RG-MCP_1.35_Build20160318

Installation Manual

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: http://www.ruijienetworks.com/
- Service Email: service_rj@ruijienetworks.com
- Technical Support: http://www.ruijienetworks.com/service.aspx
- Technical Support Hotline: +86-4008-111-000

Document Convention

The symbols used in this document are described as follows:

- Warning: Indicates a rule that users must comply with, which if ignored, could result in personal danger or equipment damage.
- Caution: Indicates important information that users must learn, which if ignored, could result in functional failure or performance deterioration.
- Note: Provides supplement, declaration, and prompts, which if ignored, will not cause a serious consequence.
- Product or version support: Describes the support status of the product or version.

1 Installation

1.1 Preparations

1.1.1 Checking Disk Partition and Physical Server

Requirements for minimum configurations of the server hardware are as follows:

Hardware	Requirement	Remarks
CPU	4 cores and 2.0 GHz CPU clock speed	
Memory	24 GB	
Hard disk	1 TB	Single hard disk
Network interface card (NIC)	Gigabit NIC	
System	CentOS 6.6 (compact edition)	X64-bit system

- Hard disk partition restrictions

Install the system according to the following partition requirements:

/: Specifies the 204800 MB root directory of the Linux system. The root directory contains all sub-directories.

/tmp: Specifies the 10240 MB directory for storing temporary files. This directory is arranged in an independent partition to avoid impact of file system overflow on system stability

Swap directory: Implements a virtual memory. It is recommended that the size of the virtual memory be one or two times the size of the physical memory. For example, configure a 64 GB virtual memory when the physical memory is 32 GB.

/project: Specifies the 204800 MB project directory for storing the installation file.

/bak: Specifies the 204800 MB backup directory for storing the backed up database, files, and logs.

/mcp: Specifies the database directory of the remaining space.

The partitions marked in red above are mandatory, each with a size larger than 100 GB.

- Port mapping

The port mapping function is used for public network deployment. CentOS is adopted on the Marketing Cloud Platform (MCP), and does not provide a self-defense function by default. Therefore, apply the port mapping mode instead of the overall system mapping mode in a case without the defense function.

Use the public network IP address of the egress device for mapping.

Intranet Port	External Network Port	Protocol	Mandatory or Optional	Remarks
80	80	TCP	Mandatory	MCP access port, which cannot be replaced by other ports.
3478	3478	UDP	Mandatory	MCP authentication port, which cannot be replaced by other ports.
3479	3479	UDP	Mandatory	MCP authentication port, which cannot be replaced by other ports.
22	Ports other	TCP	Optional	Secure shell (SSH) remote login port of the

	than port 22			MCP. Do not use port 22 for mapping. The password for running the operating system (OS) must be highly complex to avoid attacks.

- Parameter verification of the **sysctl.conf** file

Symptoms

Connection setup possibly fails when multiple clients use a same external network IP address. Specifically, the clients send synchronization packets to the server, but the server does not return the synchronization acknowledgments to the clients after receiving the synchronization packets. As a result, the clients retransmit the synchronization packets and it takes about one minute to set up connection.

Purpose

The purpose is to check whether the value of **net.ipv4.tcp_tw_recycle** is **0** in the **sysctl.conf** file in the **/etc/** directory, and change the value to **0** if not.

Modification is not required if no corresponding configuration is found in the **sysctl.conf** file.

Procedure

1. Run the **vi /etc/sysctl.conf** command to open the **sysctl.conf** file.
2. Enter **i** to move the cursor to the back of **1** in **net.ipv4.tcp_tw_recycle = 1**.
3. Replace **1** by **0**, and press **ESC**.
4. Enter **: wp**, and exit to save the modification.
5. Run the **sysctl –p** command to validate the modification.

1.1.2 Modifying System Time

If the system time is inconsistent with local standard time, manually run the **date** command to modify the time.

The following figure shows the **date** command in the format of **date** *month day hour minute year*.

```
[root@localhost bin]# date 110618152014
Thu Nov  6 18:15:00 CST 2014
[root@localhost bin]#
```

1.1.3 Copying Installation File to Server

1.1.3.1 ISO Upload Mode

CentOS provides a tool that enables users to easily implement direct interaction between Window systems and Linux systems. For details about the tool, see chapter 2.2.

1. Copy the ISO file to any directory of the server.
2. Run the **mount –o loop** */directory storing the file/file name/***mnt/** command.

Example:

To upload a file stored in the **home** directory, run the following command:

mount –o loop /home/RG-MCP_v1.35_Build20160318.iso /mnt/

Do not mount the file to the **tmp** directory; otherwise, the **tmp** directory will be read-only and the script cannot be properly executed.

1.1.3.2 USB Flash Drive Mode

1. Insert the USB flash drive into the USB port.
2. Run the **fdisk –l** command to display the partition information of the USB flash drive.

The red frame in the following figure shows the size of the USB flash drive.

```
Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x502626b1

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb2               1        6527    52428096   8e  Linux LVM
```

3. Run the **mount -o loop /dev/sdb2 /mnt/** command to mount the USB flash drive to the **mnt** directory.

Do not mount the file to the **tmp** directory; otherwise, the **tmp** directory will be read-only and the script cannot be properly executed.

```
/dev/sda3            37140        65271   223967104   8e  Linux LVM

Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x502626b1

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb2               1        6527    52428096   8e  Linux LVM
```

1.1.3.3 ISO Download Mode

1. Set up a Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP) server on a machine connected to the server, and copy the installation file to the HTTP or FTP server.
2. Log in to the MCP server, and run the following command to download the installation file:

- HTTP mode (for example, use the HFS tool to set up an HTTP server)

Run the **wget http: //** server *address/file name* command.

If a prompt is displayed, indicating that the **wget** command does not exist, perform installation via the **yum install wget** command. Ensure that the server is already connected to the Internet before performing this step.

Example:

Run the **cd /home** command to enter the **home** directory, and run the following command to download the ISO file:

wget http://172.18.3.33/RG-MCP_v1.35_Build20160318.iso

The ISO file is downloaded to the **home** directory. If the designated directory is not displayed after the **wget** command is run, the ISO file is downloaded to the current directory by default.

- FTP mode

Run the **wget ftp://***FTP user name*:*FTP password@address/directory name/file name* command.

