ISE 1.3 AD身份验证失败，出现“Insufficient Privilege to Fetch Token Groups”错误

目录

简介

本文档介绍由于ISE计算机帐户权限不足导致的错误代码“24371”，针对Active Directory(AD)的身份服务引擎(ISE)身份验证失败的解决方案。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 配置ISE并排除故障
- Microsoft AD

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE版本1.3.0.876
- Microsoft AD版本2008 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

AD身份验证因错误“24371”失败

在ISE 1.3及更高版本中，身份验证可能会针对AD失败，错误为“24371”。 故障的详细身份验证报告的步骤与下面所示的步骤类似：

```
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状态显示已加入和已连接，并且所需的AD组已正确添加到ISE配置中。

解决方案

修改AD上ISE计算机帐户的权限

详细身份验证报告中的错误意味着活动目录上ISE的计算机帐户没有足够的权限获取令牌组。

> **注意**：修复在AD端完成，因为它无法为ISE计算机帐户提供正确的权限。此后，您可能需要断开ISE与AD的连接/重新连接。

如本示例所示，可使用**dsacls**命令检查计算机帐户的当前**权限**：

```
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
```

输出很长，因此重定向到文本文件**dsacl_output.txt**，然后可以在文本编辑器（如记事本）中正确打开和查看该文本文件。

如果帐户具有读取令牌组的权限，则它将在dsacl_output.txt文件**中包含以下**条目：

```
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
```

如果权限不存在，则可使用以下命令添加：

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

如果FQDN或确切组未知，则可根据以下命令快速为域或组织单位(OU)运行此命令：

```
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
```

这些命令分别在整个域或OU中查找主机lab-ise1。

请记住，将命令中的组和主机名详细信息替换为部署中相应的组和ISE名称。此命令授予ISE计算机

帐户读取令牌组的权限。它只需在一个域控制器上运行，并且必须自动复制到其他控制器。

问题可以立即解决。在ISE上当前连接的域控制器上运行命令。

要查看当前域控制器，请导航至**Administration > Identity Management > External Identity Sources > Active Directory > Select AD join point**。

相关信息

- 有关其他帐户权限的信息可以在与Cisco ISE 1.3的Active Directory集成中找到
- Microsoft Technet链接
- **技术支持和文档 - Cisco Systems**