j – k

- java-trustpoint（已弃用），第 2 页
- join-failover-group，第 4 页
- jumbo-frame reservation，第 6 页
- kcd-server，第 8 页
- keepout，第 10 页
- kerberos-realm，第 12 页
- key (aaa-server host)，第 14 页
- key (cluster group)，第 16 页
- key chain，第 18 页
- key config-key password-encryption，第 20 页
- key-hash，第 22 页
- keypair，第 24 页
- 密钥大小，第 26 页
- keysize server，第 28 页
- key-string，第 30 页
- kill，第 32 页

java-trustpoint（已弃用）

要将 WebVPN Java 对象签名工具配置为使用指定信任点位置的 PKCS12 证书和密钥内容，请在 webvpn 配置模式下使用 **java-trustpoint** 命令。要删除 Java 对象签名工具，请使用此命令的 **no** 形式。

java-trustpoint信任点
no java-trustpoint

Syntax Description

信任点	指定 **cryptocaimport** 命令配置的信任点位置。

Command Default

默认情况下，Java 对象签名的信任点设置为 none。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(2)	添加了此命令。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

使用指南

信任点是证书颁发机构 (CA) 或身份密钥对的代表。对于 **java-trustpoint** 命令，给定信任点必须包含应用签名实体的 X.509 证书、与该证书对应的 RSA 私钥以及向上扩展至根 CA 的证书授权链。这通常通过使用 **cryptocaimport** 命令导入 PKCS12 格式的捆绑包来实现。可以从受信任的 CA 颁发机构获取 PKCS12 捆绑包，也可以使用 openssl 等开源工具从现有 X.509 证书和 RSA 私钥手动创建一个捆绑包。

注释　上传的证书无法用于签署随软件包（例如，CSD 软件包）嵌入的 Java 对象。

CR_Examples

以下示例首先配置新信任点，然后为 WebVPN Java 对象签名配置它：

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word “quit” on a line by itself.
```

```
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

以下示例配置用于对 WebVPN Java 对象签名的新信任点：

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

Related Commands

命令	说明
cryptocaimport	使用 PKCS12 数据导入信任点的证书和密钥对。

join-failover-group

要将情景分配给故障转移组，请在情景配置模式下使用**join-failover-group** 命令。要恢复默认设置，请使用此命 **no**令的形式。

join-failover-group*group_num*
no join-failover-group*group_num*

Syntax Description

group_num	指定故障转移组编号。

Command Default

故障转移组 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
上下文配置	• 是	• 支持	—	• 是	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

管理环境始终分配给故障转移组 1。您可以使用 **showcontextdetail** 命令来显示故障转移组和情景关联。

您必须先在系统情景中使用 **failovergroup** 命令创建故障转移组，然后才能将情景分配给故障转移组。在情景处于活动状态的设备上输入此命令。默认情况下，未分配的情景是故障转移组 1 的成员，因此，如果情景之前尚未分配到故障转移组，则应在使故障转移组 1 处于主用状态的设备上输入此命令。

您必须先使用 **nojoin-failover-group** 命令从故障转移组中删除所有情景，然后才能从系统中删除故障转移组。

CR_Examples

以下示例将名为 ctx1 的情景分配到故障转移组 2：

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

Related Commands

命令	说明
context	进入指定情景的情景配置模式。
failovergroup	定义主用/主动故障转移的故障转移组。
showcontextdetail	显示情景详细信息，包括名称、类、接口、故障转移组关联和配置文件URL。

jumbo-frame reservation

要为受支持的型号启用巨帧，请在全局配置模式下使用**jumbo-framereservation** 命令。要禁用巨帧，请使用此命令的 **no** 形式。

注释 此设置的更改需要您重新启动 ASA。

jumbo-frame reservation
no jumbo-frame reservation

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，ASA 硬件、 ASA virtual和 ISA 3000 上禁用巨型帧预留。

