CHAPTER 3

設定

Prime AM をインストールしてブラウザを起動した後は、Prime AM のスタート手順について次の項をお読みください。

ネットワークの検出

ネットワーク内のデバイスを表示し、管理するため、Prime AM ではまずデバイスを検出し、アクセス権を取得してから、それらのデバイスの情報を収集する必要があります。Prime AM では、SNMP と SSH/Telnet の両方を使用して、サポートされるデバイスに接続し、インベントリ データを収集します。

ここではネットワークの検出方法について説明します。

検出の実行計画

Prime AM では、SNMP ポーリングを使用して、指定された IP アドレス範囲内のネットワーク デバイスに関する情報を収集します。ネットワーク デバイスで CDP をイネーブルにしている場合、Prime AM では、指定したシード デバイスを使用してネットワーク内のデバイスが検出されます。

検出を実行する前に、次の作業を行う必要があります。

1. デバイスに SNMP クレデンシャルを設定する：Prime AM では、SNMP ポーリングを使用して、ネットワーク デバイスに関する情報を収集します。Prime AM を使用して管理するすべてのデバイスに、SNMP クレデンシャルを設定する必要があります。
2. デバイスに Syslog およびトラップ送信先を設定する：Prime AM を使用して管理するすべてのデバイスに、syslog およびトラップ送信先として Prime AM サーバを指定します（Prime AM サーバ IP アドレスおよびポートを使用）。

3. メール サーバの設定：Prime AM によるネットワーク内のデバイス検出が完了したときに、電子メール通知を受信します。

メール サーバの設定

メール サーバの設定によって、Prime AM でネットワーク内のデバイス検出が完了したときに、電子メール通知を受信できます。

ステップ 1　[Administration] > [System] > [Mail Server Configuration] を選択します。

ステップ 2　プライマリ SMTP サーバのホスト名を入力します。

ステップ 3　SMTP サーバにログインするためのパスワードを入力し、そのパスワードを確認します。

ステップ 4　セカンダリ SMTP サーバに対して同じ情報を提供します（セカンダリ メール サーバが使用できる場合）。

デフォルトでは、[From] テキスト ボックスに *NCS@<NCS server IP address>* が設定されます。これは別の送信者に変更可能です。

ステップ 5　[To] テキスト ボックスに、受信者の電子メール アドレスを入力します。

指定した電子メール アドレスは、アラームやレポートなど、その他の機能領域でデフォルト値として使用されます。カンマで区切った複数の電子メール アドレスを追加できます。

（注）　ステップ 6 で行った受信者電子メール アドレスに対するグローバルな変更は、電子メール通知が設定されている場合は無視されます。

ステップ 6　既存の電子メール通知に電子メール受信者リストを適用する場合は、[Apply recipient list to existing e-mail notifications] チェックボックスをオンにします。

ステップ 7　[Test] をクリックしてテスト メールを送信し、入力した設定に誤りがないことを確認します。

ステップ 8　[Save] をクリックします。

検出の実行

検出を実行すると、Prime AM によってデバイスが検出され、アクセス権が取得されて、デバイス インベントリ データが収集されます。

最初に Prime AM を起動するときに、次の手順に従って検出を実行することをお勧めします。

ステップ 1　[Operate] > [Discovery] を選択し、[Discovery Settings] をクリックします。

ステップ 2　[New] をクリックします。

ステップ 3　表 3-1 に示すように、プロトコル設定を入力します。

ステップ 4　次のどちらかを実行します。

- [Save] をクリックして検出設定を保存し、指定の時間に検出が実行されるようにスケジュールを設定します。
- 今すぐ検出を実行するには、[Run Now] をクリックします。

