CHAPTER 21

Cisco ISE エンドポイント プロファイリング ポリシー

この章では、Cisco ISE ネットワークに接続するエンドポイントを Cisco ISE がプロファイリングする方法、およびこれらのエンドポイントを管理し、ネットワーク リソースへのアクセスを許可するためのプロファイリング ポリシーを作成する方法について説明します。

この章では、次のトピックについて取り上げます。

Cisco ISE プロファイリング サービス

Cisco Identity Services Engine（ISE）のプロファイリング サービスは、ネットワークに接続するデバイスおよびその場所を識別します。エンドポイントは、Cisco ISE で設定されたエンドポイント プロファイリング ポリシーに基づいてプロファイリングされます。次に、Cisco ISE は、ポリシー評価の結果に基づいて、ネットワーク内のリソースにアクセスする権限をエンドポイントに付与します。

プロファイリング サービス：

- IEEE 規格 802.1X ポートベースの認証アクセス コントロール、MAC 認証バイパス（MAB）認証、およびネットワーク アドミッション コントロール（NAC）をさまざまな規模および複雑度の企業ネットワークに使用して、認証の効率的かつ効果的な展開および継続的な管理を容易にします。
- デバイス タイプにかかわらず、接続されたすべてのネットワーク エンドポイントの機能を特定、検索、および決定します。
- 一部のエンドポイントへのアクセスを誤って拒否しないようにします。

関連項目

- 「プロファイリング サービスを使用するエンドポイント インベントリ」（P.21-2）
- 「Cisco ISE プロファイラ キュー制限の設定」（P.21-2）

プロファイリング サービスを使用するエンドポイント インベントリ

ネットワークに接続されたすべてのエンドポイントの機能を検出、特定、および決定するためにプロファイリング サービスを使用できます。デバイスのタイプに関係なく、企業ネットワークへのエンドポイントの適切なアクセスを保証および維持できます。

プロファイリング サービスでは、エンドポイントの属性をネットワーク デバイスとネットワークから収集し、エンドポイントをそのプロファイルに従って特定のグループに分類します。一致したプロファイルを持つエンドポイントが Cisco ISE データベースに保存されます。プロファイリング サービスで処理されるすべての属性は、プロファイラ ディクショナリに定義されている必要があります。

プロファイリング サービスは、ネットワーク上の各エンドポイントを識別し、そのプロファイルに従ってそれらのエンドポイントを、システム内の既存のエンドポイント ID グループまたはシステムで作成できる新しいグループにグループ化することができます。エンドポイントをグループ化し、エンドポイントのプロファイリング ポリシーをエンドポイント ID グループに適用すると、対応するエンドポイント プロファイリング ポリシーへのエンドポイントのマッピングを決定できます。

Cisco ISE プロファイラ キュー制限の設定

Cisco ISE プロファイラは、ネットワークから大量のエンドポイント データを短時間で収集します。それにより、一部の遅い Cisco ISE コンポーネントがプロファイラによって生成されるデータを処理するときにバックログが蓄積されるため、Java 仮想マシン（JVM）のメモリ使用率が増大し、パフォーマンスの低下および安定性の問題が生じます。

プロファイラが JVM メモリ使用率を増やさず、また、JVM がメモリ不足になり、再起動しないように、プロファイラの次の内部コンポーネントに制限が適用されます。

- エンドポイント キャッシュ：内部キャッシュのサイズは制限され、サイズが制限を超えると定期的に消去する必要があります（最長未使用時間方式に基づく）。
- フォワーダ：プロファイラによって収集されたエンドポイント情報のメイン入力キュー。
- イベント ハンドラ：高速コンポーネントを接続解除する内部キューで、（通常、データベース クエリーに関連する）低速処理コンポーネントにデータを提供します。

エンドポイント キャッシュ

次に例を示します。

- maxEndPointsInLocalDb = 100000（キャッシュ内のエンドポイント オブジェクト）
- endPointsPurgeIntervalSec = 300（秒単位のエンドポイント キャッシュ消去スレッド間隔）

- numberOfProfilingThreads = 8（スレッド数）

制限は、すべてのプロファイラ内部イベント ハンドラに適用されます。キュー サイズ制限に達すると、モニタリング アラームがトリガーされます。

Cisco ISE プロファイラのキュー サイズの制限

次に例を示します。

- forwarderQueueSize = 5000（エンドポイント収集イベント）
- eventHandlerQueueSize = 10000（イベント）

イベント ハンドラ

- NetworkDeviceEventHandler：すでにキャッシュされているネットワーク アクセス デバイス（NAD）の重複 IP アドレスのフィルタリングのほか、ネットワーク デバイスのイベント用。
- ARPCacheEventHandler：ARP キャッシュのイベント用。

CoA ハンドラ

- CoAHandler：処理のキューにまだ残っている重複 MAC アドレスのフィルタリングのほか、CoA イベント用。

platform.properties ファイルで以下に示すようにプロファイラ キュー制限などを設定できます。このファイルは、Cisco ISE インストール中に含められ、次の場所にあります。/opt/CSCOcpm/config/

次に例を示します。

```
# ------------------------------------------------------------
# Profiler Settings
# ------------------------------------------------------------

profiler.maxEndPointsInLocalDb=100000
profiler.endPointsPurgeIntervalSec=300
profiler.numberOfProfilingThreads=8
<ucsSmall>.profiler.forwarderQueueSize=5000
<ucsLarge>.profiler.forwarderQueueSize=5000
<ibmSmallMedium>.profiler.forwarderQueueSize=5000
<ibmLarge>.profiler.forwarderQueueSize=5000
<ucsSmall>.profiler.eventHandlerQueueSize=10000
<ucsLarge>.profiler.eventHandlerQueueSize=10000
<ibmSmallMedium>.profiler.eventHandlerQueueSize=10000
<ibmLarge>.profiler.eventHandlerQueueSize=10000
```

Cisco ISE ノードでのプロファイリング サービスの設定

Cisco ISE 対応ネットワーク内のネットワーク リソースを使用しているすべてのエンドポイントのコンテキスト インベントリを提供するプロファイリング サービスを設定できます。

デフォルトで管理、モニタリング、およびポリシー サービスのすべてのペルソナを担当する単一の Cisco ISE ノード上で実行されるようにプロファイリング サービスを設定できます。

分散展開では、プロファイリング サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、管理ペルソナとモニタリング ペルソナを担当する他の Cisco ISE ノードでは実行されません。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3　[展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4　[全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5　次の作業を行います。

a. [セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにして、ネットワーク アクセス サービス、ポスチャ サービス、ゲスト サービス、およびクライアント プロビジョニング サービスを実行にします。

b. [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにして、プロファイリング サービスを実行にします。

ステップ 6　[保存（Save）] をクリックしてノード設定を保存します。

プロファイリング サービスで使用されるネットワーク プローブ

ネットワーク プローブは、ネットワーク上のエンドポイントから属性を収集するために使用される方法です。プローブを使用して、エンドポイントを Cisco ISE データベース内の一致するプロファイルで作成または更新できます。

Cisco ISE は、ネットワーク上のデバイスの動作を分析し、デバイス タイプを決定するいくつかのネットワーク プローブを使用して、デバイスをプロファイリングできます。ネットワーク プローブは、ネットワークの可視性の向上に役立ちます。

次のプローブが Cisco ISE でサポートされます。

- 「NetFlow プローブ」（P.21-4）
- 「DHCP プローブ」（P.21-5）
- 「DHCP SPAN プローブ」（P.21-6）
- 「HTTP プローブ」（P.21-7）
- 「HTTP SPAN プローブ」（P.21-7）
- 「RADIUS プローブ」（P.21-7）
- 「ネットワーク スキャン プローブ」（P.21-8）
- 「DNS プローブ」（P.21-10）
- 「SNMP クエリー プローブ」（P.21-12）
- 「SNMP トラップ プローブ」（P.21-14）

NetFlow プローブ

Cisco ISE プロファイラは Cisco IOS NetFlow Version 9 を実装しています。CNetFlow Version 9 には、プロファイラを拡張して Cisco ISE プロファイリング サービスをサポートするために必要な追加機能があり、NetFlow Version 9 を使用することを推奨します。

NetFlow Version 9 の属性を NetFlow 対応のネットワーク アクセス デバイスから収集して、エンドポイントを作成したり、Cisco ISE データベース内の既存のエンドポイントを更新できます。NetFlow Version 9 は、エンドポイントの送信元 MAC アドレスと宛先 MAC アドレスを割り当てて、更新するように設定できます。NetFlow 属性のディクショナリを作成して NetFlow ベースのプロファイリングに対応することもできます。

さらに、Cisco ISE は Version 5 以前の NetFlow バージョンをサポートします。ネットワークで NetFlow Version 5 を使用する場合は、Version 5 をアクセス レイヤのプライマリ ネットワーク アクセス デバイス（NAD）でのみ使用できます。他のデバイスでは動作しません。

Cisco IOS NetFlow Version 5 パケットには、エンドポイントの MAC アドレスが含まれません。NetFlow Version 5 から収集された属性は、Cisco ISE データベースに直接追加できません。IP アドレスを使用してエンドポイントを検出し、NetFlow Version 5 属性をエンドポイントに追加します。これは、ネットワーク アクセス デバイスの IP アドレスと NetFlow Version 5 属性の IP アドレスを組み合わせることによって行うことができます。ただし、これらのエンドポイントを RADIUS または SNMP プローブで事前に検出しておく必要があります。

NetFlow Version 5 の旧バージョンでは、MAC アドレスは IP フローの一部ではありません。NetFlow Version 5 の旧バージョンでは、ネットワーク アクセス デバイスから収集されたエンドポイント キャッシュ内の属性情報を相互に関連付けることによって、エンドポイントをその IP アドレスでプロファイリングする必要があります。

関連項目

- 詳細は、表 6 の NetFlow Version 9 フロー レコード形式の「NetFlow Version 9 Field Type Definitions」を参照してください。
  http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html
- NetFlow Version 5 レコード形式の詳細については、
  http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html#wp1030618 を参照してください。
- 「プロファイリング ノードの設定」（P.A-5）

DHCP プローブ

Cisco ISE 展開の Dynamic Host Configuration Protocol プローブを有効にすると、Cisco ISE プロファイリング サービスで INIT-REBOOT および SELECTING メッセージ タイプの新しい要求だけに基づいてエンドポイントを再プロファイリングできます。RENEWING や REBINDING などの他の DHCP メッセージ タイプは処理されますが、エンドポイントのプロファイリングには使用されません。DHCP パケットから解析された属性は、エンドポイント属性にマッピングされます。

INIT-REBOOT 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントが前に割り当てられてキャッシュされた設定を確認する場合、クライアントはサーバ識別子（server-ip）オプションを入力できません。代わりに、前に割り当てられた IP アドレスを要求された IP アドレス（requested-ip）オプションに入力する必要があります。また、DHCPREQUEST メッセージのクライアント IP アドレス（ciaddr）フィールドをゼロで埋める必要があります。要求された IP アドレスが正しくない場合、またはクライアントが誤ったネットワークに配置されている場合、DHCP サーバは DHCPNAK メッセージをクライアントに送信します。

SELECTING 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントは、サーバ識別子（server-ip）オプションで選択された DHCP サーバの IP アドレスを挿入し、要求された IP アドレス（requested-ip）オプションにクライアントによって選択された DHCPOFFER の [IP アドレス（Your IP Address）]（yiaddr）フィールドの値を入力します。また、「ciaddr」フィールドをゼロで埋めます。

表 21-1 に、DHCP クライアント メッセージのさまざまな状態を示します。

表 21-1　さまざまな状態からの DHCP クライアント メッセージ

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
ブロードキャスト /ユニキャスト	ブロードキャスト	ブロードキャスト	ユニキャスト	ブロードキャスト
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	ゼロ	ゼロ	IP アドレス	IP アドレス

関連項目

- 「DHCP ブリッジ モードでのワイヤレス LAN コントローラの設定」（P.21-6）
- 「プロファイリング ノードの設定」（P.A-5）

DHCP ブリッジ モードでのワイヤレス LAN コントローラの設定

ワイヤレス LAN コントローラ（WLC）はダイナミック ホスト コンフィギュレーション プロトコル（DHCP）ブリッジ モードで設定することを推奨します。このモードでは、ワイヤレス クライアントからのすべての DHCP パケットを Cisco ISE に転送できます。

WLC Web インターフェイスの [コントローラ（Controller）] > [詳細設定（Advanced）] > [DHCP マスター コントローラ モード（DHCP Master Controller Mode）] > [DHCP パラメータ（DHCP Parameters）] で使用可能な [DHCP プロキシの有効化（Enable DHCP Proxy）] チェックボックスをオフにする必要があります。

