目 录

1 公钥管理

1.1 公钥管理配置命令

1.1.1 display public-key local public

【命令】

display public-key local { **dsa** | **rsa** } **public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

dsa：显示 DSA 本地密钥对中的公钥信息。

rsa：显示 RSA 本地密钥对中的公钥信息。

|：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 public-key local public 命令用来显示本地非对称密钥对中的公钥信息。

相关配置可参考命令 **public-key local create**。

【举例】

显示本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public

=====================================================
Time of Key pair created: 19:59:16  2007/10/25
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A633BA0F1DB01F84E
B51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D049143656F1287502C06D39D39F28F0F5
CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCDB5DB620CD1F471401B7117139702348444A2D89004
97A87B8D5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF30203010001
```

```
=====================================================
Time of Key pair created: 19:59:17  2007/10/25
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2AACC7B2AE12B2B
1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27E054BFAA0A85E113FBDE751EE0EC
EF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

显示本地 DSA 密钥对中的公钥信息。

```
<Sysname> display public-key local dsa public

=====================================================
Time of Key pair created: 20:00:16  2007/10/25
Key name: HOST_KEY
Key type: DSA Encryption Key
=====================================================
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F0A4
23F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26CCB987
723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F0678D7722B53
41C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F
0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B
20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B612391C76C1FB2
E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF
0381850002818100CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB374D677A7A6124EBABD59FE4
8796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F72E80DBE337CB29989A23378EB21C38EE083F11ED6DC8
D4DBE001BA85450CEA071C2A471C83761E4CF32C174B418612CDD597B441F0CAA05DC01CB93A0ABB247C06FB
A4C79054
```

表1-1 display public-key local public 命令显示信息描述表

字段	描述
Time of Key pair created	本地非对称密钥对产生时间
Key name	密钥名称，取值包括： • HOST_KEY：主机公钥 • SERVER_KEY：服务器公钥。只有密钥类型为 RSA 时，才会存在 SERVER_KEY
Key type	密钥类型，取值包括： • RSA Encryption Key：密钥类型为 RSA • DSA Encryption Key：密钥类型为 DSA
Key code	公钥数据

1.1.2 display public-key peer

【命令】

display public-key peer [**brief** | **name** *publickey-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

brief：显示保存在本地的所有远端主机公钥的简明信息。

name *publickey-name*：显示保存在本地的指定远端主机公钥的详细信息，*publickey-name* 为远端主机公钥的名称，为 1～64 个字符的字符串，区分大小写。

|：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 public-key peer 命令用来显示保存在本地的远端主机的公钥信息。

如果没有指定任何参数，则显示所有保存在本地的远端主机公钥的详细信息。

可以通过 **public-key peer** 命令或 **public-key peer import sshkey** 命令将远端主机的公钥配置到本地。

相关配置可参考命令 **public-key peer** 和 **public-key peer import sshkey**。

【举例】

显示保存在本地的密钥名称为 idrsa 的远端主机公钥的详细信息。

```
<Sysname> display public-key peer name idrsa
=====================================
  Key Name  : idrsa
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B003081870281810090C46A8710216CEC0C01C7CE136BA76
C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB7442D563
93BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A775
7C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

表1-2 display public-key peer name 命令显示信息描述表

字段	描述
Key Name	远端主机公钥的名称
Key Type	密钥类型，取值包括RSA和DSA
Key Module	密钥模数的长度，单位为bit
Key Code	公钥数据

显示保存在本地的所有远端主机公钥的简明信息。

```
<Sysname> display public-key peer brief
Type   Module   Name
--------------------------
RSA    1024     idrsa
DSA    1024     10.1.1.1
```

表1-3 display public-key peer brief 命令显示信息描述表

字段	描述
Type	密钥类型，取值包括RSA和DSA
Module	密钥模数的长度，单位为比特
Name	远端主机公钥的名称

1.1.3 peer-public-key end

【命令】

peer-public-key end

【视图】

公钥视图

【缺省级别】

2：系统级

【参数】

无

【描述】

peer-public-key end 命令用来从公钥视图退回到系统视图。

相关配置可参考命令 **public-key peer**。

【举例】

退出公钥视图。

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
```

```
[Sysname]
```

1.1.4 public-key-code begin

【命令】

public-key-code begin

【视图】

公钥视图

【缺省级别】

2：系统级

【参数】

无

【描述】

public-key-code begin 命令用来进入公钥编辑视图。

进入公钥编辑视图后，可以开始输入密钥数据。在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。保存公钥数据时，将删除空格和回车符。

