目 录

1 PKI配置命令

1.1 PKI配置命令

1.1.1 attribute

【命令】

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*

undo attribute { *id* | **all** }

【视图】

证书属性组视图

【缺省级别】

2：系统级

【参数】

id：证书属性规则序号，取值范围为 1～16。

alt-subject-name：表示证书备用主题名。

fqdn：指定实体的 FQDN。

ip：指定实体的 IP 地址。

issuer-name：表示证书颁发者名。

subject-name：表示证书主题名。

dn：指定实体的 DN。

ctn：表示包含操作。

equ：表示相等操作。

nctn：表示不包含操作。

nequ：表示不等操作。

attribute-value：表示证书属性值，为 1～128 个字符的字符串，不区分大小写。

all：表示所有证书属性规则。

【描述】

attribute 命令用来配置证书颁发者名、证书主题名以及备用主题名的属性规则。**undo attribute** 命令用来删除一个或者所有证书的属性规则。

缺省情况下，对证书的颁发者名、主题名以及备用主题名没有限制。

需要注意的是，证书备用主题名属性不会以域名的方式出现，所以在证书备用主题名属性的规则配置中没有出现 **dn**。

【举例】

创建一个证书属性规则。该规则定义，主题名的 DN 包含字符串 abc。

```
<Sysname> system-view
```

```
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

创建一个证书属性规则。该规则定义，颁发者名称中的 FQDN 不等于字符串 abc。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

创建一个证书属性规则。该规则定义，主题备用名称中的 IP 地址不等于 10.0.0.1。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

1.1.2 ca identifier

【命令】

ca identifier *name*

undo ca identifier

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

name：设备信任的 CA 的名称，为 1～63 个字符的字符串，不区分大小写。

【描述】

ca identifier 命令用来指定设备信任的 CA 的名称。**undo ca identifier** 命令用来删除设备信任的 CA。

缺省情况下，未指定设备信任的 CA。

该设备证书的申请、获取、废除及查询均通过该 CA 执行。

【举例】

指定设备信任的 CA 的名称为 new-ca。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

1.1.3 certificate request entity

【命令】

certificate request entity *entity-name*

undo certificate request entity

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

entity-name：申请证书的实体所用名称，为 1～15 个字符的字符串，不区分大小写。

【描述】

certificate request entity 命令用来指定申请证书的实体名称。**undo certificate request entity** 命令用来取消申请证书所用的实体名称。

缺省情况下，未指定设备申请证书所使用的实体名称。

相关配置可参考命令 **pki entity**。

【举例】

指定设备申请证书时使用实体 entity1。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request entity entity1
```

1.1.4 certificate request from

【命令】

certificate request from { **ca** | **ra** }

undo certificate request from

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

ca：表示实体从 CA 注册申请证书。

ra：表示实体从 RA 注册申请证书。

【描述】

certificate request from 命令用来为实体配置证书申请的注册受理机构。**undo certificate request from** 命令用来取消指定的证书申请注册受理机构。

缺省情况下，未指定证书申请的注册受理机构。

【举例】

指定实体从 CA 注册申请证书。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

1.1.5 certificate request mode

【命令】

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] * | **manual** }

undo certificate request mode

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

auto：表示用自动方式申请证书。

key-length：指定 RSA 密钥长度，取值范围为 512～2048，单位为 bit，缺省值为 1024bit。

cipher：表示密码为密文显示。

simple：表示密码为明文显示。

password：指定吊销证书时使用的密码，为 1～31 个字符的字符串，区分大小写。

manual：表示用手工方式申请证书。

【描述】

certificate request mode 命令用来配置证书申请方式。**undo certificate request mode** 命令用来恢复缺省情况。

缺省情况下，证书申请为手工方式。

如果是自动方式，则在本地没有自己的证书时自动向注册机构进行申请，但不会在证书快要过期时以及证书过期之后自动申请新的证书。如果为手工方式，则需要手工完成各项证书申请工作。

