目 录

1 SSH2.0 配置命令

1.1 SSH2.0 服务器端配置命令

1.1.1 display ssh server

【命令】

display ssh server { **session** | **status** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

session：显示 SSH 服务器的会话信息。

status：显示 SSH 服务器的状态信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssh server 命令用来在 SSH 服务器端显示该服务器的状态信息或会话信息。

相关配置可参考命令 **ssh server authentication-retries**、**ssh server rekey-interval**、**ssh server authentication-timeout**、**ssh server enable** 和 **ssh server compatible-ssh1x enable**。

说明

该命令也可在 SFTP 服务器端使用。

【举例】

在 SSH 服务器端显示该服务器的状态信息。

```
<Sysname> display ssh server status
 SSH server: Disable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
```

```
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
```

表1-1 display ssh server status 命令显示信息描述表

字段	描述
SSH server	SSH 服务器功能的状态
SSH version	SSH 协议版本 SSH 服务器兼容 SSH1 时，协议版本为 1.99；SSH 服务器不兼容 SSH1 时，协议版本为 2.0
SSH authentication-timeout	认证超时时间
SSH server key generating interval	服务器密钥对更新时间
SSH authentication retries	认证尝试的最大次数
SFTP server	SFTP 服务器功能的状态
SFTP server Idle-Timeout	SFTP 用户连接的空闲超时时间

在 SSH 服务器端显示该服务器的会话信息。

```
<Sysname> display ssh server session
 Conn    Ver    Encry    State          Retry    SerType  Username
 VTY 0   2.0    DES      Established    0        SFTP     client001
```

表1-2 display ssh server session 显示信息描述表

字段	描述
Conn	用户登录使用的 VTY 界面的编号
Ver	SSH 服务器的协议版本
Encry	SSH 使用的加密算法
State	会话状态，包括： Init：初始化状态 Ver-exchange：版本协商 Keys-exchange：密钥交换 Auth-request：用户认证 Serv-request：服务请求 Established：连接已经建立 Disconnected：断开连接
Retry	认证失败的次数
SerType	服务类型，包括 SFTP 和 Stelnet 两种类型
Username	客户端登录服务器时采用的用户名

1.1.2 display ssh user-information

【命令】

display ssh user-information [*username*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

username：显示指定 SSH 用户的信息。*username* 表示 SSH 用户名，为 1～80 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssh user-information 命令用来在 SSH 服务器端显示 SSH 用户的信息。

需要注意的是：

- 本命令仅用来显示 SSH 服务器端通过 **ssh user** 命令配置的 SSH 用户信息。
- 如果没有指定参数 *username*，则显示所有 SSH 用户的信息。

相关配置可参考命令 **ssh user**。

说明

该命令也可在 SFTP 服务器端使用。

【举例】

显示所有 SSH 用户的信息。

```
<Sysname> display ssh user-information
 Total ssh users : 2
 Username     Authentication-type   User-public-key-name     Service-type
 yemx         password              null                   stelnet|sftp
 test         publickey             pubkey                    sftp
```

表1-3 display ssh user-information 显示信息描述表

字段	描述
Total ssh users	SSH 用户的总数
Username	用户名

字段	描述
Authentication-type	认证类型，如果认证类型为 password，则用户公钥名称显示为 null
User-public-key-name	用户公钥名称
Service-type	服务类型

1.1.3 ssh server authentication-retries

【命令】

ssh server authentication-retries *times*

undo ssh server authentication-retries

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

times：指定认证尝试的最大次数，取值范围为 1～5。

【描述】

ssh server authentication-retries 命令用来设置 SSH 连接认证尝试的最大次数。**undo ssh server authentication-retries** 命令用来恢复缺省情况。

缺省情况下，SSH 连接认证尝试的最大次数为 3 次。

需要注意的是：

- 本配置对新登录的用户生效。
- SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试的最大次数。
- SSH 用户的认证方式为 **password-publickey** 时，由于 SSH2.0 用户需要同时通过 **password** 和 **publickey** 认证，因此配置的 SSH 连接认证尝试最大次数必须大于等于 2。