其他型号默认支持巨型帧。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.1(1)	为 ASA 5580 添加了此命令。
8.2(5)/8.4(1)	增加了对 ASA 5585-X 的支持。
8.6(1)	增加了对 ASA 5512-X 至 ASA 5555-X 的支持。
9.3(2)	增加了对 ASA 5506-X 的支持。
9.3(3)	添加了对 ASA 5508-X 和 5516-X 的支持。

使用指南

此过程仅适用于 ASA 硬件型号、ISA 3000 和。 ASA virtual其他型号默认支持巨型帧。

RAM 小于 8GB 的 ASAv5 和 ASAv10 不支持巨型帧。

巨型帧是一种大于标准最大值 1518 字节（包括第 2 层报头和 VLAN 标记，18 字节）的以太网数据包，最大可达9216字节。请注意， **mtu** 命令仅指定 负载 值，因此对于9216字节的巨帧，请将MTU设置为 9198（9216-18 字节用于报头）

巨型帧支持需要额外的内存，这可能会限制其他功能（例如访问列表）的最大使用。

管理 *n* /*n* 接口不支持巨型帧。

确保将每个需要传输巨型帧的接口的 MTU 设置为高于默认值 1500 的值；例如，使用命令将值设置为 **mtu**9198。对于 ASASM，您无需设置**jumbo-frame** reservation 命令；默认情况下，它支持巨帧。只需将 MTU 设置为所需的值即可。

此外，使用巨帧时，请务必为 TCP 配置 MSS（最大分段大小）值。MSS 应比 MTU 少 120 字节。例如，如果您将 MTU 配置为 9000，则应将 MSS 配置为 8880。您可以使用 命令来为 **sysoptconnectiontcpmss** MSS进行配置。

主设备和辅助设备都需要重新启动，以便故障转移对支持巨帧。为避免停机，请执行以下操作：

- 在主用设备上发出 命令。
- 保存活动设备上的运行配置。
- 重新启动主设备和辅助设备，一次一台。

CR_Examples

以下示例将启用巨型帧预留、保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5
70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

Related Commands

命令	说明
mtu	指定接口的最大传输单元。指定接口的最大传输单元。
showjumbo-framereservation	显示命令的**jumbo-framereservation**当前配置。

kcd-server

要为无客户端 SSL 远程访问 VPN 配置 Kerberos 约束委派 (KCD)，请在 webvpn 配置模式下使用 **kcd-server** 命令。要禁用 KCD，请使用此命 **no**令的形式。

kcd-server*aaa-server-group_name***username***user_id***password***password* [**validate-server-certificate**]
no kcd-server

Syntax Description

username	指定具有管理员或服务级别权限可将设备添加到域的 Active Directory 用户。
password	指定用户的密码。
validate-server-certificate	（可选。）指示 ASA 验证服务器证书，从而在加入域时验证服务器的身份。如果省略此选项，系统会假定域控制器有效。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.4(1)	添加了此命令。
9.15(1)	已添加关 **validate-server-certificate** 键字。

使用指南

在 webvpn 配置模式下使用 **kcd-server** 命令允许 ASA 加入 Active Directory 域。域控制器名称和领域在 **aaa-server-groupname**命令中指定。AAA 服务器组必须是 Kerberos 服务器类型。 **username** 和 **password** 选项不对应于具有管理员权限的用户，但应对应于在域控制器上具有服务级别权限的用户。要查看现有配置，请使用 **showwebvpnkcd**命令。

ASA 环境中的 Kerberos 约束委派 (KCD) 为无客户端 SSL 远程访问 VPN 用户提供对受 Kerberos 保护的所有 Web 服务的单点登录 (SSO) 访问权限。ASA 代表用户维护凭证（服务票证），并使用此票证对服务用户进行身份验证。

为了使命令发挥 **kcd-server**作用，ASA 必须在 源 域（ASA 所在的域）和目 标 或 资源域（*Web* 服务所在的 域）之间建立信任关系。ASA跨越从源域到目标域的认证路径，并代表远程访问用户获取访问服务所需的票证。

