デバイスのオンボーディングと管理

ここでは、次の内容について説明します。

インベントリへのデバイスの追加

Crossworkにデバイスを追加する方法はいくつかあります。それぞれに独自の前提条件があり、デバイスの追加を成功させるために必要です。デバイスが通信用とテレメトリ用に適切に設定されていることを確認します。ガイドラインと設定例については、「新しいデバイスのテレメトリの前提条件 （3 ページ）」と「Cisco NSO デバイスの設定例 （4 ページ）」を参照してください。

ほとんどのユーザーの優先順位、メソッド、およびそれらの前提条件は次のとおりです。

1. **Crosswork API を使用したデバイスのインポート**：これはすべての方法の中で最も時間がかからず、効率的ですが、プログラミングスキルと API の知識が必要です。詳細については、『Inventory Management APIs On Cisco Devnet』を参照してください。
2. **デバイスの CSV ファイルからのデバイスのインポート**：この方法は時間がかかり、エラーが発生しやすく、事前にすべてのデータ（デバイスだけでなく、プロバイダ、クレデンシャルプロファイル、およびタグを含む）を作成してフォーマットし、さらに、CSV のインポート後に、これらのすべての項目がデバイスに正しく関連付けられていることを確認する必要があります。この方法を最大限に活かすには、まず次の手順を実行する必要があります。

- デバイスに関連付けるプロバイダーを作成します。「プロバイダの追加について」を参照してください。
- CSV ファイルにリストされているすべてのデバイスとプロバイダに対応するクレデンシャルプロファイルを作成します。「クレデンシャルプロファイルの作成」を参照してください。
- 新しいデバイスのグループ化に使用するタグを作成します。「タグの作成」を参照してください。
- Crosswork から CSV テンプレートファイルをダウンロードし、必要なすべてのデバイスを入力します。

3. **UI を使用したデバイスの追加**：この方法は、入力時にすべてのデータが検証されるため、3 つの方法の中で最もエラーが発生しにくい方法です。また、最も時間のかかる方法であり、一度に追加するデバイスが少ない場合にのみ適しています。適用するプロバイダー、クレデンシャルプロファイル、およびタグは事前に存在している必要があります。詳細については、「UI を使用したデバイスの追加 （5 ページ）」を参照してください。
4. **Cisco SR-PCE プロバイダからの自動オンボーディング**：この方法はかなり自動化されており、比較的簡単です。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。このソースからデバイスをオンボーディングした後、各デバイスを編集して、自動的に検出されないデバイス情報を追加する必要があります。詳細については、「Cisco SR-PCE プロバイダの追加」のプロバイダプロパティを参照してください。
5. **ゼロタッチプロビジョニングを使用した自動オンボーディング**：この方法は自動化されていますが、最初にデバイスエントリを作成し、インストールの DHCP サーバーを変更する必要があります。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。この方法を使用してデバイスをプロビジョニングおよびオンボーディングした後、各デバイスを編集して、自動的に提供されない情報を追加する必要があります。詳細については、「ゼロタッチプロビジョニング」を参照してください。

（注） Cisco Crosswork は、シングルスタック展開モードのみをサポートしています。デバイスは、IPv4 アドレスまたは IPv6 アドレスのいずれか（両方ではない）でオンボーディングできます。

Cisco Crosswork にオンボーディングされているデバイスが Cisco Crosswork Data Gateway インターフェイスと同じサブネット上にある場合、それらは Cisco Crosswork Data Gateway のサウスバウンドネットワーク上にある必要があります。これは、Cisco Crosswork Data Gateway が RPF チェックを実装しており、複数の NIC（2 NIC または 3 NIC）が展開されている、デバイスの送信元アドレスが管理ネットワークまたはノースバウンドネットワーク上にないためです。

（注） Crosswork Network Controller 3.0 に使用する IOS XR デバイス（バージョン 7.3.2 または 7.4.1）では、Cisco NSO で NETCONF NED を設定する必要があります。デフォルトでは、NSO ポリシーは CLI NED を使用してデバイスを NSO にオンボーディングします。次の方法で NETCONF NED に変更できます。

- **デバイスのオンボーディング前**：API 要求を使用してポリシーを変更します。詳細については、https://developer.cisco.com/docs/crosswork/#!cat-fp-deployment-manager-api を参照してください。
- **デバイスのオンボーディング後**：
  1. CLI コマンドを使用して NSO のデバイスタイプを変更します（例：`set devices device <device-name> device-type NETCONF ned-id cisco-iosxr-nc-7.3`）。
  2. デバイスの同期元操作を実行します（例：`request devices device <device-name> sync-from`）。

（注） 同期操作が実行されない場合、サービスのプロビジョニングが誤動作することがあります（たとえば、設定がデバイスにプッシュされていないでも、プロビジョニングのステータスが成功と表示されることがあります）。

新しいデバイスのテレメトリの前提条件

新しいデバイスをオンボーディングする前に、Cisco Crosswork でテレメトリデータを正常に収集および送信するようにデバイスを設定する必要があります。次の項では、SNMP、NETCONF、SSH、Telnet などのいくつかのテレメトリオプションの設定例を示します。管理する予定のデバイスを設定するためのガイドとして使用します。

（注） SNMPv2 トラップと SNMPv3（NoAuth/NoPriv）トラップのみがサポートされています。

オンボーディング前のデバイス設定

次のコマンドは、正しい SNMPv2 と NETCONF の設定、および SSH と Telnet のレート制限を設定するオンボーディング前のデバイス設定の例を提供します。NETCONF 設定は、デバイスが MDT 対応の場合にのみ必要です。

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
```

```
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
 server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

SNMPv3 オンボーディング前のデバイス設定

SNMPv3 データ収集を有効にする場合は、前の項の SNMPv2 設定コマンドを繰り返し、次のコマンドを追加します。

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>
```

Cisco NSO デバイスの設定例

Cisco Network Services Orchestrator（Cisco NSO）をプロバイダとして使用して Cisco Crosswork で管理するデバイスを設定する場合は、Cisco NSO デバイスの設定が次の例のガイドラインに従っていることを確認してください。

この例では、デバイス ID としてホスト名を使用する Cisco NSO 設定を示します。CSV ファイルを使用してデバイスをインポートする場合は、**ROBOT_PROVDEVKEY_HOST_NAME** を provider_node_key フィールドの列挙値として使用します。ここで使用する例のホスト名 **RouterFremont** は、CSV ファイル内のデバイスのホスト名と一致する必要があります。

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 830
```

