

知 Idap认证成功但是导入用户失败/同步用户失败

AAA 李瑞 2023-05-12 发表

组网及说明

防火墙链接Idap服务器，做用户同步

告警信息

错误 ✕

 从LDAP服务器(ldap)上导入用户失败，原因是连接服务器失败。

关闭

问题描述

需求是在对象—用户—用户管理—用户导入策略里从LDAP服务器导入身份识别用户，但导入失败。目前ss lvpn+ldap认证，这一块都正常，说明ldap的相关配置都正常，ldap连接也是正常的

解决方法

1. 去掉设备上所有的dns server配置:

```
dns server 8.8.8.8
```

```
... ..
```

2. 去掉dialer口上的所有dns相关配置:

```
#
```

```
interface Dialer0
```

```
bandwidth 1000000
```

```
mtu 1492
```

```
ppp chap password cipher XXX
```

```
ppp chap user 3601
```

```
ppp ipcp dns admit-any
```

```
ppp ipcp dns request/undo掉这两个命令，确认display dns server返回空
```

相关命令如下:

```
ppp ipcp dns admit-any命令用来配置设备可以被动地接收对端设备指定的DNS服务器的IP地址，即设备不发送DNS请求，也能接收对端设备分配的DNS服务器的IP地址。  
undo ppp ipcp dns admit-any命令用来恢复缺省情况。  
【命令】  
ppp ipcp dns admit-any  
undo ppp ipcp dns admit-any  
【缺省情况】  
设备不会被动地接收对端设备指定的DNS服务器的IP地址。  
【视图】  
接口视图  
【缺省用户角色】  
network-admin  
context-admin  
【使用指导】  
当设备通过PPP协议与其它设备相连时，通过协商，设备可以被动地接收对端设备指定的DNS服务器地址，这样设备就可以使用对端设备指定的DNS服务器来解析域名。  
正常情况下，Client端配置了ppp ipcp dns request，Server端才会为本端指定DNS服务器地址，但是一些特殊的设备，Client端并未请求，Server端却要强制为Client端指定DNS服务器地址，从而导致协商不通过，为了适应这种情况，Client端可以配置ppp ipcp dns admit-any。  
【举例】  
# 配置本地设备的Virtual-Template1接口可以被动地接收对端指定的DNS服务器地址。  
<Sysname> system-view  
[Sysname] interface virtual-template 1  
[Sysname-Virtual-Template1] ppp ipcp dns admit-any  
【相关命令】  
• ppp ipcp dns request
```

```
ppp ipcp dns request命令用来配置设备可以主动向对端请求DNS服务器地址。  
undo ppp ipcp dns request命令用来恢复缺省情况。  
【命令】  
ppp ipcp dns request  
undo ppp ipcp dns request  
【缺省情况】  
禁止设备主动向对端请求DNS服务器地址。  
【视图】  
接口视图  
【缺省用户角色】  
network-admin  
context-admin  
【使用指导】  
当设备通过PPP协议与其它设备相连时（通常为设备拨号连接运营商的接入服务器），在进行IPCP协商时，设备可以主动向对端设备为其指定DNS服务器地址，这样设备就可以使用对端设备指定的DNS来解析域名。  
如果协商到有效的DNS服务器地址，将在接口显示信息中打印出来。  
【举例】  
# 配置Virtual-Template1接口主动请求DNS服务器地址。  
<Sysname> system-view  
[Sysname] interface virtual-template 1  
[Sysname-Virtual-Template1] ppp ipcp dns request
```