这条路径称为跨领域身份验证。在跨领域身份验证的每个阶段，ASA 依赖于特定领域上的凭证和与后续领域的信任关系。

KCD 配置还要求您将域控制器配置为 DNS 服务器（例如，在 DefaultDNS 组中），并在可通过其访问域控制器的接口上启用 DNS 查找。

CR_Examples

以下是 KCD 的配置示例，其中域控制器为 10.1.1.10（可通过内部接口访问），域名为 PRIVATE.NET。此外，域控制器上的服务账户用户名和密码为 duser 和 duser123! 。

```
----Enable a DNS lookup by configuring the DNS server and Domain name --------------
ciscoasa
(config)#
dns domain-lookup inside
ciscoasa
(config)#
dns server-group DefaultDNS
ciscoasa
(config-dns-server-group)#
name-server 10.1.1.10
ciscoasa
(config-dns-server-group)#
domain-nameprivate.net
----Configure the AAA server group with Server and Realm-------------------------------
ciscoasa
(config)#
aaa-server KerberosGroup protocol Kerberos
ciscoasa
(config-asa-server-group)#
aaa-server KerberosGroup (inside) host 10.1.1.10
ciscoasa
(config-asa-server-group)#
kerberos-realm PRIVATE.NET
----Enable KCD------------------------------
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
kcd-server KerberosGroup username dcuser password dcuser123! validate-server-certificate
```

Related Commands

命令	说明
aaa-server	进入aaa-server配置模式，可以配置AAA服务器参数。
aaa-serverhost	进入 aaa-server 主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
showaaakerberos	显示 Kerberos 票证。
showwebvpnkcd	显示 KCD 配置。

keepout

要显示管理员定义的消息而不是新用户会话的登录页面（当ASA进行维护或故障排除期间时），请在 webvpn 配置模式下使用**keepout**命令。要删除之前设置的禁止布线页面，请使用该命令的 **no** 版本。

keepout
no keepout字符串

Syntax Description

string 用双引号引起来的字母数字字符串。

Command Default

无禁止布线区页面。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

此命令启用后，无客户端 WebVPN 门户页面将不可用。您会收到管理员定义的消息，说明门户不可用，而不是收到门户的登录页面。使用 **keepout** 命令禁用无客户端访问，但仍允许 AnyConnect 访问。您还可以使用此命令在维护进行时指示门户不可用。

注释 如果已安装HostScan，禁止布线区功能不会阻止ASA打开思科安全桌面门户等页面。为了避开思科安全桌面端口，需要卸载 HostScan。

CR_Examples

以下示例显示如何配置禁止布线区页面：

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
```

```
 keepout “The system is unavailable until 7:00 a.m. EST.”
ciscoasa(config-webvpn)#
```

Related Commands

命令	说明
webvpn	进入 webvpn 配置模式，在此模式下配置无客户端 SSL VPN 连接的属性。

kerberos-realm

要指定此 Kerberos 服务器的领域名称，请在 aaa-server 主机配置模式下使用 **kerberos-realm**命令。要删除领域名称，请使用以下命 **no**令的形式：

kerberos-realm字符串
no kerberos-realm

Syntax Description

string 区分大小写的字母数字字符串，最多 64 个字符。字符串中不允许有空格。

注释
Kerberos 领域名称仅使用数字和大写字母。尽管 ASA 接受字符 串参数中的小写字母，但它不会将小写字母转换为大写字母。请务必仅使用大写字母。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令仅对 Kerberos 服务器有效。

当在 Kerberos 领域的 Windows **setUSERDNSDOMAIN**2000 Active Directory 服务器上运行时，字符串参数的值应与 Microsoft Windows 命令的输出相匹配。在以下示例中，EXAMPLE.COM 是 Kerberos 领域名：

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

字符串 参数只能使用数字和大写字母。 **kerberos-realm** 命令区分大小写，ASA 不会将小写字母转换为大写字母。

CR_Examples

以下序列显示在配置 AAA 服务器主机的情景中将 kerberos 领域设置为“EXAMPLE.COM” **kerberos-realm** 的 命令：