次に、リモート名とパスワードが「cisco」の「cisco」という認証グループを作成する例を示します。次に、「Router」で始まる名前のすべてのデバイスを、ned-id「cisco-iosxr-nc-6.6」を使用して「netconf」のデバイスタイプに設定します。最後に、名前が「Router」で始まるすべてのデバイスを「cisco」認証グループに割り当てます。環境に合うように次の設定を編集します。

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
```

```
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

次の CLI コマンドは、SSH キーのロックを解除してすべてのデバイスから取得します。Cisco NSO は、各デバイスの現在の設定をアップロードして現在の設定を保存することでデバイスと同期します。次のコマンドを使用してデバイス、Cisco NSO、および Cisco Crosswork アプリケーションが共通の設定から開始されていることを確認することが重要です。

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit
```

UI を使用したデバイスの追加

UI を使用してデバイスを 1 つずつ追加するには、次の手順に従います。通常の状況では、いくつかのデバイスを追加する場合にのみこの方法を使用します。

ステップ 1 メインメニューから **[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 ⊞ をクリックします。

ステップ 3 次の表に示すように、新しいデバイスの値を入力します。

ステップ 4 [保存（Save）] をクリックします。すべての必須フィールドに入力するまで、[保存（Save）] ボタンは無効になります。

ステップ 5 （オプション）デバイスをさらに追加するには、この手順を繰り返します。

表 *1 : [*新しいデバイスの追加（*Add New Device***）*]* ウィンドウ（** =*必須）**

フィールド	説明
* [管理状態（Administration State）]	デバイスの管理状態。オプションは、次のとおりです。 • [管理対象外（UNMANAGED）] : Crosswork はデバイスをモニターしていません。 • [ダウン（DOWN）] : デバイスは管理されており、ダウンしています。 • [アップ（UP）] : デバイスは管理されており、稼働しています。

フィールド	説明
*[到達可能性チェック（Reachability Check）]	Crosswork がデバイスの到達可能性チェックを実行するかどうかを決定します。オプションは、次のとおりです。 • [有効（ENABLE）]（CSV では **REACH_CHECK_ENABLE**）：到達可能性を確認して UI の到達可能性状態を自動的に更新します。 • [無効（DISABLE）]（CSV では **REACH_CHECK_DISABLE**）：デバイスの到達可能性チェックは無効です。 常に [有効（ENABLE）] に設定することをお勧めします。[設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。
*[クレデンシャルプロファイル（Credential Profile）]	データ収集や設定変更のためにデバイスへのアクセスに使用するクレデンシャルプロファイルの名前。例：**nso23** または **srpce123**。 [設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。
ホスト名	デバイスのホスト名。
[インベントリ ID（Inventory ID）]	デバイスのインベントリ ID 値。値には最大 128 文字の英数字を使用でき、ドット（.）、アンダースコア（「_」）、コロン（「:」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。 デバイスのホスト名か、またはインベントリ ID の簡単に識別できる名前を選択します。これは、デバイス名として使用されるインベントリ ID とデバイスを Crosswork に同期するために使用されます。
[ソフトウェア タイプ（Software Type）]	デバイスのソフトウェアタイプ。
ソフトウェア バージョン（Software Version）	デバイスのソフトウェア バージョン。
UUID	デバイスの汎用一意識別子（UUID）。
[シリアル番号（Serial Number）]	デバイスのシリアル番号。
[MACアドレス（MAC Address）]	デバイスの MAC アドレス。

フィールド	説明
* [機能（Capability）]	デバイスデータの収集を可能にし、デバイスに設定される機能。これは必須の機能であるため、少なくとも **SNMP** を選択する必要があります。**SNMP** が設定されていない場合、デバイスはオンボーディングされません。その他のオプションは、**YANG_MDT**、**YANG_CLI**、および **GNMI** です。選択する機能は、デバイスのソフトウェアタイプとバージョンによって異なります。 （注） MDT 機能を備えたデバイスの場合、この段階では YANG_MDT を選択しないでください。
[タグ（Tag）]	識別およびグループ化のためにデバイスに割り当てるために使用できるタグ。 デバイスタグを使用して、モニタリングのためにデバイスをグループ化し、デバイスの物理的な場所や管理者の電子メール ID など、他のユーザーにとって重要な可能性がある追加情報を提供します。
