NAC Appliance (CCA): Configure High Availability (HA) for the Clean Access Manager (CAM)

Document ID: 99945

Contents

Introduction

This document describes how to set up a pair of Clean Access Manager (CAM) machines for High Availability (HA). When Clean Access Managers are deployed in High Availability mode, you can ensure that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown.

Note: Refer to the Configuring High Availability (HA) section of the Cisco NAC Appliance − Clean Access Server (CAS) Installation and Administration Guide in order to know how to configure the HA feature in the CAS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Network Admission Control (NAC) Appliance − CAM Version 4.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

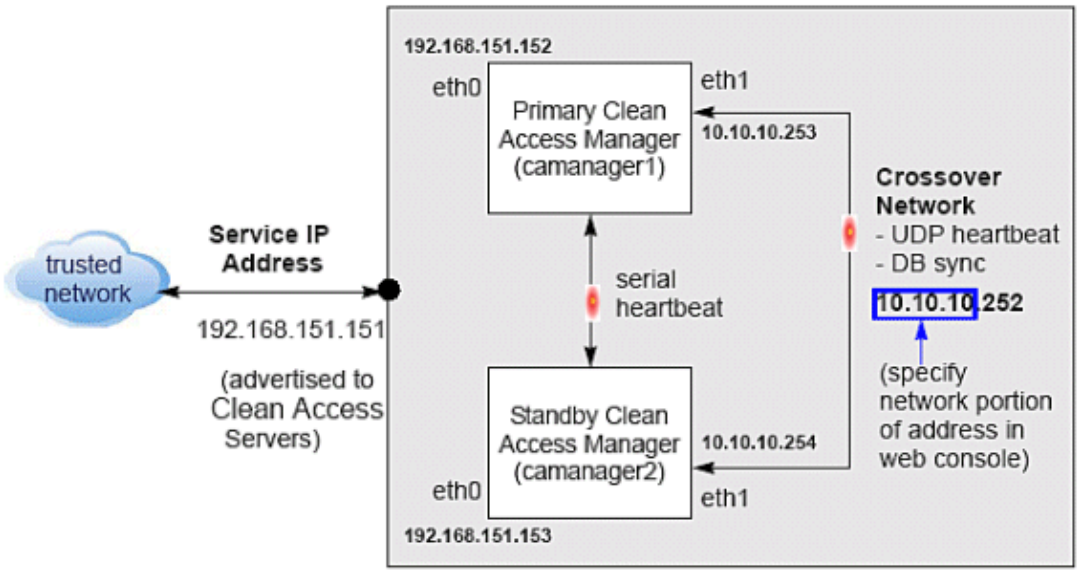
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Overview

These key points provide a high−level summary of HA−CAM operation:

1. The Clean Access Manager High Availability mode is an active/passive two−server configuration in which a standby CAM machine acts as a backup to an active CAM machine.
2. The active Clean Access Manager performs all tasks for the system. The standby CAM monitors the active CAM and keeps its database synchronized with the active CAM database.
3. Both CAMs share a virtual Service IP for the eth0 trusted interface. The domain name must be used for the SSL certificate.
4. The primary and secondary CAM machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
5. The eth1 interface and/or serial interface on the CAMs can be used for heartbeat packets and database synchronization. If both eth1 and serial interfaces are configured for heartbeat, both interfaces need to fail for failover to occur.



The Clean Access Manager High Availability mode is an active/passive two−server configuration in which a standby Clean Access Manager machine acts as a backup to an active Clean Access Manager machine. While the active CAM carries most of the workload under normal conditions, the standby monitors the active CAM and keeps its data store synchronized with the data of the active CAM.

If a failover event occurs, such as if the active CAM shuts down or does not respond to the heartbeat signal

of the peer, the standby assumes the role of the active CAM.

When you first configure the HA peers, you must specify an HA−Primary CAM and HA−Secondary CAM. Initially, the HA−Primary is the active CAM, and the HA−Secondary is the standby (passive) CAM, but the active/passive roles are not permanently assigned. If the primary CAM goes down, the secondary (standby) becomes the active CAM. When the original primary CAM restarts, it assumes the backup role.

When the Clean Access Manager starts up, it checks to see if its peer is active. If not, the CAM that starts up assumes the active role. If the peer is active, on the other hand, the CAM that starts becomes the standby.

You can configure two Clean Access Managers as an HA pair at the same time, or you can add a new Clean Access Manager to an existent standalone CAM to create a High Availability pair. In order for the pair to appear to the network and the Clean Access Servers as one entity, you must specify a Service IP address to be used as the trusted interface (eth0) address for the HA pair.