```
ciscoasa
(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

命令	说明
aaa-serverhost	进入AAA服务器主机配置子模式，以便您可以配置特定于主机的AAA服务器参数。
clearconfigureaaa-server	从配置中删除所有 AAA 命令语句。
showrunning-configaaa-server	显示所有 AAA 服务器、特定服务器组、特定组中的特定服务器或特定协议的 AAA 服务器统计信息。

key (aaa-server host)

要指定用于向 AAA 服务器验证 NAS 的服务器密钥值，请在 aaa-server 主机配置模式下使用 **key** 命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除密钥，请使用此 **no**命令的形式。

key [**0** | **8**] *key*
no key

Syntax Description

key 字母数字关键字，最长可为127个字符。您可以选择在密钥之前添加一个数字，以表示已加密：

- 0 表示密钥未加密。这是默认值。
- 8 表示密钥是 AES 加密的 base64 散列值。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

密 钥值是区分大小写的字母数字关键字，最多 127 个字符，与 TACACS+ 服务器上的密钥值相同。超出 127 个字符后的所有字符都会被忽略。该密钥在客户端和服务器之间使用，用于加密它们之间的数据。客户端和服务器系统上的密钥必须相同。密钥不能包含空格，但允许包含其他特殊字符。密钥（服务器密钥）值向 AAA 服务器对 ASA 进行身份验证。

此命令仅适用于 RADIUS 和 TACACS+ 服务器。

CR_Examples

以下示例在主机“1.2.3.4”上配置名为“srvgrp1”的 TACACS+ AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将密钥配置为“myexclusivemumblekey”。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

命令	说明
aaa-serverhost	进入 aaa-server 主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
clearconfigureaaa-server	从配置中删除所有 AAA 命令语句。
showrunning-configaaa-server	显示 AAA 服务器配置。

key (cluster group)

要设置集群控制链路上控制流量的身份验证密钥，请在 **key**集群组配置模式下使用该命令。要删除密钥，请使用此 **no**命令的形式。

key*shared_secret*
no key [*shared_secret*]

Syntax Description

shared_secret	将共享机密设置为 1 至 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

此命令不会影响数据路径流量，包括始终以明文发送的连接状态更新和转发数据包。

CR_Examples

以下示例设置共享密钥：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

Related Commands

命令	说明
clacpsystem-mac	使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。
cluster group	命名集群并进入集群配置模式。
cluster-interface	指定集群控制链路接口。
clusterinterface-mode	设置集群接口模式。
conn-rebalance	启用连接再均衡。

命令	说明
console-replicate	启用从从属设备到主设备的控制台复制。
enable(clustergroup)	启用集群。
health-check	启用集群健康检查功能，包括单元健康监控和接口健康监控。
key	为集群控制链路上的控制流量设置身份验证密钥。
local-unit	为集群成员命名。
mtucluster-interface	指定集群控制链路接口的最大传输单元。
priority(clustergroup)	设置此单元在主单元选举中的优先级。

key chain

要配置轮换密钥以对 IGP 对等体进行身份验证，请在全局配置模式下使用 **keychain** 命令。要删除配置，请使用命 **no** 令的形式。

key chain*key-chain-name***key***key-id***key-string*{**0** | **8**}*key-string-text***cryptographic-algorithm md5**[**accept-lifetime**[*local* | *start-time*][**duration**{*duration value* | *infinite* | *end-time*}]

no key chain*key-chain-name***key***key-id***key-string*{**0** | **8**}*key-string-text***cryptographic-algorithm md5**[**accept-lifetime**[*local* | *start-time*][**duration**{*duration value* | *infinite* | *end-time*}]