[製品のタイプ（Product Type）]	デバイスの製品タイプ。
[Syslog 形式（Syslog Format）]	デバイスから受信した syslog イベントの形式は、Syslog コレクタで解析する必要があります。次のオプションがあります。 • [不明（UNKNOWN）]：Syslog コレクタによる解析を行わない場合は、このオプションを選択します。Syslog 収集ジョブの出力には、デバイスから受信した syslog イベントが含まれます。 • [RFC5424]：デバイスから受信した syslog イベントを RFC5424 形式で解析するには、このオプションを選択します。 • [RFC3164]：デバイスから受信した syslog イベントを RFC3164 形式で解析するには、このオプションを選択します。 詳細については、「Syslog 収集ジョブの出力」の項を参照してください。
接続の詳細（Connectivity Details）	
[プロトコル（Protocol）]	デバイスで使用する接続プロトコル。選択肢は、[SSH]、[SNMP]、[NETCONF]、[TELNET]、[HTTP]、[HTTPS]、[GNMI]、および [GNMI_SECURE] です。 このデバイスの接続プロトコルをさらに追加するには、[接続の詳細（Connectivity Details）] パネルの最初の行の末尾にある ＋ をクリックします。入力したプロトコルを削除するには、パネル内の該当する行の横にある × をクリックします。 同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。少なくとも **SSH** と **SNMP** の詳細は入力する必要があります。**SNMP** を設定しない場合、デバイスは追加されません。デバイスを管理する場合（または XR デバイスを管理している場合）、**NETCONF** の詳細を入力する必要があります。**TELNET** 接続はオプションです。

フィールド	説明
* [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]	デバイスの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。 （注） 予期しない接続の問題が発生する可能性があるため、IP ネットワークに選択したサブネット（デバイスと接続先を含む）に重複するアドレス空間（サブネット/スーパーネット）がないことを確認してください。
* [ポート（Port）]	この接続プロトコルに使用するポート。各プロトコルはポートにマッピングされるため、選択したプロトコルに対応するポート番号を入力してください。各プロトコルの標準的なポート割り当ては次のとおりです。 • SSH：22 • SNMP：161 • NETCONF：830 • TELNET：23 • HTTP：80 • HTTPS：443 GNMI と GNMI_SECURE：ポート値は 57344 ー 57999 です。ここで入力するポート番号が、デバイスで設定されているポート番号と一致していることを確認します。
[タイムアウト（Timeout）]	このプロトコルを使用した通信試行がタイムアウトするまでの経過時間（秒単位）。デフォルト値は 30 秒です。 NETCONF を使用する XE デバイスの場合、推奨される最小タイムアウト値は 90 秒です。その他のすべてのデバイスとプロトコルの場合、推奨される最小タイムアウト値は 60 秒です。
[エンコードタイプ（Encoding Type）]	このフィールドは、**GNMI** プロトコルと **GNMI_SECURE** プロトコルにのみ適用されます。オプションは、**`PROTO`** と **`JSON IETF`** です。 デバイスの機能に基づいて、デバイスで一度にサポートされるエンコーディング形式は 1 つだけです。
[ルーティング情報（Routing Info）]	
[ISIS システム ID（ISIS System ID）]	デバイスの IS-IS システムの ID。これは、IS-IS トポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。
OSPF ルータ ID（OSPF Router ID）	デバイスの OSPF ルータの ID。これは、OSPF トポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。
* [TE ルータ ID（TE Router ID）]	各 IGP のトラフィック エンジニアリング ルータの ID。 （注） トポロジ内の L3 リンクを可視化するには、[TE ルータ ID（TE Router ID）] フィールドを入力して、デバイスを Cisco Crosswork にオンボーディングする必要があります。

フィールド	説明
[ストリーミングテレメトリの設定（Streaming Telemetry Config）]	
Vrf	モデル駆動形テレメトリ（MDT）トラフィックがルーティングされる VRF の名前。
[送信元インターフェイス（Source Interface）]	デバイスタイプのループバックの範囲。このフィールドは任意です。 （注） このフィールドは、デバイスが [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の状態の場合にのみ編集できます。
[所在地（Location）] ネットワークトポロジの地理的ビューに必要な [経度（Longitude）] と [緯度（Latitude）] を除き、ロケーションのすべてのフィールドはオプションです。	
