Cisco Prime Provisioning 6.5 Administration Guide

July 23, 2013

Cisco Systems, Inc.
www.cisco.com

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

Text Part Number: OL-29802-01

Cisco Prime Provisioning 6.5 Administration Guide

Preface

This preface contains the following sections:

Objective

The *Cisco Prime Provisioning 6.5 Administration Guide* contains detailed explanations of Cisco Prime Provisioning services and components across all applications.

Note You are able to use Prime Provisioning as a standalone product or as part of the Cisco Prime for IP Next Generation Network (IP NGN) Suite. When installed as part of the suite, you are able to launch Prime Provisioning from Prime Central portal. For more information about Prime Central, see the documentation for Cisco Prime Central 1.1.

Audience

This guide is designed for administrators who are responsible for provisioning Prime Provisioning services for their customers.

Organization

This guide is organized as follows:

- Chapter 1, “Manage Active Users and User Account,” explains how to communicate with active users and manage user account.
- Chapter 2, “Manage Control Center,” describes how to set up the Prime Provisioning services.
- Chapter 3, “Manage Security” describes how to create users, user groups, user roles, and object groups and how privileges are assigned to these entities.
- Chapter 4, “Backup and Restore of Prime Provisioning Repository” explains the steps that you can follow after installing Prime Provisioning. It also describes the objectives of backup and restore and a standby system and how to set them up for Sybase and for Oracle.
- Chapter 5, “Prime Provisioning Runtime Configuration Information” specifies the default ports and command-line interfaces (CLIs) used by Prime Provisioning.
- Chapter 6, “WatchDog Commands” provide supplementary information.

Related Documentation

The entire documentation set for Cisco Prime Provisioning, can be accessed at:

http://www.cisco.com/en/US/products/ps12199/tsd_products_support_series_home.html

An overview of the Cisco Prime Provisioning product is available at:

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

The following documents comprise the Cisco Prime Provisioning 6.5 documentation set:

General Documentation (in suggested reading order)

- *Cisco Prime Provisioning 6.5 Documentation Overview*
- *Cisco Prime Provisioning 6.5 Release Notes*
- *Cisco Prime Provisioning 6.5 Installation Guide*
- *Cisco Prime Provisioning 6.5 Supported Devices*
- *Cisco Prime Provisioning 6.5 User Guide*
- *Cisco Prime Provisioning 6.5 Administration Guide*
- *Cisco Prime Provisioning 6.5 Open Source*

API Documentation

- *Cisco Prime Provisioning 6.5 API Programmer Guide*
- *Cisco Prime Provisioning 6.5 API Programmer Reference*

Note All documents areupgraded over time and these documents are available at the specified URLs.

Other Cisco Prime Product Documentation

You can alse refer the documentation for the following Cisco Prime products:

- *Cisco Prime Central*

- *Cisco Prime Network*
- *Cisco Prime Optical*
- *Cisco Prime Performance Manager*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Manage Active Users and User Account

This chapter explains how to communicate with active users and manage the user in Cisco Prime Provisioning.

This chapter contains the following sections:

Active Users

Step 1 Choose **Administration> Active Users > Active Users.**

The Active Users window appears that shows the currently logged users.

Step 2 To disconnect the active user, you should have the privileges of **SysAdmin** or **UserAdmin** and need to perform the below steps:

a. Check the checkbox of the active user.

b. To disconnect the active user, click **Disconnect**.

Caution As soon as you disconnect the active user, their current login sessions are terminated and their unsaved work is lost.

Step 3 To exit from Active Users window, choose another feature from the main product tabs.

User Account

Step 1 Choose **Administration> Account > User Account**.

The User Account window appears that shows all the users.

Step 2 To change the password, permissions, personal information, and user preferences, click **Edit** .

Step 3 Click **Save** to save the changes or click **Cancel**.

Manage Control Center

This chapter explains how to view and change the properties in the Dynamic Component Properties Library (DCPL); how to view status information about a host, servers, the WatchDog, and logs; how to define collection zones; and how to install license keys.

This chapter contains the following sections:

Hosts

Hosts allows you to manage the various servers. To access Hosts:

Choose **Administration > Control Center > Hosts**.

The Control Center Hosts window appears.

Note Only the **Logs** button is enabled by default when there is no host selected. When any host is selected by using the check box, the Logs button is disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

- Details, page 2-1—Available only when the host system is chosen.
- Config, page 2-2—Available only when the host system is chosen.
- Servers, page 2-5—Available only when the host system is chosen.
- Watchdog, page 2-6—Available only when the host system is chosen.
- Logs, page 2-7—Available only when no host system selection is made.

Details

For details about a chosen host, follow these steps:

Step 1 Choose a host by checking the check box to the left of the hostname and then click the **Details** button.

. The Host Details window appears. This shows the details about the chosen host.

Step 2 Click **OK** to return to the **Control Center Hosts** window.

Config

To navigate to the **Properties** pane of the Host Configuration window, perform the following:

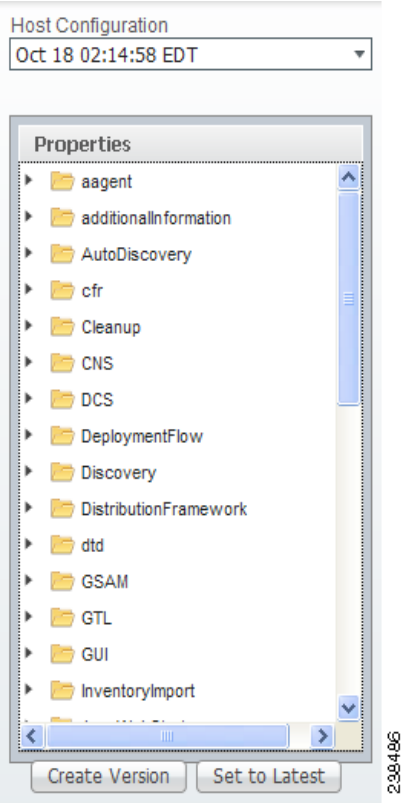
1. In the Control Center Hosts window, check the check box of the hostname.
2. Click **Config**.

You can view or modify Dynamic Component Properties Library (DCPL) properties in the properties pane by following these steps

Step 1 Select a property from the Properties pane as shown in Figure 2-1 to view its explanations, defaults, and ranges/rules.

Note Properties pane contain the details of all the properties in a folder format. If you do not know the property name, you can use a key word and do a Find.

Figure 2-1 Properties



Step 2 Click on the arrow of the property folder.

Note Expand the subfolders till you reach the specific property.

Step 3 Click on the property to view the details and instructions on how to change the value, as shown in Figure 2-2.

Figure 2-2 Properties Detail Example

Step 4 For each property that can be modified, you can modify the value and click **Set Property**. If when making your modifications, you want to return to the previous settings, click **Reset Property**.

Step 5 After making all the changes you choose in each of the specific properties, you can click **Create Version** to create a new version of these properties. This feature gives you the option of saving multiple property sets for future use.

Step 6 To view the values of previous versions of property sets, click the drop-down list on top of the window and select any version you choose.

Step 7 When you click **Set to Latest** after selecting a version in Step 6, this version is dated as the most current.

Step 8 To return, click to the navigation path you want to use next.

From this release, you are able to perform the below mentioned additional tasks using the DCPL properties:

- Configuring Prime Network(s) in Prime Provisioning, page 2-4
- Subscribing or Unsubscribing to Prime Central Device Commission and Decommission Notification, page 2-5

Note To perform the above tasks, certificates has to be imported from Prime Network. For more information about this, refer to the section **Integrating with Prime Network for Device Import** in *Cisco Prime Provisioning 6.5 Installation Guide.*

Configuring Prime Network(s) in Prime Provisioning

In the **Host Configuration** screen, you can configure Prime Network in Prime Provisioning by choosing **Properties > Inventory Import > Prime Network** and modifying the below values:

- **enablePrompts** - Prompts are present on the server so that the Prime Provisioning can execute the web services at the backend.
- **Gateway** - Multiple gateways can be configured by separating the values with a comma. The order in which the Prime Networks are configured has an impact on the inventory import.

For example, if there is a device D1 available in two instances of Prime Network configured in the order PN1 and PN2, inventory import will always import the device from the first instance PN1 and will ignore the other.

- **loginPrompts** - General configuration for the login prompts on the server.
- **logLevel** - Log level for the inventory import log.
- **Password and UserName**
  - Prime Provisioning can interface with Prime Network in both the installation modes: Standalone mode and Suite mode integrated with Prime Central.
  - When Multiple Prime Networks are configured either in Standalone or Suite mode, the login credentials provided should be able to access all the instances of Prime Network.

For example, consider a user *admin* is created in Prime Central. In Suite mode, for all the features to work as expected, *admin* should have access to Prime Provisioning with appropriate role and access to Prime Network as **Administrator**. The user should be assigned with the scope of all the Network elements in Prime Network.

In case of Standalone mode, the user should have access to Prime Network as **Administrator** and should be assigned with the scope of all the Network elements in Prime Network. For more information about Prime Network configuration, refer to *Prime Network User Guide*.

- Password provided here is encrypted both at the screen level and also in the database. Be sure to configure a valid value for the Inventory Import, Device Commission and Device Decommission features to function as expected

Subscribing or Unsubscribing to Prime Central Device Commission and Decommission Notification

When Prime Provisioning is either installed in suite mode or upgraded to suite mode, it subscribes to Prime Central device commission and decommission notifications by default. Once subscribed, Prime Central forwards the device commission and decommission notifications received from the other Domain Managers to Prime Provisioning.

To subscribe or unsubscribe to Prime Central device commission and decommission notifications, choose **InventoryImport > PrimeCentral > enableNotification** from the **Properties** pane and proceed as mentioned below**.**

- To receive notifications, set the **property** to **true**.
- To stop receiving notifications, set the **property** to **false**.

To view the notification logs when there is no host selected in the Host window, choose **Logs > PCNotification**. The information related to creation and deletion of a device are captured here.

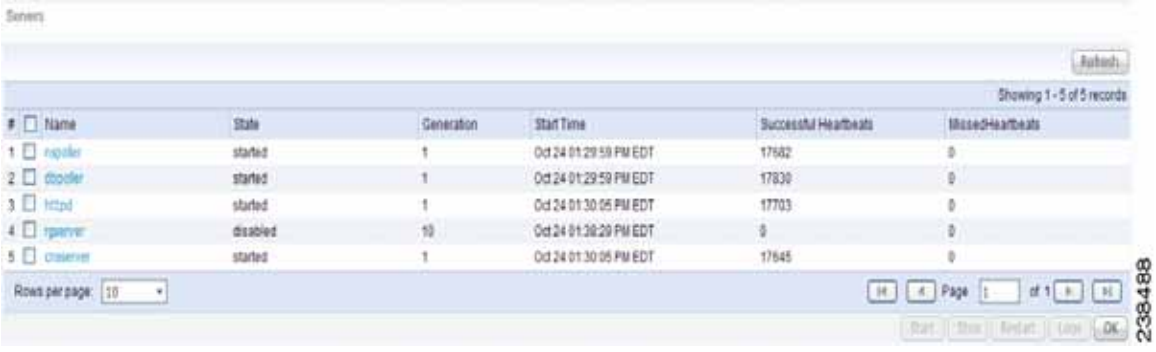
Servers

To view the status information about the servers, follow these steps:

Step 1 From the Control Center Hosts window, check a check box next to a hostname for which you want to know the server statistics and then click the **Servers** button.

A window as shown in Figure 2-3, appears.

Figure 2-3 Servers



Step 2 Check any one check box next to the server you want to address and you have access to **Start**, **Stop**, **Restart**, and **Logs**. When you click on a specific server name or the Logs button, you get a list of server logs. If you then click on the log name for which you want details, the log viewer appears. You can filter this information in the log viewer. After you complete the task of your choice, you return to Figure 2-3.

Step 3 You can click a different server and click the button for the process of your choice. Or you can unclick the server choice and click **OK**.

Step 4 After you click **OK** in Figure 2-3, you return to the Control Center Hosts window.

Watchdog

To view the log information about WatchDog, follow these steps:

Step 1 From the Control Center Hosts window, check a check box next to a hostname for which you want to know the WatchDog logs and then click the **Watchdog** button.

A window as shown in Figure 2-4, "WatchDog Logs," appears.

Figure 2-4 WatchDog Logs

Step 2 Click on a specific WatchDog log name in the **Name** column to get the contents of that log. You can filter the information in this log. Click **OK** to return to Figure 2-4.

Step 3 You can repeat the process in Step 2 or click **OK** to return to the Control Center Hosts window.

Logs

To view install and uninstall logs for the Master server, follow these steps:

Step 1 From the Control Center Hosts window, be sure that no check boxes are checked.

Step 2 Click the **Logs** drop-down list and select **Install** or **Uninstall**.

The window that appears is the log of installations or uninstallations, dependent on your selection in Step 2.

Step 3 Click the link in the **Name** column to view the detailed log information.

Step 4 Click **OK** to return to the window.

Step 5 Click **OK** again to return to the Control Center Hosts window.

Licensing

Licensing is where you install license keys, which is the only way to access services and APIs. The full version license key that is delivered, provides unlimited activation and unlimited VPNs and optional set of TEM activation license keys separately. To access Licensing:

Choose **Administration > Control Center > Licensing**.

To install license keys, follow these steps:

Step 1 Choose **Administration > Control Center > Licensing**, and a window as shown in Figure 2-5, appears.

Figure 2-5 Choose Administration > Control Center > Licensing

Step 2 From the **Installed Licenses** table, click the **Install** button, as shown in Figure 2-5. The Installed Licenses table explains the current statistics. The columns of information tell the **Type** of license keys you have installed (which can include ACTIVATION, API-L2VPN, API-L3MPLS, L2VPN, L3MPLS/VPN, TE, TE/BRG, TE/RG, VPLS, VPN); the **Size**, which is valid for the **ACTIVATION** (licensed maximum global count of services), **TE** (number of TE-enabled nodes), or the **VPN** (maximum number of VPNs licensed); the **Usage**, which gives the number currently used for the rows; and the **Date Updated**, which reflects the refresh of the license usage (on an hourly basis, by default).

