



ネットワークの検出

- [検出の概要 \(1 ページ\)](#)
- [検出ダッシュボード \(2 ページ\)](#)
- [ディスカバリの前提条件 \(2 ページ\)](#)
- [ディスカバリ クレデンシャル \(3 ページ\)](#)
- [優先管理 IP アドレス \(10 ページ\)](#)
- [設定のガイドラインと制限事項のディスカバリ \(11 ページ\)](#)
- [ディスカバリの実行 \(12 ページ\)](#)
- [ディスカバリ ジョブの管理 \(19 ページ\)](#)

検出の概要

ディスカバリ機能は、ネットワーク内のデバイスをスキャンし、検出されたデバイスの一覧をインベントリに送信します。

また、ディスカバリ機能は、デバイスの可制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（これらの設定がデバイスにまだ存在しない場合）。

デバイスは次の 4 つの方法で検出できます。

- Cisco Discovery Protocol (CDP) を使用し、シード IP アドレスを指定します。
- IP アドレスの範囲を指定します（最大 4096 デバイスの範囲がサポートされます）。
- Link Layer Discovery Protocol (LLDP) を使用し、シード IP アドレスを指定します。
- Classless Inter-Domain Routing (CIDR) を使用し、シード IP アドレスを指定します。

ディスカバリ基準を設定する際は、ネットワーク検出時間を短縮するために役立つ設定があることに注意してください。

- [CDP Level] と [LLDP Level] : CDP または LLDP をディスカバリ方式として使用する場合は、CDP レベルまたは LLDP レベルを設定して、スキャンするシードデバイスからのホップ数を指定できます。デフォルトのレベル 16 では、大規模なネットワークの場合に時間がかかる可能性があります。そのため、検出する必要があるデバイスが少ない場合は、このレベルをより低い値に設定できます。

- [Prefix Length] : 検出方法として CIDR を使用する場合は、プレフィックス長の値を 20 ～ 30 の範囲で設定できます。デフォルト値は 30 です。
- [Subnet Filters] : IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP] : CDP、LLDP、CIDR、または IP アドレスの範囲のいずれを使用する場合でも、Catalyst Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。



- (注) Cisco SD-Access ファブリックおよび Cisco Catalyst アシユアランスについては、デバイスのループバックアドレスを指定することをお勧めします。

どの方式を使用する場合でも、Catalyst Center からデバイスにアクセスできる必要があります。デバイスを検出するための特定のクレデンシャルとプロトコルを Catalyst Center で設定する必要があります。これらのログイン情報は、**[Design]>[Network Settings]>[Device Credentials]** ウィンドウで（または**[Discovery]** ウィンドウでジョブごとに）設定して保存することができます。



- (注) デバイスが Hot Standby Router Protocol (HSRP) や Virtual Router Redundancy Protocol (VRRP) などのファーストホップ解決プロトコルを使用する場合、そのデバイスは、そのフローティング IP アドレスによって検出され、インベントリに追加される可能性があります。その後、HSRP または VRRP に障害が発生すると、その IP アドレスが別のデバイスに割り当てなおされる場合があります。この場合、Catalyst Center が分析のために取得するデータによって問題が発生する可能性があります。

検出ダッシュボード

左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]>[Discovery]**の順に選択して、**[Discovery Dashboard]**を表示します。**[Discovery Dashboard]**には、インベントリの概要、最新のディスカバリ、ディスカバリタイプ、ディスカバリステータス、最近のディスカバリが表示されます。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- Catalyst Center によって検出されるデバイスの情報については、[Cisco Catalyst Center Compatibility Matrix](#)を参照してください。

- Catalyst Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間 (RTT) であることに注意してください (最大遅延は 200 ミリ秒 RTT です)。
- Catalyst Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。詳細については、[ディスカバリ クレデンシャル \(3 ページ\)](#) を参照してください。
- Catalyst Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Catalyst Center はデバイスを検出し、そのインベントリに追加します。
 - デバイスへの SSH アクセスのために Catalyst Center が使用するアカウントが、特権 EXEC モード (レベル 15) である。
 - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、[設定のガイドラインと制限事項のディスカバリ \(11 ページ\)](#) を参照してください。

ディスカバリ クレデンシャル

ディスカバリ クレデンシャルは、検出するデバイスに関する CLI、SNMPv2c、SNMPv3、HTTP (HTTPS)、および NETCONF 設定値です。検出を試みるデバイスの種類に基づいてクレデンシャルを指定する必要があります。