[経度（Longitude）]、[緯度（Latitude）]	経度と緯度の値は、地理的マップがデバイスの正しい地理的位置と他のデバイスへのリンクを表示できるようにするために必要です。経度と緯度を 10 進数（DD）形式で入力します。
[高度（Altitude）]	デバイスが設置されている高度（フィートまたはメートル）。たとえば、**123** です。
[プロバイダとアクセス（Providers and Access）] このデバイスにプロバイダを追加するには、[プロバイダとアクセス（Providers and Access）] パネルの最初の行の末尾にある ＋ をクリックします。入力したプロバイダを削除するには、パネル内のその行の横にある × をクリックします。	
[プロバイダファミリ（Provider Family）]	トポロジの計算に使用するプロバイダタイプ。リストからプロバイダを選択します。
プロバイダー名（Provider Name）	トポロジ計算に使用されるプロバイダタイプ。リストからプロバイダを選択します。
[クレデンシャル（Credential）]	プロバイダに使用するクレデンシャルプロファイル。このフィールドは読み取り専用で、選択したプロバイダーに基づいて自動的に入力されます。

CSV ファイルからのインポートによるデバイスの追加

複数のデバイスを指定する CSV ファイルを作成し、Crosswork にインポートするには、次の手順を実行します。

CSV ファイルからデバイスをインポートすると、まだデータベースにないデバイスが追加され、デバイスレコード内のデータが、インポートされたデバイスのものと一致する [インベントリキータイプ（Inventory Key Type）] フィールド値で上書きされます（これは、システムによって設定され、インポートの影響を受けない UUID を除外します）。このため、インポートする前に、すべての現在のデバイスのバックアップコピーをエクスポートすることをお勧めします。

（注）
- CSV ファイルを使用して多数のデバイスをインポートしている間に、[TE ルータ ID（TE Router ID）] フィールドの値を入力する必要があります。
- Firefox ブラウザを使用して誤った CSV 値を持つ多数のデバイスをインポートすると、ウィンドウが使用できなくなることがあります。この場合は、新しいタブまたはウィンドウで Cisco Crosswork にログインし、正しい CSV 値でデバイスをオンボーディングします。

ステップ 1 メインメニューから **[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。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

ステップ 2 をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートするデバイス CSV ファイルをまだ作成していない場合：

a) [「Device Management template（*.csv）」サンプルファイルのダウンロード（Download sample 'Device Management template (* .csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（デバイスごとに 1 行）。

（注）
- 各デバイスの TE ルータ ID 値が入力されていることを確認します。この値は、SR-PCE から学習したトポロジ内のデバイスを一意に識別するために使用されます。各デバイスの有効な TE ルータ ID がない場合、トポロジは表示されません。
- デバイスのインポート後またはデバイスのオンボーディング後は、TE ルータ ID を変更しないでください。インポート後にデバイスの TE ルータ ID を変更する必要がある場合は、次の手順を実行します。
  1. デバイスを Crosswork から削除する必要があります。
  2. すべての SR-PCE プロバイダを削除する必要があります。
  3. 新しい TE ルータ ID を使用してデバイスを再度オンボーディングします。
  4. SR-PCE プロバイダを再度追加します。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に 2 つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。たとえば、[接続タイプ（Connectivity Type）] フィールドに **SSH;SNMP;NETCONF** と入力し、[接続ポート（Connectivity Port）] フィールドに **22;161;830** と入力した場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：ポート 22
- SNMP：ポート 161

• NETCONF：ポート 830

入力する必要があるフィールドと必須値のリストについては、UI を使用したデバイスの追加 （5 ページ）の [新しいデバイスの追加（Add New Device）] フィールドのテーブルを参照してください。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

（注） CSV ファイルを使用して UI 経由でデバイスまたはプロバイダをインポートする場合、ユーザーは操作が完了するまで待機する必要があります。操作の進行中に [インポート（Import）] ボタンをクリックすると、各デバイスまたはプロバイダのエントリの重複が発生します。