Note When you purchase a full version license key all features except TE, TE/BRG, TE/RG are activated with unlimited activation and unlimited VPNs.

Note The TE licenses can be purchased separately based on the number of nodes/devices available in the inventory. The total number of devices and corresponding device type, IOS/XR version, and platform info is reported by utilizing the reporting mechanism available with the product. Refer to Reporting Mechanism, page 2-8 for the details of executing a reporting mechanism. When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses. All of these licenses *must* be installed to have access to all the Cisco Prime Provisioning TEM features, including Planning Tools for protection planning (backup tunnels). The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM (you purchase licenses and upgrade licenses based on a range of nodes); the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function

Step 3 In the resulting Enter License Key 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 o f the Installed License table, as shown in Figure 2-5.

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

Note Upgrade licenses are only available for TE and when you receive multiple Right to Use documents to upgrade TE, be sure to enter the licenses in correct order. For example if you are upgrading from 100 to 200 TE node counts there are two step to upgrade, enter the license to upgrade to 100 to 150 and then enter license key to upgrade from 150 to 200

Reporting Mechanism

Reporting mechanism is a tool used to export the devices available in the inventory. The report includes device name, device type, platform, and IOS/IOS XR version.

To execute the reporting tool, follow these steps:

Step 1 Source the environment from provisioning home directory.

./prime.sh shell

Step 2 Make sure, necessary execute permissions are available for the following files:

```
<PRIMEF _HOME>/resources/nbi/scripts/getDevices
<PRIMEF _HOME>/resources/nbi/scripts/queries/DevicesQuery
<PRIMEF _HOME>/resources/nbi/scripts/util/Login
<PRIMEF _HOME>/resources/nbi/scripts/util/checkForErrors
```

Step 3 Execute the following script from <PRIMEF_HOME>/resources/nbi/scripts

./getDevices

Step 4 The resulting report can be found in <PRIMEF _HOME>/resources/nbi/scripts/Devices_Info.csv.

Manage Security

This chapter describes how you can create, edit, and delete users, user groups, user roles, and object groups and how privileges are assigned to these entities.

The security features are only accessible to the user **admin** or users with the following roles:

- **SysAdminRole**—Gives access to all the Prime Provisioning tools. This is similar to “root” in a UNIX system.
- **UserAdminRole**—Gives access to only the user management tools.

Choose **Administration** > **Security** to access the user management tools.

This chapter contains the following sections:

Users

Choose **Administration > Security > Users** and the Users window appears.

The explanations of the buttons are given as follows:

- Details, page 3-2—View a User Detail Report
- Create, page 3-2—Create a new user
- Copy, page 3-4—Make a copy of an existing user and make changes to create a new user
- Edit, page 3-4—Edit selected user
- Delete, page 3-5—Delete selected user(s).

Details

When you click the **Details** button, located at the bottom of the Users window, you receive the following columns of information: **User ID**; **User Group** that a user belongs to; **Role** that a user occupies; **Resource Privilege** permissions that a user has for each role occupied; **Object Group** that a user role is associated with; **Customer View** that a user's role is limited to; **Provider View** that a user's role is limited to.

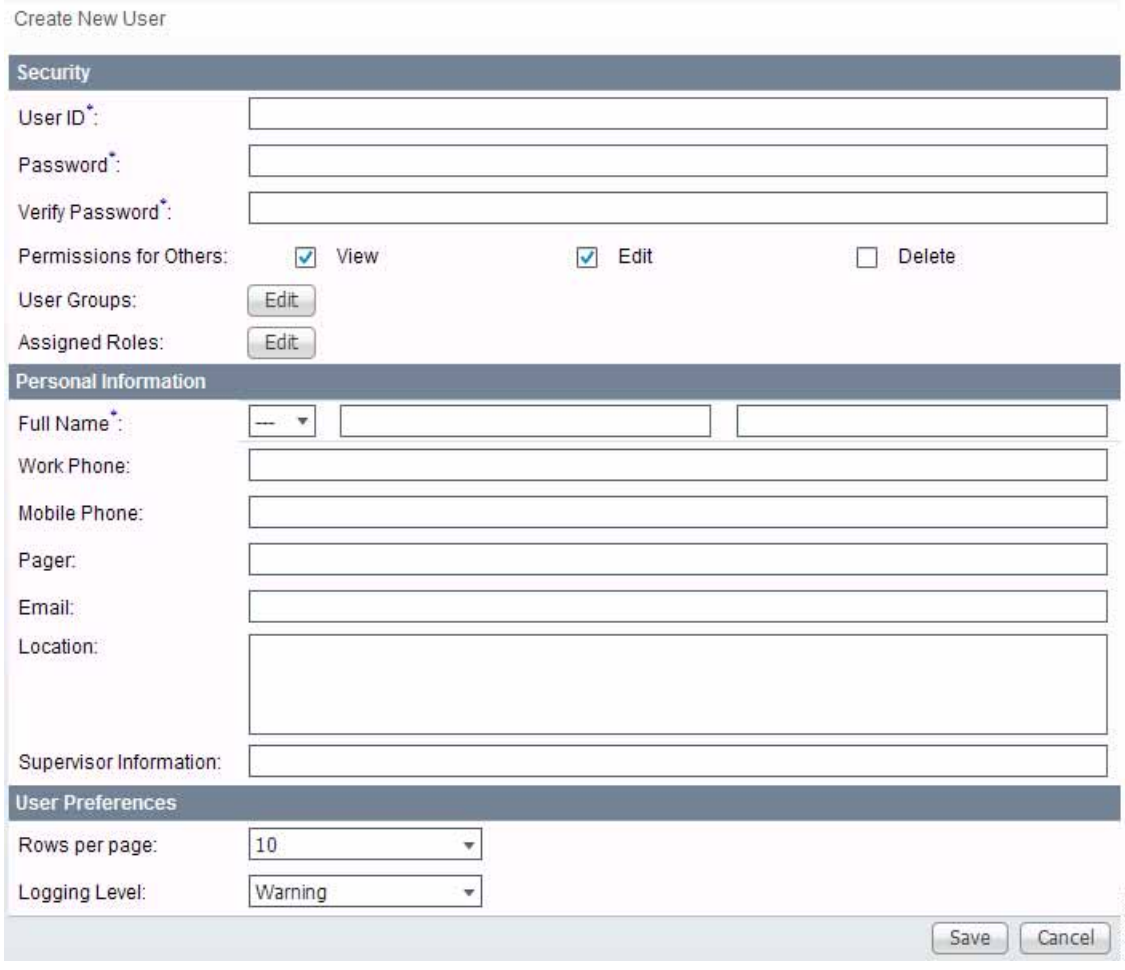
Create

When you click the **Create** button, located at the bottom of the Users window, a user with the required privileges can create a new user. To create a new user, follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Click the **Create** button and the window shown in Figure 3-1, appears.

Figure 3-1 Create/Copy/Edit Users Window



Step 3 Enter information in the **Security** section, as follows:

- **User ID** (required)—Enter a User ID for this new user.

- **Password** (required)—New password to replace any existing password:
  - Prime Provisioning requires a non-blank password.
  - Prime Provisioning passwords must be a minimum of five characters and no practical maximum length.
  - Prime Provisioning does not employ any password restrictions or complexity rules; use good judgment in determining passwords.
  - Prime Provisioning passwords are encrypted when stored in the repository.
  - Prime Provisioning passwords do not expire.
  - Prime Provisioning monitors inactivity and auto-logoff per the settings defined in the Dynamic Component Properties Library (DCPL) properties for **repository/rbac.**
- **Verify Password** (required)—Confirm by re-entering the selected password.
- **Permission for Others**—Check each of the associated check boxes for the permission that the user (to be created) wants to give to other users. The user who creates the object is the owner of the objects. The creator can allow or disallow other users to **View**, **Edit**, and/or **Delete** the objects owned by the creator by defining permissions. This is the last line of defense. For UserA to delete an object X that UserB created, UserA must first have Delete permission for object X, then UserB's settings for permissions for others is checked, to finally decide whether UserA can delete object X. Permission for others can be enabled or disabled by setting the property: **repository.rbac.checkCreatorPermissionEnabled**. After you make a change, you must restart the WatchDog by entering **stopwd** followed by **startwd**.
- **User Groups**—Click **Edit** and you receive a list of the groups. Add this user to a user group(s). The user inherits all the roles assigned to the group(s). You can filter this list. From the selected groups, check the check box next to each group to which you want to add this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

  A user's group membership can also be changed in the group editor (see the "Edit" section on page 3-6).
- **Assigned Roles**—Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role to which you want to assign this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

  The user inherits all the privileges from the groups in which it participates and from the roles assigned to it. That is, the permissions received by the user is an OR result of the permissions in each role.

Step 4 Enter information in the **Personal Information** section, as follows:

- **Full Name** (required)—Click the drop-down list and select a title; enter the first name; and then enter the last name.
- **Work Phone** (optional)—Enter the work phone number.
- **Mobile Phone** (optional)—Enter the **user's cell phone or mobile phone number.**
- **Pager** (optional)—Enter the user's pager number.
- **Email** (optional)—Enter the user's e-mail address.
- **Location** (optional)—Enter the user's location.
- **Supervisor Information** (optional)—Enter information about the supervisor.

Step 5 Enter information in the User Preferences section, as follows:

- **Language** (optional)—Click the drop-down list to select a language (at this time only English is supported).

- **Rows per page** (optional)—This defines the number of rows per page for object listing. The default is **10**. The choices are: **5**, **10**, **20**, **30**, **40**, **50**, **100**, **500**, **1000**, and **2500**.
- **Logging Level** (optional)—The default is **Warning**. The choices are: **Off**, **Severe**, **Warning**, **Config**, **Info**, **Fine**, **Finer**, **Finest**, and **All** (see all levels of logs). This defines the logging level for viewing logging events. The list progresses from the least number of messages to the most number of messages.
- **Initial Screen** (optional)—The default is **Home**. The choices are: **Home**, **Service Inventory**, **Service Design**, **Monitoring**, **Administration**, **Site Index**, and **Diagnostics**. This is a way to specify the first window you will see after logging in.

Step 6 Click **Save**.

The Users window reappears with the new user listed.

Copy

The **Copy** button, located at the bottom of the Users window, provides a convenient way to create a new User by copying the information for an existing User including User Groups, Assigned Roles, and User Preferences. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check one check box for the existing User you want to copy and edit to create a new User.

Step 3 Click the **Copy** button and the window shown in Figure 3-1, appears.

Required entries are a **User ID**, **Password**, **Verify Password, and Full Name**.

Step 4 Make all the other changes you want by following the instructions in the "Create" section on page 3-2.

Step 5 Click **Save** and you will return to the Users window.

The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of the Users window, allows a user with the required privileges to edit user-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check the check box for the row of the user you want to edit.

Step 3 Click the **Edit** button and a window as shown in Figure 3-1, appears.

Note To change your password without the SysAdmin or UserAdmin privileges, click the **Account** tab on the top of the Home page. This allows the user to edit the user profile, including changing the password.

Step 4 Enter the desired information for the user profile, as specified in the "Create" section on page 2.

Step 5 Click **Save**.

The Users window reappears with the edited user listed.

Delete

The **Delete** button, located at the bottom of the Users window, allows a user with the required privileges to delete user-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check the check box(es) for the row(s) of the user(s) you want to delete.

Step 3 Click the **Delete** button and a confirmation window appears.

Step 4 Click **Delete** to continue with the process of deleting information for the specified user(s). Otherwise click **Cancel**.

The Users window reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Groups

A user group is a logical grouping of users with common privileges. The **User Groups** feature is used to create, edit, or delete user groups.

To access the User Groups window, choose **Administration** > **Security** > **User Groups**. The User Groups window appears.

The explanations of the remainder of the buttons is given as follows:

- Create, page 3-5—Create a new user group
- Edit, page 3-6—Edit selected user group
- Delete, page 3-7—Delete selected user group(s)

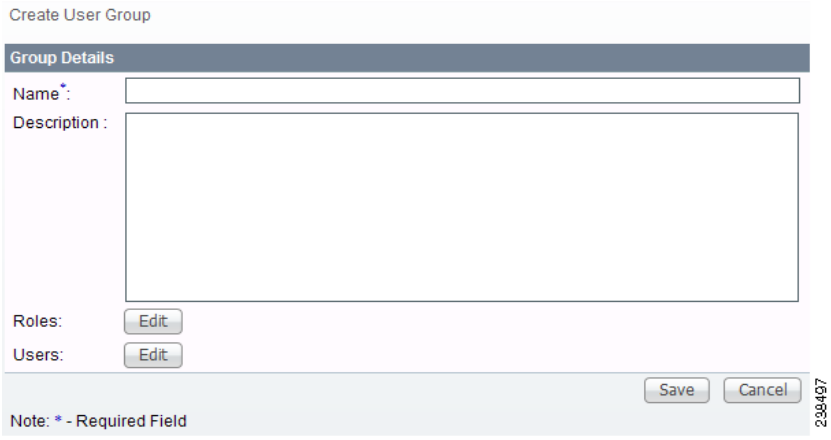
Create

The **Create** button, located at the bottom of the User Groups window, allows a user with the required privileges to create a user group. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Click the **Create** button and the window shown in Figure 3-2, appears.

Figure 3-2 Create/Edit User Groups Window



Step 3 Enter information for the user group profile, as follows:

- **Name** (required)—Enter a name for the new user group.
- **Description** (optional)—Enter a description of this new user group.
- **Roles**— This allows you to assign roles to this user group. Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.
- **Users**—This allows you to add users to this user group. Click **Edit** and you receive a list of the users. You can filter this list. From the selected users, check the check box next to each user you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 Click **Save**. The User Groups window reappears with the new user group listed.

Edit

The **Edit** button, located at the bottom of the User Groups window, allows a user with the required privileges to edit user group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Check the check box for the row of the user group you want to edit.

Step 3 Click the **Edit** button and a window as shown in Figure 3-2, appears.

Step 4 Enter the desired information for the user group profile, as specified in Step 3 of the **"Create" section on page 3-5**.

Step 5 Click **Save.**

The User Groups window reappears with the edited user group list.

Delete

The **Delete** button, located at the bottom of the User Groups window, allows a user with the required privileges to delete user group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Check the check box(es) for the row(s) of the user group(s) you want to delete.

