ACS 5.x 以降： Microsoft Active Directory との統合の設定例

目次

概要

このドキュメントでは、Microsoft Active Directory と Cisco Secure Access Control System（ACS）5.x 以降を統合するための設定例を紹介します。 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。 ACS は、AD に対してこれらのリソースを認証します。

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。

- 使用する Windows Active Directory ドメインはフル構成で操作可能である必要があります。
- これらは ACS 5.x.でサポートされている、Microsoft Windows Server 2003 ドメイン、Microsoft Windows Server 2008 ドメイン、または Microsoft Windows Server 2008 R2 ドメインを使用します。**注:** Microsoft Windows Server 2008 R2 ドメインの ACS との統合は、ACS 5.2 以降でサポートされています。

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 Secure ACS 5.3
- 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。

背景説明

Windows Active Directory は日常的なネットワークの使用における複数の機能を提供します。 ACS 5.x の AD との統合により、既存の AD ユーザ、マシン、グループ マッピングを使用できます。

AD と統合された ACS 5.x では、次の機能を提供します：

1. マシン認証
2. 許可のための属性取得
3. EAP-TLS 認証のための証明書取得
4. ユーザとマシン アカウントの制限
5. マシン アクセス制限
6. ダイヤルイン アクセス権の確認
7. ダイヤルイン ユーザのコールバック オプション
8. ダイヤルイン サポートの属性

設定

ACS 5.x Application Deployment Engine（ADE-OS）の設定

AD に ACS 5.x を統合する前に、ACS の**タイムゾーンおよび日付と時間**が AD プライマリ ドメイン コントローラのものと必ず一致するようにします。 また、ACS 5.x.のドメイン ネームを解決するには、ACS の DNS サーバを定義します。 ACS 5.x Application Deployment Engine（ADE-OS）を設定するには、次の手順を実行してください：

1. ACS アプライアンスに SSH で接続して CLI クレデンシャルを入力します。
2. ドメイン コントローラのタイムゾーンに一致するように ACS の**タイムゾーン**を設定するために、次に示すようにコンフィギュレーション モードで **clock timezone コマンド**を実行します。

   `clock timezone Asia/Kolkata` **注:** Asia/Kolkata は、このドキュメントで使用されたタイムゾーンです。 EXEC モードで **show timezones コマンドを実行すると指定したタイムゾーンを確認できます。**
3. AD のドメイン コントローラがネットワークに存在する NTP サーバと同期する場合は、ACS で同じ NTP サーバを使用することを強く推奨します。 NTP サーバがない場合は、**ステップ 4** に進んでください。 次は、NTP サーバを設定する手順です：NTP サーバは、次に示すように設定モードで **ntp server <ip address of the NTP server>** コマンドを実行すること

により設定できます。`ntp server 192.168.26.55`
`The NTP server was modified.`
`If this action resulted in a clock modification, you must restart ACS.`NTP 設定の詳細については、『ACS 5.x: NTP のサーバとの Cisco ACS の同期の設定例』を参照してください。