Example:

1. Run the following command:

wget ftp://www:www@192.168.0.1/mcp/RG-MCP_v1.35_Build20160318.iso

2. Run the **mount –o loop** */directory storing the file/file name/***mnt/** command to mount the ISO file.

Example:

To download a file to the **home** directory, run the following command:

mount –o loop /home/RG-MCP_v1.35_Build20160318.iso /mnt/

Do not mount the file to the **tmp** directory; otherwise, the **tmp** directory will be read-only and the script cannot be properly executed.

1.1.3.4 Compact Disc Mode

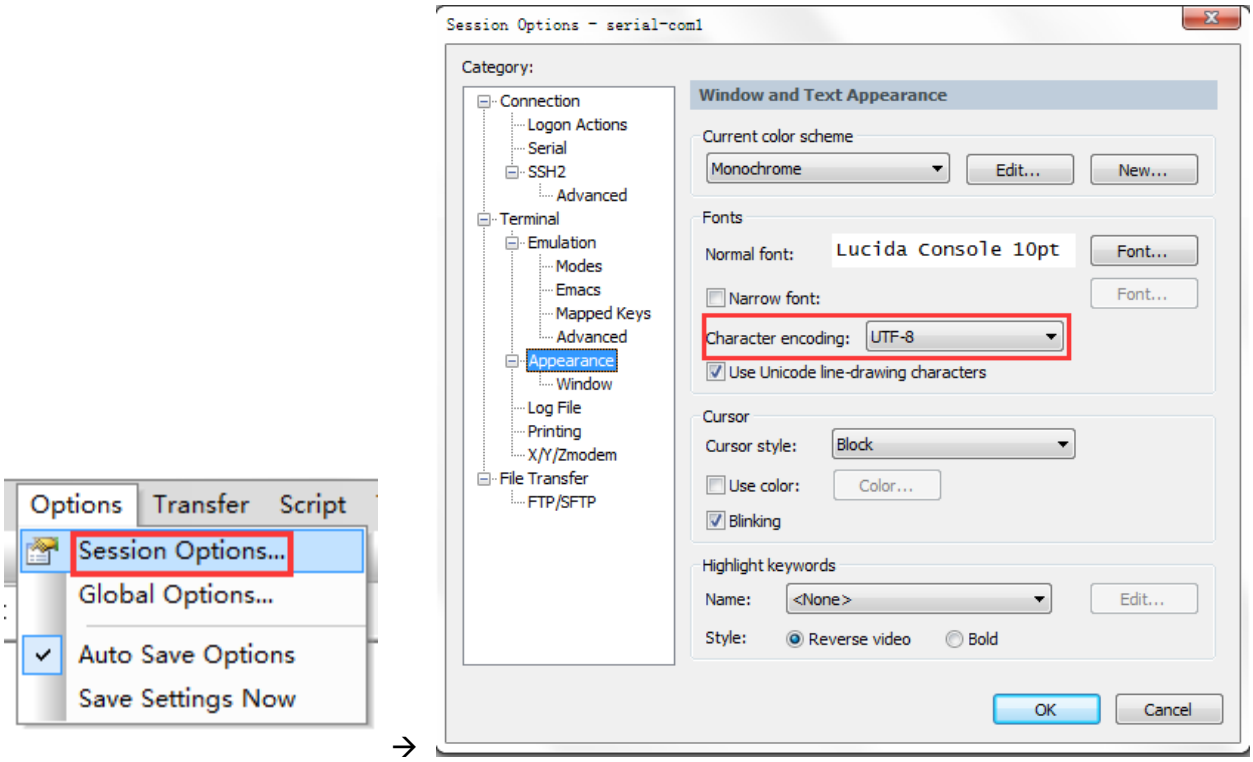
In CentOS, the installation file is in the CD-ROM form.

1. Log in to CentOS.
2. Run the **mount -o loop /dev/cdrom /mnt/** command to mount the compact disc to the **/mnt** directory.

Do not mount the file to the **tmp** directory; otherwise, the **tmp** directory will be read-only and the script cannot be properly executed.

1.1.4 Modifying Character Encoding Format

Modify the character encoding format to UTF8, as shown in the following figures:



1.2 Procedure

Enter commands manually to perform installation.

1.2.1 Initiating Script

It is possible that the **/mnt** directory is read-only. Therefore, enter a read/write directory first.

1. Run the **cd /tmp** command to enter the **tmp** directory.
2. Run the **cp –r /mnt/* /tmp** command to copy the ISO file to the **tmp** directory.
3. Run the **/install.sh.x** command to automatically perform the installation.

```
[root@nagios tmp]# ./install.sh.x
---------------------------------Basic file copy-----------------------------
installpkg/
installpkg/soft/
installpkg/soft/project.tar.gz
```

Enter the directory in which **install.sh.x** is stored; otherwise, the script cannot be executed.

After the installation succeeds (no error or other exception information is displayed), the input mode is displayed, for example:

```
[root@nagios tmp]#
```

The error shown in the following figure does not affect the MCP installation and can be ignored.

```
error: Failed dependencies:
        libperl.so()(64bit) is needed by perl-4:5.10.1-136.el6.x86_64
        perl(Module::Pluggable) is needed by perl-4:5.10.1-136.el6.x86_64
        perl(Pod::Simple) is needed by perl-4:5.10.1-136.el6.x86_64
        perl(version) is needed by perl-4:5.10.1-136.el6.x86_64
        perl-libs is needed by perl-4:5.10.1-136.el6.x86_64
        perl-libs = 4:5.10.1-136.el6 is needed by perl-4:5.10.1-136.el6.x86_64
warning: /bak/soft/rpm/perl-devel-5.10.1-136.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
error: Failed dependencies:
        /usr/bin/perl is needed by perl-devel-4:5.10.1-136.el6.x86_64
        db4-devel is needed by perl-devel-4:5.10.1-136.el6.x86_64
        gdbm-devel is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl >= 0:5.002 is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl >= 1:5.7.2 is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl = 4:5.10.1-136.el6 is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Carp) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Config) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(DynaLoader) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Exporter) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(ExtUtils::Constant) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(ExtUtils::Installed) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(ExtUtils::MakeMaker) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(ExtUtils::ParseXS) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(File::Compare) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(File::Find) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(File::Path) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(File::Spec) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Getopt::Long) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Getopt::Std) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(IO::File) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(Text::Wrap) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(constant) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(strict) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(vars) is needed by perl-devel-4:5.10.1-136.el6.x86_64
        perl(warnings) is needed by perl-devel-4:5.10.1-136.el6.x86_64
warning: /bak/soft/rpm/libstdc++-devel-4.4.7-11.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
Preparing...                ########################################### [100%]
   1:libstdc++-devel        ########################################### [100%]
warning: /bak/soft/rpm/perl-libs-5.10.1-136.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
error: Failed dependencies:
        perl = 4:5.10.1-136.el6 is needed by perl-libs-4:5.10.1-136.el6.x86_64
```

