ISE 1.3 AD身份驗證失敗，出現「Insufficient Privilege to Fetch Token Groups」錯誤

目錄

簡介

本文檔介紹針對Active Directory(AD)的身份服務引擎(ISE)身份驗證失敗的解決方案，因為ISE電腦帳戶許可權不足導致錯誤代碼「24371」。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 配置ISE並對其進行故障排除
- Microsoft AD

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE版本1.3.0.876
- Microsoft AD版本2008 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

AD身份驗證由於錯誤「24371」而失敗

在ISE 1.3及更高版本中，針對AD的身份驗證可能會失敗，錯誤為「24371」。 失敗的詳細驗證報告的步驟與下面顯示的步驟相似：

```
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狀態顯示已加入和已連線，並且所需的AD組已正確新增到ISE配置中。

解決方案

修改AD上ISE電腦帳戶的許可權

詳細身份驗證報告中的錯誤意味著Active Directory上ISE的電腦帳戶沒有足夠的許可權來獲取令牌組。

> **附註**：修復在AD端完成，因為它不能為ISE電腦帳戶提供正確的許可權。在此之後，您可能需要斷開ISE與AD的連線。

可以使用**dsacls**命令檢查電腦帳戶的當前許可權，如以下示例所示：

```
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
```

輸出很長，因此會重定向到文本檔案**dsacl_output.txt**，該檔案隨後可以在文本編輯器（如記事本）中開啟和正確檢視。

如果帳戶具有讀取令牌組的許可權，則它將在**dsacl_output.txt**檔案中包含以下條目：

```
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
```

如果許可權不存在，則可以使用以下命令新增許可權：

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

如果FQDN或確切的組未知，可以按照以下命令為域或組織單位(OU)快速運行此命令：

```
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
```

命令分別在整個域或OU中查詢主機lab-ise1。

請記得使用部署中的相應組和ISE名稱替換命令中的組和主機名詳細資訊。此命令授予ISE電腦帳戶讀取令牌組的許可權。它只需要在一個域控制器上運行，並且必須自動複製到其他控制器。

該問題可以立即得到解決。對當前在ISE上連線的域控制器運行命令。

要檢視當前域控制器，請導航到**管理>身份管理>外部身份源> Active Directory >選擇AD加入點**。

相關資訊

- 有關其他帳戶許可權的資訊可在Active Directory與思科ISE 1.3的整合中找到
- Microsoft Technet連結
- **技術支援與文件 - Cisco Systems**