相关配置可参考命令 **display ssh server**。

【举例】

指定登录认证尝试的最大次数为 4 次。

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

1.1.4 ssh server authentication-timeout

【命令】

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

time-out-value：认证超时时间，取值范围为 1～120，单位为秒。

【描述】

ssh server authentication-timeout 命令用来在 SSH 服务器端设置 SSH 用户的认证超时时间。**undo ssh server authentication-timeout** 命令用来恢复缺省情况。

缺省情况下，SSH 用户的认证超时时间为 60 秒。

相关配置可参考命令 **display ssh server**。

【举例】

设置 SSH 用户认证超时时间为 10 秒。

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

1.1.5 ssh server compatible-ssh1x enable

【命令】

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

无

【描述】

ssh server compatible-ssh1x enable 命令用来设置 SSH 服务器兼容 SSH1 版本的客户端。**undo ssh server compatible-ssh1x** 命令用来设置 SSH 服务器不兼容 SSH1 版本的客户端。

缺省情况下，SSH 服务器兼容 SSH1 版本的客户端。

该配置对新登录的用户生效。

相关配置可参考命令 **display ssh server**。

【举例】

配置服务器兼容 SSH1 版本的客户端。

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

1.1.6 ssh server enable

【命令】

ssh server enable

undo ssh server enable

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

无

【描述】

ssh server enable 命令用来使能 SSH 服务器功能。**undo ssh server enable** 命令用来关闭 SSH 服务器功能。

缺省情况下，SSH 服务器功能处于关闭状态。

【举例】

使能 SSH 服务器功能。

```
<Sysname> system-view
[Sysname] ssh server enable
```

1.1.7 ssh server rekey-interval

【命令】

ssh server rekey-interval *hours*

undo ssh server rekey-interval

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

hours：服务器密钥的更新周期，取值范围为 1～24，单位为小时。

【描述】

ssh server rekey-interval 命令用来设置 RSA 服务器密钥的更新时间。**undo ssh server rekey-interval** 命令用来恢复缺省情况。

缺省情况下，RSA 服务器密钥的更新时间为 0，表示系统不更新 RSA 服务器密钥。

相关配置可参考命令 **display ssh server**。

注意

- 此命令仅对 SSH 客户端版本为 SSH1 的用户有效。
- 系统不会定期更新 DSA 密钥对。

【举例】

设置每 3 小时更新一次 RSA 服务器密钥。

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

1.1.8 ssh user

【命令】

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

username：SSH 用户名，为 1～80 个字符的字符串，区分大小写。

service-type：SSH 用户的服务类型。包括：

all：包括 **stelnet** 和 **sftp** 两种服务类型。

sftp：服务类型为安全的文件传输。

stelnet：服务类型为安全的 Telnet。

authentication-type：SSH 用户的认证方式。包括：

- **password**：强制指定该用户的认证方式为 password。
- **any**：不指定用户的认证方式，用户既可以采用 password 认证，也可以采用 publickey 认证。
- **password-publickey**：指定客户端版本为 SSH2 的用户认证方式为必须同时进行 password 和 publickey 两种认证；客户端版本为 SSH1 的用户认证方式为只要进行其中一种认证即可。
- **publickey**：强制指定该用户的认证方式为 publickey。

assign publickey *keyname*：为 SSH 用户分配一个已经存在的公钥。*keyname* 表示已经配置的客户端公钥名，为 1～64 个字符的字符串。

work-directory *directory-name*：为 SFTP 用户设置工作目录。*directory-name* 表示 SFTP 用户的工作目录，为 1～135 个字符的字符串。

【描述】

ssh user 命令用来创建 SSH 用户，并指定 SSH 用户的服务类型和认证方式。**undo ssh user** 命令用来删除 SSH 用户。

需要注意的是：

- 对于使用 publickey 认证方式的用户，必须在设备上配置相应的用户及其公钥。对于使用 password 认证方式的用户，用户的账号信息可以配置在设备或者远程认证服务器（如 RADIUS 认证服务器）上。
- 使用该命令为用户分配公钥时，如果此用户已经被分配了公钥，则以最后一次分配的公钥为准。
- 新配置的认证方式和用户公钥，对于已经登录的 SSH 用户不会生效，只在 SSH 用户下次登录时生效。
- 如果为 SFTP 用户指定了公钥，则必须同时为该用户设置工作目录。
- SFTP 用户登录时使用的工作目录与用户使用的认证方式有关。只采用 publickey 认证方式的用户，使用的工作目录为通过 **ssh user** 命令为该用户设置的工作目录；只采用 password 认证方式的用户，使用的工作目录为通过 AAA 授权的工作目录；同时采用 publickey 和 password 两种认证方式的用户，使用的工作目录为通过 **ssh user** 命令为该用户设置的工作目录。

