Cisco IP Solution Center Installation Guide, 3.2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5524-02

Cisco IP Solution Center Installation Guide, 3.2

About This Guide

This preface defines the following:

Objective

This guide lists the hardware and software recommendations for running this product, and describes how to install, manage, and log into the Cisco IP Solution Center (ISC).

Related Documentation

The entire documentation set for Cisco IP Solution Center, 3.2 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_2

The following documents comprise the ISC 3.2 documentation set.

General documentation:

- *Cisco IP Solution Center Documentation Guide, 3.2*
- *Cisco IP Solution Center Release Notes, 3.2*
- *Cisco IP Solution Center Installation Guide, 3.2*
- *Cisco IP Solution Center System Error Messages, 3.2*
- *Cisco IP Solution Center API Programmer Guide, 3.2*
- Index: *Cisco IP Solution Center API Programmer Reference, 3.2*

Integrated VPN Management Suite documentation:

- *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2*
- *Cisco IP Solution Center Integrated VPN Management Suite L2VPN User Guide, 3.2*
- *Cisco IP Solution Center Integrated VPN Management Suite MPLS VPN User Guide, 3.2*
- *Cisco IP Solution Center Integrated VPN Management Suite Network-Based IPsec VPN User Guide, 3.2*
- *Cisco IP Solution Center Integrated VPN Management Suite Quality of Service User Guide, 3.2*
- *Cisco IP Solution Center Integrated VPN Management Suite Security User Guide, 3.2*

Security Management Suite documentation:

- *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*
- *Cisco IP Solution Center Security Management Suite Quality of Service User Guide, 3.2*
- *Cisco IP Solution Center Security Management Suite Security User Guide, 3.2*

Note All documentation *might* be upgraded.

Audience

This guide is intended primarily for the following audiences:

- System administrators who are familiar with Sun Solaris and are responsible for installing software on Solaris servers.
- System administrators who are familiar with Cisco devices and their company's network topography.

How This Book is Organized

This guide contains the following chapters:

- Chapter 1, "System Recommendations," describes the hardware and software recommendations and requirements to run ISC.
- Chapter 2, "Installing and Logging Into ISC," explains what is packaged with ISC, prerequisites for installing ISC, Cisco High Availability support, how to install ISC, how to install the data service for High Availability, logging in for the first time, remote installation and uninstallation of Processing Server, Collection Server, or Interface Server, how to install license keys, repository migration and upgrading, launching Inventory Manager and Topology Tool, and uninstalling ISC.
- Appendix A, "Setting Up Oracle for ISC," describes how to set up an Oracle 9.2.0.1 server that works with ISC.
- Appendix B, "Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3.x and 1.4 Software with ISC," describes how to set up a Cisco CNS IE2100 appliance, configure a TIBCO Rendezvous Routing Daemon (rvrd), and check router configurations for Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3.x or 1.4 software with ISC.

- Appendix C, "Back Up and Restore of ISC Repository and Standby System," describes the objectives of backup and restore and a standby system and how to set them up for Oracle and for Sybase.
- Index

Document Conventions

This section discusses conventions and terminology used throughout this manual.

- *pointer*—indicates where the mouse action is to occur
- *select*—to push and hold down the left mouse button
- *release*—to let up on a mouse button to initiate an action
- *click*—to select and release a mouse button without moving the pointer
- *double-click*—to click a mouse button twice quickly without moving the pointer
- *drag*—to move the pointer by sliding the mouse with one or more buttons selected

This manual uses this terminology throughout (even though it is possible for individual users to customize their devices to use the buttons in an alternative manner).

In situations that allow more than one item to be selected from a list simultaneously, the following actions are supported:

- To select a single item in a list, click the entry. Clicking a second time on a previously selected entry deselects it.
- To select a contiguous block of items, click the first entry; then, without releasing the mouse button, drag to the last desired entry and release. (A subsequent click anywhere on the window deselects all previous selections.)
- To extend a currently selected block, hold the **Shift** key down and click the entry at the end of the group to be added.
- To add a noncontiguous entry to the selection group, press the **Ctrl** (Control) key and click the entry to be added.

Names of on-window elements that you click or select (menu names, commands, and controls such as buttons, drop-down lists, and so on) are printed in **bold** font.

Bold font is also used for keywords, names of commands, and names of keys on the keyboard.

Text displayed as on-window examples is printed in `courier` font.

When set off from the main text, words and characters you should enter by the keyboard are printed in **`bold`** font. When the word or character string is enclosed in angle brackets (< and >), you should substitute your own character string for the example presented in the text.

For example, when you see:

login: **root**

you should specify the string **root** at the **login** prompt. However, when you see:

password: <*rootpassword*>

you should specify your own password in place of the character string <*rootpassword*>.

The *italic style* is used to emphasize words, to introduce new terms, and for titles of printed publications (however, not titles of CD-ROMs or floppy disks).

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

System Recommendations

This chapter describes the system recommendations and requirements for Cisco IP Solution Center (ISC). ISC is a web-based application you install on a Sun Solaris server, along with a web server and other supporting packages. You access ISC using a web browser.

The recommendation is to thoroughly review this list before even planning your installation, to be sure you have all the hardware and software you need to successfully install.

For the workstation, the minimal recommendations are as shown in Table 1.

Table 1 Workstation Recommendations for ISC

Number of Edge Devices	Workstation (or equivalent)	RAM	Swap Space	Disk Space
Up to 1500	Sun Fire™ V120 or equivalent (1 CPU)	1 GB	2 GB	36 GB
1500 - 3000	Sun Fire™ 280R (1 CPU)	2 GB	4 GB	36+ GB
More than 3000	Sun Fire™ 280R (2 CPUs) or V480 (2 CPUs expandable to 4 CPUs)	4 GB	8 GB	Two 36+ GB
Note: When ordering the Sun Fire™ V120, be sure to order a video card.				

Note To help you find the correct Sun hardware to run ISC, see the following URL for the most up-to-date recommended part numbers:

http://www.sun.com/oem/cisco/isc.html

This location gives recommended order numbers for Sun workstations and a description of the required and optional components.

- Solaris 8 with recommended patches of at least 108528-23 for the kernel level of the patch cluster and JDK 1.4.1 patches found at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE (where the last character in **show.pl** is the lower-case letter "l"). Table 2, "Solaris Software Requirements," explains the Solaris requirements.

Table 2 Solaris Software Requirements

Requirements	Description
Solaris 8	Install Solaris 8 on the Sun server following these guidelines: Full Distribution—Install the full distribution, which includes the following required packages. If you did not install the full distribution, you can install these packages at any time. —**SUNWlldap**—LDAP libraries —**SUNWfnsx5**—FNS support for x.500 Directory Context —**SUNWbzip**—The **bzip** compression utility To check if your installation includes these packages, enter: **pkginfo** *package* where: *package* is one of the three packages listed above.

Note When you install Solaris 8, be sure to choose either the Developer System Support or the Entire Distribution software groups. Do *not* choose the End User System software group. The Developer System Support and Entire Distribution software groups contain the software required for a correct operating system installation (such as the **SUNWbtool** and **SUNWsprot** packages).

- CD-ROM drive.
- ISC 3.2 testing on an Oracle database has been on Oracle 9.2.0.1 with US7ASCII. If you would like to use another version of Oracle, see Oracle's compatibility information.
- A web browser is needed. Internet Explorer 6.0 or later or Netscape 7.0 or later can be used.

Note When using more than one login, open a new browser instead of logging in from the same browser.

- Java Web Start applications, including Inventory Manager and Topology Tool are supported on Windows 2000 only.
- AToM PE-POP: Recommended Cisco IOS releases are 12.0(22)S or later.
- Cisco CNS IE2100 Plug-and-Play and Upload and Download: If using Cisco CNS Configuration Engine Release 1.3, the recommended Cisco IOS release is 12.2(8)T or later; if using Cisco CNS Configuration Engine Release 1.3.1, 1.3.2, or 1.4, the recommended Cisco IOS release is 12.2(11)T or later. Cisco IOS releases 12.3(1)T or later are supported only by Cisco CNS Configuration Engine Releases 1.3.2 and 1.4.
- Cisco VPN Client: Recommended releases are 3.0 or later.
- DMVPN: Recommended Cisco IOS releases are 12.2(15)T or later.
- Easy VPN Hardware Client: Recommended PIX release is 6.3 or Cisco IOS 12.3(2)T or later.
- Easy VPN Server: Recommended PIX release is 6.2 or later or Cisco IOS 12.3(4)T.

- Firewall: Recommended PIX release is 6.2 or later or Cisco IOS 12.2(13)T or later.
- IP DSL switches: Recommended Cisco IOS releases are 12.2(1)DA or later.
- IPsec Failover Cisco 7200: Recommended Cisco IOS releases are 12.2(11)YX1 or later.
- IPsec Remote Access: Recommended PIX release is 6.2 or later, Cisco IOS release 12.2(11)T or later, k8 or k9 images, or VPN 3000 releases 3.6.5, 3.6.7A, or 4.0.1E.
- IPsec Site-to-Site: Recommended PIX releases are 5.3 or later, Cisco IOS releases 12.2(11)T or later, k8 or k9 images, or VPN 3000 releases 3.6.5, 3.6.7A, or 4.0.1E.
- Metro Ethernet PE-POP (Catalyst 6500 or Cisco 7600): Recommended Cisco IOS releases are 12.1(11b)EX1 or later.
- MPLS CEs: Recommended Cisco IOS releases are 12.1 or later.
- MPLS PEs: Recommended Cisco IOS releases are 12.1(5a)T or later (except 12.2(8)T).
- MPLS PEs using Carrier Supporting Carriers (CsC) (1200): Recommended Cisco IOS releases are 12.0(14)T or later.
- MPLS PEs using EIGRP: Recommended Cisco IOS releases are 12.0(22)S or later or 12.2(15)T or later.
- Multi-VRF CE Catalyst 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- Multi-VRF CE 7400: Recommended Cisco IOS releases are 12.2(4)B3 or later.
- NAT: Recommended PIX releases are 5.3 or later or Cisco IOS 12.2(11)T or later.
- Network-based IPsec: Recommended Cisco IOS releases are 12.2(11)T or later.
- PE-CLE Catalyst 2950 and Catalyst 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- PE-CLE Catalyst 4000: Recommended CAT OS releases are 7.5 or later or Cisco IOS 12.1(12c)EW1 or later.
- PE-CLE Catalyst 6500: Recommended CAT OS releases are 7.3 or later or Cisco IOS 12.1(11)EW1 or later.
- QoS (Ethernet QoS) Cisco 3550: Recommended Cisco IOS release is 12.1(19)EA1a.
- QoS (Ethernet QoS) Cisco 4000: Recommended Cisco IOS release is 12.1(12c)EW
- QoS (IP QoS) Cisco 8xx, 17xx, 26xx, 36xx, 3745, and 72xx: Recommended Cisco IOS release is 12.3(5)
- QoS (IP QoS) Cisco 75xx: Recommended Cisco IOS release is 12.0(26)S.
- QoS (IP QoS) Cisco 10xxx (ESR): Recommended Cisco IOS release is 12.0(23)SX.
- QoS (IP QoS) Cisco 12xxx (GSR): Recommended Cisco IOS release is 12.0(26)S.
- QoS (IP QoS) Cisco RPM-PR: Recommended Cisco IOS release is 12.3(3)
- VPLS: Recommended Cisco IOS releases are 12.2S or later.
- VPN Service Module (VPNSM) (WS-SVC-IPsec-1) (Catalyst 6500 or Cisco 7600): Recommended CAT OS release is 7.6(1) or Cisco IOS 12.2(14) SY.

Caution Make sure that the file descriptor limit is *not* set in the ISC workstation login shell file (which can be the **.login** file, the **.cshrc** file, or the **.kshrc** file). If the login shell file contains a line with the **ulimit -n** command (for example, "`ulimit -n <number>`"), comment out this command line in the file.

ISC cannot override the file descriptor limitation setting in the login shell file. If the value is set incorrectly, ISC might experience operational problems.

Installing and Logging Into ISC

Use the information described in this chapter in the following order:

Note See Chapter 1, "System Recommendations," before installing ISC.

Packages Included with ISC

The ISC installer includes the following third party software:

- TIBCO Version 7.1.15
- Sun™ Java JRE Version 1.4.1
- Sybase Adaptive Server Anywhere (ASA) Version 8.0.1
- Tomcat Version 4.1.27

Initial Configuration - Creating the ISC Owner

Note If you are planning to use an Oracle database, understand that ISC 3.2 has been tested with Oracle 9.2.0.1. If you would like to use another version of Oracle, see Oracle's compatibility information. Proceed to Appendix A, "Setting Up Oracle for ISC" before continuing with the ISC installation. After you complete the Oracle set up, return here.

The first time you install ISC, create a UNIX user to own the software. This user is the default username when you log into ISC. Create the user and group using Solaris commands or the Solaris Admintool. This user must have a valid group ID and read and write permissions to the install directory.

To add a user to your server using the standard Solaris commands, follow these steps:

Step 1 At the Solaris prompt, log in as **root**.

Step 2 To create the user, enter:

```
useradd -d /users/<username> -m -s /bin/<shell_type> <username>
passwd <username>
```

where:

-m creates the directory specified in **-d**

<shell_type> is **sh** for the Bourne Shell, **ksh** for the Korn Shell, or **csh** for the C Shell

iscadm is recommended as the *<username>*.

Step 3 At the prompt, enter a password.

Cisco High Availability Support

This Cisco High Availability support is explained in the following sections (use these sections sequentially):

- Cisco High Availability Scope and Implementation, page 2-2
- Installing ISC for High Availability, page 2-3
- Installing ISC High Availability in a Distributed Setup, page 2-4

Cisco High Availability Scope and Implementation

Sun™ Cluster offers mainframe-class reliability and availability. It is designed to deliver high availability through automatic fault detection recovery, ensuring that your mission-critical applications and services are available when you need them.

ISC supports Sun™ Cluster Release 3.0 with Update 3 in Failover mode. ISC supports two nodes in this High Availability (HA) cluster. This support is only for the control tier, known as the Master server and to get this support, you must choose **HA Master** as your first server when installing ISC, as shown in Figure 2-3 on page 2-7.

In an ISC single-tier architecture (nondistributed setup), all ISC components will fail over with the control tier. In an ISC distributed environment, all ISC components installed on the distributed servers will continue to work with the new control tier on the second node. The two nodes in the HA cluster to support failover service for the control tier share the same logical host name. All external applications and servers need to use this logical host name to connect to the control tier.

When the control tier switches from one node to the other, the same ISC repository is used. Two copies of the ISC repository should *not* be on the two nodes. The ISC repository *must* be on a disk shared by the two nodes of the High Availability cluster (that is, on a Network File System (NFS) mounted disk partition accessible by both the nodes). Be sure to include the logical host name, not the Sun™ Cluster node names when installing the **HA Master**, as shown in Figure 2-4 on page 2-8.

Note High Availability requires Solaris 8.

Installing ISC for High Availability

Prior to installing ISC, be sure the two Sun™ Cluster nodes and the logical host are running.

Install and configure Sun™ Cluster and Data Service, as explained for Sun™ Cluster 3.0 with Update 3. See the Sun™ Web site or documentation:

http://wwws.sun.com/software/cluster/index.html

Note You must be trained to run Sun™ Cluster before using this ISC High Availability feature.

To install ISC, you must implement the following steps, which includes an installation on each of the two nodes:

Step 1 Create the Resource Group (for example, **isc-rg**) in Sun™ Cluster for ISC, as explained in the Sun™ Cluster documentation.

Step 2 Create a logical hostname resource (for example, **dukat.cisco.com**) under the created Resource Group, as explained in the Sun™ Cluster documentation.

Step 3 On one of the two nodes, now to be known as the first node, use the following command to enable the logical hostname.

scswitch -e -j <*logical_hostname*>

where: <*logical hostname*> is used in Figure 2-4 on page 2-8.

Step 4 Install ISC on the first node. Use the **custom** installation, as explained in the "Installing ISC" section on page 2-4.

Step 5 When ISC is installed successfully on the first node, use the following command to source the ISC environment file located in the $ISC_HOME directory:

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: **source $ISC_HOME/bin/vpnenv.csh**

Step 6 Use the following command to stop the ISC servers.

stopall

Step 7 Use the following command to switch the logical hostname resource to the second node (failover node).

scswitch -z -g <*resource-group*> **-h** <*second_node*>

where: <*resource-group*> is the resource group, for example: **isc-rg**, as created in Step 1.

<*second_node*> is the name of the second node, which will become the failover node.

Step 8 Use the following command to verify that the logical hostname on the second node is online.

scstat

Step 9 Install ISC on the second node, as explained in the "Installing ISC" section on page 2-4.

Step 10 When ISC is installed successfully on the second node, use the following command to stop the ISC servers.

stopall

Installing ISC High Availability in a Distributed Setup

When using a distributed setup, after you follow the steps in the previous sections that explain Installing ISC for High Availability and Installing ISC High Availability in a Distributed Setup, install the distributed servers, the Collection Server, the Processing Server, or the Interface Server, as explained starting with Step 10 in the section, Installing ISC.

Note When installing each distributed server, you must provide the same logical hostname that you gave for the **HA Master** in Figure 2-4 on page 2-8. And you must specify a local directory on the distributed server itself, when prompted to provide the path to the temporary files and repository, as shown in Figure 2-9 on page 2-10 and Figure 2-10 on page 2-11.

Installing ISC

To add ISC to your system, follow these steps. The ISC GUI installer checks that the required Solaris packages and patches are installed. The installer has you acknowledge the missing patches and you can then continue the installation. You can install the specified missing packages or patches later.

The installer also checks for two kinds of disk space:

- In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x or 1.4 software.
- In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

See Chapter 1, "System Recommendations" for more information about disk space and planning.

The complete installation for the ISC software requires 1.2 GB of free disk.

To install the ISC software, follow these steps.

Note If a previous installation is running, enter the **stopall** command. See *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2* for information about all WatchDog commands.

Step 1 Insert the ISC installation CD-ROM.

Caution When you insert the CD-ROM, the File Manager is invoked automatically. Do *not* use the File Manager to install the ISC product. Run the installation script from a terminal window.

Note If you choose to remotely install over a wide area network, you must add two spaces at the end of each field for which you modify the entry. This is to work around a potential problem that occurs when you you have two or more SSH tunnels between your location and your installation machine's location.

Step 2 Open a terminal window and log in as **root**.

Step 3 Change to the CD ROM directory:

```
$ cd /cdrom/cdrom0
```

Step 4 Execute the ISC product installation script:

```
cdrom> ./install.sh
```

The installation script **install.sh** is located in the **root** directory. The ISC software is installed by default in the **/opt/isc-3.2** directory.

Step 5 On your terminal window, you will see a list of the required patches. A Warning message appears for each missing patch.

After the list, you receive a message indicating either that all patches are up-to-date, **All necessary patches are installed**, or a Warning message indicating the number of missing patches. If missing patches are detected, you are asked whether you want to continue or abort.

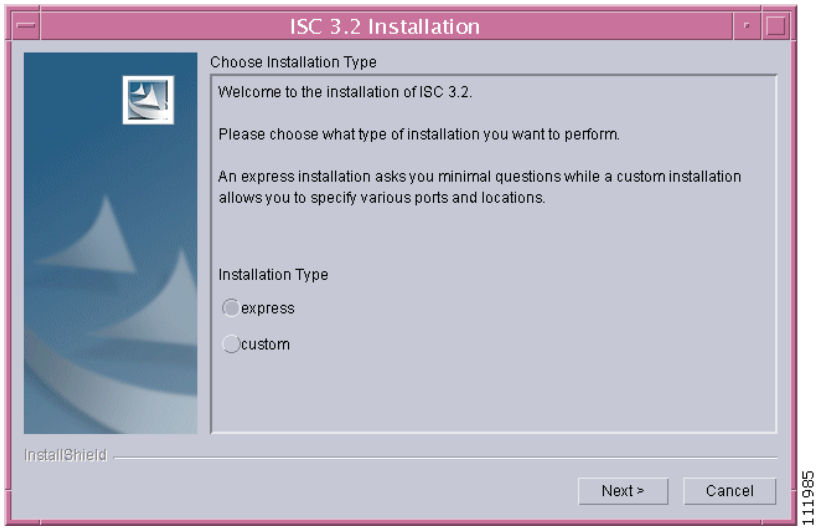
Tip If you begin the ISC installation and are informed that required patches are missing on your Sun workstation, follow the instructions in Chapter 1, "System Recommendations." You can safely exit this install script and run it again after you have installed the required patches. If required patches are missing, the ISC software lists the missing patches in the **/tmp/PatchReport.dat** file.

After you install the latest patch cluster, the ISC installation script might still report that there are missing patches. The number of missing patches should be small, in the range of 1-3. You can search the Sun™ website to verify that the missing patches are indeed included in the latest patch upgrade, but with different numbers. If a patch is missing and not included in another patch, the missing patch was probably deemed not needed. In these cases, you can safely ignore the warning message about missing patches. It is recommended you only install patch clusters and not individual patches.

Step 6 In the next window, as shown in Figure 2-1, "Choose Installation Type," choose either the default **express** option or the **custom** option, then click **Next**.

When you click **express**, you have a minimal number of choices to make. When you click **custom**, you can specify various ports and locations and you can change the watermark level for available disk space.

