

「トークン グループ」 取出す不十分な特権 エラーの ISE 1.3 AD 認証失敗

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用されているコンポーネント](#)

[エラー "24371" による AD 認証失敗](#)

[解決策](#)

[関連情報](#)

概要

この資料は Identity Services Engine (ISE) 認証失敗に不十分な 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コード "24371" による Active Directory (AD) に対して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 を設定し、解決して下さい
- Microsoft AD

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

本書の情報は、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され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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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られないので行われます。切る必要があるかもしれませんが/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 **dsacIs** と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 dsacIs command can now be used to find the privileges assigned to the machine account
C:\Windows\system32> dsacIs "CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local" >>
C:\dsac1_output.txt
```

出力はテキストエディタで開き、きちんと表示することができるテキストエディタのようなテキストファイル **dsac1_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 **dsac1_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 dsacIs command can now be used to find the privileges assigned to the machine account
C:\Windows\system32> dsacIs "CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local" >>
C:\dsac1_output.txt
```

権限がない場合、それはこのコマンドで追加することができます:

```
C:\Windows\system32>dsacIs "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が Organizational Unit (OU) のためにすぐに実行することができます:

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

```
C:\Windows\system32>dscls "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。

問題はすぐに解決することができます。現在 ISE で接続されるドメインコントローラのコマンドを実行して下さい。

現在のドメイン コントローラを表示するために、Administration > アイデンティティ管理に > 外部識別ソースをたどります > Active Directory > 選定された AD 加入ポイント ナビゲートします。

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](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)