需要注意的是，输入的密钥数据必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的密钥数据。

相关配置可参考命令 **public-key peer** 和 **public-key-code end**。

【举例】

进入公钥编辑视图，输入密钥。

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
```

1.1.5 public-key-code end

【命令】

public-key-code end

【视图】

公钥编辑视图

【缺省级别】

2：系统级

【参数】

无

【描述】

public-key-code end 命令用来从公钥编辑视图退回到公钥视图，并保存用户输入的公钥。

执行此命令后，结束公钥的编辑过程，系统自动保存配置的公钥。在存储之前，会进行密钥合法性的检测：

- 如果用户配置的公钥字符串不满足格式要求，那么将会显示相关提示信息，用户配置的密钥将被丢弃，本次配置失败；
- 如果用户配置的公钥字符串合法，则保存该公钥。

相关配置可参考命令 **public-key peer** 和 **public-key-code begin**。

【举例】

退出公钥编辑视图，并保存用户配置的公钥。

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

1.1.6 public-key local create

【命令】

public-key local create { **dsa** | **rsa** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dsa：本地密钥对类型为 DSA。

rsa：本地密钥对类型为 RSA。

【描述】

public-key local create 命令用来生成本地非对称密钥对。

缺省情况下，不存在任何非对称密钥对。

需要注意的是：

- 执行此命令后，当本地非对称密钥对类型为 DSA 或 RSA 时，会提示输入密钥模数的长度。密钥模数的最小长度为 512 比特，最大长度为 2048 比特，缺省长度为 1024 比特。如果已存在相应类型的密钥对，则需要用户确认是否覆盖原有密钥对。
- 在 FIPS 模式下执行此命令后，当本地非对称密钥对类型为 DSA 时，密钥模数的长度至少为 1024 比特；当本地非对称密钥对类型为 RSA 时，密钥模数的长度必须为 2048 比特。
- 执行此命令后，生成的密钥对将保存在设备中，设备重启后密钥不会丢失。

相关配置可参考命令 **public-key local destroy** 和 **display public-key local public**。

【举例】

生成本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++
+++++++
+++++++++
+++
```

生成本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++.++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

1.1.7 public-key local destroy

【命令】

public-key local destroy { **dsa** | **rsa** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dsa：本地密钥对类型为 DSA。

rsa：本地密钥对类型为 RSA。

【描述】

public-key local destroy 命令用来销毁本地非对称密钥对。

相关配置可参考命令 **public-key local create**。

【举例】

销毁本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
```

销毁本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] :y
```

1.1.8 public-key local export dsa

【命令】

public-key local export dsa { **openssh** | **ssh2** } [*filename*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

openssh：主机公钥格式为 OpenSSH。

ssh2：主机公钥格式为 SSH2.0。

filename：指定导出公钥存储的文件名。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【描述】

public-key local export dsa 命令用来根据指定格式显示本地 DSA 主机公钥或将其导出到指定文件。

如果执行本命令时没有指定文件名，则按照指定格式显示本地 DSA 主机公钥；如果指定了文件名，则将本地 DSA 主机公钥导出到指定文件并保存。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

相关配置可参考命令 **public-key local create** 和 **public-key local destroy**。

【举例】

以 OpenSSH 格式导出本地 DSA 主机公钥，文件名为 key.pub。

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

以 SSH2.0 格式显示本地 DSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20070625"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLo2/RyGqDJIqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示本地 DSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLo2/RyGqDJIqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22 dsa-key
```

1.1.9 public-key local export rsa

【命令】

public-key local export rsa { **openssh** | **ssh1** | **ssh2** } [*filename*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

openssh：主机公钥格式为 OpenSSH。

ssh1：主机公钥格式为 SSH1.5。

ssh2：主机公钥格式为 SSH2.0。

filename：指定导出公钥存储的文件名。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【描述】

public-key local export rsa 命令用来根据指定格式显示本地 RSA 主机公钥或将其导出到指定文件。

如果执行本命令时没有指定文件名，则显示本地 RSA 主机公钥；如果指定了文件名，则将本地 RSA 主机公钥导出到指定文件并保存。

SSH1.5、SSH2.0 和 OpenSSH 是三种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

相关配置可参考命令 **public-key local create** 和 **public-key local destroy**。

【举例】

以 OpenSSH 格式导出本地 RSA 主机公钥，文件名为 key.pub。

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

以 SSH2.0 格式显示本地 RSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20070625"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+u1riz+1LcwVTs51Q==
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示本地 RSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+u1riz+1LcwVTs51Q== rsa-key
```

1.1.10 public-key peer

【命令】

public-key peer *keyname*

undo public-key peer *keyname*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

keyname：远端主机公钥的名称，为 1～64 个字符的字符串，区分大小写。

【描述】

public-key peer 命令用来指定远端主机公钥的名称，并进入公钥视图。**undo public-key peer** 命令用来删除远端主机公钥。

通过手工配置方式创建远端主机公钥时，用户需要事先获取并记录远端主机十六进制形式的公钥，并在本地设备上执行以下操作：

(1) 执行本命令和 **public-key-code begin** 命令进入公钥编辑视图。

(2) 在公钥编辑视图，手工输入远端主机的公钥。

(3) 执行 **public-key-code end** 命令，自动保存输入的远端主机公钥，并退回到公钥视图。

(4) 执行 **peer-public-key end** 命令，从公钥视图退回到系统视图。

相关配置可参考命令 **public-key-code begin**、**public-key-code end**、**peer-public-key end** 和 **display public-key peer**。

【举例】

指定远端主机公钥名称为 key1，并进入公钥视图。

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key]
```

1.1.11 public-key peer import sshkey

【命令】

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

keyname：公钥名，为 1～64 个字符的字符串，区分大小写。

filename：指定导入公钥数据的文件名。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【描述】

public-key peer import sshkey 命令用来配置从公钥文件中导入远端主机的公钥。**undo public-key peer** 命令用来删除远端主机公钥。

执行本命令后，系统会自动对指定的公钥文件中的公钥进行格式转换（转换为 PKCS 标准编码形式），并将该远端主机的公钥保存到本地设备。这种方式需要远端主机事先将其公钥文件保存到本地设备（例如，通过 FTP 或 TFTP，以二进制方式将远端主机的公钥文件保存到本地设备）。

目前，设备能够自动识别的公钥格式为 SSH1.5、SSH2.0 和 OpenSSH。

相关配置可参考命令 **display public-key peer**。

【举例】

配置从公钥文件 key.pub 中导入远端主机的公钥，公钥名称为 key2。

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```