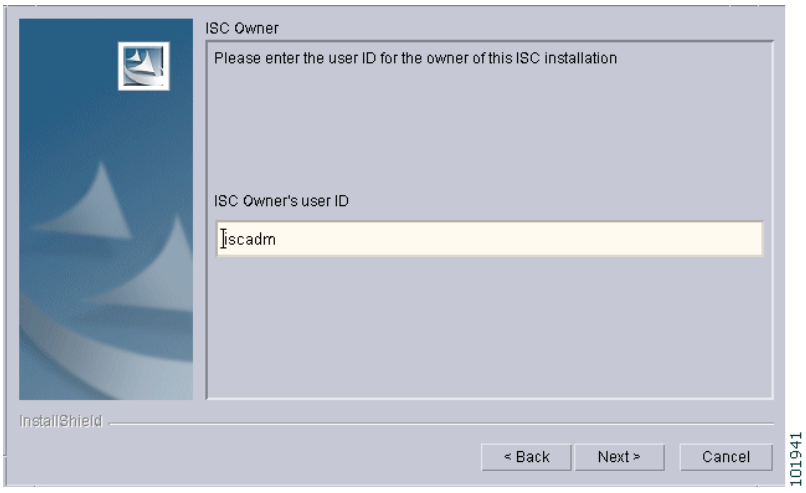
Figure 2-1 Choose Installation Type



Step 7 In the next window, shown in Figure 2-2, "Choose ISC Owner," enter the user name you created in Step 2 of the "Initial Configuration - Creating the ISC Owner" section on page 2-2.

Note This field is only used when you are installing as **root**.

Figure 2-2 Choose ISC Owner



Step 8 Independent of whether you chose **express** or **custom** in Step 6, next you must choose the Server Role, either **Master**, **HA Master**, **Processing Server**, **Collection Server**, or **Interface Server**, as shown in Figure 2-3, "Choose Server Role," then click **Next**. The servers are as follows:

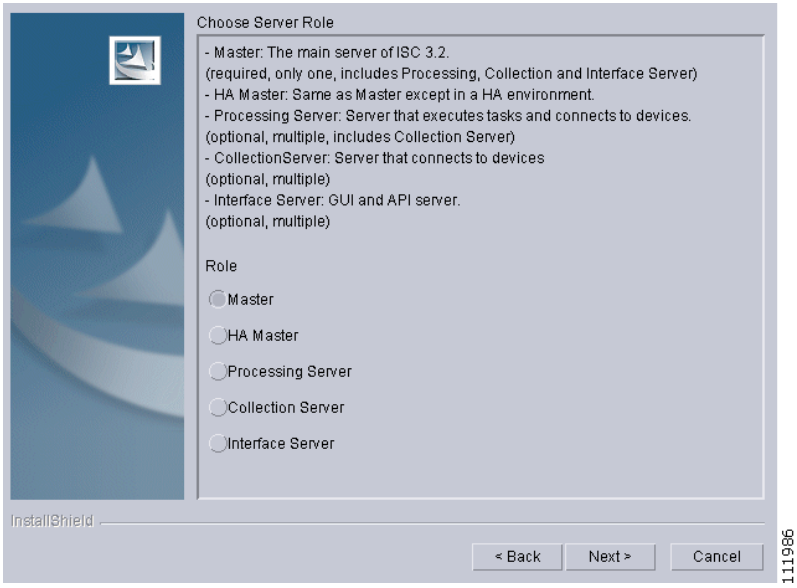
- **Master** is the main server of ISC. Only one **Master** or **HA Master** is possible and it is required. It includes all the other servers: the **Processing Server**, **Collection Server**, and **Interface Server**.
- **HA Master** is the same as a **Master** server but is configured to run in the Sun™ high availability (HA) environment.

Note Before choosing **HA Master**, you must have set up your Sun™ Cluster hardware and after ISC installation is completed, you must install the High Availability Package. See the "Cisco High Availability Support" section on page 2-2 and the "Installing the Data Service for High Availability" section on page 2-20, respectively.

- **Processing Server** is the server that executes tasks and connects to devices. This sever is optional and *can* be installed on a host separate from any of the other servers. Multiple **Processing Server**s can be installed. The **Processing Server** includes the **Collection Server**.
- **Collection Server** is the server that connects to devices. This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Collection Server**s can be installed.
- **Interface Server** is the web server for the Graphical User Interface (GUI) and the Application Program Interface (API). This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Interface Server**s can be installed.

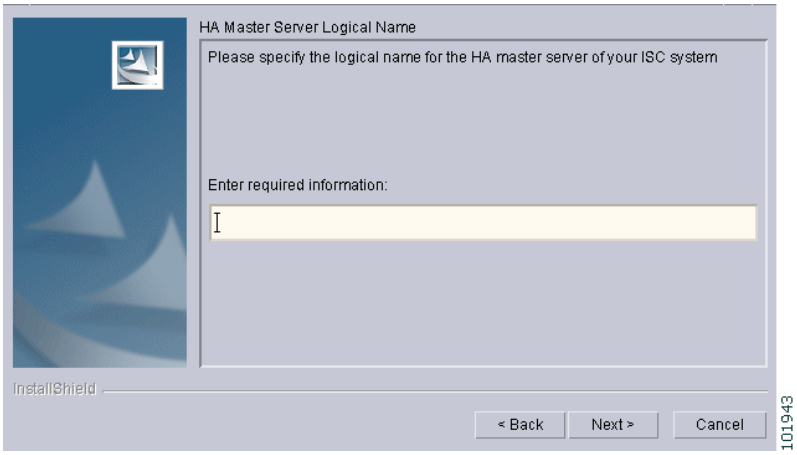
Note For the first installation, you *must* click the **Master** or **HA Master** Role.

Figure 2-3 Choose Server Role



Step 9 If you chose **HA Master** in Step 8, you receive a window, as shown in Figure 2-4, "HA Master Server Logical Name."

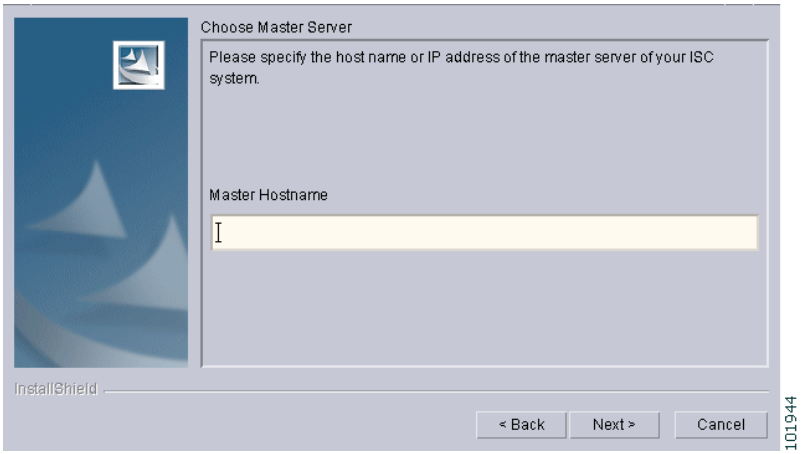
Figure 2-4 HA Master Server Logical Name



Step 10 Because you *must* click the **Master** or **HA Master** Role for the first installation, this step is only required when you click **Processing Server**, **Collection Server**, or **Interface Server**. If you are installing a **Master** or **HA Master** Role, proceed to Step 12.

Enter the hostname or IP address of the Master server, in the field shown in Figure 2-5, "Master Hostname."

Figure 2-5 Master Hostname



Step 11 If the host name entered in Step 10 is not valid, you receive a message as shown in Figure 2-6, "Invalid Host." Click **Ok** and return to Step 10. Otherwise, continue to Step 12.

Figure 2-6 Invalid Host

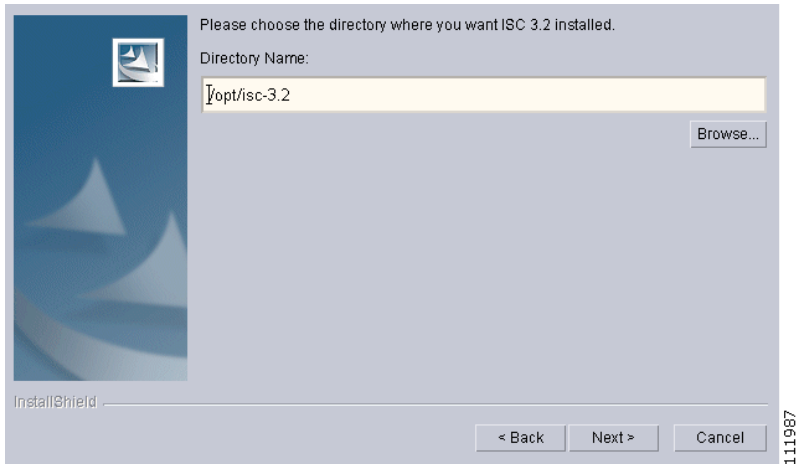
Step 12 Independent of the Server Role you chose in Step 8, next you must specify the location of the directory where you want to install, as shown in Figure 2-7, "Specify Directory Location," and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

Note If you are not installing as **root**, you must have write permission for this directory.

Note In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x or 1.4 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

Figure 2-7 Specify Directory Location

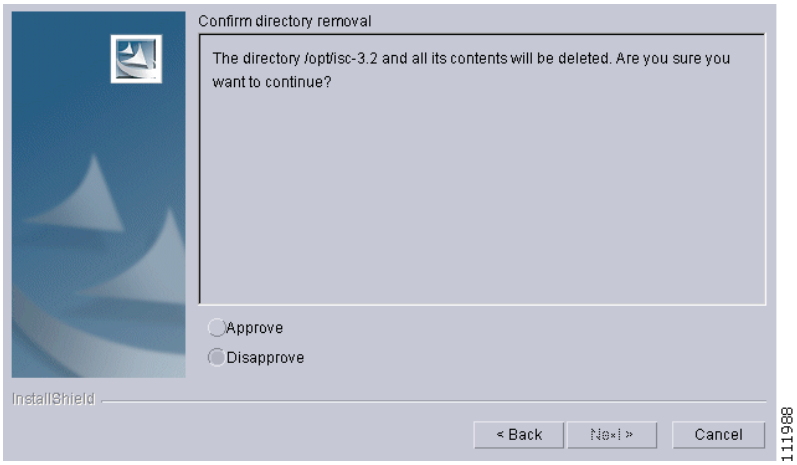


Step 13 If the directory you chose does not exist, proceed to Step 14.

In Figure 2-8, "Confirm Directory Removal," if the directory you chose already exists and you need to click the default radio button **Disapprove**, you cannot proceed. You must click **Back** and return to Step 12.

Be *very* careful. If you click the radio button **Approve**, you will overwrite the contents in the existing directory. Click **Next**.

Figure 2-8 Confirm Directory Removal



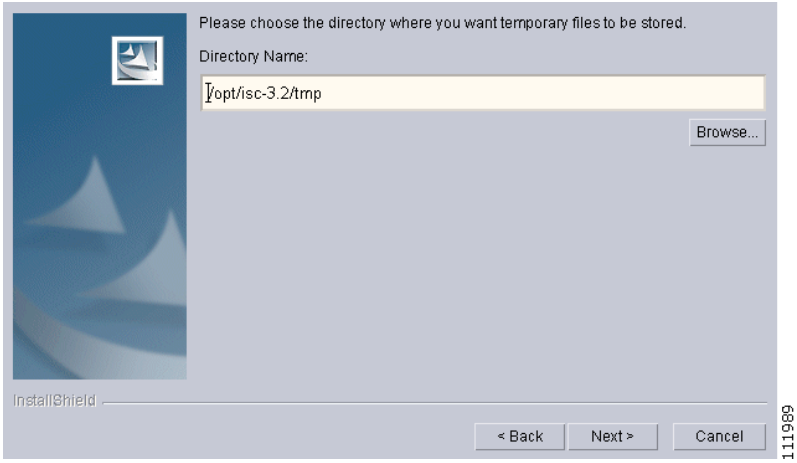
Step 14 If in Step 6 you chose **express**, proceed to Step 27. If you chose **custom**, then for any Role specified, you must enter the location where you want temporary files stored, as shown in Figure 2-9, "Choosing the Directory for Temporary Files."

Note If you are installing High Availability, specify the path of the temporary directory different from the default. This path needs to fall in the common disk area (that is, the NFS mounted disk partition) shared by the two nodes of the Sun™ Cluster.

Note In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x or 1.4 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

Figure 2-9 Choosing the Directory for Temporary Files



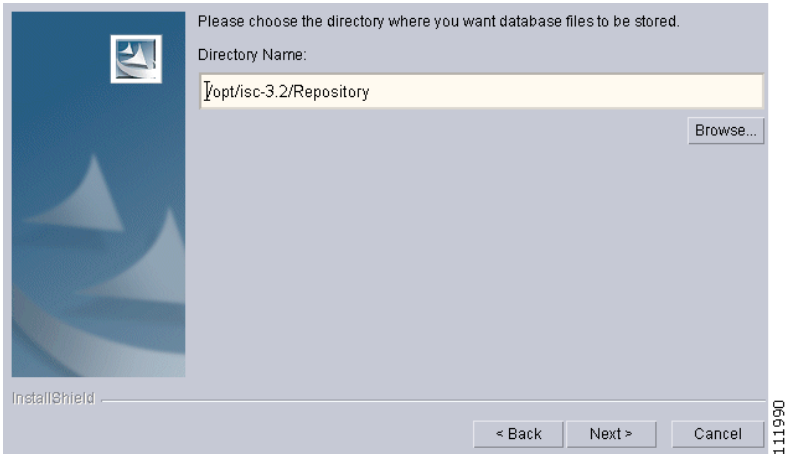
Step 15 If you chose any Role, except the Interface Server Role, in Step 8, you must specify the Directory Name where you want database files to be stored, as shown in Figure 2-10, "Where to Restore Database Files," and then click **Next**. If you chose **Interface Server** Role, you automatically proceed to Step 16.

Note If you are installing High Availability, specify the path of the repository different from the default. This path needs to fall in the common disk area (that is, the NFS mounted disk partition) shared by the two nodes of the Sun™ Cluster.

Note In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x or 1.4 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

Figure 2-10 Where to Restore Database Files



Step 16 If in Step 15 you chose a directory that already contains a repository, you have three options, as shown in Figure 2-11, "Repository Choices,": **Keep existing 3.x repository**, **Overwrite existing repository**, or **Migrate (2.x, 1.x) repository after installation**.

When you click **Keep existing 3.x repository**, after you complete your installation and before you use ISC, to upgrade your down-level ISC 3.1 or 3.1 plus patches repository, you *must* follow the steps in the "Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2" section on page 2-28.

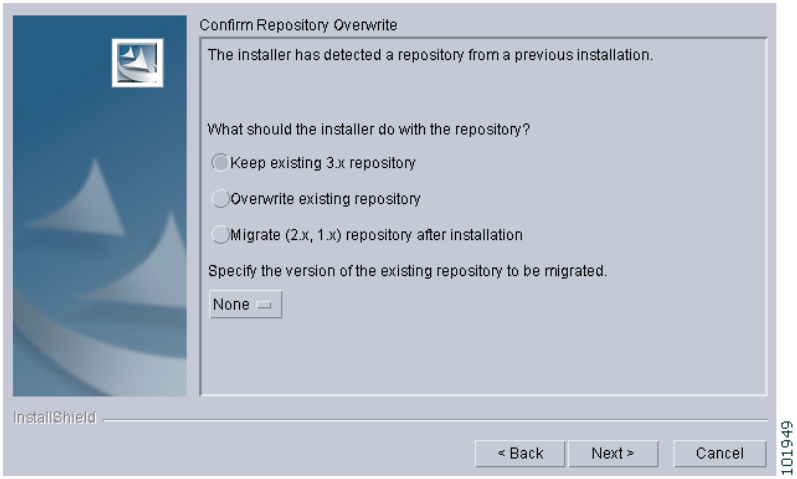
Caution There is no identified and supported way to upgrade from ISC 3.0 to ISC 3.2. To upgrade from ISC 3.0 to ISC 3.2, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

When you click **Migrate (2.x, 1.x) repository after installation**, after you complete your installation and before you use ISC, you *must* follow the steps in the "Migrating VPNSC 1.x or 2.x Repository to ISC 3.2" section on page 2-25, to upgrade your down-level VPNSC 1.x or 2.x repository.

Note If you click **Overwrite existing repository** or **Migrate (2.x, 1.x) repository after installation**, your existing repository is saved as **Repository.save**.

Click **Next** to proceed.

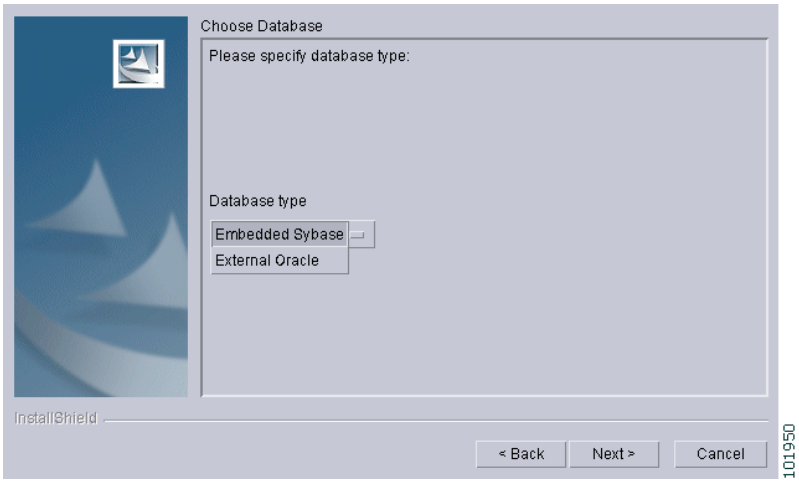
Figure 2-11 Repository Choices



Step 17 Independent of the Server Role you chose in Step 8, you must choose the database you will use, as shown in Figure 2-12, "Choosing a Database". From the drop-down menu, choose either **Embedded Sybase** (Sybase ASA, 8.0.1 is embedded) or **External Oracle** (Testing of ISC 3.2 has been done with Oracle 9.2.0.1. If you would like to use another version of Oracle, see Oracle's compatibility information.). Then click **Next**.

Note The embedded Sybase database is used for service-level agreement (SLA), independent of whether you are using Oracle as your database.

Figure 2-12 Choosing a Database

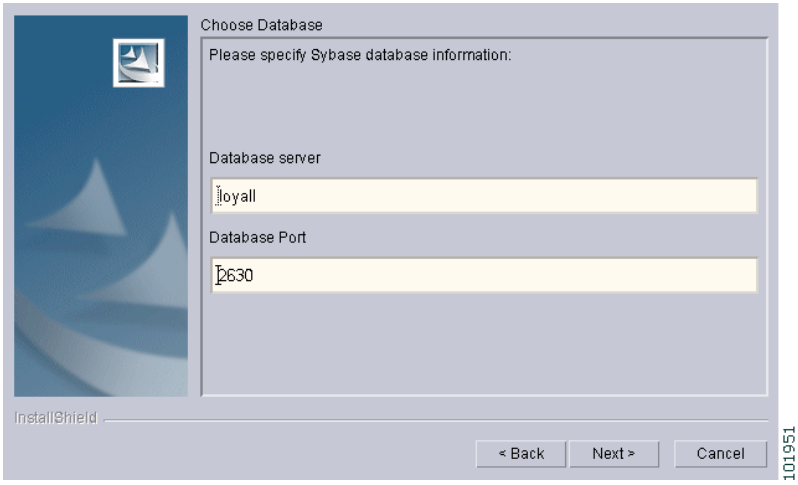


Step 18 If you chose **Embedded Sybase** in Step 17, enter the **Database server** name, as shown in Figure 2-13, "Choosing a Database—Sybase." The **Database Port** number is automatically updated. If you choose to change the database port number, enter your choice in the **Database Port** field. Click **Next,** and then proceed directly to Step 21.

If you chose **External Oracle** in Step 17, proceed to Step 19.

Note If you enter a Database Port value other than the default, be sure you specify the same port for all Server Roles you install.

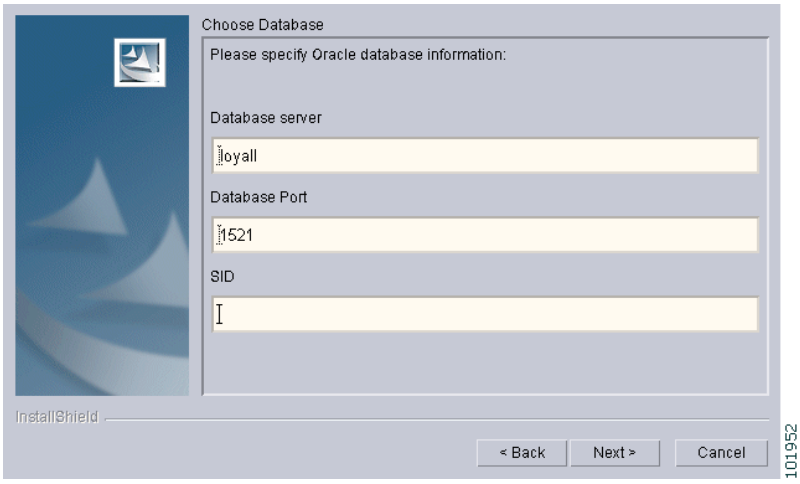
Figure 2-13 Choosing a Database—Sybase



Step 19 If you chose **External Oracle** in Step 17, you must enter the **Database server** name, the **Database Port** number, and the Oracle server instance identifier (**SID**), as shown in Figure 2-14, "Choosing a Database—Oracle." Otherwise, proceed directly to Step 21.

Note If you enter a Database Port value other than the default, be sure you specify the same port for all Server Roles you install.