ステップ 6 エラーを解決し、デバイスの到達可能性を確認します。

デバイスが最初にインポートされたときに、そのデバイスが到達不能または動作不能として表示されるのは正常です。ただし、30 分後に到達不能または動作不能と表示される場合は、調査が必要な問題がある可能性があります。調査するには、**[デバイス管理（Device Management）] > [ジョブ履歴（Job History）]** を選択し、[ステータス（Status）] 列に表示されるエラーアイコンをクリックします。一般的な問題として、関連付けられたクレデンシャルプロファイルに正しいクレデンシャルが含まれていないことが挙げられます。これをテストするには、サーバーで端末ウィンドウを開き、関連付けられているクレデンシャルプロファイルで指定されたプロトコルとクレデンシャルを使用してデバイスにアクセスします。

ステップ 7 デバイスを正常にオンボーディングしたら、Cisco Crosswork Data Gateway インスタンスにそれらをマッピングする必要があります。

CSV ファイルへのデバイス情報のエクスポート

デバイスリストをエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。デバイスリストのエクスポートは、システム内のすべてのデバイスのレコードを一度に保持するのに便利です。必要に応じて CSV ファイルを編集して再インポートし、既存のデバイスデータを上書きすることもできます。

エクスポートしたデバイス CSV ファイルには、各デバイスのクレデンシャルプロファイルの名前のみが含まれ、クレデンシャル自体は含まれません。

ステップ 1 メインメニューから **[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。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

ステップ 2 （オプション）必要に応じてデバイスリストをフィルタ処理します。

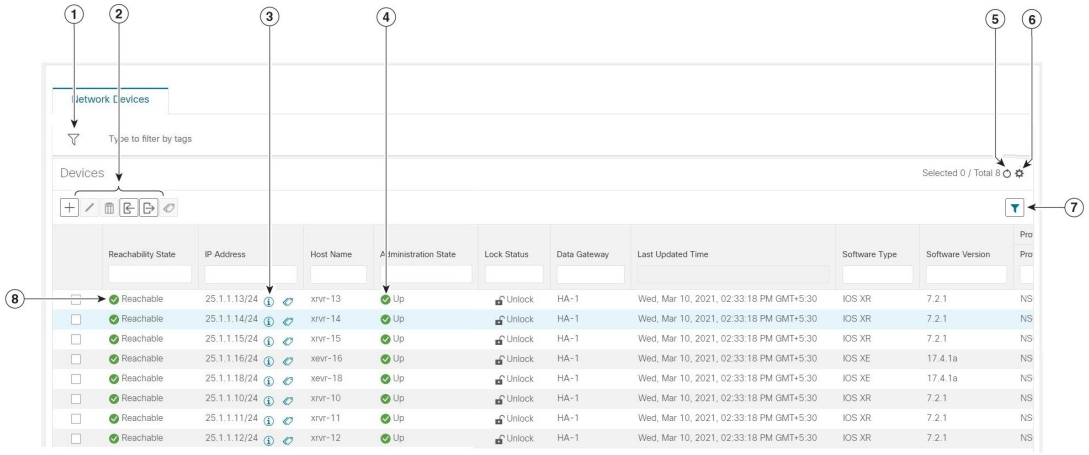
ステップ 3 エクスポートするデバイスのチェックボックスをオンにします。すべてのデバイスをエクスポートするように選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。CSV ファイルを保存する際に使用するパスとファイル名を選択するか、またはすぐに開くかを確認するプロンプトがブラウザに表示されます。

ネットワーク デバイスの管理

Cisco Crosswork の [ネットワークデバイス（Network Devices）] ウィンドウには、すべてのデバイスとそのステータスが統合されたリストが表示されます。[ネットワークデバイス（Network Devices）] ウィンドウを表示するには、**[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。 デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

図 *1 : [*ネットワークデバイス（*Network Devices***）*]* ウィンドウ**



項目	説明
1	[タグによるフィルタ処理（Filter by tags）] フィールドでは、デバイスに適用されているタグでそれらのデバイスをフィルタ処理できます。検索しようとしているデバイスに適用されているタグの名前を入力します。

項目	説明
2	新しいデバイスをデバイスインベントリに追加するには、  をクリックします。
	現在選択されているデバイスの情報を編集するには、  をクリックします。。
	現在選択されているデバイスを削除するには、  をクリックします。
	CSV ファイルを使用して、新しいデバイスをインポートし、既存のデバイスを更新するには、  をクリックします。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。
	選択したデバイスの情報を CSV ファイルにエクスポートするには、  をクリックします。
	選択したデバイスに適用されているタグを変更するには、  をクリックします。を参照してください。
3	 をクリックすると、[デバイスの詳細（Device Details）] ポップアップウィンドウが開き、選択したデバイスの重要な情報を表示できます。
4	[管理状態（Administration State）] 列のアイコンは、デバイスが動作しているかどうかを示します。
5	デバイスリストを更新するには、  をクリックします。
6	デバイスリストに表示する列を選択するには、 をクリックします。
7	デバイスリストの 1 つ以上の列にフィルタ条件を設定するには、  をクリックします。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。
8	[到達可能性状態（Reachability State）] 列のアイコンは、デバイスが到達可能かどうかを示します。

到達可能性と動作状態

Cisco Crosswork は、使用するプロバイダと管理対象デバイスの到達可能性状態、および到達可能な管理対象デバイスの動作状態を計算します。次の表のアイコンを使用してこれらの状態を示します。

表 *2:* 到達可能性と動作状態のアイコン

アイコン	意味
[到達可能性状態（Reachability State）] アイコンは、デバイスまたはプロバイダが到達可能かどうかを示します。	
	[到達可能（Reachable）]：設定されているすべてのプロトコルによってデバイスまたはプロバイダに到達できます。
