

Risoluzione dei problemi relativi al processo di individuazione del controller di dominio Cisco ISE Domain Controller Discovery durante l'aggiunta ad Active Directory

Sommario

Problema

Cisco Identity Services Engine (ISE): impossibile individuare i controller di dominio. L'aggiunta di ISE Active Directory (AD) non riuscirà.

Ambiente

- Cisco Identity Services Engine (ISE) - 3.x e versioni successive
- Microsoft Active Directory (AD) - 2016 e versioni successive
- DNS (Domain Name System) - UDP/TCP 53
- LDAP (Lightweight Directory Access Protocol) - TCP 389; TCP 636 se si utilizza Secure LDAP (LDAPS)
- Protocollo CLDAP (Lightweight Directory Access Protocol) senza connessione - UDP 389

Risoluzione

Cisco ISE individua i controller di dominio durante il processo di aggiunta ad Active Directory e utilizza più criteri per decidere quale controller di dominio scegliere.

Individuazione DNS:

- ISE utilizza query sui record del servizio DNS (SRV) per individuare i controller di dominio, i cataloghi globali (GC) e i centri di distribuzione chiavi (KDC) disponibili. Il server DNS restituisce l'elenco dei controller di dominio, dei cataloghi globali e dei KDC disponibili
- Se ISE non riceve queste informazioni, non potrà continuare il processo di aggiunta ad AD e segnerà un errore relativo al DNS.
- Dalla CLI di ISE, verificare i record di AD SRV usando:

```
nslookup
```

- Esempio:

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

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

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

- Le query devono restituire nomi host di controller di dominio validi. Verificare quindi che il nome host del controller di dominio restituito corrisponda all'indirizzo IP corretto:

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

- Il server DNS configurato nella configurazione ISE in esecuzione restituisce l'elenco dei server disponibili.
- Verificare la configurazione del server DNS ISE eseguendo questo comando

```
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
```

- Per CLDAP, utilizzare un'acquisizione di pacchetti su ISE durante l'esecuzione del join AD o l'esecuzione della diagnostica AD appropriata.
- Ad esempio, acquisire il traffico tra ISE e il controller di dominio e verificare:

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

- La risposta deve essere ricevuta da ogni controller di dominio raggiungibile. Se ISE invia la richiesta CLDAP ma non riceve risposta, controllare le regole firewall/ACL, il routing e la connettività UDP 389 tra ISE e il controller di dominio.

Identificazione sito

- ISE utilizza le informazioni CLDAP per identificare e preferire i controller di dominio nello stesso sito Active Directory, quando possibile.
- Verificare che la subnet ISE appartenga al sito AD corretto. Verificare inoltre che i controller di dominio previsti appartengano allo stesso sito AD.

Monitoraggio della connettività

- ISE utilizza periodicamente CLDAP per monitorare la disponibilità di corrente continua.
- Verificare la presenza di connettività UDP 389 intermittente, perdita di pacchetti o risposte CLDAP ritardate tra ISE e i controller di dominio utilizzando le acquisizioni di pacchetti.
- Se la risposta CLDAP richiede più di 2,5 secondi, viene generato un avviso. Se nessun controller di dominio risponde, il join AD non riesce.

Causa

- ISE: impossibile rilevare un controller di dominio.
- Il DNS non restituisce i record AD richiesti.
- ISE non è in grado di raggiungere i controller di dominio rilevati.
- I controller di dominio non rispondono alle richieste CLDAP.
- La subnet ISE è mappata al sito AD errato.
- Il controller di dominio selezionato non accetta la connessione LDAP.

Contenuto correlato

- [Guida all'integrazione di Identity Service Engine \(ISE\) e Active Directory](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).