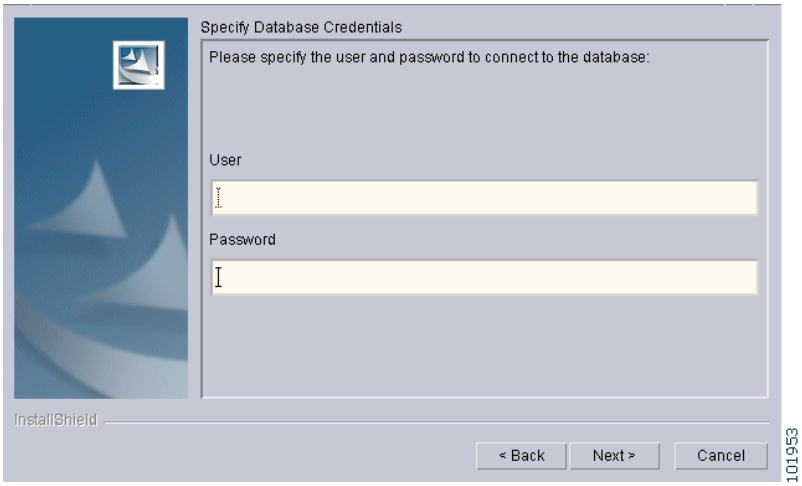
Figure 2-14 Choosing a Database—Oracle



Step 20 Because you chose **External Oracle** in Step 17, you must set the Oracle database **User** and **Password** values, as shown in Figure 2-15, "Specifying Database Credentials."

Note If you are setting up a distributed architecture environment, the Oracle **User** and **Password** *must* be the same for all servers.

Figure 2-15 Specifying Database Credentials

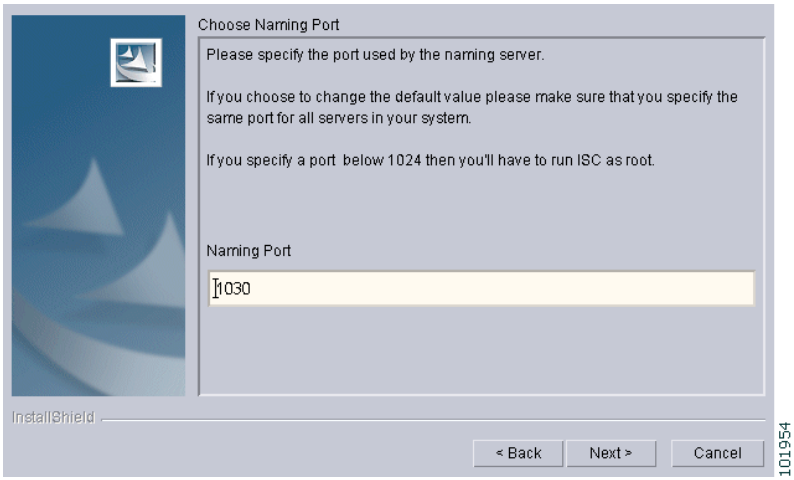


Step 21 Independent of the Server Role you chose in Step 8, you must specify the port used by the Naming Server, as shown in Figure 2-16, "Specify the Port Used by the Naming Server," then click **Next**.

Note If you choose a Naming Port other than the default, be sure you specify the same port for all the Server Roles you install.

Note If you enter a Naming Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

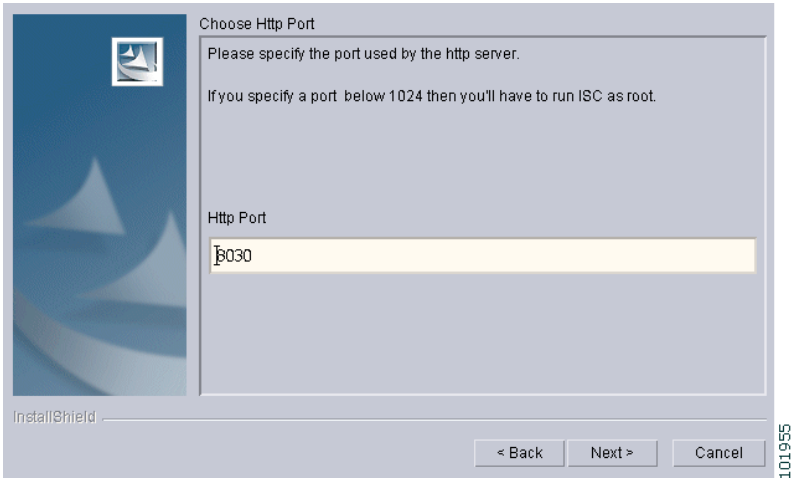
Figure 2-16 Specify the Port Used by the Naming Server



Step 22 Independent of the Server Role you chose in Step 8, you must specify the port used by the HTTP server, as shown in Figure 2-17, "Choose HTTP Port," then click **Next**.

Note If you enter an HTTP Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

Figure 2-17 Choose HTTP Port

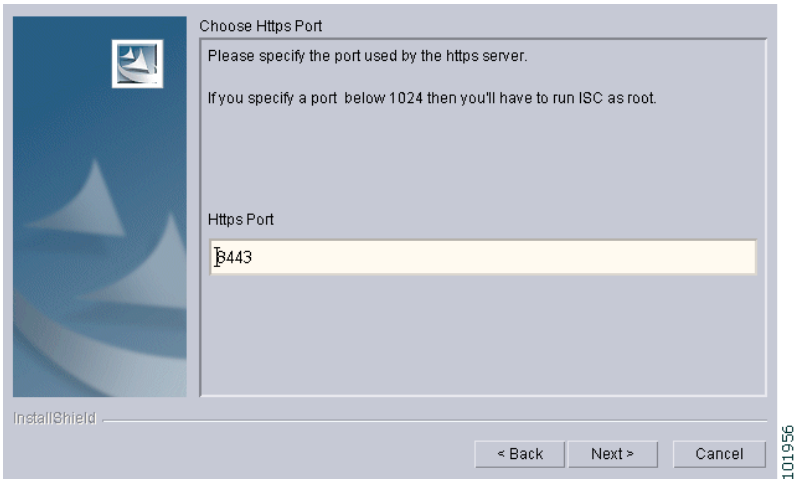


Step 23 Independent of the Server Role you chose in Step 8, you must specify the port used by the HTTPS server, as shown in Figure 2-18, "Choose HTTPS Port," then click **Next**.

Note If you enter an HTTPS Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

Note To configure the web access to ISC, you must set up the HTTPS port as explained in Step 35 and the "Configuring HTTPS" section on page 2-21.

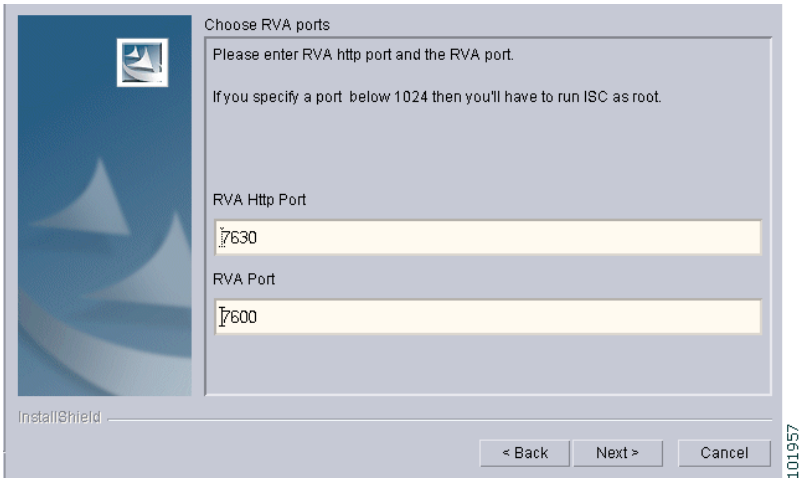
Figure 2-18 Choose HTTPS Port



Step 24 Independent of the Server Role you chose in Step 8, you must specify the port used by the Rendezvous™ Agent (RVA). You must specify the RVA HTTP Port server, a TIBCO™ bus port used by ISC processes to communicate with each other. You must also specify the RVA Client Port, as shown in Figure 2-19, "Choose RVA Ports," then click **Next**.

Note If you enter an RVA HTTP Port or RVA Client Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

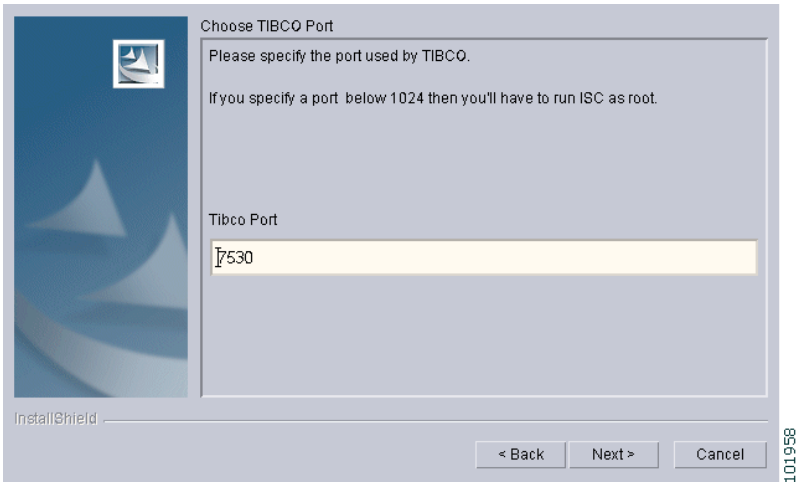
Figure 2-19 Choose RVA Ports



Step 25 Independent of the Server Role you chose in Step 8, you must specify the port used by TIBCO, as shown in Figure 2-20, "Choose TIBCO Port," then click **Next**.

Note If you enter a TIBCO Port value less than 1024, you *must* run ISC as **root**, the specification in Figure 2-2.

Figure 2-20 Choose TIBCO Port



Step 26 You can reset the High and Low watermarks for available disk space, as shown in Figure 2-21, "Setting Watermarks for Available Disk Space." The defaults are 20% and 10% for High and Low respectively. Be sure the High watermark is a larger percentage than the Low watermark. When the High and Low watermarks are reached, you receive an e-mail indicating this, based upon setting your e-mail address correctly in Step 27.

Figure 2-21 Setting Watermarks for Available Disk Space

Step 27 In Figure 2-22, "Setting e-mail Address for Receiving Watermark Information," to receive e-mail you must specify the following:

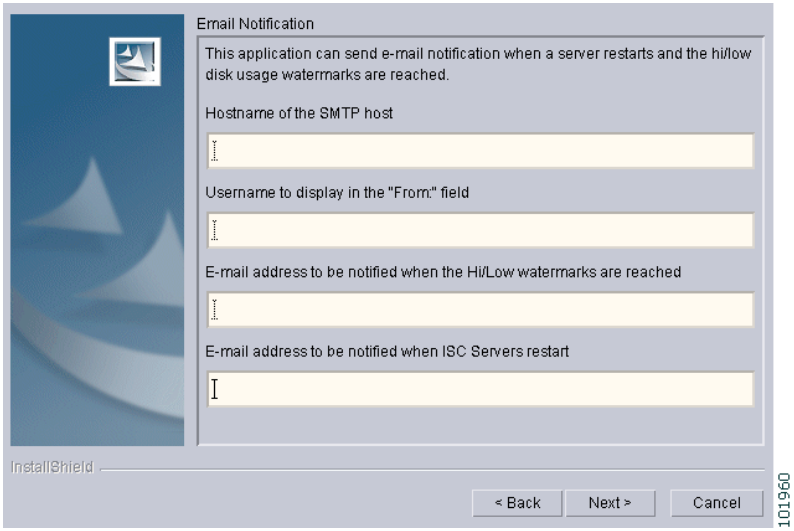
- In the first text field, specify the hostname of the Simple Mail Transfer Protocol (SMTP).
- In the second text field, specify the username to display in the "From" field.

- In the third text field, specify the e-mail address to be notified when High and Low watermarks are reached, which indicates the specified disk space availability has been reached.
- In the fourth text field, specify the e-mail address to be notified when ISC Servers restart.

Then click **Next**.

Note If incorrect information is provided, you receive an "Invalid Host" message, as shown in Figure 2-6.

Figure 2-22 Setting e-mail Address for Receiving Watermark Information



Step 28 In Figure 2-23, "Choose Menu Type," the default radio button is **Full Menus**. If you leave this selected, you receive the Graphical User Interface (GUI) that is the follow-on to what is provided in releases previous to Release 3.2. The manuals for this GUI are called the *Integrated VPN Management Suite*. If you click the radio button for **Security Management Menus**, you receive the new additional GUI introduced in Release 3.2. The manuals for this GUI are called the *Security Management Suite*. After you make your selection, click **Next**.

After you have completed your installation, you can change the GUI that you view, by running a script on the system on which you installed. To do this, go to $ISC_HOME (**cd $ISC_HOME/bin**) and run one of the following scripts:

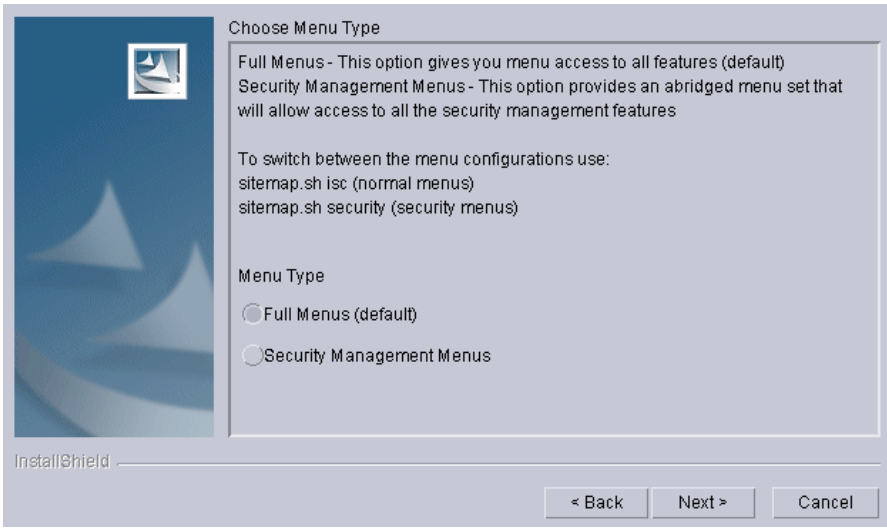
- To change from the Full Menus to the Security Management Menus, run:
  sitemap.sh security
- To change from the Security Management Menus to the Full Menus, run:
  sitemap.sh isc

In both cases, you are asked to then enter:

wdclient restart httpd

After you return to the product, anything you do makes you log back in. After you log back in (default: Login **admin**; Password: **cisco**), you will have the GUI you just chose.

Figure 2-23 Choose Menu Type



Step 29 The installation continues and the files are installed. The list of installation processes appears.

Step 30 If the installation failed, you receive a failed message.

To review the log message, click **Back**.

If there was truncation of data, reinstall and add two spaces at the end of each field for which you have modified the entry.

Step 31 If the installation was successful, you receive an Install Complete message. Even if you have a successful install, click **Back** to review the log to be sure there were no exceptions or failures. If data was truncated, reinstall and add two spaces at the end of each field for which you have modified the entry.

Step 32 The ISC product is launched automatically after the installation is successful.

Step 33 Verify that ISC is properly installed, as follows:

a. Source the ISC environment file in the $ISC_HOME directory:

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: **source $ISC_HOME/bin/vpnenv.csh**

b. Before logging in, repeat the following command until all servers are in the **started** mode. If any server is reported as **disabled**, ISC is not installed or configured correctly:

wdclient status

For more information about WatchDog commands, see *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2*.

Step 34 If you are installing ISC for High Availability, see the "Installing the Data Service for High Availability" section on page 2-20. Then, proceed to Step 36.

Step 35 If you want to set up secure web access by using HTTPS, see the "Configuring HTTPS" section on page 2-21. Then, proceed to Step 36.

Step 36 If you are logging in for the first time, proceed to the "Logging In for the First Time" section on page 2-21." Then proceed to Step 37.

Step 37 If you want to remotely install or uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, proceed to the "Remotely Installing" section on page 2-23. Then, proceed to Step 38.

Step 38 Before you can use any of the licensed services, proceed to the "Installing License Keys" section on page 2-24. Then, proceed to Step 39.

Step 39 If you have a VPNSC 1.x or 2.x repository, you *must* migrate your repository to have access to it, as explained in the "Migrating VPNSC 1.x or 2.x Repository to ISC 3.2" section on page 2-25."

If you have an ISC 3.1 or ISC 3.1 plus patches repository, you *must* upgrade your repository to have access to it, as explained in the "Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2" section on page 2-28.

Caution There is no identified and supported way to upgrade from ISC 3.0 to ISC 3.2. To upgrade from ISC 3.0 to ISC 3.2, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

Then, proceed to Step 40.

Step 40 For instructions to backup and restore an ISC repository or create a standby system, proceed to Appendix C, "Back Up and Restore of ISC Repository and Standby System." Then, proceed to Step 41.

Step 41 If you want to eventually use the Inventory Manager or the Topology Tool, your client machine *must* be set up properly. Proceed to the "Launching Inventory Manager and Topology Tool" section on page 2-30. This section explains what occurs and leads you to the launching explanations in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*. Then, proceed to Step 42.

Step 42 To uninstall ISC, proceed to the "Uninstalling ISC" section on page 2-30.

Note To determine if servers are installed correctly, use the WatchDog commands explained in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*.

Installing the Data Service for High Availability

After installing ISC for High Availability, as described in the "Installing ISC for High Availability" section on page 2-3, and then installing ISC, as described in the "Installing ISC" section on page 2-4, you can install the High Availability Package by going to the following location:

cd /cdrom/isc_ha

Shipped with ISC is the package **CSCOisc.tar.Z**, which is a set of High Availability scripts. The scripts in this package are used as call back methods by Sun™ Cluster. These scripts monitor the health of ISC servers on the active node. If ISC or any of the ISC servers fail, the scripts direct Sun™ Cluster to fail over to the other node.

Implement the following steps:

Step 1 After you install ISC on both the nodes successfully, use the following command to add the package of High Availability scripts to both of the Sun™ Cluster nodes.

pkgadd -d . CSCOisc

Step 2 Use the following command to register the data service.

scrgadm -a -t CSCO.isc

Step 3 Use the following command to create the ISC resource and bind the CSCO.isc data service to it.

scrgadm -a -j <*ISC_resource*> **-g** <*resource-group*> **-t CSCO.isc**

where: <*ISC_resource*> is the ISC resource, for example: **isc-rs**.

Step 4 Use the following command to enable the ISC resource on the desired node.

scswitch -e -j <*ISC_resource*>

where: <*ISC_resource*> is the ISC resource, for example: **isc-rs**.

Step 5 The switch to the second node (the failover node) occurs automatically when an ISC failure occurs on the first node.

Configuring HTTPS

To configure the secure web access to ISC, set up the HTTPS port as follows:

Step 1 Source the environment file, as follows:

For K shell: **. $ISC_HOME/bin/vpnenv.sh**

For C shell: **source $ISC_HOME/bin/vpnenv.csh**

Step 2 Run the command: **configSecurePort.sh** <*isc_home*> <*https_port*> <*hostname*>

where:

<*isc_home*> is the home directory for ISC, for example: **/opt/isc-3.2**

<*https_port*> is the secure HTTPS port you want to use, for example: **8443**.

<*hostname*> is the name of the machine that ISC is installed on, for example: **machinename.cisco.com**

Step 3 Open **$ISC_HOME/resources/webserver/tomcat/conf/server.xml** in the editor of your choice to manually make the following changes.

Step 4 Delete line 101. Line 101 immediately follows the line that reads: "<!-- Define a SSL Coyote HTTP/1.1 Connector…" Line 101 is "<!…".

Step 5 Delete line 110, which is the close comment line, " -->".

Step 6 Run the command: **wdclient restart httpd**.

Logging In for the First Time

To log into ISC for the first time, follow these steps:

Step 1 In your browser, enter the following URL:

`http://server:port/isc/`

See the "Installing ISC" section on page 2-4 for information about setting the port number.

Step 2 Enter the default administrative login name, **admin**, and password, **cisco**, then click **Login**.

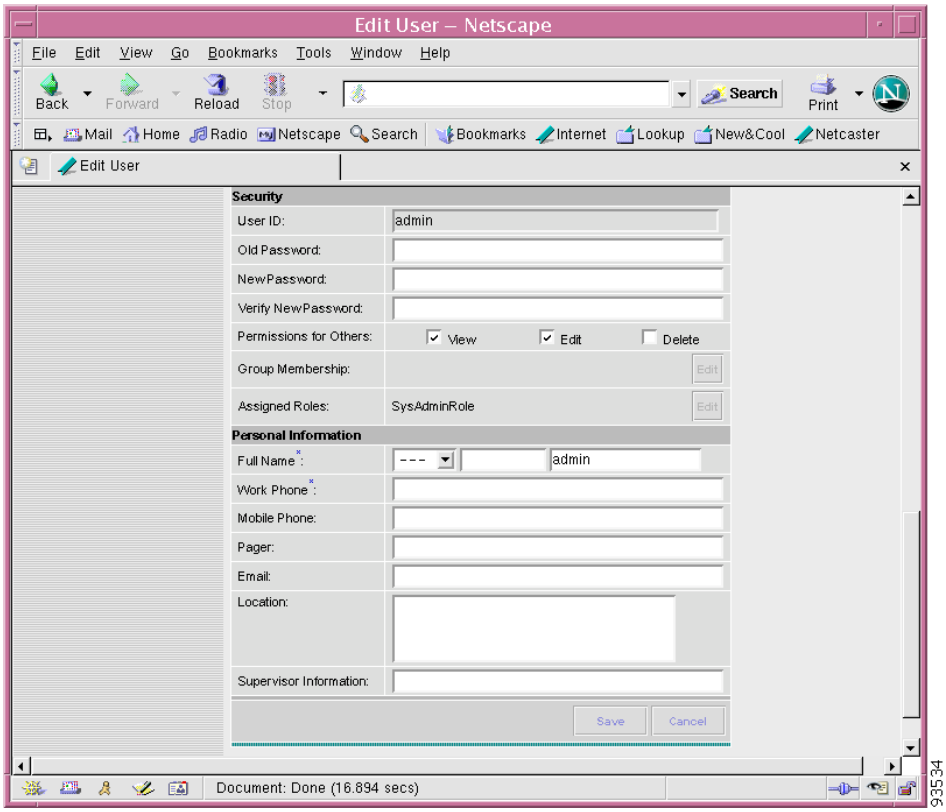
This default user provides administrative access to ISC. You cannot delete this user.