- ネットワークデバイス : CLI と SNMP のクレデンシャル。



(注) 組み込みワイヤレスコントローラなどの NETCONF 対応デバイスについては、管理者権限で SSH クレデンシャルを指定し、NETCONF ポートを選択する必要があります。

- コンピューティングデバイス (NFVIS) : CLI、SNMP、および HTTP (S) のクレデンシャル。

ネットワーク内のさまざまなデバイスが異なるクレデンシャルセットを持つことが可能であるため、Catalyst Center で複数のクレデンシャルセットを設定できます。ディスカバリプロセスでは、デバイスに使用できるクレデンシャルセットが見つかるまで、ディスカバリジョブ用に設定されているすべてのセットで反復処理されます。

ネットワーク内の大半のデバイスに同じクレデンシャル値を使用する場合は、それらを設定して保存し、複数のディスカバリジョブで再利用できます。固有のクレデンシャルを使用するデバイスを検出するために、ディスカバリジョブの実行時にジョブ固有のディスカバリクレデンシャルを追加できます。クレデンシャルタイプごとに最大 10 のグローバルクレデンシャルを設定し、そのうちの 5 つを定義できます。ジョブ固有のログイン情報を定義する必要がある

場合は、ログイン情報の種類ごとに5つのグローバルログイン情報と1つのジョブ固有のログイン情報を定義できます。

ディスカバリ クレデンシャルを定義するには、メニューアイコンをクリックして選択[Tools]>[Discovery]>[Add Discovery]の順にクリックします。続行するには、次の手順とディスカバリ クレデンシャルを使用します。

- [CDP を使用したネットワークの検出 \(12 ページ\)](#)
- [IP アドレス範囲または CIDR を使用したネットワークの検出 \(15 ページ\)](#)
- [LLDP を使用したネットワークの検出 \(17 ページ\)](#)

表 1: CLI クレデンシャル

フィールド	説明
Name/Description	CLI クレデンシャルを説明する名前または語句。 CLI の認証が失敗した場合、Catalyst Center は、認証プロセスを 300 秒 (5 分) 間再試行します。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

表 2: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [Name/Description] : 追加している SNMPv2c 設定の名前または説明。 • [Read Community] : デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Write	<ul style="list-style-type: none"> • [Name/Description] : 追加している SNMPv2c 設定の名前または説明。 • [Write Community] : デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

表 3: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • [Authentication and Privacy] : 認証と暗号化の両方を行います。 • [Authentication, No Privacy] : 認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy] : 認証も暗号化も行いません。
Auth. Type	使用する認証タイプ ([Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5 (not recommended)] : HMAC-MD5 に基づく認証。
Auth.Password]	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード (またはパスフレーズ) は、8 文字以上にする必要があります。 <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコ ワイヤレス コントローラでは、パスワード (あるいはパスフレーズ) は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Catalyst Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Privacy Type	<p>プライバシータイプ。 ([Mode] として [Authentication and Privacy] を選択した場合に有効になります)。 次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> • [AES128] : 暗号化の 128 ビット CBC モード AES。 • CISCOAES192 : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • CISCOAES256 : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。
プライバシーパスワード (Privacy Password)	<p>暗号化の標準規格をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。 パスワード (またはパスフレーズ) は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコワイヤレスコントローラでは、パスワード (あるいはパスフレーズ) は少なくとも 12 文字以上である必要があります。 ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。 パスワードに必要な最低限の文字数が守られないと、デバイスでは Catalyst Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

表 4: SNMP のプロパティ

フィールド	説明
Retries	Catalyst Center が SNMP を使用してネットワークデバイスとの通信を試行する回数。
[Timeout (in Seconds)]	再試行の時間間隔 (秒単位)。

表 5: HTTPS クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。 有効なタイプは、[Read] または [Write] です。

フィールド	説明
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none">• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。• [Username] : HTTPS 接続の認証に使用される名前です。• [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。• [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none">• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。• [Username] : HTTPS 接続の認証に使用される名前です。• [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。• [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。

