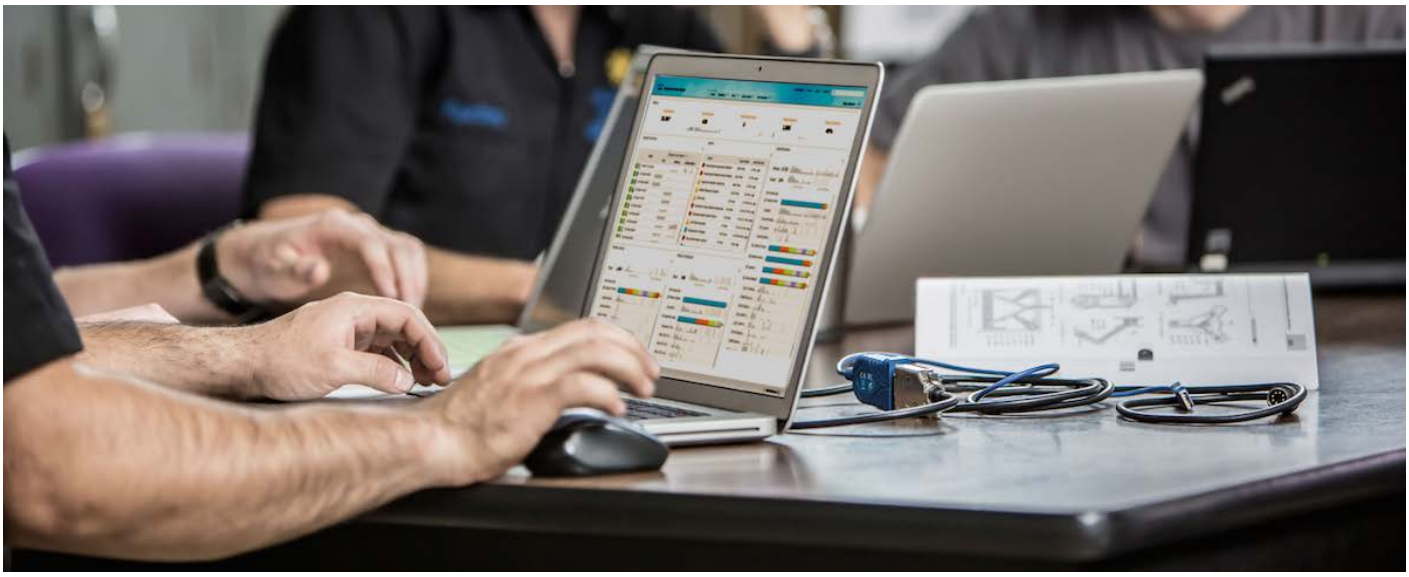


# Cisco ISE プロファイリング設計ガイド

*セキュア アクセスを実現するハウツー ガイド シリーズ*

**著者：Craig Hyps**

**日付：2012 年 8 月**

# 目次

## ソリューションの概要

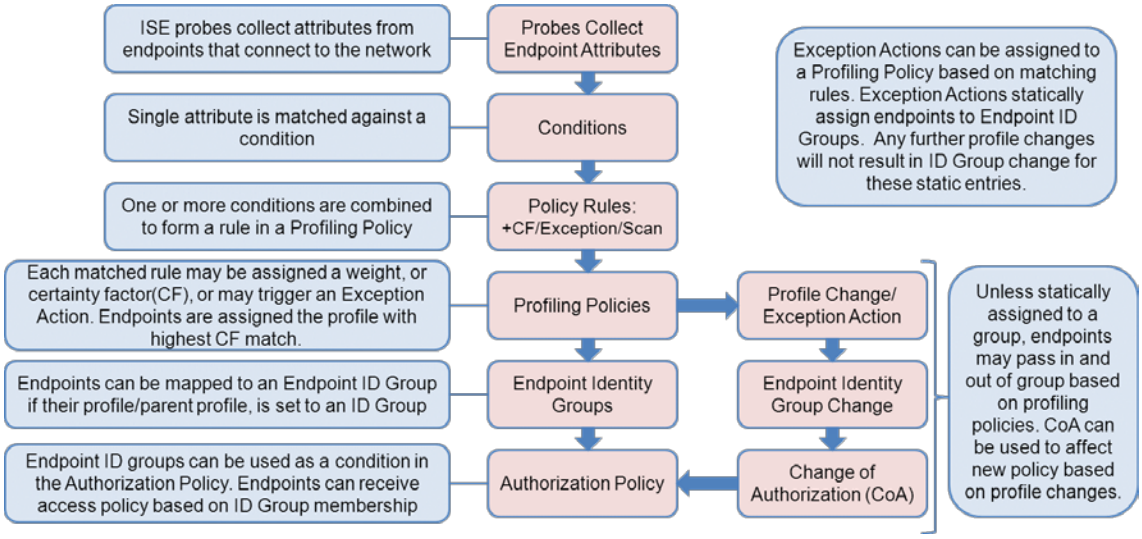
Cisco ISE プロファイリング サービスは、ネットワークに接続されたエンドポイントの動的な検出と分類を可能にします。ISE は、MAC アドレスを一意の識別子として使用し、ネットワーク エンドポイントごとにさまざまな属性を収集して、内部エンドポイント データベースを構築します。分類プロセスは、収集された属性と事前に定義された条件またはユーザ定義の条件を照合してから、拡張可能なプロファイル ライブラリに関連付けます。これらのプロファイルは、モバイル クライアント(iPad、Android タブレット、Blackberry フォンなど)、デスクトップ オペレーティング システム(Windows 7、Mac OS X、Linux など)、およびプリンタ、電話機、カメラ、ゲーム コンソールなどのさまざまな非ユーザ システムを含む広範囲のデバイス タイプに及びます。

分類されたエンドポイントは、そのプロファイルに基づいて、ネットワークに対して認可され、アクセス権が付与されます。たとえば、IP フォン プロファイルと一致したエンドポイントは、認証方式として MAC 認証バイパス(MAB)を使用する音声 VLAN に配置できます。また、使用するデバイスによって異なるネットワーク アクセス権をユーザに付与することもできます。たとえば、従業員は、会社のワークステーションからネットワークにアクセスするときはフル アクセス権を取得できますが、個人の iPhone からネットワークにアクセスするときは制限付きのネットワーク アクセス権しか付与されないようにすることができます。

## ポリシー アーキテクチャとコンポーネント

図 3 に、Cisco ISE プロファイリング サービスの一般的なポリシー アーキテクチャとキー コンポーネントを示します。設定プロセスは、ポリシー サービス ペルソナを実行している ISE アプライアンス上で特定のプローブを有効化することから始まります。さまざまなタイプのエンドポイント属性の収集に対応した、さまざまなプローブが用意されています。これらの属性は条件と照合されてから、デバイス タイプのライブラリ内のルール、つまり、プロファイルと照合可能になります。汎用の比重基準に基づいて、照合する条件ごとに異なるウェイト、つまり特定のプロファイルへのデバイスの分類に条件がどの程度貢献しているかを相対値として表す確信度係数(CF)を割り当てることができます。条件が複数のプロファイルに一致する場合もありますが、エンドポイントの累積 CF が最も高いプロファイルがエンドポイントに割り当てられます。

**図 1.** ISE プロファイリング ポリシー アーキテクチャとコンポーネント




プロファイルを ISE 認可ポリシーに提供するには、管理者が、シンプルなチェックボックスを使用して照合する ID グループを作成して、プロファイルを設定する必要があります。このシンプルなプロセスによって、プロファイルを認可ポリシーの条件としてエンドポイント ID グループの形式で選択することができます。

プロファイルは、新しい属性が学習された場合や以前に学習された属性が上書きされた場合に変更される可能性があります。また、プロファイリング ポリシーの変更の結果として変更される可能性もあります。こうした変更は、汎用 HP デバイスからより具体的なプロファイル（HP-Color-LaserJet-4500 など）へのように自動的に行われる場合もあれば、管理者が例外アクションの形で、デフォルト ポリシーをバイパスするための意図的なアクションを作成する場合もあります。例外アクションを使用すれば、エンドポイントを特定のプロファイリング ポリシーへ静的に割り当てて、その後の属性収集または関連付けが、割り当てられるプロファイルやオプションの ID グループに影響を及ぼさないようにすることが可能です。

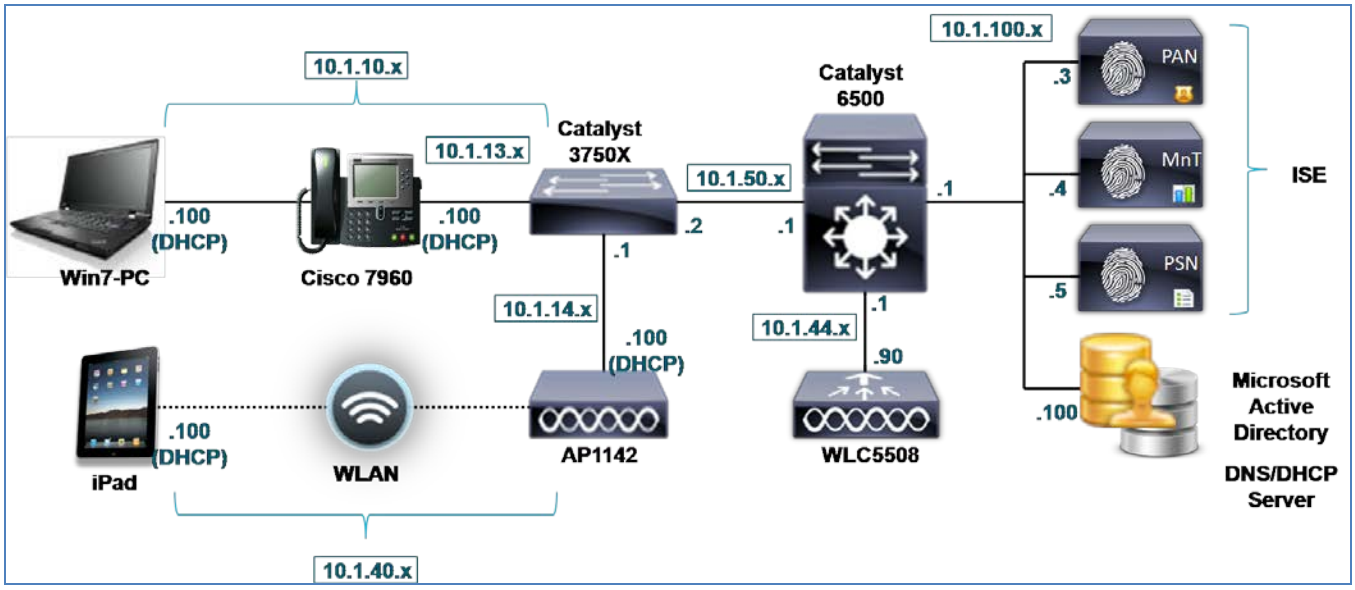
上記のそれぞれの場合（プロファイル変更と例外アクション）において、ISE で、新しいプロファイル割り当てに基づいてエンドポイントに新しいアクセス ポリシーを適用できるようにすることをお勧めします。RADIUS 認可変更（CoA）は、ISE でこのタスクを実現するための機能です。CoA 要求をエンドポイントが接続されたアクセス デバイスに送信することによって、ISE は認証および認可ポリシーに照らしたホストの再評価を要求することができます。

# シナリオの概要

## ネットワーク トポロジ

図 4 に、このガイドで使用されるハイレベルのネットワークトポロジを示します。図 1 に描かれているすべてのシナリオが TrustSec アーキテクチャの一部を構成していますが、このドキュメントでは、プロファイリングに関する有線ユーザ シナリオと無線ユーザ シナリオを中心に説明します。ISE プロファイリング サービスは、現在、プロファリング データを一意のエンドポイントに関連付けるために必要な VPN ゲートウェイからの MAC アドレス情報が不足しているリモート アクセス VPN ユース ケースではサポートされません。

**図 2.** ISE プロファイリング トポロジ




## コンポーネント

表 1 に、このガイドの執筆時に使用されたハードウェアおよびソフトウェア コンポーネントのリストを示します。

**表 1.** Cisco TrustSec 2.0 システムのテスト済みコンポーネント

| コンポーネント | ハードウェア | テスト対象機能 | ソフトウェア リリース |
|---|---|---|---|
| Cisco Identity Services Engine（ISE） | VMware ESXi4.1 を実行している Cisco UCS C200 M2 サーバ | 統合 AAA、ポリシー サーバ、およびプロファイリング サービス | Cisco ISE ソフトウェア バージョン 1.1.1（基本および詳細機能ライセンス） |
| Cisco Catalyst 3000 シリーズ スイッチ | Cisco Catalyst 3560 シリーズ | MAC 認証バイパス（MAB）、Local WebAuth（LWA）、Central WebAuth（CWA）、802.1X 認証、および認可変更（CoA）を含む基本 ID 機能。<br><br>Simple Network Management Protocol（SNMP）、RADIUS、Dynamic Host Configuration Protocol DHCP リレー、および URL リダイレクションを含むプロファイリング サポート サービス。 | Cisco IOS® ソフトウェア リリース 12.2(55)SE3（IP Base） |

| コンポーネント | ハードウェア | テスト対象機能 | ソフトウェア リリース |
|---|---|---|---|
| | Cisco Catalyst 3750-X シリーズ | MAB、LWA、CWA、802.1X 認証、および CoA を含む基本 ID 機能。<br><br>SNMP、RADIUS、DHCP リレー、URL リダイレクション、およびデバイス センサーを含むプロファイリング サポート サービス。 | Cisco IOS ソフトウェア リリース 15.0(1)SE2（IP Base） |
| Cisco Catalyst 6000 シリーズ スイッチ | Cisco Catalyst 6500 シリーズ スーパバイザ エンジン 720 ポリシー フィーチャ カード 3A（PFC3A） | Cisco NetFlow バージョン 5 およびバージョン 9 エクスポート、DHCP リレー、および Switched Port Analyzer/Remote Switched Port Analyzer（SPAN/RSPAN）を含むプロファイリング サポート サービス。 | Cisco IOS ソフトウェア リリース 12.2(33)SXJ2（高度 IP サービス） |
| Cisco Wireless LAN Controller（WLC） | Cisco 5508 Wireless LAN Controller | MAB、LWA、CWA、802.1X 認証、および CoA を含む基本 ID 機能。<br><br>SNMP、RADIUS、DHCP リレー、および URL リダイレクションを含むプロファイリング サポート サービス。 | Cisco Unified Wireless Network ソフトウェア リリース 7.2.103.0 |
| Cisco ワイヤレス アクセス ポイント | Cisco Aironet® Lightweight アクセス ポイント 1142N | MAB とプロファイル属性に基づく認可ポリシーを使用して認証されたエンドポイント | Cisco Lightweight アクセス ポイント ソフトウェア リリース 12.4(25e)JA |
| Cisco IP Phone | Cisco Unified IP Phone 7960 | MAB とプロファイル属性に基づく認可ポリシーを使用して認証されたエンドポイント | Cisco IP Phone 7940 および 7960 ファームウェア リリース 8.1(1.0) |

| コンポーネント | ハードウェア | テスト対象機能 | ソフトウェア リリース |
|---|---|---|---|
| ワークステーション | VMware Guest | MAB、LWA、CWA、および 802.1X とプロファイル属性に基づく認可ポリシーを使用して認証されたエンドポイント | Windows 7 |
| タブレット | Apple iPad（G1） | MAB、LWA、CWA、および 802.1X とプロファイル属性に基づく認可ポリシーを使用して認証されたエンドポイント | iOS 5.0.1 |
| スマートフォン | Motorola DROIDX | MAB、LWA、CWA、および 802.1X とプロファイル属性に基づく認可ポリシーを使用して認証されたエンドポイント | Android 2.3.4 |

注：Cisco ISE プロファイリング サービスは、このガイドで検証する主要機能です。他の Cisco TrustSec 機能は、主に、プロファイリング サービスの設定とテストをサポートするために展開されています。

この表に示すデバイスとバージョンは、このガイドのテストと文書化の過程で特別に使用されたものであり、TrustSec と ISE プロファイリング サービスをサポートするすべてのデバイスに対応するわけではありません。TrustSec 対応デバイスと推奨バージョンの包括的なリストについては、http://www.cisco.com/go/trustsec [英語] を参照してください。

# プロファイリング サービスの要件

## ライセンシング

ISE プロファイリングでは、次のライセンスのいずれかがポリシー管理ノード（PAN）にインストールされている必要があります。

高度エンドポイント ライセンス（有線展開またはワイヤレス展開の場合）

ワイヤレス専用ライセンス（ワイヤレス専用展開の場合）

ネットワークに対して能動的に認証され、プロファイリング データに基づいて認可ポリシーが決定されるエンドポイントごとに 1 つの高度エンドポイント ライセンスが必要です。高度エンドポイント ライセンスが必要なポスチャ アセスメントなどの他のサービスを考慮しなければ、プロファイルに静的に割り当てられるエンドポイントには高度ライセンスが必要ありません。エンドポイントの認可にプロファイル情報が使用されない場合は、高度エンドポイント ライセンスがなくても複数のエンドポイントをプロファイリングして、接続されたデバイスとその分類を可視化することができます。高度エンドポイント ライセンスまたはワイヤレス専用ライセンスの最小数は 100 です。

## アプライアンスの要件

ISE プロファイリング サービスは、ポリシー サービス ペルソナ用に設定された ISE アプライアンス上でのみ実行できます。表 2 に、ポリシー サービス専用のアプライアンスでプロファイリング可能なアクティブ エンドポイントの数に関する一般的なガイダンスを示します。VMware ベースのアプライアンスのサイジングは、ハードウェア ベースのアプライアンスの同等の仕様と一致するか、それを超えるかに基づきます。

**表 2.** ISE アプライアンスのサイジング

| ISE アプライアンス | 最大エンドポイント | プロファイルされる EPS（既存のエンドポイントのプロファイリング） | 保存される EPS（新しいエンドポイントのプロファイリング） |
|---|---|---|---|
| ACS1121/NAC3315/ISE3315 | 3000 | 43 | 33 |
| NAC3355/ISE3355 | 6000 | 該当なし | 該当なし |
| NAC3395/ISE3395 | 10,000 | 100 | 5 |
| VMware | 3000/6000/10,000 | VMware の設定に依存 | VMware の設定に依存 |

加えて、各アプライアンスは、1 秒間に処理可能な新しいイベント数（EPS）の制限を受けます。この値は、受け取るプロファイリング データが新しく発見されたエンドポイントのものか、既存のエンドポイントのものかによって異なります。既存のエンドポイントのプロファイリング レートを表 2 の「プロファイルされる EPS」の列に示します。新しく発見されたエンドポイントがデータベースに追加され、プロファイリングされるレートが「保存される EPS」の列に表示されます。

ISE プロファイリング サービスは、複数の ISE アプライアンス間でサービスを分散することによって、拡大縮小できます。プロファイリング サービスを実行している ISE ポリシー サービス ノードは、ロード バランサの背後でポリシー サービスのクラスタ化に使用されるノード グループのメンバーにすることもできます。

## ネットワークの要件

ISE プロファイリング サービスは、さまざまなコレクタ、つまりプローブを使用して、接続されたエンドポイントに関する属性を収集します。これらの属性の一部には、ネットワーク インフラストラクチャ、アクセス デバイス、場合によってエンドポイントによる個別のサポートが必要です。これらの要件については、特定のプローブに関する項でさらに詳しく説明しますが、ネットワークまたはエンドポイントから適切なデータが入手できない場合は、一部のプローブが使用できないということを理解しておくことが重要です。

# プロファイリング サービスのグローバル設定

## ISE プロファイリングのグローバル設定

ここでは、ポリシー サービス ノードで ISE プロファイリング サービスをグローバルに有効にして、グローバル プロファイリング パラメータを設定するプロセスを確認します。

## グローバル プロファイリング設定の構成

### ポリシー管理ノードからのグローバル プロファイリング設定の構成

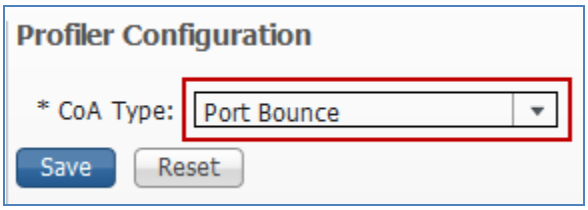
**ステップ 1** サポートされている Web ブラウザと admin クレデンシャル（**https://<ISE_PAN_FQDN_or_IP>**）を使用して、プライマリ ポリシー管理ノード（PAN）の ISE 管理インターフェイスにアクセスします。

**ステップ 2** [管理（Administration）] → [システム（System）] → [設定（Settings）] に移動します。左側（LHS）ペインで、[プロファイリング（Profiling）] を選択します。

**ステップ 3** 右側（RHS）ペインで、プロファイリング移行と例外アクションに使用するデフォルト CoA タイプを選択します（図 5）。

目的が可視性のみの場合は、[CoAなし（No CoA）] のデフォルト値のままにします。そうでない場合は、[ポートバウンス（Port Bounce）] を選択します。これにより、クライアントレス エンドポイントであっても、必要に応じて、IP アドレス更新を含む再認可プロセスを通過することが保証されます。スイッチポートで複数のエンドポイントが検出された場合は、ISE は再認証オプションの使用に戻され、他の接続済みデバイスのサービス中断を回避します。

**図 3. グローバル プロファイリング設定：CoA の設定**



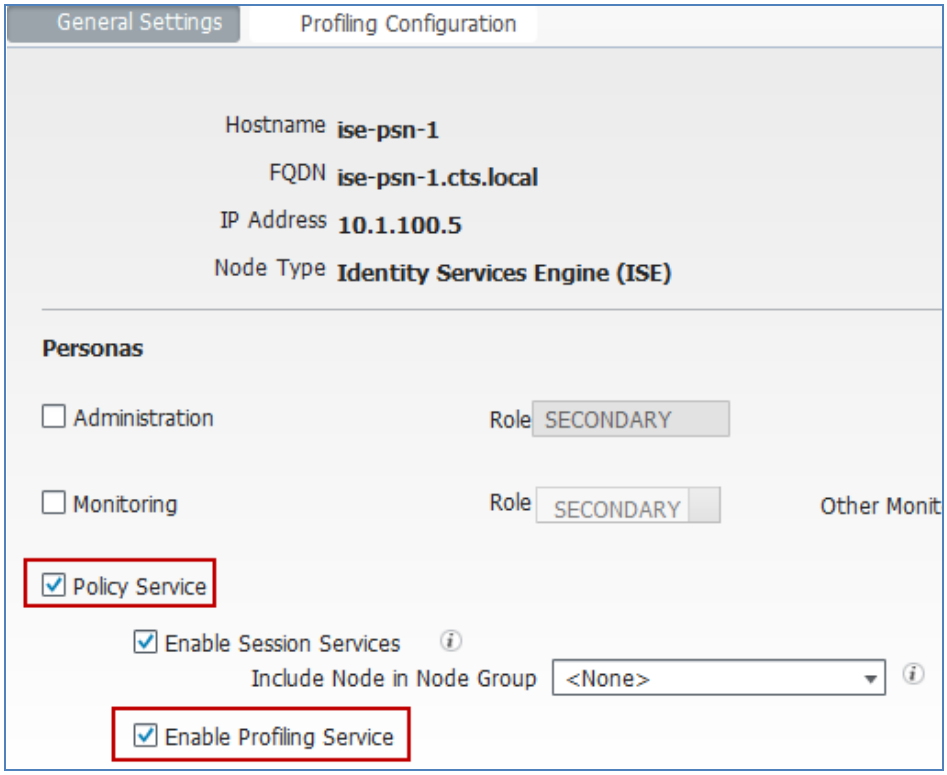

## ISE プロファイリング サービスの有効化

### ポリシー サービス ノードでのプロファイリング サービスの有効化

**ステップ 1** [管理（Administration）]→[システム（System）]→[展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [全般設定（General Settings）] タブで、[ポリシーサービス（Policy Service）] という名前のノード ペルソナがオンになっており、[プロファイリングサービスの有効化（Enable Profiling Service）] もオンになっていることを確認します（図 6）。

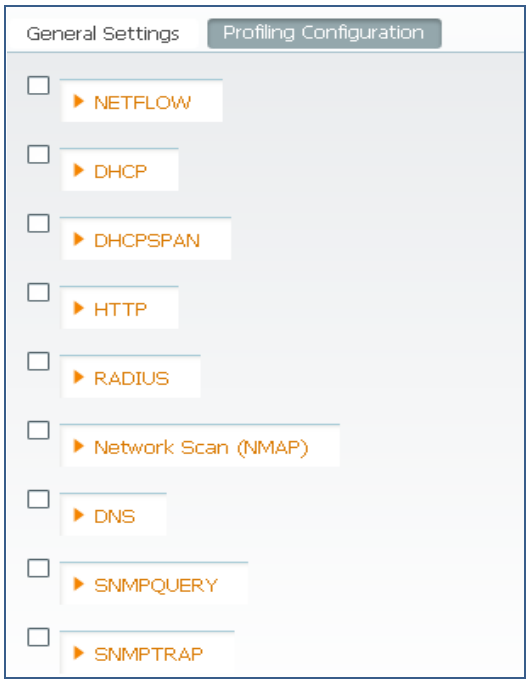
図 1 ポリシー サービス ノードでのプロファイラ サービスの有効化




## プロファイリング設定ページのアクセスと表示

**ステップ 3** [プロファイリング設定（Profiling Configuration）] タブをクリックします。該当するボックスをオンにして、オプションのプローブ パラメータを選択することによって、簡単に有効にして設定できるさまざまなプローブを表示します（図 7）。

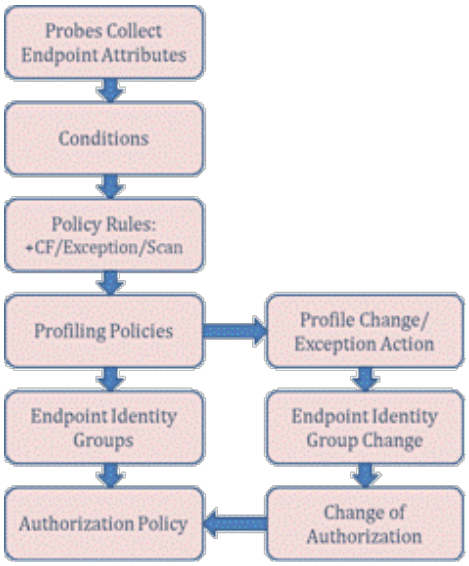
図 2 プローブの設定




**ステップ 4** プロファイリングの設定に変更を加えた場合は、必ず、ページの下部にある [保存（Save）] をクリックして変更をコミットしてください。

# プローブの設定

図 3 設定フロー：プローブと属性収集




## プローブの概要

ISE プローブは、エンドポイント属性を収集する ISE プロファイリング サービスのコンポーネントです。プローブごとに異なる収集方式が使用され、エンドポイントに関する一意の情報を収集できます。その結果として、一部のプローブが、他のプローブよりも特定のデバイス タイプの分類に適していたり、特定の環境に基づいて選択されたりします。

ISE は次のプローブをサポートします。

- RADIUS
- SNMP トラップ（SNMP Trap）
- SNMP クエリ（SNMP Query）
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- ネットワーク スキャン（NMAP）

その名前が示すとおり、DHCP や DHCP SPAN といった一部のプローブは、特定の属性（この例では、DHCP パケット内の DHCP 属性と関連するオプション フィールド）を一意的に収集することができます。DHCP と DHCP SPAN のどちらを選択するかは、特定のネットワーク環境が DHCP トラフィックの ISE ポリシー サービス ノードへの中継をサポートしているかどうかや、スイッチ ポート アナライザ（SPAN）方式を使用した方がネットワークトポロジとインフラストラクチャの機能に適しているかどうかによって異なります。このガイドでは、各プローブに関する個別の項でプローブ選択に関する詳細なガイダンスを提供します。

プローブ タイプによって、有効化が簡単か困難かが異なります。また、使用されているプロトコルやそれらの展開方法によってネットワークやエンドポイントに対する影響のレベルも異なります。プローブごとに、生成する値とネットワーク内での対象となる特定のエンドポイントの分類への適用性が異なります。このガイドでは、各プローブの設定方法と展開方法を確認し、展開のタイプに基づく各プローブの展開の困難さ、ネットワークへの影響、および相対的なプロファイリング値を全面的に理解できるように支援します。

# プローブの設定

ISE プローブは、プロファイリング サービス用に設定された ISE ポリシー サービス ノードで有効になります。ここでは、さまざまなエンドポイント属性を収集するためにさまざまな ISE プローブを有効にする手順を確認します。また、サポートするネットワーク インフラストラクチャの実用的な設定例とともに、インフラストラクチャと ISE 管理インターフェイスの両方から想定される出力を提示します。

## RADIUS プローブを使用したプロファイリング

RADIUS プローブは、RADIUS クライアント(有線アクセス スイッチとワイヤレス コントローラを含む)から RADIUS サーバ(セッション サービスを実行している ISE ポリシー サービス ノード)に送信された RADIUS 属性を収集します。標準の RADIUS ポートには、認証および認可用の UDP/1645 または UDP/1812 と、RADIUS アカウンティング用のポート UDP/1646 および UDP/1813 が含まれます。

注:RADIUS プローブは、RADIUS トラフィックを直接リッスンするのではなく、デフォルト UDP ポート 20514 上のモニタリング ノードに syslog で送信された RADIUS 属性をリッスンして解析します。その後で、キャプチャされた RADIUS プローブ属性がデフォルト UDP ポート 30514 上の内部ロガーに転送されます。

RADIUS プローブは、デバイス センサー機能を使用して RADIUS アカウンティング パケットで送信された Cisco Discovery Protocol(CDP)属性、Link Layer Discovery Protocol(LLDP)属性、および DHCP 属性も収集します。この機能については後述します(「デバイス センサー」の項を参照)。図 9 に、サンプル RADIUS プローブのトポロジを示します。

図 4 RADIUS プローブの例

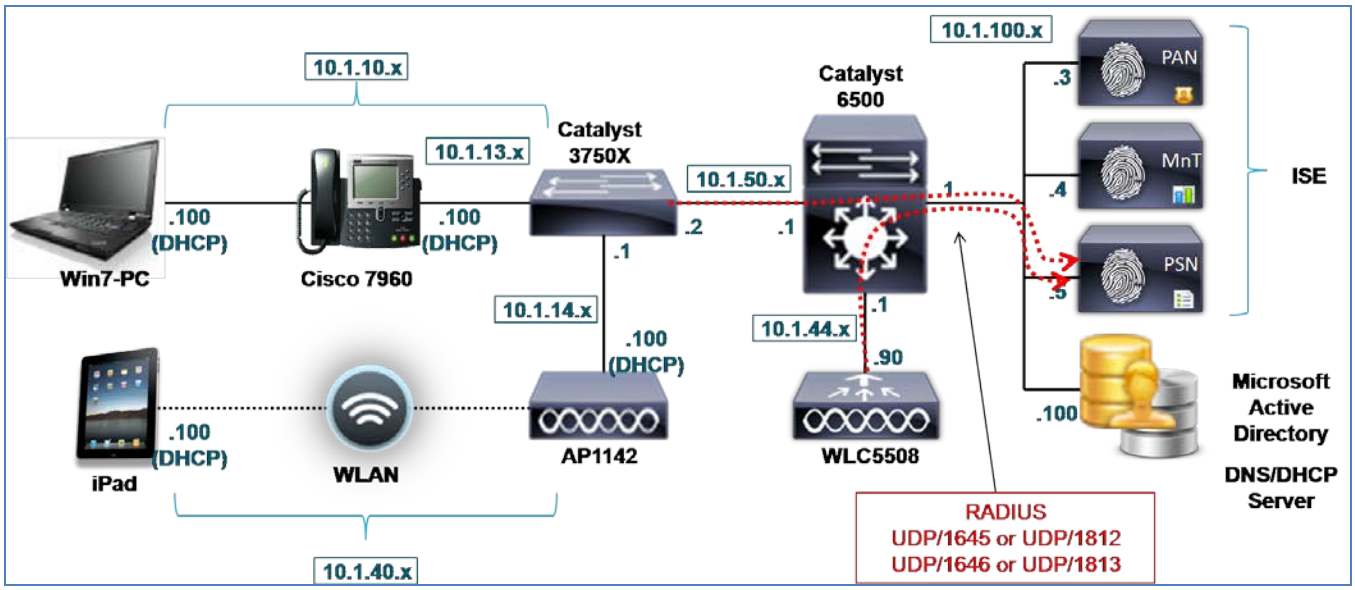



表 3 に、RADIUS プローブを使用して収集される一般的な属性を示します。

表 1 RADIUS 属性の例

| | | | |
|---|---|---|---|
| User-Name | NAS-IP-Address | NAS-Port | Framed-IP-Address |
| Calling-Station-Id | Acct-Session-Id | Acct-Session-Time | Acct-Terminate-Cause |

アクセス デバイスの設定によりますが、一般的に、Calling-Station-ID は接続しているエンドポイントの MAC アドレスです。この属性は、ネットワークに接続して認証するときに MAC アドレスに基づいて一意のエンドポイントをすばやく特定できるという直接的なメリットを提供します。また、MAC アドレスの最初の 3 バイトから抽出された Organizationally Unique Identifier（OUI）に基づくベンダー ネットワーク アダプタに関する情報も提供します。

RADIUS アカウンティング パケット内に存在する Framed-IP-Address は、接続しているエンドポイントの IP アドレスを提供します。この属性と Calling-Station-ID を組み合わせることによって、DNS、HTTP、Cisco NetFlow、NMAP などの IP アドレスに依存している他のプローブのサポートに不可欠な IP/MAC 間バインドを ISE に提供できます。

## RADIUS プローブの設定

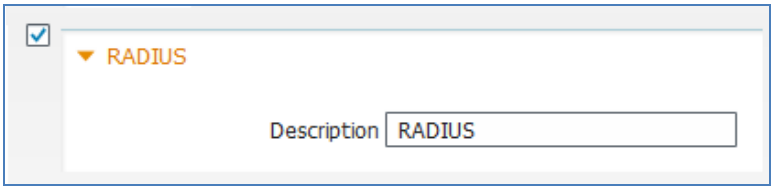
RADIUS プローブは、ネットワーク アクセス デバイスがネットワーク認証および認可のためにセッション サービスを実行している ISE ポリシー サービス ノードに RADIUS パケットを送信するようにすでに設定されているため、有効化と展開が最もシンプルなプローブの 1 つです。

## ISE での RADIUS プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスします。RHS ペインで展開されたノードのリストから、プロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択して、RADIUS プローブを有効にするボックスをオンにします。プローブが、自動的に、RADIUS サービス用に設定されたインターフェイス上で有効になります（図 10）。

図 5 RADIUS プローブの設定




**ステップ 3** [保存（Save）] をクリックして、変更をコミットします。

**ステップ 4** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

## ISE でアクセス デバイスが設定されていることの確認

このガイドでは、ネットワーク アクセス デバイスが、すでに、ISE の [管理（Administration）] → [ネットワークリソース（Network Resources）] → [ネットワークデバイス（Network Devices）] で標準の RADIUS 通信用に設定されていることを前提とします。

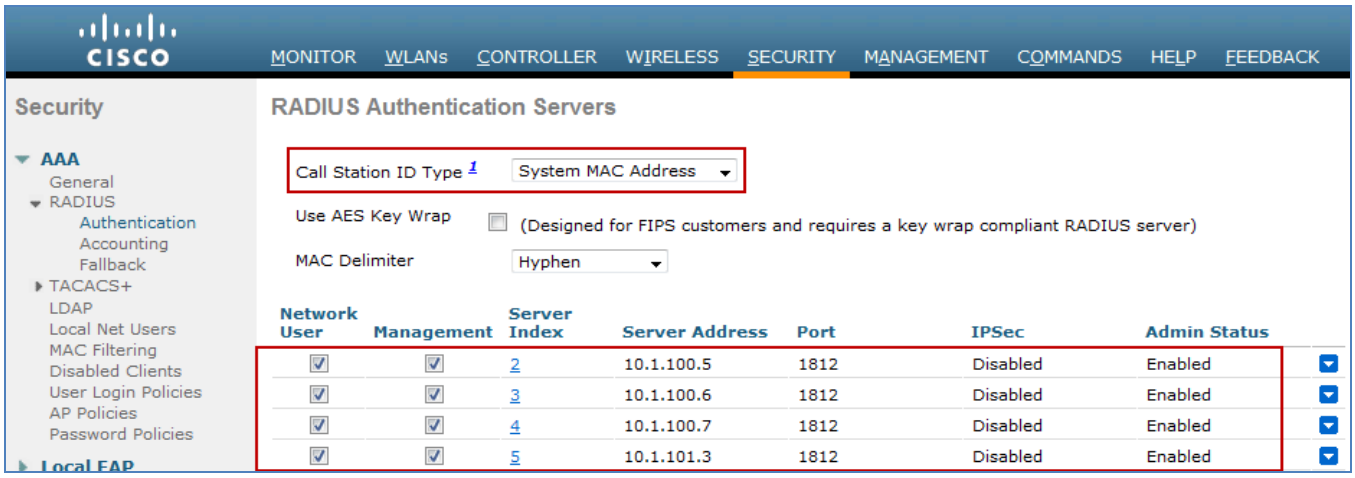
## アクセス デバイスが RADIUS を ISE PSN に送信するように設定されていることの確認

このガイドでは、ネットワーク アクセス デバイスが、すでに、ISE ポリシー サービス ノード（PSN）に対する RADIUS 認証、認可、およびアカウンティング用に設定されていることを前提とします。ここで、有線スイッチ用の RADIUS 設定の例を示します。

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
```

図 11 に、ワイヤレス コントローラ用の RADIUS サーバ設定の例を示します。この設定ページにアクセスするには、WLC Web 管理インターフェイスで [セキュリティ（Security）] → [AAA（AAA）] → [RADIUS（RADIUS）] → [認証（Authentication）] に移動します。

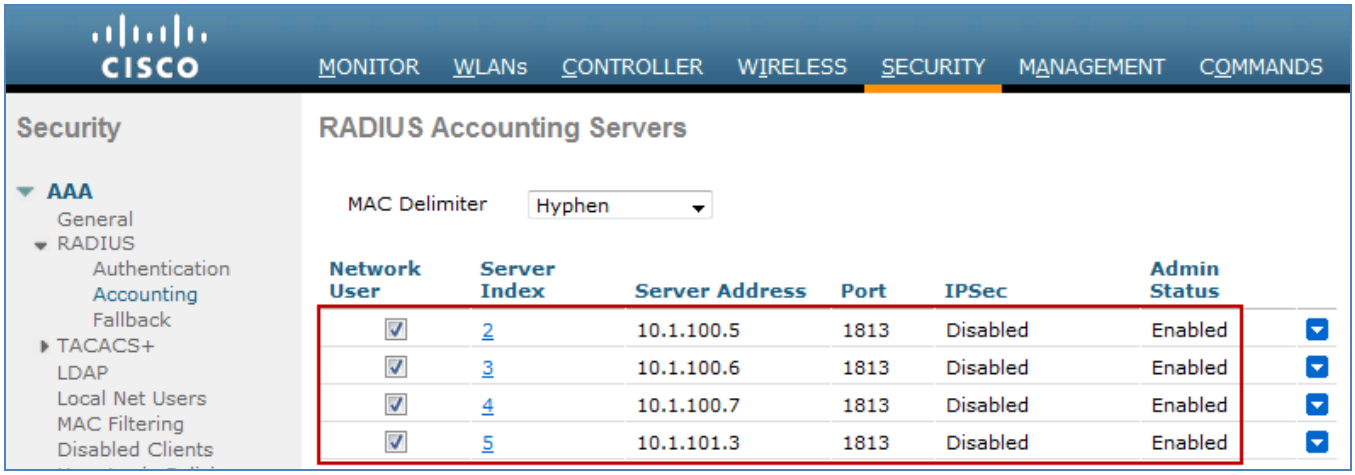
図 6 ワイヤレス コントローラ用のグローバル RADIUS サーバ設定の例




**シスコ ベスト プラクティス**：図 11 に示すように、非 802.1X クライアントのプロファイリングを可能にするために、[コールステーションIDタイプ（Call Station ID Type）] が [システムMACアドレス（System MAC Address）] に設定されていることを確認します。これにより、ISE がエンドポイントをデータベースに追加して、既知の MAC アドレスに基づいて、受信したその他のプロファイル データをそのエンドポイントに関連付けられることが保証されます。

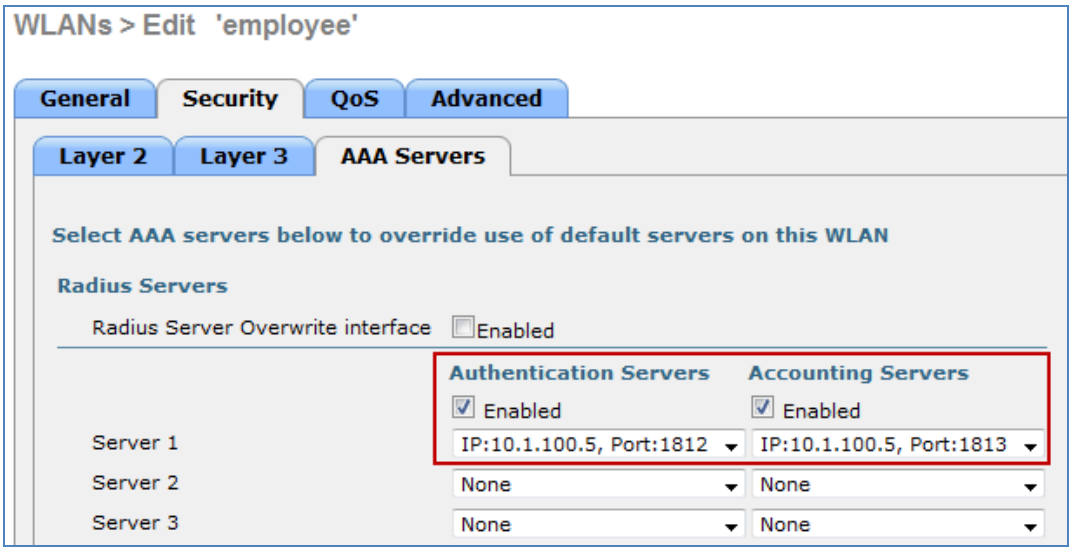
同様のエントリが、ワイヤレス コントローラ用の RADIUS アカウンティング設定にも存在するはずです（図 12）。

図 7 ワイヤレス コントローラ用のグローバル RADIUS アカウンティング設定の例




WLAN ごとに適切な ISE ポリシー サービス ノードを指定するように設定する必要もあります（図 13）。

図 8 ワイヤレス コントローラ用の WLAN RADIUS 設定の例




## RADIUS プローブ データの確認

**ステップ 1** ネットワークに対して新しいエンドポイントを認証します。

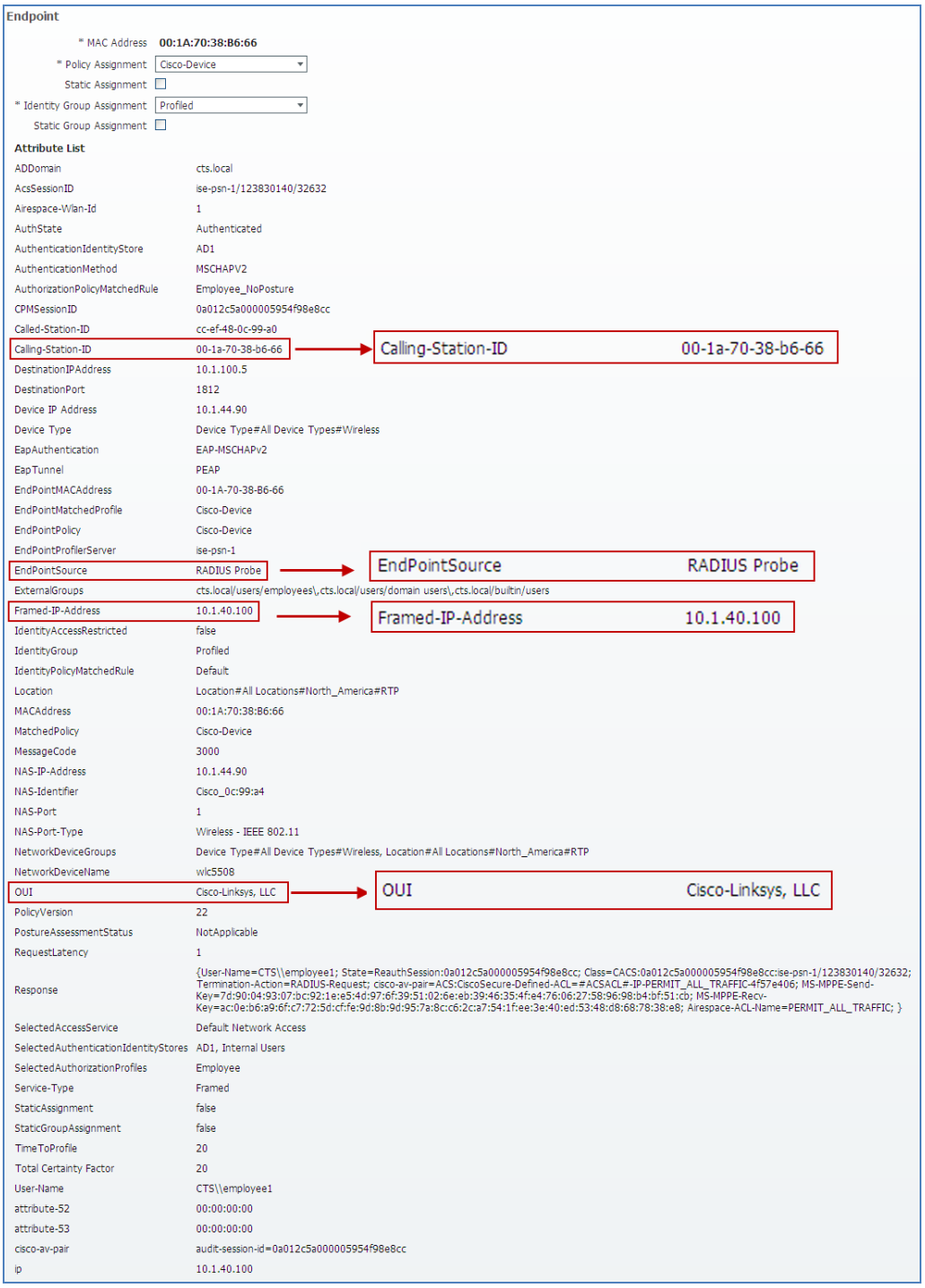
**ステップ 2** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

**ステップ 3** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 4** RADIUS プローブによってキャプチャされた属性を表示するために、新しく接続されたエンドポイントの MAC アドレスを探して選択します。

**ステップ 5** さまざまな属性をキャプチャできます。図 14 のサンプル出力で強調表示されているのは次の 4 つだけです。**Calling-Station-ID**、**EndPointSource**、**Framed-IP-Address**、および **OUI**。

図 9 RADIUS プローブ属性の例




**ステップ 6** Calling-Station-ID は **MACaddress** 属性を表します。加えて、ネットワーク アダプタのベンダー OUI が **Cisco-Linksys** と判別されています。この例では、ネットワーク アダプタは Linksys ワイヤレス USB アダプタです。OUI と照合する条件は、プロファイリング ポリシー ルール内の共通エントリです。Nintendo や Sony のゲーム コンソールのように、それだけでエンドポイントが分類できる場合があります。

**ステップ 7** Framed-IP-Address 値は **ip** 属性を表します。これで、このエンドポイントの IP/MAC アドレス間バインドが出来上がりました。

**ステップ 8** **EndPointSource** 属性は、最後のプロファイル属性更新のソースを指定します。この場合は、それがこのエンドポイント レコードに対する最後の更新を行った RADIUS プローブになります。

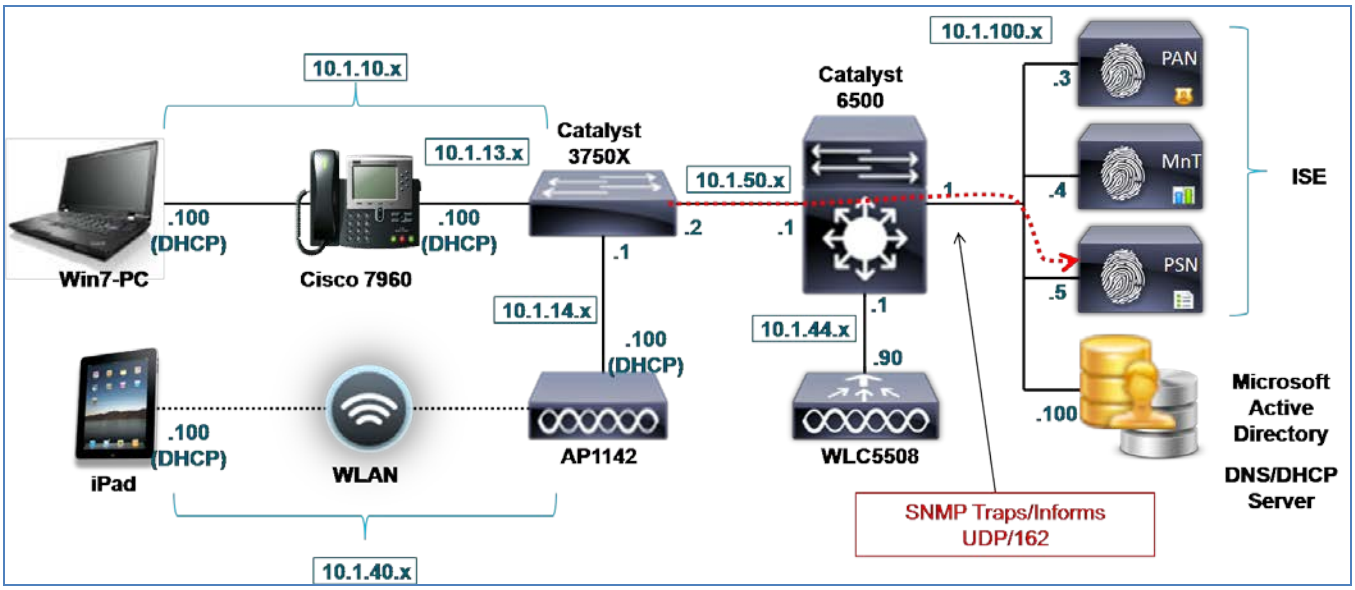
**ステップ 9** その他の RADIUS 属性をプロファイリングに使用することもできますが、そのほとんどが認可ポリシーでポリシーの条件とルールを作成するために直接使用できるため、上記属性を中心に説明します。

## SNMP トラップ プローブを使用したプロファイリング

SNMP トラップ プローブは、ネットワーク エンドポイントのプレゼンス(接続または接続解除)を ISE プロファイリング サービスに通知して、SNMP クエリ プローブをトリガーするために使用されます。

SNMP トラップ プローブを使用するには、エンドポイントが接続されたアクセス デバイスを、プロファイリング サービス用に設定された ISE ポリシー サービス ノードに SNMP トラップを送信するように設定する必要があります。図 15 に、サンプル SNMP トラップ プローブのトポロジを示します。

図 10 SNMP トラップ プローブの例




RADIUS プローブがすでに有効になっている場合は、RADIUS アカウンティング開始メッセージでも SNMP クエリ プローブをトリガーすることができるため、SNMP トラップ プローブが必要ない可能性があります。このプローブの基本的な使用例は、RADIUS をネットワーク認証用として設定すべき展開前ディスカバリ フェーズ向けです。Cisco NAC アプライアンス リリース 4.9 以降のような RADIUS に依存しない環境を統合するための使用例もあります。

# SNMP トラップ プローブの設定

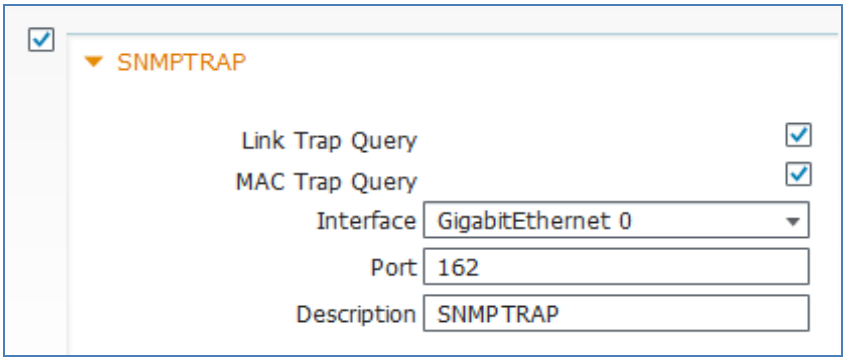
SNMP トラップ プローブを使用するには、最初にそれを ISE で有効にする必要があります。前述したように、エンドポイントが接続されたアクセス デバイスを、プロファイリング サービス用に設定された ISE ポリシー サービス ノードに SNMP トラップを送信するように設定する必要があります。ISE を、これらのネットワーク アクセス デバイスからのトラップを受け入れて処理するように設定する必要もあります。

## ISE での SNMP トラップ プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択して、SNMP トラップ プローブを有効にするボックスをオンにします（図 16）。

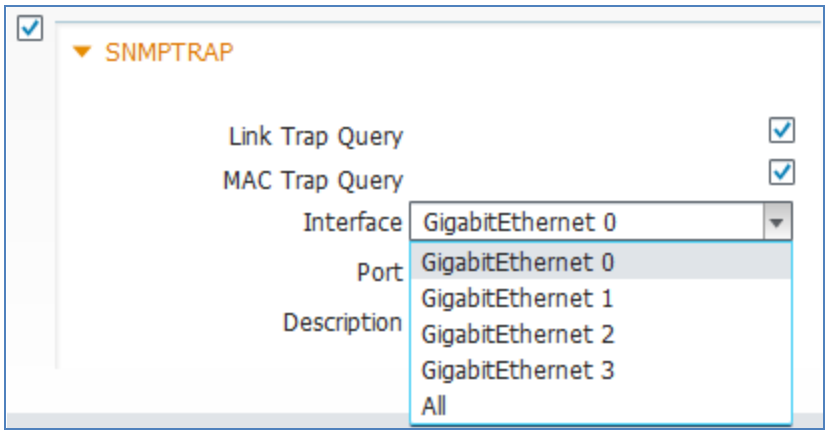
図 11 SNMPTRAP プローブの設定




**ステップ 3** プローブがトラップ タイプに合わせて応答できるようにするために、[リンクトラップクエリ（Link Trap Query）] と [MACトラップクエリ（MAC Trap Query）] というラベルの付いたボックスをオンにします。

**ステップ 4** ISE PSN インターフェイスがトラップの受信に使用されていることを確認します。ほとんどの場合、これはデフォルトの GigabitEthernet 0 インターフェイスになりますが、他のインターフェイスで受信されたトラップを処理することも、すべてのインターフェイスを選択することもできます。

図 12 SNMP トラップ プローブ：インターフェイスの設定



**ステップ 5** 他のインターフェイス上でトラップを処理することにした場合は、それらのインターフェイスが有効化され、IP アドレスが割り当てられていることを確認します。これらのアドレスは、SNMP ホストトラップ ターゲットにあるアクセス デバイスで設定する必要があります。

**ステップ 6** [保存(Save)] をクリックして、変更をコミットします。

**ステップ 7** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

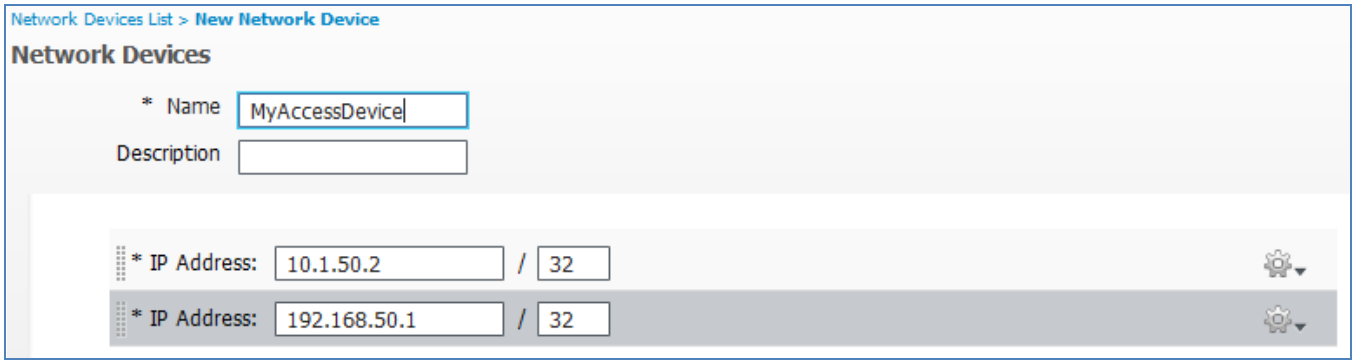
## ISE へのネットワーク アクセス デバイスの追加

通常は、RADIUS 経由でエンドポイントを認証するすべてのネットワーク アクセス デバイスが ISE で設定されますが、SNMP トラップ プローブの使用はアクセス デバイスがまだ RADIUS 用に設定されていないことを意味している場合がほとんどです。これらのアクセス デバイスがまだ設定されていない場合は、SNMP トラップを ISE に送信するアクセス デバイスを追加する必要があります。

**ステップ 1** [管理(Administration)] → [ネットワークリソース(Network Resources)] → [ネットワークデバイス(Network Devices)] にアクセスして、RHS ペインで [追加(Add)] をクリックします。

**ステップ 2** デバイス名と IP アドレス情報を入力します(図 18)。IP アドレスには、SNMP トラップを供給する IP アドレスを含める必要があります。シンプルな設定では、スイッチ上に管理 IP アドレスが 1 つしか存在しない場合があります。他のケースでは、複数の IP アドレスが存在し、デフォルトで、SNMP が出力インターフェイスの IP アドレスを使用します。必要に応じて、アクセス デバイスで SNMP パケットの供給に使用されるすべての IP アドレスを入力します。

図 13 ネットワーク デバイスの設定



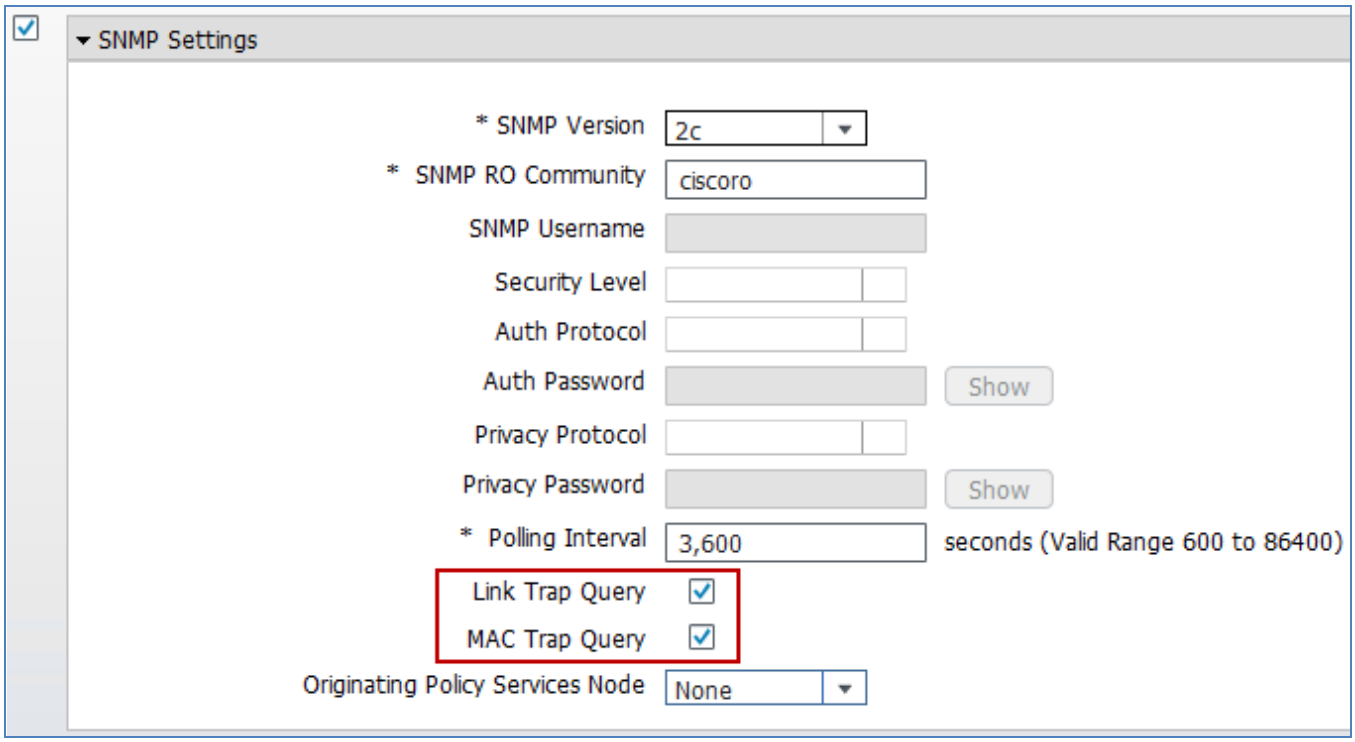

**ベスト プラクティス**:アクセス デバイスでサポートされている場合は、管理トラフィックにループバック インターフェイスを使用します。**source-interface** などのオプションを利用して、管理トラフィックを供給する特定のインターフェイスと IP アドレスを設定してください。これにより、すべての管理トラフィックに対して統一されたアドレスが提供され、特定のインターフェイスがダウンした場合の接続障害も回避されます。

**ステップ 3** [SNMPの設定(SNMP Settings)] ボックスをオンにします。

**ステップ 4** アクセス デバイスで使用される SNMP バージョンを指定して SNMP バージョン 1 および 2c の SNMP RO コミュニティ ストリングを入力するか、アクセス デバイスに適切な SNMPv3 クレデンシャルとコンフィギュレーションを入力します(図19)。

**ステップ 5** [リンクトラップクエリ(Link Trap Query)] ボックスと [MACトラップクエリ(MAC Trap Query)] ボックスがオンになっていることを確認します。これらの設定を使用すれば、ISE は、特定のアクセス デバイスから受信した SNMP トラップを受け入れたり無視したり、特定のタイプのトラップだけを受け入れたりすることができます。

図 14 ネットワーク デバイスの設定：SNMP トラップ




**ステップ 6** 完了したら変更を保存します。

**ステップ 7** ISE ポリシー サービス ノードに SNMP トラップを送信する各アクセス デバイスに対して、上記手順を繰り返します。

## ISE ポリシー サービス ノードに SNMP トラップを送信するためのアクセス デバイスの設定

**ステップ 1** アクセス デバイスの管理コンソールにアクセスして、それがプロファイリング サービスを実行している ISE ポリシー サービス ノードに SNMP トラップを送信するように設定されており、SNMP トラップ プローブで有効になっていることを確認します。

**ステップ 2** ここで、Cisco IOS を実行している Catalyst スイッチから SNMP linkUp/linkDown トラップだけでなく、MAC 通知トラップも送信する設定例を示します。

