

Fehlerbehebung beim Cisco ISE Domain Controller Discovery-Prozess während des Active Directory-Beitritts

Inhalt

Problem

Die Cisco Identity Services Engine (ISE) kann Ihre Domänencontroller (DCs) nicht erkennen, und der Beitritt zu ISE Active Directory (AD) schlägt fehl.

Umwelt

- Cisco Identity Services Engine (ISE) - 3.x und höher
- Microsoft Active Directory (AD) - 2016 und höher
- Domain Name System (DNS) - UDP/TCP 53
- Lightweight Directory Access Protocol (LDAP) - TCP 389 TCP 636 bei Verwendung von Secure LDAP (LDAPS)
- Connectionless Lightweight Directory Access Protocol (CLDAP) - UDP 389

Auflösung

Die Cisco ISE erkennt Rechenzentren während des AD-Join-Prozesses und legt anhand mehrerer Kriterien fest, welches Rechenzentrum ausgewählt werden soll.

DNS-Erkennung:

- Die ISE verwendet DNS Service (SRV)-Eintragsabfragen, um verfügbare Rechenzentren, globale Kataloge (GCs) und Key Distribution Center (KDCs) zu ermitteln. Der DNS-Server gibt die Liste der verfügbaren DCs, GCs und KDCs zurück.
- Wenn die ISE diese Informationen nicht erhält, kann sie den AD-Join-Prozess nicht fortsetzen und meldet einen DNS-bezogenen Fehler.
- Überprüfen Sie über die ISE-CLI die AD SRV-Datensätze mithilfe von:

```
nslookup
```

- Beispiel:

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

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

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

- Die Abfragen müssen gültige DC-Hostnamen zurückgeben. Überprüfen Sie anschließend, ob der zurückgegebene RZ-Hostname in die richtige IP-Adresse aufgelöst wird:

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

- Der DNS-Server, der in der aktuellen ISE-Konfiguration konfiguriert wurde, gibt die Liste der verfügbaren Server zurück.
- Überprüfen Sie die ISE DNS-Serverkonfiguration, indem Sie diesen Befehl ausführen.

```
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
```

- Für CLDAP sollten Sie eine Paketerfassung auf der ISE verwenden, während Sie den AD-Join durchführen oder die entsprechende AD-Diagnose ausführen.
- Erfassen Sie beispielsweise den Datenverkehr zwischen der ISE und dem Rechenzentrum, und überprüfen Sie Folgendes:

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

- Die Antwort muss von jedem erreichbaren Rechenzentrum eingehen. Wenn die ISE die CLDAP-Anforderung sendet, aber keine Antwort erhält, überprüfen Sie die Firewall-/ACL-Regeln, das Routing und die UDP 389-Verbindung zwischen der ISE und dem Rechenzentrum.

Standortidentifizierung

- Die ISE verwendet CLDAP-Informationen, um nach Möglichkeit DCs am selben Active Directory-Standort zu identifizieren und zu bevorzugen.
- Vergewissern Sie sich, dass das ISE-Subnetz zum richtigen AD-Standort gehört. Überprüfen Sie außerdem, ob die erwarteten Domänencontroller zum gleichen AD-Standort gehören.

Verbindungsüberwachung

- Die ISE verwendet CLDAP regelmäßig, um die Verfügbarkeit des Rechenzentrums zu überwachen.
- Überprüfen Sie mithilfe von Paketerfassungen, ob zwischen der ISE und den Rechenzentren intermittierende UDP 389-Verbindungen, Paketverluste oder verzögerte CLDAP-Antworten bestehen.
- Eine CLDAP-Antwort, die mehr als 2,5 Sekunden dauert, generiert eine Warnung. Wenn kein Rechenzentrum antwortet, schlägt der AD-Join fehl.

Ursache

- Die ISE kann ein Rechenzentrum nicht erkennen.
- DNS gibt die erforderlichen AD-Datensätze nicht zurück.
- Die ISE kann die erkannten Rechenzentren nicht erreichen.
- DCs antworten nicht auf CLDAP-Anforderungen.
- Das ISE-Subnetz ist der falschen AD-Site zugeordnet.
- Der ausgewählte Domänencontroller akzeptiert die LDAP-Verbindung nicht.

Verwandte Inhalte

- [Identity Service Engine \(ISE\) und Active Directory Integration Guide](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.