In order to create the crossover network on which High Availability information is exchanged, you connect the eth1 ports of both CAMs and specify a private network address not currently routed in your organization (the default HA crossover network is 192.168.0.252). The Clean Access Manager then creates a private, secure, two−node network for the eth1 ports of each CAM to exchange UDP heartbeat traffic and synchronize databases. Note that the CAM always uses eth1 as the UDP heartbeat interface.

For extra security, you can also connect the serial ports of each Clean Access Manager for heartbeat exchange. In this case, both the UDP heartbeat and serial heartbeat interfaces must fail for the standby system to take over.

Note: For serial cable connection for HA (either HA−CAM or HA−CAS), the serial cable must be a null modem cable.

Basic Requirements Before You Proceed

Warning: In order to prevent any possible data loss within database synchronization, always make sure that the standby (secondary) Clean Access Manager is live before failing over the active (primary) Clean Access Manager.

Before you configure High Availability, ensure that you meet these requirements:

1. You have obtained a High Availability (Failover) license.

   Note: When you install a CAM Failover (HA) license, install the Failover license to the Primary CAM first, then load all the other licenses. Standalone licenses can also be used for High Availability.
2. Both CAMs are installed and configured.
3. For heartbeat, each CAM needs to have a unique hostname (or node name). For HA CAM pairs, this host name is provided to the peer and must be resolved through DNS or added to the /etc/hosts file of the peer.
4. You have a CA−signed certificate for the domain name of the HA CAM pair.
5. The HA−Primary CAM is fully configured for runtime operation. This means that connections to authentication sources, policies, user roles, access points, and so on, are all specified. This configuration is automatically duplicated in the HA−Secondary (standby) CAM.
6. Both Clean Access Managers are accessible on the network (try to ping them to test the connection).
7. The machines on which the CAM software is installed have a free Ethernet port (eth1) and at least one free serial port. Use the specification manuals for the server hardware to identify the serial port (ttyS0 or ttyS1) on each machine.

8. In Out−of−Band deployments, Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

These procedures require you to reboot the Clean Access Manager. At that time, its services are briefly unavailable. Configure an online CAM when downtime has the least impact on your users.

Note: Cisco NAC Appliance web admin consoles support the Internet Explorer 6.0 or above browser.

Connect the Clean Access Manager Machines

There are two types of connections between HA−CAM peers: one to exchange runtime data that relates to the Clean Access Manager activities and one for the heartbeat signal. In High Availability, the Clean Access Manager always uses the eth1 interface for both data exchange and heartbeat UDP exchange. When the UDP heartbeat signal fails to be transmitted and received within a certain time period, the standby system takes over. In order to provide an extra measure of security, it is highly recommended to add a serial heartbeat connection between the Clean Access Manager peers. The serial connection provides an additional dedicated heartbeat exchange method that must fail before the standby system can take over. Note that the eth1 connection between the CAM peers is mandatory.

Physically connect the peer Clean Access Managers as shown:

- Use crossover cable to connect the eth1 Ethernet ports of the Clean Access Manager machines. This connection is used for the heartbeat UDP interface and data exchange (database mirroring) between the failover peers.
- Use null modem serial cable to connect the serial ports (highly recommended). This connection is used as an additional heartbeat serial exchange (keep−alive) between the failover peers.

Note: For serial cable connection for HA (either HA−CAM or HA−CAS), the serial cable must be a null modem cable.

Serial Connection

If the machine that runs the Clean Access Manager software has two serial ports, you can use the additional port for the serial heartbeat connection. By default, the first serial port detected on the CAM server is configured for console input/output (to facilitate installation and other types of administrative access).

If the machine has only one serial port (COM1 or ttyS0), you can reconfigure the port to serve as the High Availability heartbeat connection. This is because, after the CAM software is installed, the SSH or KVM console can always be used to access the command line interface of the CAM.

You can enable/disable the serial port with the **Disable Serial Login** check box on the HA CAM settings (under **Administration > Clean Access Manager > Network & Failover | Failover Settings | Disable Serial Login**). When there is only one serial port on the CAM machine, this check box allows administrators to disable serial login on COM1 so that it can be used as the Heartbeat Serial Interface for a pair of HA−Clean Access Managers.

Note: Serial login is **enabled** by default on the CAM. If you use COM1 for the Heartbeat Serial Interface of the CAM, you must click the **Disable Serial Login** check box to disable serial login on COM1.

