

安盟多因素身份认证系统
V9.0
基于 openEuler 操作系统服务器
安装说明



安盟电子信息安全有限责任公司

2023 年 2 月

版本管理

版本	摘要	编者	时间
1.00	基本服务器安装；设置主机名称；设置网卡	陈俊	2023/02/27
1.01	增加基本配置	陈俊	2023/02/27
1.02	增加安盟服务器安装	陈俊	2023/03/27

目录

- 1 概述.....1
- 2 基本服务器安装.....1
 - 2.1 基本配置.....1
 - 2.2 基本设置.....2
 - 2.2.1 设置日期时间.....3
 - 2.2.2 设置服务器角色.....4
 - 2.2.3 设置默认硬盘.....5
 - 2.2.4 网卡设置设置.....6
 - 2.2.5 设置 root 密码.....7
- 3 系统和软件升级.....10
- 4 VMwaretools 安装（选读）10
 - 4.1 前提条件.....11
 - 4.2 过程.....11
- 5 设置主机网卡.....13
- 6 设置主机名称.....14

1 概述

安盟多因素身份认证系统，可以安装在操作系统为 openEuler 类型的服务器上。

openEuler 为华为自主研发的欧拉主机系统，分别有两种结构一种是 x86 的传统结构，一种是 arm 类型机器结构。安盟认证系统对两者完全兼容。本文以 x86 机型进行说明。

2 基本服务器安装

2.1 资源基本配置

基本配置：

硬盘 100G 内存 8G

CPU 2 核 2 进程

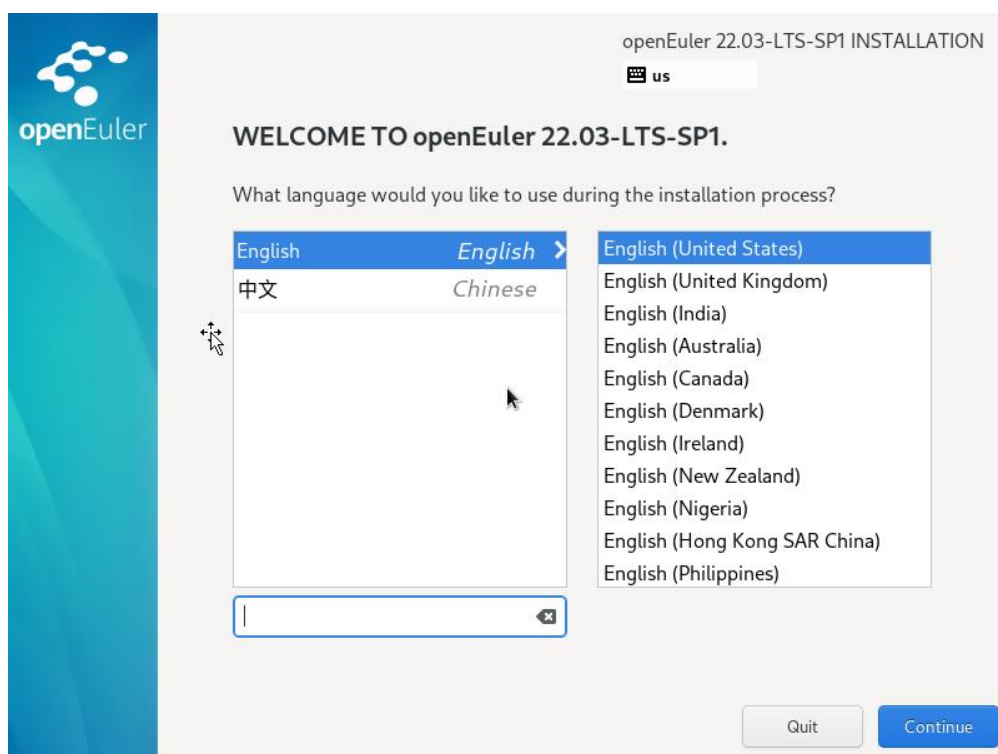
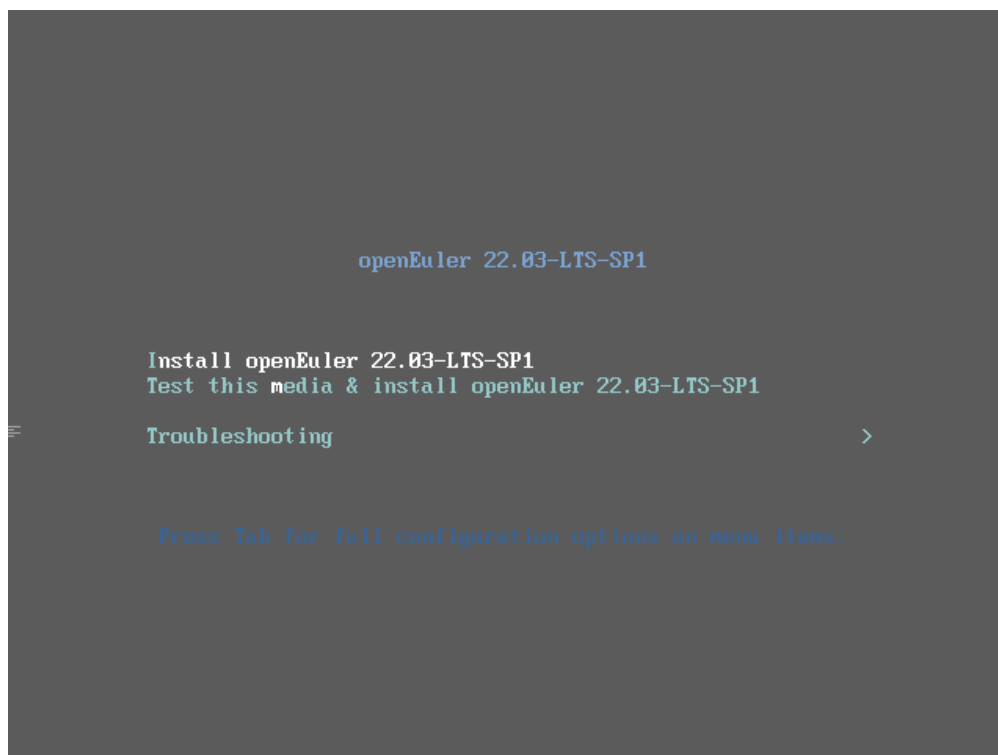
网卡 2 块

