symantec.™

Confidence in a connected world.

`

NetBackup Master Catalog Replication Using RealTime 7.0

Version 1.0 – 12th March 2010

Note: This is a living document and will be subject to periodic updates. Please check the data and version number to ensure you are referencing the latest version. If you have any feedback on this document please email IMG-TPM-Requests@symantec.com

Contents

Table of Contents

Introduction

As part of the RealTime 7 release, Symantec is granting the right to use NetBackup RealTime with a zero-cost license*, to replicate the NetBackup 6.5** and NetBackup 7 catalogs. While NetBackup RealTime can be implemented in much the same way as other replication technologies it offers both a replication mechanism and a logical corruption protection capability, which can be used to 'rewind' a data set such as the NetBackup catalog in the event that corruption of the data occurs.

NetBackup RealTime software is included in the NetBackup 7 DVD media kit and can be used to replicate the NetBackup catalog in configurations that align to the conditional support statement Technote 287636 as well as providing local Logical Corruption Protection without replication for all NetBackup master servers.

*The Licensed Software may be used by You in support of the Symantec NetBackup product to recover the Symantec NetBackup application in the event of computer failure. Notwithstanding any limitations contained in this Agreement, including Use Level limitations for the Licensed Software, You shall always have the right to use the Licensed Software to support the recovery of an authorized license of the Symantec NetBackup product application software itself. The foregoing authorization shall not apply to data backed up through the Symantec NetBackup products. If you desire to use the Licensed Software to recover such data, You must acquire a license to the Licensed Software for the number of Front End Terabytes applicable to such data.

*RealTime supports NetBackup 6.5.4 or higher for catalog replication and corruption protection.

Cookbook Objective

This document is intended to as a step-by-step guide to protecting and recovering the NetBackup catalog with RealTime Protection.

As NetBackup catalogs have grown in size over the year protecting them has become more difficult, especially for disaster recovery, where a copy needs to be physically sent offsite. As a larger NetBackup catalog means even more data is being protected, recovering the catalog becomes one of the critical first area of focus is when it comes time to do an overall recovery. Support for NetBackup Catalog replication is based on conditions documented in Technote 287636

The second area of focus is the ability to recover from unlikely event of corruption in the NetBackup catalog. Although continuous protection is available this document will focus on Replication of the NetBackup Catalog.

Previous Options

Catalog replication between master servers using conventional continuous replication technologies provides a rapid recovery capability in the event of a site loss but provides little protection against catalog corruption.

NetBackup RealTime 7 Solution

The inclusion of NetBackup RealTime in NetBackup 7 provides the ability to implement both catalog replication, for protection against site loss, and logical corruption protection at zero license cost

RealTime's Logical Corruption Protection capability protects against corruption by allowing the user to 'rewind' the catalog to a point in time before the corruption occurred.

Replication is the process of automatically duplicating and updating data across a network from source computer to destination computer(s). Disks are typically located in physically distant locations to ensure consistency between redundant resources, improve reliability, fault-tolerance, or accessibility in case of local failures or disasters. NetBackup RealTime Replication provides a block level, off-host replication technology, operating in application-centric mode. The benefit is I/Os are acknowledged as soon as they are written to the local storage. The performance impact to the host is minimal because replication is performed on the RealTime server and storage, as opposed to the production storage or host.
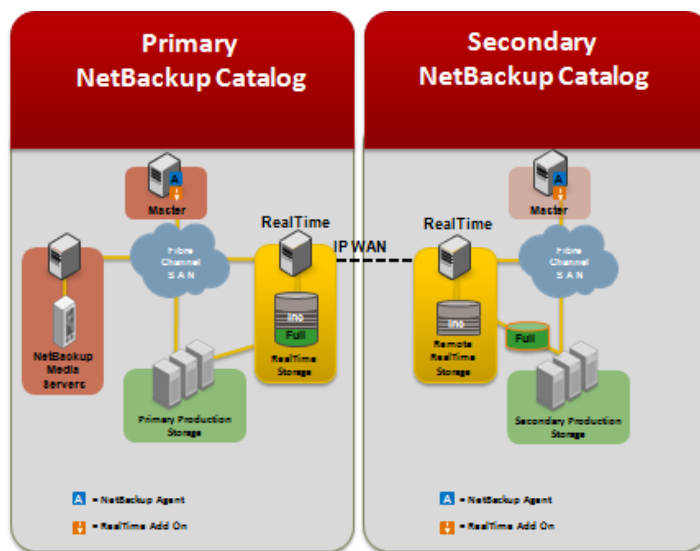
Logical corruption protection provides continuous protection for the NetBackup catalog by creating a timeline of changes to be replicated. When enabled, the protection allows access to the NetBackup catalog anywhere along the RealTime timeline, thus allowing the user to 'rewind' to a point prior to a corrupting event.

RealTime Replication and Logical Corruption Protection can be combined to provide a logical corruption mechanism within the replicated data stream. For more details on Timeline protection functionality of RealTime refers to "Symantec NetBackup™ RealTime Administration Guide. The information required to recover from logical corruption are also replicated to the secondary site including the I/O timestamps, or snapshot bookmarks indicating a transaction consistent points.

NetBackup RealTime 7 Minimum Requirements

The Symantec NetBackup RealTime [RealTime] software lets you use an existing Intel 64-bit server for the sole purpose of being a *RealTime Server**, which provides SAN-based data protection to the NetBackup catalog. For this purpose, the RealTime Server uses dedicated SAN storage that is referred to as *RealTime Storage*. If the NetBackup catalog is replicated then a second *RealTime Server** is required at the secondary location, along with the required *RealTime Storage.*

The system requirements for the *RealTime Server** components:
- System Type x86 64 bit-based PC
- Processors (minimum 4) x86 64 bit Intel
- Ethernet Controller (4) Gigabit Ethernet ports
- QLogic Corporation QLE 2462 Fibre Channel Adapter (rev 02)
- Fibre Channel HBA (2 each with2 ports)
- Total Physical Memory 32 GB or more

The storage requirements for the *RealTime Stor*age:
- RealTime storage must meet the hardware requirements in the Veritas Storage Foundation Cluster File System (SFCFS) 4.1 Maintenance Pack 3 HCL.

A NetBackup Master Server with the RealTime client installed is referred to as the *application host*. If replication is enabled, the RealTime client is installed on a standby NetBackup Master Server, referred to as the *Remote Recovery Host, and* is located at the secondary location.

The system requirements for the RealTime client components:
- Solaris 10 64-Bit SPARC
  - Sun Native Volume Manager [SVM]
  - Veritas Volume Manager [VxVM]
  - UFS file Systems (UFS)
  - Veritas file system (VxFS)

- Windows Server 2003 SP2~ 64/32-Bit
  - Microsoft Logical Volume Manager [MS LVM]
  - Microsoft NTFS file system [NTFS]
  - Microsoft Basic Disk [LVM Basic disk]

The NetBackup RealTime Compatibility List (CL) is available from the NetBackup Product Family Master Compatibility List.

*The RealTime Server's is a dedicated system and should only be used for RealTime's operations.

How RealTime Replication Works

RealTime data replication technology provides remote mirroring of production data for purposes such as remote backup, data distribution, and disaster recovery. RealTime replication is an asynchronous block-level replication technology. RealTime continuously replicates writes from the primary (source) LUNs to the secondary (target) LUNs using multiple TCP/IP streams to maximize throughput over a WAN link. RealTime replication ensures that the replicated copy of the data at the secondary is consistent. In the eventuality of a disaster at the primary site, the replicated copy of the production data is available to start the application on the secondary site. The host at the source location on which the application is running is known as the primary host, and the host at the target location is known as the Secondary host.

Write-order fidelity

To use the secondary (target) LUNs in a disaster recovery scenario, RealTime maintains write-order fidelity. The term *write-order fidelity* means that RealTime tracks writes on the primary in the order in which they are received, and applies them on the secondary in the same order. Maintaining write-order fidelity is important to ensure that the data on the secondary is consistent with the data on the primary. While the data at the secondary can be behind in time, the data must be a consistent image of the primary application at a known point in the past. Without write order fidelity, there is no guarantee that a secondary has consistent, recoverable data. RealTime maintains write-order fidelity across all of the LUNs in an application. For example, in a database environment, the log and data space are typically on different LUNs. On the primary, RealTime applies writes to the journal in the order that writes were received, and RealTime maintains this order when applying the writes on the secondary. If write-order fidelity is not maintained, a database application may not recover successfully when failed over to the secondary.

How RealTime logs writes to the Journal

The journal is a circular buffer of writes for an application dataset. The journal is maintained on the RealTime Server. Writes that come in are written to the journal. In steady state replication, the RealTime Server attempts to replicate the writes from memory as fast as possible. If the network has an outage or becomes slow and the memory usage of the RealTime Server goes above a certain limit, the writes are discarded from memory. When the network returns back to normal, the writes are read back from the journal and replicated to the secondary. In the eventuality that the network outage is prolonged and the journal fills up, the RealTime Server switches to a bitmap mode, where it maintains a bitmap of all of the changes coming from the application server. The bitmap is known as the Data Change Map (DCM). After the network outage is over, the RealTime Server re-synchronizes the changed blocks to the secondary RealTime Server. During the re-synchronization phase, a blackout window is created to prevent recover from inconsistent secondary LUNS.