表 3-1　検出プロトコルの設定

フィールド	説明
プロトコルの設定	
Ping Sweep Module	指定した IP アドレスとサブネット マスクの組み合わせから、IP アドレス範囲のリストを取得します。このモジュールは、その範囲内の各 IP アドレスに PING を送信して、デバイスの到達可能性を確認します。
CDP Module	検出エンジンは、新たに検出された各デバイスの CISCO-CDP-MIB から、次のように cdpCacheTable 内の cdpCacheAddress および cdpCacheAddressType MIB オブジェクトを読み取ります。 1. cdpCacheAddress MIB オブジェクトは、現在のデバイスから収集されます。このオブジェクトは、ネイバー デバイスのアドレス リストを提供します。 2. ネイバー デバイスのアドレスがグローバル デバイス リストにまだ存在していない場合、それらのアドレスがローカル キャッシュに追加されます。
高度なプロトコル	
Routing Table	シード ルータのルーティング テーブルを照会して分析し、サブネットおよびネクストホップ ルータを検出します。
Address Resolution Protocol	ARP 検出モジュールは、ルーティング テーブル検出モジュール（RTDM）に依存し、RTDM が処理されるときのみ実行されます。この前提条件は、DeviceObject の一部である、検出モジュールが処理するフラグに基づいて識別されます。 アクティブ ルータは（ルータの検出アルゴリズムにより）RTDM が処理し、識別する必要のあるものなので、ARP 検出モジュールから送信されるエントリは必ずしも RTDM を通過する必要はありません。 ARP テーブルが取得され、エントリがまだ RTDM に検出されていない場合、それらのエントリは（ルータを表す可能性はありますが）アクティブ ルータでなく、RTDM に渡される必要はありません。このことは、ARP 検出モジュールのフラグが Processed に設定され、RTDM のフラグが Unprocessed のままになっていることで確認できます。 RTDM は、RTDM フラグが未設定で、ARP フラグが設定されているエントリを検出すると、そのエントリを非アクティブ ルータまたはその他のデバイスとして識別し、そのエントリを Unprocessed のままにします。また、ARP 検出モジュールはアルゴリズムに従い、ARP 検出モジュールに対して設定された Processed フラグに基づいてエントリを無視します。 ARP 検出モジュールを確認したときに、デバイス情報でデバイスの MAC アドレスが更新されている必要があります。アプリケーションは、DeviceInfo オブジェクトを介してアダプタでこの情報を取得できます。デバイスの MAC アドレスをスキャンすることによって、アプリケーションはシスコ デバイスと非シスコ デバイスを区別できます。 デバイスからの ARP キャッシュは、CidsARPInfoCollector を使用して収集されます。デバイスの MAC ID はこのデータから取得され、DeviceInfo オブジェクトに設定されます。
Border Gateway Protocol	BGP 検出モジュールでは、BGP4-MIB の bgpPeerTable を使用して BGP ピアが検出されます。このテーブルには、ローカル キャッシュに情報として追加されるピアの IP アドレスが定義されています。
OSPF	Open Shortest Path First（OSPF）プロトコルは、Interior Gateway Routing Protocol です。OSPF 検出では、ospfNbrTable および ospfVirtNbrTable MIB を使用して、ネイバーの IP アドレスが検出されます。
フィルタ	
System Location Filter	検出プロセスでデバイスに設定された Sys Location ストリングに基づいて、デバイスにフィルタを適用します。

表 3-1　検出プロトコルの設定 （続き）

フィールド	説明
高度なフィルタ	
IP Filter	検出プロセスでデバイスに設定された IP アドレス ストリングに基づいて、デバイスにフィルタを適用します。
System Object ID Filter	検出プロセスでデバイスに設定されたシステム オブジェクト ID ストリングに基づいて、デバイスにフィルタを適用します。
DNS Filter	検出プロセス時にデバイスに設定された DNS ストリングに基づいて、デバイスにフィルタを適用します。
クレデンシャルの設定	
SNMP V2 Credential	SNMP コミュニティ ストリングは、ネットワーク内のデバイスを検出するための必須パラメータです。特定の IP アドレスにマッピングされる複数行のクレデンシャルを入力することも、IP アドレスを *.*.*.*, 1.2.3.* のようにワイルド カードにすることもできます。
Telnet Credential	検出時に Telnet クレデンシャルを指定し、デバイス データを収集するように設定できます。
SSH Credential	Prime AM は、SSH V1 および V2 をサポートしています。検出を実行する前に、SSH を設定できます。
SNMP V3 Credential	Prime AM は、デバイスに対する SNMP V3 検出をサポートしています。

