CHAPTER 3

セットアップ

Prime NCS（WAN）をインストールしてブラウザを起動したら、次の各項を参照して、Prime NCS（WAN）の使用開始方法を確認してください。

ネットワークのディスカバリ

ネットワークでデバイスを表示および管理するには、最初に Prime NCS（WAN）でデバイスを検出し、アクセスを取得してから、デバイスに関する情報を収集する必要があります。Prime NCS（WAN）は SNMP と SSH/Telnet の両方を使用してサポート対象のデバイスに接続し、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ディスカバリ方法について説明します。

ディスカバリ実行の計画

Prime NCS（WAN）は SNMP ポーリングを使用して、指定した IP アドレスの範囲内でネットワーク 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 を有効にしている場合、Prime NCS（WAN）は指定したシード デバイスを使用して、ネットワーク上のデバイスを検出します。

ディスカバリを実行する前に、次を行う必要があります。

1. デバイスでの SNMP クレデンシャルの設定：Prime NCS（WAN）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 NCS（WAN）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. デバイスでの Syslog およびトラップの宛先の設定：Prime NCS（WAN）サーバを（Prime NCS（WAN）サーバ IP アドレスとポートを使用して）syslog およびトラップの宛先として、Prime NCS（WAN）を使用して管理するすべてのデバイスに指定します。
3. 電子メール サーバ設定の構成：Prime NCS（WAN）によるネットワーク上のデバイスのディスカバリが完了すると、電子メール通知を受け取ります。

電子メール サーバ設定の構成

電子メール サーバ設定を構成すると、Prime NCS（WAN）によるネットワーク上のデバイスのディスカバリが完了したときに、電子メール通知を受け取ります。

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、パスワードの確認を行います。

ステップ 4　セカンダリ SMTP サーバにも同じ情報を指定します（セカンダリ メール サーバを使用できる場合）。

デフォルトで、[From] テキスト ボックスには *NCS@<NCS server IP address>* が入力されます。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。複数の電子メール アドレスをカンマで区切って入力することもできます。

（注）　電子メール通知が設定されていると、ステップ 6 で受信者の電子メール アドレスに行うグローバル変更は無視されます。

ステップ 6　電子メール受信者のリストを既存の電子メール通知に適用する場合は、[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電子メールを送信し、入力した設定が正しいことを確認します。

ステップ 8　[Save] をクリックします。

ディスカバリの実行

ディスカバリを実行すると、Prime NCS（WAN）はデバイスを検出し、アクセスを取得した後、デバイスのインベントリ データを収集します。

Prime NCS（WAN）を初めて起動する場合は、次の手順に従ってディスカバリ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、[Protocol Settings] に入力します。

ステップ 4　次のいずれかを実行します。

- [Save] をクリックしてディスカバリ設定を保存し、指定した時間にディスカバリが実行されるようにスケジュール設定を行います。

- [Run Now] をクリックして、今すぐディスカバリを実行します。

表 3-1　Discovery Protocol の設定

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	次のように、ディスカバリ エンジンは新しいデバイスを検出すると、CISCO-CDP-MIB から、cdpCacheTable にある cdpCacheAddress オブジェクトと 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、それがローカル キャッシュに追加されます。
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。
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 がチェックされた場合、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。

表 3-1　Discovery Protocol の設定（続き）

フィールド	説明
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、デバイス データの収集用の Telnet クレデンシャルを指定します。
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。
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。

ディスカバリの確認

ディスカバリが完了したら、次の手順に従って、プロセスが正常に完了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　詳細を表示するディスカバリジョブを選択します。

ステップ 3　[Discovery Job Instances] の下で、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、次を行います。

- ディスカバリ設定を変えてから、ディスカバリを再実行します。ディスカバリ設定の詳細については、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、デバイスの手動追加を参照してください。

デバイスの手動追加

次の手順に従って、デバイスを手動で追加できます。これは、単一のデバイスを追加するときに便利です。ネットワーク上のすべてのデバイスを追加するときは、ディスカバリを実行することをお勧めします。（詳細については、ディスカバリ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、[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、指定した設定で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。

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　インポートのステータスを確認するには、[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 プロファイルのセットアップ

サイト プロファイルは、ネットワーク要素を物理位置に関連付けることによって、大規模キャンパスの管理に役立つプロファイルです。サイト プロファイルは、キャンパスおよびビルディングを含む階層を持ち、ネットワークの物理構造を分割して位置に基づいてネットワークをモニタできます。

サイトをセットアップして変更できるエリアには、次の 2 つがあります。

- [Operate] > [Site Profiles & Maps]：新しいサイトを作成し、既存のサイトを変更します。
- [Operate] > [Device Work Center]：サイトを以前に作成済みの場合は、[Device Work Center] で [Add to Site] をクリックすることによりデバイスをサイトに追加できます。

サイト プロファイルを作成するときは、サイトに含めるキャンパスとビルディングの数を決定する必要があります。表 3-2 に、サイト プロファイルにどの要素を含めるかを判断する方法を示します。

表 3-2　サイト プロファイルの要素の作成

作成対象	作成する条件
キャンパス	複数のビジネス ロケーションがある
ビルディング	キャンパス内に複数のロケーションがある

どのユーザがサイト内のデバイスにアクセスできるかを制御するには、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、サイト編成の維持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、次のようにして、ビルディングをキャンパスに追加します。