表 6: NETCONF 設定

フィールド	説明
Port	<p>デバイスのポート。次のいずれかのポートを使用できます。</p> <ul style="list-style-type: none"> • ポート 830 (デフォルト) • デバイスで使用可能なその他のポート • Catalyst Center で構成するカスタムポート。(デバイス可制御性が有効になっている場合にのみ、カスタムポートを使用できます詳細については、Cisco Catalyst Center Administrator Guide の「Device Controllability」の項を参照してください) <p>NETCONF の認証に失敗した場合、Catalyst Center は認証プロセスを 300 秒 (5 分) 間再試行します。</p> <p>検出によって、複数のログイン情報を受け入れて検証し、有効なログイン情報を持つデバイスのみをインベントリに追加します。そのため、検出プロセス中に NETCONF 接続障害が発生した場合、Catalyst Center は NETCONF ポートなしでデバイスを追加します。ただし、(NETCONF が有効になっていない) デバイスを NETCONF ログイン情報を使用してインベントリに手動で追加した場合、NETCONF ポートで RPC 要求への応答がない場合、Catalyst Center には「Managed: Netconf Connection Failure」というエラーが表示されます。どちらの場合も、デバイスが NETCONF ポートなしで追加され、アプリケーションが NETCONF のみを使用してデータを収集する場合は、Catalyst Center には NETCONF ポートが見つからないというエラーが表示されます。NETCONF が設定されていないときに、アプリケーションが CLI ログイン情報を使用する場合、Catalyst Center には管理対象状態のデバイスが表示されます。これは、このデバイスが CLI ログイン情報を使用しているためです。</p>

ディスカバリログイン情報と Cisco ISE

Cisco ISE を認証サーバーとして使用する場合、ディスカバリ機能では、Cisco ISE をディスカバリプロセスの一部として使用してデバイスが認証されます。デバイスが正しく検出されるように、次の注意事項に従ってください。

- 英数字4文字未満のディスカバリ クレデンシャルを使用しないでください。デバイスは英数字4文字未満のクレデンシャルを持つことができますが、Cisco ISE で許容される最短のユーザー名とパスワードは英数字4文字です。デバイス クレデンシャルが4文字未満の場合、Catalyst Center はデバイスのインベントリ データを収集できず、デバイスは不完全な収集状態になります。
- 同じユーザー名を持つが、異なるパスワードをもつクレデンシャルを使用しないでください (cisco/cisco123 と cisco/pw123)。Catalyst Center ではユーザー名が同じでありながらパスワードの異なるデバイスのディスカバリが可能ですが、Cisco ISE では許容されません。重

複したユーザー名が使用されている場合、Catalyst Center はデバイスを認証してインベントリ データを収集することができず、デバイスは不完全な収集状態になります。

Cisco ISE を AAA サーバーとして定義する方法については、[Cisco ISE またはその他の AAA サーバーの追加](#)を参照してください。

ディスカバリ クレデンシャルのガイドラインと制約事項

Catalyst Center のディスカバリ クレデンシャルに関するガイドラインと制約事項は、次のとおりです。

- ディスカバリ ジョブで使用されるデバイス クレデンシャルを変更するには、ディスカバリ ジョブを編集し、使用しなくなったクレデンシャルの選択を解除する必要があります。その後、新しいクレデンシャルを追加してディスカバリを開始する必要があります。詳細については、「[ディスカバリ ジョブでクレデンシャルを変更 \(19 ページ\)](#)」を参照してください。
- デバイスが正常に検出された後にデバイスのクレデンシャルを変更すると、そのデバイスのその後のポーリングサイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
 - ディスカバリ ツールを使用します：
 - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
 - 既存のディスカバリ ジョブを編集し、ディスカバリを再実行します。
 - 設計ツールを使用します：
 - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
 - 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリ ジョブを再作成します。または、新しいディスカバリジョブを作成します。
- デバイス認証に失敗するために進行中のディスカバリ ポーリング サイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
 - ディスカバリ ツールを使用します：
 - 現在のディスカバリジョブを停止または削除し、デバイスのクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリジョブを実行します。
 - 現在のディスカバリ ジョブを停止または削除し、既存のディスカバリ ジョブを編集して、ディスカバリを再実行します。
 - 設計ツールを使用します：

- 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
- 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリ ジョブを再作成します。または、新しいディスカバリジョブを作成します。
- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。以前に検出されたデバイスのステータスは、認証の失敗を示しません。ただし、削除されたクレデンシャルの使用を試みる次のディスカバリは失敗します。ディスカバリは、いずれかのデバイスへの接続を試みる前に失敗します。

