NAC设备(CCA) ：为Clean Access管理器的(CAM)配置高可用性(HA)

目录

简介

本文描述如何设置一个对Clean Access高可用性的(HA)管理器(CAM)机器。当Clean Access管理器在高性能的模式时部署，您能保证在一意外的关闭情形下，重要监听，验证和报告任务继续。

注意： 参考Cisco NAC设备的配置的高性能的(HA)部分- Clean Access服务器(CAS)安装和管理指南为了会配置在CAS的HA功能。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据思科网络准入控制(NAC)设备- CAM版本4.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

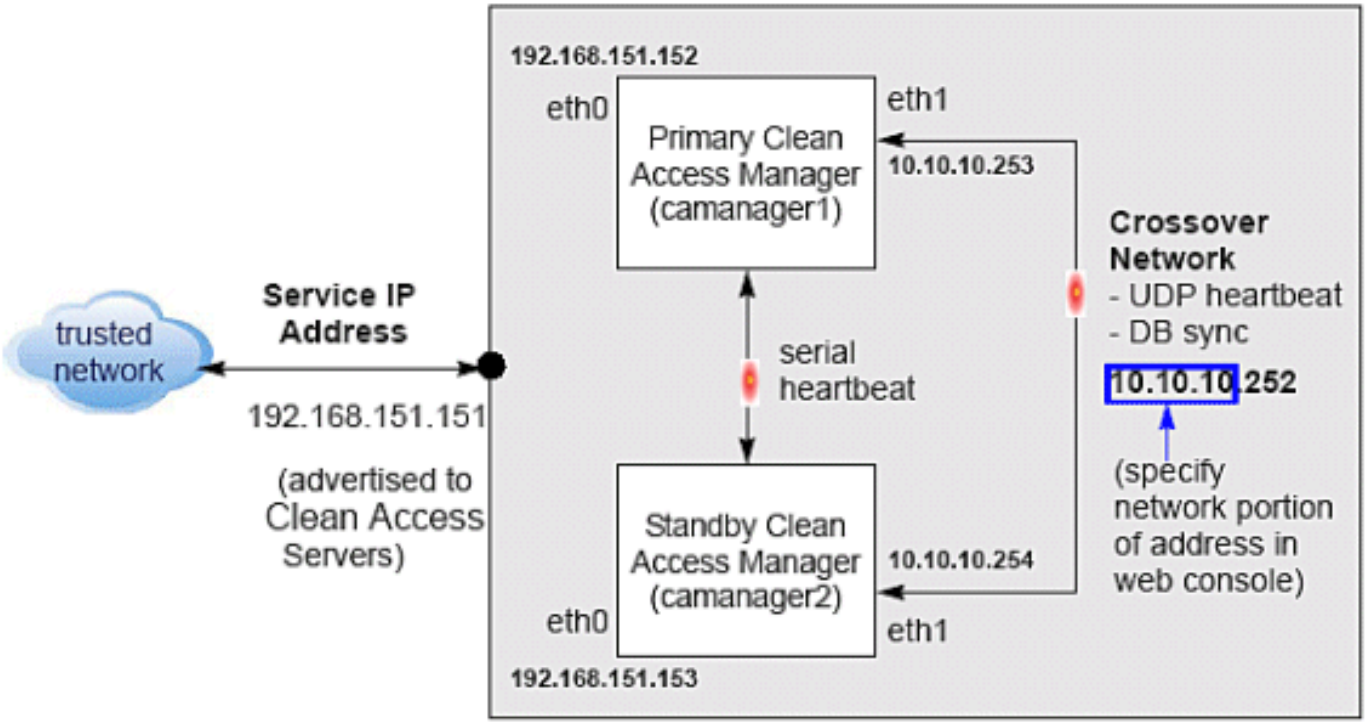
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

概述

这些关键点提供HA-CAM操作一高层次摘要：

1. Clean Access管理器高性能的模式是方面待机CAM计算机作为备份对激活CAM计算机的一个活动/被动服务器配置在。
2. 活动Clean Access管理器执行系统的所有任务。待机CAM监控激活CAM并且保持其数据库同步与激活CAM数据库。
3. 两CAM共享eth0受信接口的虚拟服务IP。必须用于域名SSL证书。
4. 主要的和附属CAM机器交换UDP心跳信息包每2秒。如果检测信号计时器超时，有状态故障切换发生。
5. eth1接口和serial interfaces在CAM可以用于心跳信息包和数据库同步。如果eth1和serial interfaces为检测信号配置，能的两接口上需要为了故障切换能发生。



Clean Access管理器高性能的模式是方面待机Clean Access管理器计算机作为备份对激活Clean Access管理器计算机的一个活动/被动服务器配置在。通常情况下时当激活CAM运载大多数工作量，备用监控程序激活CAM和保持其数据存储与激活CAM的数据同步。

如果故障切换事件发生，例如，如果激活CAM关闭或不响应对对等体的“检测信号”信号，待机呈现激活CAM的角色。

当您首先配置HA对等体时，您必须指定HA主要的CAM和HA第二CAM。最初， HA主要的是激活CAM，并且HA第二是待机(被动) CAM，但是活动/被动角色没有永久分配。如果主要的CAM断开，第二(待机)变为激活CAM。当原始主要的CAM重新启动，它呈现备份角色。