语言 英文

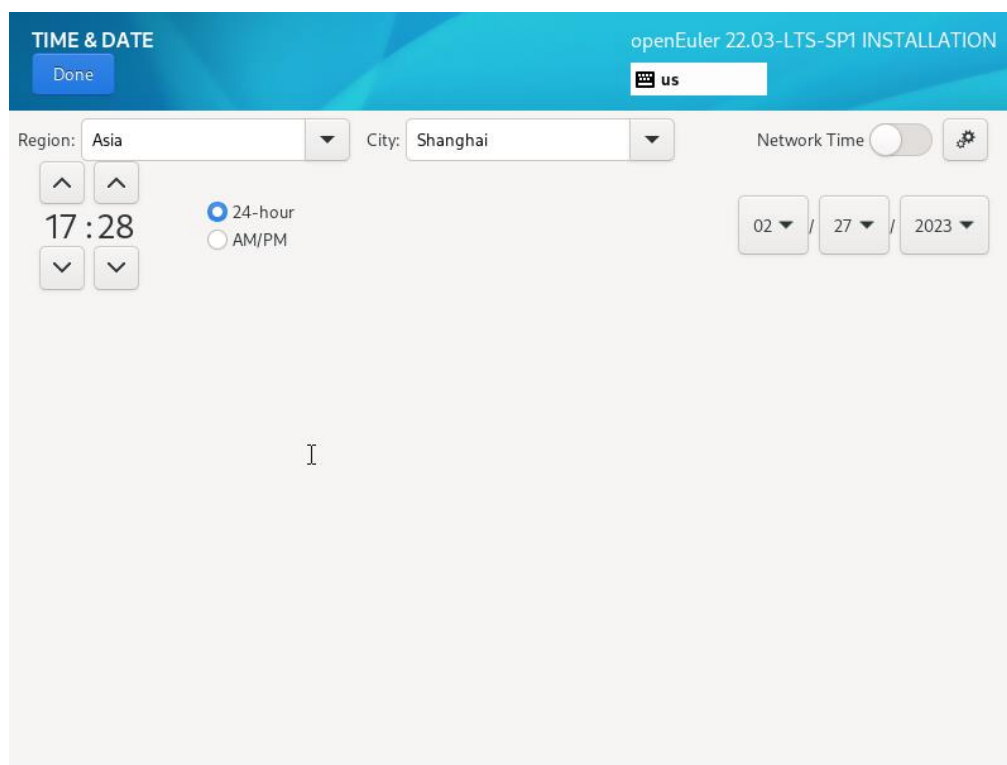
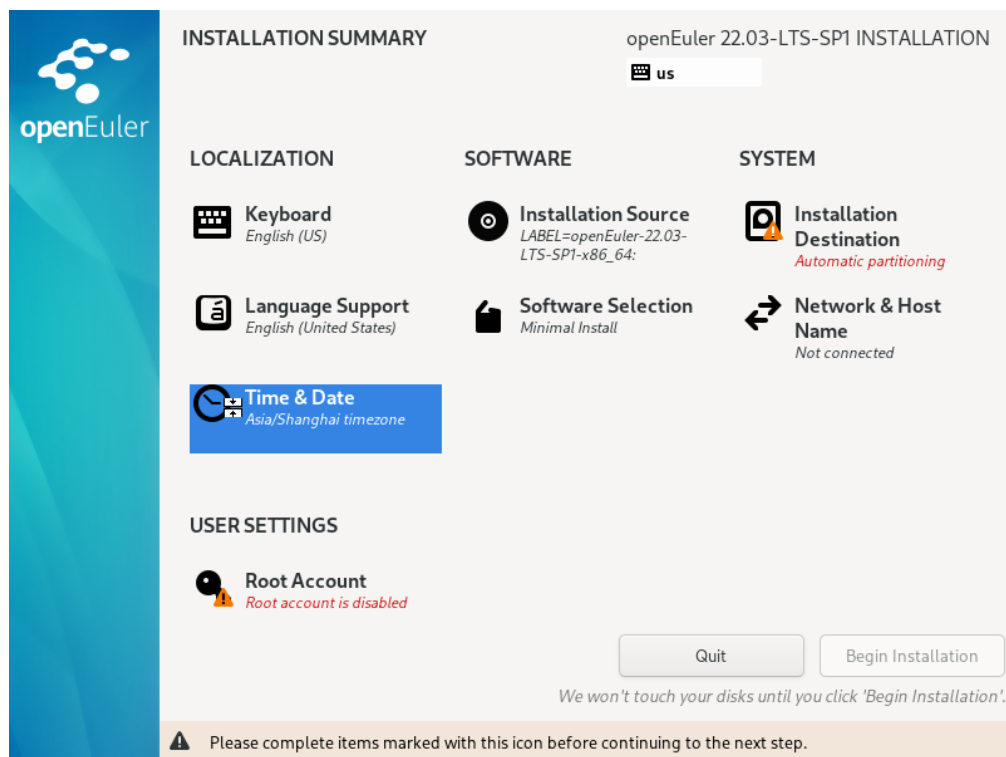
与北京时间同步

如果是虚拟机，可以直接选在 CentOS 类型 64bit 模板安装。

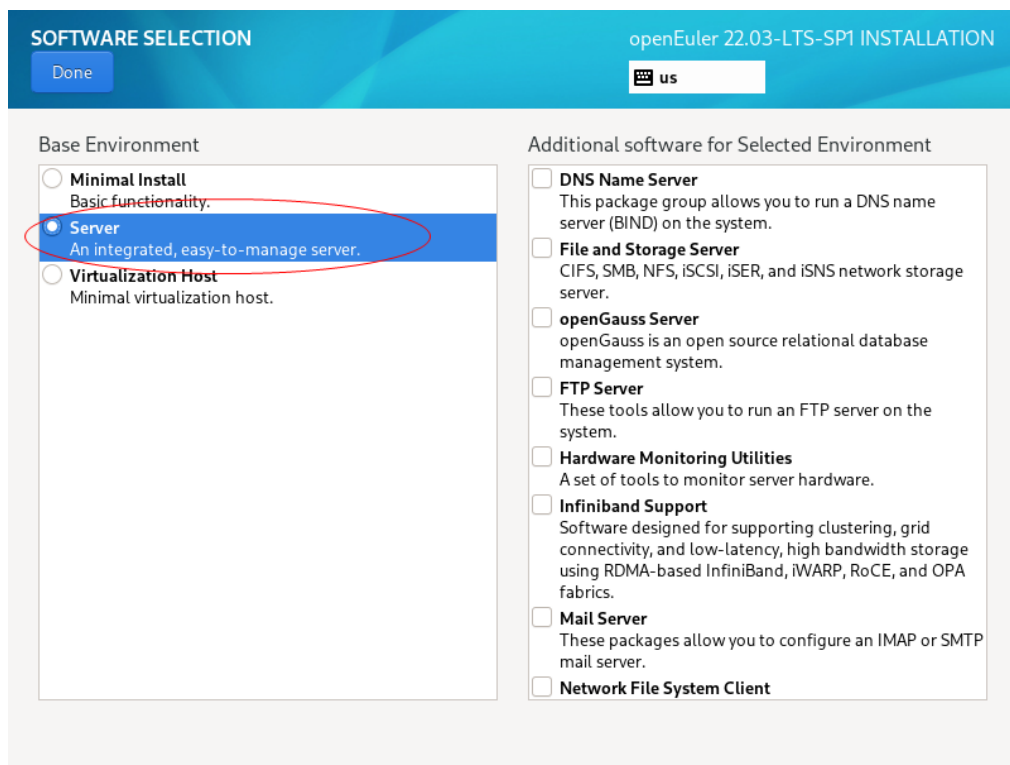
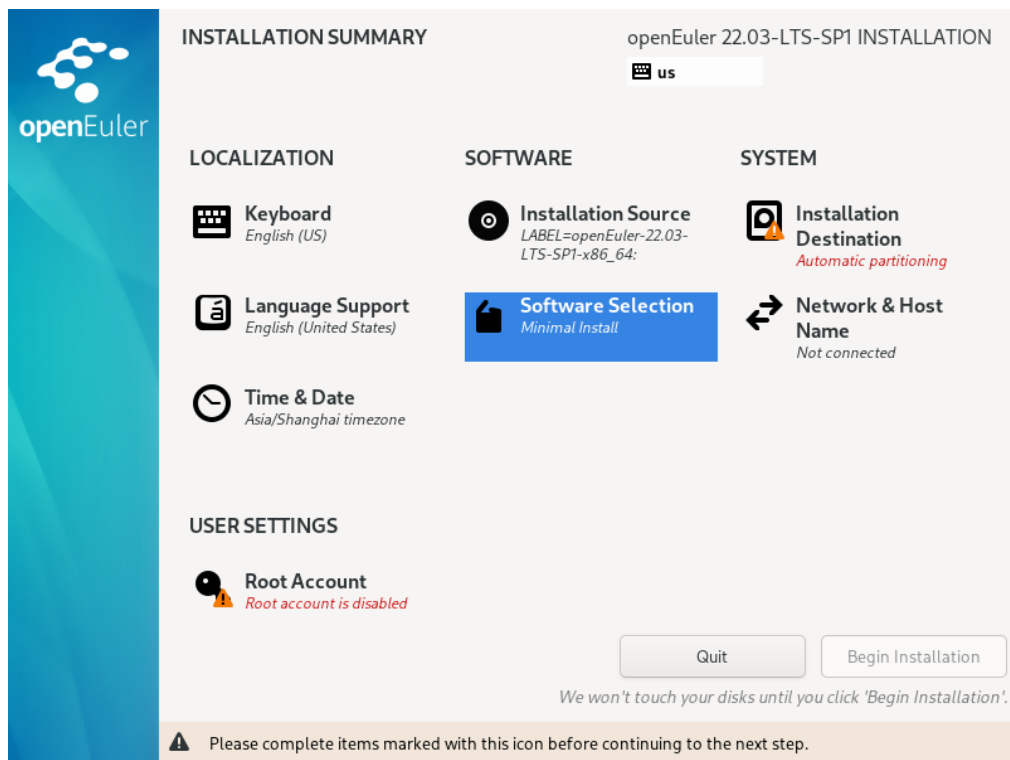
2.2 基本设置



