Configuration Guide: Configuring Public Key Infrastructure High Availability for Cisco IOS Certificate Authority Servers and Client-Side Public Key Infrastructure

Introduction

Box-to-box High Availability (HA) support in Public Key Infrastructure (PKI) provides redundancy for the Cisco IOS® Certificate Authority (CA) server and the client-side PKI.

PKI high availability for the PKI CA server uses the Stateful Switch-Over (SSO) redundancy feature in Cisco IOS Software to synchronize the configurations of the active and standby CA routers to maintain state synchronization between the active and standby systems. In this scenario, if the active CA server becomes unavailable, the standby Cisco IOS CA server will be ready to take over. The active CA server will synchronize the server configuration, certificate revocation list (CRL), serial file, CA certificate, and keys with the standby CA server if the two servers are configured with the redundancy keyword.

To use client-side PKI in a high-availability environment, the customer needs to specify the redundancy keyword in the trustpoint configurations.

For this configuration, Cisco IOS Software Release 15.1 (3)T and later is recommended.

Configuring PKI High Availability for Client-Side PKI

Configure redundancy as specified in the section “Sample Configuration for PKI High Availability” (steps 2 to 4) and include the keyword **redundancy** in the trustpoint configuration. This process will synchronize the trustpoint configuration with the standby system, and it will also synchronize the CA certificate and the router certificate associated with that trustpoint with the standby system.

Configuring PKI High Availability for Cisco IOS CA Servers

Note: These configurations refer to box-to-box or interdevice redundancy for PKI high availability.

Recommendations

- Ping the virtual IP address to be sure it is accessible from both routers.
- Do not start configuring PKI until the redundant CA servers are in the active-standby hot state.
- Start the PKI configuration from the active CA server.
- Configure the PKI server normally. After the PKI server configuration is complete, specify the keyword **redundancy** to synchronize all the configurations with the standby system.
- Start the PKI CA server with the following command: **crypto pki server-name start**

Note: If the Cisco IOS command **database level complete** is configured, the server-issued client certificate (.crt files) will not be synchronized with the standby system. To address this situation, use the network storage and have both PKI CA servers point to that storage using the command **database url**.

Debugging Tips

- Turn on debugging to help ensure that no errors occur during the synchronization process. The debugging commands are:

  debug crypto pki transaction

  debug crypto pki message

  debug crypto pki api

- Use the following **show** command to verify the state of the CA server on both the active and standby systems: **show crypto pki server <name>**

Sample Configuration for PKI High Availability

Use the steps presented here to set up PKI high availability.

Step 1. Enable HTTP service on both CA servers. This configuration is required so that the CA server can accept incoming HTTP connections from the client during enrollment. This command must be manually configured on both the active and standby CA servers

```
CA-server-1#conf t
```

Enter configuration commands, one per line. End with Ctrl+Z.

```
CA-server-1(config)#ip http server
CA-server-1(config)#end
```

Step 2. Configure the local interface that will be used for the Stream Control Transmission Protocol (SCTP) communication between the active and standby systems.

On the first CA server (CA-server-1), specify the following:

```
interface GigabitEthernet0/0
 ip address 10.1.32.83 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 standby delay minimum 30 reload 60
 standby 0 ip 10.1.32.86
 standby 0 priority 50
 standby 0 name SB
```

On the second CA server (CA-server-2), specify the following:

```
interface GigabitEthernet0/0
 ip address 10.1.32.84 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 standby delay minimum 30 reload 60
 standby 0 ip 10.1.32.86
```

```
 standby 0 priority 50
 standby 0 name SB
```

Check that both interfaces are and that the line protocol is on both CA servers:

```
CA-server-1#sh int gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0013.19ca.6350 (bia 0013.19ca.6350)
  Internet address is 10.1.32.83/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<snip……>
CA-server-1#sh int gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0013.19ca.6350 (bia 0013.19ca.6350)
  Internet address is 10.1.32.83/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<snip……>
```

Check the connectivity for the remote IP addresses from one CA server to the other—for example, from CA-server-1 to the local address of CA-server-2:

```
CA-server-1#ping 10.1.32.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.32.84, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
CA-server-1#
```

Check that the virtual IP address (VIP) is reachable from both CA servers—for example, from CA-server-2:

```
CA-server-2#ping 10.1.32.86
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.32.86, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
CA-server-2#
```