当Clean Access管理器开始时，它检查发现其对等体是否是活跃的。否则，开始的CAM呈现现任角色。如果开始的对等体是活跃的，另一方面， CAM变为待机。

您能同时配置两个Clean Access管理器作为一个HA对，或者您能添加一个新的Clean Access管理器到现存独立CAM创建一个高性能的对。为了对能出现对网络和Clean Access服务器作为一个实体，您必须指定作为受信接口(eth0)地址将使用的服务IP地址HA对。

为了创建高性能的信息交换的交叉电缆网络，您连接两CAM eth1端口并且指定在您的组织不当前路由的私有网络地址(默认HA交叉电缆网络是192.168.0.252)。Clean Access管理器然后创建每个CAM eth1端口的私有，安全，节点网络交换UDP检测信号流量和同步数据库。注意CAM总是使用eth1作为UDP检测信号接口。

对于额外的安全，您能也连接每个Clean Access管理器串行端口检测信号交换的。在这种情况下，UDP检测信号和序列检测信号接口必须不能为了备用系统能接管。

注意： 对于HA的串行电缆电缆连接(HA-CAM或HA-CAS)，串行电缆必须是“null modem”电缆。

基本要求，在您继续前

警告： 为了防止在数据库同步内的所有可能的数据丢失，总是请确保暂挂(附属) Clean Access管理器在故障切换活动(主要的) Clean Access管理器前是实际。

在您配置高可用性前，请保证您符合这些要求：

1. 您获取一个高性能的(故障切换)许可证。**注意：** 当您安装CAM故障切换(HA)时许可证，首先请安装故障切换许可证对主要的CAM，然后装载所有其他许可证。独立许可证可能也用于高可用性。
2. 两CAM安装并且配置。
3. 对于检测信号，每个CAM需要有一唯一主机名(或节点名)。对于HA CAM对，此主机名提供给对等体，并且一定是解决通过DNS或已添加对对等体的/etc/hosts文件。
4. 您有HA CAM对的域名的一个CA签发的证书。
5. HA主要的CAM为运行时操作充分地配置。这意味着对验证的连接来源，策略，用户角色，接入点，等等，是指定的全部。此配置在HA第二(待机) CAM自动地被复制。
6. 两个Clean Access管理器是可访问在网络(请设法ping他们测试连接)。
7. CAM软件安装的机器有一个自由以太网端口(eth1)和至少一个自由串行端口。请使用规格指南服务器硬件识别串行端口(ttyS0或ttyS1)每计算机的。
8. 在带外部署，端口安全在CAS和CAM连接的交换机接口没有启用。这能干涉CAS HA和DHCP交付。

这些步骤要求您重新启动Clean Access管理器。那时，其服务简要地不可用。当停机时间有在您的用户时的最少影响请配置联机CAM。

注意： Cisco NAC设备Web admin控制台支持在浏览器上的Internet Explorer 6.0或。

连接Clean Access管理器机器

有在HA-CAM对等体之间的两种连接类型：交换关连到Clean Access管理器活动和那个心跳信号的运行时数据的一。在高可用性， Clean Access管理器总是使用eth1接口数据交换和检测信号UDP交换。当UDP心跳信号不能在某一时间时传送和接收，备用系统接管。为了提供安全一次额外的测量，它是Clean Access管理器之间的一序列检测信号连接并列的高度推荐的添加。串行连接提供必须发生故障的一个另外的专用的检测信号交换方法，在备用系统能接管前。注意CAM对等体之间的eth1连接是必须。

实际上请联络对等体Clean Access管理器如显示：

- 请使用交叉电缆连接Clean Access管理器机器的eth1以太网端口。此连接使用检测信号UDP接口和数据交换(数据库镜像)在故障切换对等体之间。
- 请使用null modem串行电缆连接串行端口(高度推荐)。此连接使用作为另外的检测信号序列交换(keep-alive)在故障切换对等体之间。

注意： 对于HA的串行电缆电缆连接(HA-CAM或HA-CAS)，串行电缆必须是“null modem”电缆。

串行连接

如果计算机运行的Clean Access管理器软件有两个串行端口，您能使用额外端口序列检测信号连接。默认情况下，在CAM服务器检测的第一个串行端口为控制台输入/输出配置(实现安装和管理访问的其他类型)。

如果计算机只有一个串行端口(COM1或ttyS0)，您能重新配置端口担当高性能的检测信号连接。这是因为，在CAM软件安装后， SSH或KVM控制台可能总是用于访问CAM的命令行界面。

您能启用/禁用串行端口用在HA CAM设置的**禁用序列洛金**复选框(在**Administration > Clean Access Manager>网络&故障切换下|故障切换设置|禁用序列洛金**)。当只有CAM计算机的时一个串行端口，此复选框允许管理员禁用在COM1的序列登录，以便可以使用作为检测信号Serial interfaces一个对HA干净的访问管理器。

注意： 默认情况下序列登录在CAM**启用**。如果使用COM1 CAM的检测信号Serial interfaces，您必须点击**禁用序列洛金**复选框禁用在COM1的序列登录。