2.2.1 设置日期时间

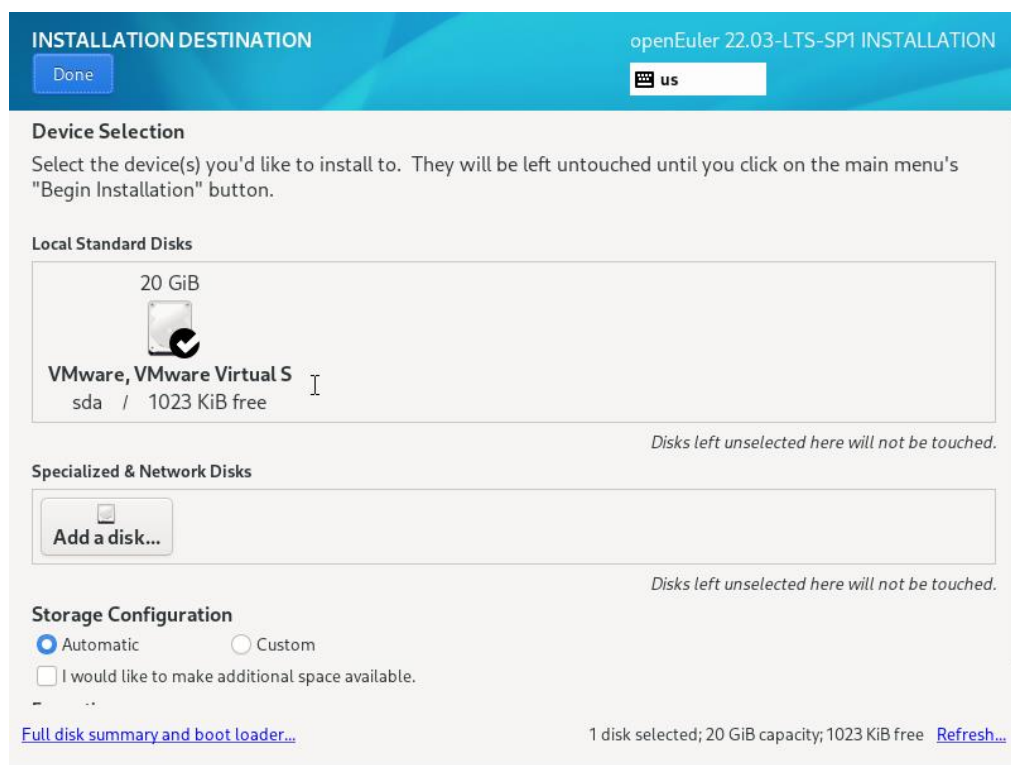
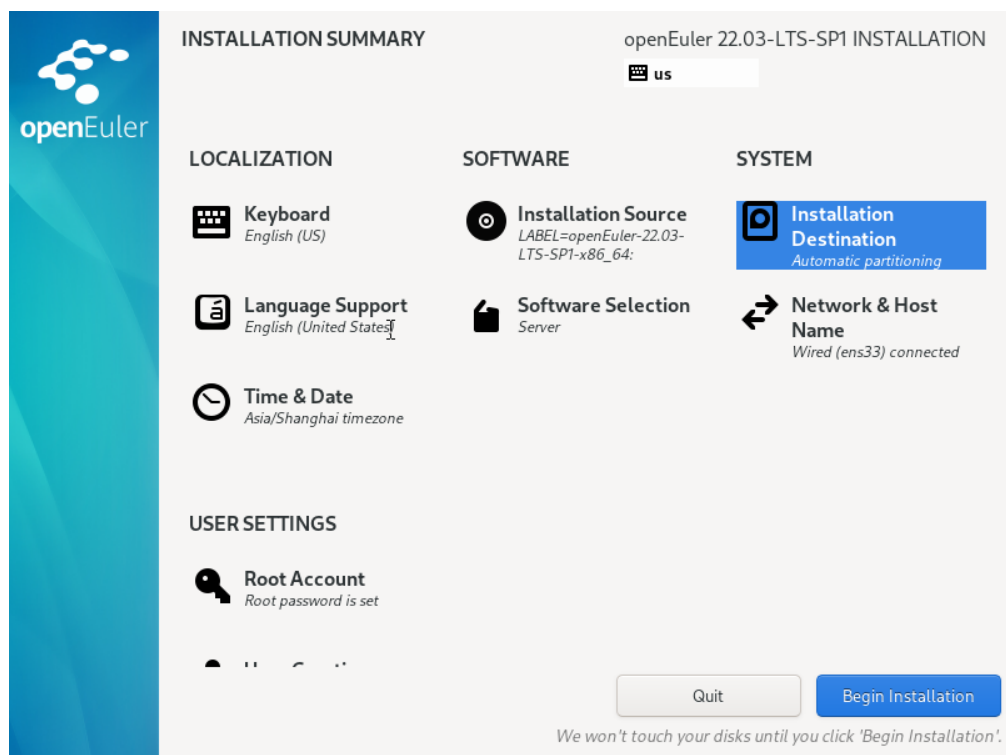


2.2.2 设置服务器角色



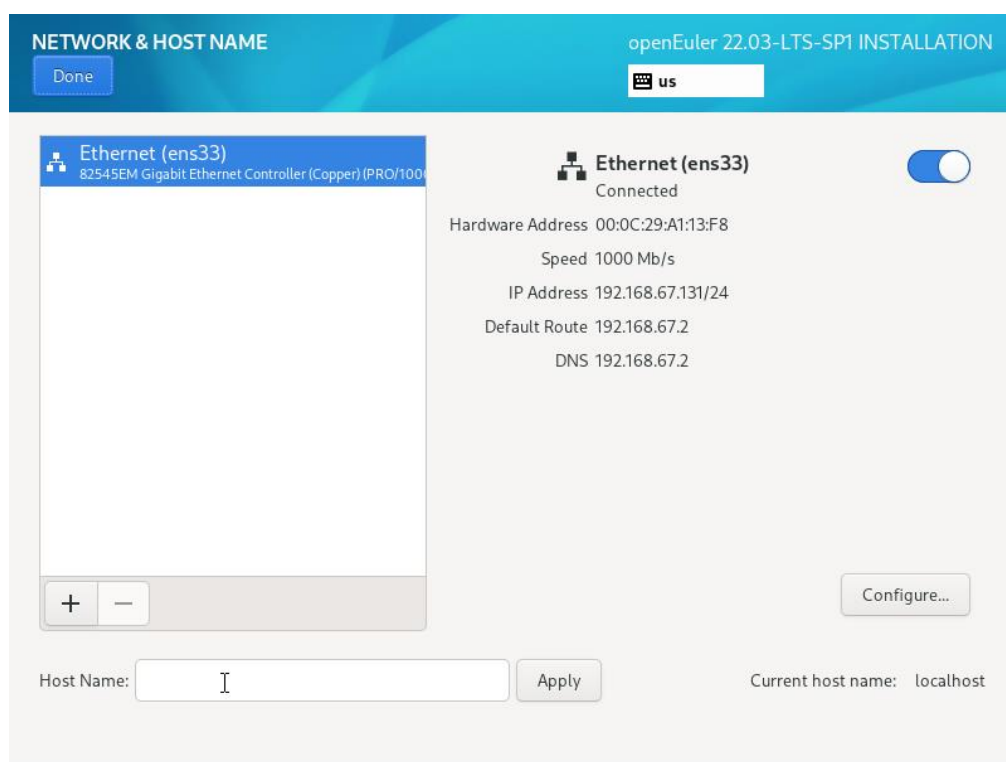
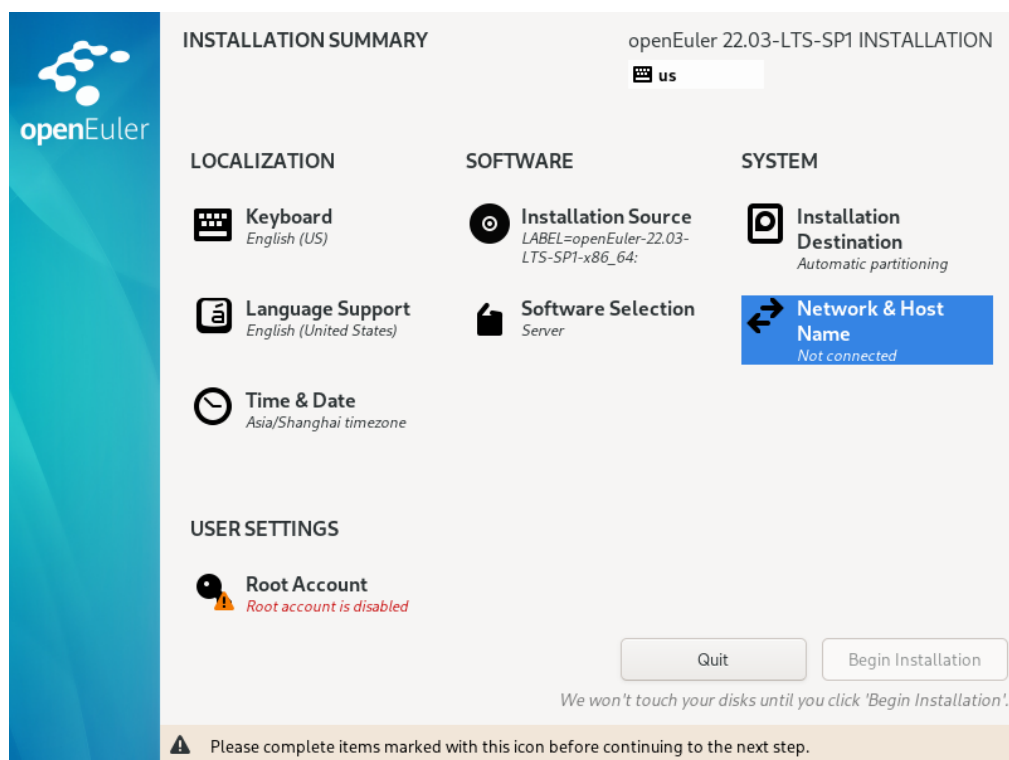
注意：选择结构化服务器模式，让操作系统具备基本的网络通信功能。

