デバイスの検出

このセクションでは、次の点について説明します。

デバイスの検出

Cisco Prime Collaboration Assurance データベースでデバイスを管理するには、検出を実行する必要があります。必要なデバイス クレデンシャルを追加すると、すべてのサポートされるデバイスを Cisco Prime Collaboration Assurance で検出し管理できます。

ライフ サイクルの検出

検出には、次の 3 つのフェーズがあります。

- アクセスレベルの検出：Cisco Prime Collaboration Assurance によって次のことが行われます。

1. デバイスに対し ICMP を使用して ping を実行できるかどうかのチェックが行われます。ICMP がデバイスで有効になっていない場合は、デバイスは [Unreachable] 状態に移行されます。ICMP 検証を無効にする方法については、「デバイスの再検出」を参照してください。
2. IPアドレスに基づいて、定義済みのクレデンシャルプロファイルがすべて取得されます。クレデンシャル プロファイルの定義方法については、デバイス クレデンシャルの管理を参照してください。
3. SNMP クレデンシャルが一致しているかどうかのチェックが行われます。
4. デバイスのタイプが特定されます。
5. デバイスのタイプに基づいて、その他すべての必須デバイス クレデンシャルが検査されます。必須クレデンシャルが定義されていない場合、検出は失敗します。必要なデバイス クレデンシャルについては、デバイス クレデンシャルの管理を参照してください。

- インベントリの検出：Cisco Prime Collaboration Assurance によって、MIB-II とその他のデバイスの MIB をポーリングし、インベントリ、近接スイッチ、デフォルト ゲートウェイの情報を収集します。また、ポーリングされたデバイスが Cisco Prime Collaboration Assurance でサポートされるかどうかも確認します。
- パス トレース検出：Cisco Prime Collaboration Assurance は、デバイスで CDP が有効になっているかどうかを確認し、CDP に基づいてトポロジを検出します。デバイス間のリンクは CDP を使用して計算され、Cisco Prime Collaboration Assurance データベースに保持されます。

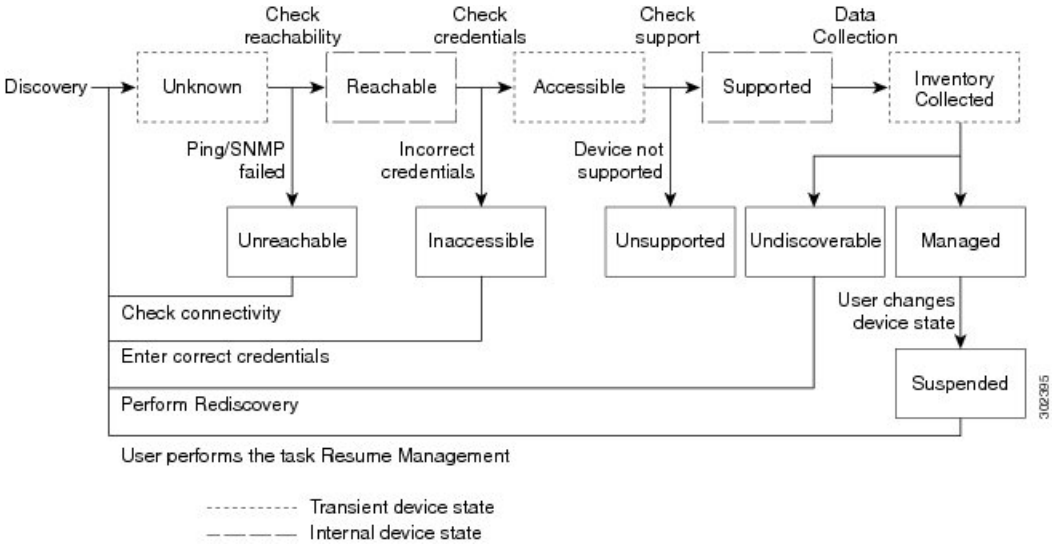
  Cisco Prime Collaboration リリース 11.1 以前の場合

  Cisco Prime Collaboration Assurance が、レイヤ 2 およびレイヤ 3 の両方のパスを検出します。レイヤ 3 パスは、トラブルシューティング ワークフローが手動あるいは自動で起動されると検出されます。デフォルトのホップ カウントは 2 で、設定はできません。

デバイス状態は、Cisco Prime Collaboration Assurance がデバイスにアクセスしてインベントリを収集できることを示しています。デバイスの状態は、ディスカバリまたはインベントリの更新タスクのいずれかを実行した後に限り更新されます。

次の図に、デバイス ディスカバリのライフサイクルを示します。

図 *1:* デバイス検出のライフサイクル



Cisco Prime Collaboration Assurance には、次のデバイス状態が表示されます。

表 *1:* ディスカバリ状態

ディスカバリ状態	説明
不明	これは、デバイスが最初に追加される際の準備中の状態です。これは一時的なステートです。

ディスカバリ状態	説明
Unreachable	Cisco Prime Collaboration Assuranc は、ICMP を使用してデバイスに ping できません。ICMP がデバイスで有効になっていない場合は、デバイスは [Unreachable] 状態に移行されます。
Unsupported	Cisco Prime Collaboration Assurance は、デバイスをデバイス カタログと比較します。デバイスがデバイス カタログのデバイスに一致しないか、SysObjectID が不明の場合、デバイスはこの状態に移行されます。
アクセス可	Cisco Prime Collaboration Assurance は、要求されたすべてのクレデンシャルからデバイスにアクセスできます。これは、アクセス レベル検出の一部であり、デバイス検出中の中間（一時的）状態です。
アクセス不可	Cisco Prime Collaboration Assurance は、要求されたいずれのクレデンシャルからもデバイスにアクセスできません。デバイス クレデンシャルの管理を参照してください。クレデンシャルを確認して、デバイスを検出する必要があります。
インベントリ収集	Cisco Prime Collaboration Assurance は、要求されたデータ コレクタを使用して必要なデータを収集できます。これはインベントリ検出の一部であり、デバイス検出中の中間（一時的）状態です。
Undiscoverable	Cisco Prime Collaboration Assurance は、要求されたデータ コレクタを使用して必要なデータを収集できません。デバイスの状態は、次の場合に検出不能になります。 • SNMP や HTTP/HTTPS のタイムアウトが原因で、接続性の問題が発生する場合があります。また、HTTP/HTTPS を使用してデータを収集する場合は、一度に 1 人の HTTP/HTTPS ユーザだけがログインできます。Cisco Prime Collaboration Assurance にこれらの問題のいずれかが存在する場合、デバイス状態は [検出不能（Undiscoverable）] 状態に移行します。再検出を実行する必要があります。 • Cisco Unified CM、CTS、CTMS、およびその他のネットワーク デバイスには、収集が必要なデータはありません。 • SNMP や HTTP/HTTPS のタイムアウトが原因で、接続性の問題が発生する場合があります。また、HTTP/HTTPS を使用してデータを収集する場合は、一度に 1 人の HTTP/HTTPS ユーザだけがログインできます。Cisco Prime Collaboration Assurance にこれらの問題のいずれかが存在する場合、デバイス状態は [検出不能（Undiscoverable）] 状態に移行します。再検出を実行する必要があります。

ディスカバリ状態	説明
Managed	Cisco Prime Collaboration Assurance により、必要なデバイス データがインベントリ データベースに正常にインポートされました。この状態のデバイスでは、すべての会議、エンドポイント、およびインベントリ データを使用できます。 **Cisco Prime Collaboration リリース 11.1 以前の場合** この状態になっているデバイスだけをトラブルシューティングできます。 （注） Cisco Prime Collaboration Assurance はサードパーティ デバイスをサポートしますが、その管理性は MIB-II サポートに依存します。 Cisco Prime Collaboration Assurance のインベントリがデバイスの制限を超えた場合は、警告メッセージが表示されます。Cisco Prime Collaboration Assurance で管理可能なデバイス数については、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』を参照してください。
Partially Managed	管理対象状態にあるものの、一部のクレデンシャルが不足しているデバイスの数。これらのクレデンシャルは、インベントリの管理に必須ではありませんが、会議のモニタリングなど、他のすべての機能に必要です。対応する数をクリックすると、インベントリ テーブルをクロス起動して、管理対象でありながらクレデンシャルが不足しているすべてのデバイスの一覧を確認できます。この数は、クレデンシャルの追加後に再検出を実行した場合にのみ更新されます。
Suspended	ユーザがデバイスのモニタリングを一時停止しています。この状態のデバイスでは、会議とエンドポイント データは表示されません。この状態のデバイスでは、定期的なポーリングも実行されません。これらのデバイスのインベントリは更新できません。これを行うには、[Resume Management] を実行する必要があります。

（注） 不明なエンドポイントがクラスタ内の登録済み状態に移行すると、[エンドポイントの診断（Endpoint Diagnostics）] ページに、同じエンドポイントのデュアル エントリ（不明および登録済み状態）が午前0時まで表示されます。登録済み状態にあるエンドポイントの単一のエントリは、毎晩行われるクラスタの検出後にのみ表示できます。

関連トピック

デバイス クレデンシャルの管理
デバイス クレデンシャル プロファイルの追加
[Credential Profiles] のフィールドの説明

管理対象デバイスの一時停止と再開

Cisco Prime Collaboration Assurance の削除時にデバイスを削除

デバイスと関連付けられたエンドポイントは、**[State（状態）]** が **[削除済み（Deleted）]** の場合、データベースには保持されません。

下の表は、削除されるデバイスと関連デバイスの一覧表示です。

デバイス	削除される関連デバイス
CUCM の削除： **1.** パブリッシャ **2.** サブスクライバ	関連デバイスは、次のとおりです **1.** クラスタに関連付けられているすべてのものを削除します。 **2.** サブスクライバとこれに登録されているエンドポイントを削除します。
CME の削除	CME とこれに登録されているエンドポイントを削除します。
VCS の削除	これに登録されているすべてのエンドポイントを削除します。
TMS の削除	TMS のみが削除され、MCU、TP_Conductor などの関連デバイスは削除されません。
ESX の削除	すべてのホストされた VM ノードを削除します。
VCENTER の削除	VCENTER が管理するすべての ESX デバイスと関連付けられているノードを削除します。
TP、UNITY CONNECTION、MULTIPOINT CONTROLLER、IM&P、その他のインフラストラクチャ デバイスの削除	デバイスのみが削除されます。