Step 3. Configure SCTP on both certificate servers:

On CA-server-1, specify the following:

```
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.1.32.83
   remote-port 5000
    remote-ip 10.1.32.84
```

On CA-server-2, specify the following:

```
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.1.32.84
   remote-port 5000
    remote-ip 10.1.32.83
```

Step 4. Configure the redundancy as **inter-device**, and configure the redundancy scheme as **standby**. The name of the group must match the standby name specified in the standby name interface configuration command (**standby 0 name SB**). Also, the standby name must be the same on both routers.

```
redundancy inter-device
 scheme standby SB
```

On the active CA server, you will see the following syslog message when the server becomes active :

```
*Jun  3 01:41:02.791: %HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 0 state Standby ->
Active
```

Similarly, the syslog message on the standby CA server is:

```
*Jun  2 08:58:47.111: %HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 0 state Speak ->
Standby
```

If you have specified **debug redundancy inter-device**, the following log messages will indicate the CA server's transition to the active state:

```
CA-server-2#
*Jun  3 01:41:00.439: REDUNDANCY INTERDEV: event: RF_INTERDEV_EVENT_HSRP_STDBY  state:
RF_INTERDEV_STATE_PC_NO_HSRP -> RF_INTERDEV_STATE_STDBY
*Jun  3 01:41:02.791: %HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 0 state Standby ->
Active
```

```
*Jun  3 01:41:02.791: REDUNDANCY INTERDEV: event: RF_INTERDEV_EVENT_HSRP_ACT  state:
RF_INTERDEV_STATE_STDBY -> RF_INTERDEV_STATE_ACT
```

Similarly, the following log messages will indicate the other CA server's transition to the standby state:

```
CA-server-1#
*Jun  2 08:58:47.111: REDUNDANCY INTERDEV: event: RF_INTERDEV_EVENT_HSRP_STDBY  state:
RF_INTERDEV_STATE_PC_NO_HSRP -> RF_INTERDEV_STATE_STDBY
```

Verify the redundancy state of both CA servers using the command **show redundancy** state:

```
CA-server-2#sh redundancy state
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
         Unit ID = 0
     Maintenance Mode = Disabled
    Manual Swact = disabled (peer unit not yet in terminal standby state)
 Communications = Up
   client count = 14
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x100    client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x100


CA-server-1#sh redundancy state
       my state = 8  -STANDBY HOT
     peer state = 13 -ACTIVE
           Mode = Duplex
         Unit ID = 0
     Maintenance Mode = Disabled
    Manual Swact = cannot be initiated from this the standby unit
 Communications = Up
   client count = 14
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x100
```

Note: If the CA servers do not achieve the standby and active states, you may see the following:

```
CA-server-1#sh redundancy state
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
         Unit ID = 0
```

```
     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode
   client count = 14
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

To correct the states, reload one or both routers after specifying the preceding redundancy configurations. If this process does not work, toggle the server association between the two devices as shown here:

```
ipc zone default
 association 1
  no shutdown
```

Step 5. After the CA servers achieve the active and standby states as discussed in step 4, configure the PKI CA server first and specify the keyword **redundancy** to synchronize the configuration with the standby CA server.

Note: This command should be run only on the active CA server.

```
CA-server-2(config)#crypto pki server PKI-HA
CA-server-2(cs-server)#redundancy
```

Start the PKI CA server on the active server:

```
crypto pki server-name start
```

This process will synchronize the CA certificate, RSA keys, serial file, and CRL with the standby CA server.

Note:

- Do not start configuring PKI until the CA routers achieve the active-standby hot state.
- Verify that the clock is the same on both CA servers.
- Specify the following debugging commands to help sequence the steps and to display the data that is being synchronized between the two CA servers:

```
debug crypto pki transaction
debug crypto pki message
debug crypto pki api
```

Some examples of debugging information generated during the synchronization of the data from the active CA server to the standby CA server are shown here.

On the active CA server (CA-server-2), the following debugging information may be generated:

```
CA-server-2(cs-server)#
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: ""
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: " redundancy"
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: " serial-number 0x0"
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: "end"
```