Step 3 Click the **Delete** button and a confirmation window appears.

Step 4 Click **Delete** to continue the process of deleting information for the specified user group(s). Otherwise click **Cancel**.

The User Groups window reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Roles

A user role is a predefined or a user-specified role defining a set of permissions. The **User Roles** feature is used to create, edit, or delete user roles.

To better understand the way roles are managed, certain specific characteristics of roles are defined as follows:

- **Parent Role**—All permission of the parent roles are inherited by the role that is being created or edited (child role). A child role always has the same or more privileges than its parent role.
- **Customer**—If a role is associated with a customer, a user of this role does not have access to the objects associated with other customers. Object types that are constrained by customer view are: Persistent Task, Customer Site, VPN, CPE, SR, Policy, Service Order, and resource pools that are associated with a Customer, Customer Site, or VPN.
- **Provider**—If a role is associated with a provider, a user of this role does not have access to the objects associated with other providers. Object types that are constrained by provider view are: Persistent Task, Access Domain, Region, PE, Policy, and some resource pools that are associated with a provider, Access Domain, Region, or PE.

Customer view and provider view within a role have no affect on those objects that do not belong to either a customer or a provider. Those object types are: task, probe, workflow, device, Prime Provisioning host, and template.

Permission operation types in a Role editor, namely View, Create, Edit, and Delete mean View, Create, Modify, and Delete a database object. For example, SR modification (or subsumption) is viewed as Role Based Access Control (RBAC) Creation. SR purge is viewed as RBAC Delete.

A Role can be enabled to be associated with Object Group(s). When Object Group association is enabled, a Role can no longer be associated with a Customer or a Provider, and it cannot have a Parent Role. Resources are limited to PE, CPE, and Named Physical Circuit only. PE and CPE permission implies Device Permission.

Note A global policy, the one that is not associated with any customer or provider, is accessible by both customer-view roles and provider-view roles.

Separate provider-view from customer-view roles when defining a role. When a role is associated with a provider, choose only the resources for which an access scope can be constrained by a provider view. Do the same for a customer-view role.

To access the User Roles window, choose **Administration > Security > Roles**. The User Roles Administration window appears.

The predefined roles are provided with associated permissions that cannot be edited or deleted. They are intended to cover most of the needed use cases to facilitate a rapid assignment of roles to users and groups with minimum manual configuration. They can also be used as examples to create new roles.

The explanations of the buttons is as follows:

- Create, page 3-8—Create a new user role
- Copy, page 3-11—Copy selected user role
- Edit, page 3-11—Edit selected user role
- Delete, page 3-11—Delete selected user role(s)

Create

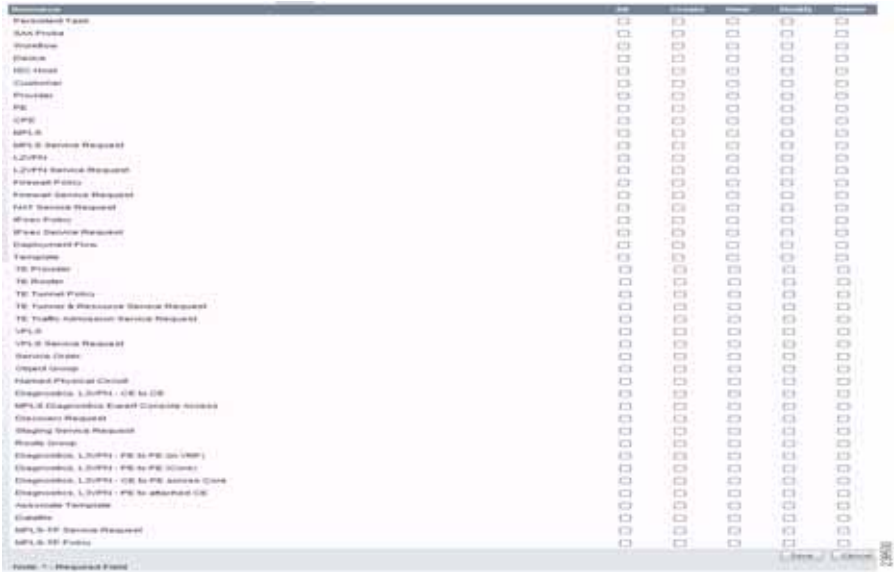
The **Create** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to create a new user role. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Roles**.

Step 2 Click the **Create** button and a window comprised of Figure 3-3 and Figure 3-4, appears.

Figure 3-3 Create/Copy/Edit User Roles Window (Top)

Figure 3-4 Create/Copy/Edit User Roles Window (Bottom)



Step 3 Enter the following information in Figure 3-3:

- **Name** (required)—Enter the name of this new user role.
- **Enable Object Group Association**—The default is that this check box is unchecked. In this case, **Parent Role**, **Customer**, and **Provider** are enabled and **Object Groups** is not enabled. A complete list of resources appears, as shown in the example in the User Roles Administration window. If you check this check box, **Parent Role**, **Customer**, and **Provider** are not enabled and **Object Groups** is enabled. A window, as shown in Figure 3-4, is reduced to just **PE**, **CPE**, and **Named Physical Circuit**.
- **Parent Role** (optional)—Click **Edit** and a list of the existing roles appears, similar to the User Roles Administration window, from which you can click the radio button for the parent role you choose. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no parent selection.
- **Customer** (optional)—Click **Edit** and a list of the existing customers appears. You can filter this list. From the selected customers, click the radio button for the customer you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no customer selection.

Note A customer can only be associated with a logical device, such as **CPE** and **PE**. This is not possible with a physical device, such as **device**.

- **Provider** (optional)—Click **Edit** and a list of the existing providers appears. You can filter this list. From the selected providers, click the radio button for the provider you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no provider selection.
- **Object Groups** (optional)—Click **Edit** and a list of the existing object groups appears. You can filter this list. From the selected object groups, check the check box(es) for the object group(s) you want to associate with this User Role. Then click **OK**. You can repeat this procedure if you want to change your selection. Deselect the **Enable Object Group Association** button if you want no object group selection.

- **Description** (optional)—Enter the descriptive information about permissions in this field, as shown in the Description column of the User Roles Administration window.
- **Users** (optional)—Click **Edit** and a list of the existing users appears. You can filter this list. From the selected users, check the check box(es) for the user(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Note A user who is associated with a specific role cannot see objects associated with other customers or with other providers.

- **User Groups** (optional)—Click **Edit** and a list of the existing user groups appears. You can filter this list. From the selected user groups, check the check box(es) for the user group(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 In Figure 3-4, click any combination of the following permissions: **Create**; **View**; **Modify**; **Delete**. If you want all the permissions, click **All**.

Note **Prime Provisioning Host** refers to **Administration > Control Center > Hosts**. Here, you can view host details, perform configuration tasks, start and stop servers, activate a watchdog, and so on.

Note **SAA Probe** is intended for management of SLA under **Inventory > Device Tools > SLA**. **Any user who wants** to generate SLA reports *must* have **View** permission on **Prime Provisioning Host** in addition to **View** permission on **SAA Probe**.

Note The **Workflow** object is currently not used.

Note **Template** controls the template manager functions and **Associate Template** controls the ability to associate templates with service requests. If you choose **Create** permission in Template, you also automatically receive **Modify** permission. If you choose any or all permissions in **Associate Template**, you automatically turn on the **View** permission in **Template**.

Note **Datafile** permission allows you to manage datafiles and list all Service Requests associating the datafile. If you choose any or all permissions in **Datafile**, you automatically turn on the **View** permission in **Template**.

Step 5 Click **Save**.

The User Roles Administration window reappears with the new user role listed.

Copy

The **Copy** button, located at the bottom of the User Roles Administration window, provides a convenient way to copy the information from an existing User Role and edit it to create a new User Role. Follow these steps:

Note All fields in the existing role are copied to the new role, even including Users and User Groups. You should edit the new role *carefully* to reflect your intention.

Step 1 Choose **Administration** > **Security** > **Roles**.

Step 2 Check one check box for the existing User Role you want to copy and edit to create a new User Role.

Step 3 Click the **Copy** button and the window comprised of Figure 3-3 and Figure 3-4 appears.

Step 4 The required entry is a **Name**. A default name is given, **Copy of** and the name of the original User Role. You cannot duplicate a **Name**.

Step 5 Make all the other changes you want by following the instructions in the "Create" section on page 3-8.

Step 6 Click **Save** and you will return to the User Roles Administration window.

The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to edit user role-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Roles**.

Step 2 Check the check box for the row of the user role you want to edit.

Step 3 Click the **Edit** button and a window appears combining Figure 3-3 and Figure 3-4 for this user role.

Step 4 Enter the desired information for the user role profile, as specified in Step 3 and Step 4 of the "Create" section on page 3-8.

Step 5 Click **Save**.

The User Roles Administration window reappears with the edited user roles listed.

Delete

The **Delete** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to delete user role-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Roles**.

Step 2 Check the check box(es) for the row(s) of the user role(s) you want to delete.

Step 3 Click the **Delete** button and a confirmation window appears.

Step 4 Click **Delete** to continue with the process of deleting information for the specified user role(s).

The User Roles Administration window reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

Otherwise click **Cancel**.

Object Groups

An Object Group is a named aggregate entity comprised of a set of objects. The object types can be PE, CE, Named Physical Circuit (NPC), and interfaces of PEs or CEs. An Object Group provides instance level of access granularity for users.

An Object Group can be associated with different roles. A role can be associated with an Object Group or it can be associated with a grouping of Customer and Provider, but it cannot be associated with both of these. The association with a grouping of Customer and Provider is either with Customer(s), with Provider(s), or with Customer(s) and Provider(s). When a role is associated with Object Group(s), you can only define permissions for PE, CE, and NPC. Permissions on interfaces is implied PEs or CEs, that is, PE Create or CE Create implies Interface Create. PE or CE Edit implies Interface Create, Edit, or Delete. CE or PE Delete implies Interface Delete.

When instance level of access is desired for PE, CE, NPC, or interface of PEs and CEs, you can usually define a role associated with Object Group(s) that contains a collection of PEs and CEs you are limited to operate. Then define other roles to include permissions on other types of objects. See the "User Roles Design Example" section on page 3-14.

If an Object Group contains PEs (or CEs) only, with no explicit interface as a group member, you can access all interfaces of grouped PEs or CEs. If an Object Group contains any explicit interface as group members, every single interface that you want to access you must manually choose to include as group members.

Note Permissions are the union of all roles that you occupy. If your intention is to limit access to a scope of devices or Named Physical Circuits (NPCs), define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

To access the Object Groups window, choose **Administration > Security > Object Groups**. The Object Groups window appears.

The explanations of the buttons is as follows:

- Create, page 3-8—Create a new object group
- Edit, page 3-11—Edit a selected object group
- Delete, page 3-11—Delete selected object group(s)

Create

The **Create** button, located at the bottom of the Object Groups window, allows a user with the required privileges to create a new object group. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Click the **Create** button and the **Create Object Group** window appears.

Step 3 Enter the following information:

- **Name** (required)—Enter the name of this new object group.
- **Description** (optional)—Enter a description of this new object group.
- **PE Group Members** (optional)—Click **Edit** and a list of the existing PEs appears. You can filter this list. From the selected PEs, check the check box(es) for the PE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column will be empty. All existing interfaces for each of the PE Groups in the **Name** column will default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a PE Group in the **Name** column.You receive a list of all the interfaces for that PE from which you can individually select only the interfaces you want to associate with that PE Group. Then click **OK**. When you return to **Create Object Group** window, the **Name** and selected **Interface Members** for each PE Group Member appear. If no entries exist in the **Interface Members** column for both **PE Group Members** and **CE Group Members**, the default is all existing interfaces for both (if any exist).
- **CE Group Members** (optional)—Click **Edit** and a list of the existing CEs appears. You can filter this list. From the selected CEs, check the check box(es) for the CE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column is empty. All existing interfaces for each of the CE Groups in the **Name** column default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a CE Group in the **Name** column.You receive a list of all the interfaces for that CE from which you can individually select only the interfaces you want to associate with that CE Group. Then click **OK**. You return to **Create Object Group** window and the **Name**, and selected **Interface Members** for each CE Group Member appear. If no entries exist in the **Interface Members** column for both **CE Group Members** and **PE Group Members**, the default is all existing interfaces for both (if any exist).
- **NPC Group Members** (optional)—Click **Edit** and a list of the existing NPCs appears. You can filter this list. From the selected NPCs, check the check box(es) for the NPC(s) you want to select to own this role. Then click **OK**. You can repeat this procedure if you want to change your selection(s). You return to **Create Object Group** window and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**.

Create Object Group window reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of **Create Object Group** window, allows a user with the required privileges to edit object group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Check the check box for the row of the object group you want to edit.

Step 3 Click the **Edit** button and a window appears as shown in the Object Groups window, with the object group chosen specified in the **Name** field.

Step 4 Enter the desired information for the object group, as specified in Step 3 of the "Create" section on page 3-12.

Step 5 Click **Save**.

The Object Groups window reappears with the edited object groups listed.

Delete

The **Delete** button, located at the bottom of the Object Groups window, allows a user with the required privileges to delete object group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Check the check box(es) for the row(s) of the object group(s) you want to delete.

Step 3 Click the **Delete** button and a confirmation appears.

Step 4 Click **Delete** to continue with the process of deleting information for the specified object group(s).

The Object Groups window reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

Otherwise click **Cancel**.

User Roles Design Example

This section gives an example situation, an illustration that shows this setup, and steps on how to set up this design:

Example

This section explains an example data center for which the following sections, "Illustration of Setup" section on page 3-15 and "Steps to Set Up Example" section on page 3-16 give an illustration setup and steps, respectively.

Finance Customer XYZ built an MPLS network to connect its branch offices to its data center. Subsidiaries of XYZ are running different parts of the MPLS network. Each subsidiary uses a different BGP AS domain, which results in different Provider Administrative Domains (PADs) inside Prime Provisioning.

