目次

概要

この資料はリダイレクションがサード パーティ ネットワーク アクセス デバイス（NADs）によって起こるようにする Identity Services Engine （ISE）で新しい 機能を説明していたものです。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE のゲスト フロー
- DNS および DHCP プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Catalys 2960 シリーズ スイッチ
- Cisco ISE、リリース 2.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

ゲストのような進んだ機能は、ポスチャ 現代のネットワークのあなた自身のデバイス（BYOD）を持って来ましたり、クライアントデバイスと AAAサーバ間の直通 通信を必要とし。前の ISE バージョンでこれは NAD へダイナミック リダイレクト URL および Access Control List（ACL）を送信 することによって達成されました。

attribute-value パリ（AV）のリダイレクションのための許可 プロファイルで送信 される 2 つの必須属性があります:

- Cisco AV ペアか。 リダイレクト URL: URL 値はダイナミックであり、各セッションのために作成されます。 リダイレクト URL の重要な部分はポリシー サービス ノード Fuly 修飾ドメイン名（PSN FQDN）およびセッションID です。
- Cisco AV ペアか。 リダイレクト ACL: この AVペアは NAD にある必要がある ACL 名前が含まれています。 この ACL の助けによって、NAD はパケットが NAD によってべきであるリダイレクトされるか、または許可されるかどうか決定します。

従来のリダイレクション アプローチは Cisco NAD デバイスによってしか設定することができません。 サード パーティ NAD サポートに関しては、静的な URL リダイレクションは ISE 2.0 に追加されました。 このアプローチはより多くのプラットフォーム依存しないの間、まだ NAD の HTTP リダイレクション サポートを必要とします。

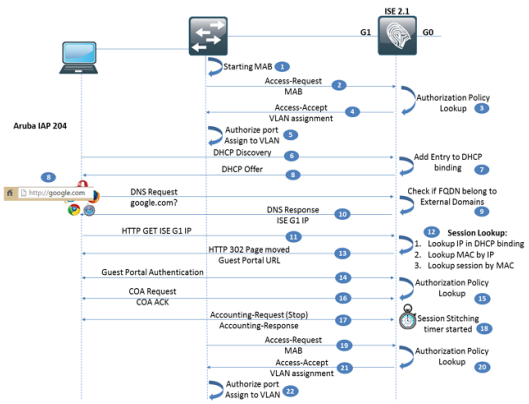
ISE 2.1 から開始はリダイレクトの新式追加されました。 このアプローチは NAD の HTTP リダイレクション サポートを必要としません。 この方式の後ろの主旨は DNS シンクホールとして ISE を使用することです。

DNS および DHCPサーバ機能性は ISE 2.1 リリースに DNS シンクホールとしてそれを使用するために追加されました。 この場合 ISE サーバはユーザに IP アドレスを割り当てるリダイレクトされる必要があることができ、DNSサーバとそれ自身を定義します。 これは ISE が NAD の Webサーバ 機能性なしでそれ自身にユーザ接続をリダイレクトするようにします。 ただし、NAD はまだ許可（COA）およびダイナミック VLAN 割り当ての変更をサポートする必要があります。

ISE では、このアプローチはこれらのリダイレクション フローに使用することができます:

- ゲスト フロー: 自身の IP アドレスのユーザによって始められる DNS 要求への ISE 返事。 この応答によりクライアントは ISE の HTTP接続を確立します。 この点について、ISE は移動する標準 HTTP コード 302 ページを使用してリダイレクト URL を戻します。
- BYOD/Posture（Anyconnect だけ）か。 両方のシナリオで、（NSP）アプリケーションか Anyconnect ポスチャ モジュールを提供するネイティブ サプリカントはゲスト フローと同じステップを使用して ISE にリダイレクトされる enroll.cisco.com への接続を開始します。

パケット フロー



1. NAD は接続装置のための MAB プロセスを開始します。 Ciscoスイッチの MAB プロセスは認証方式 優先順位に従ってない最初のフレームがエンド デバイスから受信される前に開始し。
2. MAB access-request は ISE に送信 されます。
3. ISE は着信アクセス 要求のための認証 および 権限 ポリシーを評価します。 承認ポリシー評価の間に、ネットワークデバイス型（NAD レベル設定）は許可 プロファイルで定義された型ネットワークデバイスによって比較されます。 一致するネットワークデバイス型のための許可プロファイルだけ選択することができます。

