Falha das autenticações ISE 1.3 AD com “insuficiente privilégio buscar erro dos grupos simbólicos”

Índice

Introdução

Este documento descreve a solução à falha das autenticações do Identity Services Engine (ISE) contra o diretório ativo (AD) devido ao código de erro "24371" causado por insuficientes privilégios da conta de máquina ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Configurar e pesquise defeitos o ISE
- Microsoft AD

Componentes usados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 1.3.0.876 ISE
- Versão 2008 R2 de Microsoft AD

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

As autenticações AD falham devido ao erro "24371"

Em ISE 1.3 e acima, as autenticações podem falhar contra o AD com erro "24371". O relatório

detalhado da autenticação para a falha tem as etapas similares àquelas mostradas aqui:

```
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
```

O estado AD mostra que juntado e conectado e os grupos exigidos AD estiveram adicionados corretamente na configuração ISE.

Solução

Altere permissões para a conta de máquina ISE no AD

O erro no relatório detalhado da autenticação implica que a conta de máquina do ISE no diretório ativo, não tem privilégios suficientes buscar os grupos simbólicos.

> **Note**: O reparo é feito no lado AD porque não pode dar o privilégio correto à conta de máquina ISE. Você pôde precisar de desligar/reconecta o ISE ao AD após este.

Os privilégios atuais da conta de máquina podem ser verificados com os **dsacls** comandam segundo as indicações deste exemplo:

```
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
```

A saída é longa e consequentemente reorientada em um arquivo de texto **dsacl_output.txt** que possa então ser aberto e visto corretamente em um editor de texto, tal como o bloco de notas.

Se a conta tem permissões ler os grupos simbólicos, a seguir terá estas entradas no arquivo 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
```

Se as permissões não estão atuais, a seguir pode ser adicionada com este comando:

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

Se o FQDN ou o grupo exato não são conhecidos, este comando pode rapidamente ser executado para o domínio ou a unidade organizacional (OU) conforme estes 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
```

Os comandos procuram o lab-ise1 do host no domínio ou no OU inteiro respectivamente.

Recorde substituir os detalhes do grupo e do nome de host nos comandos com o grupo correspondente e o nome ISE de seu desenvolvimento. Este comando concede à conta de máquina ISE o privilégio ler os grupos simbólicos. Precisa de ser executado em um controlador de domínio somente e deve replicate a outros controladores automaticamente.

A edição pode ser resolvida imediatamente. Execute o comando no controlador de domínio conectado atualmente no ISE.

A fim ver o controlador do domínio atual, navegue à **administração > ao Gerenciamento de identidades > fontes externos > diretório ativo da identidade > AD seleto juntam-se ao ponto**.

Informações Relacionadas

- A informação em relação a outras permissões da conta pode ser encontrada na integração do ative directory com Cisco ISE 1.3
- Link de Microsoft Technet
- **Suporte Técnico e Documentação - Cisco Systems**