安盟多因素身份认证系统网络代理认证客户端
LDAP 认证
管理员手册

四川安盟电子信息安全有限责任公司

2023 年 08 月

版本管理

版本	摘要	编　　者	日期
1.00	基本安装配置《安盟多因素身份认证系统-部署手册》	胡云辉	2023/07/04
1.01	整理成为独立的管理手册	陈俊	2023/08/15
1.02	客户端增加配置脚本说明	陈俊	2023/08/15

目录

目录

1 概述 4
2 启用 LDAP 目录服务 4
2.1 安装 LDAP 服务 4
2.2 检查 ldap 服务状态 5
2.3 配置 ldap 服务证书 5
2.4 配置账号同步插件 8
2.5 服务监控脚本 9
3 LDAP 测试认证 9
3.1. 客户端地址 9
3.2. 部署用户 9
3.3. 设置 yum 源 9
3.4. 设置时间 9
3.5. 安装配置 10
3.6. 登录测试 12
3.7. 自定义 PAM 登录配置 12
3.8. PAM 扩展 13

1 概述

安盟多因素身份认证系统 网络代理认证客户端 LDAP 协议认证，后文简称 LDAP 认证。LDAP 认证是安盟认证系统创新开发的认证功能，可以融合现有网络的 LDAP 认证协议，通过安盟认证进行第二次封装，实现由安盟认证系统统一认证的效果。启用后可以接管现有的 LDAP 认证。可以让客户端的输入转变成为安盟动态口令认证。

2 启用 LDAP 目录服务

2.1 安装 LDAP 服务

根据以下步骤安装 LDAP 服务：

cd /data/app/anmeng-9.0_2.2.XX-linux-x86_64_full/anmeng-ldap

./install_ldap.sh

```
[root@acesecond ~]# cd /data/app/anmeng-9.0_2.2.XX-linux-x86_64_full/anmeng-ldap
[root@acesecond anmeng-ldap]# ls
anmeng-ds-2.2.XX.tar.gz      install_ldap.sh                                  phpldapadmin.conf
anmeng-ldap-1.0.0.tar.gz    ltb-project-openldap-initscript-2.5.tar.gz    scripts
[root@acesecond anmeng-ldap]# ./install_ldap.sh
ACE_HOME:/data/app/aceserver
stop slapd...
uncompressioning anmeng-ldap-1.0.0.tar.gz file.....
please wait a few minutes.....
unzip ltb-project-openldap-initscript-2.5.tar.gz
Note: Forwarding request to 'systemctl enable slapd.service'.
slapd: [INFO] Using built-in configuration - this may cause some problems
slapd: [INFO] Launching OpenLDAP configuration test...
slapd: [OK] OpenLDAP configuration test successful
slapd: [INFO] Halting OpenLDAP...
slapd: [INFO] Can't read PID file, to stop OpenLDAP try: /data/app/aceserver/anmeng-ldap/sbin/slapd forcestop
slapd: [INFO] Launching OpenLDAP database recovery...
slapd: [OK] OpenLDAP /data/app/aceserver/anmeng-ldap/var/openldap-data database recovery successful
slapd: [INFO] Launching OpenLDAP...
slapd: [OK] File descriptor limit set to 2048
slapd: [OK] OpenLDAP started
……
# extended LDIF
#
# LDAPv3
# base <dc=anmengds,dc=local> with scope subtree
```

```
# filter: (objectclass=*)
# requesting: ALL
#


# anmengds.local
dn: dc=anmengds,dc=local
objectClass: dcObject
objectClass: organization
dc: anmengds
o: Anmeng Security LTD
description: Anmeng Directory Server

# ldapadmin, anmengds.local
dn: cn=ldapadmin,dc=anmengds,dc=local
objectClass: organizationalRole
cn: ldapadmin
description: Directory Manager

# otp, anmengds.local
dn: cn=otp,dc=anmengds,dc=local
objectClass: posixGroup
objectClass: top
cn: otp
gidNumber: 5000

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
```