Step 3 We highly recommend you change the password for **admin** from **cisco** to something secure for you. To do this, click the **Administration** tab, then click **Security**, then click **Users**. Select the **admin** check box and then click **Edit**.

The window, as shown in Figure 2-24, "Changing the Password for Security Reasons" appears.

Step 4 Enter the **Security** and **Personal Information**, then click **Save**.

Figure 2-24 Changing the Password for Security Reasons



Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI

After you have installed a **Master** Server and have logged into the ISC system, you can remotely install and uninstall the **Processing Server**, **Collection Server**, or **Interface Server** from the GUI.

Remotely Installing

After you have installed a **Master** Server and have logged into the ISC system, you can remotely install the **Processing Server**, **Collection Server**, or **Interface Server**, as follows.

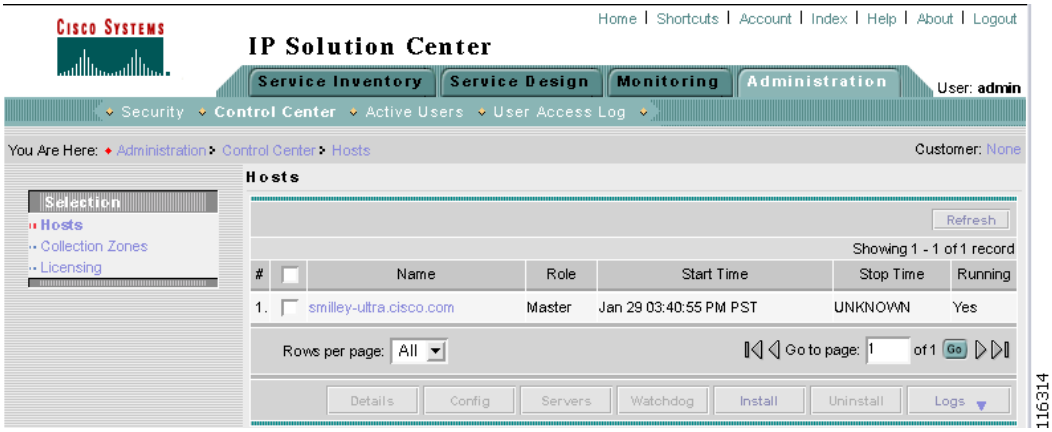
Note Telnet and ftp *must* be available on the machine on which you will perform the remote installation.

Note In this Remote Install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, this is only available through the Installation procedure explained in the "Installing ISC" section on page 2-4.

Step 1 Click the **Administration** tab.

Step 2 Click **Control Center** and you receive a window as shown in Figure 2-25, "Administration > Control Center > Hosts."

Figure 2-25 Administration > Control Center > Hosts



Step 3 From the bottom of the **Hosts** menu, click **Install**.

Step 4 From the **Remote Install** menu, provide the following information:

a. Enter the **Host name** (required)

b. Enter the **ISC User** (required)

Note Be sure you have 1 GB of disk space available in the ISC User's home directory.

c. Enter the **ISC User Password** (required)

d. For the **Role**, accept the default of **Processing Server** or choose the **Collection Server** or **Interface Server** option.

e. Enter the **Install Location** (required).

f. Enter the **Root Password** (optional).

Step 5 Click **Install**.

Step 6 The installation continues and the files are installed. The list of installation processes appears.

Step 7 Review the log message for failures or no failures.

Remotely Uninstalling

After you have installed a **Master** Server and **Processing Server**, **Collection Server**, or **Interface Server** and have logged into the ISC system, you can remotely uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, as follows:

Step 1 Click the **Administration** tab.

Step 2 Click **Control Center**.

Step 3 From the **Hosts** menu, select the check box next to the host name that you want to uninstall.

Step 4 Click **Uninstall**.

Step 5 From the **Uninstall ISC Host** menu, provide the following information:

a. Enter the **ISC User** (required)

b. Enter the **ISC User Password** (required)

Step 6 Click **Uninstall**.

Installing License Keys

To install license keys, do the following:

Note For detailed instructions, see the Licensing section in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*.

Step 1 From the **Home** page of the installed ISC product, navigate as follows: **Administration > Control Center >** from the **TOC**, click **Licensing**.

Step 2 From the **Installed Licenses** table, click **Install**.

Step 3 In the resulting window, enter a **License Key** that you received on your *Right to Use* paperwork with your product.

Step 4 Click **Save**. Your newly installed license appears in an updated version of the Installed Licenses table.

Step 5 Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

Migrating VPNSC 1.x or 2.x Repository to ISC 3.2

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 3.2.

Consider the following issues:

- NetFlow devices cannot be migrated from VPNSC to ISC 3.2.
- Numbered PE and CE IP addresses *must* be in the same subnet. Therefore, if manually assigned PE and CE numbered IP addresses are not in the same subnet, an exception occurs and the service request is not migrated.
- Collection-related data is limited to migration of the most current snapshot of the configuration files existing in the repository of your version of VPNSC, by using the **-ExportConfigs** option in Step 4. If you choose not to migrate the current snapshot of the configuration files, you can obtain the latest configuration files from the live devices. To do this, navigate to: **Monitoring > Task Manager > Create** and from the **Type** menu, click **Collect Config**.
- If you are using a Sybase repository, sample templates are pre-populated in the embedded, empty repository that is shipped with your ISC software. These templates appear in the right side pane of the Template Manager window (which is directly accessible through **Service Design > Template Manager**). If you are using an Oracle repository, the new empty repository for use with your ISC software is created during installation and, consequently, the sample templates are not pre-populated and will not appear in the Template Manager window.
- Service Level Agreements (SLAs) created in VPNSC must be re-created in ISC. Navigate to **Monitoring > SLA > Probes**.

The method you use to migrate your VPNSC 1.x or 2.x repository depends on your database, as follows:

- Migrating from VPNSC 1.x or 2.x to Sybase ASA ISC 3.2, page 2-25
- Migrating from VPNSC 1.x or 2.x to Oracle ISC 3.2, page 2-26

Migrating from VPNSC 1.x or 2.x to Sybase ASA ISC 3.2

Migrate your VPNSC 1.x or 2.x repository to Sybase ASA ISC 3.2 as follows:

Step 1 Get the migration package **ISC3.2MigrationTool_Sybase.tar** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

mkdir /opt/Migration

cp ISC3.2MigrationTool_Sybase.tar /opt/Migration

cd /opt/Migration

Step 2 Untar the migration package.

tar xvf ISC3.2MigrationTool_Sybase.tar

The result is the following files:

- **VPNSCExport.tar.Z**
- **ISC-31_UpgradePkg.tar.Z**
- **install_31_pkg.sh**

- **ConvertRepTo32.sh**
- **upgrade31To32_Sybase.tar.gz**

Step 3 Source the ISC environment files.

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: **source $ISC_HOME/bin/vpnenv.csh**

Step 4 Run the script **ConvertRepTo32.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**] [**-ExportTasks**] [**-prop_file** <*csm_properties file*>]]

where:

<*Rep_Ver*> is the version of the repository to be migrated. The valid values are: **1.x**, **2.0**, and **2.2**. If you have any version 1.x repository, use **1.x**, not the exact version number. If you have a 2.1 or 2.1.1 repository, use **2.2**.

Caution It is essential that you specify the correct version of your existing repository.

<*Rep_Dir*> is the fully qualified path to the repository to be migrated.

-dir <*output_directory*> the default if this optional parameter is not specified is **/tmp/output**.

-size <*KBytes*> the default if this optional parameter is not specified is **1** KByte.

-ExportConfigs (optional) if this optional parameter is not specified, router configuration files are not exported. If this parameter is specified, then router configuration files are exported.

-ExportTasks (optional) if this optional parameter is not specified, tasks are not exported. If this parameter is specified, then tasks are exported.

-prop_file (optional) allows you to specify the location of your <*csm_properties file*>. This value is required if you need to export the threshold value of the **maximum routes** command.

Example:
ConvertRepTo32.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs -ExportTasks -prop_file /users/vpnadm/csm.properties

Step 5 Respond to the requests to enter ISC Username, Password, and the license file.

Step 6 Check for a success message.

Migrating from VPNSC 1.x or 2.x to Oracle ISC 3.2

Migrate your VPNSC 1.x or 2.x repository to Oracle ISC 3.2 as follows:

Step 1 Get the migration package **ISC3.2MigrationTool_Oracle.tar** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

mkdir /opt/Migration

cp ISC3.2MigrationTool_Oracle.tar /opt/Migration

cd /opt/Migration

Step 2 Untar the migration package.

tar xvf ISC3.2MigrationTool_Oracle.tar

The result is the following files:

- **VPNSCExport.tar.Z**
- **ISC-31_UpgradePkg.tar.Z**
- **install_31_pkg.sh**
- **ConvertRepTo32.sh**
- **upgrade31To32_Oracle_ISCServer.tar.gz**
- **upgrade31To32_Oracle_DBServer.tar.gz**
- **3.1schema.tar**

Step 3 Source the ISC environment files.

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: **source $ISC_HOME/bin/vpnenv.csh**

Step 4 Load the **3.1schema.tar** file obtained in Step 2 on a clean Oracle database, as follows:

a. Extract the **createOracleDB.sql** file among other SQL files:

tar xvf 3.1schema.tar

b. Create the ddl/3.1 directory that contains the **createOracleDB.sql** file:

cd ddl/3.1

c. Set up the environment to run SQLPLUS, and then run the **sqlplus** command:

sqlplus

d. At the SQL> prompt, enter **start createOracleDB;**

e. At the next SQL> prompt, enter **exit;**

f. Examine the **oracle.log** log file. If no Oracle errors exist (prefix **ORA-**), the schema loading succeeded.

Step 5 Run the script **ConvertRepTo32.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**] [**-ExportTasks**] [**-prop_file** <*csm_properties file*>]]

where:

<*Rep_Ver*> is the version of the repository to be migrated. The valid values are: **1.x**, **2.0**, and **2.2**. If you have any version 1.x repository, use **1.x**, not the exact version number. If you have a 2.1 or 2.1.1 repository, use **2.2**.

Caution It is essential that you specify the correct version of your existing repository.

<*Rep_Dir*> is the fully qualified path to the repository to be migrated.

-dir <*output_directory*> the default if this optional parameter is not specified is **/tmp/output**.

-size <*KBytes*> the default if this optional parameter is not specified is **1** KByte.

-ExportConfigs (optional) if this optional parameter is not specified, router configuration files are not exported. If this parameter is specified, then router configuration files are exported.

-ExportTasks (optional) if this optional parameter is not specified, tasks are not exported. If this parameter is specified, then tasks are exported.

-prop_file (optional) allows you to specify the location of your <*csm_properties file*>. This value is required if you need to export the threshold value of the **maximum routes** command.

Example:
ConvertRepTo32.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs -ExportTasks -prop_file /users/vpnadm/csm.properties

Step 6 Respond to the requests to enter the Oracle server name, port number, Oracle SID, Oracle user name, and Oracle password.

Step 7 Respond to the requests to enter ISC Username, Password, and the license file.

Step 8 Respond to the prompts from the script, as follows:

a. On the Oracle server machine, unzip the file using:

gunzip upgrade31To32_Oracle_DBServer.tar.gz

b. On the Oracle server machine, untar the file using:

tar xvf upgrade31To32_Oracle_DBServer.tar

c. On the Oracle server machine, enter the following command:

ora-upgrade31To32_Part1.sh

d. After completed, press Enter and the script will ask you to enter the following command on the Oracle server machine:

ora-upgrade31To32_Part2.sh

Step 9 Check for a success message.

Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2

If you have an existing ISC 3.1 or ISC 3.1 plus patches repository, you *must* migrate it to be able to use it with ISC 3.2. The method depends on your database, as follows:

- Sybase ASA Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2, page 2-28
- Oracle Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2, page 2-29

Sybase ASA Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2

Upgrade your Sybase ASA ISC 3.1 or ISC 3.1 plus patches repository as follows:

Step 1 Back up your current ISC 3.1 or ISC 3.1 plus patches database as explained in Appendix C, “Back Up and Restore of ISC Repository and Standby System”.

Step 2 Get the upgrade package **upgrade31to32_Sybase.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

Step 3 Untar the upgrade tool tar file.

upgrade31to32_Sybase.tar.gz

gunzip upgrade31to32_Sybase.tar.gz

tar xvf upgrade31to32_Sybase.tar

Step 4 Source the ISC environment files.

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: source **$ISC_HOME/bin/vpnenv.csh**

Step 5 Stop ISC.

stopall

Step 6 Run the upgrade script.

upgrade31To32.sh

Step 7 Check for a success message.

Oracle Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2

Upgrade your Oracle ISC 3.1 or ISC 3.1 plus patches repository as follows:

Step 1 Back up your current ISC 3.1 or ISC 3.1 plus patches database as explained in Appendix C, "Back Up and Restore of ISC Repository and Standby System".

Step 2 Get the upgrade package **upgrade31To32_Oracle.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc**.

Step 3 Uncompress and untar the upgrade package.

gunzip upgrade31To32_Oracle.tar.gz

tar xvf upgrade31To32_Oracle.tar

You receive two tar files. Place **upgrade31To32_Oracle_ISCServer.tar.gz** on the ISC Master machine in a directory where you can access the ISC environment and place **upgrade31To32_Oracle_DBServer.tar.gz** on the Oracle DB server machine.

Step 4 Untar an upgrade tool tar file.

upgrade31To32_Oracle_ISCServer.tar.gz on the ISC Master machine

gunzip upgrade31To32_Oracle_ISCServer.tar.gz

tar xvf upgrade31To32_Oracle_ISCServer.tar

Step 5 Untar an additional upgrade tool tar file.

upgrade31To32_Oracle_DBServer.tar.gz on the Oracle DB server machine

gunzip upgrade31To32_Oracle_DBServer.tar.gz

tar xvf upgrade31To32_Oracle_DBServer.tar

Step 6 Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To32_Part1.sh**

Step 7 Source the ISC environment files.

If **sh** or **ksh** shell: **$ISC_HOME/bin/vpnenv.sh**

If **csh** shell: source **$ISC_HOME/bin/vpnenv.csh**

Step 8 Stop ISC.

stopall

Step 9 Run the following command on the ISC Server Master machine:

$ **upgrade31To32_Oracle.sh**

Step 10 Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To32_Part2.sh**

Step 11 Check for a success message.

Launching Inventory Manager and Topology Tool

ISC provides a downloadable version of Version 1.4.2 of Java Runtime Environment (JRE) for various operating systems when you launch Inventory Manager or Topology Tool. If you choose to install JRE Version 1.4.2, you must quit the browser and log in again after the installation is complete.

Specific instructions to launch the Inventory Manager and the Topology Tool are explained in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2* along with the explanations of these features.

Uninstalling ISC

To uninstall ISC, we recommend that you first remotely uninstall all the servers other than the **Master** server: the **Processing Server**, **Collection Server**, and **Interface Server**. See the "Remotely Uninstalling" section on page 2-24. Then uninstall the **Master** server, as follows:

Step 1 Log into the server that you want to uninstall.

Step 2 At the Solaris prompt, log in as the ISC owner.

Step 3 Go to the ISC installation directory.

Step 4 Source the environment, as follows:

For a sh or ksh shell:

```
. bin/vpnenv.sh
```

For a csh shell:

```
source bin/vpnenv.csh
```

Step 5 Remove ISC by entering the following command from a location outside the <*ISC_HOME directory*>:

```
uninstall.sh
```

This command removes all files from the installation directory. This command also removes the database and its contents. Database backups are not removed if they reside in a different directory from the installation directory.

Setting Up Oracle for ISC

This appendix describes how to set up an Oracle 9.2.0.1 server that works with Cisco IP Solution Center (ISC). This appendix is written for database administrators who are familiar with Oracle.

Note ISC 3.2 was tested with Oracle 9.2.0.1. If you would like to use another version of Oracle, see Oracle's compatibility information.

This chapter does not cover all the details about installing and setting up this Oracle server. For the complete information, see the Oracle Installation Guide. ISC provides schema files to be loaded on an Oracle server. The ISC customer must decide on the Oracle server configuration.

This appendix contains the following sections that should be addressed in order:

This appendix also contains a "Troubleshooting" section on page A-6.

Prerequisites

ISC support for an Oracle database is for Oracle 9.2.0.1 with US7ASCII. This is the version of Oracle with which ISC 3.2 was tested. If you would like to use another version, see Oracle's compatibility information.

The remaining prerequisites are as specified in the following steps:

Step 1 When the Oracle server is set up, the following initialization parameters should be in the database **init** file:

- db_block_size = 8192 or larger

- compatible = “8.1.0.0”
- open_cursors = 512 or larger
- processes = 70

Step 2 Record the following information about the server setup. This information is needed during the ISC installation:

- Oracle server instance identifier (SID)

Note This is specified in Figure 2-14 on page 2-13.

- database port number for client connections (default: 1521)
- Oracle user ID and password created for ISC

Note Create an Oracle database userid and password. This is needed during ISC installation. Do not use the **system** or **sys** account for ISC data. Use a separate table space other than the system table space. See Figure 2-15 on page 2-14.

Step 3 Before loading the ISC database schema, make sure the Oracle database has been successfully started and the database user has proper privileges. See the Oracle Administration Guide for detailed instructions about how to set up the database and manage user accounts.

Step 4 Proceed to the section “Installing Oracle.”

Installing Oracle

The following information about an Oracle installation is just one example.

You must install Oracle before you install the Cisco IP Solution Center (ISC) software (or at least know your Oracle home directory, host machine, and Oracle Server ID), and your database must be running when you launch the ISC servers.

If you intend to use the same Oracle installation with more than one installation of the ISC servers, you must create a unique Oracle SID and Oracle tablespace for each ISC installation.

init*ORACLE_SID*.ora

This file should already exist in the `/dbs` subdirectory of your Oracle installation. (The filename contains your database’s SID in place of *`ORACLE_SID`*. For example, if you named your database `ISC`, this file is named `initISC.ora`.)

oratab

The `oratab` file should be located in the `/var/opt/oracle` directory on the machine on which the database is installed. It is used by Oracle’s **dbstart** utility to identify your database.

The `oratab` file consists of a single line:

database_name:*location_of_your_Oracle_executables*:Y

If your Oracle home directory is `/oracle/9.2.0.1` and your database SID is `ISC`, the `oratab` entry would be as follows:

ISC:/oracle/9.2.0.1:Y

This file identifies the name and location of your database for the Oracle utility **dbstart** (and its companion **dbshut**). The **dbstart** utility starts Oracle; the "Y" at the end of the `oratab` entry tells the **dbstart** utility to open the database named `ISC`. (Substitute your database name for ISC in the sample. List the path to your Oracle installation as an absolute path, not a relative path.)

To make this happen automatically following a reboot (after a power interruption, for example), execute the **dbstart** utility from a script in the `/etc/init.d` directory on the Oracle host machine.

Verifying and Launching Oracle

Your Oracle database must be open before you can install or use the ISC software.

First, verify the Oracle processes, as described in the following section. If the processes are running, you can skip the succeeding section.

Verifying Oracle Processes

Log into the Oracle host machine and enter the following on the command line to see if the Oracle processes are running:

ps -ef | grep ora_

If there is no output displayed from the **ps** command, Oracle is not running.

If Oracle is running, you should see something similar to the following:

oracle 328 1 0 14:25:18 0:00 ora_pmon_ISC

oracle 328 1 0 14:25:18 0:00 ora_dbwr_ISC

oracle 328 1 0 14:25:18 0:00 ora_lgwr_ISC

oracle 328 1 0 14:25:18 0:00 ora_ckpt_ISC

oracle 328 1 0 14:25:18 0:00 ora_smon_ISC

oracle 328 1 0 14:25:18 0:00 ora_reco_ISC

oracle 328 1 0 14:25:18 0:00 ora_wmon_ISC

These are the Oracle processes currently running (your output might not match this list exactly, depending on which Oracle components are installed).

Launching Oracle and Opening Your Database

Your Oracle database must be open before you can install or use the ISC software.

If Oracle is not currently running, you need to use the startup utilities located in the `/bin` subdirectory of your Oracle installation.

To open your database, you must be logged into the Oracle host workstation under the Oracle administrator (DBA) user ID; you then locate your `$ORACLE_HOME/bin` subdirectory.

On the command line, enter the following:

dbstart

The `dbstart` script starts the database identified in the `oratab` file. If the database starts successfully, you should see several lines of output, including the following:

SVRMGR> Connected to an idle instance.

SVRMGR> ORACLE instance started.

...and ending with the following:

Server Manager Complete.

Database "ISC" warm started.

If the listener process is not running, you need to start that process as well. On the command line, enter the following:

lsnrctl start

You should see several lines of output as the process is invoked, then you should see output similar to the following:

Services Summary...

ISC has 1 Service handler(s)

The command completed successfully

Setting Up Your Oracle Files

To configure your database to work with the ISC software, you must create a tablespace and configure several files.

You must be logged into the Oracle host using the user ID (such as `oracle`) created during the Oracle installation procedure.

Oracle Tablespace Requirements

You must create an Oracle tablespace for your ISC tables.

To create the tablespace, Oracle must be running and your database must be open.

Log into the Oracle host using the `oracle` user ID. Identify (or create) the directory where your ISC data should be stored, and grant write permission to the `oracle` user ID. Be sure your `ORACLE_SID` and `ORACLE_HOME` environment variables are set correctly, then launch the Oracle utility `svrmgrl`, which is located in the `$ORACLE_HOME/bin` directory.