	[到達可能性低下（Reachability Degraded）]：少なくとも 1 つのプロトコルでデバイスまたはプロバイダに到達できますが、そのデバイスまたはプロバイダに設定されている他の 1 つ以上のプロトコルでは到達できません。
	[到達不能（Unreachable）]：デバイスまたはプロバイダは、そのプロトコルに設定されているプロトコルによって到達できません。
	[到達可能性不明（Reachability Unknown）]：Cisco Crosswork は、デバイスが到達可能か、機能低下か、または到達不能かどうかを判断できません。デバイスが Cisco Crosswork Data Gateway に接続されていない場合にもこの状態になる可能性があります。
[動作状態（Operational State）] アイコンは、デバイスが動作しているかどうかを示します。	
	デバイスは動作中であり、管理下にあります。すべての個別のプロトコルは「OK」（「アップ」とも呼ばれる）です。
	デバイスが動作していません（「ダウン」）。デバイスがオペレータによって「管理上ダウン」に設定されている場合も同じアイコンが使用されます。
	デバイスの動作状態または設定状態が不明です。
	デバイスの動作状態または設定状態が低下しています。

アイコン	意味
	デバイスの動作状態または設定状態がエラー状態です。到達して動作状態を計算しようとしたときに発生したエラーが原因で、アップしていないか、または到達不能です。アイコンの横に表示される円内の数字は、最近のエラーの数を示します。これらのエラーのリストを表示するには、その数字をクリックします（エラーのアイコンバッジは、ネットワークトポロジアプリケーションでは使用できません）。
	デバイスの動作状態は現在確認中です。
	デバイスは削除中です。
	デバイスは管理対象外です。

デバイスの到達可能性状態は次のように計算されます。

1. デバイスの設定状態（ユーザーによる設定）が[アップ（UP）]である限り、到達可能性は常にデバイスごとに計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 到達可能性の状態は常に [到達可能（REACHABLE）]、[到達不能（UNREACHABLE）]、または [不明（UNKNOWN）] のいずれかです。
   - 少なくとも 1 つのプロトコルを介してデバイスへのルートが 1 つ以上あり、かつ、デバイスが検出可能な場合、到達可能性状態は [到達可能（REACHABLE）] です。
   - 1 つのプロトコルを介したデバイスへのルートがない場合、またはデバイスが応答しない場合、到達可能性状態は [到達不能（UNREACHABLE）] です。
   - デバイスが [管理対象外（UNMANAGED）] の場合、到達可能性状態は [不明（UNKNOWN）] です。

デバイスの動作状態は次のように計算されます。

1. （ユーザーが設定した）デバイスの動作状態が[アップ（UP）]である限り、動作状態は常に各デバイスに対して計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 動作状態は常に [OK] または [エラー（ERROR）] です。
3. デバイスを管理上 OK の状態にするには、デバイスが到達可能で検出可能である必要があります。その他の到達可能性状態は [エラー（ERROR）] です。

4. XR デバイスまたは XE デバイスの場合のみ、管理上 OK の状態では、Crosswork ホストとデバイスクロック間のクロックドリフトの差がデフォルトの値（現在は 2 分）よりも小さいことも必要です。

注 一部のタイムゾーン設定では、実際にクロックドリフトが存在しない場合にクロックドリフトエラーが発生することがわかっています。この問題を回避するには、UTC 時間を使用するようにデバイスを設定します。

タグによるネットワークデバイスのフィルタ処理

タグを作成して特定のデバイスに割り当てることで、デバイスの物理的な位置やその管理者の電子メール ID など、他のユーザーにとって重要な可能性のある追加情報を簡単に提供できます。また、タグを使用して、デバイスを一覧表示する任意のウィンドウで同じか、または類似するタグを持つデバイスを検索してグループ化することもできます。

タグでデバイスをフィルタ処理するには、次の手順を実行します。

ステップ 1 メインメニューから **[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 ユーザーインターフェイスの上部にある [入力してタグでフィルタ処理（Type to filter by tag）] バーに、タグ名のすべてまたは一部を入力します。

[入力してタグでフィルタ処理（Type to filter by Tags）] バーには、先行入力機能があります。入力を開始すると、これまでに入力したすべての文字に一致するタグのドロップダウンリストが表示されます。使用可能なすべてのタグをドロップダウンリストに表示するには、***** を入力します。

ステップ 3 フィルタに追加するタグの名前を選択します。[入力してタグでフィルタ処理（Type to filter by tags）] フィルタバーにフィルタが表示されます。テーブルまたはマップには、そのタグを持つデバイスのみが表示されます。

ステップ 4 複数のタグでフィルタリングする場合は次の手順を実行します。

a) フィルタの一部として設定する追加タグごとに、手順 2 と 3 を繰り返します。

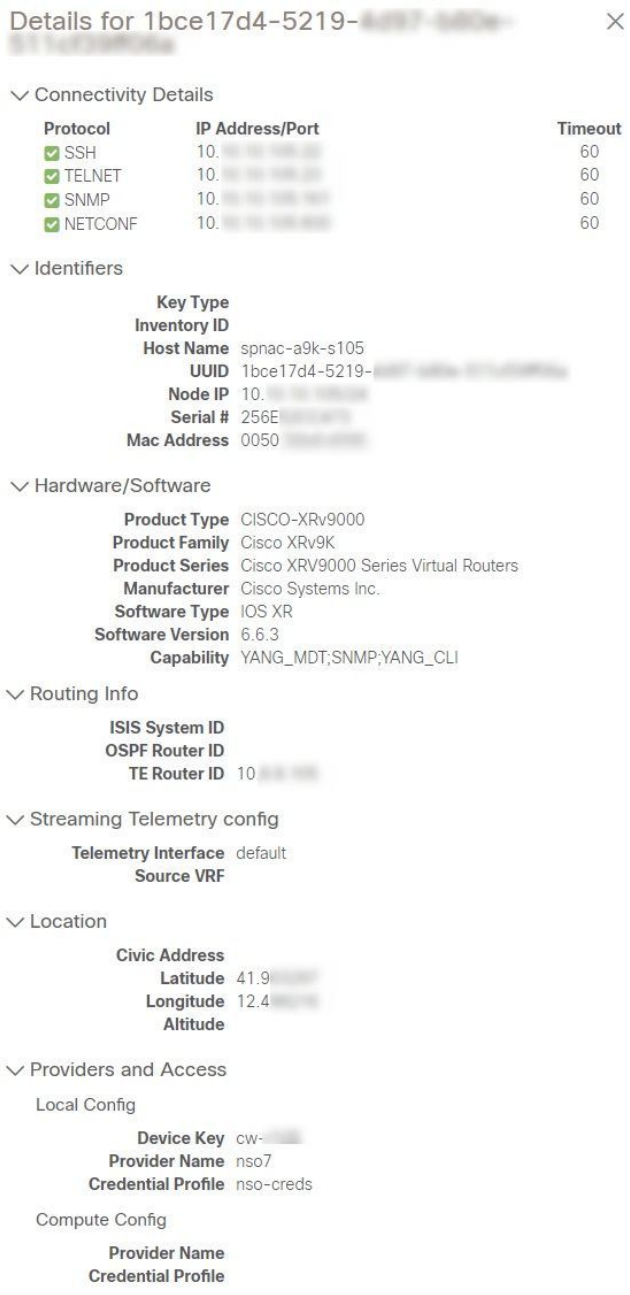