相关配置可参考命令 **pki request-certificate**。

【举例】

指定证书申请为自动方式。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

1.1.6 certificate request polling

【命令】

certificate request polling { **count** *count* | **interval** *minutes* }

undo certificate request polling { **count** | **interval** }

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

count *count*：表示证书申请状态的查询次数。*count* 表示查询次数，取值范围为 1～100。

interval *minutes*：表示证书申请状态的查询周期。*minutes* 表示查询周期，取值范围为 5～168，单位为分钟。

【描述】

certificate request polling 命令用来配置证书申请状态的查询周期和次数。**undo certificate request polling** 命令用来恢复缺省情况。

缺省情况下，证书申请状态的查询周期为 20 分钟、每一个周期查询 50 次。

实体在发送证书申请后，如果 CA 采用手工验证申请，证书的发布会需要很长时间。实体需要定期发送状态查询，以便在证书签发后能及时获取到证书。

相关配置可参考命令 **display pki certificate**。

【举例】

指定状态查询周期为 15 分钟、每一个周期查询 40 次。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

1.1.7 certificate request url

【命令】

certificate request url *url-string*

undo certificate request url

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

url-string：表示证书申请的注册机构服务器的 URL，为 1～127 个字符的字符串，不区分大小写。内容包括服务器位置及 CA 的 CGI 命令接口脚本位置，格式为 http://*server_location/ca_script_location*。其中，*server_location* 目前仅支持 IP 地址的表示方式，不支持域名解析，*ca_script_location* 是 CA 在服务器主机上的应用程序脚本的路径。

【描述】

certificate request url 命令用来配置设备通过 SCEP 进行证书申请的注册机构服务器的 URL。**undo certificate request url** 命令用来删除证书申请服务器的 URL。

缺省情况下，未指定注册服务器的 URL。

【举例】

指定注册服务器的 URL。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

1.1.8 common-name

【命令】

common-name *name*

undo common-name

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

name：实体的通用名称，为 1～31 个字符的字符串，不区分大小写，不能包含逗号。

【描述】

common-name 命令用来配置实体的通用名，比如用户名称。**undo common-name** 命令用来删除实体的通用名。

缺省情况下，未指定实体通用名。

【举例】

配置实体的通用名为 test。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] common-name test
```

1.1.9 country

【命令】

country *country-code-str*

undo country

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

country-code-str：两字符国家代码，不区分大小写。

【描述】

country 命令用来指定实体所属的国家代码，代码用标准的两字符代码，例如中国为“CN”。**undo country** 命令用来删除实体所属的国家代码。

缺省情况下，未指定实体所属国家代码。

【举例】

配置实体所属的国家代码为 CN。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

1.1.10 crl check

【命令】

crl check { **disable | enable** }

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

disable：禁止 CRL 检查。

enable：使能 CRL 检查。

【描述】

crl check 命令用来使能或者禁止 CRL 检查。

缺省情况下，CRL 检查处于开启状态。

CRL 是由 CA 签发的文件，其中包含所有被 CA 废除的证书列表，表明某些证书已被废除。废除有可能发生在证书有效期结束之前。CRL 检查的目的是查看实体的证书是否被 CA 废除，若检查结果表明实体证书已被废除，那么该证书就不再被其它实体信任。

【举例】

禁止 CRL 检查。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

1.1.11 crl update-period

【命令】

crl update-period *hours*

undo crl update-period

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

hours：指定更新周期，取值范围为 1～720，单位为小时。

【描述】

crl update-period 命令用来指定 CRL 的更新周期。**undo crl update-period** 命令用来恢复缺省情况。

缺省情况下，CRL 的更新周期由 CRL 文件中的下次更新域决定。

CRL 的更新周期是指使用证书的 PKI 实体从 CRL 存储服务器下载 CRL 的时间间隔。

【举例】

指定 CRL 的更新周期为 20 小时。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

1.1.12 crl url

【命令】

crl url *url-string*

undo crl url

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

url-string：表示 CRL 的发布点 URL，为 1～127 个字符的字符串，不区分大小写。格式为 ldap://*server_location*，或 http://*server_location*，其中，*server_location* 目前仅支持 IP 地址的表示方式，不支持域名解析。

【描述】

crl url 命令用来设置 CRL 发布点的 URL。**undo crl url** 命令用来删除该 URL。

缺省情况下，未指定 CRL 发布点的 URL。

需要注意的是，未配置 CRL 发布点的 URL 时，通过 SCEP 协议获取 CRL，该操作在获取 CA 证书和本地证书之后进行。

【举例】

指定 CRL 发布点的 URL。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0.30
```