1.2.2 Performing Initial Configuration

1.2.2.1 Public Network Server or Intranet Server

If the server is set up in the public network (namely, a public network IP address is configured in the NIC) or can be accessed directly from the intranet, perform the following steps:

1. Log in to the system, enter the **soft** directory, and run the **cd /bak/soft/** command.

```
[root@localhost ~]#
[root@localhost ~]# cd /bak/soft/
[root@localhost soft]#
```

2. Run the **./setInternetNetwork.sh.x -localhostip 172.18.117.94 –internetip 172.18.117.94 –rootpw ADMINadmin123** command.

Information marked in red must be changed according to the onsite environment based on the following rules:

- The two IP addresses behind **-localhostip** and **–internetip** must be changed to the actual NIC IP address, namely, the public network IP address or the intranet IP address. These two IP addresses shall be the same.

The two IP addresses are an IP address that can be accessed by the authentication device, and cannot be empty. If the server is set up in the public network, the IP address marked in red is a public network IP address.

- **–rootpw** is the server password of the root user. The password must contain the uppercase letter, lowercase letter, and number, with a length more than 12 characters.

The password cannot contain special symbols; otherwise, other uncontrollable exceptions may occur.

1.2.2.2 MCP Server Deployed in NAT Mode

If the server is mapped to the external network in network address translation (NAT) mode, perform the following steps:

1. Log in to the system, enter the soft directory, and run the **cd /bak/soft/** command.

Run the **/setInternetNetwork.sh.x -localhostip 172.18.117.94 –internetip 210.210.210.210 –rootpw ADMINadmin123** command. After the configuration, picture access and device correlation are normal only in the public network.

Information marked in red must be changed according to the onsite environment based on the following rules:

- The IP address behind **-localhostip** must be changed to the actual NIC IP address (intranet IP address of the NIC).
- The IP address behind **–internetip** must be changed to the actual IP address after the NAT, namely, the public network IP address.
- **–rootpw** is the server password of the root user. The password must contain the uppercase letter, lowercase letter, and number, with a length more than 12 characters.

The password cannot contain special symbols; otherwise, other uncontrollable exceptions may occur.

1.2.3 Verifying Server Deployment

1.2.3.1 Checking MCP Service

1. Enter the **jps –l** command to check whether the service is properly enabled.

If an error is prompted, exit SecureCRT and check the service again.

```
[root@localhost ~]# jps -l
4491 sun.tools.jps.Jps
3071 ./data.jar
3272 ./redis-consumer.jar
3092 org.apache.zookeeper.server.quorum.QuorumPeerMain
4246 org.apache.catalina.startup.Bootstrap
[root@localhost ~]#
```

2. Enter **ps aux | grep nginx** and **ps aux | grep redis** separately to check the service.

```
root      1848  0.0  0.0  24284   752 ?        Ss   05:55   0:00 nginx: master process ./nginx -c /usr/local/nginx/conf/nginx.conf
nobody    1850  0.0  0.0  25080  1644 ?        S    05:55   0:00 nginx: worker process
nobody    1851  0.0  0.0  25080  1644 ?        S    05:55   0:00 nginx: worker process
root      2040  0.0  0.0 103296   808 pts/1    S+   05:56   0:00 grep nginx
```

```
[root@localhost project]# ps aux |grep redis
root      5263  0.1  0.0  31464  2232 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6379
root      5264  0.1  0.0  31348  2188 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6380
root      5265  0.0  0.0  31348  2184 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6381
root      5266  0.0  0.0  31348  2196 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6382
root      5267  0.1  0.0  31348  2208 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6383
root      5268  0.0  0.0  31348  2180 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6384
root      5269  0.1  0.0  31348  2180 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6385
root      5270  0.0  0.0  31348  2180 pts/1    Sl   22:11   0:00 /usr/local/bin/redis-server 127.0.0.1:6386
```

1.2.3.2 Checking Primary Port

Run the **netstat –aon |grep** *port number* command to respectively check whether ports 3478, 3479, and 80 are properly occupied.

```
[root@localhost ~]# netstat -aon |grep 3478
udp        0      0 ::ffff:127.0.0.1:3478       :::*                                    off (0.00/0/0)
udp        0      0 ::ffff:172.18.34.147:3478   :::*                                    off (0.00/0/0)
[root@localhost ~]#
```

```
[root@localhost ~]# netstat -aon |grep 3479
udp        0      0 ::ffff:127.0.0.1:3479       :::*                                    off (0.00/0/0)
udp        0      0 ::ffff:172.18.34.147:3479   :::*                                    off (0.00/0/0)
[root@localhost ~]#
```

```
[root@localhost ~]# netstat -aon|grep 80
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LISTEN      off (0.00/0/0)
tcp        0      0 ::ffff:127.0.0.1:8006       :::*                        LISTEN      off (0.00/0/0)
tcp        0      0 :::8010                     :::*                        LISTEN      off (0.00/0/0)
tcp        0      0 :::8080                     :::*                        LISTEN      off (0.00/0/0)
tcp        0      0 :::20880                    :::*                        LISTEN      off (0.00/0/0)
tcp        0      0 ::ffff:127.0.0.1:8080       ::ffff:127.0.0.1:41509      TIME_WAIT   timewait (21.80/0/0)
tcp        0      0 ::ffff:172.18.3.62:57178    ::ffff:172.18.3.62:20880    ESTABLISHED keepalive (4468.41/0/0)
tcp        0      0 ::ffff:172.18.3.62:57159    ::ffff:172.18.3.62:20880    ESTABLISHED keepalive (4450.40/0/0)
tcp        0      0 ::ffff:172.18.3.62:20880    ::ffff:172.18.3.62:57169    ESTABLISHED off (0.00/0/0)
tcp        0      0 ::ffff:172.18.3.62:57169    ::ffff:172.18.3.62:20880    ESTABLISHED keepalive (4461.40/0/0)
tcp        0      0 ::ffff:127.0.0.1:8080       ::ffff:127.0.0.1:41510      TIME_WAIT   timewait (51.80/0/0)
tcp        0      0 ::ffff:172.18.3.62:20880    ::ffff:172.18.3.62:57178    ESTABLISHED off (0.00/0/0)
tcp        0      0 ::ffff:172.18.3.62:20880    ::ffff:172.18.3.62:57159    ESTABLISHED off (0.00/0/0)
unix  2      [ ]         DGRAM                    40180
unix  3      [ ]         STREAM     CONNECTED     14180
```

1.2.3.3 Checking the Boot Log

1. Respectively run the following commands to check the logs:

- vi /project/data/logs/data-middleware.log
- vi /project/redis-consumer/logs/redis-consumer.log
- vi /bak/soft/apache-tomcat-7.0.55/logs/catalina.out

2. To exit, press **ESC**, and enter **:q!**.

If no error is displayed, the modification is successful.