ディスカバリ クレデンシャルの例

一般的なネットワークを構成するデバイスのディスカバリ要件は、非常に多岐にわたる場合があります。Catalyst Center では、これらの多様な要件をサポートするために、複数の検出ジョブを作成できます。たとえば、200 台のデバイスで構成されるネットワークが Cisco Discovery Protocol (CDP) ネイバーを形成しているとします。このネットワークでは、190 台のデバイスはグローバルクレデンシャル (クレデンシャル0) を共有しており、残りのデバイスは独自のクレデンシャル (クレデンシャル1 ~ クレデンシャル10) を持っています。

FIPS モードの展開の場合、ディスカバリパスワードは必ず 8 文字以上とします。

このネットワーク内のすべてのデバイスを検出するために、Catalyst Center は次のタスクを実行します。

-
- ステップ1 クレデンシャル0としてCLIグローバルクレデンシャルを設定します。
 - ステップ2 SNMP (v2c または v3) グローバルクレデンシャルを設定します。
 - ステップ3 190 台のデバイスの IP アドレス (グローバルクレデンシャルを共有する 190 台のデバイス) の1つとグローバルクレデンシャル0を使用してディスカバリ ジョブを実行します。
 - ステップ4 該当するジョブ固有のログイン情報 (ログイン情報1、ログイン情報2、ログイン情報3など) を使用して、残りの10台のデバイスごとに10個の別個のディスカバリジョブを実行します。
 - ステップ5 [Inventory] ウィンドウで結果を確認します。
-

優先管理 IP アドレス

Catalyst Center でデバイスが検出されると、デバイスの IP アドレスの1つが優先管理 IP アドレスとして使用されます。IP アドレスは、デバイスの組み込み管理インターフェイス、または別の物理インターフェイス、または Loopback0 のような論理インターフェイスの IP アドレスにすることができます。デバイスのループバック IP アドレスを優先管理 IP アドレスとして使用するために Catalyst Center を設定できます (その IP アドレスが Catalyst Center から到達可能である場合)。

優先管理 IP アドレスとして [Use Loopback IP] を選択した場合、Catalyst Center では次のように優先管理 IP アドレスが指定されます。

- デバイスに1つのループバック インターフェイスがある場合、Catalyst Center は、そのループバック インターフェイスの IP アドレスを使用します。
- デバイスに複数のループバック インターフェイスがある場合、Catalyst Center は、最上位の IP アドレスを持つループバック インターフェイスを使用します。
- ループバック インターフェイスがない場合、Catalyst Center は、最上位の IP アドレスを持つイーサネット インターフェイスを使用します（サブインターフェイスの IP アドレスは考慮されません）。
- イーサネット インターフェイスがない場合、Catalyst Center は、最上位の IP アドレスを持つシリアル インターフェイスを使用します

デバイスが検出された後に、**[Inventory]** ウィンドウから管理 IP アドレスを更新できます。詳細については、[デバイスの管理 IP アドレスの更新](#)を参照してください。

設定のガイドラインと制限事項のディスカバリ

Catalyst Center による Cisco Catalyst 3000 シリーズ スイッチおよび Catalyst 6000 シリーズ スイッチの検出に関する注意事項と制約事項は、次のとおりです。

- CLI ユーザー名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これらのログイン情報は、ディスカバリ機能に関して Catalyst Center で設定する CLI ユーザー名およびパスワードと同じです。Catalyst Center にはデバイスへの最高レベルのアクセス権が必要です。
- 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポート プロトコルを明示的に指定してください。この設定には、**transport input** と **transport output** コマンドを使用してください。これらのコマンドについては、各デバイス タイプ用のコマンドリファレンス ドキュメントを参照してください。
- デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA (TACACS) ログインで設定されている場合は、Catalyst Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。
- シスコ ワイヤレス コントローラは、サービスポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のウィンドウでは、データが表示されません。

