ISE 1.3 AD 認証が次のエラーを出して失敗しました。「Insufficient Privilege to Fetch Token Groups」

目次

概要

この資料は不十分な ISE コンピューター アカウント特権によって引き起こされるエラー 24371 による Active Directory（AD）に対して失敗する Identity Services Engine（ISE）認証にソリューションを記述したものです。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- ISE 設定およびトラブルシューティング
- Microsoft Active Directory

使用されているコンポーネント

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。

- 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。

問題

エラー 24371 による AD 認証失敗

ISE 1.3 では以上に、認証はエラー 24371 の AD に対して失敗する場合があります。 失敗のための詳しい認証レポートにここに示されているそれらと同じようなステップがあります:

```
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 ステータスはおよび必須 AD グループが ISE 設定に正しく追加されたことを加入され、接続されてことを示します。

解決策

AD の ISE コンピューター アカウントのための修正する権限

詳しい認証レポートのエラーはアクティブ ディレクトリの ISE のコンピューター アカウントに、トークン グループを取出す十分な特権がないことを意味します。

> **注:** 修正は AD 側でそれが ISE コンピューター アカウントに正しい特権を与えられないので行われます。 切る必要がある場合もありましたり/これの後で ISE に AD を再接続します。

コンピューター アカウントの現在の特権はこの例に示すように dsacls を使用して命じますチェックすることができます:

```
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
```

出力はテキスト工ディタで開き、きちんと表示することができるテキスト工ディタのようなテキストファイル dsacl_output.txt に長く、従ってリダイレクトされて。

アカウントにトークン グループを読む権限がある場合 dsacl_output.txt ファイルのこれらのエントリがあります:

```
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
```

権限がない場合、それはこのコマンドを使用して追加することができます:

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

FQDN がまたはグループを知られなければ強要する場合、このコマンドはこれらのコマンドによってドメインか OU のためにすぐに実行することができます:

```
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
```

コマンドはそれぞれ全体のドメインまたは OU のホスト lab-ise1 を探します。

および配備からの ISE 名前対応した グループとコマンドのグループおよびホスト名 詳細を取り替えることを忘れないようにして下さい。 このコマンドは ISE コンピューター アカウントにトークン グループを読むために特権を与えたものです。 それは 1 人のドメインコントローラだけで動作する必要があり、他のコントローラに自動的に複製する必要があります。

問題は現在 ISE で接続されるドメインコントローラのコマンドの実行によってすぐに解決することができます。

現在のドメイン コントローラは **Administration > アイデンティティ管理**の下で **> 外部識別ソースをたどります > アクティブ ディレクトリ > 選定された AD 加入ポイント**表示することができます。

関連情報

- 他のアカウント権限に関する情報は Cisco ISE 1.3 とのアクティブディレクトリ統合で見つけることができます
- Microsoft Technet リンク