Each subsidiary acts as a Provider and owns therefore its own Devices, like PE and CE devices, and should also own logical attributes inside Prime Provisioning, like Regions, Sites, Customers, and VPNs. Therefore, the view of the devices for each subsidiary must be separated into PAD views. Thus, Provider A cannot manipulate or view the configuration files for devices of Provider B. Devices are not shared between PADs.

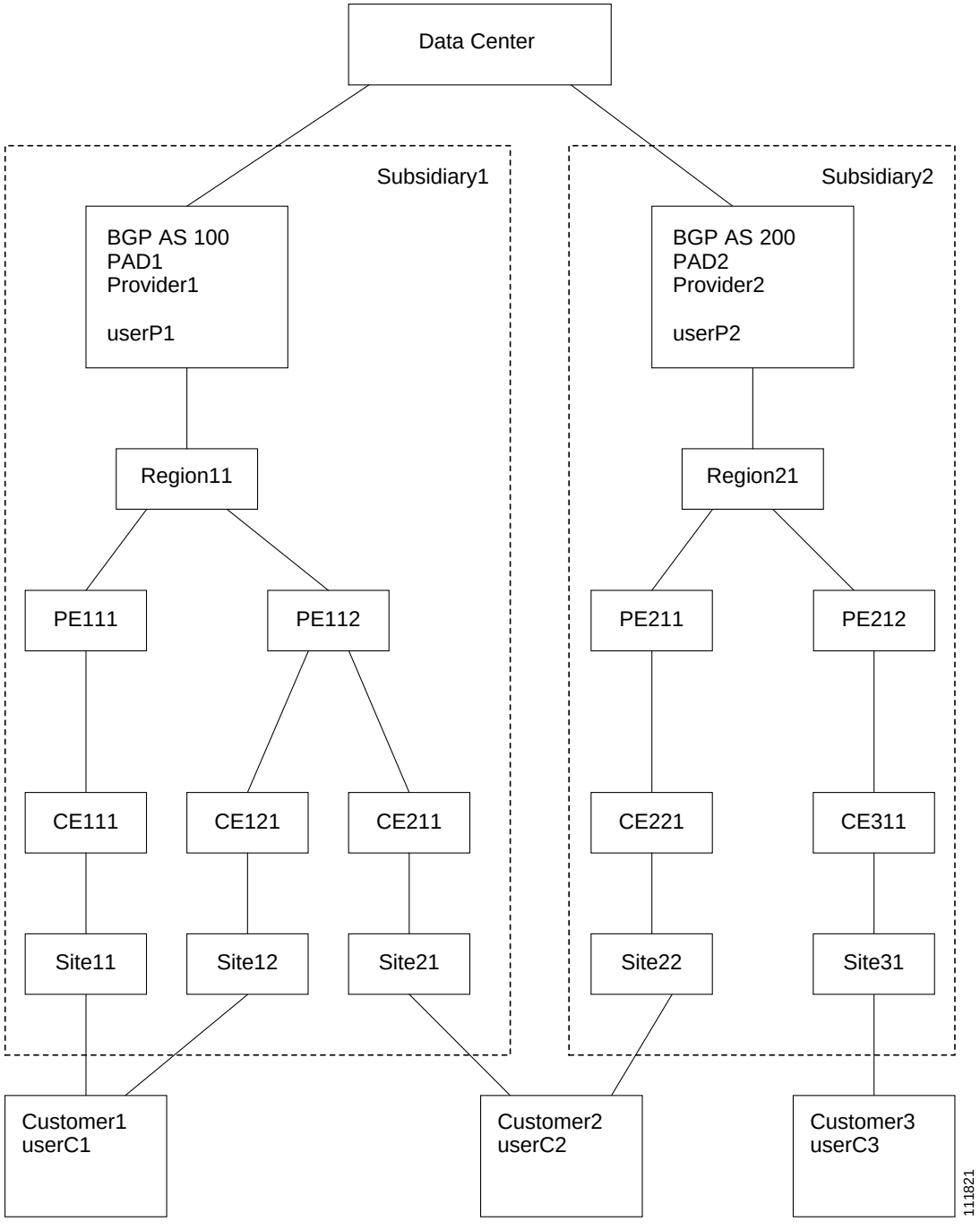
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

But there are also Customers that have sites in different PADs. This means that there is a need for Inter-AS VPNs. The Provider who owns the Customer should also have the right to share this Customer with other Providers. In this case, the VPNs and Route Targets should be shared between the providers.

Illustration of Setup

Figure 3-5 shows the set up described in the "Example" section on page 3-14.

Figure 3-5 Contents in Example



Steps to Set Up Example

This section explains the steps to create the example explained in the "Example" section on page 3-14 and shown in the "Illustration of Setup" section on page 3-15.

Step 1 Create the following Object Groups (see the "Create" section on page 3-12, which is for the section Object Groups):

- P1PEGroup that has members PE111 and PE112
- P2PEGroup that has members PE211 and PE212
- C1CEGroup that has members CE111 and CE121
- C2CEGroup that has members CE211 and CE221
- C3CEGroup that has the member CE311
- C2DeviceGroup that has members PE112, CE211, PE211, and CE221
- C3DeviceGroup that has members PE212 and CE311.

Step 2 Create the following User Roles that are associated with one or more groups created in Step 1 (see the "Create" section on page 3-8, which is for the section User Roles).

- P1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and C2CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
- P2DeviceGroupRole, associated with groups P2PEGroup, C2CEGroup, and C3CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
- C1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- C2DeviceGroupRole, associated with group C2DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- C3DeviceGroupRole, associated with group C3DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.

Step 3 Create the following User Roles that have Customer View or Provider View, as explained in the "User Roles" section on page 3-7.

- P1MplsRole, associated with Provider P1, and have permissions on Provider, Task, Prime Provisioning Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- P2MplsRole, associated with Provider P2, and have permissions on Provider, Task, Prime Provisioning Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C1MplsRole, associated with Customer C1, and have permissions on Customer, Task, Prime Provisioning Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C2MplsRole, associated with Customer C2, and have permissions on Customer, Task, Prime Provisioning Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C3MplsRole, associated with Customer C3, and have permissions on Customer, Task, Prime Provisioning Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)

Step 4 Assign the User Roles defined in Step 2 and Step 3 to Users, as explained in the "Users" section on page 3-1.

- User P1 has User Roles: P1DeviceGroupRole, P1MplsRole, C1MplsRole, and C2MplsRole.
- User P2 has User Roles: P2DeviceGroupRole, P2MplsRole, C2MplsRole, and C3MplsRole.
- User C1 has User Roles: C1DeviceGroupRole and C1MplsRole.
- User C2 has User Roles: C2DeviceGroupRole and C2MplsRole.
- User C3 has User Roles: C3DeviceGroupRole and C3MplsRole.

Backup and Restore of Prime Provisioning Repository

This chapter explains how to back up and restore your Sybase and Oracle databases. The Cisco.com location of scripts for these procedures is:

http://software.cisco.com/download/navigator.html?mdfid=284127465&flowid=37682

Note When upgrading from a earlier release of Prime Provisioning, the existing backup script will no longer work. Make sure to download and install the new backup script.

This chapter contains the following sections:

Data Items Included in Backup and Recovery

Most of the Prime Provisioning-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 Prime Provisioning to function flawlessly on restart, following a crash, it is necessary that the proposed backup and recovery feature include various Prime Provisioning-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 Prime Provisioning'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.

3. **Others:** There are a few data items that are stored in the OS level file system under various Prime Provisioning install directories, which would be part of the proposed backup and recovery plan.

Guidelines

This section explains how to use the supported backup methods in Prime Provisioning.

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 backups:

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

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

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

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

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

Step 3 It is important to keep more than one full backup 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.

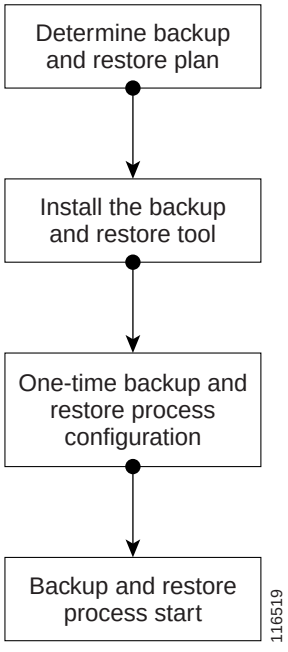
Sybase Backup and Restore Process Overview

This section describes how to back up and restore Sybase ASA for an Prime Provisioning installation. This section contains the following sections:

Overview of the Backup and Restore Process

Figure 4-1 shows an overview of the Sybase ASA backup and restore process.

Figure 4-1 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 Prime Provisioning production machine and the secondary system (if you want to run the restore process from the secondary system or you want to perform a live backup).

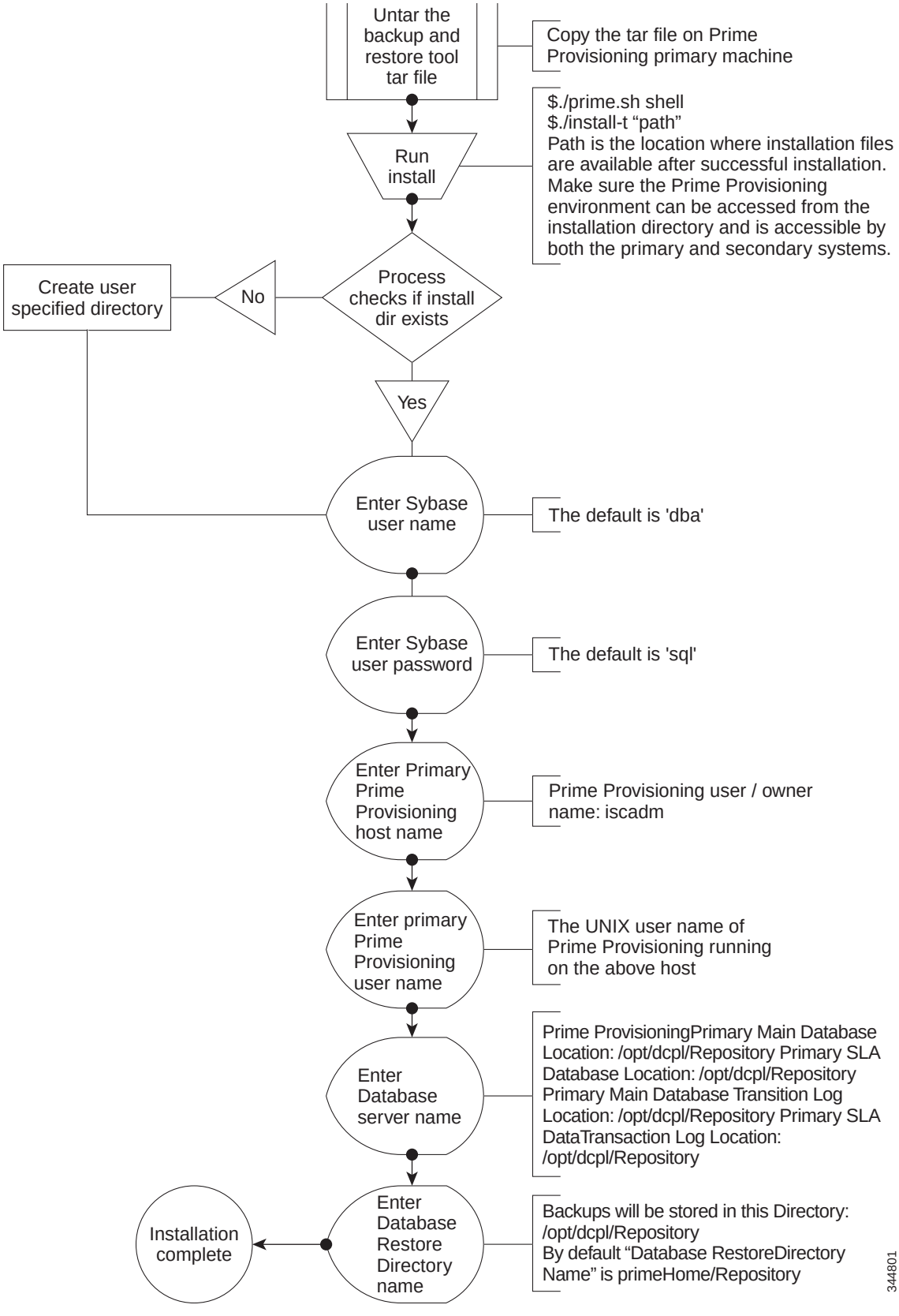
Step 4 Document the information for Step 1 to Step 3.

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

Installing the Backup and Restore Tool

Figure 4-2 shows the process flow for installing the backup and restore tool.