```
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: ""
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:15.735: PKI: pki_send_ha_peer_request: "redundancy "no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
*Jun  3 04:01:28.959: CRYPTO_PKI: Creating trustpoint PKI-HA
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: "crypto pki trustpoint PKI-HA"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: ""
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: " redundancy"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: " revocation-check crl"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: " rsakeypair PKI-HA"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: "end"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: ""
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: "exit"
*Jun  3 04:01:28.959: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:37.123: PKI: pki_send_ha_peer_request: "serial-number 0x0"
%Log packet overrun, PC 0x6278AD6C, format:
PKI:hexmode: len=%d(%d): %s
*Jun  3 04:01:44.123: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:44.127: PKI: pki_send_ha_peer_request: "serial-number 0x1"
*Jun  3 04:01:44.127: PKI: pki_send_ha_peer_request: "exit"
*Jun  3 04:01:44.127: CRYPTO_CA: certificate not found
*Jun  3 04:01:44.127: PKI: pki_send_ha_peer_request: "crypto pki certificate chain
PKI-HA"
*Jun  3 04:01:44.127: PKI: pki_send_ha_peer_request: "certificate ca 01"
*Jun  3 04:01:44.191: PKI: pki_send_ha_peer_request: "308201FB 30820164 A0030201
02020101 300D0609 2A864886 F70D0101 04050030"
<snip>……..
*Jun  3 04:01:44.191: PKI: pki_send_ha_peer_request: "quit"
*Jun  3 04:01:44.191: PKI: pki_send_ha_peer_request: "exit"
*Jun  3 04:01:44.199: CRYPTO_CS: updated crl in memory ..
<snip>…….
*Jun  3 04:01:52.127: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:52.127: PKI: pki_send_ha_peer_request: "crl"PKI:hexmode: len=216(57):
3081D530 40300D06 092A8648 86F70D01 01050500 3011310F 300D0603 55040313 06504B49
```

```
2D484117 0D313030 36303330 34303134 345A170D 31303036 30333130 30313434 5A300D06
092A8648 86F70D01 01050500 03818100 85AA2DE7 910B2B18 8D8F08D8 315C3D49 83C94AD1
F2FF3C00 52F05453 B854BE2A 2651AB3A 85C32A50 A99168B9 BF9C9278
<snip>……..
*Jun  3 04:01:52.131: PKI: pki_send_ha_peer_request: "quit"
*Jun  3 04:01:52.131: PKI: pki_send_ha_peer_request: "end"
*Jun  3 04:01:52.131: CRYPTO_CS: updated crl in memory ..

<Snip>…….

% Certificate Server enabled.
CA-server-2(cs-server)#
*Jun  3 04:01:59.143: PKI: pki_send_ha_peer_request: "+crypto pki server PKI-HA"
*Jun  3 04:01:59.143: PKI: pki_send_ha_peer_request: "crl"PKI:hexmode: len=216(57):
3081D530 40300D06 092A8648 86F70D01 01050500 3011310F 300D0603 55040313 06504B49
2D484117 0D313030 36303330 34303134 345A170D 31303036 30333130 30313434 5A300D06
092A8648 86F70D01 01050500 03818100 85AA2DE7 910B2B18 8D8F08D8 315C3D49 83C94AD1
F2FF3C00 52F05453 B854BE2A 2651AB3A 85C32A50 A99168B9 BF9C9278 2C673CDB 14BCF7DD
1B8AD292 76DA9159 4D1E99A1 CDBB3DA8 BFFF20AB 1615A24D E8DB8BAE
<snip>…….
*Jun  3 04:01:59.143: PKI: pki_send_ha_peer_request: "A07B60C5 F6638FD1 9BB9433E
94ABF5B9 F6A0563E 12CBADAB"
*Jun  3 04:01:59.143: PKI: pki_send_ha_peer_request: "quit"
*Jun  3 04:01:59.143: PKI: pki_send_ha_peer_request: "end"
*Jun  3 04:01:59.599: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: added key:
30819F30 0D06092A 864886F7 0D010101...
*Jun  3 04:01:59.599: PKI: pki_send_ha_peer_request: ".crypto pki server PKI-HA start"
*Jun  3 04:01:59.599: %PKI-6-CS_ENABLED: Certificate server now enabled.
*Jun  3 04:01:59.599: PKI: pki_send_ha_peer_request: "no shut"
```

On the standby CA server (CA-server-1), the following debugging information may be generated:

```
CA-server-1#
*Jun  2 11:17:01.295: %SYS-5-CONFIG_I: Configured from console by console
*Jun  2 11:18:26.455: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)
*Jun  2 11:18:26.459: PKI:HA msg:(null)
*Jun  2 11:18:26.459: PKI: cmd(crypto-cs-server):  redundancy [OK] CHANGE SYNC
*Jun  2 11:18:26.459: PKI: cmd(crypto-cs-server):  serial-number 0x0 [OK] CHANGE SYNC
*Jun  2 11:18:26.459: PKI: cmd(crypto-cs-server): end [OK] NO_CHANGE DONT_SYNC
*Jun  2 11:18:26.459: PKI:HA msg:(null)
*Jun  2 11:18:26.459: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)
```

```
*Jun  2 11:18:26.459: PKI: cmd(crypto-cs-server): redundancy  [OK] CHANGE SYNC

*Jun  2 11:18:39.683: PKI: cmd(crypto-cs-server): crypto pki trustpoint PKI-HA

*Jun  2 11:18:39.683: CRYPTO_PKI: Creating trustpoint PKI-HA [OK] CHANGE SYNC

*Jun  2 11:18:39.683: PKI:HA msg:(null)

*Jun  2 11:18:39.683: PKI: cmd(crypto-ca-trustpoint):  redundancy [OK] CHANGE SYNC

*Jun  2 11:18:39.687: PKI: cmd(crypto-ca-trustpoint):  revocation-check crl [OK]
CHANGE SYNC

*Jun  2 11:18:39.687: PKI: cmd(crypto-ca-trustpoint):  rsakeypair PKI-HA [OK] CHANGE
SYNC

*Jun  2 11:18:39.687: PKI: cmd(crypto-ca-trustpoint): end [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:18:39.687: PKI:HA msg:(null)

*Jun  2 11:18:39.687: PKI: cmd(configure): exit [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:18:39.687: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)

*Jun  2 11:18:47.847: PKI: cmd(crypto-cs-server): serial-number 0x0 [OK] CHANGE SYNC

*Jun  2 11:18:54.847: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)

*Jun  2 11:18:54.851: PKI: cmd(crypto-cs-server): serial-number 0x1 [OK] CHANGE SYNC

*Jun  2 11:19:02.491: PKI: cmd(crypto-cs-server): exit [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:19:02.495: PKI: cmd(configure): crypto pki certificate chain PKI-HA [OK]
CHANGE SYNC

NC

*Jun  2 11:19:02.495: PKI: cmd(crypto-ca-cert-chain): certificate ca 01 (no PRC)

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 308201FB 30820164 A0030201 02020101
300D0609 2A864886 F70D0101 04050030 [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 11310F30 0D060355 04031306 504B492D
4841301E 170D3130 30363033 30343031 [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 33375A17 0D313330 36303230 34303133
375A3011 310F300D 06035504 03130650 [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 4B492D48 4130819F 300D0609 2A864886
F70D0101 01050003 818D0030 81890281 [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 8100A7E5 ABBCD88E 75D5C96A A7131DCC
80B0F371 C83CFCE7 D75D791E 9E0407ED [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): 3F9BE314 3C78FC1F 96C57DB4 D2CAD322
01350E74 698E2533 ED3DD4F5 1514BA56 [OK] CHANGE SYNC

*Jun  2 11:19:02.495: PKI: cmd(pki-hexmode): A85E3485 5CAC0296 B5EE18BA EBF7CAA6
262C8056 36252C40 B622610D 63C87500 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 021FA1FB 6BD93BBD D0AAA8FD D8F9D3B8
EF5A818D F889DF09 FEC7B3AB 7F052DD3 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 64CD0203 010001A3 63306130 0F060355
1D130101 FF0

40530 030101FF 300E0603 [OK] CHANGE SYNC
```

```
*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 551D0F01 01FF0404 03020186 301F0603
551D2304 18301680 148167CE 62C7F671 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 41E2284F 0865709B F0C89B51 62301D06
03551D0E 04160414 8167CE62 C7F67141 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): E2284F08 65709BF0 C89B5162 300D0609
2A864886 F70D0101 04050003 818100A4 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): A5F3E9CE 08FB88AE 24C0FCA6 1A7E857F
D74466E7 61C37D26 8EBE7119 53C27638 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): A536454A 76FB04BD F3BC3ADD 47127DFF
6E9FA37A 2AAA6300 31B42E2A 25D314D4 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 3449F4CD 03BA8215 A728F325 0821C4CA
7D103CDD E5FC5FB7 DA1C33E3 282B0421 [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): 6B475AC5 9F5B03D9 84F4D29E 44BDC380
5F8FBE7B 3193A64C D949A7BE F87ADE [OK] CHANGE SYNC

