Error en las autenticaciones de ISE 1.3 AD con el error "Privilegio insuficiente para recuperar grupos de tokens"

Contenido

Introducción

Este documento describe la solución para la falla de autenticación de Identity Services Engine (ISE) frente a Active Directory (AD) debido al código de error "24371" causado por privilegios de cuenta de máquina de ISE insuficientes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- Configuración y resolución de problemas de ISE
- AD de Microsoft

Componentes Utilizados

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

- ISE versión 1.3.0.876
- Microsoft AD versión 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Falla en las autenticaciones de AD debido al error "24371"

En ISE 1.3 y superiores, las autenticaciones pueden fallar en el AD con el error "24371". El

informe de autenticación detallado para la falla tiene pasos similares a los que se muestran 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 estado de AD muestra el estado conectado y unido y los grupos AD requeridos se han agregado correctamente en la configuración de ISE.

Solución

Modificar permisos para la cuenta de máquina ISE en AD

El error en el informe de autenticación detallado implica que la cuenta de máquina de ISE en el directorio activo, no tiene privilegios suficientes para obtener grupos de token.

> **Nota:** La corrección se realiza en el lado de AD, ya que no puede dar el privilegio correcto a la cuenta de la máquina ISE. Es posible que deba desconectar/volver a conectar ISE a AD después de esto.

Los privilegios actuales de la cuenta de máquina se pueden verificar con el comando **dsacls** como se muestra en 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
```

El resultado es largo y, por lo tanto, se redirige a un archivo de texto **dsacl_output.txt** que se puede abrir y ver correctamente en un editor de texto, como el bloc de notas.

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

```
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
```

Si los permisos no están presentes, se puede agregar con este comando:

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

Si no se conoce el FQDN o el grupo exacto, este comando se puede ejecutar rápidamente para el dominio o la unidad organizativa (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 host lab-ise1 en todo el dominio u OU respectivamente.

Recuerde reemplazar los detalles del grupo y el nombre de host en los comandos por el grupo correspondiente y el nombre de ISE de su implementación. Este comando otorga a la cuenta de la máquina ISE el privilegio de leer los grupos de tokens. Debe ejecutarse sólo en un controlador de dominio y debe replicarse a otros controladores automáticamente.

El problema puede resolverse inmediatamente. Ejecute el comando en el controlador de dominio conectado actualmente en ISE.

Para ver el controlador de dominio actual, navegue hasta **Administration > Identity Management > External Identity Sources > Active Directory > Select AD Join point**.

Información Relacionada

- Puede encontrar información sobre otros permisos de cuenta en Integración de Active Directory con Cisco ISE 1.3
- Microsoft Technet Link
- **Soporte Técnico y Documentación - Cisco Systems**