APPENDIX E

Troubleshooting

The following sections describe the major areas in the Cisco IP Solution Center installation in which troubleshooting might be necessary:

Unable to Find the Hostname

Symptom

Cannot find hostname.

Recommended Action

Step 1 If you cannot find the hostname, check the **/etc/nsswitch.conf** file to determine how the hostname is resolved.

Step 2 Check the /etc/resolv.conf file to determine whether you have a DNS Server IP Address.

Step 3 If you have a DNS Server IP Address, enter **ping** <*IP Address*> to check whether it is reachable.

Step 4 If the DNS Server is reachable, use **nslookup** <*machine name*> to check if it is resolving the name properly.

Step 5 If it is not working properly, you need a system administrator to fix the DNS entry.

Step 6 If you are not using DNS, be sure there is an entry for your machine in the **hosts** file in the **/etc** directory.

Moving a Repository or Renaming an ISC Server

If you want to move an existing Repository to a new server with a new ISC installation or rename an existing ISC installation, your existing configuration *must* be updated. When renaming the ISC installation, the local configuration file needs to be modified. When moving an existing Repository to a new server, the server from which you are moving the Repository and the server to which you are moving the Repository *must* both be at the same version and patch levels. Otherwise, your Repository needs to be upgraded, as explained in Upgrading ISC Repositories to ISC 5.1, page 2-25. Both when moving an existing Repository and renaming an existing ISC installation, the changes must be inserted into the Repository.

Use the following steps:

Step 1 Stop ISC, using the following command:

stopall

Step 2 Edit the **install.cfg** file found in **$ISC_HOME/etc**. In this file are references to the old host, which must be replaced with the new hostname. Then apply these changes, using the following command:

applycfg.sh

Step 3 Start the database, using the following command:

startdb

Step 4 Incorporate the changes into the Repository by initializing the database, using the following command:

initdb.sh

Step 5 Start ISC, using the following command:

startwd

Multiple ISC Instances with the Same TIBCO Rendezvous Port

Symptom

You might not see any error messages or a page might not appear, but you might see inconsistencies with events and tasks that you have just created.

Recommended Action

You might have more than one ISC server on the same subnet of a LAN, in which case, multiple instances of the ISC server will have the same TIBCO Rendezvous port. To fix this problem, you must ensure that the TIBCO port has a unique value.

To change the value for the TIBCO port, follow these steps:

Step 1 From the terminal window where the WatchDog is running, stop the WatchDog with the following command:

stopwd -y

Step 2 Use a text editor to open the **etc/install.cfg** file.

Step 3 Change the TIBCO_PORT variable to the desired value.

The default value for the TIBCO_PORT variable is 7530.

Step 4 To update all the dependent files with the new TIBCO port value, run the **applycfg.sh** command.

Step 5 **startdb**

Step 6 **initdb.sh**

Step 7 **stopdb -y**

Step 8 **ps -e | grep rvrd**

The returned result is the process id for the rvrd process.

Step 9 **kill -9** <*process id*>

where: <process id> is the returned process from Step 8.

Step 10 **rm -f $ISC_HOME/tmp/rvrd.isc.store**

Step 11 **rvrd -store $ISC_HOME/tmp/rvrd.isc.store**

Step 12 **startwd**

Step 13 Run the following multiple line Java command:

java -classpath $VPNSC_HOME/resources/java/classes/common:

$VPNSC_HOME/thirdparty/rv/lib/rvconfig.jar:

$VPNSC_HOME/thirdparty/rv/lib/tibrvj.jar:

**$VPNSC_HOME/thirdparty/rv/lib/tibrvjweb.jar **

com.cisco.vpnsc.install.RvrdCfg <*tibco_port*> <*server*> **isc**

where:

<*tibco_port*> is the desired port specified in Step 3.

<*server*> is the server name, for example: **server1.cisco.com**.

Known Installation Issues

Known issues and solutions are as follows:

Symptom 1

Out of disk space.

Recommended Action

The error looks something like the following:

```
ISC 5.1 will be installed in /var/isc-5.1
>Copying files ...
>Copying sybase...
>tar:./shared/jre_1.3.1_solaris_sun_sparc/lib/rt.jar: HELP - extract
>write error
>Error copying Sybase
```

If you see an error like this, it is likely due to the server running out of disk space.

To verify what space is available, run the command **df -k** <*install directory*>.