1.1.13 display pki certificate

【命令】

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** } [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

ca：显示 CA 的证书。

local：显示本地的证书。

domain-name：指定证书所在的 PKI 域，为 1～15 个字符的字符串。

request-status：显示证书申请后的状态。

|：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 pki certificate 命令用来显示证书的内容或申请状态。

相关配置可参考命令 **pki retrieval-certificate**、**pki domain** 和 **certificate request polling**。

【举例】

显示本地证书。

```
<Sysname> display pki certificate local domain 1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@aabbcc.net
            C=CN
            ST=Country A
            L=City X
            O=abc
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2004 GMT
            Not After : Jan 20 09:07:21 2005 GMT
        Subject:
            C=CN
            ST=Country B
            L=City Y
```

```
        CN=pki test
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (512 bit)
            Modulus (512 bit):
                00D41D1F …
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
        DNS:hyf.xxyyzz.net
        X509v3 CRL Distribution Points:
        URI:http://1.1.1.1:447/myca.crl
        …           …
Signature Algorithm: md5WithRSAEncryption
    A3A5A447 4D08387D …
```

表1-1 display pki certificate 命令显示信息描述表

字段	描述
Version	证书版本号
Serial Number	证书序列号
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期
Subject	证书申请实体
Subject Public Key Info	申请实体公钥信息
X509v3 extensions	X509 版本 3 格式证书扩展属性
X509v3 CRL Distribution Points	X509 版本 3 格式 CRL 发布点

1.1.14 display pki certificate access-control-policy

【命令】

display pki certificate access-control-policy { *policy-name* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

policy-name：指定证书属性访问控制策略名，为 1～16 个字符的字符串。

all：所有证书属性访问控制策略。

|：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 pki certificate access-control-policy 命令用来显示证书属性访问控制策略信息。

【举例】

显示证书属性访问控制策略 mypolicy 的信息。

```
<Sysname> display pki certificate access-control-policy mypolicy
 access-control-policy name: mypolicy
     rule  1 deny    mygroup1
     rule  2 permit  mygroup2
```

表1-2 display pki certificate access-control-policy 命令显示信息描述表

字段	描述
access-control-policy	证书属性的访问控制策略名
rule number	控制规则编号

1.1.15 display pki certificate attribute-group

【命令】

display pki certificate attribute-group { *group-name* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

group-name：指定证书属性组名，为 1～16 个字符的字符串。

all：所有证书属性组。

|：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 pki certificate attribute-group 命令用来显示证书属性组的信息。

【举例】

显示证书属性组 mygroup 的信息。

```
<Sysname> display pki certificate attribute-group mygroup
 attribute group name: mygroup
      attribute  1 subject-name     dn    ctn   abc
      attribute  2 issuer-name      fqdn  nctn  app
```

表1-3 display pki certificate attribute-group 命令显示信息描述表

字段	描述
attribute group name	证书属性组名称
attribute *number*	属性规则编号
subject-name	证书主题名
dn	实体的 DN
ctn	表示包含操作
abc	属性规则 1 的证书属性值
issuer-name	证书颁发者名
fqdn	实体的 FQDN
nctn	表示不包含操作
app	属性规则 2 的证书属性值

1.1.16 display pki crl domain

【命令】

display pki crl domain *domain-name* [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

domain-name：指定证书所在的 PKI 域，为 1～15 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 pki crl domain 命令用来显示存储在本地的 CRL。

相关配置可参考命令 **pki retrieval-crl** 和 **pki domain**。

【举例】

显示 CRL。

```
<Sysname> display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=CN
            O=abc
            OU=soft
            CN=A Test Root
        Last Update: Jan  5 08:44:19 2004 GMT
        Next Update: Jan  5 21:42:13 2004 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
            Revoked Certificates:
            Serial Number: 05a234448E…
            Revocation Date: Sep  6 12:33:22 2004 GMT
            CRL entry extensions:……
            Serial Number: 05a278445E…
            Revocation Date: Sep  7 12:33:22 2004 GMT
            CRL entry extensions:…
```