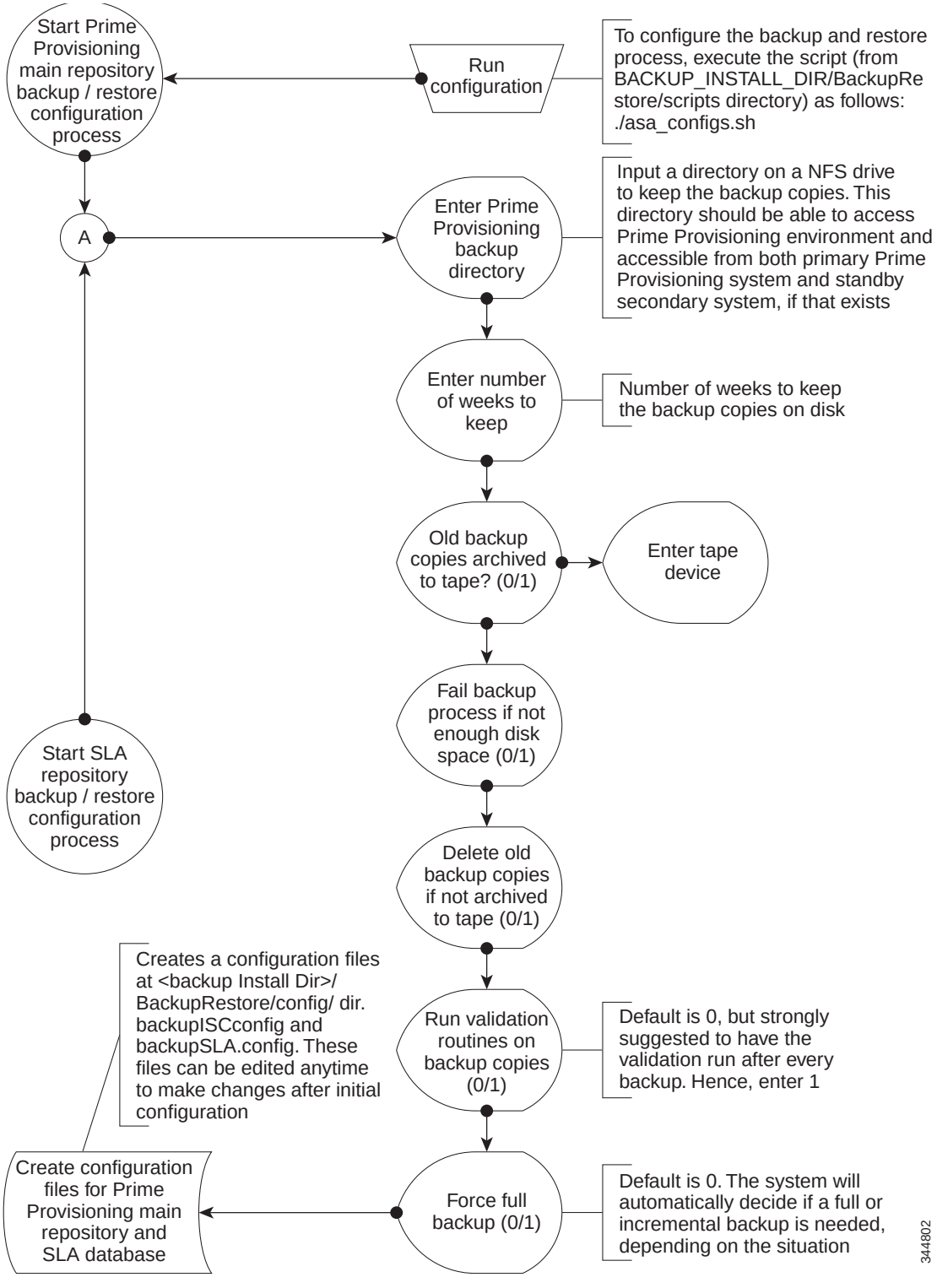
Figure 4-2 Installing the Backup and Restore Tool



Configuring the Backup and Restore Process

Figure 4-3 shows the one-time configuration process for the backup and restore.

Figure 4-3 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 Prime Provisioning database server is running.
2. The backup directory path that you specify during the configuration must be on a Network File System (NFS) drive.
3. The backup and restore tool must be installed and accessible by both the primary and secondary systems.
4. The backup and restore tasks must be carried out from the Prime Provisioning primary machine. However, the live backup and restore is done from the secondary system.
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.

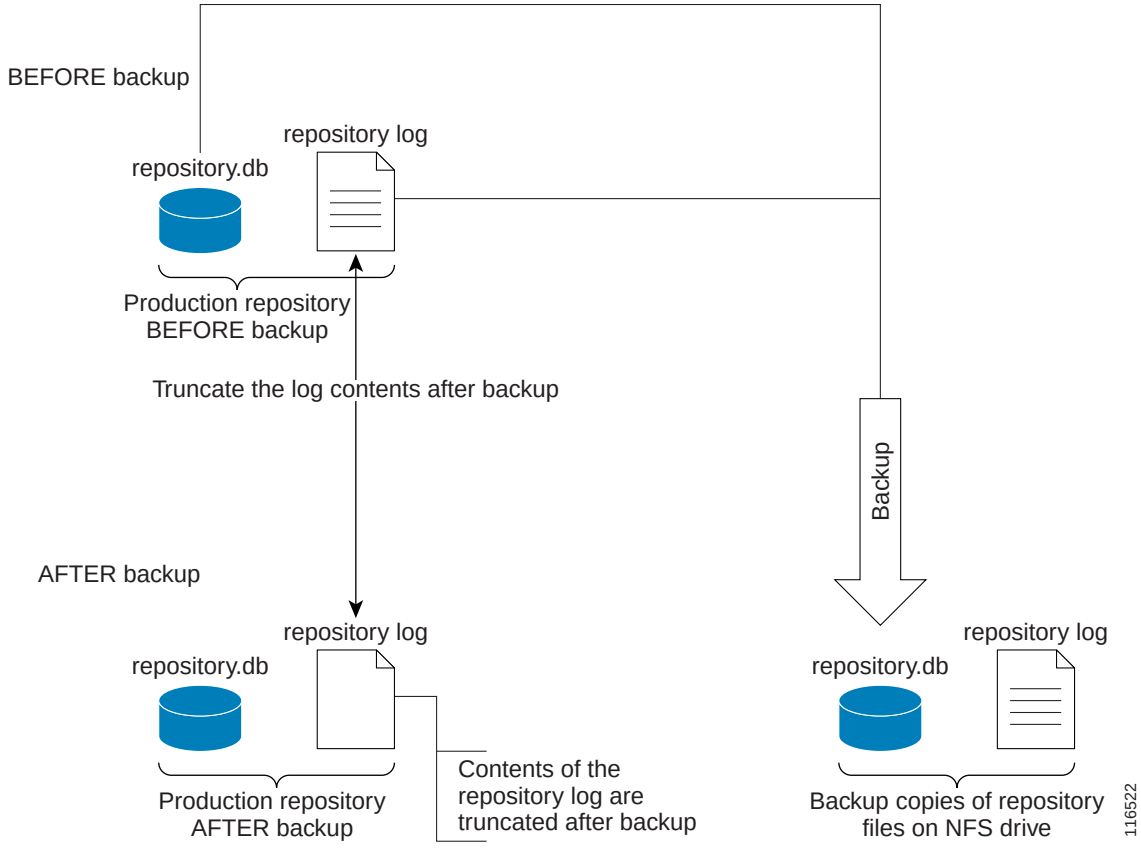
8. Both the database and the transaction log are backed up in a full backup.
9. Only the transaction log is backed up in an incremental backup.

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 4-4 shows a full backup scheme.

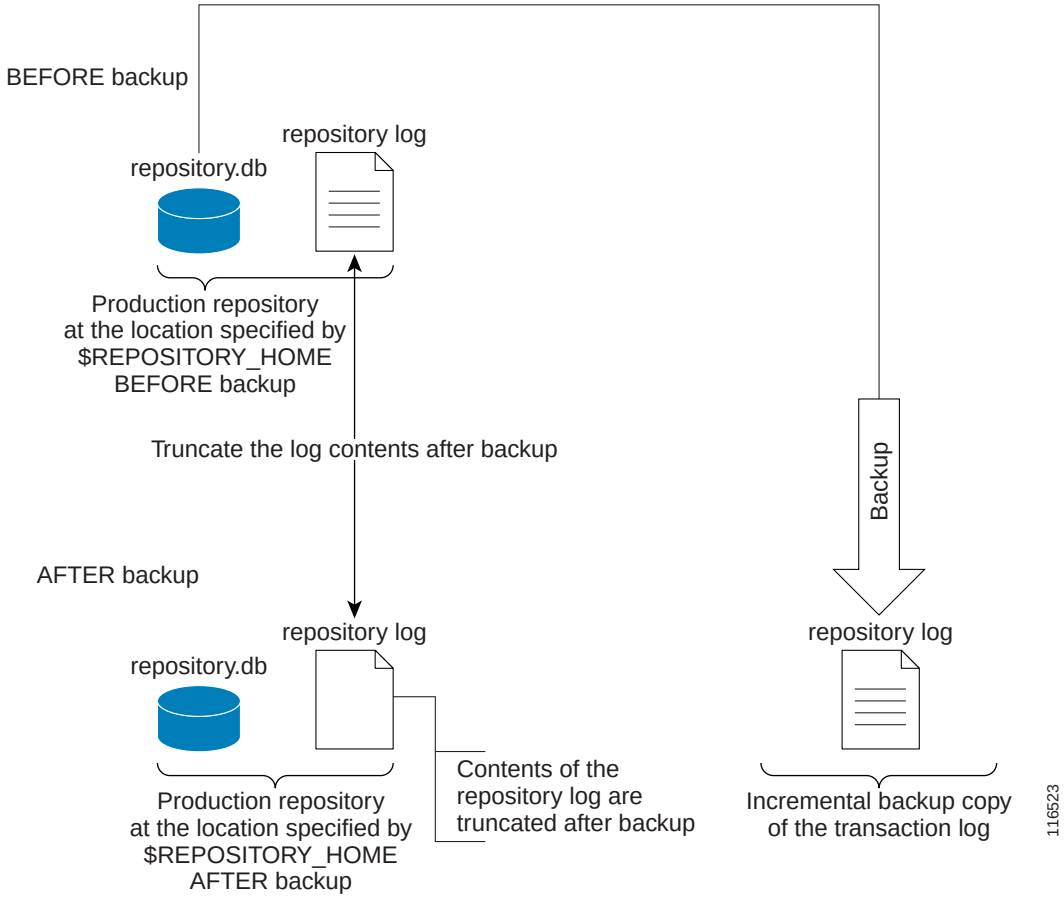
Figure 4-4 Full Backup Scheme



Incremental Backup Scheme

Figure 4-5 shows an incremental backup scheme.

Figure 4-5 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 03/14/2010 through 03/20/2010 and the Backup Dir as specified during configuration is /auto/PrimeProvisioningBackups (NFS drive). The system creates two subdirectories under user specified backup dir, ISCMain and SLA.

1. First backup run on 03/15/2010 Monday, default full backup. Creates a sub dir /03-14-2010/full_01.dir under ISCMain and SLA directories.
2. Second backup run on the same date 03/15/2010, default incremental backup.
3. Third backup run on 03/17/2010, default incremental backup.
4. Fourth backup, Forced FULL backup (after changing configuration file setting, fullBackup to 1) on 03/18/2010. Creates a new sub dir /03-14-2010/full_02.dir under ISCMain and SLA directories.

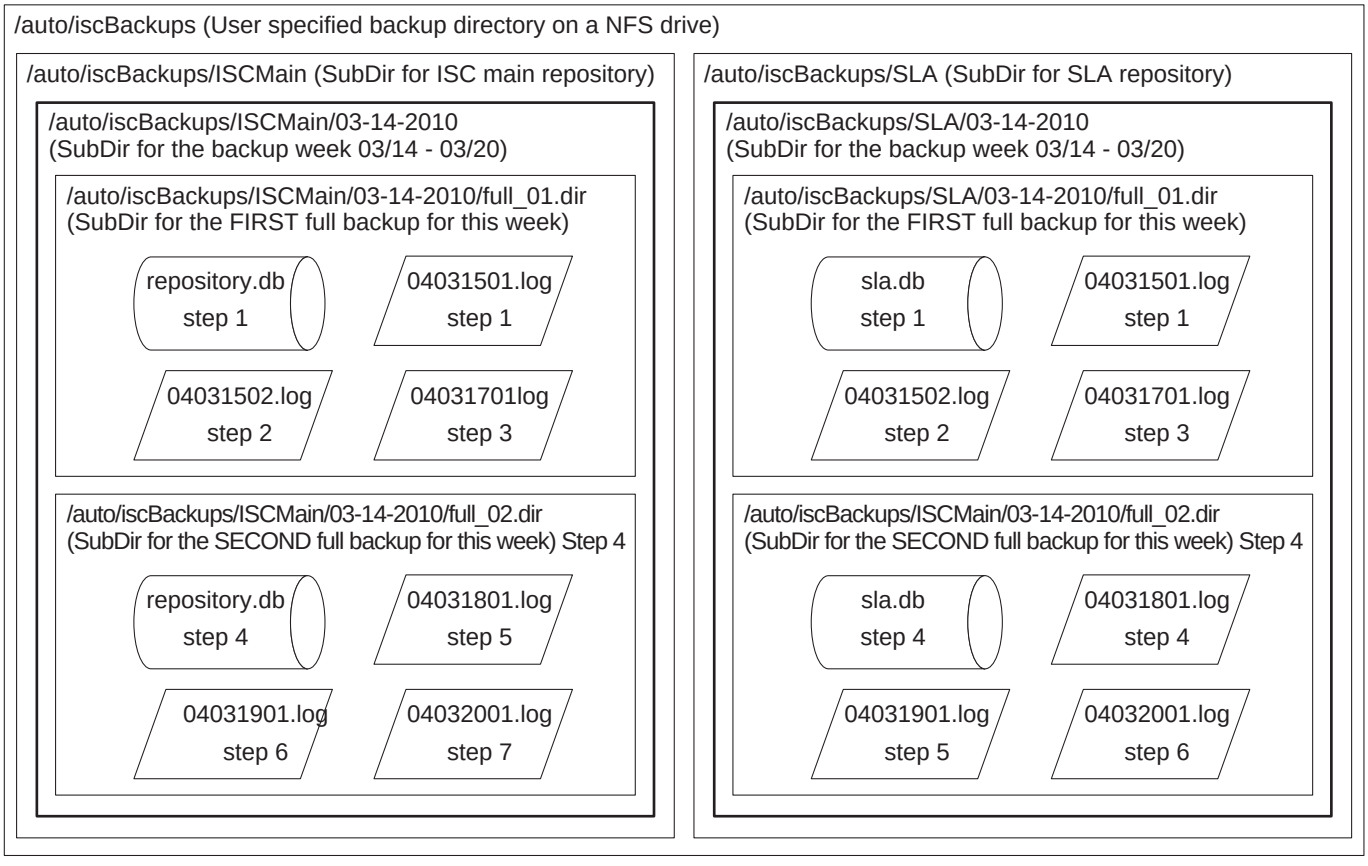
Note Configuration setting, full backup reset to 0.

5. Fifth backup, run on 03/19/2010, default incremental backup.
6. Sixth backup, run on 03/20/2010, default incremental backup.

Note Backup Week ended on 03/20/2010.

Figure 4-6 shows a typical backup directory structure on an NFS drive.