At the SVRMGR prompt, enter the following on the command line:

connect internal;

CREATE TABLESPACE ISC_DAT

DATAFILE '/*your_data_directory*/ISC_DAT_01.dbf' size 500M

autoextend on

next 50M

maxsize unlimited;

The data directory you specify must already exist. The TABLESPACE and DATAFILE names are arbitrary. You can use any names that help you keep track of which files are associated with which database. The only requirement is that the name given to the tablespace at the time of its creation (ISC_DAT in the example) must be the same as the default tablespace listed when you create the isc user account.

The autoextend option allows ORACLE to automatically extend your data file. The maximum size of the data file is limited only by the available space on the file's disk.

isc Oracle User Account

While svrmgrl is still running, create an isc user account using your ISC_DAT tablespace as follows:

CREATE USER isc IDENTIFIED BY cisco

DEFAULT TABLESPACE ISC_DAT;

GRANT CONNECT TO isc;

GRANT RESOURCE TO isc;

You should use this user and password when entering Oracle information in the script isc.configure.

Testing Your Oracle Database Connection for Oracle User isc

When you have configured your database and listener file, enter the following (for the Oracle user isc and for the database named ISC) on the command line:

sqlplus <*username*>/<*password*>

<*username*> is a database username (in our previous example, we used **isc**).

<*password*> is a database password (in our previous example, we used **cisco**).

If your system is set up properly (and your Oracle database is running), you should see a message advising you that you are connected to Oracle. Enter quit on the command line to exit the database.

Load ISC Database Schema

Before installing the ISC software, load the ISC database schema on the Oracle server, as follows:

Step 1 Mount the ISC CD on the Oracle server machine or **cd** to the ISC directory if you downloaded ISC from the web.

Step 2 Copy the **schema.tar** file from the ISC product CD or the ISC directory to a temporary directory on the Oracle server.

Step 3 Extract the createOracleDB.sql among other SQL files:

```
tar xvf schema.tar
```

Step 4 Change to the ddl/3.2 directory that contains the **createOracleDB.sql** file:

```
cd ddl/3.2
```

Step 5 Set up the environment to run SQLPLUS, and then run the **sqlplus** command:

```
sqlplus
```

Step 6 At the SQL> prompt, enter **start createOracleDB;**

Step 7 At the next SQL> prompt, enter **exit;**

Step 8 Examine the **oracle.log** log file. If no Oracle errors exist (prefix **ORA-**), the schema loading succeeded.

Step 9 Proceed to the section "ISC Software Installation."

ISC Software Installation

Do the following:

Step 1 Follow the **custom** install instructions in Chapter 2, "Installing and Logging Into ISC," section Installing ISC, page 2-4, and log in, as explained in the section Logging In for the First Time, page 2-21.

Step 2 Proceed to the section "Verify ISC Installation with Oracle".

Verify ISC Installation with Oracle

To verify the ISC installation with Oracle, do the following:

Step 1 Run **sqlplus** <*oracle_id*>/<*oracle_password*> on the Oracle server.

Step 2 From the **SQL>** prompt, run **select host_name** from **vpnsc_host;**

This command returns the installed ISC host name.

Backup of Oracle Database

See Appendix C, "Back Up and Restore of ISC Repository and Standby System."

Troubleshooting

This section lists Oracle database-related trouble shooting tips based on the following error messages:

- **ORA-01631: max # extents (4096) reached in table xyz**

  If you receive this message, it is typically an Oracle server storage configuration issue. This problem occurs when the tablespace for ISC exceeds the limit set by the database configuration. To prevent this, plan proper storage before ISC is set up. If this problem occurs, increase the initial or next extent, increase the growth percentage (such as, PCT_INCREASE), or reset the number of max extents (can be unlimited). The ISC data must be exported and imported to the tablespace with the new tablespace parameters.

- **Unable to contact Rbac Manager**

  If you receive this message on ISC and are unable to log in, this might be because ISC cannot connect to the Oracle database. To avoid this situation, increase the number of Oracle server processes.

- **Cannot log into Inventory Manager or Topology Manager**

  If you cannot log into the Inventory Manager or Topology Manager, verify that the Oracle hostname is accessible from a client machine, either by DNS or a host file.

- **Resynchronize ISC with new or updated Oracle ID and password**

  If the Oracle ID and password change after the ISC installation, you must execute the following:

  a. execjava.sh com.cisco.vpnsc.common.BootStrapHelper put repository <*oracle_id*> <*oracle_password*>

  b. update etc/spe/cns.properties and modify these two properties:

     DataAccess.principal.1 `<oracle_id>`

     DataAccess.credentials.1 `<oracle_password>`

Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3.x and 1.4 Software with ISC

Overview

Cisco IP Solution Center (ISC) supports the Device Access Protocol (DAP) of CNS for communication with any Cisco IOS device. The DAP includes:

- uploading a configuration file from a device
- downloading a configlet to a device
- executing a command on a device and obtaining the result (all communications).

ISC supports CNS Plug-and-Play.

In addition to this Overview section, this chapter contains the following major sections:

- SetUp Steps, page B-1
- Checking Router Configurations Overview, page B-8

SetUp Steps

To enable the Cisco CNS Intelligence Engine 2100 (IE2100) Series Configuration Engine functionality on ISC, set up in the following order:

1. Set up the Cisco CNS IE2100 device, as shown in "Set Up Cisco CNS IE2100 Appliance."
2. Configure a TIBCO Rendezvous Routing Daemon (**rvrd**), as shown in "Configure a TIBCO Rendezvous Routing Daemon."

Set Up Cisco CNS IE2100 Appliance

ISC supports the integration with Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3.x and 1.4 software.

For the Cisco CNS Configuration Engine 1.3.x software installation and setup, see the Cisco CNS Configuration Engine 1.3.x documentation set at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel13/index.htm

For the Cisco CNS Configuration Engine 1.4 software installation and setup, see the Cisco CNS Configuration Engine 1.4 documentation set at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel14/index.htm

On a freshly set up Cisco CNS IE2100 appliance, remove Pluto protection, as follows.

Step 1 Log in as **root**.

Step 2 Enter:

plutosetup.

Step 3 A warning appears:

"plutosetup will open some class files to public access. It is a security risk."

Continue (y/n):

Answer **y** for yes to the above warning.

Note Because the Cisco CNS IE2100 appliance and the ISC Master server are behind a secure barrier, we can safely answer **y** for yes to the security risk warning message above. This removal of Pluto protection exposes some files in Cisco CNS IE2100 that allow ISC to create, delete, and edit devices in the IE2100 repository. This is needed for proper ISC to Cisco CNS Configuration Engine 1.3.x and 1.4 integration. Removal of Pluto protection only needs to occur when a particular Cisco CNS IE2100 appliance is first used and every time the file **/opt/CSCOcnsie/bin/pluto** is deleted for any reason.

Configure a TIBCO Rendezvous Routing Daemon

In this section, do the following:

1. Configuring the rvrd Daemon on the ISC Master Machine, page B-2
2. Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance, page B-4
3. Testing rv Connectivity Between ISC and Cisco CNS IE2100, page B-6

Configuring the rvrd Daemon on the ISC Master Machine

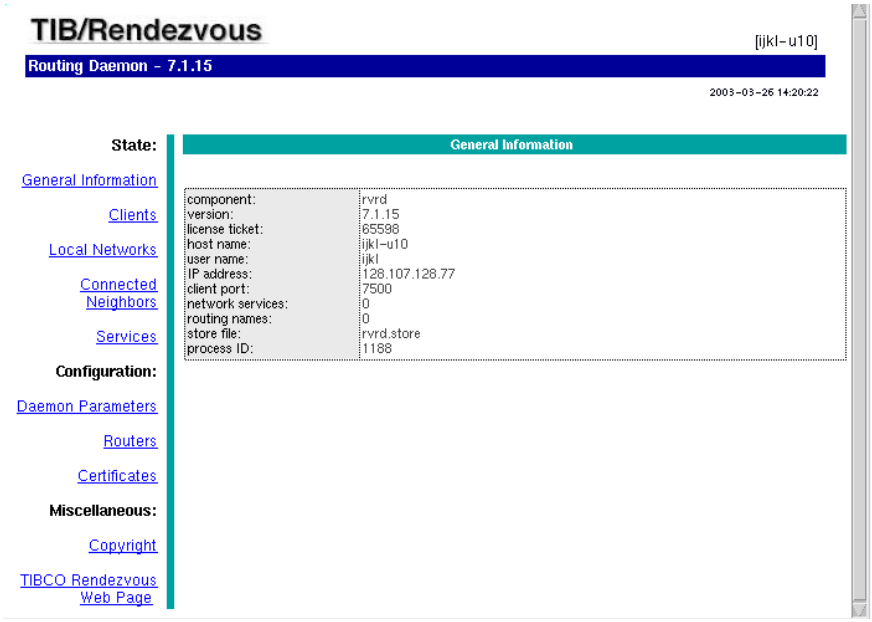
To configure an **rvrd** daemon on an ISC Master server, do the following:

Step 1 The TIBCO Rendezvous Routing Daemon (**rvrd**) is the default daemon on the ISC Master server

To configure an **rvrd** daemon on an ISC Master server, start an ISC-supported browser and go to the following URL: **http://**<*isc_hostname*>**:7580** or **http://**<*isc_ip_address*>**:7580**

Step 2 Look at the **component** field under the **General Information** link to verify that **rvrd** is running. It should say **rvrd**, as shown in Figure B-1, "ISC rvrd Verification."

Figure B-1 ISC rvrd Verification



Step 3 Click on the **Routers** link in the left column.

Step 4 A security alert window appears, asking you if you want to proceed. Answer **Yes** or **Next**, depending on your browser, to continue.

Step 5 Verify that ISC automatically created the **Router Name** <*isc_hostname*> for the ISC Master server.

Step 6 In the **Local Network** column, click the current entry in the field (this number indicates the number of local networks currently defined). Verify that ISC automatically created the **isc** network with the following values:

a. The **Local Network Name**: **isc**.

b. The **Service**, the TIBCO port number for the ISC installation (default: 7530).

c. The **Network Specification** field is optional.

d. No change in the value of the **Cost** field.

Step 7 Click on the **isc** entry created in the **Local Network Name** column.

Step 8 Verify that ISC automatically added **Subjects cisco.cns.>** and **cisco.mgmt.cns.>** to both the **Import Subjects** and **Export Subjects** columns.

Step 9 Again, click on the **Routers** link in the left column.

Step 10 In the **Neighbor** column, click the current entry in the field (this number indicates the number of neighbors currently defined).

Step 11 In the **Local Endpoint** section, if you choose a port number other than the default, be sure the **Port** for **Local Endpoint** defined on the ISC Master server equals the **Port** for **Remote Endpoint** defined on the Cisco CNS IE2100 appliance (defined in Step 22c. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").

Step 12 Add the following in the **Remote Endpoint** section:

a. In the **Host** field, add the IP address or hostname of the Cisco CNS IE2100 appliance.

b. If you choose a port number other than the default, the **Port** for **Remote Endpoint** defined on the ISC Master server must equal the **Port** for **Local Endpoint** defined on the Cisco CNS IE2100 appliance (defined in Step 22d. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").

c. In the **Router Name** field, enter the name of the Cisco CNS IE2100 appliance followed by **-ie2100**. Any unique name works, but this recommendation is synchronized with this example.

Example: <*ie2100_hostname*>**-ie2100**

Note It is very important that the **Neighbor Name** is the same as the **router** name configured on the Cisco CNS IE2100 appliance.

d. Click **Add Neighbor Interface**. The entered values appear in the corresponding columns in the upper section of the page.

Note If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Selected Neighbor Interface(s)**.

Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance

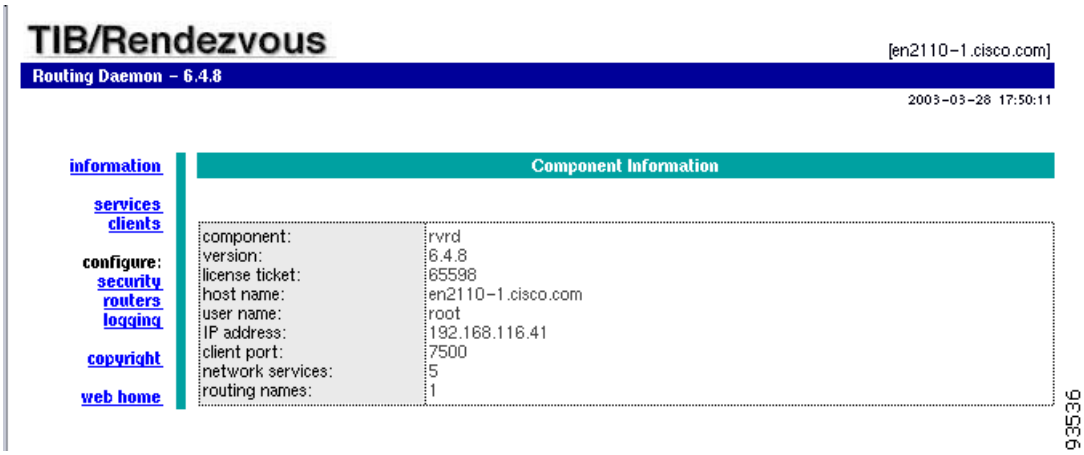
To configure an **rvrd** daemon on a Cisco CNS IE2100 appliance, do the following:

Step 1 The TIBCO Rendezvous Routing Daemon (**rvrd**) is the default daemon on the Cisco CNS IE2100 appliance.

To configure an **rvrd** daemon on a Cisco CNS IE2100 appliance, start an ISC-supported browser and go to the following URL: **http://**<*ie2100_hostname*>**:7580** or **http://**<*ie2100_ip_address*>**:7580**.

Step 2 Look at the **component** field under the **information** link to verify that **rvrd** is running. It should say **rvrd**, as shown in Figure B-2, "Cisco CNS IE2100 rvrd Verification."

Figure B-2 Cisco CNS IE2100 rvrd Verification



Step 3 Click on the **routers** link in the left column.

Step 4 In the **Add Router Name** field in the upper part of the window, enter the name of the Cisco CNS IE2100 appliance, followed by **-ie2100**. Any unique name works, but this recommendation is synchronized with this example.

Example: <*ie2100_hostname*>**-ie2100**

Step 5 Click **Add** to create an entry with the new router name.

The chosen name appears in the **Router Name** column in the lower part of the window.

Step 6 In the **Local Networks** column, click the current entry in the field (this number indicates the number of local networks currently defined).

Step 7 Specify the local Cisco CNS IE2100 network with the following values:

a. In the **Local Network Name** field, enter the unique name entered in Step 6a. of the section "Configuring the rvrd Daemon on the ISC Master Machine". In the example, this is **isc**.

b. In the **Service** field, add the TIBCO port number for the ISC installation (default: 7530).

c. The **Network Specification** field is optional. You can enter a description.

Step 8 Click **Add Local Network**. The entered values appear in the corresponding columns in the lower section of the page.

Step 9 Click on the entry just created. In this example, it is **isc**.

Step 10 In the **Add Subject** field, enter **cisco.cns.>**.

Step 11 Click **Add for Import and Export**. The entered values appear in the **Imported Subjects** and **Exported Subjects** columns in the lower part of the window.

Step 12 If you are using Cisco CNS Configuration Engine 1.3.2 or 1.4 in the **Subject** field in the lower part of the window, enter **cisco.mgmt.cns.>**, repeat Step 11, and then proceed to Step 13. If you are using Cisco CNS Configuration Engine 1.3 or 1.3.1, just proceed to Step 13.

Step 13 Click the **routers** link in the left column.

Step 14 In the **Local Networks** column, click the current entry in the field (this is at least **1** now, because you already added one local network).

Step 15 Specify the local Cisco CNS IE2100 network with the following values:

a. In the **Local Network Name** field, add a unique name. For example: **ie2100-eventBus**.

b. In the **Service** field, add the **CNS Event Bus Service Parameter** value defined in the setup of the Cisco CNS IE2100 appliance (default: 7500).

c. In the **Network Specification** field, leave it blank or enter the name of the Cisco CNS IE2100 appliance.

Note If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Marked Items**.

Step 16 Click on the entry just created in the **Local Network Name** column.

Step 17 In the **Add Subject** field in the upper part of the window, enter **cisco.cns.>**.

Step 18 Click **Add for Import and Export**. The entered values appear in the **Imported Subjects** and **Exported Subjects** columns in the upper part of the window.

Step 19 If you are using Cisco CNS Configuration Engine 1.3.2 or 1.4, in the **Subject** field in the lower part of the window, enter **cisco.mgmt.cns.>**, repeat Step 18, and then proceed to Step 20. If you are using Cisco CNS Configuration Engine 1.3 or 1.3.1, just proceed to Step 20.

Step 20 Click the **routers** link in the left column.

Step 21 In the **Neighbors** column, click the current entry in the field (this number indicates the number of neighbors currently defined).

Step 22 Add the following in the **Neighbors Configuration** window:

a. In the **Neighbor Name** column, add the router name as automatically configured on the ISC Master server, and verified in Step 5 of the section "Configuring the rvrd Daemon on the ISC Master Machine." This router name is <*isc_hostname*>.

Note It is very important that the **Neighbor Name** is the same as the **router** name configured on the ISC Master server.

b. In the **Hostname or IP addr** column, add the host name or IP address of the ISC Master server.

c. In the **Remote** column, add the **Port** number for the **Local Endpoint** defined on the ISC Master server in Step 11 of the section "Configuring the rvrd Daemon on the ISC Master Machine."

d. In the **Local** column, add the **Port** number for **Remote Endpoint** defined on the ISC Master server, in Step 12b. of the section "Configuring the rvrd Daemon on the ISC Master Machine."

Step 23 Click **Add Active [all]**.

A good indication that the connection is established is when the new name in the **Neighbor Name** column appears as a hyperlink in the bottom of the window. It takes a few seconds for this to occur. Also, it is recommended to click **Refresh** a few times to see the hyperlink.

Note If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Marked Items**.

Testing rv Connectivity Between ISC and Cisco CNS IE2100

Test that the **rvrd** setup has been successful, by testing the following:

- Connectivity from ISC Master Server to Cisco CNS IE2100 Appliance
- Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server.

Connectivity from ISC Master Server to Cisco CNS IE2100 Appliance

Test the successful setup of connectivity from an ISC Master server to a Cisco CNS IE2100 appliance:

Step 1 Telnet to the Cisco CNS IE2100 appliance.

Step 2 Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 3 Set up a TIBCO Listener to the TIBCO port the ISC installation is running and as configured above (default: 7530):

./cns-listen -service <*tibco_port_number*> **"cisco.cns.>"**

Leave the Listener running in this window.

Step 4 In a separate window, navigate to the following directory:

cd /<*isc_install_directory*>**/thirdparty/rv/bin**

Step 5 Send a TIBCO message to the Cisco CNS IE2100 appliance on the configured TIBCO port number (default: 7530):

/tibrvsend -service <*tibco_port_number*> **"cisco.cns.config-changed" "**<*variable_message*>**"**

Step 6 If the message is seen in the Listener window on the Cisco CNS IE2100 appliance, connectivity is established correctly from the ISC Master server to the Cisco CNS IE2100 appliance for the TIBCO subject **"cisco.cns.>"**.

Step 7 If you are using Cisco CNS Configuration Engine Release 1.3.2 or 1.4, proceed with Step 8 to Step 12. Otherwise, proceed to the "Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server" section on page B-7."

Step 8 Telnet to the Cisco CNS IE2100 appliance.

Step 9 Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 10 Set up a TIBCO Listener to the TIBCO port the ISC installation is running and as configured above (default: 7530):

./cns-listen -service <*tibco_port_number*> **"cisco.mgmt.cns.>"**

Leave the Listener running in this window.

Step 11 In the window created in Step 4, send a TIBCO message to the Cisco CNS IE2100 appliance on the configured TIBCO port number (default: 7530):

/tibrvsend -service <*tibco_port_number*> **"cisco.mgmt.cns.config-changed" "**<*variable_message*>**"**

Step 12 If the message is seen in the Listener window on the Cisco CNS IE2100 appliance, connectivity is established correctly from the ISC Master server to the Cisco CNS IE2100 appliance for the TIBCO subject **"cisco.mgmt.cns.>"**.

Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server

Test the successful setup of connectivity from a Cisco CNS IE2100 appliance to an ISC Master Server, as follows:

Step 1 On the ISC device, go to the following directory:

cd /<*isc_install_directory*>**/thirdparty/rv/bin**

Step 2 Set up a TIBCO Listener to the TIBCO port that **isc** installation is running and as configured above (default: 7530):

./tibrvlisten -service <*tibco_port_number*> **"cisco.cns.>"**

Leave the Listener running in this window.

Step 3 In a separate window, telnet to the Cisco CNS IE2100 appliance.

Step 4 Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 5 Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):

./cns-send -service <*tibco_port_number*> **"cisco.cns.config-changed" "<***variable_message***>"**

Step 6 If the message is seen in the Listener window on the ISC Master server, connectivity is established correctly from the Cisco CNS IE2100 appliance to the ISC Master server for the TIBCO subject **"cisco.cns.>"**.

Step 7 If you are using Cisco CNS Configuration Engine Release 1.3.2 or 1.4, proceed with Step 8 to Step 12. Otherwise, proceed to the "Checking Router Configurations Overview" section on page B-8."

Step 8 In the window created in Step 1, set up a TIBCO Listener to the TIBCO port that **isc** installation is running and as configured above (default: 7530):

./tibrvlisten -service <*tibco_port_number*> **"cisco.mgmt.cns.>"**

Leave the Listener running in this window.

Step 9 In a separate window, telnet to the Cisco CNS IE2100 appliance.

