# puppet 实战-puppet cert 命令的中文帮助信息详解

puppet cert 用于管理本地证书、查看未签名证书、签署证书、废除证书、清除证书

命令： puppet cert #证书颁发，用于签署证书

常用的操作如下：

```
clean #清除，用于清除证书
fingerprint #打印证书指纹
generate #生成客户端证书
list #查看认证客户列表
print #打印主机证书的全文信息
revoke #废除已认证的主机
sign #签署认证
verify #验证本地指定的认证
```

命令参数如下：

```
--all #执行所有操作，包括'sign','clean','list','fingerprint',
--digest #设置证书指纹加密的方式，取决于 openssl 版本
--debug #启用完整的调试模式
--help #查看帮助
--verbose #显示详细信息
--version #显示版本

[root@linuxmaster1poc ~]# puppet help cert

puppet-cert(8) -- Manage certificates and requests
========

SYNOPSIS
--------
Standalone certificate authority. Capable of generating certificates,
but mostly used for signing certificate requests from puppet clients.


USAGE
-----
puppet cert <action> [-h|--help] [-V|--version] [-d|--debug] [-v|--verbose]
  [--digest <digest>] [<host>]


DESCRIPTION
-----------
Because the puppet master service defaults to not signing client
```

```
certificate requests, this script is available for signing outstanding
requests. It can be used to list outstanding requests and then either
sign them individually or sign all of them.

ACTIONS
-------

Every action except 'list' and 'generate' requires a hostname to act on,
unless the '--all' option is set.

* clean:
  Revoke a host's certificate (if applicable) and remove all files
  related to that host from puppet cert's storage. This is useful when
  rebuilding hosts, since new certificate signing requests will only be
  honored if puppet cert does not have a copy of a signed certificate
  for that host. If '--all' is specified then all host certificates,
  both signed and unsigned, will be removed.

* fingerprint:
  Print the DIGEST (defaults to md5) fingerprint of a host's
  certificate.

* generate:
  Generate a certificate for a named client. A certificate/keypair will
  be generated for each client named on the command line.

* list:
  List outstanding certificate requests. If '--all' is specified, signed
  certificates are also listed, prefixed by '+', and revoked or invalid
  certificates are prefixed by '-' (the verification outcome is printed
  in parenthesis).

* print:
  Print the full-text version of a host's certificate.

* revoke:
  Revoke the certificate of a client. The certificate can be specified either
  by its serial number (given as a hexadecimal number prefixed by '0x') or by its
  hostname. The certificate is revoked by adding it to the Certificate Revocation
  List given by the 'cacrl' configuration option. Note that the puppet master
  needs to be restarted after revoking certificates.

* sign:
  Sign an outstanding certificate request.
```

```
* verify:
  Verify the named certificate against the local CA certificate.


OPTIONS
-------
Note that any configuration parameter that's valid in the configuration
file is also a valid long argument. For example, 'ssldir' is a valid
configuration parameter, so you can specify '--ssldir <directory>' as an
argument.

See the configuration file documentation at
http://docs.puppetlabs.com/references/stable/configuration.html for the
full list of acceptable parameters. A commented list of all
configuration options can also be generated by running puppet cert with
'--genconfig'.

* --all:
  Operate on all items. Currently only makes sense with the 'sign',
  'clean', 'list', and 'fingerprint' actions.

* --digest:
  Set the digest for fingerprinting (defaults to md5). Valid values
  depends on your openssl and openssl ruby extension version, but should
  contain at least md5, sha1, md2, sha256.

* --debug:
  Enable full debugging.

* --help:
  Print this help message

* --verbose:
  Enable verbosity.

* --version:
  Print the puppet version number and exit.


EXAMPLE
-------
    $ puppet cert list
    culain.madstop.com
    $ puppet cert sign culain.madstop.com



AUTHOR
------
Luke Kanies



COPYRIGHT
---------
Copyright (c) 2011 Puppet Labs, LLC Licensed under the Apache 2.0 License

[root@linuxmaster1poc ~]#
```