ディスカバリの実行

Link Layer Discovery Protocol (LLDP)、CDP、または IP アドレス範囲を使用してデバイスを検出できます。

[ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

- IP アドレス範囲の検出の場合、検出されたデバイスのリストには、ping 到達可能なデバイスのみが含まれます。Ping 到達不能デバイスは無視され、検出されたデバイスのリストには含まれません。
- CDP および LLDP ベースの検出の場合、CDP および LLDP プロトコルは ping 到達不能 IP にも応答するため、ping 到達不能デバイスは検出されたデバイスのリストに含まれます。
- CDP および LLDP ベースの検出の場合、クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。)
- ディスカバリ機能では、正しい SNMP 読み取り専用コミュニティストリングが必要です。SNMP 読み取り専用コミュニティストリングが指定されていない場合、ベストエフォートとして、ディスカバリ機能はデフォルトの SNMP 読み取り専用コミュニティストリングである public を使用します。
- 検出のとき、すでに検出されてサイトに関連付けられているデバイスのサイトの割り当てはスキップされます。
- CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。
- SNMPv3 ログイン情報を使用した検出中に、Catalyst Center は、デフォルトの SNMP ユーザーグループを使用して SNMPv3 ログイン情報をデバイスにプッシュし、デバイス上の既存のユーザーグループは無視します。

CDP を使用したネットワークの検出

Cisco Discovery Protocol (CDP)、IP アドレス範囲、CIDR または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリメソッドの詳細については、[IP アドレス範囲または CIDR を使用したネットワークの検出 \(15 ページ\)](#) および [LLDP を使用したネットワークの検出 \(17 ページ\)](#) を参照してください。



- (注)
- ディスカバリ機能では、正しい SNMP 読み取り専用 (RO) コミュニティストリングが必要です。SNMP RO コミュニティストリングが指定されていない場合、ベストエフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティストリングを公的に使用します。
 - CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで CDP を有効にします。
- [ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します : [Tools] > [Discovery]。


ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Let's Get Ready] ウィンドウで、[Next] をクリックします。

ステップ 4 [Discover Devices] ウィンドウで、次のフィールドに入力します。

- a) 検出ジョブの名前を入力します。
- b) [Discovery Type] で、[CDP] を選択します。
- c) [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Catalyst Center でディスカバリ スキャンを開始します。
- d) (任意) [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス ($x.x.x.x$) または Classless Inter-Domain Routing (CIDR) アドレス ($x.x.x.x/y$) としてアドレスを入力できます。ここで $x.x.x.x$ は IP アドレスを示し、 y はサブネットマスクを示します。サブネットマスクは、0 ~ 32 の値です。

- e)  をクリックします。

手順 d および e を繰り返して、ディスカバリジョブから複数のサブネットを除外します。

- f) (任意) [CDP レベル (CDP Level)] フィールドに、スキャンするシードデバイスからのホップ数を入力します。

有効値は 1 ~ 16 です。デフォルト値は 16 です。たとえば、CDP レベル 3 は、CDP がシードデバイスから最大 3 つのホップまでスキャンすることを意味します。

- g) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None] : デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP] : デバイスのループバックインターフェイスの IP アドレスを指定します。
 - (注) [ループバック IP を使用 (Use Loopback IP)] の使用を選択し、デバイスにループバックインターフェイスがない場合、Catalyst Center は **優先管理 IP アドレス (10 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。
 - (注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスが Catalyst Center から到達可能であることを確認します。

ステップ 5 [Provide Credentials] ウィンドウで、少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、**ディスカバリ クレデンシャル (3 ページ)** を参照してください。

ステップ 6 [Advanced Settings] ウィンドウで、次の手順を実行します。

- a) [Protocol Order] : [SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。
- b) [SNMP Polling Properties] を構成します。[Network Settings] > [Device Credentials] ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

ステップ 7 [Assign Devices to Site] ウィンドウで、次のいずれかを実行します。

- [Assign devices to an existing site] : [Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。
- [Assign devices to a new site] : [Already have an area] オプションボタンまたは [Create a new area] ラジオボタンをクリックし、必須フィールドに入力します。
- [Skip site assignment for now] : 後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 8 [Schedule Job] ウィンドウで、次の手順を実行します。

- a) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。
- b) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [Start Discovery] をクリックします。

[Activities] > [Tasks] ウィンドウでタスクのステータスを確認できます。

IP アドレス範囲または CIDR を使用したネットワークの検出

IP アドレス範囲、CIDR、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲または CIDR を使用してデバイスとホストを検出する方法を示します。その他の検出方法の詳細については、「[CDP を使用したネットワークの検出 \(12 ページ\)](#)」および「[LLDP を使用したネットワークの検出 \(17 ページ\)](#)」を参照してください。

始める前に


[ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools] > [Discovery]**。

ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Let's Get Ready] ウィンドウで、[Next] をクリックします。