検出方法

次のいずれかの検出方法を選択して、Cisco Prime Collaboration Assurance のデバイスを管理します。

Cisco Prime Collaboration リリース 11.1 以前の場合

検索タイプ	検出方法	説明

自動検出	論理検出	• 管理アプリケーション、会議デバイス、ならびに、Cisco TMS、Cisco VCS、Cisco Unified CM などのコール プロセッサを検出します。
		• 、Cisco TMS、Cisco Unified CM、Cisco VCS に登録されているすべてのエンドポイントとインフラストラクチャ デバイスは、論理検出の際に自動的に検出されます。
		  • Cisco C および Ex シリーズの TelePresence システムの場合、Cisco Prime Collaboration Assurance はファースト ホップ ルータとスイッチを検出しません。
		  • Cisco TMS の論理検出は、VCS、コーデック、Cisco MCU、TPS、Cisco IP Video Phone E20、Cisco MXP シリーズを検出します。
		• Cisco Unified CM Publisher の論理検出は、ネットワーク内にあるその他の Cisco Unified CM（サブスクライバ）、Cisco Unity、Cisco MGCP Voice Gateway、H.323 Voice Gateway、Gatekeeper、CTI アプリケーションを検出します。
		• Cisco Unified CM の SIP デバイス用の論理検出には、コンダクタの検出が含まれています。SIP が設定済みのコンダクタ IP では SNMP が有効ではないため、Cisco Prime Collaboration Assurance では管理されません。このような設定では、Cisco Unified CM の論理検出を実行する前に、管理者 IP を持つコンダクタを管理する必要があります。
		• 管理アプリケーション、会議デバイス、コール プロセッサのどれにも登録されていないエンドポイントとインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。
		• Cisco CTX クラスタは、論理検出を使用して検出されます。
		• Unified Contact Center デバイスは、論理検出を使用して検出されます。
		• 論理検出は、論理的にシード デバイスまたはクラスタに関連付けられている場合は、削除されたデバイスを再度検出します。

検索タイプ	検出方法	説明
自動検出	CDP	• 使用されているメディアやプロトコルとは関係なくデバイスを検出します。このプロトコルは、すべてのシスコ製の機器（ルータ、アクセス サーバ、ブリッジ、スイッチなど）で実行されます。 • この検出方法はネイバーデバイスを見つけるのにCDPネイバーテーブルを照会します。CDP がイネーブルに設定されている場合、検出はSNMP経由で各シードデバイス（およびそのピア）のCDPキャッシュを照会します。CDP検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスがCDP検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • CDP検出を実行するには、デバイス上でCDPがイネーブルに設定されている必要があります。 • CDP検索に使用可能なシードデバイス数に制限はありません。ただし、大規模なネットワークの場合は、一度にすべてのシードデバイスではなく、限られた数のシードデバイスで検索を実行するよう推奨します。

検索タイプ	検出方法	説明
自動検出	Ping Sweep	• 指定の IP アドレスとサブネット マスクの組み合わせから、IP アドレスの範囲内でデバイスを検出します。 • この方法では、デバイスの到達可能性を調べるために、範囲内の各 IP アドレスに ping が送信されます。デバイスが到達可能である場合は、ping するサブネットおよびネットワーク マスクのリストを管理者が指定する必要があります。ping スイープ検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが ping スイープ検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • コール プロセッサが展開されていない場合、またはデバイスが 1 つもコールプロセッサに登録されていない場合は、ping スイープ検出を使用します。この方法では、ターゲット ネットワーク内のすべての新しいインフラストラクチャデバイス、新しいネットワーク デバイス、およびデバイスの新しい位置が検出されます。ターゲット ネットワークのサブネットおよびネットワーク マスクのリストを指定する必要があります。スケジュールされた ping スイープ検出中に、ネットワーク内のすべてのデバイスが特定されて、一致するクレデンシャル プロファイルが検索されます。新しいデバイスが検出された場合は、そのデバイスがインベントリに追加されます。 • ping スイープ検出では、シード デバイスは必要はありません。代わりに、ping するサブネットおよびネットワーク マスクのリストを指定する必要があります。 • IP 範囲が大きい場合、Ping スイープ検出には通常よりも時間がかかることがあります。 • Ping スイープ および CDP 検出を実行するには、クレデンシャル プロファイルを作成する必要があります。 • Ping スイープは、IPv6 アドレスを持つデバイスでは機能しません。

検索タイプ	検出方法	説明
-	Add Devices	• IP アドレスを使用してデバイスを直接検出します。 • ネットワーク内の個々のデバイスを検出します。 • スケジュール設定された検索中に間違ったクレデンシャルが原因でデバイスの検出が失敗した場合は、ダイレクト検出方法を使用して、エラーが発生したデバイスのみを検出できます。 • 論理検出を使用して、SIP デバイスや Presence サーバを検出することはできません。これらのデバイスを手動で追加するか、直接検出を実行する必要があります。 • 登録されているネットワーク デバイスやビデオエンドポイントを検出せずに、シードまたはパブリッシャのデバイスを検出します。 • 新規インストールの後に検出されていない、インフラストラクチャ デバイスを検出します。 • MSP モードの場合、ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出します。
-	インポート	このオプションを使用して、次のものを追加します。 • 大量のデバイス。 • 大規模なグループのサブネット内から、デバイスのサブセット。

（注）
- CDP、Ping スイープ、追加、またはインポートのいずれかの方法を使用してエンドポイントを検出する場合は、エンドポイントが登録されている、当該の Unified CM または Cisco VCS が再検出されていることを確認します。エンドポイントは、コール コントローラに関連付けられている必要があります。
- MSP モードの場合、-ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出するには、デバイスの [追加（Add）] または [インポート（Import）] オプションを使用します。

Cisco Prime Collaboration リリース 11.5 以降の場合

検索タイプ	Discover	説明
自動検出	Communications Manager（UCM）および接続されたデバイス	• 次のパスを使用して、Cisco Unified CM の論理検出を実行します。 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）]** パス（Path） • Cisco Unified CM に登録されているすべてのエンドポイントとインフラストラク チャデバイスは、検出中に自動検出されます。 • コール プロセッサに登録されていないエンドポイントおよびインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。 • Communications Manager とここに接続したデバイスがシードデバイスまたはクラスタに関連付けられている場合、削除されたデバイスを再度検出します。 • Cisco Unified CM Publisher の論理検出は、ネットワーク内にあるその他の Cisco Unified CM（サブスクライバ）、Cisco MGCP Voice Gateway、H.323 Voice Gateway、Gatekeeper、CTI アプリケーションを検出します。 • Cisco Unified CM の SIP デバイス用の論理検出には、コンダクタの検出が含まれています。SIP が設定済みのコンダクタ IP では SNMP が有効ではないため、Cisco Prime Collaboration Assurance では管理されません。このような設定では、Cisco Unified CM の論理検出を実行する前に、管理者 IP を持つコンダクタを管理する必要があります。 • CUCM の論理検出（Communications Manager Publisher）では、SIP トランクは検出されません。 • MSP モードでは、パブリッシャ用のお客様の名前を変更する場合は、そのクラスタに含まれる他のすべてのインフラストラクチャ デバイスで新しいお客様の名前に更新します。 • Unified Communications Manager()を自動的に検出する場合 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][自動設定（Auto-Configuration）]** オプションを使用して、Unified Communications Manager servers の CDR 課金アプリケーション サーバおよび syslog レシーバとして Cisco Prime Collaboration Assurance サーバを追加できます。
		Video Communications Server（VCS）、Expressway クラスタ、接続されたデバイスの論理検出を実行します。

検索タイプ	Discover	説明
	Video Communications Server（VCS）/ Expressway クラスタおよび接続されたデバイス	
	Telepresence Management Suite（TMS）および接続されたデバイス	Telepresence Management Suite（(TMS）と接続されたデバイスの論理検出を実行します。 Cisco TMS の論理検出は、、Cisco MCU、TPS、TP コンダクタを検出します。
	Contact Center Customer Voice Portal（CVP）および接続されたデバイス	Contact Center Customer Voice Portal（CVP）および接続されたデバイスの論理検出を実行します。
	VCenter および接続された ESXi デバイス	VCenter および接続された ESXi デバイスの論理検出を実行します。 Cisco C および EX シリーズの TelePresence システムの場合、Cisco Prime Collaboration Assurance はファーストホップルータとスイッチを検出しません。
	UCS Manager	UCS Manager の論理検出を実行します。

検索タイプ	Discover	説明
自動検出	CDP を使用したネットワーク デバイス	• 使用されているメディアやプロトコルとは関係なくデバイスを検出します。このプロトコルは、すべてのシスコ製の機器（ルータ、アクセス サーバ、ブリッジ、スイッチなど）で実行されます。 • この検出方法はネイバー デバイスを見つけるのに CDP ネイバー テーブルを照会します。CDP が有効な場合、検出は SNMP を使用して各シード デバイス（およびそのピア）の CDP キャッシュを照会します。CDP 検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが CDP 検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • CDP 検出を実行するには、デバイス上で CDP がイネーブルに設定されている必要があります。 • CDP 検索に使用可能なシード デバイス数に制限はありません。ただし、大規模なネットワークの場合は、一度にすべてのシード デバイスではなく、限られた数のシード デバイスで検索を実行するよう推奨します。

検索タイプ	Discover	説明
自動検出	Ping を使用したネットワークデバイス	• 指定の IP アドレスとサブネット マスクの組み合わせから、IP アドレスの範囲内でデバイスを検出します。 • この方法では、デバイスの可用性を調べるために、範囲内の各 IP アドレスに ping が送信されます。デバイスが到達可能である場合は、ping するサブネットおよびネットワーク マスクのリストを管理者が指定する必要があります。ping スイープ検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが ping スイープ検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • コール プロセッサが展開されていない場合、またはデバイスが 1 つもコール プロセッサに登録されていない場合は、ping スイープ検出を使用します。この方法では、ターゲット ネットワーク内のすべての新しいインフラストラクチャ デバイス、新しいネットワーク デバイス、およびデバイスの新しい位置が検出されます。ターゲット ネットワークのサブネットおよびネットワーク マスクのリストを指定する必要があります。スケジュールされた ping スイープ検出中に、ネットワーク内のすべてのデバイスが特定されて、一致するクレデンシャル プロファイルが検索されます。新しいデバイスが検出された場合は、そのデバイスがインベントリに追加されます。 • ping スイープ検出では、シード デバイスは必要はありません。代わりに、ping するサブネットおよびネットワーク マスクのリストを指定する必要があります。 • IP 範囲が大きい場合、Ping スイープ検出には通常よりも時間がかかることがあります。 • Ping スイープ および CDP 検出を実行するには、クレデンシャル プロファイルを作成する必要があります。 • Ping スイープは、IPv6 アドレスを持つデバイスでは機能しません。
自動検出	任意のデバイス	コンダクタなどのその他のすべてのシード デバイスを検出します。