検出の確認

検出が完了したら、次の手順を実行して、プロセスが成功したことを確認できます。

ステップ 1　[Operate] > [Discovery] を選択します。

ステップ 2　詳細を表示する検出ジョブを選択します。

ステップ 3　[Discovery Job Instances] の下の矢印を展開して、検出されたデバイスの詳細を表示します。

デバイスが見つからない場合は、次のことを行ってください。

- 検出の設定を変更してから、検出を再実行します。検出の設定については、表 3-1 を参照してください。
- デバイスを手動で追加します。詳細については、手動によるデバイスの追加を参照してください。

手動によるデバイスの追加

次の手順に示すように、デバイスは手動で追加できます。これは、単一のデバイスを追加する場合に役立ちます。ネットワーク内のすべてのデバイスを追加する場合は、検出を実行することをお勧めします。（詳細については、検出の確認を参照してください）。

ステップ 1　[Operate] > [Device Work Center] を選択してから、[Add] をクリックします。

ステップ 2　パラメータを入力します。

ステップ 3　[Add] をクリックして、指定した設定のデバイスを追加します。

デバイスの一括インポート

デバイスがインポートされる管理システムが別に存在する場合、またはすべてのデバイスとその属性を含むスプレッドシートをインポートする場合は、デバイス情報を Prime AM にまとめてインポートできます。

ステップ 1　[Operate] > [Device Work Center] を選択し、[Bulk] をクリックします。

ステップ 2　インポートするファイルに包含する必要のある情報について、すべてのフィールドと説明が含まれたサンプル ファイルをダウンロードするためのリンクをクリックします。

ステップ 3　[Browse] をクリックしてファイルに移動し、[Import] をクリックします。

ステップ 4　インポートのステータスを表示するには、[Tools] > [Task Manager] > [Jobs Dashboard] を選択します。

ステップ 5　矢印をクリックしてジョブの詳細を展開し、インポート ジョブの詳細と履歴を表示します。

サイト プロファイルの設定

サイト プロファイルは、ネットワーク要素を物理的なロケーションに関連付けることにより、大規模なキャンパスを管理するのに役立ちます。サイト プロファイルには、キャンパスとビルディングを含む階層があり、これを利用することでネットワークの物理構造を区分し、ロケーションに基づいてネットワークをモニタできます。

サイトを設定し、変更できるエリアは次の 2 つです。

- [Operate] > [Site Profiles & Maps] : 新規サイトを作成し、既存のサイトを変更します。
- [Operate] > [Device Work Center] : サイトが以前に作成されている場合は、[Device Work Center] から [Add to Site] をクリックして、サイトにデバイスを追加できます。

サイト プロファイルを作成するときは、サイトに組み込むキャンパスとビルディングの数を決める必要があります。表 3-2 で、サイト プロファイルに組み込む要素を決定する方法を説明します。

表 3-2　サイト プロファイル内の要素の作成

作成する要素	この要素を作成する状況
Campus	複数のビジネス ロケーションが存在する場合
Building	キャンパス内に複数のロケーションが存在する場合

サイト内のデバイスにアクセスできるユーザを制御するには、仮想ドメインを作成する必要があります。詳細については、仮想ドメインの設定を参照してください。

サイトの詳細については、サイトの管理を参照してください。

サイト プロファイルの作成

キャンパス ロケーションを作成するには、次の手順でキャンパスにビルディングを追加します。

ステップ 1　[Operate] > [Site Profiles & Maps] を選択します。

ステップ 2　コマンド メニューから、[New Campus] を選択し、[Go] をクリックします。

ステップ 3　必要なパラメータを入力し、[Next] をクリックします。

ステップ 4　設定を変更し、[OK] をクリックします。

ステップ 5　作成したキャンパスをクリックします。次に、コマンド メニューから [New Building] を選択し、[Go] をクリックします。

ステップ 6　必要なパラメータを入力し、[Save] をクリックします。

これで、サイト プロファイルへのデバイスの追加の説明に従ってサイト プロファイルにデバイスを追加できます。

サイト プロファイルへのデバイスの追加

サイト プロファイルを作成した後は、それらのサイトにデバイスを割り当てることができます。キャンパスおよびビルディングにデバイスを関連付けることによって、メンテナンス作業を簡略化できます。複数のデバイスに対してメンテナンス作業を行う必要がある場合は、そのデバイスを含むサイトを選択して、サイト内のすべてのデバイスに変更を適用できます。