ステップ 4 [Discover Devices] ウィンドウで、次のフィールドに入力します。

- a) 検出ジョブの名前を入力します。
- b) [Discovery Type] で、[IP Address/Range] または [CIDR] を選択します。
- c) [IP Address/Range] 検出タイプを選択した場合は、次の手順を実行します。
 1. [From] フィールドと [To] フィールドに、スキャンする Catalyst Center の最初の IP アドレスと最後の IP アドレス (IP アドレス範囲) を入力し、 をクリックします。


検出スキャンに対して、単一の IP アドレス範囲または複数の IP アドレスを入力できます。

(注) Cisco ワイヤレス コントローラは、サービスポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレスコントローラ 360 および AP 360 のページでは、データが表示されません。

2. (オプション) 前のステップを繰り返して、追加の IP アドレス範囲を入力します。
- d) [CIDR] 検出タイプを選択した場合は、次の手順を実行します。
 1. [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Catalyst Center でディスカバリ スキャンを開始します。

2. [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス ($x.x.x.x$) または Classless Inter-Domain Routing (CIDR) アドレス ($x.x.x.x/y$) としてアドレスを入力できます。ここで $x.x.x.x$ は IP アドレスを示し、 y はサブネットマスクを示します。サブネットマスクは、0 ~ 32 の値です。

3.  をクリックします。

(オプション) 前のステップを繰り返して、検出ジョブから複数のサブネットを除外します。

4. [Prefix Length] フィールドに、プレフィックス長の値を入力します。有効な値の範囲は 20 ～ 30 です。

e) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None] : デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP] : デバイスのループバックインターフェイスの IP アドレスを指定します。

(注) [ループバック IP を使用 (Use Loopback IP)] の使用を選択し、デバイスにループバックインターフェイスがない場合、Catalyst Center は **優先管理 IP アドレス (10 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。

ステップ 5 [Provide Credentials] ウィンドウで、少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、**ディスカバリ クレデンシャル (3 ページ)** を参照してください。

ステップ 6 [Advanced Settings] ウィンドウで、次の手順を実行します。

- a) [Protocol Order] : [SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。
- b) [SNMP Polling Properties] を構成します。[Network Settings] > [Device Credentials] ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

ステップ 7 [Assign Devices to Site] ウィンドウで、次のいずれかを実行します。

- [Assign devices to an existing site] : [Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。
- [Assign devices to a new site] : [Already have an area] オプションボタンまたは [Create a new area] ラジオボタンをクリックし、必須フィールドに入力します。
- [Skip site assignment for now] : 後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 8 [Schedule Job] ウィンドウで、次の手順を実行します。

- a) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。
- b) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [Start Discovery] をクリックします。

[Activities] > [Tasks] ウィンドウでタスクのステータスを確認できます。

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol (LLDP)、CDP、CIDR、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[CDP を使用したネットワークの検出 \(12 ページ\)](#) および [IP アドレス範囲または CIDR を使用したネットワークの検出 \(15 ページ\)](#) を参照してください。



- (注)
- ディスカバリ機能では、正しい SNMP 読み取り専用 (RO) コミュニティストリングが必要です。SNMPRO コミュニティストリングが指定されていない場合、ベストエフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティストリングを公的に使用します。
 - CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで LLDP を有効にします。
- [ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します: **[Tools] > [Discovery]**。


ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Let's Get Ready] ウィンドウで、[Next] をクリックします。

ステップ 4 [Discover Devices] ウィンドウで、次のフィールドに入力します。

- a) 検出ジョブの名前を入力します。
- b) [Discovery Type] で、[LLDP] を選択します。
- c) [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Catalyst Center でディスカバリ スキャンを開始します。
- d) (任意) [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス ($x.x.x.x$) または Classless Inter-Domain Routing (CIDR) アドレス ($x.x.x.x/y$) としてアドレスを入力できます。ここで $x.x.x.x$ は IP アドレスを示し、 y はサブネットマスクを示します。サブネットマスクは、0 ~ 32 の値です。

