

安盟多因素身份认证系统  
SHELL 网络代理认证客户端  
(V2.03)



安盟（中国）电子信息安全有限责任公司

2020 年 02 月

## 版本管理

版本	摘要	作者	日期
1.00	基本配置	陈俊	2020/02/13
1.01	增加修改 passwd 操作	陈俊	2020/02/13
1.02	增加 LDAP 配置	陈俊	2020/02/14
1.03	重命名为安盟 SHELL 网络代理认证客户端	陈俊	2020/12/12
1.04	增加文件说明；authvar.ini 重命名为 authvar.ini	陈俊	2020/12/12
1.05	增加主机登录 amshell 验证保护；去除账户 2 次认证	陈俊	2020/12/23
1.06	去除复制 authvar.ini 文件操作	陈俊	2020/12/28

## 目录

## 目录

1	概述.....	1
2	安装文件.....	1
2.1	安装包文件.....	1
2.2	安装配置文件.....	1
3	安装准备.....	1
3.1	服务器端设置.....	1
3.2	客户端设置.....	2
3.2.1	安装包放置位置.....	2
3.2.2	配置文件放置位置.....	2
4	安装与卸载.....	2
4.1	安装 SHELL 程序.....	2
4.2	卸载 SHELL 程序.....	2
5	客户端直接认证测试.....	3
5.1	用户名测试.....	3
5.2	用户名口令码测试.....	3
5.3	客户端标准测试.....	3
5.4	口令直接认证测试.....	4
5.5	测试登录.....	4
5.5.1	修改 passwd 文件.....	4
5.5.2	直接使用 ssh 方式登录.....	5
6	客户端应用配置.....	5
6.1	主机 amshell 登录保护.....	5
6.1.1	设防.....	5
6.1.2	撤防.....	6
6.2	OpenLDAP 修改 loginshell 为 amshell.....	6
6.2.1	创建用户.....	7
6.2.2	修改 loginShell.....	8
6.2.3	测试登录.....	8

# 1 概述

安盟 SHELL 网络代理认证客户端是安盟身份认证系统客户端。主要用来对使用拨号登录的账户进行二次认证。操作系统 shell 登录方式是基本登录操作方式，远程用户预备访问中心服务器，都是通过 shell 方式先进行远程连接拨号验证。由于各个系统供应商都有自己的 shell 系统，常见的都有 bash, csh, sh, tcsh, ksh, zsh 等类型。尽管各种 shell 的登录机制也不尽相同，但登录成功后，都要需要指定账户文件路径和登录脚本。安盟 SHELL 客户端就是针对登录脚本设计。

## 2 安装文件

### 2.1 安装包文件

AnmengShell\_AgentV2.0X.tar

### 2.2 安装配置文件

sdconf.rec

## 3 安装准备

### 3.1 服务器端设置

在安盟认证服务器上

- 添加测试账户，
- 添加保护主机为代理主机
- 导出配置文件 sdconf.rec

## 3.2 客户端设置

### 3.2.1 安装包放置位置

以管理员身份登录服务器，在根目录下创建 `anmeng` 目录。将安装包和服务器配置文件 `sdconf.rec` 上传到该目录。

解压安装包，可以得到一个 `amshell` 的文件夹。

```
chmod 777 AnmengShell_AuthAgent2.xx.tar
tar xvf AnmengShell_AuthAgent2.xx.tar
```

### 3.2.2 配置文件放置位置

以管理员身份登录，在 `/var` 目录下创建 `ace` 目录，上传配置文件 `sdconf.rec`，放置 `/var/ace` 目录下。

## 4 安装与卸载

### 4.1 安装 SHELL 程序

```
cd /amshell
chmod 777 install_shell.sh
./install_shell.sh
```

### 4.2 卸载 SHELL 程序

注意：卸载 `amshell` 之前，先要撤防，去除安盟保护，才可以进行卸载操作。具体操作请转到本手册第 7 章 7.1.2 撤防。

```
cd /amshell
./uninstall.sh
```

## 5 客户端直接认证测试

客户端直接连接认证服务器测试，是用来验证客户端到认证服务器之间消息是否通达。

只有测试成功，才可以进行下一步应用配置。

### 5.1 用户名测试

指定用户名直接认证测试。

用法：amshell -u User-Name

```
# amshell -u xiaoan
```

### 5.2 用户名口令码测试

指定用户名和口令码直接认证测试。

用法：amshell -u User-Name -p Passcode

```
# amshell -u xiaoan -p Anmeng12#$
```

注意，该方式密码部分为可见内容，可以作为其它脚本调用内容。

### 5.3 客户端标准测试

客户端模拟登录标准认证测试，可以完成创建 PIN 码，响应下一令牌码等操作。

用法：amshell -t

```
# amshell -t
```

## 5.4 口令直接认证测试

Unix 系统当前账户认证测试，是用来验证口令内容是否正常。可以用来响应认证系统“需要修改密码”的策略。

用法：amshell -p Passcode

```
# amshell -p Anmeng12#$
```

## 5.5 测试登录

安盟 shell 认证客户端，其中测试模式也就是进入保护设防状态，修改配置文件后立即生效。

### 5.5.1 修改 passwd 文件

```
vim /etc/passwd
```

例如：用户 anmng，将/bin/bash 修改为/bin/amshell

```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
anmeng:x:1000:1000:anmeng:/home/anmeng:/bin/amshell
saslauthd:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radiusd:x:95:95:radiusd user:/var/lib/radiusd:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/sbin/nologin
~
~
~
```