```
interface <Endpoint_Interface>
 snmp trap mac-notification added
 snmp trap mac-notification removed
!
mac address-table notification change
mac address-table notification mac-move
!
snmp-server trap-source <Interface>
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host <ISE_PSN_IP_address> version 2c ciscoro
```

注：Cisco ISE は、現在、ワイヤレス LAN コントローラからの SNMP トラップをサポートしていません。

## SNMP トラップ プローブ データの確認

SNMP トラップ プローブは、LinkUp または LinkDown トラップだけに基づいてエンドポイント属性を生成できません。これは、それらのトラップ内に関連する MAC アドレスが存在しないためです。これらは、主に、リンクが確立または消失しているインターフェイスを通知します。ただし、MAC 通知トラップにはエンドポイントの MAC アドレスが含まれているため、ISE 内部エンドポイント データベースが更新される可能性があります。

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

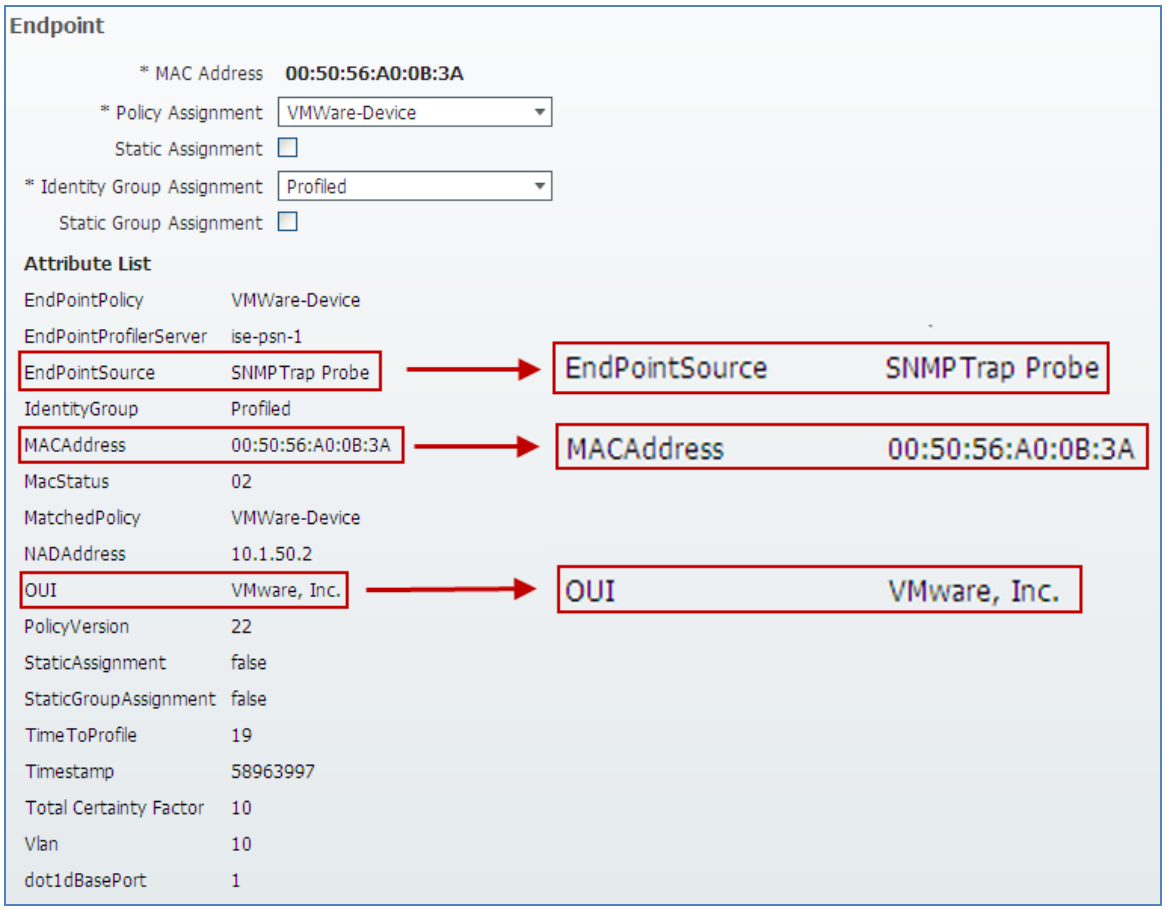
**ステップ 2** SNMP トラップ用に設定されたアクセス スイッチから有線クライアントを接続解除してから、再接続します。

**ステップ 3** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

**ステップ 4** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを探して選択し、SNMP トラップ プローブによってキャプチャされた属性を表示します（図 20）。

図 15 SNMP トラップ プローブ属性の例




強調表示されたキー属性には、**EndPointSource**、**MACAddress**、および **OUI** が含まれます。

**EndPointSource** は、SNMP トラップ プローブが情報源であることを確認します。

注:図 20 に示す例では、テストを実行する前に、他のすべてのプローブが無効にされ、エンドポイントが ISE データベースから削除されています。

**MACAddress** は MAC 通知トラップ情報から学習されており、ベンダー OUI は ISE の OUI データベースに対して関連付けることによって決定されています。この例では、仮想ネットワーク アダプタを使用するクライアントが VMware を実行していることを確認できます。

SNMP トラップがアクセス スイッチから送信されていることのオプション検証として、デバッグ ロギングを有効にして、送信された SNMP リンクと MAC 通知トラップを表示することができます。以下の出力は、次のデバッグが有効にされた Catalyst スイッチからのものです。

- debug snmp packets
- debug mac-notification

次の例では、Cisco IP Phone に接続されたスイッチポートとその電話に接続された Windows 7 PC を有効にすると、電話と PC の両方の SNMP LinkUp トラップが ISE PSN に送信され、その後に両方の MAC 通知トラップが続きます。MAC アドレスが 00:50:56:A0:0B:3A の PC に関連付けられたトラップのみが強調表示されています。

```
Apr 26 16:53:06.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Apr 26 16:53:06.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan13, changed state to up
Apr 26 16:53:06.743: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.743: SNMP: V2 Trap, reqid 296, errstat 0, erridx 0
 sysUpTime.0 = 58970958
 snmpTrapOID.0 = snmpTraps.4
 ifIndex.10 = 10
 ifDescr.10 = Vlan10
 ifType.10 = 53
 ifEntry.20.10 = up

Apr 26 16:53:06.861: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.861: SNMP: V2 Trap, reqid 299, errstat 0, erridx 0
 sysUpTime.0 = 58970970
 snmpTrapOID.0 = snmpTraps.4
 ifIndex.13 = 13
 ifDescr.13 = Vlan13
 ifType.13 = 53
 ifEntry.20.13 = up
Apr 26 16:53:06.995: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:07.246: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:08.706: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
Apr 26 16:53:09.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up
Apr 26 16:53:09.713: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:09.713: SNMP: V2 Trap, reqid 302, errstat 0, erridx 0
 sysUpTime.0 = 58971255
 snmpTrapOID.0 = snmpTraps.4
 ifIndex.10101 = 10101
 ifDescr.10101 = GigabitEthernet1/0/1
 ifType.10101 = 6
 ifEntry.20.10101 = up
Apr 26 16:53:09.964: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:12.280: MN: Enqueue MAC 0050.56a0.0b3a on port 1 vlan 10
MN: New Shadow entry..

Apr 26 16:53:12.280: MN : MAC Notify event for 0050.56a0.0b3a on port 1 vlan 10

Apr 26 16:53:12.456: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 10
MN: Got the last shadow entry..Index 11

Apr 26 16:53:12.456: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 10
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58971575
MN: Wrapping history queue..

Apr 26 16:53:12.925: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:12.925: SNMP: V2 Trap, reqid 305, errstat 0, erridx 0
 sysUpTime.0 = 58971577
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.1 =
01 00  0A 00   50 56  A0 0B    3A 00  01 01   00 0A  00 30
94 C4  52 8A   00 01  00
 cmnHistTimestamp.1 = 58971575
Apr 26 16:53:13.177: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:23.587: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 13
MN: New Shadow entry..

Apr 26 16:53:23.604: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 13
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58972696
MN: Wrapping history queue..
```

```
Apr 26 16:53:24.132: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:24.132: SNMP: V2 Trap, reqid 308, errstat 0, erridx 0
 sysUpTime.0 = 58972697
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.1 =
01 00   0D 00    30 94   C4 52     8A 00   01 00
 cmnHistTimestamp.1 = 58972696
Apr 26 16:53:24.384: SNMP: Packet sent via UDP to 10.1.100.5
```

参考のために、アクセス デバイス上で使用可能なデバッグ ロギングに加えて、ISE は独自のデバッグ ロギングもサポートします。デバッグはこのマニュアルでは扱いませんが、ISE で受信された情報を検証するために、[操作（Operations）] → [トラブルシューティング（Troubleshot）] → [診断ツール（Diagnostic Tools）] → [一般的なツール（General Tools）] にある、組み込みの TCP ダンプ ユーティリティを使用することもできます。このツールを使用すれば、ISE で、アクセス デバイスから、指定された ISE ポリシー サービス ノード インターフェイス（SNMP トラップ プローブで有効にされたもの）への SNMP トラフィックをキャプチャできます。この情報は、人間が判読可能な形式、または、Wireshark などの一般的なパケット アナライザにインポートするための標準的なパケット キャプチャ形式でダウンロードして表示できます。

## SNMP クエリ プローブを使用したプロファイリング

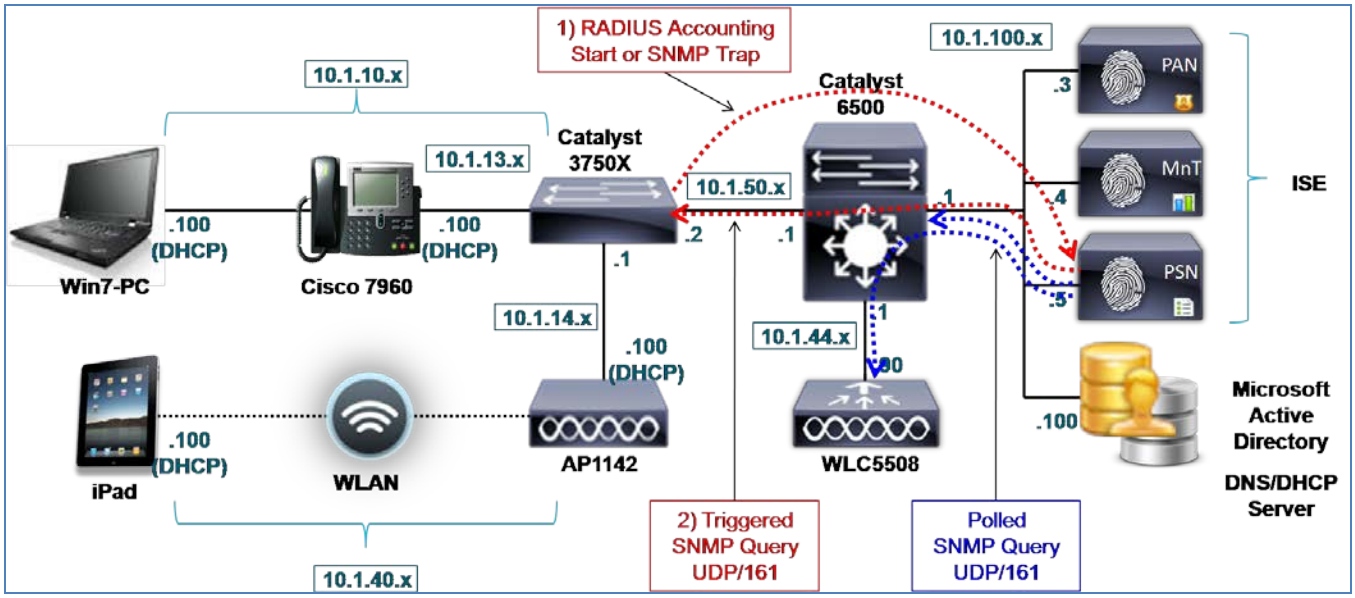
**ステップ 1** SNMP クエリ プローブは、クエリ（または SNMP GET 要求）をアクセス デバイスと、オプションで、他のインフラストラクチャ デバイスに送信して、SNMP MIB に保存されている関連するエンドポイント データを収集するために使用されます。ISE ポリシー サービス ノードで実行される SNMP クエリには、次の 2 つの一般的なタイプがあります。

**ステップ 2** システム クエリ（ポーリング対象）

**ステップ 3** インターフェイス クエリ（トリガー対象）

**ステップ 4** 図 21 に、システム クエリ プローブを使用したトポロジの例を示します。

図 16 SNMP クエリ プローブの例



## システム クエリ

システム クエリは、ISE の NAD 設定でセットされたポーリング間隔に基づいて定期的に実行されます。ポーリング対象の MIB には以下が含まれます。

- IF-MIB
- SNMPv2-MIB
- IP-MIB
- CISCO-CDP-MIB
- CISCO-VTP-MIB
- CISCO-STACK-MIB
- BRIDGE-MIB
- OLD-CISCO-INTERFACE-MIB
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-DOT11-CLIENT-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- EEE8021-PAE-MIB: RFC IEEE 802.1X
- HOST-RESOURCES-MIB
- LLDP-MIB

収集対象のキー属性には次のエントリが含まれます。

- ブリッジ、IP（ARP）
- **cdpCacheEntry**（有線のみ）
- lldpLocalSystemData（有線のみ）
- lldpRemoteSystemsData（有線のみ）
- **cLApEntry**（WLC のみ）
- cldcClientEntry（WLC のみ）

複数のポリシー サービス ノードで SNMP クエリが有効になっており、特定の PSN が特定のネットワーク デバイスをポーリングするように設定されていない場合は、ネットワーク デバイスの SNMP ポーリングが、使用可能なすべての PSN で分散されます。

このポーリング対象クエリ中に、ISE 内の IP-MAC ARP キャッシュ テーブルを作成するための Address Resolution Protocol（ARP）テーブル情報も収集されます。エンドポイントがレイヤ 2 専用スイッチ ポートに接続されている環境では、エンドポイントの ARP テーブル情報が保存されているアップストリーム レイヤ 3 デバイス（ブランチ ルータやレイヤ 3 ディストリビューション スイッチなど）を ISE ネットワーク アクセス デバイスとして設定することをお勧めします。これは、アクセス デバイスで RADIUS が設定されていない展開や DHCP プローブで必要なデータを収集できない展開で、IP/MAC 間バインド情報を提供するために必要になります。トポロジの例（図 21）では、ワイヤレス クライアントまたはダウンストリーム レイヤ 2 スイッチの ARP 情報を取得するために Cisco Catalyst 6500 シリーズ スイッチがポーリングされる場合があります。

## インターフェイス クエリ

インターフェイス クエリは、RADIUS アカウンティング開始パケット（RADIUS プローブが必要）または SNMP LinkUp/MAC 通知トラップ（SNMP トラップ プローブが必要）によってトリガーされます。

**ベスト プラクティス**：展開を簡素化して SNMP トラップによるトラフィック オーバーヘッドを削減するには、可能な限り、RADIUS プローブを使用して、RADIUS アカウンティング開始メッセージに基づいて SNMP クエリをトリガーします。

システム クエリはアクセス デバイス MIB を読み取るのに対して、インターフェイス クエリはトラップが受信される特定のインターフェイスにのみ関連した MIB または MIB の一部を要求します。次のトリガ対象クエリはアクセス デバイスから次のデータを取得します。

- インターフェイス データ（ifIndex、ifDesc など）
- ポートと VLAN のデータ
- セッション データ（インターフェイス タイプがイーサネットの場合）
- CDP データ（シスコ デバイス）
- LLDP データ

トリガー対象インターフェイス クエリ中に収集されるキー プロファイリング属性には、Cisco Discovery Protocol（CDP）テーブルと Link Layer Discovery Protocol（LLDP）テーブルが含まれます。CDP と LLDP は、スイッチが接続されたエンドポイントの属性を動的に学習できるようにするリンク プロトコルです。IP ビデオ機器、ネットワーク インフラストラクチャ、およびシスコ アプライアンスを含むさまざまなデバイスがこれらのプロトコルをサポートしています。ほとんどの大手 IP フォン メーカーが CDP または LLDP をサポートしています。これにより、多くのエンドポイントをこの情報だけに基づいて分類することができます。加えて、さまざまなクライアント オペレーティング システムで膨大な数の CDP/LLDP エージェントを最低料金または無料で利用できます。

次に、接続されたエンドポイントの CDP データを収集するための SNMP クエリを使用して収集可能な情報の出力例を示します。

```
cat3750x#show cdp neighbor detail
-------------------------
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9   ,  Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2,  Port ID (outgoing port): GigabitEthernet0
Holdtime : 123 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 1358, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):

-------------------------
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): Port 1
Holdtime : 162 sec
Second Port Status: Up

Version :
P00308010100
```

```
advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):

-------------------------
```

# SNMP クエリ プローブの設定

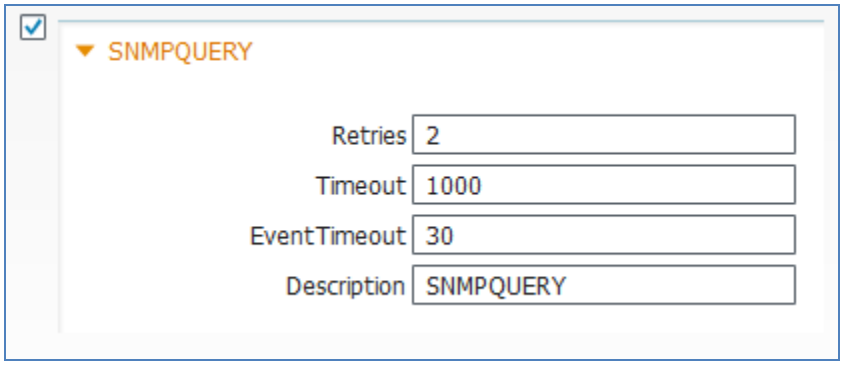
SNMP クエリ プローブを使用するには、読み取り専用(RO)コミュニティを使用して ISE ポリシー サービス ノードから SNMP 要求を受信するようにネットワーク デバイスを設定する必要があります。また、ISE では、適切な SNMP コミュニティ ストリングとともに SNMP デバイスをネットワーク デバイスとして設定する必要もあります。トリガー対象クエリが発行されるためには、RADIUS プローブまたは SNMP トラップ プローブを有効にして、関連するコンポーネントを正しく設定する必要があります。最後に、CDP または LLDP 情報を取得するためには、エンドポイントが CDP または LLDP をサポートし、アクセス スイッチでこれらのプロトコルのどちらかまたは両方が有効になっている必要があります。

## ISE での SNMP クエリ プローブの有効化

**ステップ 1** [管理(Administration)] → [システム(System)] → [展開(Deployment)] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定(Profiling Configuration)] タブを選択して、SNMP クエリ プローブを有効にするボックスをオンにします(図 22)。

図 17 SNMP クエリ プローブの設定




注:SNMP クエリ プローブ用にインターフェイスを設定する必要はありません。SNMP クエリは、アプライアンス ルーティング テーブルに基づいてアクセス デバイスに送信されます。

**ステップ 3** [再試行(Retries)]、[タイムアウト(Timeout)]、および [イベントタイムアウト(Event Timeout)] はデフォルト値のままにします。

**ステップ 4** [タイムアウト(Timeout)](ミリ秒)は、SNMP 応答を待機する時間の長さを指定します。

**ステップ 5** [再試行(Retries)] は、ポリシー サービス ノードが、失敗した最初の試行後に SNMP セッションを確立しようとする回数を指定します。

**ステップ 6** [イベントタイムアウト(EventTimeout)](秒)は、RADIUS アカウンティング開始または SNMP トラップ トリガーの後、バッチ クエリをアクセス デバイスに送信するまでに待機する時間を指定します。

**ステップ 7** トリガー対象インターフェイス クエリ用に、RADIUS プローブが有効になっていることを確認してください。ネットワーク アクセス デバイス上で RADIUS が設定されていない場合は、SNMP トラップ プローブが有効になっていることを確認してください。

**ステップ 8** [保存(Save)] をクリックして、変更をコミットします。

**ステップ 9** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

## ISE(ネットワーク リソース)でのネットワーク デバイスの設定

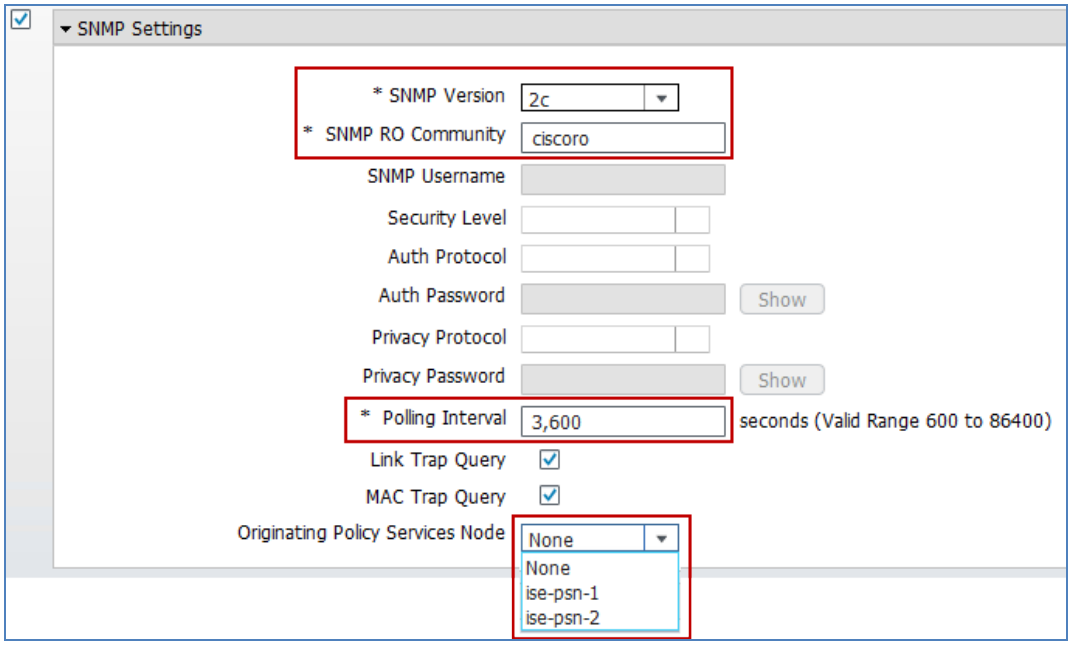
通常、RADIUS 経由でエンドポイントを認証するすべてのネットワーク アクセス デバイスは ISE 内で設定されるため、必要な操作は、それぞれの SNMP 設定を確認することだけです。RADIUS 認証が展開されていないネットワークの SNMP クエリ プローブを設定する場合は、ISE ネットワーク デバイスのリストに各アクセス デバイスを追加する必要があり、オプションでレイヤ 3 デバイス(ARP 情報用)を選択します。

**ステップ 1** [管理(Administration)] → [ネットワークリソース(Network Resources)] → [ネットワークデバイス(Network Devices)] にアクセスします。SNMP を使用して照会するデバイスがすでに存在している場合は、単にリストからデバイスを選択するか、RHS ペインで [追加(Add)] をクリックします。

**ステップ 2** 新しいデバイスの場合は、デバイス名と IP アドレス情報を入力します。

**ステップ 3** [SNMPの設定(SNMP Settings)] ボックスで、アクセス デバイスで使用される SNMP のバージョンを指定して、SNMPバージョン 1 および 2c の SNMP RO コミュニティ ストリングを入力するか、アクセス デバイスに適した SNMPv3 クレデンシャルとコンフィギュレーションを入力します(図 23)。

図 18 ネットワーク アクセス デバイスの設定:SNMP クエリ




**ステップ 4** システム(ポーリング対象)クエリの場合は、[ポーリング間隔(Polling Interval)] と [発信ポリシーサービス ノード(Originating Policy Services Node)] を次のように設定します。

**ステップ 5** [ポーリング間隔(Polling Interval)]:一般的に、RADIUS または DHCP プローブが展開されたネットワークには長いポーリング間隔が推奨されます。これは、ARP 情報への依存度が低くなるためです。

**ステップ 6** [発信ポリシーサービスノード(Originating Policy Services Node)]:SNMP クエリ プローブが有効にされた PSN が一覧表示されます。ネットワーク デバイスの定期ポーリングを実行するのに最適なポリシー サービス ノードを選択します。通常、これはネットワーク帯域幅の観点からネットワーク デバイスに最も近い PSN になります。

**ステップ 7** SNMP トラップに依存しているインターフェイス(トリガー対象)クエリの場合は、トラップ クエリ オプションのどちらかまたは両方を必ず設定してください。

**注**:(RADIUS アカウンティング開始や SNMP トラップ メッセージなどの)トリガーを受信した PSN によって常に送信されるインターフェイス クエリには、発信ポリシー サービス ノードの設定が適用されません。

**ステップ 8** 完了したら変更を保存します。

**ステップ 9** ISE ポリシー サービス ノードから SNMP を使用して照会する必要のあるアクセス デバイスごとに、上記の手順を繰り返します。

## ISE PSN からの SNMP クエリを受け入れるための有線アクセス デバイスの設定

有線アクセス デバイスの管理コンソールにアクセスして、SNMP クエリ プローブが有効になっている ISE ポリシー サービス ノードからの SNMP 読み取り専用要求をサポートするように設定されていることを確認します。

以下に、読み取り専用コミュニティ ストリング **ciscoro** を使用した ISE PSN からの SNMPv2c クエリをサポートするための IOS を実行している Cisco Catalyst スイッチの設定例を示します。

```
snmp-server community ciscoro RO
snmp-server community ciscorw RW
```

## ISE PSN からの SNMP クエリを受け入れるための無線アクセス デバイスの設定

ワイヤレス LAN コントローラの Web 管理インターフェイスにアクセスして、SNMP クエリ プローブが有効になっている ISE ポリシー サービス ノードからの SNMP 読み取り専用要求をサポートするように設定されていることを確認します。

**ステップ 1** [管理(Management)] → [SNMP(SNMP)] → [コミュニティ(Communities)] → [SNMP v1/v2cコミュニティ(SNMP v1/v2c Community)] にアクセスして、このデバイスを照会する可能性のある ISE ポリシー サービス ノードで使用される 1 つ以上の読み取り専用コミュニティ ストリングを設定します。

**ステップ 2** 次の図に、読み取り専用コミュニティ ストリング **ciscoro** を使用した ISE PSN からの SNMPv2c クエリをサポートするように設定された WLC の設定例を示します。

図 19 無線コントローラの SNMP 設定の例

SNMPv3 が展開されている場合は、必ず [管理（Management）] → [SNMP（SNMP）] → [SNMP V3ユーザ（SNMP V3 Users）] で適切な設定を行ってください。

### CDP と LLDP をサポートするためのアクセス デバイスの設定

接続先のホストから CDP と LLDP 情報を取得するには、スイッチポートでアクセス デバイスがこれらのプロトコルを受信するように設定されていることを確認します。大抵の場合、CDP はシスコ デバイス上でデフォルトで有効になっていますが、LLDP はそうなっていません。そのため、SNMP クエリ プローブを使用してこの情報を収集するには LLDP をグローバルに有効にする必要があります。

```
cdp run
interface <Endpoint_Interface>
  cdp enable
!
lldp run
interface <Endpoint_Interface>
  lldp receive
  lldp transmit
```

注：ワイヤレス LAN コントローラは、無線クライアントの CDP/LLDP をサポートしません。

### SNMP クエリ プローブ データの確認

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

**ステップ 2** ISE で SNMP アクセス用に設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

**ステップ 3** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

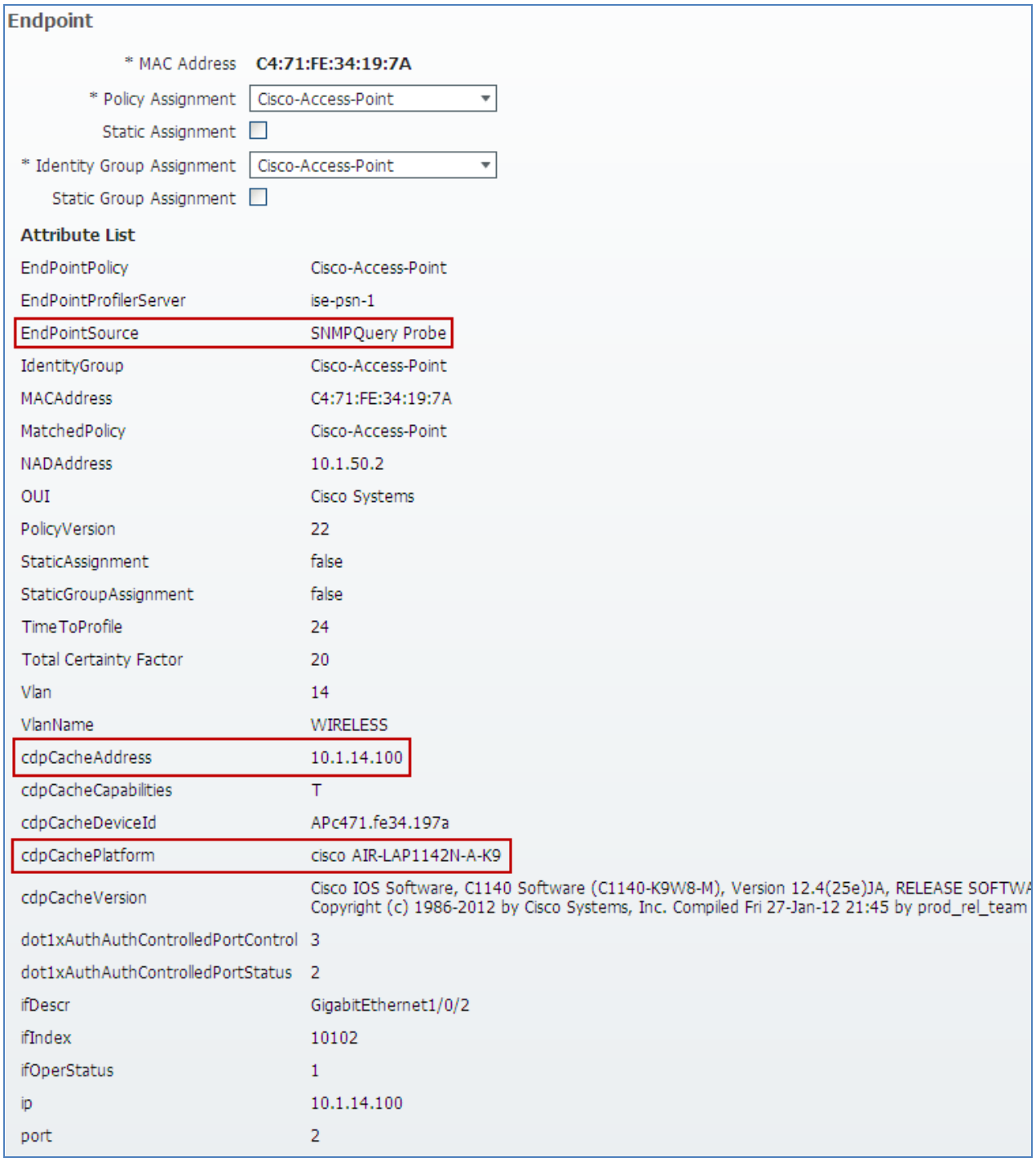
**ステップ 4** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、SNMP クエリ プローブによってキャプチャされた属性を表示します。

図 25 に示す例では、SNMP クエリを使って収集された属性を強調表示するために SNMP トラップおよび SNMP クエリ プローブだけが使用されています。強調表示されているキー属性には、**EndPointSource**、**cdpCacheAddress**、および **cdpCachePlatform** があります。

- **EndPointSource** は、最後のプロファイリング更新が SNMP クエリ プローブから受信されたことを示しています。
- **cdpCacheAddress** は IP アドレスを提供し、IP アドレスと MAC アドレスの間のバインドを可能にします。
- **cdpCachePlatform** 属性は、接続されたエンドポイントを詳しく記述しています（この例では、Cisco Aironet 1142N ワイヤレス アクセス ポイントである Cisco AIR-LAP1142N-A-K9）。

図 20 SNMP クエリ プローブ属性の例



**ステップ 6**　想定される属性データを確認するには、アクセス スイッチ コンソールから次のコマンドを使用できます。