2.2 检查 ldap 服务状态

```
[root@acesecond anmeng-ldap]# netstat -ntulp | grep -E '389|636'
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      95957/slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      95957/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      95957/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      95957/slapd
```

2.3 配置 ldap 服务证书

首先，请确定在主服务器上已经配置好了 ldap 服务证书，并将/etc/openldap/ssl 复制出

来了。

将从主服务器上复制出来的 ssl 目录复制到备服务器的/etc/openssl/目录中，并将目录权限设置为 755。

```
[root@acesecond openldap]# chmod -R 755 /etc/openldap/ssl/

[root@acesecond openldap]# ls -l /etc/openldap/ssl/

total 16

-rwxr-xr-x 1 root root 1350 May 10 14:47 cacert.pem

-rwxr-xr-x 1 root root 3728 May 10 14:47 ldapcert.pem

-rwxr-xr-x 1 root root    655 May 10 14:47 ldap.csr

-rwxr-xr-x 1 root root    887 May 10 14:47 ldapkey.pem
```

修改$ACE_HOME/anmeng-ldap/etc/openldap/slapd.conf，在 TLSCipherSuite 后面增加以下配置

```
TLSCACertificateFile /etc/openldap/ssl/cacert.pem

TLSCertificateFile /etc/openldap/ssl/ldapcert.pem

TLSCertificateKeyFile /etc/openldap/ssl/ldapkey.pem
```

详细步骤如下：

```
[root@acesecond ~]#    cd $ACE_HOME/anmeng-ldap/etc/openldap

[root@acesecond openldap]#

[root@acesecond openldap]# vim slapd.conf

……

rootdn "cn=ldapadmin,dc=anmengds,dc=local"

rootpw {SSHA}TlDlKuGgkzLfRF1iN1l7jgPfYvti7+p2



directory /data/app/aceserver/anmeng-ldap/var/openldap-data

index objectclass,entryCSN,entryUUID eq



TLSProtocolMin 3.3

TLSCipherSuite ECDHE-RSA-AES256-SHA384:AES256-SHA256:!RC4:HIGH:!MD5:!aNULL:!EDH:!EXP:!SSLV2:!eNULL

TLSCACertificateFile /etc/openldap/ssl/cacert.pem

TLSCertificateFile /etc/openldap/ssl/ldapcert.pem
```

```
TLSCertificateKeyFile /etc/openldap/ssl/ldapkey.pem


[root@acesecond openldap]# rm -rf slapd.d/*

[root@acesecond openldap]# ../../sbin/slaptest -f ./slapd.conf -F ./slapd.d/

63f625f3 mdb_monitor_db_open: monitoring disabled; configure monitor database to enable

config file testing succeeded

[root@acesecond openldap]#

[root@acesecond openldap]#    systemctl restart slapd

[root@acesecond openldap]#
```