Consistent data versus current or up-to-date data

Data is consistent if the system or application using the data can be successfully restarted to a known, usable state. The data on the secondary is consistent if the data correctly reflects the data on the primary at some point in the past. For example, if the data being replicated is used by a database, the data is consistent if the database can be started and recovered to a usable state with zero data corruption. If the data contains a file system, the data is consistent if the file system check utility can be run and the data can be recovered with no file system corruption. Data is considered consistent only if it contains all updates up to a point in time and none of the updates that come after that point. For example, if the data is a file system, the most recently created files may be missing when the file system is restarted. If the data is a database, one or more of the most recently committed transactions might be missing. Data that is current or up-to-date contains the latest changes made at the primary. For example, if you are replicating a database, the most recent transaction is available at the secondary. Whether or not the data on the secondary must always be current is a business decision and can be controlled by choosing between synchronous and asynchronous replication. Synchronous replication guarantees that the data on the secondary is current, at the cost of application performance. Asynchronous replication does not guarantee the data is current, but has less impact on application performance and provides the ability to use more cost-effective telecommunications. At all times, RealTime maintains the data at the secondary in a consistent state with the data at the primary.

Types of replication

RealTime supports only continuous asynchronous replication. Asynchronous replication guarantees that RealTime makes all completed updates to the primary LUNs on the secondary LUNs. However, the updates can be delayed depending on the replication network performance. The application is informed that the write request is complete when production storage acknowledges the completion. The write is also queued persistently on the RealTime Server to be sent to the secondary RealTime Server. The application is never informed that the write is pending on the secondary side. This queue may grow when there is a surge in the write rate. However, the queue is being continuously drained. When the surge subsides, the queue drains faster than it grows, enabling the secondary to catch up with the primary. Because asynchronous replication writes persistently and holds the writes at the primary RealTime Server for later transmission, asynchronous replication is able to compensate for temporary outages of the network or the secondary RealTime Servers without affecting the performance of the application. If a disaster strikes in asynchronous replication, the replicated data set at the secondary will be consistent. However, oftentimes the most recent writes do not reach the secondary.

Assumptions

- NetBackup may be installed* and configured as a cluster in the primary site.
- The remote NetBackup Master server may be configured after the Primary site is active
- SAN storage is available and NetBackup is configured in single or multi-node cluster with the */usr/openv or* directory structure on SAN storage.
- The SAN zone allows the NetBackup Master server(s) and the RealTime server access to the SAN storage.
- Connectivity between the primary and secondary location is adequate to provide the required bandwidth for replication.
- Optional Cluster Monitor support** is provided by Veritas Cluster Server (VCS).
- DNS or equivalent is updated to include the RealTime Virtual names and IP addresses.

*If NetBackup is *NOT* currently installed the cookbook indicated the appropriate time to install and configure the NetBackup components.*
***If VCS is *NOT* installed, and cluster support is desired, the cookbook will indicate the appropriate time to install and configure VCS.*

Implementation and Naming Conventions and DNS entries

The cookbook is based on a one-node clustered NBU master residing in the primary location, and a one-node clustered standby NBU Master server in the secondary location. Regardless, the NBU binaries and catalog MUST be installed on SAN disk, and zoned correctly. Also, consider the naming convention used when configuring replication. Virtual names should clearly identify the location and functionality of the server.   For example the cookbook uses the naming convention {service}_{location}{Node}, and those entries are included in the DNS.

Primary site SAN Zone
       realtime_p1: The NetBackup RealTime appliance.
       nbunode_p1: The first node of clustered NetBackup Master Server.
          SAN Disks: SAN disk used for /usr/openv
       nbunode_p2: The second node of clustered NetBackup Master Server.

Primary site Virtual IP Addresses and names
       nbumaster_v: The virtual name of the NetBackup master server
       rtpserver_p1: RealTime Server: Provides RealTime Services.
       rtpconsole_p2: RealTime Console: RealTime Web-based User Interface.
       rtpbroker_p3: Authentication Broker: Provides Symantec Security Services.

Secondary site Zone
       realtime_s1: The NetBackup RealTime appliance.
       nbunode_s1: The name of the single node clusters NetBackup Master Server.
          SAN Disks: SAN disk used to protect primary.

Primary site Virtual IP Addresses and names
       nbumaster_v: The virtual name of the NetBackup master server
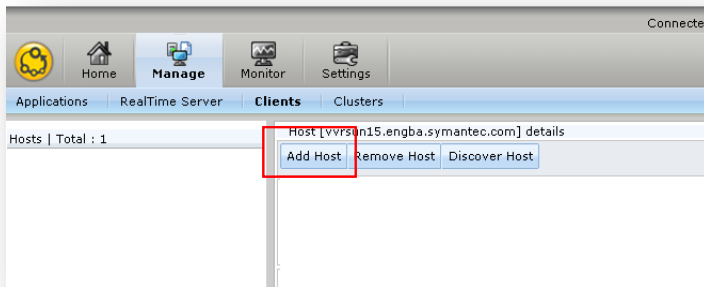   rtpserver_s1: RealTime Server
       rtpconsole_s2: RealTime Console
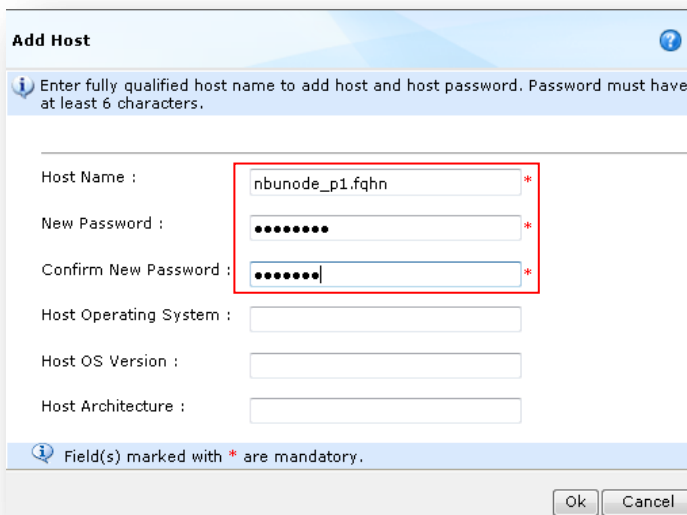   rtpbroker_s3: Authentication Broker

*Step I: Installation and initial configuration - **Primary site***

1. Install and configure NetBackup RealTime appliance at the primary site following the instructions from Symantec NetBackup RealTime 7 Installation Guide.

2. Add the member nodes of the Primary NetBackup Master Server cluster into the RealTime Configuration:

- Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

- Navigate to **Manage>Clients**

Select **Add Host** on the task panel in the right hand pane.
Enter the physical hostname and password information and click **OK**.

Use this password when you install and configure the RealTime client on the NetBackup Master Server node(s).

- Install NetBackup RealTime client on the NetBackup Master Server(s) in the primary site following the instructions from Symantec NetBackup RealTime 7 Installation Guide.

  The following is an example of the required information to complete the client installation:

RealTime Server Virtual Name:	*rtpserver_p1*
RealTime Manager Virtual Name:	*rtpconsole_p2*
RealTime Server host name:	*realtime_p1*
Authentication Broker Virtual Name:	*rtpbroker_p3*
Host Name:	*rtpserver*
Password	*{provided in the previous step}*

- On the client, navigate to */opt/VRTSrm/* directory and modify the *rm.conf* file by adding the virtual node names for the NetBackup cluster. Be careful not to modify the existing entries.

  Note: ".fqhn" represents the fully qualified hostnames for the environment.

  If there is a second-node in the NetBackup Master Server cluster then follow the previously described installation instructions.

  At the RealTime console Select **Discover Host** on the task panel in the left hand pane.

3. Installing Veritas Cluster Server(VCS) in the primary site
Skip this step if VCS is already installed, or NetBackup is installed without a cluster monitor.

- Install and configure Veritas Cluster Server (VCS) on *nbnode_p1* and *nbnode_p2* in the primary site. VCS can be installed alone or as part of the Storage Foundation HA 5.0. Follow the VCS installation guide to install and configure VCS 5.0.
- Refer to the VCS Users Guide for a list of available VCS commands.

Note: You will be warned that later versions of VRTSperl, VRTSicsco and VRTSperl is already installed on nbunodeA1 and nbunodeA2 and asked if you would like to continue. Answer 'yes' to those questions

4. Creating the File System for NetBackup in the primary site
Skip this step if a file system is already available.

- Create a file system to store the NetBackup catalogs. This must be a disk on SAN and zoned in such a way that nbnode_p1, nbunode_p2 and realtime_p1 should be able to access it.

- If Storage Foundation is not used, use Solaris 'format' utility partition the disk and use 'newfs' to create a UFS file system*. These operations can be done from either nbunode_p1 or nbunode_p2.

- If Storage Foundation is in use, bring the SAN disk under VxVM control. Initialize the disk, create a disk group, create a volume and then create a VxFS file system on the newly created volume*. These operations can be done from either nbunode_p1 or nbunode_p2.

*Test mounting the file system both nodes, and leave the file system unmounted at the end of the test.

5. Install and configure NetBackup in the primary site.
Skip this step if NetBackup is already installed*.

- Install and Configure NetBackup on all nodes of the VCS cluster as described in the NetBackup 7, or NetBackup 6.5**, High Availability Guide.

- During cluster configuration provide the file system details created in the previous step as the shared data path.

