

UniCloud License Server

安装指导

紫光云技术有限公司
<http://www.unicloud.com>

资料版本：5W100-20220407

© 紫光云技术有限公司 2022 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本档内容的部分或全部，并不得以任何形式传播。

对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光云保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光云尽全力在本手册中提供准确的信息，但是紫光云并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

UniCloud License Server 安装指导主要介绍了 License Server 软件的安装、登录及卸载方法。前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员






本书约定

1. 格式约定

格 式	意 义
<>	带尖括号“<>”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: unicloud-ts@unicloud.com

感谢您的反馈，让我们做得更好！

目 录

1 概述	1-1
2 安装前的准备工作	2-1
2.1 网络配置需求	2-1
2.2 服务器配置需求	2-1
2.2.1 硬件配置需求	2-1
2.2.2 软件配置需求	2-2
2.3 浏览器需求	2-2
2.4 运行环境配置	2-2
3 License Server 安装	3-1
3.1 安装方式介绍	3-1
3.2 安装 License Server	3-1
3.2.1 使用 ZIP 软件包安装 License Server	3-1
3.2.2 使用 ISO 软件包安装操作系统和 License Server	3-3
3.2.3 放行 License Server 相关端口、地址和协议	3-10
3.3 登录 License Server	3-17
3.4 部署 License Server HA 集群	3-18
4 卸载 License Server	4-1
5 升级 License Server	5-1
5.1 升级注意事项	5-1
5.2 单机方式部署下升级	5-1
5.3 HA 方式部署下非 ISSU 升级	5-1
6 常见问题解答	6-1
6.1 安装授权后，如需变更硬件应该如何操作？	6-1
6.2 安装授权后，如需变更操作系统应该如何操作？	6-1
6.3 变更操作系统的同时需要升级 License Server 应该如何操作？	6-2
6.4 以 HA 方式部署时其中一台 License Server 主机故障需要更换应该如何操作？	6-2

1 概述

UniCloud License Server 是 UniCloud 推出的一款授权管理软件，具有集中管理授权、集中分发授权、HA（High Availability，高可靠性）集群等功能，可以简化用户的 License 使用、解决动态业务授权控制等问题。

License Server 的主要特点如下：

- 支持授权与服务器硬件绑定，支持授权安装、存储在 License Server 上
- 支持从 License Server 向网络中的授权业务提供授权服务
- 支持主备 License Server 冗余备份功能，提供不间断的授权服务

2 安装前的准备工作

2.1 网络配置需求

在安装 License Server 之前，建议您根据具体需求先规划好基础网络，使得 License Server 所在的服务器的 IP 地址在网络中可达。

2.2 服务器配置需求

2.2.1 硬件配置需求

License Server 所需服务器的硬件配置如[表 2-1](#)所示。

表2-1 硬件配置需求

CPU架构	CPU内核	内存	所需磁盘空间	网卡	备注
x86_64(Intel64/AMD64)或ARM64	16核、2.0Ghz主频及以上	32GB及以上	64GB及以上（根目录所在的系统分区）	支持1-10Gbps带宽	推荐配置 基于该配置可支持2000个以内的客户端数量
x86_64(Intel64/AMD64)或ARM64	2核、2.0Ghz主频及以上	4GB及以上	64GB及以上（根目录所在的系统分区）	支持1-10Gbps带宽	最简配置 基于该配置仅支持20个以内的客户端数量



说明

为保证 License Server 正常运行，请将 License Server 安装在物理服务器而非虚拟机上。

2.2.2 软件配置需求

License Server 所需服务器的操作系统为:

- CentOS 7.6 x86_64
- UniCloudLinux Release 1.1.2 x86_64
- UniCloudLinux 1.1.2 ARM64
- Kylin Linux Advanced Server release V10 x86_64
- Kylin Linux Advanced Server release V10 ARM64
- BC-Linux V7.7 x86_64
- BC-Linux V7.7 aarch64

License Server 安装需要依赖软件包如[表 2-2](#)所示:

表2-2 依赖包版本号

依赖包名称	版本号
unzip	6.0

2.3 浏览器需求

用户使用浏览器即可访问 License Server。支持的浏览器类型及版本为:

- Google Chrome 55 及以上;
- Internet Explorer 11 及以上。

2.4 运行环境配置

1. 禁用 SELinux

(1) 禁用 SELinux 需要修改 SELinux 配置文件。

```
vi /etc/selinux/config
```

(2) 将 SELINUX 参数值设置为 disabled, 以禁用 SELINUX。

```
SELINUX=disabled
```

(3) 保存退出后重启系统即可生效。

2. 配置 DNS

Linux 操作系统下的/etc/resolv.conf 是 DNS 客户机的配置文件,可用于设置 DNS 服务器的 IP 地址。License Server 的授权文件在线自动安装功能需要配置 DNS 服务器的 IP 地址,以对“License 管理平台域名”进行域名解析。配置文件的内容举例说明:

```
[root@localhost opt]# cat /etc/resolv.conf
search localdomain
nameserver 192.168.1.1
```

其中, nameserver 表明 DNS 服务器的 IP 地址。可以配置很多行的 nameserver, 每一个带一个 IP 地址。在查询时就按 nameserver 在本文件中的顺序进行, 且只有当第一个 nameserver 没有反应时才查询下面的 nameserver。

3 License Server 安装

3.1 安装方式介绍

License Server 支持两种方式安装：

- 使用 ZIP 软件包安装 License Server：在已有的操作系统上安装 License Server 软件包
- 使用 ISO 软件包安装 License Server：使用 ISO 镜像同时安装操作系统和 License Server



注意

- 使用 ZIP 软件包安装 License Server 时，安装 License Server 前请校准操作系统时间，安装后请勿修改系统时间，以免造成数据紊乱。
 - 使用 ISO 软件包安装 License Server 时，在安装操作系统过程中设置成准确的系统时间或安装完成后启用 License Server 之前校准操作系统时间并重启系统，启用 License Server 后请勿修改系统时间，以免造成数据紊乱。
-

3.2 安装 License Server

3.2.1 使用 ZIP 软件包安装 License Server



说明

当前系统支持使用 root 用户和非 root 用户安装 License Server 软件包，推荐使用 root 用户进行安装。若使用非 root 用户安装软件包，则需要为非 root 用户添加权限，操作步骤为：在 root 用户视图下通过 **visudo** 命令打开配置文件，在配置文件末尾添加配置：`<username> ALL=(root) NOPASSWD:/bin/bash`，其中 *username* 表示非 root 用户名。权限添加完成后，执行安装和卸载命令时，需要在命令前添加 **sudo** 指令。

1. 上传 License Server 安装软件包

将 License Server 安装软件包拷贝至服务器的待安装目录下，或使用 FTP 等文件传输协议将软件包上传到指定目录。



说明

如果需要利用 FTP、TFTP 协议上传下载，请选择 binary 模式（二进制模式）传输，以免损坏软件包。

2. 在服务器上安装 License Server

License Server 软件的安装步骤如下所示。

- (1) 进入 License Server 软件包 (.zip 文件) 的存放路径 (以路径 /root 为例), 解压 License Server 软件包, 软件包的名称格式为 LICENSE_SERVER-version-arch.zip, 其中 version 为版本号, arch 为系统版本 (x86_64/arm64)。

```
[root@localhost ~]# unzip LICENSE_SERVER-E1201-x86_64.zip
Archive:  LICENSE_SERVER-E1201-x86_64.zip
  inflating: LICENSE_SERVER-E1201-x86_64/install.sh
  inflating: LICENSE_SERVER-E1201-x86_64/LICENSE_SERVER.tar.gz
```

- (2) 进入解压后的目录。

```
[root@localhost ~]# cd LICENSE_SERVER-E1201-x86_64
```

- (3) 执行安装脚本。

```
[root@localhost LICENSE_SERVER-E1201-x86_64]# ./install.sh
...略...
```

- (4) 提示输入授权服务端口号, 直接回车则使用默认端口号 5555。请确认使用的端口号为空闲端口号。

```
Type the license service port (1024-65535, default:5555) :
```

- (5) 提示输入 WEB 服务的 HTTPS 端口号, 直接回车则使用默认端口号, 请确认使用的端口号为空闲端口号。

```
Type the HTTPS port for the Web login (1-65535, default:28443) :
```

- (6) 提示输入监控服务的 HTTPS 端口号, 直接回车则使用默认端口号, 请确认使用的端口号为空闲端口号。

```
Type the HTTPS port for the Monitor login (1-65535, default:38443) :
```

3. 验证 License Server 是否安装成功

- (1) 查看 License Server 的 licsmgr 服务、licsmonitor 服务、licsmariadb 服务和 licsredis 数据库服务是否开启。如果都显示 active (running), 则表示 License Server 服务已开启。

```
[root@localhost ~]# service licsmgr status
Redirecting to /bin/systemctl status licsmgr.service
● licsmgr.service - LICS Manager
   Loaded: loaded (/usr/lib/systemd/system/licsmgr.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-01-04 10:10:41 EST; 9min ago
...略...

[root@localhost ~]# service licsmonitor status
Redirecting to /bin/systemctl status licsmonitor.service
● licsmonitor.service - LICS Monitor
   Loaded: loaded (/usr/lib/systemd/system/licsmonitor.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-01-04 10:10:41 EST; 10min ago
...略...

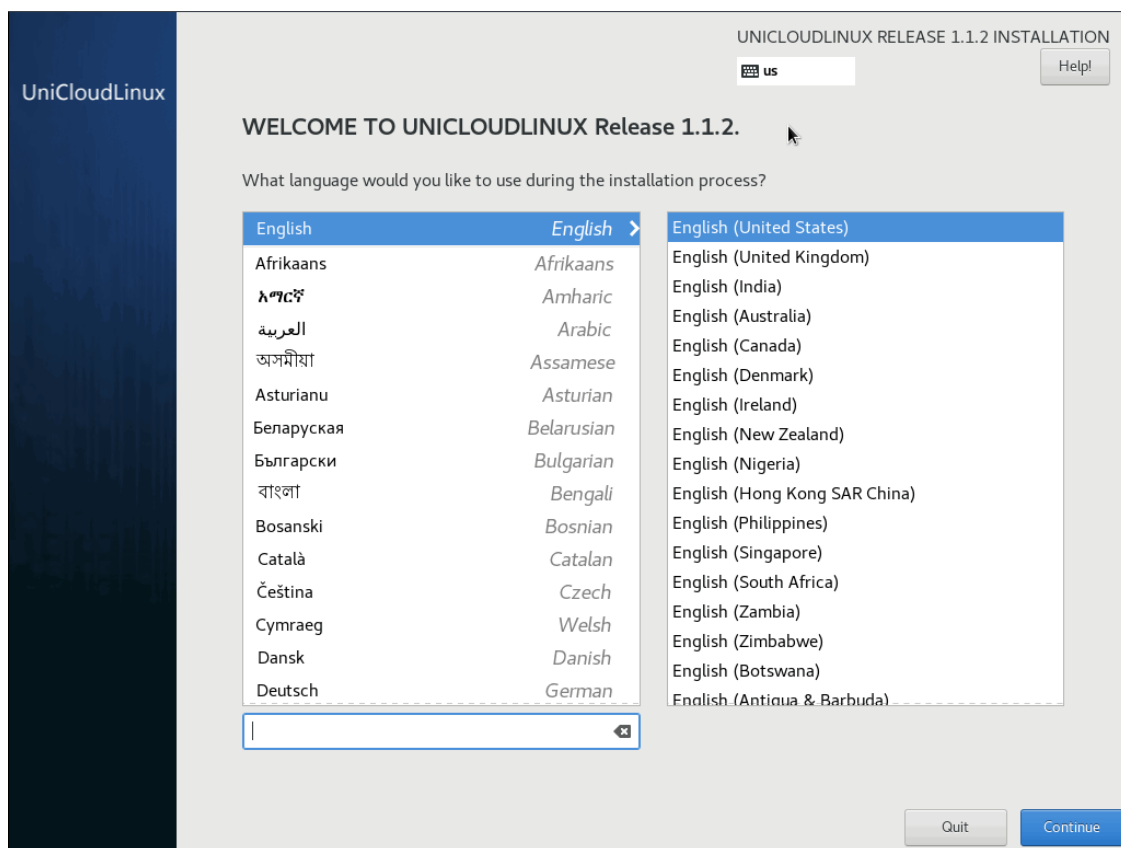
[root@localhost ~]# service licsmariadb status
Redirecting to /bin/systemctl status licsmariadb.service
● licsmariadb.service - Lics Mariadb
   Loaded: loaded (/usr/lib/systemd/system/licsmariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-01-04 12:52:01 EST; 22h ago
...略...
```

```
[root@localhost ~]# service licsredis status
Redirecting to /bin/systemctl status licsredis.service
● licsredis.service - Lics Redis
   Loaded: loaded (/usr/lib/systemd/system/licsredis.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-01-04 10:05:48 EST; 16min ago
...略...
```

3.2.2 使用 ISO 软件包安装操作系统和 License Server

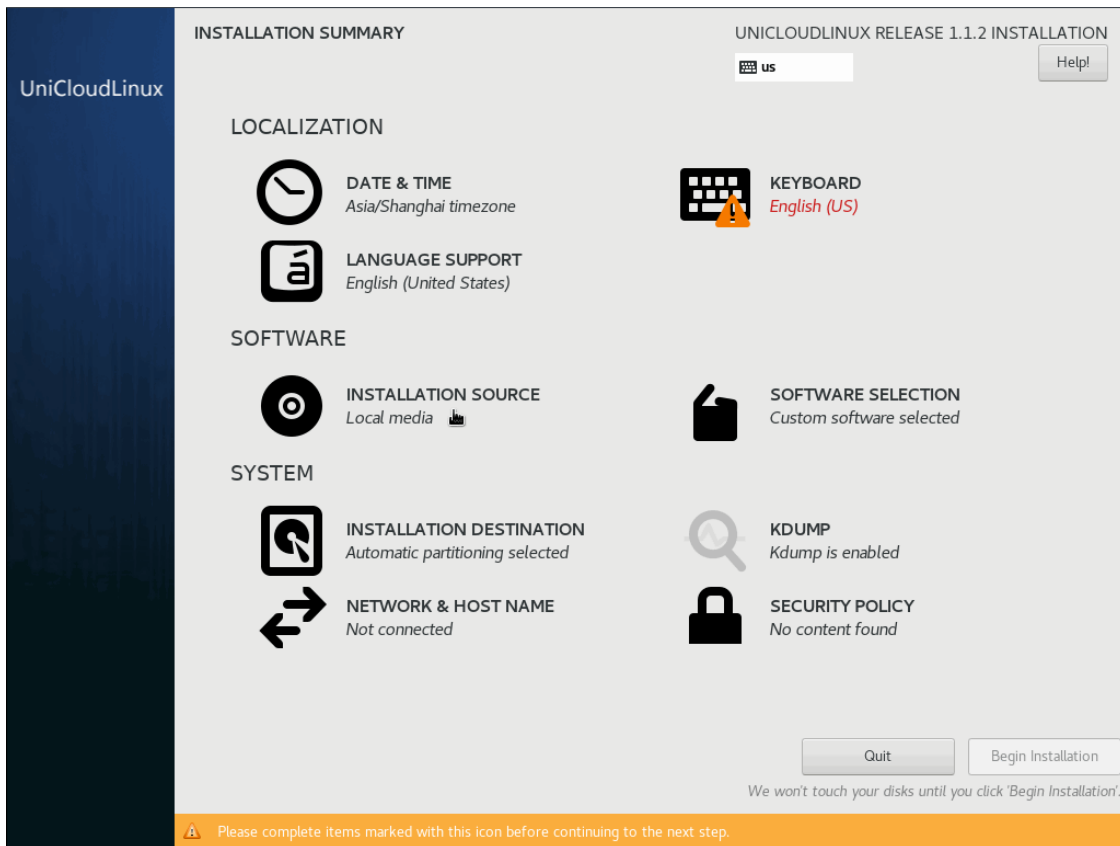
- (1) 使用服务器的远程控制台通过虚拟光驱加载安装软件包的 ISO 文件。
- (2) 重新启动服务器，重启后进入系统加载过程，加载完成后，进入 WELCOME TO UNICLOUDLINUX 界面。

图3-1 WELCOME TO UNICLOUDLINUX 界面



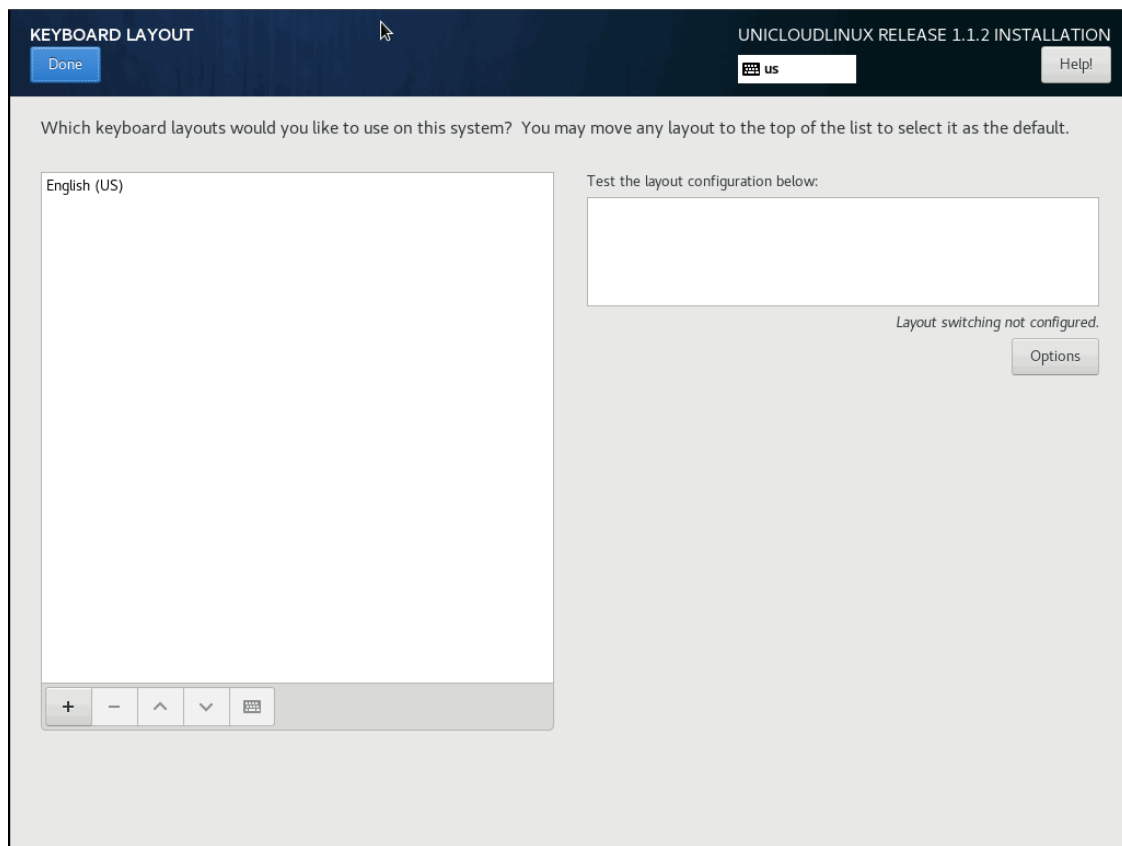
- (3) 选择语言，以 English 为例，单击<Continue>按钮进入 INSTALLATION SUMMARY 界面。

图3-2 INSTALLATION SUMMARY 界面



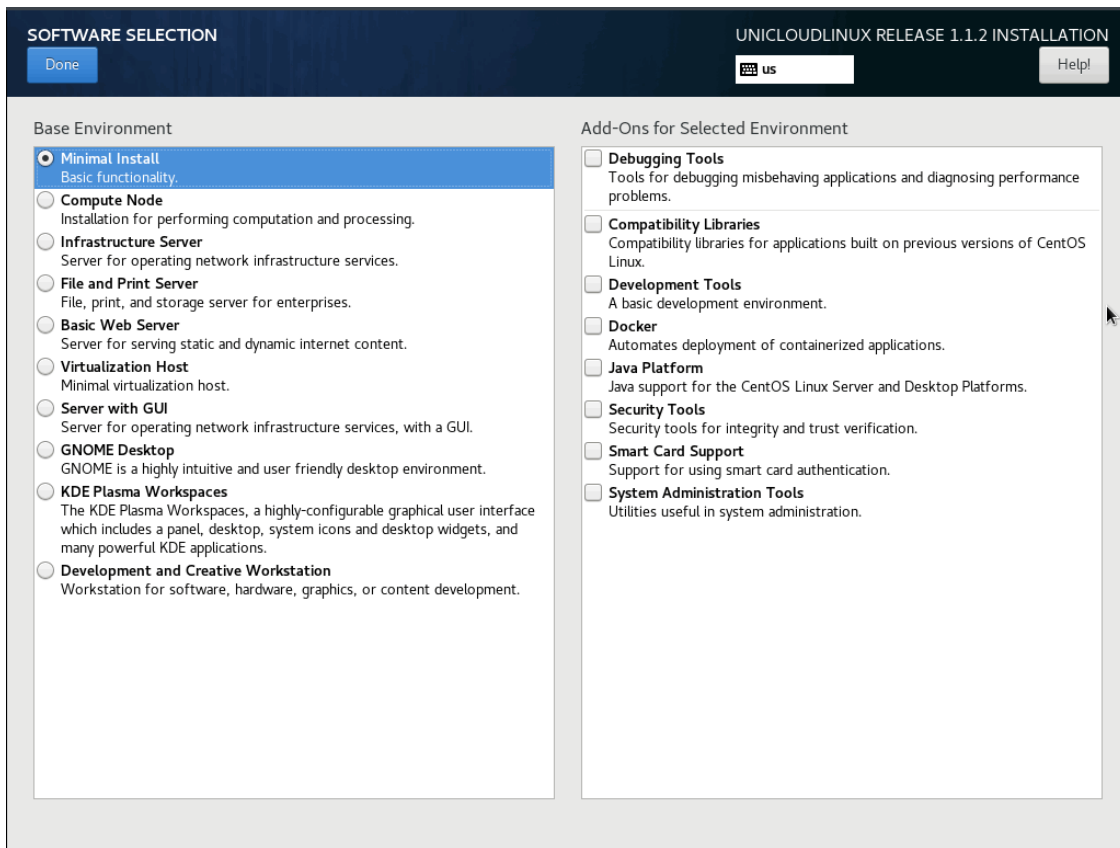
- (4) 单击“LOCALIZATION”栏目下的“DATE & TIME”链接进入时间和时区设置页面，选择当前地区的时区，例如，中国地区请选择 Asia/Shanghai 时区。时区和时间设置完成后，单击 <Done>按钮返回 INSTALLATION SUMMARY 界面。
- (5) 单击“LOCALIZATION”栏目下的“KEYBOARD”链接进入键盘布局配置页面，选择 English(US)。单击 <Done>按钮返回 INSTALLATION SUMMARY 界面。

图3-3 键盘布局配置页面



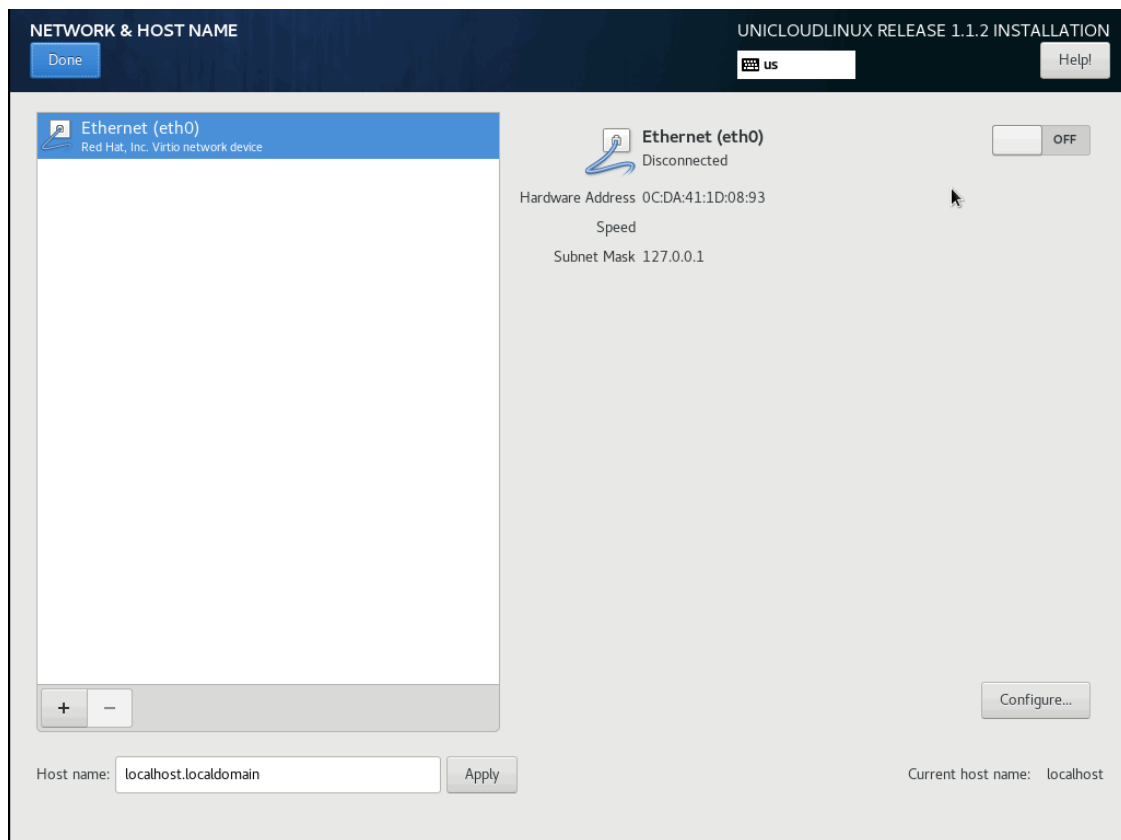
- (6) 单击“SOFTWARE”栏目下的“SOFTWARE SELECTION”链接进入软件选择页面，选择 Minimal Install。单击<Done>按钮返回 INSTALLATION SUMMARY 界面。

图3-4 软件选择页面



- (7) 单击“SYSTEM”栏目下的“NETWORK & HOST NAME”链接进入网络和主机名配置页面，如需修改主机名，可在 Host name 输入框中输入新的主机名，单击<Apply>按钮完成修改。

图3-5 网络和主机名配置页面



- (8) 在网络和主机名配置页面单击<Configure>按钮进入网络配置界面，单击<General>，勾选<Automatically connect to this network when it is available>复选框，如图 3-6 所示；然后单击<IPv4 Settings>配置 IPv4 地址，如图 3-7 所示。配置完成后单击<Save>按钮保存配置，再单击<Done>按钮返回 INSTALLATION SUMMARY 界面。

图3-6 General 配置

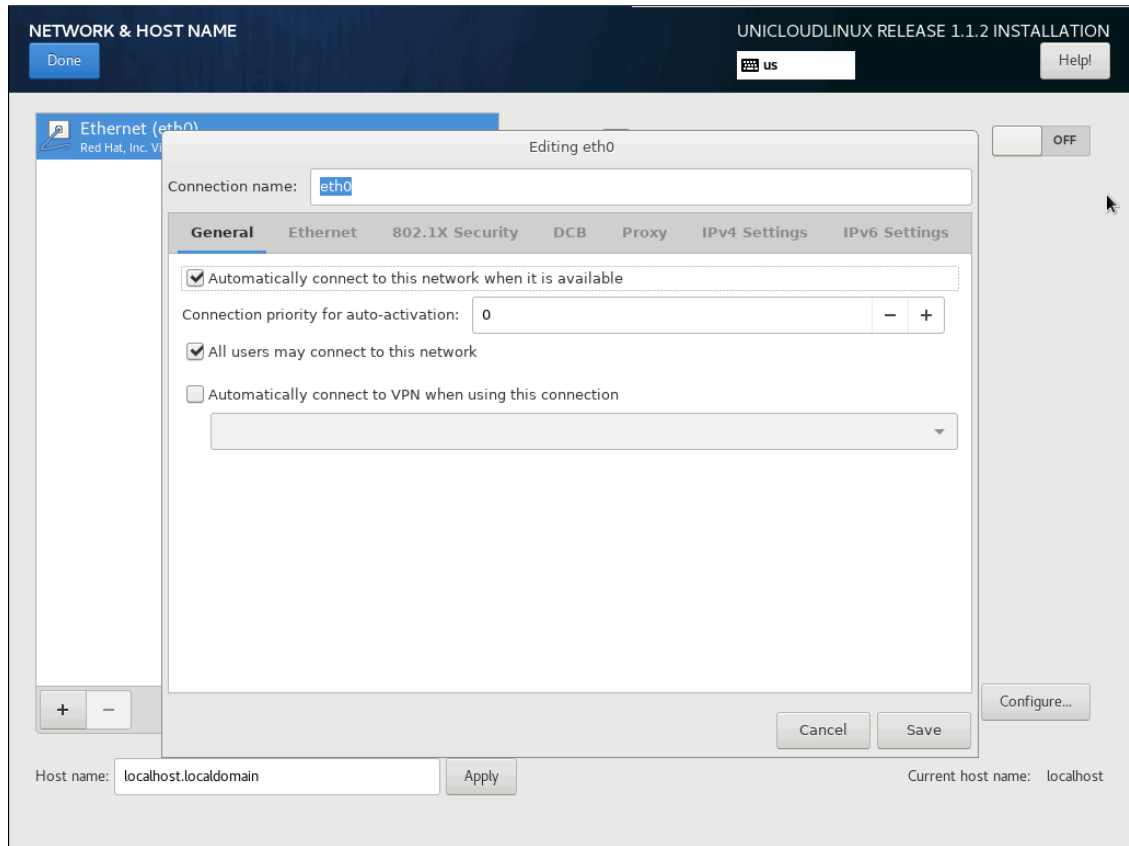
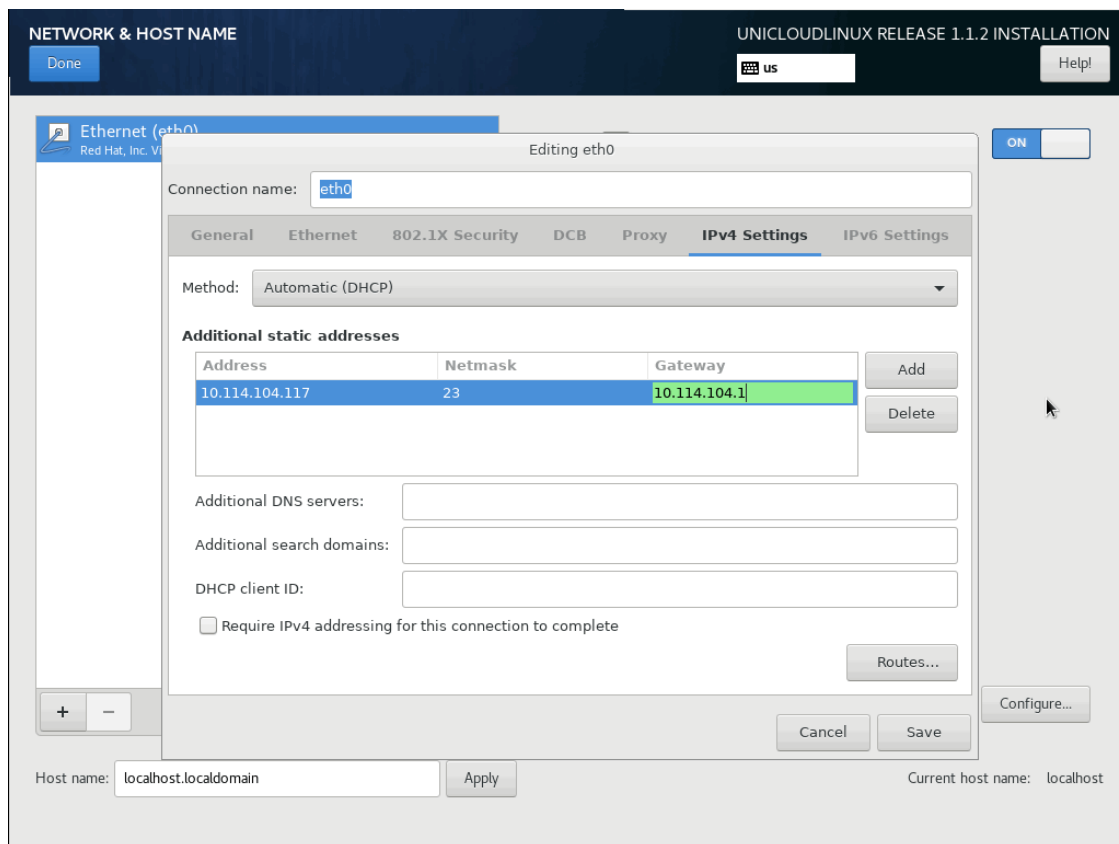
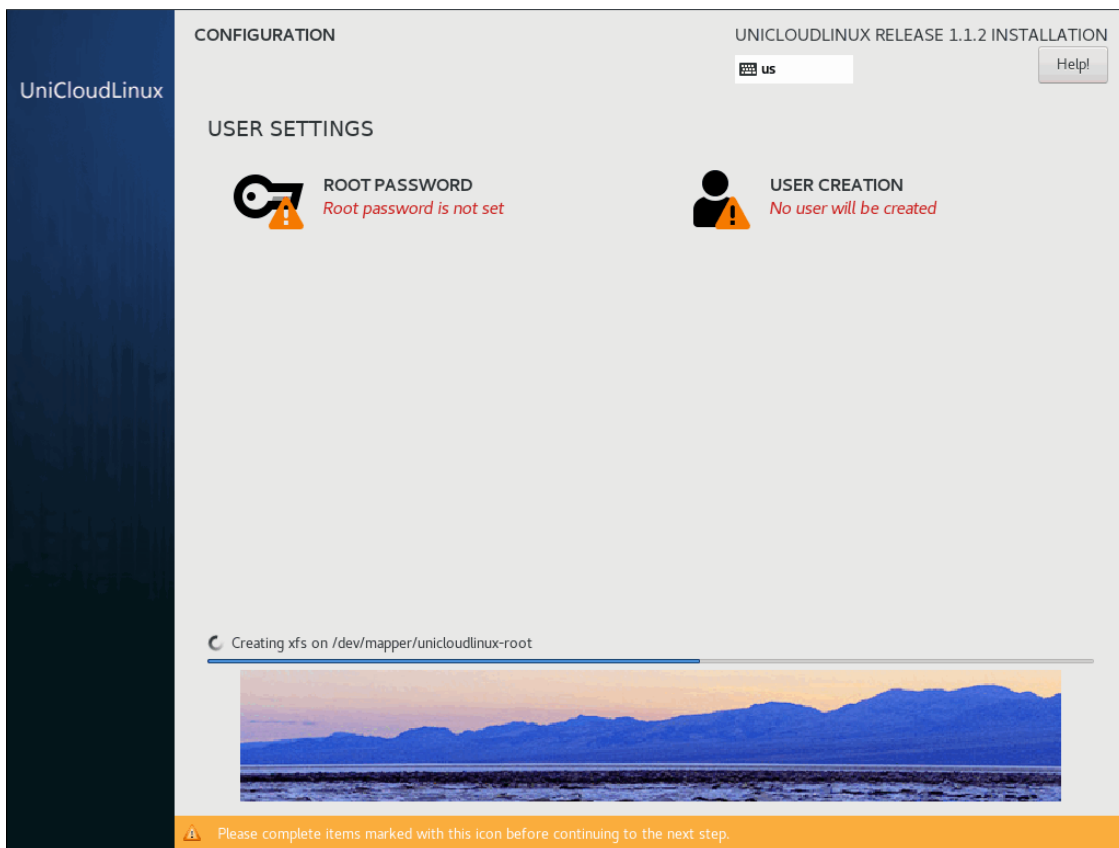


图3-7 配置 IPv4 地址



- (9) 完成上述操作后，单击<Begin Installation>按钮开始安装。在安装过程中会弹出用户配置选项，在该页面可创建 Root 用户和密码。

图3-8 设置用户及密码



(10) 安装完成后会自动重启，完成操作系统和 License Server 的安装。

3.2.3 放行 License Server 相关端口、地址和协议

可通过两种方式放行端口、地址和协议：Firewall 方式和 IPtables 方式，二者只可配置其一。可根据组网需求灵活选择配置方式。

License Server 安装完成后，需要根据 Firewall 或 IPtables 的状态进行如下处理：

- 如果 Firewall 和 IPtables 均处于关闭状态，可无需进行本章节的配置，但需要确保 Firewall 和 IPtables 处于永久关闭状态，否则可能导致 License Server 运行异常。当 License Server 暴露在公网环境中时，为提升安全性，建议开启 Firewall 或 IPtables，并按照本章节的配置步骤进行配置。
- 如果 Firewall 或 IPtables 处于开启状态，需确认 Firewall 或 IPtables 是否已放行了 License Server 相关端口、地址和协议，如果未放行，则需要通过本章节的步骤进行配置，否则 License Server 无法正常运行。需要放行的端口、地址和协议如下：
 - WEB 服务的 HTTPS 端口号
 - 监控服务的 HTTPS 端口号
 - 授权服务端口号
 - Mariadb 数据库端口号 23306
 - HA 功能 Keepalived 组播地址 244.0.0.18 (IPv6 组播地址为 ff02::12)和 VRRP 协议

1. 使用 Firewall 方式

(1) 查看 Firewall 状态

查看 Firewall 状态，如果显示 **active (running)**，则表示已开启。

```
[root@localhost ~]# service firewalld status
Redirecting to /bin/systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
   Active: active (running) since Thu 2015-07-30 12:33:26 CST; 20s ago
...略...
```

(2) 配置 Firewall 放行 License Server 的授权服务端口号和 HTTPS 端口号

- a. 验证 Firewall 是否放行了 License Server 的授权服务端口号和 HTTPS 端口号，授权服务端口号以 5555 为例，WEB 服务的 HTTPS 端口号以 28443 为例，监控服务的 HTTPS 端口号以 38443 为例，显示为 **no** 表示未放行。

```
[root@localhost ~]# firewall-cmd --query-port=5555/tcp
no
[root@localhost ~]# firewall-cmd --query-port=28443/tcp
no
[root@localhost ~]# firewall-cmd --query-port=38443/tcp
no
```

- b. 放行 License Server 相关端口号，显示 **success** 表示操作成功。

```
[root@localhost ~]# firewall-cmd --permanent --add-port=5555/tcp
success
[root@localhost ~]# firewall-cmd --permanent --add-port=28443/tcp
success
[root@localhost ~]# firewall-cmd --permanent --add-port=38443/tcp
success
```

- c. 重载配置使配置生效。

```
[root@localhost ~]# firewall-cmd --reload
success
```

- d. 验证端口是否放行成功，显示 **yes** 表示放行成功。

```
[root@localhost ~]# firewall-cmd --query-port=5555/tcp
yes
[root@localhost ~]# firewall-cmd --query-port=28443/tcp
yes
[root@localhost ~]# firewall-cmd --query-port=38443/tcp
yes
```

(3) 配置 Firewall 放行 HA 功能的 Mariadb 数据库端口号

如果 License Server 需要配置 HA 功能，则需要在主 License Server 和备 License Server 上配置 Firewall 放行 HA 功能的 Mariadb 数据库使用的端口 23306，为保证数据库安全，建议只允许在主 License Server 和备 License Server 之间开放此端口，即：在主 License Server 上配置向备 License Server 开放此端口，在备 License Server 上配置向主 License Server 开放此端口。

- a. 验证 Firewall 是否放行了 HA 功能的 Mariadb 数据库端口号，显示为 **no** 表示未放行，显示为 **yes** 表示已放行。

```
[root@localhost ~]# firewall-cmd --permanent --query-port=23306/tcp
no
```

- b. 如果已放行端口 23306，请先取消放行。

```
[root@localhost ~]# firewall-cmd --permanent --remove-port=23306/tcp
success
```

- c. 配置只对主或备 License Server 放行端口 23306，主或备 License Server 的 IP 地址以 IPv4 地址 192.168.109.15 为例。

```
[root@localhost ~]# firewall-cmd --permanent --add-rich-rule="rule family="ipv4"
source address="192.168.109.15" port protocol="tcp" port="23306" accept"
success
```

主或备 License Server 的 IP 地址以 IPv6 地址 2001::141 为例。

```
[root@localhost ~]# firewall-cmd --permanent --add-rich-rule="rule family="ipv6"
source address="2001::142" port protocol="tcp" port="23306" accept"
success
```

- d. 重载配置使配置生效。

```
[root@localhost ~]# firewall-cmd --reload
success
```

- e. 验证端口是否放行成功。

```
[root@localhost ~]# firewall-cmd --list-all
...略...
rule family="ipv4" source address="192.168.109.15" port port="23306" protocol="tcp"
accept
rule family="ipv6" source address="2001::142" port port="23306" protocol="tcp"
accept
```

(4) 配置 Firewall 放行 HA 功能 Keepalived 组播地址和 VRRP 协议

如果 License Server 需要配置 HA 功能，则需要配置 Firewall 放行 HA 功能所使用的 Keepalived 报文的组播地址和 VRRP 协议。

- a. 检查 Firewall 是否存在已放行 Keepalived 组播地址和 VRRP 协议，如果未配置规则或存在包含 Keepalived 组播地址和 VRRP 协议且状态为 DROP 的规则，表示未放行。

```
[root@localhost ~]# firewall-cmd --direct --get-all-rules
ipv4 filter INPUT 0 -d 224.0.0.18 -j DROP
ipv4 filter INPUT 0 -p vrrp -j DROP
ipv6 filter INPUT 0 -d ff02::12 -j DROP
ipv6 filter INPUT 0 -p vrrp -j DROP
```

- b. 配置 Firewall 放行 Keepalived 的 IPv4 组播地址。

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT
0 -d 224.0.0.18 -j ACCEPT
success
```

配置 Firewall 放行 Keepalived 的 IPv6 组播地址。

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT
0 -d ff02::12 -j ACCEPT
success
```

- c. 配置 Firewall 放行 IPv4 的 VRRP 协议。

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT
0 -p vrrp -j ACCEPT
success
```

配置 Firewall 放行 IPv6 的 VRRP 协议。

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT
0 -p vrrp -j ACCEPT
success
```

- d. 重载配置，使配置生效。

```
[root@localhost ~]# firewall-cmd --reload
Success
```

2. 使用 IPTables 方式 (IPv4 地址)

(1) 查看 IPTables 状态

查看 IPTables 状态，如果显示 **active (exited)**，则表示已开启。

```
[root@localhost ~]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset:
disabled)
   Active: active (exited) since Thu 2020-01-16 10:11:01 EST; 11s ago
...略...
```

(2) 配置 IPTables 放行 License Server 的授权服务端口号和 HTTPS 端口号

- a. 验证 IPTables 是否放行了 License Server 的授权服务端口号和 HTTPS 端口号，授权服务端口号以 5555 为例，WEB 服务的 HTTPS 端口号以 28443 为例，监控服务的 HTTPS 端口号以 38443 为例，未配置规则或存在目标值不是 **ACCEPT** 的规则表示未放行。

```
[root@localhost ~]# iptables -nvL | grep 5555
    0    0 DROP      tcp -- *      *      0.0.0.0/0          0.0.0.0/0          tcp
dpt:5555
```

```
[root@localhost ~]# iptables -nvL | grep 28443
```

```
[root@localhost ~]# iptables -nvL | grep 38443
```

- b. 如未配置规则，请添加以下规则放行相应端口号；如已存在目标值不是 **ACCEPT** 的规则，请将原规则删除后再添加。

```
[root@localhost ~]# iptables -I INPUT -p tcp --dport 5555 -j ACCEPT
[root@localhost ~]# iptables -I INPUT -p tcp --dport 28443 -j ACCEPT
[root@localhost ~]# iptables -I INPUT -p tcp --dport 38443 -j ACCEPT
```

- c. 保存规则。

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

- d. 重启 IPTables 服务，使配置生效。

```
[root@localhost ~]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
```

- e. 验证端口是否放行成功，目标值显示 **ACCEPT** 表示放行成功。

```
[root@localhost ~]# iptables -nvL | grep 5555
    0    0 ACCEPT    tcp -- *      *      0.0.0.0/0          0.0.0.0/0          tcp
dpt:5555
```

```
[root@localhost ~]# iptables -nvL | grep 28443
```

```
    0    0 ACCEPT    tcp -- *      *      0.0.0.0/0          0.0.0.0/0          tcp
dpt:28443
```

```
[root@localhost ~]# iptables -nvL | grep 38443
```

```

0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp
dpt:38443

```

(3) 配置 IPtables 放行 HA 功能的 Mariadb 数据库端口号

如果 License Server 需要配置 HA 功能，则需要在主 License Server 和备 License Server 上配置 IPtables 放行 HA 功能的 Mariadb 数据库使用的端口号 23306，为保证数据库安全，建议只允许在主 License Server 和备 License Server 之间开放此端口，即，在主 License Server 上配置向备 License Server 开放此端口，在备 License Server 上配置向主 License Server 开放此端口。

- a. 验证 IPtables 是否放行了 HA 功能的 Mariadb 数据库端口号，未配置规则或存在目标值不是 ACCEPT 的规则表示未放行。

```
[root@localhost ~]# iptables -nvL | grep 23306
```

- b. 如未配置规则，请添加以下规则向主或备 License Server 放行端口 23306，主或备 License Server 的 IP 地址以 192.168.109.15 为例；如已存在端口 23306 的放行规则，请将原规则删除并添加以下规则。

```
[root@localhost ~]# iptables -I INPUT -s 192.168.109.15 -p tcp --dport 23306 -j ACCEPT
```

- c. 保存规则。

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

- d. 重启 IPtables 服务，使配置生效。

```
[root@localhost ~]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
```

- e. 验证端口是否放行成功。

```
[root@localhost ~]# iptables -nvL | grep 23306
0 0 ACCEPT tcp -- * * 192.168.109.15 0.0.0.0/0 tcp
dpt: 23306
0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp
dpt: 23306
```

(4) 配置 IPtables 放行 HA 功能 Keepalived 组播地址和 VRRP 协议

如果 License Server 需要配置 HA 功能，则需要配置 IPtables 放行 HA 功能所使用的 Keepalived 报文的组播地址 244.0.0.18 和 VRRP 协议。

- a. 检查 IPtables 是否存在放行 Keepalived 组播地址和 VRRP 协议的规则，如果未配置规则或存在包含组播地址 244.0.0.18 和 VRRP 协议且目标值不是 ACCEPT 的规则，则表示未放行。

```
[root@localhost ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
348 25382 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0
32 2336 ACCEPT all -- !o * 0.0.0.0/0 0.0.0.0/0
...略...
```

- b. 如已存在目标值不是 ACCEPT 的规则，请将原规则删除后再添加。如未配置规则，请添加以下规则；

```
[root@localhost ~]# iptables -I INPUT -d 244.0.0.18/8 -j ACCEPT
[root@localhost ~]# iptables -I INPUT -p vrrp -j ACCEPT
```

c. 保存规则。

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

d. 重启 IPTables 服务，使配置生效。

```
[root@localhost ~]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
```

3. 使用 IP6tables 方式 (IPv6 地址)

(1) 查看 IP6tables 状态

查看 IP6tables 状态，如果显示 **active (exited)**，则表示已开启。

```
[root@localhost ~]# service ip6tables status
Redirecting to /bin/systemctl status ip6tables.service
```

● ip6tables.service - IPv6 firewall with ip6tables

```
Loaded: loaded (/usr/lib/systemd/system/ip6tables.service; disabled; vendor preset: disabled)
```

```
Active: active (exited) since Fri 2020-07-03 06:22:04 EDT; 31min ago
```

...略...

(2) 配置 IP6tables 放行 License Server 的授权服务端口号和 HTTPS 端口号

a. 验证 IP6tables 是否放行了 License Server 的授权服务端口号和 HTTPS 端口号，授权服务端口号以 5555 为例，WEB 服务的 HTTPS 端口号以 28443 为例，监控服务的 HTTPS 端口号以 38443 为例，未配置规则或存在目标值不是 **ACCEPT** 的规则表示未放行。

```
[root@localhost ~]# ip6tables -nvL | grep 5555
    0    0 DROP      tcp  --  *    *    0.0.0.0/0          0.0.0.0/0          tcp
dpt:5555
```

```
[root@localhost ~]# ip6tables -nvL | grep 28443
```

```
[root@localhost ~]# ip6tables -nvL | grep 38443
```

b. 如未配置规则，请添加以下规则放行相应端口号；如已存在目标值不是 **ACCEPT** 的规则，请将原规则删除后再添加。

```
[root@localhost ~]# ip6tables -I INPUT -p tcp --dport 5555 -j ACCEPT
[root@localhost ~]# ip6tables -I INPUT -p tcp --dport 28443 -j ACCEPT
[root@localhost ~]# ip6tables -I INPUT -p tcp --dport 38443 -j ACCEPT
```

c. 保存规则。

```
[root@localhost ~]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[ OK ]
```

d. 重启 IP6tables 服务，使配置生效。

```
[root@localhost ~]# service ip6tables restart
Redirecting to /bin/systemctl restart ip6tables.service
```

e. 验证端口是否放行成功，目标值显示 **ACCEPT** 表示放行成功。

```
[root@localhost ~]# ip6tables -nvL | grep 5555
    0    0 ACCEPT    tcp  *    *    :::/0              :::/0              tcp
dpt:5555
```

```
[root@localhost ~]# ip6tables -nvL | grep 28443
```

```
    0    0 ACCEPT    tcp  *    *    :::/0              :::/0              tcp
dpt:28443
```

```
[root@localhost ~]# ip6tables -nvL | grep 38443
```

```

0 0 ACCEPT tcp * * ::/0 ::/0 tcp
dpt:38443

```

(3) 配置 IP6tables 放行 HA 功能的 Mariadb 数据库端口号

如果 License Server 需要配置 HA 功能，则需要在主 License Server 和备 License Server 上配置 IP6tables 放行 HA 功能的 Mariadb 数据库使用的端口号 23306，为保证数据库安全，建议只允许在主 License Server 和备 License Server 之间开放此端口，即，在主 License Server 上配置向备 License Server 开放此端口，在备 License Server 上配置向主 License Server 开放此端口。

- a. 验证 IP6tables 是否放行了 HA 功能的 Mariadb 数据库端口号，未配置规则或存在目标值不是 ACCEPT 的规则表示未放行。

```
[root@localhost ~]# ip6tables -nvL | grep 23306
```

- b. 如未配置规则，请添加以下规则向主或备 License Server 放行端口 23306，主或备 License Server 的 IP 地址以 2001::142 为例；如已存在端口 23306 的放行规则，请将原规则删除并添加以下规则。

```
[root@localhost ~]# ip6tables -I INPUT -s 2001::142 -p tcp --dport 23306 -j ACCEPT
```

- c. 保存规则。

```
[root@localhost ~]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[ OK ]
```

- d. 重启 IP6tables 服务，使配置生效。

```
[root@localhost ~]# service ip6tables restart
Redirecting to /bin/systemctl restart ip6tables.service
```

- e. 验证端口是否放行成功。

```
[root@localhost ~]# ip6tables -nvL | grep 23306
0 0 ACCEPT tcp * * 2001::142 ::/0 tcp
dpt:23306
0 0 ACCEPT tcp * * 2001::186 ::/0 tcp
dpt:23306
```

(4) 配置 IP6tables 放行 HA 功能 Keepalived 组播地址和 VRRP 协议

如果 License Server 需要配置 HA 功能，则需要配置 IP6tables 放行 HA 功能所使用的 Keepalived 报文的 IPv6 组播地址 ff02::12 和 VRRP 协议。

- a. 检查 IP6tables 是否存在放行 Keepalived 组播地址和 VRRP 协议的规则，如果未配置规则或存在包含组播地址 ff02::12 和 VRRP 协议且目标值不是 ACCEPT 的规则，则表示未放行。

```
[root@localhost ~]# ip6tables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp * * ::/0 ::/0 tcp
dpt:28443
0 0 ACCEPT tcp * * ::/0 ::/0 tcp
dpt:38443
0 0 ACCEPT tcp * * ::/0 ::/0 tcp
dpt:5555
0 0 ACCEPT all * * ::/0 ::/0 state
RELATED, ESTABLISHED
4 272 ACCEPT icmpv6 * * ::/0 ::/0
0 0 ACCEPT all lo * ::/0 ::/0
...略...
```

- b. 如已存在目标值不是 **ACCEPT** 的规则，请将原规则删除后再添加。如未配置规则，请添加以下规则：

```
[root@localhost ~]# ip6tables -I INPUT -d ff02::12/64 -j ACCEPT
[root@localhost ~]# ip6tables -I INPUT -p vrrp -j ACCEPT
```

- c. 保存规则。

```
[root@localhost ~]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[ OK ]
```

- d. 重启 IP6tables 服务，使配置生效。

```
[root@localhost ~]# service ip6tables restart
Redirecting to /bin/systemctl restart ip6tables.service
```

3.3 登录License Server

- (1) 在浏览器中输入 License Server 的 WEB 登录地址（格式为：
`https://lics_ip4_address:port/licsmgr` 或 `https://[lics_ip6_address]:port/licsmgr`，如
`https://172.16.0.227:28443/licsmgr`），回车后会弹出如图 3-9 所示登录界面。
- o `lics_ip4_address/lics_ip6_address` 为 License Server 软件安装所在服务器的 IPv4 或 IPv6 地址，如果已配置 HA 功能，则该地址可以为虚拟 IP 地址或主 License Server 的 IP 地址；
 - o `port` 为端口号，缺省为 28443。

图3-9 License Server WEB 登录界面



- (2) 输入管理员的用户名和密码（缺省用户名为 `admin`，密码为 `admin@123`）后，单击<登录>按钮进入 License Server WEB 首页。

3.4 部署 License Server HA 集群



说明

License Server 支持两个节点的 HA 集群，使用虚拟 IP 地址对外提供服务。主 License Server 负责处理业务，备 License Server 负责备份数据，当主 License Server 出现故障时，备 License Server 可接管业务成为主并对外提供服务。为防止因单点故障导致授权功能中断，推荐您部署 License Server HA 集群。

部署 License Server HA 集群需要分别在两台服务器上安装 License Server，再对安装的两台 License Server 进行必要的 HA 功能配置，操作步骤如下：

- (1) 选定一台 License Server 作为主 License Server
 - 如果两台 License Server 都为全新安装，可选择任意一台作为主 License Server；
 - 如果由原单机方式部署改为 HA 方式部署，请选择原单机 License Server 作为主 License Server；
 - 如果两台 License Server 都使用过，请务必核对每台 License Server 上的数据，选择需要保留数据的 License Server 作为主 License Server。
 - (2) 登录主 License Server。
 - (3) 在 HA 页面单击<创建 HA>按钮，在弹出的对话框中选择 IP 地址类型，输入 HA ID、VIP（虚拟 IP 地址）、主 IP 地址及备 IP 地址。
 - (4) 单击<确定>按钮，等待创建 HA 操作完成。
 - (5) 创建 HA 操作完成后，查看 HA 页面，确认 HA 配置信息正确以及两台 License Server 的状态正常（主 License Server 角色为 primary，在位状态为 active，备 License Server 角色为 standby，在位状态也为 active）。
-



注意

- 安装 License Server 时要求主备 License Server 的各个端口号配置相同，否则会导致 HA 功能无法正常使用。
 - 配置 HA 功能前，请检查主备 License Server 系统时间，确保主备 License Server 系统时间一致。
 - 配置 HA 功能时，请使用主备 License Server 的静态 IP 地址。
 - 配置 HA 功能后，备 License Server 的 licsmgr 服务会更改为 inactive 状态，其它服务仍为 active 状态；请不要修改服务器网卡的配置文件，否则可能会导致 HA 功能运行异常。
 - 当 License Server 运行在 HA 模式时，为了确保成员 License Server 之间信息交互的性能，建议提高交换机与 License Server 连接端口的端口优先级，即将交换机与 License Server 连接端口的优先级，包括 **lp**（本地优先级）、**dot1p**（802.1p 优先级）、**dscp**（DSCP 优先级）都设置为较高的数值。
-

4 卸载 License Server

- (1) 进入 License Server 安装目录

```
[root@localhost ~]# cd /opt/license-server/
```

- (2) 执行卸载脚本，卸载 License Server 软件包。

```
[root@localhost license-server]# ./uninstall.sh
```

- (3) 提示是否进行卸载，继续卸载请输入 y 并回车；如想中断卸载则输入 n 并回车。此处以选择 y 为例。

```
Do you really want to uninstall license-server? (y/n, default:n) :y
```

…略…



说明

卸载 License Server 后激活文件仍将保留，无需再手工上传。

5 升级 License Server

5.1 升级注意事项

- (1) 升级 License Server 时，请勿主动断开客户端与 License Server 的连接，License Server 升级完成后，客户端将自动与 License Server 重新建立连接，升级过程中客户端获取的 License 授权不会中断。如果客户端主动断开连接，将导致 License Server 回收所有授权，从而导致客户端业务受限。
- (2) License Server E1204 版本优化了 HA 功能，增强了 HA 主备 License Server 之间的身份鉴权机制，以 HA 方式部署的 License Server，升级过程中主备 License Server 数据暂时无法正常同步，若此时有客户端申请授权，将导致授权信息在 License Server 集群内数据不一致。为了防止 License Server 集群升级过程中客户端申请授权，导致授权数据的不一致，以 HA 方式部署的 License Server，从 E1204 之前的版本升级到 E1204 及之后的版本时，不支持使用 License Server 的 ISSU 方式升级。为了最大限度的减少 License Server 停止服务的时间，请按照“[5.3 HA 方式部署下非 ISSU 升级](#)”中的步骤升级。

5.2 单机方式部署下升级

- (1) 卸载旧版本 License Server。
- (2) 安装新版本 License Server。

5.3 HA 方式部署下非 ISSU 升级

- (1) 通过虚拟 IP 登录 License Server，查看 HA 页面信息，确认 HA 集群中的两台 License Server 状态都正常（主 License Server 角色为 primary，在位状态为 active，备 License Server 角色为 standby，在位状态也为 active）。
- (2) 在备 License Server 上卸载旧版本。
- (3) 在主 License Server 上卸载旧版本。
- (4) 在主 License Server 上安装新版本。
- (5) 在备 License Server 上安装新版本。
- (6) 重新通过虚拟 IP 登录 License Server，查看 HA 页面信息，确认 HA 集群中的两台 License Server 状态都正常（主 License Server 角色为 primary，在位状态为 active，备 License Server 角色为 standby，在位状态也为 active）。

6 常见问题解答

6.1 安装授权后，如需变更硬件应该如何操作？

License Server 上已安装授权后，如果设备信息文件对应的服务器出现网卡变更（包括禁用网卡、新网卡启用、网卡更换或旧网卡损坏等）或 CPU 更换等硬件信息的变更，可能会导致 License 文件失效。如需变更硬件信息，需要对已安装的正式版授权进行授权迁移操作，具体步骤如下：

1. 变更硬件前导出卸载文件

登录授权所在的 License Server，在[授权管理>激活文件管理]页面中，将所有正式版 License 卸载并导出卸载文件至本地。

2. 硬件变更后，获取设备信息文件

硬件信息变更后，登录 License Server，在[授权管理>激活文件管理]页面中，单击<导出 DID>按钮获取设备信息文件至本地。

3. 设备授权迁移申请，获取新激活文件

请联系技术支持，进行授权迁移，获取新的激活文件。

4. 安装新激活文件

登录硬件变更后的 License Server，在[授权管理>激活文件管理]页面中，单击<安装激活文件>按钮，在弹出的对话框中选择保存在本地的新的激活文件，单击<安装>按钮进行安装。

6.2 安装授权后，如需变更操作系统应该如何操作？

License Server 上已安装授权后，如果需要重新安装操作系统，需要对已安装的正式版授权进行授权迁移操作，否则会导致授权无法继续使用。具体步骤如下：

(1) 变更操作系统前备份当前配置并导出卸载文件。

- a. 登录授权所在的 License Server，在[系统管理>备份与恢复]页面中，单击<保持当前配置>按钮获取当前配置文件。
- b. 在[授权管理>激活文件管理]页面中，将所有正式版 License 卸载并导出卸载文件至本地。
- c. 如果以 HA 方式部署，记录 HA 配置。

(2) 操作系统变更并重新安装 License Server 后，获取设备信息文件。

操作系统变更并重新安装 License Server 后，登录 License Server，在[授权管理>激活文件管理]页面中，单击<导出 DID>按钮获取设备信息文件至本地。

(3) 设备授权迁移申请，获取新激活文件。

请联系技术支持，进行授权迁移，获取新的激活文件。

(4) 安装新激活文件并恢复配置。

- a. 如果以 HA 方式部署，重新配置 HA。
- b. 登录重新安装的 License Server，在[授权管理>激活文件管理]页面中，单击<安装激活文件>按钮，在弹出的对话框中选择保存在本地的新的激活文件，单击<安装>按钮进行安装。

- c. 在[系统管理>备份与恢复]页面中，单击<导入配置文件>按钮，在弹出的对话框中选择备份的配置文件，单击<导入>按钮进行配置恢复。

6.3 变更操作系统的同时需要升级License Server应该如何操作？

先根据“[6.2 安装授权后，如需变更操作系统应该如何操作？](#)”中步骤完成变更操作系统操作，然后再根据“[5 升级 License Server](#)”中的步骤完成 License Server 升级。

6.4 以HA方式部署时其中一台License Server主机故障需要更换应该如何操作？

如果 HA 中有一台 License Server 故障，需要更换为新的 License Server。具体步骤如下：

- (1) 准备新 License Server 主机。
在新主机操作系统上全新安装 License Server。
- (2) 删除故障的 License Server。
 - a. 通过虚拟 IP 登录 License Server。
 - b. 在 HA 页面中，单击<删除备机>按钮删除备机。
- (3) 添加新 License Server。
 - a. 在 HA 页面中，单击<添加备机>按钮，将新 License Server 加入 HA。
 - b. 等待几分钟后，在 HA 页面中单击<刷新>按钮，确认新 License Server 的角色为 standby，在位状态为 active。
- (4) 检查授权状态并处理。
在[授权管理>激活文件管理]页面中，检查激活文件状态，如果激活文件状态正常则结束操作；如果存在激活文件进入逃生状态，则需将进入逃生状态的激活文件卸载迁移到本 License Server，具体操作步骤如下：
 - a. 在 License Server 的[授权管理>激活文件管理]页面中，将逃生状态的正式版激活文件卸载并导出卸载文件至本地。
 - b. 单击<导出 DID>按钮获取设备信息文件。
 - c. 请联系技术支持，进行授权迁移，获取新的激活文件。
 - d. 在 License Server 的[授权管理>激活文件管理]页面中，单击<安装激活文件>按钮，在弹出的对话框中选择保存在本地的新的激活文件，单击<安装>按钮进行安装。