CHAPTER 8

デバイス インベントリの更新

Prime AM には、ネットワーク内のデバイスを検出する 2 通りの方法があります。

- クイック：指定した SNMP コミュニティ ストリング、シード IP アドレス、サブネット マスクに基づいてネットワーク内のデバイスを素早く検出できます。[Operate] > [Discovery] を選択し、[Quick Discovery] をクリックします。
- 通常：プロトコル、資格情報、およびフィルタ設定を指定して検出できます。また、検出ジョブの実行スケジュールを設定できます。検出設定の変更を参照してください。

検出設定の変更

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。表 8-1 に示すように設定を入力します。

表 8-1 検出設定

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、cdpCacheTable 内の cdpCacheAddress および cdpCacheAddressType MIB オブジェクトを読み取ります。 1. 現在のデバイスの cdpCacheAddress MIB オブジェクトを取得します。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、それらのアドレスをローカル キャッシュに追加します。
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。

表 8-1　検出設定 （続き）

フィールド	説明
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 検出モジュールを選択したときに、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。
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。

表 8-1　検出設定 （続き）

フィールド	説明
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。
優先管理	
IP Method	• ループバックを使用する • SysName を使用する • DNSReverseLookup を使用する

ステップ 3　次の項目をクリックします。

- [Save]。設定を保存します。
- [Run Now]。設定を保存し、すぐに検出ジョブを起動します。

検出ジョブのスケジュール

将来の指定日時に実行する検出ジョブを作成するには、次の手順を実行します。

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 8-1 に示すように設定を入力し、[Save] をクリックします。

ステップ 4　[Discovery Settings] ウィンドウで、先ほど作成した検出ジョブを選択し、[Schedule] をクリックします。

ステップ 5　スケジュール情報を入力し、[Save] をクリックします。

検出プロセスのモニタリング

検出プロセスを表示するには、次の手順を実行します。

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すると、詳細が表示されます。

検出の繰り返し

次の手順では、既存の設定を使用して検出を繰り返す方法と進行に合わせてジョブをモニタする方法を説明します。

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

検出プロトコルと CSV ファイル形式

Prime AM は 6 種類のプロトコルを使用してデバイスを検出します。

- Ping Sweep
- Cisco Discovery Protocol（CDP）
- Routing Table
- アドレス解決プロトコル（ARP）
- ボーダー ゲートウェイ プロトコル（BGP）
- Open Shortest Path First（OSPF）

CSV ファイルをインポートして、プロトコルのデータを追加できます。表 8-2 は、各プロトコルの CSV ファイル形式について説明しています。

（注）　サポートされているバージョンの Mozilla Firefox だけを使用している場合、CSV ファイルをインポートできます。詳細については、サポートされるブラウザを参照してください。

表 8-2　検出プロトコルと CSV ファイル形式

プロトコル	CSV ファイル形式
Ping sweep	有効な IP アドレスとサブネット マスクをカンマで区切ります。追加の行を加えることによって 1 回の検出に複数のネットワークを指定できます。以下に例を示します。 1.1.1.1,255.255.240.0 2.1.1.1,255.255.255.0
Cisco Discovery Protocol（CDP）	有効な IP アドレスとホップ カウントをカンマで区切ります。以下に例を示します。 1.1.1.1,3 2.2.2.2,5
ルーティング テーブル	有効な IP アドレスとホップ カウントをカンマで区切ります。以下に例を示します。 1.1.1.1,3 2.2.2.2,5
アドレス解決プロトコル（ARP）	有効な IP アドレスとホップ カウントをカンマで区切ります。以下に例を示します。 1.1.1.1,3 2.2.2.2,5

表 8-2　検出プロトコルと CSV ファイル形式 （続き）

プロトコル	CSV ファイル形式
ボーダー ゲートウェイ プロトコル（BGP）	BGP をイネーブルにしているデバイスのシード デバイス IP アドレス。以下に例を示します。 1.1.1.1 2.2.2.2 3.3.3.3
Open Shortest Path First（OSPF）	OSPF をイネーブルにしているデバイスのシード デバイス IP アドレス。以下に例を示します。 1.1.1.1 2.2.2.2 3.3.3.3