b) 必要なすべてのタグを選択したら、[フィルタの適用（Apply Filters）] をクリックします。テーブルまたはマップには、フィルタ内の**すべて**のタグに一致するタグを持つデバイスのみが表示されます。

ステップ 5 すべてのタグフィルタをクリアするには、[フィルタのクリア（Clear Filters）] リンクをクリックします。複数のタグを含むフィルタからタグを削除するには、フィルタ内のそのタグの名前の横にある [X] アイコンをクリックします。

デバイスの詳細情報の取得

[デバイス管理（Device Management）] > **[ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）] タブにデバイスのリストを表示するたびに、リストされているデバイスの横にある をクリックすると、そのデバイスに関する詳細情報を取得できます。このアイコンをクリックすると、[デバイス名の詳細（Details for DeviceName）] ポップアップウィンドウが開きます。次に例を示します。

図 *2 : [*デバイス名の詳細（***Details for DeviceName***）*]*ウィンドウ



ポップアップウィンドウの上部にある [接続の詳細（Connectivity Details）] 領域を展開します（まだ展開していない場合）。この領域には、すべてのトランスポートタイプの到達可能性ステータスが表示されます。

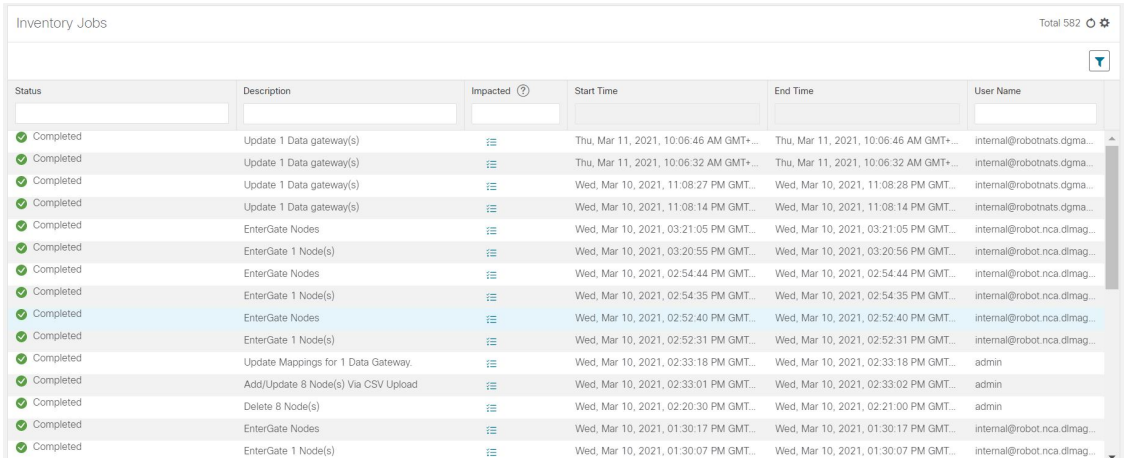
必要に応じて、ポップアップウィンドウの他の領域を展開したり、折りたたんだりします。✕をクリックしてウィンドウを閉じます。

デバイスのジョブ履歴の表示

Cisco Crossworkは、デバイス関連のジョブに関する情報を収集して保存します。作成、更新、および削除のすべてのアクティビティを追跡するには、次の手順を実行します。

ステップ1 メインメニューから **[デバイス管理（Device Management）] > [インベントリジョブ（Inventory Jobs）]** を選択します。[インベントリジョブ（Inventory Jobs）] ウィンドウが開き、次のようなデバイス関連のすべてのジョブのログが表示されます。

図 *3 : [インベントリジョブ（Inventory Jobs）] ウィンドウ*



ジョブは作成時刻の降順に表示されます。最新のジョブが最初に表示されます。テーブル内のデータをソートするには、列の見出しをクリックします。もう一度列の見出しをクリックすると、ソートの昇順と降順が切り替わります。

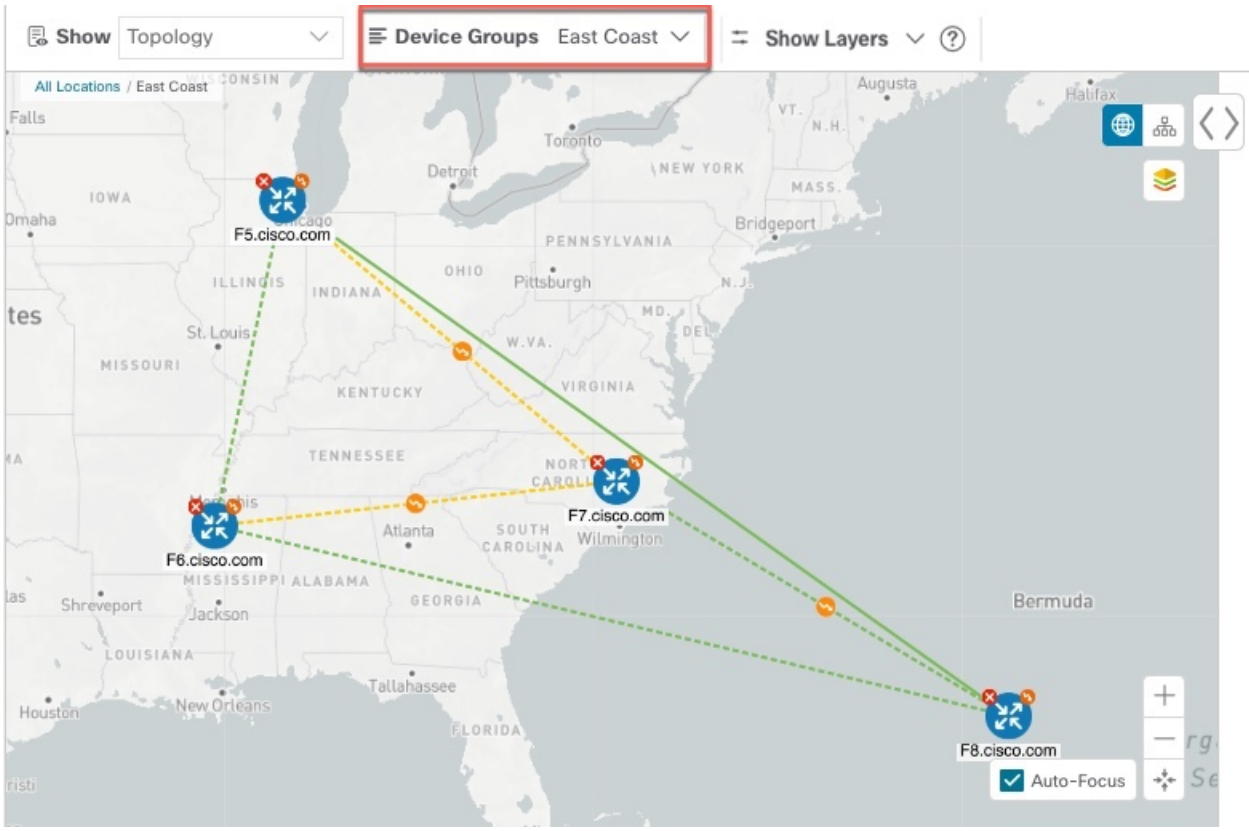
ステップ2 [ステータス（Status）]列には、完了、失敗、実行中、部分的、および警告の状態タイプが表示されます。失敗したジョブまたは部分的なジョブの場合に詳細を確認するには、エラーの横にある をクリックします。

デバイスグループを使用したトポロジビューのフィルタ処理

さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。デバイスグループでは、そのデバイスグループに固有のデータを視覚化して拡大できます。これにより、画面上の乱雑さが軽減され、最も重要なデータに集中できます。たとえば、次の図では、東海岸のデバイスグループが選択されており、トポロジマップに拡大表示

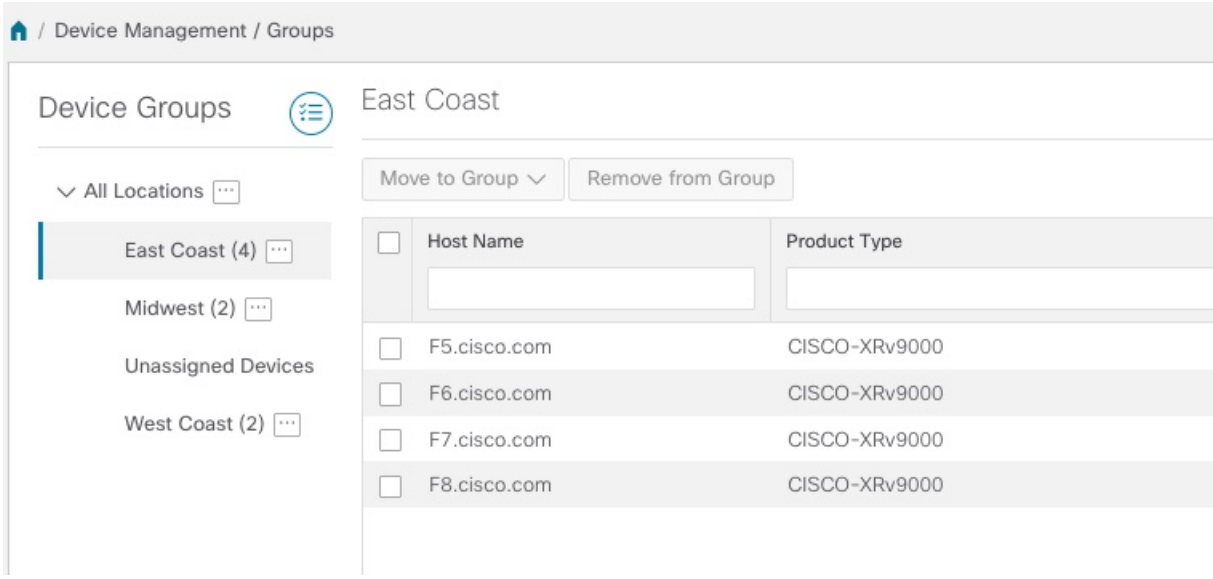
されています。また、[デバイス（Devices）]テーブルには、東海岸のデバイスグループに属するデバイスのみが表示されていることに注意してください。

図 *4:* トポロジマップでのデバイスグループの選択



[デバイスグループ（Device Groups）] ウィンドウ（**[デバイス管理（Device Management）]** > **[グループ（Groups）]**）では、デバイスグループを作成および管理できます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス（Unassigned Devices）] グループに表示されます。

図 *5 : [*デバイスグループ（***Device Groups***）*]* ウィンドウ



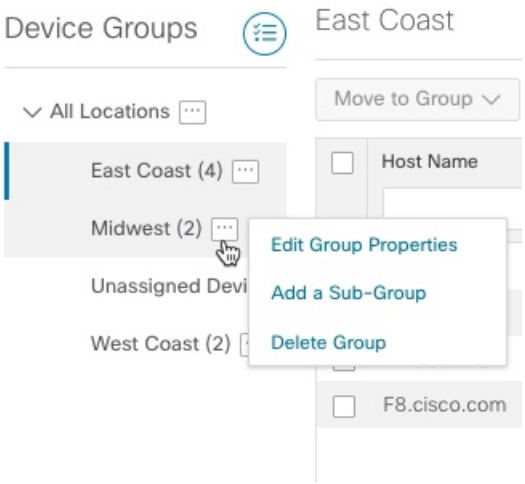
デバイスグループの作成と変更

デバイスグループ、およびグループへのデバイスの割り当ては、手動（この項で説明）または自動（次の項で説明）で実行できます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[グループ（Groups）]** を選択します。

ステップ 2 新しいサブグループを追加するには、[すべての場所（All Locations）]の横にある をクリックします。[すべての場所（All Locations）] の下に新しいサブグループが追加されます。

ステップ 3 既存グループの下で、サブグループを編集、削除、または追加するには、[デバイスグループ（Device Groups）] ツリーでグループの横にある をクリックします。



ステップ 4 グループの追加、削除、または編集（名前の変更または移動）を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

（注） デバイスは、1 つのデバイスグループにのみ属することができます。

ステップ 5 [保存（Save）] をクリックします。

ダイナミック デバイス グループの有効化

