」であることを確認する必要があります。何らかの理由でセカンダリ サーバーが現在アクティブである場合、フェールバックが完了してセカンダリ サーバーが自動的に再起動してから、フェールバックを実行して HA 設定を削除します。

ステップ 1 CLI を使用してプライマリ サーバーに接続します。「configure terminal」モードにしないでください。

ステップ 2 コマンドラインに次のように入力します。

admin# **ncs ha remove**。詳細については、CLI から接続する方法 （147 ページ）を参照してください。

関連トピック

GUI での HA の削除 （396 ページ）
フェールバックのトリガー方法 （378 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

復元中の HA の削除

Prime Infrastructure は、ハイ アベイラビリティ関連の各種設定をバックアップしません。

HA を使用した Prime Infrastructure 実装を復元するには、必ず、バックアップしたデータをプライマリ サーバーのみに復元してください。復元されたプライマリ サーバーは、そのデータ

を自動的にセカンダリ サーバーに複製します。セカンダリ サーバーで復元操作を実行する必要はありません。これを実行しようとすると、エラー メッセージが生成されます。

HA を使用する Prime Infrastructure 実装を復元するには、次の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します（「関連項目」の「GUI からの HA の削除」を参照）。

ステップ 2 必要に応じてプライマリ サーバーを復元します。

ステップ 3 復元が完了したら、HA 登録プロセスを再度実行します。

詳細については、データの復元 （70 ページ）およびCLI から接続する方法 （147 ページ）を参照してください。

関連トピック

GUI での HA の削除 （396 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

アップグレード中の HA の削除

HA を使用した Prime Infrastructure 実装をアップグレードするには、以下の手順に従います。

ステップ 1 GUI を使用して、プライマリ サーバーから HA 設定を削除します（「関連項目」の「GUI からの HA の削除」参照）。

ステップ 2 必要に応じてプライマリ サーバーをアップグレードします。

ステップ 3 現在のイメージを使用してセカンダリ サーバーを再インストールします。

セカンダリ サーバーを以前のバージョンやベータ版からアップグレードすることはできません。セカンダリ サーバーは常に新規インストールでなければなりません。

ステップ 4 アップグレードが完了したら、HA 登録プロセスを再度実行します。

（注） アップグレード後、ヘルス モニター ページに以下のヘルス モニター イベント メッセージが表示されます。

プライマリ認証キーが管理者によって変更されました（Primary Authentication Key was changed by Admin）

詳細については、CLI から接続する方法 （147 ページ）を参照してください。

関連トピック

GUI での HA の削除 （396 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）

ハイ アベイラビリティの参照情報 （391 ページ）

HA エラー ロギングの使用

ハイ アベイラビリティ機能に対するエラー ロギングは、ディスク スペースを節約し、最大限のパフォーマンスを達成するために、デフォルトで無効にされます。HAに問題がある場合は、まず、エラー ロギングを有効にして、記録されたログ ファイルを調べることから始めるのが最善です。

ステップ 1 問題のあるサーバーの Health Monitor ページを表示します。

ステップ 2 [ロギング（Logging）] 領域で、[メッセージ レベル（Message Level）] ドロップダウンから必要なエラー ロギング レベルを選択します。

ステップ 3 **[Save（保存）]** をクリックします。

ステップ 4 ログ ファイルをダウンロードする必要がある場合は、[Logs] 領域で、[Download] をクリックします。ダウンロードしたログ ファイルは、任意の ASCII テキスト エディタを使用して開くことができます。

関連トピック

ヘルス モニター Web ページへのアクセス （377 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

HA サーバーの IP アドレスまたはホスト名のリセット

プライマリまたはセカンダリ HA サーバーの IP アドレスまたはホスト名は、できるだけ変更しないようにしてください。IPアドレスまたはホスト名を変更しなければならない場合は、変更を行う前に、プライマリ サーバーから HA 設定を削除します。変更が終わったら、HA を再登録します。

関連トピック

GUI での HA の削除 （396 ページ）
プライマリ サーバーでの HA の登録方法 （362 ページ）
ハイ アベイラビリティの参照情報 （391 ページ）

任意の状態の TOFU エラーの解決

プライマリサーバーとセカンダリサーバーが通信する場合、次のTOFUエラーが発生する可能性があります。

続行する前に、次のエラーを修正する必要があります。「この接続には、ゼロトラスト（*TOFU*）ベースの証明書が設定されています。リモートホストの現在の証明書は、以前に使用されていたものとは異なります。（*A Trust-on-first-use (TOFU) based Certificate is configured for this connection. The current certificate on the remote host is different than what was used earlier.*」

この問題を修正するには、次の手順を実行する必要があります。

- プライマリサーバーとセカンダリサーバーの両方で NCS CLI コマンドを使用して既存の証明書をクリアします。

```
ncs certvalidation tofu-certs deletecert host <server-hostname>
```

MSE ハイ アベイラビリティの設定

Cisco Mobility Services Engine（MSE）は、複数のモビリティ アプリケーションをホストするプラットフォームです。MSE ハイ アベイラビリティ（HA）設定の下では、アクティブな MSE は MSE の別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （400 ページ）
MSE ハイ アベイラビリティのセットアップ：ワークフロー （403 ページ）

MSE ハイ アベイラビリティ アーキテクチャの概要

MSE ハイ アベイラビリティ システムの主要なコンポーネントは、ヘルス モニターです。ヘルス モニターは、各 MSE での HA セットアップの設定、管理、モニターを行います。プライマリ MSE とセカンダリ MSE の間でハートビートが維持されます。ヘルス モニターは、データベースのセットアップ、ファイルのレプリケーション、アプリケーションのモニタリングを行います。プライマリ MSE で障害が発生し、セカンダリ MSE に切り替わると、プライマリ MSE の仮想アドレスがセカンダリ MSE に透過的に切り替わります。次の点に注意してください。

- アクティブな各プライマリ MSE は別の非アクティブ インスタンスによりバックアップされます。セカンダリ MSE の目的は、プライマリ MSE のアベイラビリティと状態をモニターすることです。セカンダリ MSE は、フェールオーバー手順の開始後にアクティブになります。
- 1 つのセカンダリ MSE で 1 つのプライマリ MSE をサポートできます。

[Services] タブの [MSE]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [Mobile Concierge] ページは、リリース 7.3 の仮想ドメインのみで使用できます。

以下の関連項目は、MSE ハイ アベイラビリティ アーキテクチャに関する追加の詳細情報を提供します。

関連トピック

MSE ハイ アベイラビリティのペアリング マトリックス （401 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （401 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （402 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （402 ページ）
MSE ハイ アベイラビリティのライセンス要件 （403 ページ）
MSE ハイ アベイラビリティの設定 （400 ページ）

MSE ハイ アベイラビリティのペアリング マトリックス

次の表は、ハイ アベイラビリティ構成においてペアリング可能な MSE サーバーのタイプを一覧表示しています。

表 *18 : MSE* ハイ アベイラビリティ サーバーのペアリング マトリックス

プライマリ サーバー タイプ	セカンダリ サーバー タイプ				
3355	VA-2	VA-3	VA-4	VA-5	
3355	あり	なし	なし	なし	なし
VA-2	なし	あり	あり	あり	あり
VA-3	なし	なし	あり	あり	あり
VA-4	なし	なし	なし	あり	あり
VA-5	なし	なし	なし	なし	あり

関連トピック

リモート モデルの使用 （354 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （401 ページ）

MSE ハイ アベイラビリティのガイドラインと制約事項

MSE ハイ アベイラビリティを実装し、これを Prime Infrastructure から管理する予定の管理者は、以下のガイドラインと制限事項に従う必要があります。

- ヘルス モニター IP と仮想 IP の両方に Prime Infrastructure からアクセスできるようにする必要があります。
- ヘルス モニター IP と仮想 IP は常に異なる IP でなければなりません。ヘルス モニターと仮想インターフェイスは、同じネットワーク インターフェイス上にあっても別のインターフェイス上にあってもかまいません。
- 手動フェールオーバーと自動フェールオーバーのいずれかを使用できます。フェールオーバーは、一時的なものであると見なす必要があります。故障した MSE をできるだけ早く復旧して、フェールバックを再開する必要があります。故障した MSE の復旧に時間がかかるほど、ハイ アベイラビリティのサポートなしで単一 MSE を稼働する時間が長くなります。
- 手動フェールバックと自動フェールバックのいずれかを使用できます。
- プライマリ MSE とセカンダリ MSE は、同じソフトウェア バージョンを実行する必要があります。

- WAN 上のハイ アベイラビリティはサポートされません。
- LAN 上のハイ アベイラビリティは、プライマリ MSE とセカンダリ MSE の両方が同じサブネット内にある場合に限りサポートされます。
- プライマリとセカンダリのMSEが通信するポートを開ける（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。次の入力/出力ポートを開く必要があります：80、443、8080、8081、22、8001、1521、1411、1522、1523、1524、1525、9006、15080、61617、59000、12091、1621、1622、1623、1624、1625、8083、8084、8402。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （400 ページ）
MSE ハイ アベイラビリティのペアリング マトリックス （401 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （402 ページ）

MSE ハイ アベイラビリティのフェールオーバー シナリオ

プライマリ MSE で障害が検出されると、次のイベントが発生します。

- セカンダリ MSEのヘルス モニターにより、プライマリ MSEが機能していないこと（ハードウェア障害、ネットワーク障害など）が確認されます。
- 自動フェールオーバーが有効化されている場合、即座にセカンダリ MSE が起動します。
- 手動フェールオーバーが有効化されている場合は、フェールオーバーを手動で開始するかどうかを確認する電子メールが管理者に送信されます。この電子メールは、MSE アラーム用に電子メールが設定されている場合のみ送信されます。
- フェールオーバー動作の結果はヘルス モニター UI でイベントとして示され、クリティカル アラームが Prime Infrastructure に送信されます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （400 ページ）
MSE ハイ アベイラビリティのガイドラインと制約事項 （401 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （402 ページ）

MSE ハイ アベイラビリティのフェールバック シナリオ

セカンダリ MSE がすでにプライマリ MSE のフェールオーバー状態である場合、プライマリ MSE が通常の状態に戻ると、フェールバックを呼び出すことができます。

フェールバックが発生するのは、セカンダリ MSE がプライマリ インスタンスに対して次のいずれかの状態である場合だけです。

- セカンダリ MSE が実際にプライマリ MSE をフェールオーバーしている。
- 手動フェールオーバーが設定されているが、管理者が呼び出さなかった。
- プライマリ MSE で障害が発生したが、エラーが発生したため、セカンダリ MSE が引き継ぐことができない。
- フェールバックは、障害が発生したプライマリ MSE を管理者が起動する場合にだけ行われます。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （400 ページ）
MSE ハイ アベイラビリティのフェールオーバー シナリオ （402 ページ）
MSE ハイ アベイラビリティのライセンス要件 （403 ページ）

MSE ハイ アベイラビリティのライセンス要件

ハイ アベイラビリティでは、プライマリおよびセカンダリ仮想アプライアンスでアクティベーション ライセンスが必要です。他のサービスのライセンスはセカンダリ MSE に必要ありません。プライマリ MSE のみで必要です。

関連トピック

MSE ハイ アベイラビリティ アーキテクチャの概要 （400 ページ）
MSE ハイ アベイラビリティのフェールバック シナリオ （402 ページ）

MSE ハイ アベイラビリティのセットアップ：ワークフロー

MSE ソフトウェアのインストール中（または MSE セットアップ スクリプトの使用中）に、所定の重要な要素を設定します。Prime Infrastructure UI からプライマリ MSE とセカンダリ MSE を組み合わせます。

デフォルトでは、すべての MSE がプライマリとして設定されます。ハイ アベイラビリティ サポートを使用しない場合、および以前のリリースからのアップグレードを実行している場合は、引き続きその MSE の IP アドレスを使用してください。ハイ アベイラビリティをセットアップするには、ヘルス モニターの IP アドレスを設定する必要があります。したがって、ヘルス モニターが仮想 IP アドレスになります。

MSE ハイ アベイラビリティの設定は、次の手順で構成されています。

1. ハイ アベイラビリティ用の MSE の準備
2. プライマリ MSE の設定
3. セカンダリ MSE の設定

プライマリ MSE サーバーの交換が必要な場合には、MSE ハイ アベイラビリティの再設定が必要になることもあります。

詳細については、下記の該当する関連項目を参照してください。

関連トピック

ハイ アベイラビリティ用の MSE の準備 （404 ページ）
プライマリ MSE での MSE ハイ アベイラビリティの設定 （404 ページ）
セカンダリ MSE での MSE ハイ アベイラビリティの設定 （412 ページ）
プライマリ MSE の交換 （418 ページ）
MSE ハイ アベイラビリティの設定

ハイ アベイラビリティ用の MSE の準備

プライマリおよびセカンダリ MSE をハイ アベイラビリティ用に準備するには、次の手順に従ってください。

ステップ 1 プライマリ MSE とセカンダリ MSE の間のネットワーク接続が機能しており、すべての必要なポートが開いていることを確認します。

ステップ 2 正しいバージョンの MSE をプライマリ MSE 上にインストールします。

ステップ 3 同じバージョンの MSE がセカンダリ MSE にインストールされていることを確認します。

関連トピック

プライマリ MSE の交換 （418 ページ）
MSE ハイ アベイラビリティの設定 （400 ページ）

プライマリ MSE での MSE ハイ アベイラビリティの設定

プライマリ MSE をハイ アベイラビリティ用に設定するには、次の手順に従ってください。

ステップ 1 プライマリ MSE で次のコマンドを入力します。

/opt/mse/setup/setup.sh

セットアップ スクリプトにより、次のような入力要求が表示されます。用意された選択肢を使って太字で回答できます（このステップおよび次のステップが対象）。

```
------------------------------------------------------------
Welcome to the Cisco Mobility Services Engine Appliance Setup.
You may exit the setup at any time by typing <Ctrl+c>.
------------------------------------------------------------
Would you like to configure MSE using:
1. Menu mode
2. Wizard mode
Choose 1 or 2: 1
------------------------------------------------
Mobility Services Engine Setup
Please select a configuration option below and enter the requested information. You may exit setup at any time by typing <Ctrl +C>.
You will be prompted to choose whether you wish to configure a parameter, skip it, or reset it to its initial default value. Skipping a parameter will leave it unchanged from its current value.
Please note that the following parameters are mandatory and must be configured at lease once.
-> Hostname
```

-> Network interface eth0

-> Timezone settings

-> Root password

-> NTP settings

-> Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.

PRESS <ENTER> TO CONTINUE:

Configure MSE:

1) Hostname * 13) Remote syslog settings

2) Network interface eth0 settings* 14) Host access control settings

3) Timezone settings* 15) Audit Rules

4) Root password * 16) Login banner

5) NTP settings * 17) System console restrictions

6) Prime Infrastructure password * 18) SSH root access

7) Display current configuration 19) Single user password check

8) Domain 20) Login and password settings

9) High availability role 21) GRUB password

10) Network interface eth1 settings 22) Root access control

11) DNS settings 23) Auto start MSE on system boot up

12) Future restart time 24) ## Verify and apply changes ##

Please enter your choice [1 - 24]:

ステップ 2 プライマリ MSE のホスト名を設定します。

Please enter your choice [1 - 24]: **1**

Current Hostname=[mse]

Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: **y**

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a Host name [mse]:**mse1**

ステップ 3 プライマリ MSE のドメインを設定します。

Please enter your choice [1-24]: **8**

Current domain=[ ]

Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: **S**

ステップ 4 プライマリ MSE ネットワーク インターフェイス eth0 を設定します。

Please enter your choice [1 - 24]: **2**

Current eth0 interface IP address=[10.0.0.1]

Current eth0 interface netmask=[255.0.0.0]

Current IPv4 gateway address=[172.20.104.123]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: **y**

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [10.0.0.2]:

Enter the network mask for IP address 172.21.105.126

Enter network mask [255.255.255.224]:

Enter the default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface.

Enter default gateway address [172.20.104.123]:

ステップ 5 プライマリ MSE のルート パスワードを設定します。

Please enter your choice [1 - 24]: **4**

Root password has not been configured

Configure root password? (Y)es/(S)kip/(U)se default [Skip]: **y**

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password: **password**

ステップ 6 プライマリ MSE のハイ アベイラビリティ ロールを設定します。

Current role=[Primary]

Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: **y**

High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]: 1

Health monitor interface holds physical IP address of this MSE server.

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers.

This can help reduce latencies in heartbeat response times, data replication and failure detection times.

Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.

"none" implies you do not wish to use direct connect configuration.

Select direct connect interface [eth0/eth1/none] [none]:

Enter a Virtual IP address for the Primary MSE server

Enter Virtual IP address [1.1.1.1]: **10.10.10.11**

Enter network mask for IP address 10.10.10.1

Enter network mask [1.1.1.1]: **255.255.255.0**

Select to start the server in recovery mode.

You should choose yes only if this primary MSE was paired earlier and you have now lost the configuration from this box.