Syntax Description

key-chain-name	为 OSPFv2 身份验证配置的密钥链的名称。
key-id	密钥链中的唯一标识符；有效范围为 1 到 255。
0	指定将遵循未加密的密码。
8	指定将遵循的加密密码。
key-string-text	密钥 ID 的密码。该字符串可以是纯文本或加密值。
md5	支持的加密算法。仅支持 md5。
accept-lifetime	（可选）设备与另一台设备交换密钥时接受密钥的时间间隔。
send-lifetime	（可选）设备与另一台设备交换密钥时发送密钥的时间间隔。

Command Default

接受或发送生命周期如果未指定，则默认始终处于活动状态。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 否

Command History

版本	修改
9.12(1)	添加了此命令。

使用指南

使用 **keychain** 命令配置要在接口的 OSPFv2 身份验证中使用的密钥链。您必须输入 **keyid**、**keystring,** 和 **cryptographic-algorithm** 命令。输入 **acceptandsendlifetimes** 以计划密钥轮换。生命周期变量有助

于处理安全密钥滚动更新。该设备使用密钥的生命周期来确定密钥链中的哪些密钥在任何给定时间点处于活动状态。未指定生命周期时，密钥链身份验证功能与无时间轴的 MD5 身份验证类似。使**nokeychain**用 删除钥匙串的配置。

CR_Examples

以下示例显示了密钥链配置命令：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite

ciscoasa(config-keychain-key)#
```

CR_Examples

以下示例提供了运行密钥链配置的输出：

```
ciscoasa# show running key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# show runing key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Related Commands

命令	说明
showkeychain	显示已配置的钥匙串
showrunningkeychain	显示当前活动的钥匙串详细信息
clearconfigurekeychain	删除配置的密钥链

key config-key password-encryption

要设置用于生成加密密钥的主密码以便以加密格式安全地存储纯文本密码，请在全局配置模式下使用 **keyconfig-keypassword-encryption**命令。如要解密使用该密码加密的密码，请使用此命令的 no 形式。

key config-key password-encryption*passphrase*[*old_passphrase*]
no key config-key password-encryption*passphrase*

Syntax Description

passphrase	密码长度必须介于 8 到 128 个字符之间。除退格键和双引号之外的所有字符都可以作为密码。如果未在命令中输入密码，则系统将提示您输入。使用交互式提示用户输入密码，以避免密码被记录在命令历史缓冲区。
old_passphrase	如果您要更改密码，请输入旧密码。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN（远程访问和站点间）
- 故障转移
- AAA 服务器
- 日志记录

- 共享许可证

您必须以任意顺序输入 **keyconfig-keypassword-encrypt** 命令和 **passwordencryptionaes**命令才能触发密码加密。输入 **writememory** ，以将加密密码保存到启动配置。否则，启动配置中的密码可能仍然可见。在多情景模式下，请在系统执行空间中使用 **writememoryall** 保存所有情景配置。

此命令仅在安全会话中被接受，例如通过控制台、SSH 或通过 HTTPS 的 ASDM。

请谨慎使用该 **nokeyconfig-keypassword-encrypt**命令，因为它会将加密密码更改为纯文本密码。EXTENSION 当降级到不支持密码加密的 **no**软件版本时，您可能会使用此命令的形式。

如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。

在主用/备用故障转移中启用或 **writestandby**更改密码加密会导致将主用配置复制到备用单元。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主动/主动故障转移，您必须手动输入。 **writestandby** A 可 **writestandby**能会导致主动/主动模式下的流量中断，因为在同步新配置之前，辅助设备上的配置已被清除。您应该使用 **failoveractivegroup1** 和**failoveractivegroup2** 命令使主 ASA 上的所有上下文处于活动状态 **writestandby**，输入，然后使用命令将第 2 组上下文恢复到辅助单 **nofailoveractivegroup2**元。

