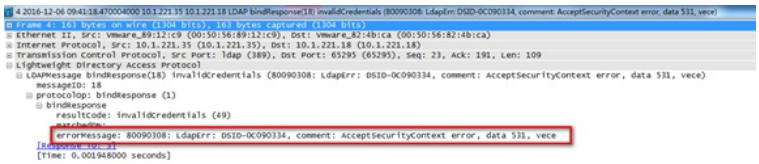
LDAP错误码解析

寻尚岩 2016-12-12 发表

某局点LDAP认证失败，现场反馈的抓包显示LDAP返回错误，但是里面的错误信息仅仅包含一段代码，那么这段代码代表的意义又是啥呢，本文就简单聊一下LDAP错误码，理解了错误码代表的错误信息，就不用怕LDAP认证失败相关的问题了。

首先看一下现场的抓包

展开4号报文如下，标红的错误信息就是LDAP返回的错误码信息，那么这个错误信息应该如何解读呢。



正常情况LDAP返回的错误信息一般是下面这个样子的：

"The exception is [LDAP: error code 49 - 80090308: LdapErr: DSID-0Cxxxxxx , comment: AcceptSecurityContext error, data xxx , vece]."

或者是这个样子的：

“errorMessage：80090308：ldaperr：DSID-0Cxxxxxx , comment: AcceptSecurityContext error, data xxx , vece].”

只要LDAP返回了上面的错误信息，就表示LDAP认证被拒绝了，接下来我们就需要根据上面的错误信息分析认证失败原因。

首先了解一下AD的错误信息代码结构，AD指令错误代码是一段在"data"之后并在"vece"或者"v893"这样文字之前的一段字符。并且这些错误代码伴随着BIND绑定过程返回，所以上面抓包的错误码就是“531”。

常见的错误代码解释如下：

525—用户不存在

52e—密码或凭据无效

530—此时不允许登录

531—在此工作站上不允许登录

532—密码过期

533—账户禁用

701—账户过期

773—用户必须重置密码

775—用户账户锁定

举例：

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 525 , v893,

在上面错误信息里面，错误码是525，该数值是十六进制，表示用户不存在 ，对应的十进制是1317，微软活动目录给出的解释：ERROR_NO_SUCH_USER（指定的账户不存在.）当用户名无效时返回此错误；

解决办法：检查帐号在AD上是否存在，如果使用EIA认证，EIA会直接提示“LDAP上没有该用户”；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 52e, v893 ； 从报错语句看到错误代码是十六进制: 0x52e ， 表示无效的凭证；对应的十进制是1326，表示ERROR_LOGON_FAILURE (登录失败，未知的用户名或者密码错误.) ，一般当用户名有效但是密码或者凭证无效的时候返回。

解决办法：确认域帐号密码是否正确；

LDAP抓包返回如下错误

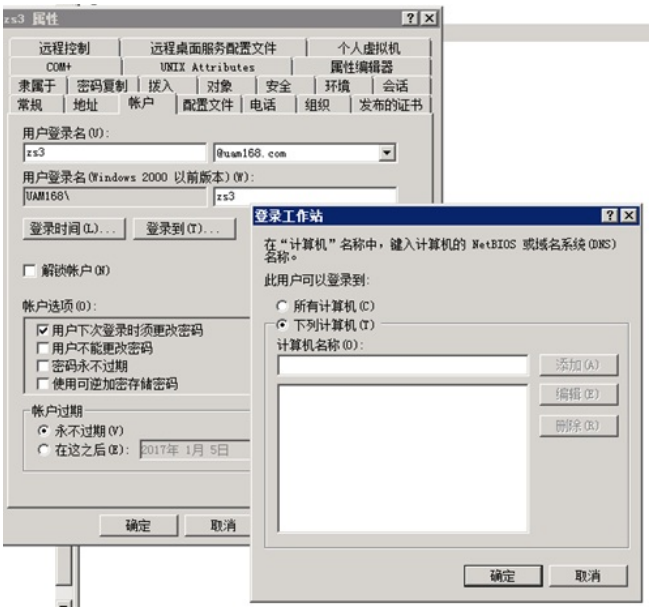
80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 530, v893 ； 错误代码对应的十六进制:是 0x530 ， 表示该时间点禁止登录；对应的十进制数值是1328，微软解释：ERROR_INVALID_LOGON_HOURS (登录失败，登录时间违规.) 。仅当输入了正确的用户名和密码或凭证时才返回此值，说明用户被禁止登录了。

解决办法：检查AD侧配置的登录时间或者取消登录时间限制；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893 ； 错误代码对应的十六进制是0x531，表示此用户禁止在当前工作站登录，对应的十进制是1329，微软解释： ERROR_INVALID_WORKSTATION (登录失败，在此计算机上该用户不允许登录.) LDAP[userWor

kstations: <multivalued list of workstation names>]，仅当输入了正确的用户名和密码或凭证时才返回此值。出现此问题一般是用户限定了登录的计算机，可以查看AD是否配置了下图的登录工作站选项。



解决办法：取消登录工作站限制；如果是采用EIA认证，EIA对这种错误会采取放行处理，即即使AD返回了531错误，EIA也会给接入设备返回Code 2号认证通过报文；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 532, v893；错误码对应的十六进制: 0x532 – 表示密码过期

十进制: 1330 - ERROR_PASSWORD_EXPIRED (登录失败，指定的账户密码过期.)

LDAP[userAccountControl: <bitmask=0x00800000>] - PASSWORDEXPIRED 仅当输入了正确的用户名和密码或凭证时才返回此值。

解决办法：重置域帐号密码；如果是采用EIA认证，EIA对这种错误会采取放行处理，即即使AD返回了532错误，EIA也会给接入设备返回Code 2号认证通过报文；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 533, v893 ； 错误码对应的十六进制: 0x533 - 账户被禁用

十进制: 1331 - ERROR_ACCOUNT_DISABLED (登录失败，账户当前被禁用了.)； LDAP[userAccountControl: <bitmask=0x00000002>] - ACCOUNTDISABLE ，当输入了正确的用户名和密码或凭证时才返回此值。

解决办法：取消禁用帐号选项；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 701, v893；错误码对应的十六进制: 0x701 - 账户已过期

对应的十进制: 1793 - ERROR_ACCOUNT_EXPIRED (用户账户已过期.) LDAP[accountExpires: <value of -1, 0, or extemely large value indicates account will not expire>] - ACCOUNTEXPIRED ，当输入了正确的用户名和密码或凭证时才返回此值。

解决办法：调整帐号的失效时间；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 773, v893；对应的十六进制: 0x773 - 账户密码必须被重置

十进制: 1907 - ERROR_PASSWORD_MUST_CHANGE (用户密码在第一次登录之前必须修改.)；LDAP[pwdLastSet: <value of 0 indicates admin-required password change>] - MUST_CHANGE_PASSWD ，只有输入了正确的用户名和密码或凭证时才返回此值。

解决办法：在AD侧修改帐号密码；如果是采用EIA认证，EIA对这种错误会采取放行处理，即即使AD返回了773错误，EIA也会给接入设备返回Code 2号认证通过报文；

LDAP抓包返回如下错误

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 775, v893

十六进制: 0x775 ， 表示账户被锁定

十进制: 1909 - ERROR_ACCOUNT_LOCKED_OUT (账户当前已被锁定，不允许登录The referenced account is currently locked out and may not be logged on to.) LDAP[userAccountControl: <bitmask=0x00000010>] - LOCKOUT ， 需要注意的是即便是输入了错误的密码也可能返回此值。

解决办法：确认帐号是否被锁定或者密码是否错误。