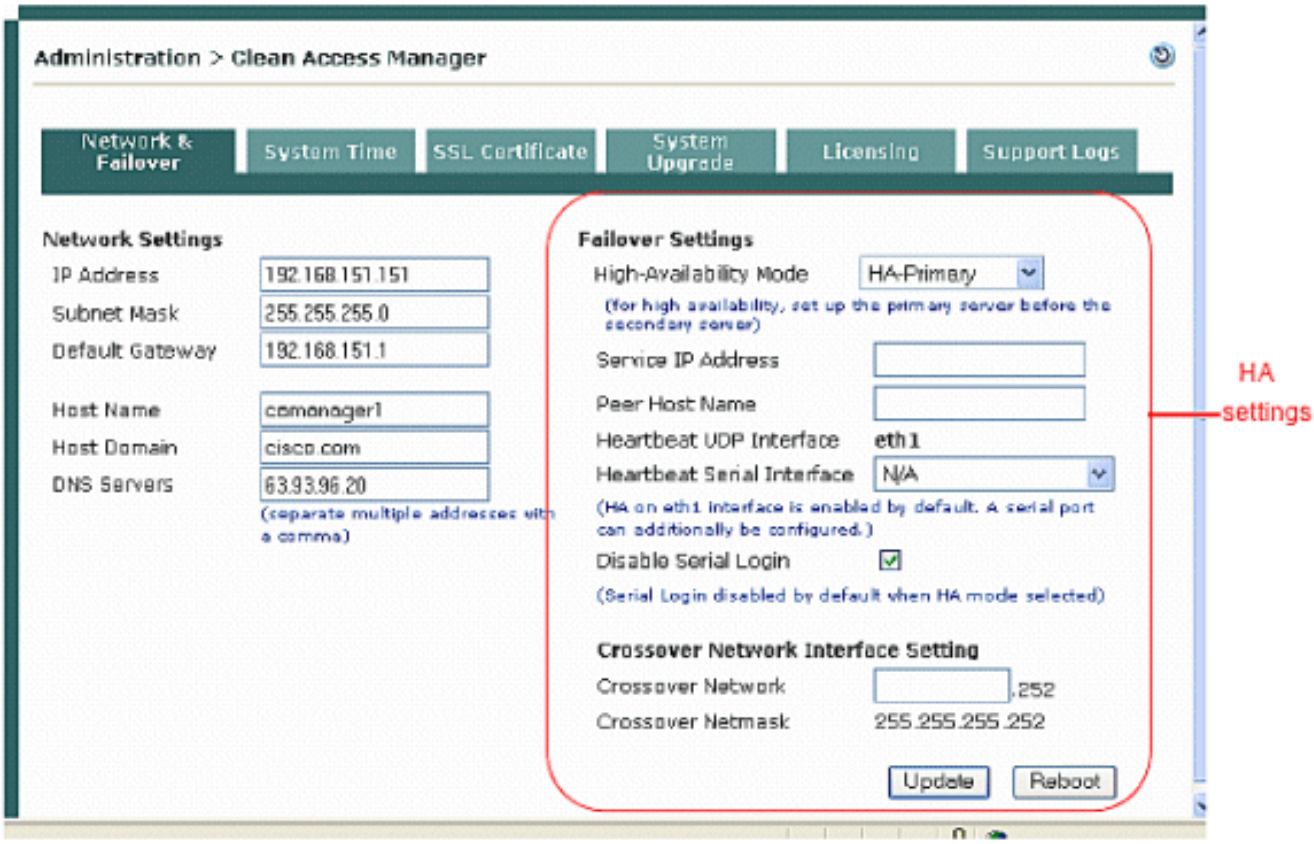
配置HA主要的CAM

一旦验证前提条件，请执行这些步骤配置Clean Access管理器作为HA主要的高性能的对的。参见图关于配置示例示例。

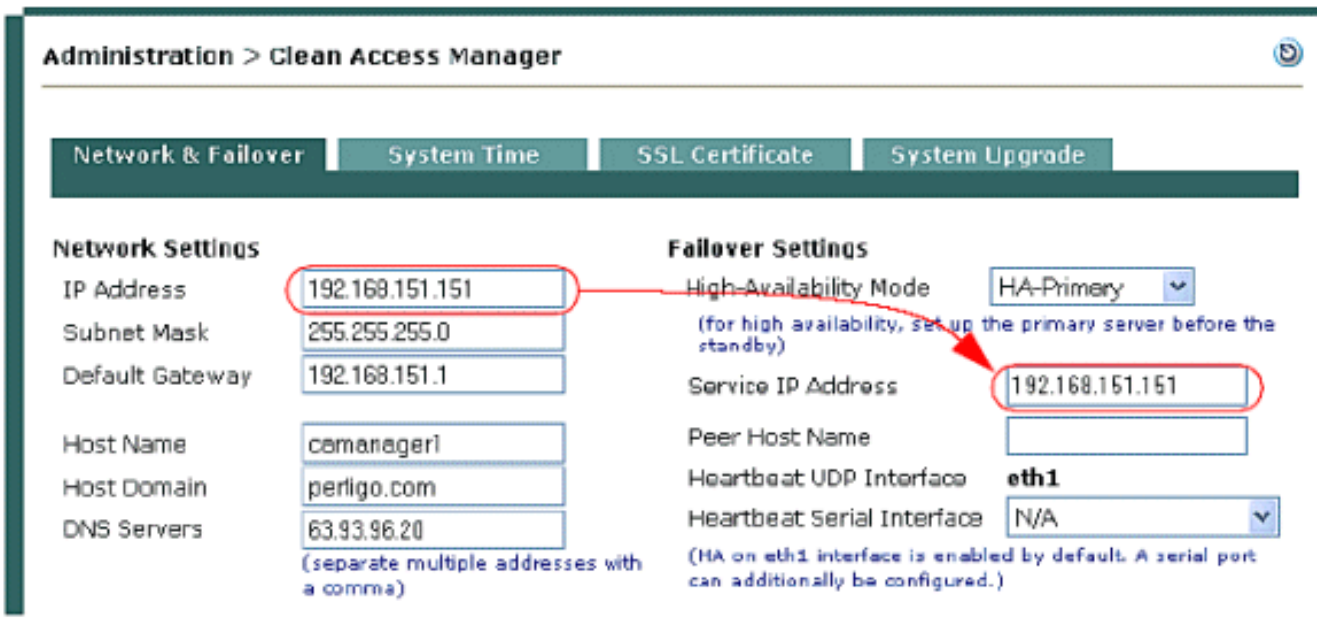
1. 打开作为HA主要的能将被选定的Clean Access管理器的Web admin控制台，并且去**Administration > CCA Manager>**配置主要的CAM的SSL证书的**SSL证书**。**生成临时证书**表出现。**注意：** 在本文的HA配置步骤假设，一临时证书从HA主要的CAM导出到HA第二CAM。*如果使用一临时证书HA对，请执行这些步骤：*填写**生成临时证书**表并且单击**生成**。必须为HA对的域名生成证书。在您生成临时证书后，请从**选择**选择**出口CSR/Private密钥/证书Action菜单**。点击**Export按钮当前安装的专用密钥的**导出SSL专用密钥。保存关键文件到磁盘。您必须导入此密钥到后HA第二的CAM。**当前**单击**Export按钮预装证书的**导出当前SSL证书。保存证书文件到磁盘。