And, now you want to restore the configuration from Secondary via Cisco Prime Infrastructure

Do you wish to start this MSE in HA receovery mode?: (yes/no} [no]:no

Current IP address = [1.1.1.10]

Current eth0 netmask=[255.255.255.0]

Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: **10.10.10.12**

Enter the network mask for IP address 10.10.10.12

Enter network mask [255.255.255.0]: **255.255.255.0**

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:**10.10.10.1**

The second Ethernet interface is currently disabled for this machine.

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

ステップ 7 プライマリ MSE のタイムゾーンを設定します。

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

1) Africa

2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) UTC - I want to use Coordinated Universal Time.
#? 2
Please select a country.
1) Anguilla 27) Honduras
2) Antigua & Barbuda
5) Bahamas 31) Montserrat
6) Barbados 32) Netherlands Antilles
7) Belize 33) Nicaragua
8) Bolivia 34) Panama
9) Brazil 35) Paraguay
10) Canada 36) Peru
11) Cayman Islands 37) Puerto Rico
12) Chile 38) St Barthelemy
13) Colombia 39) St Kitts & Nevis
14) Costa Rica 40) St Lucia
41) St Martin（フランス語）
16) Dominica 42) St Pierre & Miquelon
17) Dominican Republic 43) St Vincent
18) Ecuador 44) Suriname
19) El Salvador 45) Trinidad & Tobago
20) French Guiana 46) Turks & Caicos Is
21) Greenland 47) United States
22) Grenada 48) Uruguay
23) Guadeloupe 49) Venezuela
24) Guatemala 50) Virgin Islands (UK)

25) Guyana 51) Virgin Islands (US)

26) Haiti

#? 47

Please select one of the following time zone regions.

1) Eastern Time

2) Eastern Time - Michigan - most locations

3) Eastern Time - Kentucky - Louisville area

4) Eastern Time - Kentucky - Wayne County

5) Eastern Time - Indiana - most locations

6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties

7) Eastern Time - Indiana - Pulaski County

8) Eastern Time - Indiana - Crawford County

9) Eastern Time - Indiana - Pike County

10) Eastern Time - Indiana - Switzerland County

12) Central Time - Indiana - Perry County

13) Central Time - Indiana - Starke County

14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties

15) Central Time - North Dakota - Oliver County

16) Central Time - North Dakota - Morton County (except Mandan area)

18) Mountain Time - south Idaho & east Oregon

20) Mountain Standard Time - Arizona

21) Pacific Time

22) Alaska Time

23) Alaska Time - Alaska panhandle

24) Alaska Time - Alaska panhandle neck

25) Alaska Time - west Alaska

26) Aleutian Islands

27) Hawaii

#? 21

The following information has been given:

United States

Pacific Time

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2020. Universal Time is now: Mon Apr 7 01:45:27 UTC 2020. Is the above information OK?

1) Yes

2) No

#? 1

ステップ 8 プライマリ MSE の DNS を設定します。

Please enter your choice [1 - 24]: 11

Domain Name Service (DNS) Setup

Enable DNS (yes/no) [no]: y

Default DNS server 1=[8.8.8.8]

Enter primary DNS server IP address:

DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal :

separated v6 address

Enter primary DNS server IP address [8.8.8.8]:

Enter backup DNS server IP address (or none) [none]:

ステップ 9 プライマリ MSE の NTP を設定します。

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the

Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :

separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

ステップ 10 Prime Infrastructure パスワードを設定します。

Please enter your choice [1 - 24]: 6

Cisco Prime Infrastructure communication password has not been configured. Configure Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:

Enter a password for the admin user.

The admin user is used by the Prime Infrastructure and other northbound systems to authenticate their SOAP/XML session with the server. Once this password is updated, it must correspondingly be updated on the NCS page for MSE General Parameters so that the Prime Infrastructure can communicate with the MSE.

ステップ 11 変更を確認して適用します。

Please enter your choice: 24

Please verify the following setup information.

----------BEGIN---------- Hostname=mse1

Role= 1, Health Monitor Intercace=eth0, Direct connect interface=none

Virtual IP Address=10.10.10.11, Virtual IP Netmask=255.255.255.0

Eth0 IP address=10.10.10.12, Eth0 network mask=255.0.0.0

Default Gateway=10.10.10.1

Time zone=America/Los_Angeles

Enable DNS=yes, DNS servers=8.8.8.8

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los_Angeles

Root password is changed.

Cisco Prime Infrastructure password is changed.

----------END----------

You may enter "yes" to proceed with configuration, "no" to make

more changes.

Configuration Changed

Is the above information correct (yes or no): yes

Checking mandatory configuration information...

Root password: Not configured

WARNING

The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration. Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

ステップ 12 システムを再起動します。

[root@mse1]# reboot Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

ステップ 13 MSE サービスを開始します。

[root@mse1]# /etc/init.d/msed start

Starting MSE Platform.

Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started

Starting Admin process... Started Admin process. Starting database .....

Database started successfully. STarting framework and services..... Framework and services successfully started

ステップ 14 すべてのサービスが開始された後、次のコマンドを入力して、MSE サービスが正常に動作していることを確認します。

[root@mse1]# getserverinfo

関連トピック

ハイ アベイラビリティ用の MSE の準備 （404 ページ）
セカンダリ MSE での MSE ハイ アベイラビリティの設定 （412 ページ）
MSE ハイ アベイラビリティの設定 （400 ページ）

セカンダリ MSE での MSE ハイ アベイラビリティの設定

セカンダリ MSE をハイ アベイラビリティ用に準備するには、次の手順に従ってください。

ステップ 1 目的のセカンダリ MSE で次のコマンドを入力します。

/opt/mse/setup/setup.sh

セットアップ スクリプトにより、プライマリ MSE の場合と同じ入力要求が表示されます。

ステップ 2 セカンダリ MSE のホスト名を設定します。

Please enter your choice [1 - 24]: **1**

Current hostanme=[mse1]

Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: yes

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a hostname [mse]: **mse2**

ステップ 3 セカンダリ MSE のドメインを設定します。

Please enter your choice [1-24]: 8

Current domain=[ ]

Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S

ステップ 4 セカンダリ MSE のハイ アベイラビリティ ロールを設定します。

Current role=[Primary]

Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]: 2

Health monitor interface holds physical IP address of this MSE server.

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers.This can help reduce latencies in heartbeat response times, data replication and failure detection times.Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.

"none" implies you do not wish to use direct connect configuration.

Select direct connect interface [eth0/eth1/none] [none]:

Current IP address=[1.1.1.10]

Current eth0 netmask=[255.255.255.0] Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:

Enter an IP address for first Ethernet interface of this machine. Enter eth0 IP address [1.1.1.10]: 10.10.10.13

Enter the network mask for IP address 10.10.10.13

Enter network mask [255.255.255.0]:

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:10.10.10.1

The second Ethernet interface is currently disabled for this machine. Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

ステップ 5 セカンダリ MSE のタイムゾーンを設定します。

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

1) Africa

2) Americas

3) Antarctica

4) Arctic Ocean

5) Asia

6) Atlantic Ocean

7) Australia

8) Europe

9) Indian Ocean

10) Pacific Ocean

11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

1) Anguilla 27) Honduras

2) Antigua & Barbuda

5) Bahamas 31) Montserrat

6) Barbados 32) Netherlands Antilles

7) Belize 33) Nicaragua

8) Bolivia 34) Panama

9) Brazil 35) Paraguay

10) Canada 36) Peru

11) Cayman Islands 37) Puerto Rico

12) Chile 38) St Barthelemy

13) Colombia 39) St Kitts & Nevis

14) Costa Rica 40) St Lucia

41) St Martin（フランス語）

16) Dominica 42) St Pierre & Miquelon

17) Dominican Republic 43) St Vincent

18) Ecuador 44) Suriname

19) El Salvador 45) Trinidad & Tobago

20) French Guiana 46) Turks & Caicos Is

21) Greenland 47) United States

22) Grenada 48) Uruguay

23) Guadeloupe 49) Venezuela

24) Guatemala 50) Virgin Islands (UK)

25) Guyana 51) Virgin Islands (US)

26) Haiti

#? 47

Please select one of the following time zone regions.

1) Eastern Time

2) Eastern Time - Michigan - most locations

3) Eastern Time - Kentucky - Louisville area

4) Eastern Time - Kentucky - Wayne County

5) Eastern Time - Indiana - most locations

6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties

7) Eastern Time - Indiana - Pulaski County

8) Eastern Time - Indiana - Crawford County

9) Eastern Time - Indiana - Pike County

10) Eastern Time - Indiana - Switzerland County

11) Central Time

12) Central Time - Indiana - Perry County

13) Central Time - Indiana - Starke County

14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties

15) Central Time - North Dakota - Oliver County

16) Central Time - North Dakota - Morton County (except Mandan area)

17) Mountain Time

18) Mountain Time - south Idaho & east Oregon

19) Mountain Time - Navajo

20) Mountain Standard Time - Arizona

21) Pacific Time

22) Alaska Time

23) Alaska Time - Alaska panhandle

24) Alaska Time - Alaska panhandle neck

25) Alaska Time - west Alaska

26) Aleutian Islands

27) Hawaii

#? 21

The following information has been given: United States

Pacific Time

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2014. Universal Time is now: Mon Apr 7 01:45:27 UTC 2014. Is the above information OK?

1) Yes

2) No

#? 1

ステップ 6 セカンダリ MSE の NTP を設定します。

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :

separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

ステップ 7 変更を確認して適用します。

Please enter your choice: 24

Please verify the following setup information.

----------BEGIN---------- Hostname=mse2

Role= 2, Health Monitor Intercace=eth0, Direct connect interface=none

Eth0 IP address=10.10.10.13, Eth0 network mask=255.255.255.0

Default Gateway=10.10.10.1

Time zone=America/Los_Angeles

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los_Angeles

----------END----------

You may enter "yes" to proceed with configuration, "no" to make more changes.

Configuration Changed

Is the above information correct (yes or no): yes

Checking mandatory configuration information...

Root password: Not configured

WARNING

The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration.

Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

ステップ 8 システムを再起動します。

[root@mse2 installers]# reboot

Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

ステップ 9 MSE サービスを開始します。

[root@mse2]# /etc/init.d/msed start

Starting MSE Platform.

Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started

Starting Admin process... Started Admin process. Starting database .....

Database started successfully. STarting framework and services..... Framework and services successfully started

関連トピック

ハイ アベイラビリティ用の MSE の準備 （404 ページ）
プライマリ MSE での MSE ハイ アベイラビリティの設定 （404 ページ）
MSE ハイ アベイラビリティの設定 （400 ページ）

プライマリ MSE の交換

何らかの理由でプライマリ MSE を交換する必要がある場合、以下の手順に従うことにより、現在のペアリング情報を新しく設定したプライマリ MSE にリカバリできます。

ステップ 1 セットアップ スクリプトを使用して、MSE をプライマリとして設定します。

ステップ 2 Prime Infrastructure を使用して、プライマリ MSE とセカンダリ MSE の間のペアリングをセットアップします。

ステップ 3 プライマリ MSE からセカンダリ MSE へのフェールオーバーを開始します。

ステップ 4 セットアップスクリプトを使用して、交換用MSEをプライマリとして設定します。新しいプライマリ MSE は、セカンダリ MSE とソフトウェアのバージョンが同じであり、古いプライマリ MSE と設定が同じであることが必要です。

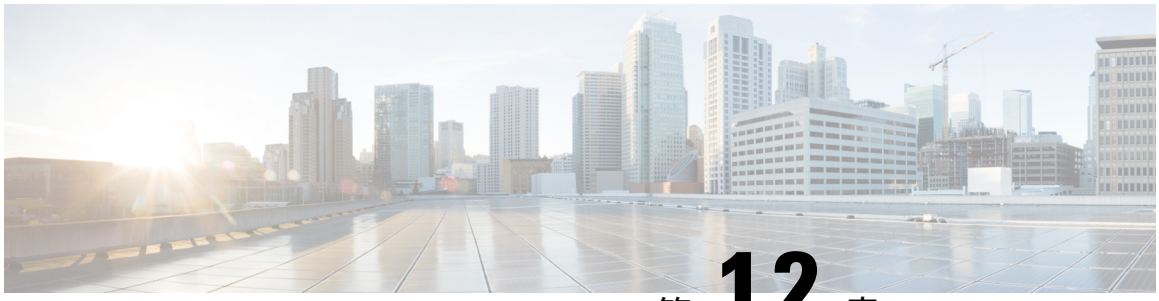
ステップ 5 リカバリ モードを選択し、指示に従います。

ステップ 6 Prime Infrastructure を使用して、新しいプライマリ MSE へのフェールバックを開始します。

この新しいプライマリ MSEには新しいライセンスが必要です。最初のライセンスは新しいプライマリ MSE の UDI に一致しないため機能しません。

関連トピック

プライマリ MSE での MSE ハイ アベイラビリティの設定 （404 ページ）
MSE ハイ アベイラビリティの設定 （400 ページ）



第 12 章

ワイヤレス冗長性の設定

ワイヤレス コントローラの冗長性について

冗長アーキテクチャでは、1 台のワイヤレス コントローラがアクティブ状態となり、もう 1 台のコントローラがスタンバイ状態となります。スタンバイ コントローラは常時、冗長ポートを介してアクティブ コントローラのヘルスをモニターします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

コントローラがスタンバイ状態になるか、アクティブ状態になるかは、製造時に発注される固有デバイス識別情報（UDI）である、冗長在庫管理単位（SKU）に基づきます。冗長 SKU UDI を持つコントローラは、起動されて永続カウントライセンスを実行するコントローラとペアになる場合、最初はスタンバイ状態です。永続カウントライセンスを持つコントローラの場合、コントローラがアクティブ状態であるか、スタンバイ状態であるかを手動で設定できます。

このリリースでは、アクセス ポイントのステートフル スイッチオーバー（AP SSO）がサポートされます。AP SSO により、AP セッションがスイッチオーバー後もそのままであることが保証されます。

クライアントのステートフル スイッチオーバーはサポートされていません。これは、ほぼすべてのクライアントが認証解除され、アクティブ状態の新しいコントローラに再び関連付けられ

ることを意味します。この規則の唯一の例外は、FlexConnectモードのアクセス ポイントでローカルに切り替えられる WLAN 上のクライアントです。

冗長性の前提条件と制限事項

ワイヤレス コントローラの冗長性を設定する前に、以下の前提条件および制限事項を考慮する必要があります。

- ワイヤレス コントローラの冗長性は、5500、7500、8500、および Wism2 のコントローラでサポートされます。
- プライマリおよびセカンダリ コントローラは、同じハードウェア モデルである必要があります。
- プライマリおよびセカンダリ コントローラは、同じコントローラ ソフトウェア リリースを実行している必要があります。
- 管理、冗長管理、およびピア冗長管理インターフェイスの IP アドレスは、同じサブネット内にある必要があります。
- サービス ポートの IP アドレスおよびルート情報はデバイスごとに維持されます。
- 冗長性がコントローラ上で有効な場合、Prime Infrastructure やその他のデバイスでもスタンバイ コントローラを管理できません。
- コントローラがサービス ポートを経由して Prime Infrastructure に追加された場合、コントローラの冗長性を有効にすることはできません。コントローラの冗長性を有効にするには、コントローラを削除し、管理インターフェイスを通じてそのコントローラを追加する必要があります。
- コントローラと Prime Infrastructure 間に監査の不一致がある場合、コントローラでは Prime Infrastructure から冗長パラメータを復元しないでください。ただし、Prime Infrastructure の冗長パラメータを更新することはできます。
- 冗長性を有効にする前に、各デバイスの証明書をダウンロードする必要があります。
- 設定がネットワークからアクティブ コントローラにダウンロードされ、続いて、詳細が冗長インターフェイス経由でスタンバイ コントローラに転送されます。
- 古いアクティブ コントローラが新しいアクティブ コントローラとペアになると、古いアクティブ コントローラには制御が移らず、新しいアクティブ コントローラのスタンバイ コントローラになります。

冗長インターフェイスの設定

冗長インターフェイスには、冗長管理インターフェイスと冗長ポート インターフェイスの 2 つがあります。冗長管理インターフェイスは、管理インターフェイスのサブネット マスク、ゲートウェイ、および VLAN ID を共有するローカル物理管理インターフェイスです。プライマリおよびセカンダリ コントローラの冗長性を有効にするには、冗長管理インターフェイスの IP アドレスだけを設定する必要があります。冗長ポート インターフェイスの IP アドレスは自動生成され、内部的に使用されます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 プライマリ コントローラとして選択したデバイスと一致するワイヤレス コントローラのグループを選択します（たとえば、Cisco 5500 シリーズ ワイヤレス LAN コントローラなど）。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 プライマリ コントローラの [Device Name] をクリックします。

ステップ 5 [Configuration] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[グローバル コンフィギュレーション（Global Configuration）] ページが表示されます。

ステップ 7 [冗長性 - 管理 IP（Redundancy-Management IP）] テキスト ボックスに、管理インターフェイスのサブネットに属している IP アドレスを入力します。

ステップ 8 [Save] をクリックします。

プライマリ コントローラの冗長性の設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 冗長性管理インターフェイス IP アドレスを設定したデバイスと一致するワイヤレス コントローラのグループを選択します（たとえば、Cisco 5500 シリーズ ワイヤレス LAN コントローラなど）。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 冗長管理インターフェイスの IP アドレスを設定したコントローラの [デバイス名（Device Name）] をクリックします。

