NAC（CCA）4.x： LDAP を使用して、ユーザを特定のロールにマッピングする設定例

目次

概要

このドキュメントでは、ネットワーク アドミッション コントロール（NAC）アプライアンスまたは Cisco Clean Access（CCA）の特定のロールにユーザをマッピングするための Lightweight Directory Access Protocol（LDAP）について説明します。

Cisco NAC アプライアンス（旧称 Cisco Clean Access）は、導入が容易な NAC 製品で、ネットワーク コンピューティング リソースにアクセスするすべてのデバイスでセキュリティ ポリシーのコンプライアンスを強化するために、ネットワーク インフラストラクチャを使用します。 ネットワーク管理者は NAC アプライアンスを使用して、有線、ワイヤレス、およびリモートでアクセスするユーザおよびそのマシンを、ネットワークにアクセスする前に認証、承認、評価、および修復することができます。 NAC アプライアンスは、ラップトップ、IP 電話、ゲーム コンソールなどのネットワーク デバイスがネットワークのセキュリティ ポリシーに準拠しているかどうかを確認し、ネットワークへのアクセスを許可する前に、脆弱性を修復します。

前提条件

要件

このドキュメントでは、CCA Manager、CCA Server、LDAP サーバがインストールされ正常に動作していることを前提としています。

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 NAC アプライアンス 3300 シリーズ：Clean Access Manager 4.0
- Cisco NAC アプライアンス 3300 シリーズ：Clean Access Server 4.0

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

バックエンドの Active Directory に対する認証

Clean Access Manager の認証プロバイダー タイプのいくつかは、Active Directory（AD）サーバに対するユーザ認証に使用できます。Active Directory サーバは Microsoft 社独自のディレクトリ サービスです。 プロバイダー タイプには、Windows NT（NTLM）、Kerberos、LDAP（優先）があります。

LDAP を使用して AD に接続する場合、通常は管理者権限または基本ユーザの特権を有するアカウントの DN に Search(Admin) Full DN（識別名）を設定する必要があります。 最初の共通名（CN）エントリは、AD 管理者、または読み取り権限を有するユーザである必要があります。 検索フィルタ SAMAccountName は、デフォルト AD スキーマのユーザ ログイン名です。

AD/LDAP の設定例

ここでは、LDAP を使用して、バックエンドの Active Directory との通信を設定する手順を示します。

1. Active Directory Users and Computers 内で Domain Admin ユーザを作成します。 このユーザを Users フォルダに入れます。
2. Active Directory Users and Computers の [Actions] メニューから [Find] を選択します。検索結果に、作成されたユーザの [Group Membership] カラムが表示されていることを確認します。 検索結果には、そのユーザ、および Active Directory 内で関連付けられているグループ メンバーシップが表示されるはずです。 この情報は、Clean Access Manager への転送に必要となります。
3. Clean Access Manager の Web コンソールから、[User Management] > [Auth Servers] > [New Server] フォームに進みます。
4. [Server Type] として [LDAP] を選択します。
5. [Search(Admin) Full DN] フィールドと [Search Base Context] フィールドに、Active Directory Users and Computers での検索結果を入力します。
6. 以下のフィールドはいずれも、この認証サーバを CAM 内で適切に設定するために必要なフィールドです。[ServerURL]： ldap://192.168.137.10:389：ドメイン コントローラの IP アドレスおよび LDAP リスニング ポート。[Search(Admin) Full DN]： CN=sheldon muir, CN=Users, DC=domainname, DC=com[Search Base Context]： DC=domainname, DC=com[Default Role]： 認証後にユーザに割り当てるデフォルト ロールを選択します。**説明**： 参考情報。[Provider Name]： CAM のユーザ ページの設定に使用される LDAP サーバ

の名前。[Search Password]： sheldon muir のドメイン パスワード[Search Filter]：SAMAccountName=$user$

7. [Add Server] をクリックします。この時点で、認証テストが機能する必要があります。
8. 認証テストを行うには、以下の手順に従います。[User Management] > [Auth Servers] > [Auth Test] タブの [Provider] リストから、証明書をテストするプロバイダーを選択します。目的のプロバイダーが表示されない場合は、そのプロバイダーが [List of Servers] タブに適切に設定されていることを確認してください。ユーザのユーザ名とパスワード、および必要に応じて LAN ID 値を入力します。[Authenticate] をクリックします。ウィンドウの下部にテスト結果が表示されます。**Authentication Successful**：任意のプロバイダー タイプに対して、 認証テストに成功した場合、[Result] に「Authentication successful」、[Role] にユーザのロールが表示されます。LDAP/RADIUS サーバの場合、認証に成功してマッピング ルールが設定されると、認証サーバ（LDAP/RADIUS）が属性/値を返す場合にはマッピング ルールに指定されている属性/値も表示されます。 次に、例を示します。`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **Authentication Failed**：認証に失敗した場合、Authentication failed の結果とともに以下のメッセージが表示されます。