Step 10 Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 11 Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):

./cns-send -service <*tibco_port_number*> **"cisco.mgmt.cns.config-changed" "<***variable_message***>"**

Step 12 If the message is seen in the Listener window on the ISC Master server, connectivity is established correctly from the Cisco CNS IE2100 appliance to the ISC Master server for the TIBCO subject **"cisco.mgmt.cns.>"**.

Checking Router Configurations Overview

The Cisco IOS image is needed for the routers used with the Cisco CNS IE2100 functionality (that is, the CNS transport mechanism and/or the CNS Plug-and-Play feature). For Cisco CNS Configuration Engine Release 1.3, the recommended Cisco IOS release is 12.2(8)T or later; for Cisco CNS Configuration Engine Release 1.3.1, 1.3.2, or 1.4, the recommended Cisco IOS release is 12.2(11)T or later. Cisco IOS releases 12.3(1)T or later are supported only by Cisco CNS Configuration Engine Releases 1.3.2 and 1.4.

Additionally, the router running a configuration must contain the following two CNS commands:

1. **cns config partial** <*IE2100 address*> **80**
2. **cns event** <*ie2100 address*> **11011**

   or

   cns event <*ie2100 address*> **11011 keepalive** <*num. of seconds*> <*num. of trials*>

Note The **keepalive** option makes sure the TCP connection between the Cisco CNS IE2100 appliance and the router is alive at all times. It sends keepalive messages at <*num. of seconds*> intervals with <*num. of trials*> retries.

Also, the router startup configuration must contain the following two CNS commands:

1. **cns config initial** <*ie2100 address*> **event**

   The **cns config initial** command should be configured in the startup configuration of the Cisco IOS device or router. It triggers the router to pick up and apply any initial configuration that might be waiting for it on the Cisco CNS IE2100 appliance. After the **cns config initial** command is executed, this command is automatically removed. The recommendation is to include the **cns config partial** command in the initial configuration that is waiting on the Cisco CNS IE2100 appliance. If a **no persist** option is used, the router does not perform a **write-mem**, thus keeping the startup configuration from being overwritten.

2. **cns event** <*ie2100 address*> **11011**

   or

   cns event <*ie2100 address*> **11011 keepalive** <*num. of seconds*> <*num. of trials*>

Note The **keepalive** option makes sure the TCP connection between the Cisco CNS IE2100 appliance and the router is alive at all times. It sends keepalive messages at <*num. of seconds*> intervals with <*num. of trials*> retries.

Different IOS versions can support additional CNS commands or different formats of the same CNS command. See the Cisco CNS software documentation for more details on the other possible CNS commands and their options.

Back Up and Restore of ISC Repository and Standby System

This chapter explains how to back up and restore your Sybase and Oracle databases and how to set up a standby system:

Back Up and Restore of ISC Repository

The CCO location of scripts for these procedures is:

http://www.cisco.com/cgi-bin/tablebuild.pl/isc

The subsections are:

Data Items Included in Back Up and Recovery

Most of the ISC-related data items are stored in a repository held on a relational database and the rest are stored in an operating system level file system. For ISC to function flawlessly on restart, following a crash, it is necessary that the proposed backup and recovery feature include various ISC-related data items as a whole. The underlying tasks involved in backup and recovery procedures differ depending on the nature of persistence of these data items. However, these procedures shall work commonly for all the data items in a seamless and transparent manner.

The following data elements are included in ISC's backup and recovery plan:

1. **Main repository**: This repository consists of data items such as Customers/Organizations, VPNs, Policies, Devices, and Interfaces. This data is held on an RDBMS, either the embedded Sybase ASA database or the customer's Oracle database.

2. **SLA repository:** This repository consists of data items pertaining to Service Level Agreements (SLA) and Probes. This repository is held on a Sybase ASA database. This is the default repository for devices that do not have a Collection Server. There will be SLA repositories in each of the collection server machines, if available. If your SLA repository is on one or more Collection Servers separate from the Main Server, you must run the back up on each Collection Server for the SLA repository.
3. Others: There are a few data items that are stored in the OS level file system under various ISC install directories, which would be part of the proposed backup and recovery plan.

Guidelines

For the backup and recovery plan to function efficiently, customers are requested to follow these guidelines:

Step 1 Support exists for the following types of supported back ups:

a. **Full back up** is a complete back up of the ISC repository, ISC repository transaction logs, and other ISC data files held in the file system. It is recommended to have a full back up on a default weekly basis, which could be reconfigured as desired by the customer.

b. **Incremental back up** is a back up of all the data from the time of the last full or incremental back up until this incremental back up. It is recommended that the full back up be interspersed with several incremental back ups, by default, daily.

c. **Archive back up** is a complete back up of all ISC data in respective archive files, typically on a tape drive. Use this back up if you are backing up directly to a tape.

d. **Live back up** creates redundant copies of transaction logs to restore the ISC repositories held on a Relational Database Management System (RDBMS) and creates redundant copies of other ISC data held on the file system on the Main server machine. These redundant copies are typically set up on a secondary machine to restart ISC if the primary server machine becomes unusable.

Step 2 The plan default schedule requires **Weekly FULL ONLINE** (while system is running) back ups interspersed with **DAILY ONLINE** incremental back ups of all ISC data items. An **ARCHIVE full** back up, preferably on a tape, is recommended on a MONTHLY basis. This archive tape back up should be stored in different premises to prevent any loss of back ups in case of acts of physical disasters at the main server location.

Step 3 It is important to keep more than one full back up to prevent accidental loss of backup copies.

Step 4 Create archive backup copies on a tape device.

Step 5 External factors such as available hardware, the size of database files, recovery medium, disk space, and unexpected errors can affect customers' recovery time. When implementing the plan, the customer shall allow additional recovery time for miscellaneous tasks that must be performed, such as entering recovery commands or retrieving, loading, and organizing tapes.

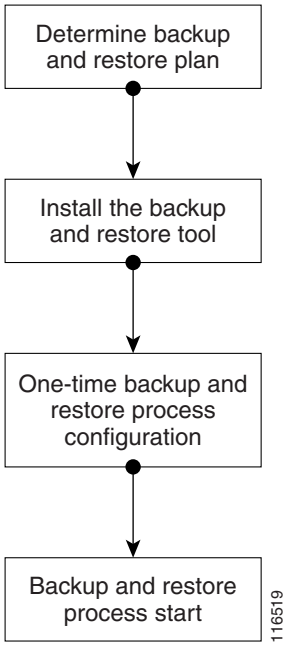
Sybase Backup and Restore Process Overview

This section describes how to backup and restore Sybase ASA for an ISC installation. This section contains the following sections:

Overview of the Backup and Restore Process

Figure C-1 shows an overview of the Sybase ASA backup and restore process.

Figure C-1 Overview - Sybase ASA Backup and Restore



Planning your Backup and Restore Process

Before backing up and restoring your Sybase installation, you must first prepare a plan. To prepare your plan, follow these steps:

Step 1 Determine the frequency for full backups.

Step 2 Determine the frequency for incremental backups.

Step 3 Determine the location for storing the backups.

Note The file system must be accessible by the primary ISC production machine and the secondary system, if you want to perform live backups.

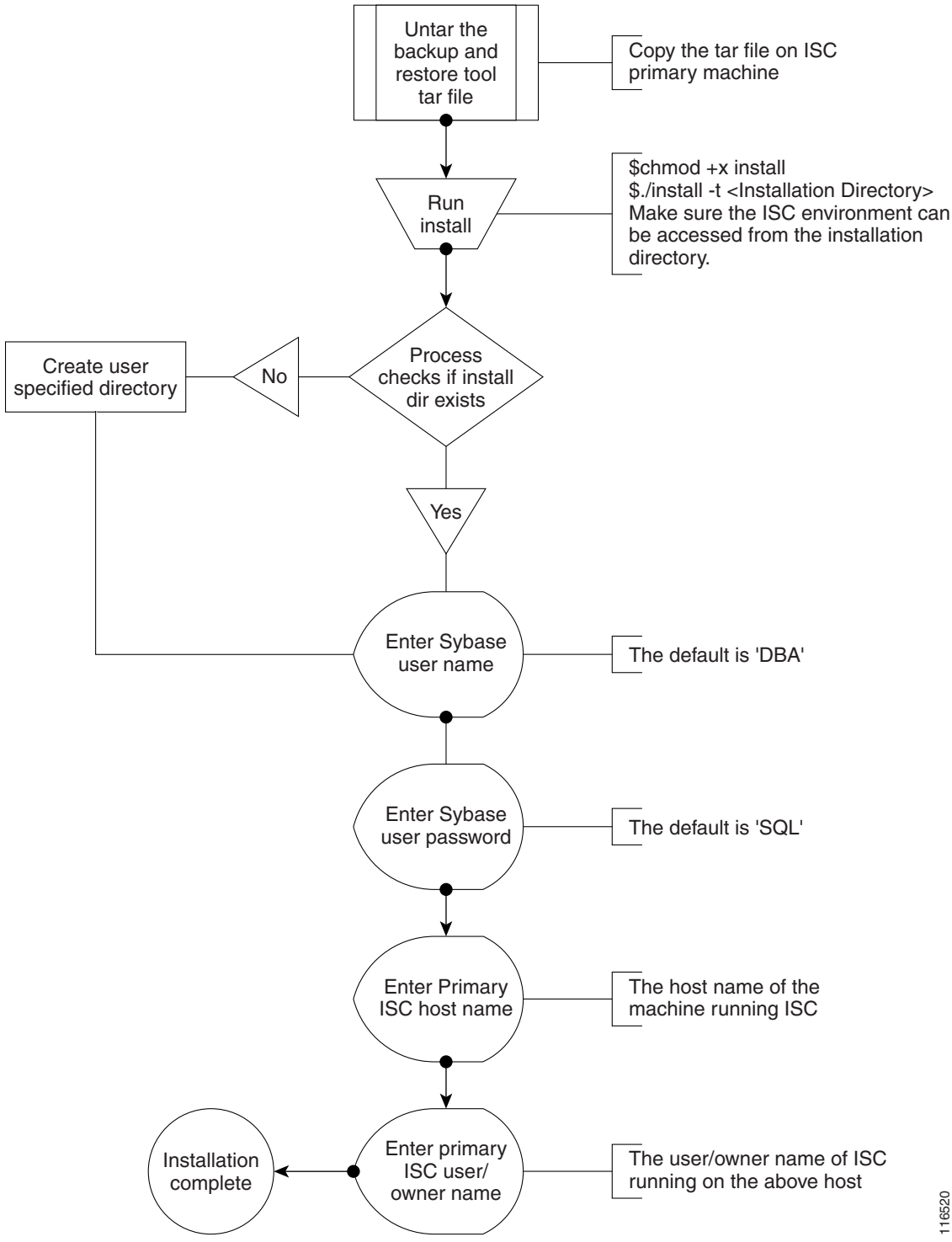
Step 4 Document the information for Step 1 to Step 3.

Step 5 Setup the proper bookkeeping for your backup and restore procedure.

Installing the Backup and Restore Tool

Figure C-2 shows the process flow for installing the backup and restore tool.

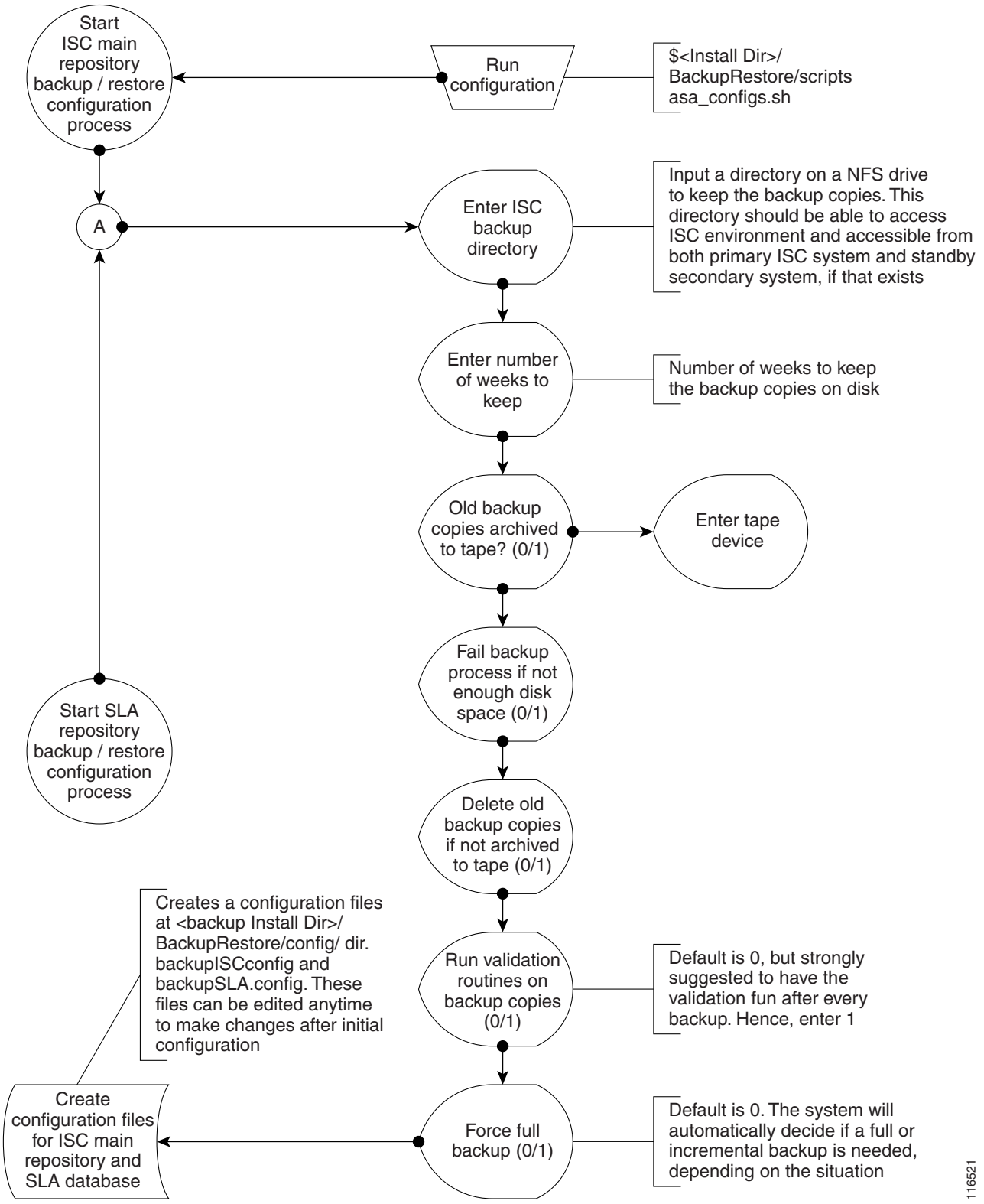
Figure C-2 Installing the Backup and Restore Tool



Configuring the Backup and Restore Process

Figure C-3 shows the one-time configuration process for the backup and restore.

Figure C-3 One-Time Configuration Process Flow



Understanding the Backup Process Flow

This section contains the following sections:

Preconditions

Before backing up your Sybase installation, you must observe the following preconditions:

1. The backup task must be carried out while the ISC database server is running.
2. The backup directory path that you specify during the configuration must be on an Network File System (NFS) drive.
3. The backup and restore tool must be installed on the ISC primary machine.
4. The backup and restore tasks must be carried out from the ISC primary machine.
5. You must not modify, rename, or move the backup directory structure after you configure it.

Functions

1. The backup follows a weekly scheme.
2. The backup week begins every Sunday.
3. A full backup occurs automatically the first time a backup is run for the backup week.
4. After the full backup, only incremental backups occur for the remainder of the week.
5. You can force a full backup during the week by changing the configuration setting to fullBackup=1 before running the backup script.
6. A new subdirectory is created for every backup week under the backup directory specified during the configuration. The name has the format mm-dd-yyyy, where the date is Sunday of the current backup week.
7. A new subdirectory is created for each full backup created during the backup week. All the associated incremental backup copies are also kept under this directory. If a full backup is forced during the same backup week, a new subdirectory is created for the full backup and after associated incremental backups.

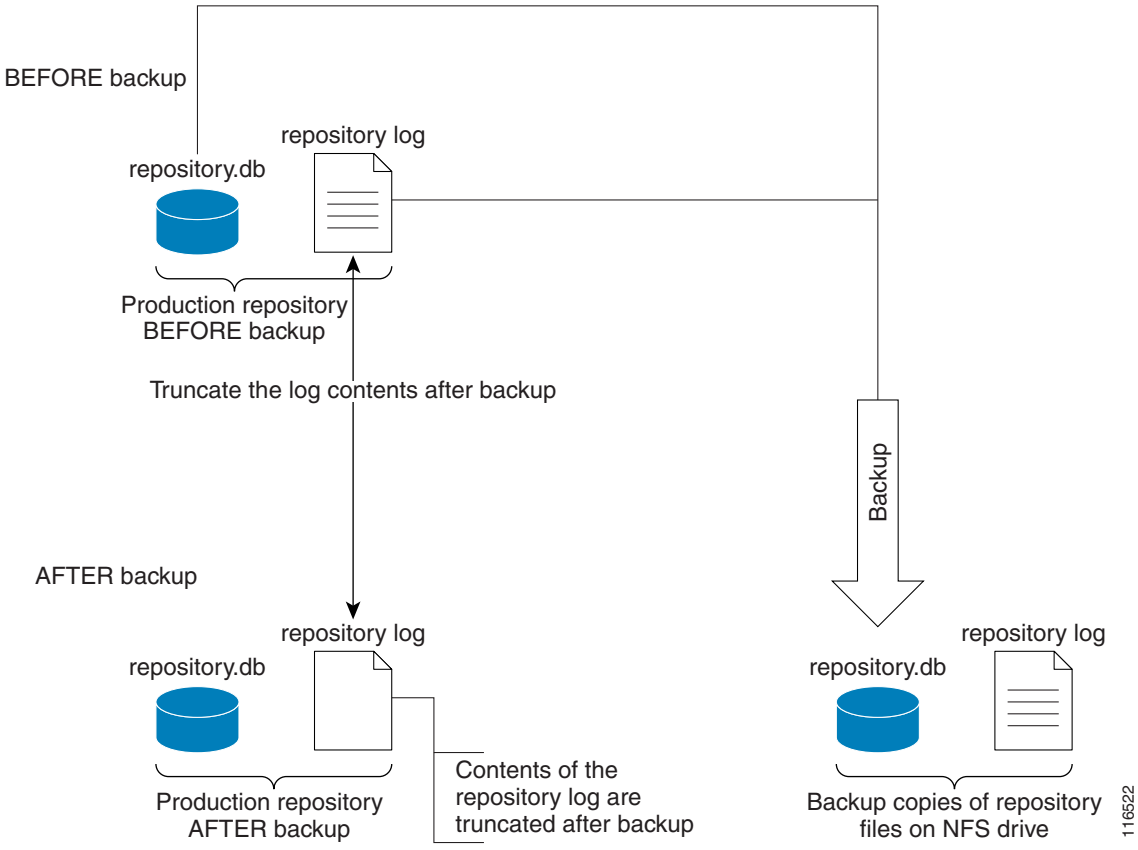
Note Do not modify, rename, delete, or move the directory structure created by the backup tool.

8. Both the database and the transaction log are backed up in a full backup.
9. Only the transaction log is backed up in an incremental backup.
10. The transaction log is truncated after each backup, either full or incremental. In other words, the transaction log is started fresh after each backup.
11. The name of the log file after backup will be of the form yymmddnn.log, where yy is the year, mm is the month, and dd is the day on which the backup is taken and nn is the serial number of this backup on a given day.

Full Backup Scheme

Figure C-4 shows a full backup scheme.

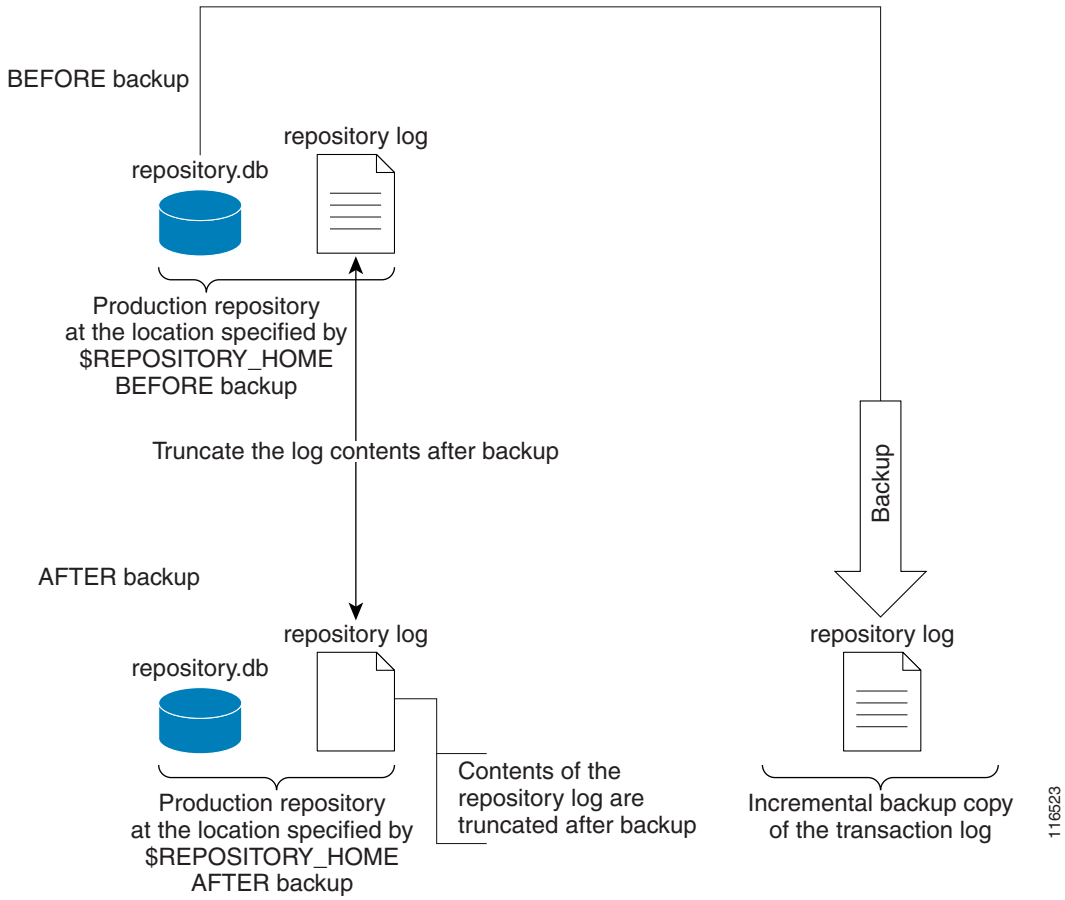
Figure C-4 Full Backup Scheme



Incremental Backup Scheme

Figure C-5 shows an incremental backup scheme.

