



Red Hat Reference Architecture Series

Red Hat Enterprise Virtualization Backup and Recovery

Using Symantec™ NetBackup™

Brett Thurber, RHCA, RHCVA
Sr. Software Engineer

Version 1.0
July 2011





1801 Varsity Drive™
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

Linux is a registered trademark of Linus Torvalds. Red Hat, Red Hat Enterprise Linux and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Symantec and NetBackup are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

UNIX is a registered trademark of The Open Group.

Intel, the Intel logo, Xeon and Itanium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

© 2011 by Red Hat, Inc. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, V1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

The information contained herein is subject to change without notice. Red Hat, Inc. shall not be liable for technical or editorial errors or omissions contained herein.

Distribution of modified versions of this document is prohibited without the explicit permission of Red Hat Inc.

Distribution of this work or derivative of this work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from Red Hat Inc.

The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Send us feedback at refarch-feedback@redhat.com



Table of Contents

1 Executive Summary.....	5
2 Red Hat Virtualization.....	6
2.1 Kernel Virtual Machine.....	6
2.2 Red Hat Enterprise Virtualization.....	7
3 Symantec NetBackup.....	10
4 Reference Architecture Configuration.....	12
4.1 Environment.....	12
4.1.1 NetBackup Specifics.....	12
4.1.1.1 Network Configuration.....	12
4.1.1.2 Name Resolution.....	13
4.1.1.3 Clients.....	13
4.1.1.4 Policies.....	13
4.1.1.5 Media.....	14
4.1.1.6 Licensing.....	14
4.1.1.7 Security.....	15
4.1.2 Red Hat Enterprise Virtualization Agents.....	16
4.2 Software Configuration.....	17
4.2.1 Operating Systems.....	17
4.2.2 Applications, Tools and Packages.....	17
4.3 Hardware Configuration.....	18
4.3.1 Servers.....	18
4.3.2 Storage.....	19
5 Backup and Restore of Virtual Machines.....	21
5.1 Red Hat Enterprise Linux Agent Installation.....	21
5.1.1 Policies.....	24
5.2 Microsoft Windows Client Installation.....	26
5.2.1 Policies.....	27
5.3 Backup.....	30
5.4 Restore.....	33
5.4.1 Red Hat Enterprise Linux File Level Recovery.....	33
5.4.2 Microsoft Windows File Level Recovery.....	37
5.4.3 Full Virtual Machine Restore.....	40



5.4.3.1 Red Hat Enterprise Linux.....	40
5.4.3.2 Microsoft Windows.....	45
5.4.3.3 Bare Metal Restore.....	52
6 Backup and Restore of Red Hat Enterprise Virtualization Manager.....	53
6.1 NetBackup Client Installation.....	53
6.2 NetBackup Microsoft SQL Agent Configuration.....	53
6.2.1 Backup Policy Creation.....	58
6.3 Backup.....	58
6.4 Restore.....	59
6.4.1 Partial.....	59
6.4.1.1 RHEV-M Application Failure.....	59
6.4.1.2 RHEV-M DB Corruption.....	62
6.4.2 Full RHEV-M Machine Crash.....	66
7 Conclusion.....	69
Appendix A: NetBackup SQL Backup and Restore Batch Files.....	70
Appendix B: Host Configuration Files.....	72
Appendix C: Iptables.....	73
Appendix D: RHEV-M Backup and Recovery Boot from SAN.....	75
D.1 Environment Setup.....	75
D.2 Snapshot of RHEV-M OS LUN.....	76
D.3 Recovering RHEV-M from Snapshot LUNs.....	79
D.4 Additional RHEV-M Backup and Recovery.....	80
Appendix E: Contributors.....	81
Appendix F: References.....	82



1 Executive Summary

More and more enterprise customers are migrating to and relying on virtualization platforms to provide mission critical services to end users. As this transition continues to grow at a rapid pace, it becomes necessary to protect data and ensure business continuity is maintained due to an unforeseen or unscheduled failure that may result in possible downtime.

A recent survey conducted by Coleman Parkes Research Ltd.¹ reports the amount of downtime and cost in North America during calendar year 2010 indicates an average downtime of 10 hours per incident at a cost of \$26.5 billion annually. By incorporating and testing backup and restore capabilities based on industry best practices, IT departments can work to mitigate this risk and reduce exposure.

Backup and recovery consists of multiple layers of data protection to include:

- Database – typically consists of using a client or agent which has the ability to quiesce a particular database type
- Operating System – includes the ability to backup specific operating system details such as system state and Active Directory with Microsoft Windows
- File Level – refers to backing up and restoring a file or set of files as opposed to an entire disk drive, database or operating system
- Snapshot – a point-in-time, read-only, disk-based copy of a client volume similar to VM snapshots with Red Hat Enterprise Virtualization
- Bare Metal – provides the ability to take a backup of a machine and restore to a previous state without the need for previously installed software

Deciding upon and implementing proper backup policies is just as important as determining what data to backup. This may include the types of backups to perform such as differential, incremental and full. Retention policies may also impact selection and type of backups depending on the needs of the business and federal requirements such as those outlined in the Sarbanes-Oxley Act².

The goal of this paper is not intended to cover all backup and recovery scenarios, however it is meant to provide guidance for proper data backup and recovery for customers utilizing Red Hat Enterprise Virtualization in combination with Symantec NetBackup to include the following:

- Virtual Machine
 - File level backup and restore
 - Virtual Machine recovery
- Red Hat Enterprise Virtualization Manager
 - Application backup and recovery
 - Database backup and recovery
 - Full system recovery

The assumption made is that an operational NetBackup and Red Hat Enterprise Virtualization environment are configured and running.



2 Red Hat Virtualization

2.1 Kernel Virtual Machine

A hypervisor is a computer software platform that allows multiple “guest” operating systems to run concurrently on a host computer. The guest virtual machines interact with the hypervisor which translates guest I/O and memory requests into corresponding requests for resources on the host computer.

Running fully-virtualized guests, i.e., guests with unmodified guest operating systems, used to require complex hypervisors and previously incurred a performance penalty for emulation and translation of I/O and memory requests.

Over the last few years chip vendors Intel and AMD have been steadily adding CPU features that offer hardware enhancements to support virtualization. Most notable are:

1. First-generation hardware assisted virtualization: Removes the requirement for hypervisor to scan and rewrite privileged kernel instructions using Intel VT (Virtualization Technology) and AMD's SVM (Secure Virtual Machine) technology.
2. Second-generation hardware assisted virtualization: Offloads virtual to physical memory address translation to CPU/chip-set using Intel EPT (Extended Page Tables) and AMD RVI (Rapid Virtualization Indexing) technology. This provides significant reduction in memory address translation overhead in virtualized environments.
3. Third-generation hardware assisted virtualization: Allows PCI I/O devices to be attached directly to virtual machines using Intel VT-d (Virtualization Technology for directed I/O) and AMD IOMMU. Also, SR-IOV (Single Root I/O Virtualization) which allows special PCI devices to be split into multiple virtual devices. This provides significant improvement in guest I/O performance.

The great interest in virtualization has led to the creation of several different hypervisors. However, many of these pre-date hardware-assisted virtualization, and are therefore somewhat complex pieces of software. With the advent of the above hardware extensions, writing a hypervisor has become significantly easier and it is now possible to enjoy the benefits of virtualization while leveraging existing open source achievements to date.

Kernel-based Virtual Machine (KVM)³ turns Linux into a hypervisor. Red Hat Enterprise Linux 5.4 and later provided the first commercial-strength implementation of KVM, which is developed as part of the upstream Linux community.



2.2 Red Hat Enterprise Virtualization

Virtualization offers tremendous benefits for enterprise IT organizations – server consolidation, hardware abstraction, and internal clouds deliver a high degree of operational efficiency.

The Red Hat Enterprise Virtualization portfolio is an end-to-end virtualization solution, with use cases for both servers and desktops, designed to overcome current IT challenges for consolidation, enable pervasive data center virtualization, and unlock unprecedented capital and operational efficiency. The Red Hat Enterprise Virtualization portfolio builds upon the Red Hat Enterprise Linux platform that is trusted by thousands of organizations on millions of systems around the world for their most mission-critical workloads. Combined with KVM, the latest generation of virtualization technology, Red Hat Enterprise Virtualization delivers a secure, robust virtualization platform with unmatched performance and scalability for Red Hat Enterprise Linux and Windows guests.

Red Hat Enterprise Virtualization consists of the following two components:

- **Red Hat Enterprise Virtualization Manager:** A feature-rich virtualization management system that provides advanced capabilities for hosts and guests.
- **Red Hat Enterprise Virtualization Hypervisor:** A modern hypervisor based on KVM which can be deployed either as a standalone bare metal hypervisor (included with Red Hat Enterprise Virtualization), or as Red Hat Enterprise Linux 5.4 and later (purchased separately) installed as a hypervisor host.

Comparison between Red Hat Enterprise Virtualization Hypervisor (RHEV-H) and Red Hat Enterprise Linux Kernel Virtual Machine Hypervisor (KVM) within Red Hat Enterprise Virtualization:

Feature	RHEV-H	RHEL + KVM
Stateless	Yes	No
Agent Support	No	Yes
Red Hat Network Support for Updates	Yes	Yes
Small Footprint for Enhanced Security	Yes	No
Storage Support (NFS, iSCSI, FC)	Yes	Yes
Automated Install	Yes	Yes
Included with RHEV	Yes	No

Table 2.2-1: Feature Comparison - RHEV-H and RHEL + KVM



Red Hat Enterprise Virtualization consists of the RHEV Manager, used to control the environment, and hosts. The hosts consist of servers that have been deployed with the KVM hypervisor. The hypervisor can be deployed as either a standalone configuration - Red Hat Enterprise Virtualization Hypervisor (RHEV-H), or integrated with a system installed with Red Hat Enterprise Linux 5.4 or later.

A **host** is a physical server which provides the CPU, memory, and connectivity to storage and networks that are used for the virtual machines (VM). The local storage of the standalone host is used for holding the RHEV Hypervisor (RHEV-H) along with logs and enough space for ISO uploads.

A **cluster** is a group of hosts of similar architecture. The requirement of similar architecture allows a virtual machine to be migrated from host to host in the cluster without having to shut down and restart the virtual machine. A cluster consists of one or more hosts, but a host can only be a member of one cluster.

A **data center** is a collection of one or more clusters that have resources in common. Resources that have been allocated to a data center can be used only by the hosts belonging to that data center. The resources relate to storage and networks.

All hosts have a network interface assigned to the logical network named *rhev*. This network is used for the communications between the hypervisor and the manager. Additionally, for the configuration in this paper this network also serves as the public-facing network. Additional logical networks are created on the data center and applied to one or more clusters. To become operational, the host attaches an interface to the local network. While the actual physical network can span across data centers, the logical network can only be used by the clusters and hosts of the creating data center.

Storage is divided into three categories:

- **ISO** - used to contain CD and DVD images and floppy disk images that can be used to install virtual machine Operating Systems and applications. NFS is the only supported type of ISO library storage for Red Hat Enterprise Virtualization.
- **Data** - used for disk images of the virtual machines, snapshots, and storage for templates. The first storage of this type attached to a data center is identified as type *Data (Master)*. Any secondary data storage is identified as type *Data*. Again, any storage is dedicated to only one data center. This storage can be either NFS, iSCSI, or Fibre Channel, however all the data storage for a data center must be of the same type.
- **Export** - used to enable the import or export of virtual machines from one virtualization technology to another. This storage can be either NFS, iSCSI, or Fibre Channel based. An Export domain can only be attached to a single data center at any given time.



Figure 2.2-1: Red Hat Enterprise Virtualization provides a graphical representation of a typical Red Hat Enterprise Virtualization Environment with each component listed.