1.2.3.4 Checking Firewall Rule

Run the **iptables –nL** command to check the firewall rules.

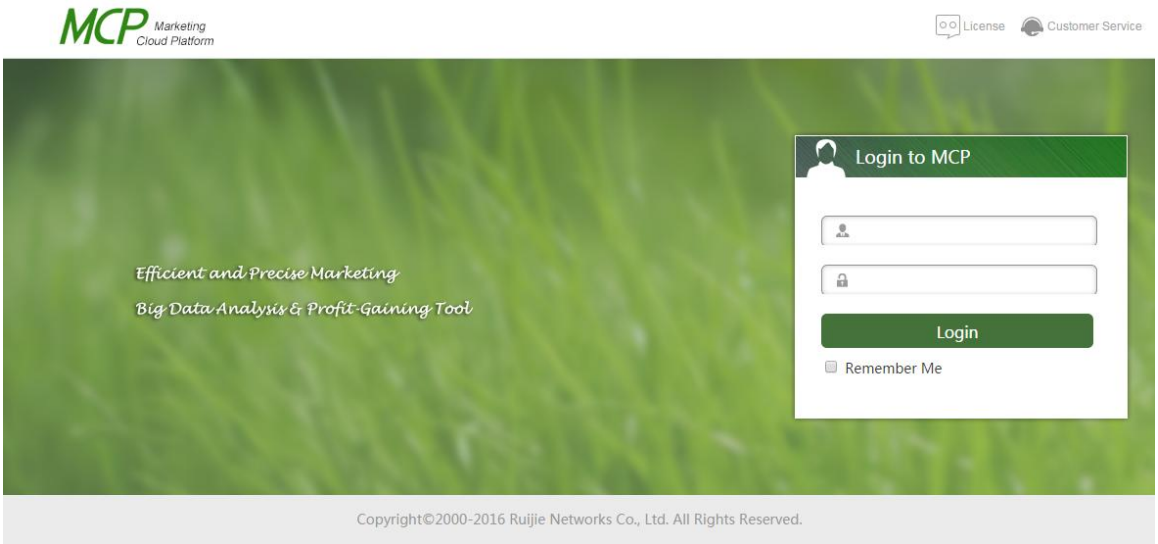
The following figure shows the firewall rules.

```
[root@localhost /]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:3479
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:3478
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3479
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3478
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:70

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost /]#
```

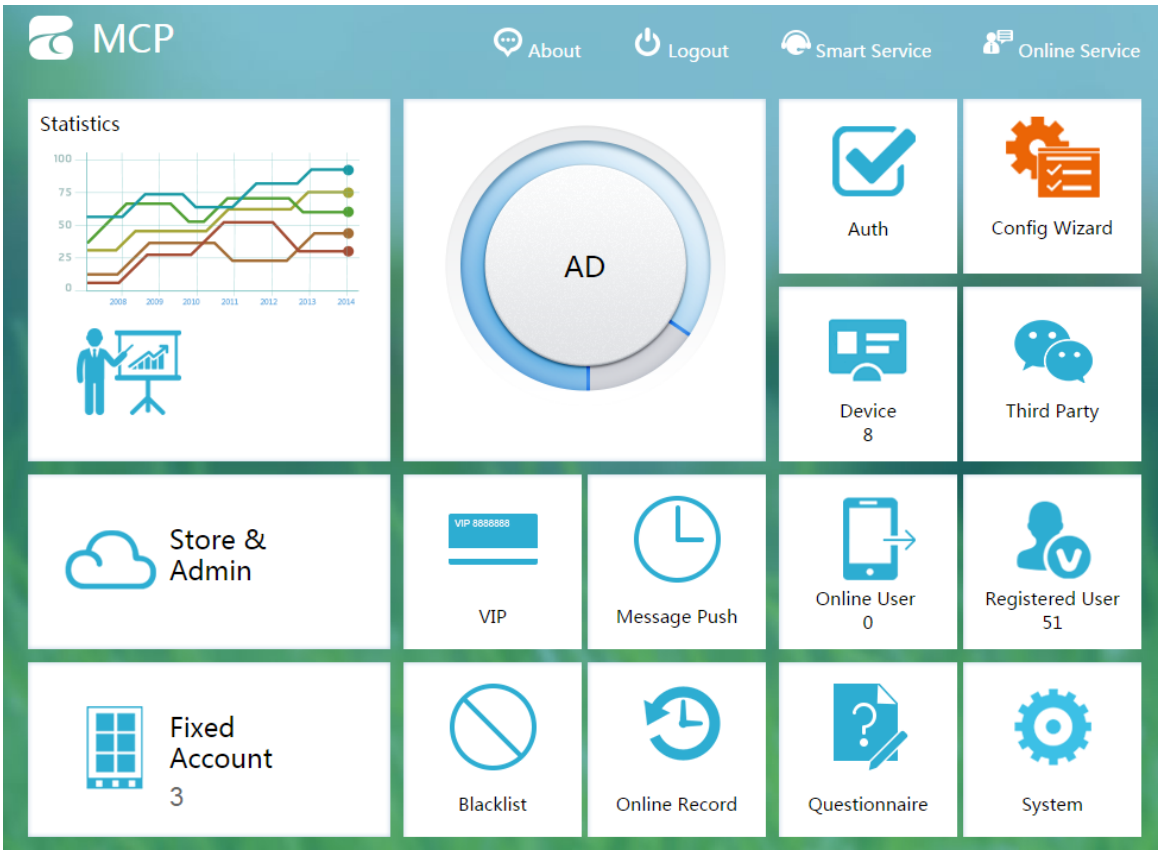
1.2.3.5 Accessing MCP Server

1. Start the Google browser, and enter **http://172.18.117.92** in the address bar to display the login page for tenants.