*Jun  2 11:19:02.499: PKI: cmd(pki-hexmode): quit

*Jun  2 11:19:02.503: CRYPTO_CA: certificate not found [OK] CHANGE SYNC

*Jun  2 11:19:02.503: PKI: cmd(crypto-ca-cert-chain): exit [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:19:02.851: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)

*Jun  2 11:19:02.855: PKI: cmd(crypto-cs-server): crl [OK] CHANGE SYNC

*Jun  2 11:19:02.855: PKI: cmd(crypto-pubkey): 3081D530 40300D06 092A8648 86F70D01
01050500 3011310F 300D0603 55040313 [OK] CHANGE SYNC

*Jun  2 11:19:02.855: PKI: cmd(crypto-pubkey): 06504B49 2D484117 0D313030 36303330
34303134 345A170D 31303036 30333130 [OK] CHANGE SYNC

*Jun  2 11:19:02.855: PKI: cmd(crypto-pubkey): 30313434 5A300D06 092A8648 86F70D01
01050500 03818100 85AA2DE7 910B2B18 [OK] CHANGE SYNC

*Jun  2 11:19:02.855: PKI: cmd(crypto-pubkey): 8D8F08D8 315C3D49 83C94AD1 F2FF3C00
52F05453 B854BE2A 2651AB3A 85C32A50 [OK] CHANGE SYNC

*Jun  2 11:19:02.859: PKI: cmd(crypto-pubkey): A99168B9 BF9C9278 2C673CDB 14BCF7DD
1B8AD292 76DA9159 4D1E99A1 CDBB3DA8 [OK] CHANGE SYNC

*Jun  2 11:19:02.859: PKI: cmd(crypto-pubkey): BFFF20AB 1615A24D E8DB8BAE 697F4C87
249385BA 80321497 80AA0354 92D88BD0 [OK] CHANGE SYNC

*Jun  2 11:19:02.859: PKI: cmd(crypto-pubkey): A07B60C5 F6638FD1 9BB9433E 94ABF5B9
F6A0563E 12CBADAB [OK] CHANGE SYNC

*Jun  2 11:19:02.859: PKI: cmd(crypto-pubkey): quit [OK] CHANGE SYNC

*Jun  2 11:19:10.519: PKI: cmd(configure): end [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:19:10.523: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)

*Jun  2 11:19:10.523: PKI: cmd(crypto-cs-server): crl [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): 3081D530 40300D06 092A8648 86F70D01
01050500 3011310F 300D0603 55040313 [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): 06504B49 2D484117 0D313030 36303330
34303134 345A170D 31303036 30333130 [OK] CHANGE SYNC
```

```
*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): 30313434 5A300D06 092A8648 86F70D01
01050500 03818100 85AA2DE7 910B2B18 [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): 8D8F08D8 315C3D49 83C94AD1 F2FF3C00
52F05453 B854BE2A 2651AB3A 85C32A50 [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): A99168B9 BF9C9278 2C673CDB 14BCF7DD
1B8AD292 76DA9159 4D1E99A1 CDBB3DA8 [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): BFFF20AB 1615A24D E8DB8BAE 697F4C87
249385BA 80321497 80AA0354 92D88BD0 [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): A07B60C5 F6638FD1 9BB9433E 94ABF5B9
F6A0563E 12CBADAB [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(crypto-pubkey): quit [OK] CHANGE SYNC

*Jun  2 11:19:10.523: PKI: cmd(configure): end [OK] NO_CHANGE DONT_SYNC

*Jun  2 11:19:10.527: PKI: cmd(exec): crypto pki server PKI-HA start [OK] CHANGE SYNC

*Jun  2 11:19:10.739: PKI: cmd(configure): no shut ??bad command

*Jun  2 11:19:10.755: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: added key:
30819F30 0D06092A 864886F7 0D010101...
```

Verify that the CA server is working correctly on both CA servers:

On the active CA server (CA-server-2), check the following:

```
CA-server-2#sh crypto pki server PKI-HA

Certificate Server PKI-HA:

    Status: enabled

    State: enabled

    Server's configuration is locked  (enter "shut" to unlock it)

    Issuer name: CN=PKI-HA

    CA cert fingerprint: FDB38019 E426C13A FDAC4B1E C324CB6A

    Granting mode is: manual

    Last certificate issued serial number (hex): 1

    CA certificate expiration timer: 06:32:59 UTC Jun 2 2013

    CRL NextUpdate timer: 12:33:00 UTC Jun 3 2010

    Current primary storage dir: nvram:

    Database Level: Minimum - no cert data written to storage

    Redundancy configured.  This is active.

