ISE 1.3 AD認証が「Insufficient Privilege to Fetch Token Groups」エラーで失敗する

内容

概要

このドキュメントでは、ISEマシンのアカウント権限の不足によるエラーコード「24371」による、Active Directory(AD)に対するIdentity Services Engine(ISE)認証の失敗のソリューションについて説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISEの設定とトラブルシューティング
- Microsoft AD

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いています。

- ISEバージョン1.3.0.876
- Microsoft ADバージョン2008 R2

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

エラー「24371」が原因でAD認証が失敗する

ISE 1.3以降では、ADに対する認証がエラー「24371」で失敗する可能性があります。 障害の詳細な認証レポートには、次のような手順があります。

```
15036     Evaluating Authorization Policy
24432     Looking up user in Active Directory - CISCO_LAB
24371     The ISE machine account does not have the required privileges to fetch groups. -
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
24371     The ISE machine account does not have the required privileges to fetch groups. -
CISCO_LAB 15048     Queried PIP - CISCO_LAB.ExternalGroups
```

ADのステータスがjoined and connectedと表示され、必要なADグループがISE設定に正しく追加されています。

解決方法

ADのISEマシンアカウントの権限の変更

詳細認証レポートのエラーは、Active Directory上のISEのマシンアカウントに、トークングループを取得するための十分な権限がないことを意味します。

> **注**：ISEマシンアカウントに正しい権限を付与できないため、修正はAD側で実行されます。この後、ISEをADに切断/再接続する必要がある場合があります。

次の例に示すように、**dsacls**コマンドを使用して、マシンアカウントの現在の権限を確認できます。

```
Open a command prompt on your AD with administrator privilege.
The dsquery command can be used to find the Fully Qualified Domain Name (FQDN) of the ISE.
C:\Users\admin> dsquery computer -name lab-ise1  //here lab-ise1 is the hostname of the ISE
"CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local"

The dsacls command can now be used to find the privileges assigned to the machine account
C:\Windows\system32> dsacls "CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local" >>
C:\dsacl_output.txt
```

出力は長いため、テキストファイル**dsacl_output.txtにリダイレクトさ**れ、メモ帳などのテキストエディタで正しく開いて表示できます。

アカウントがトークングループを読み取る権限を持っている場合、**dsacl_output.txtファイルに次のエントリがあ**ります。

```
Inherited to user
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY Inherited to group
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY
```

権限がない場合は、次のコマンドを使用して追加できます。

```
C:\Windows\system32>dsacls "CN=Computers,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

FQDNまたは正確なグループが不明な場合は、次のコマンドに従って、ドメインまたは組織単位(OU)に対してこのコマンドを迅速に実行できます。

```
C:\Windows\system32>dsacls "DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
C:\Windows\system32>dsacls "OU=ExampleOU,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

コマンドは、ドメイン全体またはOU内のホストlab-ise1をそれぞれ探します。

コマンド内のグループ名とホスト名の詳細は、配置の対応するグループとISE名に置き換えることを忘れないでください。このコマンドは、ISEマシンアカウントに、トークングループを読み取る権限を付与します。1つのドメインコントローラでのみ実行する必要があり、他のコントローラに自動的に複製する必要があります。

問題は即座に解決できます。ISEに現在接続されているドメインコントローラでコマンドを実行します。

現在のドメインコントローラを表示するには、[Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] > [Select AD join point]に移動します。

関連情報

- その他のアカウント権限に関する情報は、『Active Directory Integration with Cisco ISE 1.3』を参照してください
- Microsoft Technet Link
- テクニカル サポートとドキュメント – Cisco Systems