相关配置可参考命令 **display ssh user-information**。

【举例】

创建 SSH 用户 user1，配置 user1 的服务类型为 **sftp**，认证方式为 **publickey**，并指定用户公钥为 key1，SFTP 服务器工作目录为 cfa0:。

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey
key1 work-directory cfa0:
```

1.2 SSH2.0 客户端配置命令

1.2.1 display ssh client source

【命令】

display ssh client source [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssh client source 命令用来显示当前为 SSH 客户端设置的源 IP 地址或者源接口。

如果没有为 SSH 客户端指定源地址和源接口，则提示尚未指定。

相关配置可参考命令 **ssh client source**。

【举例】

显示 SSH 客户端的源 IP 地址或者源接口。

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

1.2.2 display ssh server-info

【命令】

display ssh server-info [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssh server-info 命令用来在 SSH 客户端显示客户端保存的服务器端的主机公钥和服务器的对应关系。

SSH 客户端需要认证服务器时，以本地保存的服务器端的主机公钥对连接的服务器进行认证。如果认证不成功，可以通过 **display ssh server-info** 命令查看服务器是否与正确的公钥对应。

相关配置可参考命令 **ssh client authentication server**。

说明

该命令也可在 SFTP 客户端使用。

【举例】

显示客户端保存的服务器端的主机公钥和服务器的对应关系。

```
<Sysname> display ssh server-info
Server Name(IP)                 Server public key name
```