検索タイプ	Discover	説明
-	Add Devices	• IP アドレスを使用してデバイスを直接検出します。 • ネットワーク内の個々のデバイスを検出します。 • スケジュール設定された検索中に間違ったクレデンシャルが原因でデバイスの検出が失敗した場合は、ダイレクト検出方法を使用して、エラーが発生したデバイスのみを検出できます。 • 論理検出を使用して、SIP デバイスや Presence サーバを検出することはできません。これらのデバイスを手動で追加するか、直接検出を実行する必要があります。 • 登録されているネットワーク デバイスやビデオ エンドポイントを検出せずに、シードまたはパブリッシャのデバイスを検出します。 • 新規インストールの後に検出されていない、インフラストラクチャ デバイスを検出します。 • MSP モードの場合、ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出します。
-	インポート	このオプションを使用して、次のものを追加します。 • 大量のデバイス。 • 大規模なグループのサブネット内から、デバイスのサブセット。

（注） 管理アプリケーション、会議デバイス、コールプロセッサのどれにも登録されていないエンドポイントとインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。

前提条件と推奨事項

検出を実行する前には次の点を確認し、必要に応じてデバイスを設定する必要があります。

すべてのデバイス

- デバイスに DNS が設定されている場合、Cisco Prime Collaboration Assurance がそのデバイスの DNS 名を解決できることを確認します。DNS サーバの設定が正しいことを確認します。これは、Cisco Unified CM、Unified Presence サーバ、Unity Connection デバイスではとても重要です。Cisco Prime Collaboration Assurance は、MGCP ゲートウェイのホスト名を解決する必要があります。これは、通常、MGCP ゲートウェイのホス

ト名はゲートウェイとして DNS サーバに追加されず、Cisco Unified CM は DNS を解決せずに同時に操作することが可能なためです。ただし、Cisco Unified CM は MGCP ゲートウェイのホスト名を FQDN として捉えるため、解決することはできません。

- パブリッシャ名とホスト名は一致する必要があります（大文字と小文字を区別）。
- CDP は、すべての 、CTMS、ネットワーク デバイス（ルータとスイッチ）で有効にする必要があります。詳細については、「Cisco IOS を実行する Cisco ルータとスイッチで Cisco Discovery Protocol を設定」を参照してください。
- および IP フォン/ソフトウェア クライアントを除くエンドポイントや TelePresence サーバなどのデバイスは、個別に検出することができます。これらのエンドポイントは、登録されているコール プロセッサの検出を介してのみ検出されます。
- 入力したデバイスのクレデンシャルが正しいことを確認する必要があります。検出プロセス中、検出するデバイスに基づき Cisco Prime Collaboration Assurance は、CLI、HTTP/HTTPS、SNMP を使用してデバイスに接続します。
- デバイスを追加するときは、HTTP（および HTTPS）ポート番号はオプションです。これらの設定は自動的に削除されます。
- 音声とビデオの両方のエンドポイントがネットワーク内に導入されている場合は、検出に時間がかかるため、ネットワーク内のすべてのクラスタを同時に検出することはありません。
- ファイアウォール デバイスはサポートされていません。
- HTTP を使用してデバイスの詳細を取得する場合は、HTTP ファイアウォールを無効にします。
- HSRP 対応デバイスはサポートされていません。
- 複数のインターフェイスと HTTP 管理アクセスを備えたデバイスを追加する場合は、HTTP 管理者アクセスを有効にしたもののと同じインターフェイスを使用し、Cisco Prime Collaboration Assurance でデバイスを管理する必要があります。
- デバイスの検出後、ネットワーク デバイスやインフラストラクチャ デバイス（、CTMS、Cisco Unified CM、Cisco MCU、Cisco VCS、Cisco TS など）の IP アドレスが変更された場合は、新しい IP アドレスまたはホスト名を指定して、これらのデバイスを再検出する必要があります。デバイスの再検出の詳細については、デバイスの再検出 （40 ページ）を参照してください。
- 管理対象デバイスがネットワークから取り外された場合は、そのデバイスは到達不能でも、次のインベントリの収集が行われるまで [Managed] 状態のままとなります。デバイスに到達できない場合は、このデバイスに対して到達不可能のイベントが発生します。
- デバイスで設定を変更した場合、Cisco Prime Collaboration Assurance はインベントリ収集プロセスのみでデバイスを検出することができます。したがって、デバイスで変更された設定は、Cisco Prime Collaboration Assurance が設定の変更後に次のインベントリ コレクションを行うまで表示されません。

- インベントリを定期的に更新し、Cisco Prime Collaboration Assurance データベースと同期させるには、インベントリの更新を実行する必要があります。詳細については、「インベントリの詳細の更新と収集」を参照してください。

Cisco Unified CM

- Cisco Prime Collaboration Assurance は、Unified Communications Manager のクラスタ検出をサポートしています。クラスタ ID は一意である必要があります。
- Unified Communications Manager の Access Control List（ACL）には、管理するすべてのエンドポイントが含まれている必要があります。Unified Communications Manager の SNMP ユーザ設定に ACL が含まれている場合、クラスタ内のすべての Unified Communications Manager ノードには、Cisco Prime Collaboration Assurance サーバの IP アドレスが含まれている必要があります。
- Cisco Prime Collaboration Assurance は、クラスタを管理するため、Unified Communications Manager パブリッシャのみを検出して管理する必要があります。サブスクライバが直接検出されることはなく、パブリッシャによって検出されます。Cisco Prime Collaboration Assurance では、パブリッシャを管理してクラスタを監視する必要があります。Computer Telephony Integration（CTI）サービスは、すべてのサブスクライバで実行されている必要があります。Unified Communications Manager のアクセス制御リストには、管理の必要があるすべてのエンドポイントが含まれていることを確認します。Unified Communications Manager の SNMP ユーザ設定にアクセス制御リストの使用が含まれている場合、Unified Communications Manager サーバの IP アドレスをクラスタ内の Unified Communications Manager ノードに入力する必要があります。
- Cisco Prime Collaboration Assurance には、適切な IP アドレス パターンを使用して、ELM または PLM デバイス タイプのクレデンシャルプロファイルを提供する必要があります。これにより、自動検出ユーザインターフェイスを使用して Unified Communications Manager パブリッシャが Cisco Prime Collaboration Assurance に追加された場合、設定した ELM または PLM が検出されて管理されます。

  Unified Communications Manager が Cisco Prime Collaboration Assurance（**[Inventory（インベントリ）]**>**[インベントリ管理（Inventory Management）]**>**[自動検出（Auto Discovery）]** で自動検出されると、自動設定オプションを使用して、Unified Communications Manager 内の syslog レシーバや CDR 課金アプリケーション サーバを自動に設定することができます。Syslog レシーバや CDR 課金アプリケーション サーバを手動で設定する場合は、[自動設定（Auto-Configuration）] オプションの下にあるチェックボックスをオフにします。Syslog レシーバまたは CDR 課金アプリケーション サーバのエントリを手動で追加する場合は、Unified Communications Manager のスロットに空きがあるかどうか確認することを推奨します。

（注） Syslog レシーバや CDR 課金アプリケーション サーバは、Unified Communications Manager が Cisco Prime Collaboration Assurance 管理されている状態にある場合のみ、自動に設定することができます。

PLM は、別のグループとして、Cisco Unified Communications（UC）アプリケーションの下で表示できます。

- JTAPI クレデンシャルは、Cisco Unified CM クラスタの場合は任意です。ただし、SNMP および HTTP クレデンシャルは Cisco Unified CM パブリッシャおよびサブスクライバに必須です。
- Cisco Unified CM の検出後に新しいエンドポイントを登録した場合は、Unified CM Publisher ノードを再検出して Cisco Prime Collaboration Assurance に追加する必要があります。デバイスの再検出の詳細については、デバイスの再検出 （40 ページ）を参照してください。

（注） 手動によるサブスクライブ ノードの追加は推奨されません。

Cisco Prime Collaboration リリース 11.5 以前の場合

MSP モードでは、Cisco Unified CM の検出前に新しいエンドポイントを登録した場合は、そのエンドポイントを削除し、Cisco Unified CM の検出後に再度追加する必要があります。

Cisco Unified CM Express および Cisco Unity Express

- Cisco Cius と Cisco Unified IP Phone 8900 および 9900 シリーズの検出では、これらのデバイスがインベントリ テーブルに表示されるよう、HTTP インターフェイスを有効にする必要があります。詳細については、『Cisco Unified Communications Manager 7.1 (3) (SIP) 用の Cisco Unified IP Phone 8961、9951、9971 管理ガイド』の 「「Web ページ アクセスの有効化と無効化」」セクションを参照してください。
- Cisco Prime Collaboration Assurance を有効にし、Cisco Unified CM Express と Cisco Unity Express（CUE）で正しい電話番号を提供するには、次の設定を使用する必要があります。

```
ephone 8 mac-address 001A。E2BC.3EFB タイプ 7945
```

type は、電話機のモデル タイプです。モデル タイプが不明な場合は、Cisco.com ですべての電話機モデル タイプについて確認するか、type ? と入力します。電話数を表示させる方法の詳細については、 および [インベントリ管理（Inventory Management）] ページにある および [デバイス管理の概要（Device Management Summary）] ウィンドウを参照してください。

- UC500 シリーズ ルータが Cisco Unified CM Express を実行している場合は、各電話機の設定で「type」を設定し、CISCO-CME_MIB の cmeEphoneModel MIB 変数が正しい電話機モデルを返す必要があります。これにより、Cisco Prime Collaboration Assurance は、Cisco Unified CM Express に登録された電話機を検出できます。
- Cisco Unified CM Express に接続されている Cisco Unity Express が Service Level View に表示されるようにするには、次の設定を使用する必要があります。

```
ダイヤル ピア音声 2999 voip < ここで voip タグ 2999 はボイスメール > 通知先パターン 2105
 < プレフィックスと異なる必要があります。設定済みのボイスメール 2105 > の完全な E.164 である必要があります。conference protocol sipv2 conference target ipv4:10.10.1.121
```

```
dtmf-relay sip-notify codec g711ulaw no vad ! ! テレフォニーサービスのボイスメール
2105
```

ここで dial-peer VoIP タグ（2999）はボイスメール番号と等しくなく、destination-pattern タグ（2105）はボイスメール番号と等しくなっています。これにより、Unity Express が Service Level View で適切に表示されます。

Cisco VCS および Cisco VCS Expressway

- Cisco VCS クラスタを検出できます。クラスタ名は一意である必要があり、Cisco Prime Collaboration Assurance が管理する必要があるすべてのエンドポイントは、Cisco VCS に登録されている必要があります。VCS の検出中には、登録されているエンドポイントも検出されます。クラスタ内のすべての VCS を必ず管理状態にすることで、会議の監視など、関連するすべての機能が動作せず、CDR の作成に影響しないようにします。

