Fall de las autenticaciones ISE 1.3 AD con el error: “Privilegio escaso de traer a los grupos simbólicos”

Contenido

Introducción

Este documento describe la solución a las autenticaciones del Identity Services Engine (ISE) que fallan contra el Active Directory (AD) debido al error 24371 causado por los privilegios escasos de la cuenta de equipo ISE.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Configuración y troubleshooting ISE
- Microsoft Active Directory

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.3.0.876 ISE
- R2 de la versión 2008 de Microsoft AD

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Las autenticaciones AD fallan debido al error 24371

En ISE 1.3 y arriba, las autenticaciones pueden fallar contra el AD con el error 24371. El informe detallado de la autenticación para el error tendrá pasos similares a ésos mostrados aquí:

```
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
```

El estatus AD muestra que unido a y conectado y han agregado a los grupos requeridos AD correctamente en la configuración ISE.

Solución

Modifique los permisos para la cuenta de equipo ISE en el AD

El error en el informe detallado de la autenticación implica que la cuenta de equipo del ISE en el Active Directory, no tiene privilegios suficientes de traer a los grupos simbólicos.

> Nota: El arreglo se hace en el lado AD pues no puede dar el privilegio correcto a la cuenta de equipo ISE. Usted puede necesitar desconectar/vuelve a conectar el ISE al AD después de esto.

Los privilegios actuales de la cuenta de equipo se pueden marcar usando los dsacls ordenan tal y como se muestra en de este ejemplo:

```
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
```

La salida es larga y por lo tanto reorientada en un archivo de texto **dsacl_output.txt** que se pueda después abrir y ver correctamente en un editor de textos, tal como libreta.

Si la cuenta tiene permisos para leer a los grupos simbólicos, después tendrá estas entradas en el archivo de **dsacl_output.txt**:

```
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
```

Si los permisos no están presentes, después puede ser agregada usando este comando:

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

Si no conocen el FQDN o al grupo exacto, este comando se puede funcionar con rápidamente para el dominio o el OU según estos comandos:

```
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
```

Los comandos buscan el lab-ise1 del host en el dominio o el OU entero respectivamente.

Recuerde substituir a los detalles del grupo y del nombre del host en los comandos por el grupo correspondiente y el nombre ISE de su despliegue. Este comando concede a cuenta de equipo ISE el privilegio de leer a los grupos simbólicos. Necesita ser ejecutado en un controlador de dominio solamente y debe replicar a otros reguladores automáticamente.

El problema puede ser resuelto inmediatamente funcionando con el comando en el controlador de dominio conectado actualmente en el ISE.

El regulador del dominio actual se puede ver bajo la **administración > Administración de la identidad > las fuentes > Active Directory externos de la identidad > AD selecto se une a la punta.**

Información Relacionada

- La información con respecto a otros permisos de la cuenta se puede encontrar en la integración de Active Directory con Cisco ISE 1.3
- Link de Microsoft Technet