最后运行以下命令验证证书：

openssl s_client -connect 192.168.0.169:636 -showcerts -state -CAfile /etc/openldap/ssl/cacert.pem

```
[root@acesecond openldap]# openssl s_client -connect 192.168.0.169:636 -showcerts -state -CAfile /etc/openldap/ssl/cacert.pem

CONNECTED(00000003)

SSL_connect:before/connect initialization

SSL_connect:SSLv2/v3 write client hello A

SSL_connect:SSLv3 read server hello A

depth=1 C = CN, ST = BeiJing, L = BeiJing, O = anmeng.com, OU = IT, CN = ca.anmeng.com

verify return:1

depth=0 C = CN, ST = BeiJing, O = anmeng.com, OU = IT, CN = 192.168.0.253

verify return:1

SSL_connect:SSLv3 read server certificate A

……

    TLS session ticket:

    0000 - c3 47 72 9b b5 e9 a0 f2-45 58 bd ac 4d df c5 8c      .Gr.....EX..M...

    0010 - fd 83 d1 8e 37 6c bf c8-0c 9c 8a 6b 49 22 11 99      ....7l.....kI"..

    0020 - f0 f0 00 ef fd 0e 64 f4-da a0 e2 16 cb 6d 39 b9      ......d......m9.

    0030 - 8c 24 1a a5 f6 17 b8 62-c1 a8 2a 88 e7 74 0f df      .$.....b..*..t..

    0040 - b3 1a 1d ee dd 2a 5a f1-8a 37 41 37 5d 5c 01 24      .....*Z..7A7]\.$

    0050 - c4 32 50 6b 52 91 2a 25-86 f1 62 45 6d 95 84 6b      .2PkR.*%..bEm..k

    0060 - bd d8 ce f7 96 96 79 fb-92 2c 0e c3 93 99 f7 24      ......y..,.....$
```

```
0070 - da 9c e6 fc d0 ca 66 22-ab 49 b0 bf f8 4d 15 b3      ......f".I...M..

0080 - 69 XX 41 d5 21 26 80 ad-cd 47 47 66 b4 7c 1e 5d      i.A.!&...GGf.|.]

0XX0 - 30 0f 30 a4 2c 8f 82 0a-38 33 45 b0 53 c1 61 72      0.0.,...83E.S.ar



Start Time: 1676781349

Timeout     : 300 (sec)

Verify return code: 0 (ok)

Extended master secret: no
```

注：当出现 Verify return code:0(ok)时，表示该工具运行完成，请按 ctrl+c 退出。

2.4 配置账号同步插件

LDAP 服务要同步安盟认证系统的账号，还需要通过 sysadmin 登录到主服务的后台管理系统，用备服务器的地址注册类型为目录服务的组件，然后登录到服务器后台，执行以下命令：

cd $ACE_HOME/anmeng-ldap/bin

./dsinit

根据提示输入主 core 服务的地址、服务端口和 sysadmin 的密码

./startup.sh

```
[root@acesecond scripts]# cd $ACE_HOME/anmeng-ldap/bin

[root@acesecond bin]# ls

dsinit        ldapadd         ldapdelete    ldapmodify    ldappasswd    ldapurl        shutdown.sh

dssyncsrv     ldapcompare     ldapexop      ldapmodrdn    ldapsearch    ldapwhoami     startup.sh

[root@acesecond bin]# ./dsinit

Do you want to initialize the database of this component? ('y' or 'n')y

Please input master server address: 192.168.0.253                主core服务的地址，需根据实际环境调整。

Please input master server port: 6580                            主core服务端口（默认是6580）

Please input the password of sysadmin:                           sysadmin的密码

sync data,please wait a few minutes.....

The component has been initialized.

[root@acesecond bin]# ./startup.sh

[root@acesecond bin]# ps -ef | grep dssyncsrv

root       1625545       1   0 10:59 pts/3       00:00:00 ./dssyncsrv
```

2.5 服务监控脚本

安盟认证系统自带服务监控脚本，通过系统的任务计划设置每隔 2 分钟探测一次系统的服务是否正常。

```
[root@acesecond bin]# crontab -l
59 23 * * * /data/app/aceserver/anmeng-core/bin/daily_task.sh >> /var/log/ace_daily.log 2>&1
@reboot /data/app/aceserver/auditserver.sh >> /var/log/anmeng_audit_reboot.log 2>&1
#*/2 * * * * /data/app/aceserver/auditserver.sh >> /var/log/anmeng_audit.task.log 2>&1
```

默认每隔 2 分钟检测服务的配置是注释状态，如需启用，将“#”号删除即可。

3 LDAP 测试认证

3.1. 客户端地址

192.168.0.118，请根据实际环境进行调整。

3.2. 部署用户

OS 系统配置双因子认证功能，需采用 root 用户。如果 root 用户无法通过 xshell 等工具直接通过 ssh 服务连接到服务器，可能是 ssh 启用了禁用 root 登录的配置，请参考 root 账号无法通过 ssh 登录解除禁用。

3.3. 设置 yum 源

OS 系统配置双因子认证功能，需要用到 sssd 服务，如果没有安装 sssd 服务，可以通过 `yum install sssd` 进行安装，此时，需要确保有可用的 yum 源，如果没有 yum 源，可参考设置 yum 源。

