ISE 1.3 AD与“不足的权限拿来标记组”错误的认证失效

目录

简介

本文描述解决方案给身份服务引擎(ISE)认证失败激活目录(AD)由于错误代码不足的ISE计算机帐户权限造成的"24371"。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 配置并且排除故障ISE
- 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认证发生故障由于错误"24371"

在ISE 1.3以上，认证可以失效与错误"24371"的AD。失败的详细的验证报告有步骤类似于显示的那些此处：

```
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状态显示加入，并且连接和需要的AD组在ISE配置里正确地被添加了。

解决方案

修改ISE计算机帐户的权限在AD

在详细的验证报告的错误暗示ISE计算机帐户在活动目录的，没有足够的权限拿来令牌的组。

> **Note**:因为不能给正确权限到ISE计算机帐户，修正在AD侧完成。您也许需要断开连接/重新连接ISE对AD在此以后。

如此示例所显示，计算机帐户的当前权限可以检查与**dsacls**发出命令：

```
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
```

输出是长并且重定向到在文本编辑可能然后打开和适当地查看的一个文本文件**dsacl_output.txt**，例如记事本。

如果帐户有权限读令牌的组，则将有在**dsacl_output.txt**文件的这些条目：

```
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
```

如果权限不存在，则可以用此命令添加：

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

如果FQDN或苛求组不知道，此命令可以为域或组织单位(OU)迅速运行根据这些命令：

```
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
```

命令寻找在各自整个域或OU的主机lab-ise1。

切记用对应的组和ISE名称替换在命令的组和主机名详细信息从您的部署。此命令授权ISE计算机帐户权限读令牌的组。它在仅一个域控制器需要运行并且必须自动地复制到其他控制器。

可以立即解决问题。运行域控制器在ISE当前连接的on命令。

为了查看当前域控制器，导航对**Administration >身份管理>外部标识来源>活动目录>挑选AD加入点**。

相关信息

- 关于其他帐户权限的信息可以在与思科ISE 1.3的激活目录集中找到
- Microsoft Technet林克
- **技术支持和文档 - Cisco Systems**