ステップ 5 [設定（Configuration）] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[グローバル コンフィギュレーション（Global Configuration）] ページが表示されます。

ステップ 7 プライマリ コントローラの冗長モードを有効にする前に、次のパラメータを設定する必要があります。

1. [Redundancy-Management IP]：冗長管理インターフェイスの詳細ページで設定した、ローカル物理管理インターフェイスの IP アドレスが表示されます。また、IP アドレスを変更することもできます。
2. [Peer Redundancy-Management IP]：ピアの冗長管理インターフェイスの IP アドレスを入力します。
3. [Redundant Unit]：[Primary] を選択します。

4. [Mobility MAC Address]：冗長ペアの仮想 MAC アドレスを入力します。入力するモビリティ MAC アドレスがプライマリおよびセカンダリの両方のコントローラで同じであることを確認します。

ステップ 8 [Save] をクリックします。冗長モードの [Enabled] チェック ボックスが有効になります。

ステップ 9 プライマリ コントローラの冗長性を有効にするには、冗長モードの [Enabled] チェック ボックスをオンにします。

冗長性を有効にした後で、[Redundancy-Management IP]、[Peer Redundancy-Management IP]、[Redundant Unit]、および [Mobility MAC Address] のパラメータを変更することはできません。

冗長ペアの処理中にこのコントローラを設定できません。

ステップ 10 [Save] をクリックします。設定が保存され、システムがリブートされます。

セカンダリ コントローラの冗長性の設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 セカンダリ コントローラとして動作するように選択したデバイスと一致するワイヤレス コントローラのグループを選択します（たとえば、Cisco 5500 シリーズ ワイヤレス LAN コントローラなど）。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 セカンダリ コントローラの [Device Name] をクリックします。

ステップ 5 [Configuration] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[グローバル コンフィギュレーション（Global Configuration）] ページが表示されます。

ステップ 7 セカンダリ コントローラの冗長モードを有効にする前に、次のパラメータを設定する必要があります。

1. [Redundancy-Management IP]：ローカル物理管理インターフェイスの IP アドレスを入力します。この IP アドレスは、プライマリ コントローラのピアの冗長管理インターフェイスの IP アドレスと同じである必要があります。
2. [Peer Redundancy-Management IP]：ピアの物理管理インターフェイスの IP アドレスを入力します。この IP アドレスは、プライマリ コントローラのローカル物理冗長管理インターフェイスの IP アドレスと同じである必要があります。
3. [Redundant Unit]：[Secondary] を選択します。
4. [Mobility MAC Address]：冗長ペアの仮想 MAC アドレスを入力します。入力するモビリティ MAC アドレスがプライマリおよびセカンダリの両方のコントローラで同じであることを確認します。

ステップ 8 [Save] をクリックします。冗長モードの [Enabled] チェック ボックスが有効になります。

ステップ 9 セカンダリ コントローラの冗長性を有効にするには、冗長モードの [Enabled] チェック ボックスをオンにします。

冗長性を有効にした後で、[Redundancy-Management IP]、[Peer Redundancy-Management IP]、[Redundant Unit]、および [Mobility MAC Address] のパラメータを変更することはできません。

冗長ペアの処理中にプライマリ コントローラを設定できません。

ステップ 10 [Save] をクリックします。設定が保存され、システムがリブートされます。

冗長性状態のモニタリング

冗長モードがプライマリおよびセカンダリ コントローラで有効になると、システムがリブートされます。両方のコントローラの冗長ステートが、[Wireless Controller Members] リスト ページで [Enabled] になります。以下のトラップがトリガーされます。

- RF_SWITCHOVER_ACTIVITY：このトラップは、スタンバイ コントローラが新しいアクティブ コントローラになるとトリガーされます。
- RF_PROGRESSION_NOTIFY：このトラップは、プライマリまたはアクティブ コントローラのステートが [Disabled] から [StandbyCold] に変更された後、[StandbyHot] に変更されると、そのピア コントローラによってトリガーされます。
- RF_HA_SUP_FAILURE_EVENT：このトラップは、アクティブとスタンバイ コントローラ間の不一致のために冗長性が失敗したときにトリガーされます。

これらのトラップについて詳しくは、『Cisco Prime Infrastructure Alarms and Events』を参照してください。

ローカルおよびピアのステート、装置、冗長管理の IP アドレス、ピアの冗長管理、冗長ポート、ピアの冗長ポート、ペア コントローラのピア サービス ポートなど、冗長ステートの詳細を表示できます。

これらの詳細を表示するには、**[モニター（Monitor）]** > **[管理対象要素（Managed Elements）]** > **[ネットワーク デバイス（Network Devices）]** > **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** > **[コントローラ グループ（Controller Group）]** > **[コントローラ（Controller）]** > **[デバイスの詳細（Device Details）]** > **[冗長性（Redundancy）]** > **[冗長性状態（Redundancy States）]** を選択します。

ピア サービス ポートの IP およびサブネット マスクの設定

ピア コントローラのステートが [StandbyHot] の場合にだけ、ピア サービス ポートの IP アドレスおよびサブネット マスクを設定できます。ピア サービス ポートの IP アドレスを設定する前に、DHCP がローカル サービス ポートで無効になっていることを確認します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 プライマリ コントローラまたはアクティブ コントローラが含まれるワイヤレス コントローラのグループを選択します。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 プライマリまたはアクティブ コントローラのデバイス名をクリックします。

ステップ 5 [設定（Configuration）] タブをクリックします。

ステップ 6 左側のサイドバー メニューで、[冗長性（Redundancy）] > [グローバル設定（Global Configuration）] を選択します。[グローバル コンフィギュレーション（Global Configuration）] ページが表示されます。

ステップ 7 次のフィールドに入力します。

1. [Peer Service Port IP]：ピア サービス ポートの IP アドレスを入力します。
2. [Peer Service Netmask IP]：ピア サービス サブネット マスクの IP アドレスを入力します。

ステップ 8 [Save] をクリックします。

ピア ネットワーク ルートの追加

ピア コントローラのステートが [StandbyHot] の場合にだけ、アクティブ コントローラでピア ネットワーク ルートを追加できます。新しいネットワーク ルート テーブルが維持されます。スタンバイ コントローラがアクティブになると、ネットワーク ルート テーブルのエントリは、ピア ネットワーク ルート テーブルのエントリとスワップされます。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 冗長管理インターフェイスの IP アドレスを設定したコントローラが含まれるワイヤレス コントローラのグループを選択します。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 冗長管理インターフェイスの IP アドレスを設定したコントローラの [デバイス名（Device Name）] をクリックします。

ステップ 5 [設定（Configuration）] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、**[冗長性（Redundancy）]** > **[ピア ネットワーク ルート（Peer Network Route）]** の順に選択します。

ステップ 7 [コマンドの選択（Select a command）] > [ピア ネットワーク ルートの追加（Add Peer Network Route）] > [実行（Go）] を選択します。[ピア ネットワーク ルートの詳細（Peer Network Route Details）] ページが表示されます。

ステップ 8 次のフィールドに入力します。

1. [IP アドレス（IP Address）]：ピア ネットワーク ルートの IP アドレスを入力します。
2. [IP ネットマスク（IP Netmask）]：ピア ネットワーク ルートのサブネット マスクを入力します。
3. [ゲートウェイ IP アドレス（Gateway IP Address）]：ピア ネットワーク ルート ゲートウェイの IP アドレスを入力します

ステップ 9 [保存（Save）] をクリックします。ピア ネットワーク ルートが追加されます。

セカンダリ サーバーのリセットおよびセカンダリ サーバーからのファイルのアップロード

セカンダリ サーバーが [StandbyHot] 状態であり、ハイアベイラビリティ ペアリング プロセスが完了している場合、セカンダリ サーバーをリセットできます。また、セカンダリ サーバーからプライマリ サーバーにファイルをアップロードすることもできます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 冗長管理インターフェイスの IP アドレスを設定したコントローラが含まれるワイヤレス コントローラのグループを選択します。このデバイス グループのメンバーが右側に表示されます。

ステップ 4 冗長管理インターフェイスの IP アドレスを設定したコントローラの [デバイス名（Device Name）] をクリックします。

ステップ 5 [設定（Configuration）] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、[冗長性（Redundancy）] > [冗長コマンド（Redundancy Commands）] の順に選択します。

ステップ 7 [管理コマンド（Administrative Commands）] で、[コマンドの選択（Select a command）] > [スタンバイのリセット（Reset Standby）] > [実行（Go）] を順に選択して、セカンダリ サーバーをリセットします。

ステップ 8 [アップロード/ダウンロード コマンド（Upload/Download Commands）] で、次のように操作します。

a) セカンダリ サーバーからプライマリ サーバーにファイルをアップロードするときに使用するトランスポート プロトコルを選択します（[TFTP] がデフォルトです）。

b) [コマンドの選択（Select a command）] > [スタンバイ コントローラのファイルのアップロード（Upload File from Standby Controller）] > [実行（Go）] を選択して、セカンダリ サーバーからプライマリ サーバーにファイルをアップロードします。

コントローラの冗長性の無効化

コントローラの冗長性を無効にすると、アクティブおよびスタンバイの両方のコントローラがリブートされます。冗長パラメータの監査の不一致を解消するには、デバイスから設定を更新する必要があります。アクティブ コントローラはスタンドアロン コントローラになり、スタンバイ コントローラはポートがすべて無効に設定されてリブートします。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] 領域で、[デバイス タイプ（Device Type）] を展開し、次に [ワイヤレス コントローラ（Wireless Controller）] を展開します。

ステップ 3 冗長性を無効にするコントローラが含まれるワイヤレス コントローラのグループを選択します。このデバイス グループのメンバーが右側に表示されます。

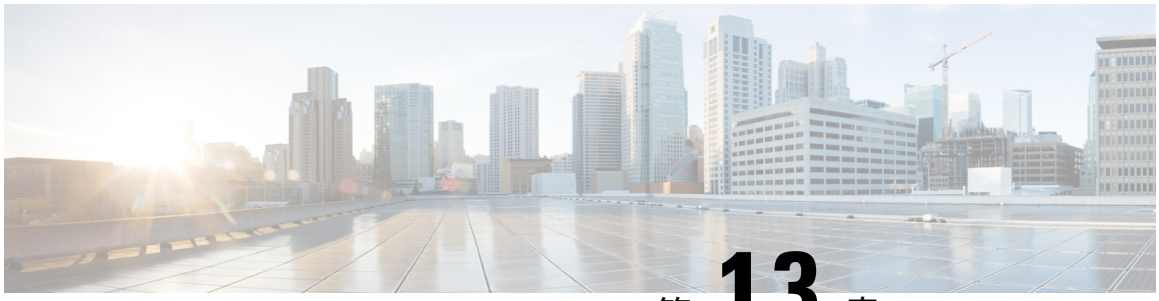
ステップ 4 冗長性を無効にするコントローラの [Device Name] をクリックします。

ステップ 5 [Configuration] タブをクリックします。

ステップ 6 左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[グローバル コンフィギュレーションの詳細（Global Configuration details）] ページが表示されます。

ステップ 7 選択したコントローラの [Redundancy Mode] の [Enabled] チェックボックスをオフにします。

ステップ 8 [Save] をクリックします。設定が保存され、システムがリブートされます。



第 13 章

トラフィック メトリックの管理

トラフィック メトリックの管理方法

（注） Mediatrace 機能は、最新の IOS リリースで廃止されました。

は、エンドポイントとサイト上でのリアルタイム転送プロトコル（RTP）と TCP のアプリケーション トラフィック パスの追跡をサポートしています。データ パスの追跡は、Cisco Medianet と Web Services Management Agent（WSMA）に依存します。どちらも、RTP と TCP のデータストリームに伴う問題を切り分けて修正するための Cisco IOS ソフトウェアと Catalyst スイッチの組み込み機能です。 は、Cisco Medianet と WSMA のすべてのバージョンをサポートしており、ルータ上でのこれらの機能の有効化を容易にします。

Cisco ネットワーク解析モジュール（NAM）トラフィック モニタリング データが利用可能ではない場合、 が Cisco Medianet Performance Monitor と Cisco IOS NetFlow を使用した RTP サービス パスのトレース（Mediatrace）をサポートします。適切に設定されていれば、Mediatrace は、RTP と TCP のアプリケーション問題を解決する最も有益なツールになります。

関連トピック

Mediatrace によるトラフィック メトリックの前提条件 （427 ページ）
ルータとスイッチ上での Mediatrace の設定 （429 ページ）
ルータとスイッチ上での WSMA 機能と HTTP（S）機能の設定 （430 ページ）

Mediatrace によるトラフィック メトリックの前提条件

の Mediatrace 機能を使用する前に、下記の「関連項目」に示す必須セットアップ タスクを完了する必要があります。これらの必須タスクは、シスコ ルータ（ISR、ISR G2、ASR）と NAM デバイスがネットワーク トラフィック（RTP と TCP）のパフォーマンス測定指標を監視するデータ（メトリック コレクション）ソースとして機能できるようにするために必要です。

関連トピック

NAM デバイスをデータ ソースとして使用するための の設定 （428 ページ）
ルータとスイッチをデータ ソースとして使用するように を設定する （429 ページ）

NAM デバイスをデータ ソースとして使用するための の設定

Cisco NAM を使用してネットワーク トラフィックを監視する場合は、RTP と TCP の両方のトラフィックのサービス パスを追跡するための次の手順を実行します。

ステップ 1 システムに NAM を追加します。この操作は、検出を使用して自動的に実行するか、または一括インポートあるいは Device Work Center を使用して手動で実行することができます（『Cisco Prime Infrastructure User Guide』の「*Add and Organize Devices*」を参照）。

ステップ 2 NAM データ収集を有効にします。手順は次のとおりです。

a) [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ ソース（Data Sources）] の順に選択します。

b) [NAM データ コレクタ（NAM Data Collector）] セクションで NAM を選択し、[有効（Enable）] を選択すると、選択した NAM でのデータ収集が有効化されます（『Cisco Prime Infrastructure User Guide』の「*Enable NAM Data Collection*」を参照）。

ステップ 3 組織のサイト構造を作成し、該当するサイトに主要ルータを割り当てます。

a) [マップ（Maps）] > [サイト マップ（Site Maps）] を選択します。

b) 1 つ以上のキャンパス、ビルディング、フロアを追加します。

ステップ 4 サイトと認可されたデータ ソースを関連付けます。

a) [Services] > [Application Visibility & Control] > [Data Deduplication] の順に選択します。

b) [データ重複除去の有効化（Enable Data Deduplication）] をクリックし、[適用（Apply）] をクリックします。その後で、ART、トラフィック分析、および音声/ビデオ データに関する信頼できるソースを割り当てることができます（データ重複排除の有効化 （176 ページ）を参照）。

ステップ 5 サイトとエンドポイント サブネットを関連付けます。

a) [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [エンドポイント アソシエーション（Endpoint Association）] の順に選択します。

b) サブネットとサイトを関連付けます（『Cisco Prime Infrastructure User Guide』の「*Associate Endpoints with a Site*」を参照）。

これに失敗した場合は、これらのエンドポイントに対して収集されたデータの中でサイトが [未割り当て（Unassigned）] に設定されます。

ステップ 6 Mediatrace と WSMA に対応するようにルータを設定します（『Cisco Prime Infrastructure User Guide』の「*Troubleshoot RTP and TCP Flows Using Mediatrace*」を参照）。

詳細については、「システム ジョブの制御」を参照してください。

ルータとスイッチをデータ ソースとして使用するように を設定する

シスコのルータとスイッチを使用してネットワーク トラフィックを監視する場合は、次の手順を実行して RTP と TCP の両方のフローのパス追跡を有効にします。

ステップ 1 組織のサイト構造を作成し、該当するサイトに主要ルータを割り当てます。

a) [マップ（Maps）] > [サイト マップ（Site Maps）] を選択します。

b) 1 つ以上のキャンパス、ビル、およびフロアを追加します（詳細については、『Cisco Prime Infrastructure User Guide』の「*Work With Site Maps*」の項を参照）。

ステップ 2 サイトと認可されたデータ ソースを関連付けます。

a) [Services] > [Application Visibility & Control] > [Data Deduplication] の順に選択します。

b) [データ重複除去の有効化（Enable Data Deduplication）] をクリックし、[適用（Apply）] をクリックします。その後で、ART、トラフィック分析、および音声/ビデオデータに関する信頼できるソースを割り当てることができます（データ重複排除の有効化 （176 ページ）を参照）。

ステップ 3 サイトとエンドポイント サブネットを関連付けます。

a) [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [エンドポイント アソシエーション（Endpoint Association）] の順に選択します。

b) サブネットとサイトを関連付けます（『Cisco Prime Infrastructure User Guide』の「*Associate Endpoints with a Site*」の項を参照）。

これに失敗した場合は、デフォルトで、これらのエンドポイントに対して収集されたデータの中でサイトが [未割り当て（Unassigned）] に設定されます。

ステップ 4 互換性のあるルータを Cisco Medianet Performance Monitor 用に設定します（「ルータとスイッチ上での Mediatrace の設定」を参照）。