Figure C-5 Incremental Backup Scheme



Typical Backup Directory Structure

To create a backup directory structure on an NFS drive, you can use the following procedure.

Assume the Backup Week is 03/14/2004 through 03/20/2004 and the Backup Dir as specified during configuration is /auto/iscBackups (NFS drive). The system creates two subdirectories under user specified backup dir, ISCMain and SLA.

1. First backup run on 03/15/2004 Monday, default full backup. Creates a sub dir /03-14-2004/full_01.dir under ISCMain and SLA directories.
2. Second backup run on the same date 03/15/2004, default incremental backup.
3. Third backup run on 03/17/2004, default incremental backup.
4. Fourth backup, Forced FULL backup (after changing configuration file setting, fullBackup to 1) on 03/18/2004. Creates a new sub dir /03-14-2004/full_02.dir under ISCMain and SLA directories.

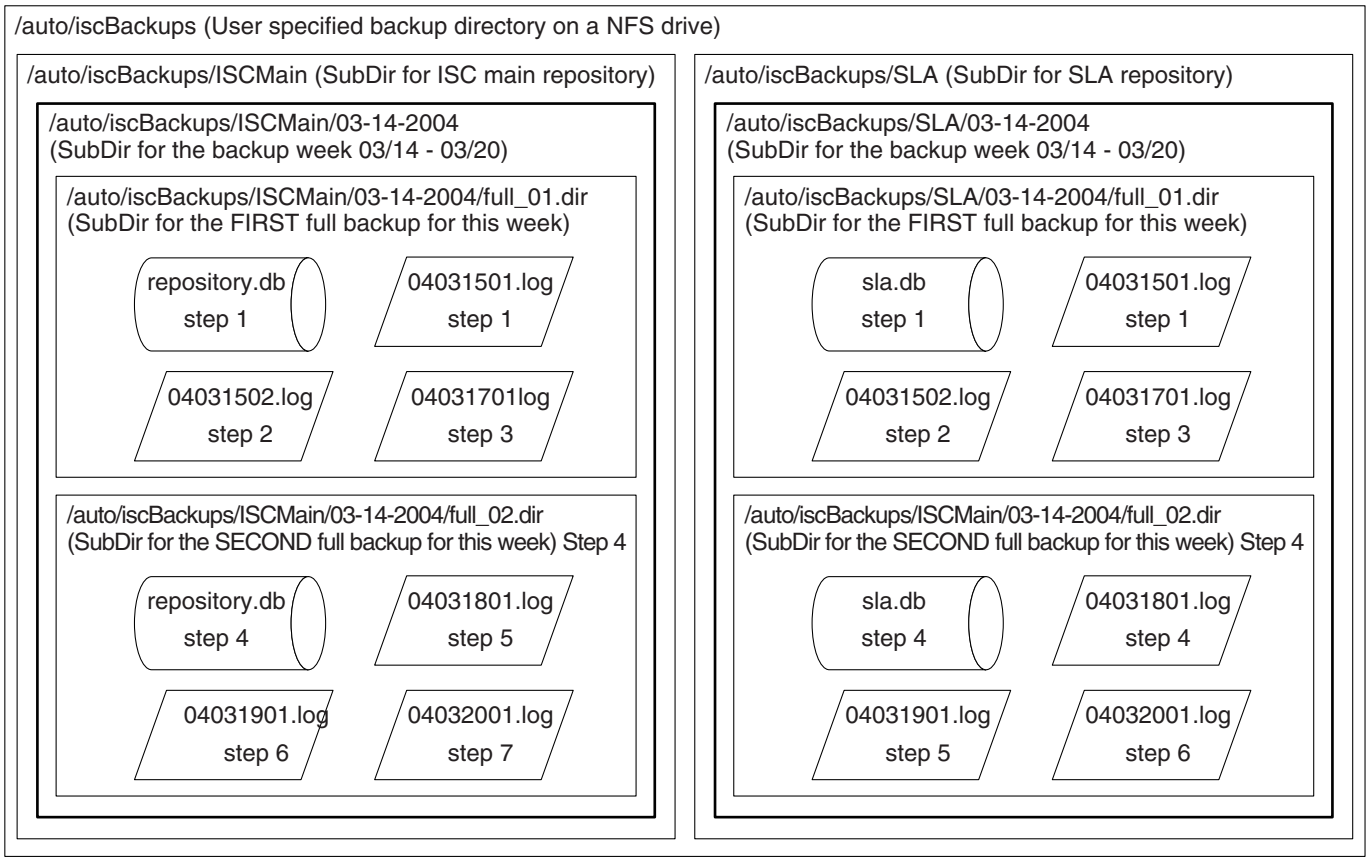
Note Configuration setting, full backup reset to 0.

5. Fifth backup, run on 03/19/2004, default incremental backup.
6. Sixth backup, run on 03/20/2004, default incremental backup.

Note Backup Week ended on 03/20/2004

Figure C-6 shows a typical backup directory structure on an NFS drive.

Figure C-6 Typical Backup Directory Structure



Understanding the Restore Process Flow

This section contains the following sections:

Preconditions

Before restoring your Sybase installation, you must observe the following preconditions:

1. The ISC database server should be stopped while running the Restore task.
2. The backup directory path specified during configuration should be on an NFS drive.
3. The backup and restore tool should have been installed on an ISC primary machine.
4. The backup and restore tasks should be carried out from an ISC primary machine.
5. The user running the restore script needs write permissions on the $REPOSITORY_HOME directory.
6. The repository files shall have write permission for the user running the restore.
7. Do not modify, rename, or move the backup directory structure after configured.
8. Do not rename, move, or delete the backup copies of the repository files.
9. Do not move, rename, or delete the production repository files under $REPOSITORY_HOME.

Functions

1. Restores the repository from existing full and incremental backup copies.
2. At least one full backup copy should be available to restore the repository.
3. The repository can be restored to a desired point in time using the available backup copies.
4. The restore process can recover the repository if there is a media failure on the database file, repository.db and/or sla.db.
5. The restore process cannot recover the repository if there is a media failure on the transaction log file. In this case, one of the following should be done to recover the database until the most recent checkpoint (partial recovery only):
   a. Using the available backup copies, the repository can be restored to a desired point in time. Use the ISC restore script to do this.
   b. Make an extra backup copy of the database file immediately. When the transaction log is gone, the only record of the changes between the last backup and the most recent checkpoint is in the database file. Delete or rename the transaction log file. Restart the database with the -f switch.

      For example, $SYBASE_HOME/bin/dbsrv8 $REPOSITORY_HOME/repository.db -f

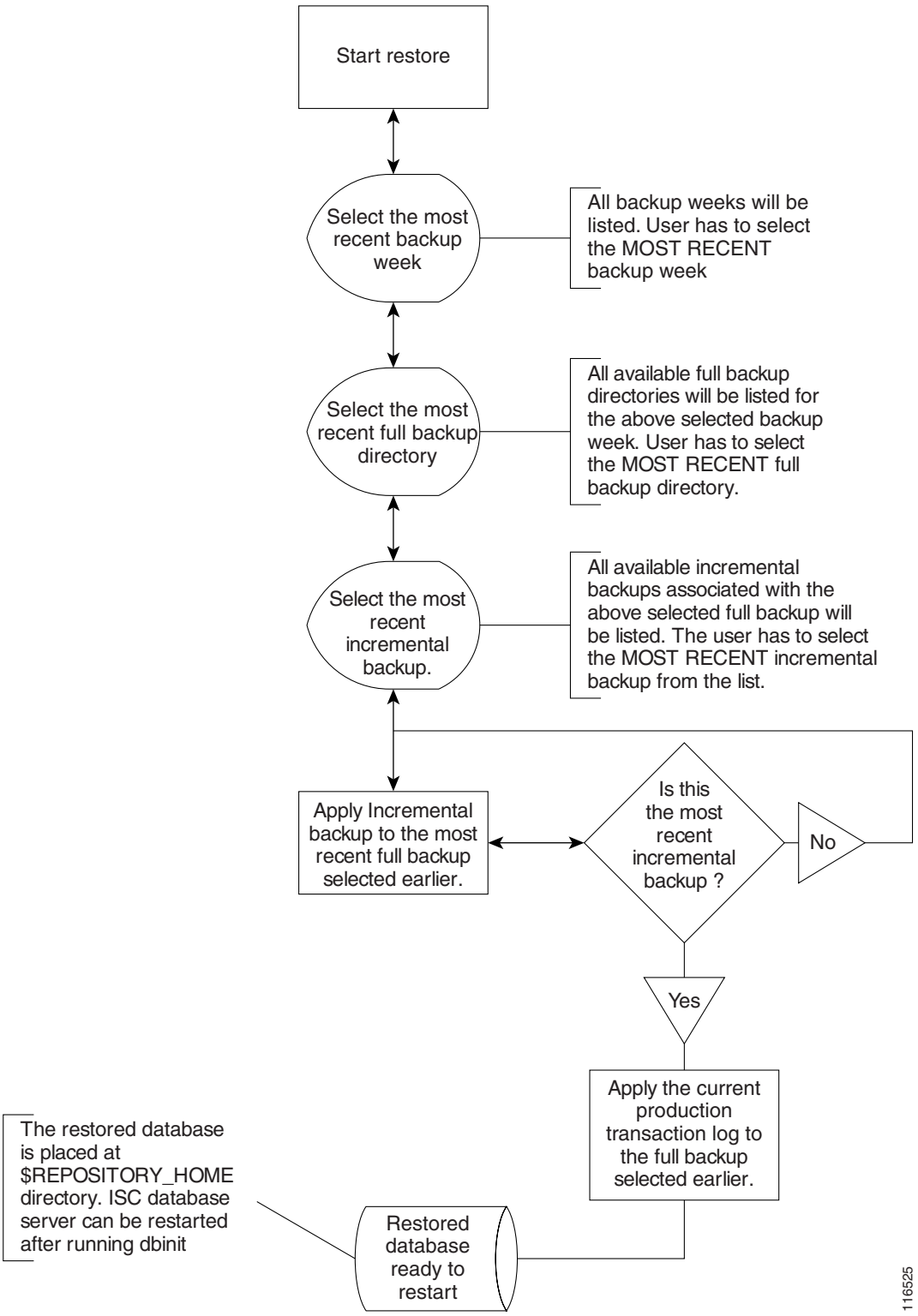
Note Please see Sybase ASA documentation for more information.

Note This option should be done by an authorized database administrator only.

Restore from Media Failure

Figure C-7 shows the process flow for how to restore from a media failure on the database file (.db).

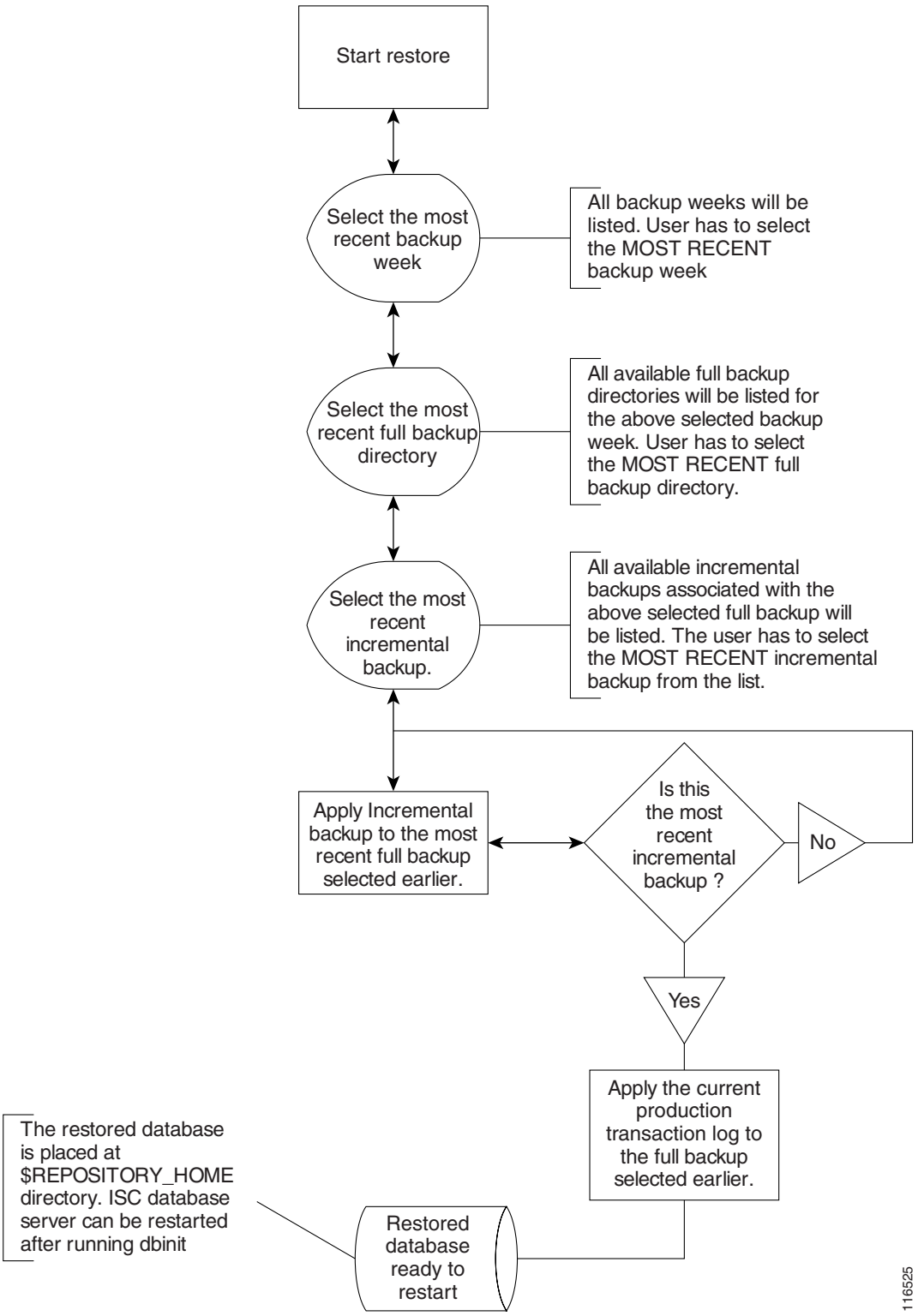
Figure C-7 Restore from Media Failure on the Database File (.db)



Restore to a Desired Point-in-Time

Figure C-8 shows the process flow for how to restore from a desired point-in-time.

Figure C-8 Restore the Database to a Desired Point-in-Time



Sybase Database Back Up and Restore

It is important to protect all ISC-related data by a well-defined backup and recovery plan. Data loss could occur due to the following reasons. The objective of ISC's backup and recovery plan is to greatly minimize the risk of data loss due to any of these reasons:

- Media failure
  - The disk drive holding database files and other data files becomes unusable.
  - The database files and other data files become corrupted due to hardware or software problems.
- System failure
  - A computer or operating system goes down while there are partially completed transactions.

The Sybase Backup and Restore tool provides a suite of scripts with several options to back up and restore your embedded Sybase database.

The backup script automatically detects whether a full back up is needed for this current backup week. If a full back up already exists for this current backup week, this script automatically takes an incremental back up. However, the user can force a full back up overriding this default behavior by changing the configuration setting.

Installing

Step 1 From the location http://www.cisco.com/cgi-bin/tablebuild.pl/isc, download the tar file iscBRToolASA.tar.gz and untar this file as follows:

mkdir -p $ISC_HOME/backup/Sybase

gzip -d < iscBRToolORA.tar.gz | tar xf -

Step 2 **chmod +x install**

Run install from where the tar file is unpacked. The install script takes command line arguments. Because **install** is also a system command, to differentiate between the system command and this installation script, run the script as follows:

```
./install -t <BACKUP_INSTALL_DIR>
```

For help in the install script, use **-h(elp)** as a command line argument.

Sample Install Prompts and User Responses

The following is a sample install session:

```
#./install -t /users/yourname/iscBRToolInstall
```

When the install script is invoked as above, if the specified target install directory already exists, the user is prompted as follows:

```
Looks like the installation already exists
Do you want to continue installation - it might remove the existing contents [y,n,?]
removing the previous installation
Enter the Sybase User Name: DBA (user input)
Enter the Sybase User Password: SQL (user input)
Enter the Primary ISC Host Name: yourname-u10 (user input, the host name of the machine
running ISC)
Enter Primary ISC user/owner name: yourname (user input, the user/owner name of ISC on the
above host)
```

Post Install Status

The installation creates an env.sh script under the <BACKUP_INSTALL_DIR>/BackupRestore/config directory.

Editing the env.sh script is NOT RECOMMENDED. This env.sh script sets the necessary environment variables needed to run ISC backup and restore scripts.

Functionality of Backup and Restore Tool

Step 1 One time configuration is needed before the first back up is carried out. Invoke the asa_configs.sh script to configure the backup and restore process. Execute this script from the directory **BACKUP_INSTALL_DIR/BackupRestore/scripts** as follows:

```
# ./asa_configs.sh
```

A sample configuration session is as follows, with the configuration prompt on the LHS and sample user response on the RHS of the prompt.

```
Starting backup Configuration for Main ISC database
DB server Name...yourname_yourname-u10

ISC Backup script invoked with the following parameters:
------------------------------------------------------------------------
Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0
------------------------------------------------------------------------
The ISC backup configuration file is nonexistent ... creating new file
Modifying ISC backup configuration settings ...
Enter new ISC backup directory path (a subdirectory ISC will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/yourname/iscBackup
Backup directory for ISC specified is "/users/yourname/iscBackup/ISCMain".
Is this correct? [y]  [y,n,?] y
Enter the number of weeks to keep [2] [?] 3
Number of weeks specified is "3".
Is this correct? [y]  [y,n,?] y
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
```

```
Is this correct? [y]  [y,n,?] y
Enter tape device [/dev/rmt/0] [?]
Tape device specified is "/dev/rmt/0".
Is this correct? [y]  [y,n,?] y
Fail backup if there is not enough space for a full backup (0=no,1=yes) [1] [?]
Fail backup if not enough space specified is "1".
Is this correct? [y]  [y,n,?] y
Delete old backups if not archived to tape (0=no, 1=yes) [0] [?]
Delete old backups specified is "0".
Is this correct? [y]  [y,n,?] y
Run validation routines on backup files (0=no, 1=yes) [0] [?] 1
Run validation routines specified is "1".
Is this correct? [y]  [y,n,?]
Force full backup (0=no, 1=yes) [0] [?] 0
Force full backup specified is "0".
Is this correct? [y]  [y,n,?] y
ISC Backup configuration settings have been modified ...
If you wish to verify the values or modify them again then re-run the script
asa_configs.sh again
The ISC backup engine is now exiting without backing up the database.You must run the
asa_backup.sh script for the backup to take place.
ISC Backup Configuration Successfully completed
ISC Backup Configuration script ending.
Starting backup Configuration for SLA database
DB server Name...rpokalor_rpokalor-u10
SLA Backup script invoked with the following parameters:
-------------------------------------------------------------------------------
Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0
-------------------------------------------------------------------------------
The SLA backup configuration file is nonexistent ... creating new file
Modifying SLA backup configuration settings ...
Enter new SLA backup directory path (a subdirectory SLA will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/yourname/iscBackup
Backup directory for SLA specified is "/users/yourname/iscBackup/SLA".
Is this correct? [y]  [y,n,?] y
Enter the number of weeks to keep [2] [?] 3
Number of weeks specified is "3".
s this correct? [y]  [y,n,?] y
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
Is this correct? [y]  [y,n,?] y
Enter tape device [/dev/rmt/0] [?]
Tape device specified is "/dev/rmt/0".
s this correct? [y]  [y,n,?] y
Fail backup if there is not enough space for a full backup (0=no,1=yes) [1] [?]
Fail backup if not enough space specified is "1".
Is this correct? [y]  [y,n,?] y
Delete old backups if not archived to tape (0=no, 1=yes) [0] [?]
Delete old backups specified is "0".
Is this correct? [y]  [y,n,?] y
Run validation routines on backup files (0=no, 1=yes) [0] [?]
Run validation routines specified is "0".
Is this correct? [y]  [y,n,?]
Force full backup (0=no, 1=yes) [0] [?]
Force full backup specified is "0".
Is this correct? [y]  [y,n,?]
```

```
LA Backup configuration settings have been modified ...
If you wish to verify the values or modify them again then re-run the script
asa_configs.sh again
The SLA backup engine is now exiting without backing up the database. You must run the
asa_backup.sh script for the backup to take place.
SLA Backup Configuration Successfully completed
SLA Backup Configuration script ending.
```

Post Configuration status

```
------------------------------------------------------------------------
The configuration creates backupISC.config and backupSLA.config files under
BACKUP_INSTALL_DIR/BackupRestore/config directory.

To modify the initial configuration settings, users can either re-run the asa_configs.sh
script or simply modify the contents of these .config files. For example, if the user
wants to suppress the validation of the database after each backup, the config file
setting validateDB property to 0 instead of 1. Similarly, if the user wants to force full
backup, set the property fullBackup=1.
```

How to Use the Backup Script

Step 1 Run the **BACUP_INSTALL_DIR/BackupRestore/script/asa_backup.sh** script to initiate the backup task.

a. The back up should be made while the ISC database server is running. There is no need to stop ISC to back up the database.

b. The backup directory path specified during the configuration process should ideally be on an NFS device.