Figure 4-6 Typical Backup Directory Structure



Understanding the Restore Process Flow

This section contains the following sections:

- Preconditions, page 4-10
- Functions, page 4-11
- Restore from Media Failure, page 4-11
- Restore to a Desired Point-in-Time, page 4-13

Preconditions

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

1. The Prime Provisioning database server should be stopped while running the Restore task.

2. The backup directory path that you specify during the configuration must be on a Network File System (NFS) drive.
3. The backup and restore tool must be installed and accessible by both the primary and secondary systems.
4. The backup and restore tasks must be carried out from the Prime Provisioning primary machine. However, the live backup and restore is done from the secondary system.
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 Prime Provisioning 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

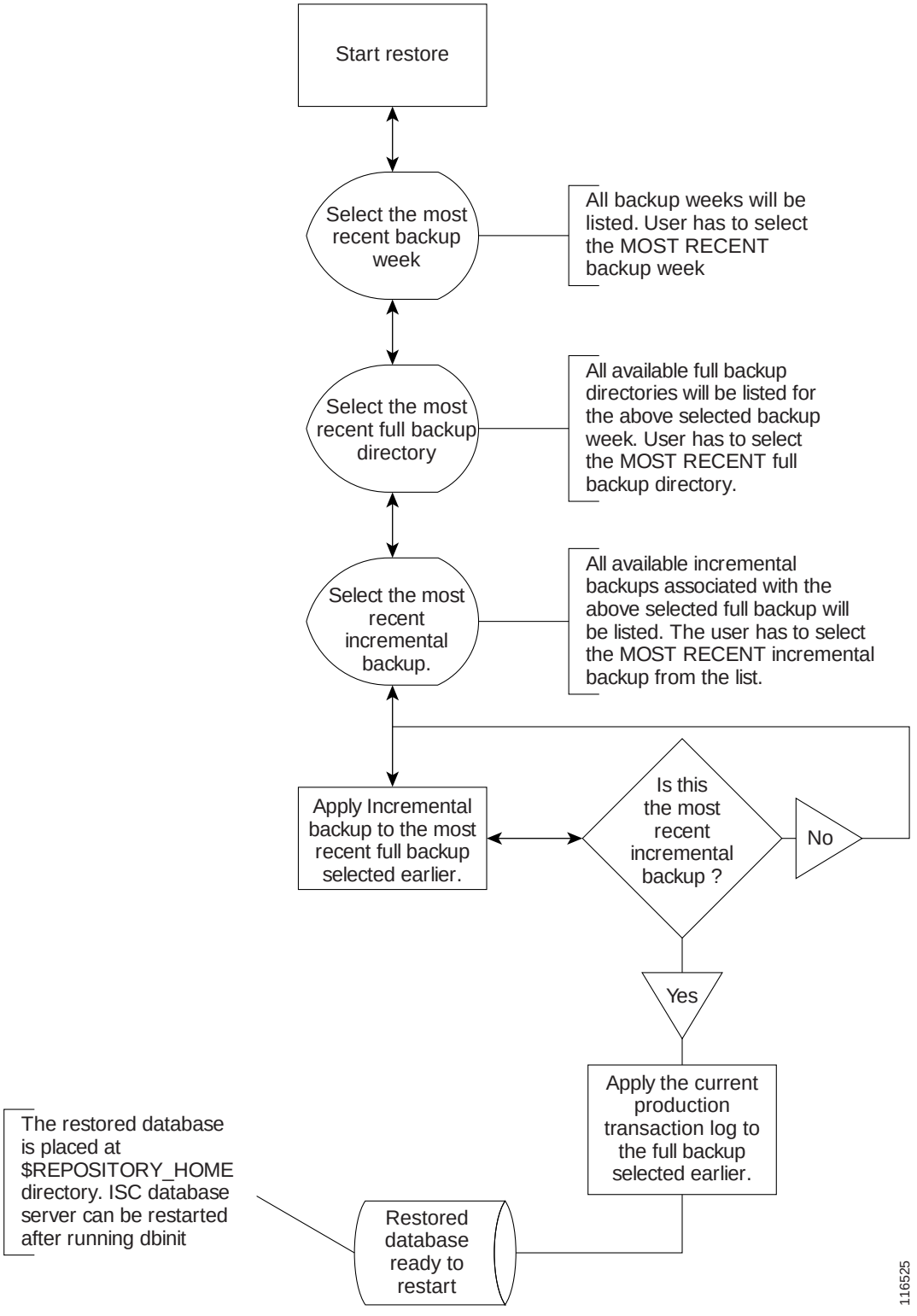
Note Please see Sybase ASA documentation for more information.

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

Restore from Media Failure

Figure 4-7 shows the process flow for how to restore from a media failure on the database file (.db).

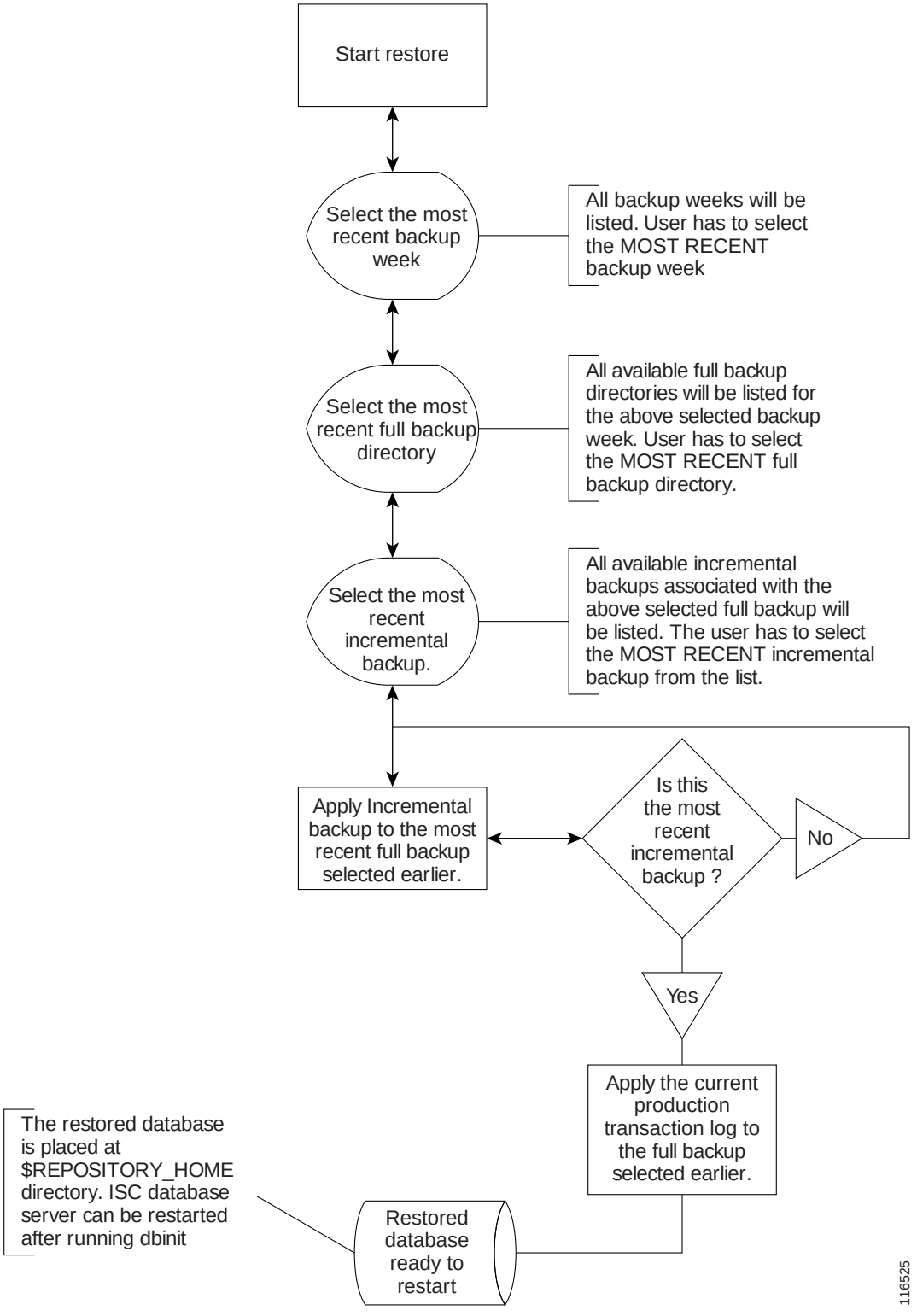
Figure 4-7 Restore from Media Failure on the Database File (.db)



Restore to a Desired Point-in-Time

Figure 4-8 shows the process flow for how to restore from a desired point-in-time.

Figure 4-8 Restore the Database to a Desired Point-in-Time



Sybase Database Backup and Restore

It is important to protect all Prime Provisioning-related data by a well-defined backup and recovery plan. Data loss could occur due to the following reasons. The objective of Prime Provisioning'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 backup is needed for this current backup week. If a full backup already exists for this current backup week, this script automatically takes an incremental backup. However, the user can force a full backup overriding this default behavior by changing the configuration setting.

Installing the Sybase Backup and Restore Tool

Step 1 From **here** download the tar file
iscBRToolASA_LINUX_12_17_2012.tar.gz (for Linux Backup and Restore Tool)
or **iscBRToolASA_SOLARIS_12_17_2012.tar.gz** (for Solaris Backup and Restore Tool)

Step 2 Untar this file as follows:

mkdir -p $PRIMEP_HOME/backup/Sybase

gzip -d < iscBRToolASA_LINUX_12_17_2012.tar.gz | tar xf -

Step 3 **./prime.sh shell**

Run install from where the tar file is unzipped. 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  "path"
```

where:
"path" is the location the installation files will be available after successful installation.
<BACKUP_INSTALL_DIR> must be NFS accessible by both the primary and secondary systems.

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 /opt/dcpl
```

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 Prime Provisioning hostname: tl-dev-v240-5 (user input, the hostname of
the machine running Prime Provisioning)
Enter Primary Prime Provisioning user/owner name: iscadm (user input, the user/owner name
of Prime Provisioning on the above host)
Enter Database server name [sarpadma_tl-dev-v240-5]: [?]
    Cisco Prime Provisioning Primary Main Database Location: /opt/dcpl/Repository
    Primary SLA Database Location: /opt/dcpl/Repository
    Primary Main Database Transaction Log Location: /opt/dcpl/Repository
    Primary SLA Data Transaction Log Location: /opt/dcpl/Repository
Enter Database Restore Directory Name (Backups will be stored in this
Directory): [?] /opt/dcpl/Repository