保存，退出。

## 5.5.2 直接使用 ssh 方式登录

```
[root@TEST171 ~]# vim /etc/passwd
[root@TEST171 ~]# ssh anmeng@192.168.0.171
anmeng@192.168.0.171's password:
Last login: Fri Feb 14 09:59:58 2020 from 192.168.0.20
user:anmeng
enter get securid file.
node path /var/ace/securid
open okconnect
input your Password:
auth by node.
Auth OK
[anmeng@TEST171 ~]$
```

测试返回认证成功，表示安盟 SHELL 认证客户端安装正常。

# 6 客户端应用配置

## 6.1 主机 amshell 登录保护

### 6.1.1 设防

启动代理认证，设置本地认证为安盟认证。

- 1, 备份 passwd 文件, cp /etc/passwd /etc/passwd\_00
- 2, 修改 passwd 文件, vim /etc/passwd
- 3, 修改/bin/bash 为/bin/amshell

例如：用户 anmng, 将/bin/bash 修改为/bin/amshell



```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
anmeng:x:1000:1000:anmeng:/home/anmeng:/bin/amshell
saslauthd:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radiusd:x:95:95:radiusd user:/var/lib/radiusd:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/sbin/nologin
~
~
~
```

4, 保存, 退出。

## 6.1.2 撤防

关闭代理认证, 去除安盟认证, 还原系统本地认证。

- 1, 以管理员身份登录主机编辑 passwd, vim /etc/passwd
- 2, 找到对应的账户, 修改 amshell 为系统默认 bash
- 3, 保存退出

注意, 每个系统默认的 shell 类型不是一样, 可以参考未设置安盟的账号类型, 进行仿照修改。

到此, 主机 amshell 登录配置完成。

## 6.2 OpenLDAP 修改 loginshell 为 amshell

LDAP 系统本身可以指定启动 shell 类型, 如果调用 amshell 类型, 启动成功后直接启用安盟认证。

## 6.2.1 创建用户

假设创建账户张三，账号 zhangsan，LDAP 密码 123456

服务器: Local LDAP Server Container (容器) : dc=teracloud2,dc=cn  
 标题: Generic User Account (posixAccount)

新建用户账号 (Step 1 of 1)

第一个名字 alias: cn

最后一个名字 alias: cn

Common Name alias: cn

User ID alias: cn

密码 alias: cn  
   
 (confirm)  
[Check password...](#)

UID号 alias: cn

GID号 alias: cn

Home directory alias: cn

Login shell alias: cn

1.2.3  
SOURCEFORGE

注意: Login shell 必须选择一个 shell 方式, 否则确认信息无法显示 login shell

服务器: Local LDAP Server Container (容器) : dc=teracloud2,dc=cn

Create LDAP Entry

Do you want to create this entry?

属性	新值	跳过
<b>cn= zhangsan,dc=teracloud2,dc=cn</b>		
Last name	zhangsan	<input type="checkbox"/>
Common Name	zhangsan	<input type="checkbox"/>
User ID	zhangsan	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1002	<input type="checkbox"/>
GID Number	500	<input type="checkbox"/>
Home directory	/home/users/zhangsan	<input type="checkbox"/>
Login shell	/bin/sh	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount	<input type="checkbox"/>

1.2.3  
SOURCEFORGE

提交并保存。

## 6.2.2 修改 loginShell

将原有的 /bin/sh 替换为 /bin/amshell



The screenshot shows a user modification interface for 'cn=zhangsan'. The 'loginShell' field is highlighted with an orange box and contains the value '/bin/amshell'. Other fields include 'homeDirectory' with '/home/users/lisi' and 'objectClass' with 'inetOrgPerson' and 'posixAccount'.



