Back Up and Restore of ISC Repository and Standby System

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

Back Up and Restore of ISC Repository

The CCO location of scripts for these procedures is:

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

The subsections are:

Data Items Included in Back Up and Recovery

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

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

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

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

Guidelines

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

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

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

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

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

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

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

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

Step 4 Create archive backup copies on a tape device.

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

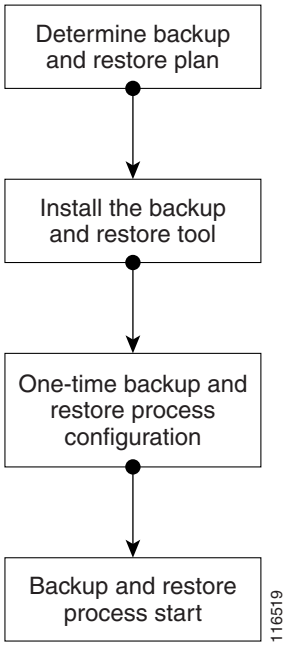
Sybase Backup and Restore Process Overview

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

Overview of the Backup and Restore Process

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

Figure C-1 Overview - Sybase ASA Backup and Restore



Planning your Backup and Restore Process

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

Step 1 Determine the frequency for full backups.

Step 2 Determine the frequency for incremental backups.

Step 3 Determine the location for storing the backups.

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

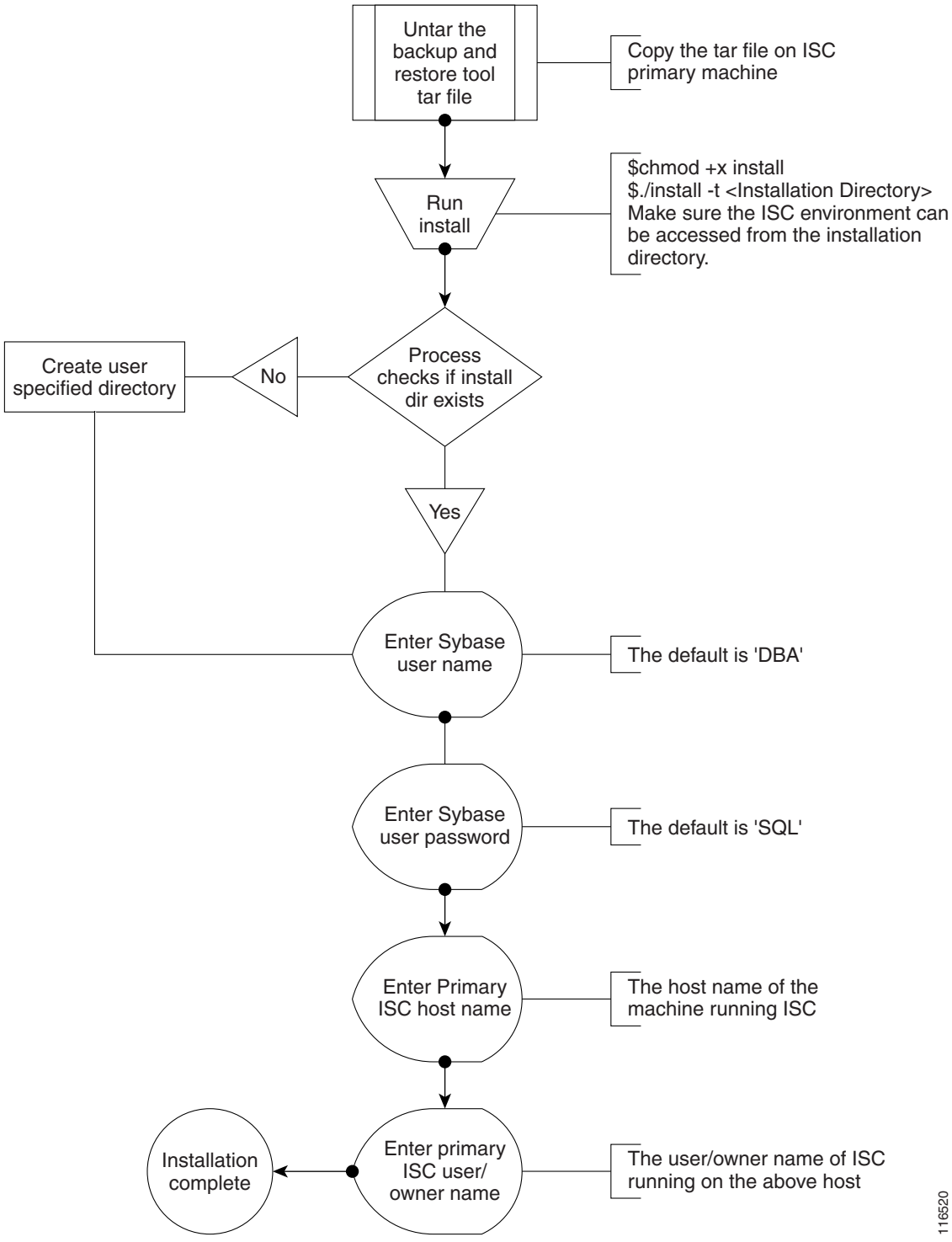
Step 4 Document the information for Step 1 to Step 3.

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

Installing the Backup and Restore Tool

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

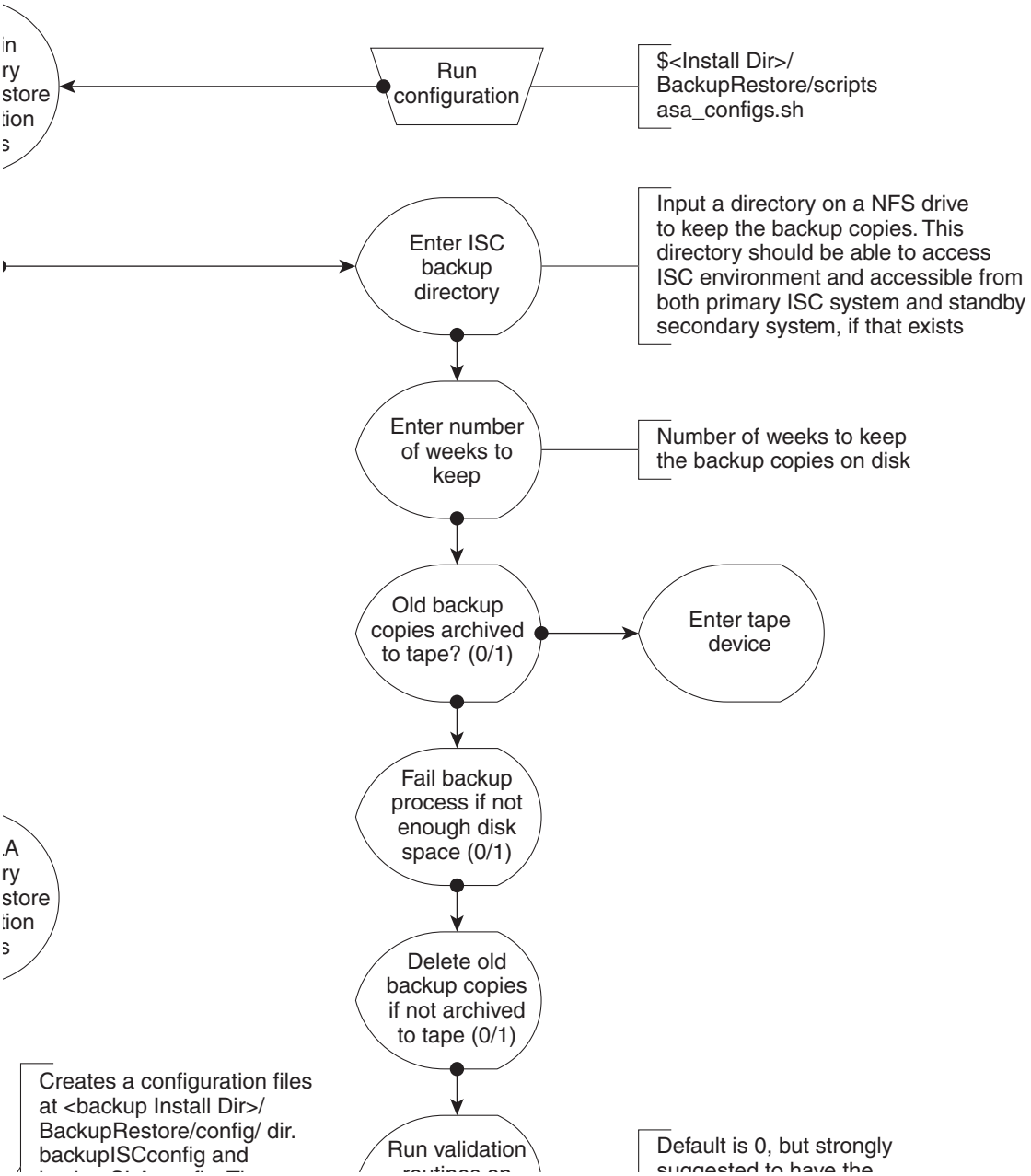
Figure C-2 Installing the Backup and Restore Tool



Configuring the Backup and Restore Process

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

Figure C-3 One-Time Configuration Process Flow



Understanding the Backup Process Flow

This section contains the following sections:

Preconditions

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

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

Functions

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

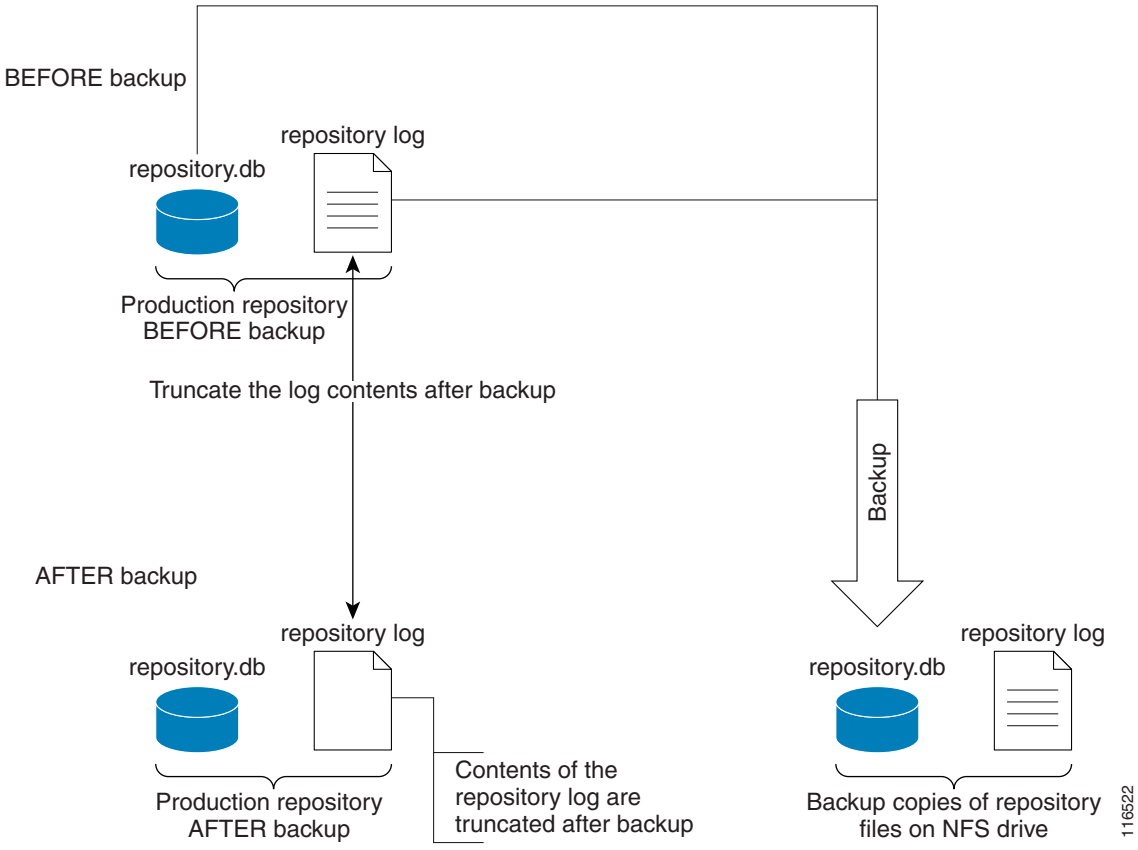
Note Do not modify, rename, delete, or move the directory structure created by the backup tool.

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

Full Backup Scheme

Figure C-4 shows a full backup scheme.

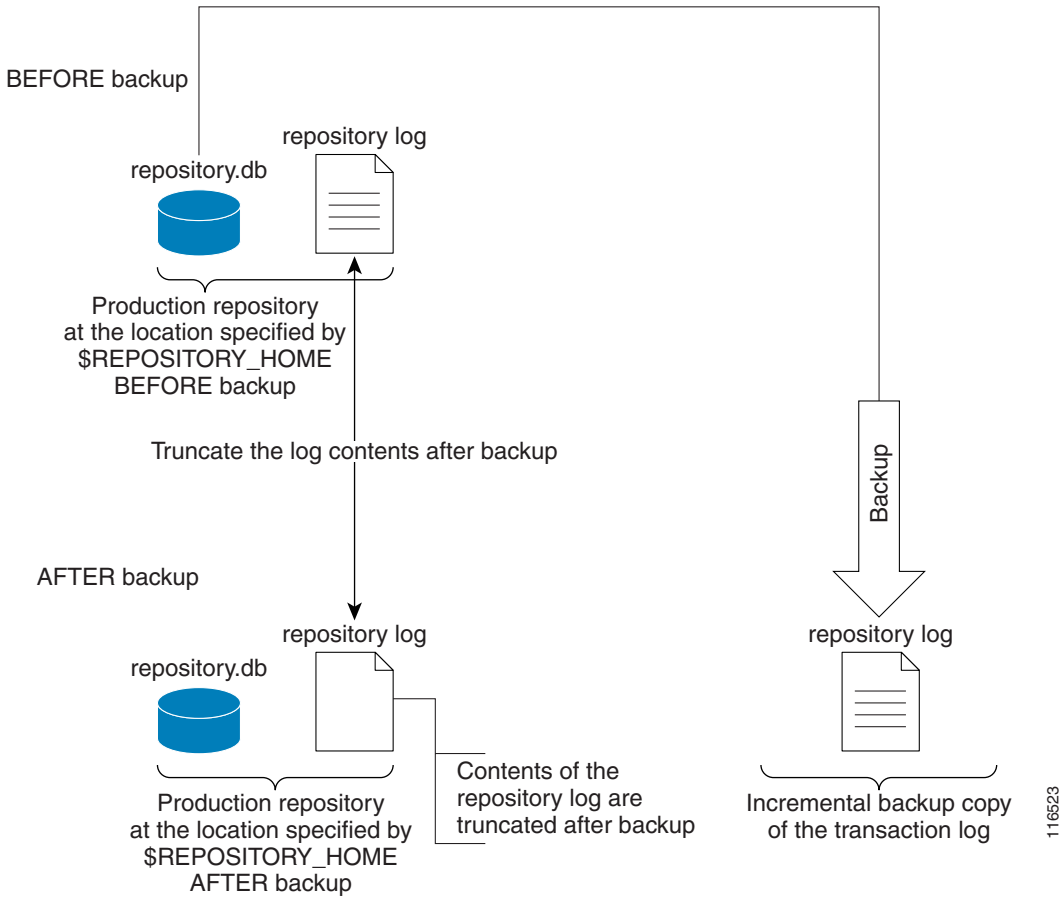
Figure C-4 Full Backup Scheme



Incremental Backup Scheme

Figure C-5 shows an incremental backup scheme.

Figure C-5 Incremental Backup Scheme



Typical Backup Directory Structure

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

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

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

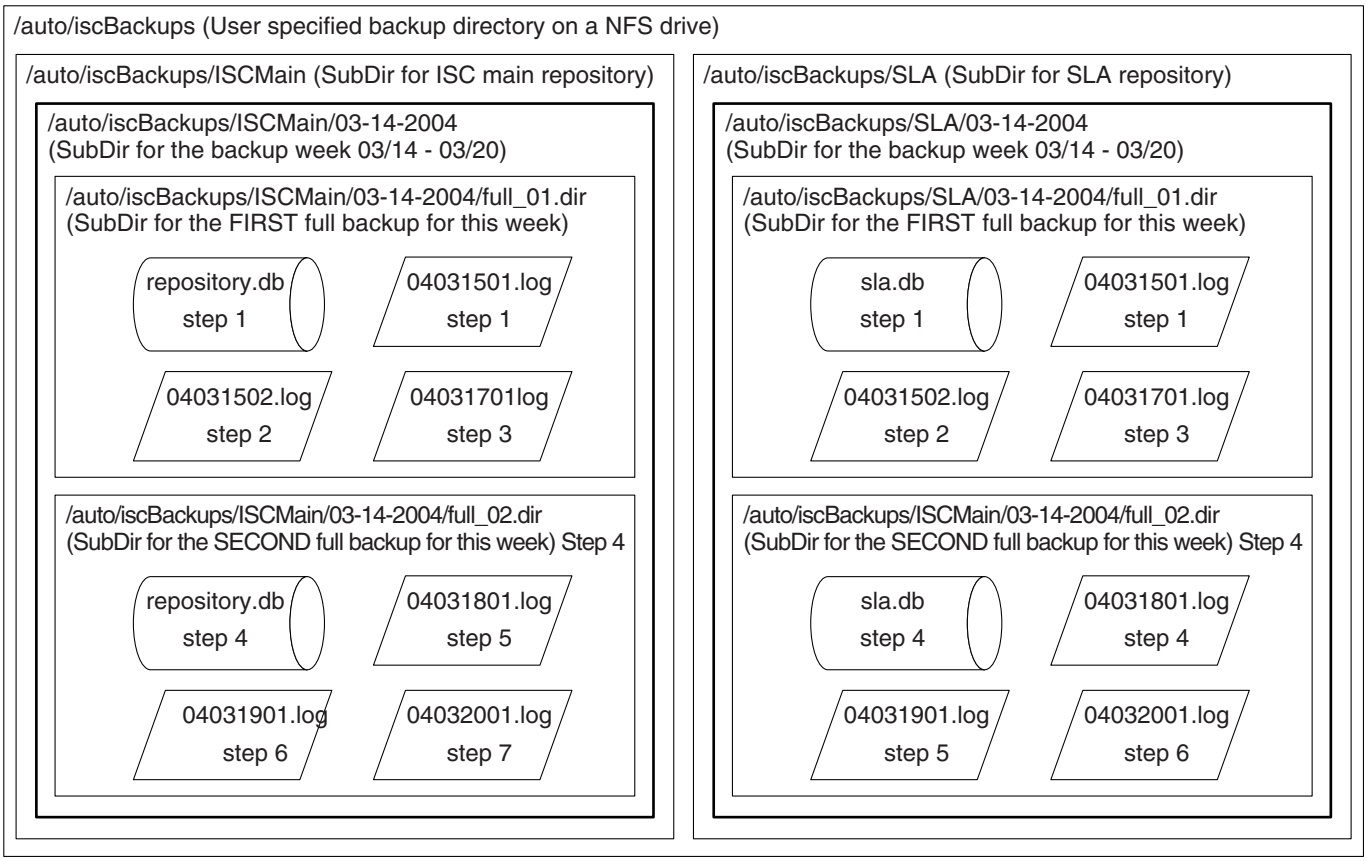
Note Configuration setting, full backup reset to 0.

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

Note Backup Week ended on 03/20/2004

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

Figure C-6 Typical Backup Directory Structure



Understanding the Restore Process Flow

This section contains the following sections:

Preconditions

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

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

Functions

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

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

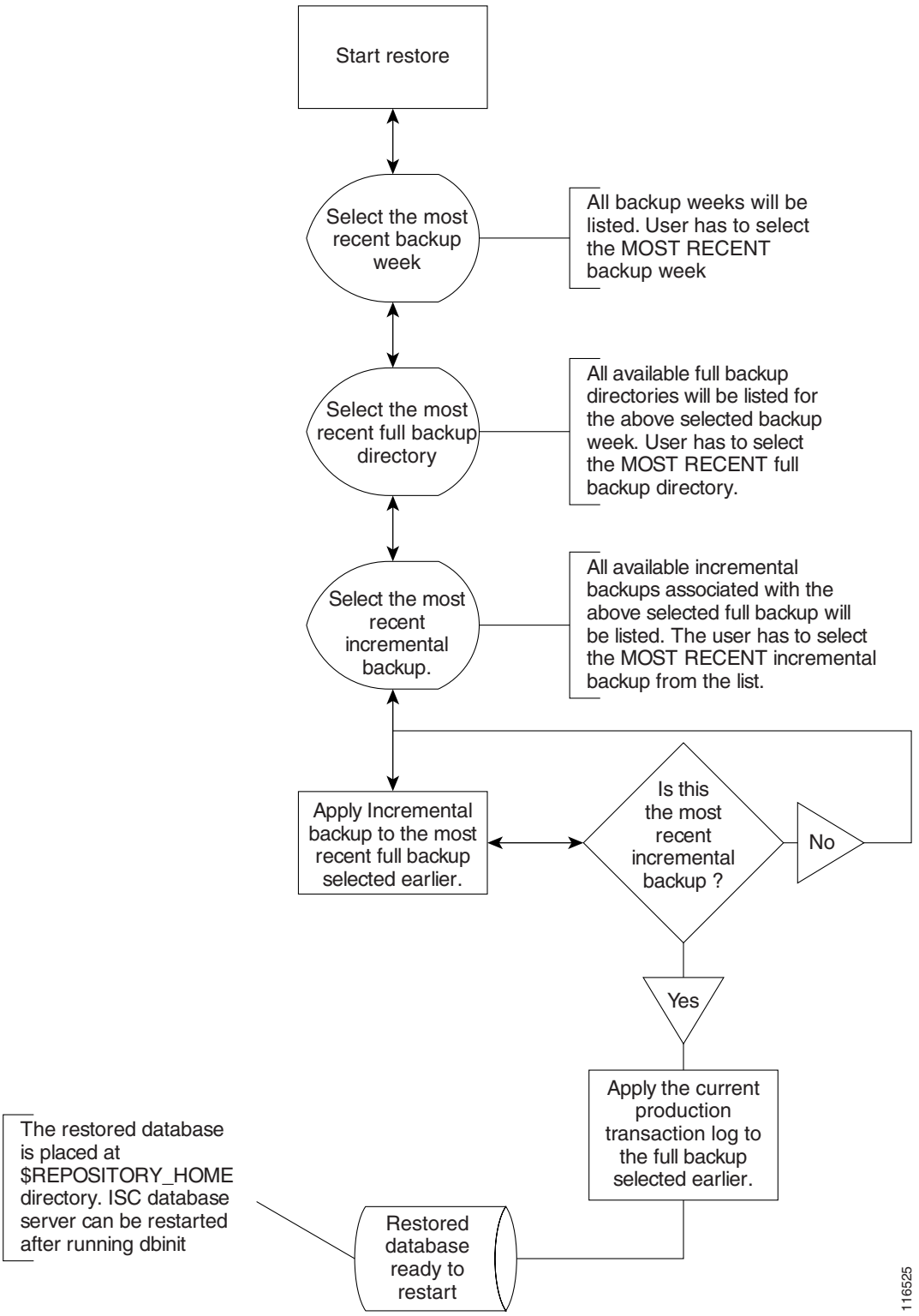
Note Please see Sybase ASA documentation for more information.

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

Restore from Media Failure

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

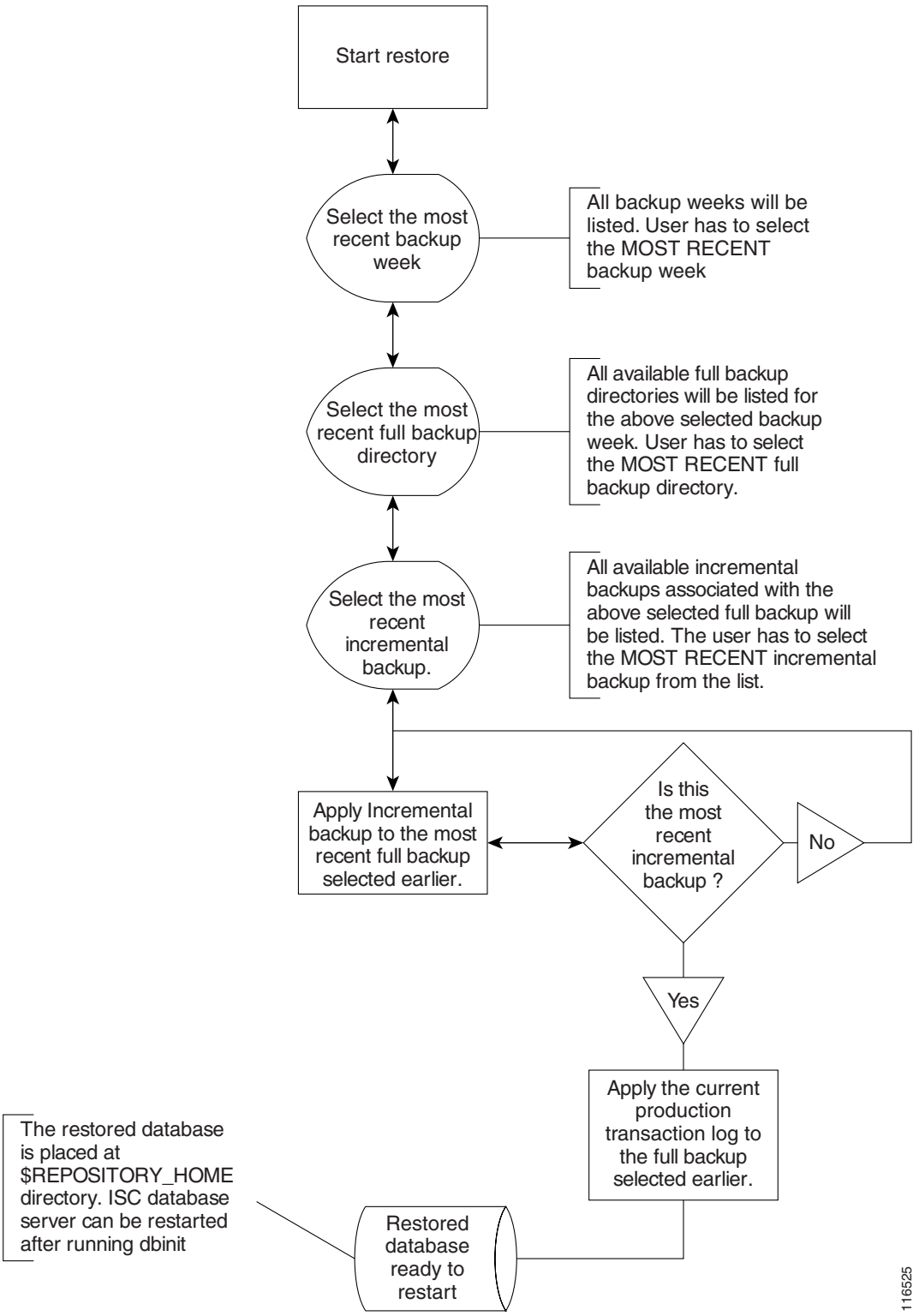
Figure C-7 Restore from Media Failure on the Database File (.db)



Restore to a Desired Point-in-Time

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

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



Sybase Database Back Up and Restore

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

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

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

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

Installing

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

mkdir -p $ISC_HOME/backup/Sybase

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

Step 2 **chmod +x install**

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

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

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

Sample Install Prompts and User Responses

The following is a sample install session:

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

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

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

Post Install Status

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

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

Functionality of Backup and Restore Tool

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

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

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

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

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

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

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

Post Configuration status

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

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

How to Use the Backup Script

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

- **a.** The back up should be made while the ISC database server is running. There is no need to stop ISC to back up the database.
- **b.** The backup directory path specified during the configuration process should ideally be on an NFS device.

  It is important to keep the backup copies on an external storage device to protect the backup copies if the main ISC system crashes.
- **c.** Install the Backup and Restore tool and implement the periodic backup tasks from the primary ISC host machine. However, the backup task can be carried out from a secondary system, provided the following conditions are met:
  - The main ISC and SLA repository files should be placed on an NFS device accessible from the primary ISC host system and the secondary ISC host system.
  - The hardware and software configuration of the secondary system should be the same as the ISC primary host system.
  - The same version of ISC should be installed on both the primary and secondary systems.
  - The Backup and Restore tool should be installed on the secondary ISC system.

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

Behavior of the Backup Process

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

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

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

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

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

How to Restore the Database from the Back Up

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

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

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

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

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

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

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

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

Oracle Database Back Up and Restore

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

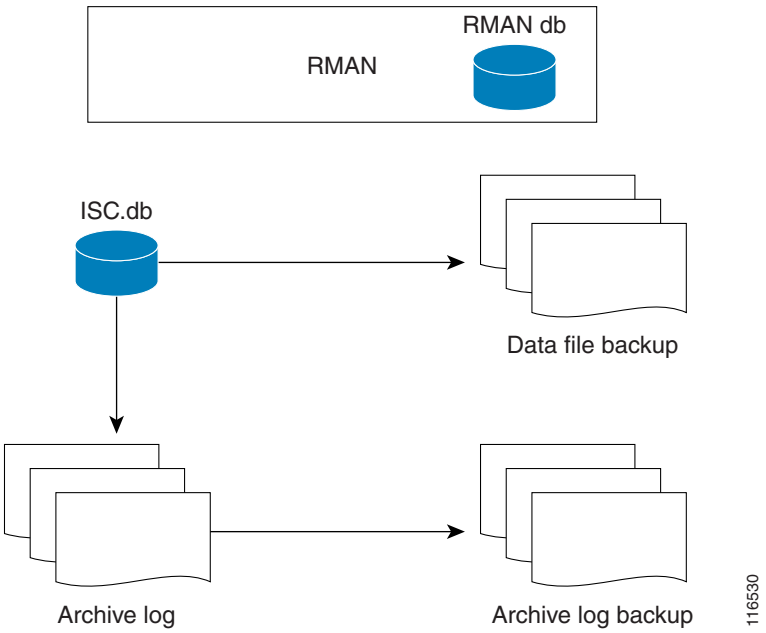
mkdir -p $ISC_HOME/backup/Oracle

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

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

Figure C-9 shows an Oracle Database Backup Diagram.

Figure C-9 Oracle Database Backup



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

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

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

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

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

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

Step 1 Turn On ARCHIVELOG Mode, page C-21

Step 2 Create RMAN Catalog Database, page C-21

Step 3 Create RMAN User, page C-21

Step 4 Create RMAN Catalog, page C-22

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

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

Step 7 Backup Database, page C-22

Step 8 Recover Database, page C-23

Turn On ARCHIVELOG Mode

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

Step 1 First, turn on the archive log mode:

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

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

Step 2 Copy the data files regularly:

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

  SQL> **select file_name from dba_data_files;**

Step 3 To recover, enter the following:

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

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

Create RMAN Catalog Database

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

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

Create RMAN User

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

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

Create RMAN Catalog

Create a catalog from the RMAN command prompt:

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

RMAN> **create catalog;**

Register the ISC Database with the RMAN Catalog

Set the ORACLE_SID environment variable = isc.

%**rman**

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

RMAN > **connect target sys/change_on_install**

RMAN > **register database;**

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

Modify ISC Database Initial Parameter File

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

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

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

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

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

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

startup mount

alter database archivelog;

alter database open

Step 3 Check the archive log mode, as follows:

SQL> **archive log list;**

Backup Database

To back up the database, do the following:

Step 1 Download the software for backup and restore from:

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

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

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

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

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

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

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

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

Backup Non-database Files

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

Recover Database

To recover a database, do the following:

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

stopall

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

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

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

"Oct 09 2003 15:25:00"

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

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

Standby System for ISC (Secondary System)

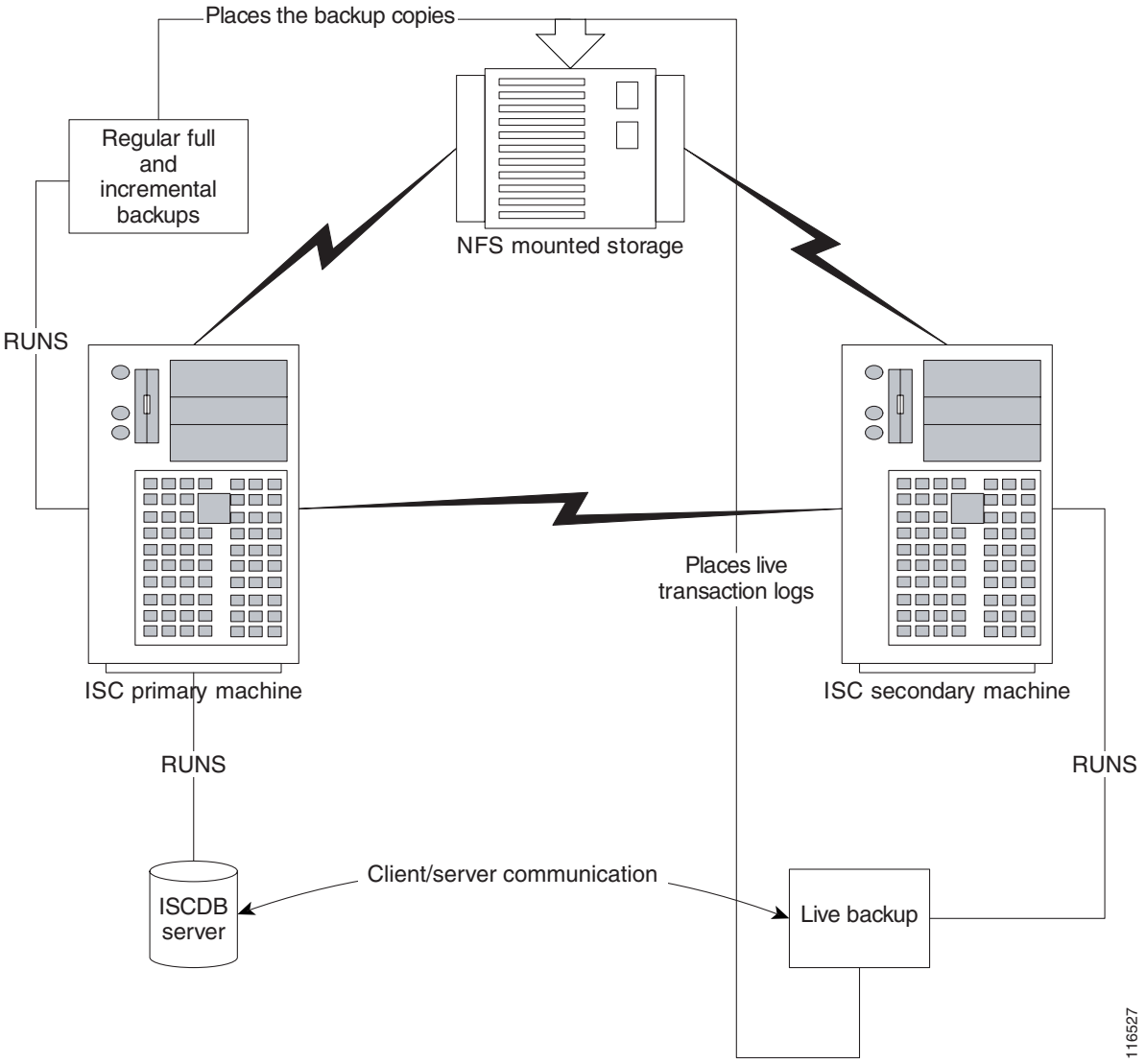
This section explains how to set up Sybase and Oracle standby systems for ISC.

The subsections are:

Sybase Standby System Process Overview

Figure C-10 shows a live backup scheme.

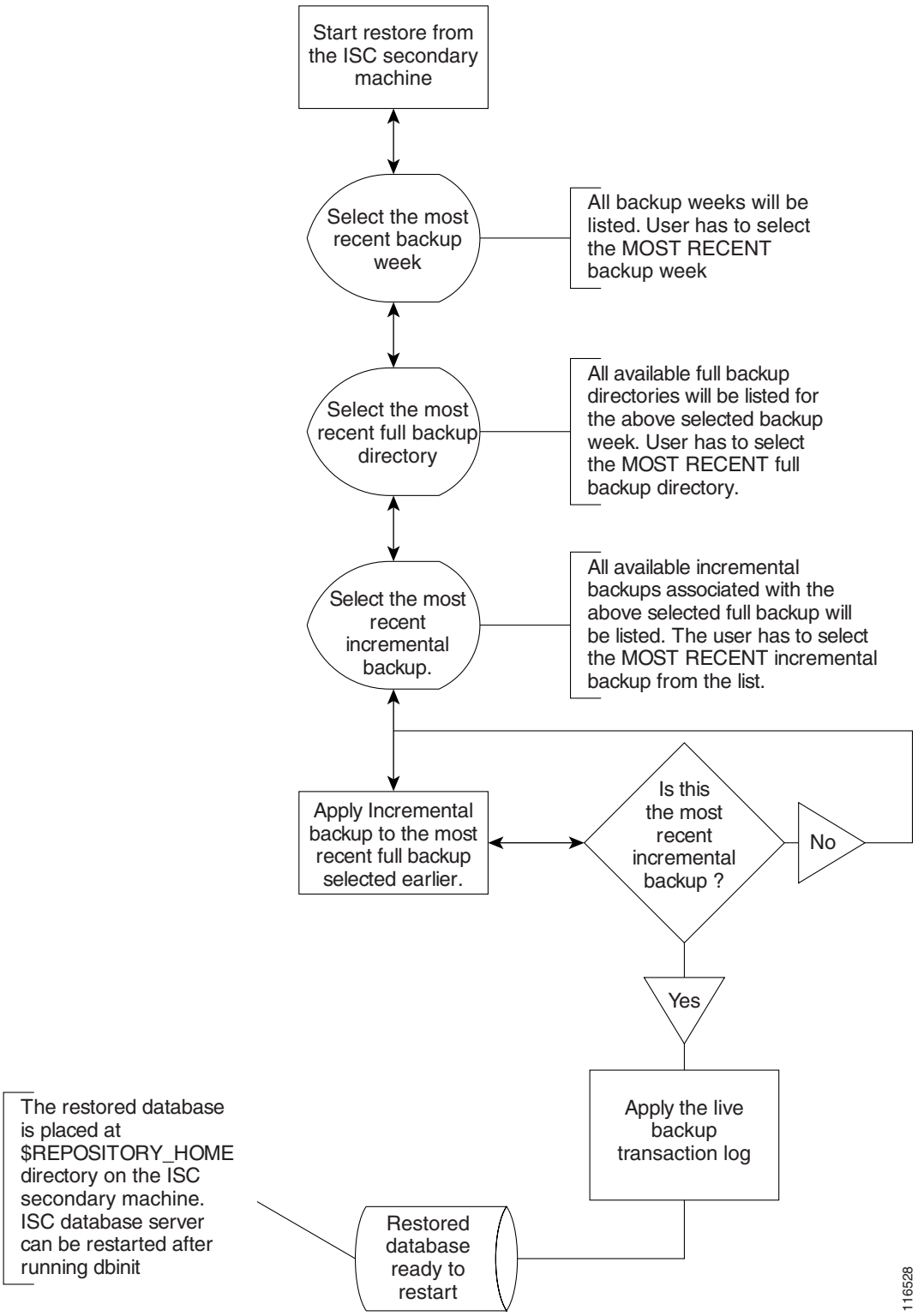
Figure C-10 Live Backup Scheme



Restore from Live Backup

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

Figure C-11 Restore from Live Backup



Sybase Standby System Set Up

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

Running Live Back Up of ISC Databases

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

Step 1 Set up a standby ISC system.

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

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

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

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

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

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

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

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

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

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

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

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

How to Restore the Database from the Live Back Up

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

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

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

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

Step 3 Run the restore from the standby machine.

Oracle Standby System Set Up

For Oracle 9i Data Guard instructions, see:

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

Note ISC only supports physical standby, not logical standby.

Restart ISC

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

stopall -y

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

execute applycfg.sh

initdb.sh

startwd

where:

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

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