CA-server-2#sh crypto pki certificates

CA Certificate

  Status: Available

  Certificate Serial Number (hex): 01

  Certificate Usage: Signature

  Issuer:
```

```
    cn=PKI-HA
  Subject:
    cn=PKI-HA
  Validity Date:
    start date: 04:01:37 UTC Jun 3 2010
    end   date: 04:01:37 UTC Jun 2 2013
  Associated Trustpoints: PKI-HA
  Storage: nvram:PKI-HA#1CA.cer
```

On the standby CA server (CA-server-1), check the following:

```
CA-server-1#sh crypto pki server PKI-HA
Certificate Server PKI-HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=PKI-HA
    CA cert fingerprint: FDB38019 E426C13A FDAC4B1E C324CB6A
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 06:32:59 UTC Jun 2 2013
    CRL NextUpdate timer: 12:33:00 UTC Jun 3 2010
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  This is standby.
CA-server-1#sh crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=PKI-HA
  Subject:
    cn=PKI-HA
  Validity Date:
    start date: 06:32:59 UTC Jun 3 2010
    end   date: 06:32:59 UTC Jun 2 2013
  Associated Trustpoints: PKI-HA
  Storage: nvram:PKI-HA#1CA.cer
```

Step 6. The RSA keys are generated automatically when the CA server is started. The **redundancy** keyword indicates that the keys are non-exportable and that they will be synchronized with the standby CA server during redundancy synchronization.

Verify that the RSA keys have been generated on the active server:

```
CA-server-2#show crypto key mypubkey rsa
% Key pair was generated at: 03:41:07 UTC Jun 3 2010
Key name: PKI-HA
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A7E5AB
  BCD88E75 D5C96AA7 131DCC80 B0F371C8 3CFCE7D7 5D791E9E 0407ED3F 9BE3143C
  78FC1F96 C57DB4D2 CAD32201 350E7469 8E2533ED 3DD4F515 14BA56A8 5E34855C
  AC0296B5 EE18BAEB F7CAA626 2C805636 252C40B6 22610D63 C8750002 1FA1FB6B
  D93BBDD0 AAA8FDD8 F9D3B8EF 5A818DF8 89DF09FE C7B3AB7F 052DD364 CD020301 0001
% Key pair was generated at: 03:41:07 UTC Jun 3 2010
Key name: PKI-HA.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B08E4F 743C894B
  5DF3F76C BB7EFBA3 936DC591 54327E5F 54702223 72882EF0 87531D28 1D44CB09
  3B479E08 B839FAD2 49D6F4A2 4D6727D4 874123FD 082F2A6A 56D93E64 C20C01BE
  CCC4D556 9A6AEE08 4B8C8101 429C9431 E245159D F1CED961 FB020301 0001
```

Verify that the RSA keys have been synchronized with the standby CA server:

```
*Jun  2 11:12:58.579: %SYS-5-CONFIG_I: Configured from console by console
CA-server-1#sh crypto key mypubkey rsa
% Key pair was generated at: 03:41:07 UTC Jun 3 2010
Key name: PKI-HA
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A7E5AB
  BCD88E75 D5C96AA7 131DCC80 B0F371C8 3CFCE7D7 5D791E9E 0407ED3F 9BE3143C
```

```
  78FC1F96 C57DB4D2 CAD32201 350E7469 8E2533ED 3DD4F515 14BA56A8 5E34855C
  AC0296B5 EE18BAEB F7CAA626 2C805636 252C40B6 22610D63 C8750002 1FA1FB6B
  D93BBDD0 AAA8FDD8 F9D3B8EF 5A818DF8 89DF09FE C7B3AB7F 052DD364 CD020301 0001
% Key pair was generated at: 10:58:18 UTC Jun 2 2010
Key name: PKI-HA.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00A1A7D3 4FEFDE58
  AF60445F E7FE8A61 CCADB10E A73B0934 50F59EDB 86C740A8 43C01ABF 4DC5D308
  7A2E079D 1FF32D58 865330F5 92AA0809 D3AF660D 0567D60D 086AFB2E 8E979A02
  9BD5B52B BAD4C026 76B0603F FC424A22 C1ED017D 5C907EFE FD020301 0001
```

Troubleshooting

Here is some guidance for troubleshooting some common errors.

If the Server Status Is “Disabled”

Sometimes, the status of the server may be “disabled” even though the RSA keys are present on the standby CA server:

```
CA-server-1#sh crypto pki server PKI-HA
Certificate Server PKI-HA:
    Status: disabled, Failed to validate selfsigned CA certificate
    State: check failed
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=PKI-HA
    CA cert fingerprint: FDB38019 E426C13A FDAC4B1E C324CB6A
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL NextUpdate timer: 12:33:00 UTC Jun 3 2010
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  This is standby.
```

The following errors may be associated with this problem:

```
CA-server-1#
*Jun  2 13:56:03.963: PKI: cmd(configure): crypto pki server PKI-HA (no PRC)
*Jun  2 13:56:06.219: PKI: cmd(crypto-cs-server): no shut
*Jun  2 13:56:06.219: CRYPTO_CS: input signal enqueued: no shut [OK] CHANGE SYNC
```

```
*Jun  2 13:56:06.219: CRYPTO_CS: enter FSM: input state check failed, input signal no shut
*Jun  2 13:56:06.219: CRYPTO_CS: SCEP server stopped
*Jun  2 13:56:06.219: CRYPTO_CS: starting enabling checks
*Jun  2 13:56:06.219: CRYPTO_CS: clock is not set but calendar is supported.
*Jun  2 13:56:06.219: CRYPTO_CS: nvram filesystem
*Jun  2 13:56:06.455: CRYPTO_CS: file opened: nvram:PKI-HA.ser
*Jun  2 13:56:06.455: CRYPTO_CS: closed ser file
*Jun  2 13:56:06.455: CRYPTO_CS: found existing serial file.
*Jun  2 13:56:06.455: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: expired key:
30819F30 0D06092A 864886F7 0D010101...
*Jun  2 13:56:06.455: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: added key:
30819F30 0D06092A 864886F7 0D010101...
```

`*Jun  2 13:56:06.455: CRYPTO_CS: The configured CA cert is invalid -no matching keys?`

```
*Jun  2 13:56:06.455: CRYPTO_CS: exit FSM: new state check failed
*Jun  2 13:56:06.455: CRYPTO_CS: cs config has been locked
```

This error message may appear even though the RSA keys are present on the standby CA server:

```
CA-server-1#sh crypto key mypubkey rsa
% Key pair was generated at: 06:26:11 UTC Jun 3 2010
Key name: PKI-HA
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00DA8BE3
  3C0C6D33 3C8279FE 27DF7AA9 78598C34 7A087804 F90FD00A E6EB6254 3FCD50E7
  7D3A7A07 A8C15FDD 3C58D9EA F9590671 6E738597 7234DA18 2FDE09C5 4213EF99
  A5419194 2FCDF132 0B55638B 5A755303 0EE75235 518C150B D41FB2A5 89735F94
  1F0A67B9 C42DB7BC ABE6A775 8927DD96 5FC72C67 7D3E70DA 366FB092 89020301 0001
% Key pair was generated at: 13:43:22 UTC Jun 2 2010
Key name: PKI-HA.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
```

```
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AC8331 54ABD360
  CB163499 FABBD450 F0318FBE A446D7CD 6534592C 8403E699 94A46FB0 92C51F56
  B7C33DFC 4EC1CCEE 6F72A2EF C5DCD4E1 2447B2CE 28725D45 CB93EF2F 52B5740F
  AF2B5D65 46EAE1C7 326007BA CD17805D 4185CBDD BBA22A6D C3020301 0001
```

Verify the clock settings to see that they match on the active and standby routers. Use the clock set command to set the time on the standby server to match that on the active CA server:

```
CA-server-1#clock set 06:53:44 Jun 3 2010
CA-server-1#end
*Jun  3 06:53:44.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 14:12:07 UTC Wed Jun 2 2010 to 06:53:44 UTC Thu Jun 3 2010, configured from console by console.
```

After the clock settings match, the following log messages may be reported on the standby CA server if debugging is turned on:

```
Jun  3 06:53:44.000: CRYPTO_CS: input signal enqueued: time set
Jun  3 06:53:44.000: CRYPTO_CS: enter FSM: input state check failed, input signal time set
Jun  3 06:53:44.000: CRYPTO_CS: SCEP server stopped
Jun  3 06:53:44.000: CRYPTO_CS: starting enabling checks
Jun  3 06:53:44.000: CRYPTO_CS: nvram filesystem
Jun  3 06:53:44.223: CRYPTO_CS: file opened: nvram:PKI-HA.ser
Jun  3 06:53:44.223: CRYPTO_CS: closed ser file
Jun  3 06:53:44.223: CRYPTO_CS: found existing serial file.
Jun  3 06:53:44.227: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: expired key: 30819F30 0D06092A 864886F7 0D010101...
Jun  3 06:53:44.227: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: added key: 30819F30 0D06092A 864886F7 0D010101...
Jun  3 06:53:44.227: CRYPTO_CS: started CA cert timer, expiration time is 06:32:59 UTC
Jun  3 06:53:44.227: CRYPTO_CS: Using existing trustpoint 'PKI-HA' and CA certificate
Jun  3 06:53:44.459: CRYPTO_CS: file opened: nvram:PKI-HA.ser
Jun  3 06:53:44.463: CRYPTO_CS: DB version 1
Jun  3 06:53:44.463: CRYPTO_CS: last issued serial number is 0x0
Jun  3 06:53:44.463: CRYPTO_CS: closed ser file
Jun  3 06:53:44.687: CRYPTO_CS: file opened: nvram:PKI-HA.crl
Jun  3 06:53:44.687: CRYPTO_CS: CRL file PKI-HA.crl exists.
Jun  3 06:53:44.687: CRYPTO_CS: Read 216 bytes from crl file.
Jun  3 06:53:44.687: CRYPTO_CS: closed crl file
Jun  3 06:53:44.691: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: expired key: 30819F30 0D06092A 864886F7 0D010101...
```

```
Jun  3 06:53:44.691: CRYPTO_PKI_API:cachekey: RSA Public Session Keys: added key:
30819F30 0D06092A 864886F7 0D010101...
Jun  3 06:53:44.691: CRYPTO_CS: set crl update timer.
Jun  3 06:53:44.691: CRYPTO_CS: shadow not configured; look for shadow cert
Jun  3 06:53:44.691: CRYPTO_CS: failed to find shadow cert in the db
Jun  3 06:53:44.691: CRYPTO_CS: SCEP server started
Jun  3 06:53:44.691: %PKI-6-CS_ENABLED: Certificate server now enabled.
Jun  3 06:53:44.691: CRYPTO_CS: exit FSM: new state enabled
Jun  3 06:53:44.691: CRYPTO_CS: cs config has been locked
```

Now verify the status of the CA server on the standby. It should be the same as that on the active CA server.

On the standby CA server, verify the status as follows:

```
CA-server-1#sh crypto pki server PKI-HA
Certificate Server PKI-HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=PKI-HA
    CA cert fingerprint: FDB38019 E426C13A FDAC4B1E C324CB6A
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 06:32:59 UTC Jun 2 2013
    CRL NextUpdate timer: 12:33:00 UTC Jun 3 2010
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  This is standby.
```

On the active CA server, verify the status as follows:

```
CA-server-2#sh crypto pki server PKI-HA
Certificate Server PKI-HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=PKI-HA
    CA cert fingerprint: FDB38019 E426C13A FDAC4B1E C324CB6A
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 06:32:59 UTC Jun 2 2013
    CRL NextUpdate timer: 12:33:00 UTC Jun 3 2010
```

```
Current primary storage dir: nvram:
Database Level: Minimum - no cert data written to storage
Redundancy configured.  This is active.
```

If RSA Keys Do Not Become Redundant

If the RSA keys do not become redundant (that is, they are not synchronized with the standby CA server), the CA server may have been started (no shutdown) before redundancy was configured. If this is the case, re-do the PKI high-availability part of the configuration.

If Keys Are Not Synchronized

Sometimes keys are not synchronized with the standby CA server. In this case, the following message may appear: **disabled, Server key not found, waiting for (offline) key.** Check the configuration and be sure to follow the steps in the recommended order.

This message also will appear if the CA server is started before the **redundancy** keyword is specified. In this case, the keys do not synchronize with the standby CA server.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-621400-00 09/10