サイト内のデバイスにアクセスできるユーザを制御するには、仮想ドメインを作成する必要があります。詳細については、仮想ドメインの設定を参照してください。

ステップ 1　[Operate] > [Device Work Center] を選択します。

ステップ 2　サイトに追加するデバイスを選択してから、[>>] アイコンをクリックして、[Add to Site] をクリックします。

ステップ 3　デバイスを割り当てるキャンパスとビルディングを選択して、[Add] をクリックします。

（注）　[Campus] フィールドと [Building] フィールドには、以前に [Operate] > [Site Profiles & Maps] に入力した設定が設定されます。詳細については、サイト プロファイルの作成を参照してください。

ポート モニタリングの設定

デバイス ポートをモニタするには、ポート グループを作成し、Prime AM ダッシュボードにモニタリング情報を表示します。

ポート グループ

ポート グループはインターフェイスの論理グループであり、それらのインターフェイスが提供する機能別にデバイス ポートをモニタできるようにします。たとえば、WAN ポートのポート グループを作成し、同じルータ上の内部ディストリビューション ポート用に別のポート グループを作成します。

ポート グループを作成した後は、ポート グループに属するすべてのデバイスをより効率的に設定できます。

グループとしてモニタするポートのタイプを決定する必要があります。次のポート グループは、ほとんどのネットワークに代表されるものです。

- ポート タイプ
- ユーザ定義
- WAN インターフェイス

モニタリング テンプレート

モニタリング テンプレートは、デバイスの機能、使用状況、ヘルス、およびその他の要因をモニタします。モニタリング テンプレートを作成し、展開した後は、Prime AM によって指定のデバイスからデータが収集および処理され、情報がダッシュボード、ダッシュレット、およびレポートに表示されます。

WAN インターフェイス モニタリングの設定

特定のポート グループのすべての WAN インターフェイスで効率的に設定を行うため、WAN インターフェイス ポート グループを作成します。

次に、エッジ ルータの WAN インターフェイスのポート グループを作成し、それらのポートに対して WAN インターフェイスのヘルス モニタリング テンプレートを作成して展開し、結果を表示する手順を示します。

ステップ 1　[Operate] > [Port Grouping] を選択します。

ステップ 2　デバイス IP アドレスを選択して WAN インターフェイス ポート グループに追加し、[Add to Group] をクリックします。

ステップ 3　[Select Group] ドロップダウン メニューから、[WAN Interfaces] を選択し、[Save] をクリックします。

WAN インターフェイスを指定したら、次は WAN インターフェイス ヘルス モニタリング テンプレートを作成する必要があります。

ステップ 4　[Design] > [Monitoring] を選択します。

ステップ 5　[Features] > [Metrics] > [Interface Health] を選択します。

ステップ 6　インターフェイス ヘルス テンプレートのパラメータを入力します。WAN インターフェイスについてモニタされるすべてのパラメータをチェックすることをお勧めします。

ステップ 7　[Save as New Template] をクリックします。

WAN インターフェイス ヘルス モニタリング テンプレートを作成したので、次はそのテンプレートをアクティブ化して展開する必要があります。

ステップ 8　[Deploy] > [Monitoring Tasks] を選択します。

ステップ 9　作成したテンプレートを選択して、[Activate] をクリックします。[OK] をクリックして確認します。

ステップ 10　作成したテンプレートを選択して、[Deploy] をクリックします。

ステップ 11　[Port Groups] を選択して、[WAN Interfaces] をクリックし、[Submit] をクリックします。

テンプレートを展開したので、これでモニタリング結果を表示できます。

ステップ 12　[Operate] > [Overview] を選択します。[Top N Interfaces by WAN Utilization] ダッシュボードには、WAN インターフェイスについてモニタするように指定したパラメータが表示されます。

