openEuler

openEuler操作系统网络管理和防火墙

课程介绍

- 本课程主要介绍了openEuler网络管理的基础知识和操作。
- openEuler默认通过NetworkManager管理网络， NetworkManager使用nmcli命令行工具配置管理，同时兼容ifcfg配置文件。本章将介绍几种常见网络配置方法和工具使用方法。
- 学完本课程后，您将能够：了解常见的OpenEuler网络配置方法；熟悉nmcli等网络配置工具使用；掌握网络管理的操作方法。

目录

CONTENT

openEuler

通过nmcli配置网络

nmcli介绍

nmcli是NetworkManager的一个命令行工具，它提供了使用命令行配置由NetworkManager管理网络连接的方法。nmcli命令的基本格式为：

```
nmcli [OPTIONS] OBJECT { COMMAND | help }
```

其中，OBJECT选项可以是general、networking、radio、connection或device等。在日常使用中，最常使用的是-t, --terse（用于脚本）、-p, --pretty选项（用于用户）及-h, --help选项。用户可以使用“ nmcli help”获取更多参数及使用信息。

用户可以使用“ nmcli help”获取更多参数及使用信息。

```
$ nmcli help
```

openEuler

通过nmcli配置网络

nmcli常用命令

显示NetworkManager状态：

```
$ nmcli general status
```

显示所有连接状态：

```
$ nmcli connection show
```

只显示当前活动连接，如下所示添加 -a, --active：

```
$ nmcli connection show --active
```

显示由NetworkManager识别到设备及其状态：

```
$ nmcli device status
```

使用nmcli工具启动和停止网络接口，在root权限下执行如下命令：

```
# nmcli connection up id em1
# nmcli device disconnect em1
```

openEuler

通过nmcli配置网络

设备管理

使用如下命令，NetworkManager将连接到对应网络设备，尝试找到合适的连接配置，并激活配置。

```
$nmcli device connect "$IFNAME"
```

说明：

- 如果不存在相应的配置连接，NetworkManager将创建并激活具有默认设置的新配置文件。

使用如下命令，NetworkManager将断开设备连接，并防止设备自动激活。

```
$nmcli device disconnect "$IFNAME"
```

通过nmcli配置网络

设置网络连接

使用如下命令，NetworkManager将连接到对应网络设备，尝试找到合适的连接配置，并激活配置。

```
$nmcli device connect "$IFNAME"
```

列出目前可用的网络连接：

```
$ nmcli con show

NAME    UUID                                  TYPE      DEVICE
enp4s0  5afce939-400e-42fd-91ee-55ff5b65deab  ethernet  enp4s0
enp3s0  c88d7b69-f529-35ca-81ab-aa729ac542fd  ethernet  enp3s0
virbr0  ba552da6-f014-49e3-91fa-ec9c388864fa  bridge    virbr0
```

说明：

- 输出结果中的NAME字段代表连接ID（名称）。

添加一个网络连接会生成相应的配置文件，并与相应的设备关联。检查可用的设备，方法如下：

```
$ nmcli dev status

DEVICE      TYPE      STATE      CONNECTION
enp3s0      ethernet  connected  enp3s0
enp4s0      ethernet  connected  enp4s0
virbr0      bridge    connected  virbr0
lo          loopback  unmanaged  --
virbr0-nic  tun       unmanaged  --
```

通过nmcli配置网络

配置动态IP连接

要使用 DHCP 分配网络时，可以使用动态IP配置添加网络配置文件，命令格式如下：

nmcli connection add type ethernet con-name connection-name ifname interface-name

要例如创建名为net-test的动态连接配置文件，在root权限下使用以下命令：

```
# nmcli connection add type ethernet con-name net-test ifname enp3s0
Connection 'net-test' (a771baa0-5064-4296-ac40-5dc8973967ab)  successfully added.
```

NetworkManager 会将参数 connection.autoconnect 设定为 yes，并将设置保存到 “/etc/sysconfig/network-scripts/ifcfg-net-test”文件中，在该文件中会将 ONBOOT 设置为 yes。在root权限下使用以下命令激活网络连接：

```
# nmcli con up net-test
Connection successfully activated (D-Bus active path:/org/freedesktop/NetworkManager/ActiveConnection/5)
```

