ACS 5.x： AD のグループ メンバーシップに基づく TACACS+ 認証およびコマンド認可の設定例

目次

概要

この資料はユーザの AD 団体会員に基づいて Cisco Secure Access Control System （ ACS ） 5.x およびそれ以降で TACACS+ 認証およびコマンド許可を設定する例を提供したものです。 ACS は外部 ID ストアとしてユーザ、マシン、グループ、および属性を保存するために Microsoft Active Directory (AD ）を使用します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ACS 5.x は望ましい AD ドメインに十分に統合。 ACS が望ましい AD ドメインと統合場合、ACS 5.x およびそれ以降を参照して下さい: 詳細については Microsoft Active Directory 設定例の統合 統合 タスクを行うため。

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 Secure ACS 5.3
- Cisco IOS ® ソフトウェア リリース 12.2(44)SE6。**注:** この設定はすべての Cisco IOSデバイスですることができます。

- Microsoft Windows Server 2003 ドメイン

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。

設定

認証 および 権限のための設定 ACS 5.x

認証 および 権限のための ACS 5.x の設定を始める前に、ACS は Microsoft AD と正常に統合必要があります。 ACS が望ましい AD ドメインと統合場合、ACS 5.x およびそれ以降を参照して下さい: 詳細については Microsoft Active Directory 設定例の統合 統合 タスクを行うため。

このセクションでは、2 組の異なるコマンド セットに 2 つの AD グループおよび 2 つのシェル プロファイルを、1 および Cisco IOSデバイスの制限されたアクセスとのフル アクセスとの他マッピング します。

1. Admin 資格情報を使用して ACS GUI にログイン して下さい。
2. 『Users』 を選択 すれば**識別は > 外部識別保存し、> アクティブ ディレクトリ 接続ステータスが接続される**ように表示されること ACS が望ましいドメインに加入したまたことを確認します**保存し。Groups タブを**『Directory』 をクリック して下さい。
3. [Select] をクリックします。
4. シェル プロファイルにマッピング される必要があり、設定のより遅い一部のセットを命じるグループを選択して下さい。 [OK] をクリックします。
5. [Save Changes] をクリックします。
6. **アクセスポリシー > アクセスを保守し、> サービス セレクション ルール**示します TACACS+ 認証を処理するアクセス サービスを選択して下さい。 この例では、それは**デフォルト デバイ Admin** です。
7. **アクセスポリシー > アクセスを保守し、> デフォルト デバイ Admin > 識別識別出典**の隣で『SELECT』 をクリック します選択して下さい。
8. [AD1] を選択し、[OK] をクリックします。
9. [Save Changes] をクリックします。
10. **アクセスポリシー > アクセス サービス > デフォルト デバイス Admin > 許可を**選択し、『Customize』 をクリック して下さい。
11. 次に **AD1:ExternalGroups を利用可能**から**カスタマイズ状態**の**選択したセクション**にコピーし、**シェル プロファイルを**移動し、**利用可能**から**カスタマイズ結果**の**選択したセクションにセットを命じて下さい**。 ここで、[OK] をクリックします。
12. 新しいルールを作成するには、[Create] をクリックします。
13. **AD1:ExternalGroups** 状態で『SELECT』 をクリック して下さい。
14. Cisco IOSデバイスでフルアクセスを提供したいと思うことグループを選択して下さい。 [OK] をクリックします。
15. シェル Profile フィールドで『SELECT』 をクリック して下さい。
16. フル アクセス ユーザ向けの新しい**シェル プロファイルを**作成するために『Create』 をク