表1-4 display pki crl domain 显示信息描述表

字段	描述
Version	CRL 版本号
Signature Algorithm	CRL 采用的签名算法
Issuer	颁发该 CRL 的 CA
Last Update	上次更新时间
Next Update	下次更新时间
CRL extensions	CRL 扩展属性
X509v3 Authority Key Identifier	发布该无效证书的 CA 的标识符，证书版本为 X509v3
keyid	公钥标识符 一个 CA 可能有多个密钥对，该字段用于标识该 CRL 的签名使用哪个密钥对
Revoked Certificates	撤销的证书
Serial Number	撤销证书的序列号

字段	描述
Revocation Date	撤销日期

1.1.17 fqdn

【命令】

fqdn *name-str*

undo fqdn

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

name-str：实体的 FQDN，为 1～127 个字符的字符串，不区分大小写。

【描述】

fqdn 命令用来配置实体的 FQDN。**undo fqdn** 命令用来删除实体的 FQDN。

缺省情况下，未指定实体 FQDN。

FQDN 是实体在网络中的唯一标识，由一个主机名和域名组成，可被解析为 IP 地址。

【举例】

配置实体的 FQDN 为 pki.domain-name.com。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

1.1.18 ip (PKI Entity view)

【命令】

ip *ip-address*

undo ip

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

ip-address：实体的 IP 地址。

【描述】

ip 命令用来配置实体的 IP 地址。**undo ip** 命令用来删除实体的 IP 地址。

缺省情况下，未指定实体 IP 地址。

【举例】

配置实体的 IP 地址为 11.0.0.1。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

1.1.19 ldap-server

【命令】

ldap-server ip *ip-address* [**port** *port-number*] [**version** *version-number*]

undo ldap-server

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

ip-address：LDAP 服务器的 IP 地址，为点分十进制格式。

port-number：LDAP 服务器的端口号，取值范围为 1～65535，缺省值为 389。

version-number：LDAP 版本号，取值范围为 2～3，缺省值为 2。

【描述】

ldap-server 命令用来配置 LDAP 服务器。**undo ldap-server** 命令用来删除指定的 LDAP 服务器。

缺省情况下，未指定 LDAP 服务器。

【举例】

指定 LDAP 服务器的位置。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

1.1.20 locality

【命令】

locality *locality-name*

undo locality

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

locality-name：地理区域的名称，为 1～31 个字符的字符串，不区分大小写，不能包含逗号。

【描述】

locality 命令用来配置实体所在的地理区域名称，比如城市名称。**undo locality** 命令用来删除实体所在的地理区域的名称。

缺省情况下，未指定实体所在地理区域。

【举例】

配置实体所在地理区域名称为 city。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

1.1.21 organization

【命令】

organization *org-name*

undo organization

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

org-name：组织名称，为 1～31 个字符的字符串，不区分大小写，不能包含逗号。

【描述】

organization 命令用来配置实体所属组织的名称。**undo organization** 命令用来删除实体所属组织的名称。

缺省情况下，未指定实体所属组织。

【举例】

配置实体所属组织名称为 test-lab。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization test-lab
```

1.1.22 organization-unit

【命令】

organization-unit *org-unit-name*

undo organization-unit

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

org-unit-name：组织部门的名称，为 1～31 个字符的字符串，不区分大小写，不能包含逗号。使用该参数在同一个单位内区分不同的部门。

【描述】

organization-unit 命令用来指定实体所属的组织部门的名称。**undo organization-unit** 命令用来删除实体所属的组织部门的名称。

缺省情况下，未指定实体所属部门。

【举例】

配置实体所属组织部门名称为 group1。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit group1
```

1.1.23 pki certificate access-control-policy

【命令】

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：表示证书属性的访问控制策略名称，为 1～16 个字符的字符串，不区分大小写，不能是“a”、“al”和“all”。

all：表示所有证书属性的访问控制策略。

【描述】

pki certificate access-control-policy 命令用来创建证书属性访问控制策略，并进入证书属性访问控制策略视图。**undo pki certificate access-control-policy** 命令用来删除一个或者所有证书属性访问控制策略。