Note- By default the "Database Restore Directory Name" is prime Home/Repository.
```

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 Prime Provisioning backup and restore scripts.

Adding PATH Statement

After installing the Prime Provisioning Backup and Restore tool and before configuring it, the PATH statement:

PATH=$PATH:/BackupRestore/scripts:/BackupRestore/config:/BackupRestore/bin export PATH

should be added to the login .profile file of the user iscadm.

Without this permanent addition, later runs of the backup and restore may fail.

Configuring the Sybase Backup and Restore Tool

A one-time configuration is needed before the first backup is carried out.

Step 1 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 Prime Provisioning database
DB server Name...yourname_yourname-u10

Prime Provisioning Backup script invoked with the following parameters:
------------------------------------------------------------------------
Backup directory: /opt/dcpl/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 Prime Provisioning backup configuration file is nonexistent ... creating new file
Modifying Prime Provisioning backup configuration settings ...
Enter new Prime Provisioning backup directory path (a subdirectory Cisco
Prime Provisioning will be added automatically.)
[/opt/dcpl/BackupRestore/Backups] [?]
Enter the number of weeks to keep [2] [?] 2
Old backups archived to tape (0=no, 1=yes) [0] [?]
Enter 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] [?]
Delete old backups specified is "0".
Run validation routines on backup files (0=no, 1=yes) [0] [?] 1
Force full backup (0=no, 1=yes) [0] [?] 0
Confirm these values
[1]Cisco Prime Provisioning backup directory path = /opt/dcpl/BackupRestore/Backups/Main
[2]number of weeks to keep = 2
[3]Old backups archived to tape  = 0
[4]tapeDevice = /dev/rmt/0
[5]Fail backup if there is not enough space for a full backup= 1
[6]Delete old backups if not archived to tape = 0
[7]Run validation routines on backup files = 0
[8]Force full backup = 0
               Do you want to modify any values ?  [n]  [y,n,?]
Cisco Prime Provisioning 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 Prime Provisioning backup engine is now exiting without backing up the database.You
must run the asa_backup.sh script for the backup to take place.
Prime Provisioning Backup Configuration Successfully completed
Prime Provisioning Backup Configuration script ending.
Starting backup Configuration for SLA database
DB server Name...yourname_yourname-u10
SLA Backup script invoked with the following parameters:
--------------------------------------------------------------------------------
Backup directory: /opt/dcpl/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) [/opt/dcpl/BackupRestore/Backups] [?]
Enter the number of weeks to keep [2] [?] 3
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
Enter 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] [?]
Confirm these values
[1]SLA backup directory path = /opt/dcpl/BackupRestore/Backups/SLA
[2]number of weeks to keep = 2
```

```
[3]Old backups archived to tape  = 0
[4]tapeDevice = /dev/rmt/0
[5]Fail backup if there is not enough space for a full backup= 1
[6]Delete old backups if not archived to tape = 0
[7]Run validation routines on backup files = 0
[8]Force full backup = 0
Do you want to modify any values ?  [n]  [y,n,?]
SLA 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

The backup script is used as follows:

Step 1 Run the *<BACKUP_INSTALL_DIR>*/**BackupRestore/script/asa_backup.sh** script to initiate the backup task.

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

b. The backup directory path specified during the configuration process *must* 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 Prime Provisioning system crashes.

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

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

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

Step 3 You can force a full backup instead of an automatic incremental backup 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 backup and all the associated incremental backups under the above weekly directory. Each time a forced full backup is made for the current backup week, there is a new subdirectory created to contain this full backup and its associated incremental backups.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 Backup

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

1. A restore of a previous Full or incremental backup.
2. A recovery from a media failure on the database file.

Note The main Prime Provisioning repository consists of repository.db and repository.log files and the SLA consists of sla.db and sla.log files. Prime Provisioning 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 1 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 Prime Provisioning 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 Backup and Restore

From the location http://software.cisco.com/download/navigator.html?mdfid=284127465&flowid=37682, download the tar file iscBRToolORA.tar.gz and untar this file as follows:

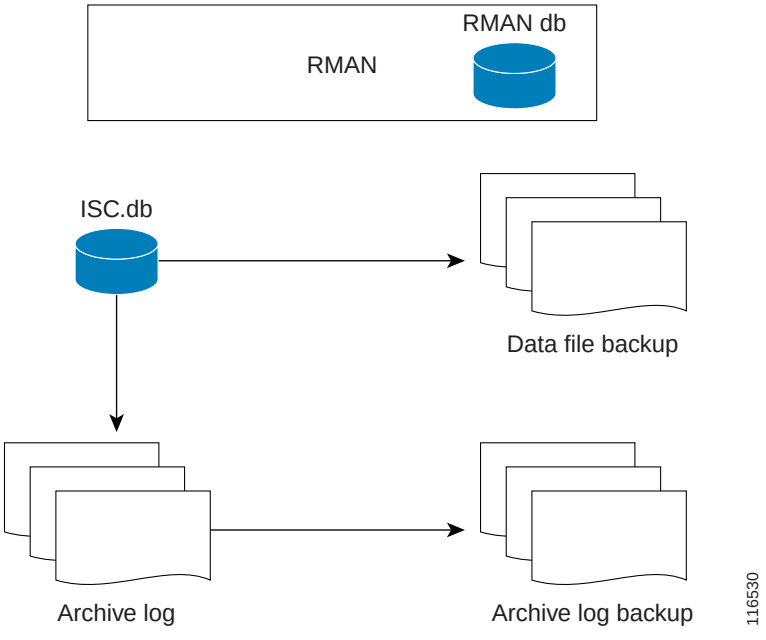
mkdir -p $PRIMEP_HOME/backup/Oracle

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

Oracle databases have a backup and restore Recovery Manager (RMAN) tool. To use this tool for online backup, the Oracle database must be in ARCHIVELOG mode, as explained in the "Create RMAN Catalog Database" section on page 4-21. RMAN maintains the bookkeeping intelligence of backup and recovery files and backs up at the block level. Therefore, RMAN can significantly speed up backups and reduce the server load by using incremental backups.

Figure 4-9 shows an Oracle Database Backup Diagram.

Figure 4-9 Oracle Database Backup



RMAN for Oracle 10g is explained in the quick start guide and reference manual, which are available from Oracle's website.

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 Prime Provisioning 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 Create RMAN Catalog Database, page 4-21.

Step 2 Create RMAN User, page 4-21.

Step 3 Create RMAN Catalog, page 4-21.

Step 4 Register the Prime Provisioning Database with the RMAN Catalog, page 4-21.

Step 5 Add PATH Statement, page 4-22

Step 6 Modify Prime Provisioning Database Initial Parameter File, page 4-22.

Step 7 Back up Database, page 4-22.

Step 8 Recover Database, page 4-23.

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 Prime Provisioning database.

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

Create RMAN User

Creating an RMAN user is the same as creating an Prime Provisioning user on an **rcat** 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 Prime Provisioning Database with the RMAN Catalog

Set the ORACLE_SID environment variable = prime.

%rman

RMAN > connect catalog rmanuser/rmanpassword@rcat

RMAN > connect target sys/**change_on_install**

RMAN > register database

RMAN> **configure controlfile autobackup on;**

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 Prime Provisioning database.

Add PATH Statement

After installing the Prime Provisioning Backup and Restore tool and before configuring it, the PATH statement:

PATH=$PATH:/BackupRestore/scripts:/BackupRestore/config:/BackupRestore/bin export PATH

should be added to the login .profile file of the user iscadm.

Without this permanent addition, later runs of the backup and restore may fail.

Modify Prime Provisioning Database Initial Parameter File

To modify the Prime Provisioning 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 Prime Provisioning 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;

Back up Database

To back up the database, do the following:

Step 1 Download the software for backup and restore from:

http://software.cisco.com/download/navigator.html?mdfid=284127465&flowid=37682

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

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

Note The file **$PRIMEP_HOME/backup/Oracle/backupenv.properties contains BACKUP_DEST, which must point to a directory that is writable by the owner of the Oracle database. To do this, specify chmod atw** <*file_defined_by_BACKUP_DEST*>

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

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

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

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

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

Back up Non-database Files

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

Recover Database

To recover a database, do the following:

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

./prime.sh stop

Step 2 To recover a database, you can execute the following from the location $PRIMEP_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:

"Mar 09 2010 15:25:00"

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

Note Do not stop the Oracle Listener during restore.

Standby System for Prime Provisioning (Secondary System)

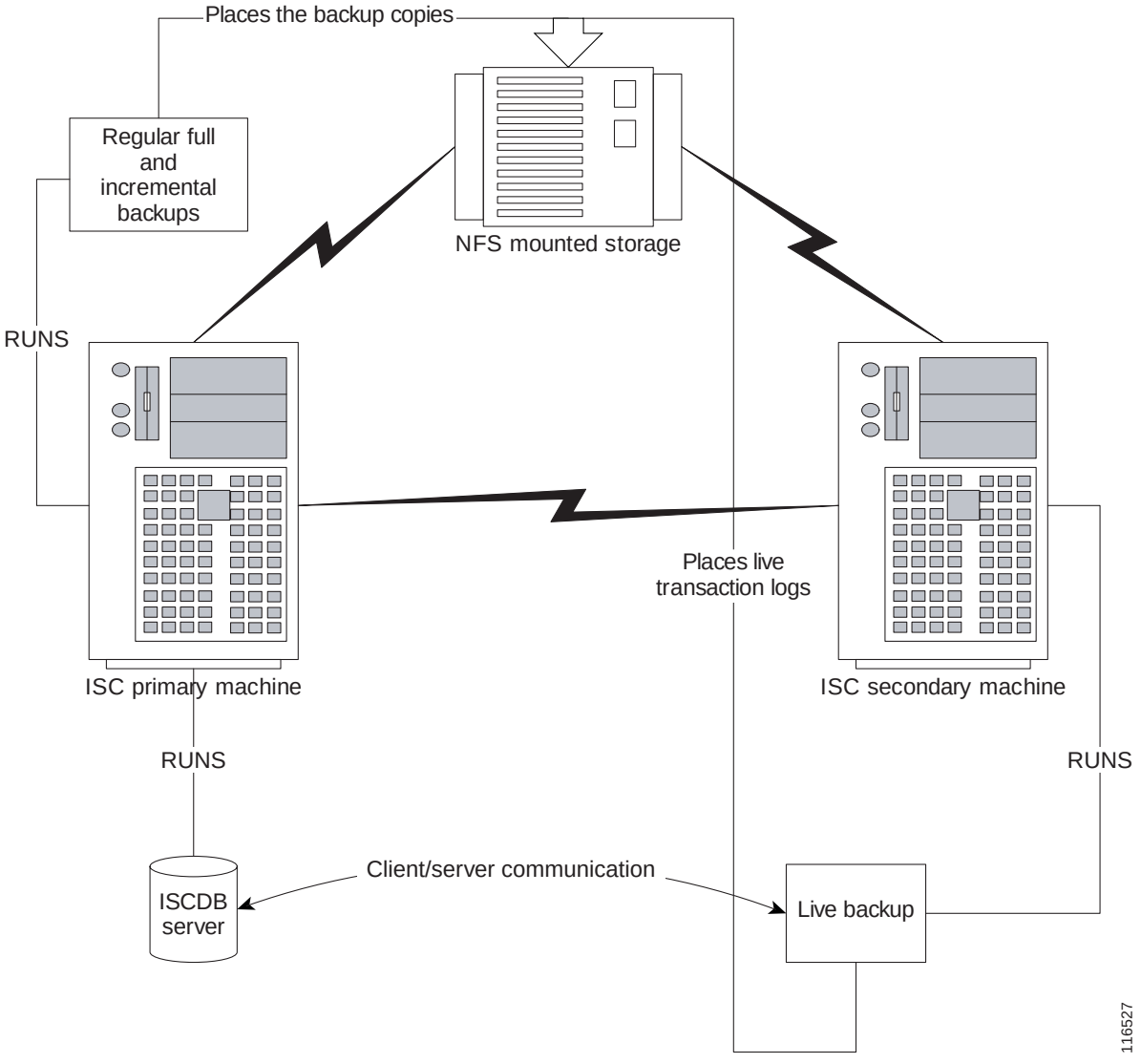
This section explains how to set up Sybase and Oracle standby systems for Prime Provisioning.

The subsections are:

Sybase Standby System Process Overview

Figure 4-10 shows a live backup scheme.

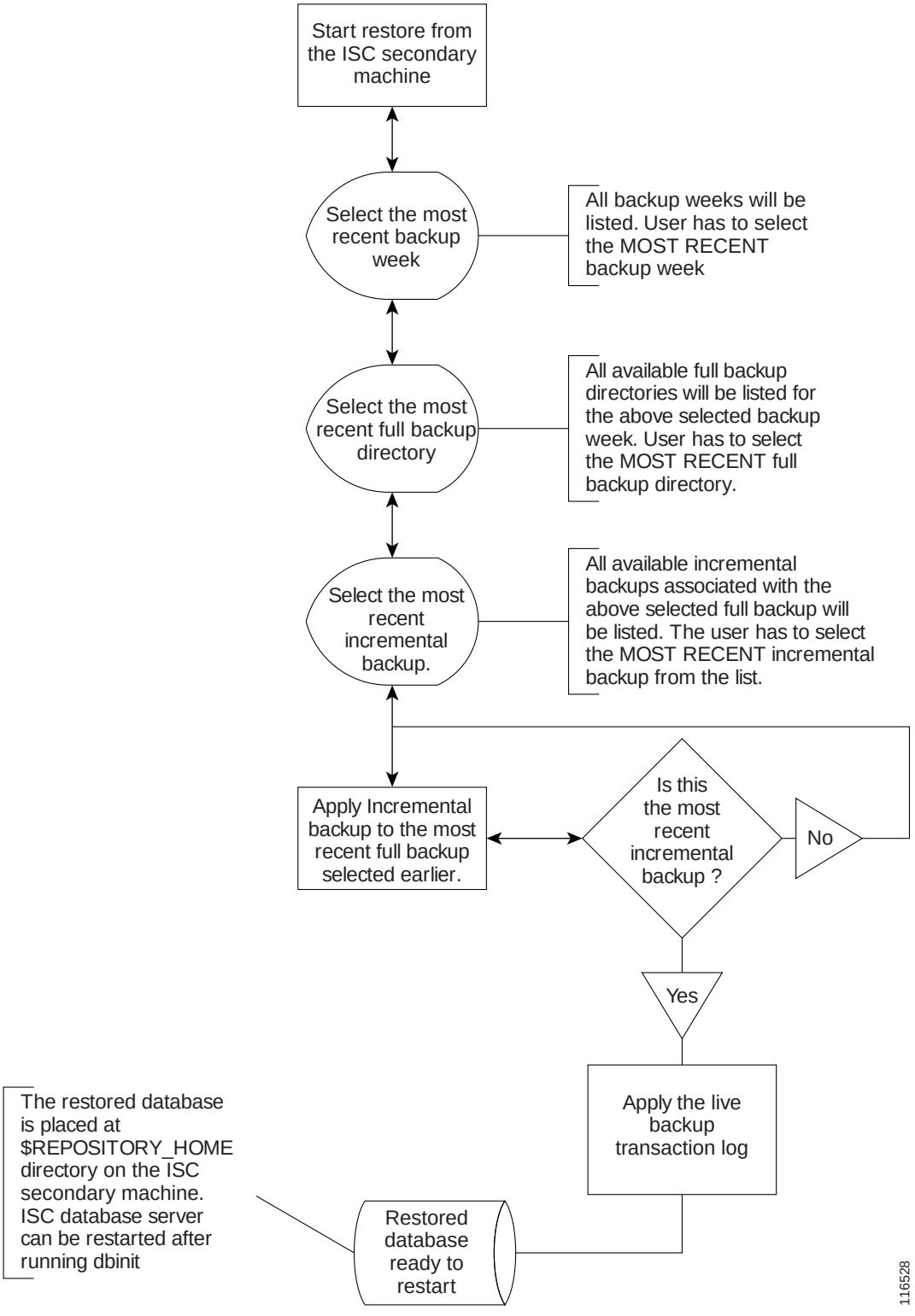
Figure 4-10 Live Backup Scheme



Restore from Live Backup

Figure 4-11 shows the process flow for how to restore from a live backup.

Figure 4-11 Restore from Live Backup



Sybase Standby System Set Up

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

- Running Live Backup of Prime Provisioning Databases, page 4-26
- How to Restore the Database from the Live Backup, page 4-26

Running Live Backup of Prime Provisioning Databases

Run <*BACKUP_INSTALL_DIR*>/**BackupRestore/scripts/asa_liveBackup.sh** from the Prime Provisioning secondary system to start the live backup after being sure to follow these preconditions:

Step 1 Set up a standby Prime Provisioning system.

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

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

Step 4 Prime Provisioning software should be installed on the secondary system and the version of Prime Provisioning 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 backup should be started from the secondary system only, you should not run the live backup from Prime Provisioning 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 backup on the standby system before starting the live backup for the first time.

Step 9 The Prime Provisioning database server must be running on the primary Prime Provisioning host before starting the live backup on the standby system.

Step 10 The live backup stops when the Prime Provisioning database server is stopped and should be restarted after restarting Prime Provisioning.

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

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

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

How to Restore the Database from the Live Backup

When the primary Prime Provisioning host fails, the standby system restores the database from the latest available full backup, the latest incremental backup, and the live backup.

Run the <*BACKUP_INSTALL_DIR*>/**BackupRestore/script/asa_restoreFromLiveBackup.sh** script on the standby system to restore the database after being sure to follow these preconditions:

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 backup and the latest associated incremental backup.

Step 3 Run the restore from the standby machine.

Oracle Standby System Set Up

Prime Provisioning 6.0 supports both physical standby and logical standby in Oracle 10g Data Guard. For information about the Oracle 10g standby concept and configuration, see the *Oracle Data Guard Concept and Administration 10g Release 1 (10.1)* Part No. B10823-01. The document can be found at Oracles' website.

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

./prime.sh stop -y

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

execute applycfg.sh

./prime.sh initdb.sh

./prime.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.

Prime Provisioning Runtime Configuration Information

This chapter explains the following Prime Provisioning information for runtime configuration:

Default TCP Port Values and Protocol Directions Used by Prime Provisioning

Prime Provisioning uses various Transmission Control Protocol (TCP) ports during its operation. Most TCP ports are configured during the installation. All other ports besides the ones mentioned in this section, can be safely turned off if required.

Note To list the ports and their respective Process names (or PIDs) currently used by Prime Provisioning, navigate to the Prime Provisioning Installation directory and execute the command: **./prime.sh listProcess**

Table 5-1 and Table 5-2 specify the most vital TCP primary and optional ports, respectively, their default values, and the direction.

Table 5-1 Prime Provisioning Primary TCP Ports, Their Default Values, and Direction

TCP Primary Ports (listed alphabetically)	Default Values	Direction	Notes
HTTP	8030	Web browser to Prime Provisioning	Used for Web GUI and NBI
Tomcat	8005	Web browser to Prime Provisioning	Used by Tomcat

Table 5-2 Prime Provisioning Optional TCP Ports, Their Default Values, and Direction

TCP Optional Ports (listed alphabetically)	Default Values	Direction	Notes
HTTPS	8443	Web browser to Prime Provisioning	If HTTPS is activated
Naming Port	1030	Web browser to Prime Provisioning	If Naming Port is required
RMID	1098	Web browser to Prime Provisioning	If RMID configuration is required
Sybase	2630	Prime Provisioning to Sybase server	Used by the Sybase database
Oracle	1521	Prime Provisioning to Oracle Server	If Oracle database is used

The value selected during the installation can be retrieved from the file **$PRIMEP_HOME/etc/install.cfg**. Most of these ports only need to be allowed if you are allowing users to access Prime Provisioning from outside your firewall.

Prime Provisioning uses or can use the protocols specified in Table 5-3 to communicate with the routers under its configuration control.

Note The selected protocol for each of the following categories must be able to pass through any firewalls between Prime Provisioning and the devices:
1. Terminal Session Protocol - **default: Telnet**; SSH; CNS*; rsh
2. Configuration Access Protocol - **default: selected Terminal Session Protocol**; TFTP; FTP; rcp
3. SNMP - **default: SNMPv1/v2c**; SNMPv3
* CNS is a transport mechanism that uses the TIB/Rendezvous event bus to communicate with a Cisco Configuration Engine server..

Table 5-3 Protocols and Directions with Prime Provisioning

Protocols (listed alphabetically)	Directions
FTP	Devices to FTP server
NFS	Between Prime Provisioning and TFTP or FTP server if server is on a different machine. (Can be blocked if you do not use FTP or TFTP.)
rcp	Prime Provisioning to devices
rsh	Prime Provisioning to devices
SSH	Prime Provisioning to devices
