凝思厂站内网主机安全监管软件 V2.0-R2.6.3 安装使用说明书

V1.0

北京凝思软件股份有限公司

四川凝思软件有限公司

目录

1 概述

该文档是用于凝思厂站内网主机安全监管软件 V2.0-R2.6.3 产品的安装使用说明。下面详细介绍了凝思厂站内网主机安全监管软件的安装过程以及配置本软件的方法。

凝思厂站内网主机安全监管软件简称为:**厂站 agent**

1.1 文档使用范围

文档版本号	安装步骤适用于厂站内网主机安全监管软件
V1.0	V2.0-R2.6.3

1.2 软件版本

厂站 agent 运行于凝思安全操作系统 V6.0.42/60/80/90/99/100 等系统下的发行版本。

安装包的名称实例：linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64.tar.gz

其中 2.6.3 是版本号，版本号会随着版本的更新而变化。

注意：厂站 R2.6.3 版本日志存放目录已更改为/usr/share/smp/log/与/usr/share/lcm/log

2 厂站 agent 的安装与卸载

厂站 agent 的安装与卸载均需在超级用户 **root** 下执行。

2.1 安装

请从凝思官网或商务获取安装软件包，并核对 md5 值是否正确。下面以软件包 linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64.tar.gz 为例。

1. 安装包放入/opt/路径下(路径可根据实际情况修改,默认推荐路径为/opt/)

```
1)进入/opt/目录
#  cd /opt/
2)核对 md5 值(从官网或商务处获取安装包时同步获取)
# md5sum linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64.tar.gz
```

2. 执行安装

```
1)解压
#  tar -xvf linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64.tar.gz
```

2)进入解压生成的目录

cd linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64

3）执行安装脚本

#./linx.sh install

安装过程如下图:

```
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64# ./linx.sh install
start os_version check
INFO: You deploy in system 6.0.60_x86_64
INFO: Start check security module
SECURITY_VERSION:
INFO:CLEAR_OLD_AGENT processing.
INFO:BACKUP_SYS_FILE processing.
Now processing /root
Now processing /home/sysadmin
Now processing /home/secadmin
Now processing /home/audadmin
Now processing /home/netadmin
Now processing /home/rocky
INFO: /etc/ld.so.conf had not been modified
INFO: not find /etc/ld.so.conf.d/smp.conf in this system
Starting install ./pkg/gmssl_2.1+Linx60_amd64.deb
(正在读取数据库 ... 系统当前共安装有 215856 个文件和目录。)
正预备替换 gmssl 2.1 (使用 .../pkg/gmssl_2.1+Linx60_amd64.deb) ...
正在解压缩将用于更替的包文件 gmssl ...
正在解压缩将用于更替的包文件 gmssl ...
正在设置 gmssl (2.1) ...
Starting install ./pkg/agent-manage_1.4.5+LinxOS6.0.60_x86_64.deb
选中了曾被取消选择的软件包 agent-manage。
(正在读取数据库 ... 系统当前共安装有 215856 个文件和目录。)
正在解压缩 agent-manage (从 .../agent-manage_1.4.5+LinxOS6.0.60_x86_64.deb) ...
正在设置 agent-manage (1.4.5+LinxOS6.0.60) ...
Starting install linx-intranet-monitor
选中了曾被取消选择的软件包 linx-intranet-monitor。
(正在读取数据库 ... 系统当前共安装有 215914 个文件和目录。)
正在解压缩 linx-intranet-monitor (从 .../linx-intranet-monitor_2.0-2.6.3+6.0.60_amd64.deb) ...
正在设置 linx-intranet-monitor (2.0-2.6.3) ...
linx_smpd                0:off  1:off  2:on   3:on   4:on   5:on   6:off
start install lcm
选中了曾被取消选择的软件包 linx-cmd-monitor。
(正在读取数据库 ... 系统当前共安装有 215980 个文件和目录。)
正在解压缩 linx-cmd-monitor (从 .../linx-cmd-monitor_1.1.2+LINX60_amd64.deb) ...
正在设置 linx-cmd-monitor (1.1.2) ...
```