```
switch# show cdp neighbor detail
switch# show lldp neighbor detail
```

## DHCP プローブと DHCP SPAN プローブを使用したプロファイリング

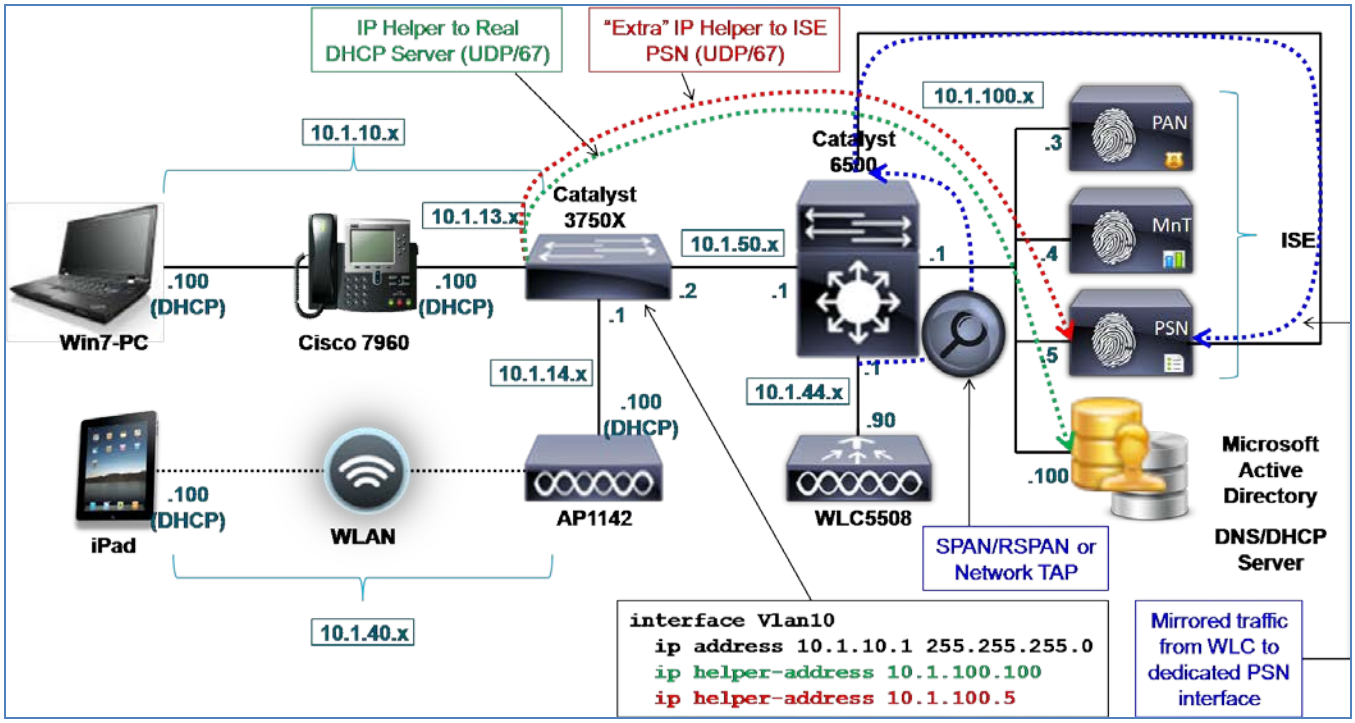
名前が示すように、DHCP プローブは DHCP パケットから属性を収集します。次のどちらかまたは両方を使用して DHCP 属性を収集できます。

- DHCP プローブ
- DHCP SPAN プローブ

## DHCP プローブ

DHCP プローブの目的は、(たとえばネットワーク内の DHCP リレー機能の結果として) DHCP 要求が ISE ポリシー サービス ノードに直接送信される方式で使用することです。シスコ ネットワークで一般的な DHCP リレーは、ローカル DHCP クライアント用のゲートウェイであるレイヤ 3 インターフェイスに適用される **ip helper-address** コマンドです。図 26 に、DHCP プローブを使用したトポロジの例を示します。

図 21 DHCP プローブの例



この図では、Cisco Catalyst 3750-X が従業員データ VLAN 10 と音声 VLAN 13 の両方を備えています。それぞれのスイッチ仮想インターフェイス（SVI）のインターフェイス設定では、10.1.100.100 にある実 DHCP サーバにローカル DHCP ブロードキャスト パケットを転送する **ip helper-address** コマンドがあります（図 26 では緑色で強調表示）。これは、DHCP 要求に応答するサーバです。同じインターフェイスで、別の **ip helper-address** コマンドが、DHCP プローブで有効になっている ISE PSN インターフェイスを指すように設定されます（赤色で強調表示）。ISE ポリシー サービス ノードはこれらのパケットに応答するわけではなく、その目的は単に、DHCP 属性の解析用に要求のコピーを ISE に送信することです。

複数の ISE ポリシー サービス ノードで DHCP 要求のコピーを受信できるように、シスコ デバイス上の複数の IP ヘルパー ターゲットを設定することができます。

注：ISE DHCP プローブは、DHCP リレーと DHCP プロキシの両方からのトラフィックを解析できます。これらの方式の主な違いは、ip helper-address コマンド経由の DHCP リレーでは、複数の宛先にトラフィックを送信できるため、複数の実 DHCP サーバと ISE ポリシー サービス ノードが DHCP 要求のコピーを受信できることです。一方、DHCP プロキシは、プライマリ DHCP サーバにだけ要求を送信し、有効な応答が受信されない場合のみ、他の設定済みの DHCP ターゲットにフォールバックします。実 DHCP サーバへのフォールバックを可能にするための最初のエントリとして ISE ノードを設定することはできますが、このような実装にするとエンドポイントが IP アドレスを取得するまでの時間が長くなります。これは、ユーザ エクスペリエンスに影響を与える可能性があり、結果的に、応答を待っているクライアントがタイムアウトする場合もあります。

## DHCP SPAN プローブ

DHCP SPAN プローブは、スイッチ ポート アナライザ（SPAN）、リモート SPAN（RSPAN）、ネットワーク タップなどの方式を使用してトラフィックが ISE ポリシー サービス ノード上のインターフェイスにミラーリングされる場合に使用されます。この方式は主に、DHCP リレーを使用した基本 DHCP プローブが利用できない場合に使用されます。

**ベスト プラクティス**：DHCP トラフィックの特定のフローごとに、そのトラフィックから属性を収集するプローブを 1 つだけ選択してください。DHCP（IP ヘルパー）プローブと DHCP SPAN プローブの両方を使用して同じ DHCP トラフィックから属性を収集する場合は値が制限されます。

可能な場合は、DHCP SPAN プローブではなく DHCP プローブを使用することをお勧めします。DHCP リレー経由で DHCP パケットのみを送信することにより、DHCP パケットからの属性を検査して解析するための ISE ポリシー サービス ノードでの全体的なトラフィック負荷が減少します。

また、DHCP SPAN プローブを使用すると、ローカル サブネット ブロードキャストから DHCP トラフィックをキャプチャできますが、DHCP プローブを使用すると、アップストリーム ゲートウェイで中継される DHCP トラフィックのみをキャプチャできます。これは、レイヤ 3 ゲートウェイがローカル クライアントの DHCP サーバを兼ねている場合に必要になることがあります。Cisco IOS DHCP サーバは、そのサブネットにも DHCP を供給するように設定されている場合、セグメントの DHCP を中継しません。

サンプル トポロジは、WLC に接続されたワイヤレス クライアントからポリシー サービス ノード上の専用インターフェイスにパケットをコピーするために SPAN またはネットワーク タップを使用する方法を示しています（図 26 では青色で強調表示）。PSN 宛ての通常のトラフィックの送受信を制限する特殊なプロパティが SPAN 宛先ポートで設定される場合があるため、専用のインターフェイスが必要です。加えて、ミラーリング トラフィックによって、RADIUS などの他の重要な PSN のインターフェイスで輻輳が発生しないようにする必要があります。SPAN 方式を使用した場合、SPAN ポートの処理能力を上回る大量のデータが送られて、パケット ドロップや重要なトラフィックの遅延が生じる可能性があります。

## DHCP 属性

DHCP プローブと DHCP SPAN プローブはどちらも同じキー プロファイリング属性を ISE に配信します。これには以下が含まれます。

- dhcp-class-identifier
- dhcp-user-class-id
- dhcp-client-identifier
- dhcp-message-type
- dhcp-parameter-request-list
- dhcp-requested-address
- host-name
- domain-name
- client-fqdn

DHCP は MAC アドレス(**dhcp-client-identifier**)と IP アドレス(**dhcp-requested-address**)の両方を提供するため、ISE ARP キャッシュ テーブル用の IP/MAC アドレス間バインドを確立することもできます。これは、MAC アドレスではなく IP アドレスに依存する他のプローブのサポートに役立ちます。それらが提供する特定のエンドポイントに関する属性を ISE データベースに適用して保存するには、IP アドレスをその MAC アドレスに基づいて特定のエンドポイントに関連付ける必要があります。

**dhcp-client-identifier** と **dhcp-requested-address** のほかに、重要な属性には **dhcp-class-identifier**、**dhcp-user-class-id**、および **dhcp-parameters-request-list** があります。プラットフォームまたは OS 情報を伝送するためにクラス ID がよく使用されます。クラス ID とユーザ クラス ID を Mac OS や Microsoft Windows などの一部のクライアント オペレーティング システム上でカスタマイズすると、プロファイリング用の固有の企業識別子としてこれを使用したり、DHCP サーバから固有の範囲値を返したりすることができます。

**dhcp-parameters-request-list** はデバイス タイプの固有のインジケータになり得ます。これは、要求されたパラメータの値とシーケンスが単一のデバイス タイプまたは限定的なデバイス タイプ セットに固有であることが多いためです。たとえば、1、3、6、15、119、252 という **dhcp-parameters-request-list** 値は、iPad、iPod、iPhone などの Apple iOS デバイスを表します。

標準的なホスト名、ドメイン名、または完全修飾ドメイン名(FQDN)の命名規則が特定のエンドポイントに適用される場合は、これらの属性を使ってそれらを分類できます。たとえば、すべての Windows XP クライアントに **jsmith-winxp** などの名前が割り当てられている場合、Windows XP エンドポイントを分類するための条件に **host-name** 属性または **client-fqdn** 属性を使用できます。同様に、**jsmith-corp-dept** などに企業エンドポイントの **host-name** を入力する規則がある場合は、この属性を使って企業資産を検証できます。

プロファイル属性を ID と混同しないように注意する必要がありますが、属性を使用すると、エンドポイントが特定のタイプであるという一定の信任レベルを追加できます。たとえば、認可ポリシーをプロファイリングとともに使用すると、(エンドポイント ID グループの照合によって示される)従業員の PC の **host-name** 属性に想定値が含まれて**いない**場合、その従業員のフル アクセス権限を拒否することができます。

一般的に、DHCP にはプロファイリング上の利点が多く、あらゆる環境においてエンドポイントの大部分を分類する基盤となります。これは、ほとんどのエンドポイントが、詳細なプラットフォーム情報を伴う DHCP「フィンガープリント」を提供するためです。

# DHCP プローブと DHCP SPAN プローブの設定

DHCP プローブを使用するには、プロファイリング サービス用に設定された ISE PSN に DHCP リレーまたは DHCP プロキシ パケットを送信するよう、アクセス デバイス（またはレイヤ 2 専用アクセス デバイスのネクスト ホップ ゲートウェイ）を設定する必要があります。DHCP SPAN プローブを使用するには、ネットワークにおいて、ネットワーク トラフィックのコピー（できれば DHCP だけを含むフィルタリングされたトラフィックのサブセット）を専用インターフェイス経由で ISE PSN に送信する必要があります。

どちらの DHCP ベースのプローブを有効にする場合も、もう 1 つの要件として、対象のエンドポイントが DHCP を使用して IP アドレスを取得する必要があります。これは明白に思えるかもしれませんが、お客様の多くが、静的 IP アドレス割り当てのクライアントレス デバイスを使用しています。そのような場合、エンドポイントが特定の IP アドレスを保持できるように静的 DHCP 予約を導入したうえで、IP アドレッシングの一元管理と DHCP 経由の ISE プロファイリングのサポートを可能にすることができます。

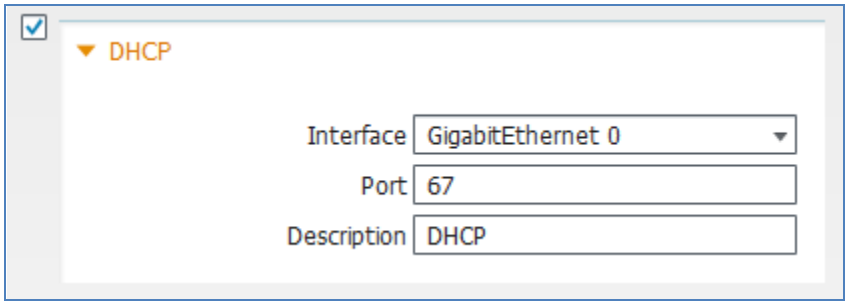
## ISE での DHCP プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択します。

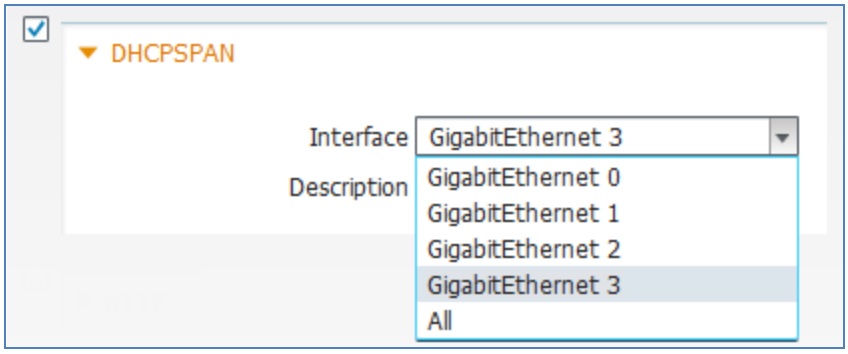
**ステップ 3** （たとえば IP ヘルパーと併用するために）DHCP プローブのサポートを追加するには、図 27 の左上に示すように、DHCP というラベルの付いたボックスをオンにします。

図 22 DHCP プローブの設定




**ステップ 4** （SPAN または他のポート ミラーリング ソリューションと併用するために）DHCP SPAN プローブのサポートを追加するには、DHCPSPAN というラベルの付いたボックスをオンにします（図 28）。

図 23 DHCP プローブの設定 - インターフェイス



**ステップ 5** DHCP トラフィックの収集に使用するインターフェイスを選択します。

IP ヘルパー（DHCP リレー）と併用する場合は、セッション サービスに使われるデフォルト インターフェイスがしばしば使用されます。しかし、大量の DHCP トラフィックが予想される大規模な環境では、専用のインターフェイス（GigabitEthernet 1、2、3 など）を使用することができます。

ミラーリング トラフィック（SPAN/RSPAN/タップ）と併用する場合は、これを専用のインターフェイスにする必要があります。

**ステップ 6** [保存（Save）] をクリックして、変更を確定します。

**ステップ 7** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

注：トラフィック ミラーリングの要件によっては、SPAN を受信する複数のポリシー サービス ノードを設定することが不可能または不適切な場合もあります。同じトラフィック フローをミラーリングする場合、同じトラフィックを複数のポリシー サービス ノードに転送するのは適切でないかもしれません。こうすると一定の冗長性が追加されますが、ISE ノードに対する負荷が大幅に増大し、その結果、他のノードに関連付けて同期させる必要のあるプロファイリング データの不要な重複が増加します。

### ISE（ネットワーク リソース）へのネットワーク デバイスの追加

RADIUS または SNMP をサポートするアクセス デバイスが（[管理（Management）] → [ネットワークリソース（Network Resources）] → [ネットワークデバイス（Network Devices）] で）ISE ネットワーク デバイスのリストにすでに追加されているとしても、DHCP を DHCP プローブまたは DHCP SPAN プローブに転送するためだけにネットワーク デバイスを ISE に追加する必要はありません。

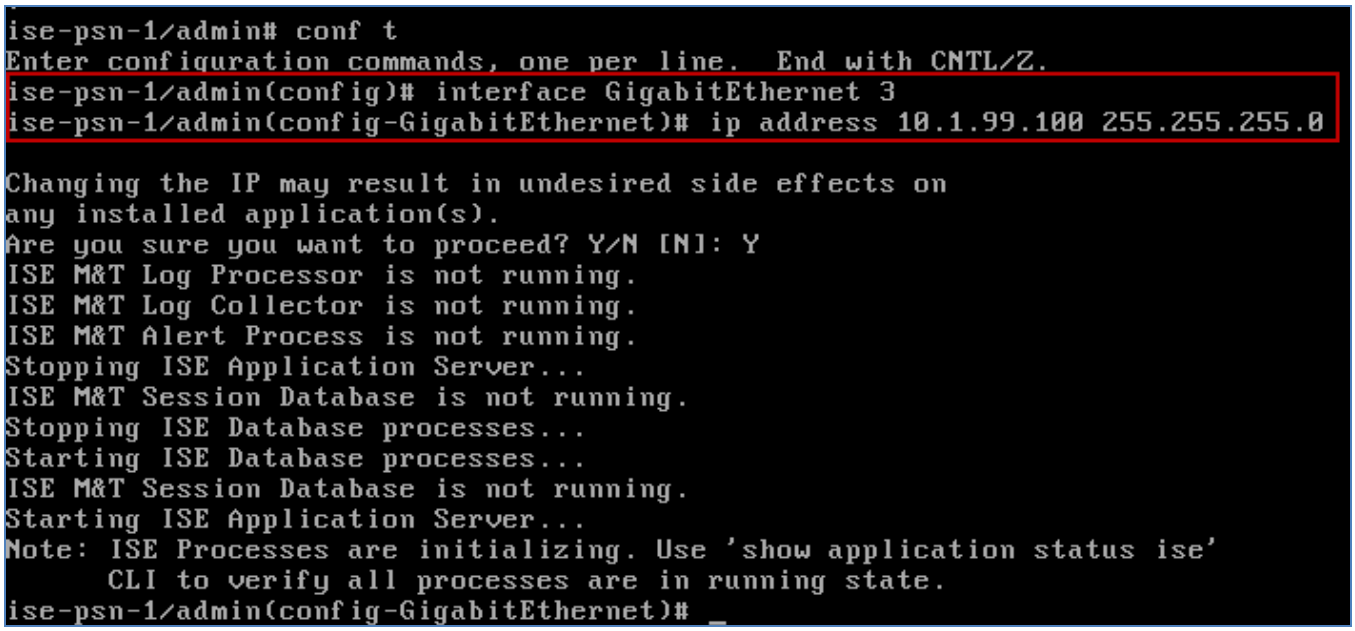
### DHCP リレー パケットを受信するための ISE ポリシー サービス ノード インターフェイスの設定（DHCP プローブのみ）

DHCP プローブがデフォルトの GigabitEthernet 0 インターフェイスで有効になっている場合は、この手順が完了しています。DHCP リレー トラフィックを受信するために別のインターフェイスを使用する必要がある場合は、次の手順を完了してください。

**ステップ 1** 該当するインターフェイスをネットワーク スイッチ ポートに物理的に接続します。

**ステップ 2** ISE PSN コンソール（CLI）にアクセスします。図 29 に示すように、該当するインターフェイスを有効にして、有効な IP アドレスを割り当てます。

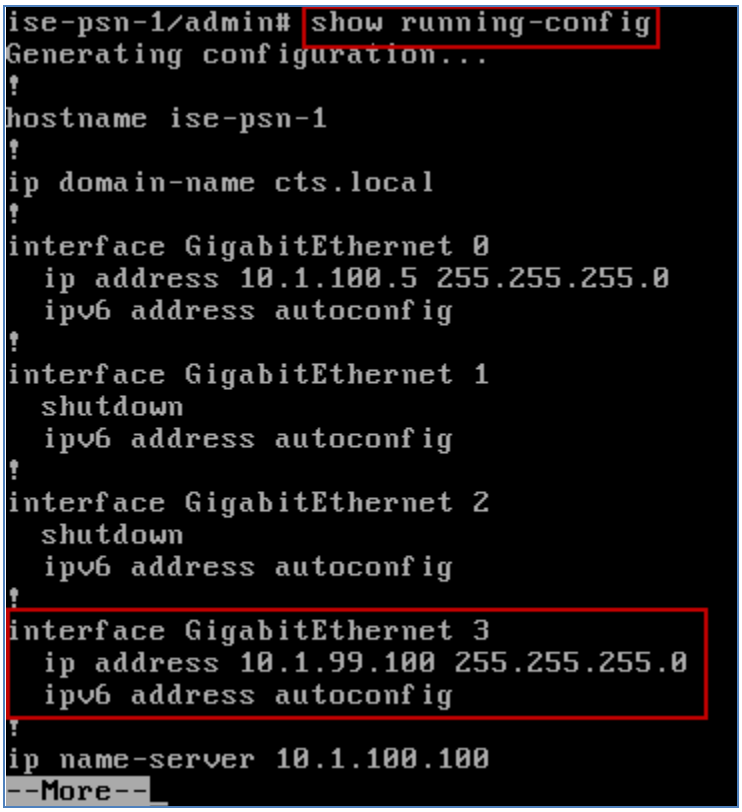
図 24 アクセス スイッチ用の DHCP リレー設定の例




**ステップ 3**　すべてのプロセスが、指示どおりの実行状態にあることを確認します。

**ステップ 4**　**show running-config** コマンドを使用して、新しく設定されたインターフェイスの設定を確認し、それが（シャットダウンではなく）有効になっていることを確認します（図 30）。

図 25 アクセス スイッチ用の DHCP リレー設定の確認




**ステップ 5** DHCP を中継する必要があるネットワーク デバイスから ICMP ping を送信することによって、新しい ISE プローブ インターフェイスへの接続を確認します。

**ステップ 6** CLI コマンド **copy running-config startup-config** を使用して変更を保存します。

## SPAN トラフィックを受信するための ISE ポリシー サービス ノード インターフェイスの設定（DHCP SPAN プローブのみ）

**ステップ 1** 該当するインターフェイスを適切な SPAN 宛先ポートまたはネットワーク タップ インターフェイスに物理的に接続します。

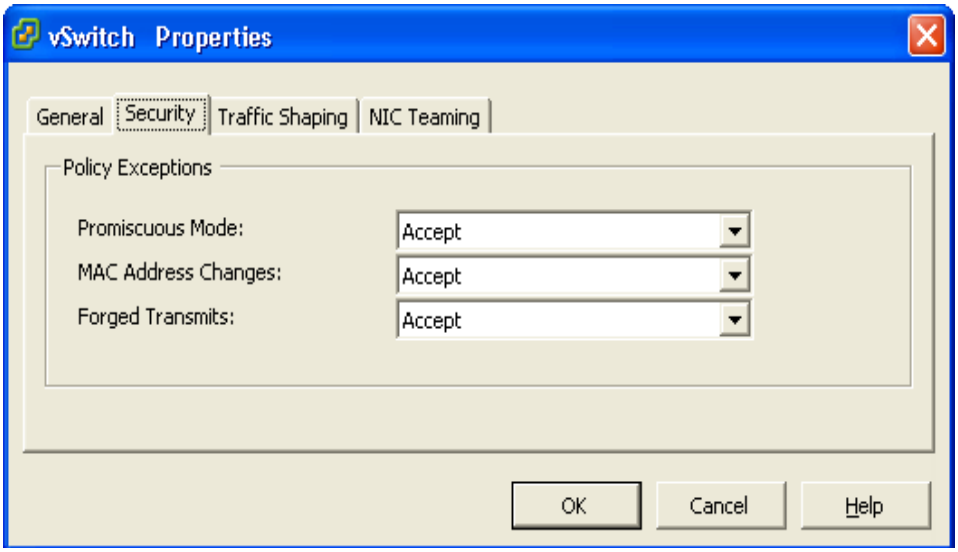
**ステップ 2** ISE PSN コンソール（CLI）にアクセスします。該当するインターフェイスのコンフィギュレーション モードで単に **no shutdown** を入力することで、適切なインターフェイスを有効にします。

**ステップ 3** ISE CLI コマンド **copy running-config startup-config** を使用して変更を保存します。

**注：VMWare アプライアンスで動作するポリシー サービス ノードの場合**

専用インターフェイスをプロファイリングに使用するには、追加の仮想インターフェイスが仮想アプライアンス用に設定されていることが想定されます。インストール時にこれが完了していない場合は、ISE 設定に進む前に、ISE ノードをシャットダウンして、必要なインターフェイス用に ESX アプライアンスのハードウェア設定とネットワーキング設定を更新する必要があります。

加えて、ISE DHCP SPAN インターフェイスで SPAN/ミラー トラフィックを受信するために、VMware アプライアンスでは、仮想スイッチ インターフェイスにおける無差別モードの設定が必要です。このモードを有効にするには、次のように、[VMwareホスト（VMware Host）] → [設定（Configuration）] → [ハードウェア（Hardware）] → [ネットワーク（Networking）] → [vSwitch（vSwitch）] → [セキュリティ（Security）] にアクセスして、[無差別モード（Promiscuous Mode）] を [許可（Accept）] に設定します（デフォルトは [拒否（Reject）]）。




## DHCP パケットを ISE PSN に中継するための有線アクセス デバイスの設定（DHCP プローブのみ）

Cisco Catalyst スイッチまたはルータの管理コンソールにアクセスします。DHCP トラフィックの起点となるエンドポイント サブネットに接続された各ルーテッド インターフェイスで、次のコマンドを追加します。

```
interface <Endpoint_VLAN>
  ip helper-address <ISE_PSN_address>
```

指定するアドレスは、DHCP プローブが有効化された PSN インターフェイスである必要があります。冗長性のために、DHCP を他のポリシー サービス ノードに中継するための IP ヘルパー ステートメントを追加できますが、これを最小限に抑えてトラフィックの重複を減らすことをお勧めします。これは、各 PSN が受信トラフィックを処理することになるためです。

## DHCP パケットを ISE PSN に中継するための無線アクセス デバイスの設定（DHCP プローブのみ）

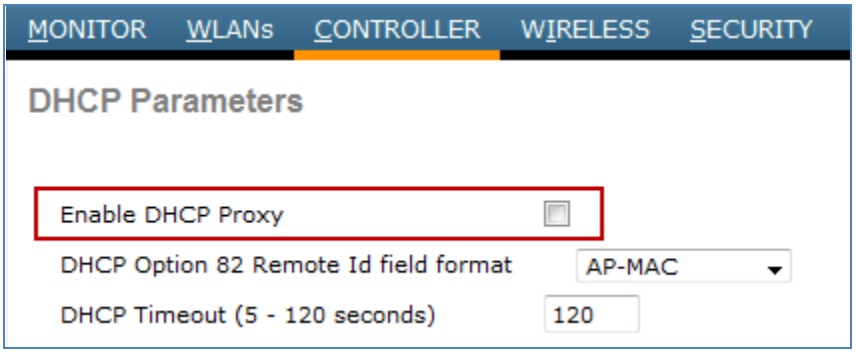
すべての DHCP パケットがワイヤレス クライアントから ISE PSN に転送されるようにするために、WLC を DHCP プロキシ モードではなく DHCP ブリッジ モードで設定することをお勧めします。

Cisco Wireless LAN Controller または Wireless Services Module の Web 管理インターフェイスにアクセスします。

**ステップ 1** [コントローラ（Controller）] → [詳細設定（Advanced）] → [DHCP（DHCP）] → [DHCPパラメータ（DHCP Parameters）] に移動します。

**ステップ 2** [DHCPプロキシを有効にする（Enable DHCP Proxy）] チェックボックスがオンになっている場合は、それをオフにします（図 31）。

図 26 ワイヤレス コントローラ用の DHCP リレー設定の例




**ステップ 3** DHCP を使って WLC で設定された WLAN ごとに、上記手順に従って、アップストリーム ゲートウェイが DHCP を ISE ポリシー サービス ノードに中継するように設定されていることを確認します。

## DHCP トラフィックのコピーを PSN に送信するためのネットワーク デバイスの設定（DHCP SPAN プローブのみ）

ISE ポリシー サービス ノードにトラフィックをミラーリングする方法は、複数あります。この手順では、Cisco Catalyst スイッチ上で基本的な SPAN を使用した一般的な方法を示します。

DHCP トラフィックの送信元となるインターフェイスまたは VLAN を決定します。WLC の出力インターフェイスや DHCP サーバへの接続などのチョークポイントは、すべてのクライアント DHCP パケットをキャプチャするための最適な場所になり得ます。

次の例では、インターフェイス GigabitEthernet 1/1 が Cisco 5500 シリーズ ワイヤレス LAN コントローラへのトランク接続です。インターフェイス GigabitEthernet 2/37 は、VMware ESXi 4.1 を実行している Cisco UCS® サーバへのスイッチポート接続です。ESX サーバは、プロファイリングが有効になっているポリシー サービス ノードとして設定された ISE 仮想アプライアンスをホストします。インターフェイス GigabitEthernet 2/37 は、ギガビット イーサネット 3 として ISE PSN にリンクされた仮想インターフェイスへのリンクです。

```
interface GigabitEthernet1/1
 description WLC5508 ETH0 (Port 1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 40-44
 switchport mode trunk

interface GigabitEthernet2/37
 description UCS1 SPAN (port 3 of 4)
 switchport
```

5500 シリーズ スイッチ接続ですべての着信/発信トラフィックをキャプチャして ISE PSN に転送するよう、SPAN を設定します。これを行うには、インターフェイス GigabitEthernet 1/1 を SPAN 送信元として設定し、インターフェイス GigabitEthernet 2/37 を宛先として設定します。ISE はタグ付きパケットを認識する必要がないため、スイッチポートで 802.1Q トランキングは有効化されません。

```
cat6500(config)# monitor session 1 source interface gigabitEthernet 1/1 both
cat6500(config)# monitor session 1 destination interface gigabitEthernet 2/37
```

設定を確認して保存します。

```
cat6500# show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi1/1
Destination Ports      : Gi2/37

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Centralized (default)
```

## DHCP プローブ データの確認

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

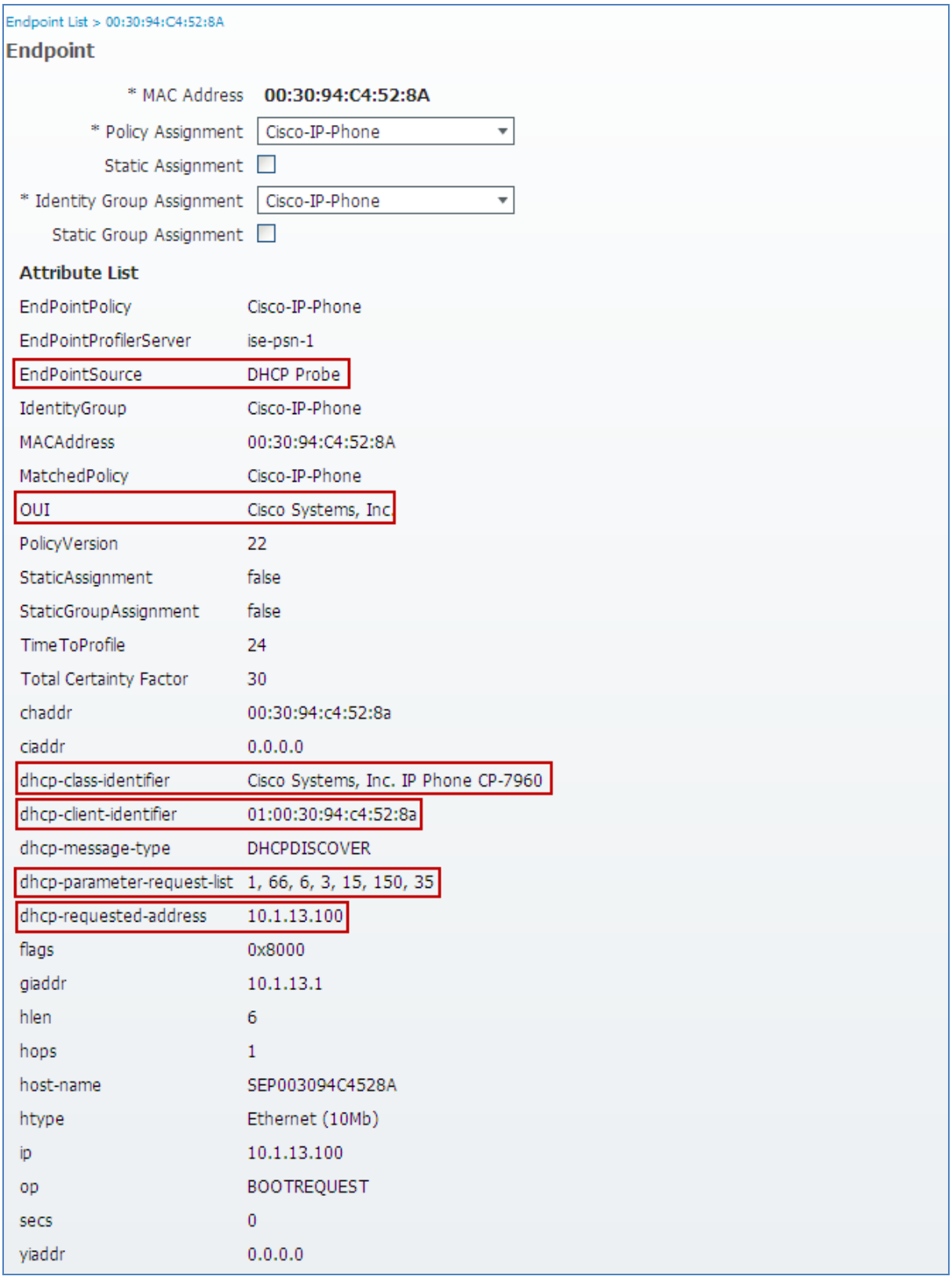
**ステップ 2** ゲートウェイ インターフェイスで DHCP を ISE PSN に転送する IP ヘルパーが使用されているアクセス デバイスから、エンドポイントを切断して再接続します。

**ステップ 3** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

**ステップ 4** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、DHCP プローブでキャプチャされた属性を表示します（図 32）。この例では、DHCP を使って収集された属性を強調表示するために DHCP プローブだけが使用されています。

図 27 DHCP プローブ属性の例



強調表示されるキー属性は次のとおりです。

- EndPointSource
- OUI
- dhcp-class-identifier
- dhcp-client-identifier
- dhcp-parameter-request-list
- dhcp-requested-address

**EndPointSource** は、DHCP プローブが最後の属性更新の送信元であることを示します。

**dhcp-client-identifier** は、通常、MAC アドレスを提供します。この MAC アドレスによって、MAC アドレス/OUI 間マッピング テーブル内の関連付けを通してベンダー OUI 情報が提供されます。

**dhcp-requested-address** は、エンドポイントから要求された IP アドレスです。これは **dhcp-client-identifier** とともに、IP アドレスと MAC アドレスの間のバインドを可能にします。

**dhcp-class-identifier** は多くの場合、一意のプラットフォーム固有の属性を提供し、さらに接続されたエンドポイントの詳しい説明（この例では Cisco Systems，Inc. IP Phone CP-7960）を提供することもあります。

また、**dhcp-parameter-request-list** もエンドポイントが Cisco IP Phone であることを示します。これは、正確なシーケンス 1、66、6、3、15、150、35、151 が通常、特定の Cisco IP Phone でのみ使用されるためです。

要約すると、DHCP を使用して 1 つ以上の属性でネットワーク エンドポイントを分類できます。後述する「デバイス センサー」の項に記載されているように、デバイス センサーと呼ばれるローカル分類テクノロジーを使用して DHCP などの情報を収集するための機能が提供されています。この機能は、IP ヘルパーまたは SPAN テクニックを通して収集できない場合でも DHCP 属性を収集できるようにします。このソリューションは、エンドポイント属性の収集と分類のための非常にスケーラブルな手法を提供します。

## HTTP プローブを使用したプロファイリング

Web ブラウザは通常、固有の識別文字列を Web サーバに送信することによって自身を識別します（アプリケーション タイプ、オペレーティング システム、ソフトウェア ベンダー、およびソフトウェア リビジョンなど）。HTTP では、これが **User-Agent** という名前の HTTP 要求ヘッダー フィールド で送信されます。

**User-Agent** は、HTTP プローブを使用して収集されるプライマリ属性です。ISE プロファイリングは、**User-Agent** 属性から Web ブラウザ情報を収集し、要求メッセージからその他の HTTP 属性をキャプチャして、それらをエンドポイント属性のリストに追加します。Cisco ISE は複数のデフォルト プロファイルを備えています。これらのプロファイルはシステムに組み込まれており、**User-Agent** 属性に基づいてエンドポイントを識別します。

HTTP トラフィックを HTTP プローブに送信するために次の 2 つの方法が使用されます。

- URL リダイレクション
- SPAN（および他のトラフィック ミラーリング方式）

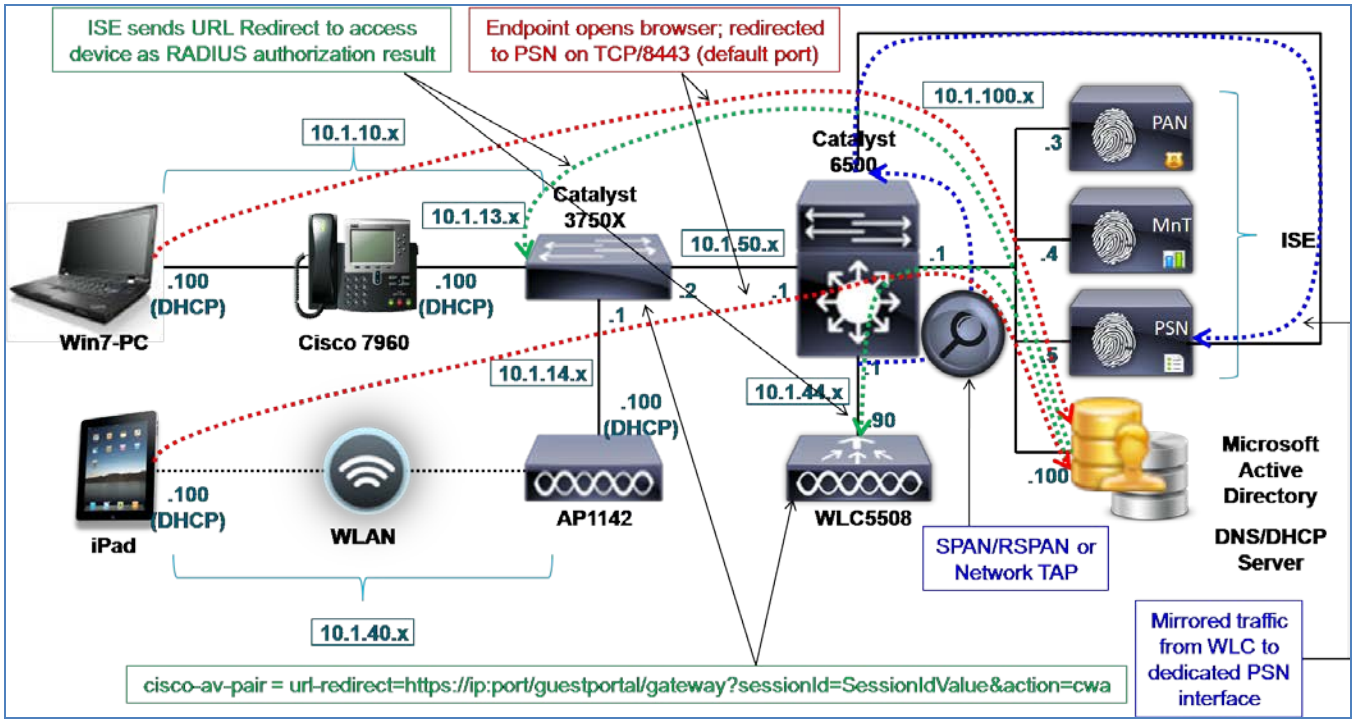
HTTP プローブは、ポート 80 とポート 8080 の両方で Web ブラウザからの通信をリッスンします。URL リダイレクション方式と SPAN 方式のどちらも **User-Agent** 属性を HTTP プローブに提供します。

## URL リダイレクションを使用した HTTP プローブ

ISE は、Central WebAuth（CWA）、Local WebAuth（LWA）、Device Registration WebAuth（DRW）、クライアント プロビジョニング、ポスチャ アセスメント、およびネイティブ サプリカント プロビジョニング（NSP）を含むさまざまなユーザ セッション サービスに URL リダイレクションを使用します。これらすべてのユースケースで、エンドポイントの Web ブラウザが ISE ポリシー サービス ノードにリダイレクトされます。このプロセス中に、ISE は **User-Agent** 属性をキャプチャすることができます。

図 33 のサンプル トポロジでは、エンドポイントの初期認可の一部として URL リダイレクションが使用され、ISE は URL リダイレクトをアクセス デバイスに送信できます（図 33 では緑色で強調表示）。クライアントが Web ブラウザを開くと、Central WebAuth などの指定されたサービスのポリシー サービス ノードにリダイレクトされます（赤色で強調表示）。

図 28 HTTP プローブの例




URL リダイレクションを、ネットワーク アクセス デバイス（NAD）の機能にすることができます。NAD 開始リダイレクトの例が Local WebAuth です。これにより、有線スイッチまたはワイヤレス コントローラがクライアントのブラウザを ISE ゲスト ポータルにリダイレクトして Web 認証ページが表示されます。

また、ISE からネットワーク アクセス デバイスへの RADIUS 認可として URL リダイレクションを開始することもできます。RADIUS 認可によってトリガーされる URL リダイレクトの例が Central WebAuth です。この場合、アクセス デバイスはリダイレクションを支援しますが、実際のセッションはクライアントと ISE ポリシー サービス ノード間で確立され、一意のセッション ID を介して追跡されます。

## SPAN を使用した HTTP プローブ

URL リダイレクションを使わずに HTTP プローブを使用するオプションとして、SPAN、RSPAN、ネットワーク タップなどの方式を使用して ISE ポリシー サービス ノード上のインターフェイスに Webトラフィックをコピーまたはミラーリングすることもできます。この方法は主に、URL リダイレクションが不適切または不可能な場合に使用されます。

**ベスト プラクティス**：RADIUS ベースの環境などのように、URL リダイレクション方式が HTTP SPAN よりも適切な場合があります。リダイレクション中にキー **User-Agent** 属性だけをキャプチャすることにより、HTTP パケットからの属性を検査して解析するための ISE ポリシー サービス ノード上の全体的なトラフィック負荷が減少します。

RADIUS ベースの認証を使用しない Cisco NAC アプライアンス展開や、RADIUS をこれからアクセス デバイスに展開するエンドポイント ディスカバリ フェーズなど、URL リダイレクションが適用されない場合には、RADIUS/URL リダイレクションを要件とせずに **User-Agent** をキャプチャできる SPAN 方式が適切です。

図 33 のサンプル トポロジは、SPAN またはネットワーク タップを使用して、WLC に接続されたワイヤレス クライアントからポリシー サービス ノード上の専用インターフェイスにパケットをコピーする方法を示しています（青色で強調表示）。PSN 宛ての通常のトラフィックの送受信を制限する特殊なプロパティが SPAN 宛先ポートで設定される場合があるため、専用のインターフェイスが必要です。加えて、ミラーリング トラフィックによって、RADIUS などの他の重要な PSN のインターフェイスで輻輳が発生しないようにする必要があります。SPAN 方式を使用した場合、SPAN ポートの処理能力を上回る大量のデータが送られて、パケット ドロップや重要なトラフィックの遅延が生じる可能性があります。

## HTTP プローブと IP/MAC アドレス間バインドの要件

HTTP トラフィックにはエンドポイントの MAC アドレスが含まれないため、HTTP プローブに送信されるデータを正しく関連付けるには、ISE ポリシー サービス ノードでエンドポイントの ARP キャッシュ テーブルに IP/MAC アドレス間バインドが設定済みであることが重要です。つまり、エンドポイントで MAC アドレスによって ISE を認識できない場合、または、関連する IP アドレスが存在しない場合は、HTTP プローブによって学習されたプロファイリング データが破棄されます。これは、学習された **User-Agent** 属性を適用可能なエンドポイントが存在しないためです。その結果、HTTP データを収集する**前**に、別のプローブを介して IP/MAC アドレス間バインドを学習する必要があります。この情報を提供するために使用可能なプローブには、以下が含まれます。

- RADIUS（**Framed-IP-Address** 属性を介して）
- DHCP（**dhcp-requested-address** 属性を介して）
- SNMP クエリ（SNMP ポーリングを介して）

IP/MAC 間バインド要件の例外となる特殊な HTTP プロファイリング シナリオがあります。これには次が含まれます。

- クライアント プロビジョニングを使用した URL リダイレクション
- Central WebAuth を使用した URL リダイレクション

## クライアント プロビジョニングを使用した URL リダイレクション

クライアント プロビジョニング（CP）は、エンドポイントにエージェントおよびコンフィギュレーション ファイルの動的ダウンロードを提供することによって、ポスチャ エージェントとネイティブ サプリカント プロビジョニング（NSP）サービスを可能にする ISE セッションです。クライアント プロビジョニングは URL リダイレクションに依存します。CP プロセス中に、適用するプロビジョニング ポリシーを識別するために、ポリシー サービス ノードはユーザ エージェントを介してクライアント OS を判別する必要があります。たとえば、エンドポイントが Windows クライアントと検出された場合、ポスチャ サポート用に Windows ポスチャ エージェントを選択する必要があります。同様に、エンドポイントが Android クライアントと検出された場合は、Android クライアント用のサプリカント プロビジョニング ファイルをエンドポイントにインストールする必要があります。

クライアント プロビジョニング サービスが **User-Agent** 属性を学習すると、ISE はこの情報でプロファイリング サービスを更新することによってこの知識を利用します。加えて、クライアント プロビジョニングはアクティブ セッションの一部であるため、ISE はセッション キャッシュから取得された MAC アドレス（**Calling-Station-ID**）にこの情報を適用できます。そのため、このプロセスだけを使用して、多数のエンドポイントを完全にプロファイリングすることができます。

## Central WebAuth を使用した URL リダイレクション

Central WebAuth（CWA）は URL リダイレクションに依存します。CWA プロセス中に、HTTP プローブは、ポリシー サービス ノードでの復号化後にリダイレクトされた HTTPS パケットから **User-Agent** 属性をキャプチャできます。クライアント プロビジョニング サービスと同様に、ゲスト フローはアクティブ セッションの一部であり、ISE はそのセッション キャッシュから MAC アドレス（**Calling-Station-ID**）を取得できます。このプロセスにより HTTP プローブは、エンドポイント データベースへの格納に必要な **User-Agent** および関連する MAC アドレスを学習できます。

一般的に、HTTP プローブは、**User-Agent** を介してクライアント OS タイプを検出するための高い忠実度を備えています。オペレーティング システムに基づくポリシーが必要な場合には、HTTP プローブが推奨されます。特に、エンドポイントが個人資産か企業資産かに基づいて差別化したアクセスを提供しなければならない無線環境の場合です。

両方のシナリオ（つまり CP を使用した URL リダイレクトと CWA を使用した URL リダイレクト）において、ISE は、既存の IP/MAC アドレス間バインドがなくても **User-Agent** 属性を MAC アドレスに適用できます。HTTP SPAN 方式では常に、既存の IP/MAC 間バインド エントリが必要です(ただしエンドポイントに隣接したレイヤ 2 のセグメントからミラーリング トラフィックが取得される場合を除きます)。この特殊なケースでは、パケット送信元 MAC アドレスが実際のエンドポイントのアドレスであるため、エンドポイント データベースの更新にそれを使用できます。

**ベスト プラクティス**：**User-Agent** を取得するには、CWA ユースケースの HTTP プローブと一緒に URL リダイレクションを使用します。ポスチャ エージェントまたはネイティブ サプリカント プロビジョニング サービスが必要な場合、クライアント プロビジョニングと一緒に URL リダイレクションを使用するプロファイリングが自動的に処理されますが、ポスチャまたはサプリカント プロビジョニングが必要でない場合でも意図的に CP をトリガーするのが適切なことがあります。これを行うには、エンドポイント プロファイルが不明/不完全と設定されている場合のクライアント プロビジョニングおよびポスチャ（CPP）サービス（ポスチャ ディスカバリ）へのリダイレクション、または（ポスチャ エージェントが有効になっている）CWA へのリダイレクションを使用できます。この目的は、プロセス内で **User-Agent** をキャプチャし、結果のポスチャ ステータスで認可変更（CoA）をトリガーできるようにすることです。再接続時に、より精緻なプロファイル照合に基づいて新しい認可ポリシー ルールを割り当てることができます。

前述したように、通常は HTTP SPAN よりも URL リダイレクションが推奨されます。後者の場合、パケット ミラーリング方式に比べて最小限のトラフィック負荷でポリシー サービス ノードが **User-Agent** 属性を取得できることに加えて、一部の特殊なケースでは、最初に ARP キャッシュを生成しなくてもプロファイリングが可能になるためです。さらに、RADIUS 認可に基づく URL リダイレクションでは、RADIUS トラフィックを終了させた同じ PSN にリダイレクトが常に送信されるため、ハイ アベイラビリティ シナリオが単純化されます。

ただし、RADIUS が展開されていないアクセス デバイスなど、SPAN 方式が唯一の現実的なオプションである場合もあります。

# HTTP プローブの設定

リダイレクトされたトラフィックと一緒に HTTP プローブを使用するには、アクセス デバイスが直接（Local WebAuth 経由など）または RADIUS 認可経由で ISE に HTTP トラフィックをリダイレクトできる必要があります。RADIUS ベースのリダイレクションでは、認可結果として **url-redirect** のシスコ属性/値ペア（AVP）を返す認可ポリシー ルールが ISE で設定される必要があります。

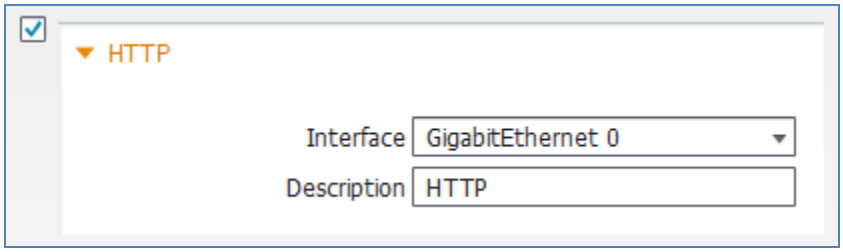
SPAN と一緒に HTTP プローブを使用するには、ネットワークにおいて、ネットワークトラフィックのコピー（できれば HTTP だけを含むフィルタリングされたトラフィックのサブセット）を専用インターフェイス経由で ISE PSN に送信する必要があります。

## ISE での HTTP プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択します。HTTP プローブのサポートを追加するには、HTTP というラベルの付いたボックスをオンにします（図 34）。

図 29 HTTP プローブの設定

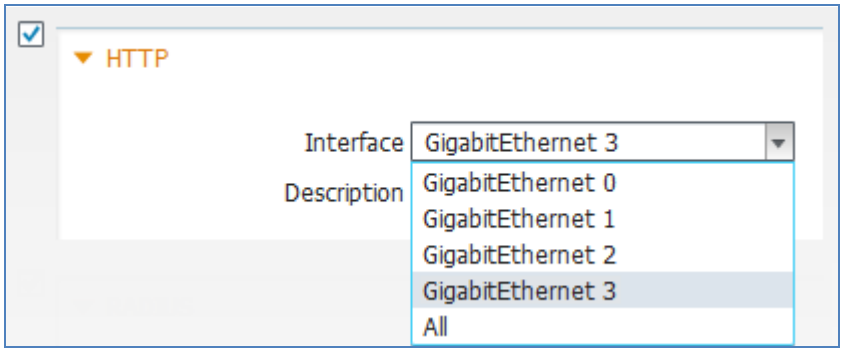



**ステップ 3** HTTP トラフィックの収集に使用するインターフェイスを選択します。

**ステップ 4** URL リダイレクションと一緒に使用するには、使用するインターフェイスを GigabitEthernet 0（つまり RADIUS、Web 認証、ポスチャなどのセッション サービスに使用されるものと同じインターフェイス）にする必要があります。

**ステップ 5** ミラーリング トラフィック（SPAN/RSPAN/タップ）と一緒に使用する場合は、これを専用インターフェイスにする必要があります（図 35）。

図 30 HTTP プローブの設定 - インターフェイス



**ステップ 6** [保存(Save)] をクリックして、変更をコミットします。
**ステップ 7** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

注:トラフィック ミラーリングの要件によっては、SPAN を受信する複数のポリシー サービス ノードを設定することが不可能または不適切な場合があります。同じトラフィック フローをミラーリングする場合は、同じトラフィックを複数のポリシー サービス ノードに転送するのは適切でないかもしれません。こうすると一定の冗長性が追加されますが、ISE ノードに対する負荷が大幅に増大し、その結果、他のノードに関連付けて同期させる必要のあるプロファイリング データの不要な重複が増加します。

## ISE(ネットワーク リソース)へのネットワーク デバイスの追加

HTTP データのキャプチャに URL リダイレクションが使用されている場合は、RADIUS ベースの認証をサポートするようにネットワーク アクセス デバイスを設定しておく必要があるため、ネットワーク アクセス デバイスを追加または編集する追加の手順は必要ありません。

HTTP データのキャプチャに SPAN 方式が使用されている場合、RADIUS ベースの認証が実行されていなければ、アクセス デバイスを ISE に追加する必要はとくにありません。

## リダイレクトされた HTTP トラフィックを受信するための ISE ポリシー サービス ノード インターフェイスの設定

URL リダイレクションが使用されている場合は、デフォルトの GigabitEthernet 0 インターフェイス上で HTTP プローブを有効にする必要があります。そのため、追加的なのインターフェイス設定は必要ありません。

## HTTP SPAN トラフィックを受信するための ISE ポリシー サービス ノード インターフェイスの設定

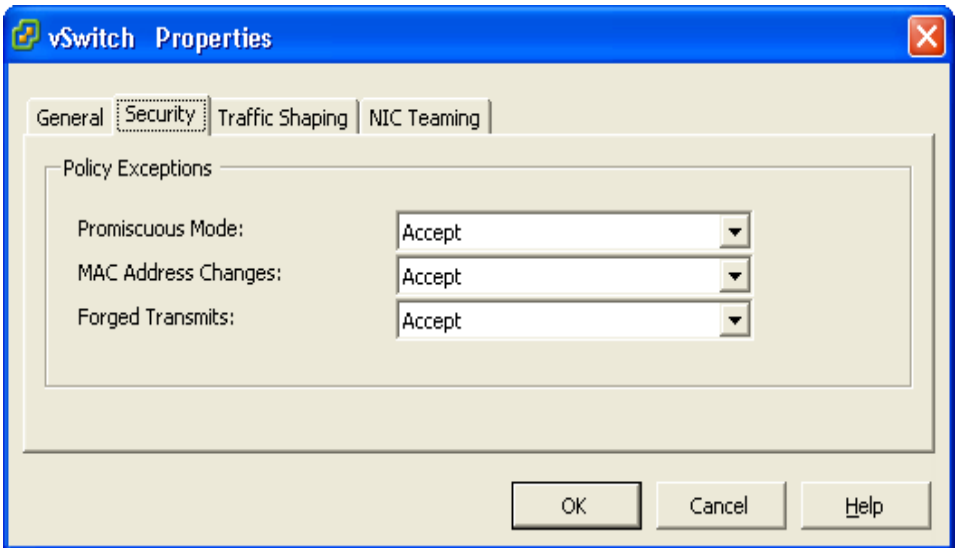
SPAN が使用されている場合は、HTTP トラフィックを受信するための専用 SPAN インターフェイス上で HTTP プローブを設定する必要があります。ISE 上で専用 SPAN インターフェイスを設定するには、次の手順を実行します。

**ステップ 1** 該当するインターフェイスを適切な SPAN 宛先ポートまたはネットワーク タップ インターフェイスに物理的に接続します。
**ステップ 2** ISE PSN コンソール(CLI)にアクセスします。該当するインターフェイスのコンフィギュレーション モードで単に **no shutdown** を入力することで、適切なインターフェイスを有効にします。
**ステップ 3** ISE CLI コマンド **copy running-config startup-config** を使用して変更を保存します

**注:VMWare アプライアンスで動作するポリシー サービス ノードの場合**

専用インターフェイスをプロファイリングに使用するには、追加の仮想インターフェイスが仮想アプライアンス用に設定されていることが想定されます。インストール時にこれが完了していない場合は、ISE 設定に進む前に、ISE ノードをシャットダウンして、必要なインターフェイス用に ESX アプライアンスのハードウェア設定とネットワーキング設定を更新する必要があります。

加えて、ISE DHCP SPAN インターフェイスで SPAN/ミラー トラフィックを受信するために、VMware アプライアンスでは、仮想スイッチまたはインターフェイスにおける無差別モードの設定が必要です。このモードを有効にするには、次のように、[VMwareホスト(VMware Host)] → [設定(Configuration)] → [ハードウェア(Hardware)] → [ネットワーク(Networking)] → [vSwitch(vSwitch)] → [セキュリティ(Security)] にアクセスして、[無差別モード(Promiscuous Mode)] を [許可(Accept)] に設定します(デフォルトは [拒否(Reject)])。




## HTTP パケットを ISE PSN にリダイレクトするための有線アクセス デバイスの設定

CWA、ポスチャ、サプリカント プロビジョニングなど、特定のサービス用に URL リダイレクトをサポートするアクセス デバイスの設定は、このマニュアルでは扱いません。要約すると、Cisco Catalyst スイッチを使用した RADIUS 認可に基づくリダイレクションをサポートするために、次のようなコマンドが必要になります。

- グローバル コンフィギュレーション モードで、HTTP サーバ（およびオプションで HTTPS サーバ）を有効にします。
- リダイレクション対象となるトラフィックを指定するために ISE RADIUS 認可で参照されるリダイレクト ACL を設定します。

