

Ucenter和LDAP认证服务器对接，使用LDAP用户无法登录Ucenter故障分析

PLAT Ucenter 张兴龙 2019-03-31 发表

组网及说明

组网不涉及

U-center: 7.3 E0508H12

第三方认证服务器: 通用LDAP服务器

问题描述

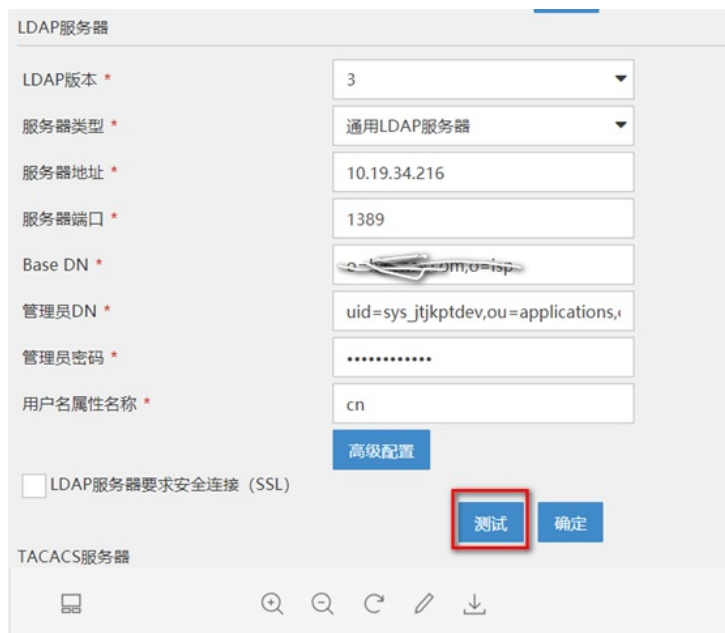
用户使用U-center和第三方认证服务器对接后，使用LDAP侧用户登录U-center失败，报错如下截图所示



过程分析

具体分析过程如下

1、使用管理员账号登录U-CENTER，进入操作员管理->认证服务器配置，检查LDAP服务器侧配置，测试Ucenter和LDAP服务器对接是否成功。现场测试结果如下，测试成功，说明和Ucenter和LDAP服务器对接没有问题。



2、在U-center服务侧后台使用wireshark抓包，查看Ucenter和LDAP服务器的交互报文，通过报文可以看到U-center向LDAP服务器发送了Bindrequest请求报文，LDAP服务器侧返回success,说明通过管理员连接LDAP没问题。

16806 65.954754	10.19.41.156	10.19.34.216	TCP	66 18008 > 16100 [ACK] Seq=1 Ack=1 Wm=14720 Len=0 TSval=1025513064 TSecr=3887952707
16808 65.954754	10.19.41.156	10.19.34.216	TCP	66 16100 > 18032 [ACK] Seq=1 Ack=80 Wm=29056 Len=0 TSval=1025513065 TSecr=3887952709
16809 65.954757	10.19.34.216	10.19.41.156	LDAP	80 b1indResponse(1) success
16810 65.954758	10.19.41.156	10.19.34.216	TCP	66 18008 > 16100 [ACK] Seq=1 Ack=80 Wm=14720 Len=0 TSval=1025513066 TSecr=3887952709
16811 65.954818	10.19.41.156	10.19.34.216	LDAP	102 endIndRequest(2)
16812 65.954819	10.19.41.156	10.19.34.216	TCP	66 18008 > 16100 [ACK] Seq=1 Ack=80 Wm=14720 Len=0 TSval=1025513068 TSecr=3887952709

3、接着看抓包，用户每次登录时，U-center服务器侧会向LDAP服务器发送的searchrequest的请求报文，注意看此时LDAP服务器侧虽然回应了serchResDone success报文，但是查询结果却是0个，说明在LDAP服务器侧没有查找到该用户，因为没有该用户，所以无法通过该用户的认证，因此Ucenter侧会登录失败。

19902 93.282199	10.19.41.156	10.19.34.216	TCP	66 18032 > 16100 [ACK] Seq=1 Ack=1 Wm=14720 Len=0 TSval=1025540392 TSecr=3887980035
19903 93.282199	10.19.41.156	10.19.34.216	LDAP	143 b1indRequest(2) "uid=sys_jtkpt,ou=applications,o=hise" scope="subtree" sizeLimit=1 timeLimit=2 typesOnly=False
19909 93.283060	10.19.34.216	10.19.41.156	TCP	66 16100 > 18032 [ACK] Seq=1 Ack=80 Wm=29056 Len=0 TSval=1025540392 TSecr=3887980036
19912 93.284152	10.19.34.216	10.19.41.156	LDAP	80 b1indResponse(2) success
19912 93.284150	10.19.41.156	10.19.34.216	TCP	66 18032 > 16100 [ACK] Seq=1 Ack=1 Wm=14720 Len=0 TSval=1025540394 TSecr=3887980037
19914 93.285600	10.19.34.216	10.19.41.156	LDAP	80 searchResDone(2) success [0 results]
19915 93.285619	10.19.41.156	10.19.34.216	TCP	66 18032 > 16100 [ACK] Seq=1 Ack=1 Wm=14720 Len=0 TSval=1025540396 TSecr=3887980038
19916 93.286621	10.19.41.156	10.19.34.216	TCP	66 16100 > 18032 [ACK] Seq=1 Ack=80 Wm=29056 Len=0 TSval=1025540399 TSecr=3887980039
19920 93.286996	10.19.41.156	10.19.34.216	TCP	66 18032 > 16100 [ACK] Seq=1 Ack=1 Wm=14720 Len=0 TSval=1025540400 TSecr=3887980039

4、查看ucenter侧发送给LDAP服务器的serchRequest请求报文详细信息，发现每次发送用户请求时，携带的用户属性都是CN，但是据用户侧反馈，他们LDAP侧的用户属性应该是uid，因为这个用户属性不一致，导致查询不到用户，从而认证失败。

Internet Protocol Version 4, Src: 10.19.41.156 (10.19.41.156), Dst: 10.19.34.216 (10.19.34.216)	
Transmission Control Protocol, Src Port: 18032 (18032), Dst Port: 16100 (16100)	
Lightweight Directory Access Protocol	
LDAPMessage searchRequest(2) "o=hise.com,o=isp" wholeSubtree	
messageID: 2	
protocolOp: searchRequest (3)	
searchRequest	
baseObject: o=hise.com,o=isp	
scope: wholeSubtree (2)	
derefAliases: derefAlways (3)	
sizeLimit: 1	
timeLimit: 2	
typesOnly: False	
Filter: (cn=sys_jtkpt)	
filter: equalityMatch (3)	
attributes: 1 item	
AttributeDescription: cn	
[Response In: 19914]	
controls: 1 item	
Control	

解决方法

根据上面的分析可以知道，认证失败主要是由于Ucenter发送用户请求时携带的用户属性不对，从而导致认证失败。

解决办法：

将Ucenter侧和LDAP服务器对接时用户属性从CN改为UID，如下图所示

管理员DN *

uid=sys_jtkpt,ou=applications,o=hise

管理员密码 *

.....

用户名属性名称 *

uid

高级配置

LDAP服务器要求安全连接 (SSL)

注意事项：

不同局点不同客户的LDAP服务器用户属性配置不一致，具体需要根据用户侧具体的配置进行更改。