您必须导入此证书文件到后HA第二的CAM。*如果使用一个CA签发的证书HA对，请执行这些步骤：***注意：** CA签发的证书必须根据域名可解决对服务IP通过DNS。参考请管理CAM SSL证书在Cisco NAC设备的管理部分下- CAM安装和管理指南欲知更多信息。从**选择**

选择**进口证明书Action菜单**。在**证书文件**领域旁边请使用**浏览按钮**并且导航对CA签发的证书。从**文件类型**下拉菜单选择**CA签名的PEM-encoded X.509 Cert**。点击**加载**导入证书。注意您需要导入此同样证书到后HA第二的CAM。单击**验证并且安装上传的证书**。从**选择**选择**出口CSR/Private密钥/证书操作**下拉列表。点击**Export按钮当前安装的专用密钥的**导出SSL专用密钥关联与CA签发的证书。保存关键文件到磁盘。您需要导入此文件到后HA第二的CAM。

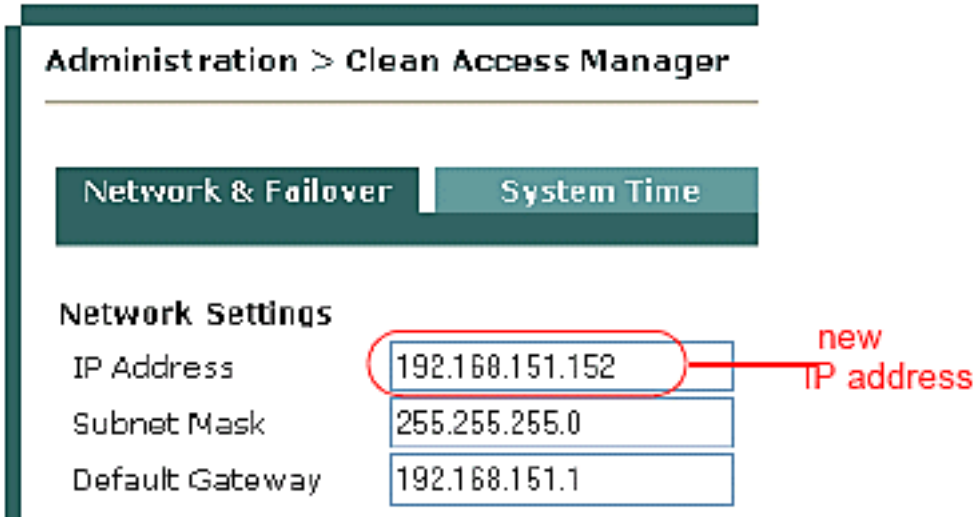
2. 去**Administration > CCA管理器**并且点击**网络&故障切换**选项卡。从**高可用性模式**下拉菜单选择HA**主要的**选项。高可用性设置出现。