属性または VLAN ID を使用したユーザとロールのマッピング

[Mapping Rules] フォームを使用し、以下のパラメータに基づいてユーザをユーザ ロールにマッピングできます。

- CAS の非信頼側からのユーザ トラフィックの VLAN ID（すべての認証サーバ タイプ）
- LDAP および RADIUS 認証サーバからの認証属性（および Cisco VPN コンセントレータからの RADIUS 属性）

たとえば、同じ IP サブネットに、ネットワーク アクセス権限の異なる 2 種類のユーザ集合（無線の従業員と学生など）がいる場合、LDAP サーバからの属性を使用して、各ユーザ集合を特定のユーザ ロールにマッピングできます。 さらに、一方のロールに対してはネットワーク アクセスを許可し、他方のロールに対してはネットワーク アクセスを拒否するトラフィック ポリシーを作成できます

Cisco NAC アプライアンスは、次に示されている順序でマッピングを実行します。

Cisco NAC アプライアンスでは、Kerberos、LDAP、RADIUS の認証サーバのマッピング ルールを定義する際に、複雑なブール式を指定できます。 マッピング ルールは条件で構成されており、ブール式を使用して複数のユーザ属性や複数の VLAN ID を組み合わせることにより、ユーザとユーザ ロールをマッピングできます。 マッピング ルールは VLAN ID の範囲に対して作成できます。また、属性の照合では、大文字と小文字は区別されません。 これにより、複数の条件を柔軟に構成してマッピング ルールを作ることができます。

マッピング ルールは、認証プロバイダー タイプ、ルール式、ユーザをマッピングするユーザ ロールで構成されます。 ルール式は、特定のユーザ ロールとのマッピングのためにユーザ パラメータが一致しなければならない条件および条件の組み合わせで構成されます。 条件は、条件タイプ、ソース属性名、演算子、および特定の属性が照合される属性値で構成されます。

マッピング ルールを作成するには、まずルール式を設定するための条件を追加（保存）します。ルール式を作成したら、特定のユーザ ロールの認証サーバにそのマッピング ルールを追加できます。

カスケード形式のマッピング ルールを作成することも可能です。 ソースに複数のマッピング ルールがある場合、これらのルールは、マッピング ルール リストに表示されている順番に評価されます。 評価結果が最初に True になったマッピング ルールのロールが使用されます。 当てはまるルールが見つかれば、その他のルールはテストされません。 どのルールも True にならない場合、その認証ソースのデフォルト ロールが使用されます。