安装脚本会对探针依赖库 MD5 值进行检查，检查通过会显示如下信息，如下图：

```
Now processing /home/secadmin
Now processing /home/audadmin
Now processing /home/netadmin
Now processing /home/rocky
INFO: Start set smp logrotate
start install version check!
INFO: Start smp library check!
check lib md5 success !!!
restart cron?[y/N](default y):y
You choose yes,now restart cron
```

当出现以下界面，是在询问是否重启定时服务，输入 y 表示重启系统定时服 务，输入 n 表示不重启。由于安装过程中可能会修改定时服务的配置文件，所以建议在这一步输入 y 重启一下定时服务，否则后续可能会导致探针无法被定时服务拉起。

```
Now processing /home/rocky
INFO: Start set smp logrotate
start install version check!
INFO: Start smp library check!
check lib md5 success !!!
restart cron?[y/N](default y):y
You choose yes,now restart cron
Restarting periodic command scheduler: cron.
```

当出现”Please input serial number in /etc/linxsn/security_sn.conf and start service.”，即表示安装过程正常并成功安装了厂站 agent。

```
restart cron?[y/N](default y):y
You choose yes,now restart cron
Restarting periodic command scheduler: cron.
Great,Install linx-intranet-monitor normal end.
Please input serial number in /etc/linxsn/security_sn.conf and start service.
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64#
```

4. 查看安装状态

```
# ./linx.sh status
```

如下图表明的就是已成功安装的状态

```
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64# ./linx.sh status
DEB linx-intranet-monitor has been installed!
期望状态=未知(u)/安装(i)/删除(r)/清除(p)/保持(h)
| 状态=未安装(n)/已安装(i)/仅存配置(c)/仅解压缩(U)/配置失败(F)/不完全安装(H)/触发器等待(W)/触发器未决(T)
|/ 错误?=(无)/须重装(R) (状态，错误：大写=故障)
||/ 名称                                  版本                                描述
+++-=======================================-===================================-==========================================================================
ii  linx-intranet-monitor                  2.0-2.6.3                           Intranet security monitoring software
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64#
```

注意事项：

1) 厂站 agent 从 2.4.3 版本开始卸载时会自动备份配置文件。如果低于 2.4.3 的版本需要保留历史配置文件，请手动备份。

2) **LinxOS 6.0.80 20220830/LinxOS 6.0.80 20220309 系统自带了可信，可能会导致 agent 停止失败**，该问题的解决方法在 6 常见问题排查章节。