   注 ゲスト VLAN リダイレクトに関しては、ISE は許可 プロファイルを選択する必要があります Web リダイレクション（CWA、MDM、NSP、CPP）および VLAN 割り当てが含まれている。 唯一の DHCPサーバとして ISE があるネットワークセグメントに割り当てられるクライアント必要。

1. ISE は VLAN 情報を用いる Access-Accept を戻します。
2. スイッチはポートを承認し、VLAN の 設定を加えます。
3. クライアントは DHCP 検出するを始めます。 PC が ISE と同じセグメントにある場合、パケットは ISE に直接到着します。 クライアントと ISE 間の L3 接続の場合には、ISE IP は DHCPリレーのための NAD の IPヘルパーアドレスで設定する必要があります。
4. ISE は DHCP バインディング テーブルにクライアント の 情報を追加します。 クライアントIP および MAC はセッション ルックアップのために ISE によって使用されます。
5. DHCP オファーはクライアントに送信 されます。 このオファーでは、ISE IP アドレスは DNSサーバとして規定 されます。
6. ユーザは ISE に DNS 要求を引き起こす Webブラウザを開き、google.com にナビゲート します。
7. ISE はターゲット FQDN が外部ドメインに属するかどうか確認します。 それが場合、ISE は DHCPプール設定で定義される DNSサーバにこの要求を送信 します。 ない ISE が応答の自身の IP アドレスを戻せば。
8. Webブラウザは ISE への TCP 接続および google.com のための要求を始めます。
9. この段階では ISE は着信 HTTP GET 要求のための認証 された セッションを調べます。 これは正しいリダイレクト URL を構築するために重要です。

   注 ISE はセッション ルックアップのためにこれらのルールを使用します:
   1. DHCP バインディングのルックアップ IP
   2. IP によるルックアップ MAC
   3. MAC によるルックアップ セッション

1. ISE はリダイレクト URL に移動する HTTP 302 ページと応答します。
2. ユーザは門脈ゲストにこうしてリダイレクトされ、ISE で設定される全体のゲスト フローはここに起こります。
3. 正常なゲスト認証の後でもう一度動作しますどの新しい属性でもセッションに追加されたかどうか、そして確認するために、ISE は承認ポリシーによってゲスト フローの間のエンドポイントは許可（CoA）の変更を必要とするかどうか。 次の承認ポリシーが識別されれば、ISE は CoA 要求を準備します。
4. CoA 要求/CoA ACK 交換は ISE と NAD の間で起こります。 これが最終的な VLAN の新しい IP アドレスを得ることを引き起こすのでポート バウンスか Admin リセット CoA は絶対必要です。 NAD ははたらくためにこのステップのための Radius か SNMP CoA をサポートする必要があります。
5. 切断されたセッションのためのアカウンティング要求停止は ISE に送信 されます。 ISE は

