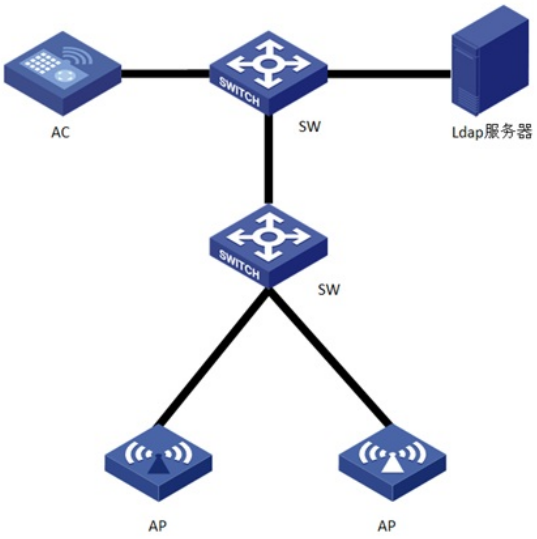
某局点WX2540H结合LDAP做认证认证不通过的经验案例

AAA 叶靖 2019-06-27 发表

组网及说明

某局点购买了一台V7版本的无线控制器WX2540H，现场配置了本地portal，另外结合第三方的ldap服务器进行AAA认证。



问题描述

现场按照官网的案例进行相关配置，目前portal页面可以正常弹出，但是在portal页面输入面时一直无法认证成功。

过程分析

对于结合ldap做认证，认证不通过的情况，需要注意一下几点：

1、 确认AC和ldap服务器之间的网络连通性，确保网络可达

ldap server ldap

login-dn cn=administrator,cn=users,dc=ldap,dc=com

search-base-dn ou=sz-ldap,ou=ldap,ou=ldapgroup,dc=ldap,dc=com

ip 192.168.1.1

2、 确认ldap服务器侧是否支持授权和计费，建议将认证域下的授权和计费配置为none测试，具体如下：

domain ldap

authorization-attribute idle-cut 15 1024

authentication portal ldap-scheme ldap

authorization portal none

accounting portal none

3、 在AC上开启debug，收集debugging ldap all的信息，查看debug信息，若debug中出现下面的信息，

*Apr 23 16:38:15:964 2019 H3C LDAP/7/ERROR:

PAM_LDAP:Failed to perform binding operation as administrator.

login-password cipher c3$VDGHvDIu1I6UHtjWSU8dAqM/J/1IvMLfeIaUNg==

上面的debug报错信息和配置说明：ldap上面的用户user1没有管理员权限。需要为user1添加管理员权限或者更换指定的用户

ldap server ldap

login-dn cn=user1,cn=users,dc=ldap,dc=com

search-base-dn ou=sz-ldap,ou=ldap,ou=ldapgroup,dc=ldap,dc=com

ip 192.168.1.1

4、 在debug信息中如果出现下面的信息：

*Apr 23 17:10:42:967 2019 H3C LDAP/7/ERROR:

PAM_LDAP:Failed to search users.

出现上述debug报错信息，说明配置的ldap服务器目录下没有认证用户，或者是配置的ldap服务器目录格式存在问题。需要注意的是，在设备上指定查询的ldap服务器目录时，需要确保目录名中没有空格及特殊字符。如下面的配置，需要将目录名sz-ldap修改为不带特殊字符。

ldap server ldap

login-dn cn=user1,cn=users,dc=ldap,dc=com

search-base-dn ou=sz-ldap,ou=ldap,ou=ldapgroup,dc=ldap,dc=com

ip 192.168.1.1

解决方法

遇到结合ldap认证不通过的问题时，需要注意修改设备侧关于ldap认证的相关配置，确认设备侧配置与ldap服务器侧一致且不违反相关限制。