- e)  をクリックします。

手順 c および d を繰り返して、ディスカバリ ジョブから複数のサブネットを除外します。

- f) (任意) [LLDP レベル (LLDP Level)] フィールドで、スキャンするシードデバイスからのホップ数を入力します。
- 有効値は 1 ~ 16 です。デフォルト値は 16 です。たとえば、LLDP レベル 3 は、LLDP がシードデバイスから最大 3 つのホップをスキャンすることを意味します。
- g) [Preferred Management IP] で、次のいずれかのオプションを選択します。
- [None] : デバイスはすべての IP アドレスを使用できます。
 - [Use Loopback IP] : デバイスのループバックインターフェイスの IP アドレスを指定します。
 - (注) このオプションを選択し、デバイスにループバック インターフェイスがない場合、Catalyst Center は **優先管理 IP アドレス (10 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。
 - (注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスが Catalyst Center から到達可能であることを確認します。

ステップ 5 [Provide Credentials] ウィンドウで、少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、**ディスカバリ クレデンシャル (3 ページ)** を参照してください。

ステップ 6 [Advanced Settings] ウィンドウで、次の手順を実行します。

a) [Protocol Order] : [SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。

b) [SNMP Polling Properties] を構成します。[Network Settings] > [Device Credentials] ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

ステップ 7 [Assign Devices to Site] ウィンドウで、次のいずれかを実行します。

- [Assign devices to an existing site] : [Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。
- [Assign devices to a new site] : [Already have an area] オプションボタンまたは [Create a new area] ラジオボタンをクリックし、必須フィールドに入力します。
- [Skip site assignment for now] : 後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 8 [Schedule Job] ウィンドウで、次の手順を実行します。

a) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。

b) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [Start Discovery] をクリックします。


[Activities] > [Tasks] ウィンドウでタスクのステータスを確認できます。


ディスカバリ ジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

ディスカバリ ジョブの停止および開始

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Tools] > [Discovery]。

ステップ 2 アクティブなディスカバリジョブを停止するには、[Actions] 列の省略記号アイコン () にカーソルを合わせ、[Stop Discovery] を選択します。

ステップ 3 非アクティブなディスカバリジョブを再開するには、[Actions] 列の省略記号アイコン () にカーソルを合わせ、[Re-discover] を選択します。


ディスカバリ ジョブでクレデンシヤルを変更

ディスカバリ ジョブで使用されるクレデンシヤルを変更し、そのジョブを再実行できます。

始める前に

少なくとも 1 つのディスカバリ ジョブが必要です。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Tools] > [Discovery]。

ステップ 2 ディスカバリジョブをコピーするには、[Actions] 列の省略記号アイコン () の上にカーソルを置き、[Copy & Edit] を選択します。

Catalyst Center では、「Clone of *Discovery_Job*」という名前でディスカバリジョブのコピーが作成されます。

ステップ 3 (任意) ディスカバリジョブの名前を変更するには、[Discovery Name] フィールドのデフォルト名を新しい名前に置き換えます。

ステップ 4 [New Discovery] ウィンドウで、[Credentials] エリアを展開し、すでに作成されているグローバルログイン情報のいずれかを選択するか独自に構成します。

既存のクレデンシャルを使用する場合は、それらを選択してください。そのクレデンシャルを使用しない場合は、選択解除します。

ステップ 5 独自のクレデンシャルを構成するには、[Add Credentials] をクリックします。

CLI および SNMPv2c ログイン情報を設定する必要があります。その他のクレデンシャルはオプションです。フィールド情報については、「[ディスカバリ クレデンシャル \(3 ページ\)](#)」[英語] を参照してください。

現在のジョブのクレデンシャルのみを保存するには、[Save] をクリックします。現在のジョブと将来のジョブのクレデンシャルを保存するには、[Save as global settings] チェックボックスをオンにして、[Save] をクリックします。

ステップ 6 [Discover] をクリックします。


ディスカバリ ジョブの複製

ディスカバリジョブを複製し、そのジョブ用に定義されているすべての情報を保持できます。

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Tools] > [Discovery]。

ステップ 2 ディスカバリジョブをコピーするには、[Actions] 列の省略記号アイコン () の上にカーソルを置き、[Copy & Edit] を選択します。

Catalyst Center では、「Clone of *Discovery_Job*」という名前でディスカバリジョブのコピーが作成されます。


ステップ 3 (任意) ディスカバリジョブの名前を変更するには、[Discovery Name] フィールドのデフォルト名を新しい名前に置き換えます。

ステップ 4 新しいディスカバリ ジョブのパラメータを定義または更新します。

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Tools] > [Discovery]。

ステップ 2 ディスカバリジョブを削除するには、[Actions] 列の省略記号アイコン () の上にカーソルを置き、[Delete] を選択します。

ステップ 3 [OK] をクリックして確定します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。