```
ip http server
ip http secure-server
ip access-list extended REDIRECT-ACL
  deny tcp any any <PSN_IP_address>
  permit tcp any any eq http
  permit tcp any any eq https
```

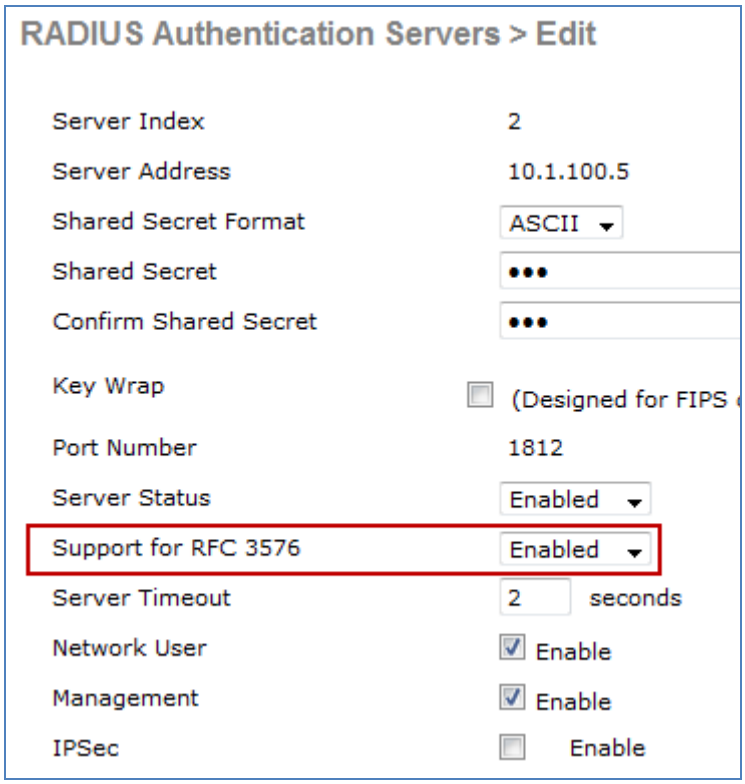
クライアントで開始されるトラフィックに関しては、HTTP トラフィックと HTTPS トラフィックの両方のリダイレクションを Catalyst スイッチでサポートできます。ISE にリダイレクトされるトラフィックは、常に HTTPS です。

## HTTP パケットを ISE PSN にリダイレクトするための無線アクセス デバイスの設定

CWA、ポスチャ、サプリカント プロビジョニングなどの特定のサービス用に URL リダイレクトをサポートするアクセス デバイスの設定は、このマニュアルでは扱いません。要約すると、ワイヤレス LAN コントローラを使用した RADIUS 認可に基づくリダイレクションをサポートするために、次の例ような手順が必要になります。

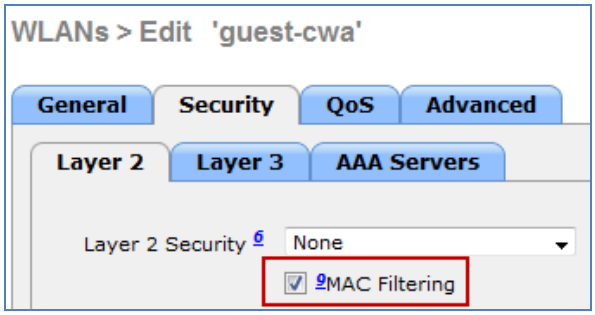
**ステップ 1** [セキュリティ（Security）] → [AAA（AAA）] → [RADIUS（RADIUS）] → [認証（Authentication）] → [（RADIUS サーバ）] → [編集（Edit）] で、[RFC 3576のサポート（Support for RFC 3576）] が [有効（Enabled）] に設定されていることを確認します（図 36）。

図 314 ワイヤレス コントローラ用の CoA 設定の例



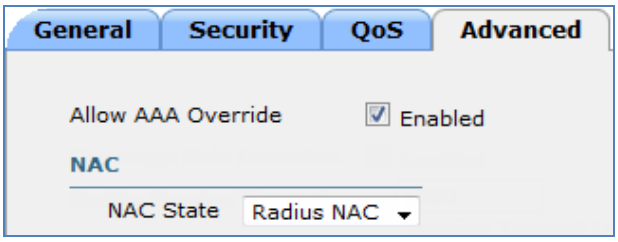

**ステップ 2** [WLAN（WLAN）] → [WLANの編集（Edit (WLAN)）] → [セキュリティ（Security）] → [レイヤ2（Layer 2）] で、MAC フィルタリング用に WLAN を設定します。[レイヤ2セキュリティ（Layer 2 Security）] と [レイヤ3セキュリティ（Layer 3 Security）] を [なし（None）] に設定する必要があります（図 37）。

図 32 ワイヤレス コントローラ用の MAC フィルタリング設定の例




**ステップ 3** [詳細設定（Advanced）] タブで、[AAAオーバーライドを許可する（Allow AAA Override）] をオンにして、[NACの状態（NAC State）] を [RADIUS NAC] に設定します（図 38）。

図 33 ワイヤレス コントローラ用の RADIUS 認可設定の例




クライアントで開始されるトラフィックに関しては、HTTP トラフィックのみのリダイレクションが Cisco Wireless LAN Controller でサポートされます。HTTPS トラフィックのリダイレクションはサポートされません。ISE にリダイレクトされるトラフィックは、常に HTTPS です。

## RADIUS 認可として URL リダイレクションを実行するための ISE の設定

CWA、ポスチャ、サプリカント プロビジョニングなどの特定のサービス用に URL リダイレクトをサポートする ISE の設定は、このマニュアルでは扱いません。要約すると、ISE 認可ポリシーで RADIUS 認可に基づくリダイレクションをサポートするために、次の例ような手順が必要になります。

**ステップ 1** ISE 管理インターフェイスで、[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] にアクセスします。

**ステップ 2** 図 39 に示すように、LHS ペインで [認証（Authorization）] → [認可プロファイル（Authorization Profiles）] の順に選択してから、RHS ペインで [追加（Add）] をクリックして **Posture_Remediation** という名前の新しい認可プロファイルを追加します。

図 34 URL リダイレクション用の認可プロファイルの設定例

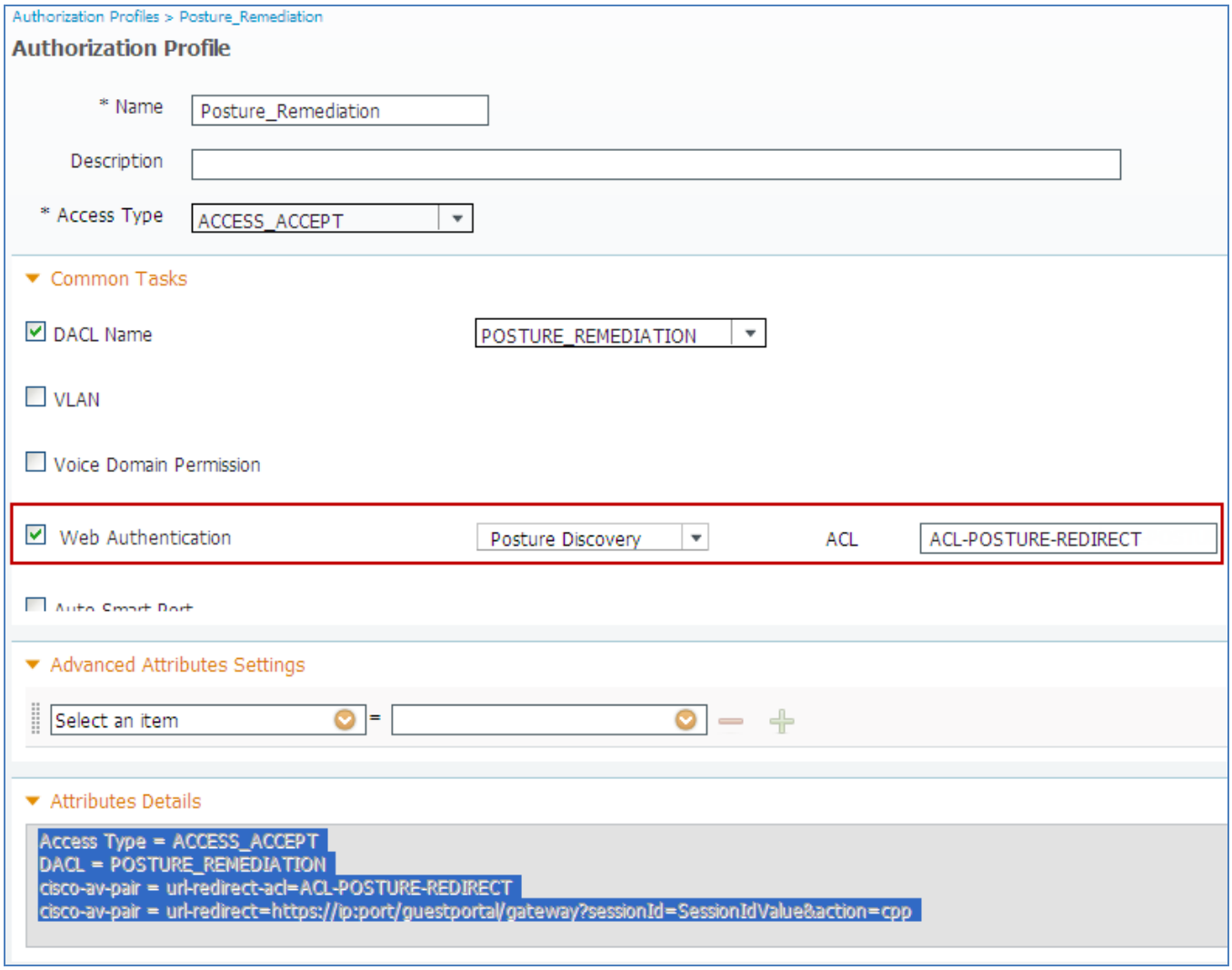



図 39 に示す例では、ポスチャ ディスカバリとして選択された特定のリダイレクトと一緒に、Web Authentication というラベルの付いた共通タスクが選択されています。これにより、エンドポイントがクライアント プロビジョニングおよびポスチャ サービス(または CPP)にリダイレクトされることになります。リダイレクト ACL は ACL-POSTURE-REDIRECT であり、アクセス デバイスで事前設定される必要があります。結果の RADIUS 認可が青色で強調表示されています。

**ステップ 1** [ポリシー(Policy)] → [認証(Authorization)] にアクセスして、**Employee_PreCompliant** という名前の認可ポリシー ルールを追加します。このルールは、使用されているデバイス タイプがワークステーションでも Apple iPad でもない従業員用の新しい認可プロファイルを使用します(図 40を参照)。

図 35 URL リダイレクション用の認可ポリシー ルールの例

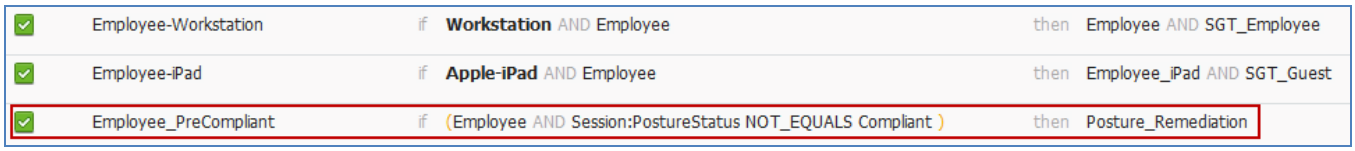



図 40 の例では、**Employee_PreCompliant** というラベルの付いたルールを意図的に以前のルールの**後ろ**に配置しています。これにより、従業員がネットワークに接続し、デバイス タイプが明示的エンドポイント ID グループ **Workstation** または **Apple-iPad** のいずれにも一致しない場合にのみ、そのルールが照合されます。認証された従業員が Employee_PreCompliant ルールに適合すると、**Posture_Redirection** という名前の認可プロファイルが割り当てられます。これにより、RADIUS 認証がアクセス デバイスに返され、クライアント プロビジョニングおよびポスチャ サービスへの URL リダイレクションが実行されます。

## HTTP トラフィックのコピーを ISE PSN に送信するためのネットワーク デバイスの設定

ISE ポリシー サービス ノードにトラフィックをミラーリングする方法は複数あります。この手順では、Cisco Catalyst スイッチ上で VACL キャプチャを使用する一般的な方法を示します。この方法には、該当する特定のトラフィックだけを ISE ポリシー サービス ノードに転送できるという利点があります。

**ベスト プラクティス**：必要なトラフィックだけを ISE プローブに送信するフィルタを使用したスケーラブルなトラフィック ミラーリングをサポートするインテリジェント タップ システムが利用可能な場合は、それを使用してください。これには、SPAN 方式を使用してプロファイリング データを取得する DHCP SPAN プローブと HTTP プローブが含まれます。より高度なタップ システムは、ミラーリング トラフィックのハイ アベイラビリティをサポートします。

または、ローカル スイッチ上の VACL キャプチャや、RSPAN と組み合わせた VACL キャプチャ/リダイレクトなど、インテリジェントな SPAN テクニックがインフラストラクチャでサポートされていれば、それを利用してネットワーク トラフィックを選択的にキャプチャすることもできます。

DHCP トラフィックの送信元となるインターフェイスまたは VLAN を決定します。WLC の出力インターフェイスや DHCP サーバへの接続などのチョークポイントは、すべてのクライアント DHCP パケットをキャプチャするための最適な場所になり得ます。

次の例では、VLAN 40 ～ 44 が Cisco Wireless LAN Controller 5500 シリーズにトランクされています。GigabitEthernet 2/37 は、VMware ESXi 4.1 を実行している Cisco UCS サーバへのスイッチポート接続です。ESX サーバは、プロファイリングが有効になっているポリシー サービス ノードとして設定された ISE 仮想アプライアンスをホストします。インターフェイス GigabitEthernet 2/37 は、ギガビット イーサネット 3 として ISE PSN にリンクされた仮想インターフェイスへのリンクです。

```
interface GigabitEthernet1/1
 description WLC5508 ETH0 (Port 1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 40-44
 switchport mode trunk

interface GigabitEthernet2/37
 description UCS1 SPAN (port 3 of 4)
 switchport
```

**ステップ 2**　VLAN 40 ～ 44 上のすべての HTTP トラフィックを照合して ISE PSN 接続に転送するよう、VACL キャプチャを設定します。

**ステップ 3** 次のように、HTTP トラフィックのみを照合する ACL と、すべての IP トラフィックを照合する別の ACL を設定します。

```
cat6500(config)# ip access-list extended HTTP_TRAFFIC
cat6500(config-ext-nacl)# permit tcp any any eq www

cat6500(config)# ip access-list extended ALL_TRAFFIC
cat6500(config-ext-nacl)# permit ip any any
```

**ステップ 4** HTTP_TRAFFIC ACL と一致するトラフィック上のキャプチャ ビットを設定するシーケンスを使って VLAN アクセス マップを設定します。(ALL_TRAFFIC ACL と一致する)他のすべてのトラフィックを転送する、同じ VLAN アクセス マップ内の別のシーケンスを設定します。

```
cat6500(config)# vlan access-map HTTP_MAP 10
cat6500(config-access-map)# match ip address HTTP_TRAFFIC
cat6500(config-access-map)# action forward capture

cat6500(config)# vlan access-map HTTP_MAP 20
cat6500(config-access-map)# match ip address ALL_TRAFFIC
cat6500(config-access-map)# action forward
```

**ステップ 5** 次のように、VLAN 40、41、42、および 43 に VLAN アクセス マップを適用する VLAN フィルタを設定します。

```
cat6500(config)# vlan filter HTTP_MAP  vlan-list 40-43
```

**ステップ 6** 次のように、アップストリーム VLAN 100 にルーティングされるトラフィックを含む VLAN 40、41、42、および 43 上の一致するすべてのトラフィックを含めるよう、キャプチャ ポート(Gi2/37)を設定します。

```
cat6500(config)# int Gi2/37
cat6500(config-if)# switchport capture allowed vlan 40-43,100
cat6500(config-if)# switchport capture
```

## URL リダイレクションを使用した HTTP プローブ データの確認(CWA の例)

**ステップ 1** [管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] → [エンドポイント(Endpoints)] からエンドポイントを削除します。

**ステップ 2** ISE PSN への HTTP リダイレクションをサポートするように設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

**ステップ 3** Web 認証を使用してエンドポイントからログインします。

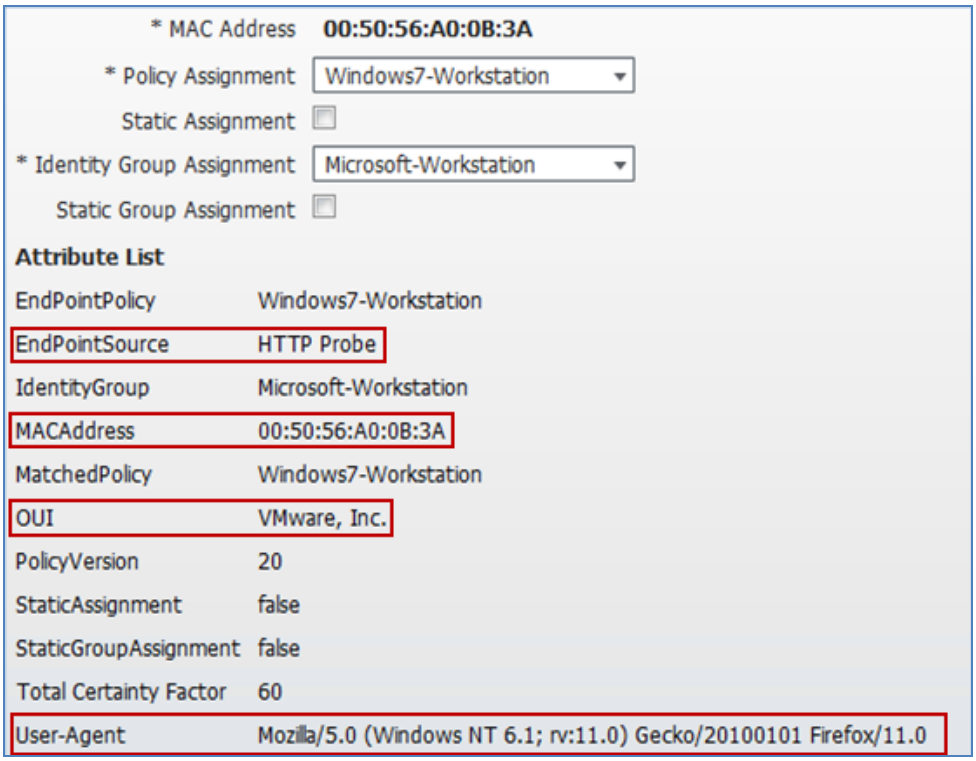
**ステップ 4** ISE ポリシー管理ノードにアクセスして、[管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] に移動します。

**ステップ 5** LHS ペインで、[エンドポイント(Endpoints)] を選択します。

**ステップ 6** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、HTTP プローブによってキャプチャされた属性を表示します。

図 41 の例では、URL リダイレクションを使って収集された属性を強調表示するために HTTP プローブだけが使用されています。

図 36 URL リダイレクションを使用した HTTP プローブ属性 - CWA の例




強調表示されるキー属性は次のとおりです。

- EndPointSource
- MACAddress
- OUI
- User-Agent

この例では、URL リダイレクションを使って収集された属性を強調表示するために HTTP プローブだけが使用されています。この特別なシナリオでは、IP/MAC アドレス間バインドを使用しなくてもエンドポイントを内部エンドポイントデータベースに追加できます。

**EndPointSource** は、最新の属性更新のソースが HTTP プローブであることを示します。

**MACAddress** は、セッション キャッシュから取得された値です。

**OUI** は、**MACAddress** 値から得られます。

**User-Agent** は、この VMware ベースのクライアントが Windows 7 オペレーティング システムを実行していることを示す重要なデータ ポイントです。

## URL リダイレクションを使用した HTTP プローブ データの確認（クライアント プロビジョニングの例）

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

**ステップ 2** ISE PSN への HTTP リダイレクションをサポートするように設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

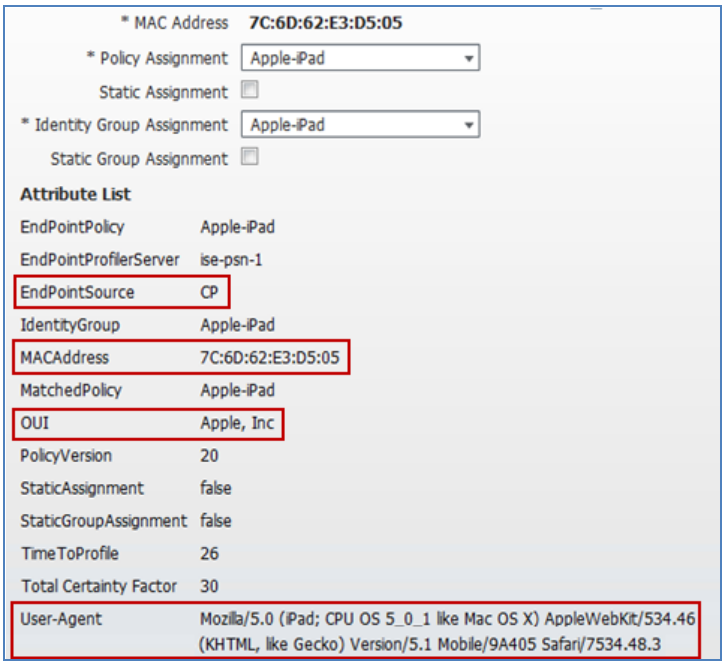
**ステップ 3** エンドポイントからログインを試みます。

**ステップ 4** [管理（Administration）] → [ID 管理（Identity Management）] → [ID（Identities）] に移動して、LHS ペインで [エンドポイント（Endpoints）] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、クライアント プロビジョニング サービスによってキャプチャされた属性を表示します。

**ステップ 6** 図 42 の例は、プローブを有効にせずに、URL リダイレクションとクライアント プロビジョニングを使用して収集された属性を強調表示しています。

図 37 URL リダイレクションを使用した HTTP プローブ属性 - クライアント プロビジョニングの例




**ステップ 7** 強調表示されたキー属性は前の例と同様ですが、**EndPointSource** が CP（クライアント プロビジョニング）に設定されている点が異なります。

## SPAN を使用した HTTP プローブ データの確認

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

**ステップ 2** 設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

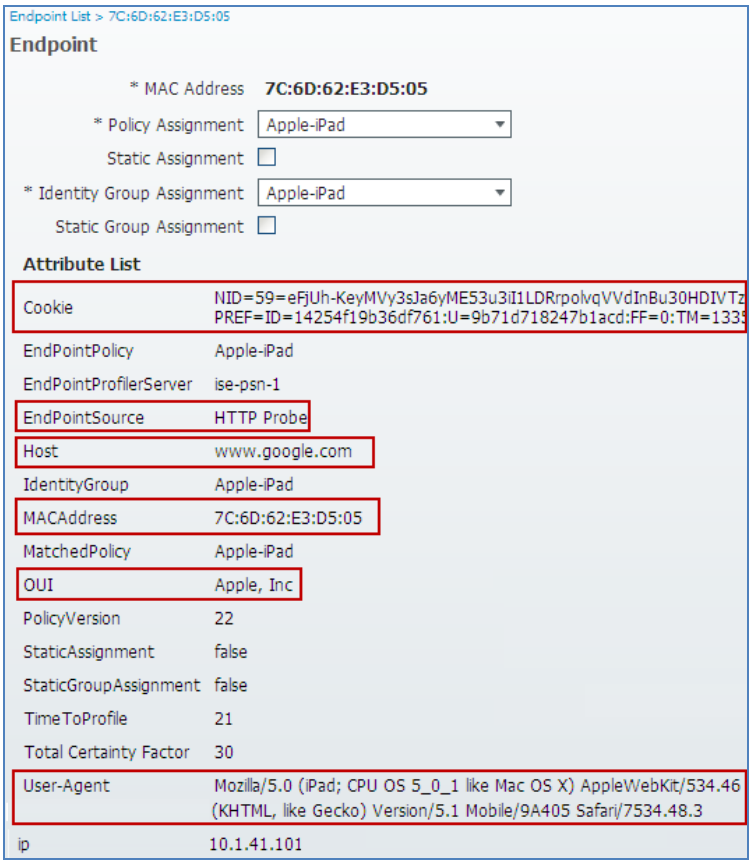
**ステップ 3** エンドポイント上で Web ブラウザを開いて、任意の Web サイトへの HTTP アクセスを試みます。

**ステップ 4** [管理（Administration）] → [ID 管理（Identity Management）] → [ID（Identities）] に移動して、LHS ペインで [エンドポイント（Endpoints）] を選択します。

**ステップ 5**　新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、HTTP プローブによってキャプチャされた属性を表示します。

**ステップ 6**　図 43 は、HTTP プローブだけを有効にした状態で、SPAN を使って収集された属性を強調表示しています。

図 38 SPAN を使用した HTTP プローブ属性の例




キー属性には、前の例と同じ属性と、いくつかの新しい属性が含まれます。

- **Cookie**（表示用に省略されている）
- ホスト

初期 CWA プロセス完了後の出力は、URL リダイレクションを使用した場合と同様です。これらの追加の属性は、通常のクライアント ブラウズ アクティビティによって収集された追加的な HTTP ヘッダー情報のキャプチャを表します。これらの属性が変化するたびに、ISE が更新され続けます。使用されないかもしれないこのような多数の属性更新が、データベース更新と同期プロセスに大きな影響を与える可能性があることは明らかです。ここでも明確に示されるとおり、HTTP プローブと URL リダイレクションを使用した **User-Agent** のキャプチャは SPAN 方式よりはるかに効率的と言えるでしょう。

要約すると、**User-Agent** 属性によって判別されるオペレーティング システムに基づいてエンドポイントを分類できます。この属性は HTTP プローブによって、および特殊なケースではクライアント プロビジョニング サービスによって収集されます。HTTP トラフィックの収集によく使用される方法として、URL リダイレクションと SPAN 技法の 2 つがあります。一般的に URL リダイレクションの方がはるかに効率的ですが、RADIUS 認証が有効になっていない環境でプロファイリングが必要な場合は SPAN が唯一のオプションになることがあります。

## DNS プローブを使用したプロファイリング

既存のエンドポイントの IP アドレスが学習された後、ISE ポリシー サービス ノードからの DNS 逆引き参照に基づいて DNS 完全修飾ドメイン名（FQDN）を取得するために DNS プローブが使用されます。そのため、IP アドレスが不明な場合は DNS プローブが機能できません。

次のプローブを使用して、エンドポイントの IP アドレスを特定できます。

- RADIUS プローブ（Framed-IP-Address 経由）
- SNMP プローブ（cdpCacheAddress 経由）
- HTTP プローブ（SourceIP 経由）
- DHCP プローブ（dhcp-requested-address 経由）

既知の IP アドレスの取得に加えて、DNS 逆引き参照を使用するためには、他のいくつかの要件があります。

- DNS では、エンドポイントごとに、アドレスつまり **A** レコード（ホスト名）とポインタつまり **PTR** レコード（IP アドレス）が必要です。
- エンドポイントで DHCP が使用されている場合は、DHCP サーバ上でダイナミック DNS（DDNS）を設定する必要があります。
- DHCP サーバの設定によっては、動的更新を要求するようにエンドポイントを設定する必要が生じることがあります。
- 動的に更新される DNS サーバからのアドレスを解決するよう ISE ポリシー サービス ノードを設定する必要があります。
- DDNS が設定されて正常に動作している場合、DNS プローブは FQDN を取得できます。そうでない場合、逆引き参照が失敗すると、属性は追加されません。

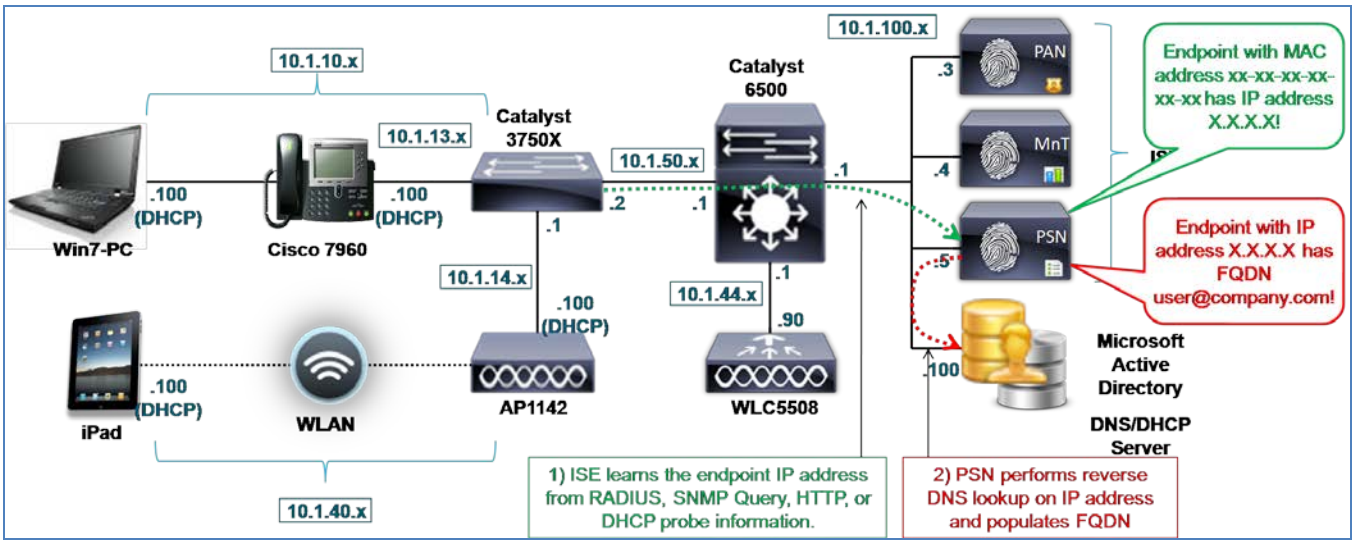
標準のホスト名、ドメイン名、または FQDN 命名規則が特定のエンドポイントに適用されている場合は、これらの属性を使用してそれらを分類できます。たとえば、すべての Windows XP クライアントに **jsmith-winxp** などの名前が割り当てられている場合、Windows CP エンドポイントを分類するために条件で **host-name** 属性または **client-fqdn** 属性を使用できます。同様に、（**jsmith-corp-dept** など）企業エンドポイントのホスト名を入力する規則が存在する場合は、企業資産の検証にそれを使用できます。

プロファイル属性を ID と混同しないように注意する必要がありますが、属性を使用すると、エンドポイントが特定のタイプであるという一定の信任レベルを追加できます。たとえば、認可ポリシーをプロファイリングとともに使用すると、（エンドポイント ID グループの照合によって示される）従業員の PC の host-name 属性に想定値が含まれて**いない**場合、その従業員のフル アクセス権限を拒否することができます。注：プロファイルとエンドポイント ID グループの関係についてはこのマニュアルで後述します。

この説明からわかるように、他のプローブを使用して FQDN またはそのコンポーネントを収集できる可能性があります。つまり、他の手段によって FQDN の同じ情報またはその一部が入手可能な場合は、DNS プローブを使用する必要がないでしょう。ただし、DDNS をよりセキュアに設定できるため、信頼できる DNS サーバへの逆引き参照経由で取得される情報よりも DHCP クライアント パケット経由で取得される情報の方が信頼性が低くなります。

図 44 に、DNS プローブを使用したサンプル トポロジを示します。この図からわかるように、ISE ポリシー サービス ノードは、複数の方式のいずれかを使用してエンドポイントの IP アドレスを学習します。その後、PSN が IP アドレスの逆引き参照を開始します。応答が受信されると、ISE プロファイリング サービスは FQDN 属性を使ってエンドポイント レコードを更新します。

図 39 DNS プローブの例




# DNS プローブの設定

DNS プローブを使用するには、ISE ポリシー サービス ノードから参照される DNS を（手動でまたは DDNS を使って動的に）設定して、FQDN の取得対象となる各エンドポイントのホスト レコードと逆ポインタ レコードを含めるようにする必要があります。

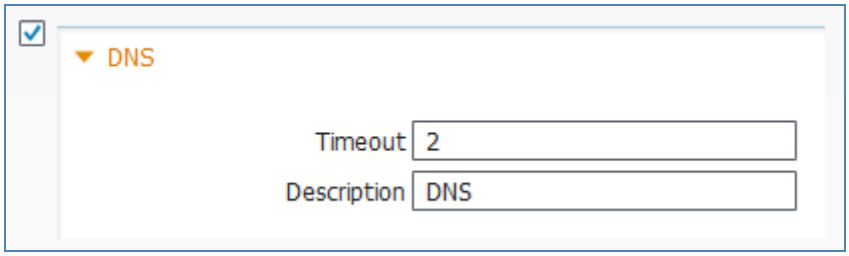
## ISE での DNS プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択します。

**ステップ 3** DNS プローブのサポートを追加するには、DNS というラベルのボックスをオンにします。

図 40：SPAN を使用した HTTP プローブ属性の例




ローカルに設定された DNS サーバへの逆引き参照用のグローバル ルーティング テーブルを使用して、ISE ポリシー サービス ノードからすべてのプローブ クエリーが開始されるため、DNS プローブでのインターフェイス選択はありません。

**ステップ 4** [タイムアウト（Timeout）] はデフォルト値のままにします。この値は、PSN が逆引き参照の応答を待つ秒数を指定します。

**ステップ 5** [保存（Save）] をクリックして、変更をコミットします。

**ステップ 6** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

## エンドポイント IP アドレスを取得するためのプローブの設定

**注**:エンドポイントの IP アドレスを取得するようにプローブを設定します。DNS プローブが FQDN の DNS 逆引き参照を実行するためには、最初に SNMP クエリー、DHCP、DHCP SPAN、HTTP、または RADIUS プローブからエンドポイントの IP アドレスを学習する必要があります。これらのプローブの設定の詳細については、このマニュアルの該当する項を参照してください。

## アドレス逆引き参照用の DNS サーバを使用した ISE の設定

ISE アプライアンスを初めてインストールするときに必要な設定手順として、1 つ以上のドメイン ネーム サーバを設定します。

必要に応じて、グローバル コンフィギュレーション モードで ISE CLI コマンド **ip name-server** を使用して、プロファイリング サービスを実行しているポリシー サービス ノードによって使われる DNS サーバのリストを更新します(図 46 を参照)。

図 41 ISE ポリシー サービス ノードの DNS サーバ設定の例

```
ise-pan-1/admin(config)# ip name-server ?
  <A.B.C.D>  Primary DNS server IP address
  <A.B.C.D>  DNS server 2 IP address
  <A.B.C.D>  DNS server 3 IP address
```

**ステップ 7** エントリを削除するには、**no name-server** コマンドを使用します。

**ステップ 8** 変更を保存するには、グローバル コンフィギュレーション モードを終了して、コマンド **copy running-config startup-config** を入力します。

**ステップ 9** 必要に応じて、プロファイリング サービスを実行している残りのポリシー サービス ノードに対して同じ手順を繰り返します。

## DNS プローブ データの確認

**ステップ 1** [管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] → [エンドポイント(Endpoints)] からエンドポイントを削除します。

**ステップ 2** ISE PSN への HTTP リダイレクションをサポートするように設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

**ステップ 3** ISE ポリシー管理ノードにアクセスして、[管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] に移動します。

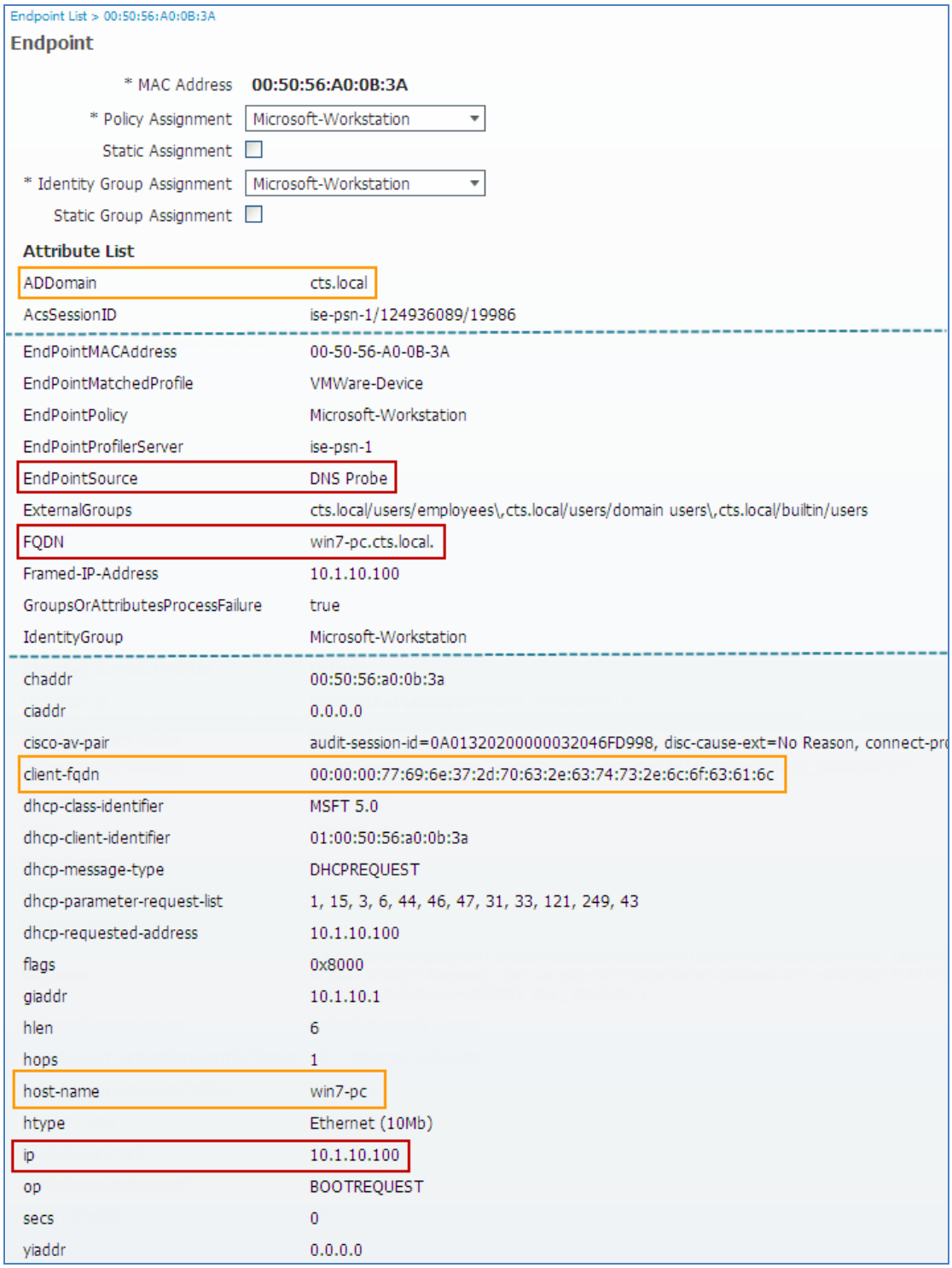
**ステップ 4** LHS ペインで、[エンドポイント(Endpoints)] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、HTTP プローブによってキャプチャされた属性を表示します。

図 47 の例は、RADIUS、DHCP(IP ヘルパー)、および DNS プローブのみが有効になっている様子を示しています。RADIUS と DHCP は、エンドポイントの MAC アドレスと IP アドレスの両方を取得する方式として有効にされます。また、これらのプローブは、さまざまなプローブを使って収集可能な同様のデータを比較するためにも選択されます。

ハッシュ マークは、表示上の理由で出力を省略しているセクションを示しています。

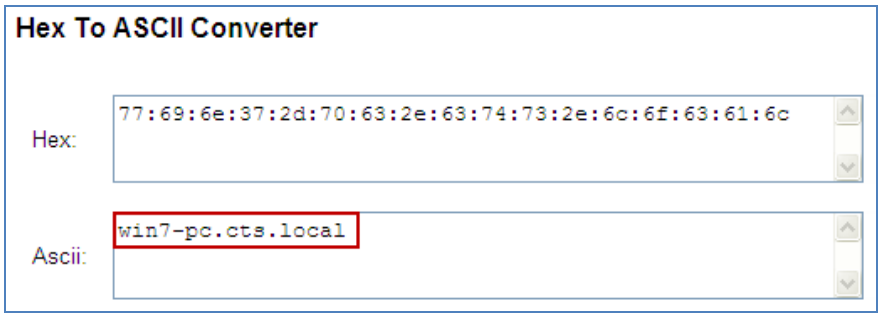
図 42 DNS プローブ属性の例




**ステップ 6** 赤色で強調表示されたキー属性には以下のものがあります。
**ステップ 7** EndPointSource = DNS Probe
**ステップ 8** FQDN = win7-pc.cts.local

**ステップ 9** ip = 10.1.10.100
**ステップ 10** **EndPointSource** は、エンドポイント属性の最後のソースを反映しています。
**ステップ 11** **FQDN** 値は、DNS プローブを使用した DNS サーバの逆引き参照が成功した場合の結果です。
**ステップ 12** **ip** 属性は、DNS プローブが機能するためにこの属性を取得する必要性を示すために強調されています。この例では、RADIUS または DHCP プローブがこの値を更新した可能性があります。
**ステップ 13** オレンジ色で強調表示されたセカンダリ属性には以下りものがあります。
**ステップ 14** ADDomain = cts.local
**ステップ 15** client-fqdn = 00:00:00:77:69:6e:37:2d:70:63:2e:63:74:73:2e:6c:6f:63:61:6c
**ステップ 16** host-name = win7-pc
**ステップ 17** **ADDomain** 値は、RADIUS プローブを使用して RADIUS 属性から学習されたドメイン名です。
**ステップ 18** **client-fqdn** 属性は、DHCP プローブから学習されたエンドポイントの完全修飾ドメイン名であり、HEX 形式で表現されます（図 48）。

図 43 HEX から ASCII への変換の例




**ステップ 19** **host-name** 属性は、DHCP プローブから学習されたエンドポイントの単純なホスト名です。
**ステップ 20** この例は、さまざまなプローブ属性が同様の情報を提供する可能性があることを示しています。最終的にポリシー管理者は、エンドポイントのプロファイリングに最も役立つ属性はどれか、またこの情報を取得するのに最適なプローブはどれかを選択する必要があります。プローブ方式とプロファイリング方式の比較については、このマニュアルで後述します。

## NetFlow プローブを使用したプロファイリング

Cisco NetFlow は、Cisco IOS ソフトウェア ベースのルータおよびレイヤ 3 スイッチからエクスポートされるテレメトリの形態です。NetFlow は、それぞれの NetFlow 対応ルータまたはスイッチを通過する（またはそこに直接到達する）トラフィックに関する情報を提供します。NetFlow 対応デバイスは、指定された UDP ポート（デフォルトは UDP/9996）でネットワーク フロー データを収集してコレクタにエクスポートします。フローは、特定の送信元/宛先間のパケットの単方向ストリームであり、次のキー フィールドを組み合わせて一意に識別されます。

ソース IP アドレス

宛先 IP アドレス

送信元ポート番号

宛先ポート番号

レイヤ 3 プロトコル タイプ

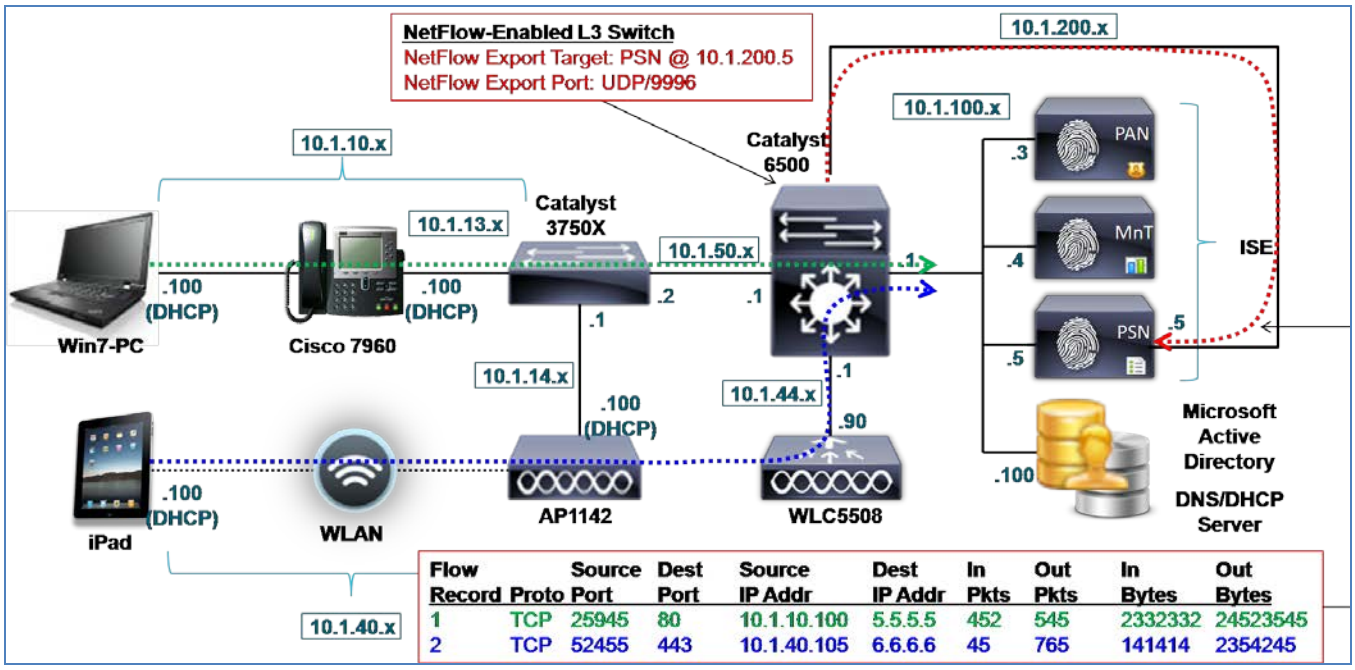
ToS バイト

入力論理インターフェイス（ifIndex）

ISE NetFlow プローブは、プロファイリングにとって重要な情報の解析を可能にする NetFlow バージョン 5 および バージョン 9 対応デバイスからフロー レコードを受信することができます。

図 49 のサンプル トポロジは、NetFlow 対応スイッチ（Cisco Catalyst 6500 シリーズ）経由でトラフィック フローを確立した 2 つの異なるエンドポイントを示しています。6500 シリーズは、UDP/9996 上の IP アドレス 10.1.200.5 を使って専用インターフェイス上で ISE ポリシー サービス ノードにフローをエクスポートするように設定されます。このインターフェイスは、RADIUS や Web 認証などのユーザ セッション サービスを終了させるインターフェイスとは別のものです。

図 44 NetFlow プローブの例




このトポロジからわかるように、対象となるトラフィックのパスに存在するルータ上またはスイッチ上で NetFlow を有効にする必要があります。たとえば、リモート ブランチ内のセグメント間のトラフィック フローを収集する必要がある場合、ハブまたは中心的な場所に展開された NetFlow は、必要な可視性を提供しません。加えて、特定のトラフィック フローを収集するには、まずそのトラフィックがネットワークで許可される必要があります。そのため、ネットワーク アクセスが NetFlow データに基づくプロファイルに依存している場合は、プロファイリングの完了に必要なトラフィックを許可しながらアクセスを制限する最適な方法を決定する必要があります。

## NetFlow 属性

表 4 に、NetFlow プローブによって収集される属性の一部を示します。

表 2 NetFlow プローブ属性

| | | |
|---|---|---|
| IN_BYTES | IN_PKTS | FLOWS |
| PROTOCOL | SRC_TOS | TCP_FLAGS |
| L4_SRC_PORT | IPV4_SRC_ADDR | SRC_MASK |
| L4_DST_PORT | IPV4_DST_ADDR | DST_MASK |
| IPV4_NEXT_HOP | LAST_SWITCHED | FIRST_SWITCHED |
| OUT_BYTES | OUT_PKTS | IPV6_SRC_ADDR |
| IPV6_DST_ADDR | IPV6_SRC_MASK | IPV6_DST_MASK |
| IPV6_FLOW_LABEL | ICMP_TYPE | DST_TOS |
| IN_SRC_MAC | OUT_DST_MAC | SRC_VLAN |
| DST_VLAN | IP_PROTOCOL_VERSION | DIRECTION |

ISE プロファイリング サービスでは、通常、生成されたトラフィックに基づくエンドポイントの識別に NetFlow が使用されます。逆に、特定のエンドポイントがそのエンドポイント特有ではないトラフィックを生成しているように見える場合、異常な動作を示す指標になり得ます。たとえば、最初に IP 電話としてプロファイリングされたエンドポイントが、NetFlow 属性で示されるポート 443 上でリモート宛先との通信を突然に開始した場合、これは異常な状態およびスプーフィング エクスプロイトの可能性を示唆しています。ただし、NetFlow と ISE プロファイリング サービスの併用はスプーフィング対策機能またはソリューションとして位置付けられていないことに注意してください。

エンドポイントの肯定的な分類に重点を置いている NetFlow は、ミッション固有の機能に汎用ハードウェアが使用され、それらを一意的に分類する唯一の情報がトラフィック関連のものであるようなシナリオで最も役立ちます。このような種類のデバイスの例には、製造業や医療の分野で使用されるデバイスが含まれます。たとえば、病院内の心臓モニタは、標準ハードウェア テクノロジーを使用して組み込み Windows OS または強化された Linux カーネルを使用ししながら、非常に特殊なプロトコル、ポート、および宛先で通信するアプリケーションを実行することができます。この種のエンドポイントでは、NetFlow が唯一の現実的なオプションでしょう。

**ステップ 21** 一般的に、NetFlow を無作為に有効にしたり、NetFlow プローブを汎用のプロファイル方式として使用したりすることはお勧めできません。よく注意せずに NetFlow を展開した場合、使用されるプラットフォームや NetFlow 設定およびトラフィック量によっては、デバイス リソースに悪影響を及ぼす可能性があります。また、大量のトラフィックが 1 つ以上のソースから連続的に送信される場合、NetFlow が ISE ポリシー サービス ノードに高い負荷をもたらす可能性もあります。他の ISE プローブと違って、NetFlow プローブは、データ収集とデータベース効率を最適化する属性フィルタをサポートしません。

**ステップ 22** ネットワーク デバイスで可能な場合は、ISE ポリシー サービス ノードへの NetFlow エクスポート用に NetFlow バージョン 5 よりも バージョン 9 を使用することお勧めします。バージョン 9 は Flexible NetFlow をサポートし、収集されて NetFlow プローブにエクスポートされるフロー データをフィルタリングするさまざまな拡張機能もサポートします。サンプリングされた NetFlow は全体のトラフィック量を減らす可能性がありますが、一部のシナリオではすべてのフローを NetFlow プローブで認識する必要があるため、サンプリングですべてのプロファイリング要件が満たされない場合もあります。

### NetFlow プローブと IP/MAC アドレス間バインドの要件

**ステップ 23** NetFlow レコードは、送信元 IP アドレスと宛先 IP アドレス間の通信に基づいています。NetFlow トラフィックには送信元/宛先エンドポイントの MAC アドレスが含まれないため、NetFlow プローブに送信されるデータを正しく関連付けるには、ISE ポリシー サービス ノードで ARP キャッシュ テーブル内に IP/MAC アドレス間バインドが設定済みであることが重要です。つまり、エンドポイントで MAC アドレスによって ISE を認識できない場合、**または**関連する IP アドレスが存在しない場合は、NetFlow プローブによって学習されたプロファイリング データが破棄されます。これは、学習されたフロー属性を適用可能なエンドポイントが存在しないためです。その結果、NetFlow データを収集する**前**に、別のプローブを介して IP/MAC アドレス間バインドを学習する必要があります。この情報を提供するために使用可能なプローブには、以下が含まれます。

**ステップ 24** RADIUS（Framed-IP-Address 経由）

**ステップ 25** DHCP（dhcp-requested-address 経由）

**ステップ 26** SNMP クエリー（SNMP ポーリングを介して）

**ステップ 27** フロー レコード内に送信元および宛先 MAC アドレスを含めるオプションは、NetFlow バージョン 9 ではサポートされますが、バージョン 5 ではサポートされないことに注意してください。ただし、これらの報告される MAC アドレスは、パス内の隣接ノード（通常はレイヤ 3 ルータとスイッチ）の MAC アドレスであって、複数ホップ離れたエンドポイントの MAC アドレスではありません。エンド システムが NetFlow デバイスに直接接続される場合を除き、この機能はあまり有益ではありません。

**ベスト プラクティス**：プロファイリングに NetFlow を使用した場合、解析用に ISE に送信されるデータ量が増える可能性があります。他のプローブでは不十分なシナリオでのみ、NetFlow を限定的に使用してください。必要に応じて、Flexible NetFlow のようなフィルタリング拡張機能を備えた NetFlow バージョン 9 を利用することをお勧めします。ISE でデフォルト インターフェイスが使用不能なわけではありませんが、NetFlow プローブ専用の ISE PSN インターフェイスにNetFlow を エクスポートすることを強くお勧めします。

## NetFlow プローブの設定

**ステップ 28** NetFlow プローブを使用するには、対象となるトラフィック フローの経路であるネットワーク デバイスが NetFlow に対応し、NetFlow バージョン 5 またはバージョン 9 をサポートしている必要があります。NetFlow データのターゲットになる各 ISE PSN 上で専用のインターフェイスを使用する必要があります。

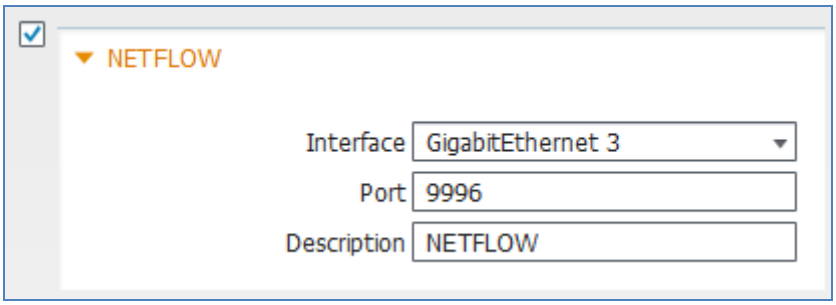
### ISE での NetFlow プローブの有効化

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択して、NetFlow プローブを有効にするボックスをオンにします（図 50）。

**ステップ 3** NetFlow トラフィックの収集に使用するインターフェイスを選択します。これは、IP アドレスがルーティング可能な専用インターフェイスである必要があります（図 50）。

図 45 NetFlow プローブ設定




**ステップ 4** エクスポートされた NetFlow をリッスンする UDP ポートを選択します。この値は、NetFlow エクスポート デバイス上で設定したものと同じである必要があります。デフォルト ポートは UDP/9996 です。

**ステップ 5** [保存(Save)] をクリックして、変更をコミットします。

**ステップ 6** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

注:多くの NetFlow 対応ルータおよびスイッチでは、NetFlow エクスポート用に 1 つのターゲットだけがサポートされます。そのため、ハイ アベイラビリティを考慮する必要があります。また、特定のエンドポイントのすべてのプロファイル データを同じポリシー サービス ノードで受信することをお勧めします。ネットワーク設定その他の制限によっては、これが常に可能なわけではありません。

## ISE(ネットワーク リソース)へのネットワーク デバイスの追加

アクセス デバイスでも NetFlow を利用できますが、NetFlow プローブに NetFlow を送信できる他のネットワーク デバイスを ISE でネットワーク デバイスとして設定する必要は特にありません。

## NetFlow トラフィックを受信するための ISE ポリシー サービス ノード インターフェイスの設定

NetFlow トラフィックを受信するには専用インターフェイス上で NetFlow プローブを設定する必要があります。ISE 上で専用 NetFlow インターフェイスを設定するには、次の手順を実行します。

**ステップ 1** 該当するインターフェイスをネットワーク スイッチ ポートに物理的に接続します。

**ステップ 2** ISE PSN コンソール(CLI)にアクセスします。図 51 に示すように、該当するインターフェイスを有効にして、有効な IP アドレスを割り当てます。

図 46 ISE プローブ専用インターフェイスの設定例

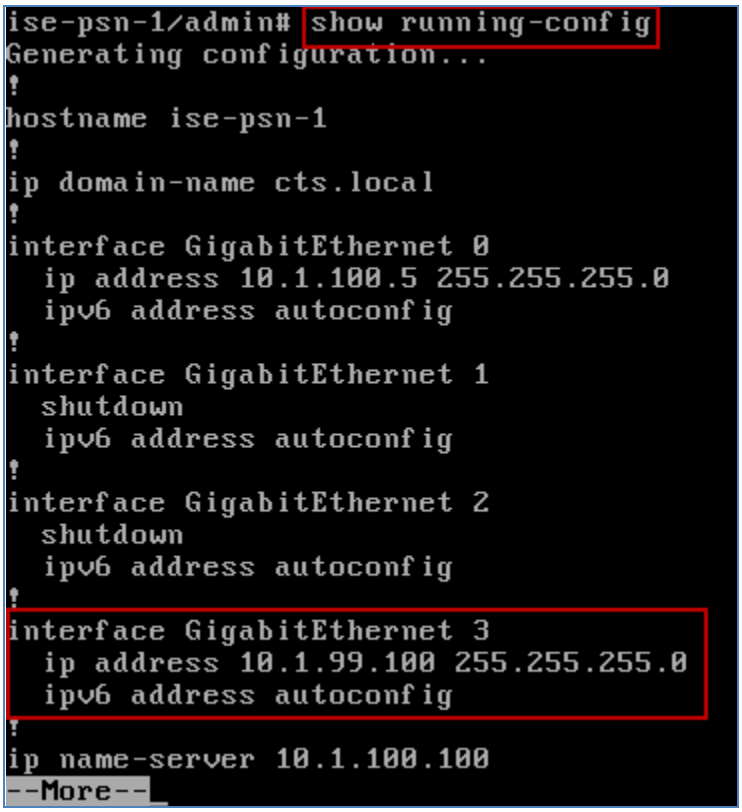
```
ise-psn-1/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

**ステップ 3**　すべてのプロセスが、指示どおりの実行状態にあることを確認します。

**ステップ 4**　**show running-config** コマンドを使用して、新しく設定されたインターフェイスの設定を確認し、それが（シャットダウンではなく）有効になっていることを確認します（図 52）。

図 47 ISE プローブ専用インターフェイスの確認例




**ステップ 5** NetFlow データをエクスポートする必要があるネットワーク デバイスから ICMP ping を送信することによって、新しいプローブ インターフェイスへの接続を確認します。

**ステップ 6** CLI コマンド **copy running-config startup-config** を使用して変更を保存します。

**ステップ 7** 該当するインターフェイスを適切な SPAN 宛先ポートまたはネットワーク タップ インターフェイスに物理的に接続します。

注：VMWare アプライアンスで動作するポリシー サービス ノードの場合

専用インターフェイスをプロファイリングに使用するには、追加の仮想インターフェイスが仮想アプライアンス用に設定されていることが想定されます。インストール時点で完了していない場合は、ISE 設定に進む前に、ISE ノードをシャットダウンして、必要なインターフェイス用に ESX アプライアンスのハードウェア設定とネットワーキング設定を更新する必要があります。

## NetFlow を ISE PSN にエクスポートするための NetFlow 対応スイッチ/ルータの設定

NetFlow 設定は、NetFlow 対応デバイスに固有のものです。この手順には、Catalyst 6500 シリーズ スイッチの設定例が含まれています。

**ステップ 1** グローバル コンフィギュレーション モードで NetFlow を有効にして、NetFlow バージョン 9 サポート、NetFlow データの供給元となるインターフェイス IP アドレス、およびデータをエクスポートするポリシー サービス ノードを設定します。ISE デフォルト ポート UDP 9996 の指定に注意してください。

```
mls netflow interface
mls flow ip interface-full
mls nde sender
mls nde interface
ip flow-cache timeout active 1
ip flow-export source Vlan100
ip flow-export version 9
ip flow-export destination 10.1.100.5 9996
```