ステップ 5 Mediatrace と WSMA 用にルータを設定します（『Cisco Prime Infrastrucutre User Guide』の「*Troubleshoot RTP and TCP Flows Using Mediatrace*」の項を参照）。

関連トピック

データ重複排除の有効化 （176 ページ）

ルータとスイッチ上での Mediatrace の設定

は、ルータとスイッチ上での Mediatrace の設定にすぐに使えるテンプレートを提供しています。サービスパスを追跡する場合は、必ず、結果に含めるすべてのスイッチとルータにこの設定を適用する必要があります。

Mediatrace でサポートされるすべてのルータとスイッチのリストを確認するには、「テンプレートの展開」を参照してください。

はじめる前に

次のタスクを実行する必要があります。

- NAM デバイスをデータ ソースとして使用するための の設定

- ルータとスイッチをデータ ソースとして使用するための の設定

[Mediatrace - レスポンダ - 設定（Mediatrace-Responder-Configuration）] テンプレートを設定するために、次の手順を実行します。

ステップ 1 [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）]>[Mediatrace - レスポンダ - 設定（Mediatrace-Responder-Configuration）] を選択します。

ステップ 2 テンプレートに関して必要な情報を入力します（「Field reference for the template」参照）。

ステップ 3 [新規テンプレートとして保存（Save as New Template）] をクリックし、新しいテンプレートに名前と説明を付けます。[保存（Save）] をクリックします。

ステップ 4 [展開（Deploy）] をクリックし、新しいテンプレートを展開します。

詳細については、「Enabling NetFlow Data Collection」、「Field Reference: Mediatrace-Responder-Configuration」、および「Deploying Templates 」を参照してください。

ルータとスイッチ上での WSMA 機能と HTTP（S）機能の設定

サービス パスの詳細を追跡するには、HTTP プロトコル経由の Web Services Management Agent（WSMA）がルータとスイッチ上で Mediatrace コマンドを実行する必要があります。この機能は、「ルータとスイッチ上での Mediatrace の設定」（「関連項目」を参照）の手順に従って設定したときと同じルータとスイッチのセット上で行います。

ステップ 1 [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）]>[HTTP-HTTPS サーバーおよび WSMA 設定 - IOS（HTTP-HTTPS Server and WSMA Configuration-IOS）] の順に選択します。

ステップ 2 テンプレートに関して必要な情報を入力します（「Field reference for the template」を参照）。

必ず HTTP プロトコルを有効化してください。現在のバージョンの Prime Infrastructure では、HTTPS 経由の WSMA がサポートされていません。

ステップ 3 [新規テンプレートとして保存（Save as New Template）] をクリックし、新しいテンプレートに名前と説明を付けます。[保存（Save）] をクリックします。

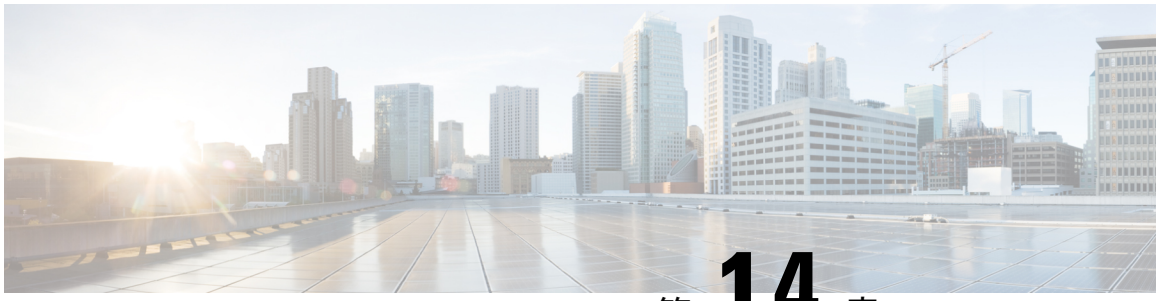
ステップ 4 [展開（Deploy）] をクリックして、新しいテンプレートを展開します。

デバイスを Prime Infrastructure に追加する際には、そのデバイスの HTTP ユーザーとパスワードを指定する必要があります。

詳細については、「Field Reference: HTTP-HTTPS Server and WSMA Configuration-IOS」、「Deploying Templates」、および「Add Devices to Prime Infrastructure」を参照してください。

関連トピック

ルータとスイッチ上での Mediatrace の設定 （429 ページ）



第 14 章

NATed Prime を使用した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの管理

NATed Cisco Prime Infrastructure を使用した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの管理

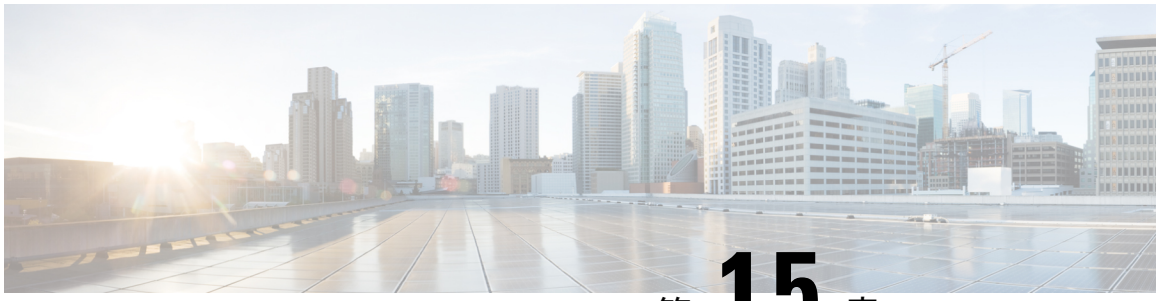
Cisco Catalyst 9800 ワイヤレス コントローラ デバイスを検出する場合、Cisco Prime Infrastructure が NATed の場合は、Prime Server の LocalHostResources.properties ファイルで Prime NATed IP を更新する必要があります。

（注） TAC サポートの助けを借りて、opt/CSCOlumos/conf/rfm/classes/com/aes/common/net/LocalHostResources.properties ファイルを変更する必要があります。これは、Prime バージョン 3.10.4 から適用されます。

1. ルートまたは管理者権限で Cisco Prime Infrastructure サーバーにログインします。
2. LocalHostResources.properties ファイルを編集し、以下のように Prime NATed IP アドレスで「PiNatIp」を更新します。

```
AddressTypes=ipv4
ManagementInterface=
PeerServerInterface=
ClientInterface=
HostName=
PiNatIp=XX.XX.XX.XX
```

3. ファイルを保存します。
4. ncs stop と ncs start を使用して、サーバーを再起動します。



第 15 章

ネットワーク容量の変更を計画する

ネットワークの容量変更の計画方法

保証機能を備えた Cisco Prime Infrastructure では、ネットワークの操作上の即応性とパフォーマンス品質の維持や向上に不可欠となる各種の主要パフォーマンス評価指標を表示およびレポートすることができます。この情報は、増え続けるネットワーク負荷に対応する上で、特に重要となります。

（注） この章で説明されている機能を使用するには、Prime Infrastructure 実装に保証ライセンスを含める必要があります。これらの機能は、ASR プラットフォームでのみサポートされています。

以下のワークフローは、ブランチオフィスの大幅なスタッフ増員が計画されていることを知らされたばかりのネットワーク管理者を前提としたものです。この変更計画では、ブランチ LAN にユーザを追加し、追加されるユーザの多くが WAN アプリケーションを使用することになります。この場合、管理者は、使用状況とトラフィックの輻輳についてブランチの主要インターフェイスをモニタする必要があります。これにより、ブランチ LAN のユーザが増えた場合に、ユーザが利用する WAN アプリケーションのパフォーマンスが低下するかどうかがわかります。全体像を十分に把握するためには、ブランチで使用するあらゆる WAN アプリケーションの短期および長期のパフォーマンス傾向を調べなければなりません。

はじめる前に

- 以下のようにして、[使用率がトップ N の WAN インターフェイス（Top N WAN Interfaces by Utilization）] ダッシュレットをセットアップします。
  - [モニター（Monitor）] > [モニタリング ポリシー（Monitoring Policies）] の順に選択して、インターフェイス ヘルス テンプレートを作成します。
  - [インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）] の順に選択し、インターフェイスを選択して [グループに追加（Add

to Group）] をクリックした後、グループとして [WAN インターフェイス（WAN Interfaces）] を選択します。

- SNMP ポーリングを有効にします。

ステップ 1 [Dashboard] > [Overview] > [General] の順に選択します。

ステップ 2 リモート ブランチ オフィスを WAN に接続するルータの WAN インターフェイスの使用状況に関する統計を表示するには、[Network Interface] を選択します。

ステップ 3 [Top N Interface Utilization] ダッシュレットを追加します（まだ追加されていない場合）。このダッシュレットには、インターフェイスごとに、WANインターフェイスをホストしているデバイスのデバイス名とIP、インターフェイス名と速度、送信/受信の最大使用率、平均使用率、および最後にポーリングされた使用率が表示されます。

ステップ 4 先月の使用状況に関する統計を表示するには、[Top N Interface Utilization] ダッシュレット タイトルの横にある [Clock] アイコンをクリックして、[Filters] 行の [Time Frame] を [Past 4 Weeks] に設定します。

ステップ 5 [トップ N のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットで、ユーザーの追加先となるブランチの WAN インターフェイスを検索します。

ステップ 6 [Interface] 列で、インターフェイスの名前をクリックし、[Dashboard] > [Performance] > [Interface] の順に選択して、そのインターフェイスの [Interface] ページを表示します。このページには、この単一インターフェイスに関する以下のダッシュレットが表示されます。

- Interface Details
- Interface Tx and Rx Utilization
- Top N Applications
- Top N Clients
- Number of Clients Over Time
- DSCP Classification
- QoS Class Map Statistics
- oS Class Map Statistics Trend
- Classification

ステップ 7 このページの [Top Application Traffic Over Time] ダッシュレットに注目します。このダッシュレットには、このインターフェイスでのトラフィックが最も多かった上位 10 個までのアプリケーションが色分けされたマップが表示されます。

ステップ 8 長期的なパフォーマンスの傾向を把握するには、[Top Application Traffic Over Time] というダッシュレット タイトルの隣にある [Clock] アイコンをクリックして、[Time Frame] を[Past 24 Hours]、[Past 4 Weeks]、または [Past 6 Months] に変更します。

グラフ内で特定の急増箇所にズームインするには、グラフ下部のパン ハンドルとズーム ハンドルを使用します。

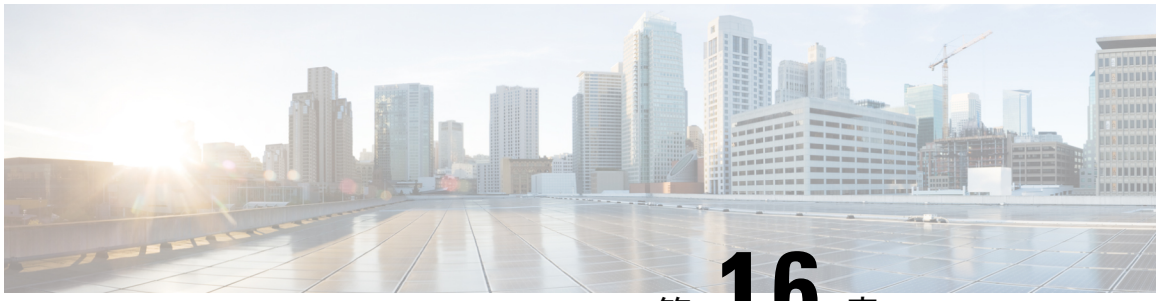
ステップ 9 このインターフェイス ページと同じデータを素早くレポートするには、[Reports] > [Report Launch Pad] の順に選択します。次に、[パフォーマンス（Performance）]>[インターフェイスの概要（Interface Summary）] を選択します。レポートのフィルタやその他の条件を指定し、[Report Criteria] で同じインターフェイスを選択してから、[Run] をクリックします。

次のタスク

以下の表に、テストに使用されるISPプロファイルを示します（このプロファイルは、Caida.org インターネット プロファイルと非常によく似ています）。

表 *19:* インターネット プロファイル：*1Gbps* あたりのトラフィック プロファイル

	TCP	UDP	HTTP	RTP	Total
接続レート（1秒あたりのフロー）	5,000	5,000	800	10	10,000
同時フロー数	150,000	150,000	50,000	300	300,000
パケットのレート	150,000	40,000	50,000	15,000	199,000
関連する帯域幅（bps）	900Mbps	100Mbps	295Mbps	25Mbps	1 Gbps
パケット サイズ（派生）	750	313	738	208	658
同時アクティブ ユーザ数	60,000 台	フロー数から導出			



第 16 章

後方互換性の有効化

Catalyst 9800 WLC デバイスと Cisco Prime Infrastructure 間の後方互換性の有効化

Cisco Prime Infrastructure 3.10 はデフォルトで Catalyst 9800 17.6.1 をサポートしていますが、Catalyst 9800 16.12.x バージョンに切り替えるオプションがあります。バージョンを切り替えるには、以下の手順に従ってください。

重要 常に、1 つのバージョン（16.12.x または 17.6.1）のコントローラのみがアクティブになります。デフォルトでは、Cisco Prime Infrastructure 3.10 を最初にインストールすると、Catalyst 9800 17.6.1 のサポートがアクティブになります。

始める前に

nscdiag にアクセスするための管理者権限があることを確認してください。

ncsdiag を有効にします。詳細については、最新の Cisco Prime Infrastructure コマンドリファレンスガイド [英語] の「ncs run diag」セクションを参照してください。

ステップ 1 **https://<prime ip>/ncsdiag/coralService.html** url を使用して Catalyst 9800 バージョンを変更します。

ステップ 2 [Coral Service] ページで、[Change coral] をクリックして、Cisco Prime Infrastructure 3.10 でサポートされている現在の Catalyst 9800 バージョンを変更します。

例：[Coral Service] ページで、[Current Coral] バージョンが「Coral 17」と表示されている場合、[Change Coral] をクリックすると、「Coral 16」に切り替わります。

図 *3 : Coral Service*

ステップ 3 Cisco Prime Infrastructure が高可用性モードの場合：

- Catalyst 9800 17.6.1 を使用していて、Catalyst 9800 16.12.x に切り替える場合は、プライマリおよびセカンダリの Cisco Prime Infrastructure インスタンスが同期するまで待つ必要があります。
- Catalyst 9800 16.12.x を使用していて、Catalyst 9800 17.6.1 に切り替える場合は、スタンバイの Cisco Prime Infrastructure の /opt/CSCOlumos パスから **.coral16** ファイルを手動で削除する必要があります。

ステップ 4 Cisco Prime Infrastructure が高可用性モードでない場合は、ステップ 5 に進んでください。

ステップ 5 Prime Infrastructure の再起動

重要 バージョン切り替え後のサーバーの再起動は、新しい Catalyst 9800 の変更を有効にするために不可欠です。

ステップ 6 /opt/CSCOlumos/coralinstances/coral2/coral/bin ディレクトリに移動し、**./coral version 1** コマンドを実行して、Catalyst 9800 バージョンが変更されているか確認します。

バージョン **Catalyst 9800 17.6.1** に変更した場合、期待される結果は次のとおりです。

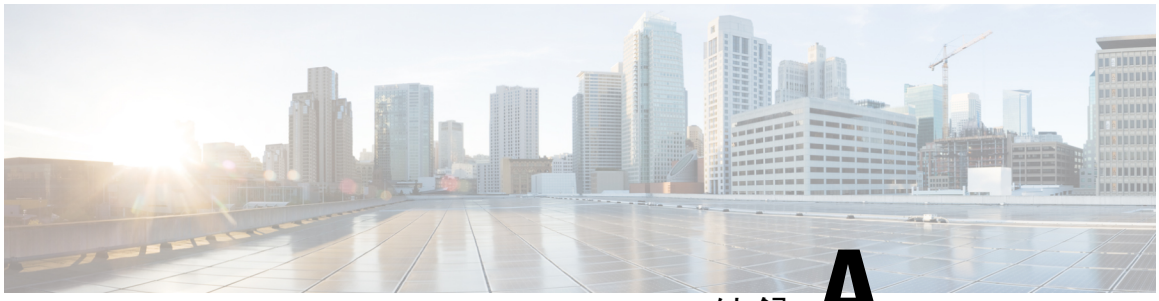
```
ade # cd /opt/CSCOlumos/coralinstances/coral2/coral/bin/
ade # sudo ./coral version 1
BuildTime: 2021-07-30_14.55
ReleaseDate: Fri-30-Jul-21-16:16
BuildArch: x86_64
Platform: CORAL
Build: 17.06.01
BuildPath: /nobackup/mcpre/release/BLD-V17_06_01_FC6/binos
Version: 17.06.01.0.250.1627682159..Bengaluru
InstallVersion: 1.0.0
BootArch: Linux Name Space Container
Host System uptime: 0 days, 23 hours, 36 minutes, 13 seconds [84973.16 sec]
Coral service uptime: 0 days, 23 hours, 15 minutes, 53 seconds [83753.89 sec]
```