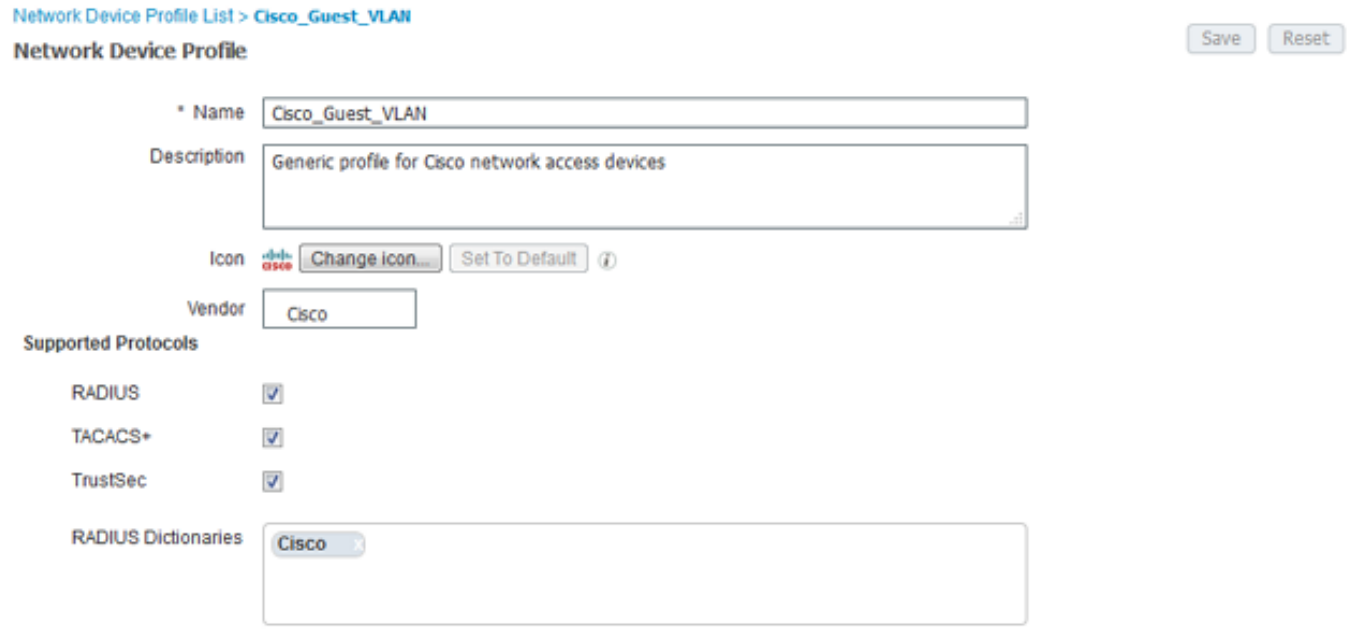
アカウンティング応答の送信によってこの要求を確認します。
6. ISE はセッションをタイマー（20 秒デフォルトで）をステッチさせ始めます。 この時間の間すべてのセッション属性（前: GUEST_TYPE は ISE によって、使用 case=Guest フロー）保存されます。 同じ起呼 端末 ID のための新しいアクセス 要求がこの時間の間に受け取られれば、すべてのセッション属性は新しいセッションに結合 されます。
7. 新しい MAB access-request はエンド デバイスのために後 CoA ポート バウンス送信 されました。
8. ISE は New 要求のための認証/許可 ポリシーを識別します。 この段階では ISE は正しいポリシー選択のためにセッション属性やエンドポイント属性を利用します。
9. Access-Accept は最終的な VLAN 情報と送信 されます。 ダウンロード可能 アクセス制御リスト（DACL）はデフォルトVLAN のトラフィックを同様に制限するために代りに送信 することができます。
10. スイッチは含まれられていた場合新しい VLAN のポートを承認し、DACL を適用します。

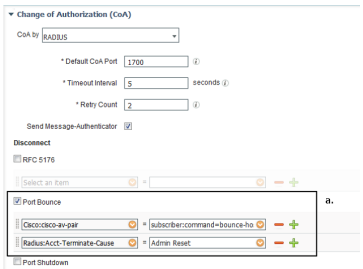
設定

ISE の設定

1. ネットワークデバイス プロファイルを作成して下さい

この特定の 例に関しては、Ciscoスイッチ NAD として使用されて。 従って、既存の Ciscoネットワークデバイス プロファイル複写され、要求に応じて修正される。 Administration > ネットワークリソース > ネットワークデバイス プロファイルにナビゲート し、新しいプロファイルを追加して下さい。