DHCP IP ヘルパー コマンドが Cisco ISE ポリシー サービス ノードを指していることも確認する必要があります。

DHCP SPAN プローブ

DHCP スイッチド ポート アナライザ（SPAN）プローブは、Cisco ISE ノードで初期化されると、特定インターフェイス上のネットワーク アクセス デバイスからのネットワーク トラフィックをリッスンします。DHCP SPAN パケットを DHCP サーバから Cisco ISE プロファイラに転送するようにネットワーク アクセス デバイスを設定する必要があります。プロファイラはこれらの DHCP SPAN パケットを受信して解析し、エンドポイントのプロファイリングに使用できるエンドポイント属性を取得します。

```
For example,
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

関連項目

「プロファイリング ノードの設定」（P.A-5）

HTTP プローブ

HTTP プローブでは、識別文字列は HTTP 要求ヘッダーのフィールド User-Agent で送信されます。これは、IP タイプのプロファイリング条件を作成し、Web ブラウザ情報をチェックするために使用できる属性です。プロファイラは Web ブラウザ情報を User-Agent 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。

Cisco ISE 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。Cisco ISE には、多くのデフォルト プロファイルが用意されています。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。

関連項目

「プロファイリング ノードの設定」（P.A-5）

HTTP SPAN プローブ

Cisco ISE 展開の HTTP プローブをスイッチド ポート アナライザ（SPAN）プローブとともに有効にすると、プロファイラは指定されたインターフェイスからの HTTP パケットをキャプチャできます。SPAN 機能は、Cisco ISE サーバが Web ブラウザからの通信をリッスンするポート 80 で使用できます。

HTTP SPAN は、HTTP 要求ヘッダー メッセージの HTTP 属性を IP ヘッダー（L3 ヘッダー）の IP アドレスとともに収集し、L2 ヘッダーのエンドポイントの MAC アドレスに基づいてエンドポイントに関連付けることができます。この情報は、Apple デバイスやさまざまなオペレーティング システムのコンピュータなどの各種モバイルおよびポータブル IP 対応デバイスを識別するのに役立ちます。ゲスト ログインまたはクライアント プロビジョニング ダウンロード時に Cisco ISE サーバはキャプチャをリダイレクトするので、各種モバイルおよびポータブル IP 対応デバイスの識別の信頼性が向上します。これにより、プロファイラは User-Agent 属性とその他の HTTP 属性を要求メッセージから取得し、Apple デバイスなどのデバイスを識別できます。

関連項目

「VMware 上で実行している Cisco ISE の HTTP 属性を収集できない」（P.21-7）

VMware 上で実行している Cisco ISE の HTTP 属性を収集できない

Cisco ISE を ESX サーバ（VMware）に展開している場合、Cisco ISE プロファイラは Dynamic Host Configuration Protocol トラフィックを収集しますが、vSphere クライアント上の設定の問題により HTTP トラフィックを収集しません。

VMware セットアップで HTTP トラフィックを収集するには、Cisco ISE プロファイラのために作成する仮想スイッチの無差別モードを Accept から Reject（デフォルト）に変更して、セキュリティを設定します。DHCP および HTTP のスイッチド ポート アナライザ（SPAN）プローブが有効になっている場合は、Cisco ISE プロファイラによって DHCP トラフィックと HTTP トラフィックの両方が収集されます。

RADIUS プローブ

Cisco ISE で認証に RADIUS を使用するように設定し、クライアント サーバ トランザクションで使用できる共有秘密を定義できます。RADIUS サーバから受信された RADIUS 要求および応答メッセージを使用して、プロファイラはエンドポイントのプロファイリングに使用できる RADIUS 属性を収集できます。

Cisco ISE は RADIUS サーバ、および他の RADIUS サーバに対する RADIUS プロキシ クライアントとして動作できます。プロキシ クライアントとして動作する場合は、外部の RADIUS サーバを使用して RADIUS 要求および応答メッセージを処理します。

関連項目

「プロファイリング ノードの設定」（P.A-5）

ネットワーク スキャン プローブ

Cisco ISE では、NMAP の手動サブネット スキャンを使用してサブネット内のデバイスを検出できます。展開内の管理者ポータルでポリシー サービス ノードを選択し、プロファイリング サービスを実行するために、有効になっているそのポリシー サービス ノードで手動でのサブネットワーク スキャンを実行する必要があります。

NMAP の各手動サブネット スキャンには一意の数値 ID があり、エンドポイント ソース情報をそのスキャン ID で更新するために使用します。エンドポイントの検出時に、エンドポイント ソース情報を更新して、ネットワーク スキャン プローブで検出されたことを示すこともできます。

NMAP の手動サブネット スキャンは、Cisco ISE ネットワークに常に接続され、スタティック IP アドレスが割り当てられているプリンタなどのデバイスの検出に便利です。これらのデバイスは、他のプローブによって検出できません。

関連項目

- 「プロファイリング ノードの設定」（P.A-5）
- 「IP アドレスと MAC アドレスのバインディング」（P.21-9）

NMAP の手動サブネット スキャンの制限

次は NMAP の手動サブネット スキャンの制限です。

- サブネットをスキャンするとリソースが大量に消費されます。
- サブネットのスキャンは、サブネットのサイズや密度によって時間のかかるプロセスです。
- アクティブなスキャンの数は常に 1 つに制限されるため、同時にスキャンできるサブネットは 1 つだけです。

サブネット スキャンの進行中にいつでもサブネット スキャンをキャンセルできます。[クリックして最新のスキャン結果を表示（Click to see latest scan results）] リンクを使用して、[管理（Administration）] > [ID（Identities）] > [最新のネットワーク スキャン結果（Latest Network Scan Results）] に保存されている最新のネットワーク スキャンの結果を表示できます。

関連項目

「WLC Web インターフェイスでの呼出端末 ID タイプの設定」（P.21-11）

NMAP の手動サブネット スキャン コマンド

次の NMAP コマンドを使用すると、サブネットがスキャンされます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX -
<subnet>
```

表 21-2　手動サブネットのスキャンの NMAP コマンド

-O	OS 検出を有効にします
-sU	UDP スキャン
-p <port ranges>	指定されたポートのみをスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

Network Mapper と Cisco ISE の統合

Network Mapper（NMAP）は、プロファイリング サービス機能を拡張して、特に iDevice などのモバイル デバイスのエンドポイント分類をより適切に行うために、Cisco ISE プロファイラに統合されています。ネットワーク スキャン プローブを使用して特定のサブネットに対して手動サブネット スキャンを実行するか、ネットワーク スキャン アクションをエンドポイント プロファイル（特定のプロファイル）に関連付けてエンドポイントに対してスキャンを実行できます。

関連項目

- NMAP の詳細については、『Network Mapper (NMAP)』および http://nmap.org/docs.html から入手できる NMAP ドキュメントを参照してください。
- ネットワーク スキャンの詳細については、「NMAP の手動サブネット スキャン コマンド」（P.21-8）を参照してください。

NMAP の手動サブネット スキャンの SNMP read-only コミュニティ ストリング

NMAP の手動サブネット スキャンは、スキャンによってエンドポイント上で UDP ポート 161 が開いていることが検出されるたびに、SNMP クエリーで拡張され、より多くの属性が収集されるようになります。NMAP の手動サブネット スキャン中は、ネットワーク スキャン プローブによって、デバイスで SNMP ポート 161 が開いているかどうかが検出されます。ポートが開いている場合は、デフォルトのコミュニティ ストリング（public）を使用して SNMP クエリーがトリガーされます。デバイスで SNMP がサポートされ、デフォルトの read-only コミュニティ ストリングが public に設定されている場合は、デバイスの MAC アドレスを MIB 値「ifPhysAddress」から取得できます。

さらに、[プロファイラ設定（Profiler Configuration）] ページで、NMAP の手動ネットワーク スキャンにカンマで区切られた追加の SNMP read-only コミュニティ ストリングを設定できます。SNMP バージョン 1 および 2c で SNMP MIB ウォークに新しい read-only コミュニティ ストリングを指定することもできます（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）]）。

関連項目

「COA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定」（P.21-15）

IP アドレスと MAC アドレスのバインディング

エンドポイントを作成または更新するには、企業ネットワークでの MAC アドレスを使用する必要があります。ARP キャッシュにエントリが見つからない場合は、Cisco ISE で HTTP パケットの L2 MAC アドレスと NetFlow パケットの IN_SRC_MAC を使用してエンドポイントを作成または更新できます。

エンドポイントが 1 ホップだけ離れている場合、プロファイリング サービスは L2 隣接関係に依存します。エンドポイントに L2 隣接関係がある場合、エンドポイントの IP アドレスと MAC アドレスはすでにマッピングされているため、IP-MAC キャッシュ マッピングは必要ありません。エンドポイントに L2 隣接関係が存在せず、エンドポイントが複数ホップ離れている場合、マッピングが信頼できない可能性があります。

収集する NetFlow パケットの既知の属性には、PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC、OUT_SRC_MAC などがあります。エンドポイントに L2 隣接関係が存在せず、L3 ホップに関して複数ホップ離れている場合は、IN_SRC_MAC 属性で L3 ネットワーク デバイスの MAC アドレスのみが伝送されます。

Cisco ISE で HTTP プローブが有効になっている場合は、エンドポイントの作成に HTTP パケットの MAC アドレスを使うしかありません。ペイロード データのエンドポイントの IP アドレスと MAC アドレスが HTTP 要求メッセージによって伝送されないためです。

Cisco ISE では、プロファイリング サービスで ARP キャッシュが実装されるため、エンドポイントの IP アドレスと MAC アドレスを確実にマッピングできます。ARP キャッシュを機能させるには、DHCP プローブまたは RADIUS プローブを有効にする必要があります。DHCP プローブと RADIUS プローブは、ペイロード データでエンドポイントの IP アドレスと MAC アドレスを伝送します。DHCP プローブの dhcp-requested address 属性と RADIUS プローブの Framed-IP-address 属性によって、エンドポイントの IP アドレスがその MAC アドレスとともに伝送されます。これらのアドレスは、マッピングして ARP キャッシュに格納できます。

DNS プローブ

Cisco ISE 展開のドメイン ネーム サーバ（DNS）プローブを使用すると、プロファイラはエンドポイントを検索し、完全修飾名（FQDN）を取得できます。Cisco ISE 対応のネットワークでエンドポイントが検出されたら、エンドポイント属性のリストが NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP プローブから収集されます。

Cisco ISE をスタンドアロンで展開する場合、または初めて分散環境に展開する場合は、セットアップ ユーティリティを実行して Cisco ISE アプライアンスを設定するように求められます。セットアップ ユーティリティを実行するときに、ドメイン ネーム システム（DNS）ドメインとプライマリ ネーム サーバ（プライマリ DNS サーバ）を設定します。設定時には、1 つ以上のネームサーバを設定できます。Cisco ISE の展開後に、CLI コマンドを使用して DNS ネームサーバを変更または追加することもできます。

関連項目

- CLI コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。
- 「WLC Web インターフェイスでの呼出端末 ID タイプの設定」（P.21-11）
- 「プロファイリング ノードの設定」（P.A-5）

DNS FQDN ルックアップ

DNS ルックアップを実行する前に、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP のいずれかのプローブを DNS プローブとともに起動する必要があります。これにより、プロファイラの DNS プローブは、Cisco ISE 展開に定義されている、指定されたネームサーバに対して逆引き DNS ルックアップ（FQDN ルックアップ）を実行できます。新しい属性がエンドポイントの属性リストに追加さ

れ、エンドポイント プロファイリング ポリシーの評価に使用できます。FQDN は、システム IP ディクショナリに存在する新しい属性です。エンドポイント プロファイリング条件を作成して、FQDN 属性およびそのプロファイリング用の値を検証できます。

次は、DNS ルックアップ、およびこれらの属性を収集するプローブに必要な特定のエンドポイント属性です。

- dhcp-requested-address 属性：DHCP プローブと DHCP SPAN プローブによって収集される属性
- SourceIP 属性：HTTP プローブによって収集される属性
- Framed-IP-Address 属性：RADIUS プローブによって収集される属性
- cdpCacheAddress 属性：SNMP プローブによって収集される属性

ブリッジ モードのインライン ポスチャ ノード展開での DNS ルックアップ

ドメイン ネーム サービス プローブをブリッジ モードのインライン ポスチャ展開で使用するには、ワイヤレス LAN コントローラ（WLC）に RADIUS メッセージで送信される callStationIdType 情報を設定する必要があります。

RADIUS メッセージの Framed-IP-Address 属性には、MAC アドレス形式の呼出端末 ID タイプは含まれません。したがって、RADIUS メッセージをエンドポイントの MAC アドレスに関連付けることも、DNS プローブで逆引き DNS ルックアップを実行することもできません。エンドポイントをプロファイリングするには、Cisco ISE で RADIUS プローブと DNS プローブを有効にし、現在の IP アドレス形式ではなく MAC アドレス形式の発信側ステーション ID を RADIUS メッセージで送信するように WLC を設定します。

WLC は、現在の IP アドレス形式ではなく MAC アドレス形式の発信側ステーション ID を RADIUS メッセージで送信するように設定する必要があります。

callStationIdType を WLC で設定すると、選択した発信側ステーション ID が RADIUS サーバおよびその他のアプリケーションとの通信に使用されます。これにより、エンドポイントが認証され、DNS プローブは指定されているネームサーバに対して逆引き DNS ルックアップ（FQDN ルックアップ）を実行し、エンドポイントの FQDN を更新します。

関連項目

- WLC GUI 設定：『*Cisco Wireless LAN Controller Configuration Guide, Release 7.0*』の「Using the GUI to Configure RADIUS」の項（第 6 章「Configuring Security Solutions」）。
- WLC CLI 設定：『*Cisco Wireless LAN Controller Command Reference, Release 7.0*』の config radius callStationIdType コマンド（第 2 章「CLI Commands」）。
- 「WLC Web インターフェイスでの呼出端末 ID タイプの設定」（P.21-11）

WLC Web インターフェイスでの呼出端末 ID タイプの設定

WLC Web インターフェイスを使用して、呼出端末 ID タイプ情報を設定できます。WLC Web インターフェイスの [セキュリティ（Security）] タブに移動して、[RADIUS 認証サーバ（RADIUS Authentication Servers）] ページで発信側ステーション ID を設定できます。WLC Web インターフェイスの [MAC デリミタ（MAC Delimiter）] フィールドはデフォルトで [コロン（Colon）] に設定されています。

ステップ 1　ワイヤレス LAN コントローラのユーザ インターフェイスにログインします。

ステップ 2　[セキュリティ（Security）] をクリックします。

ステップ 3　[AAA] を展開し、[RADIUS] > [認証（Authentication）] を選択します。

ステップ 4　[呼出端末 ID タイプ（Call Station ID Type）] ドロップダウン リストから [システム MAC アドレス（System MAC Address）] を選択します。