注:前の例では、Catalyst 6500 シリーズ スイッチにスーパーバイザ 720 が実装され、そこではポリシー フィーチャ カード(PFC)がハードウェア ベースの NetFlow を実行し、マルチレイヤ スイッチ フィーチャ カード(MSFC)に送られるフローがソフトウェアで実行されます。mls nde sender コマンドを使用して NetFlow データ エクスポート(NDE)を実行するように PFC を設定する必要があります。

**ステップ 2** オプションで、次のようにキャプチャ フィルタを設定します。

```
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses
```

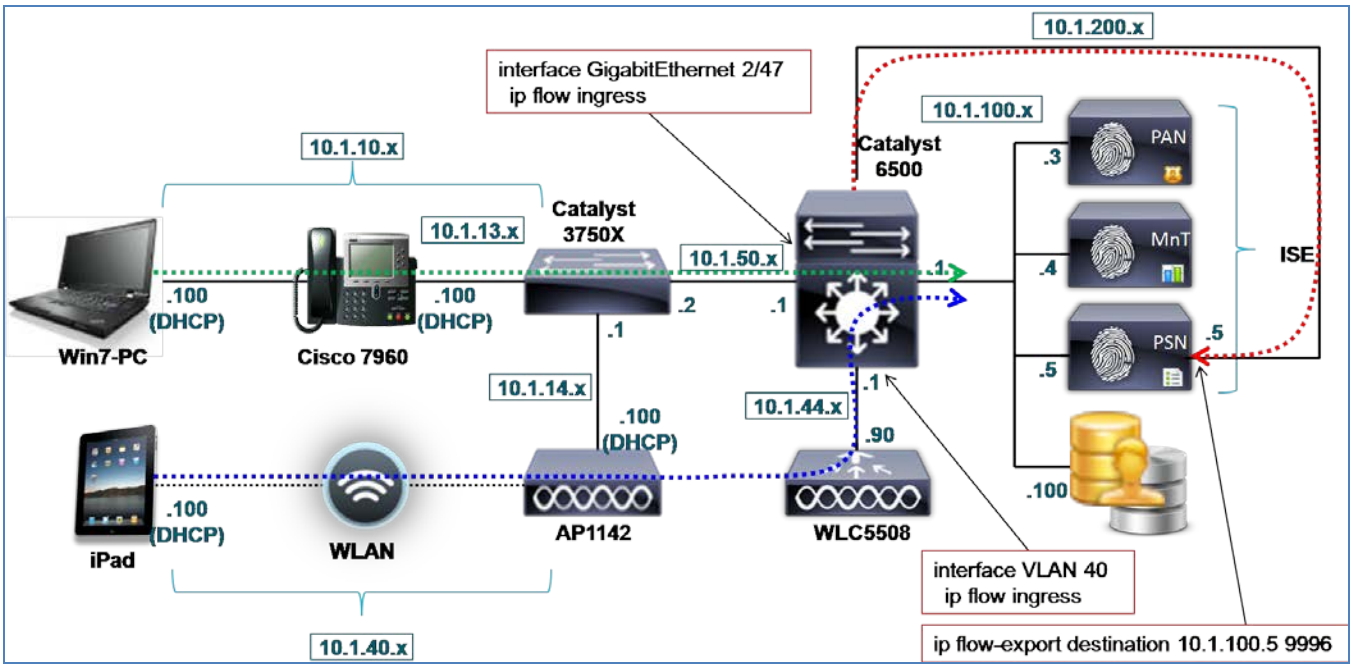
**ステップ 3** 次のように、入力インターフェイス(エンドポイントに面したインターフェイス)上で NetFlow を有効にします。

```
interface GigabitEthernet 2/47
 description To cat3750x
 ip address 10.1.50.1 255.255.255.0
 ip flow ingress
!
interface Vlan40
 説明 EMPLOYEE(Description URL)
 ip address 10.1.40.1 255.255.255.0
 ip helper-address 10.1.100.100
 ip helper-address 10.1.100.5
 ip flow ingress
!
interface Vlan41
 説明 GUEST(Description URL)
 ip address 10.1.41.1 255.255.255.0
 ip helper-address 10.1.100.100
 ip helper-address 10.1.100.5
 ip flow ingress
```

また、IP ヘルパー コマンドにより、IP/MAC アドレス間バインド情報の取得に使われる DHCP プローブをサポートする設定が強調表示されます。これにより、NetFlow プローブは一致する IP 属性に基づいて属性を適用できます。

図 53 に、NetFlow が適用されるインターフェイスと NetFlow データ エクスポート(NDE)の宛先を示します。この目的は、Cisco Catalyst 3750-X シリーズ スイッチ経由で接続されている有線エンドポイントと、Cisco 5500 シリーズ Wireless LAN Controller 経由で接続されている無線エンドポイントからトラフィックをキャプチャすることです。

図 48 NetFlow エクスポートの例




## NetFlow プローブ データの確認

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

**ステップ 2** アクセス デバイスからエンドポイントを切断した後、再接続します。

**ステップ 3** エンドポイントからログインして、ブラウザを使用した Web アクセスなどのサンプル トラフィックを生成してみます。

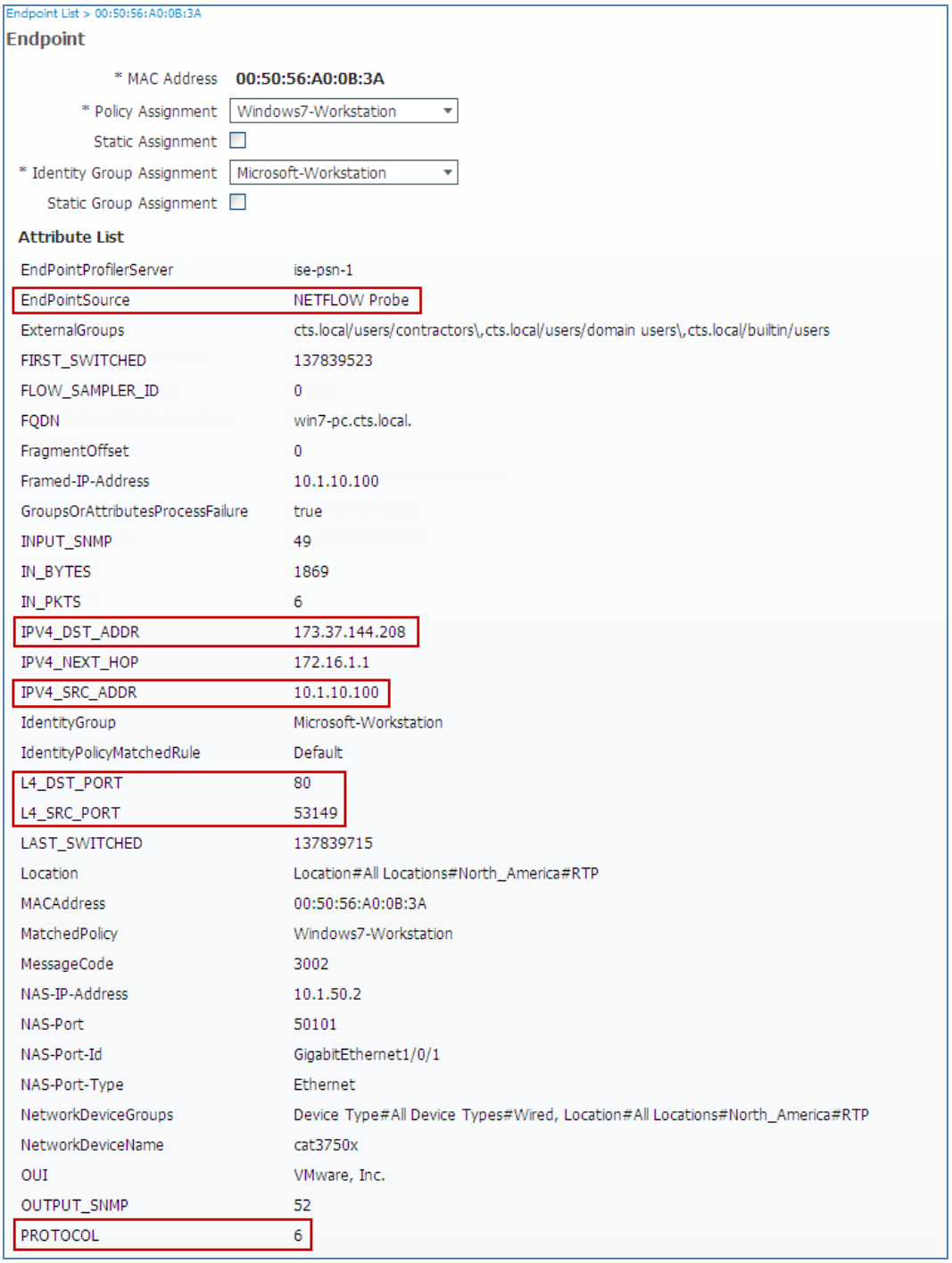
**ステップ 4** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

**ステップ 5** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 6** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、NetFlow プローブによって収集された属性を表示します（図 54）。

**ステップ 7** 図 54 の例では、NetFlow エクスポートを使用して収集された属性が強調表示されています。加えて、NetFlow プローブをサポートするための IP/MAC 間バインドを確実に取得するために RADIUS プローブと DHCP プローブが有効にされています。

図 49 NetFlow 属性の例




赤色で強調表示されたキー属性には以下のものがあります。

- EndPointSource = NetFlow Probe
- IPV4_DST_ADDR = 173.37.144.208 (cisco.com)
- IPV4_SRC_ADDR = 10.1.10.100 (win7-pc)
- L4_DST_PORT = 80 (HTTP)

- L4_SRC_PORT = 53149
- PROTOCOL = 6 (TCP)

フロー キャプチャ ステートメントが使用されている場合は、次のような追加の属性が示されることがあります。

- DST_VLAN/SRC_VLAN
- IN_SRC_MAC/OUT_DST_MAC
- MAX_TTL/MIN_TTL

NetFlow データが収集されていることを確認するために、**show ip cache flow** コマンドと **show mls netflow ip** コマンドを使用できます。次の例では、**show ip cache flow** コマンドが使用されています。

```
cat6503#show ip cache flow

------------------------------------------------------------------------------

Displaying software-switched flow entries on the MSFC in Module 1:

IP packet size distribution (348128 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .548 .342 .077 .005 .000 .000 .000 .000 .000 .000 .015 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .007 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 15760 added
  251284 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  6 active, 1018 inactive, 47280 added, 15760 added to flow
  0 alloc failures, 2775 force free
  1 chunk, 24 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          44      0.0        91    42      0.0      14.4       7.8
TCP-WWW           1361      0.0        22    45      0.0       0.0      14.2
TCP-other         1602      0.0        25    51      0.0       0.1      13.6
UDP-DNS            128      0.0         1    70      0.0       0.0      15.4
UDP-NTP           1375      0.0         1    76      0.0       0.0      15.5
UDP-other         2880      0.0         3   338      0.0       3.8      15.4
ICMP              6985      0.0        34    30      0.0       0.4      13.4
IP-other          1383      0.0        13    65      0.0      58.3       2.0
Total:           15758      0.0        22    46      0.0       6.0      13.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi2/47        10.1.50.2       Null          224.0.0.10      58 0000 0000     4
Gi2/47        10.1.13.1       Null          10.1.100.7      11 0043 0043     3

------------------------------------------------------------------------------

Displaying hardware-switched flow entries in the PFC (Active) Module 1:
 SrcIf            SrcIPaddress     DstIf            DstIPaddress    Pr SrcP DstP  Pkts

 Gi2/47           10.1.50.1        Gi2/47           10.1.50.2       58 0000 0000     0
 Gi2/47           10.1.50.2        ---              10.1.100.1      11 007B 007B     0
 Gi2/47           10.1.50.2        ---              10.1.50.1       58 0000 0000     0
 Gi2/47           10.1.100.1       Gi2/47           10.1.50.2       11 007B 007B     0
 Gi2/47           10.1.50.2        Vl100            10.1.100.5      11 CC9B 00A2    15
 Gi2/47           10.1.13.1        Vl100            10.1.100.100    11 0043 0043   124
 Gi2/47           10.1.13.1        Vl100            10.1.100.5      11 0043 0043   124
 Gi2/47           10.1.13.1        Vl100            10.1.100.6      11 0043 0043   124
```

```
Gi2/47          10.1.50.2       ---             224.0.0.10      58 0000 0000    84
Vl40            10.1.40.1       ---             224.0.0.10      58 0000 0000     0
Gi2/47          10.1.50.2       Vl100           10.1.100.4      11 C8D5 5022    30
Gi2/47          10.1.13.1       ---             10.1.100.7      11 0043 0043     0
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 CA72 0035     1
Gi2/47          10.1.50.2       Vl100           10.1.100.5      11 066E 0715   128
Vl41            10.1.41.1       ---             224.0.0.10      58 0000 0000     0
Gi2/47          10.1.50.2       Vl100           10.1.100.5      11 06A4 7195     2
Gi2/47          10.1.50.2       Vl100           10.1.100.6      11 E6D7 00A2    15
Gi2/47          10.1.50.2       ---             10.1.100.7      11 C748 00A2     0
Gi2/47          10.1.50.2       Vl100           10.1.100.5      11 066D 0714     6
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 E5CC 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 DA8B 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 C114 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 FC03 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 D295 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 ED48 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 E7E8 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 D770 0035     1
Gi2/47          10.1.10.100     Vl100           10.1.100.100    11 D5AB 0035     1
--              0.0.0.0         ---             0.0.0.0         00 0000 0000    31K
```

**ステップ 8**　次の例では、**show mls neflow ip** が使用されています。

```
at6503#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 1
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f          :AdjPtrPkts      Bytes
Age   LastSeen  Attributes

------------------------------------------------------------------------------------------------------
-------------------------------
10.1.50.2       10.1.100.1      udp :ntp    :ntp      Gi2/47           :0x00            0
43    20:26:48   L2 - Dynamic
10.1.44.90      10.1.14.100     udp :16792  :5246     Gi2/47           :0x03            359
35    20:27:26   L3 - Dynamic
10.1.100.100    10.1.13.1       udp :67     :67       Gi2/47           :0x04            1846
32    20:27:30   L3 - Dynamic
10.1.100.5      10.1.50.2       udp :52379  :162      Gi2/47           :0x015           2734
335   20:23:02   L3 - Dynamic
10.1.100.4      10.1.50.2       udp :51413  :20514    Gi2/47           :0x030           5286
334   20:23:58   L3 - Dynamic
10.1.100.5      10.1.50.2       udp :1646   :1813     Gi2/47           :0x04            2680
32    20:27:30   L3 - Dynamic
10.1.100.100    10.1.10.100     udp :51826  :dns      Gi2/47           :0x01            61
211   20:24:00   L3 - Dynamic
10.1.44.90      10.1.14.100     udp :16792  :5247     Gi2/47           :0x06            901
30    20:27:30   L3 - Dynamic
224.0.0.10      10.1.41.1       88  :0      :0        Vl41             :0x00            0
426   20:27:27   Multicast
10.1.100.5      10.1.50.2       udp :1700   :29077    Gi2/47           :0x02            132
335   20:23:56   L3 - Dynamic
10.1.100.6      10.1.50.2       udp :59095  :162      Gi2/47           :0x015           2734
335   20:23:02   L3 - Dynamic
10.1.100.7      10.1.50.2       udp :51016  :162      Gi2/47           :0x00            0
335   20:23:02   L3 - Dynamic
10.1.100.5      10.1.50.2       udp :1645   :1812     Gi2/47           :0x06            1365
270   20:23:56   L3 - Dynamic
10.1.100.100    10.1.10.100     udp :54699  :dns      Gi2/47           :0x01            64
211   20:24:00   L3 - Dynamic
10.1.100.1      10.1.50.2       udp :ntp    :ntp      Gi2/47           :0x00            0
43    20:26:48   L3 - Dynamic
17.172.232.209  10.1.40.101     tcp :61858  :443      Vl40             :0x02            173
17    20:27:14   L3 - Dynamic
17.172.232.209  10.1.40.101     tcp :61858  :443      Vl40             :0x00            0
17    20:27:14   L2 - Dynamic
```

```
10.1.40.101     17.172.232.209  tcp :443    :61858    Vl40             :0x00           0
17    20:27:14   L2 - Dynamic
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x032283       20941051
1573  20:27:31   L3 - Dynamic
```

**ステップ 9** NetFlow エクスポート設定を確認し、フローが ISE ポリシー サービス ノードに送信されていることを確認するには、次のように **show ip flow export** コマンドを使用します。

```
cat6503# sh ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       10.1.100.1 (Vlan100)
    Destination(1)  10.1.99.5 (9996)
  Version 9 flow records
  20408 flows exported in 7635 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to Card not being able to export
```

## ネットワーク スキャン（NMAP）プローブを使用したプロファイリング

ネットワーク スキャン プローブは、オープン ソース Network Mapper ユーティリティの組み込みバージョンに基づいています。Network Mapper（NMAP）は、接続されたエンドポイントを見つけるために大規模ネットワークをスキャンした後、個別のホストをスキャンして、そのオペレーティング システム（OS）、OS のバージョン、およびサービス（アプリケーション名とバージョン）を検出するように設計されています。

他の ISE プローブは、エンドポイント自体を直接調査するのではなく、デバイスによって（または他のネットワーク デバイスから）生成されたデータの解析などの間接的なデータ収集手法に依存しているという意味で「パッシブ」（受動的）と見なされます。ネットワーク スキャン プローブは、ソースから情報を得るためにエンドポイントと直接通信するため、「アクティブ」（能動的）なアセスメント メカニズムと見なされます。

## NMAP プローブ スキャン動作

NMAP プローブがスキャンを実行するときには、次の NMAP 操作の 1 つ以上を実行できます。

- オペレーティング システム スキャン
- SNMP ポート スキャン
- 一般ポート スキャン

オペレーティング システム（OS）スキャンは、エンドポイントの OS とバージョンを検出するために使用されます。これは、負荷の大きい操作です。

SNMP ポート スキャンは、UDP ポート161（SNMP デーモン）と 162（SNMP トラップ）が開いているかどうか検出を試みます。開いている場合、コミュニティ ストリング **public** を使用して SNMP クエリーがエンドポイントに発行され、システム MIB などからエンドポイントに関する追加情報が収集されます。このプローブは、デフォルト コミュニティ ストリング **public** を使ってデフォルトで SNMP が有効になっているネットワーク プリンタなどのエンドポイントで特に役立つことが実証されています。

注：NMAP プローブは、エンドポイントに直接照会するためにデフォルト コミュニティ ストリング public を限定的に使用できます。この値は現在、設定不可です。
これと SNMP クエリー プローブを混同しないでください。SNMP クエリー プローブはエンドポイントではなくネットワーク デバイスに照会し、ネットワーク デバイス設定で SNMP を設定可能です。

共通ポート スキャンは、表 5 に示すように、15 個の一般的な TCP ポートと UDP ポートのスキャンを実行します。

表 3 NMAP プローブの共通ポート スキャン：TCP ポートと UDP ポート

| TCP ポート | | | UDP ポート | |
|---|---|---|---|---|
| ポート | サービス | | ポート | サービス |
| 21/tcp | FTP | | 53/udp | ドメイン |
| 22/tcp | ssh | | 67/udp | dhcps |
| 23/tcp | telnet | | 68/udp | dhcpc |
| 25/tcp | smtp | | 123/udp | ntp |
| 53/tcp | ドメイン | | 135/udp | msrpc |
| 80/tcp | http | | 137/udp | netbios-ns |
| 110/tcp | pop3 | | 138/udp | netbios-dgm |
| 135/tcp | msrpc | | 139/udp | netbios-ssn |
| 139/tcp | netbios-ssn | | 161/udp | snmp |
| 143/tcp | imap | | 445/udp | microsoft-ds |
| 443/tcp | https | | 500/udp | isakmp |
| 445/tcp | microsoft-ds | | 520/udp | ルート |
| 3306/tcp | mysql | | 631/udp | ipp |
| 3389/tcp | ms-term-serv | | 1434/udp | ms-sql-m |
| 8080/tcp | http-proxy | | 1900/udp | upnp |

注:スキャンされた共通ポートのリストは現在、設定不可です。

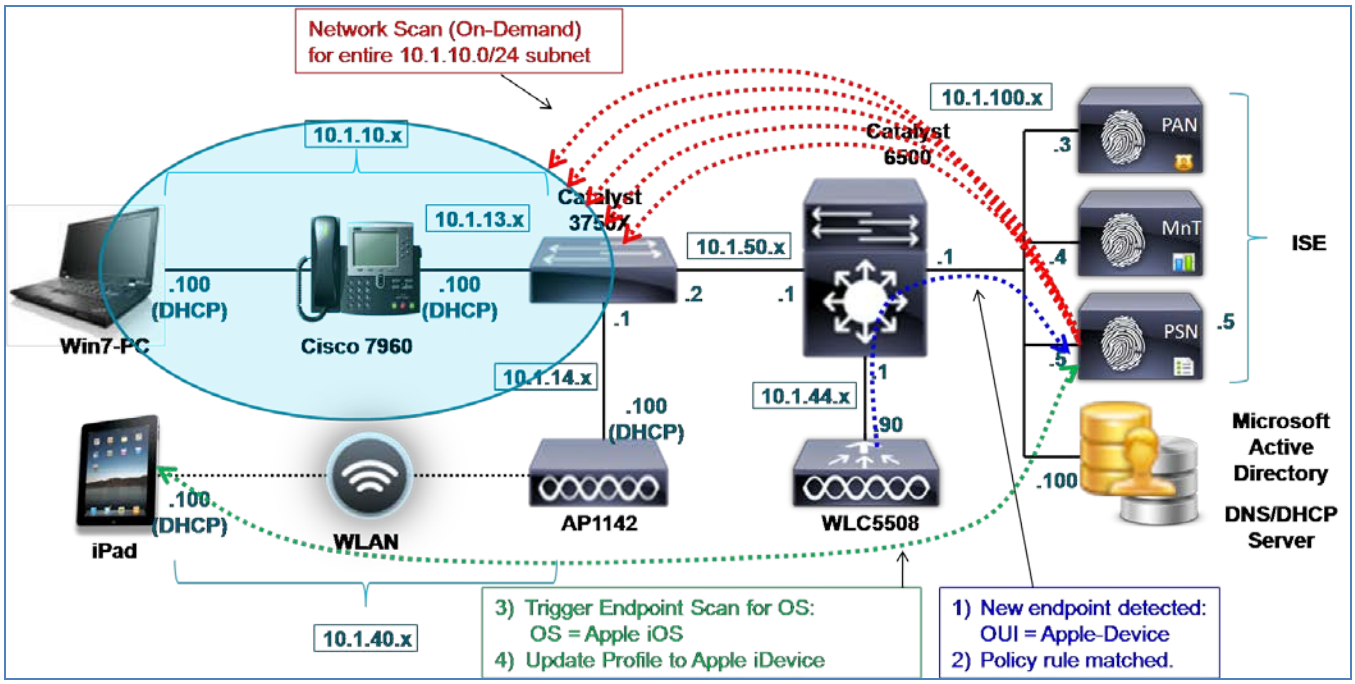
管理者は、実行されたサービスに基づいてエンドポイントを分類して個別に保護することができます。たとえば、Web サービスを実行する Windows サーバを非 HTTP 要求から確実に保護するために特定の認可ポリシー(dACL、VLAN、SGT)を適用する必要が生じることがあります。逆に、同様の認可方式を使用して、Web サーバを実行する Windows または Linux ワークステーションのアクセスを拒否または隔離する必要が生じることがあります。

次のいずれかの方法で NMAP プローブを開始できます。

- ネットワーク スキャン
- エンドポイント スキャン

図 55 のサンプル トポロジは、10.1.10/24 サブネットで開始されるネットワーク スキャンを示しています(赤色で強調表示)。

図 503 NMAP プローブの例




## NMAP プローブ ネットワーク スキャン

ネットワーク スキャンは、1 つ以上のネットワーク エンドポイントに対するオンデマンド スキャンです。これは、ISE 管理ノードから管理ユーザによって手動で開始されます。手動ネットワーク スキャンを実行するために、ポリシー サービス ノード上でプローブを有効にする必要さえありません。単に管理ユーザがスキャン対象の IP サブネットを指定して[スキャンの実行(Run Scan)]ボタンをクリックするだけです。

ネットワーク スキャンは、SNMP ポート スキャンとオペレーティング システム スキャンの両方を実行します。大規模ネットワークのスキャンは時間がかかるうえ、ポリシー サービス ノードの負荷が増えるため、サブネットの範囲を注意深く選択することをお勧めします。スキャンを開始した後、管理ユーザは結果が表示されるページに移動するリンクをクリックできます。

## NMAP プローブ エンドポイント スキャン

エンドポイント スキャンは 1 つのエンドポイントに対してトリガーされるスキャンです。これは、プロファイリング ポリシー内の一致するルールに基づいて自動的に開始されます。スキャンがトリガーされるためには、プロファイル ポリシーと、ネットワーク スキャン アクションが割り当てられた特定の条件の両方にエンドポイントが一致する必要があります。ネットワーク スキャン アクションは、プロファイル ルールごとに設定可能で、実行する特定のスキャン操作を定義します。

デフォルトで、一致したプロファイル条件への応答として割り当てることが可能な 3 つの NMAP アクションがあります。

- **CommonPortsAndOS-scan**（共通ポート + OS スキャン）
- **OS-scan**（OS スキャンのみ）
- **SNMPPortsAndOS-scan**（SNMP ポート + OS スキャン）

図 55 のサンプル トポロジはこのプロセスを示しています。最新のプローブ イベントの結果として新しいエンドポイントが検出されます（青色で表示）。収集されたプロファイル データに基づき、MAC アドレスからの OUI によってエンドポイントが Apple デバイスであることはわかりますが、それが Mac OS X ワークステーションなのか、Apple iDevice なのか、または他の Apple エンドポイントなのかは不明です。Apple デバイスに対して指定された OS スキャンをトリガーするポリシー ルールが照合されます（緑色で表示）。その結果、エンドポイントが Apple iOS を実行していることが学習され、そのプロファイルが Apple モバイル デバイス プロファイルに更新されます。

「不明」プロファイルに一致するエンドポイントは、SNMP ポート スキャンと OS スキャンの両方を使用して自動的にスキャンされます。これは、設定可能な応答ではありません。この目的は、発見されたがプロファイルされていないエンドポイントに関する詳細情報を ISE プロファイリングで迅速に取得できるようにすることです。

注：一部のエンドポイントでは、パーソナル ファイアウォールまたは他のエージェント ソフトウェアが有効化されているため、エンドポイントのスキャンがブロックされます。このようなエンドポイントは、ほとんどまたは全く NMAP データを生成しません。加えて、ネットワーク アクセスが制限されたエンドポイントは、NMAP 操作を受信または応答できない場合があります。

## NMAP プローブと IP/MAC アドレス間バインドの要件

NMAP は既知の IP アドレスに基づいています。NMAP プローブがエンドポイントの属性を収集しても、それを特定の MAC アドレスに関連付けることができない場合は、そのデータが破棄されます。ポリシー サービス ノードが、スキャン対象のエンドポイントと同じセグメントに存在する場合は、ローカル ARP キャッシュから IP/MAC アドレス間バインドを学習して、そのエンドポイントを内部エンドポイント データベースに直接追加することができます。そのため、NMAP プローブ データを収集する**前**に、別のプローブ経由で IP/MAC アドレス間バインドを学習する必要があります。この情報を提供するために使用可能なプローブには、以下が含まれます。

- RADIUS（Framed-IP-Address 経由）
- DHCP（dhcp-requested-address 経由）
- SNMP クエリー（SNMP ポーリングを介して）

**シスコ ベスト プラクティス**：ISE がまだエンドポイントを認証していない ISE 展開のディスカバリ フェーズで、より大きなネットワーク ブロックに対してネットワーク スキャンを実行して、エンドポイントおよび関連する OS 情報とエンドポイント情報をスキャン/検出することができます。また、このフェーズ中に、エンドポイント ARP テーブル情報を保存するすべてのネットワーク デバイスに関して SNMP クエリー プローブを有効にすることもお勧めします。これにより、静的にアドレス指定されたエンドポイントを含めて、エンドポイント MAC アドレスと IP アドレスの検出が可能になります。さらに、ネットワーク スキャン中に検出された IP アドレスごとの MAC アドレスがこうして PSN に提供されるため、NMAP プローブ収集がサポートされます。

# NMAP プローブの設定

前述したように、NMAP プローブを実行する方法として、手動のオンデマンド ネットワーク スキャンと、1 つのエンドポイントに対して自動的にトリガーされるスキャン イベントの 2 つがあります。それぞれの方法を使用する手順を別々に説明します。

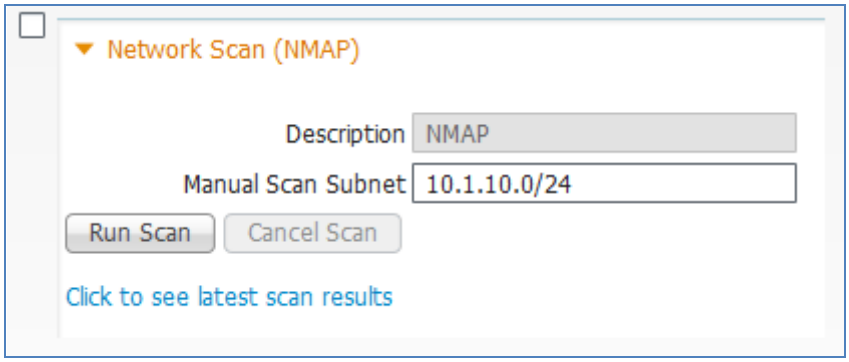
### ネットワーク スキャンの実行

**ステップ 1** [管理(Administration)] → [システム(System)] → [展開(Deployment)] にアクセスして、RHS ペインで展開されたノードのリストからネットワーク スキャンを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定(Profiling Configuration)] タブを選択します。

**ステップ 3** ネットワーク スキャンを実行するには、[ネットワークスキャン(NMAP) (Network Scan (NMAP))] オプションを選択して、その内容を展開します(図 56)。

図 51 NMAP プローブ




注:図 56 に示すように、手動ネットワーク スキャンを実行するためにプローブを有効にする必要はありません。

**ステップ 4** 例に示す形式で、スキャンする IP サブネット アドレスとマスクを入力します。この例では、クラス C サブネット(10.1.10.0)、およびクラス C サブネットに適切な数のマスク ビット(24)が入力されています。

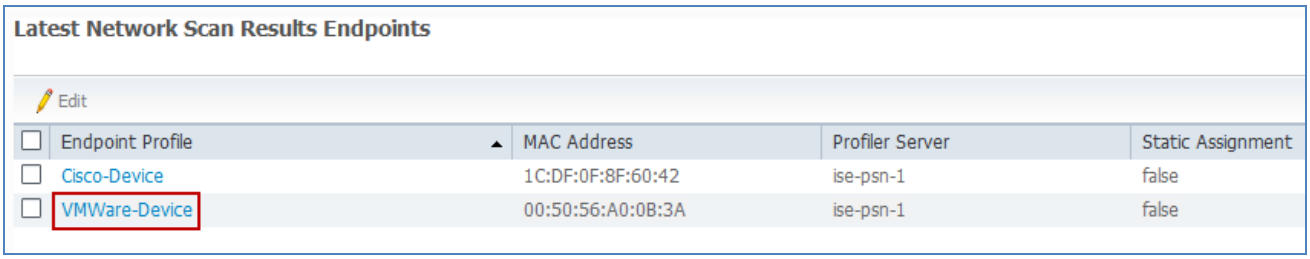
**ステップ 5** 他のサブネット サイズを選択することもできますが、スキャン実行にかかる全体的な時間と負荷を削減するために、対象となるネットワークの範囲とエンドポイントの数を考慮して選択する必要があります。

**ステップ 6** [スキャンの実行(Run Scan)] をクリックします。

**ステップ 7** アクティブ スキャンをキャンセルするには、[スキャンのキャンセル(Cancel Scan)] をクリックします。それ以外の場合は [最新のスキャン結果を表示するためにクリック(Click to see latest scan results)] を選択して、[管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] ページに直接移動します。このページから移動した後でも、スキャンは完了するまで続行されます。

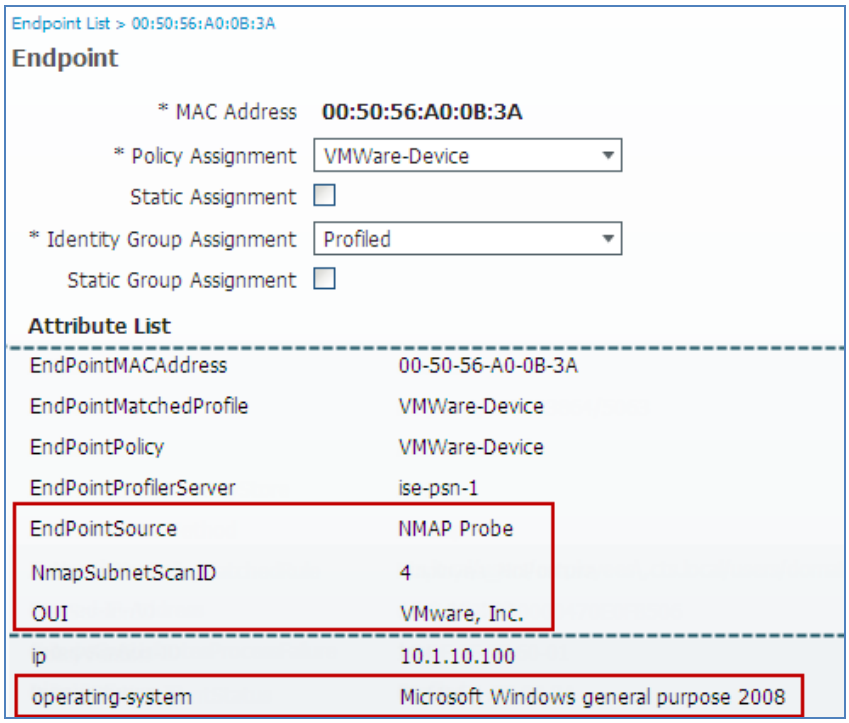
**ステップ 8** [ID(Identities)] ページの LHS ペインで、[最新のネットワークスキャン結果(Latest Network Scan Results)] を選択します。スキャンの進捗状況に応じて、有効なスキャン結果を持つエンドポイントが RHS ペインに表示されます(図 57)。

図 52 NMAP ネットワーク スキャン結果の例




**ステップ 9**　MAC アドレス別のエンドポイント エントリをクリックすると、結果が表示されます。

図 53 ネットワーク スキャンからの NMAP プローブ属性の例




選択されたエンドポイントは Windows 7 PC です。手動ネットワーク スキャンの出力からわかるように、NMAP は汎用 OS クラス（Windows 7 と Windows 2008 が共通コード ベースを共有）を検出しましたが、情報が不十分なため、OUI 条件との照合に基づく現在の VMware プロファイルを越えてエンドポイントを分類することはできません。EndPointSource が NMAP プローブとして表示されます。ScanID は、手動ネットワーク スキャン イベントに割り当てられた ID を意味します。

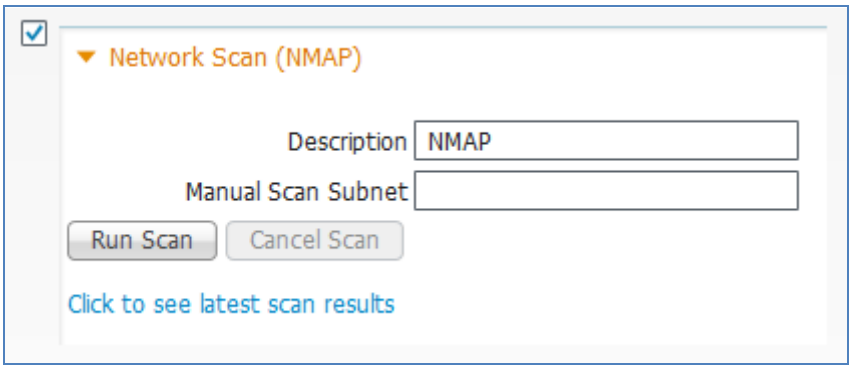
注：NMAP プローブから正常にスキャンできるようにするために、デフォルトの Windows 7 ファイアウォール設定を無効にする必要がありました。

## エンドポイント スキャン用の NMAP プローブの設定

**ステップ 1** [管理（Administration）] → [システム（System）] → [展開（Deployment）] にアクセスして、RHS ペインで展開されたノードのリストからプロファイリングを実行するポリシー サービス ノードを選択します。

**ステップ 2** [プロファイリング設定（Profiling Configuration）] タブを選択して、[ネットワークスキャン（NMAP）（Network Scan (NMAP)）] というラベルの付いたボックスをオンにします（図 59）。

図 54 NMAP プローブの設定




**ステップ 3** [保存（Save）] をクリックして、変更をコミットします。

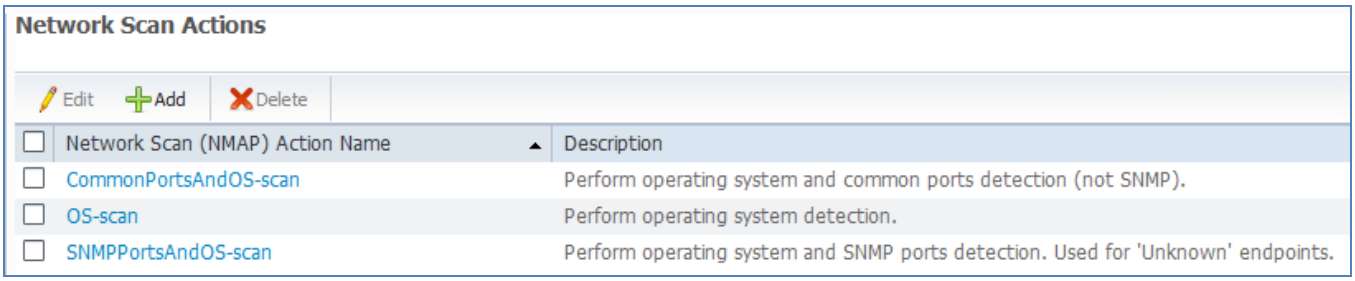
**ステップ 4** プロファイリング サービスで設定された他のすべてのポリシー サービス ノードに関して、この手順を繰り返します。

## ネットワーク スキャン（NMAP）アクションの確認

**ステップ 1** [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] にアクセスして、LHS ペインから [プロファイリング（Profiling）] → [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] を選択します。

**ステップ 2** デフォルトの NMAP アクションを確認します（図 60）。

図 55 NMAP スキャン アクション

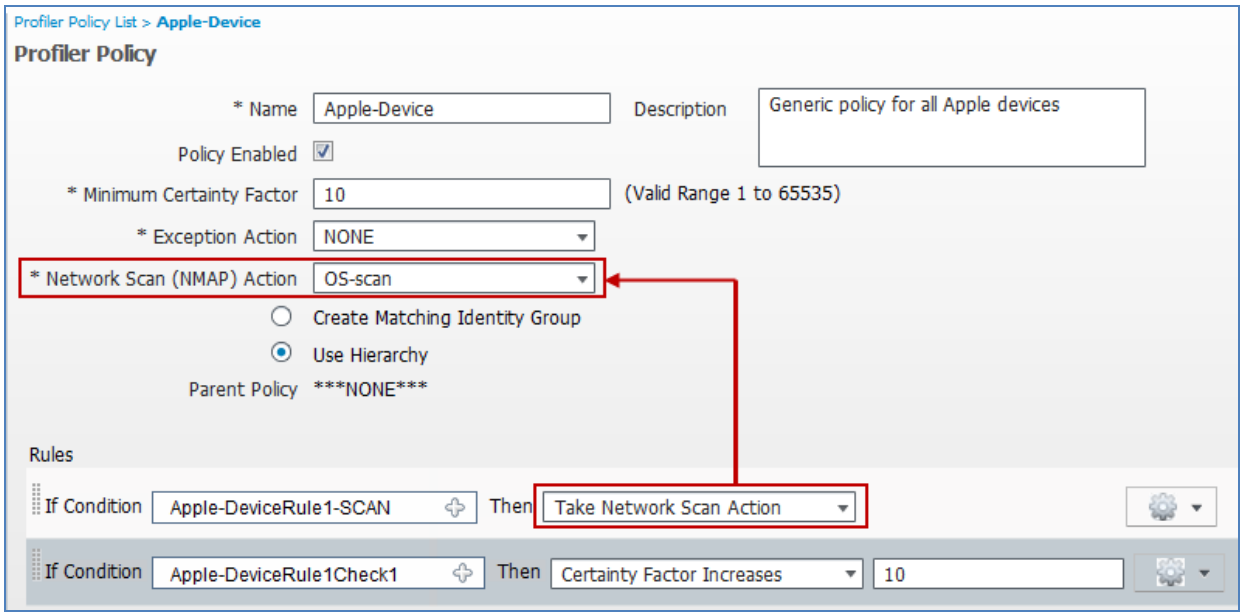



**ステップ 3** 最も一般的なオプションが設定されていますが、必要に応じて追加の NMAP アクションを定義できます。たとえば、トリガーされた応答の一部として共通ポートまたは SNMP ポートのスキャンだけを実行する **CommonPorts** または **SNMPPorts** という名前の新しいスキャン アクションを作成できます。

## プロファイリング ポリシー条件に NMAP アクションを割り当てるための設定の確認

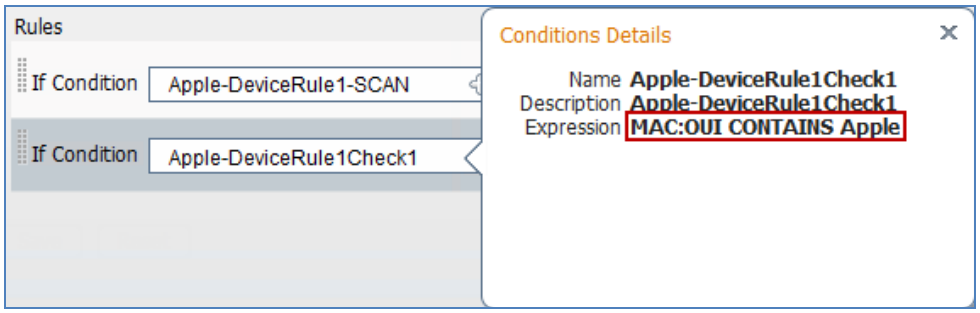
**ステップ 1** [ポリシー（Policy）] → [プロファイリング（Profiling）] にアクセスして、RHS ペインのリストから Apple-Device プロファイルを選択します（図 61）。

図 56 NMAP スキャン アクションを使用したプロファイリング ポリシーの例




**ステップ 2** Apple-Device プロファイルには 2 つの条件が含まれています。2 番目の条件名の右側をクリックして、ルール エントリの内容を確認します（図 62）。

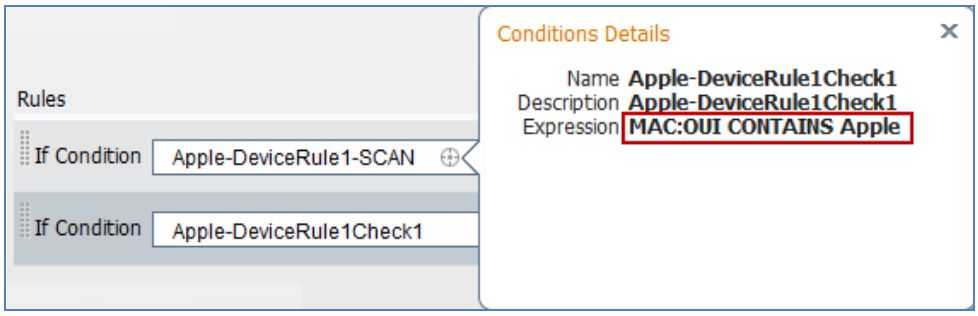
図 57 NMAP スキャンのプロファイリング ポリシー ルールの例 1




このルールは、確実度係数（CF）を増やすことでこのプロファイルにエンドポイントを照合するために使用されます。MAC アドレスの OUI が "Apple" に一致した場合、条件が一致します。

**ステップ 3** 1 番目の条件名の右側をクリックして、内容を確認します（図 63）。

図 58 NMAP スキャンのプロファイリング ポリシー ルールの例 2




このルールは、エンドポイント スキャンをトリガーするために使用されます。1 番目の条件は、2 番目のルールで使用されている条件と同じです。したがって、2 番目の条件に基づいてこのプロファイルに一致するエンドポイントは、自動的に 1 番目のルールに一致し、選択されたネットワーク スキャン アクション（OS-scan）をトリガーします。

既存のルール テーブルの右側にある歯車アイコンをクリックすると、個別のルール エントリを追加または削除できます。

**ステップ 4** 確認または変更が終わったら、ページの下部にある [保存（Save）] をクリックして変更をコミットします。

この手順の目的は、一致する条件に基づいてネットワーク スキャン アクションをプロファイルにどのように適用できるかを確認することです。プロファイリング ポリシーの設定については、「プロファイリング ポリシーの設定」の項で詳しく説明します。

### トリガーされたエンドポイント スキャン アクションに基づく NMAP プローブ データの確認

**ステップ 1** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] からエンドポイントを削除します。

**ステップ 2** NMAP プローブを使ったプロファイリングをサポートするように設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

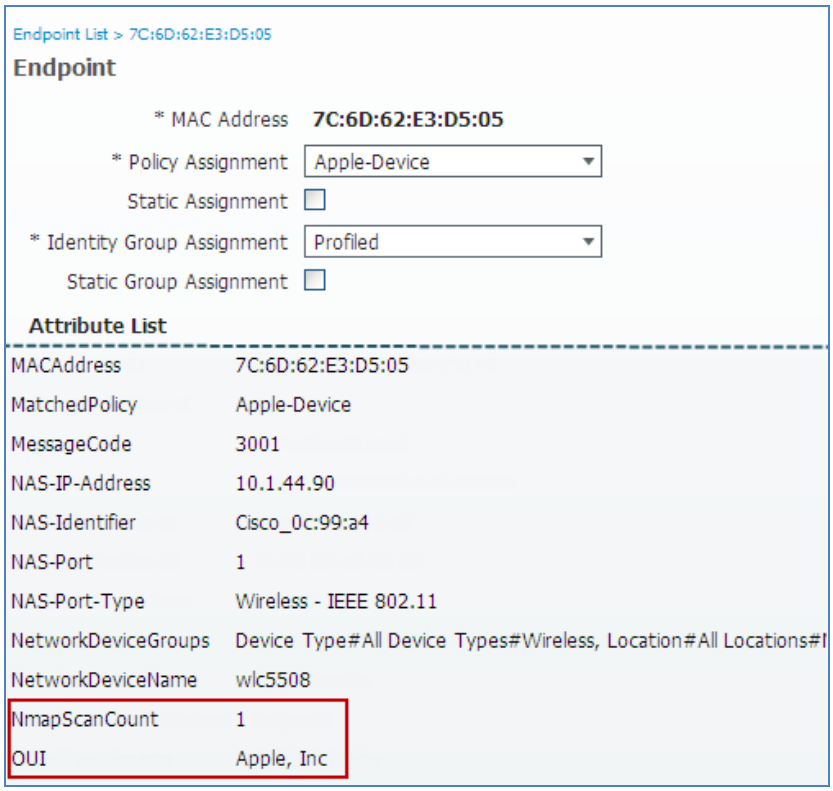
**ステップ 3** ISE ポリシー管理ノードにアクセスして、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] に移動します。

**ステップ 4** LHS ペインで、[エンドポイント（Endpoints）] を選択します。

**ステップ 5** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、HTTP プローブによってキャプチャされた属性を表示します。

**ステップ 6** この例では、NMAP プローブに加えて、RADIUS プローブと DHCP（IP ヘルパー）プローブのみが有効にされます。これらの追加のプローブを使用して新しいエンドポイントを検出し、適切な MAC アドレスおよび IP アドレス情報とともにそれらを内部エンドポイント データベースに追加します。これにより NMAP プローブ データが正しく適用され、破棄されないようになります。

図 59 エンドポイント スキャンからの NMAP プローブ属性の例 1



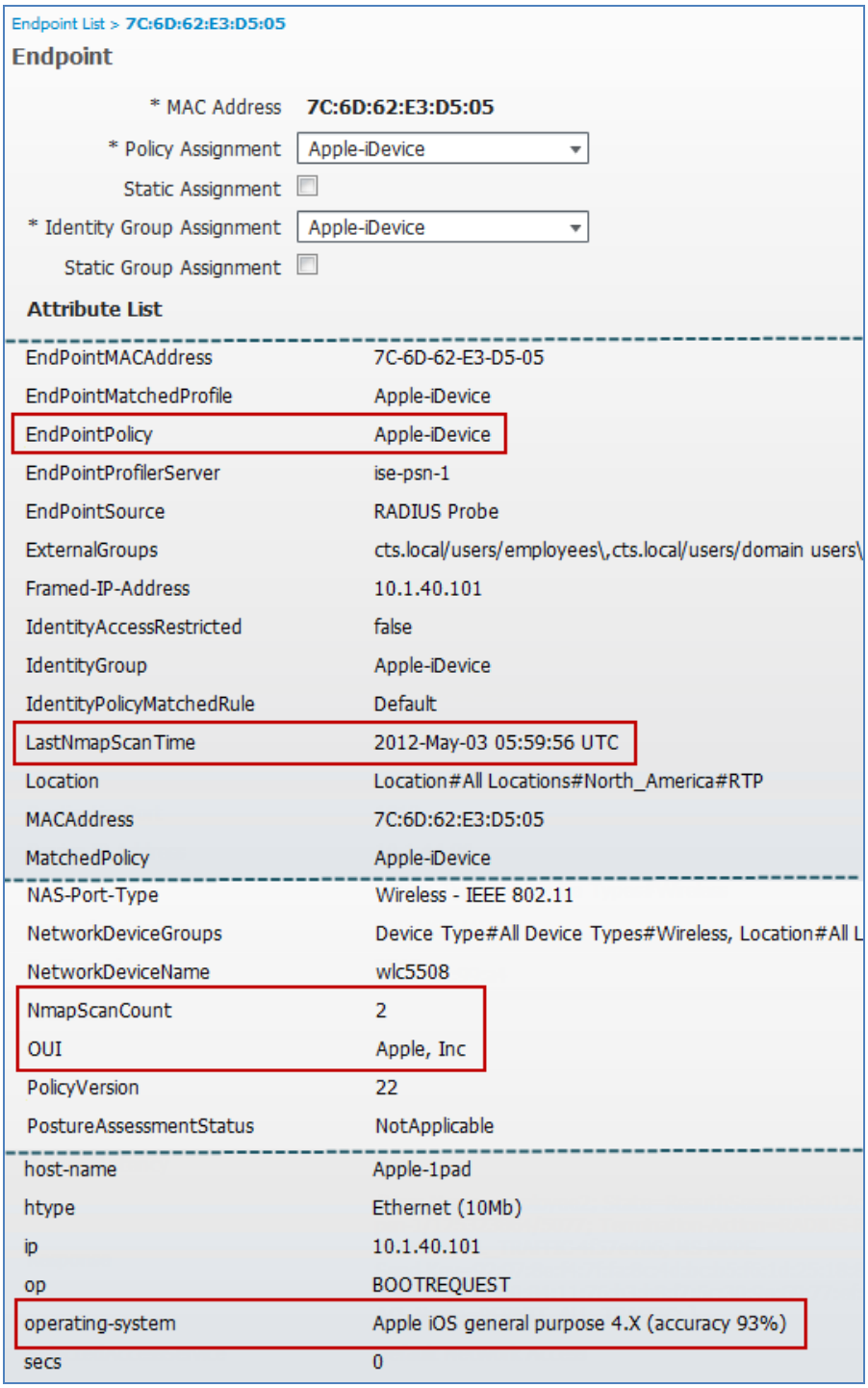

省略された出力は、このエンドポイント（**NmapScanCount**）に対して初期スキャンが実行されたが、Apple へのプロファイル割り当てがまだ OUI に基づいていることを示しています。Apple-Device に関する一致するプロファイル条件に基づいてスキャンがトリガーされます。

短時間で OS スキャンが完了するはずです。エンドポイントを終了し、同じエンドポイントを再び選択して、更新されたプロファイリング属性を確認します（図 65）。

強調表示されるキー属性は次のとおりです。

- EndPointPolicy
- LastNmapScanTime
- NmapScanCount
- OUI
- operating-system

図 60 エンドポイント スキャンからの NMAP プローブ属性の例 2

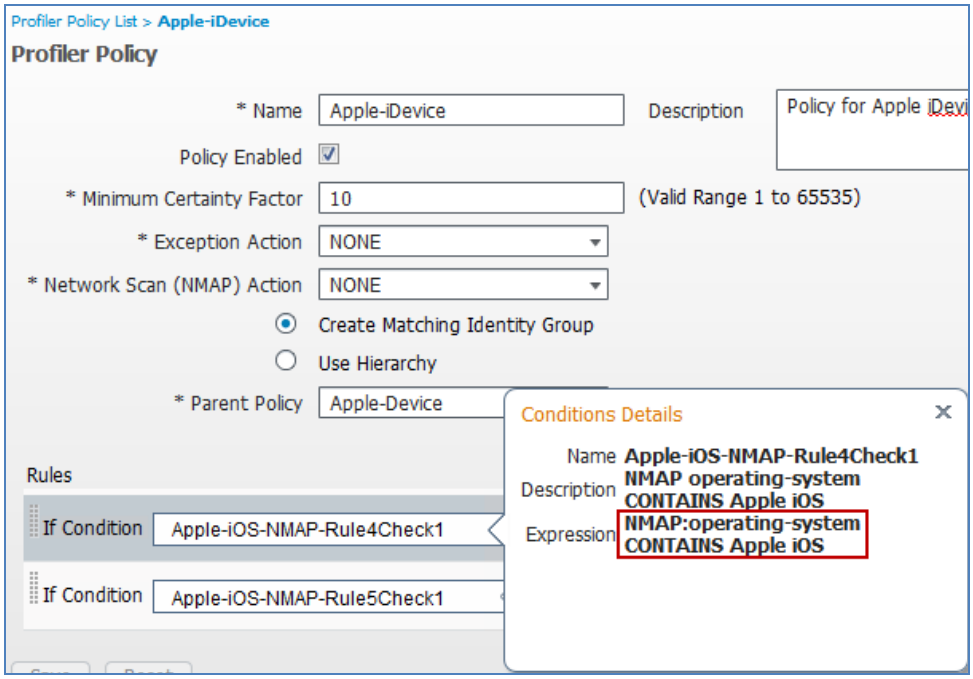



この例では、NMAP スキャンが完了していることが明らかです。**EndPointSource** 属性は、RADIUS が最後の更新を行ったことを示しています。さまざまなソースがプロファイリング データを提供するのに合わせて、値が頻繁に変化するため、この状態が発生する可能性があります。