2. ネットワークデバイスを作成して下さい

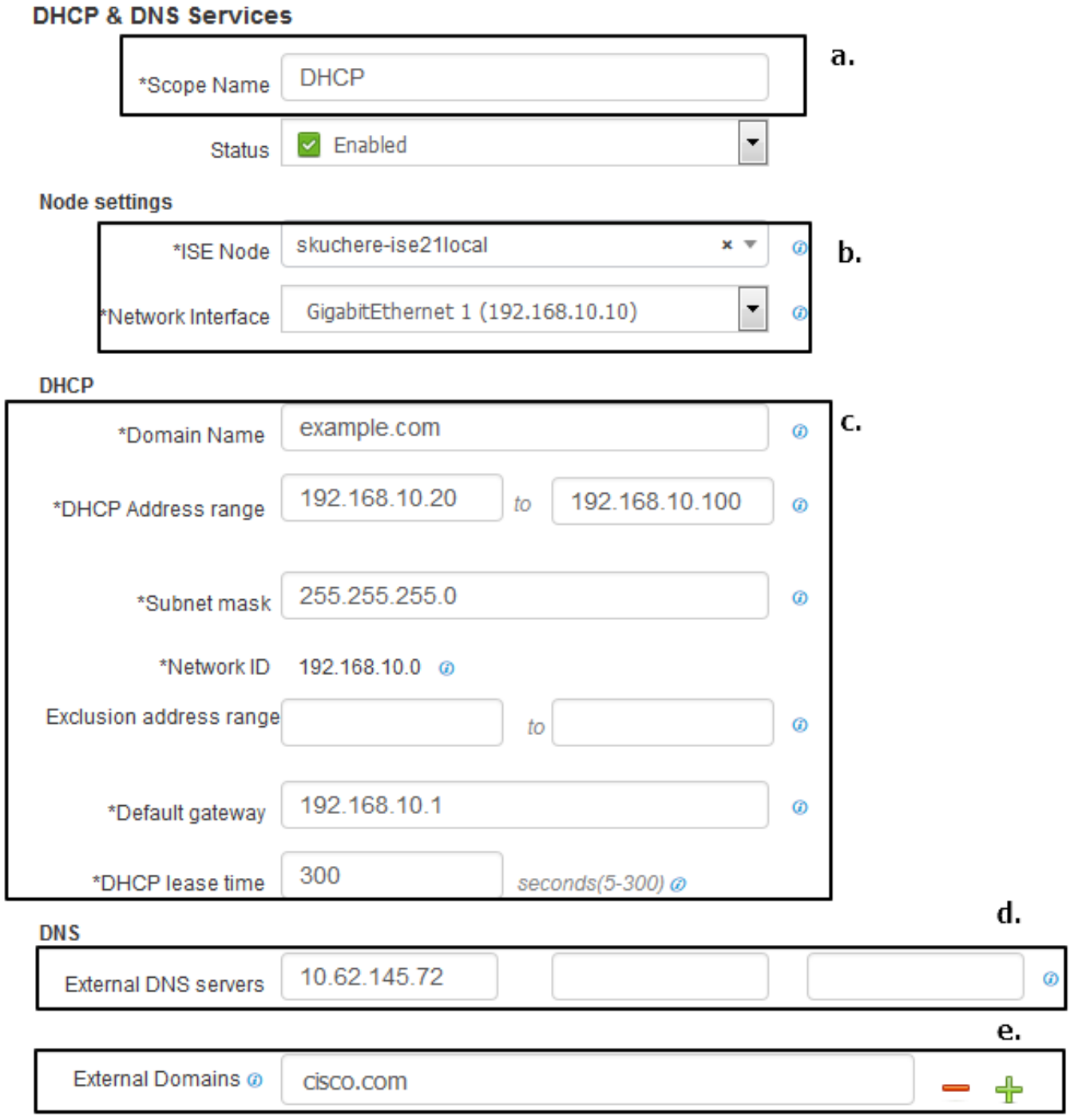
Administration > ネットワークリソース > ネットワークデバイスにナビゲート して下さい。 追加するためにナビゲート して下さい。

a. ネットワークデバイス プロファイルの設定に注意して下さい。

b. 他の設定はすべて標準です。

3. DHCPサーバを設定して下さい

DHCPサーバ プールは特定の ISE ノードおよびインターフェイスに結合 されます。 > Add は Administration > システム > 設定 > DHCP 及び DNS サービスにナビゲート します