write擦除命令（后跟reload命令）将删除主密码和所有配置（如果其丢失）。

CR_Examples

以下示例设置用于生成加密密钥的密码，并启用密码加密：

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

命令	说明
passwordencryptionaes	启用密码加密。
write erase	如果主密码在其后跟 reload 命令时丢失，则将其删除。

key-hash

要为板载安全复制 (SCP) 客户端的服务器手动添加散列 SSH 主机密钥，请在服务器配置模式下使用 **key-hash**命令。您可以通过首先输入命令来访问服务器配置 **sshpubkey-chain**模式。要删除密钥，请使用此 **no**命令的形式。

key-hash {**md5** | **sha256**} *fingerprint*
no key-hash {**md5** | **sha256**} *fingerprint*

Syntax Description

指纹	输入散列密钥。
{md5 | sha256}	设置使用的散列类型，为 MD5 或 SHA-256。ASA 在其配置中始终使用 SHA-256。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
服务器配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.1(5)	添加了此命令。

使用指南

您可以使用板载 SCP 客户端在 ASA 之间复制文件，也可以从 ASA 复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器，您可以指定 SSH 主机的 **key-stringkey-hash**（公钥）或（哈希值）。输 **key-hash** 入已经散列的密钥（使用 MD5 或 SHA-256 密钥）；例如，您从 **show**命令输出复制的密钥。

CR_Examples

以下示例为 10.86.94.170 上的服务器添加经过散列处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

命令	说明
copy	将文件复制到 ASA 或从 ASA 复制文件。
key-hash	输入散列 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
sshpubkey-chain	从 ASA 数据库中手动添加或删除服务器及其密钥。
sshstricthostkeycheck	为板载安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

keypair

要指定要认证其公钥的密钥对，请在 crypto ca trustpoint 配置模式下使用 **keypair** 命令。要恢复默认设置，请使用命 **no**令的形式。

[no]
keypair*name* | [**rsamodulus** | **2048** | **4096**] | [**ecdsaelliptic-curve256** | **384** | **521**] | [**eddsaedwards-curveEd25519**]

Syntax Description

name	指定用于非 CMP 注册的密钥对的名称。
rsa	为任何 CMP 手动和自动注册生成 RSA 密钥。
ecdsa	为任何 CMP 手动和自动注册生成 ECDSA 密钥。
eddsa	为任何 CMP 手动和自动注册生成 EdDSA 密钥。

Command Default

默认设置是不包含密钥对。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.7(1)	添加了新的 EDCSA 和 RSA 密钥对。
9.16（1）	• 删除了对 RSA 密钥大小小于 2048 位的证书的支持。因此，rsa 模数选项已修改为显示 2048 位和更大的值。 • 已添加新的 EdDSA 密钥对。

CR_Examples

以下示例进入信任点中心的 crypto ca 信任点配置模式，并指定要为信任点中心认证的密钥对：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

Related Commands

命令	说明
cryptocatrustpoint	进入加密 ca 信任点配置模式。
cryptokeygeneratedsa	生成 DSA 密钥。
cryptokeygeneratersa	生成 RSA 密钥。
defaultenrollment	将注册参数还原为其默认值。

密钥大小

要指定本地证书颁发机构 (CA) 服务器在用户证书注册时生成的公钥和私钥的大小，请在 ca-server 配置模式下使用 **keysize**命令。要将密钥大小重置为默认长度 1024 位，请使用此命令的 **no**形式。

keysize*size*
no keysize

Syntax Description

size 密钥的大小（位）。大小可以是以下其中一项：

- 512
- 768
- 1024
- 2048
- 4096

Command Default

默认情况下，密钥对中每个密钥的长度均为 1024 位。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
ca-server 配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.13(1)	此命令行已删除。

CR_Examples

以下示例为本地 CA 服务器为用户生成的所有公共密钥和专用密钥对指定 2048 位的密钥长度：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize 2048
ciscoasa
```