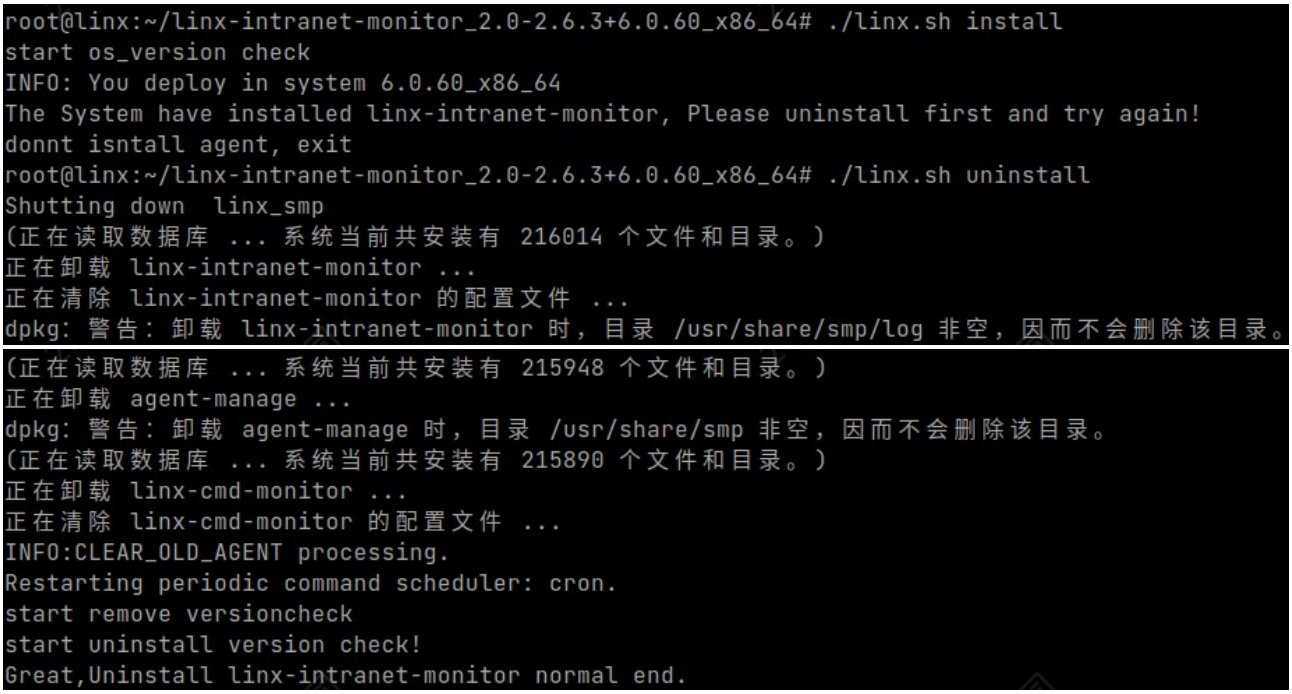
3) 若系统自带探针，需先卸载系统自带的探针，再进行安装。

2.2 卸载

1. 进入安装包所在目录
2. 执行卸载脚本 linx.sh

```
# ./linx.sh uninstall
```

卸载过程如下图：



注意：在卸载过程中若出现 “某个目录非空，因而不会删除该目录”的提示时，是正常现象，不用做其他操作。

3. 查看软件卸载后状态

```
# ./linx.sh status
```

如下图表明就是已成功卸载的状态：

```
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64# ./linx.sh status
DEB linx-intranet-monitor has been uninstalled
期望状态=未知(u)/安装(i)/删除(r)/清除(p)/保持(h)
| 状态=未安装(n)/已安装(i)/仅存配置(c)/仅解压缩(U)/配置失败(F)/不完全安装(H)/触发器等待(W)/触发器未决(T)
|/ 错误?=(无)/须重装(R) (状态，错误：大写=故障)
||/ 名称                                    版本                                    描述
+++-=======================================-=======================================-======================
un  linx-intranet-monitor                   <无>                                    (无可用描述)
root@linx:~/linx-intranet-monitor_2.0-2.6.3+6.0.60_x86_64#
```

R2.3.9 版本之后，卸载 agent 时会将配置文件备份到/usr/share/smp/目录下，备份文件的名字是 linx_config.bak。

R2.4.3 版本之后，安装时会自动恢复原备份文件。

3 厂站 agent 的配置

R2.4.9 版本之后，根据要求，厂站 agent 安装后配置文件需全程处于加密状态， 加密的配置文件为: /usr/share/smp/linx_config.en

如果需要修改配置文件，可以通过配置文件修改或 agent_manage 工具修改。

通过配置文件直接修改配置:

1. 切换至 root 用户
2. 执行/usr/share/smp/de.sh 脚本解密配置文件
3. 根据需求修改解密生成的配置文件/usr/share/smp/linx_config，保存退出
4. 执行/usr/share/smp/en.sh 脚本进行加密
5. root 用户执行/etc/init.d/linx_smpd restart 重启服务

通过 agent_manage 工具修改配置:

注意:该配置修改方式只适用于厂站 agent 2.5.4 及以上版本.若 agent 版本低于 2.5.4 请按照方法一修改配置文件或按照对应版本的安装使用说明书进行修改。

R2.5.4 版本开始，可通过图形化界面进行配置，使用 root 用户执行 agent_manage 命令，开始图形化配置。

注意：进行图形化配置时，请勿另外同时修改配置文件，否则图形化配置完成后会覆盖之前的配置。R2.5.8 及以上版本已优化图形化界面，取消了不必要的接口。

agent_manage 工具说明:

主界面各项功能解释:

(1) “系统版本”为当前主机所安装操作系统版本号;