.
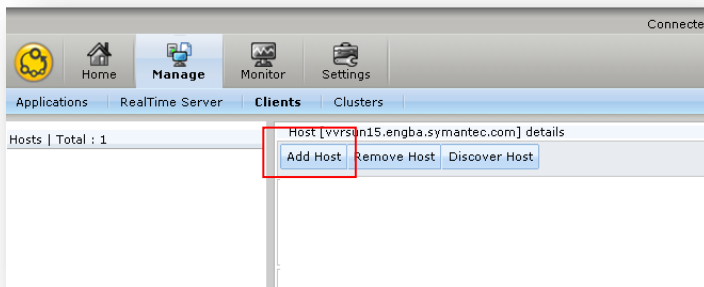** Existing NetBackup Server(s) must be installed as described in the NetBackup High Availably Guide.*
**Note: Follow the NetBackup 6.5 High Availability Guide when installing NetBackup 6.5.4 or above
***If NetBackup is configured without a cluster monitor stop all the NetBackup services on the Master at the primary site
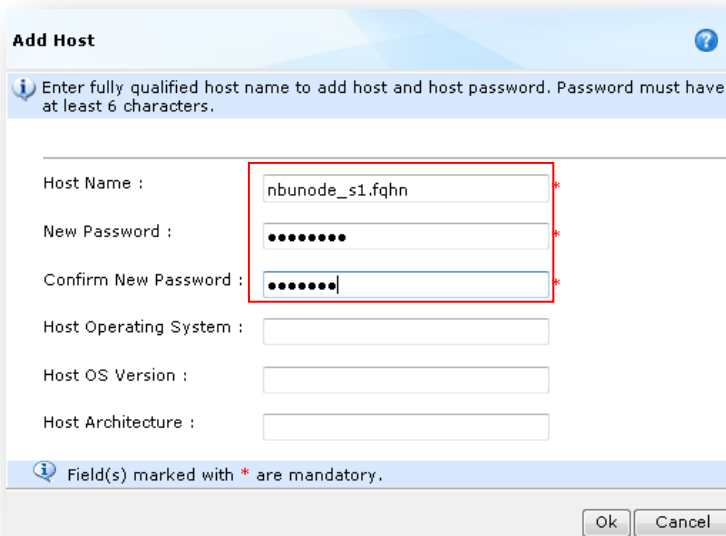
*Step II: Installation and initial configuration - **Secondary site***

Caution: *Please make sure that NetBackup is offline at the primary site before proceeding with secondary site. When NetBackup is configured on secondary site, the virtual name for NetBackup nbumaster_v needs to be brought online.*

1. Install and configure NetBackup RealTime appliance at the secondary site following the instructions from Symantec NetBackup RealTime 7 Installation Guide.

2. Add the member nodes of the standby NetBackup Master Server cluster into the RealTime Configuration:

   • Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_s1.domain.com/ and log in with the credential created during the installation process.

   • Navigate to **Manage>Clients**

   Select **Add Host** on the task panel in the right hand pane.
   Enter the physical hostname and password information and click **OK**.

   Use this password when you install and configure the RealTime clients.

- Install NetBackup RealTime client on the NetBackup Master Server(s) in the secondary site following the instructions from Symantec NetBackup RealTime 7 Installation Guide.

  The following is an example of the required information to complete the client installation:

RealTime Server Virtual Name:	*rtpserver_s1*
RealTime Manager Virtual Name:	*rtpconsole_s2*
RealTime Server host name:	*realtime_s1*
Authentication Broker Virtual Name:	*rtpbroker_s3*
Host Name:	*rtpserver*
Password	*{provided in the previous step}*

- On the client, navigate to */opt/VRTSrm/* directory and modify the *rm.conf* file by adding the virtual node names for the NetBackup cluster. Be careful not to modify the existing entries.

Note: ".fqhn" represents the fully qualified hostnames for the environment.

  If there is a second-node in the NetBackup Master Server cluster then follow the previously described installation instructions.

  At the RealTime console Select **Discover Host** on the task panel in the left hand pane.

3. Installing Veritas Cluster Server(VCS) in the secondary site
Skip step if VCS is already installed, or NetBackup is installed without a cluster monitor.

- Install and configure Veritas Cluster Server (VCS) on *nbnode_s1* in the secondary site. VCS can be installed alone or as part of the Storage Foundation HA 5.0. Follow the VCS installation guide to install and configure VCS 5.0
- Refer to the VCS Users Guide for a list of available VCS commands.

   Note: You will be warned that later versions of VRTSperl, VRTSicsco and VRTSperl is already installed on nbunodeA1 and nbunodeA2 and asked if you would like to continue. Answer 'yes' to those questions

4. Creating the File System for NetBackup binaries in the secondary site
Skip this step if a file system is already available.

- Create a file system to store NetBackup catalog. This must be a disk on SAN and zoned in such a way that nbnode_s1 and realtime_s1 should be able to access it.

- If Storage Foundation is not used, use Solaris 'format' utility partition the disk and use 'newfs' to create a UFS file system*.

- If Storage Foundation is in use, bring the SAN disk under VxVM control. Initialize the disk, create a disk group, create a volume and then create a VxFS file system on the newly created volume.

   *Test mounting the file system both nodes, and leave the file system unmounted at the end of the test.

5. Install and configure NetBackup binaries in the secondary site.
Skip this step if NetBackup is already installed*.

- Install and Configure NetBackup on all nodes of the VCS cluster as described in the NetBackup 7, or NetBackup 6.5**, High Availability Guide.

- During cluster configuration provide the file system details created in the previous step as the shared data path.

- When prompted to enter the host name of the NetBackup Master Server, enter the virtual name, for example *nbumaster_v*.

- The VCS resource group and resource names used for NetBackup *MUST* be identical to those configured at the primary site

- Offline*** the NetBackup service group at the secondary site with the VCS command:
   opt/VRTSvcs/bin/hagrp –offline{ nbu_group} –sys nbnode_s1

   * Existing NetBackup Server(s) must be installed as described in the NetBackup High Availably Guide.
   **Note: Follow the NetBackup 6.5 High Availability Guide when installing NetBackup 6.5.4 or higher.
   ***If NetBackup is configured without a cluster monitor stop all the NetBackup services on the Master on the secondary site.

*Step III: NetBackup RealTime – **Cluster Configuration***

- Configure RealTime Monitor LUN
  Skip this section if NetBackup is installed without a cluster monitor in the primary site.

  RealTime uses the Monitor LUN while protecting clustered applications to store health information of all of the nodes in a cluster. The RealTime Server reads this LUN for computing timeline movement.   The following are the requirements for the Monitor LUN:

  > At least one (1) Monitor LUN per storage enclosure.
  > Monitor LUN must be at least 1GB in size.
  > Monitor LUN must be LUN masked and zoned so that the LUN is visible to the NetBackup Master and the RealTime Server.

- Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

- Navigate to **Monitor>RealTime Server**
  Select *Storage* in the Left hand panel, which brings up the Storage panel
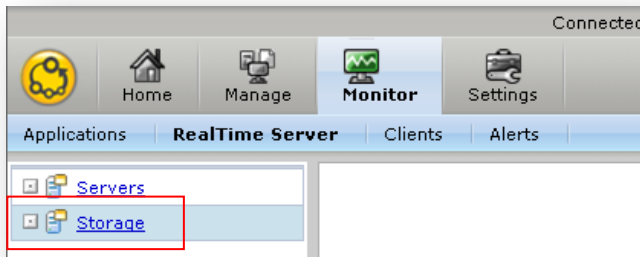
  From the lower right on the Storage panel, click the check box for the desired LUN. Select **Classify Storage** in the task panel
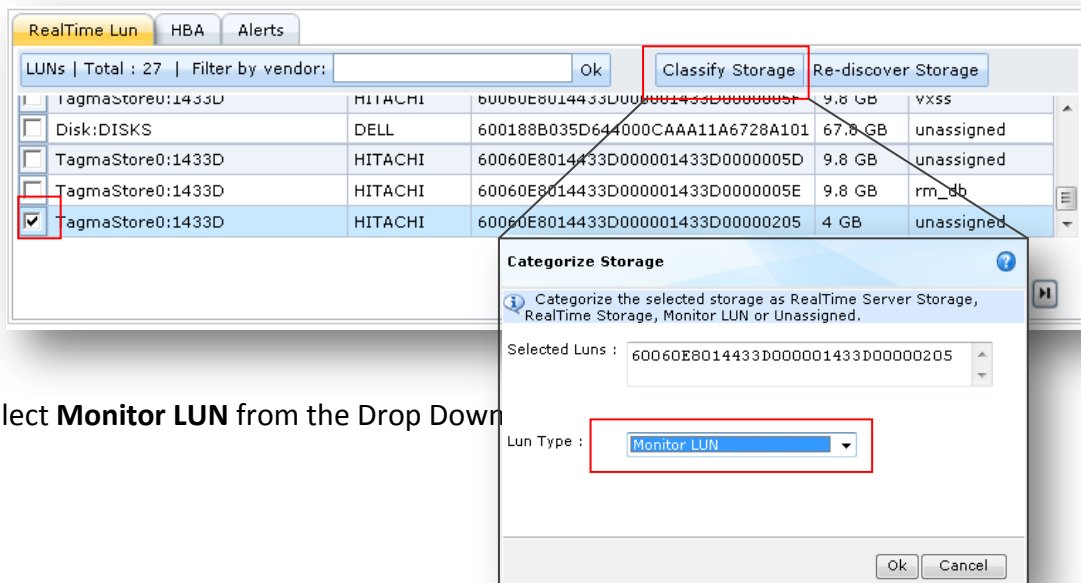
  Select **Monitor LUN** from the Drop Down

- Online* the NetBackup Service Group at the primary site with the following VCS command:
  / opt/VRTSvcs/bin/hagrp –offline{ nbu_group} –sys nbnode_p1

  *If NetBackup is configured without a cluster monitor start all the NetBackup services on the Master at the primary site.

- Configure NetBackup Cluster in RealTime Console
  Skip the step if the NetBackup Master is configured without a cluster monitor.

  Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

  - Navigate to **Manage>Cluster**
    Select **Add Cluster** on the right task panel to open the Add Cluster Wizard.
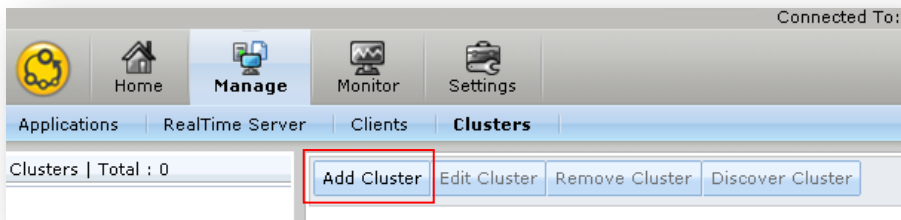
    Enter the fully qualified NetBackup virtual cluster name in the Add Cluster Wizard.
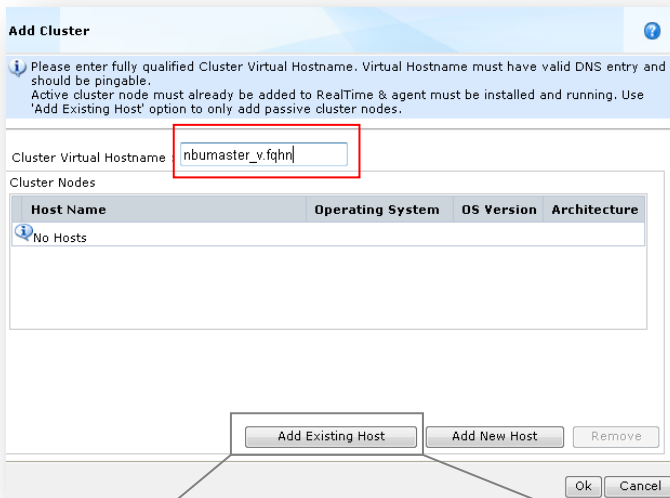
    Select **Add Existing Host** on the Add Cluster Wizard.
    Select the NetBackup Master Server node(s) from the drop down list and select **OK**
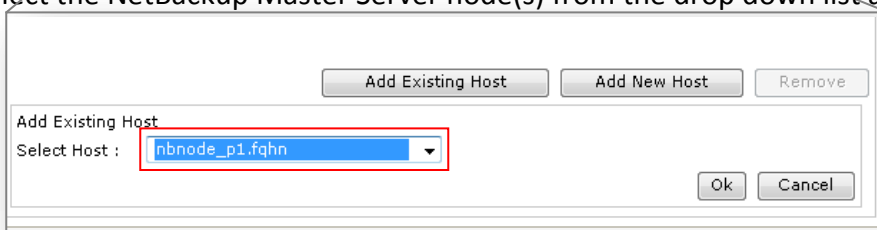
- Once the NetBackup Master Server(s) nodes are added, select **OK**
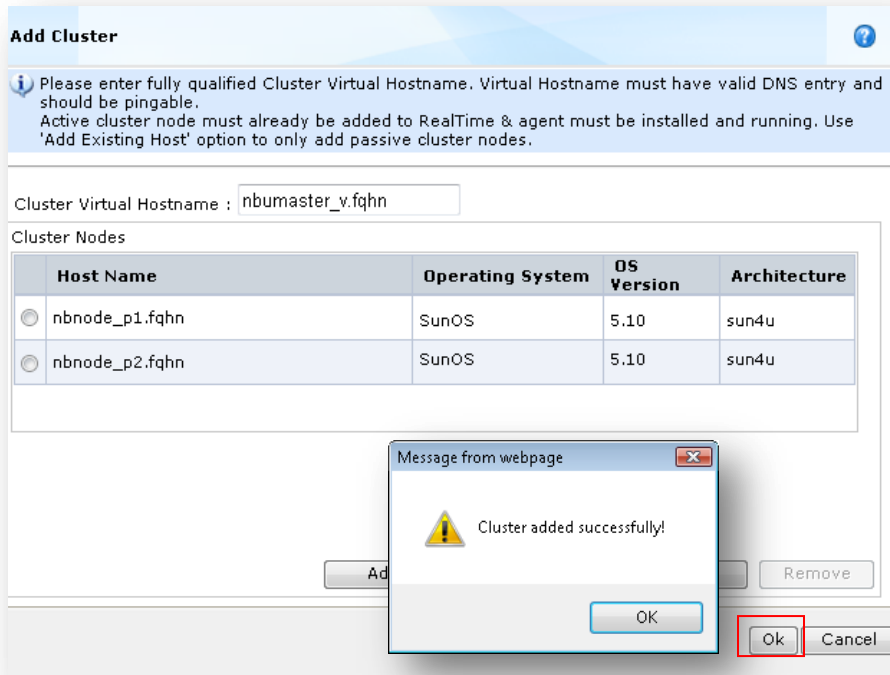
Select *Discover Cluster* on the right task panel to discover the NetBackup file system
and verify the */opt/VRTSnbu* file system is listed

symantec.
Confidence in a connected world.
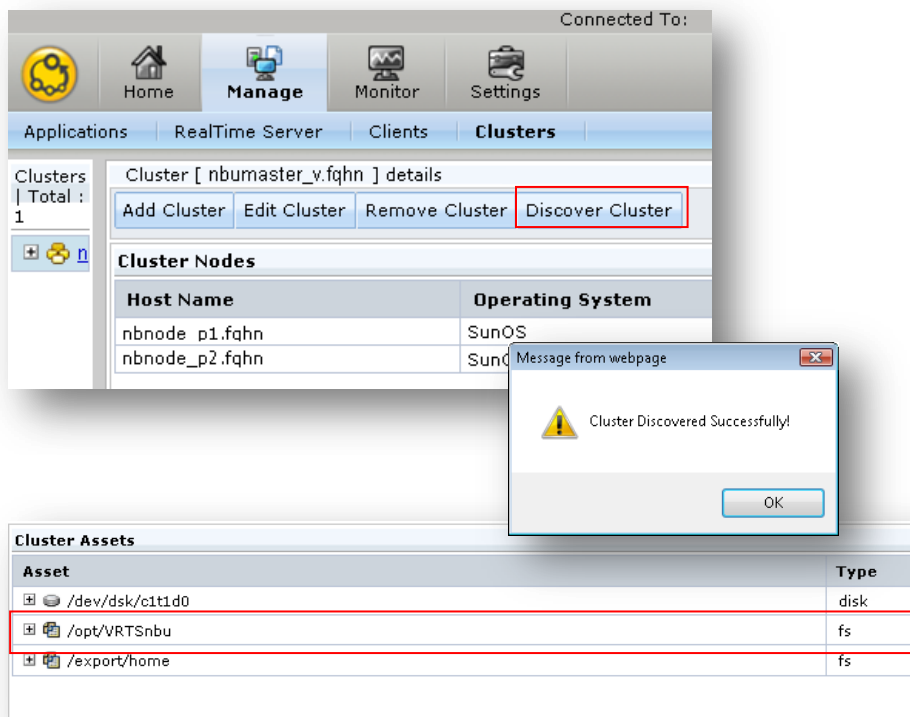
*Step IV: NetBackup RealTime – **Defining the NetBackup Application***

1. Define the NetBackup Application in the RealTime console

   - Verify and if necessary Online* the NetBackup Service Group at the primary site with the following VCS command:
     /opt/VRTSvcs/bin/hagrp –online{ nbu_group} –sys nbnode_p1

     *If NetBackup is configured without a cluster monitor start all the NetBackup services on the Master at the primary site.

   Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

   - Navigate to **Manage>Applications**
     Select **Define Application** from the task pane to open the Application Wizard.
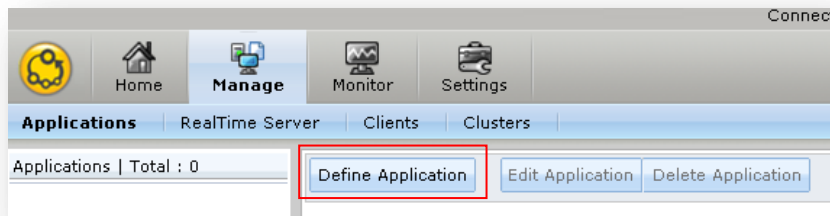
   The Define Application Wizard steps through the workflow to identify the NetBackup Catalog components to RealTime. Verify the prerequisites are satisfied prior to selecting **Next.**
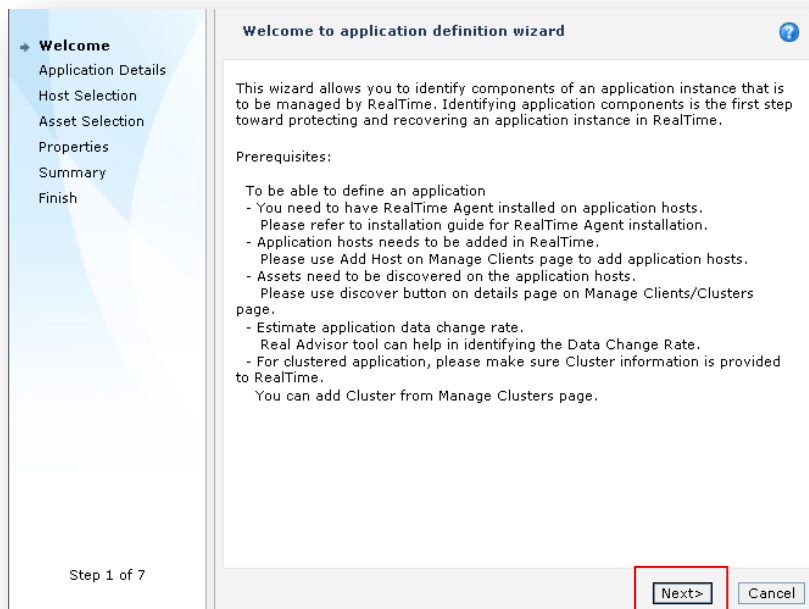
Enter a name to assign to the application in RealTime, keeping in mind this is the primary location for the NetBackup Catalog. Optionally, add the file system, Department, Criticality, and detail as desired.
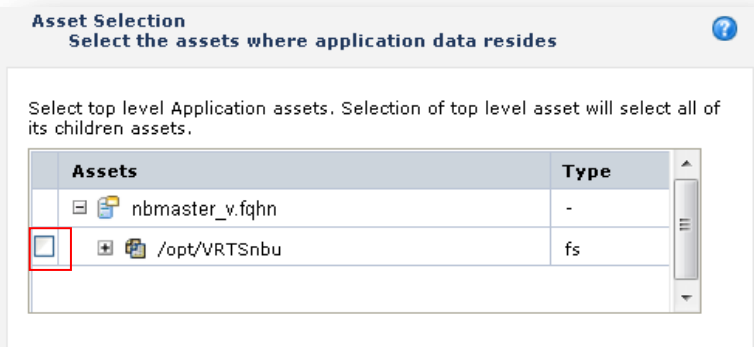

If a cluster monitor was defined in RealTime select the cluster name (*nbmasver_v.fqhn*), otherwise select the node where NetBackup is installed and configured.