See Chapter 1, "System Recommendations," for the disk space recommendations.

Symptom 2

The Installation utility GUI never displays.

Recommended Action

This problem should be accompanied with a Java stack dump.

Step 1 Run the following command to check for the $DISPLAY environment variable being set:

echo $DISPLAY.

If you use the secure shell (ssh), then this will be set up and managed for you.

If you manually change the $DISPLAY environment variable in an SSH environment, the easiest recovery method is to log off and reestablish the SSH connection.

Step 2 To set the DISPLAY environment variable, do the following:

a. For the K or Bourne shell:

export DISPLAY=<*machine name*>**:0.0**

b. For the C-shell:

setenv DISPLAY=<*machine name*>**:0.0**

Symptom 3

Cannot run command scripts.

Recommended Action

If the command scripts are not running or cannot be found, it usually means that the ISC environment has not been sourced.

- For the C-shell: **source $ISC_HOME/bin/vpnenv.csh**
- For the K-shell and Bourne-shell: **. $ISC_HOME/bin/vpnenv.sh**

Symptom 4

Could not find temporary files.

Recommended Actions

If you receive an error that says the temporary file could not be created or found, it usually means the location used to write the temporary file is write-protected or out of disk space.

The two places that ISC uses for temporary files are **/tmp** and **/var/tmp**.

- Make sure both locations have write permission by doing a long list on the directories (**ls -la**). The directory should have wide open permissions: **drwxrwxrwx**.
- There is another temporary file problem that can arise, especially in cases where there have been previous aborted installation attempts—existing temp files might be left by previous installations. If this is the case, it is best to clean out all the files in the temp directories after aborted installation attempts.

Symptom 5

Running **install.sh** fails.

Recommended Action

Running **install.sh** can fail due to the following reasons:

1. You are not root.

   Although it is possible to install as non-root if you have appropriate permissions in the target directory, this will still have problems since only root can write to **/etc/init.d** where the startup scripts reside. Therefore, it is easier to install as root.

2. You do not have enough disk space in the target directory. To find out the available disk space, issue the following command:

   df –k <*target directory*>

3. You do not have enough disk space in the **/tmp** directory. Issue the command **df –k /tmp** to determine the available disk space for **/tmp**.

4. You do not have enough disk space in the **/var/tmp** directory. Issue the command **df –k /var/tmp** to determine the available disk space for **/var/tmp**.

5. The PATH and LD_LIBRARY_PATH environment variables are incorrect.

   Make sure your PATH and LD_LIBRARY_PATH environment variables are correct.

   Example:

   ```
   PATH=/usr/bin:/usr/local/bin
   LD_LIBRARY_PATH=/usr/lib:/usr/local/lib
   export PATH LD_LIBRARY_PATH
   ```

   a. Alternatively, start a clean root shell with this command:

      env – ksh

   b. Then issue a command like the following:

      ```
      ./install.sh /opt/isc-5.1 iscadm
      ```

Symptom 6

ISC does not start on reboot.

Recommended Action

Do the following:

Step 1 Install ISC as the root user.

If you install as root, **init.d** has a script to start the Watchdog.

If you do not install as root, you do not get the startup on reboot feature.

Step 2 To become root, enter the following command:

su root

Step 3 Get the **isc.tmpl** file from the installation media.

Step 4 Edit the following fields in **isc.tmpl**:

`OWNER=_owner - replace _owner` with the username whom owns isc

`ISC_HOME=_vpnsc_home - replace _vpnsc_home` with the isc directory

Step 5 Rename isc.tmpl as isc and then enter the following commands:

```
mv isc /etc/init.d
chmod 744 /etc/init.d/isc
```

Step 6 Create the following symbolic links to **isc**:

a. `cd /etc/rc1.d`

   `ln -s /etc/init.d/isc K98ISC`

b. `cd to /etc/rc2.d`

   `ln -s /etc/init.d/isc K98ISC`

c. `cd to /etc/rc3.d`

   `ln -s /etc/init.d/isc S99ISC`

Symptom 7

Unable to create or delete IOS devices in the Cisco CNS IE2100 appliance repository when using Cisco CNS Configuration Engine 1.4 software with ISC.

Recommended Action

Log in to the Cisco CNS IE2100 appliance as **root** and modify the **web.xml** file located at **/opt/CSCOcnsie/WEB-INF** as follows.