Configure the HA−Primary CAM

Once you have verified the prerequisites, perform these steps to configure the Clean Access Manager as the HA−Primary for the High Availability pair. See the figure for a sample configuration example.

1. Open the web admin console for the Clean Access Manager to be designated as the HA−Primary, and go to **Administration > CCA Manager > SSL Certificate** to configure the SSL certificate for the primary CAM. The **Generate Temporary Certificate** form appears.

   Note: The HA configuration steps in this document assume that a temporary certificate is exported from the HA−Primary CAM to the HA−Secondary CAM.

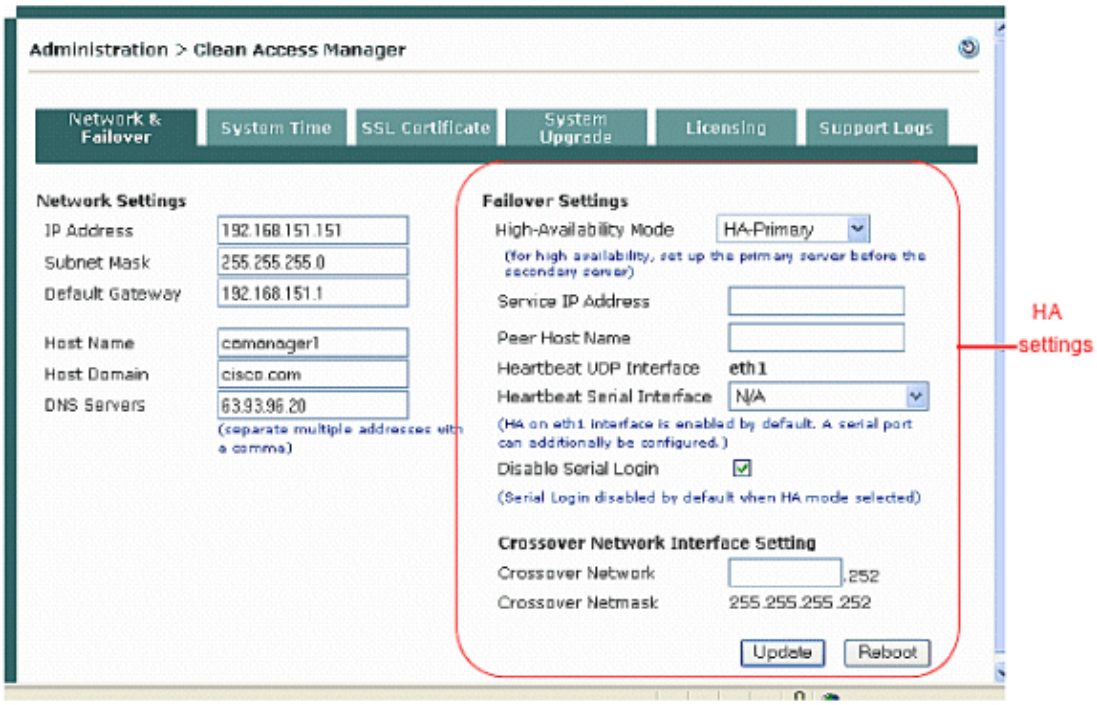
   If you use a temporary certificate for the HA pair, perform these steps:

   a. Complete the **Generate Temporary Certificate** form and click **Generate**. The certificate must be generated for the domain name of the HA pair.
   b. After you generate the temporary certificate, choose **Export CSR/Private Key/Certificate** from the **Choose an action** menu.
   c. Click the **Export** button for **Currently Installed Private Key** to export the SSL private key. Save the key file to disk. You have to import this key into the HA−Secondary CAM later.
   d. Click the **Export** button for **Currently Installed Certificate** to export the current SSL certificate. Save the certificate file to disk. You have to import this certificate file into the HA−Secondary CAM later.

