

在Active Directory加入期間對思科ISE ；域控制器發現流程進行故障排除

目錄

問題

思科身份服務引擎(ISE)無法發現域控制器(DC),ISE Active Directory(AD)加入失敗。

環境

- 思科身份服務引擎(ISE)- 3.x及更高版本
- Microsoft Active Directory(AD)- 2016及更高版本
- 網域名稱系統(DNS)- UDP/TCP 53
- 輕量型目錄存取通訊協定(LDAP)- TCP 389;如果使用安全LDAP(LDAPS) , 則為TCP 636
- 無連線輕量型目錄存取通訊協定(CLDAP)- UDP 389

解析

思科ISE在AD加入過程中發現DC , 並使用多個條件來決定選擇哪個DC。

DNS發現 :

- ISE使用DNS服務(SRV)記錄查詢發現可用的DC、全域性目錄(GC)和金鑰分發中心(KDC)。DNS伺服器返回可用DC、GC和KDC的清單

- 如果ISE未收到此資訊，則無法繼續AD加入過程並報告DNS相關錯誤。
- 在ISE CLI中，使用驗證AD SRV記錄：

```
nslookup
```

- 範例：

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

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

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

- 查詢應返回有效的DC主機名。然後驗證返回的DC主機名是否解析為正確的IP地址：

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

- 在ISE運行配置中配置的DNS伺服器返回可用伺服器清單。
- 通過運行此命令驗證ISE DNS伺服器配置

```
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
```

- 對於CLDAP，在執行AD加入或運行相關AD診斷時，在ISE上使用資料包捕獲。
- 例如，捕獲ISE和DC之間的流量並驗證：

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

- 應從每個可到達的DC接收響應。如果ISE傳送CLDAP請求但沒有收到響應，請檢查ISE和DC之間的防火牆/ACL規則、路由和UDP 389連線。

站點標識

- ISE儘可能使用CLDAP資訊識別並優先使用同一Active Directory站點中的DC。
- 驗證ISE子網屬於正確的AD站點。此外，驗證預期的DC屬於同一個AD站點。

連線監控

- ISE定期使用CLDAP監控DC可用性。
- 使用資料包捕獲，檢查ISE和DC之間的中斷性UDP 389連線、資料包丟失或延遲CLDAP響應

-
- 超過2.5秒的CLDAP響應會生成警告。如果沒有DC響應，則AD連線失敗。

原因

- ISE無法發現資料中心。
- DNS不返回所需的AD記錄。
- ISE無法到達發現的DC。
- DC不響應CLDAP請求。
- ISE子網對映到錯誤的AD站點。
- 選定的DC不接受LDAP連線。

相關內容

- [身份服務引擎\(ISE\)和Active Directory整合指南](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。