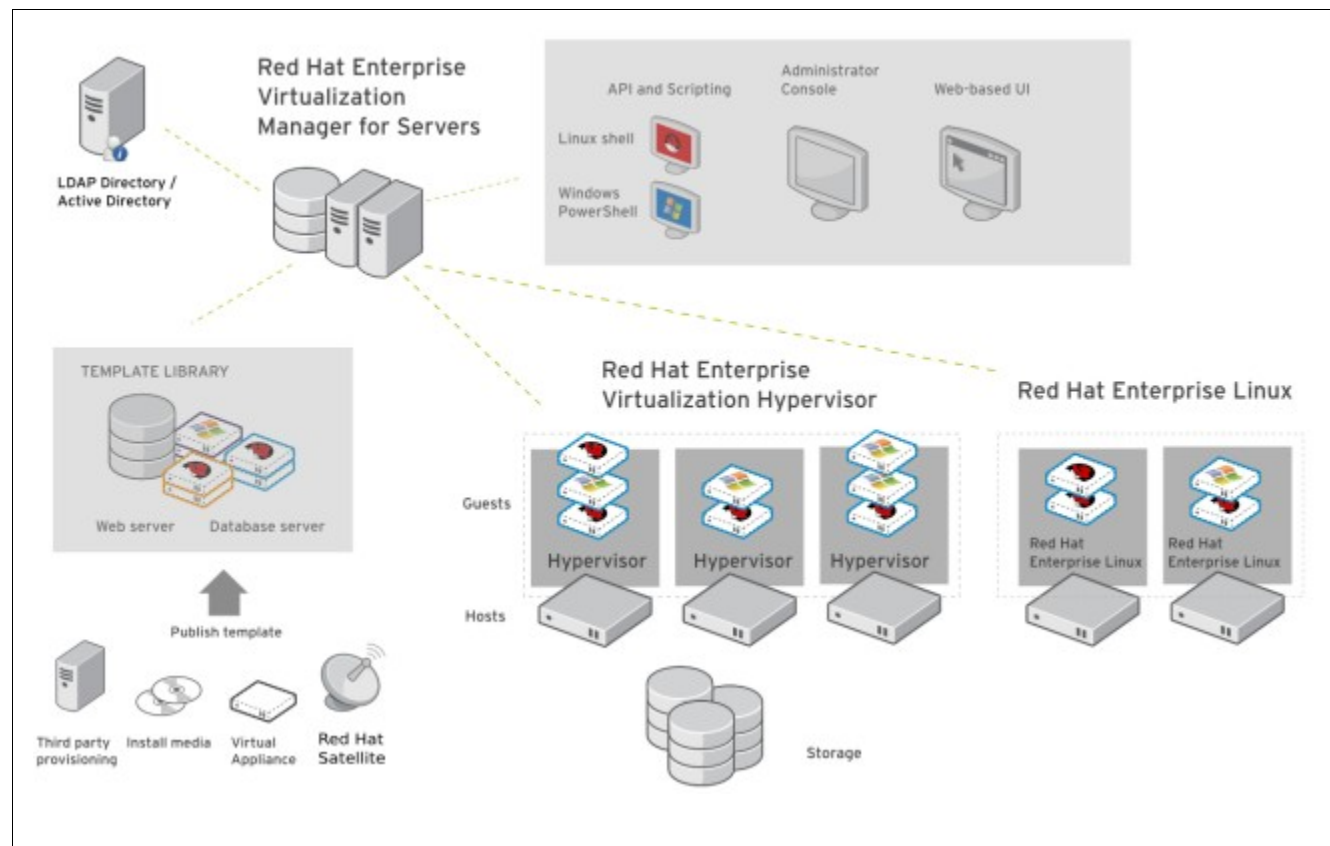


Figure 2.2-1: Red Hat Enterprise Virtualization



3 Symantec NetBackup

The Symantec NetBackup⁴ Platform simplifies the protection of your information-driven enterprise by automating advanced technologies and standardizing operations across applications, platforms, and virtual environments. That means being able to protect completely, store efficiently, recover anywhere, and manage centrally across heterogeneous operating systems and storage hardware including tape and disk. Integrated deduplication and replication helps customers improve storage efficiency, infrastructure use, and recovery times. A single console offers multi-site monitoring, analytics, and reporting, which allows customers to standardize operations and risk management. Used by companies around the world, Symantec NetBackup easily scales to protect the largest UNIX, Windows, and Linux environments.

The NetBackup Platform consists of the following Symantec products:

- NetBackup
- NetBackup Appliances
- NetBackup RealTime
- OpsCenter Analytics
- Enterprise Vault

Features of Symantec NetBackup include:

- Heterogeneous data protection—Protection across heterogeneous operating systems, applications, hypervisors, and both disk and tape architectures
- Centralized management—Increase efficiencies by managing all data protection technologies and multiple NetBackup servers and domains from one location
- Source and target data deduplication —Easily deploy and manage deduplication wherever needed, from remote offices to the data center
- Turnkey solution —NetBackup appliances for quickly deploying NetBackup backup and deduplication technologies
- Deep integration with storage appliances —The NetBackup OpenStorage API enables centralized management of deduplication and replication
- Effective disaster recovery—Fully automated and integrated system recovery with NetBackup Bare Metal Restore, built-in replication, and offsite tape management
- Highly scalable —Benefit from a flexible, three-tiered architecture that scales with the needs of today's growing data center
- Comprehensive data security—Flexible encryption technologies for maximum data security while in transit or in media
- Fast, granular recovery of data from applications—Quickly restore files, emails and other granular items



Figure 3-1: NetBackup Capabilities provides a graphical representation of Symantec NetBackup features.



Figure 3-1: NetBackup Capabilities



4 Reference Architecture Configuration

4.1 Environment

The following section details the reference architecture configuration used in this guide as depicted in **Figure 4.1-1: Logical Network Diagram**.

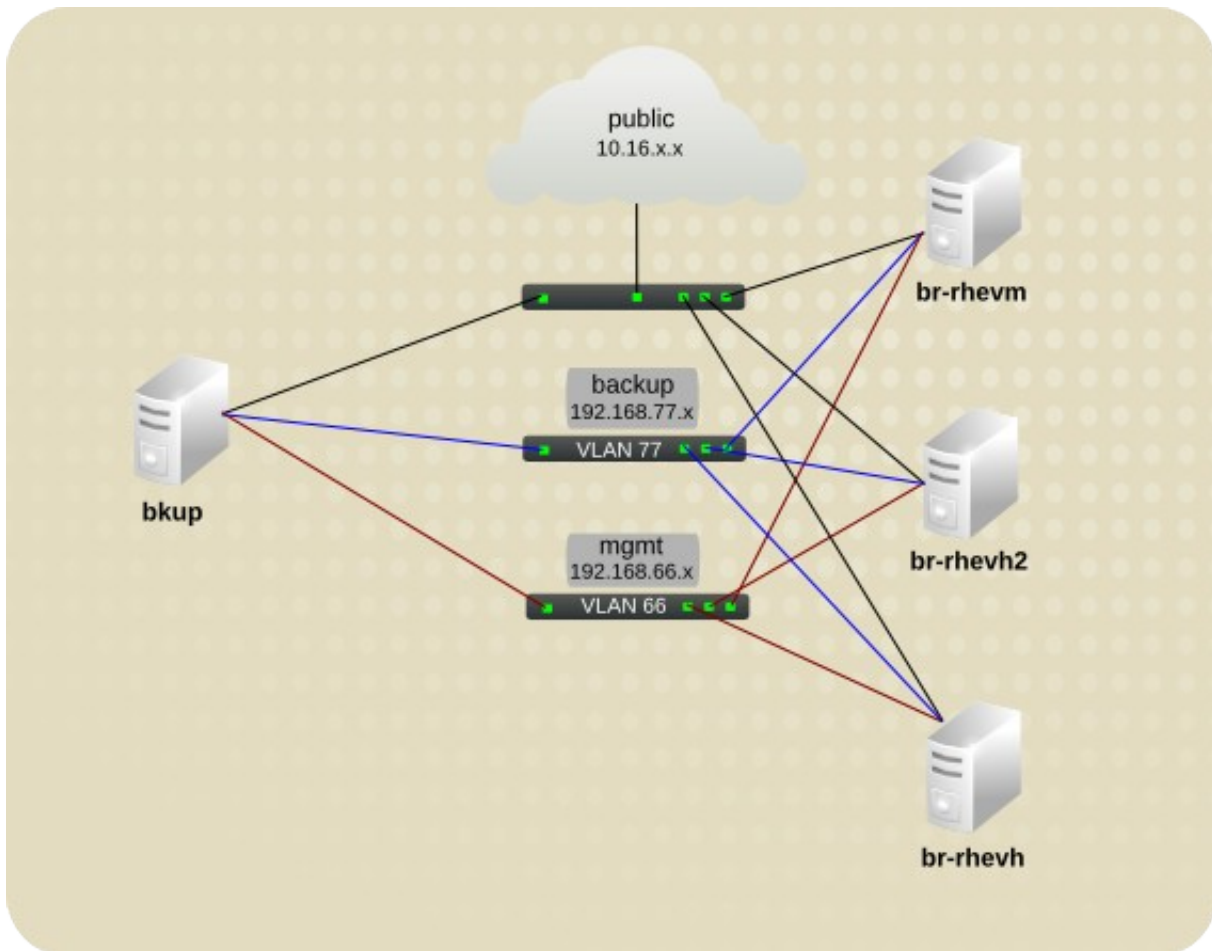


Figure 4.1-1: Logical Network Diagram

4.1.1 NetBackup Specifics

4.1.1.1 Network Configuration

When performing over-the-network backup and recovery, it is recommended to segregate traffic to a dedicated network to prevent saturation over the public network. There is no set rule of thumb when determining the need to segregate traffic. Recommendations vary based on specific environment needs to include the number of machines targeted for backup, amount of data to archive and network bandwidth utilization. Backups tend to run during non-peak hours of operation however restores can take place at any time. For this reference environment, VLAN 77 (192.168.77.x) was configured within RHEV and added to the NetBackup master server for dedicated communication between the machines.



4.1.1.2 Name Resolution

Symantec NetBackup depends greatly on proper name resolution. Within this reference environment, DNS is used for the public network for name resolution and host files are used for the dedicated backup network however DNS can be used for each network or in conjunction with host files. Example host configuration files can be found at **Appendix B: Host Configuration Files**.

4.1.1.3 Clients

The NetBackup client must be installed and running on each client machine selected for backups. This allows for backing up files, database files, bare metal recovery, and specific operating system files such as system state and Active Directory for Microsoft Windows. For this reference environment, each NetBackup client was configured to use the private hostname of the master NetBackup server to direct traffic over the *backup* network.

4.1.1.4 Policies

Table 4.1.1.4-1: Backup Policies describes the backup policies used in this reference environment. Specific policy configuration may be determined by environment needs and should be adjusted accordingly.

Policy	Clients	Type	Schedule and Retention
Linux_VMs	br-rhel56; br-rhel6	Standard	Differential – every 6 hours; 1 day Full – every day; 2 weeks
RHEVH2_OS	bkup	Standard	Full – every day; 1 month
RHEVH_DATA	bkup	Standard	Full – every day; 1 month
RHEVM_OS	br-rheVM	MS-Windows	Differential – every 2 hours; 1 day Full – every day; 2 weeks
RHEVM_SQL	br-rheVM	MS-SQL- Server	Full – every day; infinity
Windows_AD_ VMs	br-w2k8- ad	MS-Windows	Differential – every 2 hours; 1 day Full – every week; 2 weeks

Table 4.1.1.4-1: Backup Policies



4.1.1.5 Media

Backup media configured for this reference environment consists of backup to disk. A 1TB LUN was presented to the master server, *bkup*, and configured as the destination for backup jobs within the backup policies. **Figure 4.1.1.5-1: Backup to Disk Media** provides a list of the storage units configured for backup to disk. *backupArea* was the primary target used.

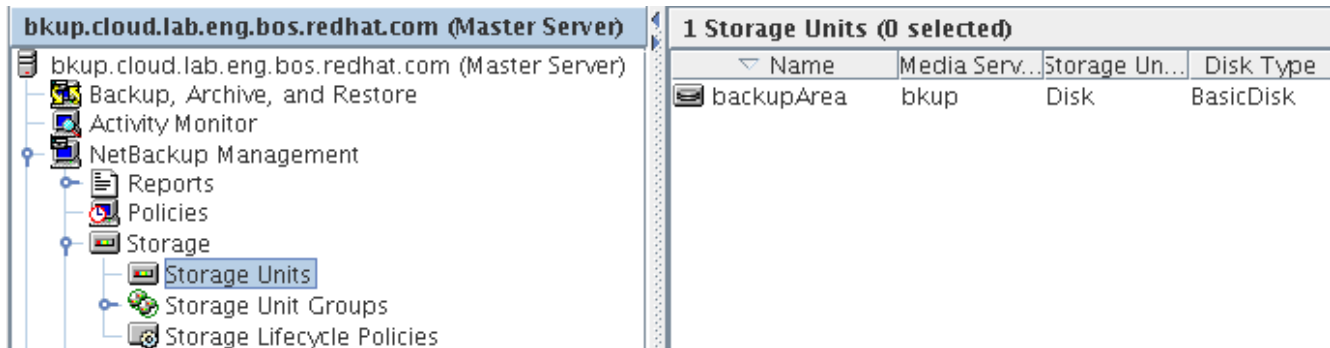


Figure 4.1.1.5-1: Backup to Disk Media

4.1.1.6 Licensing

Although the purpose of this guide is not focused on licensing, it is important to have several NetBackup features license in order to complete the necessary backup operations within a Red Hat Enterprise Virtualization environment. To verify NetBackup is licensed properly to perform the necessary backup operations, choose *Help* and *License Keys* within the NetBackup console as shown in **Figure 4.1.1.6-1: Access NetBackup License Keys**.

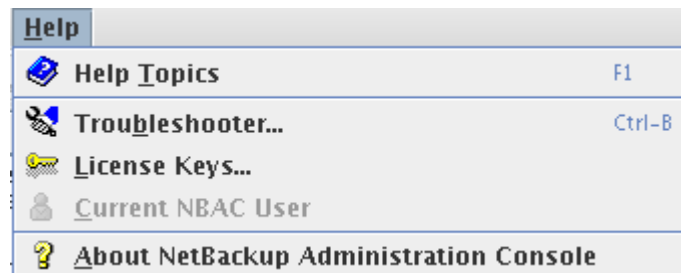


Figure 4.1.1.6-1: Access NetBackup License Keys

Minimum licensing needs are:

- MS SQL Server extension
- Base NetBackup
- Open File Backup

Note: Additional license needs may be required depending on specific environment configuration.



4.1.1.7 Security

Ports⁵

The following port(s) were configured and open between clients and servers in this reference environment:

Service	Port	Protocol
vnetd	13724	TCP
bpcd	13782	TCP

Table 4.1.1.7-1: Services and Ports NetBackup

Note: Additional ports may need to be open depending on specific environment and configuration needs.

Iptables was enabled on all Red Hat systems and appropriate ports opened in this reference environment. Example iptables configuration files are located at **Appendix C: Iptables**.

The following Windows Firewall⁶ rules were created to allow communication between the NetBackup master server and the Microsoft client machines:

Name	Profile	Protocol	Local Port	Action	Remote Address
NetBackup vnetd	All	TCP	13724	Allow	Any
NetBackup bpcd	All	TCP	13782	Allow	Any

Table 4.1.1.7-2: Windows Firewall Rules

SELinux

SELinux was enabled and enforcing on all Red Hat machines in this reference environment unless otherwise noted.