デバイスホスト名で正規表現（regex）を使用して、デバイスグループを動的に作成し、未割り当てのデバイスをこれらのグループに自動的に追加するルールを作成できます。ルールに一致する新たに追加または検出されたデバイスは、適切なグループに配置されます。

（注） ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ルールで考慮されるようにするデバイスは、[未割り当てデバイス（Unassigned Devices）] に移動する必要があります。

始める前に

[ダイナミックグループ（Dynamic Groups）] ダイアログに示されている例に従うこともできますが、正規表現に精通していると有利です。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[グループ（Groups）]** を選択します。

ステップ 2 [ダイナミックグループの管理（Manage Dynamic Groups）] アイコンをクリックして、[ダイナミックグループ作成ルールの管理（Manage Dynamic Grouping Rule）] ウィンドウを開きます。

ステップ 3 [他の詳細と例の表示（Show more details and examples）] をクリックして、必要な [ホスト名（Host Name）] フィールドと [グループ名（Group Name）] フィールドに入力します。

ステップ 4 [未割り当てデバイス（Unassigned Devices）] グループに既存のデバイスがある場合は、[ルールのテスト（Test Rule）] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。

ステップ 5 [ルールの有効化（Enable Rule）] チェックボックスをオンにします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 この方法で作成されたグループは、最初は [未割り当てグループ（Unassigned Groups）] の下に表示されます（ルールが初めて有効になったときに作成されます）。新たに作成したグループを必要なグループ階層に移動します。

ステップ 8 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。

a) [すべての場所（All Locations）] の横にある [...] を選択し、[サブグループの追加（Add a Sub-Group）] をクリックします。

b) [新しいグループ（New Group）] に詳細を入力して [保存（Save）] をクリックします。
c) 未割り当ての作成済みダイナミックグループの横にある [...] を選択し、[グループプロパティの編集（Edit Group Properties）] を選択します。
d) [親グループの変更（Change Parent Group）] をクリックし、適切なグループを選択します。

デバイスの編集

デバイスの情報を更新するには、次の手順を実行します。

デバイスを編集する前に、変更するデバイスの CSV バックアップをエクスポートしておくことをお勧めします。

ステップ 1 メインメニューから **[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 （オプション）特定の列をフィルタ処理してデバイスのリストをフィルタ処理します。

ステップ 3 変更するデバイスのチェックボックスをオンにし、  をクリックします。

ステップ 4 必要に応じて、デバイスに設定されている値を編集します。

（注） 既存のフィールドに加えて、選択したデバイスに設定されているデータゲートウェイを表示することもできます。このフィールドは読み取り専用です。

ステップ 5 [保存（Save）] をクリックします。[保存（Save）] ボタンは、すべての必須フィールドの入力が完了するまではグレー表示されます。

ステップ 6 エラーを解決し、デバイスの到達可能性を確認します。

デバイスの削除

次の手順を実行して、デバイスを削除します。

始める前に

- SR-PCE プロバイダの自動オンボーディングを [管理対象（managed）] オプションまたは [管理対象外（unmanaged）] オプションに設定した場合は、1 つ以上の SR-PCE の自動オンボーディングを [オフ（off）] に設定します。
- デバイスを削除する前に、デバイスが切断され、電源がオフになっていることを確認します。
- デバイス が MDT 機能を備えた Cisco NSO にマッピングされ、テレメトリ設定がプッシュされると、それらの設定はデバイスから削除されます。

- 自動オンボーディングが[オフ（off）]に設定されていないためにまだ機能しており、ネットワークに接続されている場合、デバイスは削除時に管理対象外として再検出されます。

ステップ 1 削除するデバイスを含んでいるバックアップ CSV ファイルをエクスポートします。

ステップ 2 メインメニューから **[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 3 （オプション）[デバイス（Devices）] ウィンドウで、[検索（Search）] フィールドにテキストを入力するか、または特定の列をフィルタ処理して、デバイスのリストをフィルタ処理します。

ステップ 4 削除するデバイスのチェックボックスをオンにします。

ステップ 5 をクリックします。

ステップ 6 確認のダイアログボックスで [削除（Delete）] をクリックします。