The IP address must be changed to the actual address.



2. Enter the username **mcp**, and the password **111111111** to log in to the MCP server.


MCP
About
Logout
Smart Service
Online Service
Statistics
AD
Auth
Config Wizard
Device
8
Third Party
Store &
Admin
VIP
Message Push
Online User
0
Registered User
51
Fixed
Account
3
Blacklist
Online Record
Questionnaire
System

2 Appendix

2.1 Manually Restarting MCP Service

By default, the MCP service is started upon system startup.

2.1.1 Restarting MCP Service

1. Log in to the system, enter the **soft** directory, and run the **cd /bak/soft/** command.
2. Run the **sh –x restart_mcp.sh** command to start the MCP service.

```
[root@localhost ~]# cd /bak/soft/
[root@localhost soft]# sh -x restart_mcp.sh
```

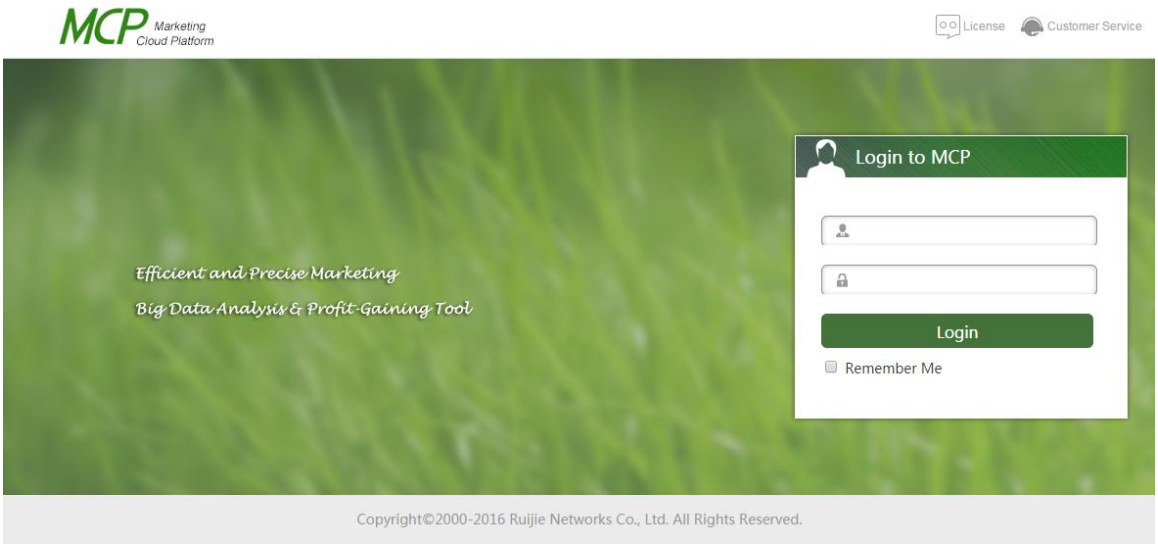
After started, the MCP service can be properly accessed if no error is displayed in the log, as shown in the following figure.

```
INFO: Deployment of web application directory /bak/soft/apache-tomcat-7.0.55/web
apps/host-manager has finished in 46 ms
Nov 12, 2014 2:09:49 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory /bak/soft/apache-tomcat-7.0.55/webapps
/examples
Nov 12, 2014 2:09:49 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory /bak/soft/apache-tomcat-7.0.55/web
apps/examples has finished in 224 ms
Nov 12, 2014 2:09:49 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-nio-80"]
Nov 12, 2014 2:09:49 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["ajp-bio-8010"]
Nov 12, 2014 2:09:49 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 36495 ms
```

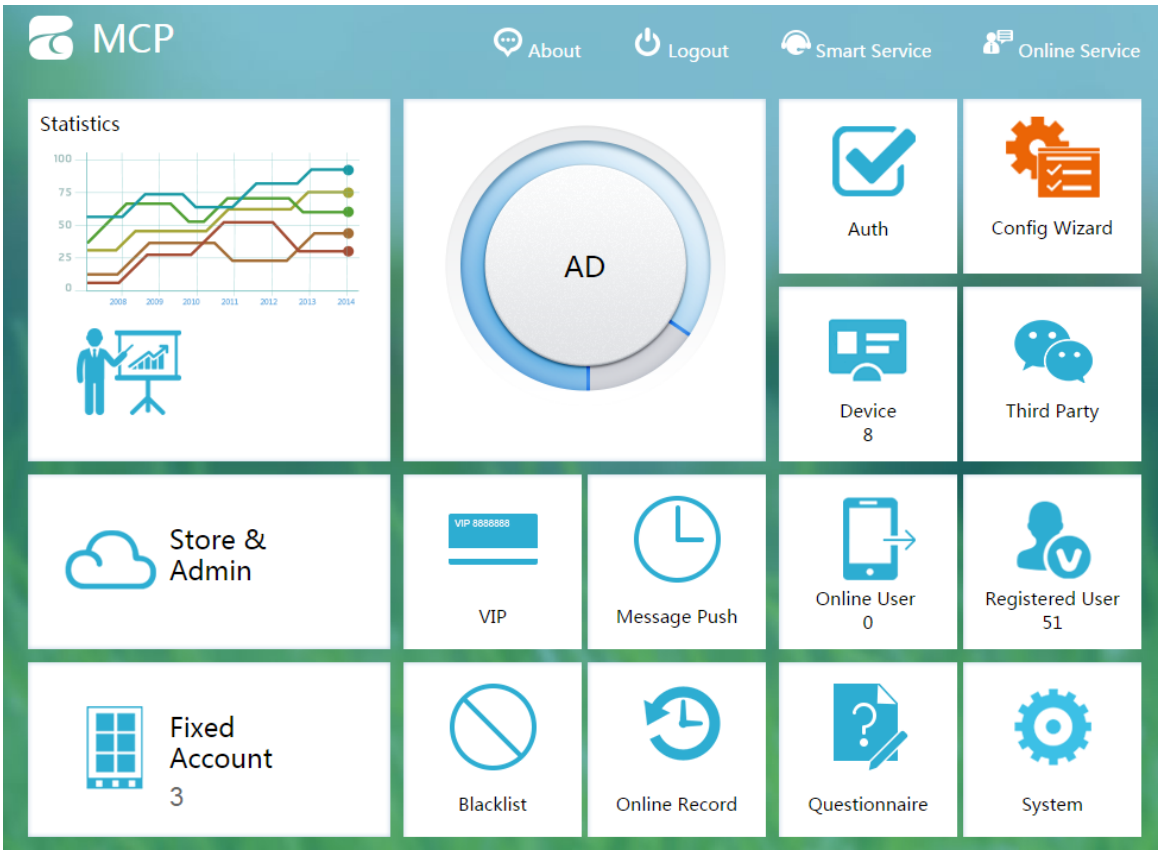
Besides, you can verify whether the MCP service is successfully started by checking the server process. For details, see chapter1.2.3.