ステップ 5　Cisco ISE を FIPS モードで実行する場合、[AES キー ラップ（AES Key Wrap）] チェックボックスをオンにします。

ステップ 6　[MAC デリミタ（MAC Delimiter）] ドロップダウン リストから [コロン（Colon）] を選択します。

関連項目

- WLC GUI 設定 :『*Cisco Wireless LAN Controller Configuration Guide, Release 7.2*』の「Using the GUI to Configure RADIUS」の項（第 6 章「Configuring Security Solutions」）。
- WLC CLI 設定 :『*Cisco Wireless LAN Controller Command Reference Guide, Release 7.2*』の config radius callStationIdType コマンド（第 2 章「Controller Commands」）。

SNMP クエリー プローブ

[ノードの編集（Edit Node）] ページの SNMP クエリー プローブの設定に加えて、次の場所で他の簡易管理プロトコルの設定を行う必要があります。[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）]。

[ネットワーク デバイス（Network Devices）] リスト ページで新しいネットワーク アクセス デバイス（NAD）の SNMP 設定を行うことができます。SNMP クエリー プローブまたはネットワーク アクセス デバイスの SNMP 設定で指定したポーリング間隔は、一定の間隔で NAD をクエリーします。

次の設定に基づいて、特定の NAD の SNMP クエリーをオンおよびオフにすることができます。

- [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- Cisco Discovery Protocol 情報に対して [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- SNMP クエリー タイマーをデフォルトでスイッチごとに 1 時間に 1 度

iDevice および SNMP をサポートしないその他のモバイル デバイスでは、ARP テーブルによって MAC アドレスを検出でき、SNMP クエリー プローブによってネットワーク アクセス デバイスからクエリーを実行できます。

関連項目

「プロファイリング ノードの設定」（P.A-5）

SNMP クエリーでの Cisco Discovery Protocol のサポート

ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスのすべてのポートで Cisco Discovery Protocol を有効（デフォルト）にする必要があります。ネットワーク デバイスのいずれかのポートで Cisco Discovery Protocol を無効にすると、接続されているすべてのエンドポイントの Cisco Discovery Protocol 情報が失われるため、正しくプロファイリングを実行できなくなる可能性があります。

ネットワーク デバイスで **cdp run** コマンドを使用して Cisco Discovery Protocol をグローバルに有効にし、ネットワーク アクセス デバイスのインターフェイスで **cdp enable** コマンドを使用して Cisco Discovery Protocol を有効にします。ネットワーク デバイスとインターフェイスで Cisco Discovery Protocol を無効にするには、コマンドの先頭に **no** キーワードを使用します。

SNMP クエリーでの Link Layer Discovery Protocol のサポート

Cisco ISE プロファイラでは、SNMP クエリーを使用して LLDP 属性を収集します。また、RADIUS プローブを使用して、ネットワーク デバイスに組み込まれている Cisco IOS センサーから LLDP 属性を収集することもできます。

表 21-3 に、ネットワーク アクセス デバイスで LLDP グローバル コンフィギュレーション コマンドと LLDP インターフェイス コンフィギュレーション コマンドを設定するために使用できるデフォルトの LLDP 設定を示します。

表 21-3　デフォルトの LLDP 設定

機能	機能
LLDP グローバル ステート	無効
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	有効（すべての TLV の送受信が可能）
LLDP インターフェイス ステート	有効
LLDP 受信	有効
LLDP 転送	有効
LLDP med-tlv-select	有効（すべての LLDP-MED TLV の送信が可能）

単一文字で表示される CDP および LLDP の機能コード

エンドポイントの属性リストには、lldpCacheCapabilities 属性と lldpCapabilitiesMapSupported 属性の 1 文字の値が表示されます。値は、CDP と LLDP を実行するネットワーク アクセス デバイスに対して表示される機能コードです。

例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

例 3

```
Switch#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
...
Switch#

Switch#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
...
Switch#
```

SNMP トラップ プローブ

SNMP トラップは、MAC 通知、linkup、linkdown、および informs をサポートする特定のネットワーク アクセス デバイスから情報を受信します。SNMP トラップ プローブは、ポートが起動するかダウンし、エンドポイントがネットワークから切断されるかネットワークに接続すると、特定のネットワーク アクセス デバイスから情報を受信します。その結果、Cisco ISE にエンドポイントを作成するのに十分でない情報を受信することになります。

SNMP トラップ プルーブを完全に機能させてにエンドポイントを作成する必要がある場合は、トラップの受信時に SNMP クエリー プローブによってネットワーク アクセス デバイスの特定のポートに対してポーリング イベントがトリガーされるように、SNMP クエリーも有効にする必要があります。この機能を完全に動作させるには、ネットワーク アクセス デバイスと SNMP トラップを設定する必要があります。

（注） Cisco ISE では、ワイヤレス LAN コントローラ（WLC）とアクセス ポイント（AP）から受信した SNMP トラップはサポートされません。

関連項目

「プロファイリング ノードの設定」（P.A-5）

Cisco ISE ノードごとのプローブの設定

次の形態でポリシー サービス ペルソナを担当する展開内の Cisco ISE ノードごとに、[プロファイリング設定（Profiling Configuration）] タブで 1 つ以上のプローブを設定できます。

- スタンドアロン ノード：デフォルトで管理、モニタリング、およびポリシー サービスのすべてのペルソナを担当する単一のノード上で Cisco ISE を展開している場合。
- マルチノード：展開内でポリシー サービス ペルソナを担当する複数のノードを登録している場合。

はじめる前に

管理ノードでのみ Cisco ISE ノードごとにプローブを設定でき、分散展開のセカンダリ管理ノードでは使用できません。

ステップ 1　[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。

ステップ 2　ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3　[展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4　[全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5　[プロファイリング サービスの有効化（Enable Profiling Services）] チェックボックスをオンにします。

ステップ 6　[プロファイリング設定（Profiling Configuration）] タブをクリックします。

ステップ 7　各プローブの値を設定します。

ステップ 8　[保存（Save）] をクリックしてプローブ設定を保存します。

関連項目

- 「プロファイリング ノードの設定」（P.A-5）

COA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定

Cisco ISE では、グローバル コンフィギュレーションが、[プロファイラ設定（Profiler Configuration）] ページで許可変更（CoA）を発行し、すで認証されているエンドポイントをプロファイリング サービスでより細かく制御できるようにします。

さらに、[プロファイラ設定（Profiler Configuration）] ページで、NMAP の手動ネットワーク スキャンにカンマで区切られた追加の SNMP read-only コミュニティ ストリングを設定できます。SNMP RO コミュニティ ストリングは、[現在のカスタム SNMP コミュニティ ストリング（Current custom SNMP community strings）] フィールドに表示されるのと同じ順序で使用されます。

[プロファイラ設定（Profiler Configuration）] ページでエンドポイント属性のフィルタリングも設定できます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] を選択します。

ステップ 2　CoA タイプを設定するには、次の設定のいずれかを選択します。

- [CoA なし（No CoA）]（デフォルト）：このオプションを使用して、CoA のグローバル コンフィギュレーションを無効にすることができます。この設定は、エンドポイント プロファイリング ポリシーごとに設定された CoA を上書きします。
- [ポート バウンス（Port Bounce）]：スイッチ ポートにセッションが 1 つしかない場合のみ、このオプションを使用できます。ポートに複数のセッションが存在する場合は、[再認証（Reauth）] オプションを使用します。
- [再認証（Reauth）]：このオプションを使用して、すでに認証されているエンドポイントをプロファイリング時に再認証します。

  1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス（Port Bounce）] オプションを設定しても、プロファイリング サービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。この機能を使用すると、他のセッションが切断されるという、[ポート バウンス（Port Bounce）] オプションで発生する可能性のある状況が回避されます。

ステップ 3　[カスタム SNMP コミュニティ ストリングの変更（Change custom SNMP community strings）] フィールドに NMAP の手動ネットワーク スキャンのカンマで区切られた新しい SNMP コミュニティ ストリング入力し、確認のために [カスタム SNMP コミュニティ ストリングの確認（Confirm custom SNMP community strings）] フィールドにそのストリングを再入力します。

ステップ 4　[エンドポイント属性フィルタ（Endpoint Attribute Filter）] チェックボックスをオンにし、エンドポイント属性のフィルタリングを有効にします。

ステップ 5　[保存（Save）] をクリックします。

関連項目

- 「NMAP の手動サブネット スキャンの SNMP read-only コミュニティ ストリング」（P.21-9）
- 「認証されたエンドポイントの許可変更のグローバル設定」（P.21-16）
- 「CoA 設定の各タイプに発行される認可変更」（P.21-18）
- 「ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定」（P.21-19）
- 「エンドポイント プロファイリング ポリシーごとの許可変更の設定」（P.21-24）

認証されたエンドポイントの許可変更のグローバル設定

デフォルトの [CoA なし（No CoA）] オプションを使用して認可変更（CoA）を無効にするか、ポート バウンスと再認証オプションを使用して CoA を有効にするグローバル コンフィギュレーション オプションを使用できます。Cisco ISE で CoA にポート バウンスを設定している場合は、「CoA 免除」の項で説明されているように、プロファイリング サービスは他の CoA を発行することがあります。

RADIUS プローブまたはモニタリング ペルソナの REST API を使用して、エンドポイントを認証できます。RADIUS プローブを有効にして、パフォーマンスを向上させることができます。CoA を有効にした場合は、高いパフォーマンスを得るために Cisco ISE アプリケーションで CoA 設定と合わせて RADIUS プローブを有効にすることを推奨します。これにより、プロファイリング サービスは収集された RADIUS 属性を使用して、エンドポイントに適切な CoA を発行できます。

Cisco ISE アプリケーションで RADIUS プローブを無効にした場合は、モニタリング ペルソナの REST API を使用して CoA を発行することができます。これにより、プロファイリング サービスで広範なエンドポイントをサポートできます。分散展開では、モニタリング ペルソナの REST API を使用して CoA を発行するために、ネットワークに少なくとも 1 つの Cisco ISE ノードが必要です。

Cisco ISE では、プライマリおよびセカンダリ モニタリング ノードは両方とも同じセッション ディレクトリ情報を持つため、分散展開での REST クエリーのデフォルトの宛先としてプライマリまたはセカンダリ モニタリング ノードのどちらかを任意に指定します。

関連項目

- 「許可変更を発行するための使用例」（P.21-16）

許可変更を発行するための使用例

次の場合に、プロファイリング サービスによって許可変更が発行されます。

- エンドポイントが削除された：エンドポイントが [エンドポイント（Endpoints）] ページから削除され、ネットワークから接続解除または削除された場合。
- 例外アクションが設定されている：エンドポイントから異常または許容できないイベントが発生する例外アクションがプロファイルごとに設定されている場合。プロファイリング サービスは、CoA を発行してエンドポイントを対応するスタティック プロファイルに移動します。
- エンドポイントが初めてプロファイリングされる：エンドポイントが静的に割り当てられておらず、初めてプロファイリングされる場合（たとえば、プロファイルが不明プロファイルから既知のプロファイルに変更された場合）。
- エンドポイント ID グループが変更された：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリング サービスは CoA を発行します。

  エンドポイント ID グループが変更され、エンドポイント ID グループが次のために許可ポリシーで使用されている場合、プロファイリング サービスは CoA を発行します。

  - 動的にプロファイリングされる場合のエンドポイントに対するエンドポイント ID グループの変更
  - ダイナミック エンドポイントに対してスタティック割り当てフラグが true に設定されている場合のエンドポイント ID グループの変更
- エンドポイント プロファイリングのポリシーが変更され、ポリシーが許可ポリシーで使用される：エンドポイント プロファイリング ポリシーが変更され、許可ポリシーで使用される論理的なプロファイルにそのポリシーが含まれる場合。エンドポイント プロファイリング ポリシーは、プロファイリング ポリシーの一致のため、または、エンドポイントが論理的なプロファイルに関連付

けられたエンドポイント プロファイリング ポリシーにスタティックに割り当てられるときに、変更される場合があります。両方の場合で、エンドポイント プロファイリング ポリシーが許可ポリシーで使用される場合のみ、プロファイリング サービスは CoA を発行します。

関連項目

「許可変更を発行するための免除」（P.21-17）.

