

在Active Directory加入期间排除思科ISE ；域控制器发现进程故障

目录

问题

思科身份服务引擎(ISE)无法发现您的域控制器(DC),ISE Active Directory(AD)加入失败。

环境

- 思科身份服务引擎(ISE)- 3.x及更高版本
- Microsoft Active Directory(AD)- 2016及更高版本
- 域名系统(DNS)- UDP/TCP 53
- 轻量级目录访问协议(LDAP)- TCP 389;TCP 636(如果使用安全LDAP(LDAPS))
- 无连接轻量级目录访问协议(CLDAP)- UDP 389

分辨率

思科ISE在AD加入过程中发现DC，并使用多个条件决定选择哪个DC。

DNS发现：

- ISE使用DNS服务(SRV)记录查询发现可用的DC、全局目录(GC)和密钥分发中心(KDC)。DNS服务器返回可用DC、GC和KDC的列表

- 如果ISE未收到此信息，则无法继续AD加入过程并报告与DNS相关的错误。
- 从ISE CLI，使用验证AD SRV记录：

```
nslookup
```

- 示例：

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

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

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

- 查询应返回有效的DC主机名。然后验证返回的DC主机名解析为正确的IP地址：

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

- 在ISE运行配置中配置的DNS服务器返回可用服务器的列表。
- 通过运行此命令验证您的ISE DNS服务器配置

```
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
```

- 对于CLDAP，在执行AD加入或运行相关AD诊断时，在ISE上使用数据包捕获。
- 例如，捕获ISE和DC之间的流量并验证：

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

- 应从每个可到达的DC接收响应。如果ISE发送CLDAP请求但没有收到响应，请检查ISE和DC之间的防火墙/ACL规则、路由和UDP 389连接。

站点标识

- ISE尽可能使用CLDAP信息识别并首选同一Active Directory站点中的DC。
- 验证ISE子网属于正确的AD站点。此外，验证预期的DC属于同一AD站点。

连接监控

- ISE定期使用CLDAP监控DC可用性。
- 使用数据包捕获检查ISE和DC之间的间断UDP 389连接、数据包丢失或延迟CLDAP响应。

- 超过2.5秒的CLDAP响应会生成警告。如果没有DC响应，则AD加入失败。

原因

- ISE无法发现数据中心。
- DNS不返回所需的AD记录。
- ISE无法访问已发现的DC。
- DC不响应CLDAP请求。
- ISE子网映射到错误的AD站点。
- 所选的DC不接受LDAP连接。

相关内容

- [身份服务引擎\(ISE\)和Active Directory集成指南](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。