

Dépannage du processus de détection du contrôleur de domaine Cisco ISE ; ; pendant la connexion à Active Directory

Table des matières

Problème

Cisco Identity Services Engine (ISE) ne peut pas détecter vos contrôleurs de domaine (DC) et la connexion à ISE Active Directory (AD) échoue.

Environnement

- Cisco Identity Services Engine (ISE) - 3.x et versions ultérieures
- Microsoft Active Directory (AD) - 2016 et versions ultérieures
- DNS (Domain Name System) - UDP/TCP 53
- Protocole LDAP (Lightweight Directory Access Protocol) - TCP 389 ; TCP 636 si LDAP sécurisé (LDAPS) est utilisé
- Protocole LDAP (Lightweight Directory Access Protocol) sans connexion - UDP 389

Résolution

Cisco ISE détecte les contrôleurs de domaine au cours du processus de jointure Active Directory et utilise plusieurs critères pour déterminer le contrôleur de domaine à choisir.

Détection DNS :

- ISE utilise des requêtes d'enregistrement de service DNS (SRV) pour détecter les DC, les catalogues globaux (GC) et les centres de distribution de clés (KDC) disponibles. Le serveur DNS renvoie la liste des contrôleurs de domaine, des contrôleurs de catalogue global et des contrôleurs de domaine
- Si ISE ne reçoit pas ces informations, il ne peut pas poursuivre le processus de jointure Active Directory et signale une erreur liée au DNS.
- À partir de l'interface de ligne de commande ISE, vérifiez les enregistrements AD SRV en utilisant :

```
nslookup
```

- Exemple :

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

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

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

- Les requêtes doivent renvoyer des noms d'hôte DC valides. Vérifiez ensuite que le nom d'hôte du contrôleur de domaine renvoyé correspond à l'adresse IP correcte :

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

- Votre serveur DNS configuré dans la configuration en cours ISE renvoie la liste des serveurs disponibles.
- Vérifiez la configuration de votre serveur DNS ISE en exécutant cette commande

```
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
```

- Pour le protocole LDAP, utilisez une capture de paquets sur ISE lors de la jointure Active Directory ou de l'exécution du diagnostic Active Directory approprié.
- Par exemple, capturez le trafic entre ISE et le data center et vérifiez les points suivants :

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

- La réponse doit être reçue de chaque contrôleur de domaine accessible. Si ISE envoie la requête LDAP mais ne reçoit aucune réponse, vérifiez les règles de pare-feu/ACL, le routage et la connectivité UDP 389 entre ISE et le contrôleur de domaine.

Identification du site

- ISE utilise les informations CLDAP pour identifier et préférer les contrôleurs de domaine dans le même site Active Directory chaque fois que cela est possible.
- Vérifiez que le sous-réseau ISE appartient au site AD approprié. Vérifiez également que les contrôleurs de domaine attendus appartiennent au même site AD.

Surveillance de la connectivité

- ISE utilise régulièrement le protocole LDAP pour surveiller la disponibilité du data center.
- Vérifiez la connectivité UDP 389 intermittente, la perte de paquets ou les réponses LDAP retardées entre ISE et les contrôleurs de domaine à l'aide de captures de paquets.
- Une réponse LDAP prenant plus de 2,5 secondes génère un avertissement. Si aucun contrôleur de domaine ne répond, la jointure Active Directory échoue.

Motif

- ISE ne peut pas détecter un contrôleur de domaine.
- DNS ne renvoie pas les enregistrements AD requis.
- ISE ne peut pas atteindre les contrôleurs de domaine détectés.
- Les DC ne répondent pas aux demandes CLDAP.
- Le sous-réseau ISE correspond au mauvais site AD.
- Le contrôleur de domaine sélectionné n'accepte pas la connexion LDAP.

Autres informations utiles

- [Identity Service Engine \(ISE\) et Guide d'intégration d'Active Directory](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.