デバイス インベントリの手動による更新

検出を実行してデバイス インベントリを更新することを推奨します。なお、次の手順で示すようにデバイスを手動で追加できます。

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　必要な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 インベントリのインポート

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。

次の作業では、既存の CSV ファイルから一括してデバイスを追加する方法を説明します。

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　[Tools] > [Task Manager] > [Jobs] を選択し、インポートのステータスを表示します。

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。

管理対象外のデバイスのトラブルシューティング

表 8-3 では、デバイスが Prime AM の管理対象外になると考えられる理由を説明しています。

表 8-3　デバイスが管理対象外になる理由

考えられる原因	アクション
デバイスがダウンしているため、または Prime AM サーバからデバイスまでの経路にあるデバイスがダウンしているため、Prime AM がデバイスに到達できません。	• ping ツールと traceroute ツールを使用して、Prime AM がデバイスに到達できることを確認します。詳細については、[360º View] の使用を参照してください。 • デバイスに到達できる場合、デバイスに設定された再試行とタイムアウトの値が十分に足りていることを確認します（[Operate] > [Device Work Center] を選択し、デバイスを選択した後、[Edit] をクリックします）。 • デバイスに SNMP を設定してイネーブルにしていることを確認します。 – SNMPv2 を使用している場合、デバイスに設定された *read-write* コミュニティ ストリングが Prime AM に入力したものと同じことを確認します。 **（注）** read-write コミュニティ ストリングは必須です。 – SMNPv3 を使用している場合、デバイスに次のパラメータが設定されるとともに、デバイスに設定されたパラメータが Prime AM に入力したものと一致することを確認します。 ユーザ名 AuthPriv モード（noAuthNoPriv、authNoPriv、authPriv） 認証アルゴリズム（たとえば、MD5、SHA など）と認証パスワード プライバシー アルゴリズム（たとえば、AES、DES など）とプライバシー パスワード • デバイスに設定された SNMP クレデンシャルが Prime AM で設定された SNMP クレデンシャルと一致することを確認します。 • Prime AM で SNMP クレデンシャルを再入力し、デバイスを再同期化します（[Operate] > [Device Work Center] を選択し、デバイスを選択した後、[Sync] をクリックします）。詳細については、デバイスの同期化を参照してください。
Telnet または SSH がデバイスに設定されていないため、Prime AM はデバイスから情報を収集できません。	• デバイスに Telnet または SSH を設定してイネーブルにしていること、および同じプロトコルを Prime AM に設定していることを確認します（[Operate] > [Device Work Center] を選択し、デバイスを選択した後、[Edit] をクリックします）。 **（注）** HTTP がデバイス タイプに必要な場合、デバイスに設定されたパラメータと Prime AM HTTP パラメータが一致することを確認します。 • ユーザ名、Telnet または SSH のパスワード、Cisco IOS デバイスのイネーブル モード パスワードがデバイスに正しく設定されていること、および Prime AM で入力されたパラメータがデバイスの設定値と一致することを確認します。認証用のユーザ名をデバイスに設定していない場合、Prime AM でこのフィールドを空白のままにできます。 • Telnet/SSH ユーザに設定された認証レベルの制限によりイネーブル特権レベルが低下しないことを確認します。

表 8-3　デバイスが管理対象外になる理由 （続き）

考えられる原因	アクション
SNMP ビューまたはアクセス リストで SNMP の制限があります。	SNMP ビューまたはアクセス リスト全体で SNMP の制限を削除します。
TACACS+ の「コマンド単位の認可」がデバイスに設定されています。	TACACS+ が設定されている場合、許可された CLI コマンドに対する Telnet/SSH ユーザの権限を確認します。Prime AM ユーザ アカウントにすべての CLI コマンドを許可することを推奨します。または、絶対に制限が必要なコマンドだけを除外してください。

Cisco IOS で SNMP、Telnet、および SSH を設定する方法の詳細については、次の資料を参照してください。

- 『Cisco IOS Software Releases 12.0 T SNMPv3』
- 『Configuring Secure Shell on Routers and Switches Running Cisco IOS』