缺省情况下，不存在证书属性访问控制策略。

【举例】

配置一个名称为 mypolicy 的访问控制策略，并进入证书属性访问控制策略视图。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

1.1.24 pki certificate attribute-group

【命令】

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

group-name：证书属性组名称，为 1～16 个字符的字符串，不区分大小写，不能是“a”、“al”和“all”。

all：表示所有属性组。

【描述】

pki certificate attribute-group 命令用来创建证书属性组并进入证书属性组视图。**undo pki certificate attribute-group** 命令用来删除一个或者所有证书属性组。

缺省情况下，不存在证书属性组。

【举例】

创建一个名为 mygroup 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

1.1.25 pki delete-certificate

【命令】

pki delete-certificate { **ca** | **local** } **domain** *domain-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ca：表示删除存储在本地的 CA 证书。

local：表示删除存储在本地的本地证书。

domain-name：指定待删除证书所在的 PKI 域，为 1～15 个字符的字符串。

【描述】

pki delete-certificate 命令用来删除本地存储的指定 PKI 域的证书。

【举例】

删除 PKI 域 cer 中的本地证书。

```
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

1.1.26 pki domain

【命令】

pki domain *domain-name*

undo pki domain *domain-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

domain-name：指定一个 PKI 域名，为 1～15 个字符的字符串，不区分大小写。

【描述】

pki domain 命令用来创建 PKI 域，并进入 PKI 域视图。如果指定的 PKI 域已存在，则直接进入其视图。**undo pki domain** 命令用来删除指定的 PKI 域。

缺省情况下，不存在 PKI 域。

【举例】

创建 PKI 域并进入其视图。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

1.1.27 pki entity

【命令】

pki entity *entity-name*

undo pki entity *entity-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

entity-name：实体名，为 1～15 个字符的字符串，不区分大小写。

【描述】

pki entity 命令用来配置实体名称，并进入该实体视图。**undo pki entity** 命令用来删除此实体的名称及其实体命名空间下的所有配置。

缺省情况下，无实体存在。

在 PKI 实体视图下可配置实体的各种属性值。*entity-name* 只是用来方便被其它命令引用，不用于证书的相关字段。

【举例】

配置实体名称为 en，并进入该实体视图。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

1.1.28 pki import-certificate

【命令】

pki import-certificate { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ca：表示 CA 证书。

local：表示本地证书。

domain-name：证书所在的 PKI 域，为 1～15 个字符的字符串。

der：指定证书文件格式为 DER 编码。

p12：指定证书文件格式为 P12 编码。

pem：指定证书文件格式为 PEM 编码。

filename *filename*：证书的文件名，为 1～127 个字符的字符串，不区分大小写。缺省的文件名就是导入后生成的文件名，即 *domain-name*_ca.cer、*domain-name*_local.cer 或者 *domain-name*_peerentity_*entity-name*.cer。

【描述】

pki import-certificate 命令用来将已有的 CA 证书或本地证书导入到本地保存。

相关配置可参考命令 **pki domain**。

【举例】

导入 PKI 域 cer 中的 CA 证书，证书文件格式为 PEM 编码。

```
<Sysname> system-view
[Sysname] pki import-certificate ca domain cer pem
```

1.1.29 pki request-certificate domain

【命令】

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

domain-name：包含证书申请中 CA 或 RA 等信息的 PKI 域名，为 1～15 个字符的字符串。

password：在证书撤销时需要提供的密码，为 1～31 个字符的字符串，区分大小写。

pkcs10：在终端上显示出 BASE64 编码的 PKCS#10 证书申请信息，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求。

filename *filename*：将 PKCS#10 证书申请信息保存到本地的文件中。其中，*filename* 表示保存证书申请信息的文件名，为 1～127 个字符的字符串，不区分大小写。

【描述】

pki request-certificate domain 命令用来通过 SCEP 协议向 CA 申请本地证书。

当 SCEP 出现异常无法正常通信时，可以通过执行指定参数 **pkcs10** 的本命令打印出本地的证书申请信息（BASE64 格式），或者通过执行指定 **pkcs10 filename** *filename* 参数的本命令将证书申请信息直接保存到本地的指定文件中，然后通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。

此命令不会被保存在配置文件中。

相关配置可参考命令 **pki domain**。

【举例】

手工申请证书，并在终端上显示 PKCS#10 证书请求。

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END CERTIFICATE REQUEST-----
```