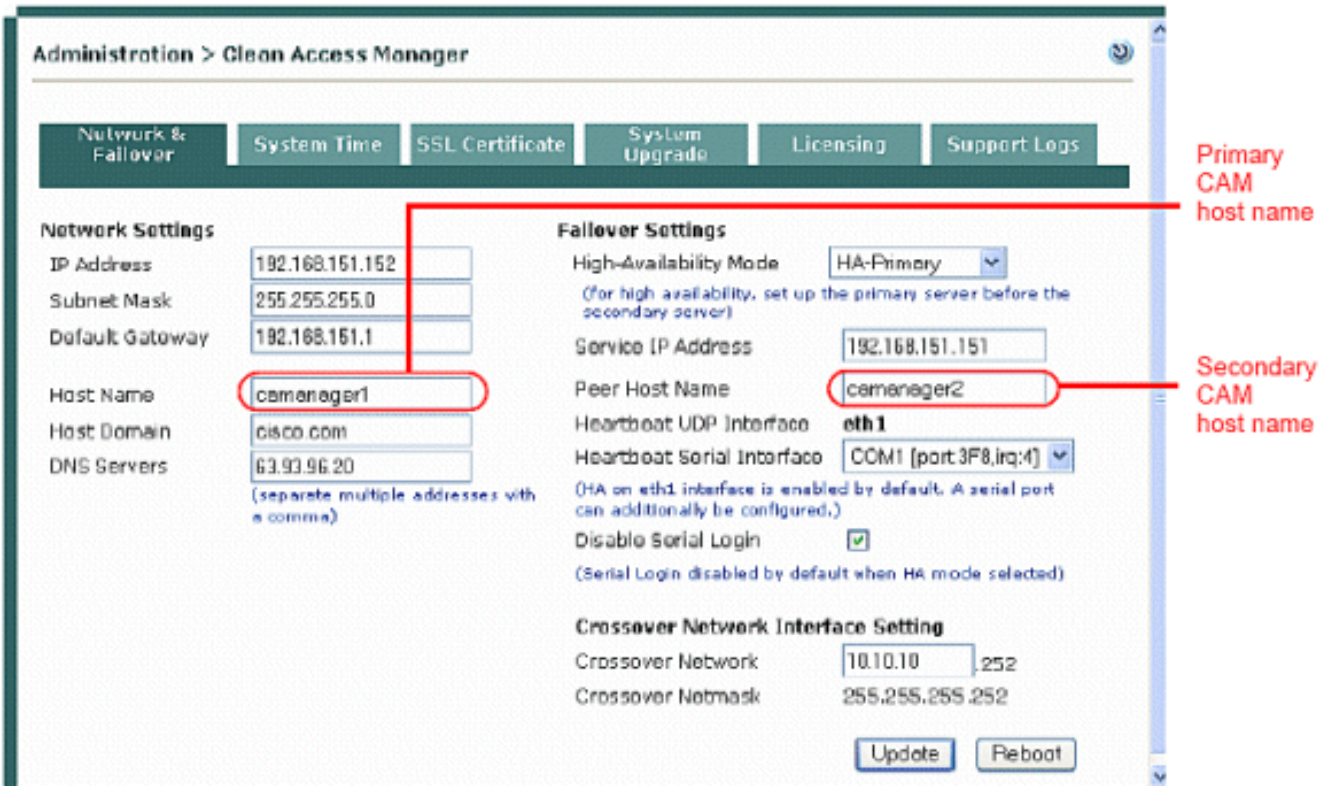
3. 复制从**IP地址字段的**值在**网络设置下**并且输入它在**服务IP地址字段**。网络设置IP地址是当前Clean Access管理器的现存IP地址。此处想法是把此IP地址变成， Clean Access服务器已经认可， Clean Access管理器对的虚拟服务IP地址。



4. 更改IP地址在**网络设置下**对可用地址，例如， n.152。



5. 每个Clean Access管理器必须有一唯一的主机名称，例如camanager1和camanager2。键入HA主要的CAM的主机名在**主机名字段**在**网络设置下**，并且键入HA第二CAM的主机名在**对等体主机名字段**在**故障切换设置下**。