   It is important to keep the backup copies on an external storage device to protect the backup copies if the main ISC system crashes.

c. Install the Backup and Restore tool and implement the periodic backup tasks from the primary ISC host machine. However, the backup task can be carried out from a secondary system, provided the following conditions are met:

   - The main ISC and SLA repository files should be placed on an NFS device accessible from the primary ISC host system and the secondary ISC host system.
   - The hardware and software configuration of the secondary system should be the same as the ISC primary host system.
   - The same version of ISC should be installed on both the primary and secondary systems.
   - The Backup and Restore tool should be installed on the secondary ISC system.

Step 2 Re-run the config script to make changes to the initial configuration settings, if needed.

Behavior of the Backup Process

Step 1 The backup scripts follow a weekly backup scheme; the backup week begins on Sunday.

Step 2 A full back up (both .db and .log files) is taken the first time the backup script is run during the backup week. Only incremental (only .log file) back ups are taken for the remainder of the current backup week.

Step 3 You can force a full back up instead of an automatic incremental back up by setting the fullBackup property to 1 in the backupISC.config and backupSLA.config file, before running the asa_backup.sh script.

Step 4 A new subdirectory (under the user-specified backup directory) is created for each backup week. This directory is named as MM-DD-YYYY, where MM is the month and DD is the date of the Sunday of this backup week and YYYY is the year.

Step 5 A subdirectory is created for each full back up and all the associated incremental back ups under the above weekly directory. Each time a forced full back up is made for the current backup week, there is a new subdirectory created to contain this full back up and its associated incremental back ups.The full backup directory for the current backup week is named full_0*n*.dir, where *n* is 1,2...9.

How to Restore the Database from the Back Up

The asa_restore.sh script supports the following types of database restore:

Step 1 A restore of a previous Full or incremental back up.

Step 2 A recovery from a media failure on the database file.

Note The main ISC repository consists of repository.db and repository.log files and the SLA consists of sla.db and sla.log files. ISC does not support placing the .db and.log files in different locations. Thus, if there is a media failure on the .db file, then the associated .log file also becomes unusable and thus this option might not be useful.

Step 3 Run BACKUP_INSTALL_DIR/BackupRestore/script/asa_restore.sh script to initiate the restore task after being sure to follow these pre-conditions:

a. The database server of ISC should not be running. Failing to stop the database server results in an inconsistent database after the restore.

b. Follow the instructions and prompts carefully while running the scripts.

c. Do not copy, move, or delete the repository files under $REPOSITORY_HOME.

Oracle Database Back Up and Restore

From the location http://www.cisco.com/cgi-bin/tablebuild.pl/isc, download the tar file iscBRToolORA.tar.gz and untar this file as follows:

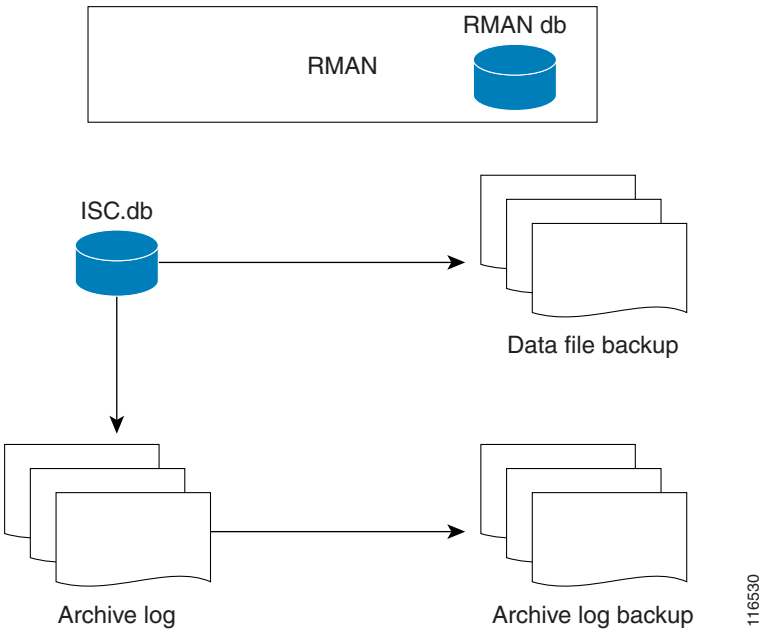
mkdir -p $ISC_HOME/backup/Oracle

gzip -d < iscBRToolORA.tar.gz | tar xf -

Oracle databases have a backup and restore Recovery Manager (RMAN) tool. To use this tool for online back up, the Oracle database must be in ARCHIVELOG mode, as explained in the "Turn On ARCHIVELOG Mode" section on page C-21. RMAN maintains the bookkeeping intelligence of backup and recovery files and backs up at the block level. Therefore, RMAN can significantly speed up back ups and reduce the server load by using incremental back ups.

Figure C-9 shows an Oracle Database Backup Diagram.

Figure C-9 Oracle Database Backup



RMAN for Oracle 9i is explained in the user guide, which is available as follows:

http://download-west.oracle.com/docs/cd/B10501_01/server.920/a96566/part3.htm

Note RMAN is convenient to use. However, it only provides a command line interface. And it still demands database analyst knowledge when recovery is needed.

Be sure that the backup data and RMAN catalog are located on a different disk from where the Oracle database (data files, redo logs, and control files) are located. Both can reside on the same ISC database server.

Oracle Enterprise manager (GUI) can be used to set up RMAN.

Alternatively, RMAN configuration is explained in the following areas that should be implemented sequentially:

Step 1 Turn On ARCHIVELOG Mode, page C-21

Step 2 Create RMAN Catalog Database, page C-21

Step 3 Create RMAN User, page C-21

Step 4 Create RMAN Catalog, page C-22

Step 5 Register the ISC Database with the RMAN Catalog, page C-22

Step 6 Modify ISC Database Initial Parameter File, page C-22

Step 7 Backup Database, page C-22

Step 8 Recover Database, page C-23

Turn On ARCHIVELOG Mode

Oracle allows manual back up when turning on ARCHIVELOG mode. This makes the database log all transactions into the redo logs. When one log is full, a task is started to copy the redo log to an archive log directory and at the same time the system starts logging to a different redo log. This requires the user to manage and purge archive logs that are no longer needed.

Step 1 First, turn on the archive log mode:

- **startup mount;**
- **alter database archivelog;**
- **archive log start;**

Check archive log using **archive log list**.

Step 2 Copy the data files regularly:

- turn the tablespace into **backup** mode
- show data files, as follows:

  SQL> **select file_name from dba_data_files;**

Step 3 To recover, enter the following:

SQL> **recover datafile** <*file_number_or name*>**;**

where <*file_number_or name*> is the file number, however a file name can be placed here. Recovery will be from /var/tmp/oracle/backup and the specified data file, where the recover command determined that the redo is needed for the recovery in the archive log.

Create RMAN Catalog Database

The catalog database holds the recovery catalogs. This database typically is set up on a different server from any database being registered in it. It also works if this database is set up on the same database server as the ISC database.

Use the Oracle utility **dbassist** to create a catalog database. (This is the same as ISC database creation, except you should name the RMAN global name **rman**, and you should name the SID **rman**.)

Create RMAN User

Creating an RMAN user is the same as creating an ISC user on an **rman** database. Name the RMAN user ID **rmanuser** and name the password **rmanpassword**. Make sure **rmanuser** has proper privileges. For example:

SQL> **grant connect, resource, recovery_catalog_owner to rmanuser;**

Create RMAN Catalog

Create a catalog from the RMAN command prompt:

RMAN> **connect catalog rmanuser/rmanpassword@rcat**

RMAN> **create catalog;**

Register the ISC Database with the RMAN Catalog

Set the ORACLE_SID environment variable = isc.

%**rman**

RMAN > **connect catalog rmanuser/rmanpassword@rman**

RMAN > **connect target sys/change_on_install**

RMAN > **register database;**

The default password for an Oracle sys account after Oracle installation is **change_on_install**. Replace this sys account password with the correct sys account password for the ISC database.

Modify ISC Database Initial Parameter File

To modify the ISC database initial parameter file, do the following:

Step 1 To ensure the database is in archive log mode, enter the following:

SQL> **alter system set log_archive_dest_1 = 'location=**</*var/tmp/oradata/arch*>**' SCOPE=BOTH;**

SQL> **alter system archive log start;**

where </*var/tmp/oradata/arch*> is the location of the archive destination.

Step 2 Restart the ISC database server with the ARCHIVELOG mode turned on, as follows:

startup mount

alter database archivelog;

alter database open

Step 3 Check the archive log mode, as follows:

SQL> **archive log list;**

Backup Database

To back up the database, do the following:

Step 1 Download the software for backup and restore from:

http://www.cisco.com/cgi-bin/tablebuild.pl/isc

Step 2 Before you run the backup scripts, make sure you update the file **$ISC_HOME/backup/Oracle/backupenv.properties**

Use a text editor to open this file and read the directions on how to update each property.

Step 3 To perform a full database back up, execute the following:

$ISC_HOME/backup/Oracle/oracle_backup.sh -f

Step 4 You can perform incremental back ups after a minimum of one full back up. To perform an incremental back up, execute the following:

$ISC_HOME/backup/Oracle/oracle_backup.sh -i

Note These backup scripts can be run as cron jobs or scheduled by the ISC task manager.

Backup Non-database Files

On the ISC server machine, to back up non-database related files, such as task logs or ISC system properties, execute the script: **non_db_backup.sh**.

Recover Database

To recover a database, do the following:

Step 1 Stop the ISC watchdog before recovering a database, as follows:

stopall

Step 2 To recover a database, you can execute the following from the location $ISC_HOME/backup/Oracle/oracle_recover.sh

%**oracle_recover.sh** [**"**<*date_time*>**"**]

The **"**<*date_time*>**"** is optional. The format is **"**mmm dd yyyy hh**:**mm**:**ss**"**, where the first mmm is the month and must be alphabetic characters with an initial capitalization, for example:

"Oct 09 2003 15:25:00"

If you do not specify <*date_time*>, the script does a full database recovery.

Note Note: Do not stop the Oracle Listener during restore.

Standby System for ISC (Secondary System)

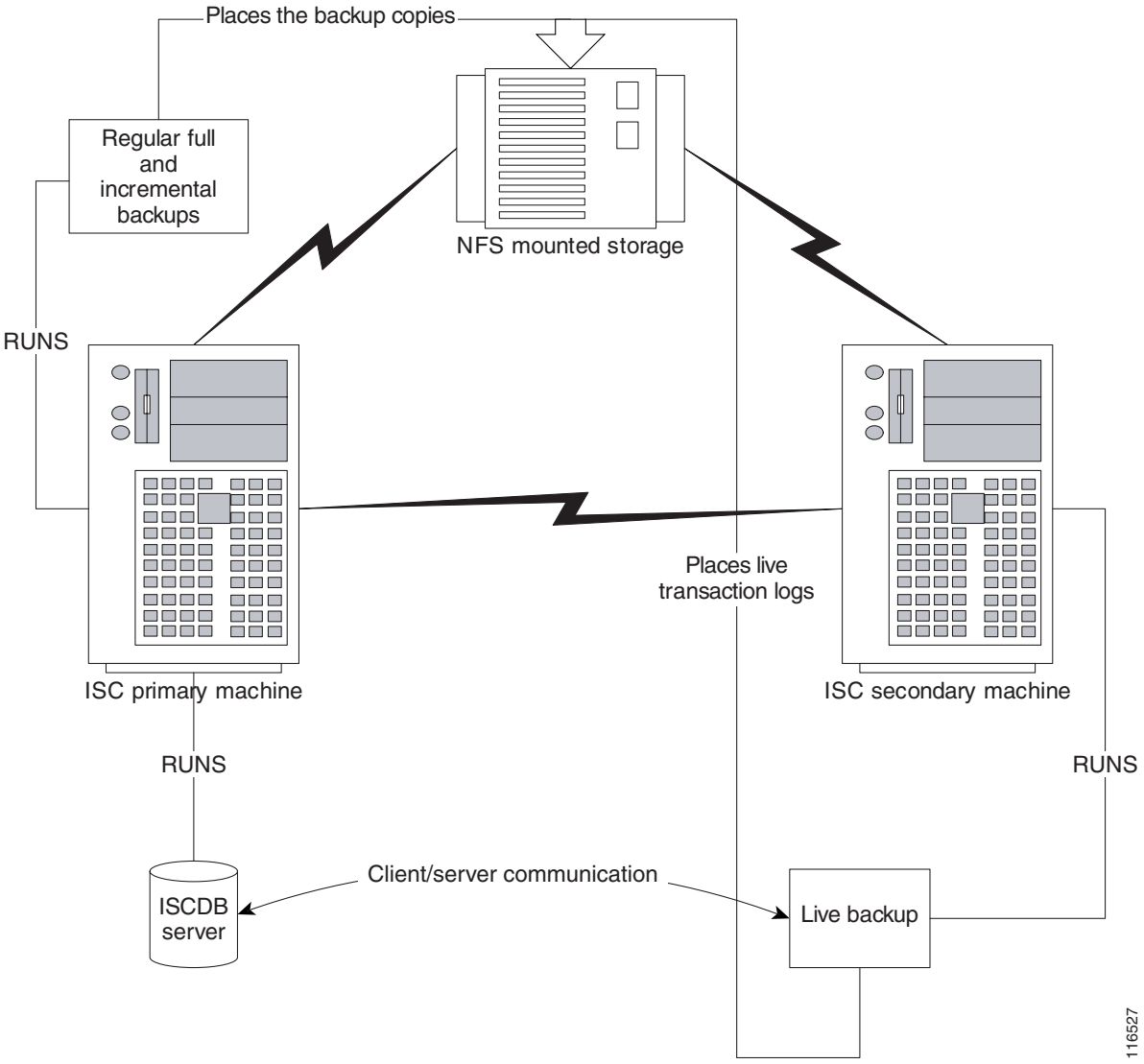
This section explains how to set up Sybase and Oracle standby systems for ISC.

The subsections are:

Sybase Standby System Process Overview

Figure C-10 shows a live backup scheme.

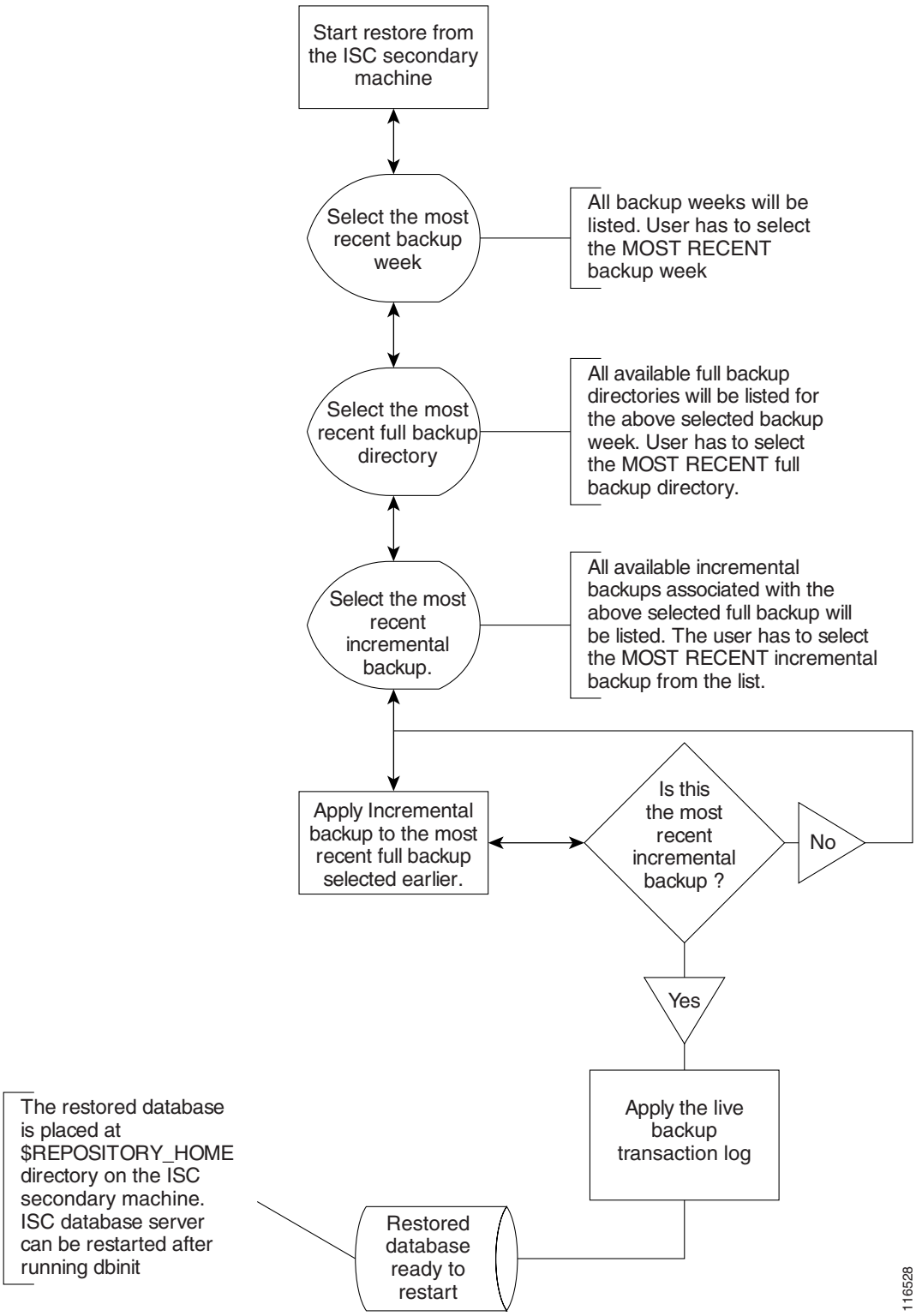
Figure C-10 Live Backup Scheme



Restore from Live Backup

Figure C-11 shows the process flow for how to restore from a live backup.

Figure C-11 Restore from Live Backup



Sybase Standby System Set Up

The explanation of setting up a Sybase standby system is explained as follows:

Running Live Back Up of ISC Databases

Run BACKUP_INSTALL_DIR/BackupRestore/scripts/asa_liveBackup.sh to start the live back up after being sure to follow these pre-conditions:

Step 1 Set up a standby ISC system.

Step 2 The standby system should be similar to the primary ISC host system in hardware and software configurations.

Step 3 The ISC primary and standby systems should be on the same LAN.

Step 4 ISC software should be installed on the secondary system and the version of ISC on the primary and standby systems should be the same.

Step 5 The backup and restore tool should be installed on the primary and the secondary systems.

Step 6 The live back up should be started from the secondary system only, you should not run the live back up from ISC primary system.

Step 7 The storage device where the regular backup copies are placed should be accessible from the standby system.

Step 8 You *must* run BACKUP_INSTALL_DIR/BackupRestore/scripts/asa_liveBackupConfig.sh to configure the live back up on the standby system before starting the live back up for the first time.

Step 9 The ISC database server must be running on the primary ISC host before starting the live back up on the standby system.

Step 10 The live back up stops when the ISC database server is stopped and should be restarted after restarting ISC.

Step 11 At least one full back up must be taken before starting the live back up.

Step 12 Regular periodic full/incremental back ups should be taken even if the live back up is running on the secondary system.

Step 13 There should not be more than one live back up running simultaneously.

How to Restore the Database from the Live Back Up

When the primary ISC host fails, the standby system restores the database from the latest available full back up, the latest incremental back up, and the live back up.

Run the BACUP_INSTALL_DIR/BackupRestore/script/asa_restoreFromLiveBackup.sh script on the standby system to restore the database after being sure to follow these pre-conditions:

Step 1 At least one full backup copy should be available to restore the database.

Step 2 If more than one backup copy is available, use only the latest full back up and the latest associated incremental back up.

Step 3 Run the restore from the standby machine.

Oracle Standby System Set Up

For Oracle 9i Data Guard instructions, see:

http://download-west.oracle.com/docs/cd/B10501_01/server.920/a96653/preface.htm#971610

Note ISC only supports physical standby, not logical standby.

Restart ISC

When the standby database is activated, use the following commands to point ISC to the new database server:

stopall -y

update $ISC_HOME/etc/install.cfg and replace <*old_db_server*> **with** <*new_db_server*>.

execute applycfg.sh

initdb.sh

startwd

where:

<*old_db_server*> is the name of the old database server

<*new_db_server*> is the name of the new database server.

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 If you are using DNS, use **nslookup** <*machine name*> to check if it is working properly.

Step 3 If it is not working properly, you need a system administrator to fix the DNS entry.

Step 4 If you are not using DNS, be sure there is an entry for your machine in the **hosts** file in the **/etc** directory.

Multiple ISC Instances with the Same TIBCO Rendezvous Port

Symptom

You might not see any error messages, 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 3.2 will be installed in /var/isc-3.2
>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 *Cisco IP Solution Center Installation Guide* for the disk drive space recommendation:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_2/install/index.htm

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 created or found, it usually means the location used to write the temporary 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. 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 this command:

```
./install.sh /opt/isc32 master
```

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`

A

B

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W