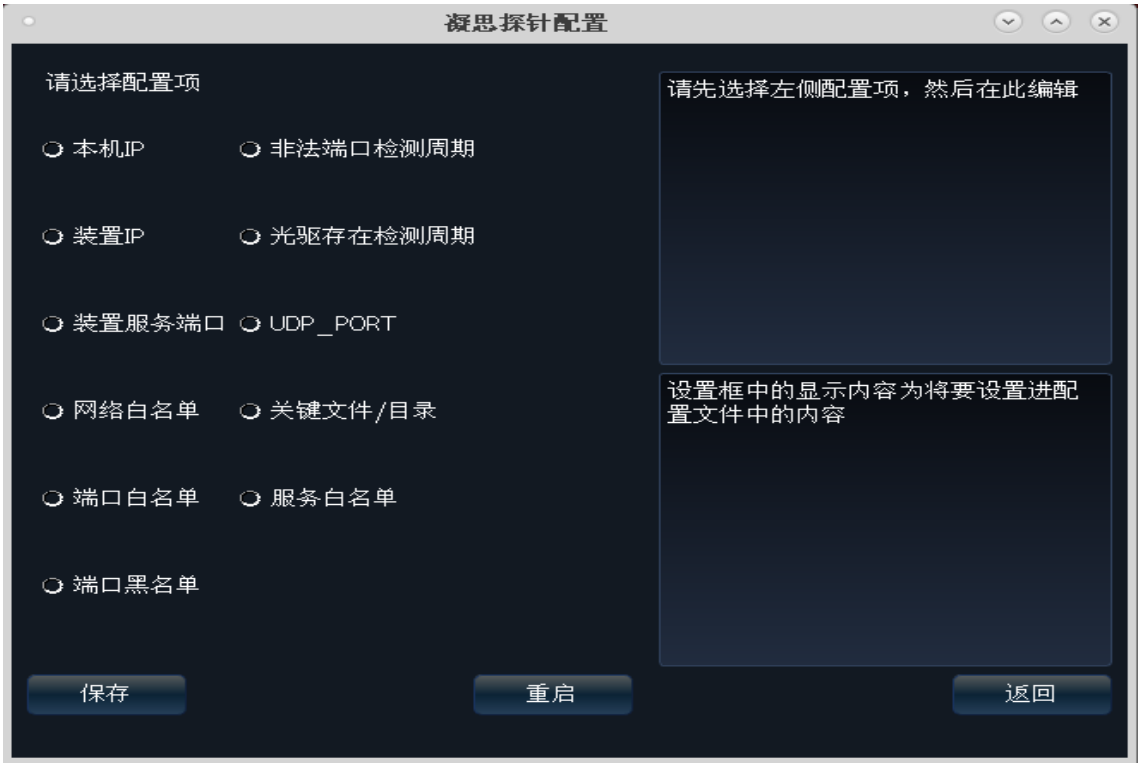
(2) “探针版本”为当前主机所安装厂站 agent 版本号;

(3) “配置”可进入配置界面;

(4) “日志调试”可进入调试界面;

(5) “关闭”退出程序。

配置界面如图所示:



按钮说明

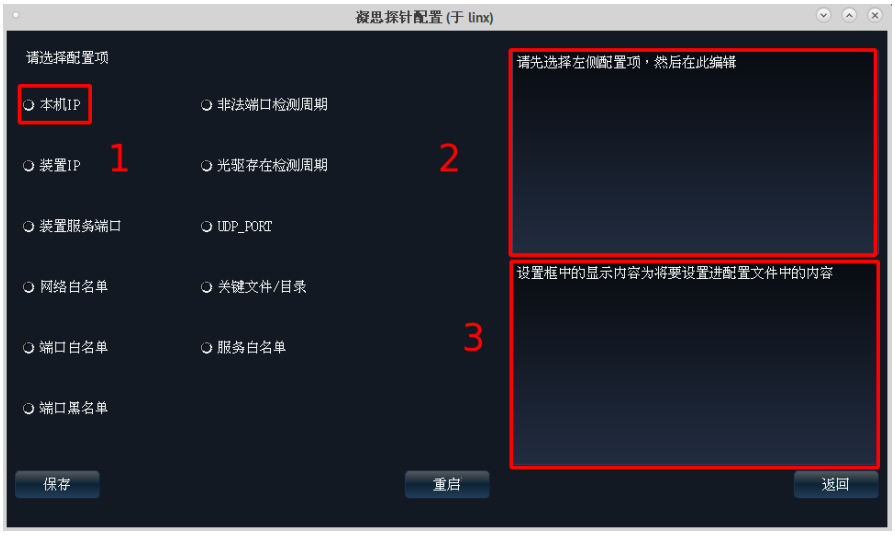
(1) 保存按钮：将当前的界面的配置信息保存到 agent 的配置文件中并进行加密