```
(config-ca-server)
#
```

以下示例将本地CA服务器为用户生成的所有公共密钥和专用密钥对的密钥大小重置为默认长度 1024 位：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cryptocaserver	提供对 ca-server 配置模式命令集的访问，允许您配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
subject-name-default	指定要在CA服务器颁发的所有用户证书中与用户名一起使用的通用主题名称 DN。

keysize server

如要指定本地证书颁发机构 (CA) 服务器为配置 CA 密钥对大小而生成的公钥和私钥的大小，请在 ca-server 配置模式下使用 **keysizeserver** 命令。要将密钥大小重置为默认长度 1024 位，请使用此命令的 **no**形式。

keysize server*size*
no keysize server

Syntax Description

size 密钥的大小（位）。大小可以是以下其中一项：

- 512
- 768
- 1024
- 2048
- 4096

Command Default

默认情况下，密钥对中每个密钥的长度均为 1024 位。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Ca-server配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.13(1)	此命令行已删除。

CR_Examples

以下示例为 CA 证书指定 2048 位的密钥长度：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# keysize server 2048
ciscoasa
```

```
(config-ca-server)
#
```

以下示例将 CA 证书的密钥大小重置为默认长度 1024 位：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize server
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cryptocaserver	提供对 ca-server 配置模式命令集的访问，允许您配置和管理本地 CA。
issuer-name	指定证书颁发机构证书的使用者名称 DN。
keysize	指定用户证书的密钥对大小。
subject-name-default	指定要在CA服务器颁发的所有用户证书中与用户名一起使用的通用主题名称 DN。

key-string

要为板载安全复制 (SCP) 客户端的服务器手动添加公共 SSH 主机密钥，请在服务器配置模式下使用 **key-string**命令。您可以通过首先输入命令来访问服务器配置 **sshpubkey-chain**模式。此命令提示您输入密钥字符串。将字符串保存到配置中时，系统会使用 SHA-256 对其进行散列处理，并存储为 **key-hash** 命令中输入字符串。因此，要删除该字符串，请使用 **nokey-hash** 命令。

key-string*key_string*

Syntax Description

key_string	输入公钥。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
服务器配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.1(5)	添加了此命令。

使用指南

您可以使用板载 SCP 客户端在 ASA 之间复制文件，也可以从 ASA 复制文件。ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以在 ASA 数据库中手动添加或删除服务器及其密钥。

对于每个服务器，您可以指定 SSH 主机的 **key-stringkey-hash**（公钥）或（哈希值）。*key_string* 是远端对等体的采用 Base64 编码的 RSA 公钥。您可以从打开的 SSH 客户端（即 .ssh/id_rsa.pub 文件）获得公钥值。在您提交采用 Base64 编码的公钥之后，系统会通过 SHA-256 对其进行散列处理。

CR_Examples

以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

以下示例显示了已保存的散列密钥：

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

Related Commands

命令	说明
copy	将文件复制到 ASA 或从 ASA 复制文件。
key-hash	输入散列 SSH 主机密钥。
key-string	输入公共 SSH 主机密钥。
sshpubkey-chain	从 ASA 数据库中手动添加或删除服务器及其密钥。
sshstricthostkeycheck	为板载安全复制 (SCP) 客户端启用 SSH 主机密钥检查。

kill

要终止 Telnet 会话，请在特权 EXEC 模式下使用 **kill** 命令。

kill*telnet_id*

Syntax Description

telnet_id	指定 Telnet 会话 ID。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该 **kill**命令允许您终止 Telnet 会话。使用 who 命令查看 Telnet 会话 ID。终止 Telnet 会话时，ASA 允许终止任何活动命令，然后丢弃连接，而不发出警告。

CR_Examples

以下示例显示如何终止 ID 为“2”的 Telnet 会话。首先，输入 who命令可显示活动 Telnet 会话的列表。然后输入 **kill2**命令终止 ID 为“2”的 Telnet 会话。

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

Related Commands

命令	说明
telnet	配置对 ASA 的 Telnet 访问。
who	显示活动 Telnet 会话的列表。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。