3. After the MCP service is successfully started, start the Google browser, and enter **http://172.18.117.92** in the address bar to display the login page for tenants.

The IP address must be changed to the actual address.



4. Enter the username **mcp**, and the password **111111111** to log in to the MCP server.



2.1.2 Changing Server IP Address

To change the server IP address, the following three MCP configuration files need to be modified:

⚠ Do not execute the **setInternetwork.sh.x** file again.

- **businessconfig** file

Run the **vi /alidata/wmc_common_config/businessconfig.properties** command, enter **i** to move the cursor to the IP address, and change the IP address as required.

After the change, enter **:wq** to save and exit.

```
common.server.internetip=172.18.86.160
common.sms.custom.ip=http://baas.ruijieyun.com
common.server.ip=172.18.86.160
tr069.dir.prefix=/mcp/ngProxy/mcp_file/
common.upload.dir=/mcp/ngProxy
network.interface.card=eth0

auth.weixinwifi.project.type=MCP
auth.weixinwifi.wmc.acesstoken.ip=112.124.31.88
auth.weixinwifi.appid=wxb5584d05f15952a1
auth.weixinwifi.secret=2269a08252a0ba5961a1eb5eb92b188f

elog.webservice.url=http://40.1.1.200:8080/elog/webservice/UserTagService
elog.enable=false

adCloseUrl=http://#common.server.ip#/auth/servlet/LinkVisitCloseCountServlet
~
```

Local NIC IP address for intranet mode
NATted public network IP address for NAT mode

Local NIC IP address

- **dubbo** file

1. Run the **vi /alidata/wmc_common_config/dubbo.properties** command, enter **i** to move the cursor to the IP address, and change the IP address as required.
2. After the change, enter **:wq** to save and exit.

```
dubbo.registry.protocol=zookeeper
dubbo.registry.address=172.18.86.160:2181

dubbo.application.name.admin=admin
dubbo.application.name.auth=auth
dubbo.application.name.chain=chain
dubbo.application.name.open=open
dubbo.application.name.tr069=tr069
dubbo.application.name.data=data-middleware
dubbo.application.name.sms=sms
dubbo.application.name.monitor=wmc-monitor

dubbo.protocol.port.auth=20885
dubbo.protocol.port.chain=20893
dubbo.protocol.port.tr069=22385
dubbo.protocol.port.sms=20887
dubbo.protocol.port.admin=20888
~
```

Local NIC IP address

- **NG** file

1. Run the **vi /usr/local/nginx/conf/nginx.conf** command, enter **i** to move the cursor to the IP address, and change the IP address as required.
2. After the change, enter **:wq** to save and exit.

```
upstream 172.18.86.160 {
     server 127.0.0.1:8080 max_fails=2;
    }

upstream tr069 {
     server 127.0.0.1:8080;
     keepalive 1024;
    }

server {
    listen       80;
    server_name  localhost;
    #charset koi8-r;
    access_log  /dev/null;
    #access_log  logs/host.access.log  main;

    location ~*auth/servlet/authServlet {
        add_header Content-Type "text/html;charset=utf-8";
        return 200 "<script>window.location.href='http://172.18.86.160/auth/servlet/authNewServlet?$args'</script>";

    }


    location ~*auth/wifidogAuth/login/ {
        add_header Content-Type "text/html;charset=utf-8";
        return 200 "<script>window.location.href='http://172.18.86.160/auth/wifidogAuth/newLogin/?$args'</script>";

    }

    location ~*auth/wxwifiAuth/autoPortal/ {
        add_header Content-Type "text/html;charset=utf-8";
        return 200 "<script>self.location.href='http://172.18.86.160/auth/wxwifiAuth/newAutoPortal/?$args'</script>";
    }

    location ~*ngProxy {
        root   /mcp/;
        expires 1d;
    }


    location /mcp {
       proxy_redirect          off;
      # nginx非80端口处理
       proxy_set_header        Host $host:$server_port;
```

Local NIC IP address for intranet mode
NATted public network IP address for NAT mode

```
}

location ~*.(gif|jpg|jpeg|js|css|bmp|png)$ {
    proxy_next_upstream error timeout http_500 http_502 http_504 http_404;
    proxy_read_timeout 20s;
    proxy_redirect              off;
   # nginx非80端口处理
    proxy_set_header            Host $host:$server_port;
    proxy_set_header            Cookie $http_cookie;
    proxy_set_header            REMOTE-HOST $remote_addr;
    # 获取真实IP
    proxy_set_header            X-Real-IP $remote_addr;
   # 获取代理者的真实ip
    proxy_set_header            X-Forwarded-For    $proxy_add_x_forwarded_for;
    client_max_body_size        50m;
    client_body_buffer_size 128k;
    proxy_connect_timeout       600;
    proxy_send_timeout          600;
    proxy_buffer_size           4k;
    proxy_buffers               4 32k;
    proxy_busy_buffers_size 64k;
    proxy_temp_file_write_size 64k;
    proxy_cache ngcache;
    proxy_cache_valid 200 304 12h;
    proxy_cache_key $host$uri$is_args$args;
    proxy_pass http://172.18.86.160;
}

location / {
    proxy_next_upstream error timeout http_500 http_502 http_504 http_404;
    proxy_read_timeout 20s;
    proxy_redirect              off;
   # nginx非80端口处理
    proxy_set_header            Host $host:$server_port;
    proxy_set_header            Cookie $http_cookie;
    proxy_set_header            REMOTE-HOST $remote_addr;
    # 获取真实IP
    proxy_set_header            X-Real-IP $remote_addr;
   # 获取代理者的真实ip
    proxy_set_header            X-Forwarded-For    $proxy_add_x_forwarded_for;
    client_max_body_size        50m;
    client_body_buffer_size 128k;
    proxy_connect_timeout       600;
    proxy_send_timeout          600;
    proxy_buffer_size           4k;
    proxy_buffers               4 32k;
    proxy_busy_buffers_size 64k;
    proxy_temp_file_write_size 64k;
    proxy_pass http://172.18.86.160;
```