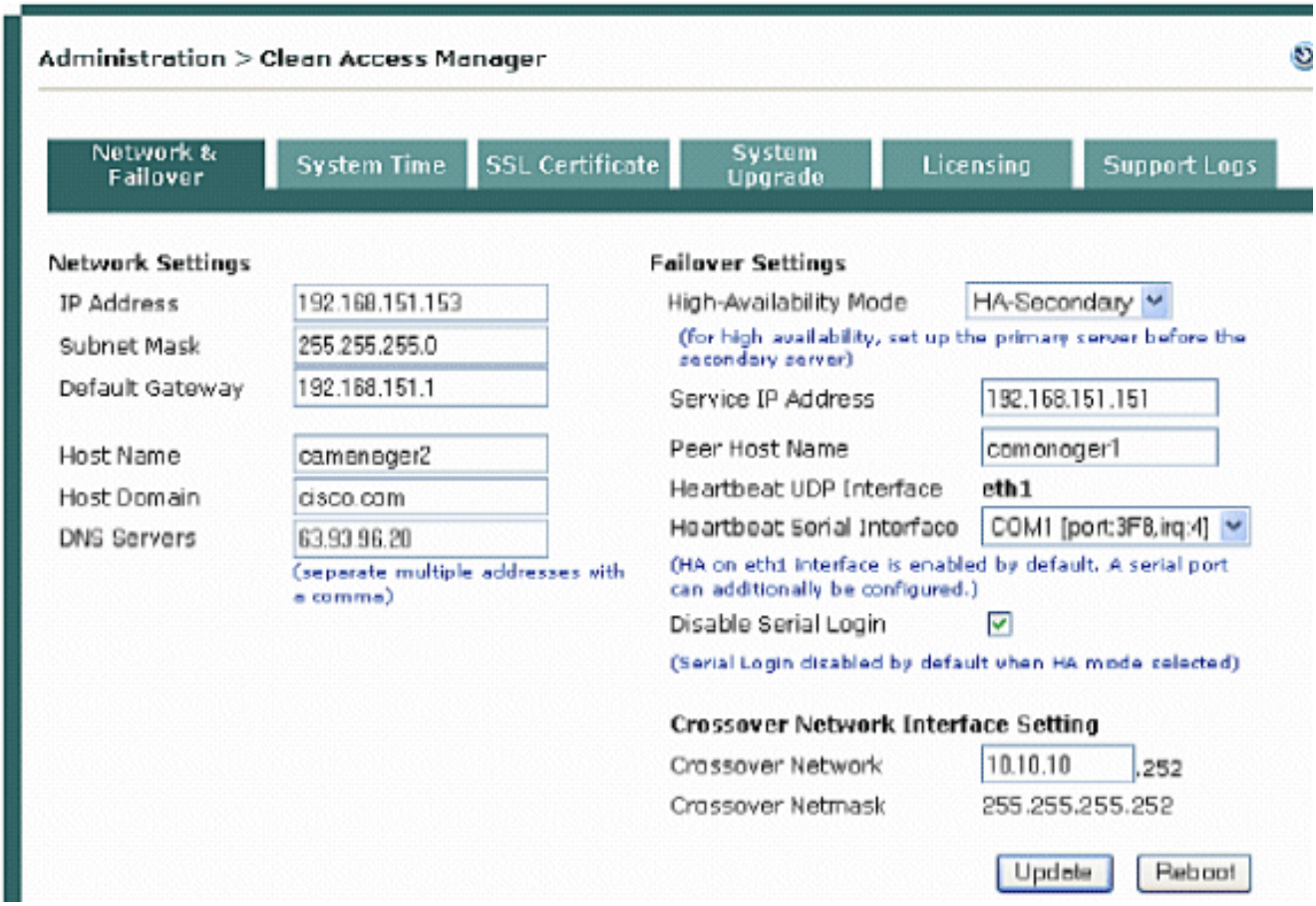
主机名值是必须，当您设置高可用性时，而**主机域名**可选。**主机名**和**对等体主机名字段**区分大小写。确保匹配什么键入此处与什么为后HA第二的CAM被键入。

6. 从**检测信号Serial interfaces**下拉菜单，请选择您连接HA主要的CAM的串行电缆的串行端口，或者留下此n/a，如果不使用串行连接。
7. 如果您的计算机只有一个串行端口，并且使用COM1作为检测信号Serial interfaces，您必须检查**禁用序列洛金**复选框保证序列登录在COM1禁用。请参阅串行连接关于更详细的资料。
8. 为了通过交叉电缆网络保持同步， Clean Access管理器对等体交换数据。您必须指定在您的组织不当前路由的私有网络地址空间在**交叉电缆网络字段**，例如10.10.10。提供的默认交叉电缆网络是192.168.0.252。如果此与您的网络的地址冲突，确保指定一个不同的专用地址空间。例如，如果您的组织使用私有网络192.168.151.0，使用10.1.1.x作为交叉电缆网络。IP地址的子网掩码和最后一个八位位组在**交叉电缆网络字段**修复，那么只输入IP地址的网络部分。
9. 点击**更新**然后**重新启动**重新启动Clean Access管理器。在Clean Access管理器重新启动，确保后， CAM计算机适当地运作。确认Clean Access服务器是否连接，并且新用户验证。

配置HA第二CAM

执行这些步骤配置HA第二CAM。

1. 打开作为HA第二能将被选定的Clean Access管理器的Web admin控制台，并且去**Administration > CCA Manager> SSL证书**。
2. 在您继续前，请执行这些步骤：备份第二CAM的专用密钥。确保专用密钥，并且SSL证书文件关联与服务IP/HA主要的CAM是可用的(以前导出正如所描述请配置HA主要的CAM)。
3. 导入HA主要的CAM的专用密钥文件和证书如描述：在**SSL证书**选项卡，请从**选择**选择**进口证明书Action菜单**。单击在**证书文件**领域旁边**浏览**，并且浏览对您的专用密钥文件的备份副本生成与使用HA对的证书。选择**专用密钥**作为文件类型。点击**加载**上传专用密钥。当**进口证明书**选择从**选择Action菜单**，浏览对关联与专用密钥的证书(临时或CA签名的)。选择**CA签名的PEM-encoded X.509 Cert**作为文件类型。点击**加载**上传临时证书或CA签发的证书。单击**验证并且安装上传的证书**。参考管理CAM SSL证书在Cisco NAC设备的管理部分下- CAM安装和管理指南欲知更多信息。
4. 去**Administration > CCA Manager>网络&故障切换|网络设置**和更改第二CAM的IP地址对是与HA主要的CAM IP地址和服务IP地址不同的地址。