バージョン **Catalyst 9800 16.12.x** に変更した場合、期待される結果は次のとおりです。

```
ade # sudo ./coral version 1
BuildTime: 2019-07-30_16.43
ReleaseDate: Tue-30-Jul-19-08:15
BuildArch: x86_64
Platform: CORAL
Build: 16.12.01
BuildPath: /scratch/mcpre/release/BLD-V16_12_01_FC4/binos
Version: 16.12.1.0.544.1564530231..Gibraltar
InstallVersion: 1.0.0
BootArch: Linux Name Space Container
```

```
Host System uptime: 4 days, 22 hours, 24 minutes, 7 seconds [426247.80 sec]
Coral service uptime: 4 days, 0 hours, 16 minutes, 28 seconds [346588.20 sec]


ade #
```



付録 A

ベスト プラクティス：サーバー セキュリティの強化

以下のセクションで、セキュリティ上の弱点を個別に排除または制御して、サーバーセキュリティを高める方法について説明します。

セキュアでないサービスの無効化

使用する予定のない、セキュアでないサービスは無効化する必要があります。たとえば、TFTP および FTP はセキュアなプロトコルではありません。これらのサービスは、通常、ネットワーク デバイスと Prime Infrastructure の間でファームウェアやソフトウェアのイメージを転送するために使用されます。また、システムバックアップを外部ストレージに転送するためにも使用されます。このようなサービスにはセキュアなプロトコル（SFTP または SCP など）を使用することを推奨します。

FTP および TFTP サービスを無効にするには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [サーバー（Server）]** の順に選択します。

ステップ 3 [FTP] および [TFTP] に対して、[無効化（Disable）] ボタンを選択します。

ステップ 4 Cisco Prime Infrastructure を再起動して、設定の更新を適用します。

root アクセスの無効化

管理ユーザーは、トラブルシューティングの目的で基盤となるオペレーティング システムに対する root シェル アクセスを有効化できます。このアクセスは、シスコ サポート チームが製品関連の運用上の問題をデバッグするために使用されます。このアクセスは無効な状態のままにし、必要な場合にのみを有効化することを推奨します。root アクセスを無効化するには、コマンド ラインから root_disable コマンドを実行します（CLI から接続する方法 （147 ページ）を参照）。

インストール時に、Prime Infrastructure は Web root ユーザー アカウントも作成し、このアカウントに使われるパスワードを入力するようインストール担当者に促します。Prime Infrastructure サーバーとその Web ユーザー インターフェイスに初めてログインする際には、Web root アカウントが必要です。通常の動作にこのアカウントを使用しないことを推奨します。このアカウントの用途は、日常的な運用およびネットワーク管理を行うための適切な権限を持つユーザー ID と、Prime Infrastructure 自体を管理するための管理ユーザー ID を作成することです。これらのユーザー アカウントを作成したら、インストール時に作成されたデフォルトの「Web root」アカウントを無効化し、その後は、管理ユーザー ID を使用してユーザー アカウントを作成します。

シェル パスワードを忘れた場合は、管理者パスワードを復元するための以下の手順に従って、シェル パスワードを復元（およびリセット）できます。「仮想アプライアンスの管理者パスワードの回復」を参照してください。管理者パスワードを復旧した場合 Prime Infrastructure サーバーを再起動する必要が生じるため、システムが 20 分程度ダウンする可能性があります。

root アカウントを無効にするには、次の手順に従います。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法 （147 ページ）を参照）。「端末設定」モードは開始しないでください。

ステップ 2 次のコマンドを入力して、Web root アカウントを無効化します。

PIServer/admin# **ncs webroot disable**

Prime Infrastructure により Web root アカウントが無効化されます。

ステップ 3 プロンプトで次のコマンドを入力して、root シェル アカウントを無効化します。

PIServer/admin# **shell disable**

root シェル アカウントのパスワードを入力するよう Prime Infrastructure から求められます。パスワードを入力すると、root シェル アカウントの無効化が完了します。

SNMPv2 の代わりに SNMPv3 を使用する

SNMPv3 は、SNMPv2 よりもセキュリティ機能が高いプロトコルです。SNMPv2 の代わりに SNMPv3 を使用して管理が行われるように管理対象デバイスの設定にすることにより、ネットワーク デバイスと Prime Infrastructure サーバー間の通信のセキュリティを強化できます。

新しいデバイスの追加時、デバイスの一括インポート時、またはデバイス検出の一環として、SNMPv3 の有効化を選択できます。それぞれの作業の実行手順については、「関連項目」を参照してください。

関連トピック

SNMPv3 を使用したデバイスの追加 （445 ページ）
SNMPv3 を使用したデバイスのインポート （445 ページ）
SNMPv3 を使用した検出の実行 （446 ページ）

SNMPv3 を使用したデバイスの追加

新規デバイスを追加する際に SNMPv3 を指定するには、次の手順に従います。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。
ステップ 2 [デバイスの追加（Add Device）] を選択します。
ステップ 3 [SNMP パラメータ（SNMP Parameters）] エリアの [バージョン（Version）] で、[v3] を選択します。
ステップ 4 他のフィールドに適宜入力してから、[追加（Add）] をクリックします。

関連トピック

SNMPv3 を使用したデバイスのインポート （445 ページ）
SNMPv3 を使用した検出の実行 （446 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （445 ページ）

SNMPv3 を使用したデバイスのインポート

デバイスを一括インポートする際に、SNMPv3 の使用を指定するには、次の手順に従います。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。
ステップ 2 [一括インポート（Bulk Import）] を選択します。[一括インポート（Bulk Import）] ページが表示されます。
ステップ 3 デバイス追加サンプル テンプレートを [Bulk Import] ページの [here] リンクからダウンロードします。
ステップ 4 任意の CSV 互換アプリケーションを使用してテンプレート ファイルを編集します。CSV インポート ファイル内で、デバイスを表す各行ごとに次の手順を実行します。

a) [snmp version] 列に 3 と入力します。
b) [snmpv3_user_name]、[snmpv3_auth_type]、[snmpv3_auth_password]、[snmpv3_privacy_type]、および [snmpv3_privacy_password] の各列に適切な値を入力します。
c) 使用するデバイスに合わせて、適宜他の列に入力します。

ステップ 5 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択し、[一括インポート（Bulk Import）] をクリックして、変更した CSV ファイルをインポートします。

関連トピック

SNMPv3 を使用したデバイスの追加 （445 ページ）
SNMPv3 を使用した検出の実行 （446 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （445 ページ）

SNMPv3 を使用した検出の実行

SNMPv3 をデバイス検出の一部として指定するには、次の手順に従います。

ステップ 1 [Inventory] > [Device Management] > [Discovery] の順に選択します。[検出ジョブ（Discovery Jobs）] ページが表示されます。
ステップ 2 ページの右上隅にある [検出設定（Discovery Settings）] リンクをクリックします。[検出設定（Discovery Settings）] ページが表示されます。
ステップ 3 [New] をクリックして、新しい SNMP v3 クレデンシャルを追加します。
ステップ 4 必要に応じてフィールドに入力します。
ステップ 5 [保存（Save）] をクリックして、SNMPv3 の設定を保存し、使用を開始します。

関連トピック

SNMPv3 を使用したデバイスの追加 （445 ページ）
SNMPv3 を使用したデバイスのインポート （445 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （445 ページ）

外部 AAA による認証

ユーザー アカウントとパスワードを RADIUS や TACACS+ などのセキュアな認証プロトコルを実行する専用のリモート認証サーバーにより一元管理すると、管理がより安全になります。

外部 AAA サーバーを使用してユーザーを認証するように Prime Infrastructure を設定できます。Prime Infrastructure グラフィック ユーザー インターフェイス（GUI）から外部認証をセットアップするには、[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）] ページにアクセスする必要があります。コマンドライン インターフェ

イス（CLI）から外部認証をセットアップすることもできます。それぞれの手法による AAA のセットアップ手順については、「関連項目」を参照してください。

関連トピック

GUI からの外部 AAA の設定 （447 ページ）
CLI からの外部 AAA の設定 （447 ページ）

GUI からの外部 AAA の設定

リモート ユーザー認証を GUI から設定するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [TACACS+] または [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [RADIUS] を選択します。

ステップ 3 該当するフィールドに TACACS+ または RADIUS サーバーの IP アドレスと共有秘密を入力します。

ステップ 4 [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 Settings）] の順に選択します。

ステップ 5 必要に応じて AAA モードを設定します。

関連トピック

外部 AAA による認証 （446 ページ）
CLI からの外部 AAA の設定 （447 ページ）

CLI からの外部 AAA の設定

リモート ユーザー認証を CLI から設定するには、次の手順に従います。

ステップ 1 CLI から接続する方法 （147 ページ）の説明に従って、コマンドラインを使用して Prime Infrastructure にログインします。必ず「端末設定」モードにしてください。

ステップ 2 プロンプトで次のコマンドを入力し、外部 TACACS+ サーバーをセットアップします。

PIServer/admin/terminal# aaa authentication tacacs+ server **tacacs**-ip key plain *shared-secret*

ここで、

- **tacacs**-ip はアクティブな TACACS+ サーバーの IP アドレスです。
- *shared-secret* はアクティブな TACACS+ サーバーのプレーンテキストの共有秘密です。

ステップ 3 プロンプトで次のコマンドを入力し、管理者権限を持つユーザーを作成します。このユーザーは上記の AAA サーバーによって認証されます。

PIServer/admin/terminal# **username** *username password* **remote role admin email** *emailID*

ここで、

- *username* はユーザー ID の名前です。
- *password* はユーザーのプレーンテキストのパスワードです。
- *emailID* はユーザーのメール アドレスです（オプション）。

関連トピック

外部 AAA による認証 （446 ページ）
GUI からの外部 AAA の設定 （447 ページ）

NTP 更新認証の有効化

Network Time Protocol（NTP）バージョン 4 は、サーバーの日付と時刻の更新を認証し、サーバー セキュリティを強化する重要な方法です。Prime Infrastructure では最大 3 台の NTP サーバーを設定できます。

認証された NTP 更新をセットアップするには、次の手順に従います。

ステップ 1 CLI から接続する方法 （147 ページ）の説明に従って、コマンドラインで Prime Infrastructure にログインします。必ず「端末設定」モードにしてください。

ステップ 2 プロンプトで次のコマンドを入力し、外部 NTPv4 サーバーをセットアップします。

PIServer/admin/terminal# ntp server serverIP userID plain password

ここで、

- serverIP は、使用する認証 NTPv4 サーバーの IP アドレスです。
- userID は、NTPv4 サーバーの MD5 キー ID です。
- password は NTPv4 サーバーに対応する md5 プレーン テキスト パスワードです。

  例：ntp server 10.81.254.131 20 plain MyPassword

ステップ 3 NTP 認証が適切に動作していることを確認するには、次のコマンドを実行してテストします。

- NTP 更新の詳細を確認する：sh run
- NTP 同期の詳細を確認する：sh ntp

Prime Infrastructure サーバー上の OCSP 設定の有効化

Online Certificate Status Protocol（OCSP）は、OCSP レスポンダを使用して Web クライアントの証明書ベース認証を可能にします。通常、OCSP レスポンダの URL は証明書の Authority Information Access（AIA）から読み取られます。フェールオーバー メカニズムとして、Prime Infrastructure サーバー上で同じ URL を設定できます。

OCSP レスポンダのカスタム URL をセットアップするには、次の手順に従います。

ステップ 1 CLI から接続する方法（147 ページ）の説明に従って、コマンドラインを使用して、Prime Infrastructure サーバーにログインします。「端末設定」モードは開始しないでください。

ステップ 2 プロンプトで次のコマンドを入力し、クライアント証明書認証を有効化します。

PIServer/admin# **ocsp responder custom enable**

ステップ 3 プロンプトで次のコマンドを入力し、カスタム OCSP レスポンダ URL を設定します。

PIServer/admin# **ocsp responder set url** *Responder#URL*

ここで、

- *Responder#* は定義する OCSP レスポンダの数です（たとえば、1、2 など）。
- *URL* はクライアントの CA 証明書から取得される OCSP レスポンダ の URL です。

  Responder# 値と *URL* 値の間にスペースを入れないことに注意してください。

ステップ 4 Prime Infrastructure サーバーで定義されている既存のカスタム OCSP レスポンダを削除するには、次のコマンドを使用します。

PIServer/admin# **ocsp responder clear url** *Responder#*

削除する OCSP レスポンダの数が不明な場合は、**show security-status** コマンドを使用して、サーバー上で現在設定されている OCSP レスポンダを確認します。詳細については、「サーバー セキュリティ ステータスの確認」を参照してください。

ローカル パスワード ポリシーの設定

Prime Infrastructure 独自の内部認証を使用してユーザーをローカルで認証する場合、強力なパスワードの選択ルールを適用することにより、システムのセキュリティを向上させることができます。

これらのポリシーは、ローカルの Prime Infrastructure ユーザー ID のパスワードにのみ影響します。集中型つまりリモート AAA サーバーで Prime Infrastructure ユーザーを認証している場合、AAA サーバーの機能を利用して、同様の保護を適用できます。

ローカル パスワード ポリシーを適用するには：

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles, & AAA）] > [ローカル パスワード ポリシー（Local Password Policy）] の順に選択します。

ステップ 3 適用するパスワードポリシーの横にあるチェックボックスを選択します。パスワードポリシーには以下が含まれます。

- パスワードに含める必要がある最小文字数。
- パスワードにユーザ名または「cisco」（またはこれらの一般的な並べ替え）を使用しない。
- ルート パスワードに「public」を使用しない。
- どのパスワード文字についても連続する繰り返しは 3 回以下。
- パスワードには大文字、小文字、数字、特殊文字という文字クラスのうち 3 つから少なくとも 1 文字ずつを含める必要がある。
- パスワードは ASCII 文字のみを含む必要があるかどうか。
- パスワードを再利用するまでの最小経過日数。
- パスワードの有効期限。
- パスワード失効の事前警告。

パスワード ポリシー要件に応じて、次のパスワード ポリシーも指定できます。

- 最小パスワード長（文字の数）。
- パスワード再利用間の最小経過期間。
- パスワード有効期間。
- 将来のパスワード失効に関してユーザへの警告を開始する事前日数。

ステップ 4 [Save] をクリックします。

個々の TCP/UDP ポートの無効化

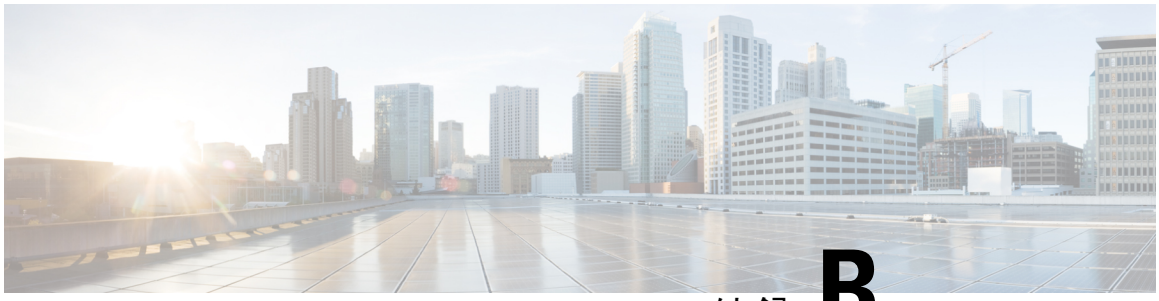
次の表に、Prime Infrastructure が使用する TCP および UDP ポート、これらのポート上で通信するサービスの名前、およびポート使用における製品の目的を示します。「安全」列は、Prime Infrastructure の機能に影響を与えることなくポートとサービスを無効化できるかどうかを示します。

ベスト プラクティス：サーバー セキュリティの強化

表 *20 : Prime Infrastructure* の *TCP/UDP* ポート

[ポート（Port）]	サービス名（Service Name）	目的	安全?
21/tcp	FTP	デバイスとサーバの間のファイル転送	Y
22/tcp	SSHD	システムへ、またシステムからのSCP、SFTP、およびSSH接続で使用される	N
69/udp	TFTP	デバイスとサーバの間のファイル転送	Y
80/tcp	HTTP	Nexusデバイスのプロビジョニング	Y
162/udp	SNMP-TRAP	SNMPトラップを受信する	N
443/tcp	HTTPS	製品へのプライマリWebインターフェイス	N
514/udp	SYSLOG	Syslogメッセージを受信する	N
1522/tcp	Oracle	Oracle/JDBCデータベース接続：これらは内部サーバ接続とハイ アベイラビリティ ピア サーバとの接続の両方を含みます。	N
8082/tcp	HTTPS	ヘルス モニタリング	N
8087/tcp	HTTPS	HAセカンダリ システムのソフトウェア アップデート	N
9991/udp	NETFLOW	Netflowストリームを受信する（保証ライセンスがインストールされている場合に有効）	N
9992/tcp	PI Tomcatプロセス	保証内のLyncモニタリング	N
61617/tcp	JMS（over SSL）	リモートのプラグ アンド プレイ ゲートウェイ サーバーとの対話用	あり

ベスト プラクティス：サーバー セキュリティの強化



付録 B

内部 SNMP トラップの生成

内部トラップ生成について

適切に設定されている場合、Prime Infrastructure は通知宛先に SNMP トラップを送信し、Prime Infrastructure システム自体で発生する次のイベントを通知します。