**LastNmapScanTime** 属性と **NmapScanCount** 属性はデバイス分類にとってそれほど重要ではありませんが、NMAP プローブによって追加された属性を示すために強調表示されています。

**OUI** 属性は Apple ですが、割り当てられているプロファイルは、より一般的な Apple-Device ではなく Apple-iDevice のプロファイルになりました。これは、トリガーされた NMAP スキャン結果の一致により、エンドポイント OS が Apple iOS であることが明らかになったためです。[ポリシー(Policy)] → [プロファイリング(Profiling)] で Apple iDevice プロファイルの内容を確認すれば、このプロファイルが NMAP OS スキャン結果に基づいて 2 つの条件のどちらかで一致することを確認できます(図 66)。

図 61 Apple-iDevice 用のプロファイリング ポリシー




**ステップ 7** このプロファイルは、Apple iOS と Apple iPhone OS のどちらかを含む **operating-system** 属性値が NMAP スキャンから返された場合に一致します。この例では、Apple iOS で一致しています。

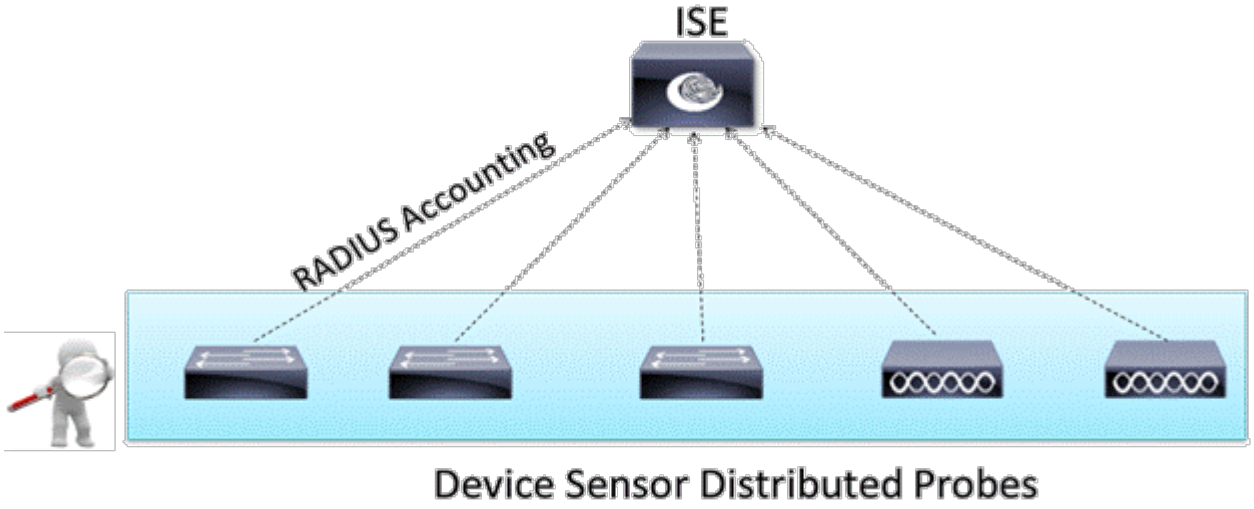
**ステップ 8** 要約すると、NMAP プローブは、オペレーティング システム スキャンによって判別されるオペレーティング システムに基づいてエンドポイントを分類するうえで役立ちます。クライアントレス デバイスの多くが、デバイス分類のために照会可能な SNMP エージェントをサポートします。他のデバイスはオープン ポートに基づいて分類することができ、ポリシーによって、特定のサービスを実行する特定のデバイスにさまざまな程度の制限付き権限を付与するよう制御できます。認可ポリシーの割り当てに関係なく、各プローブは可視性をさらに高めることができ、これはネットワーク全体の運用管理とセキュリティ管理にとって重要になる可能性があります。

# デバイス センサー

## デバイス センサーの概要

デバイス センサーは、Cisco Catalyst 3650 シリーズ スイッチ、3750 シリーズ スイッチ、4500 シリーズ スイッチなどのシスコ アクセス スイッチやワイヤレス コントローラで現在サポートされているアクセス デバイス機能です。デバイス センサーは、接続されたエンドポイントから Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Dynamic Host Configuration Protocol（DHCP）などのプロトコルを介してネットワーク情報を収集し、RADIUS アカウンティング パケットで ISE PSN に転送します（図 67）。ISE は、RADIUS プローブだけを使用して、プロファイリング データを収集して解析できます。

図 62 デバイス センサーの概要




## デバイス センサーの詳細

デバイス センサーは、ネットワーク デバイスから未加工のエンドポイント データを収集します。収集されたエンドポイント情報は、スイッチのプロファイリング機能の実行を支援します。アクセス デバイスのプロファイリング機能は、次の 2 つの部分で構成されます。

コレクタ：ネットワーク デバイスからエンドポイント データを収集します。

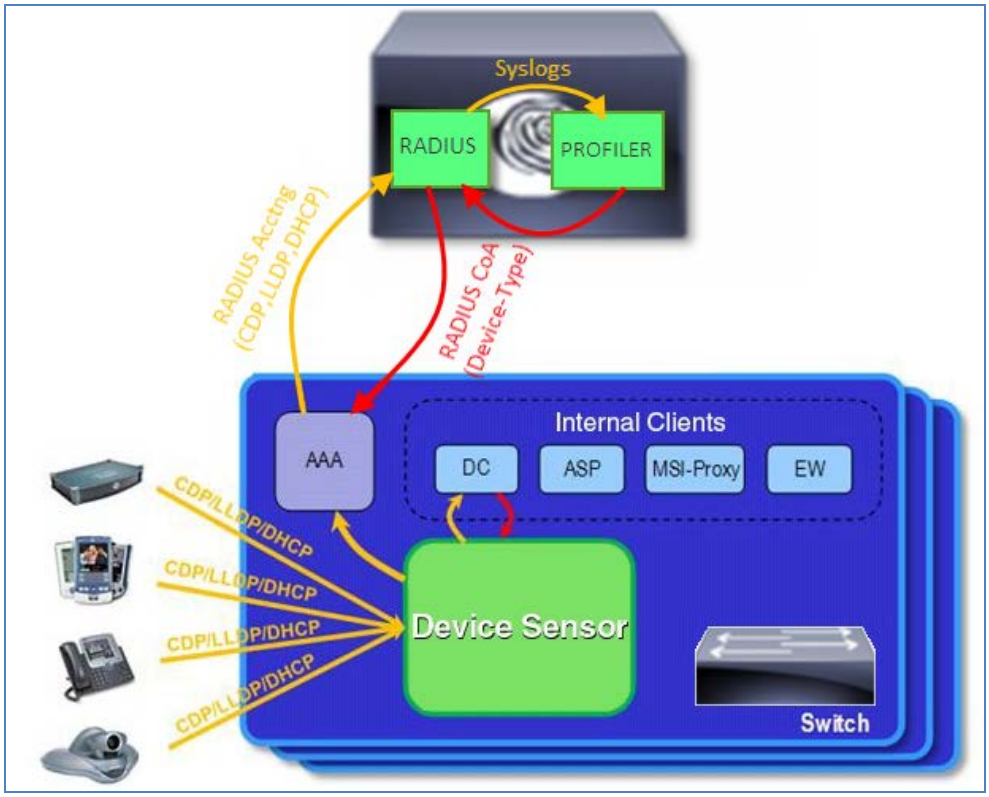
アナライザ：データを処理して、デバイスのタイプを決定します。

デバイス センサーは、Cisco Catalyst スイッチやシスコ ワイヤレス LAN コントローラなどのアクセス デバイスの組み込みコレクタ機能です。図 68 では、プロファイリング システムとデバイス センサーの関係を示すとともに、考えられる他のセンサー データのコンシューマも示しています。

センサー機能を備えたスイッチまたはワイヤレス コントローラは、CDP、LLDP、DHCP などのプロトコルを使用して、ネットワーク デバイスから、静的に設定されたフィルタの対象となるエンドポイント情報を収集し、登録済みクライアントがアクセス セッションのコンテキストでこの情報を使用できるようにします。アクセス セッションは、ネットワーク デバイスへのエンドポイントの接続を表します。

デバイス センサーには内部クライアントと外部クライアントがあります。内部クライアントには、組み込みの Device Classifier（DC またはローカル アナライザ）、Cisco Auto SmartPorts（ASP）、MSI-Proxy、Cisco EnergyWise™（EW）などのコンポーネントが含まれます。デバイス センサーは、RADIUS アカウンティングを使用して、Identity Services Engine（ISE）プロファイリング「アナライザ」などの外部クライアントにデータを送信します。

図 63 デバイス センサーの動作の詳細




プロファイリング データおよびセッション イベントや他のセッション関連データ（MAC アドレスや入力ポート データなど）を含むクライアント通知とアカウンティング メッセージが生成され、内部クライアントと外部クライアント（ISE）に送信されます。デフォルトで、サポートされている各ピア プロトコルごとに、プロファイリング属性、つまり、特定のセッションのコンテキストでまだ受信されていない type-length 値（TLV）が着信パケットに含まれている場合にのみクライアント通知とアカウンティング イベントが生成されます。新しい TLV が受信された、または、以前受信された TLV が CLI コマンドを使用して別の値で受信された、すべての TLV 変更に関するクライアント通知とアカウンティング イベントを有効にできます。

センサーは、ポート（アクセス ポートとトランク ポート）あたりの最大デバイス モニタリング セッション数を 32 に制限します。つまり、ポートごとに最大 32 のエンドポイントをモニタできます。非アクティビティ タイマーは、12 時間以上前のセッションをエージ アウトします。

## デバイス センサーの要件

表 6 に、アクセス デバイスとバージョン別のデバイス センサーのプロトコル サポートを示します。

表 4 デバイス センサーの要件

| プラットフォーム | CDP | LLDP | DHCP | HTTP | mDNS |
|---|---|---|---|---|---|
| Catalyst 3560/3750 シリーズ スイッチ | 15.0(1)SE1 | 15.0(1)SE1 | 15.0(1)SE1 | - | - |
| Catalyst 4500 シリーズ スイッチ | 15.1(1)SG IOS-XE 3.3.0SG | 15.1(1)SG IOS-XE 3.3.0SG | 15.1(1)SG IOS-XE 3.3.0SG | - | 15.1(1)SG IOS-XE 3.3.0SG |
| WLC/WiSM2 ワイヤレス コントローラ | - | - | 7.2.110.0 | 7.3 | - |

注:ソフトウェア バージョンと機能サポートを確認するには、プラットフォームの該当するリリース ノートを参照してください。たとえば、Cisco IOS ソフトウェア リリース 15.0(1)SE1 とデバイス センサー機能の要件を満たしていない Catalyst 3560 スイッチと 3750 スイッチがあります。

Catalyst 3560-C と 3560-CG シリーズ スイッチに対するデバイス センサー機能のサポートは、Cisco IOS ソフトウェア リリース 15.0(2)SE で提供されます。

デバイス センサーがシスコ ワイヤレス コントローラに展開されている場合は、検知用に設定された WLAN に参加しているすべてのクライアントに対して DHCP プロファイリングが有効にされます。DHCP プロキシ モードとブリッジド モードの両方がクライアント DHCP 要求に対してサポートされます。7.2MR1 の制約事項には以下が含まれます。

スタンドアロン アクセス ポイントはサポートされません。

ローカル スイッチングを使用したローカル認証はサポートされません。

つまり、デバイス センサーは ISE プロファイリング サービスのデータ収集のスケーリングに大きなメリットをもたらします。デバイス センサーを使用すると、データ収集がアクセス レイヤ、エンドポイントに最も近いポイント、およびデータのソース全体で高度に分散されます。その後で、情報が発信源で選択的にフィルタリングされ、RADIUS アカウンティング パケットで集中型ポリシー サービス ノードに送信されて、そこで分析および分類されます。これにより、従来の ISE プローブを使用してこの同じデータをキャプチャする場合の設計の課題とインフラストラクチャの要件の多くが軽減されます。

# ISE プロファイリング用のデバイス センサーの設定

Device Classifier は、MAC-OUI およびプロトコル（CDP、LLDP、DHCP など）から、デバイスを識別する情報を収集します。CDP 情報と LLDP 情報を収集するには、Catalyst スイッチ上で CDP と LLDP を有効にする必要があります。DHCP オプション情報を DC で入手できるようにするには、スイッチ上で DHCP スヌーピング機能を有効にする必要があります。シスコ ワイヤレス LAN コントローラは、現在、DHCP データしかサポートしていません。そのため、アナライザ（ISE）に送信される特定の属性とオプションを指定するフィルタを定義できます。センサー データを ISE に送信するには、アクセス デバイスで RADIUS アカウンティングを有効にする必要があります。ISE は、RADIUS プローブが有効になっており、正しく設定されている必要があります。

注：センサー データを ISE に転送するには、RADIUS アカウンティングが必要です。ただし、センサー データを収集して ISE に送信するために、RADIUS 認証および認可は必要ありません。そのため、モニタ モードのみの場合でも、組織が RADIUS 認証を有効にする準備ができていないネットワーク ディスカバリ フェーズ中に ISE 前展開にデバイス センサーを使用することができます。このサポートは、RADIUS アクセス制御が展開されていない Cisco NAC アプライアンスと ISE プロファイリング サービスを使用した展開にまで及びます。

## ISE での RADIUS プローブの有効化

**ステップ 9** RADIUS プローブを有効にする手順は、「RADIUS プローブの設定」の項で詳しく説明します。RADIUS プローブの正しい有効化と設定に関する項を参照してください。

**ステップ 10** この項に記載された手順に対する例外は、RADIUS ベースの認証および認可を使用しない展開でのデバイス センサーの使用に関係します。このシナリオでは、アクセス デバイスが ISE に追加されていないものとしますが、アクセス デバイスが RADIUS アカウンティングを ISE に伝達する必要があるため、[管理（Administration）] → [ネットワークリソース（Network Resources）] → [ネットワークデバイス（Network Devices）] でデバイス センサーをサポートするすべてのアクセス デバイスを追加する必要があります。

**ステップ 11** ISE で入力された IP アドレスが、RADIUS を送信するためにアクセス デバイスから供給された値と一致することを確認します。また、RADIUS 共有キーがアクセス デバイス上で設定された値と一致することを確認します。これらのステップは、デバイス センサーからの RADIUS アカウンティング パケットの受信をサポートするために必要です。

## シスコ有線スイッチ上でのプロファイリング プロトコルの有効化

エンドポイントから CDP、LLDP、または DHCP 属性を収集するには、アクセス スイッチでこれらのプロトコルを有効にして、関連する属性を読み取って収集できるようにする必要があります。

**ステップ 12** デバイス センサー サポートを備えたアクセス スイッチのコマンド コンソールにアクセスします。

**ステップ 13** CDP をサポートするスイッチを有効にします。

**ステップ 14** CDP は、デフォルトで、シスコ スイッチ上でグローバルに有効になっています。無効になっている場合は、次のグローバル コマンドを使用して有効にします。

```
cat3750x(config)# cdp run
```

**ステップ 15** CDP は、デフォルトで、スイッチポートごとに有効になっています。無効になっている場合は、次のインターフェイス コマンドを使用して有効にします。

```
cat3750x(config-if)# cdp enable
```

**ステップ 16** 次に示す **show cdp neighbors** コマンドを使用して、CDP がスイッチ上で動作していることを確認します。

```
cat3750x# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
APc471.fe34.197a Gig 1/0/2         137              T    AIR-LAP11 Gig 0
SEP003094C4528A  Gig 1/0/1         150            H P M  IP Phone  Port 1
cat6503.cts.local
                 Gig 1/0/24        140            R S I  WS-C6503  Gig 2/47
```

ここで、詳細ビューを示します。

```
cat3750x# show cdp neighbors detail
-------------------------
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9   ,  Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2,  Port ID (outgoing port): GigabitEthernet0
Holdtime : 133 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 21756, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):

-------------------------
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): Port 1
Holdtime : 147 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):
```

```
-------------------------
Device ID: cat6503.cts.local
Entry address(es):
  IP address: 10.1.50.1
Platform: cisco WS-C6503,  Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/24,  Port ID (outgoing port): GigabitEthernet2/47
Holdtime : 136 sec

Version :
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Versio
n 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 14-Dec-11 19:51 by prod_rel_team

advertisement version: 2
VTP Management Domain: 'cts'
Duplex: full
Management address(es):
  IP address: 10.1.50.1
```

**ステップ 17** LLDP をサポートするスイッチを有効にします。

**ステップ 18** LLDP は、デフォルトで、シスコ スイッチ上でグローバルに無効になっています。これを有効にするには、次のグローバル コマンドを入力します。

```
cat3750x(config)# lldp run
```

**ステップ 19** LLDP は、デフォルトで、スイッチポートごとに有効になっています。無効になっている場合は、次のインターフェイス コマンドを使用して有効にします。

```
cat3750x(config-if)# lldp receive
```

**ステップ 20** 次に示す **show lldp neighbors** コマンドを使用して、LLDP がスイッチ上で動作していることを確認します。

```
cat3750x# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID Local Intf Hold-time Capability Port ID
AVA4FF00E Gi1/0/9 120 B 0004.0d4f.f00e
AVAEC8C79 Gi1/0/10 120 B 0004.0dec.8c79
AVAF694AC Gi1/0/15 120 B 0004.0df6.94ac
AVAEC8C79 Gi1/0/17 120 B 0004.0dec.8c79

Total entries displayed: 4
```

ここで、詳細ビューを示します。

```
cat3750x# show lldp neighbors detail
------------------------------------------------
Chassis id: 10.6.104.29
Port id: 0004.0d4f.f00e
Port Description - not advertised
System Name: AVA4FF00E
System Description - not advertised

Time remaining: 106 seconds
System Capabilities: B,T
Enabled Capabilities: B
Management Addresses:
IP: 10.X.104.29
OID:
1.3.6.1.4.1.6889.1.69.1.5.
Auto Negotiation - supported, enabled
Physical media capabilities:
Symm Pause(FD)
Pause(FD)
100base-TX(FD)
100base-TX(HD)
10base-T(FD)
10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

MED Codes:
(NP) Network Policy, (LI) Location Identification
(PS) Power Source Entity, (PD) Power Device
(IN) Inventory

H/W revision: 4620D01B
F/W revision: b20d01b2_9_1.bin
S/W revision: a20d01b2_9_1.bin
Serial number: 051606020284
Manufacturer: Avaya
Model: 4620
Capabilities: NP, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN dot1p, tagged, Layer-2 priority: 6, DSCP: 46
Power requirements - not advertised
Location - not advertised

----<snip>----

Total entries displayed: 4
```

**ステップ 21** DHCP をスヌープするスイッチを有効にします。グローバル コンフィギュレーション モードで次のコマンドを入力して、特定のアクセス VLAN 上で DHCP スヌーピングを有効にします。

```
cat3750x(config)# ip dhcp snooping
cat3750x(config)# ip dhcp snooping vlan <VLANs>
```

**ステップ 22** 少なくとも、プロファイリングするエンドポイントに接続されたアクセス VLAN がこのリストに含まれている必要があります。

**ステップ 23** 信頼できる DHCP サーバに直接的または間接的に接続されたインターフェイスから送信される DHCP 情報を信頼するには、次のインターフェイス コンフィギュレーション コマンドを使用します。

```
cat3750x(config)# interface <interface_to_DHCP_Server>
cat3750x(config-if)# ip dhcp relay information trusted
```

**ステップ 24** 次に示す **show ip dhcp snooping** コマンドを使用して、DHCP スヌーピングがスイッチ上で有効になっていることを確認します。

```
cat3750x# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-14
DHCP snooping is operational on following VLANs:
10-14
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 1cdf.0f8f.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
```

**ステップ 25** 次に示す **show ip dhcp snooping binding** コマンドを使用して、DHCP スヌーピングがスイッチ上で動作している（DHCP クライアント用のバインド テーブルが作成されている）ことを確認します。

```
cat3750x# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:94:C4:52:8A   10.1.13.100      691187      dhcp-snooping   13    GigabitEthernet1/0/1
00:50:56:A0:0B:3A   10.1.10.100      653260      dhcp-snooping   10    GigabitEthernet1/0/1
C4:71:FE:34:19:7A   10.1.14.100      653068      dhcp-snooping   14    GigabitEthernet1/0/2
Total number of bindings: 3
```

**ステップ 26** スイッチ設定に対する変更を保存します。

## シスコ有線スイッチ上でのデバイス センサーの設定

**ステップ 27** データ収集に含めるまたはそこから除外する CDP、LLDP、または DHCP 属性を選択するフィルタを定義します。

**ステップ 28** グローバル コンフィギュレーション モードで CDP 属性用のフィルタの開始を定義します。

```
cat3750x(config)# device-sensor filter-list cdp list <my_cdp_list>
cat3750x(config-sensor-cdplist)# tlv name device-name
cat3750x(config-sensor-cdplist)# tlv name address-type
cat3750x(config-sensor-cdplist)# tlv name capabilities-type
cat3750x(config-sensor-cdplist)# tlv name platform-type
cat3750x(config)# device-sensor filter-spec cdp include list <my_cdp_list>
```

**ステップ 29** CDP TLV 値は名前または番号で入力できます。CDP TLV 名には以下が含まれます。

| | |
|---|---|
| address-type | Address Type |
| capabilities-type | Capabilities Type |
| cos-type | COS Type |
| device-name | Device Name |
| duplex-type | Duplex Type |
| external-port-id-type | External Port Id Type |
| ipprefix-type | IP Prefix Type |
| mgmt-address-type | Management Address Type |
| mtu-type | MTU Type |
| native-vlan-type | Native VLAN Type |
| platform-type | Platform Type |
| port-id-type | Port Id type |
| power-available-type | Power Available Type |
| power-request-type | External Port Id Type |
| power-type | Power Type |
| protocol-hello-type | Protocol Hello Type |
| trigger-type | Trigger Type |
| trust-type | Trust Type |
| twoway-connectivity-type | Twoway Connectivity Type |
| unidirectional-mode-type | Unidirectional Mode Type |
| version-type | Version Type |
| vtp-mgmt-domain-type | VTP Management Domain Type |
| vvid-type | VVID Type |

**ステップ 30** 次のように、グローバル コンフィギュレーション モードで LLDP 属性用のフィルタの開始を定義します。

```
cat3750x(config)# device-sensor filter-list lldp list <my_lldp_list>
cat3750x(config-sensor-lldplist)# tlv name system-name
cat3750x(config-sensor-lldplist)# tlv name system-description
cat3750x(config)# device-sensor filter-spec lldp include list <my_lldp_list>
```

**ステップ 31** LLDP TLV 値は名前または番号で入力できます。LLDP TLV 名には以下が含まれます。

| | | |
|---|---|---|
| chassis-id | Chassis ID | Chassis Id |
| end-of-lldpdu | End Of LLDP | |
| management-address | Management Address | |
| port-description | Port Description | |
| port-id | Port Id | |
| system-capabilities | System Capabilities | |
| system-description | System Description | |
| system-name | System Name | |
| time-to-live | Time To Live | |

**ステップ 32** 次のように、グローバル コンフィギュレーション モードで DHCP 属性用のフィルタの開始を定義します。

```
cat3750x(config)# device-sensor filter-list dhcp list my_dhcp_list
cat3750x(config-sensor-dhcplist)# option name host-name
cat3750x(config-sensor-dhcplist)# option name default-ip-ttl
cat3750x(config-sensor-dhcplist)# option name requested-address
cat3750x(config-sensor-dhcplist)# option name parameter-request-list
cat3750x(config-sensor-dhcplist)# option name class-identifier
cat3750x(config-sensor-dhcplist)# option name client-identifier
cat3750x(config)# device-sensor filter-spec dhcp include list my_dhcp_list
```

**ステップ 33** DHCP オプションは名前または番号で入力できます。対象となる一般的なオプションには以下が含まれます。

| | |
|---|---|
| class-identifier | Class Identifier |
| client-fqdn | Client FQDN |
| client-identifier | Client Identifier |
| default-ip-ttl | Default IP Time To Live |
| domain-name | Domain Name |
| host-name | Host Name |
| server-identifier | Server ID |
| user-class-id | User Class ID |

…

**ベスト プラクティス**：CDP、LLDP、および DHCP に関して示したサンプル フィルタは、ほとんどのユースケースに適合する選択肢になります。使用可能な属性を調査するには、CDP と LLDP 用の show コマンドを使用して、ネットワーク内のエンドポイントが存在する TLV を確認し、特定の属性がエンドポイントの一意の分類を支援するかどうかを判断します。デバイス センサーをフィルタなしで展開してから、[管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] で ISE に提示される属性を確認することもできます。カスタマー エンドポイントのプロファイリング条件と一致する必要があると判断された属性に基づいて適切なフィルタを適用することができます。

注：特定の TLV またはオプション値を入力しても、その情報がエンドポイントによって送信されるわけではありません。フィルタは、エンドポイントがスイッチまたはネットワークに提示した属性に基づいて適用されます。たとえば、DHCP オプション client-fqdn がフィルタによって受け入れとして選択されていても、DHCP クライアントから要求されなければ、そのオプションに関する情報がデバイス センサーまたは ISE から参照できません。

**ステップ 34** 次のように、すべての変更を含む、センサー データが RADIUS アカウンティングで送信されるようにします。

```
cat3750x(config)# device-sensor accounting
cat3750x(config)# device-sensor notify all-changes
```

**ステップ 35** 重複更新が ISE に送信されないようにローカル アナライザを無効にします。

```
cat3750x(config)# no macro auto monitor
cat3750x(config)# access-session template monitor
```

組み込みの Device Classifier は、デフォルトで、シスコ スイッチ上で有効になっているため、自動的にデバイス センサーが有効になります。したがって、デバイス センサーもデフォルトで有効になります。RADIUS 認証およびアカウンティングがセンサー データを ISE に送信するために有効になっている場合は、TLV が変更されるたびに、重複した RADIUS アカウンティング パケットが送信されます。この原因は、ローカル アナライザによるセッション モニタリングです。アカウンティング メッセージの重複を避けるには、ローカル アナライザを無効にする必要があります。

RADIUS 認証が無効になっている（ISE 前展開/ディスカバリ フェーズ中のネットワークや Cisco NAC アプライアンスと ISE プロファイリング サービスが実装されているネットワークなどで）場合は、ローカル アナライザが無効になっていると、センサー データが送信されません。ローカル アナライザに関係なく、センサー データを送信できるようにするには、コマンド **access-session template monitor** を使用します。

**ステップ 36** RADIUS アカウンティングを使用して ISE にセッション アカウンティング情報を送信するようにスイッチを設定します。

**ステップ 37** RADIUS 認証および認可が設定されていれば、この手順はすでに完了しているはずです。RADIUS と ISE が通信するためのスイッチの設定方法については、「RADIUS プローブの設定」の項を参照してください。

**ステップ 38** RADIUS/802.1X がまだ展開されていない場合は、次のコマンドがスイッチ コンフィギュレーションに含まれていることを確認します。

```
cat3750x(config)# aaa new-model
cat3750x(config)# aaa accounting dot1x default start-stop group radius
cat3750x(config)# radius-server host <PSN_ip> auth-port <port> acct-port <port> key <shared-secret>
cat3750x(config)# radius-server vsa send accounting
```

**ステップ 39** デバイス センサーがプロファイリング情報を収集していることを確認します。

次のように、コマンド **show device-sensor cache** を使用して、デバイス センサーが正しく動作していることを確認します。

```
cat3750x# show device-sensor cache all
Device: 0050.56a0.0b3a on port GigabitEthernet1/0/1
-----------------------------------------------
Proto Type:Name                          Len Value
dhcp    55:parameter-request-list         14 37 0C 01 0F 03 06 2C 2E 2F 1F 21 79 F9 2B
dhcp    60:class-identifier               10 3C 08 4D 53 46 54 20 35 2E 30
dhcp    12:host-name                       9 0C 07 77 69 6E 37 2D 70 63
dhcp    50:requested-address               6 32 04 0A 01 0A 64
dhcp    61:client-identifier               9 3D 07 01 00 50 56 A0 0B 3A

Device: 0012.d9e3.427e on port GigabitEthernet1/0/24
-----------------------------------------------
Proto Type:Name                          Len Value
cdp      4:capabilities-type               8 00 04 00 08 00 00 00 29
cdp      2:address-type                   17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 32 01
cdp      6:platform-type                  18 00 06 00 12 63 69 73 63 6F 20 57 53 2D 43 36 35 30 33
cdp      1:device-name                    21 00 01 00 15 63 61 74 36 35 30 33 2E 63 74 73 2E
                                             6C 6F 63 61 6C

Device: c471.fe34.197a on port GigabitEthernet1/0/2
-----------------------------------------------
Proto Type:Name                          Len Value
cdp      4:capabilities-type               8 00 04 00 08 00 00 00 02
cdp      2:address-type                   17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0E 64
cdp      6:platform-type                  30 00 06 00 1E 63 69 73 63 6F 20 41 49 52 2D 4C 41
                                             50 31 31 34 32 4E 2D 41 2D 4B 39 20 20 20
cdp      1:device-name                    20 00 01 00 14 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp    50:requested-address               6 32 04 0A 01 0E 64
dhcp    60:class-identifier               16 3C 0E 43 69 73 63 6F 20 41 50 20 63 31 31 34 30
dhcp    55:parameter-request-list         10 37 08 01 06 0F 2C 03 21 96 2B
dhcp    12:host-name                      18 0C 10 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp    61:client-identifier               9 3D 07 01 C4 71 FE 34 19 7A

Device: 0030.94c4.528a on port GigabitEthernet1/0/1
-----------------------------------------------
Proto Type:Name                          Len Value
cdp      2:address-type                   17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0D 64
cdp      6:platform-type                  23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
                                             6E 65 20 37 39 36 30
cdp      4:capabilities-type               8 00 04 00 08 00 00 04 90
cdp      1:device-name                    19 00 01 00 13 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41
dhcp    50:requested-address               6 32 04 0A 01 0D 64
dhcp    55:parameter-request-list          9 37 07 01 42 06 03 0F 96 23
dhcp    60:class-identifier               39 3C 25 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
                                             20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
                                             50 2D 37 39 36 30 00
dhcp    12:host-name                      18 0C 10 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41 00
dhcp    61:client-identifier               9 3D 07 01 00 30 94 C4 52 8A
```

## シスコ ワイヤレス コントローラでのデバイス センサーの設定

サポートされているワイヤレス コントローラ上の DHCP 用のデバイス センサーは、CLI または Web 管理インターフェイスを使用して有効にできます。

**ステップ 40** CLI 経由でシスコ ワイヤレス コントローラ上のデバイス センサーを設定するには、次のコマンドを入力します。

```
> config wlan profiling radius enable <wlan-id>
```

デバイス センサーは、指定された WLAN 上のすべてのクライアントに対して有効になります。

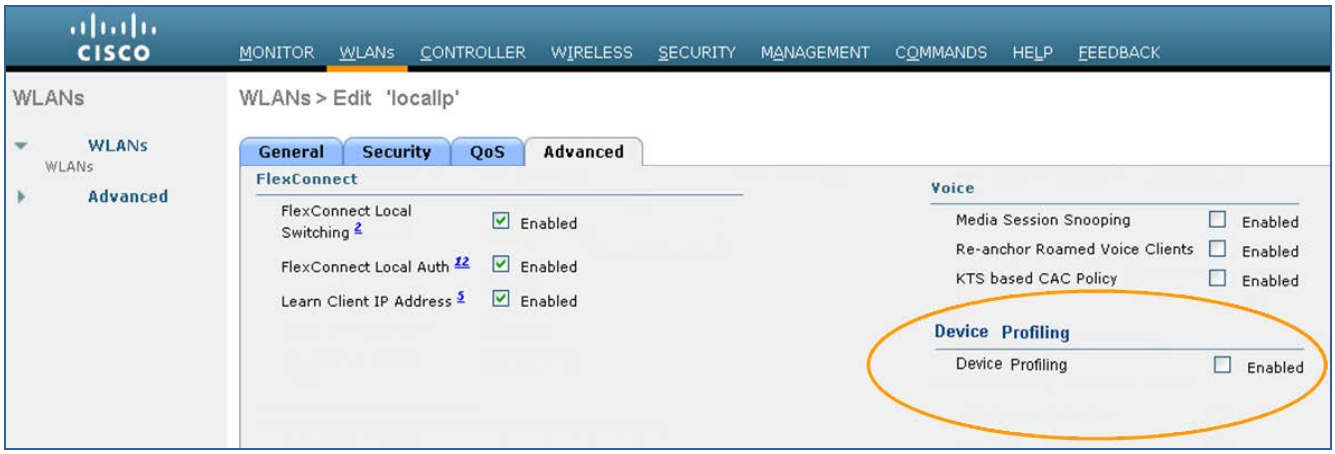
**ステップ 41** RADIUS アカウンティングを使用して、セッション アカウンティング情報を ISE に送信するようにワイヤレス コントローラを設定します。

**ステップ 42** RADIUS 認証および認可が設定されていれば、この手順はすでに完了しているはずです。

**ステップ 43** RADIUS と ISE が通信するためのワイヤレス コントローラの設定方法については、「RADIUS プローブの設定」の項を参照してください。

**ステップ 44** WLC Web インターフェイスから、[WLAN] → [(WLAN ID)] → [編集(Edit)] にアクセスします。図 69 の画面表示は、デバイス センサーを有効にする場所を示しています。

図 64 ワイヤレス コントローラ用のデバイス センサー設定の例




## デバイス センサーを使用したプロファイリングの確認

**ステップ 45** [管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] → [エンドポイント(Endpoints)] からエンドポイントを削除します。

**ステップ 46** NMAP プローブを使ったプロファイリングをサポートするように設定されたアクセス デバイスからエンドポイントを切断した後、再接続します。

**ステップ 47** ISE ポリシー管理ノードにアクセスして、[管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] に移動します。

**ステップ 48** LHS ペインで、[エンドポイント(Endpoints)] を選択します。

**ステップ 49** 新しく接続されたエンドポイントの MAC アドレスを見つけて選択し、HTTP プローブによってキャプチャされた属性を表示します。

図 70 では、ISE ポリシー サービス ノードで RADIUS プローブだけが有効になっています。強調表示されたキー属性には以下が含まれます。

EndPointPolicy

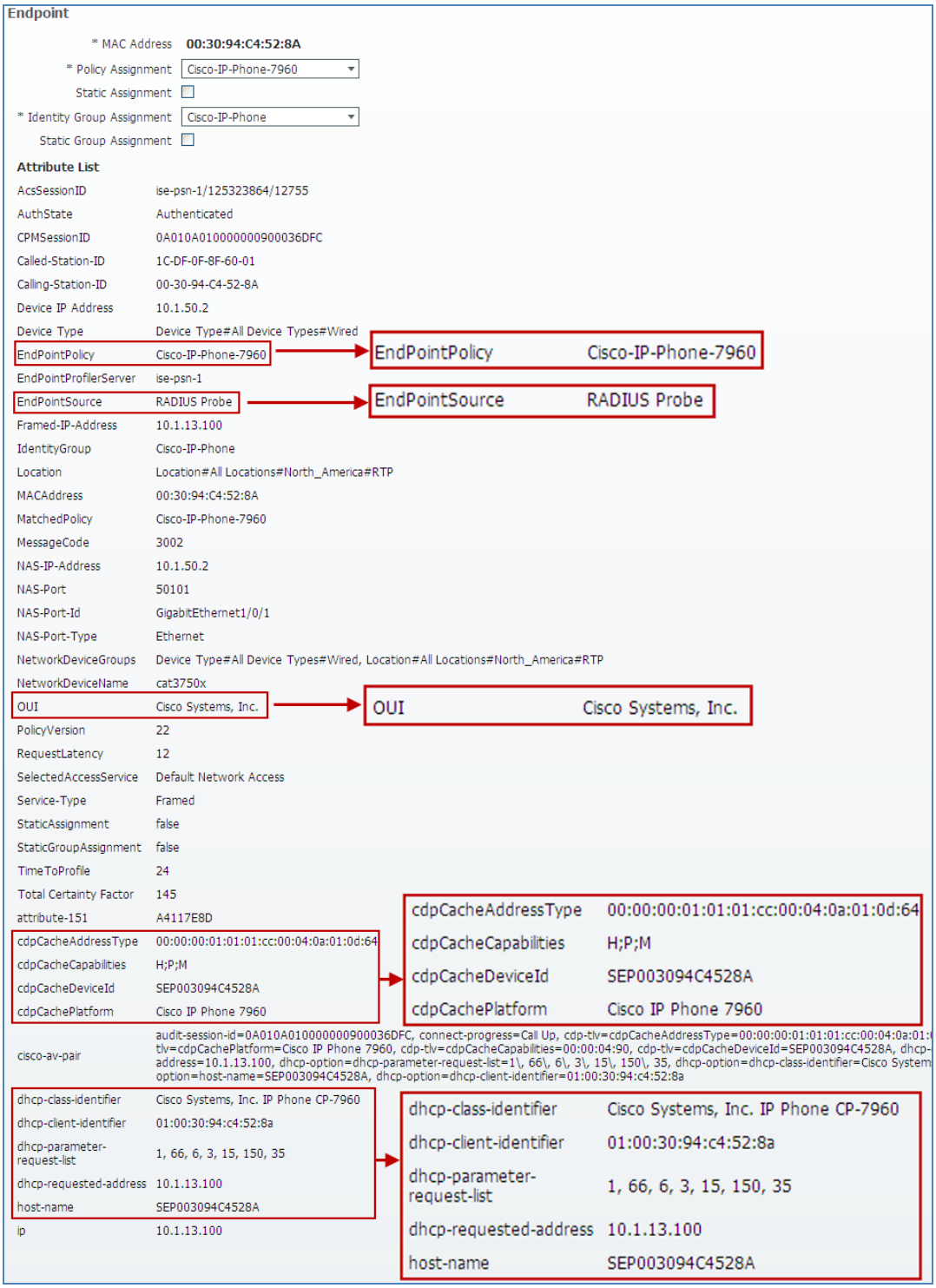
EndPointSource

OUI

CDP 属性(cdpCacheAddressType、cdpCacheCapabilities、cdpCacheId、cdpCachePlatform)

DHCP 属性(dhcp-class-identifier、dhcp-client-identitifier、dhcp-parameter-request-list、dhcp-requested-address、host-name)

図 65 デバイス センサー属性の例



**EndPointSource** が RADIUS プローブに設定されたデバイス センサーを単独で使用している場合は、**EndPointPolicy** が Cisco-IP-Phone-7960 と完全に一致することを確認できます。プロファイル照合に参加したデバイス センサーから受信されたプロファイリング属性には、**OUI** = Cisco Systems, Inc.、**cdpCachePlatform** = Cisco IP Phone 7960、および **dhcp-class-identifier** = Cisco Systems, Inc, IP Phone CP-7960 が含まれます。

CDP 属性と DHCP 属性にはフィルタによって指定された属性のみが含まれていることに注意してください。これはデータ収集が最適化されていることを示しています。ポリシー サービス ノードでは、ISE 展開内のすべての管理ノードとポリシー サービス ノードで不要な属性を解析して同期させる必要がありませんでした。デバイス センサー設定に基づいて、更新は変更が行われた場合にだけ受信されます。一方、SNMP クエリーと DHCP プローブは、クエリーまたは DHCP の更新ごとに属性を更新します。

**ベスト プラクティス**：拡張性が大幅に向上し、全体の管理とプロファイリング設定が簡素化する可能性がある場合は、デバイス センサーを使用して ISE プロファイリングを展開します。デバイス センサーは、RADIUS 認証環境と他の展開タイプ（ISE 前ディスカバリ フェーズや NAC アプライアンスとの統合など）の両方の有線アクセス スイッチとワイヤレス コントローラに展開できます。

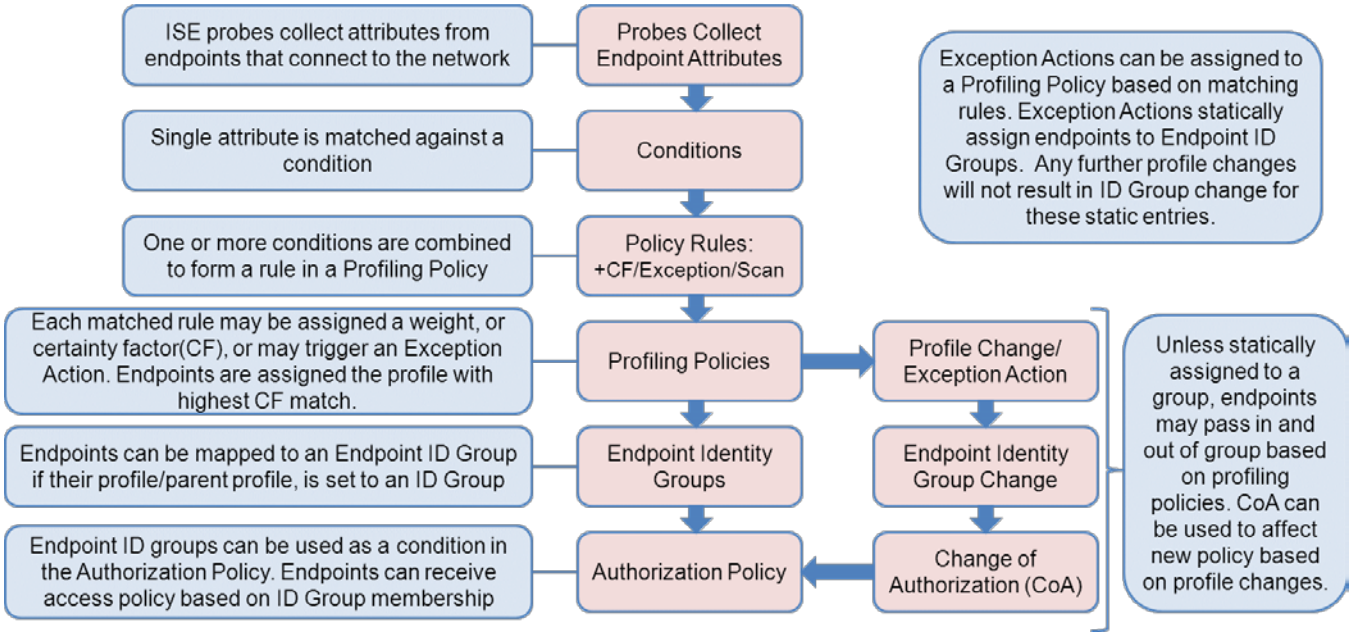
# プロファイリング ポリシーの設定

## プロファイリング ポリシーの設定の概要

ここまで、図 71 に示すように、ISE プロファイリング サービスのハイレベルのアーキテクチャを紹介してきました。これは、ISE プロファイリングの設定と全体的なプロセス フローに関する一般的なガイドラインとしても機能します。

フローの最初のコンポーネントである、エンドポイント属性を収集するためのプローブの設定が完了したところです。ここでは、お客様のプロファイリング要件をサポートするプロファイリング ポリシーと認可ポリシーを設定するための残りのコンポーネントに進みます。

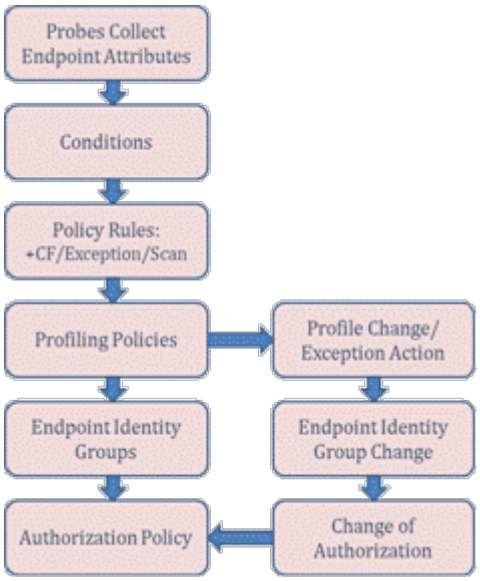
図 66 ISE プロファイリング ポリシーの設定フロー




## プロファイリング条件

さまざまな ISE プローブでさまざまなプロファイリング属性を収集することができます。ISE ポリシー サービス ノードで属性が収集されたら、プロファイリング プロセスの次のステップは、これらの属性とプロファイリング条件を照合することです（図 72）。各条件は、[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [辞書（Dictionary）] にあるシステム辞書に列挙されたサポート対象属性との一致を表します。

図 67 設定フロー：プロファイリング条件




## 辞書属性

表 7 に、[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [辞書（Dictionary）] にあるシステム辞書に列挙された属性を示します。これらの属性は、[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [条件（Conditions）] →
[プロファイリング（Profiling）] でプロファイリング条件を作成または変更するときに選択できます。

表 5 辞書属性

| RADIUS | MAC | SNMP | CDP | NetFlow | NMAP |
|---|---|---|---|---|---|
| Acct-Authentic | MACAddress | cafSessionAuthorizedBy | cdpCacheAddress | MAX_PKT_LNGTH | 110-tcp |
| Acct-Delay-Time | OUI | cafSessionAuthUserName | cdpCacheCapabilities | MAX_TTL | 123-udp |
| Acct-Input-Octets | | cafSessionAuthVlan | cdpCacheDeviceId | MIN_PKT_LNGTH | 135-tcp |
| Acct-Input-Packets | | cafSessionClientMacAddress | cdpCachePlatform | MIN_TTL | 135-udp |
| Acct-Interim-Interval | | cafSessionDomain | cdpCacheVersion | nexthop | 137-udp |
| Acct-Link-Count | | cafSessionStatus | | OUT_BYTES | 138-udp |
| Acct-Multi-Session-Id | **IP** | cLApIfMacAddress | **LLDP** | OUT_PKTS | 139-tcp |
| Acct-Output-Octets | | cLApName | | output | 139-udp |
| Acct-Output-Packets | EndpointSource | cLApNameServerAddress | lldpCacheCapabilities | OUTPUT_SNMP | 143-tcp |
| Acct-Session-Id | FQDN | cLApNameServerAddressType | lldpCapabilitiesMapSupported | prot | 1434-udp |
| Acct-Session-Time | Host | cLApSshEnable | lldpChassisId | PROTOCOL | 161-udp |
| Acct-Status-Type | ip | cLApSysMacAddress | lldpManAddress | sampling_interval | 162-udp |
| Acct-Terminate-Cause | mask | cLApTelnetEnable | lldpPortDescription | source_id | 1900-udp |
| Acct-Tunnel-Connection | PortalUser | cLApTertiaryControllerAddres | lldpPortId | src_as | 21-tcp |
| Acct-Tunnel-Packets-Los | User-Agent | cLApTertiaryControllerAddres | lldpSystemCapabilitiesMapEna | SRC_MAC | 22-tcp |
| | | | | SRC_MASK | |
| | | | | SRC_TOS | |

| | | | | | |
|---|---|---|---|---|---|
| （未完成） | **DHCP**<br>boot-file<br>client-fqdn<br>client-identifier<br>device-class<br>dhcp-class-identifier<br>dhcp-client-identifier<br>dhcp-message-type<br>dhcp-parameter-request-list<br>dhcp-requested-address<br>dhcp-user-class-id<br>domain-name<br>host-name<br>name-servers<br>pxe-client-arch<br>pxe-client-machine-id<br>pxe-client-network-id<br>server-identifier<br>vendor-class | （未完成） | | | |

# プロファイリング条件の設定

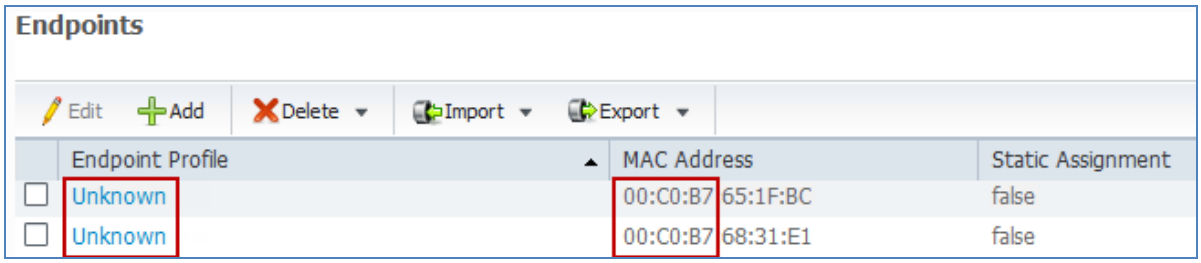
Cisco ISE には、プロファイリング ポリシーで大規模なプロファイル ライブラリを構築するために使用される事前作成されたプロファイリング条件の拡張可能なリストが付属しています。新しいカスタム条件を作成したり、特定のエンドポイントのセットや特定の環境に合わせて既存の条件を変更したりしなければならない場合があります。

## カスタム（ユーザ定義）プロファイリング条件の設定

**ステップ 50** [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [条件（Conditions）] にアクセスして、LHS ペインでプロファイリングを選択します。条件のリストをスクロールして、**OUI**、**dhcp-class-identifier**、**host-name**、**User-Agent** などの条件と **cdpCachePlatform**、**lldpSystemDescription**、**hrDeviceDescr** などの SNMP MIB データを作成するために使用される共通属性を理解します。

**ステップ 51** カスタム プロファイリング条件の作成プロセスを説明するために、実際の例を使用します。[エンドポイント（Endpoints）] → [ID（Identities）] のリストに、次のエンドポイントが表示されます（図 73）。

図 68 不明なエンドポイントの例




**ステップ 52** 図の中の 2 つのエントリはどちらも不明プロファイルを示しています。また、同じ MAC プレフィックスを共有しています。最初のエンドポイントの詳細な属性を確認すると次のように表示されます（図 74）。

図 69 エンドポイント スキャンからの NMAP プローブ属性の例 1

| | |
|---|---|
| MACAddress | 00:C0:B7:65:1F:BC |
| MatchedPolicy | Unknown |
| MessageCode | 3000 |
| NAS-IP-Address | 10.1.50.2 |
| NAS-Port | 50108 |
| NAS-Port-Id | GigabitEthernet1/0/8 |
| NAS-Port-Type | Ethernet |
| NetworkDeviceGroups | Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP |
| NetworkDeviceName | cat3750x |
| OUI | AMERICAN POWER CONVERSION CORP |

**ステップ 53** これは、これらのエンドポイントがラボ データセンターに設置された APC 無停電電源装置（UPS）用の SNMP ネットワーク管理接続になっている OUI（American Power Conversion Corp）からの GigabitEthernet1/0/8 または簡易ディダクションに接続されたエンドポイントの直接検査によって決定されます。これらのエンドポイントのライブラリ内にはデフォルト条件が存在しないため、それらを作成して、最終的に、ネットワーク全体のすべてのデバイスをサポートする新しいポリシーを構築します。

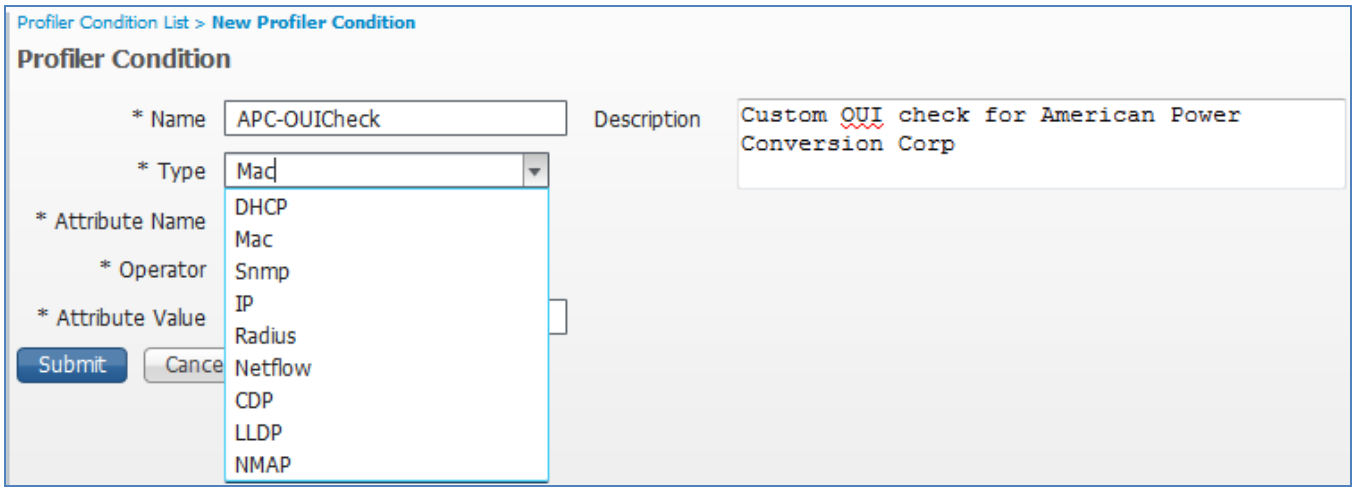
**ステップ 54** RHS ペインで [追加（Add）] をクリックします。

