SSLVPN结合LDAP认证不成功报密码没有设置的错误

SSL VPN 李瑞 2021-11-03 发表

组网及说明

标准的sslvpn+ldap认证的组网

具体配置方法可参考如下链接：https://zhiliao.h3c.com/Theme/details/165528

问题描述

配置完成后inode拨号失败，debug ldap看有如下的报错：

<H3C>

*Nov 2 08:33:24:364 2021 H3C LDAP/7/EVENT: PAM_LDAP:Processing LDAP authentication.

*Nov 2 08:33:24:364 2021 H3C LDAP/7/EVENT: PAM_LDAP:Data of authentication request successfully sent.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:Processing AAA request data.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:LDAP server is: 172.31.0.238.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:Created new connection.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:Current bind state is 0. *Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP[State]:State switch from init to binding admin.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/ERROR: PAM_LDAP:Password not set.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/ERROR: PAM_LDAP:Failed to start state machine.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:Processing LDAP authentication.

*Nov 2 08:33:24:365 2021 H3C LDAP/7/EVENT: PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

过程分析

一般这种情况就是认证时遇到了问题，具体定位可以抓包分析，ldap认证报文是明文，可以在防火墙上写明细acl抓包进一步确认。

上述报错是由于ldap服务器上配置了中文的用户名，但是inode不支持中文输入，我们输入了用户属性中的用户登录名【这个就是ldap服务器上的登录名（即sAMAccountName），这里需要注意，一般默认不更改的情况下，ldap服务器上的登录名是用户的中文名称的英文拼音（使用英文拼音，即用户属性中的用户名登录）】
而防火墙默认情况下使用的是cn进行协商，cn默认的编码格式是UTF-8，这个时候就会导致我们防火墙发出用户名是错误的（即用UTF-8编码的英文用户名登录名），导致ldap服务器无法识别或者张冠李戴。

```
[F1070-IRF-ldap-server-test2021]user-parameters user-name-attribute ?
  STRING<1-64>  Custom specified user name attribute
  cn            Common name (default)
  uid           Unique ID
```

解决方法

```
# ldap server test2021
 user-parameters user-name-attribute samaccountname
```

附注：

通用名标识分为“cn”和“sAMAccountName”,官网给出的提示是：配置“cn”时，同步和认证使用标识名（中文用用户名或者英文名），配置“sAMAccountName”时，同步和认证使用登录名（中文名的拼音）