2.2.3 设置默认硬盘

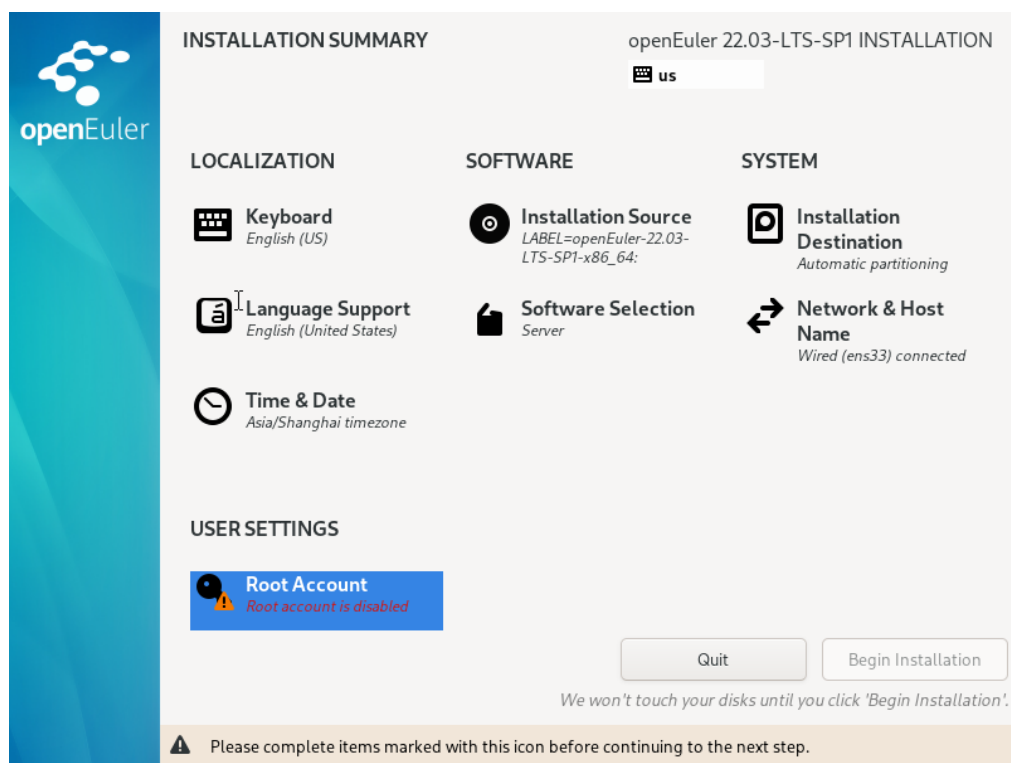


默认设置即可。

2.2.4 网卡设置设置



2.2.5 设置 root 密码



设置管理员用户

ROOT ACCOUNT

openEuler 22.03-LTS-SP1 INSTALLATION

Done

us

The root account is used for administering the system.

The root user (also known as super user) has complete access to the entire system. For this reason, logging into this system as the root user is best done only to perform system maintenance or administration.

☐ **Disable root account**

Disabling the root account will lock the account and disable remote access with root account. This will prevent unintended administrative access to the system.

☒ **Enable root account**

Enabling the root account will allow you to set a root password and optionally enable remote access to root account on this system.

Root Password:

Good

Confirm:

☐ Use SM3 to encrypt the password

开始安装

INSTALLATION SUMMARY

openEuler 22.03-LTS-SP1 INSTALLATION

us

LOCALIZATION	SOFTWARE	SYSTEM
Keyboard English (US)	Installation Source LABEL=openEuler-22.03-LTS-SP1-x86_64:	Installation Destination Automatic partitioning
Language Support English (United States)	Software Selection Server	Network & Host Name Wired (ens33) connected
Time & Date Asia/Shanghai timezone		