**ステップ 55** この例では、ベンダーとチェックのタイプを示すために、名前 **APC-OUICheck** が使用されます。

**ステップ 56** 説明を入力します。この例では、**Custom OUI check for American Power Conversion Corp** です。作成されたすべてのユーザ定義条件の迅速なフィルタリングと表示を可能にする一意の ID（この例では "Custom"）を追加することをお勧めします。

**ステップ 57** [タイプ（Type）] にはいくつかのカテゴリがあります。このチェックでは、[タイプ（Type）] は **Mac** です（図 75）。

図 70 ユーザ定義プロファイラ条件の例 1




**ステップ 58** 属性名は **OUI** です。
**ステップ 59** 演算子は **EQUALS** です。
**ステップ 60** 属性値は、OUI に割り当てられたベンダー名です。この例では、**AMERICAN POWER CONVERSION CORP** です。

注:属性値文字列を指定するときに、大文字と小文字を区別してください。

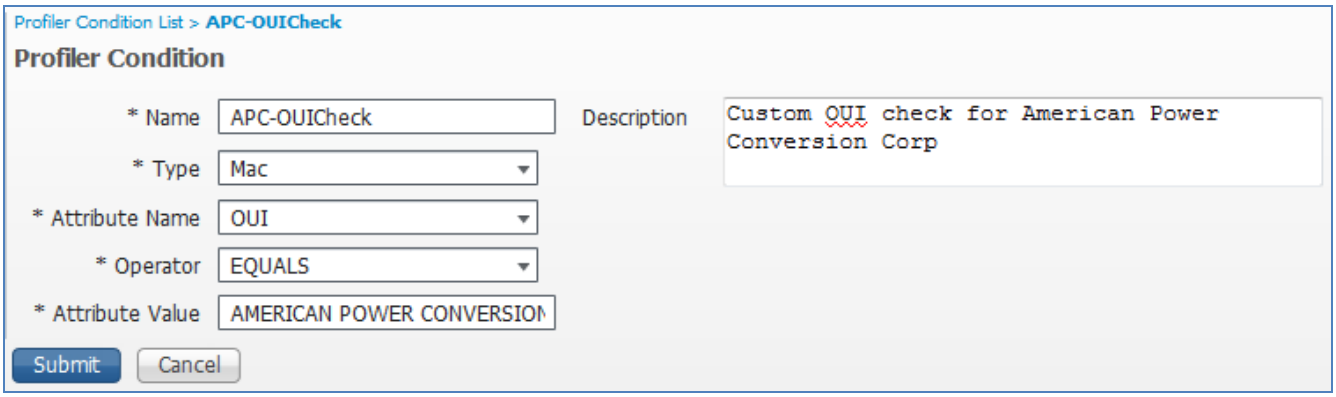
この例では、オプションで、完全一致(EQUALS)ではなく、属性値が "AMERICAN POWER" または "AMERICAN POWER CONVERSION" に設定された MATCH 演算子を使用することもできます。

OUI データベースで特定の MAC アドレス プレフィックスのエントリが欠けている場合は、次の設定を使用して不明な OUI の条件を作成できます。

- Type = Mac
- Attribute Name = MACAddress
- Operator = CONTAINS
- Attribute Value = XX:XX:XX(MAC アドレスの 3 バイト プレフィックス)

**ステップ 61** 図 76 に、ユーザ定義プロファイル条件の最終形態を示します。

図 71 ユーザ定義プロファイラ条件の例 2

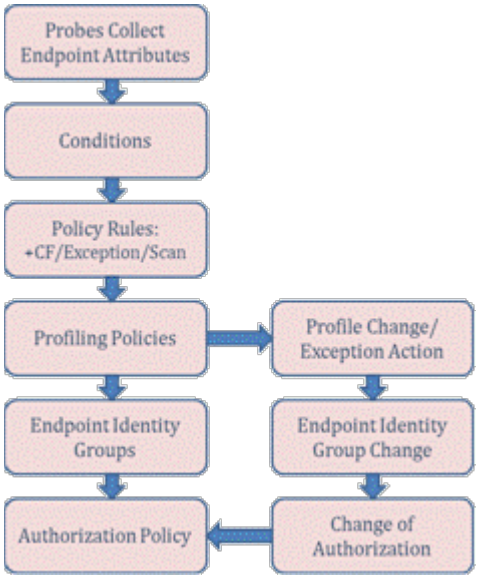



**ステップ 62** [送信(Submit)] ボタン(または連続編集の場合は [保存(Save)])をクリックします。

## プロファイリング ポリシーとルール

プロファイリング ポリシー、または、プロファイルは、プロファイル一致と見なされるエンドポイントに適合するポリシー ルールを定義します。ポリシー ルールには、1 つ以上の条件が含まれています。ルールのすべての条件が満たされた場合(AND 演算子を使用)、または、ルールの 1 つの条件が満たされた場合(OR 演算子を使用)に、指定されたアクションが実行されます。図 77 に、プロファイリング ポリシーの設定フローを示します。

図 72 設定フロー:プロファイリング ポリシーとルール



## プロファイリング ポリシー ルールのアクション

サポートされているプロファイリング ポリシー ルールのアクションには以下が含まれます。

Certainty Factor Increases <X>

Take Exception Action

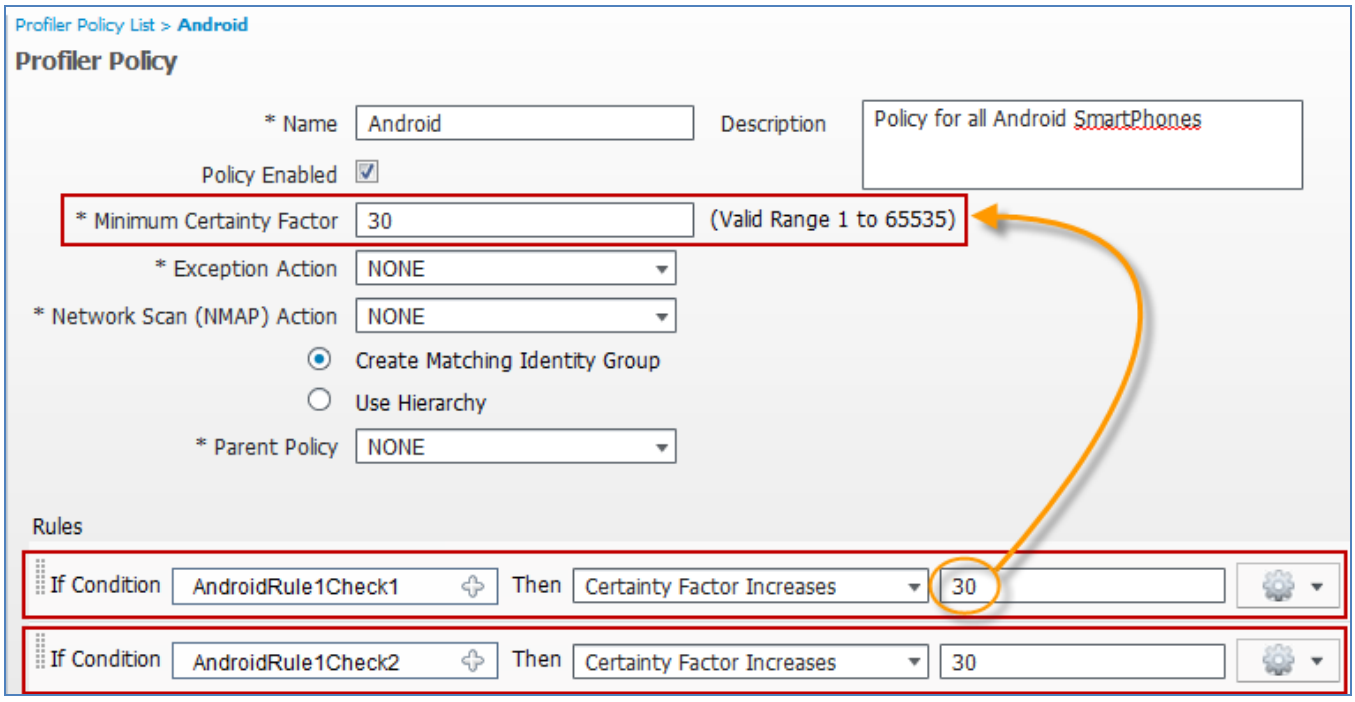
Take Network Scan Action

## 確実度係数（CF）

Android という名前の単純なプロファイリング ポリシーを図 78 に示します。このポリシーには 2 つのルールが含まれています。各ルールは、一致したらアクション Certainty Factor Increases 30 を実行するという単一条件で構成されます。CF は、一般的な重み付け、つまり、エンドポイントのプロファイルが照合対象条件ごとに完全に一致する確実度の相対レベルを示すために使用されます。

Android プロファイルの最小確実度係数は 30 に設定されています。そのため、いずれかのルールが一致すれば、そのエンドポイントがこのプロファイルに割り当てられる候補になります。エンドポイントは複数の条件とその結果の複数のプロファイルに同時に一致する可能性があるため、照合するプロファイルごとに累積 CF 値を計算する必要があります。

図 73 プロファイリング ポリシーの例




4 つのプロファイリング ポリシー割り当て条件があります。次のすべての条件が満たされた場合に、エンドポイントがプロファイルに割り当てられます。

HTTP サーバが有効になっていること（[ポリシーの有効化（Policy Enabled）] チェックボックスをオンにする必要があります）。

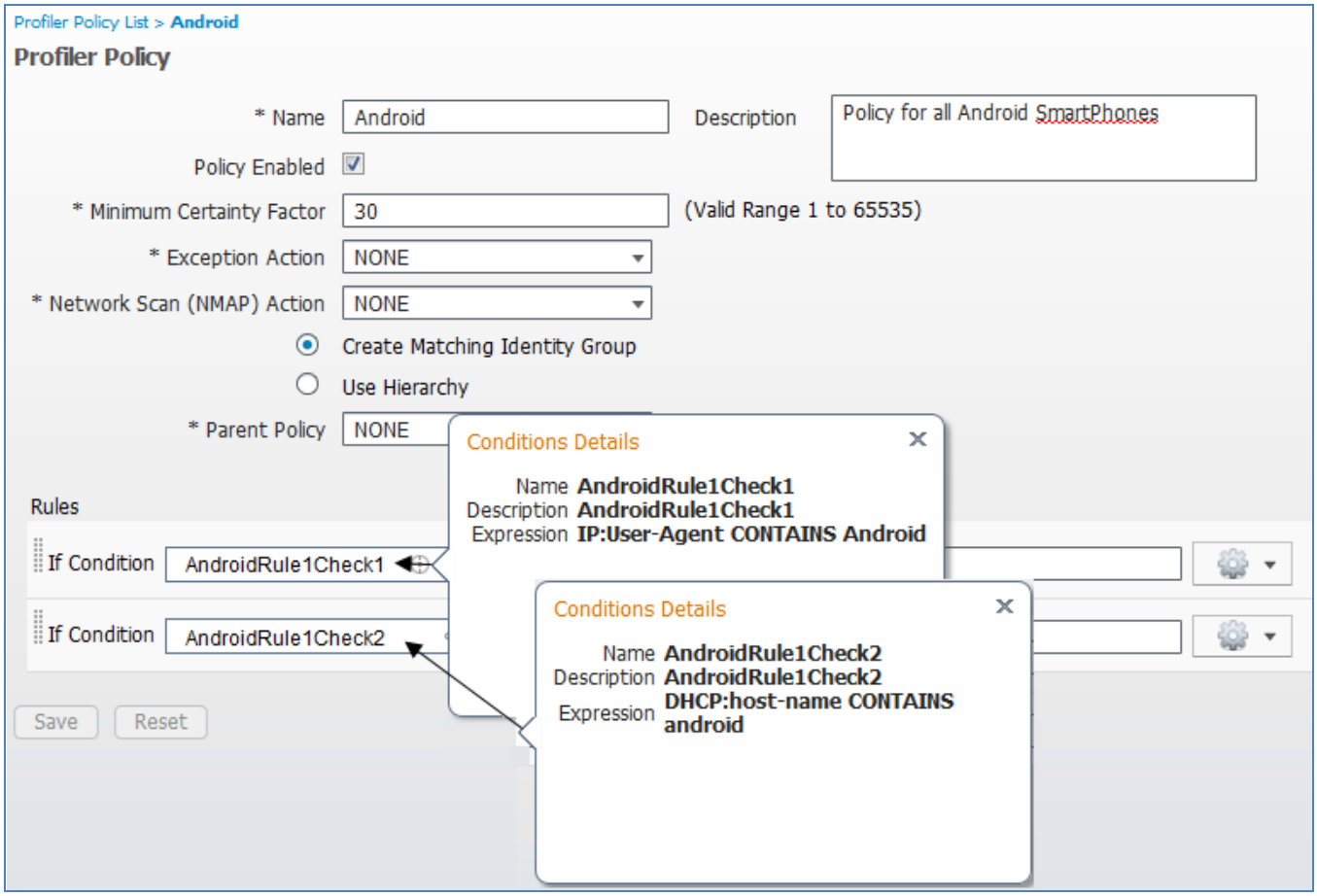
プロファイルのエンドポイント累積 CF 値が最小確実度係数を満たしていること。

プロファイルの CF 評価が、1 と 2 が true になっている他のプロファイルより高いこと。

エンドポイントが親プロファイルの最小 CF を満たしていること（プロファイルが階層の一部の場合）。

図 79 に示す Android ポリシーの例の最初のルールによれば、エンドポイントの **User-Agent** に文字列 "Android" が含まれている場合は、このプロファイルの CF が 30 に増加されます。エンドポイントが 2 つ目のルール（DHCP **host-name** 値に文字列 "Android" が含まれている）と一致した場合も、このプロファイルの CF が 30 に増加されます。両方のルールの条件と一致した場合は、その CF が 60 になります。

図 74 プロファイリング ポリシー ルールの例




60 の CF を使用した場合でも、技術的には、CF 値が 60 を超える別のポリシーの条件とエンドポイントが一致する可能性があります。他のすべての条件が満たされている場合は、エンドポイントが、Android ポリシーのすべての条件を満たしていても、そのプロファイルに割り当てられます。

一般的に、事前定義のポリシーの CF 値はデフォルト値のままにしておく必要があります。ネットワーク ポリシーまたはプリファレンスに基づいて特定のポリシーを他より優先するためにデフォルト値を変更しなければならない場合があります。その場合は、優先ポリシー内の該当するルールの CF 値を必要なプロファイリング目標を達成するための最小量だけ増やします。

同様に、新しいプロファイルを作成している場合は、初期 CF 値を比較的低い値（10 か 20）に設定して、ポリシー割り当てを監視し、必要な結果を検証します。初期値を高く設定しすぎると、あるプロファイルのルールが他のポリシーに比べて異常に高い CF 値に設定された場合、CF 計算に基づいて、より近い他のプロファイルに実際のエンドポイントが適用されない可能性があります。

たとえば、エンドポイントが CF を 100 の値に増やすカスタム Profile_A の 1 つのルールと一致する場合、CF を 20 ずつしか増やさない 4 つのルールと一致する Profile_B に、そのエンドポイントが割り当てられることはありません。Profile_A 内のルールと Profile_B 内のルールは同じでも、別々の CF 値が割り当てられている場合もあります。したがって、ポリシー ルール全体で一貫した CF 評価を使用することをお勧めします。

**シスコ ベスト プラクティス**：一般的に、CF 値はデフォルト設定のままにすることをお勧めします。特定のプロファイル割り当てが優先されるようにデフォルト設定を変更する必要がある場合は、優先するプロファイル内のルールの値を必要なポリシー割り当てを達成する最小値に増やすだけにしてください。

カスタム プロファイルを作成する場合は、CF の初期値を比較的低く維持するか、他のプロファイルに設定された値と同じにします。

## 例外と NMAP アクション

照合するルールに対して使用可能なアクションには、他にも、Take Network Scan Action と Take Exception Action があります。Take Network Scan Action を使用すれば、ポリシー サービス ノードで [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Action）] フィールドの設定に基づいて、エンドポイントに対する NMAP スキャンをトリガーすることができます。この機能については、「ネットワーク スキャン（NMAP）プローブを使用したプロファイリング」の項でさらに詳しく説明します。

Take Exception Action を使用すれば、[例外アクション（Exception Action）] フィールドの設定に基づいて、エンドポイントをポリシーに静的に割り当てることができます。この機能については、「例外アクション」の項でさらに詳しく説明します。

これらのアクションはどちらも、エンドポイントがポリシーと一致し、かつ、指定された条件と一致した場合にだけトリガーされます。条件が一致しても、エンドポイントがプロファイル ポリシーと一致しない場合は、アクションは実行されません。

また、ポリシー内の複数のルールと一致して複数のアクションが実行される場合があることに注意してください。たとえば、ポリシーも照合する場合は、CF を 10 だけ増やすルールと一致してから、Take Exception Action や Take Network Scan Action などの別のルールとも一致する可能性があります。

## カスタム（ユーザ定義）プロファイリング ポリシーの設定

**ステップ 63** この手順では、既に設定されている条件を使用して、ラボの APC UPS デバイス用のカスタム プロファイリング ポリシーを作成します。

**ステップ 64** [ポリシー（Policy）] → [プロファイリング（Profiling）] にアクセスします。RHS ペインのメニューで [追加（Add）] をクリックします。

**ステップ 65** APC-UPS というプロファイル名を入力します。

**ステップ 66** [説明(Description)] に「**Custom profile for APC UPS Network Management module**」と入力します。APC カスタム条件に関する説明と同様に、キーワード **Custom** を使用すれば、この文字列に基づいて、すべてのユーザ定義ポリシーに対する単純なフィルタリングが可能になります。

**ステップ 67** 最小確実度係数の設定を 10 のデフォルト値のままにします。

**ステップ 68** デフォルト設定の [照合するIDグループの作成(Create Matching Identity Group)] ではなく、[階層の使用(Use Hierarchy)] オプション ボタンを選択します。

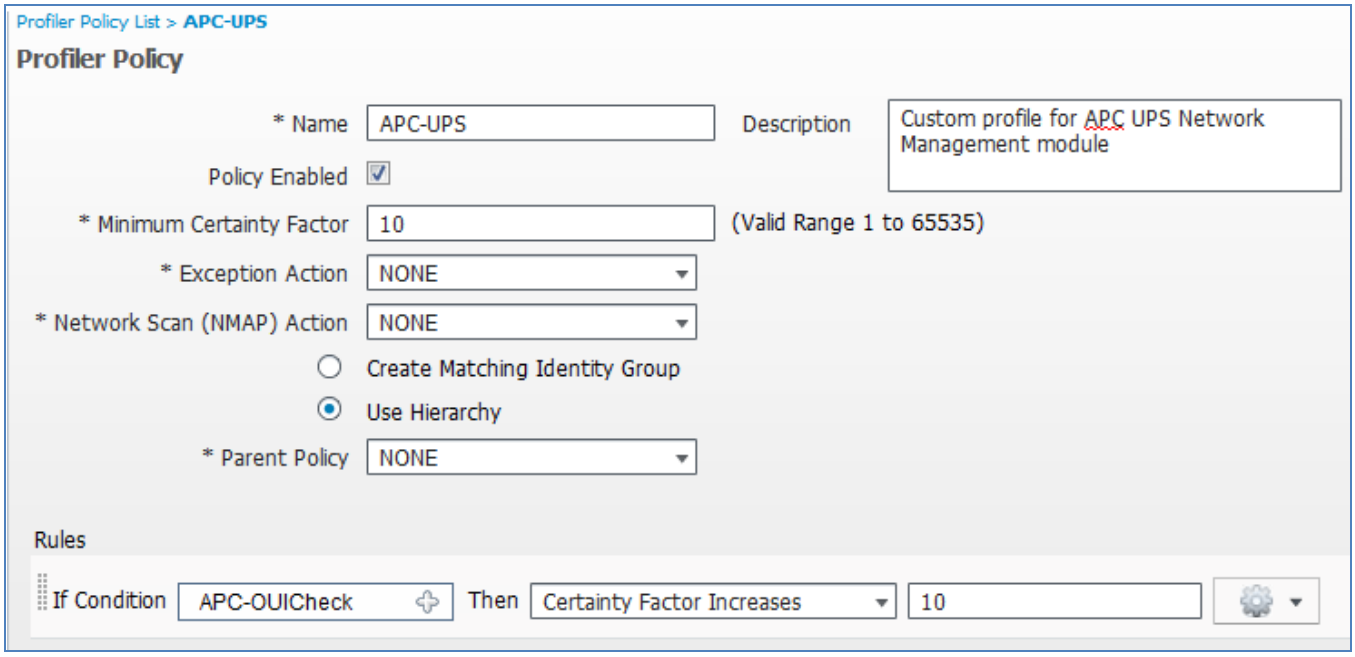
**ステップ 69** [ルール(Rules)] で、条件の横にある ✣ 記号をクリックして、ライブラリから [既存の条件の選択(Select Existing Condition)] を選択します。

**ステップ 70** [条件名(Condition Name)] → [条件の選択(Select Condition)] で、APC-OUICheck を選択します。

注:プロファイリング条件を作成してから、別のタスクでプロファイリング ポリシーを作成する代わりに、[新しい条件の作成(Create New Condition)] オプション(詳細オプション)を使用して、プロファイリング ポリシー自体から新しい条件を作成することもできます。作成された新しい条件は、ポリシー ルール内に名前付き条件として表示されます。

**ステップ 71** デフォルト ルール アクションの 10 の値を使用した Certainty Value Increases はそのままにします(図 80)。

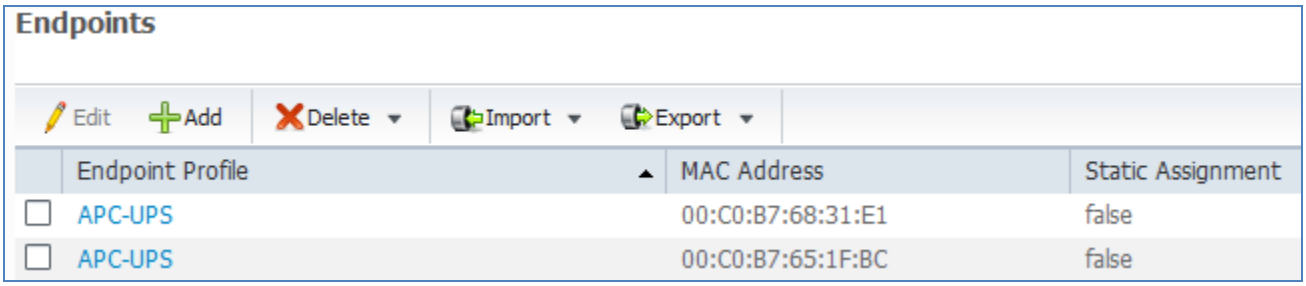
図 75 ユーザ定義のプロファイリング ポリシーの例




**ステップ 72** [送信(Submit)] をクリックして変更を保存します。

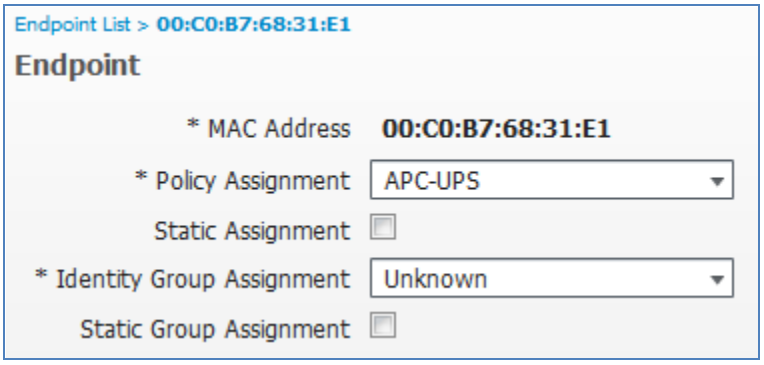
**ステップ 73** [管理(Administration)] → [ID管理(Identity Management)] → [ID(Identities)] にアクセスして、LHS ペインで [エンドポイント(Endpoints)] を選択します。図 81 に示すように、APC デバイスはリスト内で [不明(Unknown)] ではなく、新しい照合するプロファイリング ポリシー割り当てで表示されます。

図 76 ユーザ定義プロファイルを使用したエンドポイントの例




**ステップ 74** リスト内の 1 つのエンドポイントの APC-UPS をクリックします（図 82）。

図 77 ユーザ定義プロファイルを使用したエンドポイント詳細の例



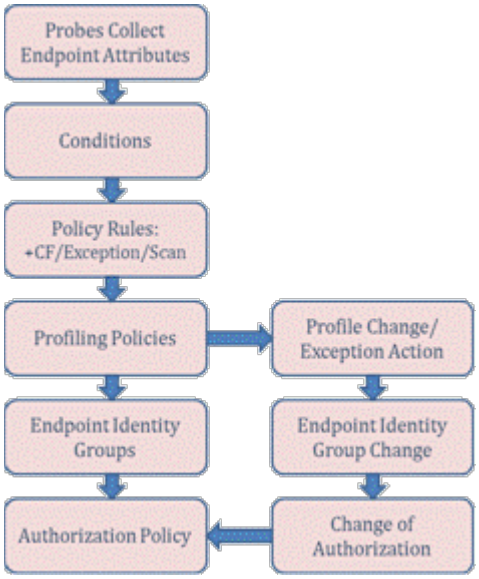

**ステップ 75** [ポリシー割り当て（Policy Assignment）] は [APC-UPS] ですが、[IDグループ割り当て（Identity Group Assignment）] は [不明（Unknown）] に設定されていることに注意してください。これは、プロファイル内のデフォルト設定を [照合するIDグループの作成（Create Matching Identity Group）] から [ユーザ階層（User Hierarchy）] に変更したためです。このオプションは、プロファイリング ポリシーとエンドポイント ID グループの関係を示すために意図的に選択されたものです。

## エンドポイント ID グループ

デバイス プロファイリングは、ネットワーク管理者とセキュリティ管理者がネットワークに接続されているデバイスのタイプをより正確に把握するための非常に重要なツールになり得ます。単なる可視性だけでなく、エンドポイントのデバイス分類またはプロファイリング ポリシー割り当てに基づいて認可ポリシー決定を下すには、プロファイルをエンドポイント ID グループに関連付ける必要があります。ISE 認可ポリシーは、現在、未加工のプロファイリング属性またはポリシー割り当てを条件として受け入れませんが、プロファイリング ポリシー割り当てにマッピングされたエンドポイント ID グループを作成することができます。これにより、認可ポリシーで間接的にエンドポイントのプロファイリング ポリシー割り当てをルール条件として参照することができます。

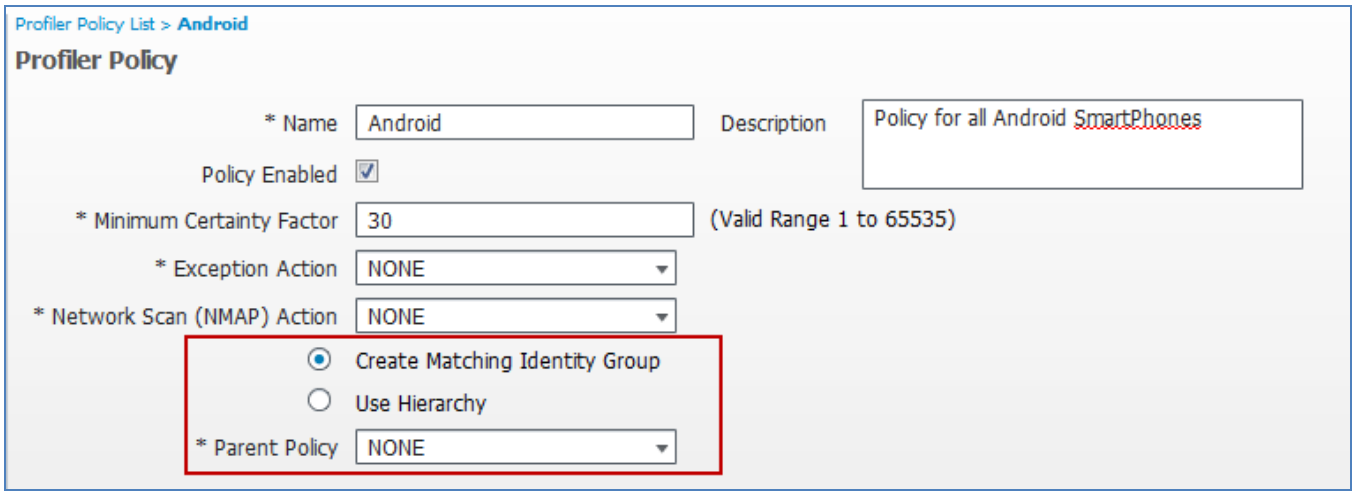
図 83 に、エンドポイント ID グループの設定フローを示します。

図 78 設定フロー：エンドポイント ID グループ




プロファイリング ポリシーをエンドポイント ID グループにマッピングするには、図 84 に示すように、プロファイルの下の [照合するIDグループの作成（Create Matching Identity Group）] というラベルの付いたオプション ボタンを選択します。

図 79 プロファイリング ポリシー - [照合するIDグループの作成（Create Matching Identity Group）] の例

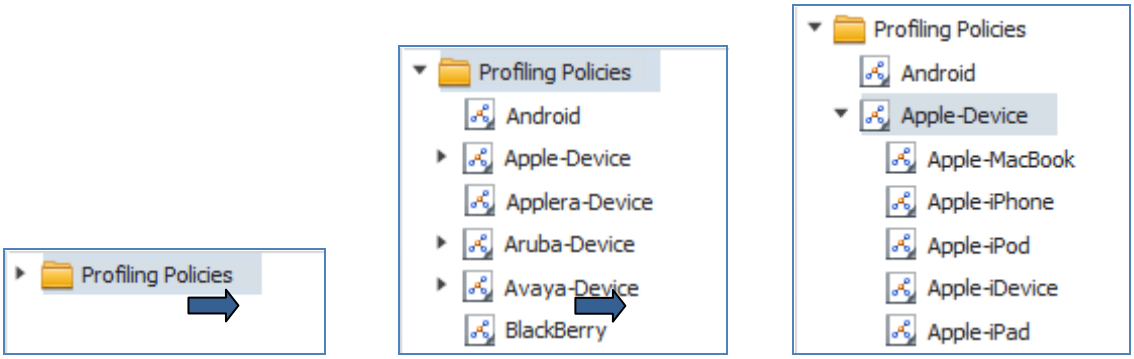



[照合するIDグループの作成（Create Matching Identity Group）] オプションの選択は、[ユーザ階層（Use Hierarchy）] 設定、つまり、ほとんどの事前構築プロファイルのデフォルト選択と相互排他的です。図 84 の Android ポリシーの例では、ポリシー名に基づいてエンドポイント ID グループを作成するようにデフォルト設定が変更されています。ユーザ定義プロファイルのデフォルト設定は、照合する ID グループを作成することです。

## プロファイリング ポリシー階層

プロファイリング ポリシーの照合用に列挙されたリストの最後の条件は、エンドポイントが親ポリシーの最小 CF を満たすことです。これは、プロファイリング ポリシー内の階層の項目を紹介したものです。[親ポリシー（Parent Policy）] が [なし（NONE）] に設定される Android プロファイルと違って、図 84 に示すように、Apple-iPad や Apple-iPhone などのプロファイルは親プロファイルが Apple-Device の子プロファイルです。ポリシー階層を表示するには、[ポリシー（Policy）] → [プロファイリング（Profiling）] に移動します。ラベルの手前の右矢印記号（ ）をクリックすることによって、LHS ペインでプロファイリング ポリシーを展開します。これにより、すべての第 1 階層ポリシーが表示されます（図 85）。

図 80 プロファイリング ポリシー階層




特定のエントリの手前にある右矢印は、そのプロファイルの子ポリシーが存在することを示します。上の図では、Android ポリシーには子がなく、Apple-Device は親ポリシーです。矢印をクリックすると、Apple-Device の子ポリシーが表示されます。

階層は、表示の整理とポリシーの管理に役立ちます。また、より詳細なルールの下でより上位の条件を繰り返し定義しなくても、子ポリシーの照合が親の照合を意味するように複数の子ポリシーに共通する一連の条件を定義する手段も提供します。

階層の一般的な用途は OUI での照合です。たとえば、すべての Apple デバイスには Apple と同じ OUI が割り当てられています。そのため、iPad、iPod、iPhone などに対してこの条件を繰り返す必要がありません。Apple-iPhone プロファイルと一致するためには、エンドポイントにも Apple OUI が割り当てられている必要があります。これが、他のブラウザの **User-Agent** 文字列だけを模倣した User Agent Switch という名前の単純な Firefox ブラウザ プラグインを使用しても、Apple iPhone のプロファイル条件が満たされない理由です。Apple MAC アドレスがなければ、親条件がテストで不合格になります。前述したように、プロファイリングはスプーフィング対策ソリューションとして位置付けられていませんが、特定のスプーフィング アクティビティを自動的に阻止するソリューションの機能を備えています。

階層は、ID グループ割り当ての照合を簡素化するのにも役立ちます。親ポリシーが ID グループにマッピングされている場合は、すべての子ポリシーを ID グループにマッピングする必要がありません。たとえば、Cisco IP Phone 用の事前構築プロファイルが多数存在します。Cisco-IP-Phone（デフォルト設定）用の照合する ID グループを作成することによって、子ポリシーごとに別々の ID グループを用意しなくても、この親に基づく認可ポリシーを作成するだけで済みます。これにより、認可ポリシー ルールを大幅に簡素化できます。個別の IP フォン モデルに固有の処理が必要ない場合は、それらを親プロファイルと ID グループ割り当ての参照を通して均一に扱うことができます。

## プロファイリング ポリシー用の照合する ID グループの作成

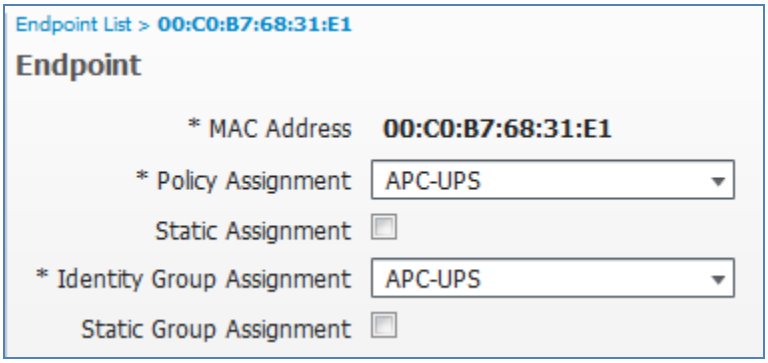
**ステップ 76** この手順では、**APC-UPS** という名前のユーザ定義プロファイル ポリシー用の ID グループを作成します。

**ステップ 77** [ポリシー（Policy）] → [プロファイリング（Profiling）] にアクセスして、プロファイルのリストから APC-UPS を選択します。

**ステップ 78** オプション [照合するIDグループの作成（Create Matching Identity Group）] をオンにして、[保存（Save）] をクリックし、変更をコミットします。

**ステップ 79** [管理（Administration）] → [ID管理（Identity Management）] → [ID（Identities）] → [エンドポイント（Endpoints）] で内部エンドポイントのリストに戻り、APC-UPS プロファイルに割り当てられたエンドポイントの 1 つを再度選択します（図 86）。

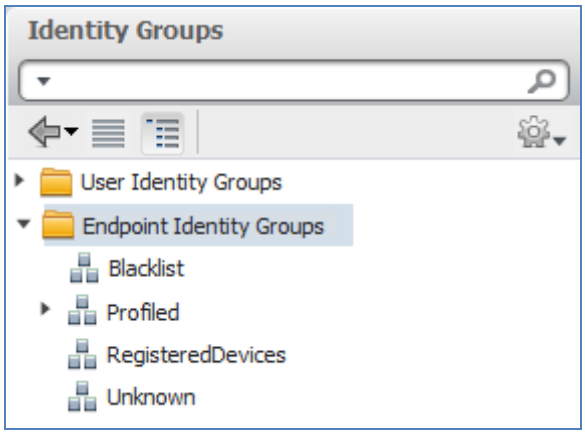
図 81 ユーザ定義プロファイル用のエンドポイント ID グループの例




注：[IDグループ割り当て（Identity Group Assignment）] が [不明（Unknown）] から [APC-UPS（APC-UPS）] に変更されています。

**ステップ 80** 図 87 に示すように、[管理(Administration)] → [ID管理(Identity Management)] → [グループ(Groups)] にアクセスして、LHS ペインでエンドポイント ID グループのリストの左側にある矢印(▸)をクリックし、その内容を展開します。

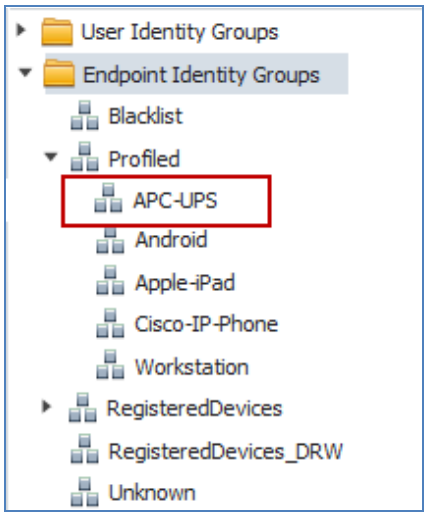
図 82 エンドポイント ID グループの表示の例 1




**ステップ 81** このリストは、デフォルトの最上位 ID グループの指定を示しています。デフォルトで、照合する ID グループを**持たない**プロファイリング ポリシーに割り当てられたすべてのエンドポイントが ID グループ **Unknown** のメンバーになります。照合する ID グループを持つプロファイリング ポリシーに割り当てられたすべてのエンドポイントは、親 ID グループ **Profiled** の下にその ID グループのメンバーとして表示されます。**Blacklist** と **RegisteredDevices** は特別なグループです。Blacklist は、ネットワーク アクセスが拒否されるエンドポイントを識別するために使用されます。RegisteredDevices は、MyDevicesPortal とネイティブ サプリカント プロビジョニングでネットワーク アクセス ユーザが登録したエンドポイントを指定するため使用されます。

**ステップ 82** [プロファイリング済み(Profiled)] の左側にある ▸ をクリックして、その内容を展開します(図 88)。

図 83 エンドポイント ID グループの表示の例 2

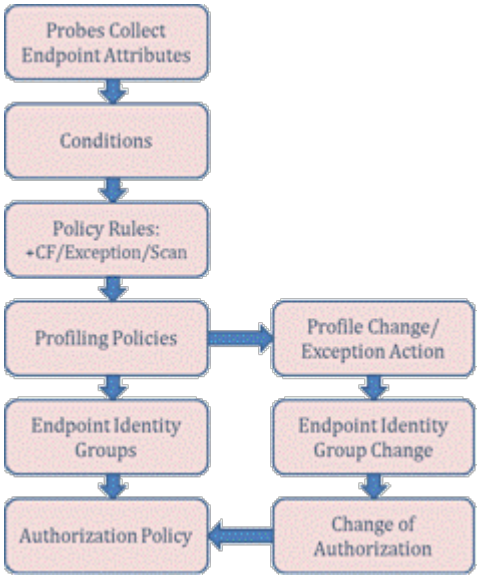


**ステップ 83** デフォルトで、Cisco-IP-Phone や Workstation などの照合する ID グループを持つプロファイリング ポリシーが存在することに注意してください。APC-UPS もエンドポイント ID グループのリストに表示されるため、認可ポリシー ルール内の照合する条件として選択できます。

## プロファイリング ポリシーと認可ポリシー

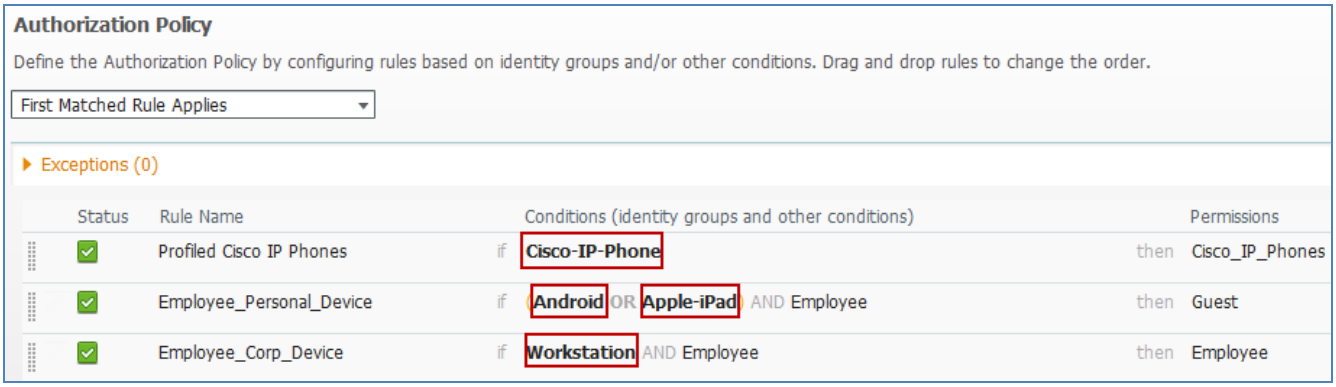
認可ポリシーは、照合するルールに基づいてネットワークに接続されたエンドポイントのアクセス権限を定義します。認可ポリシー ルールは、指定された権限を割り当てる前に、エンドポイントに対して true にすべき条件を指定します。プロファイリングに基づいてポリシーをエンドポイントに割り当てるには、照合する ID グループを持つプロファイリング ポリシーにエンドポイントを割り当てる必要があります。図 89 に、認可ポリシーの設定フローを示します。

図 84 設定フロー：認可ポリシー




ISE プロファイリング サービスを使用してデバイスを分類し、それらを ID グループに割り当てることによって、ISE は、MAB を使用してさまざまなポリシーをプリンタや IP フォンなどの認証の要らないエンドポイントに適用したり、認証された従業員が会社のワークステーションではなく、iPad などの個人用デバイスを使用して接続するときに別のポリシーを適用したりできます（図 90）。

図 85 認可ポリシーの例



**ステップ 84** サンプル認可ポリシーに示すように、Cisco IP Phone としてプロファイリングされたエンドポイントに特殊な電話認可を割り当てるために、Cisco-IP-Phone という名前の ID グループが使用されています。これらのエンドポイントは、MAB を使用して認証されます。また、階層型ポリシーを使用すれば、特定の IP フォン モデルに対するプロファイル照合に関係なく、このポリシーをすべての Cisco IP Phone に適用できます。

**ステップ 85** 認可ポリシーは、Apple-iPad や Android に分類される個人用デバイスを使用してインターネット専用アクセスに接続する従業員を一意的に認可する（ゲスト権限）と同時に、ワークステーション経由で接続する従業員にはフル アクセスを付与する（従業員権限）プロファイリングの使用も特徴とします。

## 認可ポリシーでのエンドポイント ID グループの使用

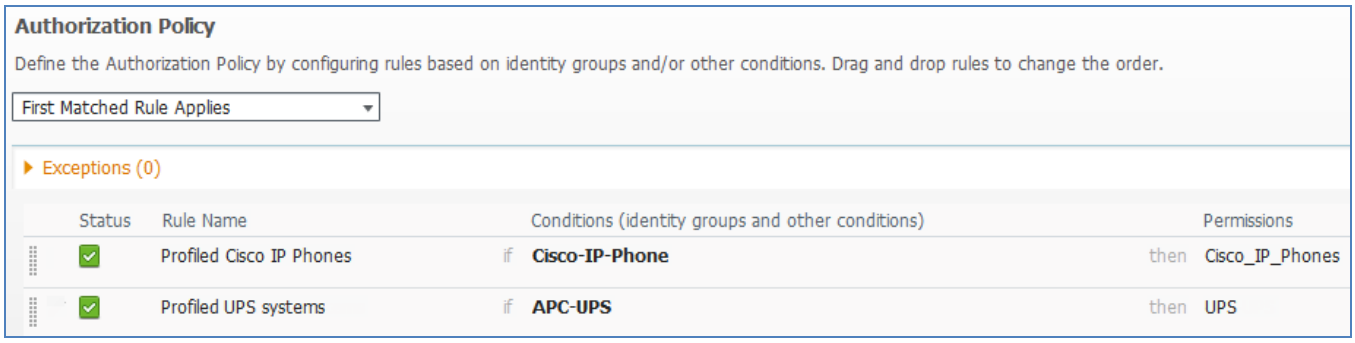
**ステップ 86** この手順では、APC UPS デバイスとしてプロファイリングされたエンドポイントに、APC-UPS という名前の ID グループに対する MAB 認証および認可ポリシー ルール照合に基づいて特別な権限を割り当てます。

**ステップ 87** [ポリシー（Policy）] → [認証（Authorization）] にアクセスして、Profiled UPS Systems という名前のプロファイリングされた Cisco IP Phone ルールの下に新しいルールを挿入します。

**ステップ 88** [IDグループ条件（Identity Group condition）] で、[エンドポイントIDグループ（Endpoint Identity Groups）] → [プロファイリング済み（Profiled）] に移動して、APC-UPS を選択します。

**ステップ 89** [権限（Permissions）] で、UPS などの該当する認可プロファイルを選択してから、[保存（Save）] をクリックして変更をコミットします。図 91 のようにポリシー ルールが表示されるはずです。

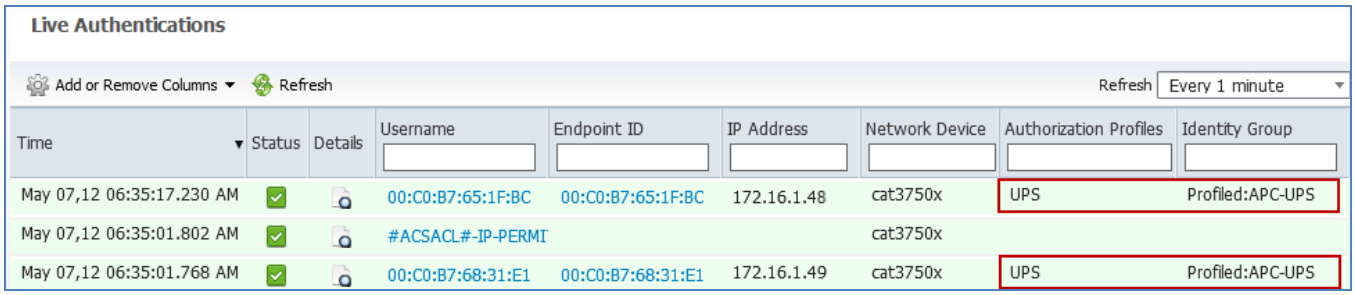
図 86 認可ポリシー設定の例 1




**ステップ 90** UPS デバイスの接続を解除してから再接続するか、該当するインターフェイス上で **shut/no shut** コマンドを発行して接続しているスイッチポートをリセットすることによって、認可ポリシーが正しく機能していることを確認します。

**ステップ 91** [操作（Operations）] → [認証（Authentications）] にアクセスしてライブ認証ログを表示します。次の図 92 のようなエントリが表示されるはずです。

図 87 認可ポリシー設定の例 2




**ステップ 92** このログには、UPS という名前の認可プロファイルを使用して認証および認可される、APC-UPS としてプロファイリングされた 2 つのエンドポイントが表示されています。この例では、最初のエンドポイントが認可されてから、ダウンロード可能な ACL（dACL）がスイッチに送信されます。2 つ目のエンドポイントはすでにダウンロードされた dACL を再利用するため、2 つ目の dACL は送信されません。

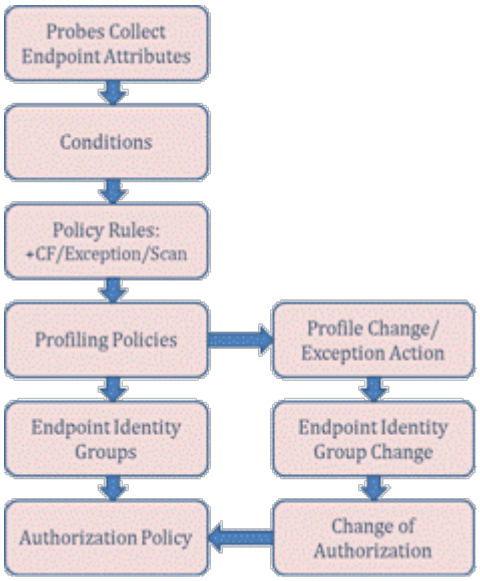
## プロファイル移行と認可変更

プロファイリングの過程で、エンドポイントは、不明な ID グループから Apple-Device などのより具体的なプロファイルに移行する可能性があります。Apple-iPad などに直接移行する場合もありますが、ネットワークから新しいプロファイル データが取得されるたびに移行が段階的に行われる場合もあります。まれに、エンドポイントの「否定的」なプロファイリング データが原因で、より具体的なプロファイルからより具体的でない親プロファイルまたは全く異なるプロファイルへの移行が行われる場合があります。

プロファイル移行のタイプに関係なく、ネットワークに対して照合するエンドポイントを認証するときに別の認可ポリシー ルールを適用するようにエンドポイント ID グループ割り当てが変更されることがよくあります。問題は、ネットワークに対して認証および認可されたエンドポイントに新しい認可を適用する方法です。

図 93 に、プロファイル移行と認可変更（CoA）の設定フローを示します。

図 88 設定フロー：プロファイル移行と CoA




## 認可変更（CoA）

CoA は、特定の状態またはポリシーが変化したときに、RADIUS サーバ（ISE）がネットワーク アクセス デバイス（RADIUS クライアント）への未承諾通信を開始して、エンドポイント用のアクセス ポリシーを更新することができる標準ベースの RADIUS 機能（RFC 3576）です。更新するのに、エンドポイントによる再認証は必要ありません。

ISE プロファイリング サービスは、次の 2 つの主要な条件に基づいて CoA をトリガーします:

プロファイル移行によって、例外アクションがトリガーされた。

プロファイル移行によって、認可ポリシー ルールごとのエンドポイント アクセスが変更された。

## 例外アクション

デフォルトで、3 つの設定不能な例外アクションが事前定義されています。[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] → [プロファイリング（Profiling）] → [例外アクション（Exception Action）] にアクセスしてリストを表示します（図 94）。

図 89 例外アクション

| Profiler Action Name ▲ | Description |
|---|---|
| EndpointDelete | When endpoint is deleted or reassigned to the unknown profile. |
| FirstTimeProfile | When an endpoint profile changes from unknown to known for the first time. |
| StaticAssignment | When an endpoint has connected to the network and is now statically assigned. |

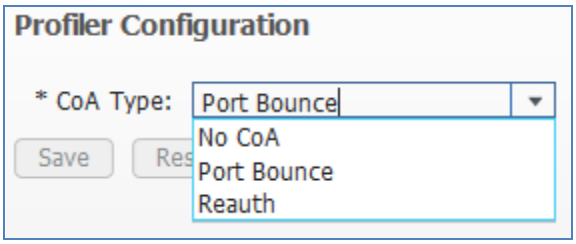
**EndpointDelete** は、エンドポイントが削除されたとき、または、エンドポイントがプロファイリングされたプロファイルから不明なプロファイル（プロファイリング ポリシーが一致しない）に移行したときに CoA を送信します。

**FirstTimeProfile** は、エンドポイントが不明なプロファイルから特定のプロファイリング ポリシー割り当てに移行したときに CoA を生成します。この例外アクションは、エンドポイントが既知のプロファイル間（Apple-Device と Apple-iPod 間など）で移行した場合は CoA をトリガー**しません**。

**StaticAssignment** は、エンドポイントが動的プロファイル割り当てからのプロファイルに静的に割り当てられたときに CoA を生成します。静的ポリシー割り当てに割り当てた場合は、プロファイリング属性が通常どおりの移行を示していても、新しいエンドポイント プロファイリング ポリシーを割り当てることができません。

例外アクションごとに送信されるデフォルト CoA タイプは、[管理（Administration）] → [システム（System）] → [設定（Settings）] → [プロファイリング（Profiling ）] にあるグローバル設定で構成します（図 95）。

図 90 グローバル プロファイラ CoA の設定




グローバル プロファイリング設定の構成方法については、このガイドの「グローバル プロファイリング設定の構成」の項で説明します。他のセッションの中断を最小限に抑えるために複数のセッションが同じスイッチ ポートを介して接続される場合は、ポート バウンス設定が再認証設定に縮小されます。

システム定義の例外アクションは、設定することができず、プロファイリング ポリシーに基づくアクションとして割り当てることができません。これらは定義された移行に基づいて自動的にトリガーされます。ただし、管理者は、カスタム例外アクションを定義できます。このようなユーザ定義の例外は、プロファイリング ポリシー内で、静的プロファイリング ポリシー割り当てを適用して、CoA を送信するかどうかを指定するために使用できます。

