

Solucionando problemas do processo de descoberta do controlador de domínio do Cisco ISE durante a associação ao Active Directory

Contents

Problema

O Cisco Identity Services Engine (ISE) não pode descobrir seus Controladores de Domínio (DCs) e o ingresso no Active Directory (AD) do ISE falha.

Ambiente

- Cisco Identity Services Engine (ISE) - 3.x e superior
- Microsoft Active Directory (AD) - 2016 e posterior
- Sistema de Nomes de Domínio (DNS) - UDP/TCP 53
- Lightweight Directory Access Protocol (LDAP) - TCP 389 TCP 636 se LDAP Seguro (LDAPS) for usado
- CLDAP (Lightweight Directory Access Protocol) sem conexão - UDP 389

Resolução

O Cisco ISE descobre DCs durante o processo de união ao AD e usa vários critérios para decidir qual DC escolher.

Descoberta de DNS:

- O ISE usa consultas de registro de Serviço DNS (SRV) para descobrir DCs, Catálogos Globais (GCs) e Centro de Distribuição de Chaves (KDCs) disponíveis. O servidor DNS retorna a lista de DCs, GCs e KDCs disponíveis
- Se o ISE não receber essas informações, ele não poderá continuar o processo de ingresso no AD e relatará um erro relacionado ao DNS.
- Na CLI do ISE, verifique os registros do AD SRV usando:

```
nslookup
```

- Exemplo:

```
nslookup ldap.tcp.example.com querytype SRV
```

```
nslookup kerberos.tcp.example.com querytype SRV
```

```
nslookup ldap.tcp.dc._msdcs.example.com querytype SRV
```

- As consultas devem retornar nomes de host DC válidos. Em seguida, verifique se o nome de host do DC retornado resolve para o endereço IP correto:

```
nslookup dc01.example.com
```

- O servidor DNS configurado na configuração atual do ISE retorna a lista de servidores disponíveis.
- Verifique a configuração do servidor ISE DNS executando este comando

```
show running-config
```

```
amysorea-36-san/admin#show running-config
interface GigabitEthernet 0
 ip address [REDACTED] 255.255.255.0
 ipv6 enable
 ipv6 address autoconfig
 !
 ntp server [REDACTED]
 repository local
 url disk: /
 !
 hostname amysorea-36-san
 icmp echo on
 ip domain-name amysorea.iselab.local
 ip default-gateway [REDACTED]
 ip name-server [REDACTED] ←
 ipv6 enable
 logging loglevel 6
```

- Para o CLDAP, use uma captura de pacotes no ISE ao executar a junção do AD ou ao executar o diagnóstico relevante do AD.
- Por exemplo, capture o tráfego entre o ISE e o DC e verifique:

```
ISE → DC01 : UDP/389  CLDAP Request
DC01 → ISE : UDP/389  CLDAP Response
```

- A resposta deve ser recebida de cada DC alcançável. Se o ISE enviar a solicitação CLDAP, mas não receber resposta, verifique as regras de firewall/ACL, roteamento e conectividade UDP 389 entre o ISE e o DC.

Identificação do local

- O ISE usa as informações do CLDAP para identificar e preferir DCs no mesmo local do Active Directory sempre que possível.
- Verifique se a sub-rede ISE pertence ao local correto do AD. Além disso, verifique se os DCs esperados pertencem ao mesmo local do AD.

Monitoramento de conectividade

- O ISE usa periodicamente o CLDAP para monitorar a disponibilidade do DC.
- Verifique se há conectividade UDP 389 intermitente, perda de pacotes ou respostas CLDAP atrasadas entre o ISE e os DCs usando capturas de pacotes.
- Uma resposta do CLDAP que leve mais de 2,5 segundos gera um aviso. Se nenhum controlador de domínio responder, a junção ao AD falhará.

Causa

- O ISE não pode detectar um DC.
- O DNS não retorna os registros do AD necessários.
- O ISE não pode acessar os DCs descobertos.
- Os DCs não respondem às solicitações do CLDAP.
- A sub-rede ISE mapeia para o local errado do AD.
- O controlador de domínio selecionado não aceita a conexão LDAP.

Conteúdo relacionado

- [Identity Service Engine \(ISE\) e Guia de integração do Ative Directory](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.