（注） たとえクラスタ内の 1 つの VCS でも管理状態にないと、データレポートに不整合が発生する場合があります。

- Cisco VCS の検出後には、新しく登録されたエンドポイントが自動的に検出されます。また、エンドポイントの IP アドレスを変更すると、Cisco Prime Collaboration Assurance は IP アドレスの変更を自動的に検出します。
- Cisco VCS Expressway が DMZ 内で設定されている場合、Cisco Prime Collaboration Assurance は SNMP を介して Cisco VCS Expressway にアクセスする必要があります。アクセスできない場合、このデバイスは [Inaccessible] 状態になります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定

Cisco Prime Collaboration リリース 11.1 以前の場合

CTS-Manager

- Cisco Prime Collaboration Assurance のライセンス版をインストールしている場合は、CTS-Manager Reporting API を設定する必要があります。この機能が CTS-Manager 1.7、1.8、または 1.9 に設定されていない場合、Cisco Prime Collaboration Assurance は CTS-Manager を管理しません。詳細については、『Cisco TelePresence Manager Reporting API 開発者ガイド』を参照してください。
- Cisco Prime Collaboration Assurance は、2 つのスタンドアロン型 CTS-Manager を管理できません。複数の CTS-Manager を使用している場合は、Cisco Prime Collaboration Assurance アプリケーション用にクラスタ内で設定して管理する必要があります。検出を実行する前に、プライマリ サーバの IP アドレスとホット スタンバイサーバまたはセカンダリ サーバの詳細を次のページに入力します。 **[デバイス インベントリ**

（**Device Inventory**）] > **[インベントリ管理（Inventory Management）]** > **[CTS-MAN/TMS/CTX クラスタの管理（Manage CTS-MAN/TMS/CTX Clusters）]**。

Cisco Prime Collaboration リリース 11.1 以前の場合

CTX クラスタ

- Cisco Prime Collaboration Assurance は、Managed Service Provider（MSP）モードのみで Cisco TelePresence Exchange（CTX）クラスタをサポートします。クラスタ名は一意である必要があります。各 CTX クラスタは、1 つのサーバをプライマリ管理サーバ、もう 1 つをセカンダリ サーバとして指名する必要があります。Cisco Prime Collaboration Assurance がクラスタを管理するには、プライマリとセカンダリの管理サーバを検出して管理する必要があります。データベース サーバとコール エンジン サーバは自動的に検出されます。
- 管理ノードでは、API ユーザと SNMP クレデンシャルが必要です。コール エンジンとデータベース ノードでは、SNMP クレデンシャルのみが必要です。詳細については、「Cisco Prime Collaboration Assurance 用のデバイスをセットアップ」を参照してください。
- 検出を実行する前に、プライマリおよびセカンダリ管理サーバの詳細の IP アドレスを次のページに入力します。 。

Cisco TelePresence Conductor

Cisco Prime Collaboration Assurance は、スタンドアロン モデル内で Cisco TelePresence Conductor XC バージョン 1.2 から 3.0.1 をサポートします。クラスタ モデルはサポートしていません。

Cisco TelePresence Management Suite（TMS）の自動検出では、Cisco TelePresence Conductor も検出します。

Cisco TelePresence Conductor は、Cisco Prime Collaboration Assurance サーバのエンタープライズ モードのみでサポートされています。

メディア サーバ

CDP（Cisco Discovery Protocol）がメディア サーバで有効になっていない場合（無効になっているまたは応答しない場合）、Cisco Prime Collaboration Assurance はデバイスを正常に検出することはなく、デバイスは Unsupported 状態へと移行します。

モバイルおよびリモートアクセス（MRA）クライアント

Cisco Jabber、Cisco TelePresence MX シリーズ、Cisco TelePresence System EX シリーズ、Cisco TelePresence System SX シリーズなどのモバイル リモート アクセス（MRA）クライアントは、Cisco Unified Communications Manager の一部としてのみ検出されます。

MRA を正常に検出するには、Cisco Prime Collaboration Assurance で Cisco Expressway のコア機能を搭載した Cisco VCS が Managed 状態にある必要があります。Cisco Expressway のコア機能を搭載した Cisco VCS が Managed 状態にはなく、Cisco Unified Communications Manager が直接検出された場合、[インベントリ管理（Inventory Management）] の では重

複した IP アドレス（Cisco Expressway のコア機能を搭載した Cisco VCS と同じもの）を持つ MRA クライアントが表示されます。

VCS Core が Cisco Prime Collaboration Assurance で管理されていない場合、（インベントリで表示されている）TP MRA エンドポイントは検出されません。

Cisco Unified Contact Center Enterprise（Unified CCE）およびパッケージ化されたContact Center Enterprise（PCCE）

- Cisco Prime Collaboration Assurance は Simple Network Management Protocol（SNMP）機能を使用して、Unified CCE および PCCE デバイスの検出をサポートします。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- SNMP エージェントが機能するには、Unified ICM/CCE サーバに Microsoft Windows SNMP コンポーネントをインストールする必要があります。Microsoft Windows SNMP サービスは Web セットアップの一部として無効になっており、SNMP 要求を処理するため、Cisco Contact Center SNMP Management サービスによって置き換えられています。
- Cisco SNMP エージェント管理の設定は、Windows Management Console Snap-in を使用して設定することができます。
- Cisco Prime Collaboration Assurance では、[SNMP Agent Management Snap-in] ウィンドウの下にある **[システムの説明（System Description）]** フィールドに特殊文字を入力すると、認証エラーと間違ったデバイス情報が表示されます。説明にハイフン（-）、二重引用符（"）、アスタリスク（*）、オクトソープ（#）、ドル（$）、アンダースコア（_）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角カッコ（[ ]）を含めることはできません。

Cisco Unified Contact Center Express（Unified CCX）

SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

Cisco SocialMiner

SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

Cisco Integrated Management Controller（CIMC）

- Cisco Prime Collaboration Assurance は、CIMC デバイス用のアラームとイベントに関するトラップを生成し、トラップの受信者に通知を送信します。トラップは SNMPv1c 通知に変換され、CISCO-UNIFIED-COMPUTING-MIB に従いフォーマットされます。
- システムは CIMC デバイスを自動検出できません。**[デバイスの追加（Add Device）]** ボタンを使用して、デバイスを手動で追加する必要があります。 **[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  システムは CIMC デバイスを自動検出できません。**[デバイスの追加（Add Device）]** ボタンを使用して、デバイスを手動で追加する必要があります。 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**。
- SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- CIMC デバイスは、正しい IP アドレスと SNMP クレデンシャルを入力しないと、管理状態には入りません。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Unified Attendant Console

システムは、サードパーティの Windows デバイスとして Cisco Unified Attendant Console をサポートします。Cisco Prime Collaboration Assurance で Cisco Unified Attendant Console をサポートするには、SNMP を設定する必要があります。詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

Cisco Prime Collaboration リリース 11.6 以降の場合

CE イメージ搭載の ciscoDX70 および ciscoDX80

システムは、CE イメージ搭載の ciscoDX70 および ciscoDX80 デバイスをサポートします。ciscoDX70 および ciscoDX80 デバイスは、Cisco TelePresence デバイスと同様の機能を備えています。Cisco Prime Collaboration Assurance で ciscoDX70 および ciscoDX80 デバイスを検出するには、DX シリーズ デバイスを Cisco Unified Call Manager（UCM）に登録する必要があります。Cisco Prime Collaboration Assuranceで ciscoDX70 および ciscoDX80 デバイスをサポートするには、SNMP、HTTP、CLI を設定する必要があります。詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

（注） Cisco Prime Collaboration Assurance は、CE イメージ搭載の ciscoDX70 および ciscoDX80 デバイスでは、CMR レポートおよびエンドポイントの診断機能をサポートしません。

デバイスの自動検出

エンドポイントとサブスクライバ デバイスが登録されている場合は、シード デバイスまたはパブリッシャ デバイスを検出できます。

（注）
- 探索ジョブは、いったん開始されると、停止したり取り消したりすることはできません。
- ネットワークで ping スイープと CDP 検出の両方を同時に実行することはできません。

論理検出を使用してクラスタを検出するには、クラスタのパブリッシャを検出する必要があります。これによって自動的に、そのサブスクライバが検出され、パブリッシャとサブスクライバの両方に登録されているすべてのエンドポイントとインフラストラクチャデバイスも検出されます。

DHCP 対応エンドポイントの IP アドレスが Cisco Unified CM に登録されていない場合、Cisco Prime Collaboration Assurance によってこのエンドポイントを自動検出できない可能性があります。Cisco Unified CM に登録されているすべての Cisco TelePresence システムについても同様です。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

TelePresence のエンドポイントの検出（TC/CE）は、HTTPS フィードバックを受信するために、slot2 を専用スロットとして使用します。再検出の際には必ず、Cisco Prime Collaboration Assurance は、その登録解除と登録を再度行う必要があります。エンドポイントが Managed 対象の状態であり、登録されている場合にのみ、TC/CE HTTPS フィードバックを登録します。

自動検出ユーザ インターフェイスを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されると、設定されている ELM または PLM も検出されて管理されます。これは、Cisco Prime Collaboration Assurance に、ELM または PLM のデバイス タイプと、正しい IP アドレス パターンを使用したクレデンシャル プロファイルが含まれている場合にのみ可能です。

Cisco Prime Collaboration リリース 11.5 以降の場合

自動検出は、非 NAT 環境でのみ動作します。NAT 環境で、エンドポイントまたはサブスクライバをシード デバイスと関連付けるには、シード デバイスの再検出を実行し、**[論理検出を有効にする（Enable Logical Discovery）]** ボタンを選択します。

自動検出は、非 MSP 展開でのみ動作します。MSP 展開で、エンドポイント、サブスクライバ、ゲートウェイなどのデバイスをクラスタに関連付けるには、関連付けられているすべてのデバイスを Cisco Prime Collaboration Assurance で管理し、クラスタのパブリッシャ CUCM を再検出する必要があります。

Unified Contact Center デバイスを検出するには、タスクのシード デバイスとして CVP - OAMP サーバを入力する必要があります。

デバイスを自動検出するには、次のようにします。

始める前に

自動検出を実行する前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理：検索を実行する前に、必要なクレデンシャルを入力する必要があります。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。
- クラスタのセットアップ：複数の 、Cisco TMS、または CTX クラスタを管理している場合は、特定のアプリケーションの詳細を入力する必要があります。

ステップ 1 選択 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.1 以前の場合

移行方法 **[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

ステップ 2 [インベントリの管理（Inventory Management）] ページで、[自動検出（Auto Discovery）] をクリックします。

ステップ 3 ジョブ名を入力して、[デバイスアクセシビリティのチェック（Device Accessibility）] チェックボックスをオンにします。

ステップ 4 検出方法を選択します。使用に最適な検出オプションの詳細については、および前提条件と推奨事項を参照してください。

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）]「」 を選択すると、ステップ 7 と 8 で説明されている追加の自動設定オプションが表示されます。