(2) 重启按钮：重启厂站 agent，一般在修改配置信息并保存后点击

(3) 返回按钮：返回上级界面

配置说明

agent-manage 会根据配置文件内容初始化开关状态和配置选项的值，所以在配置时只需要去点击想要更改的选项，不用逐个去配置。



在“请选择配置项”下方勾选任意一个配置项开始配置，如编辑“本机 IP”:

(1) 勾选方框 1;

(2) 在方框 2 所示区域进行编辑;

(3) 方框 3 所示区域为各项配置的帮助说明;

编辑其它配置也是如此，未勾选配置项时方框 2 是处于不可编辑状态。

注意：agent_manage 自带前台输入检验功能，如选择配置 ip 项目时，编辑框 2 只接受输入正确的 ip 格式，选择配置检测周期项目时只接受输入数字信息。

配置完所有需要配置的项目后需要点击保存按钮，如一些必须要配置的项目未配置，会弹出如下提示框，需要将必配项目配置上有效内容后重新点击保存。

配置详情参考 **3.1 配置文件说明**。

点击重启按钮后，厂站 agent 会重启，暂无提示，无需重复点击。

格式校验说明

agent_manage 针对厂站配置文件做了一个配置信息的格式校验功能，当配置信息不符合正确的格式点击保存时会弹出提示框，提示框如下:

可点击确定按钮关闭此对话框（点击对话框右上角的×不能关闭此对话框），也可点击详细信息按钮了解错误格式的具体信息。

调试界面如下图所示：

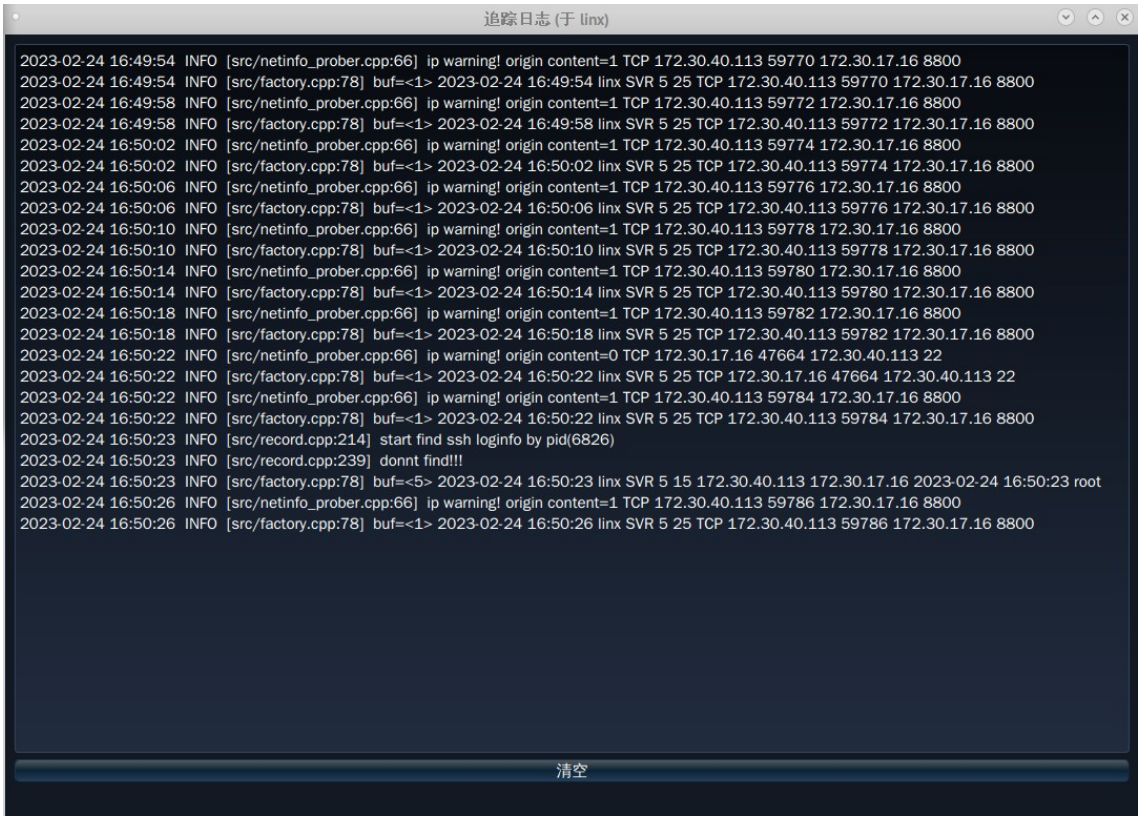
日志调试界面按键功能说明：

(1) 探针状态：显示当前探针运行状态；

(2) 日志位置：探针生成的日志所处位置；

(3) 打包位置：当点击打包日志按钮时，会将日志复制到指定目录（默认拷贝到/tmp 目录）；

(4) 点击“追踪日志”后，会将此后日志新增内容展现出来（如下图所示），当没有新增日志时，会展现空白内容，等待一段时间即可。



3.1 配置文件说明

配置文件内容如下图所示:

```
[SERVER]
SIGN_SM2=no
SCRIPT_DEBUG=no
SERVERIP=192.168.22.18
SERADDR_TCP=192.168.22.175
SERPORT_TCP=8800
IP_WHITELIST=tcp,192.168.22.0,0
PORT_WHITELIST=2,x
PORT_RANGE=0-1;
PORT_BLACKLIST=1;2;3
PORT_INTERVAL=60
CD_INTERVAL=60
UDP_PORT=9999
MONPATH=/home/
ECHO=yes
```

配置文件主要字段介绍:

字段	说明	示例
SIGN_SM2	这是 sm2 验签的开关，当 SIGN_SM2=yes 表明打开 sm2 验签;当 SIGN_SM2=no 表明关闭 sm2 验签	SIGN_SM2=yes
SERVERIP	本机 ip 地址，即：agent 所在的主机的 IP 地址。	若厂站 agent 所在主机的 ip 地址为 192.168.11.110，则配置为: SERVERIP=192.168.11.110
SERADDR_TCP	网络监控装置（服务端）的 IP 地址。若配置双网，IP 以分号分隔。多装置间用’/‘分开	若两台网安装置的 IP 分别是 172.30.17.19 和 172.30.17.16,则配置为: SERADDR_TCP=172.30.17.19/172.30.17.16
SERPORT_TCP	与网络监控装置通信的端口号。这是固定值 8800	SERADDR_TCP=8800
IP_WHITELIST	IP 地址白名单，一条完整的 IP 地址白名单的格式为:“协议号（tcp/udp）,远端 IP 地址,远端端口（0 表示不限）;” 可多条 注：远端 IP 地址和远端端口均可以是一个范围，当设置成范围时，采用“-”隔开	IP_WHITELIST=tcp,192.168.11.120,0;tcp,192.168.22.0-192.168.22.255,0-15;tcp,192.168.22.130,0-25;
PORT_WHITELIST	端口白名单，一条完整的端口白名单为“端口号，服务名称;”或者填写范围 注：服务名称未知时，可用字符“x”代替。	PORT_WHITELIST=22,sshd;177,xdhcp;1024-65535

PORT_BLACKLIST	端口黑名单。端口黑名单的优先级大于端口白名单。	PORT_BLACKLIST=1;2;3;
PORT_INTERVAL	非法端口检测周期，单位：秒	PORT_INTERVAL=60
CD_INTERVAL	光驱存在检测周期，单位：秒	CD_INTERVAL=60
MONPATH	关键目录/文件清单，将要监控的关键文件和目录添加到该字段后面。	MONPATH=/home/;/etc/