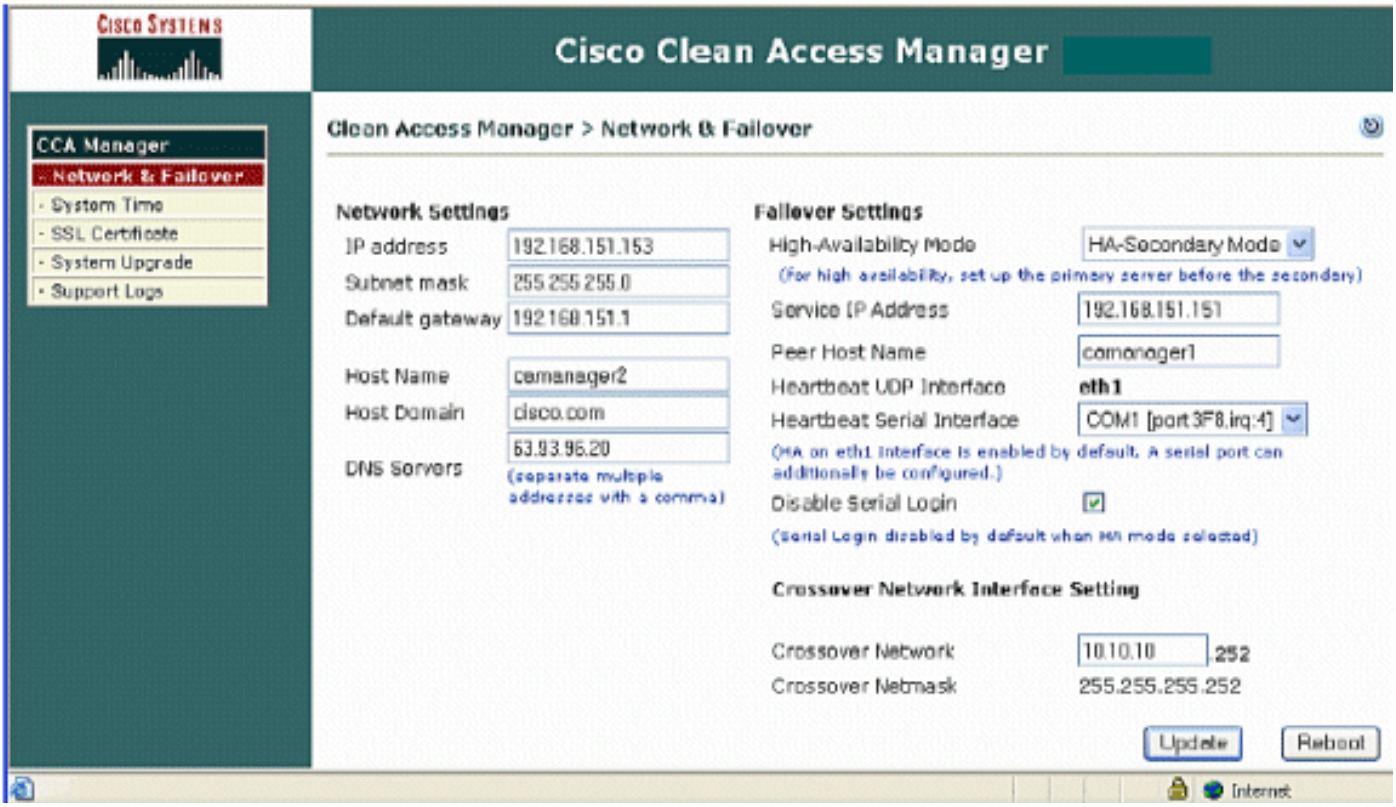
5. 设置**主机名**值在**网络设置下**为**对等体主机名的**同一值集在HA主要的CAM配置里。参见在HA主要的部分的图。**注意： 主机名**和**对等体主机名字段**区分大小写。确保匹配什么键入此处与什么为HA主要的CAM被键入了。
6. 选择在**高可用性模式**下拉菜单的HA**第二**。高可用性设置出现。
7. 设了**服务IP Address值**下面**故障切换设置**为**服务IP地址的**同一值集在HA主要的CAM配置里。
8. 设置**对等体主机名**值在**故障切换设置下**为HA主要的CAM的主机名。
9. 从**检测信号Serial interfaces**下拉菜单，请选择您连接HA主要的CAM的串行电缆的串行端口，或者留下此n/a，如果不使用串行连接。
10. 如果您的计算机只有一个串行端口，并且使用COM1作为检测信号Serial interfaces，您必须

检查**禁用序列洛金**复选框保证序列登录在COM1禁用。请参阅串行连接关于更详细的资料。

11. 键入和一样您为HA主要的CAM输入了的**交叉电缆网络接口**设置。
12. 点击**更新**然后**重新启动**。

当待机CAM开始时，与激活CAM自动地同步其数据库。

最后，再请打开待机的admin控制台并且完成配置。注意待机的admin控制台只当前有一个管理模块。



完成配置

验证在**网络&故障切换**页的设置待机CAM的。

高性能的配置当前完成。

故障切换一个HA-CAM对

警告： 为了防止在数据库同步内的所有可能的数据丢失，总是请确保待机CAM在故障切换激活CAM前是实际。

为了故障切换每HA-CAM对，对活动计算机的SSH在对和执行这些命令之一：

- **关闭**或
- **重新启动**或
- **服务perfigo终止**这终止在活动计算机的所有服务。当检测信号发生故障时，暂挂计算机呈现现任角色。进行**服务perfigo开始**重新启动在被终止的计算机的服务。这造成被终止的计算机呈现暂挂角色。**注意： 服务不**能用于**perfigo重新启动**测试高可用性(故障切换)。反而，思科推荐**关闭**或**重新启动**在计算机测试故障切换或CLI命令，**服务perfigo终止**和**服务perfigo开始**。