ステップ 5 デバイスの IP アドレスまたはホスト名を入力します。検索プロトコルが単一でない場合は、次のように入力します。

例：

- 論理検出、Cisco Discovery Protocol、および直接検出の場合は、サポートされるデリミタの 1 つ（カンマ、コロン、パイプ、または空白）を使用して複数の IP アドレスまたはホスト名を入力できます。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  Communications Manager（UCM）クラスタおよび接続デバイス、Video Communications Server（VCS）/ Expressway クラスタおよび接続デバイス、Telepresence Management Suite（TMS）および接続デバイス、Contact Center Customer Voice Portal（CVP）および接続デバイス、VCenter および接続 ESXi デバイス、UCS Manager 検出、CDP 検出を使用したネットワーク デバイス、直接検出の場合は、サポートされるデリミタの 1 つ（カンマ、コロン、パイプ、または空白）を使用して複数の IP アドレスまたはホスト名を入力できます。

- ping スイープ検出を使用したネットワーク デバイスでは、/netmask 指定を使用し、IP アドレス範囲をカンマで区切って指定します。たとえば、172.20.57.1 から始まり、172.20.57.255 で終わる ping スイープ範囲を指定する場合は、172.20.57.1/24 を使用します。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、デバイスを検出するお客様を選択することができます。非 NAT 環境では、パブリック IP（管理 IP）には検出された IP アドレスが入力され、プライベート IP にはデフォルトでパブリック IP（管理 IP）が入力されます。Cisco Prime Collaboration Assurance を Enterprise モードで展開した場合は、デバイスを検出する **Assurance ドメイン** を選択できます。自動検出によって検出されたすべてのエンドポイントは、シード デバイス用に選択された同じ **Assurance ドメイン**に関連付けられます。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、デバイスを検出するお客様を選択することができます。非 NAT 環境では、パブリック IP（管理 IP）には検出された IP アドレスが入力され、プライベート IP にはデフォルトでパブリック IP（管理 IP）が入力されます。Cisco Prime Collaboration Assurance を Enterprise モードで展開した場合は、検出するデバイスの **ドメインに関連付け**オプションを選択できます。自動検出によって検出されたすべてのエンドポイントは、シード デバイス用に選択された同じ [ドメインに関連付け（Associate to Domain）]に関連付けられます。

ステップ 6 （任意）[Filter] および [Advanced Filter] の詳細を入力します（論理、CDP、および ping スイープ検出方法の場合のみ使用可能）。ワイルドカードを使用して、含めるか、または除外する IP アドレスと DNS 情報を入力することができます。フィールドの説明については、「検出フィルタとスケジュールオプション」を参照してください。

ステップ 7 （任意）ステップ 4 で、[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）]「」を選択し、Unified Communications Manager サーバで CDR 課金サーバの自動設定を有効にしない場合は、[自動設定（Auto-Configuration）] ペインで、[Unified CM サーバで Prime Collaboration サーバを CDR 接続先として追加する（Add the Prime Collaboration Server as a CDR Destination in the Unified CM Servers）] チェックボックスをオフにしてください。

（注） CDR 課金サーバの自動設定の一部として、Cisco Prime Collaboration Assurance は、Unified Communications Manager のパブリッシャとサブスクライバの両方で CDR フラグと CMR フラグを有効にします。ただし、Cisco Prime Collaboration Assurance が CDR 課金サーバの自動設定を実行するのは、管理対象の Unified Communications Manager のパブリッシャのみです。

ステップ 8 （**Cisco Prime Collaboration リリース 11.5 以降の場合**）（任意）ステップ 4 で、[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）] 「」を選択し、Unified Communications Manager サーバで syslog 受信者の自動設定を有効にしない場合は、[自動設定（Auto-Configuration）] ペインで、[Unified CM サーバで Prime Collaboration サーバを syslog 送信先として追加する（Add the Prime Collaboration Server as a CDR Destination in the Unified CM Servers）] チェックボックスをオフにしてください。

（注） Cisco Prime Collaboration Assurance は、syslog 受信者の自動設定を、管理対象の Unified Communications Manager のパブリッシャだけでなく、サブスクライバに対しても実行します。Unified Communications Manager は、設定されたすべての Syslog 受信者に対して、アラームおよびイベントのレベルを「情報」に更新します。

ステップ 9 定期的な検出ジョブをスケジュールするか（フィールドの説明については「検出フィルタとスケジュール オプション」を参照）、またはステップ 10 に従って検出ジョブをすぐに実行します。

ステップ 10 [すぐに実行（Run Now）] をクリックして検出ジョブをすぐに実行するか、[スケジュール（schedule）] をクリックして定期的な検出ジョブをスケジュールし、後で実行します。検索スケジュールを設定している場合は、ジョブの作成後に通知が表示されます。[ジョブの進行状況（Job Progress）] をクリックすると、[ジョブの管理（job management）]ページにジョブのステータスを表示できます。あるいは、すぐに検出を実行している場合は、[デバイス ステータスの概要（Device Status Summary）] ハイパーリンクをクリックして、検出対象のデバイスの現在の状態を確認することができます。

（注）
- Unified Communications Manager の特定のノードを削除すると、Cisco Prime Collaboration Assurance によって、そのノードの IP アドレスの syslog または CDR の設定も削除されます。同じデバイスの、他の syslog または CDR の設定変更は、影響を受けません。
- CDR 課金サーバまたは syslog 受信者の自動設定や手動設定が、Unified Communications Manager のパブリッシャあるいはそのいずれかのサブスクライバで利用できない場合、システムは、デバイスの [ステータス理由（Status Reason）] を [部分管理対象（Partially Managed）]「」 と表示し、同時にその理由（たとえば、「デバイス上の syslog 設定が見つからない」など）も表示します。ただし、Cisco Prime Collaboration Assurance では、デバイスの状態は 「[管理対象（Managed）]」 のままです。

トラブルシューティング

1. **問題**：Cisco Prime Collaboration Assurance がデバイスに CDR アプリケーション課金サーバとして追加されない。

   推奨処置：

   - [自動検出（Auto Discovery）]「」オプションを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されていることを確認します。
   - インベントリを検出した後、デバイスが Managed の状態であることを確認します。また、デバイスは、[コール品質データ ソース（Call Quality Data Source）] の下に表示される必要があります。**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDS ソース設定（CDR Source Settings）]**。
   - [Unified Communications Managerの管理（Unified Communications Manager Administration）] ページで、[サービスアビリティ（Serviceability）]ページを選択し、[CDR管理（CDR Management）] ページに移動します。自動設定が実行されるように、少なくとも 1 台の CDR 課金サーバが使用可能であることを確認してください。

2. **問題**：Cisco Prime Collaboration Assurance がデバイスのリモート Syslog 受信者として追加されない。

   推奨処置：

   - [自動検出（Auto Discovery）]「」オプションを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されていることを確認します。
   - インベントリを検出した後、デバイスが Managed の状態であることを確認します。

- [Unified Communications Manager の管理（Unified Communications Manager Administration）] ページで、[サービスアビリティ（Serviceability）] ページを選択し、**[アラーム（Alarm）]** > **[設定（Configuration）]**。自動設定が実行されるように、少なくとも 1 台の Syslog 受信者が使用可能であることを確認してください。

3. **問題**: TMS 検出では、一部の接続済みデバイスが検出されるわけではありません。

   推奨処置：

   Cisco Prime Collaboration Provisioning Assurance 12.1 以降は、TMS の検出によって、TMS で管理されている CUCM、VCS、およびエンドポイントを自動的に検出しません。

検出フィルタとスケジュール オプション

検出のフィルタ

次の表に、検出の実行の際に使用可能なフィルタを示します。

表 *2*:検出のフィルタ

フィルタ	説明
[IPアドレス（IP Address）]	included または excluded デバイスのカンマ区切りの IP アドレスまたは IP アドレス範囲。1 ～ 255 のオクテット範囲では、アスタリスク（*）ワイルドカードを使用するか、[xxx-yyy] 表記を使用して制限します。次に例を示します。 • 172.20.57/24 サブネット内にあるすべてのデバイスを含める場合は、172.20.57.* という組み込みフィルタを入力します。 • 172.20.57.224 から 172.20.57.255 の IP アドレス範囲内のデバイスを除外するには、172.20.57.[224-255] の除外フィルタを入力します。 両方のワイルドカード タイプを同じ範囲で使用することができます。例：172.20.[55-57].* 組み込みフィルタと除外フィルタの両方が指定されている場合は、除外フィルタが適用されてから組み込みフィルタが適用されます。自動検出されたデバイスにフィルタを適用すると、その他のフィルタ基準はデバイスに適用されません。デバイスに複数の IP アドレスがある場合、include フィルタを満たす IP アドレスが 1 つの場合に限り、デバイスが自動検出に対して処理されます。
詳細フィルタ	

フィルタ	説明
DNS ドメイン	included または excluded デバイスのコンマ区切りの DNS ドメイン名。 アスタリスク（*）ワイルドカードは、任意の長さ、任意の英数字、ハイフン（-）、およびアンダースコア（_）の組み合わせに一致します。 疑問符（?）のワイルドカードは、単一の英数字、ハイフン（-）、またはアンダースコア（_）に一致します。 たとえば、「*. cisco.com」は、「cisco.com」で終わる任意の DNS 名と一致し、「*.?abc.com」は、「aabc.com」や「babc.com」などで終わる任意の DNS 名と一致します。
Sys Location	（CDP 方式と ping スイープ検出方式でのみ使用できます。）included または excluded デバイスに対する、MIB-II の ysLocation OID に保存されたコンマ区切りの文字列値に一致するコンマ区切りの文字列。 アスタリスク（*）ワイルドカードは、英数字、ハイフン（-）、アンダースコア（_）、および空白文字（スペースとタブ）を任意の長さで組み合わせたものに一致します。たとえば、San * という SysLocation フィルタは、San Francisco、San Jose などで始まるすべての SysLocation 文字列に一致します。 疑問符（?）のワイルドカードは、1 つの英数字、ハイフン（-）、アンダースコア（_）、または空白文字（スペースまたはタブ）と一致します。

Schedule Options

次の表で、使用可能なスケジュール オプションについて説明します。

表 *3 : Schedule Options*

フィールド	説明
Start Time	[開始時刻（Start Time）] をクリックして、開始の日時を yyyy/MM/dd と hh:mm AM/PM の形式で入力します。 カレンダーから開始日と開始時刻を選択する場合は、日付ピッカーをクリックします。表示される時刻は、クライアント ブラウザの時刻です。スケジューリングされた定期的ジョブは、この指定時刻に実行されます。
繰り返し	[なし（None）]、[毎時（Hourly）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）] のいずれかをクリックし、ジョブの期間を指定します。
設定	ジョブ期間の詳細を指定します。
終了時刻	終了日時を指定する必要がない場合は、[終了日時なし（No End Date/Time）] をクリックします。[Every number of Times] をクリックして、指定した期間にジョブが終了するまで、そのジョブが実行される回数を設定します。終了日と終了時刻をそれぞれ yyyy/MM/dd と hh:mm AM/PM 形式で入力します。