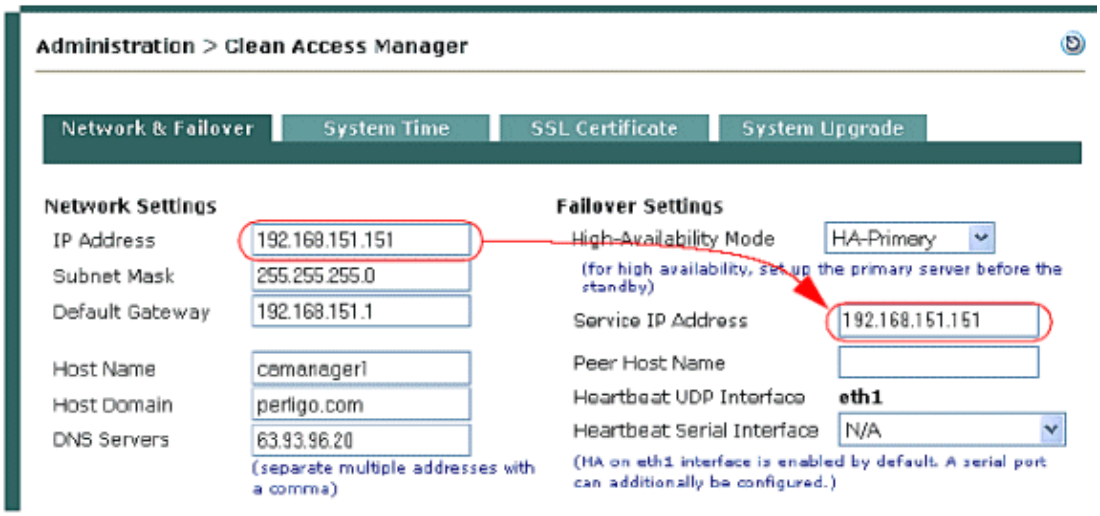
   If you use a CA−signed certificate for the HA pair, perform these steps:

   Note: The CA−signed certificate must be based on the domain name resolvable to the Service IP through DNS. Refer to Manage CAM SSL Certificates under the Administration section in the Cisco NAC Appliance − CAM Installation and Administration Guide for more information.

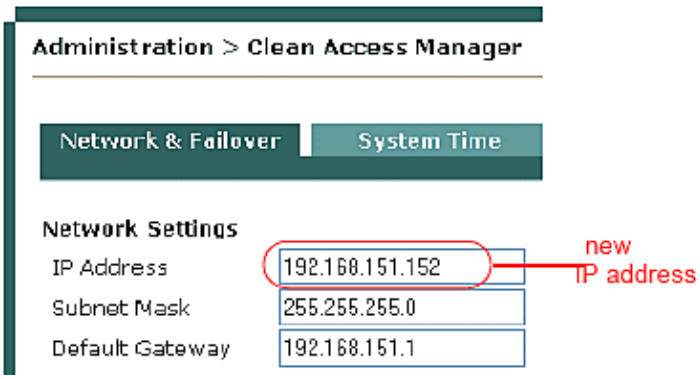
   a. Choose **Import Certificate** from the **Choose an action** menu.
   b. Use the **Browse** button next to the **Certificate File** field and navigate to the CA−signed certificate.
   c. Choose **CA−signed PEM−encoded X.509 Cert** from the **File Type** drop−down menu.
   d. Click **Upload** to import the certificate. Note that you need to import this same certificate into the HA−Secondary CAM later.
   e. Click **Verify and Install Uploaded Certificates**.
   f. Choose **Export CSR/Private Key/Certificate** from the **Choose an action** drop−down list.
   g. Click the **Export** button for the **Currently Installed Private Key** to export the SSL private key associated with the CA−signed certificate. Save the key file to disk. You need to import this file into the HA−Secondary CAM later.
2. Go to **Administration > CCA Manager** and click the **Network & Failover** tab. Choose the **HA−Primary** option from the **High−Availability Mode** drop−down menu. The High Availability settings appear.