```
192.168.0.1                     abc_key01
192.168.0.2                     abc_key02
```

表1-4 display ssh server-info 显示信息描述表

字段	描述
Server Name(IP)	服务器名称或者 IP 地址
Server public key name	服务器端的主机公钥名称

1.2.3 ssh client authentication server

【命令】

ssh client authentication server *server* **assign publickey** *keyname*

undo ssh client authentication server *server* **assign publickey**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

server：服务器的 IP 地址或名称，为 1～80 个字符的字符串。

assign publickey *keyname*：指定服务器端的主机公钥。*keyname* 表示主机公钥名称，为 1～64 个字符的字符串。

【描述】

ssh client authentication server 命令用来在客户端上指定要连接的服务器端的主机公钥名称，以便客户端判断认证连接的服务器是否为可信赖的服务器。**undo ssh client authentication server** 命令用来取消在客户端上指定要连接的服务器端的主机公钥。

缺省情况下，客户端不指定要连接的服务器端的主机公钥名称，而是在客户端登录服务器的时候使用登录服务器时所用的 IP 地址或主机名作其对应的公钥名称。

如果客户端不支持首次认证，客户端将拒绝访问未经认证的服务器。此时，需要在客户端配置服务器端的公钥，并指定该公钥与服务器端的对应关系，以便在客户端对连接的服务器端进行认证时，能够根据该对应关系使用正确的公钥对服务器端进行认证。

需要注意的是，指定的服务器端的主机公钥必须已经存在。

相关配置可参考命令 **ssh client first-time enable**。

【举例】

服务器的 IP 地址为 192.168.0.1，在客户端指定该服务器的公钥名称为 key1。

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

1.2.4 ssh client first-time enable

【命令】

ssh client first-time enable

undo ssh client first-time

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ssh client first-time enable 命令用来设置 SSH 客户端对访问的 SSH 服务器进行首次认证。**undo ssh client first-time** 命令用来取消 SSH 客户端对访问的 SSH 服务器进行首次认证。

缺省情况下，客户端进行首次认证。

所谓首次认证，是指当 SSH 客户端首次访问服务器，而客户端没有配置服务器端的公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。

如果不支持首次认证，则当客户端没有配置服务器端的公钥时，客户端将被拒绝访问该服务器。用户必须事先通过其它途径将要访问的服务器端的主机公钥配置在本地，同时指定要连接的服务器端的主机公钥名称，以便客户端认证连接的服务器是否为可信赖的服务器。

需要注意的是，由于服务器端可能会定期更新密钥对，为保证服务器认证成功，客户端需要及时获取最新的服务器主机公钥。

【举例】

设置 SSH 客户端对访问的 SSH 服务器进行首次认证。

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

1.2.5 ssh client ipv6 source

【命令】

ssh client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo ssh client ipv6 source

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

ipv6 *ipv6-address*：源 IPv6 地址。

interface *interface-type interface-number*：源接口类型与源接口编号。

【描述】

ssh client ipv6 source 命令用来为 SSH 客户端指定源 IPv6 地址或源接口。**undo ssh client ipv6 source** 命令用来清除指定的源 IPv6 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SSH 服务器。

相关配置可参考命令 **display ssh client source**。

【举例】

指定 SSH 客户端的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

1.2.6 ssh client source

【命令】

ssh client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo ssh client source

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

ip *ip-address*：源 IPv4 地址。

interface *interface-type interface-number*：源接口类型与源接口编号。

【描述】

ssh client source 命令用来为 SSH 客户端指定源 IPv4 地址或源接口。**undo ssh client source** 命令用来清除指定的源 IPv4 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SSH 服务器。

相关配置可参考命令 **display ssh client source**。

【举例】

指定 SSH 客户端的源 IPv4 地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

1.2.7 ssh2

【命令】

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

【视图】

用户视图

【缺省级别】

0：访问级

【参数】

server：服务器 IPv4 地址或主机名称，为 1～20 个字符的字符串，不区分大小写。

port-number：服务器端口号，取值范围为 0～65535，缺省值为 22。

vpn-instance *vpn-instance-name*：服务器所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示服务器位于公网中。

identity-key：publickey 认证采用的公钥算法，缺省算法为 **dsa**。

dsa：公钥算法为 DSA。

rsa：公钥算法为 RSA。

prefer-ctos-cipher：客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

3des：3des-cbc 加密算法。

aes128：aes128-cbc 加密算法。

des：des-cbc 加密算法。

prefer-ctos-hmac：客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

md5：HMAC 算法 hmac-md5。

md5-96：HMAC 算法 hmac-md5-96。

sha1：HMAC 算法 hmac-sha1。

sha1-96：HMAC 算法 hmac-sha1-96。

prefer-kex：密钥交换首选算法，缺省算法为 **dh-group-exchange**。

dh-group-exchange：密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1：密钥交换算法 diffie-hellman-group1-sha1。

dh-group14：密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher：服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac：服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【描述】

ssh2 命令用来建立 SSH 客户端和 IPv4 服务器端的连接，并指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法。

需要注意的是，当服务器端指定客户端的认证方式为 publickey 认证时，客户端需要读取本地的私钥进行验证。由于 publickey 认证可以采用 RSA 和 DSA 两种加密算法，所以需要用 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。缺省情况下，加密算法为 DSA。

【举例】

登录地址为 10.214.50.51 的远程 SSH2 服务器，采用的算法为：

- 首选密钥交换算法为 **dh-group1**；
- 服务器到客户端的首选加密算法为 **aes128**；

- 客户端到服务器的首选 HMAC 算法为 **md5**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
```

1.2.8 ssh2 ipv6

【命令】

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

【视图】

用户视图

【缺省级别】

0：访问级

【参数】

server：服务器的 IPv6 地址或主机名称，为 1～46 个字符的字符串，不区分大小写。

port-number：服务器的端口号，取值范围为 0～65535，缺省值为 22。

vpn-instance *vpn-instance-name*：服务器所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示服务器位于公网中。

identity-key：publickey 认证采用的公钥算法，缺省算法为 **dsa**。

dsa：公钥算法为 DSA。

rsa：公钥算法为 RSA。

prefer-ctos-cipher：客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

3des：3des-cbc 加密算法。

aes128：aes128-cbc 加密算法。

des：des-cbc 加密算法。

prefer-ctos-hmac：客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

md5：HMAC 算法 hmac-md5。

md5-96：HMAC 算法 hmac-md5-96。

sha1：HMAC 算法 hmac-sha1。

sha1-96：HMAC 算法 hmac-sha1-96。

prefer-kex：密钥交换首选算法，缺省算法为 **dh-group-exchange**。

dh-group-exchange：密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1：密钥交换算法 diffie-hellman-group1-sha1。

dh-group14：密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher：服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac：服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**

