

telnet/xinetd原理与配置汇总

笔记本: Linux系统服务

创建时间: 2018-08-17 23:32

更新时间: 2021-02-02 13:47

作者: hualf

telnet/xinetd原理与配置汇总

telnet概述:

- Linux远程登录的3种主要方式:

1. 基于命令行: ssh、telnet
2. 基于图形化: vnc

- telnet服务基于C/S架构（客户端/服务端，telnet/telnet-server），需分别安装

客户端与服务端软件。

- telnet的应用场景:

1. 在公网（WAN）中使用telnet是非常不好的想法，它会以明文的格式传输登入数据。
2. 强烈建议只在局域网（LAN）内部使用。
3. 确保不要用root用户登录telnet，因为telnet客户端连接服务器时，密码是以明文
- 传输的，因此默认root不允许直接登录服务器。
4. 可以在公网中使用ssh作为替代方法。

- 不同Linux发行版中的telnet服务原理差异:

1. 只有当用户远程登陆后才生成telnet进程，即每一个telnet客户端的连接都需要生成一个telnet服务进程去处理。
2. telnet服务端只允许root用户同时只能进行一次登录，普通用户可同时多次登录。
3. RHEL 7.x: systemd -> in.telnetd
telnet服务由systemd守护进程控制，不受xinetd超级守护进程（super damon）控制，可单独启动服务。
telnet服务启动后没有守护进程，实际为systemd接管telnet服务。
4. RHEL 6.x/SLES 11 SP4: xinetd -> in.telnetd
telnet服务受xinetd超级守护进程控制，xinetd作为telnet的守护进程。
5. xinetd是新一代的网络守护进程服务程序，又叫超级Internet服务器，常用来管理多种轻量级Internet服务。

telnet服务器搭建配置:

- RHEL 7.x:

```
$ sudo rpm -qa | grep telnet-server
# 查看是否已安装telnet服务端软件包

$ sudo rpm -ql telnet-server
# 列出telnet服务端软件包的全部文件
# /usr/sbin/in.telnetd: systemd守护进程调用的telnet服务进程程序

$ sudo echo -e "pts/0\npts/1\npts/2" >> /etc/securetty
# telnet默认拒绝root远程登陆，由于引用 /etc/pam.d/login 配置文件，按照PAM
  规则pam_securetty.so
# 模块使用 /etc/securetty 配置文件，其中允许的的终端类型才能使root远程登
陆，
    因此允许root远程登陆
# 必须包含虚拟终端pts/X。

$ sudo systemctl start telnet.socket && \
  systemctl enable telnet.socket && \
  systemctl status telnet.socket
# 启动telnet服务并配置为开机自启动

$ sudo ps -ef | grep telnet
# 查看telnet服务进程状态
# telnet服务只有当客户端连入时才生成telnet进程，在无客户端连入时不生成
telnet进程。
# telnet进程: /usr/sbin/in.telnetd

$ sudo netstat -tunlp | grep 23
# 查看telnet服务端口状态
# telnet服务端口: 23
# telnet服务由systemd守护进程接管，因此systemd进程监听23端口。

$ sudo firewall-cmd --permanent --add-service=telnet && \
  firewall-cmd --reload
# 防火墙放行telnet服务，并重载防火墙。
```

- RHEL 6.x/SLES 11 SP4（注释与RHEL 7.x相似）:

```
$ sudo rpm -qa | grep telnet-server
$ sudo rpm -ql telnet-server
$ sudo echo -e "pts/0\npts/1\npts/2" >> /etc/securetty
$ sudo vim /etc/xinetd.d/telnet
```

```

$ sudo vim /etc/xinetd.d/telnet
// RHEL 6.x/SLES 11 SP4中telnet服务由super daemon xinetd控制
// 将/etc/xinetd.d/telnet中disable改为no, root即可通过telnet远程登录。

# default: on
# description: The telnet server serves telnet sessions; it uses \
#   unencrypted username/password pairs for authentication.
service telnet
{
    flags                = REUSE
    socket_type          = stream
    wait                 = no
    user                  = root                # root身份运行
    server                = /usr/sbin/in.telnetd # telnet-server服务命令运行路径
    log_on_failure += USERID                  # 用户登录失败时依次记录用户名
    disable               = no                 # 允许root远程登录
}

```

```

$ sudo service xinetd restart
$ sudo chkconfig --level 35 xinetd on
$ sudo service xinetd status
$ sudo ps -ef | grep telnet
$ sudo netstat -tunlp | grep 23
$ sudo iptables -A INPUT -i ethX -p tcp --dport 23 -j ACCEPT
$ sudo service iptables save
# 防火墙放行telnet服务, 即开启23端口, 并保存防火墙规则。

```

telnet客户端连接方式:

- Linux客户端连接 (SLES 11 SP4为例):

```
mysuse:~ # telnet 192.168.0.120
```

- Windows客户端连接:

1. Windows默认没有添加telnet客户端, 需要手动添加:

控制面板 -> 程序 -> 启用或关闭Windows功能 -> 勾选"Telnet客户端" -> 确

定

2. cmd > telnet 192.168.0.120

xinetd守护进程的主配置文件: man xinetd.conf

- \$ sudo vim /etc/xinetd.conf

```
$ sudo vim /etc/xinetd.conf
```

```
#
# This is the master xinetd configuration file. Settings in the
# default section will be inherited by all service configurations
# unless explicitly overridden in the service configuration. See
# xinetd.conf in the man pages for a more detailed explanation of
# these attributes.

defaults
{
# The next two items are intended to be a quick access place to
# temporarily enable or disable services.
#
#   enabled          =                // 表示启用与禁用的服务
#   disabled         =

# Define general logging characteristics.
log_type             = SYSLOG daemon info    // 日志类型，默认日志保存于/var/log/messages。
log_on_failure        = HOST                 // 若telnet登录失败，记录主机。
log_on_success        = PID HOST DURATION EXIT // telnet登录成功的记录信息

# Define access restriction defaults
#
#   no_access         =                // 限制访问的主机
#   only_from         =                // 允许访问的主机
#   max_load          = 0              // 最大负载：0表示不限制
cps                   = 50 10           // 最大连接限制：50（最大连接数/秒）、10（上一次失败连接到下一次建立连接的等待秒数）
instances             = 50             // 同时工作实例数（类似最大连接数）
per_source             = 10             // 每个源IP（客户端）最多建立的实例数（次数）

# Address and networking defaults
#
#   bind              =                // 绑定到某个网络接口（IP地址）上
#   mdns              = yes
ip6only               = no

# setup environmental attributes
#
#   passenv           =                // 传递环境变量到服务器
groups               = yes            // 能够使用组权限
umask                 = 002           // 默认权限限制

# Generally, banners are not used. This sets up their global defaults
#
#   banner            =                // 输出给客户端的一些提示信息
#   banner_fail       =
#   banner_success    =
}

includedir /etc/xinetd.d           // 将/etc/xinetd.d中的文件与内容全部包含在内
```