

Resolución de problemas del proceso de detección del controlador de dominio Cisco ISE durante la incorporación a Active Directory

Contenido

Problema

Cisco Identity Services Engine (ISE) no puede detectar los controladores de dominio (DC) y la unión a ISE Active Directory (AD) falla.

Entorno

- Cisco Identity Services Engine (ISE) - 3.x y superior
- Microsoft Active Directory (AD) - 2016 y versiones posteriores
- Sistema de nombres de dominio (DNS): UDP/TCP 53
- Protocolo ligero de acceso a directorios (LDAP): TCP 389; TCP 636 si se utiliza LDAP seguro (LDAP)
- Protocolo ligero de acceso a directorios sin conexión (CLDAP): UDP 389

Resolución

Cisco ISE detecta los DC durante el proceso de unión a AD y utiliza varios criterios para decidir qué DC elegir.

Detección de DNS:

- ISE utiliza consultas de registro de servicio DNS (SRV) para detectar los DC disponibles, los catálogos globales (GC) y el centro de distribución de claves (KDC). El servidor DNS devuelve la lista de DC, GC y KDC disponibles
- Si ISE no recibe esta información, no puede continuar el proceso de unión a AD e informa de un error relacionado con DNS.
- En la CLI de ISE, verifique los registros de AD SRV mediante:

```
nslookup
```

- Ejemplo:

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

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

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

- Las consultas deben devolver hostnames de DC válidos. A continuación, verifique que el nombre de host del DC devuelto se resuelva con la dirección IP correcta:

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

- El servidor DNS configurado en la configuración de ejecución de ISE devuelve la lista de servidores disponibles.
- Ejecute este comando para verificar la configuración del servidor DNS de ISE

```
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 CLDAP, utilice una captura de paquetes en ISE mientras realiza la unión AD o ejecuta el diagnóstico AD relevante.
- Por ejemplo, capture el tráfico entre ISE y el DC y verifique:

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

- La respuesta debe recibirse de cada DC accesible. Si ISE envía la solicitud CLDAP pero no recibe respuesta, compruebe las reglas de firewall/ACL, el routing y la conectividad UDP 389 entre ISE y el DC.

Identificación del sitio

- ISE utiliza la información de CLDAP para identificar y preferir los DC del mismo sitio de Active Directory siempre que sea posible.
- Verifique que la subred de ISE pertenezca al sitio de AD correcto. Además, compruebe que los DC esperados pertenezcan al mismo sitio de AD.

Supervisión de conectividad

- ISE utiliza CLDAP periódicamente para supervisar la disponibilidad del DC.
- Compruebe si hay conectividad UDP 389 intermitente, pérdida de paquetes o respuestas CLDAP retrasadas entre ISE y los DC mediante capturas de paquetes.
- Una respuesta CLDAP que tarda más de 2,5 segundos genera una advertencia. Si no responde ningún DC, la unión de AD falla.

Causa

- ISE no puede detectar un DC.
- DNS no devuelve los registros de AD requeridos.
- ISE no puede alcanzar los DC detectados.
- Los DC no responden a las solicitudes CLDAP.
- La subred de ISE se asigna al sitio de AD incorrecto.
- El DC seleccionado no acepta la conexión LDAP.

Contenido relacionado

- [Guía de integración de Identity Service Engine \(ISE\) y Active Directory](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).