許可変更を発行するための免除

エンドポイント ID グループが変更され、スタティック割り当てがすでに true の場合、プロファイリング サービスは CoA を発行しません。

Cisco ISE は次の理由で CoA を発行しません。

- ネットワークから切断されたエンドポイント：ネットワークから切断されているエンドポイントが検出された場合。
- 認証された有線（拡張認証プロトコル）EPA 対応エンドポイント：認証された有線 EAP 対応エンドポイントが検出された場合。
- 各ポートの複数のアクティブ セッション：1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス（Port Bounce）] オプションを設定しても、プロファイリング サービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。
- ワイヤレス エンドポイント検出時の切断パケット CoA（セッション終了）：エンドポイントがワイヤレスとして検出された場合、ポート バウンス CoA ではなく切断パケット CoA（セッション終了）が発行されます。この変更の利点は、ワイヤレス LAN コントローラ（WLC）CoA のサポートです。
- ゲスト デバイス登録フローを介して作成されたエンドポイント：エンドポイントがゲストのデバイス登録を介して作成された場合。CoA が Cisco ISE で全体的に有効になっていても、プロファイリング サービスは、デバイス登録フローに影響を与えないように CoA を発行しません。特に、PortBounce CoA グローバル コンフィギュレーションは、エンドポイントの接続フローを切断します。
- グローバル CoA なし設定によるポリシー CoA の上書き：エンドポイント プロファイリング ポリシーごとに設定された CoA に関係なく Cisco ISE で発行された CoA がないので、グローバル CoA なしはエンドポイント プロファイリング ポリシーのすべての設定を上書きします。

（注） [CoA なし（No CoA）] および [再認証（Reauth）] 設定は影響を受けず、プロファイラ サービスは同じ [CoA] 設定を有線エンドポイントとワイヤレス エンドポイントに適用します。

関連項目

表 21-4、「各 CoA 設定の許可変更」

CoA 設定の各タイプに発行される認可変更

表 21-4 は、Cisco ISE における CoA 設定のタイプごとに各種環境の CoA をまとめたものです。

表 21-4　各 CoA 設定の許可変更

シナリオ	CoA なし設定	ポート バウンス設定	再認証設定	その他の情報
Cisco ISE における CoA グローバル コンフィギュレーション（一般的な設定）	CoA なし	ポート バウンス	再認証	—
エンドポイントがネットワークで検出された場合	CoA なし	CoA なし	CoA なし	認可変更は、RADIUS 属性の Acct -Status -Type 値 Stop で判別されます。
同じスイッチ ポートで複数のアクティブ セッションと有線接続	CoA なし	再認証	再認証	再認証は、他のセッションの切断を回避します。
ワイヤレス エンドポイント	CoA なし	切断パケット CoA（セッション終了）	再認証	ワイヤレス LAN コントローラに対するサポート
不完全な CoA データ	CoA なし	CoA なし	CoA なし	原因は RADIUS 属性の欠落。

ISE データベースの持続性とパフォーマンスの属性フィルタ

Cisco ISE は、Dynamic Host Configuration Protocol（DHCP ヘルパーと DHCP SPAN の両方）、HTTP、RADIUS、および簡易ネットワーク管理プロトコル プローブ（パフォーマンスの低下に対処するために NetFlow を除く）のフィルタを実装します。各プローブ フィルタには、一時的でエンドポイント プロファイルとは関係のない属性のリストが含まれ、これらの属性はプローブによって収集された属性から削除されます。

isebootstrap ログ（isebootstrap-yyyymmdd-xxxxxx.log）には、ディクショナリの作成およびディクショナリからの属性のフィルタリングを処理するメッセージが含まれます。エンドポイントがフィルタリング フェーズを通過するときに、フィルタリングが行われたことを示すデバッグ メッセージをログに記録するように設定することもできます。

Cisco ISE プロファイラは次のエンドポイント属性フィルタを呼び出します。

- DHCP ヘルパーと DHCP SPAN の両方の DHCP フィルタには、不要なすべての属性が含まれ、これらの属性は DHCP パケットの解析後に削除されます。フィルタリング後の属性は、エンドポイントのエンドポイント キャッシュ内にある既存の属性とマージされます。
- HTTP フィルタは、HTTP パケットからの属性のフィルタリングに使用され、フィルタリング後の属性セットに大幅な変更はありません。
- RADIUS フィルタは、syslog 解析が完了すると使用され、エンドポイント属性がプロファイリングのためにエンドポイント キャッシュにマージされます。

- SNMP クエリーの SNMP フィルタには個別の CDP および LLDP フィルタが含まれ、すべて SNMP クエリー プローブに使用されます。

ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定

収集ポイントで頻繁に変更されないエンドポイント属性の数を削減することによって、持続的なイベントおよび複製イベントの数を減らすことができます。エンドポイント属性フィルタを有効にすると、Cisco ISE プロファイラは重要な属性のみ保持し、その他の属性をすべて廃棄するようになります。重要な属性とは、Cisco ISE システムで使用される属性、または特にエンドポイント プロファイリングのポリシーまたはルールで使用される属性です。

ホワイト リストは、エンドポイントのプロファイリングのためにカスタム エンドポイント プロファイリング ポリシーで使用され、許可変更（CoA）、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠の属性のセットです。ホワイトリストは、無効なときでさえ、エンドポイントの所有権の変更時（属性が複数のポリシー サービス ノードによって収集されるとき）に、常に基準として使用されます。

デフォルトでは、ホワイト リストは無効であり、属性フィルタが有効の場合にだけ属性がドロップされます。プロファイリング ポリシーに新しい属性を含めるためにフィードからを含めエンドポイント プロファイリング ポリシーが変更されるときに、ホワイトリストが動的に更新されます。ホワイト リストに存在しない属性は収集時にただちにドロップされ、その属性はエンドポイントのプロファイリングに参加できません。バッファリングと組み合わせた場合に、持続的なイベントの数を削減できます。

ホワイト リストに次の 2 つのソースから決定された一連の属性が含まれることを確認する必要があります。

- エンドポイントをプロファイルに一致できるようにデフォルト プロファイルで使用される属性のセット。
- 許可変更（CoA）、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）、デバイス登録 WebAuth（DRW）などが期待どおりに機能するために不可欠の属性のセットです。

表 21-5　　ホワイトリスト属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address

表 21-5　ホワイトリスト属性 （続き）

NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

スイッチに組み込まれた IOS センサーからの属性の収集

IOS センサーの統合によって、Cisco ISE ランタイムと Cisco ISE プロファイラでスイッチから送信された任意またはすべての属性を収集できるようになりました。RADIUS プロトコルを使用して、DHCP、CDP、および LLDP 属性をスイッチから直接収集できます。DHCP、CDP、および LLDP について収集された属性は、解析され、次の場所のプロファイラ ディクショナリの属性にマッピングされます。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]。

関連項目

『Cisco Identity Services Engine Network Component Compatibility, Release 1.2』

ネットワーク アクセス デバイスに組み込まれた IOS センサー

ネットワーク アクセス デバイスに組み込まれた IOS センサーと Cisco ISE の統合には次のコンポーネントが含まれます。

- IOS センサー
- DHCP、CDP および LLDP のデータを収集するためにネットワーク アクセス デバイス（スイッチ）に組み込まれたデータ コレクタ
- データを処理し、エンドポイントのデバイス タイプを決定するためのアナライザ

  アナライザを展開するには次の 2 つの方法がありますが、2 つを組み合わせて使用することは想定されていません。

- アナライザを Cisco ISE に展開する
- アナライザをセンサーとしてスイッチに組み込む

IOS センサー対応ネットワーク アクセス デバイスの設定チェックリスト

この項では、スイッチから直接 DHCP、CDP、および LLDP の属性を収集するために、IOS センサー対応スイッチと Cisco ISE で設定する必要のある作業のリストの概要を説明します。

- RADIUS プローブが Cisco ISE で有効になっていることを確認します。
- ネットワーク アクセス デバイスで DHCP、CDP、および LLDP 情報を収集するための IOS センサーがサポートされていることを確認します。
- ネットワーク アクセス デバイスで、エンドポイントから CDP 情報と LLDP 情報を取得するために次の CDP コマンドと LLDP コマンドが実行されていることを確認します。

```
cdp enable
lldp run
```

- 標準の AAA コマンドと RADIUS コマンドを使用して、セッション アカウンティングが個別に有効になっていることを確認します。

  コマンドの使用例を示します。

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS センサー固有のコマンドを実行していることを確認します。
  - アカウンティング拡張の有効化

    ネットワーク アクセス デバイスで IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加したり、新しいセンサー プロトコル データの検出時に追加のアカウンティング イベントを生成したりできるようにする必要があります。つまり、RADIUS アカウンティング メッセージには、すべての CDP、LLDP、および DHCP 属性が含まれている必要があります。

    次のグローバル コマンドを入力します。

    device-sensor accounting
  - アカウンティング拡張の無効化

    （アカウンティング機能がグローバルに有効になっている場合、）（アカウンティング）ネットワーク アクセス デバイスで、特定のポートでホストされているセッションについて IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加できないようにするには、適切なポートで次のコマンドを入力します。

    no device-sensor accounting
  - TLV 変更のトラッキング

    デフォルトでは、サポートされている各ピア プロトコルで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るのは、特定のセッションのコンテキストで前に受信したことのないタイプ、長さ、値（TLV）が着信パケットに含まれている場合だけです。

    新しい TLV が存在するか、または前に受信した TLV の値が異なる場合は、すべての TLV 変更に対するクライアント通知とアカウンティング イベントを有効にする必要があります。次のコマンドを入力します。

    device-sensor notify all-changes
- ネットワーク アクセス デバイスで IOS Device Classifier（ローカル アナライザ）が無効になっていることを確認します。

次のコマンドを入力します。

```
no macro auto monitor
```

（注）　このコマンドにより、ネットワーク アクセス デバイスは変更ごとに 2 つの同じ RADIUS アカウンティング メッセージを送信できなくなります。

エンドポイント プロファイリング ポリシー ルール

ルールを定義すると、以前作成し、ポリシー要素ライブラリに保存したライブラリから 1 つ以上のプロファイリング条件を選択し、確実度係数の整数値を各条件に関連付けるか、または例外アクションまたはネットワーク スキャン アクションをその条件に関連付けることができます。例外アクションまたはネットワーク スキャン アクションは、Cisco ISE がエンドポイントの分類全体に関するプロファイリング ポリシーを評価しているときに、設定可能なアクションをトリガーするために使用します。

特定のポリシー内のルールが、個別に、OR 演算子を使用して評価されると、各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。エンドポイント プロファイリング ポリシーのルールが一致した場合、プロファイリング ポリシーおよび一致するポリシーは、ネットワーク上で動的に検出されるときにエンドポイントで同じです。

ルール内で論理的にグループ化される条件

エンドポイント プロファイリング ポリシー（プロファイル）には、単一の条件、または AND 演算子や OR 演算子を使用して論理的に結合された複数の単一条件の組み合わせを含めることができます。これらの条件と照合してポリシー内の特定のルールに対してエンドポイントのチェック、分類、およびグループ化を行うことができます。

条件は、収集されたエンドポイント属性値をエンドポイントの条件に指定されている値と照合するために使用されます。複数の属性をマッピングする場合は、条件を論理的にグループ化して、ネットワーク上のエンドポイントの分類に使用できます。ルールで対応する確実度メトリック（定義済みの整数値）が関連付けられている 1 つ以上の条件とエンドポイントを照合するか、または、条件に関連付けられた例外アクション、または条件に関連付けられたネットワーク スキャン アクションをトリガーすることができます。

エンドポイント プロファイリング ポリシーを Cisco ISE 1.1.x から Cisco ISE 1.2 にインポートする場合、ポリシーをインポートする前にエクスポートされた profilier_policies.xml の条件名を変更する必要があります。

確実度係数

プロファイリング ポリシーの最小の確実度メトリックで、エンドポイントの一致するプロファイルを評価します。エンドポイント プロファイリング ポリシーの各ルールは、最小の確実度メトリック（整数値）がプロファイリング条件に関連付けられています。確実度メトリックは、エンドポイント プロファイリング ポリシーのすべての有効なルールに対して追加される尺度であり、それにより、エンドポイント プロファイリング ポリシー内の各条件がエンドポイントの全体的な分類の向上にどの程度役立っているかがわかります。

各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。すべての有効なルールの確実度メトリックが合計され、照合の確実度が求められます。この値は、エンドポイント プロファイリング ポリシーに定義されている最小の確実度係数を超えている必要があります。デフォルトでは、すべての新しいプロファイリング ポリシー ルールおよび事前に定義されたプロファイリング ポリシーの最小の確実度係数は 10 です。

エンドポイント プロファイリング ポリシーの作成

[プロファイリング ポリシー（Profiling Policies）] ページを使用して、Cisco ISE の管理者として作成したエンドポイント プロファイリング ポリシー、および導入時に Cisco ISE によって提供されたエンドポイント プロファイリング ポリシーも管理することができます。

[新規プロファイラ ポリシー（New Profiler Policy）] ページの次のオプションを使用して、新しいプロファイリング ポリシーを作成してエンドポイントをプロファイリングできます。

- ポリシー有効（Policy Enabled）
- 一致するエンドポイント ID グループを作成するか、またはエンドポイント ID グループ階層を使用するために、ポリシーの ID グループを作成します。
- 親ポリシー（Parent Policy）
- 関連 CoA タイプ

（注）　[プロファイリング ポリシー（Profiling Policies）] ページでエンドポイント ポリシーを作成する場合は、Web ブラウザの停止ボタンを使用しないでください。この操作で、次のようになります。[新規プロファイラ ポリシー（New Profiler Policy）] ページのロードが中止され、他のリスト ページおよびそのリスト ページ内のメニュー（アクセスした場合）がロードされ、リスト ページ内の [フィルタ（Filter）] メニュー以外のすべてのメニューに対する操作を実行できなくなります。リスト ページ内ですべてのメニューの操作を実行するには、Cisco ISE からログアウトし、再度ログインする必要があります。

似た特性を持つプロファイリング ポリシーを作成するには、エンドポイント プロファイリングのポリシーを複製し、それにより、すべての条件を定義して新しいプロファイリング ポリシーを作成する代わりに、既存のプロファイリング ポリシーを変更できます。

ステップ 1　[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　作成する新しいエンドポイント ポリシーの名前と説明を入力します。エンドポイントをプロファイリングする際検証に使用するエンドポイント プロファイリング ポリシーを含めるために、[ポリシー有効（Policy Enabled）] チェックボックスは、デフォルトでオンになっています。

ステップ 4　有効範囲 1 ～ 65535 の最小の確実度係数の値を入力します。

ステップ 5　[例外アクション（Exception Actions）] ドロップダウン リストの横にある矢印をクリックして例外アクションを関連付けるか、または [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）] ドロップダウン リストの横にある矢印をクリックしてネットワーク スキャン アクションを関連付けます。

ステップ 6　[ポリシーの ID グループの作成（Create an Identity Group for the policy）] で次のいずれかのオプションを選択します。

- **はい、一致する ID グループを作成します（Yes, create matching Identity Group）**
- **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**

ステップ 7　[親ポリシー（Parent Policy）] ドロップダウン リストの隣にある矢印をクリックして、親ポリシーを新しいエンドポイント ポリシーに関連付けます。

ステップ 8　[関連 CoA タイプ（Associated CoA Type）] ドロップダウン リストで、関連付ける CoA タイプを選択します。

ステップ 9　条件を追加するルールをクリックし、各条件の確実度係数の整数値を関連付けるか、エンドポイントの全体の分類のためにその条件の例外アクションまたはネットワーク スキャン アクションを関連付けます。