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

ステップ 2　コマンド メニューで、[New Campus] を選択してから [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てから、[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、コマンド メニューから [New Building] を選択して、[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てから、[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デバイスをサイト プロファイルに追加できます。

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すると、デバイスをそのサイトに割り当てることができます。デバイスをキャンパスとビルディングに関連付けることによって、メンテナンス タスクを単純化できます。デバイスでメンテナンス タスクを実行する必要がある場合は、そのデバイスを含むサイトを選択して、サイトのすべてのデバイスに変更を適用できます。

どのユーザがサイト内のデバイスにアクセスできるかを制御するには、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、[>>] 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　デバイスの割り当て先にするキャンパスおよびビルディングを選択し、[Add] をクリックします。

（注）　[Campus] フィールドと [Building] フィールドに、以前に [Operate] > [Site Profiles & Maps] に入力した設定が取り込まれます。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 グループを作成してから、モニタリング情報を Prime NCS（WAN）ダッシュボードに表示できます。

ポート グループ

ポート グループとはインターフェイスの論理グループであり、提供される機能によってデバイス ポートをモニタできます。たとえば、WAN ポート用のポート グループを作成し、同じルータ上の内部分散ポート用に別のポート グループを作成できます。

ポート グループを作成すると、各ポート グループに属するすべてのデバイスを効率よく設定できます。

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。大部分のネットワークには、次のような代表的ポート グループがあります。

- 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、使用率、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および展開すると、Prime NCS（WAN）は指定したデバイスからデータを収集して処理し、ダッシュボード、ダッシュレット、およびレポートに情報を表示します。

WAN インターフェイス モニタリングの設定

WAN インターフェイス ポート グループを作成すると、特定のポート グループにあるすべての WAN インターフェイスで効率的に設定を構成できます。

次の手順は、エッジ ルータの WAN インターフェイス用のポート グループを作成して、それらのポートで 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および展開し、結果を表示する方法を示しています。

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

ステップ 2　WAN インターフェイス ポート グループに追加するデバイスの IP アドレスを選択して、[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。

これで WAN インターフェイスが指定されました。次に、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対して、すべてのパラメータがモニタされるかどうか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。

これで、WAN インターフェイス ヘルス モニタリング テンプレートが作成されました。次に、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] をクリックして確定します。

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

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

これで、テンプレートが展開され、モニタリング結果を表示できるようになりました。

ステップ 12　[Operate] > [Overview] を選択します。[The Top N Interfaces by WAN Utilization] ダッシュボードに、WAN インターフェイスをモニタするために指定したパラメータを使用してデータが取り込まれます。

関連項目

- ポート グループの更新

仮想ドメインの設定

仮想ドメインを使用して、特定のサイトおよびデバイスにどのユーザがアクセス権を持つかを制御できます。Prime NCS（WAN）にデバイスを追加後、仮想ドメインを設定できます。仮想ドメインとはデバイスの論理グループであり、これを使用して、どのユーザがグループを管理できるかが制御されます。仮想ドメインを作成することで、管理者は、関連情報を具体的に指定してユーザに表示したり、他のエリアへのユーザのアクセス権を制限したりすることができます。仮想ドメイン フィルタを使用すると、ネットワーク内でユーザに割り当てられた部分*だけ*で、ユーザがデバイスの設定、アラームの表示、およびレポートの生成を行えるようにできます。

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、または選択するあらゆる指定項目に基づいて設定できます。

仮想ドメインをセットアップする前に、ネットワーク内のどのサイトとデバイスに、どのユーザがアクセス権を持つ必要があるの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、Prime NCS（WAN）には 1 つの仮想ドメイン（*root*）だけが定義されています。

サイト指向の仮想ドメインを作成すると、特定のサイトの情報をユーザに表示したり、他のエリアへのユーザのアクセス権を制限したりすることができます。

次の手順は、特定の場所ですべてのデバイスのセグメントを選択し、それらを「Site 1 Routers」仮想ドメインの一部にする方法を示しています。

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

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

（注）　デフォルトでは、Prime NCS（WAN）に 1 つの仮想ドメイン（*root*）だけが定義されています。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] カラムに移動し、[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後、仮想ドメインを特定のユーザに割り当てることができます。これにより、関連情報を具体的に指定してユーザに表示したり、他のエリアへのユーザのアクセス権を制限したりすることができます。仮想ドメインに割り当てられたユーザは、自分に割り当てられた仮想ドメインに対してのみ、デバイスの設定、アラームの表示、レポートの生成を行えます。

次の手順では、前に作成した Site 1 Routers 仮想ドメインを担当するユーザを作成する方法を説明します。

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] タブをクリックして、[Available] リストから [Selected] リストまで対象の仮想ドメインを移動します。

ステップ 4　[Submit] をクリックします。

（注）　外部 AAA を使用しているときは、外部 AAA サーバの該当するユーザ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。

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が完了し、次のタスクを実行できます。

表 3-3　セットアップ タスク完了後の手順

タスク	GUI パス	参照ドキュメント
追加ユーザのセットアップ	[Administration] > [Users, Roles & AAA] を選択して、[Users] をクリック	ユーザ アクセスの制御
仮想ドメインの追加	[Administration] > [Virtual Domains]	仮想ドメインの設定
サイトの調整	[Operate] > [Site Profiles & Maps]	サイト編成の維持
追加ポート グループの作成と、既存のポート グループの変更	[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の開始	[Operate] > [Alarms & Events]	アラームのモニタリング