3.4. 设置时间

确保服务器的时间和北京时间相同，如采用 ntpdate 命令同步网络时间。

```
[root@client ~]# ntpdate ntp1.aliyun.com
19 Feb 11:35:19 ntpdate[24584]: step time server 120.25.115.20 offset -28800.399087 sec
[root@client ~]# date
Sun Feb 19 11:35:21 CST 2023
[root@client ~]#
```

如果服务器不能联接外网，则无法读取网络时间，可通过 date 命令手动设置时间。

```
[root@client ~]# date -s ‘2023-03-27 11:34:21’
Sun Feb 19 11:35:21 CST 2023
```

3.5. 安装配置

```
#/bin/bash
#set -e
#########################################################
#功能：ldap客户端的安装配置脚本
#版本：1.0
#用法：  1）先将证书文件cacert.pem和脚本放在同一目录中
#       2）运行脚本的时候，可带4个参数，不带参数时，请设置运行参数(deploy_mode,auth_mode,ldapserver_ip,white_list)或根据提示进行操作。
#           参数1：部署模式[install|uninstall|switch]，install：安装与配置，uninstall：卸载还原，switch：切换sshd的认证模式
#           参数2：认证模式[1|2|3]，
#               1：同时支持本地和双因子账号登录
#               2：只允许本地的root和双因子账号登录
#               3：支持本地白名单和双因子账号登录
#           参数3：ldap服务地址。注意：如果部署模式为switch，该参数为本地白名单列表。
#           参数4：本地白名单列表，多个以英文冒号(:)分隔，如user1:user2
#           如：sh install_ldap_client.sh install 3 192.168.1.151 user1:user2，
#               表示安装配置ldap客户端，ldap服务器的地址为192.168.1.151，并将sshd的认证模式设置为"支持本地白名单和双因子账号登录"
#               本地白名单的内容为user1:user2
#
#########################################################
```

请上传安装配置脚本 ldap-authconf 目录到服务器，如/opt 目录中，包括安装配置脚本：install_ldap_client.sh（在工具软件/Linux 客户端配置脚本目录中）、卸载脚本：uninstall_ldap_client.sh(在工具软件/Linux 客户端配置脚本目录中)和证书 cacert.pem（从主服务器的/etc/openldap/ssl 目录中获取），完整的文件列表如下所示：

```
[root@ecs-anmng-arm-c91c ldap-authconf]# ls -l
total 20
-rw------- 1 root root 1350 May 29 16:34 cacert.pem
-rwx------ 1 root root 8865 May 29 16:34 install_ldap_client.sh
-rwx------ 1 root root 2991 May 29 16:34 uninstall_ldap_client.sh
[root@ecs-anmng-arm-c91c ldap-authconf]#
```

在运行安装配置脚本之前，需先修改脚本中关于 LDAP 服务器的地址和域名。

vim install_ldap_client.sh

```
#/bin/bash
#set -e
############################
#这是一个ldapclinet的安装脚本
############################

############################
#填写ldap服务端IP地址，需根据实际环境进行调整。
ldapserver_ip=192.168.0.216
#请填写ldap服务器端口
ldapserver_port=636
#日志名称
monitor_log=install_ldap.log
#域名
dc_name1=anmengds
dc_name2=local
……
```

验证证书是否有效（192.168.0.216 为本文档环境中的负载地址，需根据实际环境进行调整）：

openssl s_client -connect 192.168.0.216:636 -showcerts -state -CAfile /opt/ldap-authconf/cacert.pem

```
[root@client ldap-authconf]# openssl s_client -connect 192.168.1.60:636 -showcerts -state -CAfile /opt/ldap-authconf/cacert.pem
```

