

Problemen oplossen met het detectieproces van Cisco ISE Domeincontroller tijdens Active Directory Join

Inhoud

uitgifte

Cisco Identity Services Engine (ISE) kan uw domeincontrollers (DC's) niet vinden en de ISE Active Directory (AD) -verbinding mislukt.

milieu

- Cisco Identity Services Engine (ISE) – 3.x en hoger
- Microsoft Active Directory (AD) – 2016 en hoger
- Domeinnaamsysteem (DNS) – UDP/TCP 53
- Lightweight Directory Access Protocol (LDAP) – TCP 389; TCP 636 als Secure LDAP (LDAPS) wordt gebruikt
- Connectionless Lightweight Directory Access Protocol (CLDAP) – UDP 389

resolutie

Cisco ISE ontdekt DC's tijdens het AD-join-proces en gebruikt meerdere criteria om te beslissen welke DC moet worden gekozen.

DNS-detectie:

- ISE maakt gebruik van SRV-recordquery's (DNS Service) om beschikbare DC's, Global Catalogs (GC's) en Key Distribution Center (KDC's) te ontdekken. De DNS-server geeft de lijst met beschikbare DC's, GC's en KDC's terug
- Als ISE deze informatie niet ontvangt, kan het niet doorgaan met het AD-aanmeldingsproces en rapporteert het een DNS-gerelateerde fout.
- Controleer vanuit de ISE CLI de AD SRV-records met behulp van:

```
nslookup
```

- Voorbeeld:

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

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

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

- De query's moeten geldige DC-hostnamen retourneren. Controleer vervolgens of de geretourneerde DC-hostnaam is opgelost naar het juiste IP-adres:

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

- De DNS-server die in de ISE-configuratie is geconfigureerd, retourneert de lijst met beschikbare servers.
- Controleer de configuratie van de ISE DNS-server door deze opdracht uit te voeren

```
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
```

- Gebruik voor CLDAP een pakketopname op ISE tijdens het uitvoeren van de AD-join of het uitvoeren van de desbetreffende AD-diagnose.
- Leg bijvoorbeeld het verkeer tussen ISE en de DC vast en controleer:

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

- Het antwoord moet worden ontvangen van elke bereikbare DC. Als ISE het CLDAP-verzoek verzendt maar geen antwoord ontvangt, controleert u de firewall/ACL-regels, routing en UDP 389-connectiviteit tussen ISE en de DC.

site-identificatie

- ISE gebruikt CLDAP-informatie om DC's waar mogelijk in dezelfde Active Directory-site te identificeren en te prefereren.
- Controleer of het ISE-subnet tot de juiste AD-site behoort. Controleer ook of de verwachte DC's tot dezelfde AD-site behoren.

Connectiviteitsbewaking

- ISE maakt periodiek gebruik van CLDAP om de beschikbaarheid van DC te monitoren.
- Controleer op intermitterende UDP 389-connectiviteit, pakketverlies of vertraagde CLDAP-responsen tussen ISE en de DC's met pakketopnamen.
- Een CLDAP-respons die meer dan 2,5 seconden duurt, genereert een waarschuwing. Als er geen DC reageert, mislukt de AD-join.

Oorzaak

- ISE kan geen DC ontdekken.
- DNS retourneert de vereiste AD-records niet.
- ISE kan de ontdekte DC's niet bereiken.
- DC's reageren niet op CLDAP-verzoeken.
- Het ISE-subnet brengt de verkeerde AD-site in kaart.
- De geselecteerde gelijkstroom accepteert de LDAP-verbinding niet.

Gerelateerde inhoud

- [Identity Service Engine \(ISE\) en Active Directory Integration Guide](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.