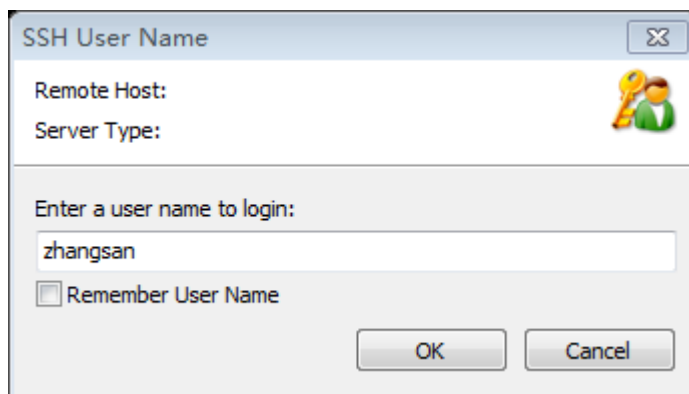
The screenshot shows a confirmation dialog box titled 'cn=zhangsan'. It asks '你想应用这些变化吗?' (Do you want to apply these changes?). Below the question is a table with columns for '属性' (Attribute), '旧值' (Old Value), '新值' (New Value), and '跳过' (Skip). The table shows 'loginShell' with old value '/bin/sh' and new value '/bin/amshell'. There is an unchecked checkbox in the '跳过' column. Below the table are 'Update Object' and '取消' (Cancel) buttons.

属性	旧值	新值	跳过
loginShell	/bin/sh	/bin/amshell	<input type="checkbox"/>

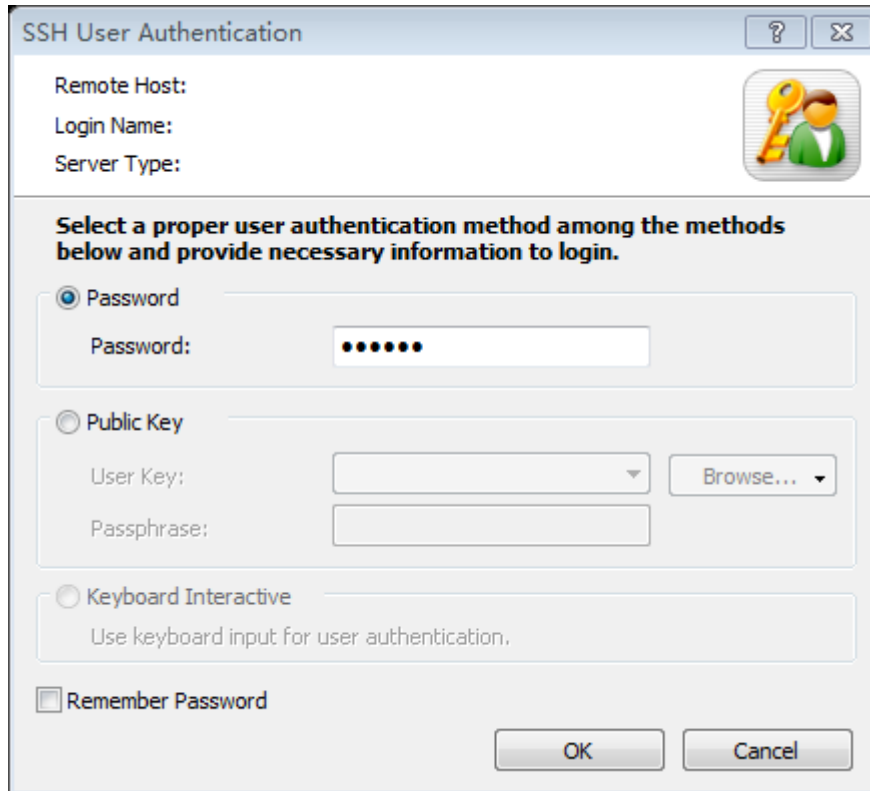
1.2.3  
SOURCEFORGE

提交并保存。

## 6.2.3 测试登录



The screenshot shows an 'SSH User Name' dialog box. It has fields for 'Remote Host:' and 'Server Type:'. Below these is a text input field with the user name 'zhangsan' entered. There is a checkbox for 'Remember User Name' which is unchecked. At the bottom are 'OK' and 'Cancel' buttons.



The image shows a Windows-style dialog box titled "SSH User Authentication". It has a title bar with a question mark and a close button. The dialog is divided into several sections. At the top, there are labels for "Remote Host:", "Login Name:", and "Server Type:". To the right of these labels is a small icon of a person with a key. Below this, there is a bold instruction: "Select a proper user authentication method among the methods below and provide necessary information to login." There are three radio button options: "Password" (which is selected), "Public Key", and "Keyboard Interactive". The "Password" section has a "Password:" label and a text input field containing seven black dots. The "Public Key" section has a "User Key:" label, a dropdown menu, and a "Browse..." button. Below it is a "Passphrase:" label and a text input field. The "Keyboard Interactive" section has a label and a text input field with the text "Use keyboard input for user authentication." At the bottom left, there is a checkbox labeled "Remember Password". At the bottom right, there are "OK" and "Cancel" buttons.

输入 LDAP 密码 123456。

```
WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Fri Feb 14 14:37:01 2020 from 192.168.0.20
user:zhagsan
enter get securid file.
node path /var/ace/securid
open okconnect
input your Password:
auth by node.
Auth OK
'abrt-cli status' timed out
[zhagsan@TEST171 ~]$ █
```

输入安盟动态口令。