1.1.30 pki retrieval-certificate

【命令】

pki retrieval-certificate { **ca** | **local** } **domain** *domain-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ca：表示下载 CA 证书。

local：表示下载本地证书。

domain-name：包含证书申请中 CA 或 RA 等信息的域名。

【描述】

pki retrieval-certificate 命令用来从证书发布服务器上在线获取证书并下载至本地。

相关配置可参考命令 **pki domain**。

【举例】

从证书发布服务器上下载 CA 证书。

```
<Sysname> system-view
[Sysname] pki retrieval-certificate ca domain 1
```

1.1.31 pki retrieval-crl domain

【命令】

pki retrieval-crl domain *domain-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

domain-name：包含证书申请中 CA 或 RA 等信息的域名，为 1～15 个字符的字符串。

【描述】

pki retrieval-crl domain 命令用来从 CRL 发布服务器上获取最新的 CRL。

下载 CRL 的目的是验证当前证书的合法性。

相关配置请参考命令 **pki domain**。

【举例】

从 CRL 发布服务器上获取 CRL。

```
<Sysname> system-view
[Sysname] pki retrieval-crl domain 1
```

1.1.32 pki validate-certificate

【命令】

pki validate-certificate { **ca** | **local** } **domain** *domain-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ca：表示验证 CA 证书。

local：表示验证本地证书。

domain-name：指明待验证证书所在的域，为 1～15 个字符的字符串。

【描述】

pki validate-certificate 命令用来检查证书的有效性。

证书验证的核心就是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除。

相关配置可参考命令 **pki domain**。

【举例】

检查本地证书的有效性。

```
<Sysname> system-view
[Sysname] pki validate-certificate local domain 1
```

1.1.33 root-certificate fingerprint

【命令】

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

【视图】

PKI 域视图

【缺省级别】

2：系统级

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹。当选择 MD5 指纹时，*string* 必须为 32 个字符，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符，并且以 16 进制的形式输入。

【描述】

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹。**undo root-certificate fingerprint** 命令用来取消配置的指纹。

缺省情况下，未指定验证 CA 根证书时使用的指纹。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
[Sysname-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

1.1.34 rule (PKI Cert access control policy view)

【命令】

rule [*id*] { **deny** | **permit** } *group-name*

undo rule { *id* | **all** }

【视图】

证书属性的访问控制策略视图

【缺省级别】

2：系统级

【参数】

id：证书属性访问控制规则编号，取值范围为 1～16，缺省值为 1～16 中未被使用的最小的编号。

deny：当证书的属性与属性组里定义的属性匹配时，认为该证书无效，访问控制策略检测不通过。

permit：当证书的属性与属性组里定义的属性匹配时，认为该证书有效，访问控制策略检测通过。

group-name：规则所关联的证书属性组名称，为 1～16 个字符的字符串，不区分大小写，不能是“a”、“al”和“all”。

all：所有控制规则。

【描述】

rule 命令用来创建证书属性的访问控制规则。**undo rule** 命令用来删除指定或者所有访问控制规则。

缺省情况下，不存在证书属性的访问控制规则。

需要注意的是，规则所关联的证书属性组必须已经存在。

【举例】

创建一个访问控制规则，该规则表示，当证书与 mygroup 证书属性组匹配时，认为该证书有效，访问控制策略检测通过。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

1.1.35 state

【命令】

state *state-name*

undo state

【视图】

PKI 实体视图

【缺省级别】

2：系统级

【参数】

state-name：州或省的名称，为 1～31 个字符的字符串，不区分大小写，不能包含逗号。

【描述】

state 命令用来配置实体所属的州或省的名称。**undo state** 命令用来删除所属的州或省的名称。

缺省情况下，未指定实体所在州或省。

【举例】

配置实体所在省为 country。

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] state country
```