a. DHCP スコープ名前は設定される必要があります。

b.動作する必要があるおよび使用する必要があるそのノードのインターフェイス DNS および DHCP サービス ノードを選択して下さい。

c. DHCP IPアドレス範囲、スコープから除かれるデフォルト ゲートウェイ、アドレスおよびDHCPリース時間を定義して下さい。

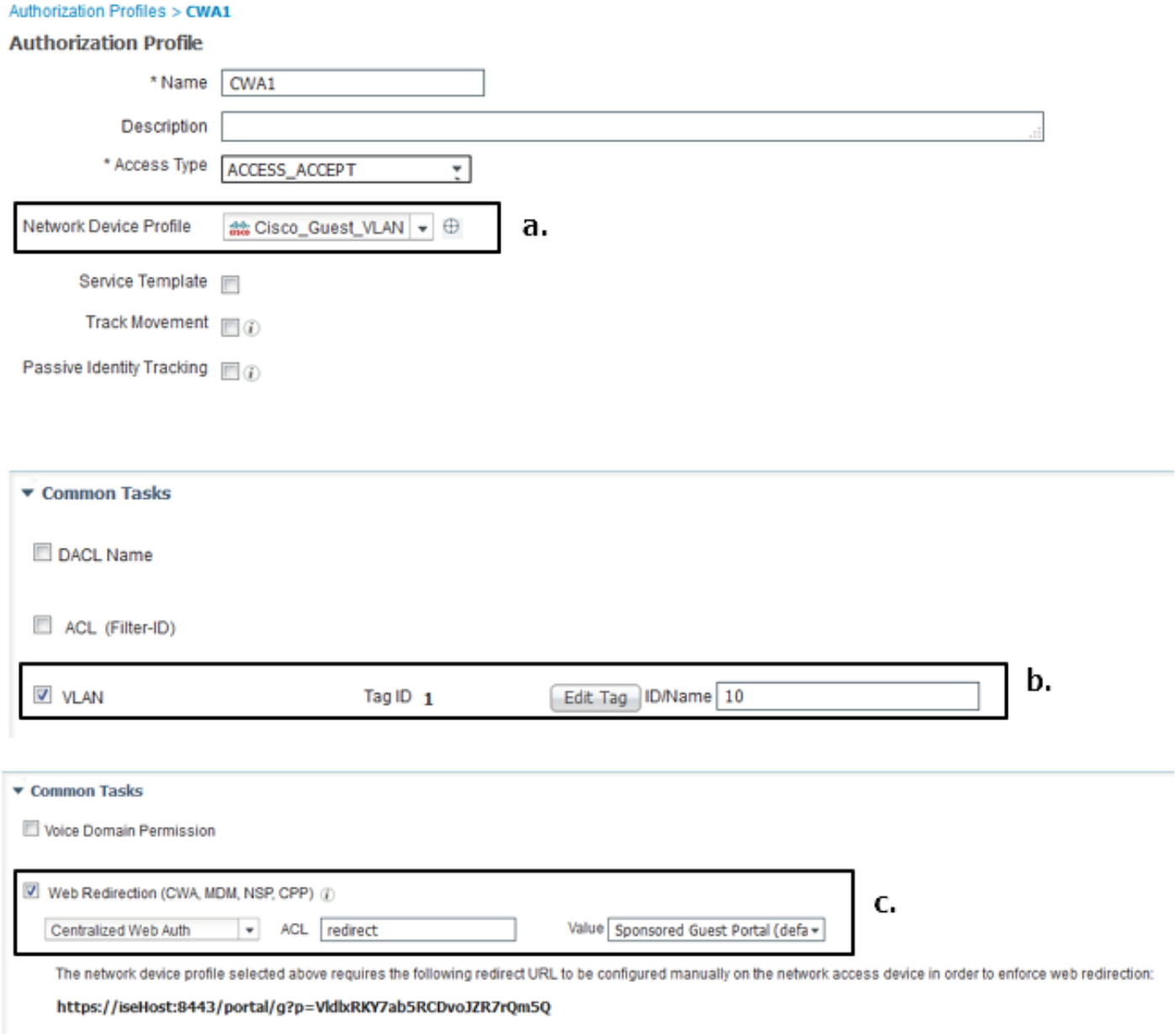
D.任意で、外部 DNSサーバ IP アドレスを定義して下さい。 これらは外部ドメインのために問い合わせる必要があります。

e.任意で、外部ドメイン名前を定義して下さい。 ISE は外部 DNSサーバを問い合わせ、専有物の代りに実際の IP アドレスを戻します。

4. 許可 プロファイルを設定して下さい

ポリシー > ポリシー要素へのナビゲートは > > 許可 > 許可プロファイル生じます。 2 つの許可プロファイルは完全なゲスト フローのために必要です:

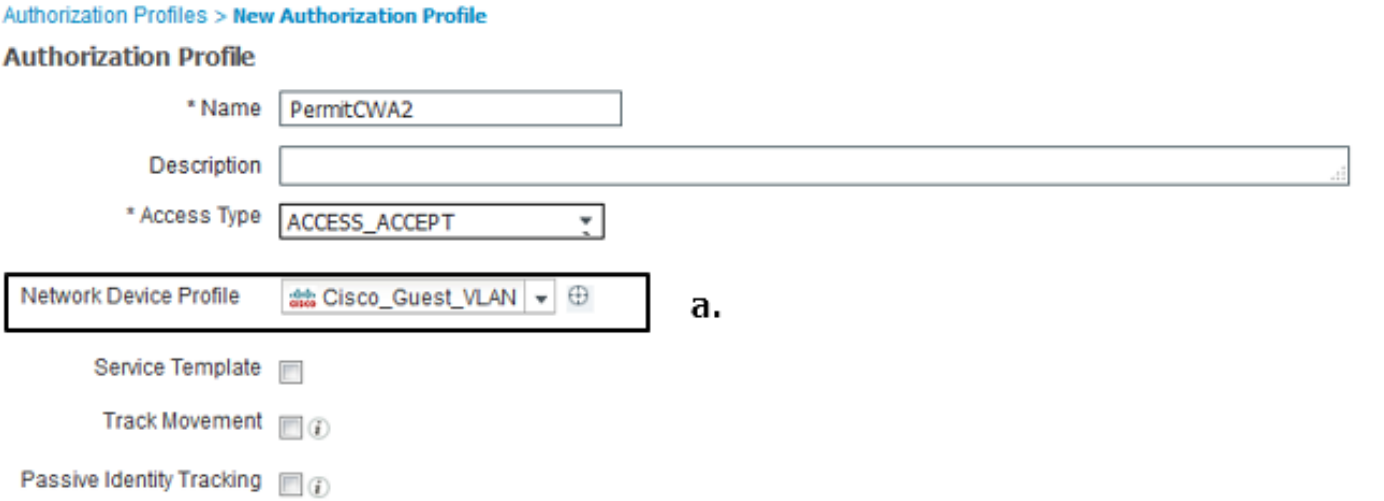
- リダイレクト 許可 プロファイル（CWA1）
- 割り当てアクセス 許可 プロファイル（PermitCWA2）

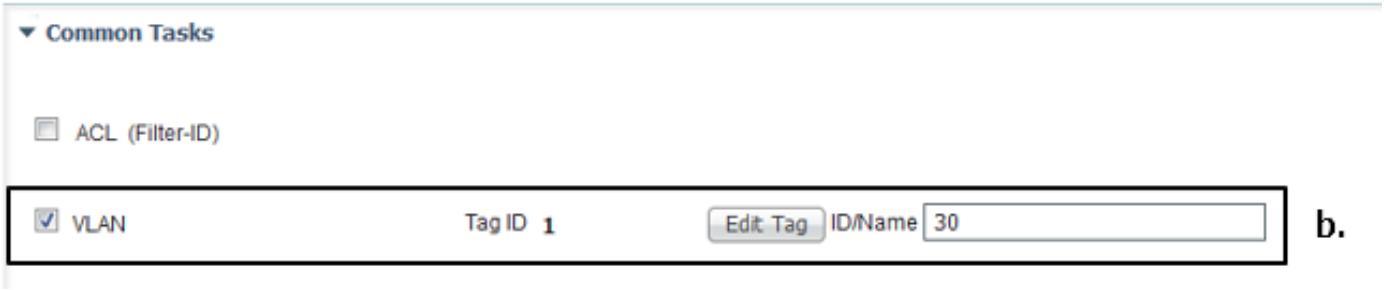


a.ネットワークデバイス プロファイル: NADs から来る認証要求だけこの許可 プロファイルという結果にこのプロファイルに終るかもしれません割り当てました

b. VLAN の 設定: ここに定義される VLAN は NAD にある必要があります。 DHCP のために設定される ISE インターフェイスはこの VLAN を保守するゲートウェイの IPヘルパーでこの VLAN にまたは設定する必要があります属する必要があります。

c.リダイレクト設定: 中央 Web 現在の例に関しては認証はリダイレクト型および後援されたゲスト ポータルとゲスト ポータルと定義されて定義されました。 形式はまだリダイレクト ACL 名前の入力を求めます。 ネットワークデバイス プロファイルがスタティック URL リダイレクトのために再構成されたので、この ACL 名前は NAD に決して送られません。



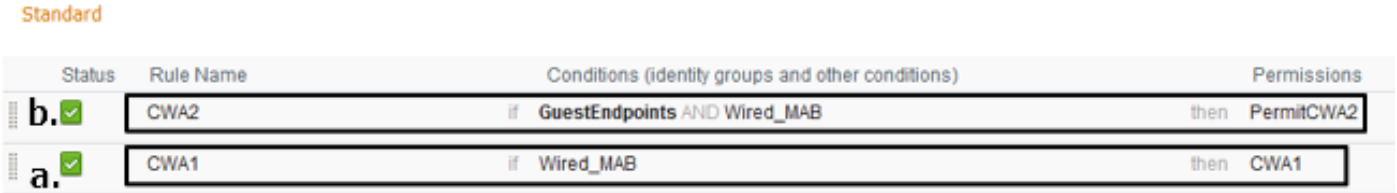


a.ネットワークデバイス プロファイル: NADs から来る認証要求だけこの許可 プロファイルという結果にこのプロファイルに終るかもしれません割り当てました

b. VLAN の 設定: この VLAN にクライアント ポートを割り当てた後、ユーザは規則的な DHCPサーバから IP アドレスを得る必要があります。

5. ゲスト アクセスのための承認ポリシーを設定して下さい

[Policy] > [Authorization] に移動します。 2 つのポリシーを設定して下さい: ゲスト ポータルの認証の後のユーザアクセスのリダイレクト操作のための 1 つおよび他。