【描述】

ssh2 ipv6 命令用来建立 SSH 客户端和 IPv6 服务器端的连接，并指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法。

需要注意的是，当服务器端指定客户端的认证方式为 publickey 认证时，客户端需要读取本地的私钥进行验证。由于 publickey 认证可以采用 RSA 和 DSA 两种加密算法，所以需要用 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。缺省情况下，加密算法为 DSA。

【举例】

登录地址为 2000::1 的远程 SSH2 服务器，具体加密算法配置如下：

- 首选密钥交换算法为 **dh-group1**；
- 服务器到客户端的首选加密算法为 **aes128**；
- 客户端到服务器的首选 HMAC 算法为 **md5**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
```

1.3 SFTP服务器端配置命令

1.3.1 sftp server enable

【命令】

sftp server enable

undo sftp server enable

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

无

【描述】

sftp server enable 命令用来启动 SFTP 服务器。**undo sftp server enable** 命令用来关闭 SFTP 服务器。

缺省情况下，SFTP 服务器处于关闭状态。

相关配置可参考命令 **display ssh server**。

【举例】

启动 SFTP 服务器。

```
<Sysname> system-view
[Sysname] sftp server enable
```

1.3.2 sftp server idle-timeout

【命令】

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

time-out-value：超时时间，取值范围为 1～35791，单位为分钟。

【描述】

sftp server idle-timeout 命令用来在 SFTP 服务器端设置 SFTP 用户连接的空闲超时时间。**undo sftp server idle-timeout** 命令用来恢复缺省情况。

缺省情况下，SFTP 用户连接的空闲超时时间为 10 分钟。

相关配置可参考命令 **display ssh server**。

【举例】

设置 SFTP 用户连接的空闲超时时间为 500 分钟。

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

1.4 SFTP客户端配置命令

1.4.1 bye

【命令】

bye

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

无

【描述】

bye 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

该命令功能与 **exit**，**quit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp-client> bye
Bye
Connection closed.
<Sysname>
```

1.4.2 cd

【命令】

cd [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-path：服务器上的路径名。

【描述】

cd 命令用来改变远程 SFTP 服务器上的工作路径。

如果没有指定 *remote-path*，则显示当前工作路径。

说明

- 命令“cd ..”用来返回到上一级目录。
- 命令“cd /”用来返回到系统的根目录。

【举例】

改变工作路径到 new1。

```
sftp-client> cd new1
Current Directory is:
/new1
```

1.4.3 cdup

【命令】

cdup

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

无

【描述】

cdup 命令用来返回到上一级目录。

【举例】

从当前工作目录/new1 返回到上一级目录。

```
sftp-client> cdup
Current Directory is:
/
```

1.4.4 delete

【命令】

delete *remote-file*&<1-10>

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-file&<1-10>：服务器上的文件名。&<1-10>表示最多可以输入 10 个文件名，每个文件名之间用空格分隔。

【描述】

delete 命令用来删除 SFTP 服务器上指定的文件。

该命令和 **remove** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

1.4.5 dir

【命令】

dir [**-a** | **-l**] [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

-a：显示指定目录下文件及文件夹的名称。

-l：以列表的形式显示指定目录下文件及文件夹的详细信息。

remote-path：查询的目录名。

【描述】

dir 命令用来显示指定目录下文件及文件夹的信息。

如果没有指定**-a** 和**-l** 参数，则以列表的形式显示指定目录下文件及文件夹的详细信息。

如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

该命令功能与 **ls** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息。

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

1.4.6 display sftp client source

【命令】

display sftp client source [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display sftp client source 命令用来显示当前为 SFTP 客户端设置的源 IP 地址或者源接口。

如果没有为 SFTP 客户端指定源地址和源接口，则提示尚未指定。

相关配置可参考命令 **sftp client source**。

【举例】

显示 SFTP 客户端的源 IP 地址。

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

1.4.7 exit

【命令】

exit

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

无

【描述】

exit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

该命令功能与 **bye**，**quit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp-client> exit
Bye
Connection closed.
<Sysname>
```

1.4.8 get

【命令】

get *remote-file* [*local-file*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-file：远程 SFTP 服务器上的文件名。

local-file：本地文件名。

【描述】

get 命令用来从远程服务器上下载文件并存储在本地。

如果没有指定本地文件名，则认为本地文件与远程 SFTP 服务器上的文件同名。

【举例】

下载 temp1.c 文件，并以 temp.c 文件名保存。