4.1.2 Red Hat Enterprise Virtualization Agents

Red Hat Enterprise Virtualization Manager (RHEV-M) requires that both the Microsoft SQL database and Windows operating system be properly backed up. In addition to installing and configuring the NetBackup client, the Microsoft SQL client must be configured as well.

There are several methods to performing a backup of a Red Hat Enterprise Virtualization Hypervisor (RHEV-H) machine to include LUN snapshots and direct LUN data backups for boot from SAN installations. **Appendix D: RHEV-M Backup and Recovery Boot from SAN** outlines steps for performing off-line backup and recovery for boot from SAN RHEV-M or RHEV-H. Advantages of boot from SAN include:

- LUN copy – perform an off-line image copy of the boot LUN to another. This can be used as a point-in-time recovery option in the event of a LUN failure. In the case of RHEV-M, the backup LUN can be attached to a server with like hardware and brought on-line minimizing downtime impact.
- Off-site backup – it may be desired to perform a raw level backup of a SAN LUN for off-site storage.
- Datacenter redundancy – some SAN vendors provide utilities that allow for LUN replication between primary and secondary datacenter sites.

Symantec NetBackup provides the capability to integrate with various SAN vendor utilities to perform backup consistent LUN snapshots. This method can be used as a viable alternative to off-line direct LUN copies if desired.

Note: RHEV-H does not support the installation of backup clients as it is stateless. Generally it is not considered a great need to backup as re-installing is painless and simple to perform in the event of a failure.



4.2 Software Configuration

4.2.1 Operating Systems

Operating systems with revisions used as referenced in **Table 4.2.1-1: Operating System Revisions**.

Software	Role	Version
Windows Server 2008 R2	RHEV-M Host	6.1.7600
Red Hat Enterprise Virtualization Hypervisor (RHEV-H)	Hypervisor	5.6-10.2.el15 KVM 83-224.el15
Red Hat Enterprise Linux (RHEL)	NetBackup Host	5.5 2.6.18-194.17.1.el5
Windows Server 2008 R2	Virtual Machine	6.1.7600
Red Hat Enterprise Linux (RHEL)	Virtual Machine	6.0 2.6.32-71.el16
Red Hat Enterprise Linux (RHEL)	Virtual Machine	5.6 2.6.18-238.el15

Table 4.2.1-1: Operating System Revisions

4.2.2 Applications, Tools and Packages

Applications, tools and package revisions used as referenced in **Table 4.2.2-1: Applications, Tools and Package Revisions**.

Software	Version
Red Hat Enterprise Virtualization Manager (RHEV-M)	2.2.4.52920
Symantec NetBackup	7.0

Table 4.2.2-1: Applications, Tools and Package Revisions



4.3 Hardware Configuration

4.3.1 Servers

Server hardware with configuration specifics used as referenced in **Table 4.3.1-1: Server Hardware**.

Hardware Systems	Specifications
NetBackup Host [1 x HP ProLiant BL460c G6]	Quad Socket, Quad Core (16 cores) Intel® Xeon® CPU X5550 @2.67GHz, 48GB RAM
	2 x 146 GB SAS internal disk drive (mirrored)
	2 x QLogic ISP2532-based 8Gb FC HBA
	2 x Broadcom NetXtreme II BCM57711E Flex-10 10Gb Ethernet Controller
RHEV-H Systems [2 x HP ProLiant BL460c G6]	Quad Socket, Quad Core, (16 cores) Intel® Xeon® CPU W5550 @2.67GHz, 48GB RAM
	2 x 146 GB SAS internal disk drive (mirrored)
	2 x QLogic ISP2532-based 8Gb FC HBA
	2 x Broadcom NetXtreme II BCM57711E Flex-10 10Gb Ethernet Controller
RHEV-M Host [1 x HP ProLiant BL460c G6]	Quad Socket, Quad Core (16 cores) Intel® Xeon® CPU X5550 @2.67GHz, 48GB RAM
	2 x 146 GB SAS internal disk drive (mirrored)
	2 x QLogic ISP2532-based 8Gb FC HBA
	2 x Broadcom NetXtreme II BCM57711E Flex-10 10Gb Ethernet Controller

Table 4.3.1-1: Server Hardware



4.3.2 Storage

Table 4.3.2-1: Storage Hardware displays the storage hardware used in this reference environment with firmware revision information.

Hardware	Specifications
2 x HP StorageWorks MSA2324fc Fibre Channel Storage Array + HP StorageWorks 70 Modular Smart Array with Dual Domain IO Module [24+25 x 146GB 10K RPM SAS disks]	Storage Controllers: Code Version: M111R06 Loader Code Version: 19.009
	Memory Controller: Code Version: F300R22
	Management Controller Code Version: W441P25 Loader Code Version: 12.015
	Expander Controller: Code Version: 1109
	CPLD Code Version: 8
	Hardware Version: 56
1 x HP StorageWorks 8/24 SAN Switch	Firmware: v1.0.9

Table 4.3.2-1: Storage Hardware

Table 4.3.2-2: Storage LUNs displays the LUN configuration and mappings for each host in the reference environment.

Volume	Size	Host Presentation	Purpose
netbackup	1 TB	bkup	Back up to disk storage unit.
br-rhevm	20 GB	br-rhevm	OS boot from SAN
br-rhev2	45 GB	br-rhevh2, bkup	OS boot from SAN
br-rhev-data	200 GB	br-rhevh, br-rhevh2, bkup	RHEV Data Domain

Table 4.3.2-2: Storage LUNs



Figure 4.3.2-1: Server and Storage Layout provides a logical view into the server and storage configuration used in this reference environment.

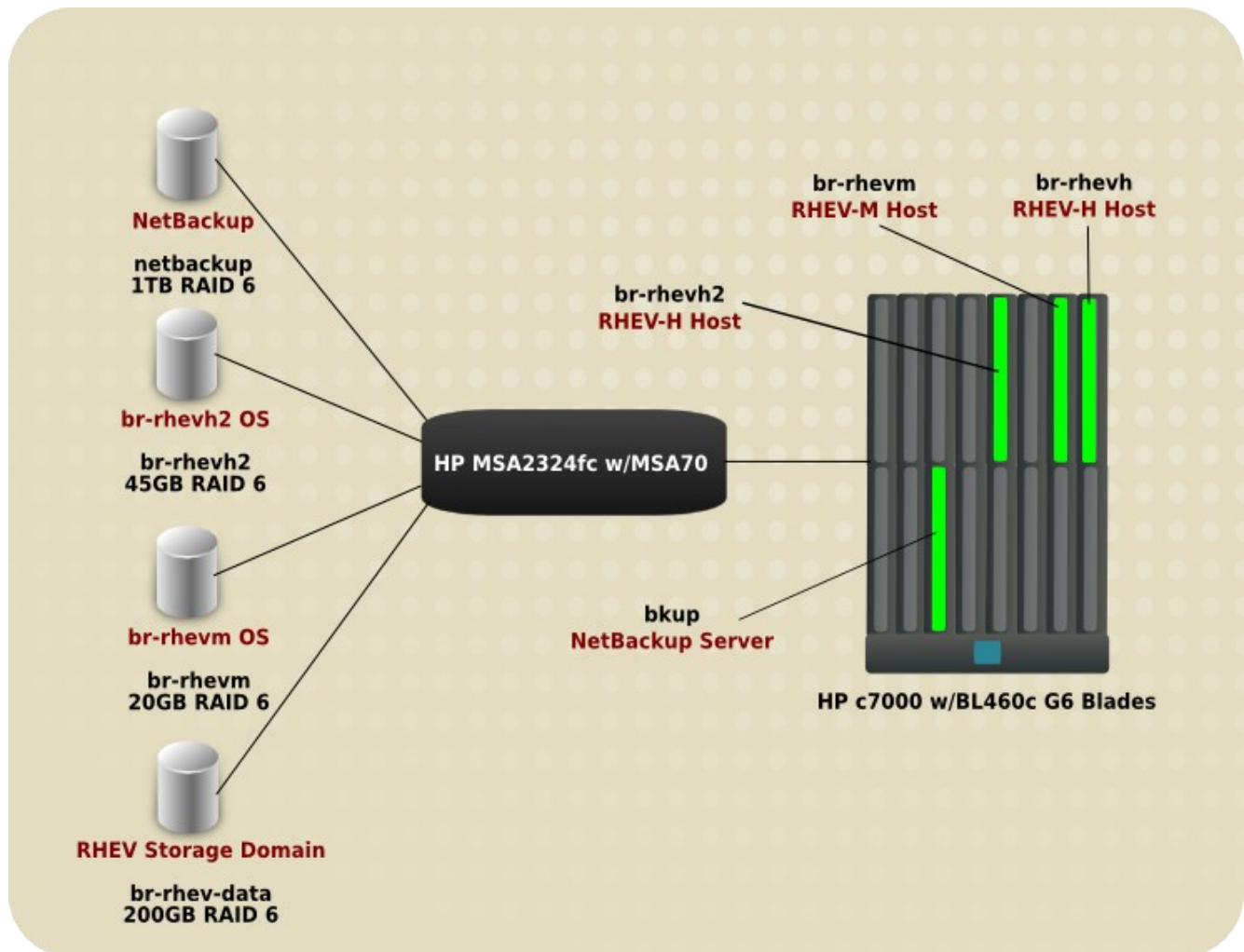


Figure 4.3.2-1: Server and Storage Layout



5 Backup and Restore of Virtual Machines

In the following section, the process of backup and recovery of virtual machines is discussed. The type and focus of backup and recovery discussed in this section are file level, client based. A client machine is defined as a target machine that is to be backed up. Full details regarding the NetBackup Client installation can be found in the following guides:

- *Symantec NetBackup 7.0 Installation Guide for Unix*⁷
- *Symantec NetBackup 7.0 Installation Guide for Windows*⁸

5.1 Red Hat Enterprise Linux Agent Installation

There are several methods to install the NetBackup client onto Red Hat Enterprise Linux machines. It can be pushed from inside the NetBackup Administration Console or individually installed on each machine with the client software or via command line from the master server. For this reference architecture, the Red Hat Enterprise Linux client software was installed remotely via the NetBackup master server from the command line. To install the client software remotely, perform the following steps:

1. Generate a shared SSH key for use between the clients and server
2. From the NetBackup master server, remotely install the client software

Shared SSH Keys

When remotely installing the NetBackup client from the master server, if SSH shared keys are not configured between the master server and client machine, upon execution of the `ssh_to_client` script will result in password prompting three times posing a barrier when automating the installation.

As root from the NetBackup master server, execute the following command:

```
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
4f:b6:1a:d0:19:41:f2:a9:37:9c:ad:39:cf:5c:79:9e root@bkup

[ ... output truncated ... ]
```

This generates a private/public key pair. The private key in this example is called `id_rsa`. The public key is called `id_rsa.pub`.

Note: Always protect the private key, `id_rsa`, and never share it with others. If it becomes compromised, the user account is at risk for malicious activities.



Ensure that the specified user account on each client has a `.ssh` directory located under the user's home directory by performing the following command:

```
# ls -all -l /home/<user>
total 84
dr-xr-x---.  3 root root  4096 Jun 20 03:09 .
dr-xr-xr-x. 23 root root  4096 Jun 20 01:18 ..
-rw-----.  1 root root 14527 Apr 27 13:21 anaconda-ks.cfg
-rw-----.  1 root root  4317 Jun 20 01:59 .bash_history
-rw-r--r--.  1 root root    18 May 20 2009 .bash_logout
-rw-r--r--.  1 root root   176 May 20 2009 .bash_profile
-rw-r--r--.  1 root root   176 Sep 22 2004 .bashrc
-rw-r--r--.  1 root root    0 Apr 27 13:21 cobbler.ks
-rw-r--r--.  1 root root   100 Sep 22 2004 .cshrc
-rw-r--r--.  1 root root 15922 Apr 27 13:21 install.log
-rw-r--r--.  1 root root  5267 Apr 27 13:20 install.log.syslog
-rw-----.  1 root root  1866 Apr 27 13:21 ks-rhn-post.log
-rw-r--r--.  1 root root   129 Dec  3 2004 .tcshrc
```

Command options:

- `-l` – use a long listing format

If the `.ssh` directory does not exist for the specified user on the client machine, simply SSH to another system from the client to automatically generate. Once generated, the `.ssh` directory will be listed.

```
# ls -all -l /home/<user>
total 84
dr-xr-x---.  3 root root  4096 Jun 20 03:09 .
dr-xr-xr-x. 23 root root  4096 Jun 20 01:18 ..
-rw-----.  1 root root 14527 Apr 27 13:21 anaconda-ks.cfg
-rw-----.  1 root root  4317 Jun 20 01:59 .bash_history
-rw-r--r--.  1 root root    18 May 20 2009 .bash_logout
-rw-r--r--.  1 root root   176 May 20 2009 .bash_profile
-rw-r--r--.  1 root root   176 Sep 22 2004 .bashrc
-rw-r--r--.  1 root root    0 Apr 27 13:21 cobbler.ks
-rw-r--r--.  1 root root   100 Sep 22 2004 .cshrc
-rw-r--r--.  1 root root 15922 Apr 27 13:21 install.log
-rw-r--r--.  1 root root  5267 Apr 27 13:20 install.log.syslog
-rw-----.  1 root root  1866 Apr 27 13:21 ks-rhn-post.log
drwx-----.  2 root root  4096 Jun 20 02:29 .ssh
-rw-r--r--.  1 root root   129 Dec  3 2004 .tcshrc
```

Copy the `id_rsa.pub` file to each client machine via the following command:

```
# ssh-copy-id -i /home/<user>/.ssh/id_rsa.pub br-rhel6-bkup
21
root@br-rhel6-bkup's password:
Now try logging into the machine, with "ssh 'br-rhel6-bkup'", and check
in:
```



```
.ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

Command option:

- **-i** – specify an identity file and append to `~/.ssh/authorized_keys`

Finally, test SSH access to the client machine(s) to ensure no prompt for password is required:

```
# ssh br-rhel6-bkup
Last login: Mon Jun 20 02:29:43 2011 from bserve-bkup

RHN Satellite kickstart on 2011-04-27
```

Remote Client Install

From the NetBackup master server, a script was created to automate the installation of the NetBackup client using `ssh_to_client` located at: `/usr/opensv/netbackup/client/Linux/RedHat2.6`
`netbackup_client_install.sh` utilizes a hosts file for targeted machines, initiates the `ssh_to_client` function for client installation and logs results under `/tmp` for the date and time the script was executed.