Step 1 Locate the following entry:

```
<servlet>
<servlet-name>ServletLoadComplete</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ServletLoadComplete</servlet-class>
<load-on-startup>105</load-on-startup>
</servlet>
```

Step 2 Immediately after the entry found in Step 1, insert the following lines:

```
<servlet>
<servlet-name>ImportDevice</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ImportDevice</servlet-class>
<load-on-startup>100</load-on-startup>
</servlet>


<servlet>
<servlet-name>ImportTemplate</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ImportTemplate</servlet-class>
<load-on-startup>100</load-on-startup>
</servlet>
```

<servlet>
<servlet-name>**RemoveDevice**</servlet-name>
<servlet-class>**com.cisco.cns.cfgsrv.RemoveDevice**</servlet-class>
<load-on-startup>**100**</load-on-startup>
</servlet>

<servlet>
<servlet-name>**RemoveTemplate**</servlet-name>
<servlet-class>**com.cisco.cns.cfgsrv.RemoveTemplate**</servlet-class>
<load-on-startup>**100**</load-on-startup>
</servlet>

Step 3 Locate the following entry:

```
<servlet-mapping>
<servlet-name>ServletLoadComplete</servlet-name>
<url-pattern>/ServletLoadComplete</url-pattern>
</servlet-mapping>
```

Step 4 Immediately after the entry found in Step 3, insert the following lines:

```
<servlet-mapping>
<servlet-name>ImportDevice</servlet-name>
<url-pattern>/ImportDevice</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>ImportTemplate</servlet-name>
<url-pattern>/ImportTemplate</url-pattern>
</servlet-mapping>
```

<servlet-mapping>
<servlet-name>**RemoveDevice**</servlet-name>
<url-pattern>**/RemoveDevice**</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>**RemoveTemplate**</servlet-name>
<url-pattern>**/RemoveTemplate**</url-pattern>
</servlet-mapping>

Step 5 Reboot the Cisco CNS IE2100 appliance.

Symptom 8

Not able to connect to the database.

Recommended Action

Use the following steps:

Step 1 Check that the following values are substituted correctly in the installation window:

- Oracle database server name
- Oracle port number
- SID

Step 2 If everything is correct, check that the server is reachable by entering:

ping <*Oracle database server name*>

Step 3 Issue the following to determine whether the database is running:

netstat -an | grep <*oracle port number*>

If no responses are found, your database is not running and you must restart, as explained in detail in the section, "Launching Oracle and Opening Your Database," in Appendix A, "Setting Up Oracle for ISC."

Symptom 9

Unable to access ISC with your web browser.

Recommended Action

Check the server status with the command **wdclient status**.

If any server state is other than s**tarted**, attempt to restart by entering the command, **wdclient restart** <*server name*>. If this command does not succeed, enter the commands **stopall** and then **startwd**.

Note The most common server not to start is the **httpd** server.

Daylight Saving Time

If Daylight Saving Time (DST) is not working correctly, follow these steps:

Step 1 Go to the following URL to determine which patch is needed for your time zone:
http://java.sun.com/javase/timezones/tzdata_versions.html

Step 2 To download the Java Runtime Environment (JRE) patch, go to:
http://java.sun.com/javase/downloads/index.jsp#timezone

Step 3 Enter: **source $ISC_HOME/bin/vpnenv.csh**

Step 4 Enter: **stopall**

Step 5 Follow this link to install the missing DST patch that you downloaded from Step 2:
http://java.sun.com/javase/tzupdater_README.html

1

Error - DBSPAWN ERROR: -84

The error: **DBSPAWN ERROR: -84** is normally seen when the existing log files are not removed before loading a new **repository.db** file. The **repository.log** and **sla.log** files in the Repository/ directory must be deleted before initiating the **startdb** command.

Error - No VPNSC Host Entry in the Database, When Starting ISC

To correct the error: **No VPNSC Host Entry in the Database**, run **initdb.sh** in the following order:

Step 1 **stopall**
Ensure that no other ISC processes are running. To do this, you can enter: **ps -ef | grep isc**

Step 2 **startdb**

Step 3 **initdb.sh**
This step adds the host entry into the repository.

Step 4 **startwd**

Error - Could Not Connect to the Name Server, When Starting ISC

The error: **com.cisco.vpnsc.watchdog.WDRuntimeException: WD_108 :: Could not connect to the name server** is normally seen when the domain name cannot be extracted from **resolv.conf**. The result is that the nameserver does not start, because it fools the system into thinking it is not a Master server.