Local NIC IP address for intranet mode
NATted public network IP address for NAT mode

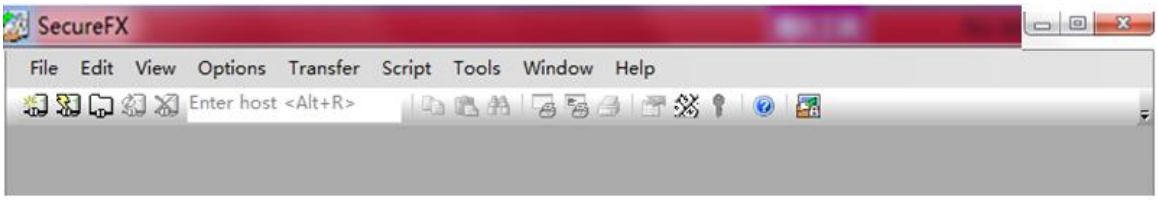
2.2 SecureFXPortable (File Copy Tool)

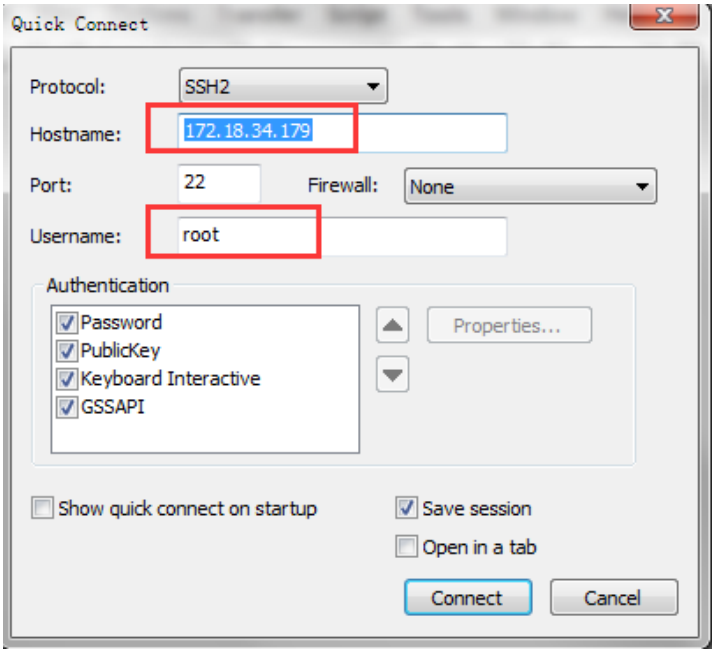
The SecureFXPortable tool is used to connect to the Linux server in SFTP mode for file transfer.

The installation process is not described herein.

1. Double-click the desktop icon 

to start SecureFXPortable.



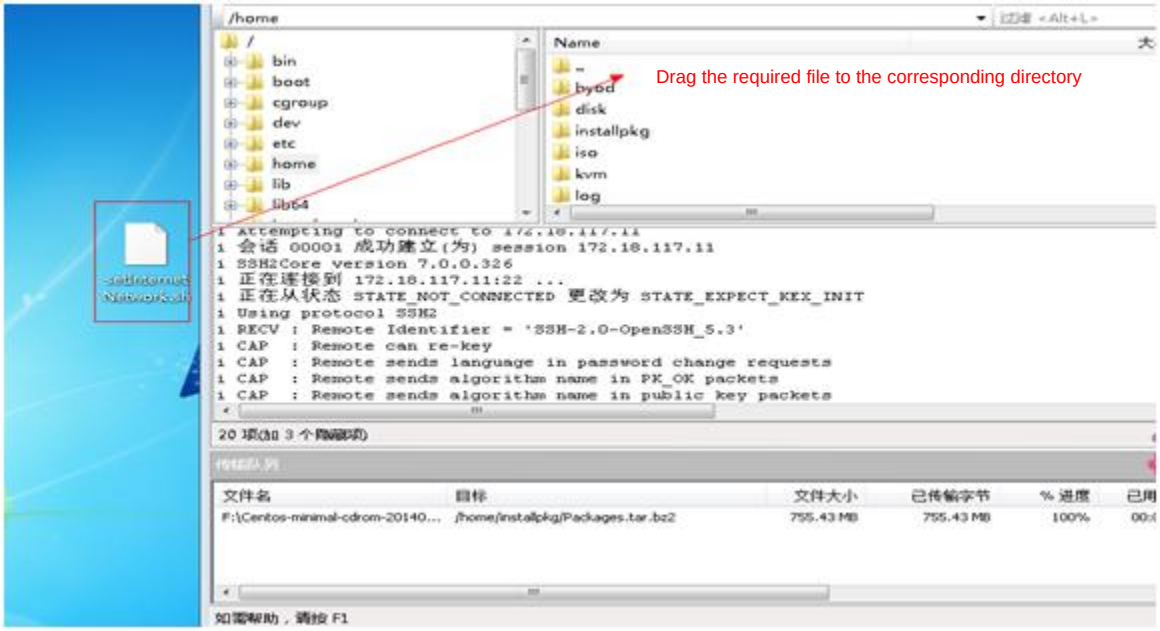


2. Enter the hostname and username, and click **Connect**.

3. On the displayed page, enter the password.

4. Copy the required file, select a directory, and paste the file to copy it to the server.

Alternatively, you can drag the file to the corresponding directory.