デバイス グループの使用

デフォルトでは、Prime AM はルールベースのデバイス グループを作成し、適切な [Device Type] フォルダにデバイスを割り当てます。このデバイス グループは編集できません。[device group] フォルダにカーソルを置くと、デバイス グループのルールを表示できます。

デバイス グループはデバイスの論理グループです。デバイスの更新と管理を効率化するためにデバイス グループを作成します。たとえば、特定のモジュールを持つデバイスが含まれるデバイス グループを作成できます。後で特にそのモジュールに関連する機能を設定する場合、作成したデバイス グループを使用して、グループ内のすべてのデバイスに設定の変更を追加します。

次の 2 種類のいずれかのグループを新規に作成できます。

- スタティック：デバイスを追加する新しいデバイス グループを作成し、名前を付けます。[Operate] > [Device Work Center] の [Add to Group] ボタンを使用します。
- ダイナミック：新しいデバイス グループを作成し、名前を付けます。また、このデバイス グループに追加するためにデバイスが準拠する必要のあるルールを指定します。詳細については、新しいデバイス グループの作成を参照してください。

デバイス グループを作成した場合、そのデバイスのグループをネットワーク内の他のグループから区別することになります。たとえば、異なる時間帯に存在するデバイスがある場合は、あるグループ内のデバイスが別のグループ内のデバイスの時間帯設定と異なる設定を持つように、地域に基づいてデバイス グループを作成できます。

すべてのデバイスを同じ設定で構成できる小規模の構成では、ただ 1 つの一般的なデバイス グループを作成するだけで済みます。この手順により、グループ用の設定を構成し、すべてのデバイスにそれらの設定を一貫して適用できます。

グループは、複数のデバイスを設定する時間を節減するだけでなく、設定がネットワーク全体に一貫して適用されることを保証します。

（注）　デバイス グループにアクセスできるユーザは制御できません。すべてのユーザがすべてのデバイス グループを表示できます。ロールベース アクセス コントロール（RBAC）では、サイトと仮想ドメインを作成する必要があります。

デバイス グループの作成

表 8-4 で新しいデバイス グループを作成する方法について説明します。

表 8-4　デバイス グループを作成する手順

作業	その他の情報
1. 新しいデバイス グループを作成します。	新しいグループの一般情報を定義します。たとえば、このグループに割り当てられるグループ名や親グループなどです。 詳細については、新しいデバイス グループの作成を参照してください。
2. デバイス グループにデバイスを割り当てます。	デバイスがグループ設定を継承できるように、グループにデバイスを割り当てます。 詳細については、次のサイトを参照してください。
3. デバイス グループで作業を行います。	グループに属するすべてのデバイスに適用される作業を実行できます。

新しいデバイス グループの作成

デバイス グループを作成する前に、必ず、グループに含める固有のプロパティを理解してください。たとえば、異なる認証設定や異なる時間帯設定を持つ 2 つのデバイス グループを準備できます。

ダイナミック デバイス グループを作成するには、次の手順を実行します。

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

ステップ 2　左側の [Groups] メニューで [Settings] アイコンをクリックして、[Create Group] をクリックします。

ステップ 3　グループ名とグループの説明を入力します。また、必要に応じて親グループを選択します。

ステップ 4　グループに追加するためにすべてのデバイスが準拠する必要があるルールを指定できるよう [Save as a Static Group] チェックボックスをオフにします。デバイスをグループに手動で追加し、グループをルールベースにしない場合は、[Save as a Static Group] をクリックします。

ステップ 5　デバイスのルールが一致するように指定します。

ステップ 6　[Save] をクリックし、デバイス グループと指定した設定を追加します。作成したデバイス グループは、ユーザ定義グループの下に表示されます。

グループへのデバイスの割り当て

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

ステップ 2　グループに割り当てるデバイスを選択し、[Add To Group] をクリックします。

ステップ 3　グループを選択した後、次の項目をクリックします。

- [Save]。デバイスを選択したグループに追加します。
- [Cancel]。変更を保存せずに終了します。

デバイスの同期化

Prime AM データベースをデバイス上で現在動作中の設定に同期させるために、インベントリを強制的に収集できます。

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

ステップ 2　Prime AM データベースに保存された設定と同期させるデバイスを選択します。

ステップ 3　[Sync] をクリックします。