

Active Directory参加中のCisco ISEのトラブルシューティング(); ; ドメインコントローラ検出プロセス

内容

問題

Cisco Identity Services Engine(ISE)がドメインコントローラ(DC)を検出できず、ISE Active Directory(AD)の参加が失敗します。

環境

- Cisco Identity Services Engine(ISE) - 3.x以降
- Microsoft Active Directory(AD) - 2016以上
- ドメインネームシステム(DNS) - UDP/TCP 53
- Lightweight Directory Access Protocol(LDAP):TCP 389、Secure LDAP(LDAPS)が使用されている場合はTCP 636
- コネクションレス型Lightweight Directory Access Protocol(CLDAP):UDP 389

解決方法

Cisco ISEはAD参加プロセス中にDCを検出し、複数の基準を使用してどのDCを選択するかを決定します。

DNSディスカバリ :

- ISEは、DNSサービス(SRV)レコードクエリを使用して、使用可能なDC、グローバルカタログ(GC)、およびキー配布センター(KDC)を検出します。DNSサーバは、使用可能なDC、GC、およびKDCのリストを返します
- ISEがこの情報を受信しない場合、AD参加プロセスを続行できず、DNS関連のエラーが報告されます。
- ISE CLIで、を使用してAD SRVレコードを確認します。

```
nslookup
```

- 例：

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

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

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

- クエリは有効なDCホスト名を返す必要があります。次に、返されたDCホスト名が正しいIPアドレスに解決されることを確認します。

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

- ISE実行コンフィギュレーションで設定されたDNSサーバが、使用可能なサーバのリストを返します。
- 次のコマンドを実行して、ISE DNSサーバ設定を確認します

```
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
```

- CLDAPについては、AD参加の実行中または関連するAD診断の実行中にISEでパケットキャプチャを使用します。
- たとえば、ISEとDCの間のトラフィックをキャプチャして次を確認します。

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

- 応答は、到達可能な各DCから受信する必要があります。ISEがCLDAP要求を送信しても応答を受信しない場合は、ISEとDCの間のファイアウォール/ACLルール、ルーティング、およびUDP 389接続を確認します。

サイトID

- ISEはCLDAP情報を使用して、可能な限り同じActive Directoryサイト内のDCを識別し、優先します。
- ISEサブネットが正しいADサイトに属していることを確認します。また、想定されるDCが同じADサイトに属していることを確認します。

接続の監視

- ISEは定期的にCLDAPを使用してDCの可用性を監視します。
- パケットキャプチャを使用して、ISEとDCの間で断続的なUDP 389接続、パケット損失、遅延したCLDAP応答がないかを確認します。
- 2.5秒を超えるCLDAP応答があると、警告が生成されます。DCが応答しない場合、AD参加は失敗します。

原因

- ISEはDCを検出できません。
- DNSは必要なADレコードを返しません。
- ISEが検出されたDCに到達できません。
- DCはCLDAP要求に応答しません。
- ISEサブネットが間違ったADサイトにマッピングされている。
- 選択されたDCはLDAP接続を受け入れません。

関連コンテンツ

- [Identity Service Engine\(ISE\)およびActive Directory統合ガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。