## 認可ポリシーが変更された場合のプロファイル移行時の自動 CoA

Cisco ISE ソフトウェア リリース 1.1.1 以前では、例外アクションがプロファイル間移行、つまり、ある既知のプロファイルから別の既知のプロファイルへの移行に対して CoA を強制するためによく使用されており、エンドポイントをプロファイリング ポリシーに静的に割り当てることの悪影響が出ていました。ISE 1.1.1 以降では、プロファイル移行によって認可ポリシー ルールごとのエンドポイント アクセスが変更されるたびに ISE ポリシー サービス ノードが CoA を発行します。認可ポリシー ルール内で ID グループが使用されているエンドポイント ID グループの変更に基づいて決定が下されます。この拡張機能によって、プロファイル間移行に対して CoA を送信するユースケースに対処する例外アクションが不要になります。また、エンドポイントは動的プロファイル割り当てを維持することができるため、プロファイリング属性とポリシー設定に基づく追加の移行が可能になります。

ユーザ定義の例外アクションは、特定の条件が満たされたときにエンドポイントを優先ポリシー割り当てに静的に割り当てたり、オプションで、ポリシー割り当て時に CoA が送信されないようにするために使用できます。使用例は、製造施設内のプロセス制御エンドポイントや医療設備内のネットワークに接続された医療機器などの重要なネットワーク デバイスです。このような例では、管理者がエンドポイントをポリシーと関連する ID グループに静的に割り当てることができます。例外経由の静的割り当てを使用すれば、偽のプロファイル データによってエンドポイントのプロファイルが書き換えられ、そのネットワーク接続に影響が出るようなリスクを回避できます。

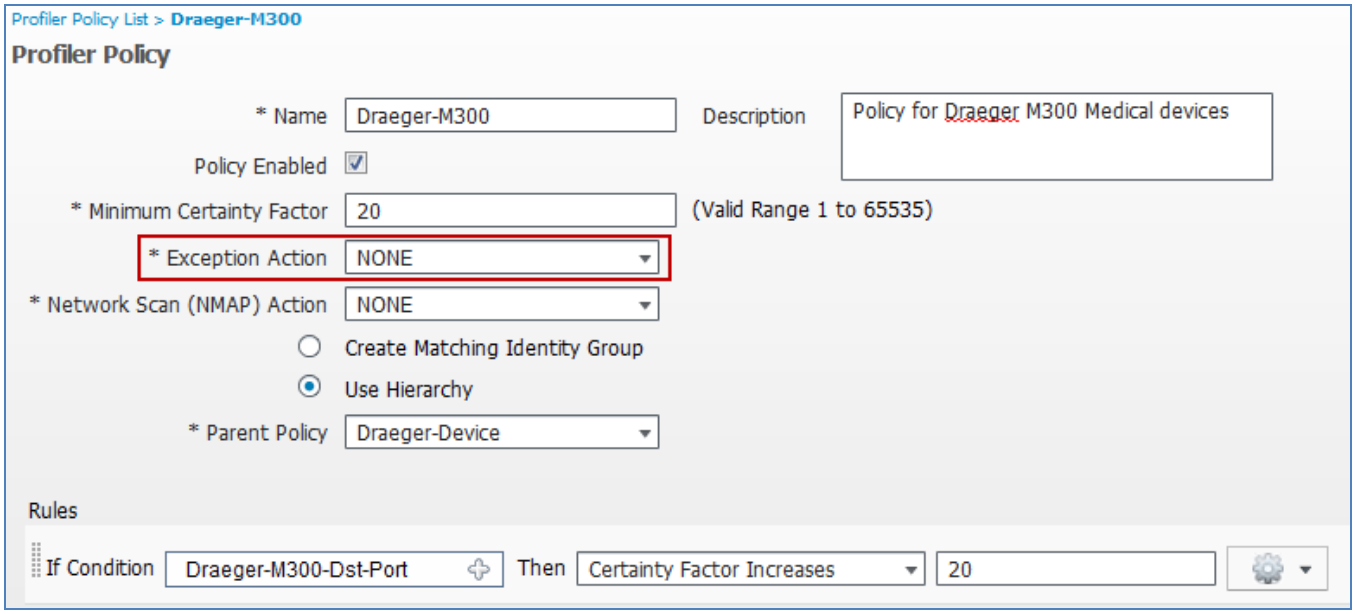
## カスタム(ユーザ定義)例外アクションの設定

**ステップ 93** この手順では、指定された条件が一致したときに医療機器を静的プロファイリング ポリシーに割り当てるように例外アクションを設定します。使用するデバイスは、Draeger M300、ポータブル無線心臓モニタです。

注意:医療ソリューションには特有のコンプライアンス要件があるため、厳密に言えば、この例の目的はカスタム例外アクションの使い方を示すことです。医療機器のネットワーク アクセスを保護する手段としての ISE プロファイリング サービスの妥当性の検証は行いません。

**ステップ 94** [ポリシー(Policy)] → [プロファイリング(Profiling)] にアクセスして、リストから Draeger-M300 を選択します。デフォルトで、このプロファイルには、例外アクションを参照するルールが含まれていません。加えて、例外アクションが定義されていません(図 96)。

図 91 Draeger-M300 プロファイリング ポリシーの例



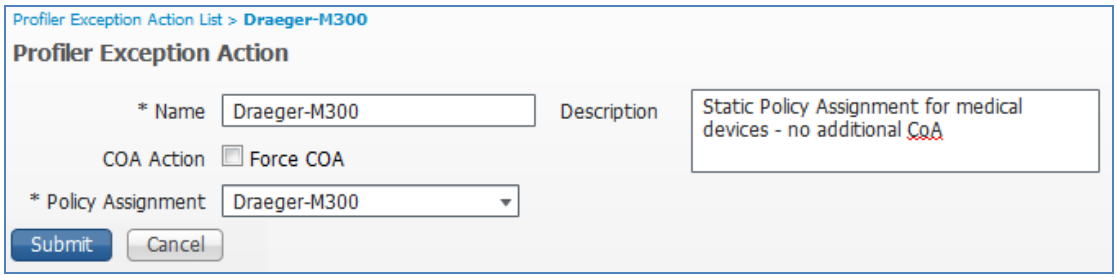

**ステップ 95** 新しい例外アクションを追加します。

**ステップ 96** [ポリシー(Policy)] → [ポリシー要素(Policy Elements)] → [結果(Results)] にアクセスして、LHS ペインでプロファイルの左側にある矢印(▸)をクリックし、その内容を展開します。

**ステップ 97** LHS ペインで [例外アクション(Exception Actions)] を選択して、RHS ペインのメニューで [追加(Add)] をクリックします。

**ステップ 98** 図 97 に示す値を使用して、新しい例外アクションが追加されます。

図 92 ユーザ定義例外アクションの例



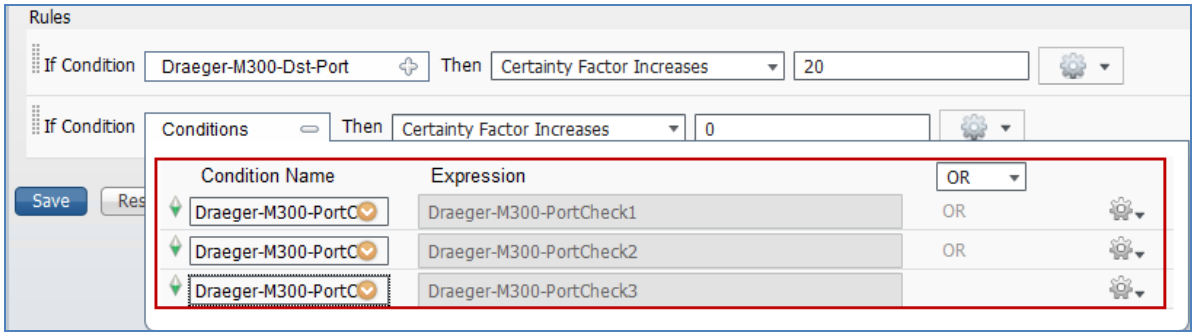

**ステップ 99** この例では、プロファイル Draeger-M300 に対する静的ポリシー割り当てで追加の CoA が送信されません。これは、以前示したものと同じプロファイルです。

**ステップ 100** [ポリシー(Policy)] → [プロファイリング(Profiling)] で Draeger-M300 プロファイリング ポリシーに戻って、プロファイル用の例外アクションを定義するために次の手順を実行します。

**ステップ 101** [例外アクション(Exception Action)] を [Draeger-M300(Draeger-M300)] に設定します。

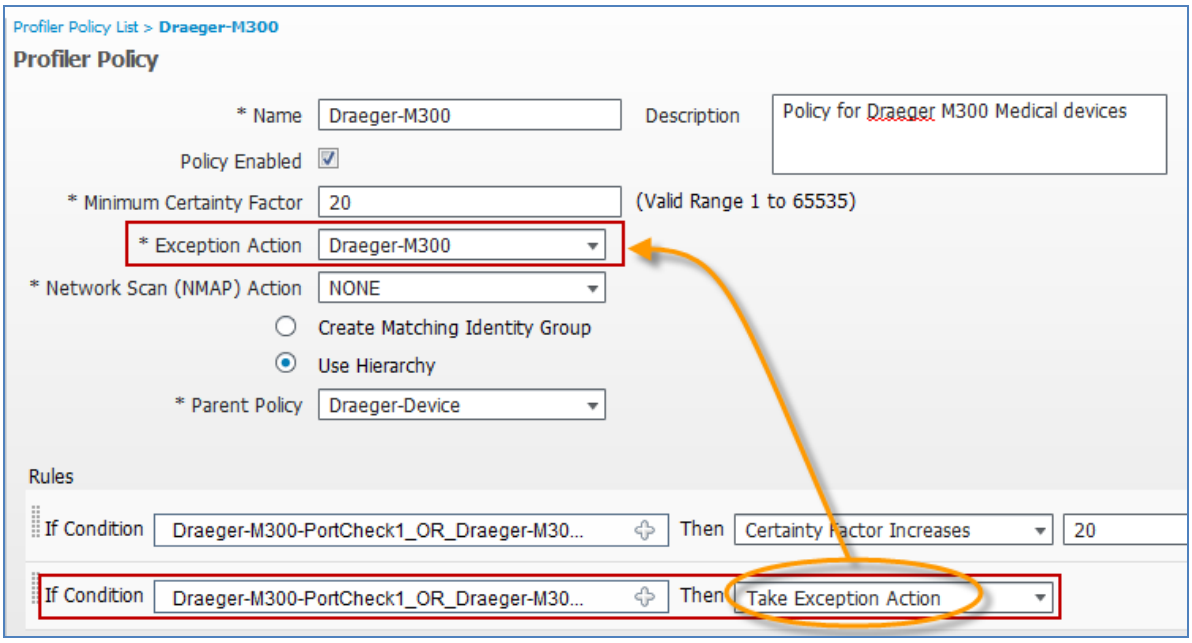
**ステップ 102** プロファイルを照合するために使用される既存のルールと同じ条件で新しいルールを作成します(図 98)。

図 93 ユーザ定義例外アクションを使用したプロファイリング ポリシー ルールの例 1




**ステップ 103** アクション([Then])をデフォルト値の [Certainty Factor Increases] から [Take Exception Action] に変更します。結果のプロファイリング ポリシーは、図 99 のように表示されるはずです。

図 94 ユーザ定義例外アクションを使用したプロファイリング ポリシー ルールの例 2




**ステップ 104** 変更を保存します。

**ステップ 105** このポリシー例では、エンドポイントをポリシーに静的に割り当てるためのエンドポイントへのポリシー割り当てに使用されたものと同じ条件を使用しました。認可ポリシーは、Draeger-Device という名前の親ポリシーに照合する ID グループが割り当てられているという事実を利用できます。そうでない場合は、このポリシーに ID グループを割り当てることができるため、認可ポリシーで特定のプロファイルが参照されます。

**ステップ 106** CoA をサポートするように有線スイッチを設定します。次のように、グローバル コンフィギュレーション モードで **aaa server radius dynamic-author** コマンドを使用します。

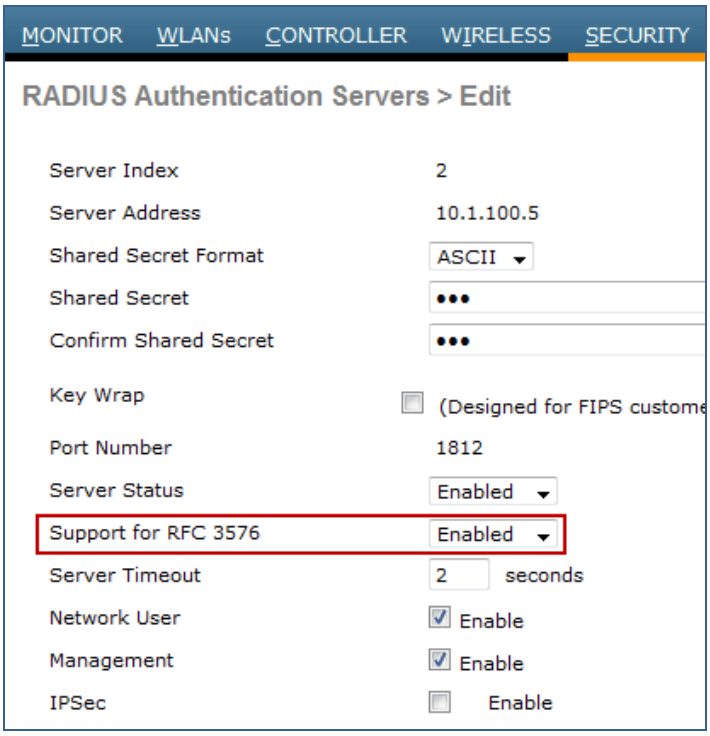
```
cat3750x(config)# aaa server radius dynamic-author
cat3750x(config-locsvr-da-radius)# client <ISE_PSN_IP_address> server-key <secret-key>
```

**ステップ 107** RADIUS 経由でスイッチと通信する ISE ポリシー サービス ノードごとに別々のクライアント エントリを追加します。

**ステップ 108** CoA をサポートするようにワイヤレス コントローラを設定します。

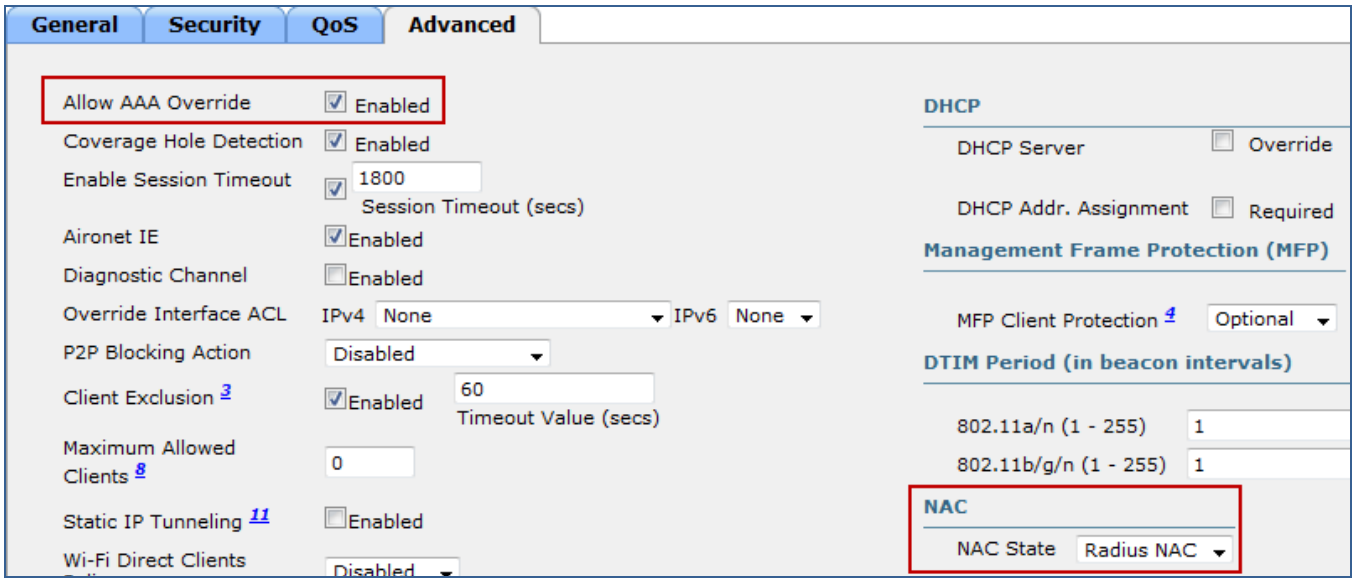
**ステップ 109** WLC Web 管理インターフェイスで、[セキュリティ(Security)] → [AAA] → [RADIUS] → [認証(Authentication)] にアクセスします。図 100 に示すように、RADIUS サーバ定義で、[RFC 3576のサポート(Support for RFC 3576)] が [有効(Enabled)] になっていることを確認します。

図 95 ワイヤレス コントローラ用の CoA 設定の例 1




**ステップ 110** [WLANs] → [(WLAN)] → [編集（Edit）] → [詳細設定（Advanced）] にアクセスします。図 101 に示すように、CoA をサポートする WLAN ごとに、[AAAオーバーライドの許可（Allow AAA Override）] を [有効（Enabled）] に設定し、[NAC状態（NAC State）] を [RADIUS NAC（RADIUS NAC）] に設定します。

図 96 ワイヤレス コントローラ用の CoA 設定の例 2




**ステップ 111** プラットフォームごとに必要に応じて変更を保存します。

# プロファイリング設計とベスト プラクティス

ここでは、さまざまな展開とユースケース用の一般的なプロファイリング設計とベスト プラクティスの推奨事項について説明します。

## プロファイリング設計の留意点

ISE プロファイリング要件を計画する場合、始めに、ネットワーク アクセス ポリシーをサポートするために分類が必要なエンドポイントのタイプを理解することが重要です。たとえば、特定のタイプの複数のネットワーク デバイスが 802.1X または Web ベースの認証をサポートしていないことがわかっている場合は、デバイス分類に基づく認可を使用した MAB 認証が必要になる可能性があります。ネットワーク アクセスにプロファイリングが必要なすべての既知のデバイス タイプを列挙することが重要です。

### 既知のデバイス タイプのプロファイリング

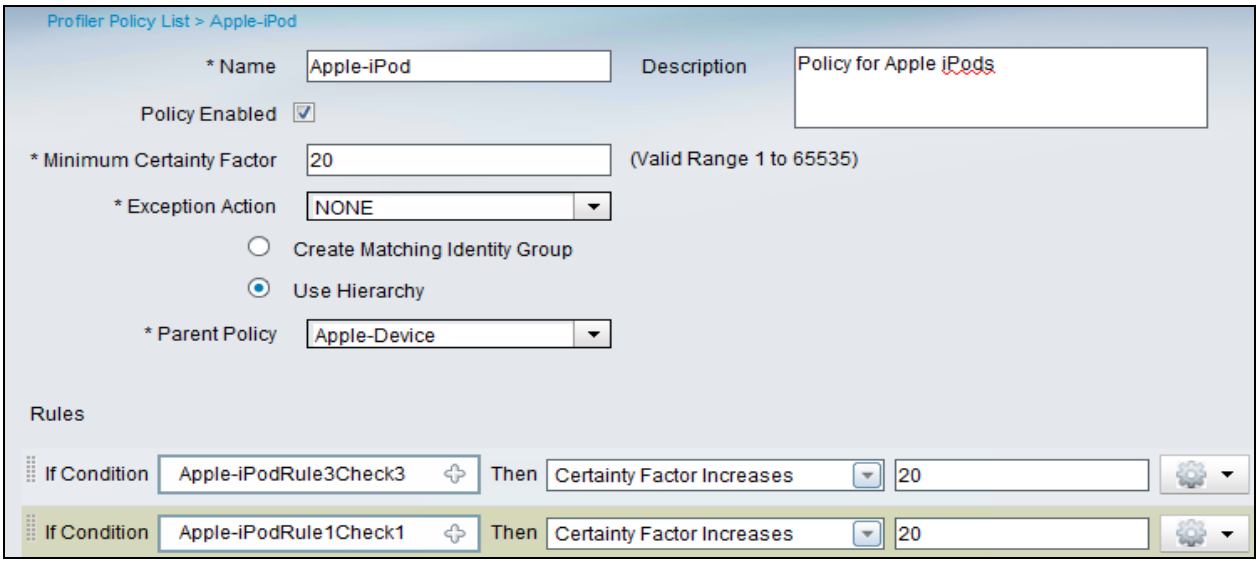
ISE の計画段階で、デバイス分類（プロファイル属性に基づく認可）が必要なエンドポイントを特定して、それらのエンドポイントのプロファイリングに必要な属性を決定します。認可が必要なデバイスのタイプがわかっている場合、次のステップはそれらの適切なプロファイリングに必要な属性と関連プローブを決定することです。

ほとんどの一般的なエンドポイントには、ISE プロファイル ライブラリ内に事前構築ポリシーが付属しています。これらのデフォルトの ISE プロファイルを確認して、属性とプローブの要件を特定します。たとえば、プロファイル X に条件 A、B、および C が含まれていることがわかっている場合は、そのデータの収集に必要な属性とプローブを推測できます。プロファイル ライブラリ内で特定の一致が見つからない場合は、同様のタイプのデバイスのプロファイルを参照してください。大抵の場合、同様のデバイス タイプのプロファイリング要件は似通っています。

既存のプロファイルが存在しない場合は、プローブを一時的に有効にして、エンドポイントに関する属性を収集できます。多くの場合、エンドポイントのリセットまたはネットワークの接続解除/再接続によって、管理者は通常の起動時にデバイスに使用可能な属性をキャプチャできます。ISE に表示される属性の多くには、エンドポイントを一意的に分類可能な関連属性が含まれています。デバイスによっては、パケット キャプチャを含むトラフィック分析で OUI、DHCP オプション、ユーザ エージェント、TCP/UDP ポート、または DNS の命名に関する一意の属性を決定する必要があります。

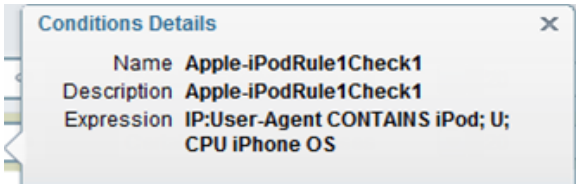
次の例（図 102）に、Apple-iPod プロファイルでの照合に使用される属性の検索方法を示します。このプロファイルが DHCP 属性または **User-Agent** に基づいていることを確認できます。したがって、Apple iPod をプロファイリングする場合は、DHCP と HTTP を使用することをお勧めします。

図 97 Apple-iPod のプロファイリング条件の例




プロファイル ライブラリ（[ポリシー（Policy）] → [プロファイリング（Profiling）]）を確認して、プロファイラ条件（[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [条件（Conditions）] → [プロファイリング（Profiling）]）（図 103）を参照すれば、それらのエンドポイントまたは同様のエンドポイントのプロファイリングに使用される属性と必要なプローブの理解を深めることができます。

図 98 プローブとプロファイラの条件




キー プロファイリング属性がわかったら、必要なプロファイル データを収集するために使用可能なプローブなどの収集手段から最適なオプションを決定します。各プローブ タイプをサポートする特定の要件の詳細については、ISE プローブ設定に関する各項を参照してください。その他のプローブ選択のベスト プラクティスに関する推奨事項については、この項の最後で説明します。

## 不明なデバイス タイプのプロファイリング

プロファイリングするエンドポイントのリストには、プリンタ、FAX 機、電話機、カメラ、ストレージ アプライアンス、または任意の数の IP 対応エンドポイントが含まれます。重要なデバイスのリストは、大規模な IP テレフォニー展開を含む環境などで簡単にわかる場合があります。最初にエンドポイントを発見する必要のある不明なホストが多数存在する場合もあります。段階的な ISE 展開が、モニタ モードで開始する一般的なベスト プラクティスです。これにより、管理者は、ネットワークに接続するエンドポイントのタイプと、スイッチポートが強制モードに移行した場合にネットワーク アクセスを拒否されるエンドポイントのタイプを把握することができます。

ワイヤレスには「モニタ モード」がありませんが、ワイヤレス プロファイリングは、802.1X、Web 認証、または MAC フィルタリングを使用して接続されたエンドポイントの分類に使用できます。シスコ ワイヤレス LAN コントローラ ソフトウェア リリース 7.0.116.0 以降では、ISE がワイヤレス 802.1X エンドポイントのプロファイリングをサポートします。WLC リリース 7.2.103.0 以降では、ISE が Central WebAuth を使用して認証されたものも含めて MAC フィルタリングを使用したワイヤレス エンドポイントのプロファイリングをサポートします。これは、このような WLAN 認証方式のために導入された CoA のサポートによるものです。

7.2.103.0 より前は、ワイヤレス クライアントをプロファイリングすることはできますが、ISE はプロファイル移行に CoA を適用できません。ただし、インベントリ（可視性）の目的で、エンドポイントを分類し、オプションで、それらをエンドポイント ID グループに割り当てることができます。加えて、現在の ID グループ割り当てに基づく認可ポリシーを、ワイヤレス ネットワークへの再接続時にエンドポイントに適用できます。プロファイル変更がアクティブ セッション中に検出された場合は、簡単に認可を変更することができません。

**ベスト プラクティス**：上の図に示すように、[ステーションIDタイプの呼び出し（Call Station ID Type）] を [システムMACアドレス（System MAC Address）] に設定して、非 802.1X クライアントのプロファイリングを可能にします。これにより、ISE がエンドポイントをデータベースに追加して、既知の MAC アドレスに基づいて、受信したその他のプロファイル データをそのエンドポイントに関連付けられることが保証されます。

可能であれば、展開の早い段階で ISE プロファイリングを展開します。ISE は、ネットワーク認証または認可を使用せずにディスカバリ プロセスを開始する有線エンドポイントをプロファイリングできます。これにより、可視性の観点で大きなメリットが得られるうえに、ネットワークへの接続を試みているエンドポイントのタイプを把握できます。この初期段階で、ネットワーク アクセスのプロファイリングが必要な特定のエンドポイント タイプがまだ判明していなければ、ISE プロファイリング ポリシーを改良することができます。

## プロファイリングに対するアクセス ポリシーとデバイス設定の影響

プロファイリング結果は、使用された 802.1X 展開モード（オープン認証対クローズ モード）とアクセス デバイス上で設定された認証方式の順序/プライオリティによって異なります。たとえば、ポートがクローズ モードの場合は、ポートが認可されるまで DHCP パケットを送信できません。特定のトラフィックが送信されなかった場合は、プローブがプロファイリング決定を下すために必要なデータを収集できない可能性があります。オープン認証（モニタ モードとローインパクト モード）を使用すれば、ポート認可前に特定のトラフィックを通過させることができます。プロファイリングはどちらのシナリオにも対応できますが、属性収集の能力とタイミングに対する特定の展開モードの影響を理解することが重要です。

フレキシブル認証（FlexAuth）の場合は、認証方式の順序も、属性が収集され、認可時にプロファイルが割り当てられるタイミングに影響する可能性があります。たとえば、順序が最初に MAB 認証を実行してから、モニタ モードまたはローインパクト モードの 802.1X を実行するように設定されている場合は、初期接続時に必要なポリシーを割り当てるプロファイル データが ISE で不足する可能性があります。MAB ルックアップの実行時には、まだ、エンドポイントが不明なままであったり、一般的なプロファイリング済み ID グループに入っている可能性があります。順序が 802.1X を最初に実行するように設定されている場合は、802.1X がタイムアウトする前に、DHCP とその他のプロファイル属性を収集できる可能性があります。その後で、MAB ルックアップが、初期接続中に収集された追加属性に基づいて適切なプロファイルに進むことができます。

注:エンドポイントに対する影響は通常、ネットワークへの最初の接続にのみ見られます。エンドポイントのプロファイリングが完了したら、ISE は、ID グループ割り当てを使用して、ネットワークへの連続再接続時に即時ポリシー照合を実行できます。

もう 1 つの留意点は、最初にポートに適用されるか、中間または最終認可状態で適用される全体的なアクセス ポリシーです。たとえば、エンドポイントが初めてネットワークに接続した場合は、ポート ACL(ローインパクト モードが前提)または初期 VLAN に基づいてアクセス権が付与されます。エンドポイントが不明で MAB ルックアップが失敗するか、そのポスチャ状態が不明な場合は、ポートまたは VLAN 割り当てに新しい ACL を配置する、Central WebAuth またはポスチャ状態に進むことができます。Web 認証または修復が成功すると、ポートが新しい ACL または VLAN を使って認可されます。状態ごとに、ネットワーク アクセスのレベルが異なります。プロファイリングが特定のデータの収集に依存する場合は、そのアクセスを許可する必要があります。

単純な例が DHCP です。DHCP が許可されていない場合は、DHCP プローブからのデータに依存するプロファイリングが使用できません。ネットワーク スキャンが使用されているが、NMAP プローブから問い合わされるポートへのアクセスがブロックされている場合は、その情報がプロファイリングの決定に使用できません。これには、エンドポイント上で有効になっている SNMP ポートへのアクセスも含まれます。加えて、エンドポイント自体がトラフィックを許可する必要があります。一般的な例は、NMAP を使用して OS スキャンを実行する場合です。パーソナル ファイアウォールがエンドポイントのスキャンをブロックしている場合は、プローブが結果を生成しません。

NetFlow プローブの使用は特に困難な場合があります。これは、エンドポイントがネットワーク上で NetFlow データを収集するための通信アクセスを許可する必要があるためです。そのため、任意のエンドポイントの完全なネットワークアクセスを前提とせずに、ポリシーで初期データ収集を許可する必要があります。考えられる 1 つのソリューションは、VLAN A 上でエンドポイントをプロファイリングすることです。保護されたリソースへのアクセスは拒否して、指定されたポートへの一般的なアクセスは許可します。照合するトラフィックに基づいてプロファイリングしたら、エンドポイントを VLAN B に対して再認可することによって、保護されたリソースへの特権アクセスを許可することができます。

もう 1 つの選択肢は、最初はトラフィックを許可するものの、特徴的ではないトラフィックが検出されたら、ポート認可を変更するより具体的なプロファイルを照合する方法です。たとえば、プロセス制御エンドポイントが想定外のポート上で通信している場合は、エンドポイントを検疫 ID グループとポリシーに割り当てる例外アクションを適用できます。繰り返しになりますが、ISE プロファイリングは、スプーフィング対策ソリューションのターゲットにはならないものの、異常なトラフィックやその他のプロファイリング属性に基づいてポリシーを強制するために使用される場合があります。重要なデバイスが含まれている環境では、これらのデバイスがロック ダウンされたり、既知のエンドポイントのリストへのアクセスが制限されたりします。このような場合は、プロファイリングの値が、特定のプロファイリング ポリシーと一致するすべてのエンドポイントに、それらのデバイス タイプに適合する属性が表示されることを保証する、可視性に関するものになります。

例外アクションの使用は、静的ポリシー割り当てを実行しなければならない場合の手段です。ただし、エンドポイントがプロファイルに静的に割り当てられている場合は、管理者しかその割り当てを変更できないことに注意してください。

# プローブ選択のベスト プラクティス

展開ごとに使用できるプローブが異なります。ここでは、各プローブで入手可能な情報を中心に説明し、展開のタイプに基づくプローブ選択プロセスを辿ります。

## プローブ属性

ネットワークで有効にするプローブを決定したら、プローブごとに収集可能な属性が明確になります。表 8 に、さまざまなプローブ、収集されるキー属性、および適用可能なユースケースを示します。

表 6 プローブとキー属性

| プローブ | キー プロファイリング属性 | 一般的なエンドポイント プロファイリング ユースケース |
|---|---|---|
| RADIUS | • MAC アドレス(OUI)<br>• IP アドレス | MAC アドレス → OUI = デバイス ベンダーの指定。一部のエンドポイントは、ベンダーが特定のデバイスを製造している場合にだけ、この属性を使ってプロファイリングできます。例:サードパーティ製 IP フォン、モバイル デバイス、およびゲーム コンソール。MAC/IP 間バインドとプローブのサポート。 |
| RADIUS とデバイス センサー | • CDP/LLDP<br>• DHCP | CDP/LLDP 情報については SNMP プローブを参照DHCP 情報については DHCP プローブを参照 |
| SNMP | • MAC アドレス/OUI<br>• CDP/LLDP<br>• ARP テーブル | CDP/LLDP を使用するベンダーにとって重要。Cisco IP Phone、カメラ、アクセス ポイント、アプライアンスなど。<br>DHCP(DHCP プローブ情報を参照)<br>MAC アドレス(RADIUS プローブを参照)<br>デバイス ARP テーブルのポーリングによって、ISE MAC/IP 間バインドが生成されます。 |
| DHCP | • DHCP | ハードウェアとソフトウェア用の一意のベンダー ID。OS 検出用の DHCP フィンガープリント。一般名のパターンのホスト名/FQDN が OS またはデバイス タイプを示している場合があります。加えて、他のプローブをサポートするために MAC/IP 間バインドを提供します。 |

| プローブ | キー プロファイリング属性 | 一般的なエンドポイント プロファイリング ユースケース |
|---|---|---|
| NMAP | • オペレーティング システム<br>• 一般ポート<br>• エンドポイント SNMP データ | ネットワーク/クライアント FW によってブロックされないオペレーティング システム検出 IF スキャン。<br>ネットワーク プリンタなどの SNMP エージェントを実行するエンドポイントの分類を提供します。<br>一般 UDP/TCP ポートでリッスンするエンドポイントの検出に適しています。 |
| DNS | • FQDN | 値は、共通命名規則がホスト名/DNS に使用されているかどうかによって異なります。 |
| HTTP | • User-Agent | オペレーティング システム検出。Chrome などの一部のブラウザは実際の OS をマスクします。 |
| NetFlow | • プロトコル<br>• 送信元/宛先 IP<br>• 送信元/宛先/ポート | 一意のトラフィック パターンを持つ、または、汎用ハードウェア/ソフトウェアを使用する特定用途向けエンドポイントの検出に適しています。<br>特定のエンドポイントの異常なトラフィックを検出する場合があります。 |

表 9 に、プローブごとのキー属性の詳細リストを示します。他の属性もプローブごとに使用できますが、次のリストは標準的な展開にとって最も一般的なまたは有益な属性を示しています。

**表 7 プローブとプロファイリング属性の詳細**

| プローブ | キー プロファイリング属性 |
|---|---|
| RADIUS | • **Called-Station-ID（OUI）**<br>• **Framed-IP-Address** |

| | |
|---|---|
| RADIUS とデバイス センサー | • **cdpCachePlatform**<br>• **cdpCacheAddress**<br>• **cdpCacheCapabilities**<br>• **lldpSystemDescription**<br>• **lldpSystemName**<br>• **dhcp-requested-address**<br>• **dhcp-class-identifier**<br>• **dhcp-client-identifier**<br>• **dhcp-parameter-request-list**<br>• **host-name**<br>• **domain-name**<br>• **client-fqdn** |
| SNMP クエリー（SNMP Query） | • **MACAddress（OUI）**<br>• **MAC-IP（ARP）**<br>• **cdpCachePlatform**<br>• **cdpCacheAddress**<br>• **cdpCacheCapabilities**<br>• **lldpSystemDescription**<br>• **lldpSystemName** |
| DHCP | • **dhcp-requested-address**<br>• **dhcp-class-identifier**<br>• **dhcp-client-identifier**<br>• **dhcp-parameter-request-list**<br>• **host-name**<br>• **domain-name**<br>• **client-fqdn** |
| NMAP | • **operating-system**<br>• **tcp-x**<br>• **udp-x**<br>• **SNMP 属性** |
| DNS | • **FQDN** |
| HTTP | • **User-Agent** |

| | |
|---|---|
| NetFlow | • **IPV4_DST_ADDR**<br>• **IPV4_SRC_ADDR**<br>• **PROTOCOL**<br>• **L4_SRC_PORT**<br>• **L4_DEST_PORT**<br>• **MIN_TTL**<br>• **MAX_TTL** |
| その他 | • **PortalUser**<br>• **EndPointSource**<br>• **DeviceRegistrationStatus** |

## プローブ選択の非公式ガイド

特定のユースケース用として選択するプローブを検討するときに、次の疑問を解決する汎用メトリックに基づいて各プローブを評価すると役立つ場合があります。

展開が最も容易なプローブと最も困難なプローブはどれですか。

自社のネットワークへの影響(トラフィック オーバーヘッド、ISE サーバの負荷、またはサポートする追加のコンポーネントに関して)が最も小さいプローブと最も大きいプローブはどれですか。

自社のエンドポイントのプロファイリングにこのプローブを使用するメリットは何ですか。

表 10 に、表 11、12、および 13 に使用されるメトリックと評価の凡例を示します。これらは、さまざまなユースケースのプローブ選択に役立ちます。

表 8 プローブ評価の凡例

| メトリック | | 評価 | | |
|---|---|---|---|---|
| 名前 | 説明 | 1 | 2 | 3 |
| DDI | 展開困難指標 | 容易 | 中型 | 困難 |
| NII | ネットワーク影響指標 | 影響小 | 影響中 | 影響大 |
| PVI | プローブ価値指標 | 価値大 | 価値中 | 価値小 |

## ディスカバリ フェーズ – プローブのベスト プラクティス

表 11 に、ISE 展開のディスカバリ フェーズでのプローブ選択に推奨されているベスト プラクティスとガイダンスを示します。前提条件は、ネットワーク アクセス デバイスを RADIUS ポートの認証と認可用に設定しなければならないことです。そのため、RADIUS プローブなどのキー プローブで、ネットワーク認証に関するデータを収集することができません。

これらの推奨事項は、ISE プロファイリング サービスとの統合が必要な Cisco NAC アプライアンス インストールなどの RADIUS 認証が有効になっていないその他の展開に適用されます。

表 9 プローブ選択 - ディスカバリ フェーズ

| プローブ（方式） | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| RADIUS | - | - | - | • 該当なし | ISE が認証コントロール プレーンにないため適用されません。 |
| RADIUS とデバイス センサー | 2 | 1 | 1 | • CDP/LLDP<br>• DHCP | ネットワークがデバイス センサーをサポートしている場合は、認証コントロール プレーンに関係なく、RADIUS アカウンティングを使用できます。 |
| SNMPTrap | 1 | 1 | 1 | • LinkUp/Down トラップ<br>• MAC 通知トラップ<br>• 情報 | エンドポイント接続の検出/SNMPQuery プローブのトリガー |
| SNMPQuery | 1 | 2 | 1 | • MAC アドレス（OUI）<br>• CDP/LLDP<br>• ARP テーブル | デバイス ARP テーブルのポーリングによって、ISE MAC/IP 間バインドが生成されます。再認証や一時更新による過剰な RADIUS アカウンティング更新によってトリガーされる高い SNMP クエリー トラフィックに注意してください。 |
| DHCP（ヘルパー） | 2 | 1 | 1 | • DHCP | MAC/IP 間バインドを提供します。ネットワークへの影響は比較的小さいですが、低い DHCP リース タイマーに注意してください。 |
| DHCP SPAN | 2 | 3 | 1 | • DHCP | MAC/IP 間バインドを提供します。 |
| NMAP | 1 | 2 | 2 | • オペレーティング システム<br>• 一般ポート<br>• エンドポイント SNMP データ | SNMP データは、UDP/161 公開文字列を前提とします。NMAP の相対値は、お客様のネットワークと OS 検出が有線アクセス ポリシー内の重要な要素かどうかによって決まります。 |

| プローブ（方式） | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| DNS | 1 | 1 | 2 | • FQDN | 値は、共通命名規則が使用されているかどうかによって異なります。 |
| HTTP（リダイレクト） | - | - | - | • 該当なし | ISE が認証コントロール プレーンにないため、適用されません。 |
| HTTP（SPAN） | 2 | 3 | 2 | • User-Agent | インテリジェント SPAN/タップ ソリューションや VACL キャプチャを使用したサーバやインターネット エッジなどの主要な HTTP チョークポイントの SPAN を考慮します。 |
| NetFlow | 3 | 3 | 2 | • プロトコル<br>• 送信元/宛先 IP<br>• 送信元/宛先ポート | 一般的なプロファイリングではなく、特定のユースケースに対してのみ推奨されています。 |

## 有線ネットワーク – プローブのベスト プラクティス

表 12 に、有線ネットワークに展開されたプローブに推奨されているベスト プラクティスとガイダンスを示します。

表 10 プローブ選択 - 有線ネットワーク

| プローブ(方式) | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| RADIUS | 1 | 1 | 1 | • MAC アドレス(OUI)<br>• IP アドレス<br>• ユーザ名、その他 | デバイスの検出とその他のプローブの有効化用の基本的なプローブ。 |
| RADIUS とデバイス センサー | 2 | 1 | 1 | • CDP/LLDP<br>• DHCP | デバイス センサーのサポートを伴う 3000 または 4000 シリーズ アクセス スイッチを実行している場合は、これが特定の属性を収集する最適な方法です。 |
| SNMPTrap | 1 | 1 | 3 | • LinkUp/Down トラップ<br>• MAC 通知トラップ<br>• 情報 | エンドポイント接続の検出/SNMP クエリー プローブのトリガー |
| SNMPQuery | 1 | 2 | 1 | • MAC アドレス(OUI)<br>• CDP/LLDP<br>• ARP テーブル | デバイス ARP テーブルのポーリングによって ISE MAC/IP 間バインドが生成されます。再認証や一時更新による過剰な RADIUS アカウンティング更新によってトリガーされる高い SNMP クエリー トラフィックに注意してください。 |
| DHCP (ヘルパー) | 2 | 1 | 1 | • DHCP 属性 | MAC/IP 間バインドを提供します。低い DHCP リース タイマーに注意してください。 |
| DHCP SPAN | 2 | 3 | 1 | • DHCP 属性 | MAC/IP 間バインドを提供します。 |
| NMAP | 1 | 2 | 2 | • オペレーティング システム<br>• 一般ポート<br>• エンドポイント SNMP データ | SNMP データは、UDP/161 公開文字列を前提とします。 |
| DNS | 1 | 1 | 2 | • FQDN | 値は、共通命名規則が使用されているかどうかによって異なります。 |
| HTTP (リダイレクト) | 2 | 1 | 2 | • ユーザ エージェント | 値は、有線アクセスに対する OS の相対的重要性によって異なります。 |

| プローブ（方式） | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| HTTP（SPAN） | 2 | 3 | 2 | • ユーザ エージェント | インターネット エッジなどの主要な HTTP チョークポイントの SPAN を考慮します。可能な限り、スマート SPAN ソリューションや VACL キャプチャを利用します。 |
| NetFlow | 3 | 3 | 2 | • プロトコル<br>• 送信元/宛先 IP<br>• 送信元/宛先ポート | 一般的なプロファイリングではなく、特定のユースケースに対してのみ推奨されています。 |

## ワイヤレス ネットワーク – プローブのベスト プラクティス

表 13 に、ワイヤレス ネットワークに展開されたプローブに推奨されているベスト プラクティスとガイダンスを示します。

表 11 プローブ選択 - ワイヤレス ネットワーク

| プローブ(方式) | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| RADIUS | 1 | 1 | 1 | • MAC アドレス(OUI)<br>• IP アドレス<br>• ユーザ名、その他 | デバイスの検出とその他のプローブの有効化用の基本的なプローブ。 |
| RADIUS とデバイス センサー | 2 | 1 | 1 | • CDP/LLDP<br>• DHCP | デバイス センサーのサポートを伴う 3000 または 4000 シリーズ アクセス スイッチを実行している場合は、これが特定の属性を収集する最適な方法です。 |
| SNMPTrap | 1 | 1 | 3 | • LinkUp/Down トラップ<br>• MAC 通知トラップ<br>• 情報 | エンドポイント接続の検出/SNMPQuery プローブのトリガー |
| SNMPQuery | 1 | 2 | 1 | • MAC アドレス(OUI)<br>• CDP/LLDP<br>• ARP テーブル | デバイス ARP テーブルのポーリングによって、ISE MAC/IP 間バインドが生成されます。再認証や一時更新による過剰な RADIUS アカウンティング更新によってトリガーされる高い SNMP クエリー トラフィックに注意してください。 |
| DHCP (ヘルパー) | 2 | 1 | 1 | • DHCP | MAC/IP 間バインドを提供します。低い DHCP リース タイマーに注意してください。 |
| DHCP SPAN | 2 | 3 | 1 | • DHCP | MAC/IP 間バインドを提供します。 |
| NMAP | 1 | 2 | 2 | • オペレーティング システム<br>• 一般ポート<br>• エンドポイント SNMP データ | SNMP データは、UDP/161 公開文字列を前提とします。 |
| DNS | 1 | 1 | 2 | • FQDN | 値は、共通命名規則が使用されているかどうかによって異なります。 |
| HTTP(リダイレクト) | 2 | 1 | 2 | • ユーザ エージェント | 値は、有線アクセスに対する OS の相対的重要性によって異なります。 |

| プローブ（方式） | EDI | NII | PVI | キー プロファイリング属性 | 注記 |
|---|---|---|---|---|---|
| HTTP（SPAN） | 2 | 3 | 2 | • ユーザ エージェント | インターネット エッジなどの主要な HTTP チョークポイントの SPAN を考慮します。可能な限り、スマート SPAN ソリューションや VACL キャプチャを利用します。 |
| NetFlow | 3 | 3 | 2 | • プロトコル<br>• 送信元/宛先 IP<br>• 送信元/宛先ポート | 一般的なプロファイリングではなく、特定のユースケースに対してのみ推奨されています。 |

# プロファイリング計画

デバイス分類（デバイス タイプに基づく可視性またはネットワーク アクセス用）が必要なさまざまなタイプのエンドポイントを確認して、必要なデータを収集するために最適なプローブを決定したら、次のステップはプロファイリング計画を文書化することです。この計画には、少なくとも、プロファイリングするすべてのデバイスと、プロファイリング データを使用してネットワーク アクセスを許可する方法を含める必要があります。また、計画には、エンドポイントの分類に必要な一意の属性のリスト、それらの属性のキャプチャに使用されるプローブまたは方法、および収集方法の詳細も含める必要があります。たとえば、HTTP のキャプチャに URL リダイレクションまたは SPAN を使用するか。データはどこからキャプチャするか。どの PSN でデータを受信するか。計画のもう 1 つの重要な側面は、拡張性と冗長性をどのように展開するかです。

注：ロード バランシングを含む高可用性と拡張性のプロファイリングについては、このドキュメントでは扱いません。

表 14 に、サンプル企業の基本プロファイリング計画を示します。

表 12 サンプル プロファイリング計画

| デバイス プロファイル | 認証ポリシー ルールの使用場所 | 一意の属性 | 使用されるプローブ | 収集方法 |
|---|---|---|---|---|
| Cisco IP Phone | Cisco-IP-Phones（MAB） | OUI | RADIUS | RADIUS 認証 |
| | | CDP | SNMP クエリー（SNMP Query） | RADIUS 開始によるトリガー |
| IP カメラ | Cisco-IP-Cameras（MAB） | OUI | RADIUS | RADIUS 認証 |
| | | CDP | SNMP クエリー（SNMP Query） | RADIUS 開始によるトリガー |
| プリンタ | プリンタ（MAB） | OUI | RADIUS | RADIUS 認証 |
| | | DHCP クラス識別子 | DHCP | ローカル レイヤ 3 スイッチ SVI からの IP ヘルパー |
| Point of Sale（PoS）ステーション（静的 IP） | POS（MAB） | MAC アドレス（MAC Address） | RADIUS（MAC アドレス検出） | RADIUS 認証 |
| | | MAC/IP 間マッピング用の ARP キャッシュ | SNMP クエリー（SNMP Query） | RADIUS 開始によるトリガー |
| | | DNS 名 | DNS | IP 検出によるトリガー |

| デバイス プロファイル | 認証ポリシー ルールの使用場所 | 一意の属性 | 使用されるプローブ | 収集方法 |
|---|---|---|---|---|
| Apple iDevice | Employee_Personal（802.1X/CWA） | OUI | RADIUS | RADIUS 認証 |
| | | ブラウザ ユーザ エージェント | HTTP | 中央のポリシー サービス ノード クラスタへの認可ポリシー ポスチャ リダイレクト |
| | | DHCP クラス識別子と MAC/IP 間マッピング | DHCP | ローカル レイヤ 3 スイッチ SVI からの IP ヘルパー |
| デバイス X | Critical_Device_X（MAB） | MAC アドレス（MAC Address） | RADIUS（MAC アドレス検出） | RADIUS 認証 |
| | | MAC/IP 間マッピング用に要求された IP アドレス | DHCP | ローカル ポリシー サービス ノードへの DHCP サーバ ポートの RSPAN |
| | | MAC/IP 間マッピング用の ARP キャッシュを取得するためのオプション | SNMP クエリー（SNMP Query） | RADIUS アカウンティング開始によるトリガー |
| | | 宛先ポート/IP へのトラフィック | NetFlow | Distribution 6500 スイッチから中央のポリシー サービス ノードへの NetFlow エクスポート |

## プロファイリングのベスト プラクティスと推奨事項のまとめ

ここでは、ISE プロファイリングに関するベスト プラクティスの推奨事項をまとめます。

可能な場合は、デバイス センサーを使用してデータ収集を最適化します。

- 可能な場合は、必ず、特定のエンドポイントのプロファイル データが同じポリシー サービス ノードに送信されるようにします。そうしなかった場合は、複数の PSN によるエンドポイント データの過剰な更新と競合が発生する可能性があります。
- 多くの場合、ISE はこの状態を自動的に処理します。
- SNMP クエリーは、RADIUS アカウンティング開始または SNMP トラップ パケットを受信した同じ PSN から発行されます。
- URL リダイレクションから発生した HTTP トラフィックは、RADIUS セッションを処理している PSN に送信されます。
- DHCP ヘルパーは複数の PSN に送信できるため、特定のアクセス デバイスの RADIUS 用に設定されたものと同じ PSN に送信することをお勧めします。

- DNS クエリーは IP アドレスを学習するものと同じ PSN から送信されます。通常、この PSN は、RADIUS セッションを処理し、RADIUS アカウンティングからの Framed-IP-Address、DHCP からの dhcp-requested-address、cdpCacheAddress のトリガーされた SNMP クエリーのいずれかから IP アドレスを受信する PSN です。
- トリガーされた NMAP スキャンは、ポリシー ルールが一致して抽出されたプロファイリング データを受信するものと同じ PSN によって供給されます。たとえば、NMAP アクションが OUI 照合に基づいてプロファイル ルール条件に割り当てられる場合は、RADIUS、DHCP、またはその他のプローブを介してエンドポイント MAC アドレスを受信した最初の PSN が NMAP スキャンを供給する PSN になります。
- また、DHCP SPAN、HTTP SPAN、NetFlow プローブなどを使用するケースでは、トラフィックが分散展開内の同じ PSN に必ず到達するようにできないことがあります。

HTTP プローブ:

- SPAN の代わりに URL リダイレクションを使用して収集を一元化することによって、SPAN/RSPAN に関連したトラフィック負荷を削減します。
- なるべく、HTTP SPAN を使用したデータ収集は避けるようにしてください。使用する場合:
- インターネット エッジやワイヤレス コントローラ接続などの重要なトラフィック チョークポイントを探します。
- インテリジェント SPAN/タップ オプションまたは VACL キャプチャを使用して、IS に送信されるデータ量を制限します。
- インテリジェント ネットワーク タップ インフラストラクチャを使用せずに SAPN の高可用性を実現するのは困難な可能性があります。

DHCP プローブ:

- 可能な場合は、DHCP リレー(IP ヘルパー)を使用します。
- なるべく、DHCP SPAN を使用したデータ収集は避けるようにしてください。使用する場合は、プローブが中央の DHCP サーバへのトラフィックをキャプチャしていることを確認します。
- DHCP を供給しているレイヤ 3 デバイスは、同じネットワークに対して DHCP を中継しないことに注意してください。
- インテリジェント ネットワーク タップ インフラストラクチャを使用せずに SAPN の高可用性を実現するのは困難な可能性があります。
- SNMP プローブ:
- 高い再認証(低いセッション/再認証タイマー)または頻繁な中間アカウンティング更新の結果としてトリガーされる RADIUS アカウンティング更新による高い SNMP トラフィックに注意してください。
- ポーリングするクエリーに対して、ポーリング間隔を低く設定しすぎないように注意してください。ISE ネットワーク デバイスの設定でポーリングに最適な PSN を設定してください。
- SNMP トラップは、RADIUS ベースの認証および認可を使用したネットワークではなく、主に、NAC アプライアンスとの統合などの非 RADIUS 展開に役立ちます。
- NetFlow:特定のユースケースに対してのみ使用します。NetFlow は、ネットワーク デバイスと PSN に高い負荷をもたらす可能性があります。

# 付録 A：参考資料

## Cisco TrustSec System：

http://www.cisco.com/go/trustsec

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

## デバイス設定ガイド：

Cisco Identity Services Engine ユーザ ガイド：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco NX-OS ソフトウェアのリリースに関する詳細については、次の URL を参照してください。

Cisco Catalyst 2900 シリーズ スイッチの場合：
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000 シリーズ スイッチの場合：
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000-X シリーズ スイッチの場合：
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

Cisco Catalyst 4500 シリーズ スイッチの場合：
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

Cisco Catalyst 6500 シリーズ スイッチの場合：
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

Cisco ASR 1000 シリーズ ルータの場合：
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

シスコ ワイヤレス LAN コントローラの場合：
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html