CHAPTER 8

デバイス インベントリの更新

Prime NCS（WAN）には、ネットワークのデバイスを検出する方法として次の 2 つが用意されています。

- クイック：指定する SNMP コミュニティ ストリング、シード IP アドレス、およびサブネット マスクに基づいて、ネットワークのデバイスをすばやく検出できます。[Operate] > [Discovery] を選択し、[Quick Discovery] をクリックします。
- 通常：ディスカバリ用のプロトコル、クレデンシャルおよびフィルタの設定を指定し、ディスカバリ ジョブを実行するタイミングをスケジュールできます。ディスカバリ設定の変更を参照してください。

ディスカバリ設定の変更

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 ディスカバリ設定

フィールド	説明
Protocol Settings	
Ping Sweep Module	指定した組み合わせの IP アドレスとサブネット マスクから 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、デバイスの到達可能性を確認するために、範囲の各 IP アドレスに ping を送信します。
CDP Module	ディスカバリ エンジンは、新しく検出されたデバイスごとに CISCO-CDP-MIB から cdpCacheTable の MIB オブジェクト cdpCacheAddress および cdpCacheAddressType を読み取ります。 1. 現在のデバイスから MIB オブジェクト cdpCacheAddress を取り出します。これで、ネイバー デバイス アドレスのリストが得られます。 2. ネイバー デバイス アドレスがグローバル デバイス リストにもう存在しない場合は、それらをローカル キャッシュに追加します。
Advanced Protocols	
Routing Table	サブネットおよびネクスト ホップ ルータを検出するためにシード ルータでルーティング テーブルに問い合わせて分析します。

表 8-1　ディスカバリ設定（続き）

フィールド	説明
Address Resolution Protocol	ARP Discovery Module は Routing Table Discovery Module（RTDM）に依存し、RTDM が処理されたときだけ実行されます。この前提条件は、DeviceObject の一部である Discovery-module-processed フラグに基づいて識別されます。 アクティブ ルータ（ルータ ディスカバリ アルゴリズムに従う）は RTDM が処理および識別すべきものであるため、ARP Discovery Module からのエントリは、必ずしも RTDM を通過する必要はありません。 ARP テーブルを取り出し、エントリが RTDM によってまだ検出されていない場合、それらのエントリは（ルータを表すものであっても）はアクティブ ルータではなく、RTDM に渡す必要はありません。これは、ARP Discovery Module フラグを Processed に設定し、RTDM フラグを Unprocessed のままにすることによって確保されます。 RTDM フラグが設定解除され ARP フラグが設定された状態のエントリを RTDM が見つけた場合、RTDM はそのエントリを非アクティブ ルータまたは他のデバイスとして識別し、エントリを Unprocessed のままにします。ARP Discovery Module に対して設定された Processed フラグに基づき、ARP Discovery Module も、アルゴリズムに従ってそのエントリを無視します。 ARP Discovery Module が選択された場合、デバイス情報のデバイス MAC アドレスを更新する必要があります。アプリケーションは、アダプタでのこの情報を DeviceInfo オブジェクトにより取得できます。デバイス MAC アドレスをスキャンすることにより、アプリケーションはシスコ デバイスとシスコ以外の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て DeviceInfo オブジェクトに設定されます。
Border Gateway Protocol	BGP Discovery Module は BGP4-MIB の bgpPeerTable を使用してその BGP ピアを見つけます。このテーブルには、ピアの IP アドレスが格納されます。それらのアドレスは、ローカル キャッシュへの手がかりとして追加されています。
OSPF	Open Shortest Path First（OSPF）プロトコルは内部ゲートウェイ ルーティング プロトコルです。OSPF ディスカバリは ospfNbrTable および ospfVirtNbrTable MIB を使用してネイバーの IP アドレスを検出します。
Filters	
System Location Filter	ディスカバリ プロセス中にデバイスに設定されたシステム ロケーション ストリングに基づいてデバイスをフィルタ処理します。
Advanced Filters	
IP Filter	ディスカバリ プロセス中に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をフィルタ処理します。
System Object ID Filter	ディスカバリ プロセス中に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をフィルタ処理します。
DNS Filter	ディスカバリ プロセス中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をフィルタ処理します。
Credential Settings	
SNMP V2 Credential	SNMP コミュニティ ストリングは、ネットワーク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 アドレスにマップされた複数行のクレデンシャルを入力したり、IP アドレスをワイルドカードにすることができます（たとえば、*.*.*.*、1.2.3.*）。
Telnet Credential	ディスカバリ設定の作成時に、telnet クレデンシャルを指定してデバイス データを収集できます。
SSH Credential	Prime NCS（WAN）は SSH V1 および V2 をサポートします。ディスカバリの実行前に SSH を設定できます。