ステップ 10　[送信（Submit）] をクリックしてエンドポイント ポリシーを追加するか、または [新規プロファイラ ポリシー（New Profiler Policy）] ページで [プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックして、[プロファイリング ポリシー（Profiling Policies）] ページに戻ります。

関連項目

- 「エンドポイント プロファイリング ポリシーの設定」（P.B-5）
- 「事前定義されたエンドポイント プロファイリング ポリシー」（P.21-26）
- 「例外アクションの作成」（P.21-31）
- 「ネットワーク スキャン アクションの作成」（P.21-32）

エンドポイント プロファイリング ポリシーごとの許可変更の設定

Cisco ISE の許可変更（CoA）タイプのグローバル コンフィギュレーションに加えて、各エンドポイント プロファイリング ポリシーに関連付けられた特定のタイプの CoA も発行するように設定できます。

グローバル CoA なしタイプの設定は、エンドポイント プロファイリング ポリシーで設定された各 CoA タイプを上書きします。グローバル CoA タイプが CoA なしタイプ以外に設定されている場合、各エンドポイント プロファイリング ポリシーはグローバル CoA の設定を上書きできます。

CoA がトリガーされると、各エンドポイント プロファイリング ポリシーは、次のように実際の CoA タイプを決定できます。

- 全般設定：これは、グローバル コンフィギュレーションごとに CoA を発行するすべてのエンドポイント プロファイリング ポリシーのデフォルトの設定です。
- CoA なし：この設定はグローバル コンフィギュレーションを上書きし、そのプロファイルの CoA を無効にします。
- ポート バウンス：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、ポート バウンス CoA を発行します。
- 再認証：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、再認証 CoA を排出します。

（注）　プロファイラ グローバル CoA 設定がポート バウンス（または再認証）に設定されている場合は、モバイル デバイスの個人所有デバイス持ち込み（BYOD）フローが切断されないように、対応するエンドポイント プロファイリング ポリシーを [CoA なし（No CoA）]、[ポリシーごとの CoA（per-policy CoA）] オプションを指定して設定していることを確認します。

表 21-6 では、グローバルおよびエンドポイント プロファイリング ポリシー設定に基づいて各場合に発行されたすべての CoA タイプと実際の CoA タイプが組み合わされた設定について説明します。

表 21-6　設定のさまざまな組み合わせに発行された CoA タイプ

グローバル CoA タイプ	ポリシーごとにセットされたデフォルトの CoA タイプ	ポリシーごとの CoA なしタイプ	ポリシーごとのポート バウンス タイプ	ポリシーごとの再認証タイプ
CoA なし	CoA なし	CoA なし	CoA なし	CoA なし
ポート バウンス	ポート バウンス	CoA なし	ポート バウンス	再認証
再認証	再認証	CoA なし	ポート バウンス	再認証

エンドポイント プロファイリング ポリシーのインポート

エクスポート機能で作成できるのと同じ形式を使用して、XML ファイルからエンドポイント プロファイリング ポリシーをインポートできます。親ポリシーが関連付けられている、新しく作成されたプロファイリング ポリシーをインポートする場合は、子ポリシーを定義する前に親ポリシーを定義する必要があります。

インポート ファイルでは、エンドポイント プロファイリング ポリシーの階層構造が含まれ、最初に親ポリシー、次にポリシーに定義されているルールとチェックとともにインポートしたプロファイルが含まれます。

ステップ 1　[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）] を選択します。

ステップ 2　[インポート（Import）] をクリックします。

ステップ 3　[参照（Browse）] をクリックして、前にエクスポートしてこれからインポートするファイルを特定します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　[プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックすると、[プロファイリング ポリシー（Profiling Policies）] ページに戻ります。

関連項目

「事前定義されたエンドポイント プロファイリング ポリシー」（P.21-26）

エンドポイント プロファイリング ポリシーのエクスポート

エンドポイント プロファイリング ポリシーを他の Cisco ISE 展開にエクスポートできます。または、独自のポリシーを作成するためのテンプレートとして XML ファイル使用してインポートできます。ファイルをシステムのデフォルトの場所にダウンロードして、後でインポートに使用することもできます。

エンドポイント プロファイリング ポリシーをエクスポートするときにダイアログが表示され、profiler_policies.xml を適切なアプリケーションで開くか保存するように求められます。これは XML 形式のファイルで、Web ブラウザまたは他の適切なアプリケーションで開くことができます。

ステップ 1　[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）] を選択します。

ステップ 2　[エクスポート（Export）] を選択し、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [プロファイリング ポリシー（Profiling Policies）] ページで選択したエンドポイント プロファイリング ポリシーだけをエクスポートできます。
- [選択済みおよびエンドポイントをエクスポート（Export Selected with Endpoints）] : 選択したエンドポイント プロファイリング ポリシー、および選択したエンドポイント プロファイリング ポリシーでプロファイルされたエンドポイントをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトでは、[プロファイリング ポリシー（Profiling Policies）] ページのすべてのプロファイリング ポリシーをエクスポートできます。

ステップ 3　[OK] をクリックして、エンドポイント プロファイリング ポリシーを profiler_policies.xml ファイルにエクスポートします。

関連項目

「事前定義されたエンドポイント プロファイリング ポリシー」（P.21-26）

事前定義されたエンドポイント プロファイリング ポリシー

Cisco ISE には Cisco ISE が展開されたときに事前定義されたデフォルトのプロファイリング ポリシーが含まれ、その階層構造により、ネットワーク上で識別されたエンドポイントを分類し、一致するエンドポイント ID グループに割り当てることができます。エンドポイント プロファイリング ポリシーは階層構造になっているため、[プロファイリング ポリシー（Profiling Policies）] ページには、デバイスの一般的な（親）ポリシーおよび [プロファイリング ポリシー（Profiling Policies）] リスト ページで親ポリシーが関連付けられている子ポリシーのリストが表示されます。

[プロファイリング ポリシー（Profiling Policies）] ページには、エンドポイント プロファイリング ポリシーとともに、その名前、タイプ、説明、およびステータス（検証が有効になっているかどうか）が表示されます。

エンドポイント プロファイリング ポリシー タイプは次のように分類されます。

- シスコ提供 : Cisco ISE で事前定義されたエンドポイント プロファイリング ポリシーはシスコ提供タイプとして識別されます。
- 管理者による変更 : 事前定義されたエンドポイント プロファイリング ポリシーを変更したときに、エンドポイント プロファイリング ポリシーは管理者による変更タイプとして識別されます。Cisco ISE では、事前定義されたエンドポイント プロファイリング ポリシーに行った変更がアップグレード時に上書きされます。

  管理者によって変更されたポリシーは削除できますが、Cisco ISE によりシスコ提供のポリシーの最新バージョンで置き換えられます。
- 管理者作成 : 作成したエンドポイント プロファイリング ポリシー、またはシスコ提供のエンドポイント プロファイリング ポリシーを複製したときのエンドポイント プロファイリング ポリシーは、管理者作成タイプとして識別されます。

一連のエンドポイントの一般的なポリシー（親）を作成して、その子がルールと条件を継承できるようにすることを推奨します。エンドポイントを分類する必要がある場合は、エンドポイントをプロファイリングするときに、まずエンドポイント プロファイルを親ポリシーと、次にその子孫（子）ポリシーと照合する必要があります。

たとえば、Cisco-Device は、すべてのシスコ デバイスの一般的なエンドポイント プロファイリングのポリシーであり、シスコ デバイスの他のポリシーは、Cisco-Device の子です。たとえば、エンドポイントを Cisco-IP-Phone 7960 として分類する必要がある場合は、まずこのエンドポイントのエンドポイント プロファイルを親の Cisco-Device ポリシー、その子の Cisco-IP-Phone ポリシーと照合する必要があり、その後さらに分類するために Cisco-IP-Phone 7960 プロファイリング ポリシーと照合します。

アップグレード中に上書きされる事前定義済みエンドポイント プロファイリング ポリシー

[プロファイリング ポリシー（Profiling Policies）] ページで既存のエンドポイント プロファイリング ポリシーを編集できます。事前定義されたエンドポイント プロファイリング ポリシーを変更する場合、事前定義されたエンドポイント プロファイルのコピーにすべての設定を保存する必要があります。

アップグレード時に、事前定義されたエンドポイント プロファイルに保存した設定が上書きされます。

エンドポイント プロファイリング ポリシーを削除できない

[プロファイリング ポリシー（Profiling Policies）] ページで選択したエンドポイント プロファイリング ポリシーまたはすべてのエンドポイント プロファイリング ポリシーを削除できます。デフォルトでは、[プロファイリング ポリシー（Profiling Policies）] ページからすべてのエンドポイント プロファイリング ポリシーを削除できます。[プロファイリング ポリシー（Profiling Policies）] ページですべてのエンドポイント プロファイリング ポリシーを選択し、削除しようとした場合、エンドポイント プロファイリング ポリシーが他のエンドポイント プロファイリングポリシーにマッピングされている親ポリシーか、または許可ポリシーにマッピングされている親ポリシーであり、他のエンドポイント プロファイリング ポリシーの親ポリシーであるとき、その一部が削除されない場合があります。

次に例を示します。

1. シスコ提供のエンドポイント プロファイリング ポリシーは削除できません。

1. エンドポイント プロファイルが他のエンドポイント プロファイルの親として定義されている場合は、[プロファイリング ポリシー（Profiling Policies）] ページで親プロファイルを削除できません。たとえば、Cisco-Device は、シスコ デバイスの他のエンドポイント プロファイリング ポリシーの親です。

2. 許可ポリシーにマッピングされているエンドポイント プロファイルは削除できません。たとえば、Cisco-IP-Phone は Profiled Cisco IP Phones 許可ポリシーにマッピングされ、Cisco IP Phone の他のエンドポイント プロファイリング ポリシーの親です。

Draeger 医療機器用の事前定義済みプロファイリング ポリシー

Cisco ISE には、デフォルトのエンドポイント プロファイリング ポリシーがあります。これには、Draeger 医療機器の一般的なポリシー、Draeger-Delta 医療機器のポリシー、および Draeger-M300 医療機器のポリシーが含まれます。両方の医療機器はポート 2050 と 2150 を共有するため、デフォルトの Draeger エンドポイント プロファイリング ポリシーを使用しても、Draeger-Delta 医療機器と Draeger-M300 医療機器を分類できません。

使用中の環境では、これらの Draeger デバイスはポート 2050 と 2150 を共有するため、デフォルトの Draeger-Delta and Draeger-M300 エンドポイント プロファイリング ポリシーでデバイスの宛先 IP アドレスのチェックに加えて、これらの医療機器を区別するためのルールを追加する必要があります。

Cisco ISE には、Draeger 医療機器のエンドポイント プロファイリング ポリシーで使用される次のプロファイリング条件があります。

- ポート 2000 が含まれる Draeger-Delta-PortCheck1
- ポート 2050 が含まれる Draeger-Delta-PortCheck2
- ポート 2100 が含まれる Draeger-Delta-PortCheck3
- ポート 2150 が含まれる Draeger-Delta-PortCheck4
- ポート 1950 が含まれる Draeger-M300PortCheck1
- ポート 2050 が含まれる Draeger-M300PortCheck2
- ポート 2150 が含まれる Draeger-M300PortCheck3

不明なエンドポイントのエンドポイント プロファイリング ポリシー

既存のプロファイルに一致せず、Cisco ISE でプロファイリングできないエンドポイントは、不明なエンドポイントです。不明プロファイルは、エンドポイントに割り当てられるデフォルトのシステム プロファイリング ポリシーで、そのエンドポイントについて収集された属性は Cisco ISE の既存のプロファイルと一致しません。

不明プロファイルは次のシナリオで割り当てられます。

- エンドポイントが Cisco ISE で動的に検出され、そのエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。
- エンドポイントが Cisco ISE で静的に追加され、静的に追加されたエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。

  ネットワークにエンドポイントを静的に追加した場合、そのエンドポイントは Cisco ISE のプロファイリング サービスによってプロファイリングされません。後に不明プロファイルを適切なプロファイルに変更することができ、Cisco ISE は割り当てたプロファイリング ポリシーを再割り当てしません。

静的に追加されたエンドポイントのエンドポイント プロファイリング ポリシー

静的に追加されたエンドポイントをプロファイリングするために、プロファイリング サービスは、新しい MATCHEDPROFILE 属性をエンドポイントに追加することによって、エンドポイントのプロファイルを計算します。計算されたプロファイルは、そのエンドポイントが動的にプロファイリングされるときのエンドポイントの実際のプロファイルです。これにより、静的に追加されたエンドポイントの計算されたプロファイルと動的にプロファイリングされたエンドポイントに一致するプロファイルの間の不一致を見つけることができます。

スタティック IP デバイスのエンドポイント プロファイリング ポリシー

静的に割り当てられた IP アドレスを持つエンドポイントがある場合、そのスタティック IP デバイスのプロファイルを作成できます。

スタティック IP アドレスが割り当てられているエンドポイントをプロファイリングするには、RADIUS プローブまたは SNMP クエリー プローブと SNMP トラップ プローブを有効にする必要があります。

エンドポイント プロファイリング ポリシーの一致

Cisco ISE では、エンドポイントに選択されたポリシーが考慮されます。これは、1 つ以上のルールに定義されているプロファイリング条件がプロファイリング ポリシーで満たされたときに評価されるポリシーではなく一致するポリシーです。ここで、そのエンドポイントのスタティック割り当てのステータスがシステムで false に設定されます。ただし、エンドポイントの編集時にスタティック割り当て機能を使用して、システム内の既存のプロファイリング ポリシーに静的に再割り当てした後は、true に設定されることがあります。