デバイスの手動検出

[デバイス ワーク センター（Device Work Center）][デバイス管理（Inventory Management）] ページで [デバイスの追加（Add Device）] オプションを使用して、1 つまたは複数のデバイスを Cisco Prime Collaboration Assurance に手動で追加できます。

新しいデバイスを追加し、検出を実行するには、次の手順を実行します。

始める前に

デバイスを追加する前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理：検索を実行する前に、必要なクレデンシャルを入力する必要があります。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

ステップ 2 [インベントリ管理（Inventory Management）] ページで、**[デバイスの追加（Add Device）]** をクリックします。

ステップ 3 [デバイスの追加（Add Device）] ウィンドウで、必要な情報を入力します。異なるクレデンシャルの詳細については、「クレデンシャル プロファイル フィールドの説明」 を参照してください。

展開に基づいて、[デバイス情報（Device Information）] ペインでデバイスを追加する [顧客（Customer）] または[ドメインに関連付け（Associate to Domain）] を選択できます。

- NAT：検出対象のデバイスが NAT 環境内にある場合は、このチェックボックスをオンにします。
- 顧客：デバイスを検出する顧客を選択できます。
- IP アドレス：パブリック IP アドレスまたは管理対象 IP を入力します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
- プライベート IP アドレス：プライベート IP アドレスを入力します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
- プライベート ホスト名：プライベート ホスト名を入力します。

（注） Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、Unified CM または ELM に登録されているエンドポイントを設定する際に、[プライベートホスト名（Private Host Name）] フィールドに FQDN を入力する必要があります。

（注） 各顧客のデバイスを個別のインスタンスに追加する必要があります。1 つのインスタンスで 1 つの顧客に対して最大 5 台のデバイスを追加できます。デバイスを追加するには、[デバイスの追加（Add Device）] ボタンをクリックします。空の行を必ず削除してください。

ステップ 4 [Discover] をクリックします。検出ジョブのステータスは、[ジョブの管理（Job Management）] ページで確認できます。デバイスは、検出後にインベントリ テーブルに表示されます。詳細については、「検出ステータスの確認」を参照してください。

また、[Assuranceインベントリの概要（Device Status Summary）] を表示して、検出されたデバイスの数と、検出が進行中のデバイスの数を確認することもできます。

ステップ 5 **[検出（Discover）]** をクリックします。ポップアップが表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

デバイスの検出が開始されます。検出されるデバイスの現在の状態を確認するには、[デバイスステータスの概要（Device Status Summary）] のハイパーリンクをクリックします。

デバイスのインポート

デバイス リストとクレデンシャルを含むファイルをインポートすることによって、Cisco Prime Collaboration Assurance にデバイスをインポートすることができます。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、グローバル カスタマー選択フィールドで選択したお客様のデバイスのみがインポートされます。

デバイスをインポートするには、デバイスごとに次を追加する必要があります。

- ホスト名
- [IP アドレス（IP Address）]
- プロトコルのクレデンシャル

（注） クレデンシャルはプレーンテキストでも暗号化してもかまいませんが、同じファイルに両方を追加することはできません。

- デバイスが NAT 環境にある場合は、そのデバイスの顧客名、プライベート IP アドレスとパブリック IP アドレス、およびプライベート ホスト名を追加してください。
- Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、Unified CM または ELM に登録されているエンドポイントを設定する際に、ホスト名を FQDN として指定する必要があります。
- パブリッシャに登録されているすべてのエンドポイントまたはサブスクライバは、パブリッシャから顧客名を継承します。

（注） デバイスの詳細のみを変更するようにしてください。それ以外の行を変更すると、このファイルが破損し、インポート タスクが失敗する原因になります。

ファイルからデバイスをインポートするには、次のようにします。

始める前に

デバイスをインポートする前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理（Manage Device Credentials）：デバイスの管理に必要なクレデンシャル。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。
- デバイスリストとクレデンシャルのエクスポート（Export Device Lists and Credentials）：インポートとエクスポートのファイル形式は同じです。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

ステップ 2 **[インポート（Import）]** をクリックします。

警告 **Cisco Prime Collaboration リリース 11.5 以降の場合**

セキュリティ上の理由により、エクスポートされたデバイスのクレデンシャル ファイルは、同じサーバ上でのみインポートできます。

ステップ 3 [インポート（Import）]ダイアログボックスで、インポートするデバイスとクレデンシャルのリストを含むファイルを参照します。（CSV または XML ファイル形式のみがサポートされています）。暗号化されたクレデンシャルを含むファイルをインポートする場合は、[ファイルは暗号化されたクレデンシャルを含む（File contains Encrypted Credentials）] チェックボックスをオンにします。

ステップ 4 **[インポート（Import）]** をクリックします。

（注） シードまたはパブリッシャ デバイスに対し、インポートベースの検出を実行すると、クラスタ名などの登録済みエンドポイントの登録や関連付けの情報が、完全には取得できません。このような場合は、シードデバイスの再検出を実行して、登録と関連付けの情報を完全に取得してください。

インポートされたデバイスのステータス理由は、デバイスの再検出を実行すると更新されますが、自動検出がそのデバイスを検出するまで待てば更新されます。

インポートされたデバイス リストとクレデンシャルに対するクレデンシャル プロファイルは作成されません。インポート後に、デバイス検出が自動的にトリガーされます。このときに使用されるのは、インポートファイルにあるクレデンシャルです。インポートベースの検出ジョブのステータスは、[ジョブ管理（Job Management）]ページで確認できます。詳細については、「検出ステータスの確認」を参照してください。インポートされたデバイスのクレデンシャルが正しくない場合は、そのデバイスは [Managed] 状態になることができません。

検出後に、インポートされたデバイスがインベントリに表示されます。他のデバイスの詳細、物理情報、アクセス情報は、インベントリ テーブルの下にあるそれぞれのペインに表示されます。また、[デバイスステータスの概要（Device Status Summary）] を表示して、検出されたデバイスの数と、検出が進行中のデバイスの数を確認することもできます。

デバイス リストとクレデンシャルのエクスポート

デバイス リストとデバイスのクレデンシャルをファイルにエクスポートできます。このファイルを使用して、デバイス リストとクレデンシャルを変更し、後でインポートすることができます。この機能は、ネットワーク管理者、システムの上級管理者、およびシステム管理者の役割を持つユーザのみが使用できます。

デバイス リストとクレデンシャルをエクスポートするには、次の手順を実行します。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）] > [エクスポート（Export）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[ベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [エクスポート（Export）]**

ステップ 2 [デバイス リストとクレデンシャル（Device list and Credentials）] を選択し、出力ファイル名を入力します（サポートされているのは、CSV および XML ファイル形式のみです）。

ステップ 3 [Export] をクリックします。このファイルに含まれているのは、暗号化されたクレデンシャルのみです。

Cisco Prime Collaboration リリース 11.5 以降の場合

警告 セキュリティ上の理由により、エクスポートされたデバイスのクレデンシャル ファイルは、同じサーバ上でのみインポートできます。

ステップ 4 ダイアログボックスが表示されたら、次のいずれかの操作を実行します。

- [開く（Open）] をクリックして情報を確認します。
- [保存（Save）] をクリックして、CSV または XML ファイルをローカルのシステムに保存します。

（注） デバイスが NAT 環境にある場合は、顧客名、プライベート IP アドレスとパブリック IP アドレス、およびプライベート ホスト名も更新されます。

トラブルシューティング

1. **問題**：1 つのサーバから別のサーバにデバイス クレデンシャルをインポートするときに、デバイスが検出されません。

   推奨事項：エクスポートされたデバイス クレデンシャル ファイルは、同じサーバ上のみでインポートできます。

2. **問題**：最新リリースにインポートするため、以前のリリースでエクスポートしたクレデンシャルを使用したときにデバイスが検出されません。

   推奨事項：エクスポートされたデバイス クレデンシャル ファイルは、同じサーバ上のみでインポートできます。

Cisco Unified Computing System（UCS）の検出

次の手順を実行して、NAT 導入環境内の Cisco UCS を検出し、vCenter、ESX、UCS Manager デバイスが Cisco Prime Collaboration Assurance に追加されていることを確認します。

始める前に

- 非 NAT 展開では、VMware vCenter Server（vCenter）、VMware ESX Server（ESX）、および Cisco UCS Manager（UCS Manager）デバイスがサポートされる必要があります。
- 検出中に仮想マシン（VM）の電源をオンにする必要があります。

（注） 新たに追加された仮想マシン（VM）の中で、ポーリングまたは ESXi ホストの再検出によって検出されないものは、論理検出を使用して検出することができます。

- 検出を実行する前に、VMware ツールを VM にインストールする必要があります。これにより、VMware ESX サーバの検出中にツールが確実に検出されます。
- NAT 導入では、管理対象 ESX サーバ内の VM 名は、Cisco Prime Collaboration Assurance 内の VM のプライベート ホスト名と同じである必要があります。
- vCenter を設定し、UCS ブレードでイベントおよびアラームの相関ルールを確認します。詳細については、「vCenter の構成 （37 ページ）」を参照してください。
- Cisco UCS Manager の SNMP を有効にして設定し、SNMP マネージャと SNMP エージェント間の関係を作成します。
  1. Cisco UCS Manager で、[管理（Admin）] タブに移動してタブを展開し、[通信サービス（Communication Services）] タブを選択します。
  2. SNMP ウィンドウのフィールドを設定し、変更を保存します。

ステップ 1 Cisco Prime Collaboration Assurance サーバにログインし、次のページに移動します。**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance サーバにログインして、**[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]** に移動します。

ステップ 2 [クレデンシャルの管理（Manage Credentials）] ボタンをクリックすると、VMware ESX Server（ESX）、Cisco UCS MANAGER（UCS manager）、および VMware vCenter Serve（vCenter）のクレデンシャル プロファイルが作成されます。

（注）
- VMware ESX サーバの SNMP クレデンシャルを設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- VMware ESX Server のクレデンシャル プロファイルの HTTP クレデンシャルは、VMware ESX Server デバイスのクレデンシャルと同じである必要があります。
- クラスタ シナリオでは、Cisco UCS Manager のクレデンシャル プロファイルの HTTP クレデンシャルは、プライマリ ファブリック インターコネクト デバイスのクレデンシャルと同じである必要があります。
- スタンドアロン シナリオでは、Cisco UCS Manager のクレデンシャル プロファイルの HTTP クレデンシャルは、ファブリック インターコネクト デバイスのクレデンシャルと同じである必要があります。
- vCenter クレデンシャル プロファイルの HTTP クレデンシャルは、vCenter デバイス管理者のログイン クレデンシャルと同じである必要があります。
- 仮想マシンは、NAT 展開と非 NAT 展開の両方でサポートされています。