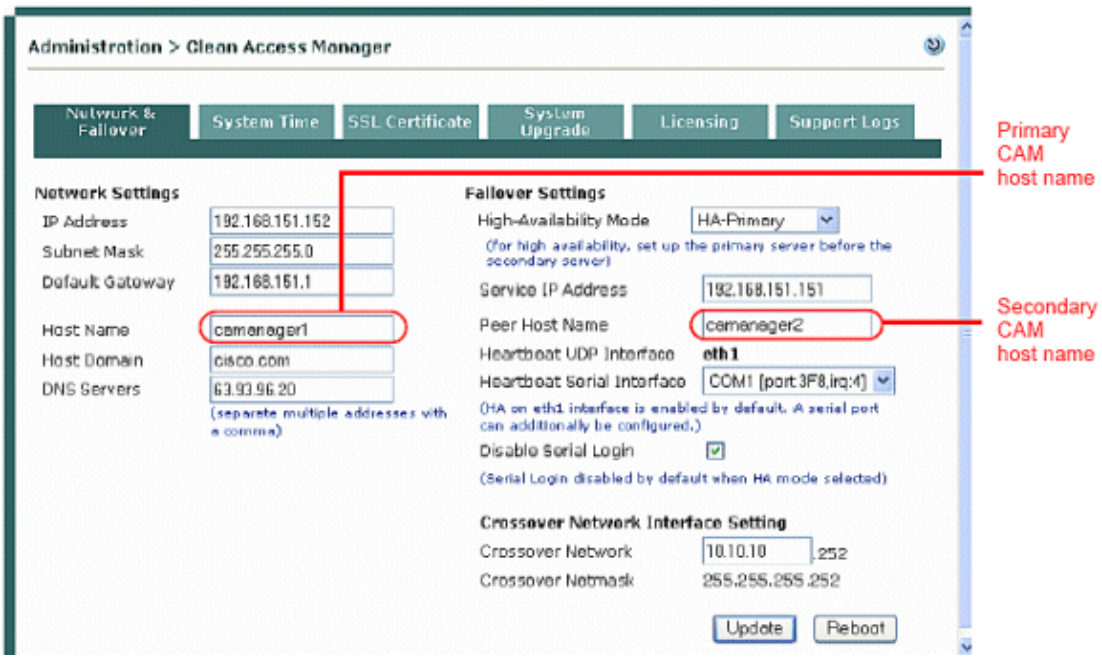
3. Copy the value from the **IP Address** field under **Network Settings** and enter it in the **Service IP Address** field. The Network Settings IP address is the existent IP address of the current Clean Access Manager. The idea here is to turn this IP address, which the Clean Access Servers already recognize, into the virtual Service IP address for the Clean Access Manager pair.



4. Change the IP address under **Network Settings** to an available address, for example, n.152.



5. Each Clean Access Manager must have a unique host name, such as camanager1 and camanager2. Type the host name of the HA−Primary CAM in the **Host Name** field under **Network Settings**, and type the host name of the HA−Secondary CAM in the **Peer Host Name** field under **Failover Settings**.



   - A **Host Name** value is mandatory when you set up High Availability, while the **Host Domain** name is optional.
   - The **Host Name** and **Peer Host Name** fields are case−sensitive. Make sure to match what is typed here with what is typed for the HA−Secondary CAM later.
6. From the **Heartbeat Serial Interface** drop−down menu, choose the serial port to which you connected the serial cable of the HA−Primary CAM, or leave this n/a if you do not use a serial connection.
7. If your machine only has one serial port and you use COM1 as the Heartbeat Serial Interface, you must check the **Disable Serial Login** check box to ensure that the serial login is disabled on COM1. See Serial Connection for further details.
8. In order to maintain synchronization, the Clean Access Manager peers exchange data by a crossover network. You must specify a private network address space not currently routed in your organization in the **Crossover Network** field, such as 10.10.10. The default crossover network provided is 192.168.0.252. If this address conflicts with your network, make sure to specify a different private address space. For example, if your organization uses the private network 192.168.151.0, use 10.1.1.x as the crossover network. The subnet mask and last octet of the IP address are fixed, so only enter the network portion of the IP address in the **Crossover Network** field.
9. Click **Update** and then **Reboot** to restart the Clean Access Manager.

   After the Clean Access Manager restarts, make sure that the CAM machine works properly. Check to see if the Clean Access Servers are connected and new users are authenticated.

Configure the HA−Secondary CAM

Perform these steps to configure the HA−Secondary CAM.

1. Open the web admin console for the Clean Access Manager to be designated as the HA−Secondary, and go to **Administration > CCA Manager > SSL Certificate**.
2. Before you proceed, perform these steps:

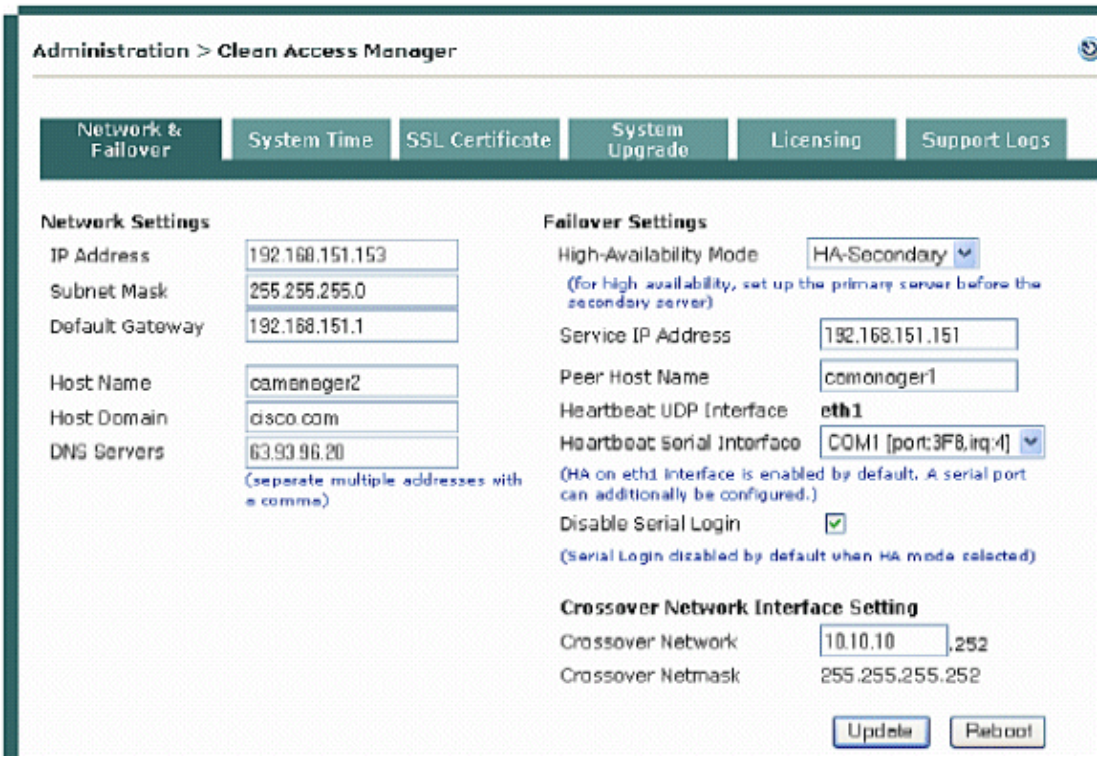
a. Back up the private key of the secondary CAM.
b. Make sure the private key and SSL certificate files associated with the Service IP/HA−Primary CAM are available (previously exported as described in Configure the HA−Primary CAM).

3. Import the private key file and certificate of the HA−Primary CAM as described:

a. In the **SSL Certificate** tab, choose **Import Certificate** from the **Choose an action** menu.
b. Click **Browse** next to the **Certificate File** field, and browse to your backup copy of the private key file generated with the certificate that is used for the HA pair.
c. Choose **Private Key** as the File Type.
d. Click **Upload** to upload the private key.
e. With **Import Certificate** chosen from the **Choose an action** menu, browse to the certificate (either temporary or CA−signed) that is associated with the private key.
f. Choose **CA−signed PEM−encoded X.509 Cert** as the File Type.
g. Click **Upload** to upload the temporary certificate or CA−signed certificate.
h. Click **Verify and Install Uploaded Certificates**.

Refer to Manage CAM SSL Certificates under the Administration section in the Cisco NAC Appliance − CAM Installation and Administration Guide for more information.

4. Go to **Administration > CCA Manager > Network & Failover | Network Settings** and change the IP address of the secondary CAM to an address that is different from the HA−Primary CAM IP address and the Service IP address.



5. Set the **Host Name** value under **Network Settings** to the same value set for the **Peer Host Name** in the HA−Primary CAM configuration. See the figure in the HA Primary section.