次は、エンドポイントの一致したポリシーに適用されます。

- 静的に割り当てられたエンドポイントの場合、プロファイリング サービスは MATCHEDPROFILE を計算します。
- 動的に割り当てられたエンドポイントの場合、MATCHEDPROFILE は一致するエンドポイント プロファイルと同じです。

プロファイリング ポリシーに定義された 1 つ以上のルールを使用して動的なエンドポイントに一致するプロファイリング ポリシーを決定し、エンドポイント ID グループを適切に割り当てて分類することができます。

エンドポイントが既存のポリシーにマッピングされる場合、プロファイリング サービスは、ポリシーの一致するグループを持つ最も近い親プロファイルをプロファイリング ポリシーの階層で検索し、エンドポイントを適切なエンドポイント ポリシーに割り当てます。

許可に使用されるエンドポイント プロファイリング ポリシー

許可ルールでエンドポイント プロファイリングを使用でき、そこに、エンドポイント プロファイリング ポリシーのチェックを属性として含む新しい条件を作成することができます。その属性値には、エンドポイント プロファイリング ポリシーの名前を使用します。次の属性を含むエンドポイント ディクショナリからエンドポイント プロファイリング ポリシーを選択できます。PostureApplicable、EndPointPolicy、LogicalProfile および BYODRegistration。

EndPointPolicy、BYODRegistration、および ID グループの組み合わせを含む許可ルールを定義できます。

論理プロファイルにグループ化されるエンドポイント プロファイリング ポリシー

論理プロファイルは、エンドポイント プロファイリング ポリシーがシスコ提供か、または管理者作成かに関係なく、プロファイルまたは関連付けられているプロファイルのカテゴリのコンテナです。エンドポイント プロファイリング ポリシーは、複数の論理プロファイルに関連付けることができます。

認可ポリシー条件で論理プロファイルを使用して、プロファイルのカテゴリでネットワーク全体のアクセス ポリシーの作成に役立でることができます。許可の単純条件を作成し、許可ルールに含めることができます。許可条件で使用できる属性と値のペアは、論理プロファイル（属性）および論理プロファイル（値）の名前であり、エンドポイント システム ディクショナリ内にあります。

たとえば、カテゴリに一致するエンドポイント プロファイリング ポリシーを論理プロファイルに割り当てることによって、Android、Apple iPhone、または Blackberry などのすべてのモバイル デバイスの論理プロファイルを作成できます。Cisco ISE には、すべての IP フォンのデフォルトの論理プロファイルである IP-Phone が含まれ、IP-Phone には IP-Phone、Cisco-IP-Phone、Nortel-IP-Phone-2000-Series、および Avaya-IP-Phone プロファイルが含まれます。

関連項目

「論理プロファイルの作成」（P.21-30）

論理プロファイルの作成

エンドポイント プロファイリング ポリシーのカテゴリをグループ化するために使用できる論理プロファイルを作成でき、それにより、プロファイルまたは関連付けられているプロファイルのカテゴリ全体を作成できます。エンドポイント プロファイリング ポリシーを割り当てられたセットから削除して、使用可能なセットに戻すこともできます。

ステップ 1　[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling）] > [論理プロファイル（Logical Profiles）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　[名前（Name）] と [説明（Description）] のテキスト ボックスに新しい論理プロファイルの名前と説明を入力します。

ステップ 4　[使用可能なポリシー（Available Policies）] からエンドポイント プロファイリング ポリシーを選択して、論理プロファイルに割り当てます。

ステップ 5　右矢印をクリックして、選択したエンドポイント プロファイリング ポリシーを [割り当てられたポリシー（Assigned Policies）] 移動します。

ステップ 6　[送信（Submit）] をクリックします。

関連項目

「例外アクションの作成」（P.21-31）

プロファイリング例外アクション

例外アクションは、エンドポイント プロファイリング ポリシーで参照できる単一の設定可能なアクションであり、アクションに関連付けられている例外条件が満たされるとトリガーされます。

例外アクションは次のいずれかのタイプになります。

- シスコ提供：シスコ提供の例外アクションは削除できません。Cisco ISE では、Cisco ISE のエンドポイントをプロファイリングするときに、次の編集不能なプロファイリング例外アクションがトリガーされます。
  - 許可変更：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリング サービスは許可変更を発行します。
  - エンドポイント削除：エンドポイントが [エンドポイント（Endpoints）] ページでシステムから削除されるか、Cisco ISE ネットワーク上で編集ページから不明プロファイルに再割り当てされると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
  - FirstTimeProfiled：エンドポイントが Cisco ISE で初めてプロファイリングされ、そのエンドポイントのプロファイルが不明プロファイルから既存のプロファイルに変更されて、そのエンドポイントが Cisco ISE ネットワーク上で認証に失敗すると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
- 管理者作成：Cisco ISE では、作成したプロファイリング例外アクションがトリガーされます。

関連項目：

- 「事前定義されたエンドポイント プロファイリング ポリシー」（P.21-26）
- 「例外アクションの作成」（P.21-31）

例外アクションの作成

1 つ以上の例外ルールを定義し、1 つのプロファイリング ポリシーに関連付けることができます。この関連付けにより、Cisco ISE でエンドポイントをプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つの例外ルールが一致する場合、例外アクション（単一の設定可能なアクション）がトリガーされます。

ステップ 1　[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 Actions）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　[名前（Name）] と [説明（Description）] のテキスト ボックスに例外アクションの名前と説明を入力します。

ステップ 4　[CoA アクション（CoA Action）] チェックボックスをオンにします。

ステップ 5　[ポリシー割り当て（Policy Assignment）] ドロップダウン リストをクリックしてエンドポイント ポリシーを選択します。

ステップ 6　[送信（Submit）] をクリックします。

関連項目

「プロファイリング例外アクションの設定」（P.B-27）

プロファイリング ネットワーク スキャン アクション

エンドポイント スキャン アクションは、エンドポイント プロファイリング ポリシーで参照できる設定可能なアクションであり、ネットワーク スキャン アクションに関連付けられている条件が満たされるとトリガーされます。

Cisco ISE システムにおけるリソース使用量を制限するために、エンドポイントをスキャンする場合はエンドポイント スキャンが使用されます。ネットワーク スキャン アクションでは、リソースを大量に消費するネットワーク スキャンとは異なり、1 つのエンドポイントをスキャンします。これにより、エンドポイントの全体的な分類が向上し、エンドポイントのエンドポイント プロファイルが再定義されます。エンドポイント スキャンは、1 度に 1 つずつしか処理できません。

1 つのネットワーク スキャン アクションをエンドポイント プロファイリング ポリシーに関連付けることができます。Cisco ISE には、ネットワーク スキャン アクションに 3 つの走査方式が事前定義されています。たとえば、OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scan といった 3 つの走査方式のいずれか、またはすべての含めることができます。OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scanOS スキャンを編集または削除できません。これらは、Cisco ISE の事前定義済みネットワーク スキャン アクションです。独自の新しいネットワーク スキャン アクションを作成することもできます。

エンドポイントを適切にプロファイリングしたら、設定済みのネットワーク スキャン アクションをエンドポイントに対して使用できません。たとえば、Apple-Device をスキャンすると、スキャンされたエンドポイントを Apple デバイスに分類できます。OS-scan によってエンドポイントで実行されているオペレーティング システムが特定されたら、Apple-Device プロファイルに一致しなくなりますが、Apple デバイスの適切なプロファイルに一致します。

関連項目

- 「事前定義されたエンドポイント プロファイリング ポリシー」（P.21-26）
- 「ネットワーク スキャン アクションの作成」（P.21-32）

ネットワーク スキャン アクションの作成

エンドポイント プロファイリング ポリシーに関連付けられたネットワーク スキャン アクションでは、エンドポイントのオペレーティング システム、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ポート、および一般ポートがスキャンされます。

1 つ以上のネットワーク スキャン ルールを定義し、エンドポイント プロファイリング ポリシーに関連付けることができます。各ネットワーク スキャン アクションのスキャン タイプを定義することもできます。この関連付けにより、Cisco ISE でエンドポイントをプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つのネットワーク スキャン ルールが一致する場合、ネットワーク スキャン アクションがトリガーされます。

はじめる前に

ルールで定義したネットワーク スキャン アクションをトリガーするには、ネットワーク スキャン（NMAP）プローブが有効になっていることを確認する必要があります。

ステップ 1　[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）] > [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　[追加（Add）] をクリックします。

ステップ 3　作成するネットワーク スキャン アクションの名前と説明を入力します。

ステップ 4　次のエンドポイントをスキャンする場合、1 つ以上のチェックボックスをオンにします。

- [OS のスキャン（Scan OS）]：オペレーティング システムをスキャンします
- [SNMP ポートのスキャン（Scan SNMP Port）]：SNMP ポート（161、162）をスキャンします
- [一般ポートのスキャン（Scan Common Port）]：一般ポートをスキャンします

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「オペレーティング システムのスキャン」（P.21-33）
- 「SNMP ポート スキャン」（P.21-33）
- 「一般ポート スキャン」（P.21-34）
- 「一般ポート」（P.21-34）

オペレーティング システムのスキャン

オペレーティング システムスキャン（OS-scan）タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされます。これはリソースを大量に使用するスキャンです。

OS-scan に使用する NMAP ツールの制限のため、エンドポイントのオペレーティング システムのスキャンの結果が信頼できなくなる可能性があります。たとえば、スイッチやルータなどのネットワークデバイスのオペレーティング システムをスキャンすると、NMAP OS-scan から、それらのデバイスについて正しくない operating-system 属性が返されることがあります。Cisco ISE は、精度が 100% ではない場合、オペレーティング システムの属性を表示します。

これらのデバイスについては、ルールで NMAP:operating-system 属性を使用するエンドポイント プロファイリング ポリシーに低い確実度値の条件（確実度係数の値）を設定できます。
NMAP:operating-system 属性に基づいてエンドポイント プロファイリング ポリシーを作成ときに必ず、プロファイリング ポリシーには AND 条件を含める必要があります。たとえば、
NMAP:operating-system には 100 が含まれます。

（注） 精度が 100% でなければ、NMAP:operating-system 属性に基づいてエンドポイント プロファイリング ポリシーを作成しないでください。

[OS のスキャン（Scan OS）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドはオペレーティング システムをスキャンします。

nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>

表 21-7　エンドポイントの OS スキャンの NMAP コマンド

-sS	TCP SYN スキャン。SYN スキャンがデフォルトです。
-O	OS 検出を有効にします。
-F	（高速（限定ポート）スキャン）。デフォルトよりも少ないポートをスキャンするように指定します。通常、Nmap では、スキャン対象のプロトコルごとに最も一般的な 1000 個のポートをスキャンします。-F を指定すると、これが 100 個に減少します。
oN	通常の出力。
oX	XML 出力。
IP-address	スキャン対象のエンドポイントの IP アドレス。

SNMP ポート スキャン

SNMPPortsAndOS-scan タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされ、SNMP ポート（161 と 162）が開いている場合は SNMP クエリーがトリガーされます。さらに分類するために、識別されて不明プロファイルと最初に一致したエンドポイントに使用できます。

[SNMP ポートのスキャン（Scan SNMP Port）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドは SNMP ポート（UDP 161 と 162）をスキャンします。

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 21-8　エンドポイントの SNMP ポート スキャンの NMAP コマンド

-sU	UDP スキャン。
-p <port-ranges>	指定されたポートのみをスキャンします。たとえば、UDP ポート 161 と 16.2 をスキャンします
oN	通常の出力。
oX	XML 出力。
IP-address	スキャン対象のエンドポイントの IP アドレス。

一般ポート スキャン

CommanPortsAndOS-scan タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされ、SNMP ポートではなく一般ポート（TCP と UDP）もスキャンされます。

[一般ポートのスキャン（Scan Common Port）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドは一般ポートをスキャンします。

nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

表 21-9　エンドポイントの一般ポート スキャンの NMAP コマンド

-sTU	TCP 接続スキャンと UDP スキャンの両方。
-p <port ranges>	TCP ポート 21、22、23、25、53、80、110、135、139、143、443、445、3306、3389、8080 および UDP ポート 53、67、68、123、135、137、138、139、161、445、500、520、631、1434、1900 をスキャンします。
oN	通常の出力。
oX	XML 出力。
IP address	スキャン対象のエンドポイントの IP アドレス。

一般ポート

次の表に、NMAP でスキャンに使用される 30 個の一般ポート（15 個の TCP ポートと 15 個の UDP ポート）を示します。

表 21-10　一般ポート

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	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns

表 21-10　一般ポート （続き）

TCP ポート		UDP ポート	
ポート	サービス	ポート	サービス
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	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

Cisco ISE と Cisco NAC アプライアンスの統合

Cisco ISE は、Cisco Network Admission Control（NAC）アプライアンス リリース 4.9 との統合のみサポートし、Cisco ISE に拡張ライセンスまたはワイヤレス ライセンスがインストールされている場合に使用できます。

Cisco ISE プロファイラは、Cisco NAC 展開内のエンドポイントを管理する Cisco Network Admission Control（NAC）プロファイラに似ています。この統合により、Cisco NAC 展開にインストールされている既存の Cisco NAC プロファイラを置き換えることができます。Cisco ISE プロファイラからのプロファイル名およびエンドポイント分類の結果を Cisco Clean Access Manager（CAM）と同期できます。

関連項目

- *『Cisco NAC Appliance Hardware Installation Guide, Release 4.9』*
- *『Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9』*
- *『Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9 to install, configure and administer the Cisco NAC Appliance, Release 4.9』*
- *『Release Notes for Cisco NAC Appliance, Release 4.9』*

管理ノードでの Cisco Clean Access Manager の設定

Cisco ISE では、REST API 通信設定のために分散展開のプライマリ管理ノードで複数の Clean Access Manager（CAM）を登録できます。Cisco ISE に登録されている CAM のリストは、すべてのプロファイラ設定変更が通知されるリストです。プライマリ管理ノードは、Cisco ISE と Cisco NAC アプライアンス間のすべての通信を担当します。Cisco ISE では、CAM をプライマリ管理ノードでのみ設定できます。1 つ以上の CAM をプライマリ管理ノードで登録するときに使用されたクレデンシャルが CAM との接続の認証に使用されます。