関連項目

- ポート グループの更新

仮想ドメインの設定

仮想ドメインを利用して、特定のサイトおよびデバイスにアクセスできるユーザを制御できます。デバイスを Prime AM に追加した後は、仮想ドメインを設定できます。仮想ドメインはデバイスの論理グループであり、このドメインを使用してグループを管理できるユーザを制御します。管理者は、仮想ドメインを作成することにより、ユーザが特に直接関連のある情報を表示できるようにするとともに、他のエリアへのユーザによるアクセスを制限できます。ユーザは、仮想ドメイン フィルタを利用して、割り当てられたネットワーク部分のみのデバイスの設定、アラームの表示、およびレポートの生成を行うことができます。

仮想ドメインは、物理サイト、デバイス タイプ、ユーザ コミュニティ、またはその他の任意の指定項目をベースにすることができます。

仮想ドメインを設定する前に、ネットワーク内のどのサイトおよびデバイスにどのユーザがアクセスできるかを決定する必要があります。

サイト指向の仮想ドメインの作成

デフォルトでは、Prime AM に 1 つの仮想ドメインだけが定義されます（*ルート*）。

サイト指向の仮想ドメインを作成すると、ユーザが特定のサイトの情報を表示できるようにするとともに、他のエリアへのユーザによるアクセスを制限できます。

次に、特定のロケーションのすべてのデバイスのセグメントを選択し、「Site 1 Routers」仮想ドメインの一部にする手順を示します。

ステップ 1　[Administration] > [Virtual Domains] を選択します。

ステップ 2　左側の [Virtual Domain Hierarchy] サイドバー メニューから、[New] をクリックします。

（注）　デフォルトでは、1 つの仮想ドメイン（*ルート*）だけが Prime AM に定義されます。選択した仮想ドメインが、新規作成するサブ仮想ドメインの親仮想ドメインとなります。

ステップ 3　仮想ドメイン名に **Site 1 Routers** と入力し、[Submit] をクリックします。

ステップ 4　[Sites] タブで、仮想ドメインに関連付けるサイトを [Selected Sites] 列に移動して、[Submit] をクリックします。

ステップ 5　確認画面で [OK] をクリックします。

仮想ドメインへのユーザの割り当て

仮想ドメインを作成した後は、その仮想ドメインを特定のユーザに関連付けることができます。これにより、ユーザは特に直接関連のある情報を表示でき、他のエリアへのユーザのアクセスが制限されます。仮想ドメインに割り当てられたユーザは、割り当てられた仮想ドメインのみのデバイスの設定、アラームの表示、およびレポートの生成を行うことができます。

次に、前に作成した Site 1 Routers 仮想ドメインを担当するユーザの作成手順を示します。

ステップ 1　[Administration] > [Users, Roles, & AAA] を選択します。

ステップ 2　仮想ドメインに割り当てるユーザ名をクリックします。

ステップ 3　[Virtual Domains] タブをクリックし、特定の仮想ドメインを [Available] リストから [Selected] リストに移動します。

ステップ 4　[Submit] をクリックします。

（注）　外部の AAA を使用する際は、必ず、仮想ドメインのカスタム属性をその外部 AAA サーバの適切なユーザまたはグループ設定に追加してください。

関連項目

- ユーザ アクセスの制御

次の手順

これで基本的なセットアップ手順は完了ですが、任意で次の作業を行ってください。

表 3-3　セットアップ作業完了後の次の手順

作業	GUI パス	参照ドキュメント
追加ユーザを設定する	[Administration] > [Users, Roles & AAA] の次に、[Users] をクリックします。	ユーザ アクセスの制御
稼動ドメインを追加する	[Administration] > [Virtual Domains]	仮想ドメインの設定
サイトの詳細を設定する	[Operate] > [Site Profiles & Maps]	サイトの管理
追加のポート グループを作成し、既存のポート グループを変更する	[Operate] > [Port Grouping]	ポート グループの変更
モニタリングとアラームへの応答を開始する	[Operate] > [Alarms & Events]	アラームのモニタリング