表 8-1　ディスカバリ設定（続き）

フィールド	説明
SNMP V3 Credential	Prime NCS（WAN）はデバイスの SNMP V3 ディスカバリをサポートします。
Preferred Management	
IP Method	• Loopback の使用 • SysName の使用 • DNSReverseLookup の使用

ステップ 3　次のいずれかをクリックします。

- 設定を保存するには [Save]。
- 設定を保存してただちにディスカバリ ジョブを開始するには [Run Now]。

ディスカバリ ジョブのスケジューリング

今後実行するスケジュールを指定したディスカバリ 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、作成したディスカバリ 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。

ディスカバリ プロセスのモニタリング

ディスカバリ 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　詳細を表示するディスカバリ ジョブを選択すると、詳細が表示されます。

ディスカバリの繰り返し

次の手順では、既存の設定を使用してディスカバリを繰り返す方法と、進行するジョブをモニタする方法について説明します。

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

ディスカバリ プロトコルと CSV ファイル形式

Prime NCS（WAN）は次の 6 つ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
- Address Resolution Protocol（ARP）
- Border Gateway Protocol（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 に、各プロトコルの CSV ファイル形式を示します。

（注）　CSV ファイルをインポートできるのは、サポートされているバージョンの Mozilla Firefox を使用している場合に限られます。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　ディスカバリ 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	カンマで区切った、任意の有効な IP アドレスとサブネット マスク。行を追加すると、単一のディスカバリに複数のネットワークを指定できます。次に例を示します。 1.1.1.1,255.255.240.0 2.1.1.1,255.255.255.0
Cisco Discovery Protocol（CDP）	カンマで区切った、任意の有効な IP アドレスとホップ カウント。次に例を示します。 1.1.1.1,3 2.2.2.2,5
Routing table	カンマで区切った、任意の有効な IP アドレスとホップ カウント。次に例を示します。 1.1.1.1,3 2.2.2.2,5
Address Resolution Protocol（ARP）	カンマで区切った、任意の有効な IP アドレスとホップ カウント。次に例を示します。 1.1.1.1,3 2.2.2.2,5

表 8-2　ディスカバリ 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
Border Gateway Protocol（BGP）	BGP 対応の任意のデバイスのシード デバイス IP アドレス。次に例を示します。 1.1.1.1 2.2.2.2 3.3.3.3
Open Shortest Path First（OSPF）	OSPF 対応の任意のデバイスのシード デバイス IP アドレス。次に例を示します。 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更新

デバイス インベントリを更新するには、ディスカバリを実行することをお勧めします。ただし、次の手順に示すように手動でデバイスを追加できます。

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

ステップ 2　必須パラメータを入力します。

ステップ 3　[Add] をクリックして、指定した設定で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システムに別の管理システムがある場合、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、一括してデバイス情報を Prime NCS（WAN）にインポートできます。

次のタスクでは、既存の CSV ファイルからデバイスを一括して追加する方法について説明します。

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　リンクをクリックして、インポートされるファイルに入れる必要のある情報のすべてのフィールドと説明が格納された、サンプル ファイルをダウンロードします。

ステップ 3　[Browse] をクリックして自分のファイルの場所に移動し、[Import] をクリックします。

ステップ 4　[Tools] > [Task Manager] > [Jobs Dashboard] を選択して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。

管理対象外デバイスのトラブルシューティング

表 8-3 に、デバイスが Prime NCS（WAN）で管理不能となる理由を示します。

表 8-3　管理不能デバイスの理由

考えられる原因	処理
デバイスがダウンしているため、あるいは Prime NCS（WAN）サーバからデバイスまでのパスにあるいずれかのデバイスがダウンしているため、Prime NCS（WAN）がデバイスに到達できない。	• ping および traceroute ツールを使用して、Prime NCS（WAN）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、360 度ビューの使用を参照してください。 • デバイスに到達可能な場合は、デバイスに設定された再試行およびタイムアウトの値が十分であることを確認します。（[Operate] > [Device Work Center] を選択し、デバイスを選択して、[Edit] をクリックします）。 • 次のようにして、SNMP がデバイスに設定されイネーブルになっていることを確認します。 – SNMPv2 を使用している場合は、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 NCS（WAN）に入力したものと同じであることを確認します。 **（注）** 読み書き可能なコミュニティ ストリングは必須です。 – SMNPv3 を使用している場合は、次のパラメータがデバイスに設定されていること、およびデバイスに設定されたパラメータが、Prime NCS（WAN）に入力したものと一致してい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（MD5、SHA など）と認証パスワード プライバシー アルゴリズム（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ている SNMP クレデンシャルが、Prime NCS（WAN）で設定した SNMP クレデンシャルと一致することを確認します。 • Prime NCS（WAN）に SNMP クレデンシャルを再入力し、デバイスを再同期します。（[Operate] > [Device Work Center] を選択し、デバイスを選択して、[Sync] をクリックします）。詳細については、デバイスの同期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 NCS（WAN）が情報をデバイスから収集できない。	• Telnet または SSH がデバイスに設定されイネーブルになっていること、および同じプロトコルが Prime NCS（WAN）に設定されていることを確認します。（[Operate] > [Device Work Center] を選択し、デバイスを選択して、[Edit] をクリックします）。 **（注）** デバイス タイプに HTTP が必要な場合は、Prime NCS（WAN）の HTTP パラメータが、デバイスに設定されているものと一致していることを確認します。 • Cisco IOS デバイスのユーザ名、Telnet または SSH パスワード、およびイネーブル 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 NCS（WAN）に入力したパラメータが、デバイスに設定されているものと一致していることを確認します。認証のためにデバイスにユーザ名を設定しなかった場合は、Prime NCS（WAN）のこのフィールドを空のままにします。 • Telnet/SSH ユーザに設定されている認可レベルが、より低いイネーブル特権レベルに制限されていないことを確認します。