Select the checkbox for file system where NetBackup is installed, */opt/VRTSnbu*.

Enter the peak hourly change rate of the NetBackup Catalog. If the change rate is unknown the RealTime Sizing Advisor planning tool can helps determine the write rate for your NetBackup Catalog by analyzing a sample of the catalog writes to the NetBackup Master Server. This is accomplished by collecting a sample of data that represents the application write rate and analyzing this sample of data.
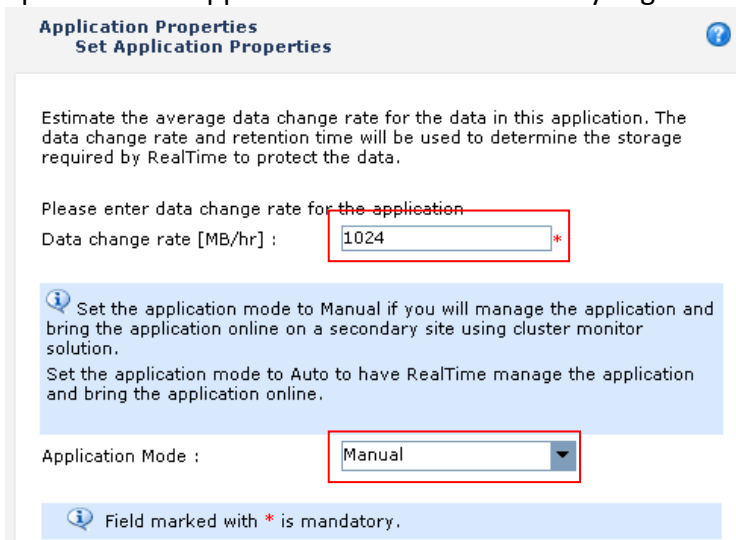
Select **Manual** from the Application Mode drop down list if NetBackup is clustered in the remote site.

Click **Submit** on the summary page to complete the application definition wizard.
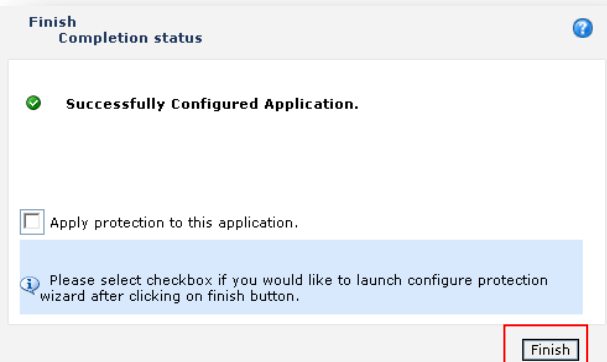
*Step V: NetBackup RealTime – **Remote Mirror Configuration***

1. Define the NetBackup Application in the RealTime console

   Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

   - Navigate to **Manage>RealTime Server**
   Select **Add** from the task pane to open the Add Remote Server Wizard.
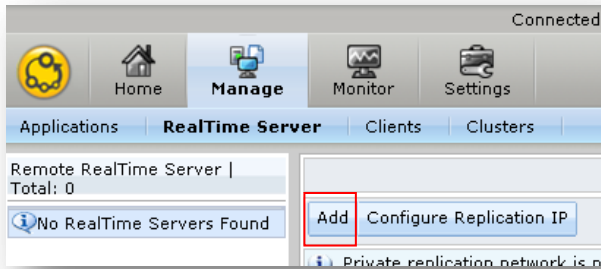
   Enter the details for the RealTime Server and Authentication Broker in the secondary site. Click **Test Authentication** to verify the primary and secondary sites can communicate and the information entered is correct.
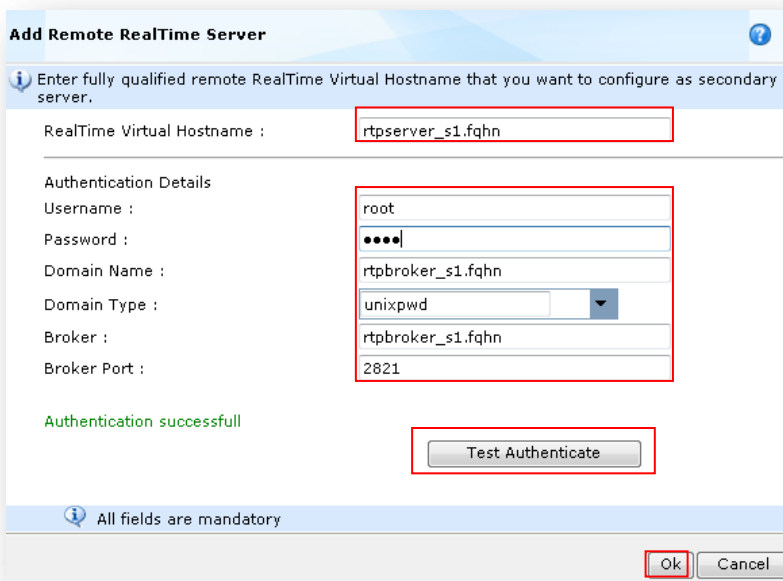
- Navigate to **Manage>Application**
  Select **New** from the Configure Protection task pane on the bottom right panel to open the Configure Protection Wizard.
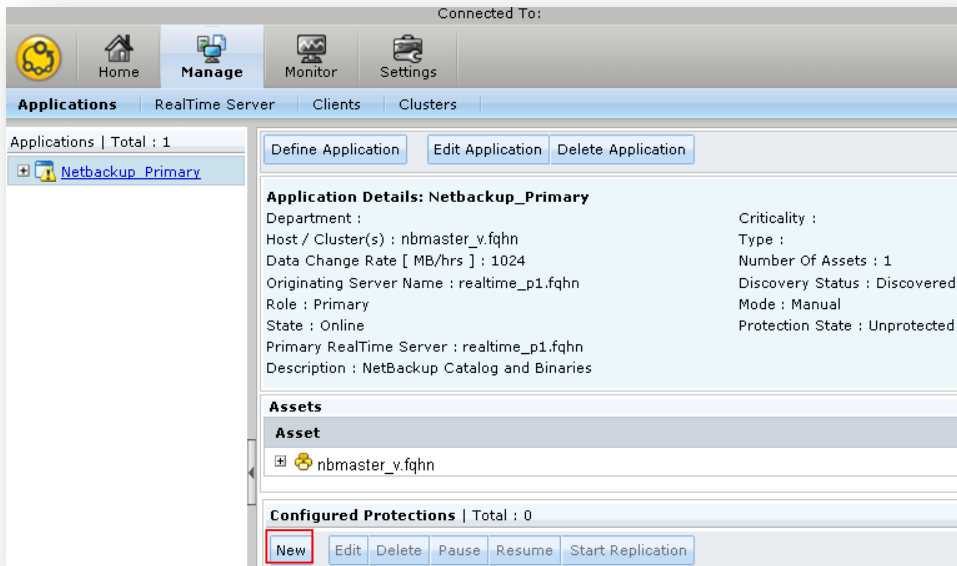
The Configure Protection Wizard steps through the workflow to add replication services to the NetBackup Catalog. Verify the prerequisites are satisfied prior to selecting **Next.**
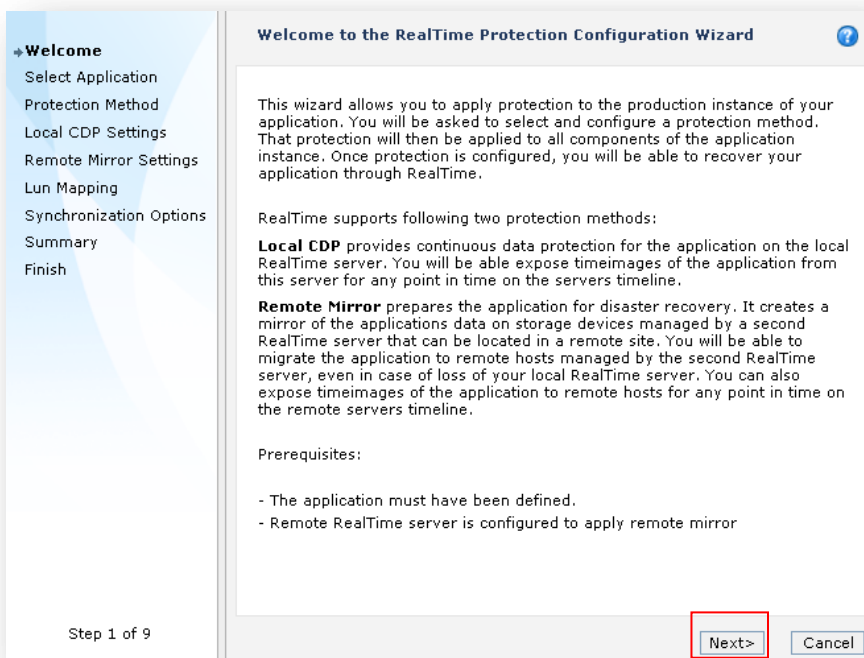
- Select the Remote Mirror checkbox and select the remote RealTime Server

Specify your desired retention time in hours. RealTime allocates RealTime storage on the remote server to this application based on the desired retention time and the estimated data change rate that you specified when you defined the application.

Click **Check Required Storage** to display the storage size required based on the parameters that you entered, and whether the RealTime Server has that amount of storage available. The actual retention time is determined by the amount of storage allocated and the actual data change rate of the application, which may vary over time.
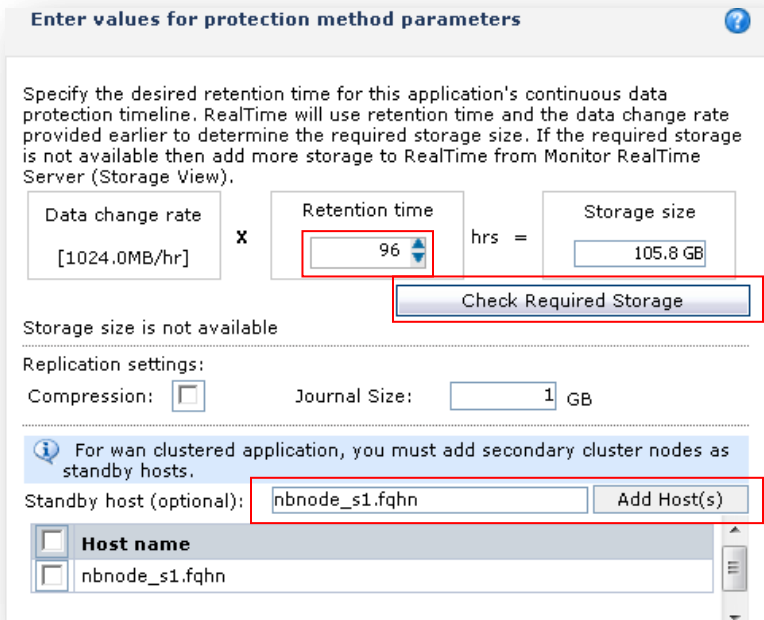

Specify the standby (secondary) hosts, *nbnode_s1*, for the application in the remote site. Specifying a standby host enables the RealTime client component on the standby host to block writes to the secondary LUNs, thus preventing any inadvertent corruption of the replicated data set.

- Allocate the LUNS on the secondary RealTime Server

  For each LUN in NetBackup, select a LUN of matching size to which the application's LUN's data will be replicated. The Secondary LUN drop-down list contains all LUNs of matching size that are visible to the selected remote RealTime Server. If insufficient LUNs are available to complete your map, you must first create and zone LUNs in the remote site to be visible to that RealTime Server.
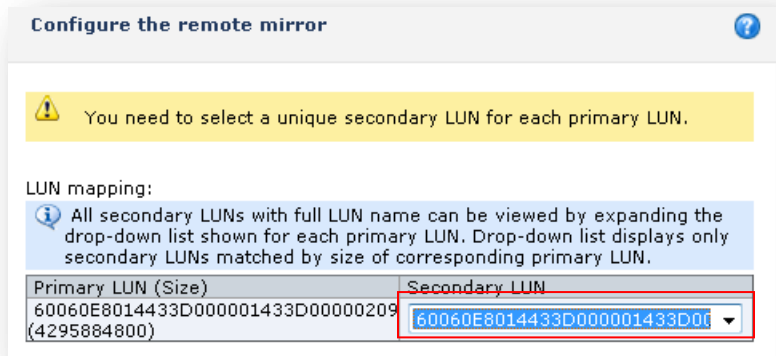
- Start synchronizing the data over the replication link by selecting the radio button next to **Start Automatic Synchronization Now**.
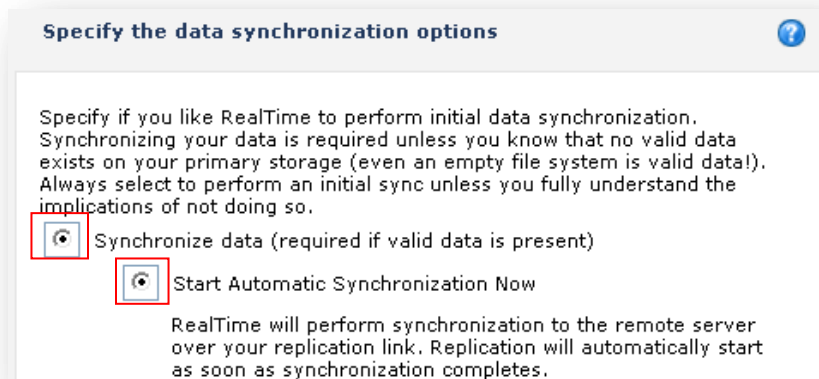
- Click **Submit** from the Summary Page
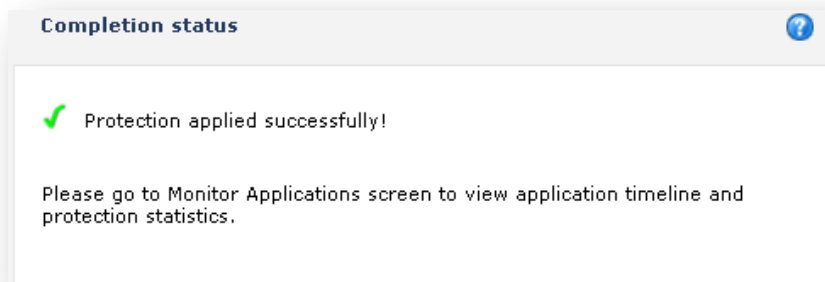
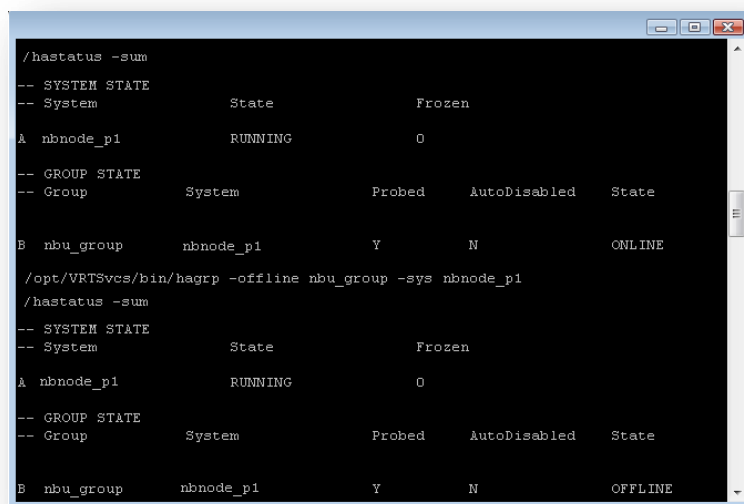*Step VI: NetBackup RealTime – **Testing NetBackup Catalog Migration***

WARNING: *Do not perform any DR tests until primary and secondary are fully synchronized.*
WARNING: *This test is destructive, and results in the primary catalog demoted to secondary.*
Verify your NetBackup catalog is copied to an alternate media prior to executing.

- Verify the status of NetBackup application in RealTime Console from the **Home** screen.   Click on the valid (green) timeline for the NetBackup application on the remote mirror to open the Detail dialog. The Detail dialog should indicate Valid and the start and end time for the replication link.
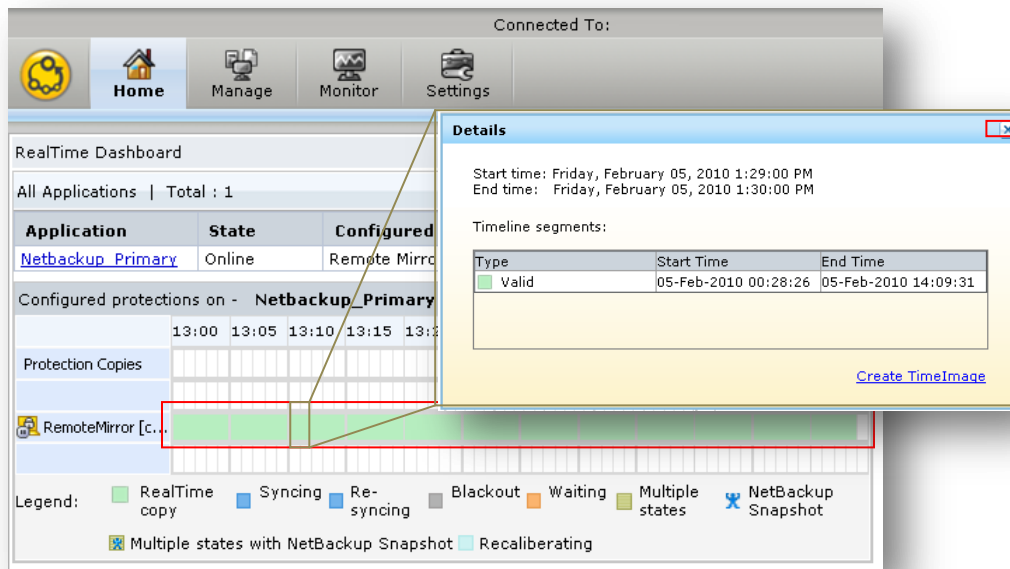

- Offline* the NetBackup service group at the primary site with the VCS command:
opt/VRTSvcs/bin/hagrp –offline{ nbu_group} –sys nbnode_p1


If NetBackup is configured without a cluster monitor stop all the NetBackup services on the Master at the primary site.

symantec.
Confidence in a connected world.

Connect to the RealTime console by pointing your Web browser to a URL similar to the following example: http://rtpserver_p1.domain.com/ and log in with the credential created during the installation process.

- Navigate to **Monitor>Applications**
  Select **Migrate** from the task pane to open the Migrate Application Wizard.
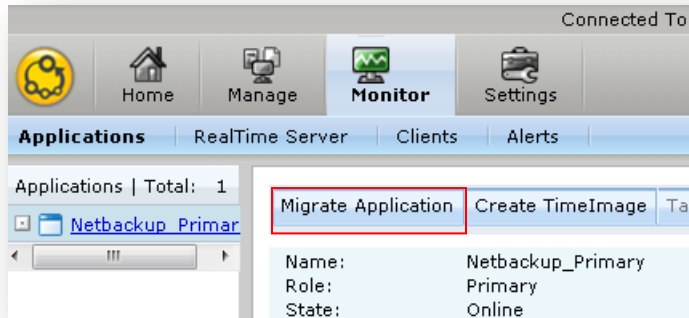
- The Migrate Application Wizard steps through the workflow to migrate the NetBackup catalog between the primary and secondary locations.   Verify the prerequisites are satisfied prior to selecting **Next.**
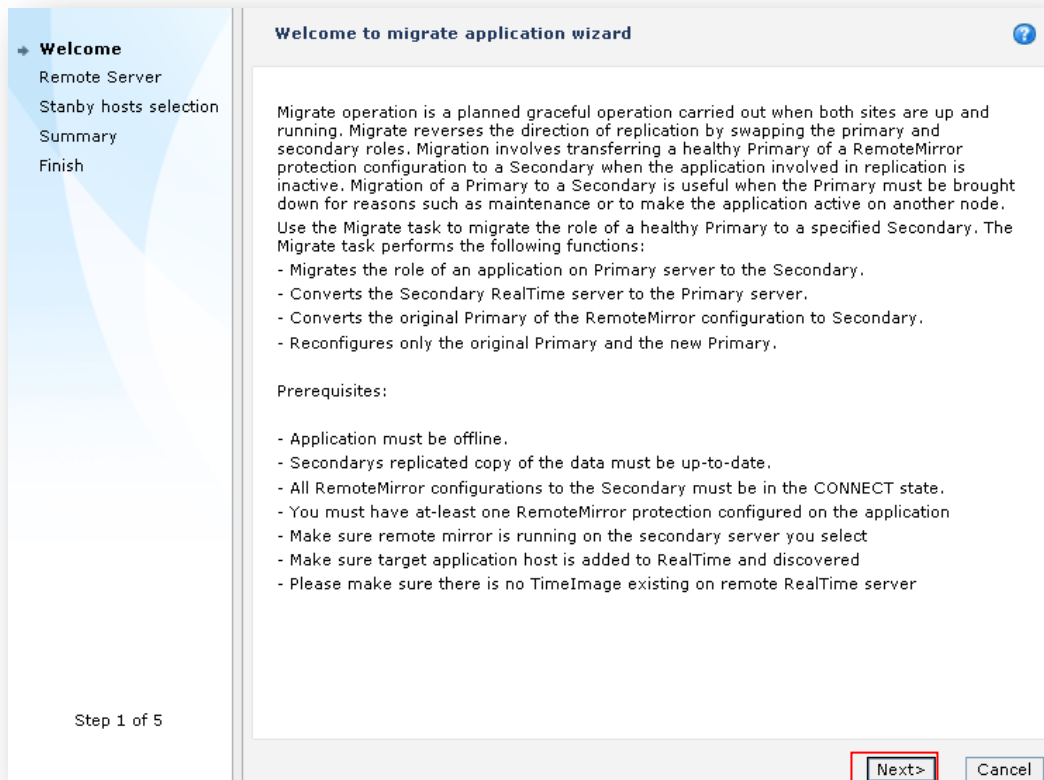
- Select the "*Change application mode to manual*" if NetBackup is installed in a VCS cluster in the primary location.

Enter the Fully Qualified hostname for the standby NetBackup Master Server, for example nbumaster_v.fqhn. The Mount Point should remain the same as the primary site, for example */opt/VRTSnbu*.

Review the summary detail, verify the target directory is not in use, and click **Submit**.

*Step VII: NetBackup RealTime – **Testing Remote Corruption Protection***

WARNING: *Do not perform any DR tests until primary and secondary are fully synchronized.*
WARNING: *This test requires the primary NetBackup Master server be offline during the test and will result in loss of access to the backup environment.*

Navigate to the **Home** screen.   Click on the timeline to open the Detail dialog.
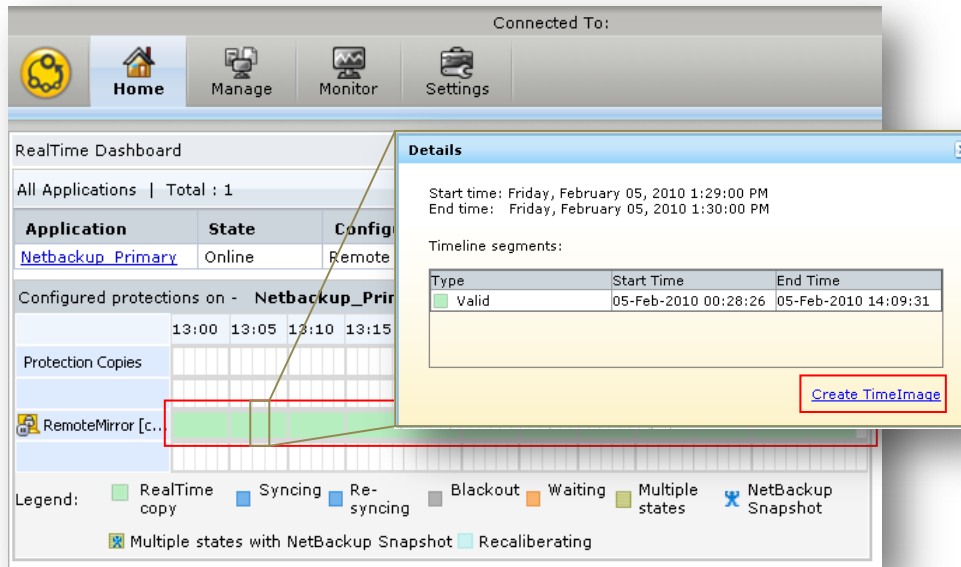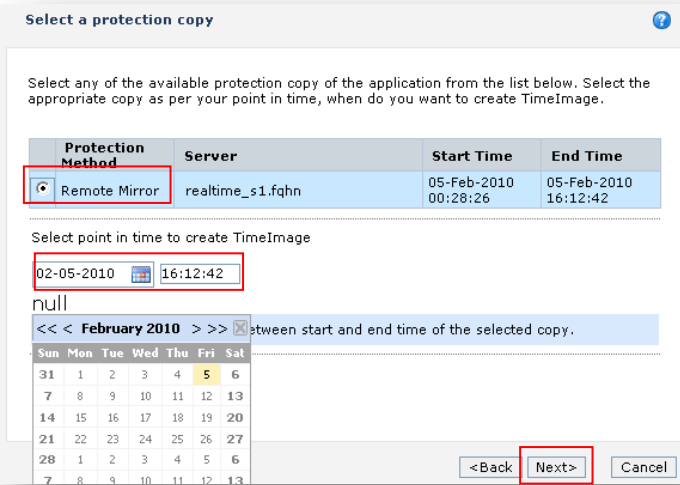
Select Create TimeImage from the Detail dialog to open the TimeImage Wizard.

- The Create Time Image Wizard steps through the workflow to create a Read/Write Virtual LUN of the NetBackup catalog at the secondary location.   Verify the prerequisites are satisfied prior to selecting **Next.**
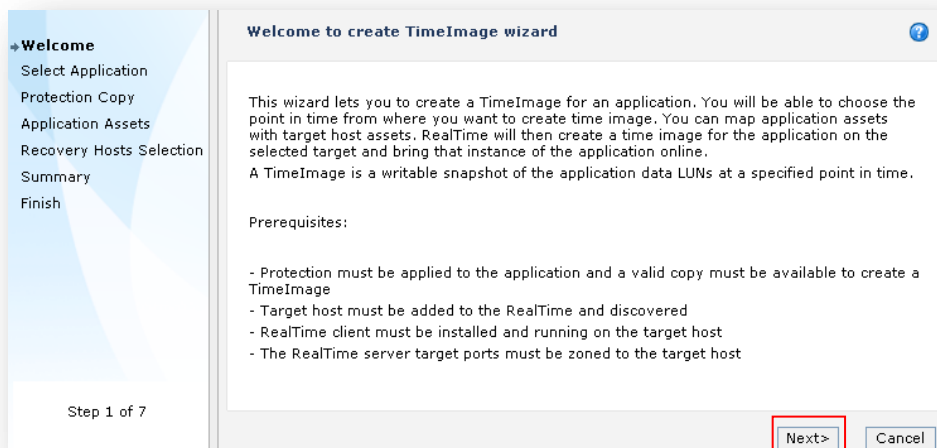
Select Remote Mirror and enter the point in time to provision the TimeImage

Enter the Fully Qualified hostname for the standby NetBackup Master Server. The Mount Point should remain the same as the primary site, for example */opt/VRTSnbu*.

Review the summary detail, verify the target directory is not in use, and click **Submit**.

Completion status

✓ Create TimeImage is successful!

Finish

- Offline* the NetBackup service group at the primary site with the VCS command:
  opt/VRTSvcs/bin/hagrp –offline{ nbu_group} –sys nbnode_p1.

```
/hastatus -sum

-- SYSTEM STATE
-- System                State              Frozen

A  nbnode_p1            RUNNING              0

-- GROUP STATE
-- Group          System           Probed     AutoDisabled    State


B  nbu_group       nbnode_p1        Y          N               ONLINE
 /opt/VRTSvcs/bin/hagrp -offline nbu_group -sys nbnode_p1
 /hastatus -sum
-- SYSTEM STATE
-- System                State              Frozen

A  nbnode_p1            RUNNING              0

-- GROUP STATE
-- Group          System           Probed     AutoDisabled    State


B  nbu_group       nbnode_p1        Y          N               OFFLINE
```

*If NetBackup is configured without a cluster monitor stop all the NetBackup services on the Master at the primary site.

- Online* the NetBackup Service Group at the secondary site with the following VCS
  command: / *opt/VRTSvcs/bin/hagrp –online{ nbu_group} –sys nbnode_s1*

```
nbunode_s1# /opt/VRTSvcs/bin/hastart -onenode
nbunode_s1# /opt/VRTSvcs/bin/hastatus -sum

-- SYSTEM STATE
-- System                State              Frozen

A  nbunode_s1           RUNNING              0

-- GROUP STATE
-- Group          System           Probed     AutoDisabled    State


B  nbu_group       nbunode_s1       Y          N               ONLINE
nbunode_s1#
```
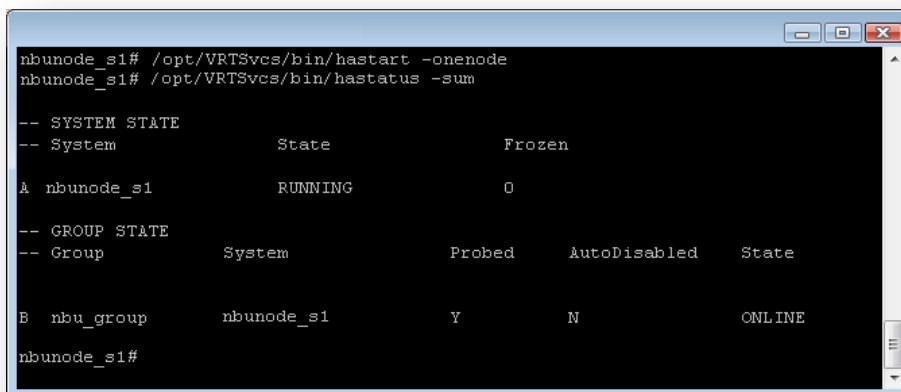
*If NetBackup is configured without a cluster monitor start all the NetBackup services on the Master at the secondary site.

This page intentionally left blank

Glossary

Agent	An agent is used to support host-based features that relate to assets and applications. The agent also performs asset discovery.
Application	An instance of an application. Applications are directly accessed by the user. Examples include: SAP, Share point, NetBackup, a file server, or a database sandbox with SQL server instances.
Authentication Broker	Issues a certificate used by AT clients to communicate with each other.
Blackout Window	A window of time during which the orders of writes may not be recoverable.
Client host	The application hosts that are making use of the RealTime Server Cluster. Also called application hosts.
Cluster	A set of hosts (each termed a node) that share a set of disks and are connected by a set of redundant heartbeat networks. An object in RealTime representing a clustered user application having a virtual host name. An example is an NFS file system with a virtual host name that is clustered using Veritas Cluster Server. The user defines a cluster object in RealTime to represent the application.
Cluster monitor	Cluster manager software. Examples: Veritas Cluster Server (VCS), Microsoft Cluster Server (MSCS).
Clustered application	An instance of a cluster-enabled application. Examples include: Oracle, Exchange.
Configured protection method	Multiple protection methods may be available for each asset group. Protection methods configured to protect the asset group are the configured methods. Multiple configured methods may be applied to an asset group using the same or different protection services to achieve the recovery objectives defined.
Data Change Map (DCM)	The Data Change Map, or DCM, is a bitmap that represents the data difference between the primary and secondary.
local/node failover	A failover of a node among the nodes in a RealTime Server Cluster
Monitor LUN	A dedicated LUN that is used for protecting clustered applications. A monitor LUN is accessible to both application hosts and the RealTime Server. A monitor LUN reliably conveys to the RealTime Server information that is required to move the timeline.
Node death timeout	A tunable parameter that specifies the time interval for which the RealTime Server waits for a heartbeat from a host. After this interval elapses and the RealTime Server does not receive a heartbeat from the host, the RealTime Server marks the host as dead. You can tune the parameter in the /opt/VRTScdpr/config/drl.properties file on the RealTime Server. The Default value is 120 seconds.

Glossary

PR (persistent reservations)	A SCSI-3 feature, which allows hosts to be fenced off from writing to a disk.
Primary site	A site that is designated as primary or current.
Production host	The SAN host on which a targeted application runs. Also called application host, application server, or production server.
Production Storage	Storage that the application uses for reading/writing.
Production Volume	The primary storage for the protected application.
Protection method	The method of protection a protection service provides. Each protection service provides one or more protection methods. Multiple protection methods may be available for each asset group. Examples include: RealTime, Snapshot, Replication, D2D, and D2T.
Protection service	A protection service is used to protect asset groups. A protection service provides one or more protection methods. Examples include: RealTime (Recovery Server or Recovery Cluster), NetBackup, and Enterprise Vault.
Protection service storage	The collection of storage that a protection service uses for collecting the time-ordered writes. RealTime Storage is one form of protection service storage.
RealTime user interface	The graphical user interface (GUI) and command line interface (CLI) that drive the RealTime Server Cluster.
RealTime Server	A soft appliance operating in Fibre Channel SANs that provides data protection recovery services
RealTime Storage	The collection of storage that the RealTime Server cluster uses for collecting the time-ordered writes. Internally, the collection may be broken up, such as into a Production Image storage, an Indexing storage, a Log, a Journal storage or scratch space for holding writes to a TimeImage, or an Event storage
Recovery Host	A host that drives the recovery and restoration of the production data after a failure. This is a NetBackup term designating the host that drives the recovery.
RealTime agent	A CORBA-based service installed on application hosts. The RealTime agent exposes interfaces for running scripts on the application hosts. The output and the exit status of the scripts are communicated back to RealTime. Scripts are pushed to the agent every time they are executed.
Secondary site	A site that is designated as a disaster recovery site. In case the primary site is unavailable, the secondary site becomes the primary. The roles are reversible. Also called remote site.
Sideband	A sideband appliance means that it is not in the path of the I/O. If a sideband appliance dies, it does not affect the application.

NETBACKUP 7 COOKBOOK SERIES

Glossary

Soft appliance	A term for packaging software that runs on a standard x86 box. No specialized hardware or ASICs are required. Also called RealTime Server
Target host bus adapter	The host bus adapter that provides the interface for I/O between an application host SAN and the RealTime Server
Target mode driver	A target mode driver implementation, which provides virtual targets in a Fibre Channel fabric. Also called ISP driver.
TimeImage	An exact reproduction of a specified Consistency Group at a specific point in time. When the RealTime Server generates a TimeImage view, that image is made available via new virtual host-side TimeImage volumes. A SAN host, used specifically as the TimeImage host, can access the TimeImage view just as if it were the up-to-date RealTime Server Consistency Group, and can manipulate the TimeImage Consistency Group. However, the TimeImage view is completely independent of the up-to-date Consistency Group maintained in the MirrorStore volume.
TimeImage host	A host on the SAN used to access a TimeImage view. The TimeImage host relies exclusively on the TimeImage view for its data storage; the host treats the TimeImage view as its up-to-date application Consistency Group. As a consequence, the TimeImage host cannot also be the production host; the hosts must be two different SAN hosts.
TimeImage volume	A virtual host-side volume that allows a TimeImage host on the SAN to access a TimeImage. The RealTime Server exports these volumes to the SAN when a TimeImage is generated.
Timeline	The record of all changes made to the application Consistency Group, maintained by the RealTime Server as a result of the data capture process. When data capture is initiated, that is, when the timeline is started, the appliance begins capturing all writes made to the Consistency Group via the virtual volumes. This record of write transactions is saved in the timeline and is what the system uses when it creates a TimeImage or performs a restore. Thus, the timeline represents the window during which the RealTime Server has been protecting the targeted application's Consistency Group, as well as the repository from which an historical image of the Consistency Group can be recreated.
TimeStore daemon	A daemon that implements the RealTime Virtualization layer and Manages TimeStore for each Consistency Group.

Glossary

vLUN (virtual logical unit number)	A LUN that is virtual LUN for the RealTime Server, and is exposed by the RealTime target mode driver. A vLUN is treated as a normal LUN by an application host.
VSA (volume set addressing)	An addressing scheme that uses virtual busses, targets, and LUNs to increase greatly the number of LUNs that can be addressed on a target port. Volume Set Addressing is supported for HP-UX.
WWN(world wide name)	A unique, worldwide, 64-bit unsigned name identifier. A RealTime Server-internal World Wide Name is a name that is used internally by the RealTime Server but is not exported to the SAN.
WWNN (world wide node name)	A unique, worldwide, 64-bit identifier assigned to each Fibre Channel node process.
WWPN(world wide port name)	A unique, worldwide, 64-bit identifier assigned to each Fibre Channel port. It is Analogous to the Ethernet/MAC address in the IP world