注：未标出的字段采用默认配置即可，无需修改。

3.2 密钥证书放置方法

通过网安装置厂家的工作人员获取验签的公钥证书。

将公钥证书放置在/usr/share/smp/certs/ 下，并重命名为 device.cer 即可。

3.3 对时

在运行软件之前，务必将厂站 agent 主机与网安装置主机进行对时。厂站 agent 判断厂站 agent 主机与网安装置主机的时间差，如果时间差超过 30 秒即判断为对时失败。

注：参数设置、基线核查、主动断网、漏洞扫描、版本管理、特征数据更新才会进行验签和对时。

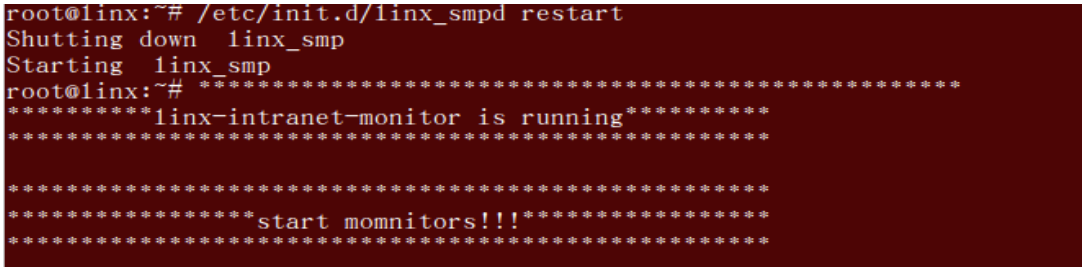
3.4 序列号

1. 向凝思的商务人员申请厂站 agent 序列号;
2. 存放序列号的文件是：/etc/linxsn/security_sn.conf，将申请的序列号正确地输入到这个文件中即可;
3. 已经配置过序列号的主机，升级厂站 agent 会自动将序列号添加进/etc/linxsn/security_sn.conf 文件中，无需再手动添加。

4 厂站 agent 的启停

4.1 启动服务

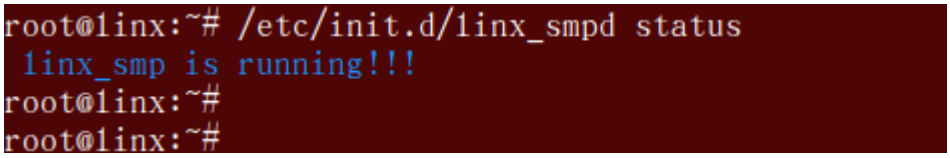
启动厂站 agent 服务，执行/etc/init.d/linx_smpd start 命令，执行成功如下图所示：



注意：执行启动命令后，如果出现“start momnitors”提示，厂站 agent 服务已正常运行，敲回车键即可回到终端的正常状态。

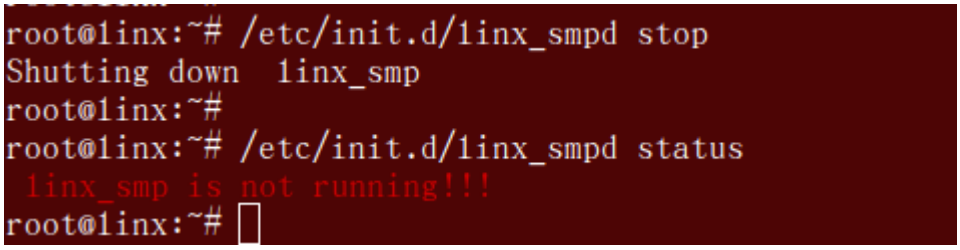
4.2 查询服务状态

查询厂站 agent 服务，执行/etc/init.d/linx_smpd status 命令，厂站 agent 服务正常运行显示如下图所示：



4.3 停止服务

停止厂站 agent 服务，执行/etc/init.d/linx_smpd stop 命令，再用/etc/init.d/linx_smpd status 命令查看显示如下图所示：