**eg. 查看所有签名和未签名的证书 备注：**符号+表示已经签署过证书

```
[root@linuxmaster1poc ~]# puppet cert list --all
+ "puppet_linux57poc.dev.shanghaigm.com"
(4B:1D:76:C6:F2:9D:53:7D:85:BC:8F:51:94:0D:81:F7)
+ "puppet_linux58poc.dev.shanghaigm.com"
(A8:1C:79:CC:66:39:4E:E0:B4:A7:3C:5A:87:6E:80:53)
+ "puppet_linux64poc.dev.shanghaigm.com"
(B5:A8:5F:7A:5D:9B:9B:01:89:14:82:0A:7D:E1:8B:E0)
+ "puppetagent-win"
(20:F6:13:A2:DE:40:54:37:31:4A:B6:6D:E2:0E:C2:51)
+ "puppetmaster.dev.shanghaigm.com"
(13:8C:4B:5C:0E:D7:37:83:18:22:DF:7D:A7:BD:82:9B)
```

**eg. 删除某一个证书**

```
[root@linuxmaster1poc ~]# puppet cert clean puppet_linux57poc.dev.shanghaigm.com
notice: Revoked certificate with serial 5
notice: Removing file Puppet::SSL::Certificate puppet_linux57poc.dev.shanghaigm.com
at '/etc/puppet/ssl/ca/signed/puppet_linux57poc.dev.shanghaigm.com.pem'
notice: Removing file Puppet::SSL::Certificate puppet_linux57poc.dev.shanghaigm.com
at '/etc/puppet/ssl/certs/puppet_linux57poc.dev.shanghaigm.com.pem'
```

**eg. 注册一个新的证书**

节点先删除证书

```
[root@linux57poc modules]# rm -rf /var/lib/puppet/ssl/*
[root@linux57poc modules]# puppet agent -t
info: Creating a new SSL key for puppet_linux57poc.dev.shanghaigm.com
info: Caching certificate for ca
info: Creating a new SSL certificate request for
puppet_linux57poc.dev.shanghaigm.com
```

```
info: Certificate Request fingerprint (md5):
08:19:B4:15:F5:38:63:1B:F8:CD:21:03:DC:AF:15:46
Exiting; no certificate found and waitforcert is disabled
```

master 端查看节点未注册的证书

```
[root@linuxmaster1poc ~]# puppet cert list
  "puppet_linux57poc.dev.shanghaigm.com"
(08:19:B4:15:F5:38:63:1B:F8:CD:21:03:DC:AF:15:46) #未注册
[root@linuxmaster1poc ~]# puppet cert list --all
  "puppet_linux57poc.dev.shanghaigm.com"
(08:19:B4:15:F5:38:63:1B:F8:CD:21:03:DC:AF:15:46) #未注册
+ "puppet_linux58poc.dev.shanghaigm.com"
(A8:1C:79:CC:66:39:4E:E0:B4:A7:3C:5A:87:6E:80:53)
+ "puppet_linux64poc.dev.shanghaigm.com"
(B5:A8:5F:7A:5D:9B:9B:01:89:14:82:0A:7D:E1:8B:E0)
+ "puppetagent-win"
(20:F6:13:A2:DE:40:54:37:31:4A:B6:6D:E2:0E:C2:51)
+ "puppetmaster.dev.shanghaigm.com"
(13:8C:4B:5C:0E:D7:37:83:18:22:DF:7D:A7:BD:82:9B)
```

注册单个节点证书

```
[root@linuxmaster1poc ~]# puppet cert sign puppet_linux57poc.dev.shanghaigm.com
notice: Signed certificate request for puppet_linux57poc.dev.shanghaigm.com
notice: Removing file Puppet::SSL::CertificateRequest
puppet_linux57poc.dev.shanghaigm.com at
'/etc/puppet/ssl/ca/requests/puppet_linux57poc.dev.shanghaigm.com.pem'
```

更多详细信息可参考 http://kisspuppet.com/categories/Puppet_Basics/

——————————————————————————————————

为了能够和大家更好的交流和学习 Puppet，本人 2014 年又新开辟了微信公众号进行交流学习，目前已经有 300 多人同时收听，喜欢 Puppet 的大神们可自行加入哦。

如果你有好的有关 Puppet 的咨询也可以给我投稿，投稿地址：admin@kisspuppet.com

**微信公众号：“puppet2014”，可搜索加入，也可以扫描以下二维码**