Cisco ISE と Cisco NAC アプライアンス間の通信は、Secure Sockets Layer（SSL）上で安全に行われます。Cisco ISE はプロファイラ設定の変更を CAM にプッシュし、CAM はエンドポイントの MAC アドレスと対応するプロファイルのリストおよびすべてのプロファイル名のリストを Cisco ISE から定期的にプルするため、通信は実際には双方向です。

Cisco ISE と CAM 間でセキュアな通信を適切に行えるように、[管理（Administration）] > [Clean Access Manager] > [SSL] で X509 証明書の内容を Clean Access Manager からエクスポートし、それを [管理（Administration）] > [システム（System）] > [証明書（Certificates）] [証明書信頼ストア（Certificate Trust Store）] で Cisco ISE のプライマリ管理ノードにインポートする必要があります。

関連項目

「NAC マネージャの設定」（P.A-50）

Cisco ISE Profiler と Cisco Clean Access Manager の通信

Cisco ISE プロファイラは、プロファイラ設定の変更をプライマリ管理ノードからすべての登録済み Clean Access Manager（CAM）に通知します。これにより、Cisco ISE 分散展開における通知の重複が回避されます。Cisco ISE データベースでエンドポイントの追加や削除、およびエンドポイント プロファイリング ポリシーの変更が行われると、プロファイラ設定の変更を通知するために REST API が使用されます。エンドポイントのインポート時、Cisco ISE プロファイラはインポートの完了後にのみ CAM に通知します。

プロファイラ設定の変更を CAM にプッシュするために、次の REST API フローが実装されます。

Cisco ISE プロファイラ エンドポイント変更のプッシュ：Cisco ISE でエンドポイントがプロファイリングされ、エンドポイントのプロファイルに変更がある場合、Cisco ISE プロファイラは、エンドポイント プロファイルの変更をすべての登録済み CAM に通知します。

CAM で Cisco ISE を設定し、CAM の [同期設定（Sync Settings）] に応じて CAM を Cisco ISE と同期することができます。ルールを作成し、Cisco ISE プロファイルのリストから 1 つ以上の一致するプロファイルを選択し、エンドポイントを CAM のいずれかのアクセス タイプにマッピングできます。CAM はエンドポイントと対応するプロファイル、およびプロファイル名のリストを Cisco ISE プロファイラから定期的に取得します。

プロファイラ設定の変更を Cisco ISE プロファイラからプルするために、次の REST API フローが実装されます。

- NAC Manager のエンドポイント プル：エンドポイントの MAC アドレスと既知のエンドポイントの対応するプロファイルのリストをプルします。
- NAC Manager のプロファイル プル：プロファイル名を Cisco ISE プロファイラからプルします。

Cisco ISE プロファイラは、Cisco ISE と Cisco NAC アプライアンス リリース 4.9 との統合のモニタとトラブルシューティングに使用できるすべてのイベントを Cisco ISE モニタリング ペルソナに通知します。

Cisco ISE プロファイラ ログには、統合のモニタリングとトラブルシューティングに関する次のイベントが取り込まれます。

- NAC 設定の変更（情報）
- NAC 通知イベント障害（エラー）

Cisco Clean Access Manager の追加

Cisco ISE を Cisco NAC アプライアンス リリース 4.9 と統合すると、Cisco NAC 展開で Cisco ISE プロファイリング サービスを利用できます。Cisco NAC 展開で Cisco ISE プロファイリング サービスを利用できます。

[NAC Managers] ページでは、複数の Clean Access Manager（CAM）を設定でき、登録した CAM をフィルタリングするためのオプションを使用できます。このページには、CAM が名前、説明、IP アドレス、および CAM でエンドポイント通知が有効になっているかどうかを示すステータスとともに表示されます。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [NAC Managers] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　Cisco Access Manager の名前を入力します。

ステップ 4　[ステータス（Status）] チェックボックスをオンにして、CAM への接続を認証する Cisco ISE Profiler からの REST API 通信を有効にします。

ステップ 5　次の IP アドレス以外の CAM の IP アドレスを入力します。0.0.0.0 および 255.255.255.255。

ステップ 6　CAM のユーザ インターフェイスにログインするために使用する CAM 管理者のユーザ名とパスワードを入力します。

ステップ 7　[送信（Submit）] をクリックします。

関連項目

「NAC マネージャの設定」（P.A-50）

ポリシーおよび ID グループのスタティック割り当てを持つエンドポイントの作成

[エンドポイント（Endpoints）] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。[エンドポイント（Endpoints）] ページには、スタティック割り当て用のエンドポイント プロファイリング ポリシーおよび ID グループを選択することもできます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　エンドポイントの MAC アドレスをコロンで区切られた 16 進形式で入力します。

ステップ 4　[ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。

ステップ 5　[スタティック割り当て（Static Assignment）] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。

ステップ 6　[ID グループ割り当て（Identity Group Assignment）] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。

ステップ 7　エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て（Static Group Assignment）] チェックボックスをオンにします。

ステップ 8　[送信（Submit）] をクリックします。

関連項目

- 「エンドポイント設定」（P.A-27）
- 「エンドポイントの ID グループでの静的エンドポイントの追加」（P.21-46）
- 「Cisco ISE Profiler がエンドポイントのデータを収集できない」（P.G-5）
- 「プロファイリングされたエンドポイントで認証を実行できない」（P.G-20）

CSV ファイルからのエンドポイントのインポート

Cisco ISE サーバからエンドポイントをすでにエクスポートしている CSV ファイル、または Cisco ISE から作成し、エンドポイントの詳細で更新した CSV ファイルからエンドポイントをインポートできます。

このファイル形式は、デフォルトのインポート テンプレートで指定された形式になっており、エンドポイントのリストが「MAC, エンドポイント ポリシー , エンドポイント ID グループ」のように表示される必要があります。

エンドポイント ポリシーとエンドポイントの ID グループは、CSV ファイルでのエンドポイントのインポートのオプションです。エンドポイントのエンドポイント ポリシーなしでエンドポイントの ID グループをインポートする場合でも、値はカンマで区切られます。

次に例を示します。

- MAC1, エンドポイント ポリシー 1, エンドポイント ID グループ 1
- MAC2
- MAC3, エンドポイント ポリシー 3
- MAC4, , エンドポイント ID グループ 4

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] > [インポート（Import）] を選択します。

ステップ 2　[ファイルからインポート（Import From File）] をクリックします。

ステップ 3　[参照（Browse）] をクリックして、Cisco ISE サーバからすでにエクスポートした CSV ファイル、または指定されたファイル形式で作成し、エンドポイントで更新した CSV ファイルを検索します。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

- 「エンドポイントで使用可能なデフォルトのインポート テンプレート」（P.21-38）
- 「インポート中に際プロファイリングされる不明なエンドポイント」（P.21-39）
- 「インポート中に保持されるエンドポイントのポリシーおよび ID グループのスタティック割り当て」（P.21-40）
- 「LDAP サーバからのエンドポイントのインポート」（P.21-40）

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存でき

ます。ファイルは、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] > [インポート（Import）] > [ファイルからインポート（Import From File）] にあります。

[テンプレートの生成（Generate a Template）] リンクを使用してテンプレートを作成でき、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。

デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、およびエンドポイント ID グループのカラムが表示されるヘッダー行が含まれています。エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループを更新し、エンドポイントのインポートに使用できる異なるファイル名でこのファイルを保存する必要があります。

表 21-11 に、[テンプレートの生成（Generate a Template）] リンクを使用したときに作成される template.csv ファイルのヘッダー行を示します。

表 21-11　CSV テンプレート ファイル

MAC	エンドポイント ポリシー（Endpoint Policy）	エンドポイント ID グループ（Endpoint Identity Group）
00:1f:f3:4e:c1:8e	Cisco-Device	RegisteredDevices

インポート中に際プロファイリングされる不明なエンドポイント

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイント プロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。

表 21-12 に、Cisco ISE がインポート時に Xerox_Device プロファイルに一致した不明プロファイルを再プロファイリングする方法を示します。また、Cisco ISE が未割り当てのエンドポイントを再プロファイリングする方法も示します。

表 21-12　不明プロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:03	不明。	Xerox-Device
00:00:00:00:01:04	不明。	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポート中に保持されるエンドポイントのポリシーおよび ID グループのスタティック割り当て

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイント プロファイリング ポリシーがスタティック割り当てである場合、インポート時に再プロファイリングされることはありません。

表 21-13 に、Cisco ISE が、Cisco-Device プロファイル（エンドポイントのスタティック割り当て）をインポート時に保持する仕組みを示します。

表 21-13　スタティック割り当て：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	Cisco-Device（スタティック割り当て）	Cisco-Device

インポートされない無効なプロファイルを持つエンドポイント

エンドポイントが、インポートに使用するファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。

表 21-14 に、エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされないことも示します。

表 21-14　無効なプロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE で使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

関連項目

「CSV ファイルからのエンドポイントのインポート」（P.21-38）

LDAP サーバからのエンドポイントのインポート

エンドポイントの MAC アドレスおよび関連付けられているエンドポイント ID グループを LDAP サーバからセキュアにインポートできます。

はじめる前に

エンドポイントのインポートを開始する前に、LDAP サーバがインストール済みであることを確認します。

LDAP サーバからインポートする前に、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：(LDAP import failed:)」メッセージが表示されます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] > [インポート（Import）] > [LDAP からのインポート（Import From LDAP）] を選択します。

ステップ 2　接続設定の値を入力します。

ステップ 3　クエリー設定の値を入力します。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

「LDAP からのエンドポイントのインポート設定」（P.A-29）

カンマで区切られた値ファイルでのエンドポイントのエクスポート

選択したエンドポイントまたはすべてのエンドポイントを、カンマで区切られた値（CSV）ファイルで Cisco ISE サーバから別の Cisco ISE サーバにエクスポートできます。CSV ファイルでは、エンドポイントは、MAC アドレス、エンドポイント プロファイリング ポリシー、およびそれらが割り当てられたエンドポイント ID グループでリスト表示されます。

[すべてエクスポート（Export All）] がデフォルトのオプションです。エンドポイントが [エンドポイント（Endpoints）] ページでフィルタリングされている場合、[すべてエクスポート（Export All）] オプションを使用すると、フィルタリングされたエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が [profiler_endpoints.csv を開く（Opening profiler_endpoints.csv）] ダイアログボックスから CSV ファイルを開くか、または CSV ファイルを保存するデフォルトのアプリケーションです。たとえば、選択したエンドポイントまたはすべてのエンドポイントを profiler_endpoints.csv ファイルにエクスポートし、これらのエンドポイントをインポートするためにそのファイルを使用できます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] を選択します。

ステップ 2　[エクスポート（Export）] をクリックし、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [エンドポイント（Endpoints）] ページで選択したエンドポイントだけをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトでは、[エンドポイント（Endpoints）] ページのすべてのエンドポイントをエクスポートできます。

ステップ 3　[OK] をクリックして、profiler_endpoints.csv ファイルを保存します。

識別されたエンドポイント

Cisco ISE では、[エンドポイント（Endpoints）] ページにネットワークに接続し、ネットワーク上のリソースを使用する識別されたエンドポイントが表示されます。エンドポイントは、通常、有線またはワイヤレスのネットワーク アクセス デバイスおよび VPN を介してネットワークに接続しているネットワーク対応デバイスです。エンドポイントとして、パーソナル コンピュータ、ラップトップ、IP Phone、スマート フォン、ゲーム コンソール、プリンタ、ファクス機などがあります。

16 進数形式で表現されたエンドポイントの MAC アドレスは、常にエンドポイントを一意に表現したものですが、属性のさまざまなセットとその属性に関連付けられた値（属性値ペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているエンドポイント プロファイリング ポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに関連付けるときに、エンドポイントを静的にプロファイリングできます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明エンドポイント

エンドポイントに一致するプロファイリング ポリシーがない場合は、不明プロファイリング ポリシー（不明）を割り当てることができます。このため、そのエンドポイントは不明としてプロファイリングされます。不明エンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明エンドポイント ID グループにグループ化されます。

関連項目

- 「ポリシー サービス ノードのデータベースにローカルに保存されている識別されたエンドポイント」（P.21-42）
- 「ポリシー サービス ノード」（P.3-3）
- 「Cisco ISE Profiler がエンドポイントのデータを収集できない」（P.G-5）
- 「プロファイリングされたエンドポイントで認証を実行できない」（P.G-20）

ポリシー サービス ノードのデータベースにローカルに保存されている識別されたエンドポイント

Cisco ISE は、識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカルに保存すると、これらのエンドポイントは、重要な属性がエンドポイントで変更された時のみ管理ノードのデータベースで使用できる（リモート書き込み）ようになり、他のポリシー サービス ノードのデータベースに複製されます。

次に、重要な属性を示します。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE のエンドポイント プロファイル定義を変更すると、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシー サービス ノードは、これらのエンドポイントの再プロファイリングを担当します。

ポリシー サービス ノードが、属性が別のポリシー サービス ノードによって最初に収集されたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権は、現在のポリシー サービス ノードに変更します。新しいポリシーのサービス ノードは、前のポリシーのサービス ノードから最新の属性を取得して、収集した属性をすでに収集されたこれらの属性と調整します。

重要な属性がエンドポイントで変更されたとき、エンドポイントでの最新の大幅な変更を保持するために、エンドポイントの属性は自動的に管理ノードのデータベースに保存されます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理者 ISE ノードはオーナーを失ったエンドポイントを再プロファイリングし、管理者はこのようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタ内のポリシー サービス ノード