リック して下さい。
17. General タブの名前および Description (optional) を提供し、コモン タスク タブをクリックして下さい。
18. 値 15 を用いるスタティックにデフォルト特権および最大特権を変更して下さい。 [Submit] をクリックします。
19. この場合新しく作成されたフル アクセス シェル プロファイル (この例の全特権) を選択し、『OK』 をクリック して下さい。
20. コマンド セット フィールドで『SELECT』 をクリック して下さい。
21. フル アクセス ユーザ向けに設定 される新しいコマンドを作成するために『Create』 をクリック して下さい。
22. 名前をつけ、下記の表にない割り当ての隣のチェックボックスがあらゆるコマンド チェックされるようにして下さい。 [Submit] をクリックします。注: コマンド セットに関する詳細についてはデバイス 管理のための作成し、複写し、Editing コマンド セットを参照して下さい。
23. [OK] をクリックします。
24. [OK] をクリックします。 これは Rule-1 の設定を完了します。
25. 制限されたアクセス ユーザ向けの新しいルールを作成するために『Create』 をクリック して下さい。
26. AD1:ExternalGroups を選択し、『SELECT』 をクリック して下さい。
27. 制限されたアクセスをに提供し、『OK』 をクリック したいと思うことグループ (または) グループを選択して下さい。
28. シェル Profile フィールドで『SELECT』 をクリック して下さい。
29. 制限されたアクセスのための新しいシェル プロファイルを作成するために『Create』 をクリック して下さい。
30. General タブの名前および Description (optional) を提供し、コモン タスク タブをクリックして下さい。
31. 値 1 および 15 を用いるスタティックにデフォルト特権および最大特権をそれぞれ変更して下さい。 [Submit] をクリックします。
32. [OK] をクリックします。
33. コマンド セット フィールドで『SELECT』 をクリック して下さい。
34. 制限されたアクセス グループのために設定 される新しいコマンドを作成するために『Create』 をクリック して下さい。
35. 名前をつけ、下記の表にない割り当ての隣のチェックボックスがあらゆるコマンド選択されないようにして下さい。 タイプの後で show コマンドだけ制限されたアクセス グループのユーザ向けに許可されるように示し、指揮 班で提供されるスペースで選択しますグラント セクションの許可を『Add』 をクリック して下さい。
36. 同様に Add の使用の制限されたアクセス グループのユーザを可能にされる他のどのコマンドも追加して下さい。 [Submit] をクリックします。注: コマンド セットに関する詳細についてはデバイス 管理のための作成し、複写し、Editing コマンド セットを参照して下さい。
37. [OK] をクリックします。
38. [OK] をクリックします。
39. [Save Changes] をクリックします。
40. ACS の AAA クライアントとして Cisco IOSデバイスを追加するために『Create』 をクリック して下さい。
41. 名前を、IP アドレス、共有秘密 TACACS+ につけ、『SUBMIT』 をクリック して下さい。

認証 および 権限のための Cisco IOSデバイスを設定して下さい

認証 および 権限のための Cisco IOSデバイスおよび ACS を設定するためにこれらのステップを完了して下さい。

1. ここに示されているように **username コマンド**でフォールバックのための完全な特権で口ーカルユーザを作成して下さい:`username admin privilege 15 password 0 cisco123!`
2. ACS の IP アドレスを AAA を有効に し、TACACSサーバとして ACS 5.x を追加するために提供します。`aaa new-model`
   `tacacs-server host 192.168.26.51 key cisco123`**注: キーは**共有されると-この Cisco IOSデバイスに ACS で提供されるシークレット 一致する必要があります。
3. 次に示すように、aaa コマンド により、TACACS サーバの到達可能性をテストします。
   ```
   test aaa group tacacs+ user1 xxxxx legacy
   Attempting authentication test to server-group tacacs+ using tacacs+
   User was successfully authenticated.
   ```
   前のコマンドの出力では、TACACS サーバが到達可能であり、ユーザが正常に認証されたことを示しています。**注:** User1 およびパスワード xxx は AD に属します。 テストが失敗したように共有されるして下さい-前の手順で提供されるシークレットは正しいです。
4. ログオンを設定し、認証を有効に し、次にここに示されているように Exec およびコマンド許可を使用して下さい:
   ```
   aaa authentication login default group tacacs+ local
   aaa authentication enable default group tacacs+ enable
   aaa authorization exec default group tacacs+ local
   aaa authorization commands 0 default group tacacs+ local
   aaa authorization commands 1 default group tacacs+ local
   aaa authorization commands 15 default group tacacs+ local
   aaa authorization config-commands
   ```
   注: それぞれ TACACSサーバが到達不能なら口ーカルおよび Enable キーワードは Cisco IOS 口ーカルユーザおよび enable secret へのフォールバックのために使用されます。

確認

認証 および 権限を確認するために Telnet によって Cisco IOSデバイスに口グインして下さい。

1. AD のフル アクセス グループに属する user1 として Cisco IOSデバイスに Telnet で接続して下さい。 ネットワーク Admin グループは ACS で設定 される マッピング された全特権シェル プロファイルおよびフル アクセス コマンドの AD のグループです。 コマンドをフル アクセスがあることを確認するために実行することを試みて下さい。
2. と同時に AD の制限されたアクセス グループに属する user2 が Cisco IOSデバイスに Telnet で接続します。 （**ネットワークメンテナンス チーム** グループは ACS で**設定 される** マッピング された限られ**特権 シェル プロファイル**および示**アクセス コマンド**の） AD のグループです。 設定 される示アクセス コマンドで述べられる物以外コマンドを実行することを試みる場合 user2 に制限されたアクセスがあることを示す 得る必要があります。
3. ACS GUI に口グインし、**モニタリング**を起動させ、**ビューアを報告します。 AAAプロトコル > TACACS+Authorization を** user1 および user2 によって実行された アクティビティを確認するために選択して下さい。

関連情報

- Cisco Secure Access Control System

- テクニカルサポートとドキュメント - Cisco Systems