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=1 C = CN, ST = BeiJing, L = BeiJing, O = anmeng.com, OU = IT, CN = ca.anmeng.com
verify return:1
depth=0 C = CN, ST = BeiJing, O = anmeng.com, OU = IT, CN = 192.168.1.60
    0000 - c9 43 11 36 4e fc 00 b4-17 60 f1 f9 6d b3 32 49      .C.6N....`..m.2I
    0010 - a0 af 63 48 d3 e4 66 28-6c 07 25 f9 24 81 d0 b2      ..cH..f(l.%.$...
    0020 - 20 50 9d b5 e9 4a fb 40-b1 ff 5c 75 9b 8b a0 48       P...J.@..\u...H
    0030 - 34 d5 47 44 23 26 ac 50-4a XX 9a 86 c9 21 32 f3      4.GD#&.PJ....!2.
    0040 - 2b bb b6 2f 7e 36 06 b8-40 20 b3 f7 48 f0 78 0b      +../~6..@ ..H.x.
    0050 - c8 47 54 4f 9a ba 67 ed-90 6a 93 e5 13 1d 5c eb      .GTO..g..j....\.
    0060 - 43 87 a3 cf dc 78 25 7a-0f 89 3c 9a 80 f6 f1 21      C....x%z..<....!
    0070 - dd 81 5d ce aa e8 7f 8a-cc db 6e a0 a3 59 d6 fb      ..].......n..Y..
    0080 - fb b4 0b 64 4f fd 81 ac-70 c5 3d e1 eb 4e 2d 6e      ...dO...p.=..N-n
    0XX0 - 3a 1f 8a c9 cb 27 d8 70-86 fc e9 50 d0 80 e0 f8      :....'.p...P....

    Start Time: 1676797538
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
```

注：当出现 Verify return code:0(ok)时，表示该工具运行完成，请按 ctrl+c 退出。

运行配置脚本自动配置

cd /opt/ldap-authconf

./install_ldap_client.sh （需检查该脚本是否有执行权限，如果没有，需通过 chmod +x install_ldap_client.sh 命令为其添中可执行权限。）

```
[root@aceprimary ldap-authconf]# ls -l
total 16
-rw-r--r--. 1 root root 1330 Apr  4 15:47 cacert.pem
-rw-r--r--. 1 root root 9103 Apr  4 15:47 install_ldap_client.sh
[root@aceprimary ldap-authconf]# chmod +x install_ldap_client.sh
[root@aceprimary ldap-authconf]# ls -l
total 16
-rw-r--r--. 1 root root 1330 Apr  4 15:47 cacert.pem
-rwxr-xr-x. 1 root root 9103 Apr  4 15:47 install_ldap_client.sh
[root@client ldap-authconf]# ./install_ldap_client.sh
ls: cannot access /etc/sssd/sssd.bak-anmeng-*: No such file or directory
ls: cannot access /etc/nsswitch.bak-anmeng-*: No such file or directory
ls: cannot access /etc/pam.d/sshd.bak-anmeng-*: No such file or directory
安装开始
正在存放证书
等待中:[================================================== ][100%]
证书存放完成
```

```
sssd正在安装，请等待:
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Package sssd-1.16.0-19.5.h5.eulerosv2r7.x86_64 already installed and latest version
Nothing to do
等待中:[================================================== ][100%]
SSSD安装完毕，结果如下:
SSSD安装成功
开始修改/etc/sssd/sssd.conf
……
开始修改/etc/pam.d/sshd
开始检查/etc/pam.d/sshd是否存在...
检测/etc/pam.d/sshd已存在，开始备份文件，请稍后...
等待中:[================================================== ][100%]
备份已完成，备份文件为/etc/pam.d/sshd.bak-anmeng-2023-03-12,22:03:03
开始修正配置文件/etc/pam.d/sshd,请稍后...
等待中:[================================================== ][100%]
修改完毕，查看修改后的内容
session     optional      pam_mkhomedir.so umask=0077
安装完成！
[root@client ldap-authconf]# id test1 (注：test1是在2.2.3.2创建测试账号中创建的)
uid=5003(test1) gid=5000(otpuser) groups=5000(otpuser)
[root@client ldap-authconf]#
```

显示正常即 OK。

3.6. 登录测试

通过 SSH 工具登录，登录成功后，会在后台生成一条认证日志，此时可能通过 auditadmin（默认密码为 Anmeng12#$）登录到 https://192.168.0.253:8443/（请根据实际环境调整地址）查看日志。

认证时间	认证用户	认证主机	受影响对象	认证结果	认证来源	来源地址	租户名称
2023-05-29 16:46:25	test1	192.168.0.118	域口令	LDAP认证成功	directory	192.168.0.169	公共资源区
2023-05-29 16:46:18	test1	192.168.0.118	00000000000005	登录成功	directory	192.168.0.169	公共资源区

3.7. 自定义 PAM 登录配置

通过 install_ldap_client.sh 脚本默认允许 os 服务器本地账号和双因子账号（LDAP 账号加动态密码）都可以登录，即 os 服务器本地账号可以通过本地的静态密码登录到服务器，也可以通过双因子账号登录到服务器。

除上述配置外，我们还可以设置成只允许双因子账号登录，本地非 root 账号不能登录，具体配置是修改/etc/pam.d/sshd，修改 auth 部分，格式如下：