ステップ 3 次の論理検出を実行します。

- [ESX 論理検出（ESX Logical Discovery）]：Esx Server の IP アドレスをシード デバイスとして使用し、そこで実行されているすべての VM を検出します。
- [UCS Manager論理検出（UCS Manager Logical Discovery）]：クラスタ シナリオでは、Cisco UCS Manager の仮想 IP アドレスを、論理検出のシード IP アドレスとして使用します。UCS Manager が管理している UCS シャーシを検出し、さらに、管理対象 ESX サーバを適切な UCS シャーシに関連付けます。スタンドアロン シナリオでは、ファブリック インターコネクト デバイスの IP アドレスを論理検出のシード IP アドレスとして使用します。
- [vCenter 論理検出（vCenter Logical Discovery）]：vCenter IP アドレスをシード デバイスとして使用し、vCenter サーバで管理される vCenter および ESX のサーバを検出します。

（注）
- 管理対象 ESX server 内の VM 名は、VM のプライベート ホスト名と同じであり、Cisco Prime Collaboration Assurance で VM を適切にグループ化できる必要があります。
- 論理検出は MSP 展開ではサポートされていません。

NAT を導入していない環境で、Cisco UCS および 1 つ以上の関連付けられた仮想マシンを検出するには、次の手順を実行します。

1. **Cisco Prime Collaboration リリース 11.1 以前の場合**

   選択 **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][検出方法（Discovery Methods）]** ドロップダウン リストで **[論理検出（Logical Discovery）]** を選択します。

   Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][検出（Discover）]** ドロップダウン リストで **[UCSマネージャ（UCS Manager）]** を選択します。

vCenter IP アドレスをシード デバイスとして、論理検出を実行します。これにより、vCenter と vCenter で管理される ESX サーバや、ESX サーバの関連する仮想マシン、または Cisco Unified Communications（UC）アプリケーションが検出されます。ESX サーバのモデルには、デバイスが C シリーズであるか、または B シリーズであるかが表示されます。

2. **Cisco Prime Collaboration リリース 11.1 以前の場合**

   （オプション）vCenter で構成されない ESX ホストを個別に検出します。[デバイスの追加（Add Device）]（**[インベントリ管理（Inventory Management）]** > **[デバイスの追加（Add Device）]**）または [インポート（Import）] 機能（**[インベントリ管理（Inventory Management）]** > **[インポート（Import）]**）を使用できますが、論理検索を実行して ESX と VM/UC アプリケーション間の関連付けを取得する必要があります。

   Cisco Prime Collaboration リリース 11.5 以降の場合

   （オプション）vCenter で構成されない ESX ホストを個別に検出します。[デバイスの追加（Add Device）]（**[インベントリ管理（Inventory Management）]** > **[デバイスの追加（Add Device）]**）または [インポート（Import）] 機能（**[インベントリ管理（Inventory Management）]** > **[インポート（Import）]**）を使用できますが、論理検索を実行して ESX と VM/UC アプリケーション間の関連付けを取得する必要があります。

3. （オプション）展開内で UCS Manager を使用している場合は、次のように論理検出を実行します。

   - クラスタ シナリオでは、Cisco UCS Manager の仮想 IP アドレスをシード IP アドレスとして使用します。
   - スタンドアロン シナリオでは、ファブリック インターコネクト デバイスの IP アドレスをシード IP アドレスとして使用します。

   これにより UCS シャーシが検出されます。さらに、管理対象 ESX Server を UCS シャーシに関連付けます。UCS Manager の論理検出によってブレードが検出されない場合は、ブレードを個別に検出する必要があります。UCS ホストの検出後に、UCS manager の論理検出を実行してシャーシとブレードの関連付けを構築します。

（注） UCS シャーシの [インベントリ管理（Inventory Management）] には、IP アドレスの代わりに UCS Manager 名と UCS シャーシ名の組み合わせが表示されます。これは、UCS シャーシには IP アドレスがないためです。

検出が成功すると、インフラストラクチャ グループの下にある [デバイス グループ セレクタ（Device Group Selector）] ペイン内のデバイスまたはアプリケーションに関連付けられている Cisco UCS に関連するグループを表示できます。

UCS-B シリーズ ブレード サーバ グループでは、すべての管理対象 Cisco UCS シャーシと、各シャーシの下の管理対象ブレードが一覧表示されます。シャーシの一覧をクリックすると、右側のペインに特定のシャーシの管理対象ブレードのすべての詳細を表示し、シャーシの下のデバイス セレクタ内の管理対象ブレードの IP アドレスを表示できます。管理下のブレード IP アドレスをクリックすると、そのブレードに

関連付けられている管理対象の仮想マシンである Cisco Unified Communications（UC）アプリケーションのリストが右側のペインに表示されます。

UCS-C シリーズのラック サーバ グループでは、すべての管理対象 ESX サーバがノードとして表示されます。ESX サーバの IP アドレスをクリックすると、ESX サーバ 上で実行中のすべての管理対象仮想マシンまたは Cisco Unified Communications（UC）アプリケーションを右側のペインに表示できます。

vCenter の構成

vCenter で SNMP、トリガー、およびアラームを設定するには、次の手順を実行します。

ステップ 1　vCenter の SNMP の設定

a) vSphere を使用して vCenter にログインし、次のページに移動します。 **[管理（Administration）] > [vCenter Serverの設定（vCenter Server Settings）]**
b) SNMP の設定を構成するには、ページの左側にある [SNMP（SNMP）] メニューを選択します。

ステップ 2　vCenter でのトリガーとアラームの設定

a) 仮想マシンを選択して、次のページに移動します。 **[アラーム（Alarms）] > [定義（Definition）]**。
b) vCenter 名をクリックし、アラームを選択して設定項目を設定します。
c) [トリガー（Triggers）] タブに移動し、次のリンクの「「VMware vCenter Server のアラームのトリガー」」セクションの説明に従ってトリガーを選択します。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

d) [Alert（Alert）]「」 の状態を選択し、[OK（OK）] をクリックします。
e) [アクション（Actions）] をクリックし、「異常なし -> 警告」、「警告 - > エラー」、「エラー -> 警告」、「警告 -> 異常なし」 のすべてのケースで [繰り返し（Repeat）] を選択します。
f) [OK] をクリックします。

Unified CM クラスタ データの検出

Unified CM パブリッシャが Cisco Prime Collaboration Assurance で管理されるように設定したら、クラスタ データ検出を実行して、追加のインベントリ データを収集する必要があります。この検出は、次の情報を収集するために役立ちます。

- Redundancy group、Devicepool、Location、Region、RouteList、RouteGroup、RoutePattern、Partition などを含むクラスタ設定データこれには、電話、ボイスメール エンドポイント、メディア リソース、ゲートウェイ、およびトランクなどのクラスタでプロビジョニングされたエンティティが含まれます。

- Unified CM クラスタに登録されているすべてのエンティティに関する登録情報。これには、デバイス IP、登録ステータス、エンティティが現在登録されている Unified CM サーバ、最新の登録または登録解除のタイムスタンプ、およびステータス理由が含まれます。

  登録情報はコンフィギュレーションファイルを使用して設定できます。この情報は、電話機やゲートウェイなどのエンティティが登録されているクラスタ内のすべてのサブスクライバ ノードから収集されます。

Cisco Prime Collaboration Assurance は、起動時および 1 日に 1 回、Cisco Unified CM からクラスタ設定を収集します。この定期的な検出データ収集は、デフォルトで毎日午前 0 時に実行されます。このデフォルトのスケジュールは変更することができます。

（注）

- 検出されるのは Unified CM に登録されているエンドポイントだけです。Cisco VCS に登録されているエンドポイントは個別に検出されます。
- SIP デバイスは検出されません。
- Cisco Prime Collaboration Assurance は、混合モードの Cisco Unified CM クラスタをサポートしています。CUCM 混合モードについては、Cisco Unified Communications Manager のメンテナンスとオペレーション ガイドを参照してください。
- Cisco Prime Collaboration Assurance 用に設定された CUCM 混合モードでは、Standard CTI Secure Connection アクセス コントロール グループまたはロールを JTAPI アプリケーション ユーザに関連付けないでください。

クラスタ デバイスの検出をスケジュール

始める前に

Unified CM クラスタ検出を実行する前に、次の条件を満たしている必要があります。

- データは、パブリッシャまたは最初のノードから AXL を介して収集されます。そのため、Publisher は適切な HTTP クレデンシャルが入力されている完全な監視状態にあり、AXL Web Service はこの Publisher で実行されている必要があります。
- Unified CM の バージョン 7.x で動作する Cisco RIS Data Collector。
- Cisco SOAP：Unified CM の他のバージョンで動作している CDRonDemand サービス。
- Unified CM Publisher が [Unified CM] セクションまたは Unified CM Administration の [システム サーバ（System Server）] セクションの名前を使用して構成されている場合、この名前は Cisco Prime Collaboration Assurance サーバから DNS を使用して解決可能である必要があります。そうでない場合は、データ収集が続行されるように、この名前のエントリをホストファイル内で設定する必要があります。
- Unified CM で必要な syslogs とプロセスの設定を Cisco Prime Collaboration Assurance で受信可能にするには、[syslog レシーバ（Syslog Receiver）] のセクションの手順を実行する必要

があります。登録情報の変更は、Cisco Unified CM から関連する syslogs を処理することによって更新されます。

Syslog 処理では、Cisco Unified CM クラスタに登録されたエンティティの次のような変更を検出できます。

- 電話、ボイスメールエンドポイント、ゲートウェイなどのエンティティの登録情報の変更。
- クラスタ内でプロビジョニングされる新しい電話が検出され、インベントリが更新されます。

他のデバイスでも、デバイスからの Syslog の設定が必要な場合があります。必要なデバイスの設定の詳細については、次のリンクにある「syslog レシーバの設定」セクションを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ スケジュール（Inventory Schedule）]** > **[クラスタ データ検出のスケジュール（Cluster Data Discovery Schedule）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ スケジュール（Inventory Schedule）]** > **[クラスタ データ検出スケジュール（Cluster Data Discovery Schedule）]**。

Cisco Prime Collaboration リリース 12.1 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**。

ステップ 2 [適用（Apply）] をクリックして後日の検出のスケジュールを設定するか、または [今すぐ実行（Run Now）] をクリックしてクラスタの検出を即座に実行します。

スケジュールされた定期的なデータ収集の前に以下の変更がクラスタ設定で発生していて、これらの変更をすぐに Cisco Prime Collaboration Assurance に反映させる必要がある場合は、[今すぐ実行（Run Now）] オプションを使用して、次のタイプのデータを収集する必要があり ます。