- Prime Infrastructure サーバーの内部ソフトウェア プロセスのクラッシュまたは障害。
- 登録、フェールオーバー、およびフェールバックを含む高可用性（HA）状態の変更。
- CPU、メモリ、ディスクの高い使用率。
- CPU、ディスク、ファン、または電源装置（PSU）の障害。
- バックアップ障害、証明書の失効、ライセンス違反。

これらの内部 SNMP トラップに関連付けられているシビラティ（重大度）を編集できます。CPU、メモリ、およびディスクの使用率に関するしきい値限度を変更することもできます（これらの SNMP トラップはシステム ハードウェアが設定されたしきい値を超えた場合に送信されます）。

その他のイベント（CPU、ディスク、ファン、および PSU の障害、または HA 状態の変更など）の場合は、障害や HA 状態の変更が検出されるとすぐに SNMP トラップが送信されます。

SNMP トラップは次のイベントに対してカスタマイズされたしきい値とシビラティ（重大度）に基づいて生成されます。

- サーバ プロセス障害
- 高可用性操作
- CPU 使用率
- メモリ使用率

- ディスク使用率
- ディスク障害
- ファン障害
- PSU の障害
- バックアップ障害
- 証明書の失効

Prime Infrastructure は SNMPv2 通知も SNMPv3 通知も送信しません。

（注） デバイスのトラップが無効になっていても、Prime Infrastructure にはポートの使用不可を示すアラームが表示されます。

Prime Infrastructure SNMP トラップ タイプ

次の表に、Prime Infrastructure が独自の機能に対して生成する SNMP トラップを示します。リストはトラップ タイプ別になっています。表では、各トラップが生成される状況のほか、提案される操作対応を説明しています。

表 *21 : Prime Infrastructure SNMP* トラップ タイプ

トラップ タイプ	トラップ	説明
アプライアンス プロセス障害	FTP、MATLAB、TFTP	Prime Infrastructure サーバーで FTP、MATLAB、または TFTP プロセスの障害が発生した場合、サーバーは常に障害トラップを生成し、サーバーのヘルス モニター インスタンスはプロセスを自動的に再起動することを試みます。ヘルス モニターが 3 回の試行で再起動できなかった場合、HA サーバーは別の障害トラップを送信します。
アプライアンス プロセス障害	NMS	サーバーの NMS プロセスが開始するか、または障害を起こすと、Prime Infrastructure サーバーのヘルス モニター スレッドは常に、対応するトラップを生成します。 プロセスを停止または再起動するには、サーバーに CLI から接続し、管理者でログインします。次に、適宜、nms stop コマンドまたは nms start コマンドを実行します。
HA 操作	登録トリガー	Prime Infrastructure はプライマリ サーバーが HA 登録を開始すると常に、このトラップを生成します。登録が失敗するか成功するかは関係ありません。HA 登録がトリガーされると、プライマリ サーバーは操作の開始を示すトラップを生成します。
HA 操作	登録成功	HA 登録が成功すると、プライマリ サーバーは成功を示すこのトラップを生成します。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
HA 操作	登録失敗	HA 登録が何らかの理由で失敗した場合、障害が発生したプライマリまたはセカンダリ サーバーは、失敗を示すトラップを生成します。このトラップには、障害に関する詳細が含まれます。支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。
HA 操作	フェールオーバー トリガー	このトラップは Prime Infrastructure プライマリ サーバーに障害が発生した場合、自動的に生成され、フェールオーバーの一部として、セカンダリ サーバーのアクティブ化を試みます（フェールオーバーの成否やセカンダリ サーバーのアクティブ化の成否に関係なく行われます）。HA 設定（登録時の設定）に手動フェールオーバー タイプがある場合、ユーザーはフェールオーバーをトリガーする必要があります。そうでない場合、ヘルス モニターはセカンダリ サーバーへのフェールオーバーを自動的にトリガーします。 フェールオーバーがトリガーされたことを示すために 1 個のトラップが生成されます。フェールオーバーが完了する前にトラップが送信されるため、セカンダリ サーバーにはロギングされません。
HA 操作	フェールオーバー成功	トリガーされたフェールオーバー操作が成功すると、セカンダリ サーバーは成功を示すトラップを生成します。ユーザーはセカンダリ サーバーのアラーム ブラウザでトラップを表示できます。
HA 操作	フェールオーバー失敗	トリガーされたフェールオーバー操作が失敗すると、失敗を示すトラップが生成されます。ユーザーは hm-#-#.log でトラップを表示できます（「Prime Infrastructure SNMP トラップのトラブルシューティング方法 （475 ページ）」を参照）。このトラップには、障害に関する詳細が含まれます。サポートが必要な場合は、Cisco TAC にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
HA 操作	フェールバック トリガー	このトラップはセカンダリ サーバーでプライマリ サーバーへのフェールバックがトリガーされると自動的に生成されます（フェールバックの成否に関係なく行われます）。プライマリ サーバーが復元された後、ユーザーはセカンダリ サーバー ヘルス モニターの Web ページにある [フェールバック（Failback）] ボタンを使用して、セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーする必要があります（自動のフェールバック オプションはありません）。トリガーされると、セカンダリ サーバーは操作の開始を示すトラップを生成します。
HA 操作	フェールバック成功	トリガーされたフェールバック操作が成功すると、セカンダリ サーバーは成功を示すトラップを生成します。フェールバック成功により、プライマリ サーバーは「アクティブ」状態に設定され、セカンダリ サーバーは「同期」状態に設定されます。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
HA 操作	フェールバック失敗	トリガーされたフェールバック操作が失敗すると、失敗を示すトラップが生成されます。障害はどちらのサーバーでも発生する可能性があるので、障害が発生したサーバーがトラップを生成します。ユーザーは hm-#-#.log およびノースバウンド管理サーバーでトラップを表示できます。 フェールバック失敗は自動ロールバックをトリガーし、セカンダリ サーバーは前のアクティブ状態に戻ることを試みます。この操作に失敗すると、セカンダリ サーバーはロールバック失敗を示す追加のトラップを生成します。この障害トラップには障害に関する詳細が含まれます。サポートが必要な場合は、Cisco TAC にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	CPU 使用率	トラップは CPU 使用率がプリセットされた使用率のしきい値を超える場合にのみ送信されます。これらのトラップを表示するには、トラップを生成したサーバーのジョブとアクティブ セッションを確認します。
ハードウェア トラップ	ディスク使用率	トラップはディスク使用率が設定されたディスク使用率のしきい値限度を超える場合にのみ送信されます。対応するには、/opt および /localdisk パーティションの下のディスク領域を解放してみます。Cisco TAC の指導なしで /opt/CSCOlumos の下のフォルダを削除しないでください。
ハードウェア トラップ	メモリ使用率	トラップはメモリ使用率が設定されたメモリ使用率のしきい値限度を超える場合にのみ SNMP トラップ レシーバに送信されます。
ハードウェア トラップ	ディスク障害	トラップはディスク障害が検出された場合に SNMP トラップ レシーバに送信されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	ファン障害	トラップはファン障害が検出された場合に SNMP トラップ レシーバに送信されます。トラップまたはアラーム メッセージに不良または欠落したファンが表示されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	PSU の障害	トラップは PSU 障害が検出された場合に SNMP トラップ レシーバに送信されます。トラップまたはアラーム メッセージに問題のある電源が表示されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
しきい値トラップ	バックアップ障害	Prime Infrastructure サーバー バックアップの毎日のバックグラウンド タスクで障害が検出されると、トラップが SNMP トラップ レシーバに送信されます。バックグラウンドタスクは毎日実行され、スケジュール設定された時刻にサーバーのバックアップが取得されます。ディスク領域の不足によりバックアップに失敗すると、そのイベントが処理されます。バックアップが正常に実行されると、アラームはクリアされます。
しきい値トラップ	バックアップしきい値	Prime Infrastructure でスケジュール設定された毎日のバックアップが、しきい値日数の間取得されなかった場合、ユーザーに通知されます。デフォルトのしきい値は 7 日です。バックアップが 7 日間取得されなかった場合、ユーザーはこのイベントによって通知されます。
しきい値トラップ	証明書有効期日	証明書が有効期日間近になると、トラップが SNMP トラップ レシーバに送信されます。証明書の有効期日の 15 日前になると Critical トラップが送信され、証明書の有効期日の 60 日前になると Major トラップが送信されます。
システム トラップ	ライフサイクル	ライフサイクル ライセンスは、デバイスの管理に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	保証	保証ライセンスは、NetFlow を Prime Infrastructure に送り込むデバイスの表示に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	コレクタ	コレクタ ライセンスは、Prime Infrastructure に送り込まれた NetFlow の量の表示に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	ライフサイクル ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。
システム トラップ	保証ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。
システム トラップ	コレクタ ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。

汎用 SNMP トラップの形式

次に、Prime Infrastructure の SNMP トラップ通知のシンタックスを示します。

Component：コンポーネント名、**Server**：Primary、Secondary、または Standalone、**Type**：Process、Sync、Activity など、**Service**：サービス名、**When**：Prime Infrastructure ライフサイクルでのフェーズ、**State**：サーバーの HA および HM の状態、**Result**：Warning、Failure、Success、Information、Exception、**MSG**：通知される SNMP トラップに関する自由形式のメッセージ

表 A-2 に、汎用トラップ形式の各属性について可能な値を示しています。

表 *22 :* 汎用 *SNMP* トラップ形式の属性値

属性	値
コンポーネント	Health Monitor または High Availability
サーバ	このトラップの送信元サーバ（Primary、Secondary、または Standalone）
タイプ	このトラップの原因となったアクションのタイプ（Process、Sync、Activity など）
サービス	この問題を報告した Prime Infrastructure サービス。取り得る値には、Registration、Failover、Failback、NMS、NCS、Health Monitor、All、Prime Infrastructure、Database、Disk Space などがあります。
日時（When）	このトラップが発生した Prime Infrastructure サーバーのライフサイクルにおける時点（Startup、Shutdown など）
状態（State）	サーバの状態（Standalone、Failover、Failback、Registration など）
結果	この SNMP トラップがレポートされている条件
MSG	各 SNMP トラップに固有の詳細を提供する自由形式のテキスト

ノースバウンド SNMP トラップとアラームのマッピング

次の表に、ノースバウンド トラップが Prime Infrastructure のイベントとアラームにマッピングされる仕組みに関する説明を示します。次の表の「イベント」列の項目は、「Prime Infrastructure Supported Events」ドキュメントの [イベント（Events）] タブの列名であり、追加情報が含まれています。たとえば、この表の MIB 変数「cWNotificationSubCategory」では、「*Supported Events*」ドキュメントの [イベント/アラーム条件（Event/Alarm Condition）] 列を調べ、転送されたイベントまたはアラームで報告または解決されている問題のタイプを調べます。

内部 SNMP トラップの生成

表 *23 :* ノースバウンド *SNMP* トラップとアラームのマッピング

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationIndex	なし。各トラップに対して一意に生成されます。	なし	なし	各ノースバウンド トラップが送信されると増加する（折り返して 1 に戻る）インデックス値。
cWNotificationTimestamp	alarmCreationTime	アラーム検出日時（Alarm Found At）	なし	関連付けられているアラームが作成された時刻。
cWNotificationUpdatedTimestamp	lastModifiedTimestamp	[タイムスタンプ（Timestamp）]（列）、[アラーム最終更新日時（Alarm Last Updated At）]	なし	関連付けられているアラームが最後に更新された時刻。
cWNotificationKey	applicationSpecificAlarmID	なし	なし	アラーム条件を一意に識別する（不明瞭な）文字列。これは基本的にアラームの「識別子」です。同じ cWNotificationKey で 2 つのノースバウンドトラップ（最初のトラップはシビラティ（重大度）がクリアされていない、2 番目のトラップはシビラティ（重大度）がクリアされている）を受信した場合は、最初のトラップで報告された問題が 2 番目のトラップでクリアされていると判断できます。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationCategory	category	カテゴリ（Category）	デフォルトカテゴリ	関連付けられているアラームのカテゴリ。実際の値は数値であり、「*Prime Infrastructure Supported Events*」ドキュメントに含まれている実際のカテゴリ名にマップできます。マッピングはMIBで使用可能です。
cWNotificationSubCategory	eventType	条件	イベント/アラーム条件	報告または解決されている問題のタイプを示します。
cWNotificationManagedObjectAddressType	なし	なし	なし	IPv4 を示します。
cWNotificationManagedObjectAddress	reportingEntityAddress	なし	なし	問題を報告するデバイスのアドレス。トラップの実際の送信元アドレスではない可能性があります。1 つのアドレスを管理アドレスとして使用して Prime Infrastructure にデバイスを追加したが、別のアドレスからトラップを送信した場合、この値はデバイスが追加されたときのアドレスになります。
cWNotificationSourceDisplayName	displayName	障害の原因（Failure Source）	なし	影響を受けたリソースの名前の表現。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationDescription	description (ciscoLwappIpsType, ciscoLwappIpsDescId, ciscoLwappIpsDescriptionParams)	メッセージ（Message）	Prime Infrastructure メッセージ	発生した問題または解決を示すメッセージ。これは通常、アラームの説明から取得されますが、WIPS アラームの場合は、他のフィールドから取得されます（左側の「関連付けられているアラームのフィールド」列を参照）。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationSeverity	severity	シビラティ（重大度）（Severity）	デフォルトのシビラティ（重大度）	

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
				アラームのシビラティ（重大度）。これは、CISCO-TC MIB で定義されているアラームのシビラティ（重大度）を数値で表したものです。値は、[クリア済み（1）（cleared(1)）]、[不確定（2）（indeterminate(2)）]、[クリティカル（3）（critical(3)）]、[メジャー（4）（major(4),）]、[マイナー（5）（minor(5)）]、[警告（6）（warning(6)）]、[情報（7）（info(7)）] です。イベントタイプのシビラティ（重大度）は必要に応じて変更できるため、シビラティ（重大度）が変更されている場合は、「*Prime Infrastructure Supported Events*」のシビラティ（重大度）と一致しないことがあります。シビラティ（重大度）は、ノースバウンドトラップを介して通知されるアラームの変更を制御することによって変更できます（つまり、[クリティカル（CRITICAL）] アラームのみがノースバウンドトラップになるように指定し、不要なアラームのシビラティ（重大度）を [クリティカル

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
				（CRITICAL）] から [メジャー（MAJOR）] に変更することができます）。
cWNotificationSpecialAttributes	すべてのアラーム フィールド	特定のアラーム フィールドに基づいて異なる	特定のアラーム フィールドに基づいて異なる	アラーム自体の内容（フィールドと値）が含まれます。
cWNotificationType	なし	なし	なし	トラップがアラームの作成/更新に基づいているか、またはイベントの作成に基づいているかを示します。一部のイベント（シビラティ（重大度）が [情報（Informational）] である場合）ではアラームが生成されないため、そのような情報イベントについては、ノースバウンドトラップを取得することができます。
cWNotificationVirtualDomains	なし	なし	なし	MIBから：「このオブジェクトは、cWNotificationTypeで表されるネットワーク条件の送信元が論理的に割り当てられる 1 つ以上の仮想ドメインの名前（カンマで区切られている）を表します」。たとえば、「root, California, San Jose」は、ネットワーク条件の送信元が論理的に複数の仮想ドメインに割り当てられていることを示します。

Prime Infrastructure SNMP トラップのリファレンス

次の表に、Prime Infrastructure で生成される SNMP トラップ通知の各クラスの詳細を示します。WCS ノースバウンド通知 MIB のマッピング済み OID は 1.3.6.1.4.1.9.9.712.1.1.2.1.12 です。この OID は、Prime Infrastructure のソフトウェア関連とハードウェア関連のトラップによって参照されます。ノースバウンド MIB のトラップ OID は、常に 1.3.6.1.4.1.9.9.712.0.1 です。詳細については、CISCO-WIRELESS-NOTIFICATION-MIB の一覧と関連項目の「ノースバウンド SNMP トラップにアラーム マッピング」を参照してください。

表 *24 :* アプライアンス プロセス障害

目的	特定の Prime Infrastructure サーバー サービスが停止していること、およびヘルス モニターがそのサービスの再起動を試みていることをユーザーに通知します。
送信される条件	トラップは、ヘルス モニターがプロセスを再起動しようとするときに送信されます。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: Health Monitor, Server: Primary, Type: Process, Service: NCS, When: Startup, State: Stand Alone, Result: Warning, MSG: FTP service is down and an attempt will be made to automatically restart the service
MSG コンテンツ	PI **servername**：serviceName のサービスが停止しています。このサービスを自動的に再起動することを試みます。
値のタイプ、範囲、および制約	MSG 属性中の **servername** パラメータは、Prime Infrastructure サーバーのホスト名の値を取得します。このパラメータは、NMS Server、FTP、TFTP、または MATLAB のいずれかの値を取ることができます。

表 *25 : Failback*

目的	セカンダリ サーバーからプライマリ サーバーへのフェールバックが開始されたことをユーザーに通知します。
送信される条件	このトラップは、セカンダリ サーバーからプライマリ サーバーへのフェールバックが開始されると送信されます。フェールバック操作が失敗するか成功するかは関係ありません。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: High Availability, Server: Secondary, Type: Process, Service: Database, When: Failback, State: Primary Failback, Result: Failure, MSG: Error in Failback: Failed to recover the primary database using Duplicate DB.