```
#%PAM-1.0
#双因子账号能登录
#但本地有账号时，双因子账号不能登录
```

```
#auth            required        pam_sepermit.so
#auth            required        pam_env.so
#auth            [success=done default=die]     pam_unix.so
#auth            sufficient      pam_sss.so
#auth            required        pam_deny.so

#本地账号和双因子账号都能登录
#auth            required        pam_sepermit.so
#auth            required        pam_env.so
#auth            sufficient      pam_unix.so
#auth            sufficient      pam_sss.so
#auth            required        pam_deny.so

#双因子账号能登录
#本地仅root账号可以登录，非root账号不能登录
auth            required        pam_sepermit.so
auth            required        pam_env.so
auth            sufficient      pam_sss.so
auth            requisite       pam_succeed_if.so uid = 0
auth            sufficient      pam_unix.so
auth            required        pam_deny.so
```

注：上述配置保存后立即生效，为防止配置错误导致无法登录，请多连接一个 SSH 会话。

本地账号和双因子账号不允许同名。

3.8. PAM 扩展

可通过 pam_access.so 来控制可访问的用户，配置如下：

1、先在/etc/pam.d/sshd 中，增加 auth required pam_access.so，如下所示：

```
auth        required      pam_sepermit.so
auth        required      pam_env.so
auth        sufficient    pam_sss.so
#auth        requisite     pam_succeed_if.so user in root:dbuser:appuser
auth        required      pam_access.so
auth        sufficient    pam_unix.so
auth        required      pam_deny.so
```

上述配置表示，优先通过 pam_sss.so 去 ldap 上进行认证，认证成功后，立即返回，认证失败后，调用 pam_access.so 模块检查登录规则，如果是被允许的账号登录，则调用本地验证。

2、pam_access.so 会读取配置文件：/etc/security/access.conf，在该文件中，增加以下配置：

```
+:root:ALL
+:dbuser:ALL
-:ALL:ALL
```

+:root:ALL 表示允许 root 从任何地方登录，最后一个 ALL 表示登录地址，可以是 ipv4 或 ipv6。
+:dbuser:ALL 表示允许 dbuser 从任何地方登录
-:ALL:ALL 表示禁止其他用户登录

pam_succeed_if.so 的用法

```
auth        required      pam_sepermit.so
auth        required      pam_env.so
# 判断用户名是否不在root:dbuser:appuser列表中
#success = ignore表示如果此测试成功,则忽略此行并继续正常，即执行pam_sss.so
#default = 1表示在所有其他情况下，跳过下一行，即执行pam_succeed_if.so user in root:dbuser:appuser
auth        [default=1 success=ignore] pam_succeed_if.so user notin root:dbuser:appuser
auth        sufficient    pam_sss.so
auth        requisite     pam_succeed_if.so user in root:dbuser:appuser
auth        sufficient    pam_unix.so
auth        required      pam_deny.so
```