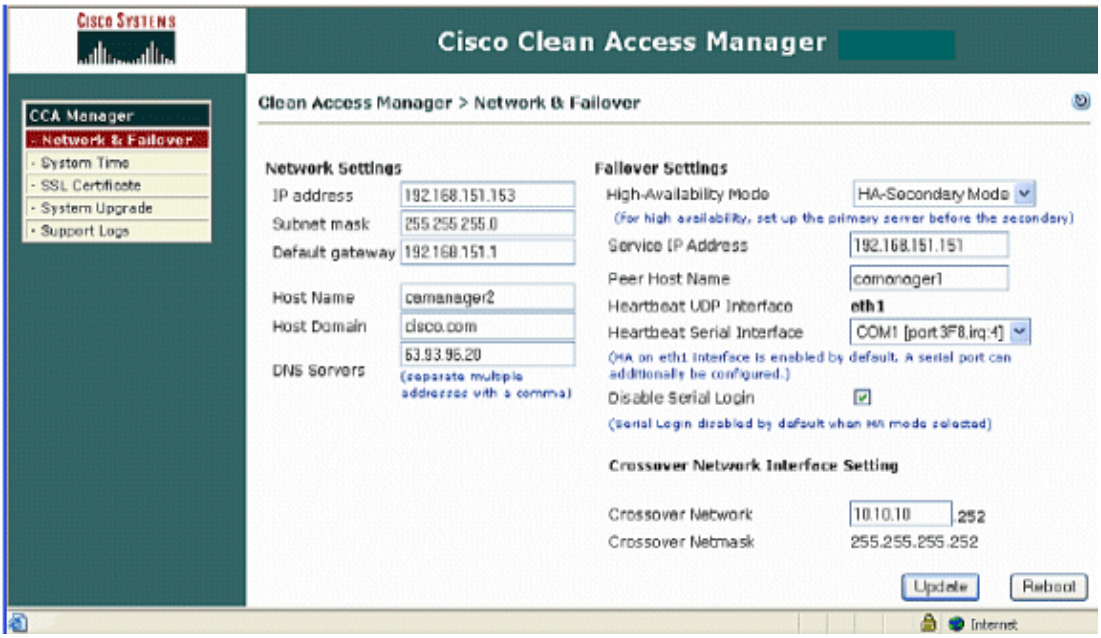
Note: The **Host Name** and **Peer Host Name** fields are case−sensitive. Make sure to match what is typed here with what was typed for the HA−Primary CAM.

6. Choose **HA−Secondary** in the **High−Availability Mode** drop−down menu. The High Availability settings appear.
7. Set the **Service IP Address** value under **Failover Settings** to the same value set for the **Service IP Address** in the HA−Primary CAM configuration.
8. Set the **Peer Host Name** value under **Failover Settings** to the host name of the HA−Primary CAM.

9. From the **Heartbeat Serial Interface** drop−down menu, choose the serial port to which you connected the serial cable of the HA−Primary CAM, or leave this n/a if you do not use a serial connection.
10. If your machine only has one serial port and you use COM1 as the Heartbeat Serial Interface, you must check the **Disable Serial Login** check box to ensure that the serial login is disabled on COM1. See Serial Connection for further details.
11. Type the same **Crossover Network Interface** settings as you had entered for the HA−Primary CAM.
12. Click **Update** and then **Reboot**.

When the standby CAM starts up, it automatically synchronizes its database with the active CAM.

Finally, open the admin console for the standby again and complete the configuration. Notice that the admin console for the standby now has only one management module.



Complete the Configuration

Verify the settings in the **Network & Failover** page for the standby CAM.

The High Availability configuration is now complete.

Failing Over an HA−CAM Pair

Warning: In order to prevent any possible data loss within database synchronization, always make sure that the standby CAM is live before failing over the active CAM.

In order to failover an HA−CAM pair, SSH to the active machine in the pair and perform one of these commands:

- **shutdown** or
- **reboot** or
- **service perfigo stop**

This stops all services on the active machine. When heartbeat fails, the standby machine assumes the active role. Perform **service perfigo start** to restart services on the stopped machine. This causes the stopped machine to assume the standby role.

Note: service perfigo restart must not be used to test High Availability (failover). Instead, Cisco recommends **shutdown** or **reboot** on the machine to test failover or the CLI commands, **service perfigo stop** and **service perfigo start**.

Useful CLI Commands for HA

These are useful directories to know for HA on the CAM:

- `/etc/ha.d/perfigo/conf`
- `/etc/ha.d/ha.cf`

This example shows the location of the HA debug/log files, as well as the name of each CAM (node) in the HA pair:

```
[root@cam1 ha.d]#more ha.cf
# Generated by make-hacf.pl
udpport 694
bcast   eth1
auto_failback      off
apiauth default  uid=root
log_badpack     false
debug   0
debugfile       /var/log/ha-debug
logfile /var/log/ha-log
#logfacility    local0
watchdog        /dev/watchdog
keepalive       2
warntime        10
deadtime        15
node    cam1
node    cam2
```

How to Verify Active/Standby Runtime Status on the HA CAM

This example shows how to use the CLI to determine the runtime status (active or standby) of each CAM in the HA pair. You can generally find the **fostate.sh** command from the /store directory of your last upgrade, for example, `/store/cca_upgrade-4.x.x.`

1. Run the **fostate.sh** script on the first CAM:

```
[root@cam1 cca_upgrade-4.x.x]# ./fostate.sh
My node is active, peer node is standby
[root@cam1 cca_upgrade-4.x.x]#

!--- This CAM is the active CAM in the HA-pair
```

2. Run the **fostate.sh** script on the second CAM:

```
root@cam2 cca_upgrade-4.x.x]# ./fostate.sh
My node is standby, peer node is active
[root@cam2 cca_upgrade-4.x.x]#

!--- This CAM is the standby CAM in the HA-pair
```

How to Verify Primary/Secondary Configuration Status on the HA CAM

This example shows how to use the CLI to determine the HA mode (Primary/Secondary) for which each CAM was initially configured in the HA pair.