表 8-3　管理不能デバイスの理由（続き）

考えられる原因	処理
SNMP ビューまたはアクセス リストによって、SNMP に対する制限が課せられた。	SNMP ビューまたはアクセス リストによる、SNMP に対するすべての制限を取り除きます。
TACACS+ の「コマンドごと認可」がデバイスに設定されている。	TACACS+ が設定されている場合は、許可されている CLI コマンドに対する Telnet/SSH ユーザの権限を確認します。Prime NCS（WAN）ユーザ アカウントにすべての CLI コマンドを許可するか、あるいは、あくまで制限する必要があるコマンドのみを除外することをお勧めします。

Cisco IOS デバイスでの SNMP、Telnet、および SSH の設定の詳細については、次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 NCS（WAN）がルールベースのデバイス グループを作成して、デバイスを適切な Device Type フォルダに割り当てます。これらのデバイス グループは編集できません。カーソルをデバイス グループ フォルダに合わせると、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を論理的にグループ分けしたものです。デバイス グループを作成すると、より効率的にデバイスの更新および管理ができるようになります。たとえば、特定のモジュールを持つデバイスを含むデバイス グループを作成できます。そのモジュールに特に関係する機能をあとで設定する場合は、作成したデバイス グループを使用して、そのグループに含まれるすべてのデバイスに設定変更をプッシュします。

作成する新しいグループは、次のいずれかのタイプにできます。

- スタティック：新しいデバイス グループを作成して名前を付けます。このグループには、[Operate] > [Device Work Center] の [Add to Group] ボタンを使用してデバイス追加できます。
- ダイナミック：新しいデバイス グループを作成して名前を付け、ルールを指定します。このデバイス グループに追加されるデバイスは、このルールに従う必要があります。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 グループを作成すると、そのグループのデバイスがネットワーク内の他のデバイスから区別されます。たとえば、異なる時間帯に存在するデバイスがある場合、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 グループを作成することもできます。

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。このセットアップにより、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適用することができます。

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）　どのユーザがどのデバイス グループにアクセスできるかを制御することはできません。すべてのユーザが、すべてのデバイス グループを認識できます。ロールベース アクセス コントロール（RBAC）の場合は、サイトおよび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 に、新しいデバイス グループを作成する方法を示します。

表 8-4　デバイス グループを作成する手順

タスク	追加情報
1. 新しいデバイス グループを作成します。	このグループに割り当てるグループ名や親グループなど、新しいグループに関する一般情報を定義します。 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。
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、グループへのデバイスの割り当てを参照してください。
3. デバイス グループで操作を実行します。	グループのメンバになっているすべてのデバイスに適用されるタスクを実行できます。

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、グループに入れ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 グループをセットアップできます。

（注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

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　左の [Groups] メニューで [Settings] アイコンをクリックし、[Create Group] をクリックします。

ステップ 3　グループ名、グループの説明を入力します。親グループがあればそれを選択します。

ステップ 4　グループに追加されるすべてのデバイスが従う必要のあるルールを指定するには、[Save as a Static Group] 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] をオンにします。

ステップ 5　デバイスが適合すべきルールを指定します。

ステップ 6　[Save] をクリックして、指定した設定でデバイス グループを追加します。作成したデバイス グループは、[User Defined] グループに表示されます。

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、次のいずれかをクリックします。

- 選択したグループにデバイスを追加するには [Save]。
- 変更内容を保存しないで終了するには [Cancel]。

デバイスの同期

強制的にインベントリ収集を実行すると、Prime NCS（WAN）データベースとデバイスで実行中のコンフィギュレーションを同期できます。

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

ステップ 2　Prime NCS（WAN）データベースに保存されている設定と同期する設定を持つデバイスを選択します。

ステップ 3　[Sync] をクリックします。