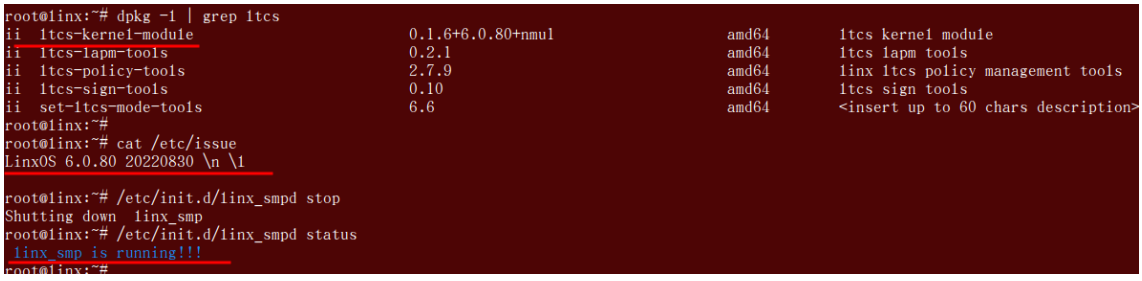
5 注意事项

1. 在本机图形界面测试退出登录时，必须使用“注销”来退出登录的用户，不能使用切换用户。
2. 在终端使用 ssh 测试退出登录时，必须在终端输入“exit”或者使用 CTRL+d 来退出登录的用户。不能直接关闭终端。
3. 新建用户时，建议指定 shell 环境为/bin/bash，如:

   useradd -m 用户名 -s /bin/bash

6 常见问题排查

1. 厂站 agent 的进程名是 linx_smp，使用 ps aux | grep linx_smp 可查询到详细的进程信息，正常的情况是查询到 linx_smp 进程总共有 1 个。如果查询出进程数量不等于 1 个则运行/etc/init.d/linx_smpd restart 重启软件。
2. 若厂站 agent 未连接上网络装置，首先查看/usr/share/smp/linx_config 文件中是否正确填写了网安装置的 IP 地址以及厂站 agent 主机的 IP 地址。
3. 若 sm2 验签失败：请确认是否按照 **3.2 章节**的方法配置了签名证书，并查看日志信息: /usr/share/smp/log/linx_smp.log。
4. 若对时失败：请将厂站 agent 主机的时间与网安装置的时间进行对时，确认两台主机的时间误差在 30 秒之内。
5. 若网口 up/down 检测失效：请确认网口配置是否正常。
6. 若出现 exit 退出终端时卡住，可以通过叉掉终端界面的方式退出。
7. LinxOS 6.0.80 20220830/LinxOS 6.0.80 20220309 系统自带了可信，可能会导致 agent 停止失败，失败现象如下:



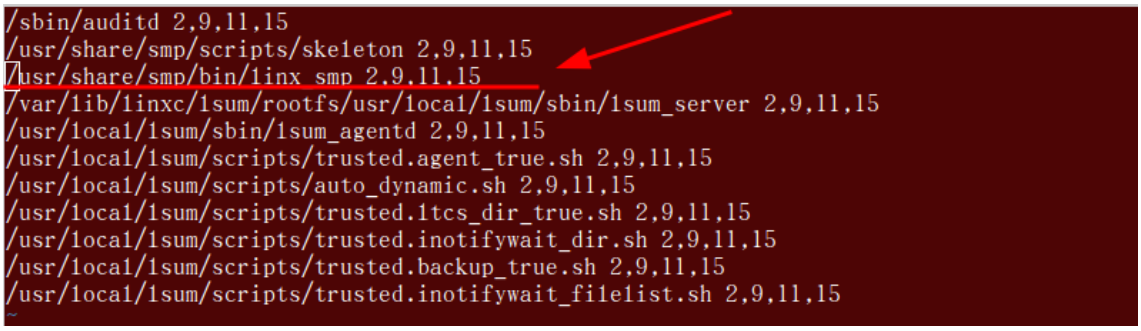
解决措施:

1) 清除防杀列表

执行如下命令:

```
#  vim /etc/security/linx_sig_block
```

将如下图片中红线部分删除:



2) 使能配置

执行如下命令:

```
#  echo s > /sys/kernel/security/ltcs/signal_block_trigger
```

执行以上操作后该系统停止 agent 正常，如下图:

注意：LinxOS 6.0.80 20220309 系统若直接清空防杀列表再执行使能配置会使系统卡死，且无法通过重启解决