To correct this error, you must have root privileges. As root, add the correct domain statement to the **/etc/resolv.conf** file for your server (not **$ISC_HOME/etc**); for example, **domain cisco.com**.

Error - This Is Not a Database Server

The following error could occur after you install ISC:
<*server name*> **startdb Master database server is: This is not a database server. There is no need to start the database**
Adding this host to the database ... com.cisco.cns.security.common.CannotConnectException: Cannot connect to the data store:Cannot connect to the data store. No valid connection to server type: com.cisco.cns.security.dataaccess
at com.cisco.cns.security.dataaccess.ConnectionPool.acquire (ConnectionPool.java:240)

Specifically, this could occur after issuing the command: **./install.sh** <*directory_where_ISC_is_to_be_installed*> **iscadm**.

The error could be Domain Naming System (DNS) related. In the **install.cfg** file, <*server name*>**.cisco.com** needs to be changed to <*server name*> only. Then run **applycfg.sh** followed by **initdb.sh** and **startwd**.

Error - Cannot Connect to the Data Store

The primary reason for the error: **Cannot Connect to the Data Store** is DNS related. As **root**, make sure **/etc/resolv.conf** (not the **$ISC_HOME/etc** directory) is correct for your server.

If you need more information, set the Security Policy Engine (SPE) logging to DEBUG and attempt to execute **initdb.sh**. This provides more details. If an unknown host exception is created, double check the **/etc/hosts** file and the **/etc/nsswitch.conf** file. This controls the flow and sequence of the hostname lookup.

If DNS is not enabled or working, add the IP address to the following files: **cns**, **vpnsc**, and **HA properties** files, to use IP addresses instead of hostnames.

The **cns properties** files is located at **$ISC_HOME/etc/spe/cns.properties**.

The **vpnsc properties** file is located at **$ISC_HOME/etc/vpnsc.properties**.

The **HA properties** file is located at **$ISC_HOME/etc/HA.properties.**

Echo Mode

This explanation of Echo mode is specified in the following subsections:

What is Echo Mode?

Echo mode is a setting in ISC that is accessible through the ISC configuration window. Echo mode affects service provisioning. When you set ISC to run in echo mode, ISC performs service provisioning tasks without downloading the resulting commands to the physical hardware. The resulting service provisioning is stored only in the Repository, and no attempt is made to connect to the target devices.

Who Should Use Echo Mode and When Should It Be Used?

In a production environment, echo mode can be used to perform service provisioning on devices that are either temporarily offline or not yet commissioned. The service provisioning only occurs within the ISC Repository. When these devices become active, you can force the deployment of the previously provisioned services and ISC downloads the configurations to the devices.

Echo mode is a global configuration setting that affects the Service Provisioning for *all* users. Therefore, echo mode should be used with care. To enable echo mode, set the Dynamic Component Properties Library (DCPL) **GTL/echo-mode** to **true** (**Administration > Control Center > Hosts**, as explained in Appendix C, Property Settings of the *Cisco IP Solution Center Infrastructure Reference, 5.1*). When echo mode is enabled, no attempt is made to contact any devices and no attempt is made to audit the Service Request. This affects all Service Requests during the time period when echo mode is enabled.

How Should You Use Echo Mode?

Because echo mode affects all of ISC's provisioning, be sure that all provisioning requests that require device access are complete before turning on echo mode.

Turn on echo mode, as explained in the "Who Should Use Echo Mode and When Should It Be Used?" section on page E-10.

Configure your Service Request as normal for the device that is not commissioned or is offline. Save and deploy the Service Request. No attempt is made to contact the device or audit the Service Request. The Service Request transitions into the Deployed state.

Now, you can disable echo mode, by changing the **GTL/echo-mode** property to **false** (see the "Who Should Use Echo Mode and When Should It Be Used?" section on page E-10). From this point forward, all provisioning requests contact the devices and all provisioning requests are audited. You can now safely resume provisioning for all users.

After the device has been commissioned or brought back online, Force deploy the provisioning request for this device (see Chapter 3 in the *Cisco IP Solution Center Infrastructure Reference, 5.1*). This forces the provisioning request to go through the provisioning cycle and deploy the configlet onto the device.