a. 認証方式およびリダイレクト 許可 プロファイルとして最初の承認ポリシー一致によって配線される MAB はその結果割り当てられます。

b. 第 2 承認ポリシーはセッション属性（使用例 = ゲスト フロー/ゲスト タイプ外部 AD グループ AD を使用して認証されるゲストユーザなら）にまたはエンドポイント属性（エンドポイント識別グループ）に基づいていることができます。 デバイス 登録はエンドポイント識別グループを使用するためにゲスト ポータルで有効に なる必要があります。

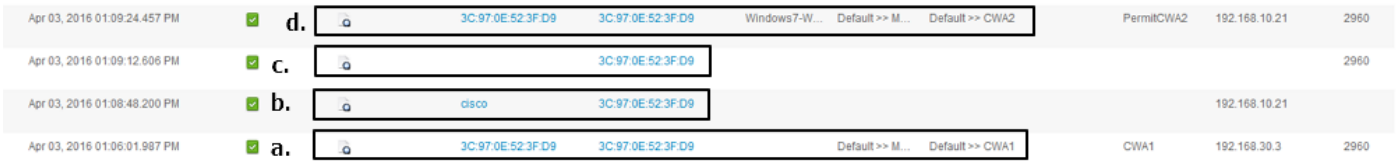
NAD を設定して下さい

Ciscoスイッチはインターフェイスの MAB のために設定され、COA サポートがあります。

> **注** Cisco Technical Assistance Center （ TAC ）はサード パーティ NADs の設定のためのサポートを提供しません。

確認

ISE オペレーション > Radius Livelog のこのように正常なゲスト フローな:



a. これは最初の MAB 認証です。 リダイレクトの許可 プロファイルはその結果選択されます。

b. これはゲスト認証です。 CoA は必要であるかどうか決定するためにこの操作 ISE がポリシー再評価をした後。

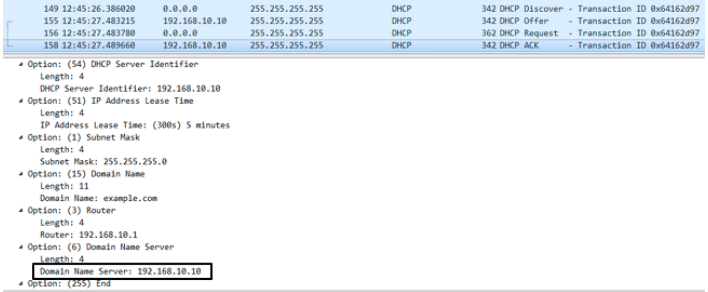
c. CoA は正常に完了しました。

D. これは第 2 MAB 認証です。 ゲスト アクセスのための許可 プロファイルはその結果選択されます。

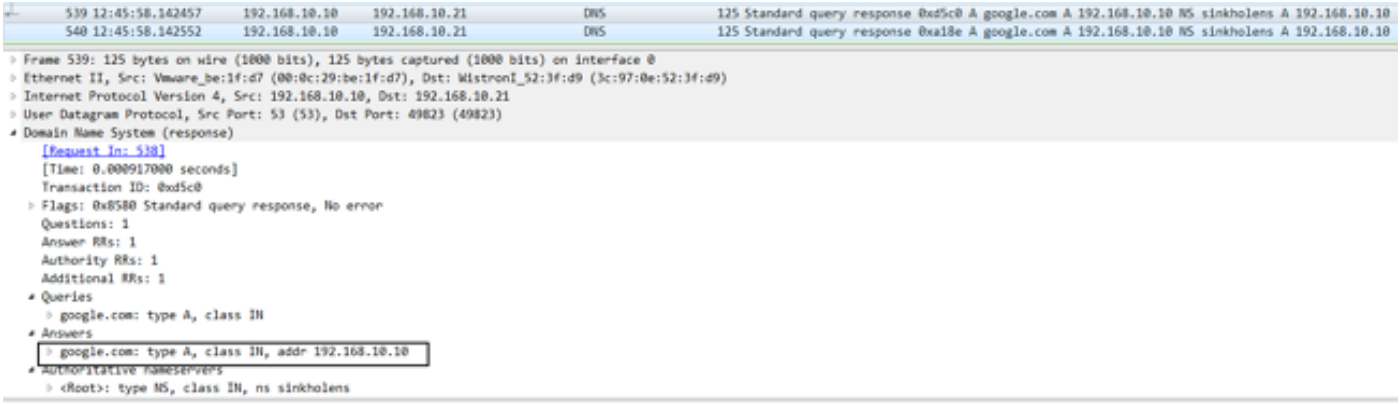
トラブルシューティング

IP アドレスがクライアントに正しく割り当てられるかどうか確認して下さい。 これはクライアントまたは ISE のパケットキャプチャの収集によって実行することができます。

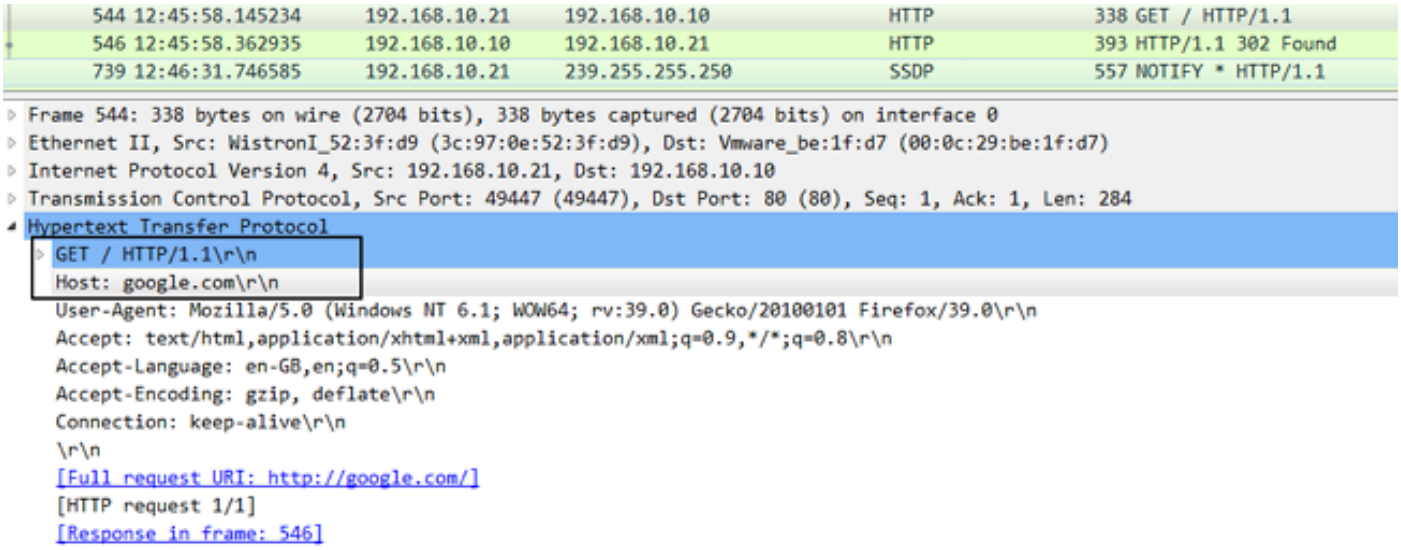
クライアントからのこのキャプチャは ISE と DNS IP の正常な DHCP ハンドシェイクに同じを示します。



ISE が DNS シンクホールとしてきちんと機能しているかどうか確認して下さい。 パケットキャプチャは助けることができます要求が ISE に行っているかどうか、そして確認を ISE が自身の IP アドレスとそれに応答すれば:



HTTP リダイレクトがきちんとはたらくかどうか確認して下さい。 それがリソース IP アドレスを得た、ISE への TCP 接続を確立する後、クライアントは ISE に HTTP GET 要求を送信 します。 これはクライアント側パケットキャプチャで確認することができます:



同時に、ISE はかどうかこのクライアントのために存在 するあらゆるセッション確認しました。 ISE のセッション ルックアップのこのプロセスはチェックインされた prrt 管理 ログである場合もあります:

セッション ルックアップの後で、ISE は HTTP 302 応答のクライアントにリダイレクト URL を戻します: