

Disaster Recovery on the Sun Cobalt™ Qube 3 Appliance

User Manual



Copyright © 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems, the Sun Logo, Sun Cobalt and the Sun Cobalt Logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Legato NetWorker is a registered trademark of Legato Systems, Inc.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303-4900 États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient des droits de propriété intellectuelle sur la technologie réunie dans le produit qui est décrit par ce document. Ces droits de propriété intellectuelle peuvent s'appliquer en particulier, sans toutefois s'y limiter, à un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et à un ou plusieurs brevets supplémentaires ou brevets en instance aux États-Unis et dans d'autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Sun, Sun Microsystems, le logo Sun, Sun Cobalt et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Legato NetWorker est une marque déposée de Legato Systems, Inc.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Part Number / Numéro de pièce : 070-00337-02

Date : 06-2001

Contents

1 Disaster Recovery on the Sun Cobalt™ Qube 3 Appliance	1
How disaster recovery works	1
Locking the UI databases	2
General steps to perform disaster recovery	3
General notes regarding backup services	4
Knox Arkeia	5
Tailoring the backup service	5
Files associated with Knox Arkeia tailoring	6
Backing up a Sun Cobalt Qube 3 appliance with Knox Arkeia	6
Performing disaster recovery of a Sun Cobalt Qube 3 appliance with Knox Arkeia	7
Preparing for disaster recovery	7
Performing a disaster-recovery operation	8
Legato NetWorker®	9
Tailoring the backup service	9
Files associated with Legato NetWorker tailoring	9
Backing up a Sun Cobalt Qube 3 appliance with Legato NetWorker	10
Performing disaster recovery on a Sun Cobalt Qube 3 appliance with Legato NetWorker	10
Preparing for disaster recovery	10
Performing a disaster-recovery operation	11
Technical note	11

Contents

Veritas NetBackup	12
Tailoring the backup service	12
Files associated with Veritas NetBackup tailoring	12
Backing up a Sun Cobalt Qube 3 appliance with Veritas NetBackup	13
Performing disaster recovery on a Sun Cobalt Qube 3 appliance with Veritas NetBackup	14
Preparing for disaster recovery	14
Performing a disaster-recovery operation	15
Configuring client agents on the Sun Cobalt Qube 3 appliance	16
Configuring Knox Arkeia	16
Configuring Legato NetWorker	17
Configuring Veritas NetBackup	17

Disaster Recovery on the Sun Cobalt™ Qube 3 Appliance

The Sun Cobalt™ Qube 3 appliance supports the use of third-party backup solutions for performing disaster recovery. The supported backup solutions are:

- Knox Arkeia
- Legato NetWorker®
- Veritas NetBackup

Each of these solutions requires customization to correctly recover the Cobalt configuration database in the Cobalt Configuration Engine (CCE). This technical paper describes how disaster recovery works on the Sun Cobalt Qube 3 appliance, the steps required to perform general disaster recovery, and detailed instructions on how to customize and use each of the specific backup solutions.

How disaster recovery works

For the Sun Cobalt Qube 3 appliance, the term *disaster recovery* means restoring the appliance after performing an operating-system (OS) restore operation which wipes the hard drive clean and returns it to a factory-fresh state. This is also known as “bare-metal recovery”. The entire appliance must be restored in order for the configuration database and the machine configuration to be in synchronization.

For most files on the Sun Cobalt Qube 3 appliance, disaster recovery is straightforward: the files are recovered from the backup service and written to the file system. However, the Cobalt Configuration Engine (CCE) requires additional work and the three supported backup services must be tailored to handle it.

The approach used to recover the configuration database using Knox Arkeia and Veritas NetBackup works as follows:

Before a backup operation begins, the pre-backup script `cobalt_prebackup` creates an archive of the configuration database in the directory `/var/cobalt/backups`.

The backup makes a copy of the archive:

```
/var/cobalt/backups/cce.tar
```

When the backup is complete, the post-backup script `cobalt_postbackup` deletes the archive.

During the disaster-recovery process, the entire appliance must be restored. This restores the archive to the directory `/var/cobalt/backups`. When the backup is complete, you must reboot the appliance; the appliance does not reboot automatically. During the reboot process, the `cobalt_restore` startup script detects the archive and restores the configuration database. At this point, everything should be in a consistent state and disaster recovery is complete.

Legato NetWorker works in a different manner: it recovers the database during the file recovery phase since this service permits per-file scripting at both backup and recover time. The `cceasm` script is used for this purpose.

Locking the UI databases

For all types of backup, the database for the Server Desktop user interface (UI) is locked for as short a period of time as possible. For Arkeia and NetBackup, the Server Desktop UI is locked during the pre-backup creation of the database archives. NetWorker locks the Server Desktop UI only during the backup of the CCE database.



Important: Changes to the configuration of the appliance should not be made during the backup of the appliance; otherwise, the configuration of the appliance and the configuration databases may not be synchronized after the disaster-recovery process is complete.

This is also true for modifications to system configurations that do not use the Server Desktop UI. After disaster recovery, the appliance may be in an inconsistent state if the configuration databases and the system configuration files do not agree.

This begs the question: “So why not lock the UI until the backup ends?” Unfortunately, that would entail shutting down CCE for an unknown duration while the machine writes to the backup server. Because this would affect both the responsiveness of the Server Desktop UI and, potentially, WebMail, Sun Microsystems decided against locking the UI for the duration of the backup process.

Sun Microsystems recommends that you schedule backups for times when it is unlikely that system configuration changes are in progress. Partly for this reason, most backup systems automatically schedule backups for the early hours in the morning.

General steps to perform disaster recovery

The general procedure for performing disaster recovery is as follows:

1. Perform an OS restore to wipe the hard disk drive and return the Sun Cobalt Qube 3 appliance to a factory-fresh state.
2. Configure the appliance through the Setup Wizard and return it to the network. The appliance must be able to communicate with the backup server.
3. Through the Server Desktop UI on the appliance, configure the backup service with which you backed up your appliance. The tasks include enabling the backup client and entering a backup server name. The specific configuration information is discussed later in this technical paper.
4. Use the backup solution to perform the recovery.
5. Reboot the appliance.
6. Verify the restoration.

General notes regarding backup services

The following recommendations are stressed for configuring your backup service:

1. Backup systems are very sensitive to time. If possible, configure the appliance to use a network time protocol (NTP) server to set the clock on the appliance.

On the Server Desktop UI, select **Administration > System > Time** to configure the time settings or to specify an NTP server.

2. Backup systems are very sensitive to correct DNS configuration.

Ensure that your appliance has both forward and reverse DNS lookups available to the backup server so that the backup solution functions properly.

For more information on DNS records, see Appendix E in the user manual.

3. Always backup and recover the `/etc` and `/usr/sausalito` directories together.

These directories contain both the appliance configuration and the CCE database. Backing up and recovering these directories at different times can lead to inconsistencies between the configuration of your appliance and the configuration reported in the Server Desktop UI.

Knox Arkeia

Tailoring the backup service

Server-side tailoring is required for Knox Arkeia. Arkeia performs backups with groups of clients called *savepacks*. When adding a Sun Cobalt Qube 3 appliance to a savepack on the Knox Arkeia backup server, the tree options must be modified to use a pre-backup and post-backup command.

To set these parameters, select the appliance from the list of clients in the savepack and edit the tree options for that client.



Important: For the *hostname*, enter the host name only. Do not enter the fully qualified domain name.

1. Next to the option “command before tree”, uncheck the option “Backup tree if command fails”.

2. In the field following this option, enter:

```
hostname: /usr/local/sbin/cobalt_prebackup
```

where *hostname* is the client name of the appliance you are backing up.

3. Next to the option “command after tree”, check the option “Execute if tree backup fails”.

4. In the field following this option, enter:

```
hostname: /usr/local/sbin/cobalt_postbackup
```

where *hostname* is the client name of the appliance you are backing up.

Files associated with Knox Arkeia tailoring

Table 1 lists the files associated with the Knox Arkeia software. These files are located on the Sun Cobalt Qube 3 appliance.

Table 1. Files associated with Knox Arkeia tailoring

Path and file name	Description
<code>/usr/local/sbin/cobalt_prebackup</code>	Script that runs before a backup to create an archive of the CCE database.
<code>/usr/local/sbin/cobalt_postbackup</code>	Script that runs after a backup to delete the archive created by <code>cobalt_prebackup</code> .
<code>/etc/rc.d/init.d/cobalt_restore</code>	Script that runs at startup and detects whether an archive of the configuration database exists. An extant archive is recovered and has its name changed.
<code>/var/cobalt/backups/cce.tar</code>	Archive of the CCE database. It is created by <code>cobalt_prebackup</code> and deleted by <code>cobalt_postbackup</code> . The archive is renamed to <code>restored.cce.tar</code> by <code>cobalt_restore</code> after disaster recovery.

Backing up a Sun Cobalt Qube 3 appliance with Knox Arkeia

To back up your appliance with Knox Arkeia, you must first configure and enable the Arkeia agent on the appliance. For more information, see “Configuring client agents on the Sun Cobalt Qube 3 appliance” on page 16.

Backups are started by using the Knox Arkeia UI. Once a backup of an appliance has begun, the `cobalt_prebackup` script creates the `cce.tar` file in the `/var/cobalt/backups` directory if the tree options for the appliance were configured correctly.



Important: The Sun Cobalt Qube 3 appliance will not restore properly if the tree options do not execute the `prebackup` and `postbackup` commands.

When the backup has successfully completed, the script `cobalt_postbackup` removes the `cce.tar` file.

Performing disaster recovery of a Sun Cobalt Qube 3 appliance with Knox Arkeia

To perform a restore with the Knox Arkeia software, you must have backed up the appliance to an Arkeia server.

Preparing for disaster recovery

Prepare your Sun Cobalt Qube 3 appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the appliance to a factory-fresh state.
2. Configure the appliance through the Setup Wizard and return it to the network. The appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the appliance to use a network time protocol (NTP) server to set the clock on the appliance.

On the Server Desktop UI, select **Administration > System > Time** to configure the time settings or to specify an NTP server.

4. On the Server Desktop UI, select **Administration > Maintenance > Knox Arkeia**. The “Knox Arkeia Backup Settings” table appears.
5. Configure the Knox Arkeia client on the appliance.
 - **Enable Client**—Click to enable the check box Enable Client.
 - **Backup Server Name**—Enter the fully qualified domain name of the Knox Arkeia backup server.

This server must be the Arkeia server to which you backed up your appliance.
 - **Port Number**—Enter the port number to which your Knox Arkeia backup server is listening. The default port number is 617.
6. Click **Save**. The table refreshes and displays the new configuration.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt Qube 3 appliance is now ready to be restored.

The restoration options on the Knox Arkeia backup server should include “Files modified since backup date” and “by user ID”.

Only certain directories can be recovered during disaster recovery. Select the following directories using the Arkeia tree navigator:

```
/home
/root
.nsr
/usr
/nsr
/var
/etc
opt
```



Important: DO NOT select `/lib`, `/boot`, or `/vmlinuz.gz` or your appliance will crash during recovery and most likely will not reboot.



Note: The `/nsr` directory and the `.nsr` file exist only if you have loaded the Legato NetWorker client software on the appliance.

When the restore process is complete, reboot the appliance for all the changes to take effect.



Important: Disaster recovery is not complete until you reboot the Sun Cobalt Qube 3 appliance.

The appliance does not reboot automatically.

After the appliance has rebooted, ensure that the CCE database was recovered. Inspect the directory `/var/cobalt/backups/` for files. If `cce.tar` exists and does not have a ‘restored’ prefix, then you need to run the command:

```
/etc/rc.d/init.d/cobalt_restore start
```

as the root user and reboot the appliance again.

The Arkeia log window indicates that the following files are “busy” and that it cannot overwrite the files. This is both normal and acceptable.

```
/usr/bin/perl5.00503
/usr/sbin/httpd
/usr/sausalito/cced.socket
/usr/sausalito/sbin/cced
/usr/knox/bin/opbs
/usr/knox/bin/nlservd
```

Legato NetWorker®

Tailoring the backup service

No server-side tailoring is required for Legato NetWorker other than adding the client to the backup server.



Important: When adding a Sun Cobalt Qube 3 appliance to a Legato NetWorker backup server, select “UNIX® Standard Directives” when creating the appliance client resource.

Do not select “Compression directives”. If you select “Compression directives”, the tailoring for the appliance will not work properly.

Files associated with Legato NetWorker tailoring

Table 2 lists the files associated with the Legato NetWorker software. These files are located on the Sun Cobalt Qube 3 appliance.

Table 2. Files associated with Legato NetWorker

Path and file name	Description
/.nsr	Directives for handling Sun Cobalt Qube 3 appliance file systems.
/usr/bin/cceasm	An external Application Specific Module (ASM) for the CCE database. <i>Note:</i> External ASMs are not compatible with “Compression directives”.

Backing up a Sun Cobalt Qube 3 appliance with Legato NetWorker

To back up your appliance with Legato NetWorker, you must first configure and enable the NetWorker agent on the appliance. For more information, see “Configuring client agents on the Sun Cobalt Qube 3 appliance” on page 16.

Sun Microsystems recommends specifying the “All” saveset when using Legato NetWorker. If you must specify individual savesets for an appliance, you must backup up the following directories together to ensure consistency:

```
/etc  
/usr/sausalito
```

Performing disaster recovery on a Sun Cobalt Qube 3 appliance with Legato NetWorker

To perform a restore with the Legato NetWorker software, you must have backed up the appliance to a NetWorker server.

Preparing for disaster recovery

Prepare your Sun Cobalt Qube 3 appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the appliance to a factory-fresh state.
2. Configure the appliance through the Setup Wizard and return it to the network. The appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the appliance to use a network time protocol (NTP) server to set the clock on the appliance.

On the Server Desktop UI, select **Administration > System > Time** to configure the time settings or to specify an NTP server.

4. On the Server Desktop UI, select **Administration > Maintenance > Legato NetWorker**. The “Legato NetWorker Backup Settings” table appears.
5. Configure the Legato NetWorker client on the appliance.
 - **Enable Client**—Click to enable the check box to enable the backup client.
 - **Legato Server Hostnames**—Enter the fully qualified domain names of Legato NetWorker backup servers. Legato servers must have valid host names.

This server must be the NetWorker server to which you backed up your appliance.
 - **Service port range**—Sets the range of the system’s service ports to the one specified (default range is 9000—9010).
 - **Connection Port Range**—Sets the range of the system’s connection ports to the one specified (default range is 9011—9999).
6. Click **Save**. The table refreshes and displays the new configuration.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt Qube 3 appliance is now ready to be restored.

Restore the file systems for your appliance in the following order:

```

/var
/
/home

```

When the restore process is complete, reboot the appliance for all the changes to take effect.



Important: Disaster recovery is not complete until you reboot the Sun Cobalt Qube 3 appliance.

The appliance does not reboot automatically.

Technical note

Legato NetWorker restores the Cobalt configuration database independently. It is possible to restore the CCE database without restoring the machine configuration files in `/etc`. If this is done, the configuration database and the Server Desktop UI will have different information than the actual system, which is generally considered to be a bad situation.

Veritas NetBackup

Tailoring the backup service

No server-side tailoring is required for Veritas NetBackup. Pre- and post-backup scripts are already installed and are run automatically by the NetBackup client. See Table 3 for a list of files associated with the Veritas NetBackup software.

Files associated with Veritas NetBackup tailoring

Table 3 lists the files associated with the Veritas NetBackup software. These files are located on the Sun Cobalt Qube 3 appliance.

Table 3. Files associated with Veritas NetBackup

Path and file name	Description
/opt/opensv/netbackup/bin/bpstart_notify	Started automatically by NetBackup before a backup runs. It calls the script cobalt_prebackup.
/opt/opensv/netbackup/bin/bpend_notify	Started automatically by NetBackup after a backup runs. It calls the script cobalt_postbackup.
/usr/local/sbin/cobalt_prebackup	Runs before a backup to create an archive of the CCE database.
/usr/local/sbin/cobalt_postbackup	Runs after a backup to delete the archive created by cobalt_prebackup.
/etc/rc.d/init.d/cobalt_restore	Runs at startup and detects whether an archive of the configuration database exists. An extant archive is recovered and has its name changed.
/var/cobalt/backups/cce.tar	Archive of the CCE database that is created by cobalt_prebackup and deleted by cobalt_postbackup. The archive is renamed to restored.cce.tar by cobalt_restore after disaster recovery.

Backing up a Sun Cobalt Qube 3 appliance with Veritas NetBackup

To back up your appliance with Veritas NetBackup, you must first configure and enable the NetBackup agent on the appliance. For more information, see “Configuring client agents on the Sun Cobalt Qube 3 appliance” on page 16.

Backups are started by using the Veritas NetBackup UI. Once a backup of an appliance has begun, the `cobalt_prebackup` script creates the `cce.tar` file in the `/var/cobalt/backups` directory.

When the backup has successfully completed, the script `cobalt_postbackup` removes the `cce.tar` file.

Sun Microsystems recommends specifying the “ALL_LOCAL_DRIVES” option when using Veritas NetBackup. If you must specify individual savesets for an appliance, you must backup up the following directories together to ensure consistency:

```
/etc  
/usr/sausalito
```

Performing disaster recovery on a Sun Cobalt Qube 3 appliance with Veritas NetBackup

To perform a restore with the Veritas NetBackup software, you must have backed up the appliance to a NetBackup server.

Preparing for disaster recovery

Prepare your Sun Cobalt Qube 3 appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the appliance to a factory-fresh state.
2. Configure the appliance through the Setup Wizard and return it to the network. The appliance must be able to communicate with the backup server; otherwise the recovery will fail.
3. If possible, configure the appliance to use a network time protocol (NTP) server to set the clock on the appliance.

On the Server Desktop UI, select **Administration > System > Time** to configure the time settings or to specify an NTP server.

4. On the Server Desktop UI, select **Administration > Maintenance > Veritas NetBackup**. The “Veritas NetBackup Backup Settings” table appears.
5. Configure the Veritas NetBackup client on the appliance.
 - **Enable Client**—Click the check box to enable the Veritas NetBackup backup client.
 - **Master Veritas Server**—Enter the fully qualified domain name of Veritas NetBackup master backup server. The Veritas master backup server must have a valid host name.

This server must be the NetBackup server to which you backed up your appliance.
 - **Extra Veritas Servers**—Enter the fully qualified domain names of any extra Veritas NetBackup backup servers. All Veritas servers must have valid host names.
6. Click **Save**. The Veritas NetBackup License Agreement appears.
7. Click **I agree** or **I do not agree**.

If you select **I do not agree**, the system does not save the configuration settings for the Veritas NetBackup client.

If you select **I agree**, the table refreshes and displays the new configuration.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the appliance is now ready for disaster recovery. When recovering your Sun Cobalt Qube 3 appliance, include only the following files and directories:

```
/home
/root
.nsr
/usr
/nsr
/var
/etc
opt
```



Important: DO NOT select `/lib`, `/boot`, or `/vmlinuz.gz` or your appliance will crash during recovery and most likely will not reboot.



Note: The `/nsr` directory and the `.nsr` file exist only if you have loaded the Legato NetWorker client software on the appliance.

When the restore process is complete, reboot the appliance for all the changes to take effect.



Important: Disaster recovery is not complete until you reboot the Sun Cobalt Qube 3 appliance.

The appliance does not reboot automatically.

After the appliance has rebooted, ensure that the CCE database was recovered. Inspect the directory `/var/cobalt/backups/` for files. If `cce.tar` exists and does not have a 'restored' prefix, then you need to run the command:

```
/etc/rc.d/init.d/cobalt_restore start
```

as the root user and reboot the appliance again.

The restore is initiated at this point.



Note: The restore log indicates that the restore was only partially completed. This is due to warnings concerning any files that were in use during the recovery process.

You should verify the files for which you received a warning, but this not normally a problem.

Configuring client agents on the Sun Cobalt Qube 3 appliance

To use a third-party backup solution, you must first enable the agent and enter the information for the backup server on the Sun Cobalt Qube 3 appliance. The following paragraphs explain how to do this for each of the backup solutions.



Note: To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items.

For example, select **Administration > Users and Groups > User List** means to click the **Administration** tab in the top menu bar, click the **Users and Groups** menu category in the left menu bar and finally click the **User List** sub-menu item.

Configuring Knox Arkeia

To configure the Knox Arkeia backup solution:

1. On the Server Desktop UI, select **Administration > Maintenance > Knox Arkeia**. The “Knox Arkeia Backup Settings” table appears.
2. Configure the Knox Arkeia client.
 - **Enable Client**—Click to enable the check box Enable Client.
 - **Backup Server Name**—Enter the fully qualified domain name of the Knox Arkeia backup server.
 - **Port Number**—Enter the port number to which your Knox Arkeia backup server is listening. The default port number is 617.
3. Click **Save**. The table refreshes and displays the new configuration.

Configuring Legato NetWorker

To configure the Legato NetWorker backup solution:

1. On the Server Desktop UI, select **Administration > Maintenance > Legato NetWorker**. The “Legato NetWorker Backup Settings” table appears.
2. Configure the Legato NetWorker client.
 - **Enable Client**—Click to enable the check box to enable the backup client.
 - **Legato Server Hostnames**—Enter the fully qualified domain names of Legato NetWorker backup servers. Legato servers must have valid host names.
 - **Service port range**—Sets the range of the system’s service ports to the one specified (default range is 9000—9010).
 - **Connection Port Range**—Sets the range of the system’s connection ports to the one specified (default range is 9011—9999).
3. Click **Save**. The table refreshes and displays the new configuration.

Configuring Veritas NetBackup

To configure the Veritas NetBackup backup solution:

1. On the Server Desktop UI, select **Administration > Maintenance > Veritas NetBackup**. The “Veritas NetBackup Backup Settings” table appears.
2. Configure the Veritas NetBackup client.
 - **Enable Client**—Click the check box to enable the Veritas NetBackup backup client.
 - **Master Veritas Server**—Enter the fully qualified domain name of Veritas NetBackup master backup server. The Veritas master backup server must have a valid host name.
 - **Extra Veritas Servers**—Enter the fully qualified domain names of any extra Veritas NetBackup backup servers. All Veritas servers must have valid host names.
3. Click **Save**. The Veritas NetBackup License Agreement appears.
4. Click **I agree** or **I do not agree**.

If you select **I do not agree**, the system does not save the configuration settings for the Veritas NetBackup client.

If you select **I agree**, the table refreshes and displays the new configuration.