检查这些设备及连接的状态，使用以下命令：

```
$ nmcli device status

DEVICE     TYPE     STATE     CONNECTION
enp4s0     ethernet  connected  enp4s0
enp3s0     ethernet  connected  net-test
virbr0     bridge    connected  virbr0
lo         loopback  unmanaged  --
virbr0-nic  tun      unmanaged  --
```

openEuler

通过nmcli配置网络

配置静态IP连接一(设置IP)

添加静态 IPv4 配置的网络连接，可使用以下命令：

nmcli connection add type ethernet con-name connection-name ifname interface-name ip4 address gw4 address

例如创建名为 net-static的静态连接配置文件，在root权限下使用以下命令：

nmcli con add type ethernet con-name net-static ifname enp3s0 ip4 192.168.0.10/24 gw4 192.168.0.254

NetworkManager 会将其内部参数 ipv4.method 设定为 manual，将 connection.autoconnect 设定为yes，并将设置写入 /etc/sysconfig/network-scripts/ifcfg-my-office 文件，其中会将对应 BOOTPROTO 设定为 none，将 ONBOOT 设定为 yes。设定两个 IPv4 DNS 服务器地址，在root权限下使用以下命令：

nmcli con mod net-static ipv4.dns "*.*.*.* *.*.*.*"

openEuler

通过nmcli配置网络

配置静态IP连接二（激活IP）

激活新的网络连接，在root权限下使用以下命令：

```
# nmcli con up net-static ifname enp3s0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
```

检查这些设备及连接的状态，使用以下命令：

```
$ nmcli device status

DEVICE     TYPE      STATE      CONNECTION
enp4s0     ethernet  connected  enp4s0
enp3s0     ethernet  connected  net-static
virbr0     bridge    connected  virbr0
lo         loopback  unmanaged  --
virbr0-nic tun       unmanaged  --
```

查看配置的连接详情，使用以下命令（使用 -p, --pretty 选项在输出结果中添加标题和分段）：

```
$ nmcli -p con show net-static
===============================================================================
Connection profile details (net-static )
===============================================================================
connection.id:                          net-static
connection.uuid:                        b9f18801-6084-4aee-af28-c8f0598ff5e1
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              enp3s0
connection.autoconnect:                 yes
.......
```

通过nmcli配置网络

配置静态路由

使用nmcli命令为网络连接配置静态路由，使用命令如下：

```
$ nmcli connection modify enp3s0 +ipv4.routes "192.168.122.0/24 10.10.10.1"
```

使用编辑器配置静态路由，使用如下命令：

```
$ nmcli con edit type ethernet con-name enp3s0
===| nmcli interactive connection editor |===
Adding a new '802-3-ethernet' connection
Type 'help' or '?' for available commands.
Type 'describe [<setting>.<prop>]' for detailed property description.
You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, ipv4, ipv6, dcb
nmcli> set ipv4.routes 192.168.122.0/24 10.10.10.1
nmcli> save persistent
Saving the connection with 'autoconnect=yes'. That might result in an immediate activation of the connection.
Do you still want to save? [yes] yes
Connection 'enp3s0' (1464ddb4-102a-4e79-874a-0a42e15cc3c0) successfully saved.
nmcli> quit
```

随堂测

- 1. nmcli配置网络通常包括以下几个步骤（多选题）

  A. 连接网络设备

  B. 设置IP

  C. 激活IP

  D. 重启网络

- 2. nmcli配置网络IP地址后需要激活才能生效。（判断题）

openEuler

目录

CONTENT

openEuler

通过ifcfg文件配置网络

配置静态网络

以enp4s0网络接口进行静态网络设置为例，通过在root权限下修改ifcfg文件实现，在/etc/sysconfig/network-scripts/目录中生成名为ifcfg-enp4s0的文件中，修改参数配置，示例如下：

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
DEVICE=enp4s0
BOOTPROTO=none
ONBOOT=yes
IPADDR=192.168.0.10
PREFIX=24
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp4s0static
UUID=08c3a30e-c5e2-4d7b-831f-26c3cdc29293
```

说明：

- 通过ifcfg文件配置的网络配置不会立即生效，需要在root权限下执行**systemctl reload NetworkManager**命令以重启网络服务后才生效。
- 配置文件中包含了完整配置参数，也可以仅配置上面黑体部分最小配置。
- 网卡配置文件只支持以ifcfg-ifname方式命名，多个网卡不建议配置同网段IP。
- PREFIX也可以通过NETMASK来设置。

通过ifcfg文件配置网络

Ifcfg配置文件参数

Ifcfg配置文件主要参数说明如下，参数值不区分大小写，参数值可以选择使用引号：

配置参数	参数说明
TYPE	配置文件接口类型
DEVICE	设备名称
BOOTPROTO	系统启动地址协议
ONBOOT	系统启动时是否激活接口
IPADDR	IP地址
PREFIX	网络地址的位数
GATEWAY	网关地址
BROADCAST	广播地址

通过ifcfg文件配置网络

配置动态网络

要通过ifcfg文件为em1接口配置动态网络，请按照如下操作在/etc/sysconfig/network-scripts/目录中生成名为 ifcfg-em1 的文件，示例如下：

```
DEVICE=em1
BOOTPROTO=dhcp
ONBOOT=yes
```

要配置忽略由DHCP服务器发送的路由，防止网络服务使用从DHCP服务器接收的DNS服务器更新/etc/resolv.conf。请在ifcfg文件中新增一行内容，如下所示：

```
PEERDNS=no
```

要配置一个接口使用具体DNS服务器，请将参数PEERDNS=no，并在ifcfg文件中添加以下行：

```
DNS1=ip-address
DNS2=ip-address
```

说明：

- 其中ip-address是DNS服务器的地址。这样就会让网络服务使用指定的DNS服务器更新/etc/resolv.conf。

openEuler

通过ifcfg文件配置网络

配置默认网关

在确定默认网关时，首先解析 /etc/sysconfig/network 文件，然后解析 ifcfg 文件 ，将最后读取的 GATEWAY 的取值作为路由表中的默认路由。

在动态网络环境中，使用 NetworkManager 管理主机时，建议设置为由 DHCP 来分配。

通过/etc/sysconfig/network配置默认网关，示例如下：

```
GATEWAY=192.168.0.1
```

通过Ifcfg文件中配置默认网关，如为em1接口配置默认网关，示例如下：

```
GATEWAY=192.168.0.1
```

说明：

- /etc/sysconfig/network提供全局默认路由配置，但是优先级较低，建议通过ifcfg文件配置。
- 默认路由仅能生效一个，如果配置多个行数较小的生效。

openEuler

随堂测

- 1.通过ifcfg文件配置的网络时，以下参数必须配置（多选题）

  A. TYPE
  B. PREFIX/NETMASK
  C. IPADDR
  D. DEVICE

- 2. ifcfg配置文件保存在以下哪个目录。（单选题）

  A. /etc
  B. /etc/network
  C. /etc/sysconfig/network
  D. /etc/sysconfig/network-scripts/

openEuler

目录

CONTENT

openEuler

通过IP命令配置网络

配置IP地址

使用ip命令为接口配置地址，命令格式如下，其中 interface-name 为网卡名称。

ip addr [add | del] address dev interface-name

在root权限下，配置设置IP地址，使用示例如下：

ip address add 192.168.0.10/24 dev enp3s0

查看配置结果，在root权限使用如下命令：

```
# ip addr show dev enp3s0
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:aa:ad:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.248/16 brd 192.168.255.255 scope global dynamic noprefixroute enp3s0
       valid_lft 9547sec preferred_lft 9547sec
    inet 192.168.0.10/24 scope global enp3s0
       valid_lft forever preferred_lft forever
    inet6 fe80::32e8:cc22:9db2:f4d4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

注意：

- 使用ip命令配置的网络配置可以立即生效但系统重启后配置会丢失。

openEuler

通过IP命令配置网络

配置多个IP地址

ip 命令支持为同一接口分配多个地址，可在root权限下重复多次使用 ip 命令实现分配多个地址。使用示例如下：

```
# ip address add 192.168.2.223/24 dev enp4s0
# ip address add 192.168.4.223/24 dev enp4s0
```

查看配置结果，在root权限使用如下命令：

```
# ip addr

3: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:aa:da:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.203.12/16 brd 192.168.255.255 scope global dynamic noprefixroute enp4s0
       valid_lft 8389sec preferred_lft 8389sec
    inet 192.168.2.223/24 scope global enp4s0
       valid_lft forever preferred_lft forever
    inet 192.168.4.223/24 scope global enp4s0
       valid_lft forever preferred_lft forever
    inet6 fe80::1eef:5e24:4b67:f07f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

openEuler

通过IP命令配置网络

配置静态路由

如果需要静态路由，可使用 ip route add 命令在路由表中添加，使用 ip route del 命令删除。最常使用的 ip route 命令格式如下：

ip route [add | del | change | append | replace] destination-address

在root权限下使用 ip route 命令显示当前的 IP 路由表。示例如下：

ip route

default via 192.168.0.1 dev enp3s0 proto dhcp metric 100
default via 192.168.0.1 dev enp4s0 proto dhcp metric 101
192.168.0.0/16 dev enp3s0 proto kernel scope link src 192.168.202.248 metric 100
192.168.0.0/16 dev enp4s0 proto kernel scope link src 192.168.203.12 metric 101
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown

在主机地址中添加一个静态路由，在 root 权限下，使用以下命令格式：

ip route add 192.168.2.1 via 10.0.0.1 [dev interface-name]

其中 192.168.2.1 是用点分隔的十进制符号中的 IP 地址，10.0.0.1 是下一个跃点，interface-name 是进入下一个跃点的退出接口。

要在网络中添加一个静态路由，即代表 IP 地址范围的 IP 地址，请在root权限下运行以下命令格式：

ip route add 192.168.2.0/24 via 10.0.0.1 [dev interface-name]

其中 192.168.2.1 是目标网络的 IP 地址，10.0.0.1 是网络前缀，interface-name 为网卡名称。

openEuler

随堂测

- 1.以下关于IP命令功能的说法，错误的是（单选题）

  A. 配置IP地址

  B. 配置路由

  C. 配置主机名

  D. 查看网络

- 2. 使用IP命令配置网络，重启操作系统后依然生效。（判断题）

目录

CONTENT

openEuler

配置主机名

主机名简介

HOSTNAME 有三种类型：

static、transient和pretty。

- static：静态主机名，可由用户自行设置，并保存在/etc/hostname 文件中。
- transient：动态主机名，由内核维护，初始是 static 主机名，默认值为“localhost”。可由DHCP或mDNS在运行时更改。
- pretty：灵活主机名，允许使用自由形式（包括特殊/空白字符）进行设置。静态/动态主机名遵从域名的通用限制。

说明：

- static和transient主机名只能包含a-z、A-Z、0-9、“-”、“_”和“.”，不能在开头或结尾处使用句点，不允许使用两个相连的句点，大小限制为 64 个字符。

openEuler

配置主机名

使用hostnamectl配置主机名

查看当前的主机名，使用如下命令：

```
$ hostnamectl status
```

说明：

- 如果命令未指定任何选项，则默认使用status选项。

在root权限下，设定系统中的所有主机名，使用如下命令：

```
# hostnamectl set-hostname name
```

在root权限下，通过不同的参数来设定特定主机名，使用如下命令：

```
# hostnamectl set-hostname name [option...]
```

其中option可以是--pretty、--static、--transient中的一个或多个选项。

如果--static或--transient与--pretty选项一同使用时，则会将static和transient主机名简化为pretty主机名格式，使用“-”替换空格，并删除特殊字符。

当设定pretty主机名时，如果主机名中包含空格或单引号，需要使用引号。命令示例如下：

```
# hostnamectl set-hostname "Stephen's notebook" --pretty
```

配置主机名

使用hostnamectl管理主机名

要清除特定主机名，并将其还原为默认形式，在root权限下，使用如下命令：

```
# hostnamectl set-hostname "" [option...]
```

说明：

- 其中 "" 是空白字符串，option是--pretty、--static和--transient中的一个或多个选项。

远程更改主机名，在远程系统中运行hostnamectl命令时，要使用-H，--host 选项，在root权限下使用如下命令：

```
# hostnamectl set-hostname -H [username]@hostname new_hostname
```

说明：

- 其中hostname是要配置的远程主机，username为自选项，new_hostname为新主机名。hostnamectl会通过SSH连接到远程系统。

openEuler

配置主机名

使用nmcli配置主机名

查询static主机名，使用如下命令：

```
$ nmcli general hostname
```

在root权限下，将static主机名设定为host-server，使用如下命令：

```
# nmcli general hostname host-server
```

要让系统hostnamectl感知到static主机名的更改，在root权限下，重启hostnamed服务，使用如下命令：

```
# systemctl restart systemd-hostnamed
```

随堂测

- 1. HOSTNAME包括以下几种类型
- （多选题）

A. static
B. transient
C. dynamic
D. pretty

- 2. hostnamectl修改主机名后直接生效。（判断题）

openEuler

目录

CONTENT

openEuler

防火墙基本概念

Openeuler的防火墙解决方案， 作为内核提供的iptables数据包筛选系统的前端，防火墙通过区域划分管理。

区域：防火墙守护进程使用称为“区域”的实体管理规则组。区域基本上是一组规则，根据计算机连接到的网络的信任级别，规定应允许哪些网络流量。网络接口被分配一个区域，以指示防火墙应允许的行为。

从最不信任到最受信任的顺序，防火墙中的预定义区域是：

- **drop（丢弃）**：最低信任级别。所有传入连接在没有回复的情况下丢弃，并且只能进行传出连接。
- **block（限制）**：与上述类似，但传入请求不是简单地丢弃连接，而是使用 或 消息被拒绝。
- **public（公共）**：表示公共、不受信任的网络。您不信任其他计算机，但可能会根据情况允许选定的传入连接。
- **external（外部）**：使用防火墙作为网关时的外部网络。它配置为 NAT 伪装，以便你的内部网络保持私有但可访问。
- **internal（内部）**：外部区域的另一侧，用于网关的内部部分。计算机是相当值得信赖的，一些额外的服务是可用的。
- **dmz:** 用于位于 DMZ 中的计算机（无法访问网络其余部分的隔离计算机）。仅允许某些传入连接。
- **work（工作）**：用于工作机器。信任网络中的大多数计算机。可能允许使用更多服务。
- **home（家）**：家庭环境。它通常意味着你信任大多数其他计算机，并且将接受更多服务。
- **trusted（受信任）**：信任网络中的所有计算机。最开放的可用选项，应谨慎使用。

防火墙管理

管理防火墙

防火墙默认安装后如果没有启动，需要手动激激活开机启动防火墙服务：

```
# systemctl enable firewalld
Created symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service → /usr/lib/systemd/system/firewalld.service.
Created symlink /etc/systemd/system/multi-user.target.wants/firewalld.service → /usr/lib/systemd/system/firewalld.service.
```

启动和查看防火墙状态

```
# systemctl start firewalld
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-06-14 16:10:53 CST; 3s ago
……
```

也可以通过防火墙命令来查看是否运行：

```
# firewall-cmd --state
running
```

openEuler

防火墙区域管理

防火墙区域管理

防火墙默认区域为public，查看默认区域方法如下：

```
# firewall-cmd --get-default-zone
public
```

查看每个区域绑定的接口：

```
# firewall-cmd --get-active-zones
public
  interfaces: ens3
```

修改接口绑定的区域，例如将ens3从public修改为external：

```
# firewall-cmd --zone=external --change-interface=ens3
Success
# firewall-cmd --get-active-zones
external
  interfaces: ens3
```

如果只接入一个防火墙区域，可以直接修改默认区域：

```
# firewall-cmd --set-default-zone=external
Success
# firewall-cmd --get-default-zone
external
```

openEuler

随堂测

- 1.系统中防火墙的默认区域是
- （多选题）

A. drop
B. Public
C. external
D. internal

- 2.防火墙区域中public比external更受信任。（判断题）

openEuler

Thank you

openEuler