```
sftp-client> get temp1.c temp.c
Remote  file:/temp1.c --->  Local file: temp.c
Downloading file successfully ended
```

1.4.9 help

【命令】

help [**all** | *command-name*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

all：显示所有命令的名字。

command-name：命令名。

【描述】

help 命令用来显示 SFTP 客户端命令的帮助信息。

如果没有指定参数，系统将显示所有命令的名字。

【举例】

查看命令 **get** 的帮助信息。

```
sftp-client> help get
get remote-path [local-path]  Download file.Default local-path is the same
                              as remote-path
```

1.4.10 ls

【命令】

ls [**-a** | **-l**] [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

-a：显示指定目录下文件及文件夹的名称。

-l：以列表的形式显示指定目录下文件及文件夹的详细信息。

remote-path：查询的目录名。

【描述】

ls 命令用来显示指定目录下文件及文件夹的信息。

如果没有指定**-a** 和**-l** 参数，则以列表的形式显示指定目录下文件及文件夹的详细信息。

如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

该命令功能与 **dir** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息。

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

1.4.11 mkdir

【命令】

mkdir *remote-path*

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-path：远程 SFTP 服务器上的目录名。

【描述】

mkdir 命令用来在远程 SFTP 服务器上创建新的目录。

【举例】

在远程 SFTP 服务器上建立目录 test。

```
sftp-client> mkdir test
New directory created
```

1.4.12 put

【命令】

put *local-file* [*remote-file*]

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

local-file：本地的文件名。

remote-file：远程 SFTP 服务器上的文件名。

【描述】

put 命令用来将本地的文件上传到远程 SFTP 服务器。

如果没有指定远程服务器上的文件名，则认为服务器上的文件与本地文件同名。

【举例】

将本地 temp.c 文件上传到远程 SFTP 服务器，并以 temp1.c 文件名保存。

```
sftp-client> put temp.c temp1.c
Local file:temp.c --->  Remote file: /temp1.c
Uploading file successfully ended
```

1.4.13 pwd

【命令】

pwd

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

无

【描述】

pwd 命令用来显示远程 SFTP 服务器上的当前工作目录。

【举例】

显示远程 SFTP 服务器上的当前工作目录。

```
sftp-client> pwd
/
```

1.4.14 quit

【命令】

quit

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

无

【描述】

quit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

该命令功能与 **bye**，**exit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp-client> quit
Bye
Connection closed.
<Sysname>
```

1.4.15 remove

【命令】

remove *remote-file*&<1-10>

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-file&<1-10>：服务器上的文件名。&<1-10>表示最多可以输入 10 个文件名，每个文件名之间用空格分隔。

【描述】

remove 命令用来删除 SFTP 服务器上指定的文件。

该命令和 **delete** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

1.4.16 rename

【命令】

rename *oldname newname*

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

oldname：原文件名或者目录名。

newname：新文件名或者目录名。

【描述】

rename 命令用来改变 SFTP 服务器上指定的文件或者目录的名字。

【举例】

将 SFTP 服务器上的文件 temp1.c 改名为 temp2.c。

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

1.4.17 rmdir

【命令】

rmdir *remote-path*&<1-10>

【视图】

SFTP 客户端视图

【缺省级别】

3：管理级

【参数】

remote-path&<1-10>：远程 SFTP 服务器上的目录名。&<1-10>表示最多可以输入 10 个目录名，每个文件名之间用空格分隔。

【描述】

rmdir 命令用来删除 SFTP 服务器上指定的目录。

【举例】

删除 SFTP 服务器上当前工作目录下的 temp1 目录。

```
sftp-client> rmdir temp1
Directory successfully removed
```

