交换机SSH结合LDAP登录失败

AAA 杨凌轩 2019-10-18 发表

组网及说明

无

问题描述

交换机做SSH结合LDAP登录，现场反馈登录SSH登录失败

过程分析

ldap server longson
 login-dn cn=administrator,cn=users,dc=longson,dc=com
 search-base-dn dc=longson,dc=com
 ip 1.1.1.1
 login-password cipher admin@123

ldap scheme longson-shml
 authentication-server longson

domain longson
 authentication login ldap-scheme longson-shml local
 accounting login none

 domain default enable longson
 role default-role enable
现场配置比较简单，查看没有特殊异常
于是从报文交互入手
在SSH交互登录过程抓包发现
报文交互到了bindrequest阶段后，设备回复了unbindrequest的终止报文
进一步对服务器发送的bindrequest报文分析，正常该报文应该包含对应用户的属性信息及Distinguished Name (CN= , CN= , DC= ,DC=)
检查报文发现CN属性与设备侧不一致

解决方法

修改两端配置一致后解决。对于配置较少的情况可以从报文交互过程入手，查看具体哪一段交互产生问题来寻找问题故障点
正常LDAP报文交互过程
1、TCP的三次握手
2、 Client发送一个BindRequest给到LDAP Server，BindRequest相当于认证的请求。 在RFC 4511 4.2.1 提到，当Client发送了BingRequest之后，Client Must NOT发送更多的LDAP PDUs 直到收到BingResponse。同时从这个包中，我们可以直接看到这个Client端发送的明文密码。进一步回复的报文BingResponse中 ResultCode为Success，代表BindRequest处理成功。如果返回的是错误的话，需要去检查相应的LDAP Result Codes。
3. LDAP Client发送一个SearchRequest给LDAP Server去查询相应的用户信息，过滤条件两者与的关系，即对象为user 与accountname为登录帐号。下一个报文LDAP Server返回Search对应的结果，并且包含对应用户的属性信息及Distinguished Name (CN= , CN= , DC= ,DC=)
4. 下一步报文是LDAP Client向server发送用户名和密码验证的过程。从包中可以看到明文的密码。进一步报文是server端返回的认证结果。
至此完成认证过程