Cisco ISE は、ポリシー サービス ノード グループをクラスタとして使用し、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときにエンドポイント属性を交換できるようにします。すべてのポリシー サービス ノードがロード バランサの背後に存在するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性から作成される属性のリスト（ホワイトリスト）に基づいて決定されます。表 21-5（P.21-19）を参照してください。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment

- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

関連項目

- 「ポリシー サービス ノードのデータベースにローカルに保存されている識別されたエンドポイント」（P.21-42）
- 「ポリシー サービス ノード」（P.3-3）

エンドポイント ID グループの作成

[エンドポイント ID グループ（Endpoint Identity Groups）] ページで、エンドポイント ID グループを作成、編集、または削除できます。自分がシステムで作成した ID グループでは、ID グループの名前と説明のみを編集でき、ID グループを削除できます。Cisco ISE によりシステムに作成されたエンドポイント ID グループでは、名前は編集できませんが、説明は編集でき、エンドポイント ID グループを削除できません。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4　作成するエンドポイント ID グループの説明を入力します。

ステップ 5　[親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成されたエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6　[送信（Submit）] をクリックします。

関連項目

- 「エンドポイント ID グループ設定」（P.A-31）
- 「エンドポイントの ID グループでの静的エンドポイントの追加」（P.21-46）

エンドポイント ID グループでグループ化された識別済みエンドポイント

Cisco ISE は、検出されたエンドポイントを、エンドポイント プロファイリング ポリシーに基づいて、対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントをエン

ドポイント ID グループにグループ化し、プロファイリング ポリシーをエンドポイント ID グループに適用すると、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE は一連のエンドポイント ID グループをデフォルトで作成し、エンドポイントを動的または静的に割り当てることができる独自の ID グループを作成することができます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つに ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、プロファイリング サービスは ID グループを再割り当てできなくなります。

関連項目

- 「エンドポイント ID グループの作成」（P.21-44）
- 「エンドポイント用に作成されるデフォルトのエンドポイント ID グループ」（P.21-45）
- 「一致したエンドポイント プロファイリング ポリシーに対して作成されたエンドポイント ID グループ」（P.21-46）

エンドポイント用に作成されるデフォルトのエンドポイント ID グループ

Cisco ISE は、ブラックリスト、ゲスト エンドポイント、プロファイル済み、登録済みデバイス、および不明の 5 つのエンドポイント ID グループを作成します。さらに、プロファイル済み（親）ID グループに関連付けられている Cisco-IP-Phone やワークステーションなどの追加の 2 つの ID グループを作成します。親グループは、システムに存在するデフォルトの ID グループです。

Cisco ISE は、次のエンドポイント ID グループを作成します。

- ブラックリスト：このエンドポイント ID グループには、Cisco ISE のこのグループに静的に割り当てられ、デバイス登録ポータルでブラックリストに記載されたエンドポイントが含まれます。このグループのエンドポイントへのネットワーク アクセスを許可または拒否するように許可プロファイルを Cisco ISE で定義できます。
- ゲスト エンドポイント：このエンドポイント ID グループには、ゲスト ユーザが使用するエンドポイントが含まれます。
- プロファイル済み：このエンドポイント ID グループには、Cisco ISE の Cisco IP Phone およびワーク ステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- 登録済みデバイス：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスに対して、Cisco ISE の [エンドポイント（Endpoints）] ページのエンドポイント リストで編集、削除およびブラックリストへの記載を実行できます。デバイス登録ポータルでブラックリストに記載されたデバイスは、ブラックリスト エンドポイント ID グループに割り当てられ、Cisco ISE に存在する許可プロファイルは、ブラックリストに記載されたデバイスを URL（「無許可ネットワーク アクセス」と表示される、ブラックリストに記載されたデバイスのデフォルト ポータル ーページ）にリダイレクトします。
- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムにより作成されたたエンドポイントに加え、Cisco ISE は、プロファイル済み ID グループに関連付けられている次のエンドポイントの ID グループを作成します。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済み Cisco IP Phone が含まれる ID グループです。
- ワークステーション：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

関連項目

「一致したエンドポイント プロファイリング ポリシーに対して作成されたエンドポイント ID グループ」（P.21-46）

一致したエンドポイント プロファイリング ポリシーに対して作成されたエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイント ID グループを作成できます。この ID グループは、プロファイル済みエンドポイント ID グループの子になります。エンドポイント ポリシーを作成する場合、[プロファイリング ポリシー（Profiling Policies）] ページの [一致する ID グループの作成（Create Matching Identity Group）] チェックボックスをオンにして、一致するエンドポイント ID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

関連項目

「静的に追加されたエンドポイントのエンドポイント プロファイリング ポリシー」（P.21-28）

エンドポイントの ID グループでの静的エンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント（Endpoints）] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] を選択します。

ステップ 2　エンドポイント ID グループを選択して [編集（Edit）] をクリックします。

ステップ 3　[追加（Add）] をクリックします。

ステップ 4　[エンドポイント（Endpoints）] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5　[エンドポイント グループ リスト（Endpoint Group List）] リンクをクリックして、[エンドポイント ID グループ（Endpoint Identity Groups）] ページに戻ります。

関連項目

「ID グループで追加または削除後に再プロファイリングされる動的エンドポイント」（P.21-47）

ID グループで追加または削除後に再プロファイリングされる動的エンドポイント

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイントはエンドポイント ID グループで追加または削除した後に再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、デフォルトですべてのタイプの Cisco IP Phone 用の許可ルールが、Cisco ISE の次の場所で使用できます。[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）]。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー（他のエンドポイント プロファイリング ポリシーの親でない）であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

プロファイラ フィード サービス

プロファイラ フィード サービスの導入により、プロファイラ条件、例外アクション、および NMAP スキャン アクションが、Cisco ISE でシスコ提供または管理者作成（システム タイプ属性を参照）として分類されます。また、エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更（システム タイプ属性を参照）として分類されます。

システム タイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャン アクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャン アクションは編集または削除できません。シスコが提供するエンドポイント ポリシーは削除できません。ポリシーを編集すると、管理者による変更と見なされます。管理者によって変更されたポリシーが削除されると、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

指定 Cisco フィード サーバからサブスクリプションを介して Cisco ISE へのフィードとして、新規および更新されたエンドポイント プロファイリング ポリシーおよび更新された OUI データベースを取得できます。また、適用、成功、および失敗メッセージに対して設定した、Cisco ISE の管理者としての電子メール アドレスに電子メール通知を受信できます。通知を受信するために追加の加入者情報も提供できます。レコードを維持するために加入者情報をシスコに送り返すことができ、それらは特権および機密として処理されます。

デフォルトでは、プロファイラ フィード サービスは無効なっており、サービスを有効にするには拡張ライセンスが必要です。プロファイラ フィード サービスを有効にすると、Cisco ISE は毎日ローカル Cisco ISE サーバのタイム ゾーンの午前 1:00 にフィード サービス ポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバ ポリシーを自動的に適用し、また、これらの変更を以前の状態に復元できるように一連の変更を保存します。最後に適用した一連の変更から復元すると、新しく追加されたエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

更新が行われるとき、シスコ提供のプロファイリング ポリシーと、以前の更新で変更されたエンドポイント プロファイリング ポリシーのみが更新されます。シスコ提供の無効のプロファイリング ポリシーも更新されますが、無効のままです。管理者作成または管理者による変更のプロファイリング ポリシーは、上書きされません。管理者による変更のエンドポイント プロファイリング ポリシーをシスコ提供のエンドポイント プロファイリング ポリシーに復元する場合は、管理者による変更のエンドポイント プロファイリング ポリシーを削除するか、または管理者による変更のエンドポイント プロファイリング ポリシーを以前のシスコ提供のエンドポイント プロファイリング ポリシーに復元します。

関連項目

- 「OUI フィード サービス」（P.21-48）
- 「プロファイラ フィード サービスの設定」（P.21-48）
- 「エンドポイント プロファイリング ポリシーの更新の削除」（P.21-50）

OUI フィード サービス

指定 Cisco フィード サーバは、次の場所から更新された OUI のデータベースをダウンロードします。*http://standards.ieee.org/develop/regauth/oui/oui.txt*、これは MAC OUI に関連付けられているベンダーのリストです。更新された OUI データベースは、Cisco ISE が自身のデータベースにダウンロードするフィードとして ISE 展開に使用できます。Cisco ISE はエンドポイントを更新してから、エンドポイントの再プロファイリングを開始します。

指定 Cisco フィード サーバは、https://ise.cisco.com:8443/feedserver/ にあります。サービスへのアクセスに問題がある場合は、ネットワーク セキュリティ コンポーネント（ファイアウォールまたはプロキシ サーバなど）がこの URL への直接アクセスを許可していることを確認します。

プロファイラ フィード サービスの設定

新規および更新されたエンドポイント プロファイリング ポリシーおよび MAC OUI の更新を、指定 Cisco フィード サーバからのフィードとして受信するように Cisco ISE を設定できます。プロファイラ フィード サービスを有効にすると、Cisco ISE は、最後のフィード サービス更新および MAC OUI 以降に作成された新規および更新されたプロファイルをチェックできます。フィード サービスが使用できない場合や、その他のエラーが発生している場合、操作監査レポートで報告されます。

Cisco ISE の管理者としてフィード サービス使用状況レポートをシスコに送り返すように設定したり、代替 Cisco ISE 管理者詳細（任意の属性）を [フィード サービス加入者情報（Feed Service Subscriber Information）] セクションに指定したりできます。

次のデータを送り返すことができます。

- Hostname：Cisco ISE ホスト名
- MaxCount：エンドポイントの合計数
- ProfiledCount：プロファイリングされたエンドポイント カウント
- UnknownCount：不明なエンドポイント カウント
- MatchSystemProfilesCount：シスコ提供のプロファイル カウント
- UserCreatedProfiles：ユーザ作成のプロファイル カウント

フィード サーバからダウンロードしたプロファイリング ポリシーの CoA タイプは、ローカルで設定され、ダウンロードされません。ダウンロードされたポリシーの CoA タイプを変更した場合、状態は更新されません。それはシステム ポリシーのままで、フィード サーバを介してポリシーを更新する必要があります。

はじめる前に

プロファイラ フィード サービスは、分散展開またはスタンドアロン ISE ノードの Cisco ISE 管理者ポータルからのみ設定できます。

フィード サービス クライアントは HTTPS を使用してフィード サービス プラットフォームと対話するので、Cisco ISE は通信するためにフィード サーバ証明書を要求します。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] に移動して、証明書ストアから証明書をダウンロードできます。

電子メール通知を送信するには、管理者ポータル（[管理（Administration）] > [システム（System）] > [設定（Settings）]）で Simple Mail Transfer Protocol（SMTP）サーバを設定する必要があります。

ステップ 1　[管理（Administration）] > [バックアップ / 復元（FeedService）] > [プロファイラ（Profiler）] を選択します。

ステップ 2　[フィード サービスの有効化（Enable Profiler Feed Service）] チェックボックスをオンにします。

ステップ 3　[フィード サービス スケジューラ（Feed Service Scheduler）] セクションに HH:MM 形式で時刻（Cisco ISE サーバのローカル タイム ゾーン）を入力します。デフォルトでは、Cisco ISE プロファイラ フィード サービスは毎日午前 1:00 にスケジュールされます。

ステップ 4　[管理者通知オプション（Administrator Notification Options）] セクションで [ダウンロードが行われたら管理者に通知（Notify administrator when download occurs）] チェックボックスをオンにして、[管理者の電子メール アドレス（Administrator email address）] テキスト ボックスに Cisco ISE の管理者として電子メール アドレス入力します。

ステップ 5　[フィード サービス加入者情報（Feed Service Subscriber Information）] セクションで [加入者情報をシスコに提供（Provide subscriber information to Cisco）] チェックボックスをオンにして、フィード サーバの使用状況レポートをシスコに送り返します。

ステップ 6　[同意する（Accept）] をクリックします。詳細については、http://www.cisco.com/web/siteassets/legal/privacy.html を参照してください。

ステップ 7　[保存（Save）] をクリックします。

ステップ 8　[今すぐ更新（Update Now）] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの認可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新（Update Now）] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定（Profiler Feed Service Configuration）] ページから別の場所に移動し、このページに戻ります。

ステップ 9　[はい（Yes）] をクリックします。

関連項目

- 「エンドポイント プロファイリング ポリシーの更新の削除」（P.21-50）
- 「プロファイラ フィード サービス」（P.21-47）
- 「OUI フィード サービス」（P.21-48）
- 「通知をサポートするように SMTP サーバを設定」（P.5-5）

エンドポイント プロファイリング ポリシーの更新の削除

以前の更新で更新されたエンドポイント プロファイリング ポリシーを復元し、プロファイラ フィード サービスの以前の更新によって新しく追加されたエンドポイント プロファイリング ポリシーを削除することができますが、OUI の更新は変更されません。

エンドポイント プロファイリング ポリシーは、フィード サーバからの更新後に変更された場合は、システムで変更されません。

ステップ 1　[管理（Administration）] > [バックアップ / 復元（FeedService）] > [プロファイラ（Profiler）] を選択します。

ステップ 2　[フィード サービスの有効化（Enable Profiler Feed Service）] チェックボックスをオンにします。

ステップ 3　[更新レポート ページへ移動（Go to Update Report Page）] をクリックして、変更設定監査レポートで行われた設定変更を表示します。

ステップ 4　[最新を元に戻す（Undo Latest）] をクリックします。

ステップ 5　[保存（Save）] をクリックします。

関連項目

- 「プロファイラ フィード サービスの設定」（P.21-48）
- 「プロファイラ フィード サービス」（P.21-47）

プロファイラ レポート

Cisco ISE には、エンドポイント プロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティング ツールが用意されています。履歴および現在のデータのレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイント別の上位許可
- 登録済みエンドポイント

関連項目

第 26 章「レポート」