```
#!/bin/bash

#This script installs the NetBackup client to multiple machines remotely from the master server.

FILE=`cat /root/hosts`

# Set the name of the logfile. Currently set to ThisProgramName.Date.Time.log
LOGFILE=/tmp/$0-$(date +%F_%T).log

# Loop through the hosts list.
for server in $FILE
do
    /usr/opensv/netbackup/client/Linux/RedHat2.6/ssh_to_client -L ${server}
    RC=$?

    # Check the return code to see if it was successful. If it was not,
    # capture the return code since it can indicate the cause for failure.
    if [ ${RC} -eq 0 ]
    then
        echo "${server} completed successfully"
    else
        echo "*** ${server} completed unsuccessfully (Return Code ${RC})"
    fi
done 2>&1 | tee -a ${LOGFILE}
```



Note: The NetBackup client binaries must exist under `/usr/opensv/netbackup/client` for the above procedure to succeed. Refer to the *Symantec NetBackup Installation Guide for UNIX and Linux*⁹ regarding additional information.

5.1.1 Policies

Once the NetBackup client is installed on the target machines, policies can be created on the NetBackup master server via the NetBackup Administration Console. For this reference environment, there was a single backup policy created for Red Hat Enterprise Linux virtual machine backups.

Policy	Clients	Type	Backup Selections
LINUX_VMs	br-rhel56, br-rhel6	Standard	Complete file system

Table 5.1.1-1: Linux Backup Policies

This policy contained a full and differential backup. Section 4.1.1.4 Policies describe the schedule and retention settings for all policies used.

Figure 5.1.1-1: Linux_VMs Policy Attributes displays the properties for policy *Linux_VMs*.

The screenshot displays the 'Attributes' tab for a NetBackup policy. The 'Policy type' is set to 'Standard'. Under 'Destination', 'Data classification' is '<No data classifi...', 'Policy storage' is 'backupArea', and 'Policy volume' is 'NetBackup'. The 'Take checkpoint...' checkbox is unchecked, and 'Limit jobs per policy' is set to 3. 'Job priority' is 2. 'Media Owner' is 'Any'. The 'Snapshot Client' section has 'Perform block level incremental b...' and 'Perform snapshot bac...' checked, with 'Opti...' next to the latter. Other options like 'Retain snapshots for Instant Re...', 'Hyper-V server', and 'Perform off-host b...' are unchecked. The 'Microsoft Exchange Server Attributes' section shows 'Exchange 2010 DAG or Exchange 2007 replication (LCR/CCR)' selected for the 'Database backup source', with 'Preferred serv...' and '(Exchange 2010 DAG only)' below it. The 'Active' checkbox is checked, and the 'Go into effect at' date is '02/03/1991 14:25:54'. Other options like 'Follow NFS', 'Cross mount points', 'Compress', 'Encrypt', 'Intelligent Disaster Recovery', 'Bare Metal Restore', 'Collect true image restore information', 'Allow multiple data streams', 'Disable client-side deduplication', and 'Enable granular recovery' are unchecked. A 'Keyword phrase (optional):' field is also present.

Figure 5.1.1-1: Linux_VMs Policy Attributes



Note: Enable *Cross mount points* to back up all files and directories in the selected path, regardless of the file system. For example, if root (/) is specified as the file path on a UNIX/Linux system, NetBackup backs up root (/) and all files and directories under root in the tree. NetBackup specifically excludes mapped directories even if *Follow NFS* and *Cross mount points* are enabled.

Choose ALL_LOCAL_DRIVES under the *Backup Selections* tab as shown in **Figure 5.1.1-2: Linux_VMs Backup Selections**.

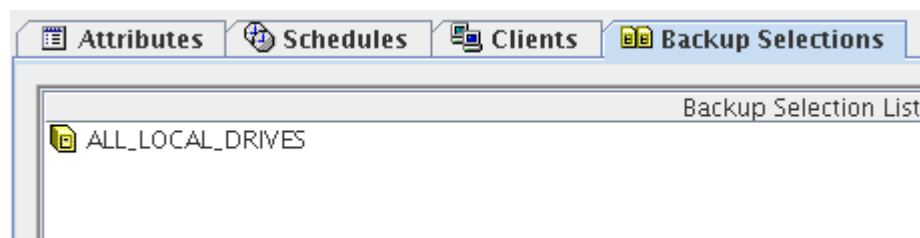


Figure 5.1.1-2: Linux_VMs Backup Selections

Finally, client machines need to be added within the policy. Click on the *Clients* tab, fill in the appropriate information and click *Add* as depicted in **Figure 5.1.1-3: Red Hat Enterprise Linux Client Addition for Policies**.

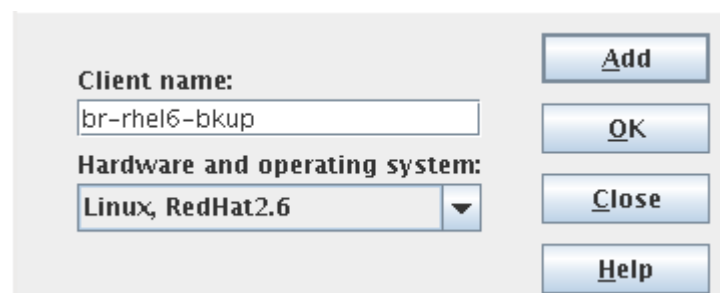


Figure 5.1.1-3: Red Hat Enterprise Linux Client Addition for Policies

For this reference environment, the hostname associated with the client backup network was used as the *Client name* and appropriate kernel level chosen for the *Hardware and operating system* field.

Note: Policy attributes may vary depending on environmental needs. Refer to the *Symantec NetBackup Administrators Guide Volume 1: UNIX and Linux*¹⁰ regarding additional information.



5.2 Microsoft Windows Client Installation

There are several ways to install the NetBackup client onto a machine running a Windows operating system however each requires access to the install executable from a client machine. Upon installation of the NetBackup client, the option to install the client to multiple target machines at the same time is provided, as depicted in **Figure 5.2-1: NetBackup Client Installation**.

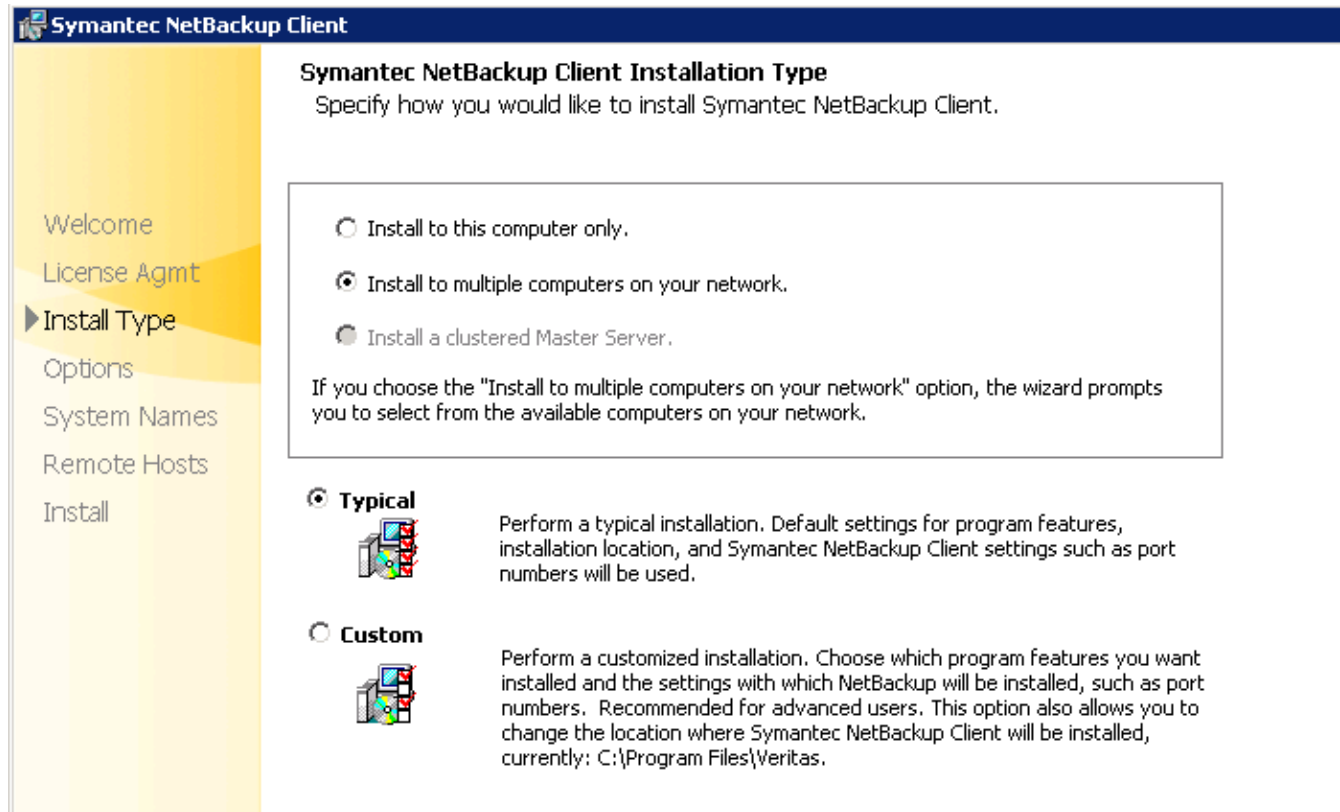


Figure 5.2-1: NetBackup Client Installation



Figure 5.2-2: Adding Remote Hosts references adding additional client destination machines for installation.

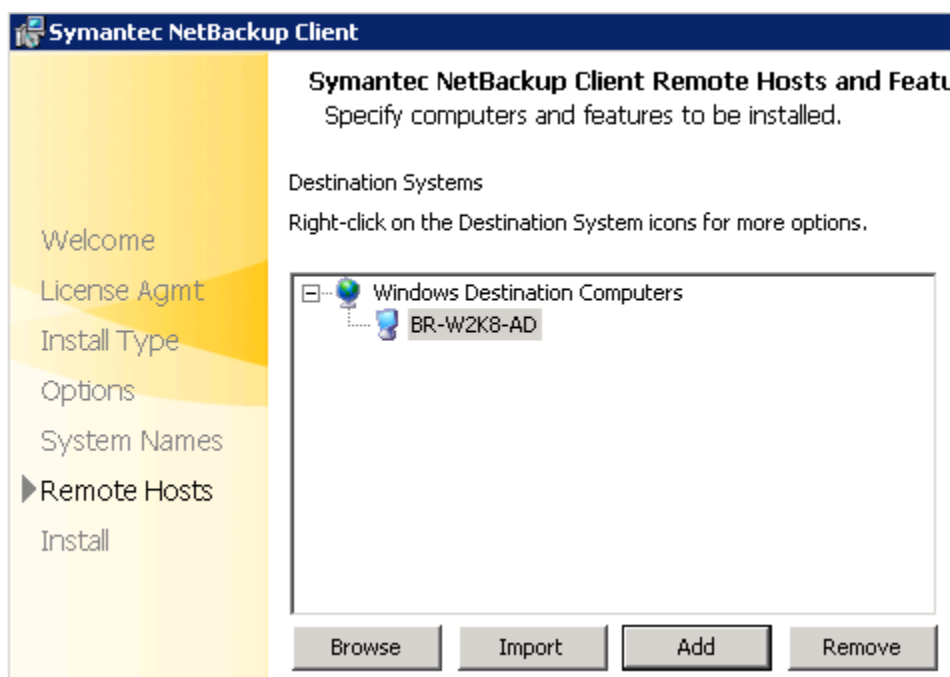


Figure 5.2-2: Adding Remote Hosts

5.2.1 Policies

Once the NetBackup client is installed on the target machines, policies can be created on the NetBackup master server via the NetBackup Administration Console. For this reference environment, there were three backup policies created for Windows backups. One specific for Windows machines running Active Directory, one for non-Active Directory machine, and a policy specific to Microsoft SQL server database backups.

Policy	Clients	Type	Backup Selections
RHEVM_OS	br-rhevm	MS-Windows	System state, operating system and shadow copy components
RHEVM_SQL	br-rhevm	MS-SQL-Server	MSSQL database
Windows_AD_VMs	br-w2k8-ad	MS-Windows	System state, operating system, shadow copy components and Active Directory application mode

Table 5.2.1-1: Windows Backup Policies



The policies listed contain a full and differential backup. Section **4.1.1.4 Policies** describe the schedule and retention settings for all policies used.

Figure 5.2.1-1: RHEVM_OS Policy Attributes display the properties for policy *RHEVM_OS*.

The screenshot shows the 'Attributes' tab of the RHEVM_OS Policy configuration window. The 'Policy type' is set to 'MS-Windows'. Under 'Destination', 'Data classification' is '<No data classifi...', 'Policy storage' is 'backupArea', and 'Policy volume' is 'NetBackup'. The 'Take checkpoint' checkbox is unchecked, and 'Limit jobs per policy' is set to 0. 'Job priority' is 1, with a note that higher numbers indicate greater priority. 'Media Owner' is set to 'Any'. The 'Snapshot Client' section has 'Perform snapshot backup' checked, with options for 'Retain snapshots for Instant Re...', 'Hyper-V server', and 'Perform off-host backup'. The 'Microsoft Exchange Server Attributes' section is also visible, showing 'Exchange 2010 DAG or Exchange 2007 replication (LCR/CCR)' and a 'Database backup source' dropdown.

Figure 5.2.1-1: RHEVM_OS Policy Attributes

Select All_LOCAL_DRIVES, System State and Shadow Copy Components as shown in **Figure 5.2.1-2: RHEVM_OS Backup Selections**.

The screenshot shows the 'Backup Selections' tab of the RHEVM_OS Policy configuration window. It displays a 'Backup Selection List' with three items: 'ALL_LOCAL_DRIVES', 'System State', and 'Shadow Copy Components'. Each item is preceded by a folder icon.

Figure 5.2.1-2: RHEVM_OS Backup Selections



Figure 5.2.1-3: Windows_AD_VMs Policy Attributes and **Figure 5.2.1-4: Windows_AD_VMs Backup Selections** display the properties for policy *Windows_AD_VMs*.

Policy type: MS-Windows

Destination:

- Data classifi...** <No data classifi...
- Policy stora...** backupArea
- Policy volu...** NetBackup

☐ **Take checkpoint...** 0 ...

☐ **Limit jobs per policy:** ...

Job priority: 0 (higher number is greater priority)

Media Own... Any

Snapshot Client

- ☐ Perform block level incremental b...
- ☒ Perform snapshot bac... Opti...
- ☐ Retain snapshots for Instant Re...
- ☐ Hyper-V server: ...
- ☐ Perform off-host b...
- Use:** ...
- Machine:** ...

Microsoft Exchange Server Attributes

Exchange 2010 DAG or Exchange 2007 replication (LCR/CCR)

Database backup source: ...

Preferred serv... (Exchange 2010 DAG only)

Active. Go into effect at: 02/03/1991 14:25:54

- ☐ Backup network drives
- ☐ Cross mount points
- ☐ Compress
- ☐ Encrypt

Collect disaster recovery information for:

- ☐ Intelligent Disaster Recovery
- ☐ Bare Metal Restore
- ☐ Collect true image restore information
- ☐ with move detection

(Required for synthetic backups and Bare Metal Restore)

- ☐ Allow multiple data streams
- ☐ Disable client-side deduplication
- ☐ Enable granular recovery

Keyword phrase (optional): ...

Figure 5.2.1-3: Windows_AD_VMs Policy Attributes

Backup Selection List

- Active Directory Application Mode:\
- ALL_LOCAL_DRIVES
- Shadow Copy Components:\
- System State:\

Figure 5.2.1-4: Windows_AD_VMs Backup Selections

Note: For proper full system recovery, *System State*, *Shadow Copy Components* and *Active Directory Application Mode* (if configured as a Active Directory Domain Controller), along with *ALL_LOCAL_DRIVES*, must be part of the *Backup Selections* for Microsoft Windows machines.



Within each policy, client machines need to be added. Simply click on the *Clients* tab, fill in the appropriate information and click *Add* as depicted in **Figure 5.2.1-5: Windows Client Addition for Policies**.

Figure 5.2.1-5: Windows Client Addition for Policies

For this reference environment, the hostname associated with the client backup network was used as the *Client name* and appropriate operating system chosen, *Windows-x64, Windows 2008*, for the *Hardware and operating system* field.

Note: Policy attributes may vary depending on environmental needs. Refer to the *Symantec NetBackup Administrators Guide Volume 1: UNIX and Linux* regarding additional information.

5.3 Backup

With the NetBackup client installed, policies created/defined, and client machines targeted, the next step is to execute backups. Typically a backup administrator will allow the backups to run on the defined policy schedule. There are occasions when executing a backup manually is preferred such as impromptu system outages, hardware reallocation, or test purposes. Backups, much like restores, are only as-good-as the success of the configured job or policy. It is highly recommended to manually execute a test backup once the policy has been configured. Any issues or errors should be addressed and resolved before determining a configured policy is working properly.



To manually execute a backup within the NetBackup Administration Console, highlight the chosen policy, right-click and select *Manual Backup* as depicted in **Figure 5.3-1: Manual Backup**.

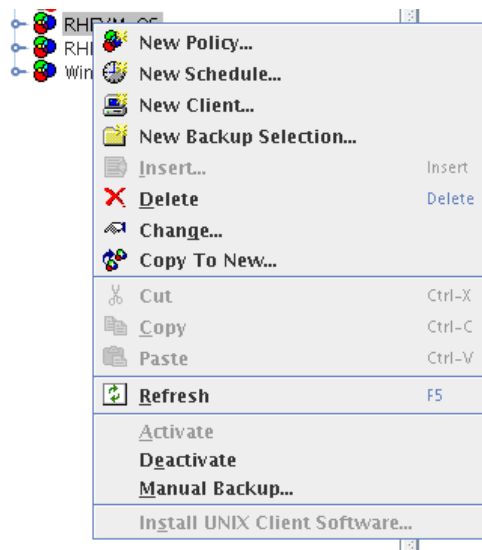


Figure 5.3-1: Manual Backup

Select the type of backup and the client machine to perform the backup against as shown in **Figure 5.3-2: Manual Backup Selection** and click OK.

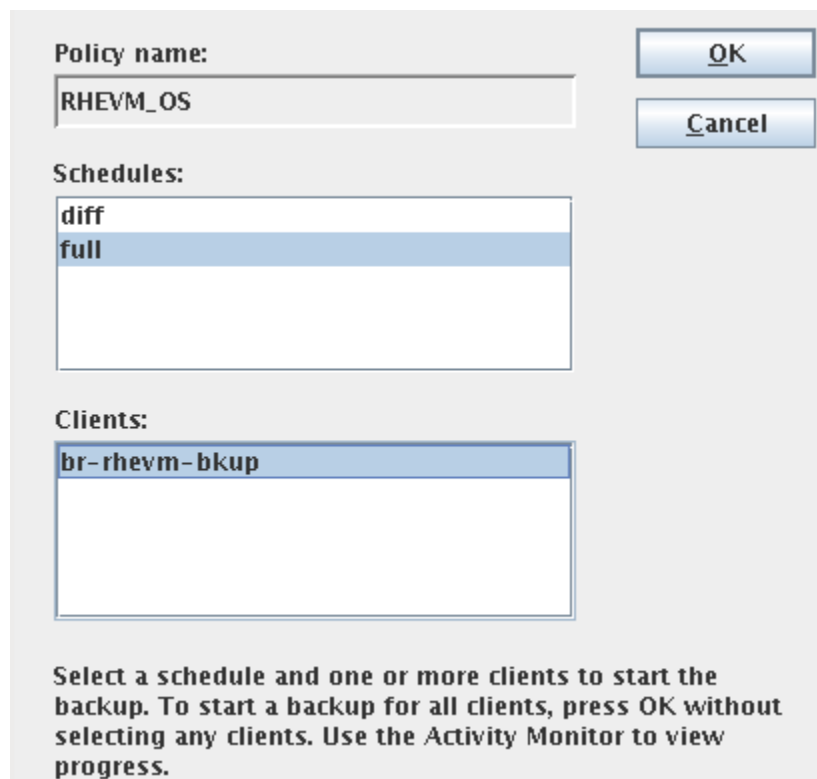


Figure 5.3-2: Manual Backup Selection



Once the backup has been initiated, status of the backup can be checked within Activity Monitor as displayed in **Figure 5.3-3: Manual Backup Status**.

Job Id	Type	State	State Details	Status	Policy	Schedule	Client
12247	Backup	Active			RHEVM_OS	full	br-rhevm-bkup
12246	Image Cleanup	Done		0			
12245	Backup	Done		0	Windows_...	Differentia...	br-w2k8-ad-bkup

Figure 5.3-3: Manual Backup Status

Upon job completion, check the job details to determine the final status. **Figure 5.3-4: Manual Backup Job Details** indicates that the manually executed backup was successful without errors.

Job Details: 12247

Job ID: 12247

Job state: Done

Job Overview

Detailed Status

Attempt: 1

Attempt started: 05/12/2011 17:07:05

Job PID: 21220

Attempt elapsed: 00:17:48

Storage unit: backupArea

Attempt ended: 05/12/2011 17:24:53

Media server: bkup

KB per second: 9675

Transport type: LAN

Status:

05/12/2011 17:07:05 - granted resource bkup.NBU_POLICY.MAXJOBS.RHEVM_OS
05/12/2011 17:07:05 - granted resource MediaID=@aaaac;Path=/bckupArea;MediaServer=bkup
05/12/2011 17:07:05 - granted resource backupArea
05/12/2011 17:07:05 - estimated 12152211 kbytes needed
05/12/2011 17:07:06 - started process bpbm (pid=21220)
05/12/2011 17:07:09 - connecting
05/12/2011 17:07:13 - connected; connect time: 0:00:00
05/12/2011 17:07:17 - begin writing
05/12/2011 17:24:44 - end writing; write time: 0:17:27
the requested operation was successfully completed (0)

Current Kilobytes written: 10127088

Estimated Kilobytes: 12152211

Current Files written: 27079

Estimated Files: 27097

Current File:

Troubleshooter...

Percent complete: 100%

Refresh

Close

Help

Figure 5.3-4: Manual Backup Job Details

With backup validation complete for the policies, monitoring scheduled jobs for errors through e-mail notification, activity monitor or through the use of reports is recommended to ensure backups are executing without error. Additional information for reporting and job monitoring can be found in: *Symantec NetBackup Administrators Guide Volume 1: UNIX and Linux*.



5.4 Restore

Data recovery is critical to business continuity. It becomes imperative to perform test recovery of data to validate backup procedures. Within some business environments, data backup and recovery policies are mandated by law. The following use cases detail file level and full virtual machine recovery.

5.4.1 Red Hat Enterprise Linux File Level Recovery

For this scenario, a Linux system administrator has modified the following file, `/etc/sysconfig/network-scripts/ifcfg-eth0`, restarted the network services and now `eth0` will not come on-line. They are unable to recall the changes made and need to restore functionality to the server. Production has become affected by this unforeseen outage. The backup administrator begins the process to quickly restore a previous configuration file to the affected machine via the dedicated backup network. The following actions are performed:

1. Select a recovery point for the affected machine
2. Choose the file to restore
3. Initiate file recovery
4. Verify completion
5. Bring `eth0` back on-line

Recovery Point

Figure 5.4.1-1: br-rhel6 Restore from Date depicts choosing a recovery point-in-time for the selected machine from the NetBackup Administrator Console.

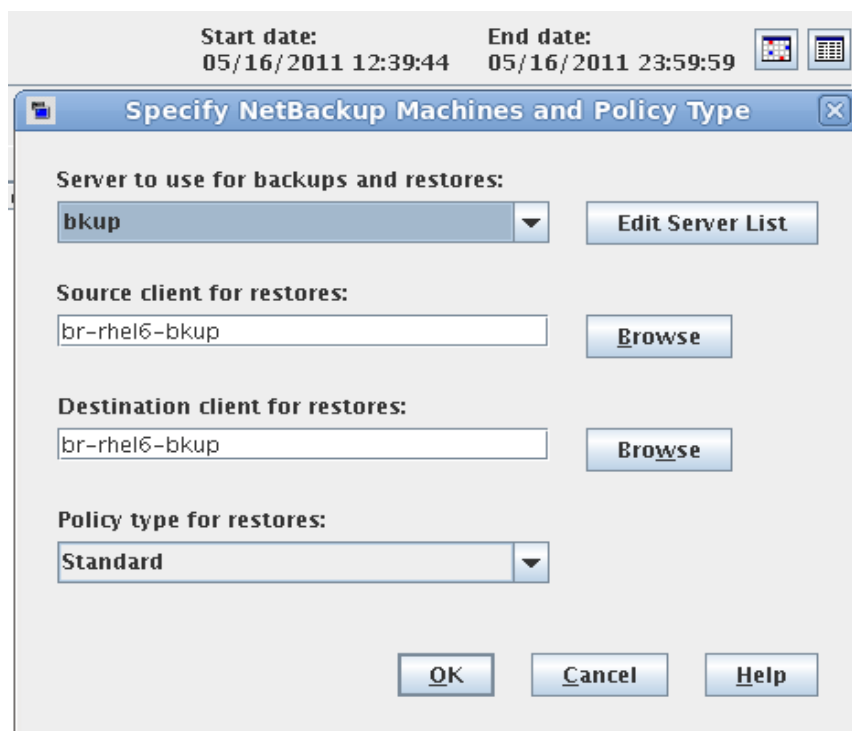


Figure 5.4.1-1: br-rhel6 Restore from Date



File Selection

Figure 5.4.1-2: br-rhel6 Target File Selection displays files selected to be restored.

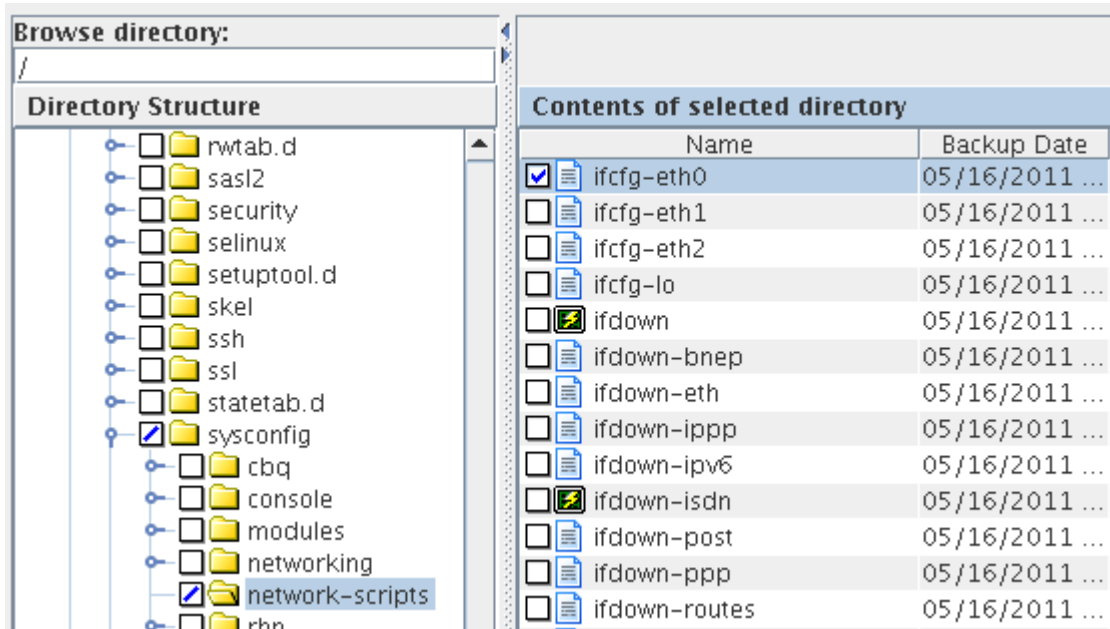


Figure 5.4.1-2: br-rhel6 Target File Selection



File Recovery

Choose the location and options for the file recovery as shown in **Figure 5.4.1-3: br-rhel6 Recovery Options**. Ensure *Overwrite existing files* is checked under *Options*. Once complete, click *Start Restore*.

General

Destination

☒ Restore everything to its original location.

☐ Restore everything to a different location (maintaining existing structure).

Destination:
/etc/sysconfig/network-scripts/

☐ Restore individual directories and files to different locations.

Source	Destination	Backup Date	Modified
/etc/sysconfig/network-s...		05/16/2011 12:39:44	04/27/2011 13:21:40

Change Selected Destination(s)... Change All Destinations...

Add Destination... Remove Selected Destination(s)

☐ Create virtual disks and redirect to them (Make sure if your operating system supports this feature)

Setting

Options

☒ Overwrite existing files ☐ Rename hard links

☐ Restore directories without crossing mount points ☐ Rename soft links

☐ Restore without access-control attributes (Windows clients only)

☐ Override default priority

Job Priority: 0 (higher number is greater priority)

☒ Use default progress log filename

Progress log filename

Start Restore Cancel

Figure 5.4.1-3: br-rhel6 Recovery Options

Note: Overwriting may not be the desired option. In the event the data to be restored is not validated or the destination machine is unavailable, choose an alternate restore location. This can be the same machine, if accessible, or an alternate machine.



Recovery Completion

With the recovery job initiated, status can be check via the *Task Progress* tab as noted in **Figure 5.4.1-4: br-rhel6 Recovery Status**.

Task	Date	Status
Restore	05/16/2011 12:23:54	Incomplete
Restore	05/16/2011 12:25:18	Incomplete
Restore	05/16/2011 12:27:13	Incomplete
Restore	05/16/2011 12:31:15	Successful
Restore	05/16/2011 12:52:04	Successful
Restore	05/16/2011 13:25:16	Successful
Restore	05/16/2011 17:15:57	Successful

Results of the Task Selected Above

☐ Auto Refresh Rate (seconds): 10

Restore started 05/16/2011 17:15:56