USER SETTINGS

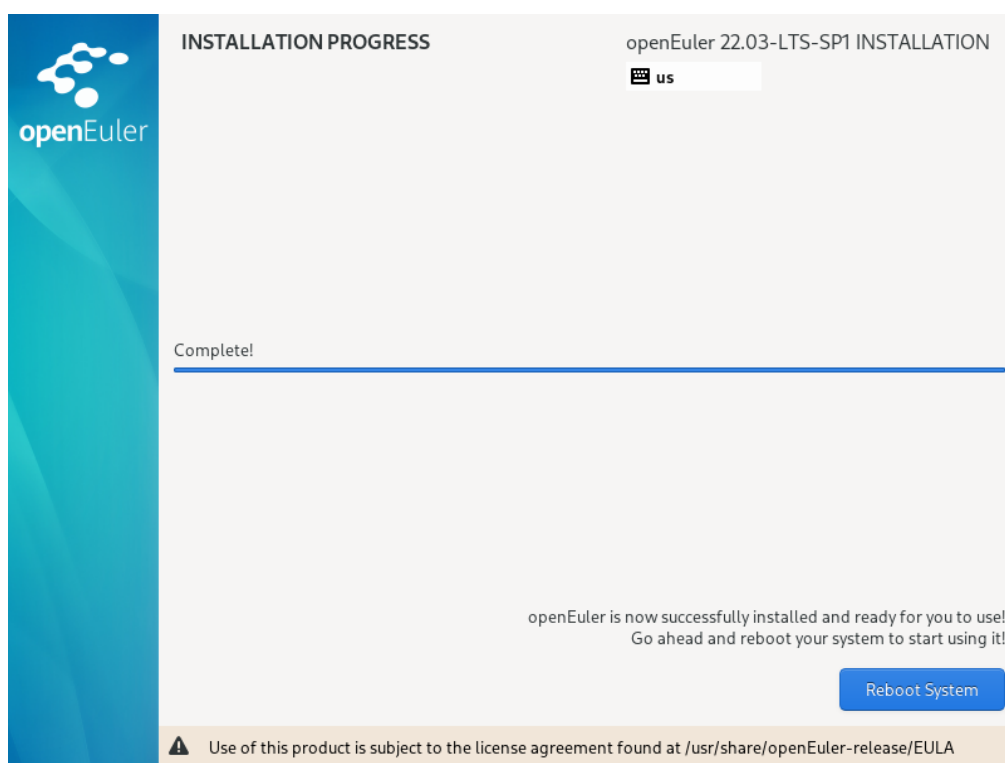
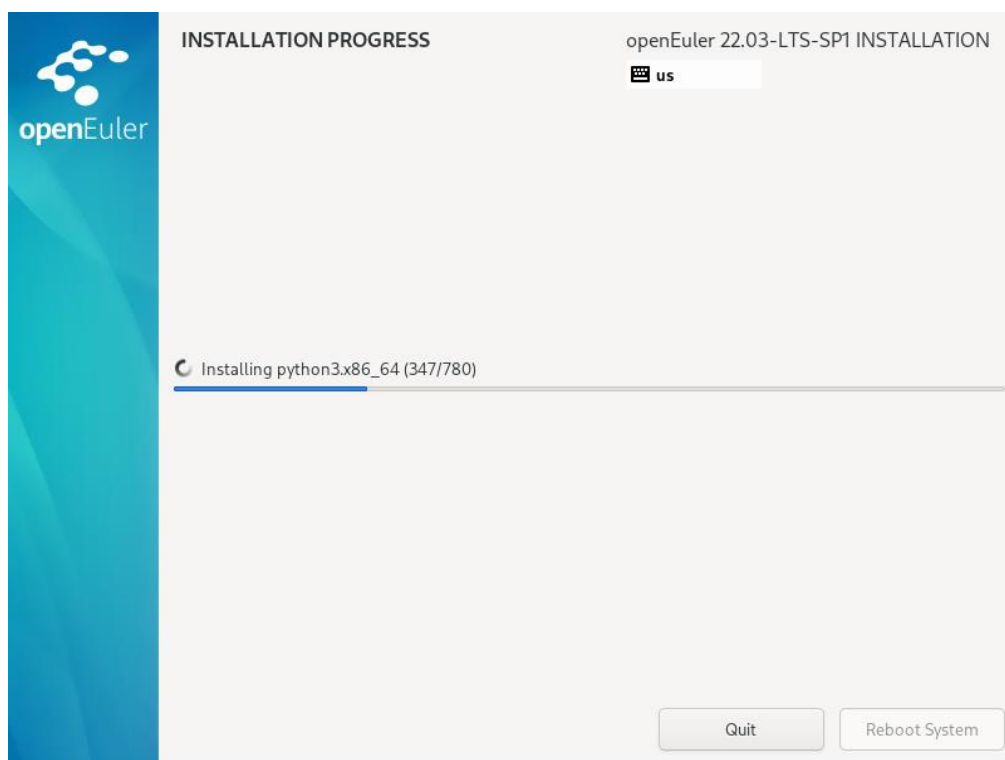
Root Account
Root password is set

Quit

Begin Installation

We won't touch your disks until you click 'Begin Installation'.

安装完成



```
openEuler 22.03 (LTS-SP1)
Kernel 5.10.0-136.12.0.86.oe2203sp1.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: root
Password:

Authorized users only. All activities may be monitored and reported.

Welcome to 5.10.0-136.12.0.86.oe2203sp1.x86_64

System information as of time: Mon Feb 27 06:28:10 PM CST 2023

System load:  0.00
Processes:    144
Memory used:  19.0%
Swap used:    0%
Usage On:     14%
IP address:   192.168.67.131
IP address:   192.168.122.1
Users online: 1

[root@localhost ~]# _
```

3 系统和软件升级

升级所有包同时也升级软件和系统内核

```
yum -y update
```

升级所有软件包

```
yum -y upgrade
```

4 VMwaretools 安装（选读）

虚拟机增强工具各个厂家安装方式基本一样，我们以 VMwaretools 为例，演示安装过程。

<https://docs.vmware.com/cn/VMware-Workstation-Pro/12.0/com.vmware.ws.using.doc/GUID-08BB9465-D40A-4E16-9E15-8C016CC8166F.html>

对于 Linux 虚拟机，您可以使用命令行工具手动安装或升级 VMware Tools。

4.1 前提条件

- 开启虚拟机。
- 确认客户机操作系统正在运行。
- 由于 VMware Tools 安装程序是使用 Perl 编写的，因此，请确认在客户机操作系统中安装了 Perl。

4.2 过程

1. 在主机上，从 Workstation Pro 菜单栏中选择虚拟机 > 安装 VMware Tools。

如果安装了早期版本的 VMware Tools，则菜单项是 更新 VMware Tools。

2. 在虚拟机中，以 root 身份登录到客户机操作系统并打开终端窗口。
3. 不带参数运行 mount 命令以确定 Linux 发行版是否自动装载 VMware Tools 虚拟 CD-ROM 映像。

如果装载了 CD-ROM 设备，将按以下方式列出 CD-ROM 设备及其装载点：

```
/dev/cdrom on /mnt/cdrom type iso9660 (ro,nosuid,nodev)
```

4. 如果未装载 VMware Tools 虚拟 CD-ROM 映像，请装载 CD-ROM 驱动器。
 - a. 如果装载点目录尚不存在，请创建该目录。

```
mkdir /mnt/cdrom
```

某些 Linux 发行版使用不同的装载点名称。例如，某些发行版上的装载点是 /media/VMware Tools 而不是 /mnt/cdrom。请修改该命令以反映您的发行版使用的约定。

- b. 装载 CD-ROM 驱动器。

```
mount /dev/cdrom /mnt/cdrom
```

某些 Linux 发行版使用不同的设备名称，或者以不同的方式组织 /dev 目录。如果 CD-ROM 驱动器不是 /dev/cdrom 或 CD-ROM 装载点不是 /mnt/cdrom，则必须修改该命令以反映您的发行版使用的约定。

5. 转到工作目录，例如 /tmp。

```
cd /tmp
```

6. 在安装 VMware Tools 之前，删除以前的 `vmware-tools-distrib` 目录。

该目录的位置取决于以前安装时的存储位置。通常，该目录位于 `/tmp/vmware-tools-distrib`。之所以删除旧的 `vmware-tools-distrib`，重新解压的工具包会重新生成该目录。

7. 列出挂载点目录的内容，并记下 VMware Tools tar 安装程序的文件名。

```
ls mount-point
```

8. 解压缩安装程序。

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

`x.x.x` 值是产品版本号，`yyyy` 是产品版本的内部版本号。

如果尝试安装 `tar` 安装以覆盖 `RPM` 安装或相反，安装程序将检测以前的安装并且必须转换安装程序数据库格式，然后才能继续操作。

9. 如果需要，请卸载 CD-ROM 映像。

```
umount /dev/cdrom
```

如果 Linux 发行版自动装载 CD-ROM，则不需要卸载该映像。

10. 运行安装程序并配置 VMware Tools。

```
cd vmware-tools-distrib  
./vmware-install.pl
```

通常，在安装程序文件结束运行后，将运行 `vmware-config-tools.pl` 配置文件。

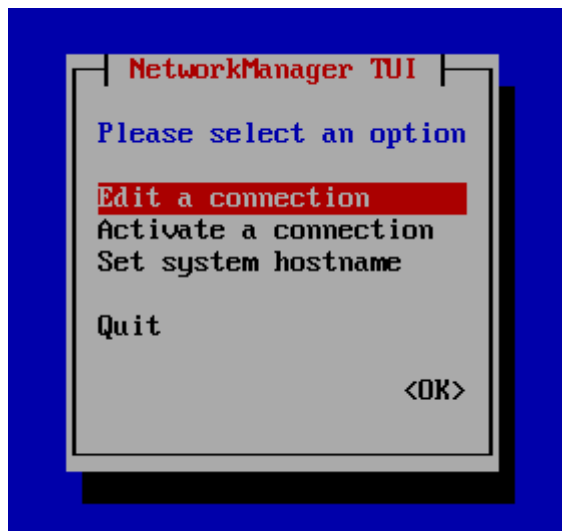
11. 如果适合您的配置，请按照提示接受默认值。
12. 按照脚本结尾处的说明进行操作。

根据使用的功能，这些说明可能包括重新启动 X 将话、重新启动网络连接、重新登录以及启动 VMware 用户进程。或者，也可以重新引导客户机操作系统以完成所有这些任务。

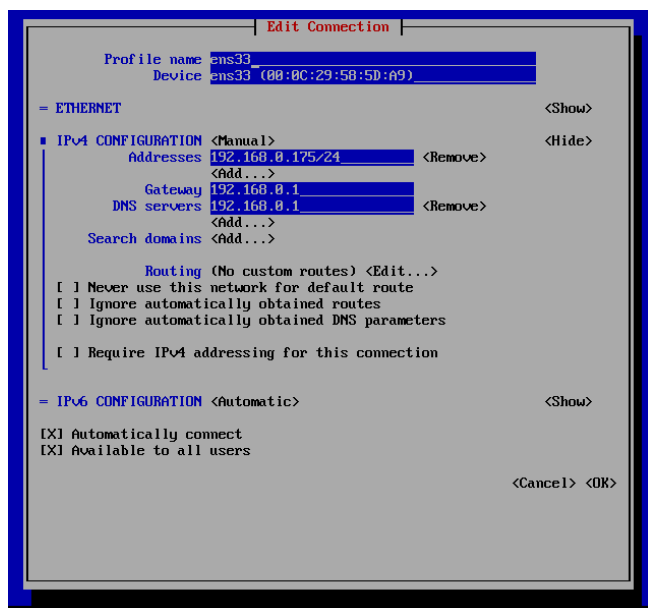
5 设置主机网卡

nmtui

手动设置网卡



编辑网卡



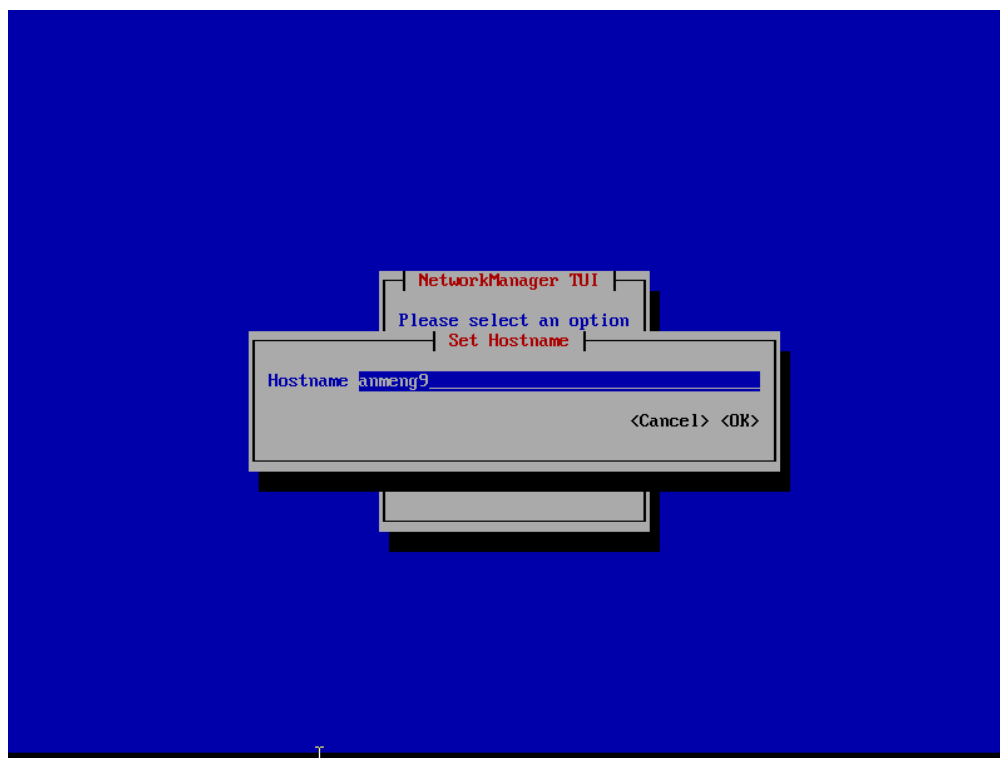
重新启动网卡

systemctl restart network

6 设置主机名称



Setup



注意需要修改 hosts 文件
vim /etc/hosts

```

127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1        localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.0.210 anmeng9.anmeng.com.cn anmeng9

```

-- INSERT --

3,44 all

基本测试

Hostname

Hostname -i

```

"/etc/hosts" 3L, 202B written
[root@localhost ~]# hostname
anmeng9
[root@localhost ~]# hostname -i
192.168.0.210
[root@localhost ~]# _

```

7 安装服务端

```
[root@anmeng9 opt]# vim /etc/profile
```

尾部添加 export ACE_HOME=/opt/aceserver

```

Windows PowerShell
if [ "$HISTCONTROL" = "ignoreospace" ] ; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want unmask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "$/usr/bin/id -gn" = "$/usr/bin/id -un" ] ; then
    unmask 002
else
    unmask 022
fi

for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do
    if [ -r "$i" ] ; then
        if [ "$<#i" != "-" ] ; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
    fi
done

unset i
unset -f pathmunge

if [ -n "$BASH_VERSION" ] ; then
    if [ -f /etc/bashrc ] ; then
        # Bash login shells run only /etc/profile
        # Bash non-login shells run only /etc/bashrc
        # Check for double sourcing is done in /etc/bashrc.
        . /etc/bashrc
    fi
fi

export ACE_HOME=/opt/aceserver

```

更新管径变量

source /etc/profile

7.1 启动安装脚本

以管理员身份启动脚本安装，转入解压目录

./install.sh

```

[root@anmeng9 anmeng-9.0_2.2.07-linux-x86_64_full]# source /etc/profile
[root@anmeng9 anmeng-9.0_2.2.07-linux-x86_64_full]# ./install.sh
ACE_HOME:/opt/aceserver
install dependency package...
上次元数据过期检查: 0:41:26 前, 执行于 2022 年 09 月 24 日 星期六 07 时 20 分 09 秒。
软件包 vim-enhanced-2:8.2.1412-3.uelc20.01.x86_64 已安装。
软件包 net-tools-2.0-0.53.20160912git.uelc20.2.x86_64 已安装。
install mysql
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/dependency_software/mysql
##### A tool to auto-compile & install MySQL on Redhat/CentOS 6 or 7 Linux #####
##### Check environment .....#####
Checking user :
user is root, this is ok!

```

```

checking os version
os is linux,this is ok!
mysql datadir /data/mysql is not exist,this is ok!
os version is el6 or el7, this is ok!
mysql port is not 3306! this is ok!

MySQL root'password is:Anmeng12#$
You will install MySQL.....

##### MySQL installing.....#####
uncompressing mysql-5.7.28-linux-glibc2.12-x86_64.tar.gz file.....
please wait a few minutes.....
directory /data/mysql created succeed!
directory /data/slowlog created succeed!
Starting MySQL... SUCCESS!
Shutting down MySQL.. SUCCESS!
Starting MySQL.. SUCCESS!
=====MySQL 5.7.28 install completed=====

===== Check install =====
Checking...
MySQL: OK
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN
tcp6       0      0 :::111                  :::*                     LISTEN
tcp6       0      0 :::22                   :::*                     LISTEN
tcp6       0      0 :::631                  :::*                     LISTEN
root      45754      1  1 08:07 pts/0      00:00:00 /bin/sh /usr/local/mysql/bin/mysqld_safe --
datadir=/data/mysql --pid
-file=/data/mysql/mysql.pid
mysql      46867      45754 13 08:07 pts/0      00:00:00 /usr/local/mysql/bin/mysqld --
basedir=/usr/local/mysql --datadir=/da
ta/mysql --plugin-dir=/usr/local/mysql/lib/plugin --user=mysql --log-error=/data/mysql/error.log --open-files-
limit=8192
--pid-file=/data/mysql/mysql.pid --socket=/tmp/mysql.sock --port=3306
root      47905      6001  0 08:07 pts/0      00:00:00 grep mysql
=====checked succeeded!checking result MySQL completed! =====

```

```
#####Finish#####
install anmeng core
ACE_HOME:/opt/aceserver
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/anmeng-core
##### A tool to auto-compile & install ACE Core Component on Redhat/CentOS 6 or 7 Linux
#####
##### Check the environment..... #####
Checking user :
user is root, this is ok!
checking os version
os is linux,this is ok!
os version is el6 or el7, this is ok!
directory /opt/aceserver created succeed!

##### ACE Core Comonent Installing..... #####
uncompressing anmeng-core-2.2.07.tar.gz file.....
please wait a few minutes.....
===== ACE Core Component install completed=====

install java
ACE_HOME:/opt/aceserver
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/dependency_software/java
##### A tool to auto-compile & install Java on Redhat/CentOS 6 or 7 Linux #####
##### Check the environment..... #####
Checking user :
user is root, this is ok!
checking os version
os is linux,this is ok!
os version is el6 or el7, this is ok!

##### Java installing..... #####
uncompressing jdk-8u311-linux-x64.tar.gz file.....
please wait a few minutes.....
=====Java install completed=====

install tomcat
ACE_HOME:/opt/aceserver
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/dependency_software/tomcat
##### A tool to auto-compile & install Apache Tomcat on Redhat/CentOS 6 or 7 Linux #####
##### Check the environment..... #####
```

```
Checking user :
user is root, this is ok!
checking os version
os is linux,this is ok!
os version is el6 or el7, this is ok!

##### Apache Tomcat installing..... #####
uncompressing apache-tomcat-8.5.82.tar.gz file.....
please wait a few minutes.....
=====Apache Tomcat install completed=====

install anmeng manang component
ACE_HOME:/opt/aceserver
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/anmeng-amm
##### A tool to auto-compile & install ACE AMM Component on Redhat/CentOS 6 or 7 Linux
#####
##### Check the environment..... #####
Checking user :
user is root, this is ok!
checking os version
os is linux,this is ok!
os version is el6 or el7, this is ok!
directory /opt/aceserver created succeed!
directory /opt/aceserver/tomcat/webapps is ok!

##### ACE Manage Comonpent Installing..... #####
uncompressing anmeng-amm-2.2.07.tar.gz file.....
please wait a few minutes.....
===== ACE Manage Component install completed=====

Using CATALINA_BASE:  /opt/aceserver/tomcat
Using CATALINA_HOME:  /opt/aceserver/tomcat
Using CATALINA_TMPDIR: /opt/aceserver/tomcat/temp
Using JRE_HOME:       /opt/aceserver/java
Using CLASSPATH:      /opt/aceserver/tomcat/bin/bootstrap.jar:/opt/aceserver/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
install anmeng ag
ACE_HOME:/opt/aceserver
/opt/anmeng-9.0_2.2.07-linux-x86_64_full/anmeng-ag
```

```
##### A tool to auto-compile & install ACE Auth Gateway Component on Redhat/CentOS 6 or 7 Linux
#####
##### Check the environment..... #####
Checking user :
user is root, this is ok!
checking os version
os is linux,this is ok!
os version is el6 or el7, this is ok!
directory /opt/aceserver created succeed!

##### ACE Auth Gateway Comonent Installing.....
#####
uncompressioning anmeng-ag-2.2.07.tar.gz file.....
please wait a few minutes.....
===== ACE Auth Gateway Component install
completed=====

[root@anmeng9 anmeng-9.0_2.2.07-linux-x86_64_full]#
```

7.2 配置认证角色

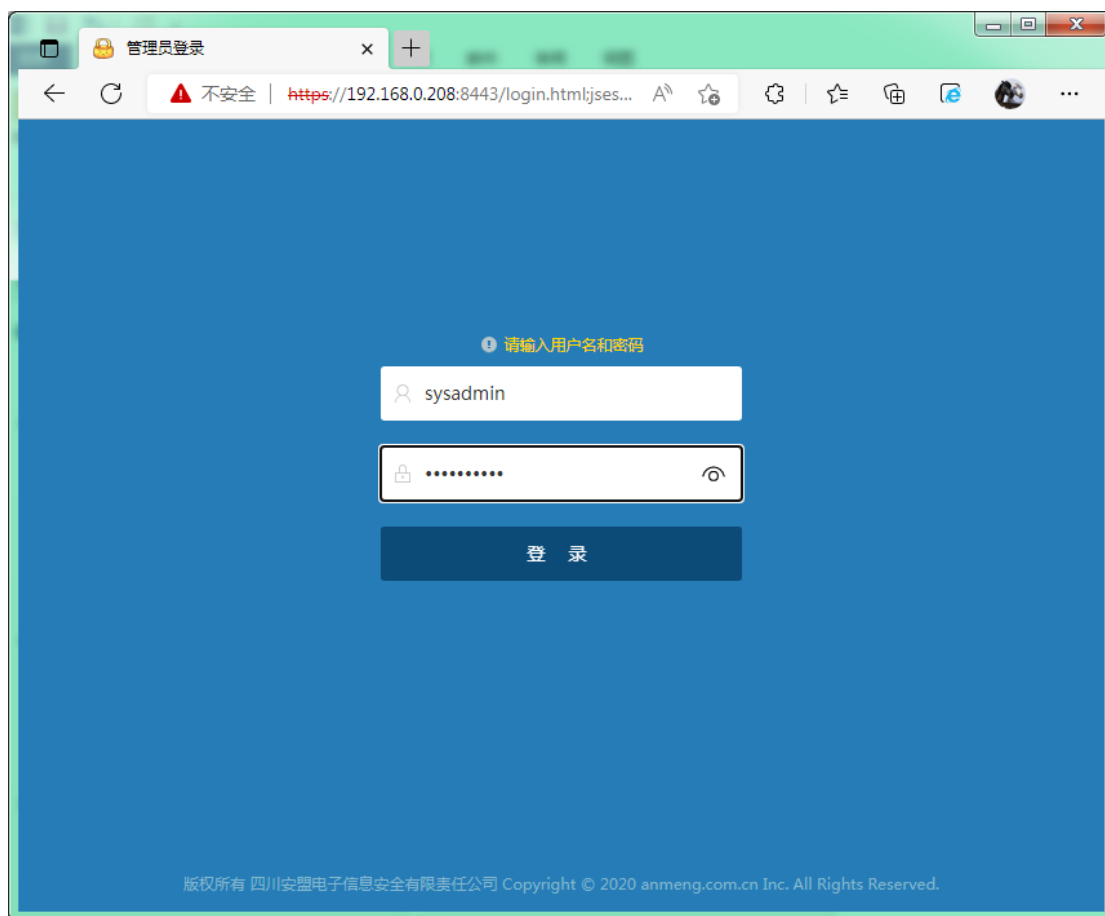
```
[root@anmeng9 bin]# cp /opt/license.xml ./
[root@anmeng9 bin]# cd /opt/aceserver/anmeng-core/bin
[root@anmeng9 bin]# cp /opt/license.xml ./
[root@anmeng9 bin]# ./createdb
```

```
Please select operation type:
1. Create a new server
2. Restore data
3. Quit
1
Please select the type of server
1. master server
2. slave server
1
szMsg:execute sql sentence successful.

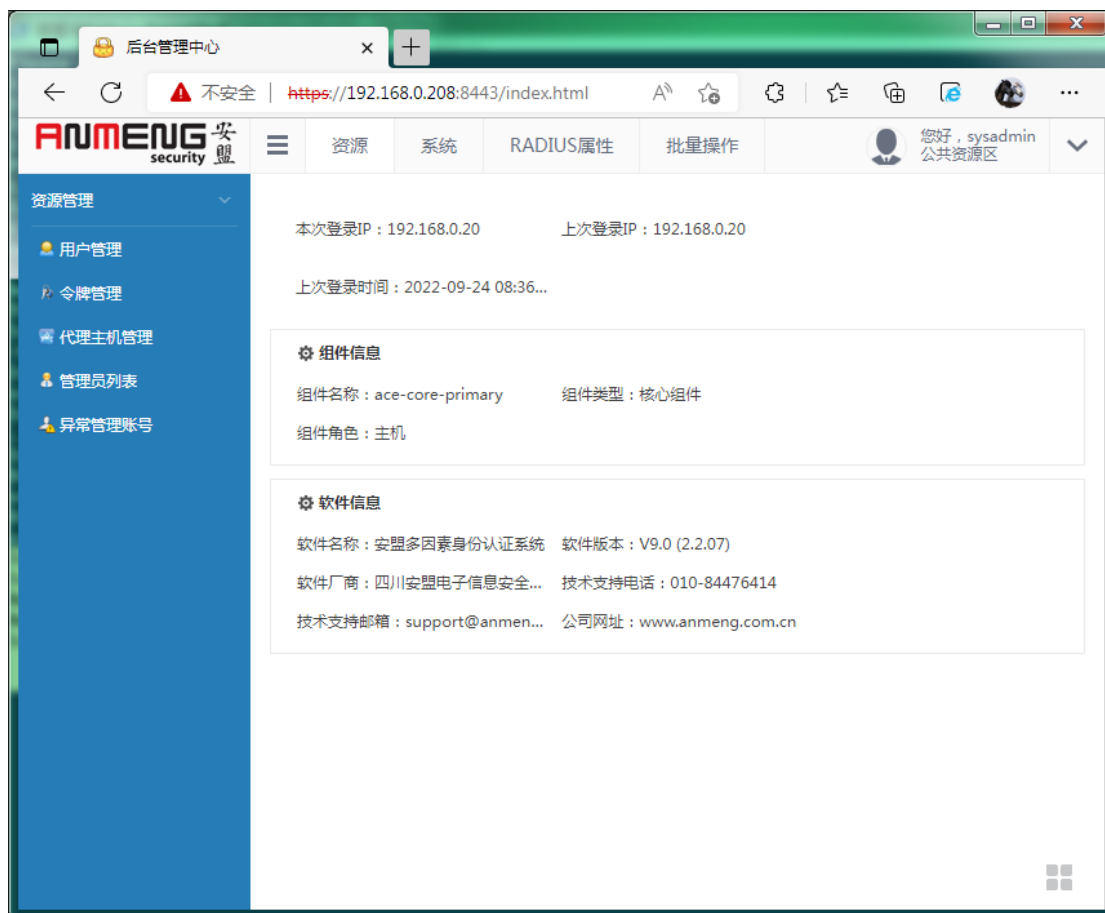
host ip = 192.168.0.208 ,do you want to change it? ('y' or 'n')n
The database has been created.
[root@anmeng9 bin]#
```

```
[root@anmeng9 bin]# ./aced start
Start core service.....
core service started.
Start core syncsrv.....
core sync service started.
[root@anmeng9 bin]#
```

浏览器打开



安装完成




7.3 添加认证网关

注意，安盟所有组件使用都是“注册机制”。

安盟认证网关的启用，需要先在管理组件 AMM 中注册，然后在初始化安装。只有系统管理员 Sysadmin 才能安装 AG 组件。如果密码已经更改，请务必识记，因为初始化 AG 组件需要用到密码进行确认。

首次运行，以管理员身份登录管理组件，在组件管理中，添加一台认证网关组件，如下图所示：



系统设置

- 系统参数
- 运行参数
- 组件管理**
- 导入用户
- 导入令牌
- 系统许可
- 代理主机配置文件
- LDAP策略
- 会话管理

新建组件 删除组件 修改地址

搜索

组件名称	组件地址	组件类型	组件角色	状态	创建时间
ace-core-primary	192.168.1.200	核心	主机	启用	2020-03-11 22:19:40

显示第 1 到第 1 条记录, 总共 1 条记录

基本资料

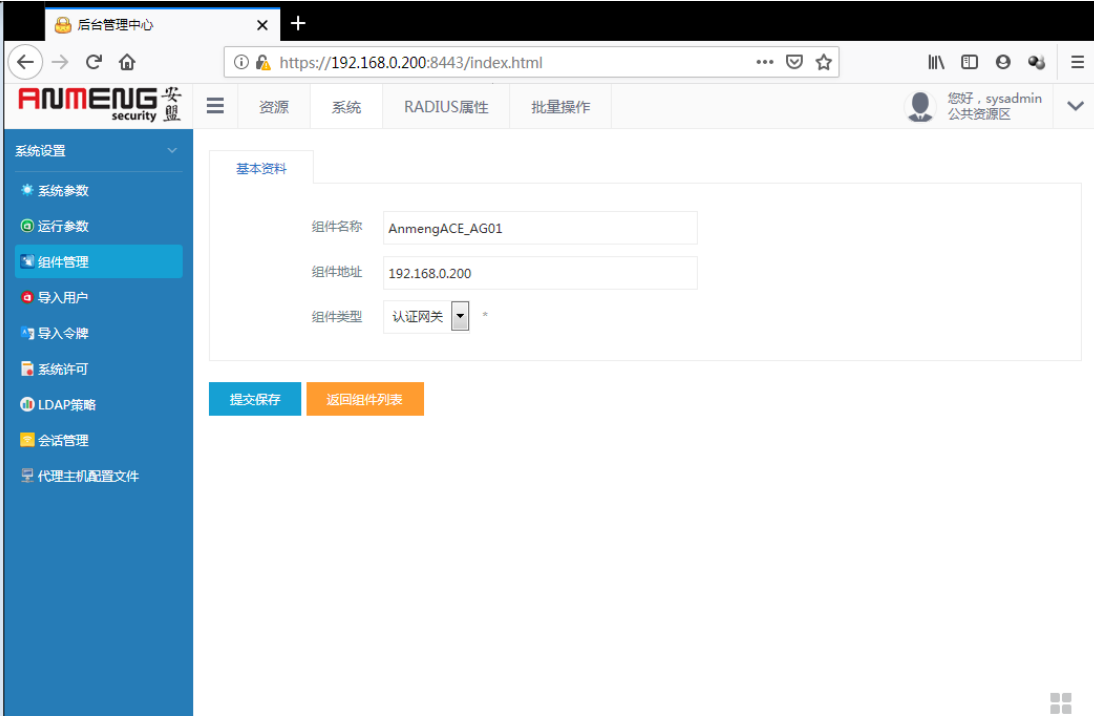
组件名称: ag1

组件地址: 192.168.1.200

组件类型: 认证网关 *

提交保存 返回组件列表

注：核心组件和认证网关可以安装在同一台电脑上。



后台管理中心

https://192.168.0.200:8443/index.html

系统设置

- 系统参数
- 运行参数
- 组件管理**
- 导入用户
- 导入令牌
- 系统许可
- LDAP策略
- 会话管理
- 代理主机配置文件

基本资料

组件名称: AnmengACE_AG01

组件地址: 192.168.0.200

组件类型: 认证网关 *

提交保存 返回组件列表

初始化 AG 服务

```
cd /opt/aceserver/anmeng-ag/prog
./createdb
```

```
[root@ace-primary prog]#
[root@ace-primary prog]# ./createdb
Do you want to initialize the database of this component? ('y' or 'n')y
Please input master server address: 192.168.1.200
Please input master server port: 6580
Please input the password of sysadmin:
Create database.....
Downloading data from core server.....
The database has been initialized.
[root@ace-primary prog]#
```

需输入sysadmin的密码

注意：sysadmin 密码就是系统管理员密码

```
[root@ACEPrimary prog]# ./createdb
Do you want to initialize the database of this component? ('y' or 'n')y
Please input master server address: 192.168.0.200
Please input master server port: 6580
Please input the password of sysadmin:
Create database.....
Downloading data from core server.....
The database has been initialized.
[root@ACEPrimary prog]#
```

启动 AG 服务

组件初始化成功之后，运行./startserver 就可以启动组件，如下所示：

```
cd /opt/aceserver/anmeng-ag/prog
./startserver
```

```
[root@ace-primary prog]#
[root@ace-primary prog]# ./startserver
Start broker.....
Broker started.
Start authengine.....
Autheticate engine started.
Start radiusserver.....
radius service started.
Start syncsrv.....
sync service started.
[root@ace-primary prog]#
```

通过 netstat-ano | grep -E '1812|1813|6500' 查看 udp 1812,1813,6500 等端口是否在监听，如下图所示：

```
[root@ace-primary prog]# netstat -ano | grep -E '1812|1813|6500'
udp      0      0 0.0.0.0:6500 0.0.0.0:*        off (0.00/0/0)
udp      0      0 0.0.0.0:1812 0.0.0.0:*        off (0.00/0/0)
udp      0      0 0.0.0.0:1813 0.0.0.0:*        off (0.00/0/0)
[root@ace-primary prog]#
```

检查状态

```
netstat-ano | grep -E '1812|1813|6500'
```

到此，安盟认证系统主机安装完。