4. 手動で日時を設定するには、**EXEC モード**で **clock set コマンド**を使用します。 次に例を示します。`clock set Jun 8 10:36:00 2012`
```
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```
5. ここで **show clock コマンド**を使用して**タイムゾーンおよび日時を確認します。** show clock コマンドの出力を次に示します：`acs51/admin# show clock Fri Jun 8 10:36:05 IST 2012`
6. 次に示すように、**設定モードで <ip name-server <ip address of the DNS>** コマンドの実行により ACS の DNS を設定します：`ip name-server 192.168.26.55`**注:** DNS の IP アドレスは Windows のドメイン管理者によって提供されます。
7. 次に示すように、ドメイン名の到達可能性を検証するには、**nslookup <domain name>** コマンドを実行します。`acs51/admin#nslookup MCS55.com Trying "MCS55.com" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; QUESTION SECTION: ;MCS55.com. IN ANY ;; ANSWER SECTION: MCS55.com. 600 IN A 192.168.26.55 MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com. MCS55.com. 3600 IN SOA admin-zq2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ;; ADDITIONAL SECTION: admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55 Received 136 bytes from 192.168.26.55#53 in 0 ms` **注: ANSWER SECTION** が空の場合、Windows のドメイン管理者に問い合わせてドメインの正しい DNS サーバを確認してください。
8. 次に示すように、ACS で **DOMAIN-NAME** を設定するには、**ip domain-name <domain name>** コマンドを実行します。`ip domain-name MCS55.com`
9. 次に示すように、ACS の**ホスト名**を設定するには、**hostname <hostname>** コマンドを実行します：`hostname acs51`**注:** NETBIOS の制限により、ACS ホスト名は 15 文字以下にする必要があります。
10. ACS に設定を保存するには、**write memory コマンド**を実行します。

ACS 5.x の AD への結合

ACS5.x を AD に結合させるには、次の手順を実行してください：

1. [Users and Identity Stores] > [External Identity Stores] > [Active Directory] を選択し、ドメイン名、AD のアカウント（ユーザ名）とパスワードを指定し、[Test Connection] をクリックします。**注:** ACS でのドメイン アクセスに必要な AD のアカウントには、次のいずれかが必要です：対応するドメインのドメイン ユーザ権限にワークステーションを追加。ACS マシンのアカウントが ACS マシンをドメインに追加する前に作成される対象のコンピュータ コンテナに対して、コンピュータ オブジェクトを作成する権限またはコンピュータ オブジェクトを削除する権限。**注:** ACS アカウントのロックアウト ポリシーをディセーブルにし、不正なパスワードがこのアカウントに使用された場合に、管理者にアラートを送信するように AD インフラストラクチャを設定することを推奨します。 これは、誤ったパスワードを入力した場合、ACS が必要なときにマシン アカウントを作成および変更しないため、すべての

認証が拒否されるためです。**注:** AD ドメインに ACS を追加する Windows AD アカウントは、独自の組織単位（OU）に作成できます。 この AD アカウントは、作成時または後で独自の OU に置かれ、アプライアンス名が AD アカウント名に一致する必要があります。
2. このスクリーン ショットは、AD への接続テストが正常であることを示しています。 次に [OK] をクリックします。**注:** Centrify 設定は、AD のドメインを持つ ACS 接続をテストする間、サーバから応答が遅くなると影響を受けるか、場合によっては接続解除されます。 ただし、他のアプリケーションでは正常に動作します。
3. ACS に AD を結合するには、[Save Changes]をクリックします。
4. ACS が正常に AD のドメインを結合する場合、接続の状態が表示されます。**注:** AD ID ストアを設定すると、ACS は以下も作成します。2 個の属性を持つ AD ID ストア用の新しいディクショナリ： [Directory Attributes] ページから取得した属性の ExternalGroups ともう 1 個の属性。新しい属性 IdentityAccessRestricted。 この属性のカスタム条件は手動で作成できます。ExternalGroup 属性からのグループ マッピングに対するカスタム条件である カスタム条件名「AD1:ExternalGroups」、および [Directory Attributes] ページで選択された各属性に対する別のカスタム条件（ たとえば「AD1:cn」 ）。

アクセス サービスの設定

ACS が新しく設定された AD の統合を使用できるようにアクセス サービスの設定を完了するには、次の手順を実行します。

1. ユーザを AD から認証するサービスを選択して、[Identity] をクリックします。 ここで [Identity Source] フィールドの隣の [Select]をクリックします。
2. [AD1] を選択し、[OK] をクリックします。
3. [Save Changes] をクリックします。

確認

AD の認証を確認するには、AD のクレデンシャルを使用して NAS からの認証要求を送信します。 NAS が ACS で設定され、要求が前のセクションで設定したアクセス サービスによって処理されることを確認します。

1. NAS ログから ACS GUI への認証の成功後に、[Monitoring and Reports] > [AAA Protocol] > [TACACS+Authenticationn] を選択します。 リストから正常な認証を識別し、次に示すように虫眼鏡の形の記号をオンにします。
2. ACS が AD に認証要求を送信したことをステップから確認できます。

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