```
17:15:59 (12553.001) INF - Beginning restore from server bkup to client br-rhel6-bkup.  
17:15:59 (12553.001) /etc/sysconfig/network-scripts/ifcfg-eth0  
17:15:59 (12553.001) (12553.001) INF - TAR EXITING WITH STATUS = 0  
17:15:59 (12553.001) (12553.001) INF - TAR RESTORED 1 OF 1 FILES SUCCESSFULLY  
17:15:59 (12553.001) (12553.001) INF - TAR KEPT 0 EXISTING FILES  
17:15:59 (12553.001) (12553.001) INF - TAR PARTIALLY RESTORED 0 FILES
```

Figure 5.4.1-4: br-rhel6 Recovery Status



Verify Functionality

With `ifcfg-eth0` restored, the system administrator attempts to bring the interface on-line using `ifup`.

```
# ifup eth0

Determining IP address information for eth0... done.
```

Interface statistics can be checked to verify traffic is passing through `eth0` using the `ip` command.

```
# ip -statistics link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX: bytes    packets  errors  dropped overrun mcast
      2836         44        0        0        0        0
    TX: bytes    packets  errors  dropped carrier collsns
      2836         44        0        0        0        0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UNKNOWN qlen 1000
    link/ether 00:1a:4a:a8:4c:06 brd ff:ff:ff:ff:ff:ff
    RX: bytes    packets  errors  dropped overrun mcast
  2037282491  5933742    0        0        0        0
    TX: bytes    packets  errors  dropped carrier collsns
   9313337    125543    0        0        0        0
```

Note: If a dedicated backup network does not exist or the machine only has a single network connection, an restore operation to an alternate machine and location may be used to recover the configuration file.

5.4.2 Microsoft Windows File Level Recovery

In the following scenario, a end user has accidentally deleted the project files for *Project RH* within their mapped home directory. They have contacted the backup administrator for help in restoring the most recent version of the files. The backup administrator begins the process of restoring the deleted files to the server hosting the user's home directory by performing the following actions:

1. Select a recovery point from the affected machine
2. Choose the files to restore
3. Initiate file recovery
4. Verify completion
5. Ensure the end user is able to access the restored files



Recovery Point

Figure 5.4.2-1: br-w2k8-ad Restore from Date depicts choosing a recovery point-in-time for the selected machine.

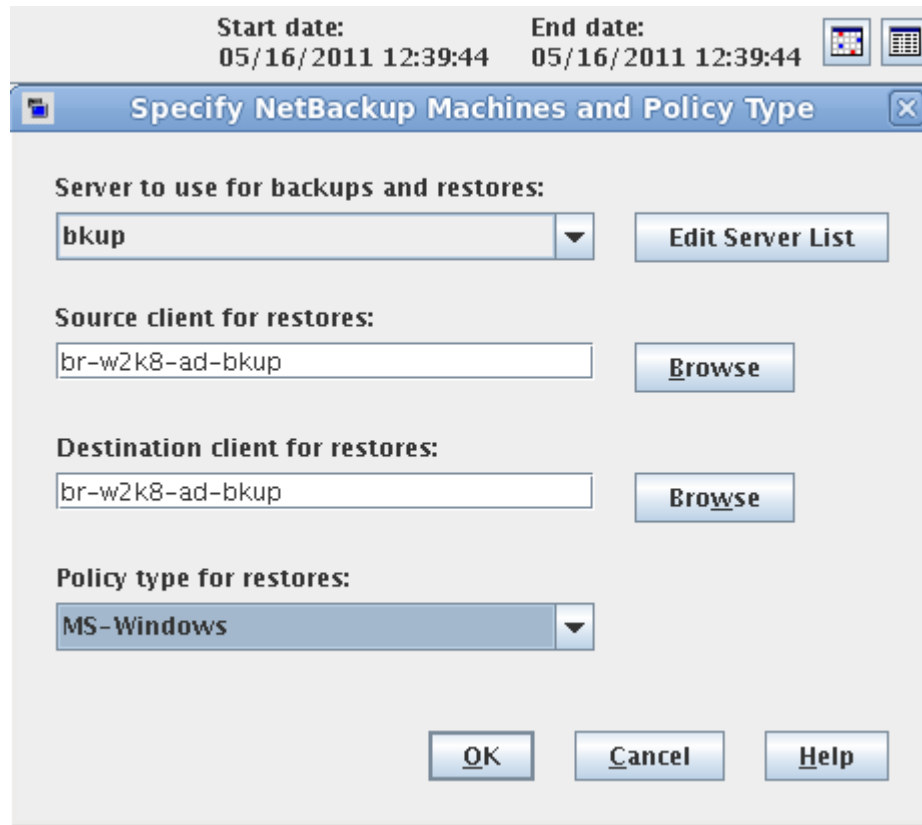


Figure 5.4.2-1: br-w2k8-ad Restore from Date

File Selection

Figure 5.4.2-2: br-w2k8-ad Target File Selection displays the selected files to be restored.

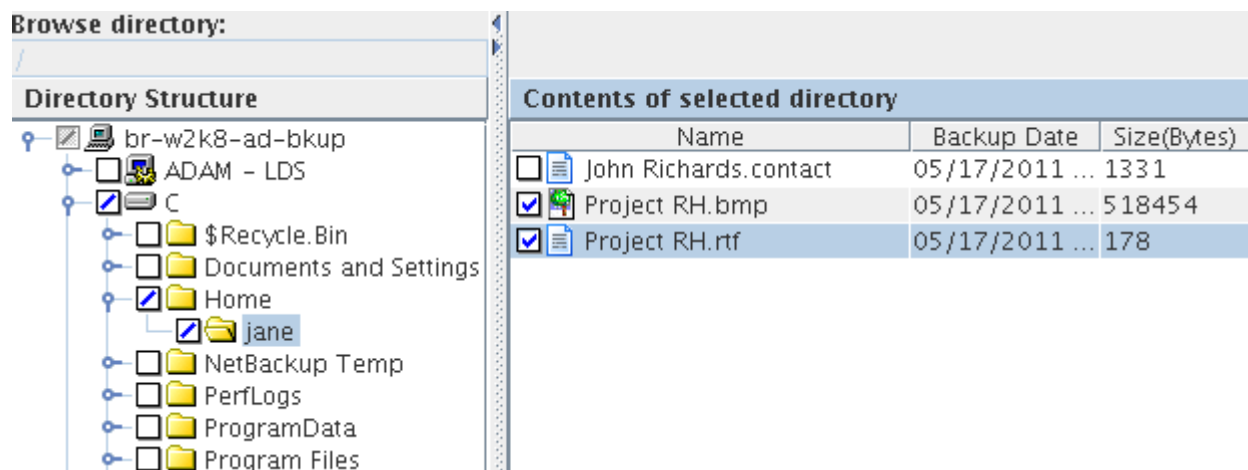
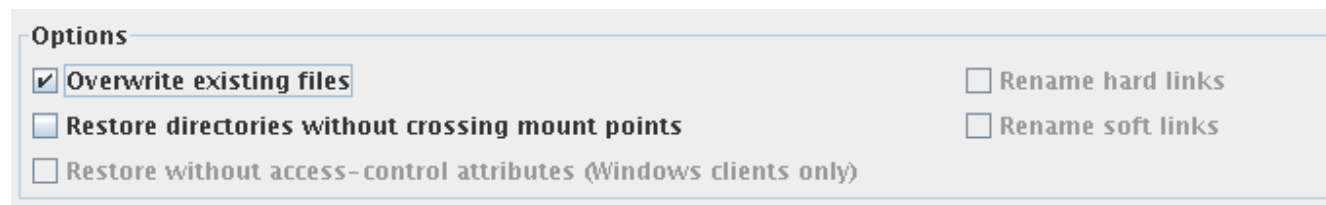


Figure 5.4.2-2: br-w2k8-ad Target File Selection



File Recovery

Choose the location and options for the file recovery as shown in **Figure 5.4.2-3: br-w2k8-ad Recovery Options**. Ensure *Overwrite existing files* is checked under *Options*. Once complete, click *Start Restore*.



Options

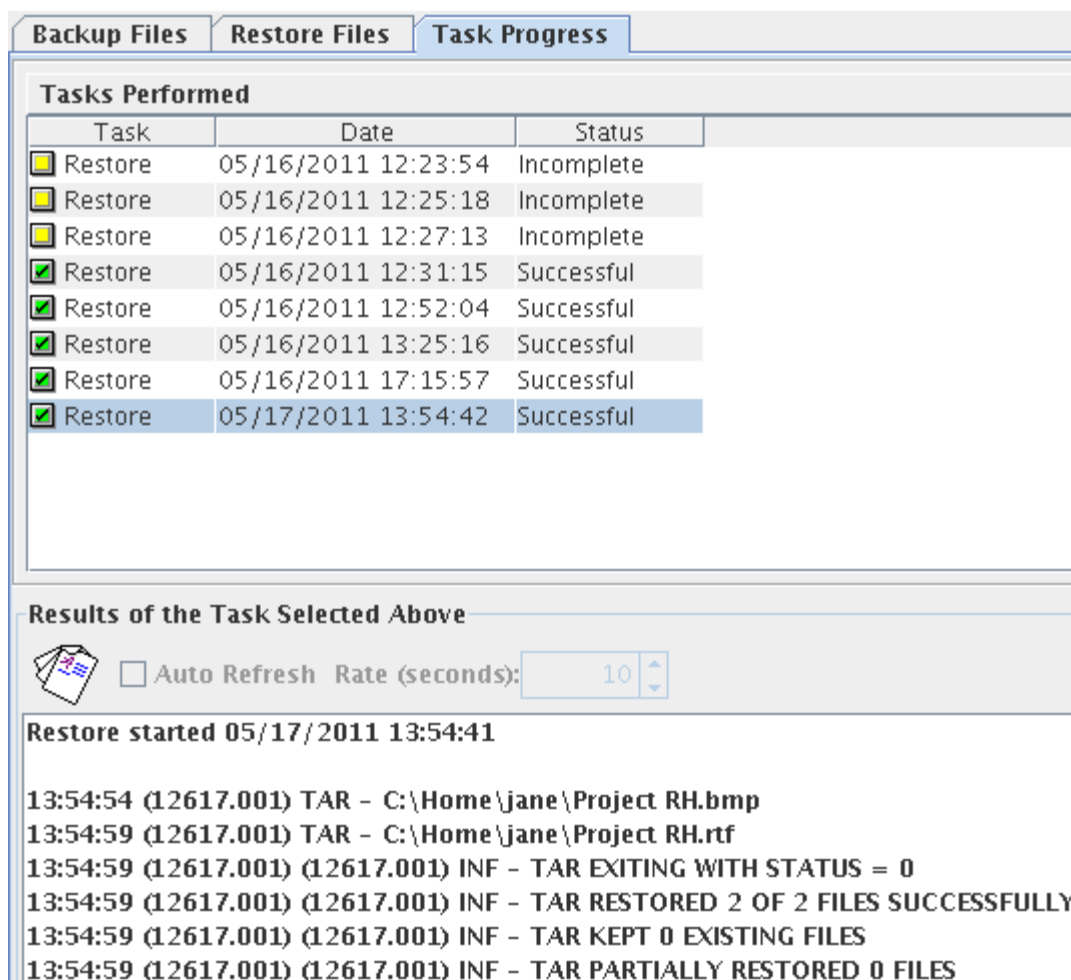
- ☒ Overwrite existing files
- ☐ Restore directories without crossing mount points
- ☐ Restore without access-control attributes (Windows clients only)
- ☐ Rename hard links
- ☐ Rename soft links

Figure 5.4.2-3: br-w2k8-ad Recovery Options

Note: Overwriting may not be the desired option. In the event the data to be restored is not validated, choose an alternate restore location to verify data.

Recovery Completion

With the recovery job initiated, status can be check via the *Task Progress* tab as noted in **Figure 5.4.2-4: br-w2k8-ad Recovery Status**.



Backup Files Restore Files Task Progress

Tasks Performed

Task	Date	Status
Restore	05/16/2011 12:23:54	Incomplete
Restore	05/16/2011 12:25:18	Incomplete
Restore	05/16/2011 12:27:13	Incomplete
Restore	05/16/2011 12:31:15	Successful
Restore	05/16/2011 12:52:04	Successful
Restore	05/16/2011 13:25:16	Successful
Restore	05/16/2011 17:15:57	Successful
Restore	05/17/2011 13:54:42	Successful

Results of the Task Selected Above

☐ Auto Refresh Rate (seconds): 10

Restore started 05/17/2011 13:54:41

13:54:54 (12617.001) TAR - C:\Home\jane\Project RH.bmp
13:54:59 (12617.001) TAR - C:\Home\jane\Project RH.rtf
13:54:59 (12617.001) (12617.001) INF - TAR EXITING WITH STATUS = 0
13:54:59 (12617.001) (12617.001) INF - TAR RESTORED 2 OF 2 FILES SUCCESSFULLY
13:54:59 (12617.001) (12617.001) INF - TAR KEPT 0 EXISTING FILES
13:54:59 (12617.001) (12617.001) INF - TAR PARTIALLY RESTORED 0 FILES

Figure 5.4.2-4: br-w2k8-ad Recovery Status



Verify Functionality

With the files restored, the backup administrator contacts Jane to verify accessibility. Jane accesses the files in her home directory and provides confirmation to the backup administrator the *Project RH* files were successfully restored as depicted in **Figure 5.4.2-5: br-w2k8-ad File Recovery Validation**.

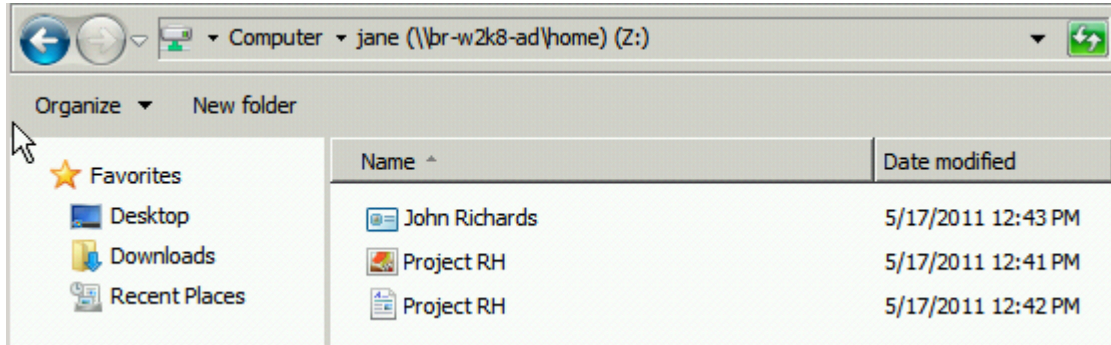


Figure 5.4.2-5: br-w2k8-ad File Recovery Validation

5.4.3 Full Virtual Machine Restore

On occasion there may be instances where a business critical server has had an unexpected outage due to a critical failure. This could be caused by a catastrophic failure. In these situations, it becomes necessary to restore the virtual machine back to an operational state. There are several methods to perform this action, through the use of a backup client or a bare metal restore.

5.4.3.1 Red Hat Enterprise Linux

In the following scenario, a systems administrator has been notified by an application developer that they can no longer access their development server. Upon further investigation, the system administrator discovers that the machine rebooted and does no longer boots to the operating system. The root cause appears to be Logical Volume Management related. The application developer has a deadline to meet for production and desperately needs the server back up and operational. The backup administrator determines that deploying a new virtual machine from a template within RHEV and restoring from backup is the most efficient method to restore operation of the server. The following steps are taken to recover functionality and service:

1. Provision a new virtual machine
2. Configure network settings
3. Install the NetBackup client
4. Select files to restore
5. Verify functionality



Provision Virtual Machine

The first step in recovery is to provision a new virtual machine running the same operating system as the failed machine. This can be accomplished by deploying from a template within RHEV where the NetBackup client, virtio drivers and RHEV Guest Tools are installed resulting in saved configuration time or by creating a new virtual machine from scratch and installing the operating system through automated deployment methods. For this reference environment, a template was used to deploy a base operating system. When using this method, ensure the number and size of virtual disks used, along with the network configuration, match the failed VM configuration. Refer to section **4 Reference Architecture Configuration** regarding specific network setup for this reference environment.

Figure 5.4.3.1-1: Deploy Red Hat Enterprise Linux VM from Template depicts deploying a new virtual machine from a template from within the Red Hat Enterprise Virtualization Management Console.

The screenshot shows the 'New Server Virtual Machine' dialog box. On the left is a sidebar with tabs: 'General' (selected), 'Console', 'High Availability', 'Allocation', and 'Boot Sequence'. The main area contains the following fields:

- Data Center: RHEV-Backup (dropdown)
- Host Cluster: RHEV-Backup (dropdown)
- Default Host: Auto Assign (dropdown)
- Name: br-rhel6-rcvr (text input)
- Description: (empty text input)
- Based on Template: RHEL6 (dropdown)
- Memory Size: 2 GB (text input)
- Total Cores: 2 (spin box) with a slider from 2 to 16
- CPU Sockets: 2 (spin box) with a slider from 1 to 16
- Operating System: Red Hat Enterprise Linux 6.x x64 (dropdown)

At the bottom right are 'OK' and 'Cancel' buttons.

Figure 5.4.3.1-1: Deploy Red Hat Enterprise Linux VM from Template



Figure 5.4.3.1-2: Recovery Red Hat Enterprise Linux VM Network Configuration displays the recovery virtual machine network configuration.

Data Centers		Clusters		Hosts		Storage		Virtual Machines		Pools		Templates		Users					
New Server		New Desktop		Edit		Remove				Migrate		Make Template		Export		Move		Guide Me	
Name				Cluster		Host		IP Address		Memory		CPU		Network					
br-rhel56				RHEV-Backup		br-rhevhost.cloud.l				<div><div></div></div> 0%		<div><div></div></div> 0%		<div><div></div></div> 0%					
br-rhel6				RHEV-Backup						<div><div></div></div> 0%		<div><div></div></div> 0%		<div><div></div></div> 0%					
br-w2k8-ad				RHEV-Backup						<div><div></div></div> 0%		<div><div></div></div> 0%		<div><div></div></div> 0%					
br-w2k8-ad-rcvr				RHEV-Backup						<div><div></div></div> 0%		<div><div></div></div> 0%		<div><div></div></div> 0%					
br-rhel6-rcvr				RHEV-Backup						<div><div></div></div> 0%		<div><div></div></div> 0%		<div><div></div></div> 0%					

General

Users

Network Interfaces

Virtual Disks

Snapshots

Applications

New

Edit

Remove

Name	Network Name	Type	MAC
nic3	backup	Red Hat VirtIO	00:1a:4a:a8:4d:06
nic2	mgmt	Red Hat VirtIO	00:1a:4a:a8:4d:09
nic1	rhev	Red Hat VirtIO	00:1a:4a:a8:4d:0a

Figure 5.4.3.1-2: Recovery Red Hat Enterprise Linux VM Network Configuration

Note: The MAC addresses assigned to each NIC within RHEV-M can be modified to reflect the assigned MAC address for each NIC configuration file inside the virtual machine operating system. The important part is that the MAC address assigned within RHEV-M and the operating system for each NIC match.

Install NetBackup Client

Once the virtual machine is provisioned and the necessary network information configured, install the NetBackup client. For detailed specifics on installation, refer to section **5.1 Red Hat Enterprise Linux Agent Installation**. Alternatively, the NetBackup client could be installed within the template to reduce configuration and recovery time.



File Recovery

With the NetBackup client installed and configured, file recovery can commence. Symantec NetBackup allows both server directed restores and client redirected restores. There are certain circumstances to consider when choosing one over the other. An explanation of each type of restore can be found in: *Symantec NetBackup Administrators Guide Volume 1: UNIX and Linux*. For this scenario, a server directed restore was selected.

Figure 5.4.3.1-3: Red Hat Enterprise Linux File Restore Selection displays the file selection.

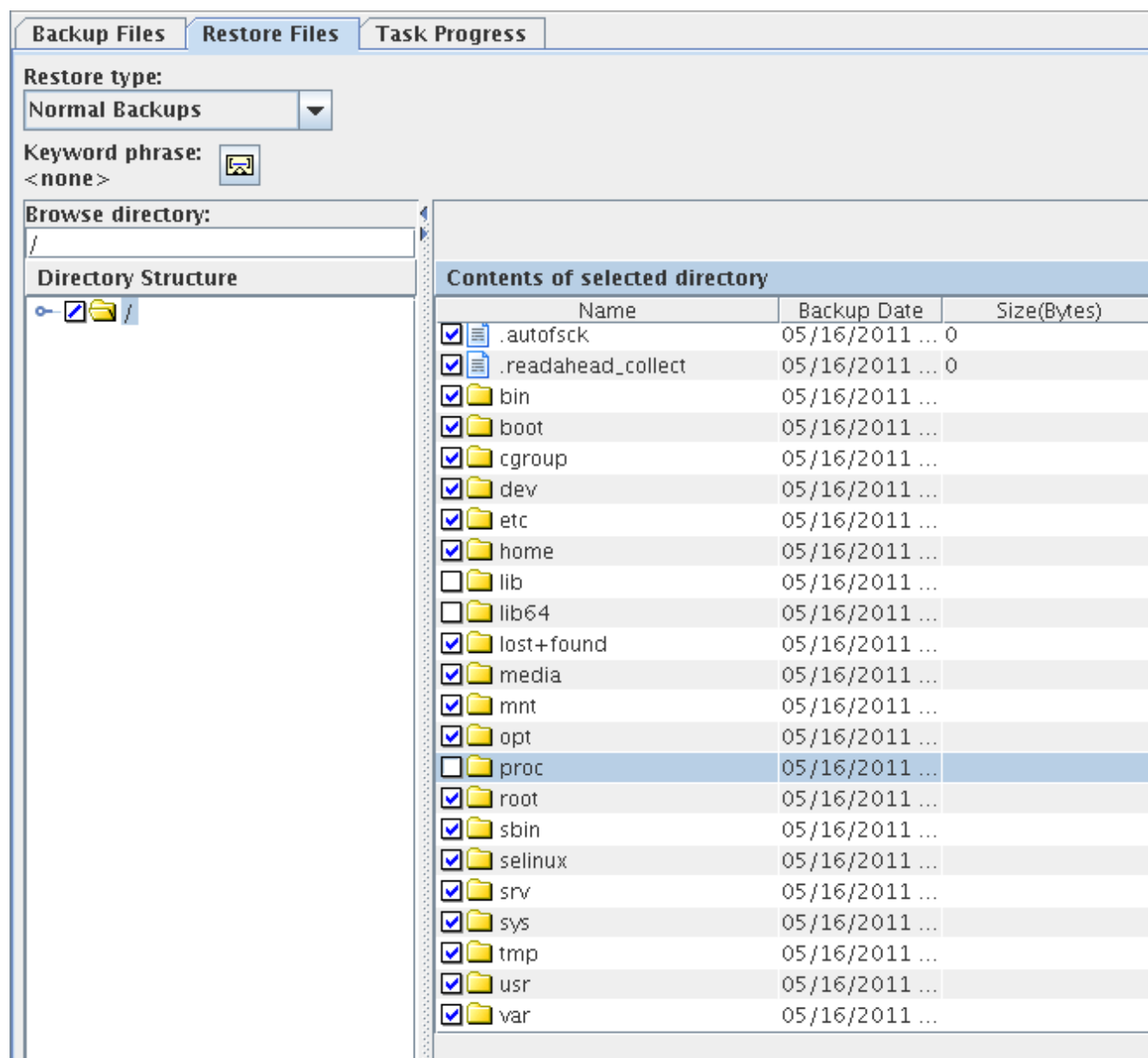


Figure 5.4.3.1-3: Red Hat Enterprise Linux File Restore Selection



Note: As observed in the reference environment, do not select to restore `/proc`, `/lib`, or `/lib64`. Doing so will result in a kernel panic of the machine during the restore process.

It may be desired to perform an operating system install, application(s) install, and perform operating system updates prior to restoring application data and necessary configuration files.

With the file selection complete, click the *Restore* button and select the restore job options. Ensure that *Overwrite existing files* is checked as depicted in **Figure 5.4.3.1-4: Red Hat Enterprise Linux VM Restore**. Click *Start Restore* and monitor the job for completion.

Destination

☒ Restore everything to its original location.

☐ Restore everything to a different location (maintaining existing structure).

Destination:

☐ Restore individual directories and files to different locations.

Source	Destination	Backup Date	Modified
/boot/		05/16/2011 12:39:44	04/27/2011 13:21:23
/.readahead_collect		05/16/2011 12:39:44	04/27/2011 15:07:01
/.autofsck		05/16/2011 12:39:44	04/27/2011 13:22:23
/opt/		05/16/2011 12:39:44	04/27/2011 14:15:55
/srv/		05/16/2011 12:39:44	12/04/2009 08:33:25
/usr/group/		05/16/2011 12:39:44	07/14/2010 07:45:33

☐ Create virtual disks and redirect to them (Make sure if your operating system supports this feature)