内部 SNMP トラップの生成

表 *26 :* フェールオーバー

目的	セカンダリ サーバーが起動したときにユーザーに通知します。
送信される条件	プライマリ サーバーが停止し、フェールオーバーの一部として、セカンダリ サーバーがアクティブになると、トラップが生成されます。フェールオーバー操作が失敗するか成功するかは関係ありません。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: High Availability, Server: Secondary, Type: Process, Service: Failover, When: Failover, State: Secondary Synching, Result: Success, MSG: Completed failover from primaryAddressInfo to secondaryAddressInfo.
MSG コンテンツ	MSG 属性中の primaryAddressInfo および secondaryAddressInfo は、サーバーの IP アドレスまたはホスト名を取得します。

表 *27 : CPU* 使用率

目的	CPU 使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	CPU 使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1.
例	CPU Utilization is at 85% and has violated threshold limit of 80%.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_CPU, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178170, severity=4, eventType=APPLIANCE_CPU_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=CPU, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: CPU Utilization is at 3% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

内部 SNMP トラップの生成

表 *28 :* ディスク使用率

目的	ディスク使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	ディスク使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	PI opt disk volume utilization is at 85% and has violated threshold limit of 0%. PI opt disk volume is within the recommended disk usage range, less than 80% used. PI local disk volume utilization is at 85% and has violated threshold limit of 80%. PI local disk volume is within the recommended disk usage range, less than 80% used.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。
ワイヤ形式	[OctetString] applicationSpecificAlarmID=LocaldiskDiskSpace, reportingEntityAddress=10.77.240.246,lastModifiedTimestamp=Sun Mar 23 08:44:06 UTC 2014, alarmCreationTime=2014-03-14 13:29:31.069, eventCount=1, mayBeAutoCleared=false, instanceId=483484, severity=1, eventType=NCS_LOW_DISK_SPACE, authEntityId=93093, previousSeverity=MAJOR, category=System(17), transientNameValue={}, source=10.77.240.246, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=PI localdisk volume is within the recommended disk usage range, less than 70% used., isAcknowledged=false, authEntityClass=983576643, displayName=NCS 10.77.240.246
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

表 *29 :* メモリ使用率

目的	メモリ使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	メモリ使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1.
例	Memory Utilization is at 85% and has violated threshold limit of 80%.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。

内部 SNMP トラップの生成

ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_MEMORY, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178171, severity=4, eventType=APPLIANCE_MEM_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=MEMORY, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: MEMORY Utilization is at 38% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

表 *30* : ディスク障害

目的	ドライブが欠落しているか不良であることをユーザーに通知します。
送信される条件	ディスク ドライブの問題が検出されると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Component: Appliance, Server: Standalone, Type: Hardware, Message: A problem was detected in the RAID device. A rebuild is in progress. Device at enclosure 252 slot ZERO is bad or missing. Drive0 is missing or bad.
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。システムの再起動時にドライブが取り外されていると、トラップが生成されます。

表 *31* : ファン障害

目的	ファンに障害が発生したときにユーザーに通知します。
送信される条件	ファンに障害が発生すると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Fan is either bad or missing.
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_Fan1, lastModifiedTimestamp=Sun Apr 13 15:24:11 IST 2014, alarmCreationTime=Sun Apr 13 15:24:11 IST 2014, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=2875873, severity=4, eventType=APPLIANCE_FAN_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=Fan1, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Fan is either bad or missing, isAcknowledged=false, displayName=NMS: 10.77.240.246
制限事項と警告	問題が次のポーリング サイクルの前に解決するか、またはシステムの再起動時にファンが取り外された場合、トラップは生成されません。

内部 SNMP トラップの生成

表 *32 : PSU* の障害

目的	電源装置が取り外されていることをユーザーに通知します。
送信される条件	電源が取り外されると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing.
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_PS1, lastModifiedTimestamp=19 Aug 2015 01:41:26 UTC, alarmCreationTime=19 Aug 2015 01:41:26 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=1424089, severity=4, eventType=APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=x.x.x.x, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing, isAcknowledged=false, displayName=NMS:x.x.x.x
制限事項と警告	PSU が取り外されている場合、Prime Infrastructure で電源アラームが発生し、トラップが送信されます。システムのシャットダウン時に PSU が取り外されている場合、Prime Infrastructure は再起動までアクティブにならず、アラームは生成されません。

表 *33 :* サービス エンジン停止の識別

目的	ISE が到達不能な場合に、ユーザーに通知します。
送信される条件	ISE が停止または到達不能の場合、トラップがポーリングによって生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Identity services engine **ISEIPAddress** is unreachable.

表 *34 :* ライセンス違反

目的	Prime Infrastructure が実際に管理しているデバイスの数が管理のライセンス付与数を超えるとユーザーに通知します。
送信される条件	Prime Infrastructure インベントリに余分なデバイスを追加したジョブの完了後の翌日午前2時10分 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Number of managed devices **N** is greater than licensed devices **N**. Please purchase and install a license that will cover the number of managed devices, or remove unused devices from the system.

表 35 : Prime Infrastructure にバックアップ用の十分なディスク容量がありません

目的	Prime Infrastructure がバックアップを実行するために、指定のディレクトリに十分な容量を確保できない場合にユーザーに通知します。
送信される条件	Prime Infrastructure がサーバー バックアップ ジョブを実行し、指定されたバックアップ リポジトリ（つまり「defaultrepo」）が 100 % フルである場合は毎回。トラップはジョブが完了した後に生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Prime Infrastructure with address **localIPAddress** does not have sufficient disk space in directory **directoryName** for backup. Space needed: **Needed** GB, space available **Free** GB.

表 36 : Prime Infrastructure の電子メールの失敗

目的	電子メール通知の送信試行に失敗したことをユーザーに通知します。
送信される条件	このトラップは、Prime Infrastructure が無効なユーザーに電子メール通知を送信しようとした場合、または、Prime Infrastructure で電子メール サーバーを指定せずに電子メール通知が有効になっている場合に、ポーリングによって生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Prime Infrastructure with address **localIPAddress** failed to send email. This may be due to possible SMTP misconfiguration or network issues.

表 37 : ノースバウンド OSS サーバーが到達不能です

目的	ノースバウンド通知サーバーが到達不能であることをユーザーに通知します。
送信される条件	このトラップは、宛先のノースバウンド通知サーバーが到達不能の場合にポーリングによって生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Northbound notification server **OSSIPAddress** is unreachable. NCS alarms will not be processed for this server until it is reachable.

Prime Infrastructure トラップの設定

以下のセクションでは、Prime Infrastructure トラップ通知を設定および使用する方法について説明します。

関連トピック

通知の設定 （471 ページ）
トラップの送信に使用するポート （472 ページ）

通知の設定

Prime Infrastructure にノースバウンド SNMP トラップ通知を送信させるには、[Prime Infrastructure イベント通知（Prime Infrastructure Event Notification）] ページと [通知宛先（Notification Destiantion）]ページの両方で正しい設定を行う必要があります。設定が完了すると、トラップは、次の SNMP イベントのしきい値とシビラティ（重大度）に関連付けられた値に基づいて生成されます。

- アプライアンス プロセス障害
- HA 操作
- CPU、ディスク、およびメモリの使用率
- ディスク、ファン、および PSU の障害
- バックアップ障害、証明書有効期日、ライセンス違反

各イベントに関連付けられるしきい値とシビラティ（重大度）を編集し、関連イベントのトラップ生成を有効または無効に設定できます。

ステップ 1 ルート ドメイン権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [システム イベント設定（System Event configuration）] の順に選択します。

ステップ 3 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントのシビラティ（重大度）（Event Severity）] レベルを [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、メモリ使用率、ライクサイクル、アシュアランス、およびコレクタのトラップについては、[しきい値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。しきい値設定が NA と表示されるイベントのしきい値は設定できません。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) バックアップしきい値、証明書の失効（重大）、ライフサイクル ライセンス、アシュアランス ライセンス、およびコレクタ ライセンスのトラップについては、[しきい値（Threshold）] に日数（x-y の形式。x は最小日数値、y は最大日数値）を入力します。

e) [イベント ステータス（Event Status）] を [有効（Enabled）] または [無効（Disabled）] に設定します。[有効（Enabled）] に設定すると、このイベントに対応するトラップが生成されます。

f) CPU、ディスク、メモリの使用率について、[アラームの反復の作成とクリア（Create and Clear Alarm Iteration）] の値を入力します。デフォルト値は 2 です。反復値を設定した後の最初のポーリングの所要時間は、入力された反復値（分単位）の 2 倍です。その後のポーリングはいずれも 20 分しかかかりません。

デフォルトのポーリング時間は 20 分です。

ステップ 4 完了したら、[保存（Save）] をクリックして変更を保存します。

関連トピック

アラーム通知先の設定 （285 ページ）

トラップの送信に使用するポート

Prime Infrastructure はトラップを通知宛先のポート 162 に送信します。このポートは現時点ではカスタマイズできません。ノースバウンド管理システムは、[通知宛先（Notification destination）] Web ページで自分自身を登録する必要があります（アラーム通知先の設定 （285 ページ） を参照）。

電子メール サーバー設定の構成

Prime Infrastructure で電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メール サーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 管理者権限のユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールおよび通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** の順に選択します。

ステップ 3 [プライマリ SMTPサーバー（Primary SMTP Server）] で、Prime Infrastructure で使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、[ポート（Port）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力します。仮想 IP アドレスを [Hostname/IP] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 4 [接続セキュリティ（Connection Security）] ドロップダウンリストからいずれかのオプションを選択します。使用可能なオプションは、[プレーンテキスト（Plain Text）]、[STARTTLS]、および [SSL/TLS] です。

（注） 対応するポート番号を [ポート（Port）] テキストボックスに入力する必要があります。

ステップ 5 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。

ステップ 6 [送信者および受信者（Sender and Receivers）] で、Prime Infrastructure サーバーの正当なメール アドレスを入力します。

ステップ 7 （任意）[件名（Subject）] テキスト ボックスに件名を入力します。

ステップ 8 完了したら、[保存（Save）] をクリックします。

関連トピック

SNMP トラップのイベントとアラームの表示 （473 ページ）
SNMP トラップのイベントとアラームのフィルタ処理 （473 ページ）

SNMP トラップのアラームの消去 （475 ページ）
Prime Infrastructure SNMP トラップのトラブルシューティング方法 （475 ページ）
通知の設定 （471 ページ）
トラップの送信に使用するポート （472 ページ）

SNMP トラップのイベントとアラームの表示

Prime Infrastructure の内部 SNMP トラップのすべてのイベントとアラームは[システム（System）] カテゴリに分類されます。これらは Prime Infrastructure の [アラームおよびイベント（Alarms and Events）] ダッシュボードで表示できます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

SNMP トラップのイベントとアラームのフィルタ処理

Prime Infrastructure のフィルタ機能を使用して、アラームの表示をシステム カテゴリだけに絞り込んだり、条件と演算子の組み合わせを使用して、明確に限定したアラームのリストに焦点を合わせたりすることができます。以下のセクションで、この方法について説明します。

関連トピック

クイック フィルタを使用した SNMP トラップ用のフィルタ処理 （473 ページ）
高度なフィルタを使用する SNMP トラップのフィルタ処理 （474 ページ）

クイック フィルタを使用した SNMP トラップ用のフィルタ処理

Prime Infrastructure のクイック フィルタを使用すると、特定のテーブル列にフィルタを適用することで、テーブル内のデータにすばやく焦点を合わせることができます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 3 [表示（Show）] ドロップダウン リストで、[クイック フィルタ（Quick Filter）] を選択します。Prime Infrastructure はテーブル ヘッダー フィールドのリストを表示し、[シビラティ（重大度）（Severity）]、[メッセージ（Message）]、および [カテゴリ（Category）] などのクイック フィルタを実行できます。

ステップ 4 [カテゴリ（Category）] フィールドに、「System」と入力します。Prime Infrastructure にはシステム アラームだけが表示されます。

ステップ 5 クイックフィルタをクリアするには、[表示（Show）]ボックスの横に表示される漏斗アイコンをクリックします。

高度なフィルタを使用する SNMP トラップのフィルタ処理

Prime Infrastructure の高度なフィルタを使用すると、複数のタイプのデータと論理演算子を組み合わせたフィルタ（「次を含まない（Does not contain）」、「等しくない（Does not equal）」、「次で終わる（Ends with）」など）を適用して、テーブル内のデータを絞り込むことができます。たとえば、カテゴリに基づいてアラーム テーブルをフィルタにかけ、さらにシビラティ（重大度）でフィルタリングすることで、データを減らすことができます（次の手順を参照）。高度なフィルタを保存して、後で再利用することもできます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 [モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択します。

ステップ 3 [表示（Show）] ドロップダウン リストで、[高度なフィルタ（Advanced Filter）] を選択します。Prime Infrastructure はフィルタ内の最初のルールの条件を示すテーブル ヘッダーを表示します。

ステップ 4 次のように、最初のルールを完成させます。

a) 最初のフィールドで、ドロップダウン リストから [Category] を選択します。
b) 2 番目のフィールドで、ドロップダウン リストから [Contains] を選択します。
c) ルールの 3 番目のフィールドに、[System] を入力します。
d) [実行（Go）] をクリックします。Prime Infrastructure にはシステム アラームだけが表示されます。

ステップ 5 プラス記号のアイコンをクリックして別のルールを追加し、次のように、2番目のルールを完成させます。

a) 最初のフィールドで、ドロップダウンリストから[シビラティ（重大度）（Severity）]を選択します。
b) 2 番目のフィールドで、ドロップダウン リストから [equals (=)] を選択します。
c) ルールの 3 番目のフィールドで、ドロップダウン リストから [メジャー（Major）] を選択します。
d) [実行（Go）]をクリックします。Prime Infrastructure はシビラティ（重大度）がメジャーのシステム アラームのみを表示します。

必要に応じてこの手順を繰り返します。

ステップ 6 高度なフィルタを保存するには、[Save] アイコンをクリックし、フィルタの名前を入力します。

ステップ 7 高度なフィルタをクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

詳細については、SNMP トラップのアラームの消去 （475 ページ）を参照してください。

関連トピック

Prime Infrastructure SNMP トラップのトラブルシューティング方法 （475 ページ）
通知の設定 （471 ページ）
トラップの送信に使用するポート （472 ページ）
SNMP トラップのイベントとアラームの表示 （473 ページ）

SNMP トラップのイベントとアラームのフィルタ処理 （473 ページ）

SNMP トラップのアラームの消去

アラーム リストに含まれるアラームは、ステータスを [認知済み（Acknowledged）] から [クリア済み（Cleared）] に変更することで削除できます。これらのアラームに対して電子メールは生成されません。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 3 アラームを選択し、**[ステータスの変更（Change Status）] > [確認（Acknowledge）]** または **[ステータスの変更（Change Status）] > [クリア（Clear）]** を選択します。

Prime Infrastructure SNMP トラップのトラブルシューティング方法

Prime Infrastructure の内部トラップおよび関連する通知で問題が生じた場合は、次の点を確認してください。

ステップ 1 Prime Infrastructure サーバーから通知宛先に ping を実行し、Prime Infrastructure と管理アプリケーションの間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** を選択し、ログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

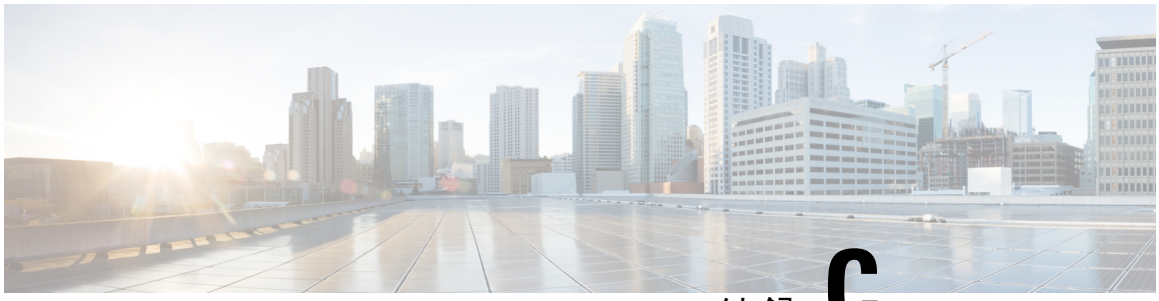
- ncs_nb.log：これは、Prime Infrastructure が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これは、最近のその他の Prime Infrastructure アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。
- hm-#-#.log：これはヘルス モニター アクティビティのすべてのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

内部 SNMP トラップの生成

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポートケースを開き、疑わしいログ ファイルをケースに添付してください。

関連トピック

Prime Infrastructure SNMP トラップ タイプ （454 ページ）
Prime Infrastructure SNMP トラップのリファレンス （465 ページ）
Prime Infrastructure トラップの設定 （470 ページ）