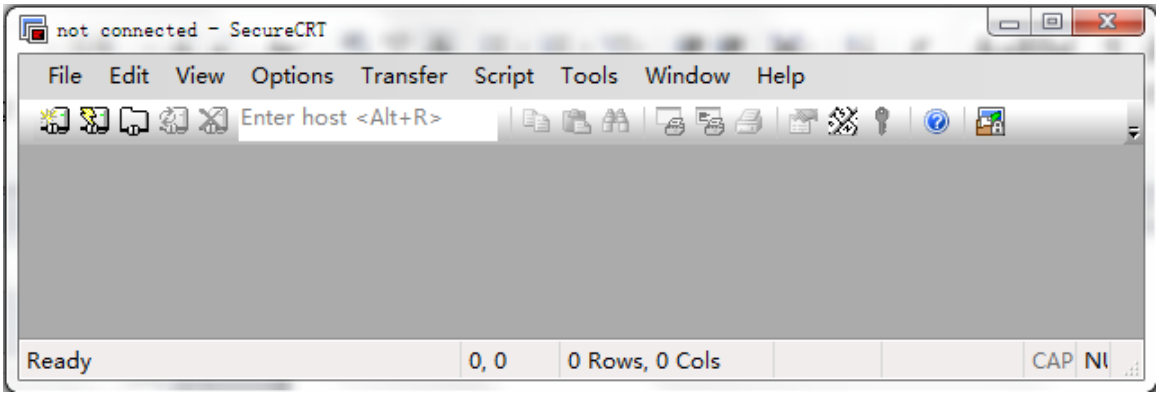


2.3 SecureCRTPortable (Maintenance Tool)

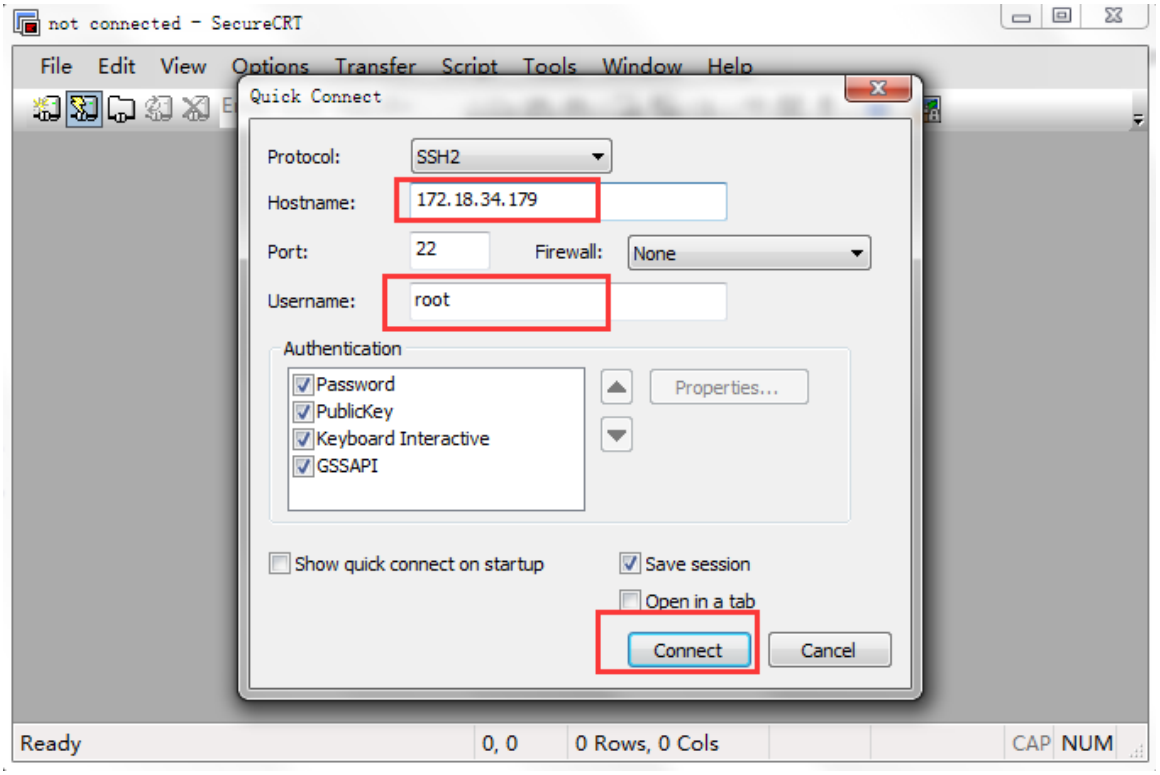
The SecureCRTPortable tool is used to connect to the Linux server in SSH2 mode for configuration.

SecureCRTPortable is a commonly used SSH2 tool.

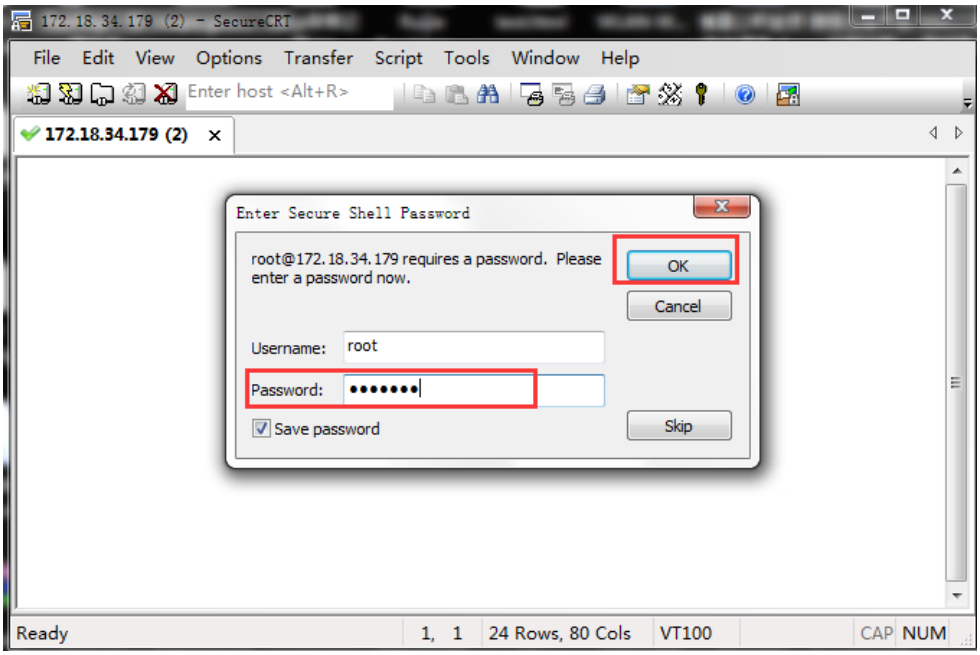
1. Start SecureCRT, and click **Quick Connect** in the toolbar.



2. Enter the hostname and username, and click **Connect.**



3. Enter the server password **123456**, and click **OK**.



The following figure shows the interface displayed after the login.