1.4.18 sftp

【命令】

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

【视图】

用户视图

【缺省级别】

3：管理级

【参数】

server：服务器 IPv4 地址或主机名称，为 1～20 个字符的字符串，不区分大小写。

port-number：服务器端口号，取值范围为 0～65535，缺省值为 22。

vpn-instance *vpn-instance-name*：服务器所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示服务器位于公网中。

identity-key：publickey 认证采用的公钥算法，缺省算法为 **dsa**。

dsa：公钥算法为 DSA。

rsa：公钥算法为 RSA。

prefer-ctos-cipher：客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

3des：3des-cbc 加密算法。

aes128：aes128-cbc 加密算法。

des：des-cbc 加密算法。

prefer-ctos-hmac：客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

md5：HMAC 算法 hmac-md5。

md5-96：HMAC 算法 hmac-md5-96。

sha1：HMAC 算法 hmac-sha1。

sha1-96：HMAC 算法 hmac-sha1-96。

prefer-kex：密钥交换首选算法，缺省算法为 **dh-group-exchange**。

dh-group-exchange：密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1：密钥交换算法 diffie-hellman-group1-sha1。

dh-group14：密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher：服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac：服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【描述】

sftp 命令用来与远程 IPv4 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

需要注意的是，当服务器端指定客户端的认证方式为 publickey 认证时，客户端需要读取本地的私钥进行验证。由于 publickey 认证可以采用 RSA 和 DSA 两种加密算法，所以需要用 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。缺省情况下，加密算法为 DSA。

【举例】

连接 IP 地址为 10.1.1.2 的 SFTP 服务器，采用的算法为：

首选密钥交换算法为 **dh-group1**；

服务器到客户端的首选加密算法为 **aes128**；

客户端到服务器的首选 HMAC 算法为 **md5**；

服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5
prefer-stoc-hmac sha1-96
Input Username:
```

1.4.19 sftp client ipv6 source

【命令】

sftp client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo sftp client ipv6 source

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

ipv6 *ipv6-address*：源 IPv6 地址。

interface *interface-type interface-number*：源接口类型与源接口编号。

【描述】

sftp client ipv6 source 命令用来为 SFTP 客户端指定源 IPv6 地址或源接口。**undo sftp client ipv6 source** 命令用来取消指定的源 IPv6 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SFTP 服务器。

相关配置可参考命令 **display sftp client source**。

【举例】

指定 SFTP 客户端的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

1.4.20 sftp client source

【命令】

sftp client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo sftp client source

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

ip *ip-address*：源 IPv4 地址。

interface *interface-type interface-number*：源接口类型与源接口编号。

【描述】

sftp client source 命令用来为 SFTP 客户端指定源 IPv4 地址或源接口。**undo sftp client source** 命令用来取消指定的源 IPv4 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SFTP 服务器。

相关配置可参考命令 **display sftp client source**。

【举例】

指定 SFTP 客户端的源 IP 地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

1.4.21 sftp ipv6

【命令】

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

【视图】

用户视图

【缺省级别】

3：管理级

【参数】

server：服务器的 IPv6 地址或主机名称，为 1～46 个字符的字符串，不区分大小写。

port-number：服务器的端口号，取值范围为 0～65535，缺省值为 22。

vpn-instance *vpn-instance-name*：服务器所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示服务器位于公网中。

identity-key：publickey 认证采用的公钥算法，缺省算法为 **dsa**。

dsa：公钥算法为 DSA。

rsa：公钥算法为 RSA。

prefer-ctos-cipher：客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

3des：3des-cbc 加密算法。

aes128：aes128-cbc 加密算法。

des：des-cbc 加密算法。

prefer-ctos-hmac：客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

md5：HMAC 算法 hmac-md5。

md5-96：HMAC 算法 hmac-md5-96。

sha1：HMAC 算法 hmac-sha1。

sha1-96：HMAC 算法 hmac-sha1-96。

prefer-kex：密钥交换首选算法，缺省算法为 **dh-group-exchange**。

dh-group-exchange：密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1：密钥交换算法 diffie-hellman-group1-sha1。

dh-group14：密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher：服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac：服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【描述】

sftp ipv6 命令用来与远程 IPv6 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

需要注意的是，当服务器端指定客户端的认证方式为 publickey 认证时，客户端需要读取本地的私钥进行验证。由于 publickey 认证可以采用 RSA 和 DSA 两种加密算法，所以需要用 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。缺省情况下，加密算法为 DSA。

【举例】

连接 IPv6 地址为 2:5::8:9 的 SFTP 服务器，采用的加密算法为：

首选密钥交换算法为 **dh-group1**；

服务器到客户端的首选加密算法为 **aes128**；

客户端到服务器的首选 HMAC 算法为 **md5**；

服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
Input Username:
```