SSHv2	Prime Provisioning to devices
SNMP	Prime Provisioning to devices
SNMPv3	Prime Provisioning to devices
Telnet	Prime Provisioning to devices
TFTP	Devices to TFTP server

Note Device creation is explained in the chapter Service Inventory—Inventory and Connection Manager, in the *Cisco Prime Provisioning 6.5 User Guide*.

Table 5-4 lists some important administrative ports and their respective protocols.

Table 5-4 Prime Provisioning Administrative Ports and Their Respective Protocals

Port	Protocol	Notes
20	FTP Data	For transfering FTP data
21	FTP Control	For starting the FTP connection
22	SSH	For secure remote administration which uses SSL to encrypt the transmission
23	Telnet	For insecure remote administration
25	SMTP	Mail Transfer Agent for e-mail servers such as SEND mail
53	DNS	Special servers which use both TCP and UDP.
161	SNMP	For network monitoring

Command-Line Interfaces Used by Prime Provisioning

This section specifies the command-line interfaces (CLIs) used by Prime Provisioning. This list gives commands supported in IOS and IOS XR unless otherwise indicated:

- commit (not supported in IOS)
- configure exclusive (not supported in IOS)
- config term
- copy (many variations)
- enable (not supported in IOS XR)
- end
- exit
- ping [vrf]
- reload
- show diag (not supported in IOS XR)
- show diags (not supported in IOS)
- show etherchannel port (not supported in IOS XR)
- show interfaces switchport (not supported in IOS XR)
- show modules (not supported in IOS XR)
- show port (not supported in IOS XR)

- show running
- show startup (not supported in IOS XR)
- show ver
- term (length, width, editing) (editing not supported in IOS XR)
- write mem (not supported in IOS XR)
- [no] logging console

WatchDog Commands

The WatchDog is responsible for bootstrapping Prime Provisioning and starting the necessary set of server processes. In addition, the WatchDog monitors the health and performance of each server to ensure it is functioning properly. In the event of a software error that causes a server to fail, the WatchDog automatically restarts the errant server.

The WatchDog is a background daemon process that is automatically installed as part of the installation procedure for Prime Provisioning. After the installation procedure has completed, WatchDog is started automatically. You can execute the **startwd** command to run the WatchDog after the installation. The WatchDog can be configured to automatically start any time the machine is rebooted.

In addition to the commands that are specified in this chapter, in the product you can choose **Administration > Control Center > Hosts** and from there you can start, stop, restart, and view log files for the individual Prime Provisioning servers.

This chapter provides the description, syntax, and arguments (listed alphabetically) for the following WatchDog commands:

startdb Command

This section provides the description and syntax for the **startdb** command.

Description

The **startdb** command starts the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startdb

The **startdb** command has no arguments and starts the database.

The location of **startdb** is: <*Prime Provisioning Directory*>**/bin**.

Note Do *not* run **startdb** in the background. Do *not* enter **startdb &**.

startns Command

This section provides the description and syntax for the **startns** command.

Description

The **startns** command starts the name server. The **orbd** process provides the name server functionality. **orbd** (from JDK) is required, but **startwd** starts it if it is not already running. The **startns** and **stopns** commands deal with **orbd**.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startns

The **startns** command has no arguments and starts the name server.

The location of **startns** is: <*Prime Provisioning Directory*>**/bin**.

startwd Command

This section provides the description and syntax for the **startwd** command.

Description

The **startwd** command starts the WatchDog and all Prime Provisioning processes. The **startwd** command includes the functionality of **startdb** (see the "startdb Command" section on page 6-1) and **startns** (see the "startns Command" section on page 6-2). Executing this command is a necessary procedure and occurs automatically as part of the installation. Use this **startwd** command after issuing a **stopwd** command to restart the WatchDog.

If for some reason the Prime Provisioning host is stopped, either inadvertently or by issuing the **stopwd** command, it can be restarted by using the **startwd** command.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startwd

The **startwd** command has no arguments and starts the WatchDog only for the machine where it is executed.

The location of **startwd** is: <*Prime Provisioning Directory*>**/bin**

Note Do *not* run **startwd** in the background. Do *not* enter **startwd &**.

stopall Command

This section provides the description and syntax for the **stopall** command.

Description

The **stopall** command stops the database, name server, and WatchDog on the machine on which it is run. The **stopall** command includes the functionality of **stopdb -y** (see the "stopdb Command" section on page 6-3), **stopns -y** (see the "stopns Command" section on page 6-4), and **stopwd -y** (see the "stopwd Command" section on page 6-4). Normally this is only necessary before installing a new version of Prime Provisioning.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopall

Caution There is no **-y** parameter. Therefore, everything stops without the ability to cancel.

The location of **stopall** is: <*Prime Provisioning Directory*>**/bin**.

stopdb Command

This section provides the description and syntax for the **stopdb** command.

Description

The **stopdb** command stops the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopdb [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the database?” You are then prompted to reply **yes** or **no**.

The location of **stopdb** is: <*Prime Provisioning Directory*>**/bin**.

stopns Command

This section provides the description and syntax for the **stopns** command.

Description

The **stopns** command stops the name server. The **startns** and **stopns** commands deal with **orbd**.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopns [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the nameserver?” You are then prompted to reply **yes** or **no**.

The location of **stopns** is: <*Prime Provisioning Directory*>**/bin.**

stopwd Command

This section provides the description and syntax for the **stopwd** command.

Description

The **stopwd** command stops the WatchDog and all Prime Provisioning processes other than the name server and the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopwd [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the watchdog and all of its servers? Other users may be using this system as well. No activity (for example: collections, performance monitoring, provisioning) occurs until the system is restarted.” You are then prompted to reply **yes** or **no**.

The location of **stopwd** is: <*Prime Provisioning Directory*>**/bin**.

wdclient Command

This section provides the description, syntax, and options (listed alphabetically) for the **wdclient** subcommands. These subcommands are diagnostic tools. This section also describes the column format of the output of each of the subcommands.

Note The location of **wdclient** is: <*Prime Provisioning Directory*>**/bin**.

The following are the **wdclient** subcommands:

Note If you enter **wdclient -help**, you receive a listing of all the wdclient subcommands.

wdclient disk Subcommand

This section provides the description and syntax for the **wdclient disk** subcommand.

Description

The **wdclient disk** subcommand gives the disk space statistics for the directories where Prime Provisioning is installed.

Syntax

wdclient disk

wdclient group <*group_name*> Subcommand

This section provides the description and syntax for the **wdclient group** <***group_name***> subcommand.

Description

The **wdclient group** <***group_name***> subcommand lists the servers in the specified server group. Server groups provide a convenient way to start or stop a group of servers with a single command.

Syntax

wdclient group <*group_name*>

where:

<*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient groups Subcommand

This section provides the description and syntax for the **wdclient groups** subcommand.

Description

The **wdclient groups** subcommand lists all the active server groups.

Syntax

wdclient groups

wdclient health Subcommand

This section provides the description and syntax for the **wdclient health** subcommand.

Description

The **wdclient health** subcommand indicates whether all the servers are stable.

Syntax

wdclient health

wdclient restart Subcommand

This section provides the description and syntax for the **wdclient restart** subcommand.

Description

The **wdclient restart** subcommand restarts one or more servers. Any dependent servers are also restarted.

Note It is not necessary to restart servers in a properly functioning system. The **wdclient restart** command should only be run under the direction of Cisco Support.

Syntax

wdclient restart [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments:

all is all servers. This is the default if no argument is specified.

<*server_name*> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 6-1, "Servers and Their Functions," for server descriptions.

group <*group_name*> where, <*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient start Subcommand

This section provides the description and syntax for the **wdclient start** subcommand.

Description

The **wdclient start** subcommand starts one or more servers. Other servers that depend on the specified server(s) might also start.

Note It is not necessary to stop and start servers in a properly functioning system. The **wdclient start** command should only be run under the direction of Cisco Support.

Syntax

wdclient start [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments:

all is all servers. This is the default if no argument is specified.

<*server_name*> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 6-1, "Servers and Their Functions," for server descriptions.

group <*group_name*> where, <*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient status Subcommand

This section provides the description, syntax, and information produced for the **wdclient status** subcommand.

Description

The **wdclient status** subcommand lists all the servers and their states. See Table 6-1 on page 6-8, "Servers and Their Functions," for server descriptions. See Table 6-2 on page 6-9, "Valid States," for the list of all the states.

Syntax

wdclient [**-poll** <*seconds*>] **status**

where:

-poll <*seconds*> is an optional parameter. <*seconds*> is the number of seconds. A number other than zero indicates that when new status data is available it is displayed every <*seconds*> seconds, where <*seconds*> is the specified number of seconds. The default **-poll** value is zero (0), which shows the status just once.

Information Produced: Name Column

The **Name** column provides the name of each of the servers. Table 6-1 provides a list of the servers and a description of the function that each server provides.

Table 6-1 Servers and Their Functions

Server	Function
cnsserver	Handles TIBCO messages from Cisco Configuration Engine servers and takes appropriate actions.
dbpoller	Monitors database server.
discovery	Devices and Service Discovery Engine.
httpd	Web server.
nspoller	Monitors name service.
rgserver	Executes various Prime Provisioning traffic engineering computations, such as tunnel repairing.

Note The processes that no longer exist includes dispatcher, lockmanager, scheduler, and worker.

Information Produced: State Column

The **State** column provides the current state of the server. Table 6-2 provides a description of each of the states in normal progression order.

Table 6-2 Valid States

State	Description
start_depends	This server has been asked to start, but is waiting for servers it depends on to start. After all dependent servers have started, this server transitions to the state of starting.
starting	This server is currently starting. After a successful heartbeat occurs, this server transitions to the state of started.
started	This server is currently started and running.
stop_depends	This server is supposed to be stopped, but it is waiting for servers it depends on to be stopped first.
stopping_gently	This server is in the process of stopping in a gentle fashion. That is, it was notified that it is to stop.
stopping_hard	This server is in the process of being killed because either it did not have a way to stop gently or because the gentle stop took too long.
stopped	This server is stopped. The WatchDog either starts it again or disables it if it has been frequently dying.
disabled_dependent	This server is disabled because one or more servers it depends on are disabled. If all servers it depends on are started, this server automatically starts.
disabled	This server is disabled and must be manually restarted.
restart_delay	This server is delaying before restarting. There is a short delay after a server stops and before it is restarted again.

Information Produced: Gen Column

The **Gen** column provides the generation of the server. Each time the server is started, the generation is incremented by 1.

Information Produced: Exec Time Column

The **Exec Time** column provides the date and time the server was last started.

Information Produced: Success Column

The **Success** column provides the number of successful heartbeats since the server was last started. Heartbeats are used to verify that servers are functioning correctly.

Information Produced: Missed Column

The **Missed** column provides the number of missed heartbeats since the server was last started.

A few missed heartbeats could simply indicate the system was busy. However, more than a couple of missed heartbeats per day could indicate a problem. See the logs to diagnose the reason.

Three missed heartbeats in a row is the default for restarting the server.

wdclient stop Subcommand

This section provides the description and syntax for the **wdclient stop** subcommand.

Description

The **wdclient stop** subcommand stops one or more servers. Other servers that depend on the specified servers also stop.

Note It is not necessary to stop servers in a properly functioning system. The **wdclient stop** command should *only* be run under the direction of Cisco Support.

Syntax

wdclient stop [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments.

all is all servers. This is the default if no argument is specified.

<*server_name*> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 6-1, "Servers and Their Functions," for server descriptions.

group <*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.