1. Find the name of the CAMs (nodes) with `/etc/ha.d/ha.cf.`
2. Then check status on each CAM, for example:

```
[root@cam1 ~]# /perfigo/control/bin/check-ha cam1
active
[root@cam1 ~]# /perfigo/control/bin/check-ha cam2
active
```

3. Go to `/perfigo/control/tomcat and perform ls -la`.

   - If webapps points to **normal-webapps**, it is the primary CAM.
   - If webapps points to **admin-webapps**, it is the secondary CAM.

   For example, this CAM is the primary CAM:

```
[root@cam1 tomcat]# cd /perfigo/control/tomcat
[root@cam1 tomcat]# ls -la
total 216
drwxr-xr-x 12 root root 4096 Sep 14 23:28 .
drwxr-xr-x 8 root root 4096 Aug 28 22:12 ..
drwxr-xr-x 4 root root 4096 Aug 28 22:12 admin-webapps
<output cut&..>
drwxr-xr-x 2 root root 4096 Aug 28 22:12 temp
lrwxrwxrwx 1 root root 38 Sep 14 23:28 webapps ->
/perfigo/control/tomcat/normal-webapps
drwxr-xr-x 3 root root 4096 Aug 28 15:15 work
```

   This CAM is the secondary CAM:

```
[root@cam2 tomcat]# ls -la
total 216
drwxr-xr-x 12 root root 4096 Sep 14 23:33 .
drwxr-xr-x 8 root root 4096 Sep 15 2006 ..
drwxr-xr-x 4 root root 4096 Sep 15 2006 admin-webapps
<output cut &>
drwxr-xr-x 2 root root 4096 Sep 15 2006 temp
lrwxrwxrwx 1 root root 37 Sep 14 23:33 webapps ->
/perfigo/control/tomcat/admin-webapps
drwxr-xr-x 3 root root 4096 Sep 14 23:25 work
```

Troubleshoot

Problem 1

An error occurs on CAM **"SSKEY on server doesn't match the value in database"** when the secondary CAS in HA pair becomes active.

Solution

Resolve this problem when you manually push the primary CAS SSKEY to the secondary one (reset SSKEY button, or manual override on the /etc/.GUSSK file on the CAS). Usually, this problem occurs when you replace an appliance and do not delete/re-add it from/to the CAM. In this case, the CAS has its own SSKEY based on its MAC address and possibly does not match the one previously set on the CAM. This is especially true for the secondary CAS because it has a SSKEY based on its own MAC address. On the HA

configuration, even the secondary one has to use the primary CAS SSKEY based on the primary CAS MAC.

Problem 2

In the Failover CAM pair, the primary CAM shows the `WARNING! Closed connections to peer [x.x.x.x](standby IP Address) database! Please restart peer node to bring databases in sync!!` error message.

Solution

When the primary eth1 link has been disconnected and only the serial link remains, the CAM returns a database error that indicates that it cannot sync with its HA counterpart, and the administrator sees this error in the CAM web console: .

```
WARNING! Closed connections to peer [standby
         IP] database! Please restart peer node to bring databases in
         sync!!
```

Use self−signed or third−party certificates on the CAM pair in order to resolve this issue.

Problem 3

How to change the IP address for High Availability on CAM

Solution

Try to bring down the secondary CAM with **service perfigo stop**. This way, it does not run the perfigo services, but it is still accessible by SSH. On the primary CAM, change the IP in **Administration > CCA Manager > Network**. Do not let it reboot yet. Then go to the Failover tab, and change the Service IP address. After this step, then reboot it.

Once it is fully up, make sure it is reachable. Then run **service perfigo start** on the secondary CAM, and make the same changes as you did to the primary. Then, reboot it, and it should come up as the secondary. For the SSL cert, if it is issued to a name, then change the DNS entry so that the name resolves to the new service IP. If it is issued to the IP, regenerate a new temporary certificate. At this point, you probably want to have a test user login. If that succeeds, failover to the secondary, and make sure you are also able to login.

Related Information

- **Cisco NAC Appliance Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 05, 2009 Document ID: 99945