Falha nas autenticações do AD do ISE 1.3 com o erro "Privilégio insuficiente para buscar grupos de token"

Contents

Introduction

Este documento descreve a solução para falha de autenticação do Identity Services Engine (ISE) contra o Ative Diretory (AD) devido ao código de erro "24371" causado por privilégios insuficientes de conta da máquina do ISE.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- Configurar e solucionar problemas do ISE
- Microsoft AD

Componentes Utilizados

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

- ISE versão 1.3.0.876
- Microsoft AD versão 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.

Falha nas autenticações do AD devido ao erro "24371"

No ISE 1.3 e superior, as autenticações podem falhar no AD com o erro "24371". O relatório de autenticação detalhado para a falha tem etapas semelhantes às 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 status do AD mostra associado e conectado e os grupos do AD necessários foram adicionados corretamente na configuração do ISE.

Solução

Modificar permissões para a conta da máquina do ISE no AD

O erro no relatório de autenticação detalhado implica que a conta da máquina do ISE no ative diretory não tem privilégios suficientes para buscar grupos de token.

> **Note**: A correção é feita no lado do AD, pois não é possível conceder o privilégio correto à conta da máquina do ISE. Talvez seja necessário desconectar/reconectar o ISE ao AD após isso.

Os privilégios atuais da conta da máquina podem ser verificados com o comando **dsacls**, como mostrado neste 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, portanto, redirecionada para um arquivo de texto **dsacl_output.txt** que pode ser aberto e visualizado corretamente em um editor de texto, como o notepad.

Se a conta tiver permissões para ler grupos de token, ela terá estas entradas no arquivo **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
```

Se as permissões não estiverem presentes, elas poderão ser adicionadas 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 for conhecido, esse comando poderá ser executado rapidamente para o domínio ou Unidade Organizacional (OU) de acordo com 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 host lab-ise1 em todo o domínio ou OU, respectivamente.

Lembre-se de substituir os detalhes do nome do grupo e do host nos comandos pelo grupo correspondente e o nome do ISE da sua implantação. Esse comando concede à conta da máquina ISE o privilégio de ler os grupos de token. Ele precisa ser executado somente em um controlador de domínio e deve ser replicado para outros controladores automaticamente.

O problema pode ser resolvido imediatamente. Execute o comando no controlador de domínio atualmente conectado ao ISE.

Para visualizar o controlador de domínio atual, navegue para **Administration > Identity Management > External Identity Sources > Ative Diretory > Select AD join point**.

Informações Relacionadas

- Informações sobre outras permissões de conta podem ser encontradas na Integração do Ative Diretory com o Cisco ISE 1.3
- Microsoft Technet Link
- **Suporte Técnico e Documentação - Cisco Systems**