付録 C

プラグ アンド プレイ ゲートウェイのハイ アベイラビリティの設定

シスコ プラグ アンド プレイ ゲートウェイ HA の機能

の以前のリリースは、次のモードのいずれかで単一のシスコ プラグ アンド プレイ ゲートウェイをサポートしていました。

- プラグ アンド プレイ ゲートウェイ スタンドアロン サーバー モード
- プラグ アンド プレイ ゲートウェイ統合サーバー モード

HA はこの両方のソリューションで使用できず、シスコ プラグ アンド プレイ ゲートウェイはセカンダリ サーバーに自動的には接続されません。また、セカンダリ サーバーに手動でリダイレクトする必要があります。

は、現在のリリースの HA でプラグ アンド プレイ ゲートウェイをサポートしています。シスコ プラグ アンド プレイ HA 機能の目的は以下を可能にすることです。

- セカンダリ スタンバイ プラグ アンドプレイ ゲートウェイを提供することによる、スタンドアロン サーバー プラグ アンド プレイ ゲートウェイ上の HA。
- スタンドアロン プラグ アンド プレイ ゲートウェイと HA 間の HA サポート。
- 統合プラグ アンド プレイ ゲートウェイに対する HA サポート。

シスコ プラグ アンド プレイ ゲートウェイ HA の前提条件

シスコ プラグ アンド プレイ ゲートウェイの HA 機能を使用する前に、次の手順を実行する必要があります。

- プライマリとセカンダリの サーバーを設定します。これらは、プラグ アンド プレイ ゲートウェイ スタンドアロン サーバーからアクセスできる必要があります。詳細については、ハイ アベイラビリティの設定 （341 ページ） を参照してください。
- メッセージ キュー ポート 61617 とヘルス モニター ポート 8082 に使用されるプライマリとセカンダリの SSL サーバー証明書が、IP アドレスが異なる HA モードのプライマリ サーバーとセカンダリ サーバーから抽出できることを確認します。詳細については、ハイ アベイラビリティのセットアップ （359 ページ）を参照してください。
- 仮想 IP アドレス ベースの HA の場合は、プライマリ サーバとセカンダリ サーバの両方にその仮想 IP アドレスと証明書を割り当てる必要があります。詳細については、HA での仮想 IP アドレッシングの使用 （348 ページ）を参照してください。
- HA の役割を担うサービスに応じて、 サーバー メッセージ キュー ポート 61617 のいずれかを常時アクティブにする必要があります。
- プライマリとセカンダリのプラグ アンド プレイ ゲートウェイ仮想マシンをインストールします。OVA ファイルからの仮想マシンのインストール方法については、最新の『Cisco Prime Infrastructure Quick Start Guide』を参照してください。

Prime Infrastructure HA 用のスタンドアロン シスコ プラグ アンド プレイ ゲートウェイのセットアップ

HA の Cisco Prime Infrastructure サーバーは次の 2 つのモードで設定できます。

- プライマリ サーバとセカンダリ サーバの仮想 IP アドレス。詳細については、HA での仮想 IP アドレッシングの使用 （348 ページ）を参照してください。
- プライマリ サーバーとセカンダリ サーバーで別々の IP アドレス。詳細については、ハイ アベイラビリティのセットアップ （359 ページ）を参照してください。

セットアップ手順に少し変更を加えることにより、両方のモードで機能するように、スタンドアロン シスコ プラグ アンド プレイ ゲートウェイを設定できます。

関連トピック

仮想 IP アドレスが割り当てられた HA の （479 ページ）
IP アドレスが異なる HA の （479 ページ）

仮想 IP アドレスが割り当てられた HA の

は、アクティブなサーバーに応じて、プライマリ サーバーとセカンダリ サーバー上を移動する仮想 IP アドレスで設定できます。シスコ プラグ アンド プレイ ゲートウェイのセットアップ中に HA の の仮想 IP アドレスを入力します。

に統合されたプラグ アンド プレイ ゲートウェイは、同じ仮想 IP アドレスがアクティブ ノードに転送される場合に機能します。Prime Infrastructure に統合されたシスコ プラグ アンド プレイ ゲートウェイは、仮想 IP アドレスを使用するように自動的に設定されます。シスコ プラグ アンド プレイ ゲートウェイの設定で必要な特定の設定はありません。

関連トピック

IP アドレスが異なる HA の （479 ページ）

IP アドレスが異なる HA の

は、IP アドレスが異なるプライマリ サーバーとセカンダリ サーバーで設定できます。シスコ プラグ アンド プレイ ゲートウェイの設定では、詳細セットアップで **pnp setup advance** コマンドを実行して、次の情報を入力します。

- プライマリ IP アドレス。
- セカンダリ サーバーを設定する場合は、プロンプトで y を入力します。
- セカンダリ IP アドレス。

コマンドの実行方法については、『Command Reference Guide for Cisco Prime Infrastructure』を参照してください。

（注） に統合されたシスコ プラグ アンド プレイ ゲートウェイは、プライマリ サーバーとセカンダリ サーバーに別々の IP アドレスが割り当てられている場合は機能しません。アクティブ ノードに基づいて、ブートストラップ設定を変更する必要があります。

関連トピック

シスコ プラグ アンド プレイ ゲートウェイ HA の前提条件 （478 ページ）
Prime Infrastructure HA 用のスタンドアロン シスコ プラグ アンド プレイ ゲートウェイのセットアップ （478 ページ）
HA のシスコ プラグ アンド プレイ ゲートウェイの削除 （482 ページ）
シスコ スタンドアロン プラグ アンド プレイ ゲートウェイ サーバー HA のセットアップ （480 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA と の組み合わせ （483 ページ）

シスコ スタンドアロン プラグ アンド プレイ ゲートウェイ サーバー HA のセットアップ

シスコ スタンドアロン プラグ アンド プレイ ゲートウェイは、フェールオーバー用のセカンダリ サーバで HA に設定することもできます。HA のシスコ プラグ アンド プレイ ゲートウェイは、必ず、アクティブ ノードの仮想 IP アドレスで設定されます。HA のスタンドアロン プラグ アンド プレイ ゲートウェイをセットアップする場合は、次の手順を実行する必要があります。

- 2 つの到達可能なシスコ プラグ アンド プレイ ゲートウェイを別々の IP アドレスでインストールします。
- プライマリ シスコ プラグ アンド プレイ ゲートウェイで **pnp setup** または **pnp setup advance** コマンドを実行します。詳細については、『Command Reference Guide for Cisco Prime Infrastructure』を参照してください。セットアップの終了時点で、プライマリ サーバーによって、自動的にセカンダリ シスコ プラグ アンド プレイ ゲートウェイが設定されます。
- プライマリ シスコ プラグ アンド プレイ ゲートウェイ HA サーバーで HA を設定する場合は、プロンプトで **y** を入力します。

（注） HA の を使用したスタンドアロン シスコ プラグ アンド プレイ ゲートウェイは、プライマリからセカンダリへの自動フェールオーバーを備えています。手動フェールオーバーは使用できません。

HA の を使用したスタンドアロン シスコ プラグ アンド プレイ ゲートウェイは、セカンダリ サーバーからプライマリ サーバーに手動または自動でフェールバックするように設定できます。

pnp セットアップの一部として、シスコ プラグ アンド プレイ ゲートウェイの仮想 IP アドレス、仮想ホスト名、IP アドレス、およびセカンダリ サーバーのユーザー名とパスワードを入力します。セットアップ中にプロンプトが表示されたら、手動フェールバックの場合は **0** を、自動フェールバックの場合は **1** を入力します。

（注） 手動フェールバックをお勧めします。フラッピング インターフェイスなどのシナリオでは、フェールオーバーとフェールバックが連続して発生するため、自動フェイルバックはお勧めしません。

関連トピック

シスコ プラグ アンド プレイ ゲートウェイのステータス （481 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA の機能 （477 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA のセットアップ
シスコ プラグ アンド プレイ ゲートウェイ HA と の組み合わせ （483 ページ）

シスコ プラグ アンド プレイ ゲートウェイのステータス

シスコ プラグ アンド プレイ ゲートウェイ のステータス インターフェイスは、次のステータスに関する詳細情報を提供します。

HA ステータス：

- セットアップ中に仮想 IP アドレスが入力された場合は、このステータスにアドレスだけが表示されます。シスコ プラグ アンド プレイ ゲートウェイ ステータスでは、プライマリ サーバーとセカンダリ サーバーのどちらに接続されているかは識別できません。
- シスコ プラグ アンド プレイ HA ステータス

両方のゲートウェイが稼働している場合は、別のシスコ プラグ アンド プレイ ゲートウェイ プロセスのステータスとともに、シスコ プラグ アンド プレイ ゲートウェイがアクティブ モードで表示されます。このステータスには、表内の追加の値として、プライマリ サーバとセカンダリ サーバ間の接続ステータスも表示されます。

シスコ プラグ アンド プレイ ゲートウェイ サーバーのステータスをチェックするには、そのゲートウェイ サーバーにログインして、**pnp status** コマンドを実行します。ゲートウェイ サーバーの状態が表示されます。

コマンドの実行方法については、『Command Reference Guide for Cisco Prime Infrastructure』を参照してください。

```
SERVICE                          |  MODE                 |  STATUS        |  ADDITIONAL
INFO
-------------------------------------------------------------------------------------------
System                           |                       |  UP            |
-------------------------------------------------------------------------------------------
Event Messaging Bus              |  PLAIN TEXT           |  UP            |  pid: 6808
CNS Gateway Dispatcher           |  PLAIN TEXT           |  UP            |  pid: 7189,
port: 11011
CNS Gateway                      |  PLAIN TEXT           |  UP            |  pid: 7223,
port: 11013
CNS Gateway                      |  PLAIN TEXT           |  UP            |  pid: 7262,
port: 11015
CNS Gateway                      |  PLAIN TEXT           |  UP            |  pid: 7306,
port: 11017
CNS Gateway                      |  PLAIN TEXT           |  UP            |  pid: 7410,
port: 11019
CNS Gateway                      |  PLAIN TEXT           |  UP            |  pid: 7493,
port: 11021
CNS Gateway Dispatcher           |  SSL                  |  UP            |  pid: 7551,
port: 11012
CNS Gateway                      |  SSL                  |  UP            |  pid: 7627,
port: 11014
CNS Gateway                      |  SSL                  |  UP            |  pid: 7673,
port: 11016
CNS Gateway                      |  SSL                  |  UP            |  pid: 7793,
port: 11018
CNS Gateway                      |  SSL                  |  UP            |  pid: 7905,
port: 11020
CNS Gateway                      |  SSL                  |  UP            |  pid: 7979,
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           |  Connection:
1, Connection Detail: ::ffff:10.104.105.170:61617
bgl-dt-pnp-ha-216/admin#
SERVICE                         |  MODE                 |  STATUS       |  ADDITIONAL
INFO
-------------------------------------------------------------------------------------------
System                          |                       |  UP           |
-------------------------------------------------------------------------------------------
Event Messaging Bus             |  PLAIN TEXT           |  UP           |  pid: 6426
CNS Gateway Dispatcher          |  PLAIN TEXT           |  UP           |  pid: 7107,
port: 11011
CNS Gateway                     |  PLAIN TEXT           |  UP           |  pid: 7141,
port: 11013
CNS Gateway                     |  PLAIN TEXT           |  UP           |  pid: 7180,
port: 11015
CNS Gateway                     |  PLAIN TEXT           |  UP           |  pid: 7224,
port: 11017
CNS Gateway                     |  PLAIN TEXT           |  UP           |  pid: 7263,
port: 11019
CNS Gateway                     |  PLAIN TEXT           |  UP           |  pid: 7309,
port: 11021
CNS Gateway Dispatcher          |  SSL                  |  UP           |  pid: 7381,
port: 11012
CNS Gateway                     |  SSL                  |  UP           |  pid: 7537,
port: 11014
CNS Gateway                     |  SSL                  |  UP           |  pid: 7581,
port: 11016
CNS Gateway                     |  SSL                  |  UP           |  pid: 7685,
port: 11018
CNS Gateway                     |  SSL                  |  UP           |  pid: 7855,
port: 11020
CNS Gateway                     |  SSL                  |  UP           |  pid: 7902,
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           |  Connection:
1, Connection Detail: ::ffff:10.104.105.170:61617
PnP Gateway Monitoring          |  SSL                  |  UP           |  port: 11010
PnP Gateway HA                |  SSL                |  UP           |  Primary Server
 is in Active state
bgl-dt-pnp-ha-217/admin#
```

HA のシスコ プラグ アンド プレイ ゲートウェイの削除

スタンドアロン シスコ プラグ アンド プレイ ゲートウェイ内のプライマリ IP アドレスとセカンダリ IP アドレスが異なる の HA 設定を削除するには、**pnp setup advance** 詳細セットアップコマンドを実行し、プロンプトが表示されたら n を入力します。

シスコ プラグ アンド プレイ ゲートウェイ HA を削除する場合は、pnp setup または pnp setup advance コマンドを実行し、プロンプトが表示されたら n を入力します。

詳細については、『Command Reference Guide for Cisco Prime Infrastructure』を参照してください。

（注） シスコ プラグ アンドプレイ ゲートウェイ HA を削除する場合、管理者は手動で、動的ポート割り当て **cns event** コマンドを変更し、HA がオフになったらセカンダリ サーバーを使用停止にする必要があります。シスコ プラグ アンド プレイ ゲートウェイ セカンダリ サーバーは、使用停止にされなければ、仮想 IP アドレスで動作を継続します。

関連トピック

シスコ プラグ アンド プレイ ゲートウェイ HA と の組み合わせ （483 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA の制限 （484 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA の機能 （477 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA のセットアップ

シスコ プラグ アンド プレイ ゲートウェイ HA と の組み合わせ

シスコ プラグ アンドプレイ ゲートウェイ機能は、 との HA 用のさまざまな設定を可能にします。使用可能な設定オプションに応じて、以下のようなさまざまな組み合わせがあります。

- HA を備えていないスタンドアロン シスコ プラグ アンド プレイ ゲートウェイ（単一のシスコ プラグ アンド プレイ ゲートウェイ）
  - HA を備えていない サーバー。
  - 仮想 IP アドレスを使用し、HA を備えた サーバー。
  - IP アドレスが異なるプライマリ サーバーとセカンダリ サーバーを使用し、HA を備えた サーバー。
- 仮想 IP アドレスを使用し、HA を備えたスタンドアロン シスコ プラグ アンドプレイ ゲートウェイ（2 つのシスコ プラグ アンド プレイ ゲートウェイ）
  - HA を備えていない サーバー。
  - 仮想 IP アドレスを使用し、HA を備えた サーバー。
  - IP アドレスが異なるプライマリ サーバーとセカンダリ サーバーを使用し、HA を備えた サーバー。
- 内の統合型シスコ プラグ アンド プレイ ゲートウェイ
  - HA を備えていない サーバー。
  - 仮想 IP アドレスを使用し、HA を備えた サーバー。

関連トピック

シスコ プラグ アンド プレイ ゲートウェイ HA の制限 （484 ページ）

シスコ プラグ アンド プレイ ゲートウェイ HA の機能 （477 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA のセットアップ
HA のシスコ プラグ アンド プレイ ゲートウェイの削除 （482 ページ）
シスコ プラグ アンド プレイ ゲートウェイのステータス （481 ページ）

シスコ プラグ アンド プレイ ゲートウェイ HA の制限

シスコ プラグ アンド プレイ ゲートウェイ HA 機能には次の制限があります。

- フェールオーバーとフェールバック（とシスコ プラグ アンド プレイ ゲートウェイ スタンドアロン サーバー）中にシスコ プラグ アンド プレイ ゲートウェイで部分的に完了したプラグ アンド プレイ要求は、サーバー上で不完全なままとなり、デバイス上で正常に設定されない可能性があります。
- フェールオーバーとフェールバックには 5 ～ 10 分かかり、その間シスコ プラグ アンド プレイ ゲートウェイのプロビジョニングは行われません。cns config initial を使用してブートストラップを受信したデバイスは、引き続き、プロビジョニングのためにシスコ プラグ アンド プレイ ゲートウェイに到達できます。詳細については、『Command Reference Guide for Cisco Prime Infrastructure』を参照してください。
- IP アドレスがアクティブ サーバーからスタンバイ サーバーに移動されてからデバイスがバックアップ サーバーに接続するまでの時間は、cns event コマンドで使用可能な再接続時間に関する設定によって異なります。
- 統合プラグ アンド プレイ ゲートウェイは、Prime 内の HA 設定が仮想 IP アドレスに基づいている場合に HA をサポートします。プライマリ サーバーとセカンダリ サーバーの IP アドレスが異なる HA は、統合サーバー内のプラグ アンド プレイ ゲートウェイ HA 機能をサポートしません。
- 統合プラグ アンド プレイ ゲートウェイでは、すべてのゲートウェイ SSL ポート（たとえば、ポート 11012、11014 など）において SSLv3 がデフォルトで無効化されています。
- 関連項目

関連トピック

シスコ プラグ アンド プレイ ゲートウェイ HA の機能 （477 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA のセットアップ
HA のシスコ プラグ アンド プレイ ゲートウェイの削除 （482 ページ）
シスコ プラグ アンド プレイ ゲートウェイ HA と の組み合わせ （483 ページ）

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。