- クラスタ内で追加、削除、または変更された新しいデバイス プール、Location、Region、Redundancy Group、Route List、Route Group、Route Pattern、または Partition。
- デバイス プールへの任意のエンドポイントのメンバーシップの変更、または任意のエンドポイントの冗長グループへの関連付けの変更。
- Unified CM クラスタに追加された、または Unified CM クラスタから削除された新しいサブスクライバ。
- 冗長グループに対する任意のサブスクライバのメンバーシップでの変更。

- ルート グループへの任意のゲートウェイのメンバーシップ、またはルート リストへのルート グループのメンバーシップの変更。

変更が特定のクラスタに制限されている場合は、次の手順でクラスタのパブリッシャを再検出することができます。**[デバイスインベントリ（Device Inventory）]**>**[インベントリ管理（Inventory Management）]**>**[再検出（Rediscover）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

変更が特定のクラスタに制限されている場合は、次の手順でクラスタのパブリッシャを再検出することができます。**[デバイスインベントリ（Device Inventory）]**>**[インベントリ管理（Inventory Management）]**>**[再検出（Rediscover）]**。

新しい Unified CM クラスタの場合、検出または再検出の後、そのクラスタの電話機検出が実行されます。他の電話機同期の処理（クラスタの電話機検出、XML の検出など）が進行中の場合、クラスタベースの電話機検出は処理が完了するまで待機します。したがって、他の電話機同期の処理が進行中のときは、Cisco Prime Collaboration Assurance の電話機の状態変更が反映されるまで予想外に時間がかかります。

関連トピック

Cisco Prime Collaboration Assurance のデバイス設定

デバイスの再検出

すでに検出されたデバイスを再検出できます。すでに入力されているクレデンシャルは、Cisco Prime Collaboration Assurance データベースですでに使用可能になっており、変更によってシステムが更新されます。どの状態のデバイスでも再検出できます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

（注） 再検出の際には必ず、Cisco Prime Collaboration Assurance は、登録解除と再登録を行う必要があります。

再検出を実行するのは、次のときです。

- デバイスを最初に追加してから再検出する必要があります。
- ファースト ホップ ルータ設定に変更があり、ソフトウェア イメージを更新するため。
- クレデンシャル、ロケーション、タイムゾーン、IP アドレスやホスト名、SIP URI、H.323 ゲートキーパーのアドレスなどのデバイスの設定が変更されたとき。
- Cisco Prime Collaboration Assurance のバックアップや復元を実行した後。

[現在のインベントリ（Current Inventory）] ペインの [再検出（Rediscover）] ボタンを使用して、[現在のインベントリ（Current Inventory）] テーブルに表示されているデバイスを再検出します。再検出は、単一のデバイスだけでなく、複数のデバイスに対しても実行できます。

[インベントリ管理（Inventory Management）] で以前に管理された IP アドレスを使用して、到達不能になったデバイス（ルータ、スイッチ、または音声ゲートウェイ）の再検出を実行すると、デバイスは、いずれかのインターフェイスの IP アドレスで再検出されます。この動作を変更するには、*emsam.properties* ファイルの *com.cisco.nm.emms.discovery.ip.swap* プロパティの値を**false**に設定します。この場合、デバイス（ルータ、スイッチ、または音声ゲートウェイ）は、インターフェイスの IP アドレスによって再度検出されることはありません。 ここでは、以前に管理された IP アドレスを使用してデバイスを再検出します（[操作（Operate）] > [デバイス ワーク センター（Device Work Center）]）。

Cisco Prime Collaboration リリース 11.1 以前の場合

選択 **[インベントリ管理（Inventory Management）]** を選択して、以前に管理された IP アドレスでデバイスを再検出します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[インベントリ管理（Inventory Management）]** を選択して、以前に管理された IP アドレスでデバイスを再検出します。

（注） アクセシビリティ情報は、再検出中にはチェックされません。

再検出のワークフローは、検出の場合と同じです。詳細については、「ライフ サイクルの検出」を参照してください。

検出ステータスの確認

すべての検出ジョブのステータスが [ジョブ管理（Job Management）] ページに表示されます。検出を実行すると、[ジョブ進行状況の詳細（Job Progress Details）] リンクを含むダイアログボックスが表示され、検出ステータスを確認できるようになります。検出ジョブの完了までの時間は、ネットワークによって異なります。検出が完了すると、詳細が [現在のインベントリ（Current Inventory）] テーブルに表示されます。

検出ステータスを確認するには、以下を行います。

ステップ 1 Choose を選択します。**[Device Inventory（デバイスインベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[Inventory（インベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]**。

ステップ 2 [ジョブ管理（Job Management）] ページで、詳細を表示する検出ジョブを選択します。

検出のステータス、および検出中に検出されたすべてのデバイスが [Job Management] テーブルの下のペインに表示されます。

ステップ 3 [ジョブ管理（Job Management）] テーブルで検出ステータスを確認するか、[ジョブの詳細（Job details）] ペインで検出されたデバイスの詳細を確認します。

ステップ 4 結果に応じて、次のいずれかを実行します。

- 誤ったクレデンシャルが原因で検出されなかったデバイスについては、それらのデバイスのクレデンシャルを確認し、検出を再実行します。
- 同じデバイスを複数回検出するには、Rediscover オプションを使用します。詳細については、「デバイスの再検出」を参照してください。

トラブルシューティング

1. **問題**：Cisco TelePresence Video Communication Server（Cisco VCS）Edgeで、外部インターフェイスの IP アドレスにアクセスできず、アラームが発生する。

   推奨処置：Cisco Unified Communications Manager を検出する前に、Cisco VCS Core および Cisco VCS Edge を検出する必要があります。これにより、Cisco VCS - Edge の外部インターフェイスと内部インターフェイスのすべての IP アドレスが、Cisco Prime Collaboration Assurance インベントリで認識されるようになります。Cisco Unified Communications Manager のパブリッシャが検出されると、インターフェイス IP アドレスは、収集されたインベントリと照合されるため、アクセスできないというアラームが発生しません。

2. **問題**：Cisco TelePresence Management Suite（TMS）に関連付けられたデバイスが検出されない。

   推奨処置：関連付けられたデバイスを検出するように、Cisco TelePresence Management Suite（TMS）の論理検出を実行したことを確認します。[デバイスの追加（Add Device）] オプションは、TMS のみを検出し、関連付けられたデバイスを検出しません。

   [論理検出の有効化（Enable Logical discovery）] オプションを選択して、TMS を再検出します。関連付けられたすべてのデバイスに対して、クレデンシャルが追加されていることを確認します。

3. **問題**：Cisco TelePresence のタッチ パネルで、コーデック エンドポイントに直接接続せずに syslog イベントを送信できない。

   推奨処置：Cisco TelePresence のタッチ パネルがコーデックに接続されていて、そのコーデックが Cisco Prime Collaboration Assurance で再検出されることを確認します。

4. **問題**：DX80 や電話機が正常に検出されない。

   推奨処置：DX80 およびその他の電話機は、電話機の同期、CDT、または Cisco Unified Communications Manager のパブリッシャ クラスタ検出の一部としてのみ検出されます。登録や登録解除のステータスとは別に、電話機の任意の設定変更は、クラスタ データ検出の後にのみ、Cisco Prime Collaboration Assurance のインベントリに反映されます。

DX IP アドレスを追加することによって、DX80 デバイスを個別に検出しないでください。

5. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが正常に検出されない。

   推奨処置：CiscoDX80/DX70 デバイスが Cisco Unified Communications Manager に存在することを確認してください。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

6. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが正常に検出され、そのデバイスがアクセス不能な状態になっている。

   推奨処置：CiscoDX80/DX70 デバイスのクレデンシャルプロファイルを追加し、さらに、Cisco Prime Collaboration Assurance が Device360 ビューの ping オプションで、デバイスに ping を実行できることを確認します。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

7. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが、サポートされていない状態になっている。

   推奨処置：Ensure Cisco Prime Collaboration Assurance が 11.6 よりも上位のバージョンであることを確認してください。バージョン 11.6 未満の場合は、CE イメージを含む CiscoDX80/DX70 デバイスはサポートされません。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

8. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが [会議診断（Conference Diagnostics）] ページに表示されない。

   推奨処置：これらの電話機が登録されている管理対象 Unified CM に対して、適切な JTAPI クレデンシャルが追加されていることを確認してください。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

9. **問題**：電話機のシリアル番号が見つからない。

   推奨処置：電話機の [デバイス360度ビュー（Device 360° View）] に、シリアル番号が表示されます。デバイス上で**[インベントリ（Inventory）]**>**[インベントリ管理（Inventory Management）]**をクリックして、電話機の IP アドレス上のアイコンをクリックして、[デバイス 360° 表示（Device 360° View）] を起動します。

10. **問題**：Cisco Unified Communications Manager が非 Cisco デバイスとして表示される。

    推奨アクション：Cisco Unified Communications Manager の Cisco Unified Communications Manager SNMP サービスを有効にします。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

    - Cisco Prime Collaboration Assurance のデバイス設定
    - Cisco Prime Collaboration Assurance のデバイス設定

11. **問題**：Cisco Prime Collaboration Assurance のインベントリで、エンドポイント名がすぐに更新されない。

    推奨処置：次のことを確認してください。

    - クラスタに属するエンドポイントのエンドポイント名が更新されるのは、クラスタデータ検出を実行した後のみです。
    - エンドポイントの説明を変更した後、Cisco Unified Communications Manager でエンドポイントをリセットします。エンドポイント名は syslog 通知によって、Cisco Prime Collaboration Assurance ですぐに更新されます。syslog が Cisco Prime Collaboration Assurance で設定されているか確認してください。

12. **問題**：Cisco SocialMiner デバイスにカウンタが読み込まれず、カスタム ダッシュボードに「**使用可能なデータがありません**」と表示される。

    推奨処置：次の条件が満たされていることを確認します。

    - Cisco SocialMiner デバイスが稼働中であり、[インベントリの管理（Inventory Management）] ページに [Managed（Managed）] の状態で表示されることを確認します。
    - ブラウザで次の URL を入力して、サービスが実行されていることを確認します。

      ```
      http://<ServerIP>:8080/sm-dp/rest/DiagnosticPortal/GetPerformanceInformation
      ```

13. **問題**：CCisco Finesse デバイスにカウンタが読み込まれず、カスタム ダッシュボードに「**使用可能なデータがありません**」と表示される。

    推奨処置：次の条件が満たされていることを確認します。

    - Cisco Finesse デバイスが稼働中であり、[インベントリの管理（Inventory Management）] ページに [管理対象（Managed）] の状態で表示されることを確認します。
    - ブラウザで次の URL を入力して、サービスが実行されていることを確認します。

      ```
      https://<server>/finesse-dp/rest/DiagnosticPortal/GetPerformanceInformation
      ```