HA的有用的CLI命令

这些是要知道的有用的目录为在CAM的HA ：

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

此示例显示HA调试/日志文件的位置，以及名称每个CAM (节点)在HA对：

```
[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
```

如何验证在HA CAM的活动/等待运行时状态

此示例显示如何使用CLI确定运行时状态(能起作用的或备用的)在HA对的每个CAM。您能通常找到fostate.sh命令从您的最后升级/store目录，例如， /store/cca_upgrade-4.x.x

1. 运行在第一个CAM的fostate.sh脚本：[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. 运行在第二个CAM的fostate.sh脚本：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*

如何验证在HA CAM的首选/备用的配置状态

此示例显示如何使用CLI确定HA模式(首选/备用的)哪些每个CAM在HA对最初配置。

1. 查找CAM (节点)的名称与/etc/ha.d/ha.cf
2. 例如然后请检查在每个CAM的状态， ：[root@cam1 ~]# /perfigo/control/bin/check-ha cam1
   active
   [root@cam1 ~]# /perfigo/control/bin/check-ha cam2
   active
3. 去/perfigo/control/tomcatls - la。如果webapps指向正常webapps，它是主要的CAM。如果webapps指向Adminwebapps，它是第二CAM。例如，此CAM是主要的CAM ：[root@cam1
   tomcat]# cd /perfigo/control/tomcat
   [root@cam1 tomcat]# ls -la
   total 216
   drwxr-xr-x12 root root4096 Sep 14 23:28 .
   drwxr-xr-x8 root root4096 Aug 28 22:12 ..
   drwxr-xr-x4 root root4096 Aug 28 22:12 admin-webapps
   <output cut…..>
   drwxr-xr-x2 root root4096 Aug 28 22:12 temp
   lrwxrwxrwx1 root root38 Sep 14 23:28 **webapps -> /perfigo/control/tomcat/normal-webapps** drwxr-xr-x 3 root root 4096 Aug 28 15:15 work 此CAM是第二CAM ：[root@cam2
   tomcat]# ls -la
   total 216
   drwxr-xr-x12 root root4096 Sep 14 23:33 .
   drwxr-xr-x8 root root4096 Sep 152006 ..
   drwxr-xr-x4 root root4096 Sep 152006 admin-webapps
   <output cut …>
   drwxr-xr-x2 root root4096 Sep 152006 temp
   lrwxrwxrwx1 root root37 Sep 14 23:33 **webapps -> /perfigo/control/tomcat/admin-webapps**
   drwxr-xr-x 3 root root 4096 Sep 14 23:25 work

故障排除

问题 1

当在HA对的第二CAS变得激活时，错误在CAM **“在服务器的SSKEY出现不匹配在数据库的值”**。

解决方案

请解决此问题，当您手工推送主要的CAS SSKEY到附属一个时(重置SSKEY按钮或者人工改写在/etc/.GUSSK文件在CAS)。通常，当您替换设备，并且不删除/重新加写它从/至CAM，此问题发生。在这种情况下， CAS有根据其MAC地址的其自己的SSKEY和可能不匹配在CAM以前设置的那个。因为独自地有SSKEY基于MAC地址，这是准确无误的对第二CAS。在HA配置，附属一个必须使用根据主要的CAS MAC SSKEY的主要的CAS。

问题 2

在故障切换CAM对，主要的CAM显示`![x.x.x.x] (IP)!!!`错误消息。

解决方案

当主要的eth1链路被断开了时，并且仅串行链路依然存在， CAM返回表明的数据库错误不能同步与其HA副本，并且管理员看到在CAM Web控制台的此错误：.。

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

请使用在CAM对的自己签署的或第三方证书为了解决此问题。

问题 3

如何更改高可用性的IP地址在CAM

解决方案

设法减少与**服务perfigo终止的**第二CAM。这样，它不管理perfigo服务，但是由SSH是可访问。在主要的CAM，请更改在**Administration > CCA Manager>网络的**IP。请勿让它重新启动。然后请去故障切换选项卡，并且更改服务IP地址。在此步骤，然后重新启动它后。

一旦它充分地，请确保它可及的。然后请运行**服务**在第二CAM的**perfigo开始**，并且做和一样您完成对主要的变动。然后，请重新启动它，并且应该出现作为第二。对于SSL cert，如果发出对名称，然后请更改DNS条目，以便名称解决对新的服务IP。如果它发出对IP，请重新生成一新的临时证书。这时，您很可能要有测试用户登录。如果那成功，对第二的故障切换，和确保您也能登陆。

相关信息

- Cisco NAC设备支持页面
- 技术支持和文档 - Cisco Systems