マッピング ルールの設定

次の手順を実行します。

1. [User Management] > [Auth Servers] > [Mapping Rules] の順番に進み、認証サーバの [Add Mapping Rule] リンクをクリックします。[Add Mapping Rule] フォームが表示されます。
2. マッピング ルールの条件を設定する（A）：[Provider Name]：この認証サーバ タイプ用の [Mapping Rules] フォームのフィールドを設定します。 たとえば、Kerberos、Windows NT、Windows NetBIOS SSO、および S/Ident の認証サーバ タイプの場合、このフォームで設定できるのは VLAN ID マッピング ルールだけです。 RADIUS、LDAP、および Cisco VPN SSO 認証タイプの場合は、このフォームで VLAN ID または属性のマッピング ルールを設定できます。[Condition Type]： マッピング ルールを追加する前に、まず条件を設定し、追加します（図の手順**A** ）。 ドロップダウン メニューからこれらのいずれかを選択し、[Condition] フォームのフィールドを設定します。[Attribute]：LDAP、RADIUS、Cisco VPN SSO の認証プロバイダーの場合のみです。VLAN ID：すべての認証サーバ タイプです。VLAN ID の条件タイプの場合（図を参照）、このフィールドは [Property Name]と 呼ばれます。 デフォルトでは、「VLAN ID」の値で埋められています（編集できないようになっています）。[Attribute Name]：LDAP サーバの場合（図を参照）、[Attribute Name] は、テスト対象のソース属性を入力するテキスト フィールドです。 条件の作成で **equals ignore case** 演算子を選択していない場合、この名前を、認証ソースから渡される属性名と一致させる必要があります（大文字と小文字が区別されます）。[Attribute Value]：ソースの [Attribute Name].に対してテストされる値を入力します。[Operator (Attribute)]：ソース属性の文字列のテストを定義する演算子を選択します。**equals**：[Attribute Name]の値が [Attribute Value] と一致する場合に True になります。**not equals**：[Attribute Name]の値が [Attribute Value] と一致しない場合に True になります。**contains**：[Attribute Name] の値が [Attribute Value] を含む場合に True になります。**start with**：[Attribute Name]の値が [Attribute Value] で始まる場合に True になります。**end with**：[Attribute Name]の値が [Attribute Value] で終わる場合に True になります。**equals ignore case**：[Attribute Name]の値が [Attribute Value] と一致する場合に True になります。 大文字と小文字は区別されません。[Operator（VLAN ID）]：[Condition Type] として VLAN ID を選択した場合は、整数 VLAN ID に対するテスト条件の定義に使用する演算子を以下の中から 1 つ選択します。**equals**：VLAN ID が [Property Value] フィールドの VLAN ID と一致する場合に True になります。**not equals**：VLAN ID が [Property Value] フィールドの VLAN ID と一致しない場合に True になります。**belongs to**：VLAN ID が [Property Value] フィールドに設定した値の範囲内に含まれる場合に True になります。 値は、複数のカンマで区切られた VLAN ID です。 VLAN ID の範囲は、[2,5,7,100-128,556-520] のように、ハイフン（-）で指定できます。 入力できるのは、整数だけです。文字列は入力できません。 カッコの入力は任意です。**例：**[Add Condition (Save Condition)]：条件の設定を確認してから、[Add Condition] をクリックし、その条件をルール表現に追加します（クリックしないと設定が保存されません）。
3. マッピング ルールをロールに追加する（B）： 条件を設定し追加した後にマッピング ルールを追加します（図の手順 **B** ）。[Role Name]：条件を少なくとも 1 つ追加したら、そのマッピングを適用するユーザ ロールをドロップダウン メニューから選択します。[Priority]：ド

ロップダウン メニューからマッピング ルールのテストの順番を決めるプライオリティを選択します。 最初に True であると評価されたルールがユーザへのロール割り当てに使用されます。[Rule Expression]：そのマッピング ルール用の条件ステートメントの設定に役立つように、追加される最後の条件の内容がこのフィールドに表示されます。 条件を追加したら、すべての条件をルールに保存するために、[Add Mapping Rule] をクリックしなければなりません。[Description]：そのマッピング ルールの説明です（任意）。[Add Mapping（Save Mapping）]：条件の追加が完了したら、このボタンをクリックして、そのロールのマッピング ルールを作成します。 特定のロールごとにマッピングを追加または保存しないと、行った設定および作成した条件は保存されません。

マッピング ルールの編集

- [Priority]：設定後にマッピング ルールのプライオリティを変更する場合は、[User Management] > [Auth Servers] > [List of Servers] の該当エントリの横にある上/下矢印をクリックします。 プライオリティによって、そのルールのテストの順番が決まります。 最初に True であると評価されたルールがユーザへのロール割り当てに使用されます。
- [Edit]：マッピング ルールの変更またはルールからの条件の削除を行うには、そのルールの横にある [Edit] ボタンをクリックします。 複合条件を変更する場合、その下にある条件（それより後に作成されたもの）は表示されません。 これは、ループを回避するためです。
- [Delete]：個々のマッピング ルールを削除するには、認証サーバのマッピング ルール エントリの横にある [Delete] ボタンをクリックします。 マッピング ルール内の条件を削除する場合は、[Edit Mapping Rule] フォーム上の条件の横にある [Delete] ボタンをクリックします。 複合ステートメント内の別のルールに依存している条件は、削除できません。 個々の条件を削除するためには、まず複合条件を削除する必要があります。

トラブルシューティング

AD ユーザの CCA ユーザ ロールへのマッピングが機能しない場合は、Attribute Names= memberof、Operator=contains、Attribute Value=（グループ名）属性に基づいてユーザをロールにマッピングしていることを確認します。

関連情報

- Cisco NAC アプライアンスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems