openEuler

SSH管理及安全

课程介绍

- 本课程主要介绍了SSH服务的搭建、安全配置和管理：

- SSH为Secure Shell的缩写，由IETF的网络小组（Network Working Group）所制定；SSH为建立在应用层基础上的安全协议。SSH是较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用SSH协议可以有效防止远程管理过程中的信息泄露问题。SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。SSH在正确使用时可弥补网络中的漏洞。SSH客户端适用于多种平台。几乎所有UNIX平台—包括HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix，以及其他平台，都可运行SSH。（参考自：https://baike.baidu.com/item/ssh/10407?fr=aladdin）

- 学完本课程后，您将能够： 基于openEuler系统的SSH服务搭建及安全配置；使用SSH客户端连接SSH服务端；SSH运维与故障排除

目录

CONTENT

openEuler

SSH服务搭建（1）

安装SSH服务总共需要至少三个套件，包括：openssh、openssh-server、openssh-clients

- openssh：这个套件提供交互算法使用的素数模数（/etc/ssh/moduli），生成主机认证公私密钥的工具（/usr/bin/ssh-keygen）
- openssh-server：这个套件主要包含SSH服务端的主程序（/usr/sbin/sshd）、daemon配置（/usr/lib/systemd/system/sshd.service）、SSH服务端配置（/etc/ssh/sshd_config）
- openssh-clients：这个套件则提供了当openEuler作为SSH客户端时，所需要的工具命令（/usr/bin/scp、/usr/bin/sftp、/usr/bin/ssh）、SSH客户端配置（/etc/ssh/ssh_config）

openEuler默认安装包含这几个套件。如果环境中没有这些套件，可参考前面教程的DNF管理套件进行安装，此处不再赘述。

SSH服务搭建（2）

可以使用rpm命令，查看环境中已安装的SSH相关套件，以及这些套件包含的文件清单。

```
[root@localhost ~]# rpm -qa | grep openssh
openssh-8.8p1-2.oe2203.x86_64
openssh-server-8.8p1-2.oe2203.x86_64
openssh-clients-8.8p1-2.oe2203.x86_64
[root@localhost ~]#
```

```
[root@localhost ~]# rpm -ql openssh-server
/etc/ima/digest_lists.tlv/0-metadata_list-compact_tlv-openssh-server-8.8p1-2.oe2203.x86_64
/etc/ima/digest_lists/0-metadata_list-compact-openssh-server-8.8p1-2.oe2203.x86_64
/etc/pam.d/sshd
/etc/ssh/sshd_config
/etc/sysconfig/sshd
/usr/lib/systemd/system/sshd-keygen.target
/usr/lib/systemd/system/sshd-keygen@.service
/usr/lib/systemd/system/sshd.service
/usr/lib/systemd/system/sshd.socket
/usr/lib/systemd/system/sshd@.service
/usr/lib/tmpfiles.d/openssh.conf
/usr/libexec/openssh/sftp-server
/usr/libexec/openssh/sshd-keygen
/usr/sbin/sshd
/var/empty/sshd
```

```
[root@localhost ~]# rpm -ql openssh
/etc/ima/digest_lists.tlv/0-metadata_list-compact_tlv-openssh-8.8p1-2.oe2203.x86_64
/etc/ima/digest_lists/0-metadata_list-compact-openssh-8.8p1-2.oe2203.x86_64
/etc/ssh
/etc/ssh/moduli
/usr/bin/ssh-keygen
/usr/libexec/openssh
/usr/libexec/openssh/ssh-keysign
/usr/share/doc/openssh
/usr/share/doc/openssh/CREDITS
/usr/share/doc/openssh/README.platform
/usr/share/licenses/openssh
/usr/share/licenses/openssh/LICENCE
[root@localhost ~]#
```

```
[root@localhost ~]# rpm -ql openssh-clients
/etc/ima/digest_lists.tlv/0-metadata_list-compact_tlv-openssh-clients-8.8p1-2.oe2203.x86_64
/etc/ima/digest_lists/0-metadata_list-compact-openssh-clients-8.8p1-2.oe2203.x86_64
/etc/ssh/ssh_config
/etc/ssh/ssh_config.d/05-redhat.conf
/usr/bin/scp
/usr/bin/sftp
/usr/bin/ssh
/usr/bin/ssh-add
/usr/bin/ssh-agent
/usr/bin/ssh-copy-id
/usr/bin/ssh-keyscan
/usr/lib/systemd/user/ssh-agent.service
/usr/libexec/openssh/ssh-pkcs11-helper
/usr/libexec/openssh/ssh-sk-helper
[root@localhost ~]#
```

SSH服务端安全配置（1）

SSH配置文件目录存放于/etc/ssh，SSH服务端主要的配置文件有sshd_config。部分安全配置参数说明如下：

注：‘默认值’表示不配置该参数时，程序按该配置值处理

- Port：监听端口，默认为22。SSH服务监听端口业界标准是22，但容易被攻击者端口扫描。用户可以根据合理的端口规划，配置为其他值。
- ListenAddress：监听地址，默认为全网监听。全网监听扩大了攻击面，应根据业务需要配置固定的监听地址。建议仅配置管理面的IP地址。
- PermitRootLogin：允许root登录，默认为prohibit-password。建议配置为no，即禁止root远程登录。如果未禁止root账号远程登录，那么攻击者获取到root口令之后就可以从网络上远程登录服务器进行攻击行为，否则只能从服务器机房内部近端登录，可大幅减小攻击面。
- PermitEmptyPasswords：允许空密码，默认为no。应禁止配置该字段为yes，避免无密码用户登录。
- UsePAM：使用PAM策略，默认为no。PAM策略对用户认证和管理，有登录次数限制，超次锁定用户，到时解锁用户功能。sshd_config的MaxAuthTries仅有登录次数限制。该字段应配置为yes，使用PAM策略，可以起到防暴力破解。

SSH服务端安全配置（2）

- SyslogFacility：系统日志设施，默认为AUTH。该配置表示，可通过rsyslog服务的设施分类规则记录日志。在/etc/rsyslog.conf已有规则authpriv.* /var/log/secure用于记录安全日志。建议对照该规则配置SyslogFacility为AUTHPRIV，这样可以记录SSH服务日志，比如用户的认证鉴权日志，等入登出日志等，为安全事件提供日志支撑。
- IgnoreRhosts：忽略Rhosts，默认为yes。在Rlogin协议中，Rhosts配置表示授权远程访问，由于Rlogin协议已不安全，所以应禁止使用Rhosts配置。建议配置为yes。

当SSH服务的配置文件/etc/ssh/sshd_config被修改，需要重启sshd服务才能使修改的参数生效。相关命令，在SSH服务管理中进行介绍。

SSH服务端安全配置（3）

可以使用命令sshd -T，查看当前/etc/ssh/sshd_config中的配置是否存在错误：

```
[root@localhost ~]# sshd -T
/etc/ssh/sshd_config line 142: Deprecated option RSAAuthentication
/etc/ssh/sshd_config line 144: Deprecated option RhostsRSAAuthentication
reprocess config line 142: Deprecated option RSAAuthentication
reprocess config line 144: Deprecated option RhostsRSAAuthentication
port 22
addressfamily any
listenaddress [::]:22
listenaddress 0.0.0.0:22
usepam yes
logingracetime 120
x11displayoffset 10
x11maxdisplays 1000
maxauthtries 6
maxsessions 10
clientaliveinterval 0
clientalivecountmax 0
streamlocalbindmask 0177
permitrootlogin yes
ignorerhosts yes
ignoreuserknownhosts no
hostbasedauthentication no
hostbasedusesnamefrompacketonly no
pubkeyauthentication yes
kerberosauthentication no
kerberosorlocalpasswd yes
kerberosticketcleanup yes
kerberosuniqueccache no
kerberosusekuserok yes
gssapienablek5users no
gssapiauthentication yes
gssapicleanupcredentials no
gssapikeyexchange no
gssapistrictacceptorcheck yes
gssapistorecredentialsonrekey no
gssapikexalgorithms gss-group14-sha256-,gss-group16-sha512-,gss-curve25519-sha256-
```

SSH服务管理（1）

应将SSH服务设置为开机启动，并启动SSH服务。修改SSH服务配置后，需要重启SSH服务生效。

SSH服务常用管理命令如下：

- 设置SSH服务为开机启动：

  systemctl enable sshd.service

- 设置SSH服务禁止开机启动：

  systemctl disable sshd.service

- 查看SSH服务是否开机启动：

  systemctl is-enabled sshd.service

下图显示enabled，表示已设置SSH服务为开机启动

```
[root@localhost ~]# systemctl is-enabled sshd.service
enabled
[root@localhost ~]#
```

SSH服务管理（2）

- 启动SSH服务

  systemctl start sshd.service

- 停止SSH服务

  systemctl stop sshd.service

- 查看SSH服务是否在运行：

  systemctl is-active sshd.service

下图显示active，表示SSH服务正在运行

```
[root@localhost ~]# systemctl is-active sshd.service
active
[root@localhost ~]#
```

SSH服务管理（3）

- 查看SSH服务运行信息：

  systemctl status sshd.service

下图展示了sshd服务的运行信息，包括：daemon配置、状态、运行时长、主进程PID、子进程PID，等等。

```
[root@localhost ~]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-06-13 14:27:02 CST; 3h 25min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 871 (sshd)
      Tasks: 12 (limit: 21604)
     Memory: 43.4M
     CGroup: /system.slice/sshd.service
             ├─ 871 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
             ├─6090 "sshd: root [priv]" "" "" ""
             ├─6092 "sshd: root@pts/1" "" "" "" ""
             ├─6093 -bash
             ├─6887 "sshd: root [priv]" "" "" ""
             ├─6895 "sshd: root@pts/2" "" "" "" ""
             ├─6896 -bash
             ├─7681 "sshd: root [priv]" "" "" ""
             ├─7683 "sshd: root@pts/3" "" "" "" ""
             ├─7684 -bash
             ├─9109 systemctl status sshd.service
             └─9110 less
```

SSH客户端配置

SSH客户端配置参数生效顺序为：命令参数 > 配置文件参数 > 默认值参数。以端口为例：先检查是否有命令参数配置了端口，有则使用该参数；否则，检查配置文件是否有配置了端口，有则使用该参数；否则，使用默认值22。配置文件选用顺序为：命令参数-F指定的配置文件 > ~/.ssh/config > /etc/ssh/ssh_config。注意：“检查配置文件是否配置了参数” 只会在选定的配置文件中检查，而不是每个文件都检查。

配置文件中部分配置参数说明如下：

注：’ 默认值’ 表示不配置该参数时，程序按该配置值处理

- Port：连接的目标端口，默认为22。在连接SSH服务端时，如果SSH客户端不指定端口则使用此配置端口。
- StrictHostKeyChecking：强校验主机密钥，默认为ask。 对于~/.ssh/known_hosts中无记录的服务端，该参数，配置为no时，将无任何提示就将服务端的主机认证密钥添加到~/.ssh/known_hosts中；配置为yes时，将拒绝连接；配置“ask”时，将提示用户是否接受该主机认证密钥，在得到用户允许后，才将服务端的主机认证密钥添加到~/.ssh/known_hosts中。建议配置为ask。

SSH客户端工具--/usr/bin/ssh（1）

/usr/bin/ssh是SSH远程登录客户端。

语法：

ssh [option] destination [command [argument ...]]

注：destination中不指定user时，表示使用运行客户端的用户来作为连接用户。

部分参数说明如下：

- -p（小写）：指定连接的目标端口。该端口号为SSH服务端监听的端口号。如果SSH客户端配置端口，不是SSH服务端监听端口时，ssh工具需要使用-p指定端口号，才能正确连接到SSH服务端。该端口号将覆盖配置文件指定的端口。
- -F：指定配置文件。
- -E：指定记录日志的文件。将调试日志附加到log_file中，而不是标准错误。不影响标准输出。建议在问题定位调试时使用。
- -v：详细模式。这可以使程序打印有关其进度的调试消息。这有助于调试连接、身份验证和配置问题。多个-v选项增加了详细程度，最多可以配置三个v。

SSH客户端工具--/usr/bin/ssh（2）

下图为通过SSH客户端工具ssh首次远程登录IP 8.4.185.106主机：

```
[root@localhost ~]# ssh -p 22 root@8.4.185.106
The authenticity of host '8.4.185.106 (8.4.185.106)' can't be established.
ED25519 key fingerprint is SHA256:[redacted]
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '8.4.185.106' (ED25519) to the list of known hosts.
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
Authorized users only. All activity may be monitored and reported.
Last login: Sat Jun 11 14:27:12 2022 from [redacted]
[root@host-8-4-185-106 ~]#
```

SSH客户端工具--/usr/bin/ssh（3）

下图为通过SSH客户端工具ssh，在远程主机（IP 8.4.185.106）上执行命令：

```
[root@localhost ~]# ssh -p 22 root@8.4.185.106 "echo \"Hello.\"; hostname; echo \"Bye.\""
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
Hello.
host-8-4-185-106
Bye.
[root@localhost ~]#
```

SSH客户端工具--/usr/bin/scp（4）

/usr/bin/scp是远程文件拷贝程序，用于非交互模式文件拷贝。

语法：

scp [option] [[user@]host1:]file1 [[user@]host2:]file2

注：不指定user时，表示使用运行客户端的用户来作为连接用户。

部分参数说明如下：

- -P（大写）：指定连接的目标端口。该端口号为SSH服务端监听的端口号。如果SSH客户端配置端口，不是SSH服务端监听端口时，scp工具需要使用-P指定端口号，才能正确连接到SSH服务端。该端口号将覆盖配置文件指定的端口。
- -F：指定配置文件。
- -v：详细模式。这可以使程序打印有关其进度的调试消息。这有助于调试连接、身份验证和配置问题。多个-v选项增加了详细程度，最多可以配置三个v。

SSH客户端工具--/usr/bin/scp（5）

下图为通过SSH客户端工具scp将/root/hello.txt文件，拷贝到远程主机（IP 8.4.185.106），并重命名为/root/world.txt。然后通过工具ssh远程查看了文件world.txt的输出：

```
[root@localhost ~]# cat /root/hello.txt
Hello
[root@localhost ~]# scp -P 22 /root/hello.txt root@8.4.185.106:/root/world.txt
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
hello.txt                                     100%    6    11.0KB/s   00:00
[root@localhost ~]# ssh -p 22 root@8.4.185.106 "cat /root/world.txt"
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
Hello
[root@localhost ~]#
```

注意：工具scp使用-P（大写）指定端口，工具ssh使用-p（小写）指定端口

SSH客户端工具--/usr/bin/sftp（6）

/usr/bin/sftp是远程安全文件传输程序，常用于交互模式文件传输。

语法：

sftp [option] destination

注：destination中不指定user时，表示使用运行客户端的用户来作为连接用户。

部分参数说明如下：

- -P（大写）：指定连接的目标端口。该端口号为SSH服务端监听的端口号。如果SSH客户端配置端口，不是SSH服务端监听端口时，scp工具需要使用-P指定端口号，才能正确连接到SSH服务端。该端口号将覆盖配置文件指定的端口。
- -F：指定配置文件。
- -v：详细模式。这可以使程序打印有关其进度的调试消息。这有助于调试连接、身份验证和配置问题。多个-v选项增加了详细程度，最多可以配置三个v。

SSH客户端工具--/usr/bin/sftp（7）

下图实现了通过SSH客户端工具sftp将/root/hello.txt、/root/world.txt文件，拷贝到远程主机（IP 8.4.185.106），以及从远程主机上下载/root/helloworld.txt文件到本地：

```
[root@localhost ~]# cat hello.txt
Hello
[root@localhost ~]# cat world.txt
World
[root@localhost ~]# ls helloworld.txt
ls: cannot access 'helloworld.txt': No such file or directory
[root@localhost ~]# sftp -P 22 root@8.4.185.106
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
Connected to 8.4.185.106.
sftp> pwd
Remote working directory: /root
sftp> put /root/hello.txt /root/hello.txt
Uploading /root/hello.txt to /root/hello.txt
hello.txt                                     100%    6    17.9KB/s   00:00
sftp> put /root/world.txt /root/helloworld.txt
Uploading /root/world.txt to /root/helloworld.txt
world.txt                                     100%    6    25.2KB/s   00:00
sftp> get /root/helloworld.txt /root/helloworld.txt
Fetching /root/helloworld.txt to /root/helloworld.txt
helloworld.txt                                100%    6    12.0KB/s   00:00
sftp> bye
[root@localhost ~]# cat helloworld.txt
World
[root@localhost ~]#
```

SSH故障排除（1）

在SSH服务使用过程中，如客户端遇到连接失败的情况，常见的错误包括：

- Connection refused：拒绝连接。常见情况和解决办法：
  - a、SSH服务端服务异常。检查SSH服务端服务状态，比如服务未启动，则将服务启动。
  - b、SSH客户端连接端口，与SSH服务端监听端口不同。执行SSH客户端时，指定目标端口号。
  - c、SSH客户端发起的网络平面，与SSH服务端监听地址的网络平面不同。根据SSH客户端的网络平面，增加SSH服务的监听地址。

```
[root@localhost ~]# ssh -p 22 root@8.4.189.85
ssh: connect to host 8.4.189.85 port 22: Connection refused
[root@localhost ~]# ssh -p 222 root@8.4.185.106
ssh: connect to host 8.4.185.106 port 222: Connection refused
[root@localhost ~]#
```

SSH故障排除（2）

- Too many authentication failures：认证失败次数过多。常见情况和解决办法：
  - a、输入密码错误次数超过SSH服务端限定次数。请检查密码是否正确，用户是否正确。使用正确用户、密码登录。
  - b、SSH服务端侧，该用户被限制登录。比如用户的SHELL为/sbin/nologin或/bin/false或用户被锁定。SHELL为禁止登录的用户，需要修改SHELL属性（根据业务设计确定）；锁定用户，需要解锁后才能登录。
  - c、SSH服务端侧，sshd_config的黑白名单限制了用户。在SSH服务端侧将用户配置到白名单范围内，且不被黑名单限制。

```
[root@localhost ~]# ssh -p 22 root@8.4.185.106
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
(root@8.4.185.106) Password:
(root@8.4.185.106) Password:
Received disconnect from 8.4.185.106 port 22:2: Too many authentication failures
Disconnected from 8.4.185.106 port 22
[root@localhost ~]# ssh -p 22 test@8.4.185.106
Authorized users only. All activity may be monitored and reported.
(test@8.4.185.106) Password:
(test@8.4.185.106) Password:
(test@8.4.185.106) Password:
Received disconnect from 8.4.185.106 port 22:2: Too many authentication failures
Disconnected from 8.4.185.106 port 22
[root@localhost ~]#
```

SSH故障排除（3）

- REMOTE HOST IDENTIFICATION HAS CHANGED：SSH服务端主机认证密钥发生变更。SSH客户端侧根据提示，将~/.ssh/known_hosts中相应的主机认证密钥记录删除即可。

```
[root@localhost ~]# ssh -p 22 root@8.4.185.106
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:[illegible].
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ED25519 key in /root/.ssh/known_hosts:2
Host key for 8.4.185.106 has changed and you have requested strict checking.
Host key verification failed.
[root@localhost ~]# sed -i "2 d" /root/.ssh/known_hosts
[root@localhost ~]# ssh -p 22 root@8.4.185.106
The authenticity of host '8.4.185.106 (8.4.185.106)' can't be established.
ED25519 key fingerprint is SHA256:[illegible].
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '8.4.185.106' (ED25519) to the list of known hosts.
Authorized users only. All activity may be monitored and reported.
(root@8.4.185.106) Password:
Authorized users only. All activity may be monitored and reported.
Last login: Mon Jun 13 19:59:31 2022 from 8.4.189.213
[root@host-8-4-185-106 ~]#
```

随堂测试

1、（单选题）下面哪个套件不是搭建SSH服务必须的：（选B）

A、openssh; B、openssh-askpass; C、openssh-server；D、openssh-clients

2、（单选题）下面哪个工具不是SSH客户端工具：（选C）

A、ssh；B、scp；C、rsync；D、sftp

3、（单选题）下面哪个不是SSH客户端配置：（选A）

A、/etc/ssh/sshd_config

B、/etc/ssh/ssh_config;

C、~/.ssh/config

D、/etc/ssh/ssh_config.d/05-redhat.conf

Thank you

openEuler