Options

☒ Overwrite existing files ☐ Rename hard links

☐ Restore directories without crossing mount points ☐ Rename soft links

☐ Restore without access-control attributes (Windows clients only)

☐ Override default priority

Job Priority

(higher number is greater priority)

☒ Use default progress log filename

Progress log filename

Figure 5.4.3.1-4: Red Hat Enterprise Linux VM Restore



Verify Functionality

With the newly provisioned virtual machine restored, the backup administrator contacts the application developer to verify accessibility and functionality. The application developer reports they are able to access the machine and can proceed with their activities.

5.4.3.2 Microsoft Windows¹¹

In the following scenario, a systems administrator notices that their virtual machine running Windows 2008 R2 with Active Directory has become unresponsive and several users have complained about not being able to login. Upon further investigation, it is determined that the virtual machine has become corrupted and no longer boots. Several recovery methods were attempted without resolution. The backup administrator determines the quickest path to resolution is a full system restore of the failed machine. The following steps were taken to restore functionality and service:

1. Provision a new virtual machine
2. Configure network settings
3. Install the NetBackup client
4. Restoring selected files
5. Verify functionality

Provision Virtual Machine

The first step in recovery is to provision a new virtual machine running the same operating system as the failed machine. This can be accomplished by deploying from a template within RHEV where the NetBackup client, virtio drivers and RHEV Guest Tools are installed resulting in saved configuration time or by creating a new virtual machine from scratch and installing the operating system through automated deployment methods. For this reference environment, a template was used to deploy a base operating system. When using this method, ensure the number and size of virtual disks used, along with the network configuration, match the failed VM configuration. Refer to **Figure 4.1-1: Logical Network Diagram** to review this reference environment configuration.



Figure 5.4.3.2-1: Deploy Windows VM from RHEV Template depicts deploying a new virtual machine from a template from within the Red Hat Enterprise Virtualization Management Console.

New Server Virtual Machine

General

Windows Sys. Prep.

Console

High Availability

Allocation

Boot Sequence

Data Center: RHEV-Backup

Host Cluster: RHEV-Backup

Default Host: Auto Assign

Name: br-w2k8-ad-rcvr

Description:

Based on Template: WINNOAD

Memory Size: 4 GB

Total Cores: 2

CPU Sockets: 2

Operating System: Windows 2008 R2

OK Cancel

Figure 5.4.3.2-1: Deploy Windows VM from RHEV Template



Figure 5.4.3.2-2: Recovery Windows VM Network Configuration displays the recovery virtual machine network configuration.

Data Centers	Clusters	Hosts	Storage	Virtual Machines	Pools	Templates	Users
New Server	New Desktop	Edit	Remove	▶ ▼ □ ☰ ▼ Migrate	Make Template	Export	Move Guide Me
Name	Cluster	Host	IP Address	Memory	CPU	Network	
▶ br-rhel56	RHEV-Backup	br-rhevh.cloud.l		0%	0%	0%	
■ br-rhel6	RHEV-Backup			0%	0%	0%	
■ br-rhel6-recover	RHEV-Backup			0%	0%	0%	
■ br-w2k8-ad	RHEV-Backup			0%	0%	0%	
■ br-w2k8-ad-rcvr	RHEV-Backup			0%	0%	0%	

General	Users	Network Interfaces	Virtual Disks	Snapshots	Applications
New	Edit	Remove			
Name	Network Name	Type	MAC		
nic1	backup	Red Hat VirtIO	00:1a:4a:a8:4d:1e		
nic2	mgmt	Red Hat VirtIO	00:1a:4a:a8:4d:1f		
nic3	rhevm	Red Hat VirtIO	00:1a:4a:a8:4d:20		

Figure 5.4.3.2-2: Recovery Windows VM Network Configuration

Configure Network and NetBackup Client

Once the virtual machine has been provisioned and the necessary network information configured (refer to section **4 Reference Architecture Configuration** regarding specific network setup), the NetBackup client needs to be installed. For detailed specifics on installing the client, refer to section **5.2 Microsoft Windows Client Installation**.

File Recovery

With the NetBackup client installed and configured, file recovery can commence. When performing a system restore using the NetBackup client running on a Windows operating system, the following is a defined process¹² recommended to be followed:

1. Launch the NetBackup BAR (Backup, Archive & Restore) GUI application from the client.
2. Select the images that contain the Full and Incremental (if applicable) backups of the system drive first. Enable the overwrite option. **Do not elect to restore the System State/Shadow Copy Components at the same time.**

Note: DO NOT REBOOT after the system drive(s) restore is completed.



System drive selection as shown in **Figure 5.4.3.2-3: System Drive Restore Selection.**

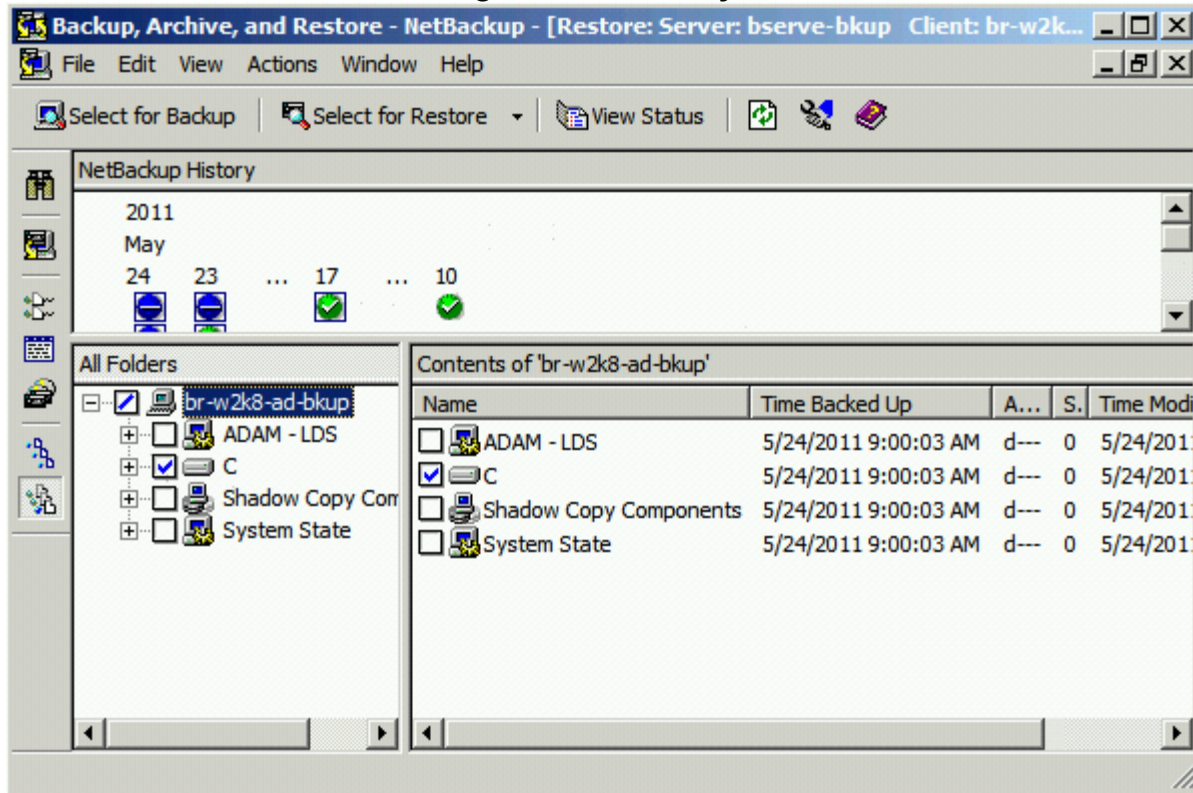


Figure 5.4.3.2-3: System Drive Restore Selection

3. When the restore is complete, check the client's tar log (found in `C:\Program Files\Veritas\NetBackup\logs\tar`) for confirmation of a successful restore. If the restore had errors, this log will provide more detail and any issues found should be resolved before continuing.
4. System State and Shadow Copy Components

CAUTION: This is the most critical part of the restore that could result in a non-bootable system.

Select the images that contain the Full and Incrementals (if applicable) backups and start a restore of the System State and Shadow Copy Components with the overwrite option enabled.



System State and Shadow Copy selection as displayed in **Figure 5.4.3.2-4: System State and Shadow Copy Selection**.

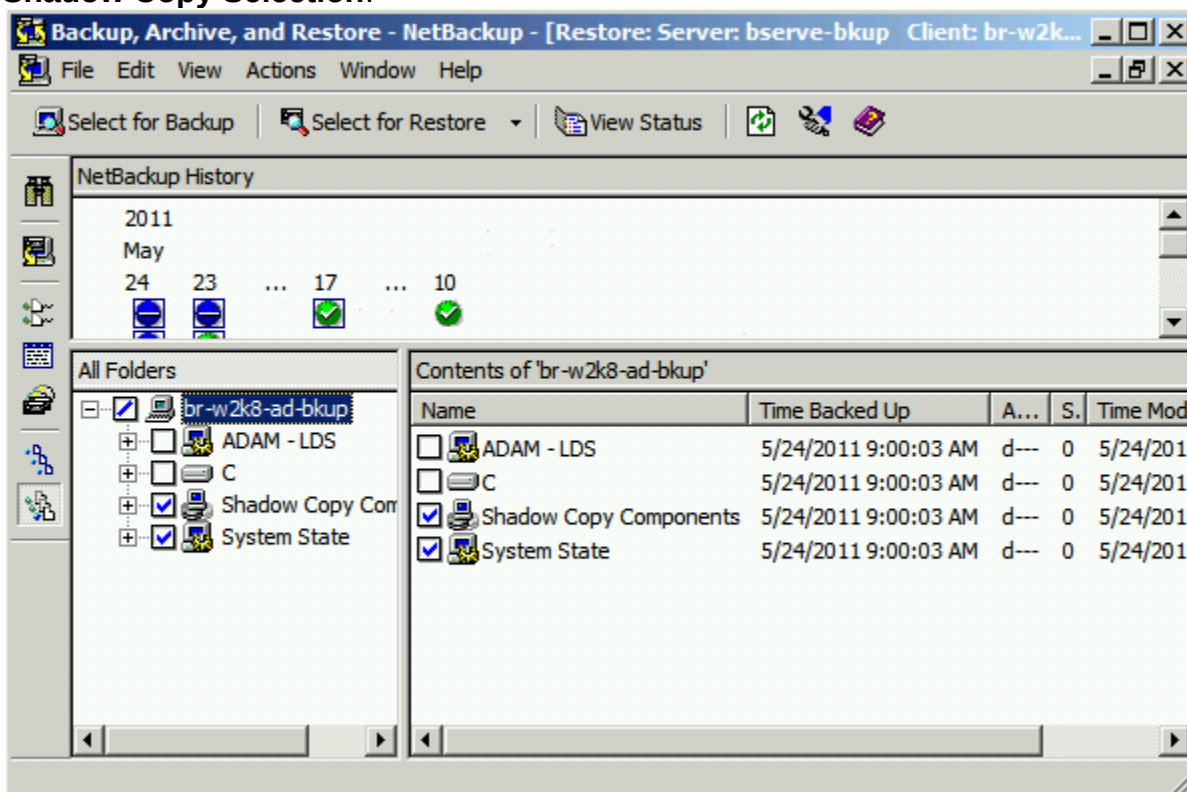


Figure 5.4.3.2-4: System State and Shadow Copy Selection

If the restore being attempted is to the ORIGINAL virtual machine, use the `W2koption.exe`¹³ utility supplied with the NetBackup Windows Client. **THIS SHOULD NOT BE USED IF THE RESTORE IS NOT TO THE ORIGINAL MACHINE.** Running `W2koption.exe`:

- A. If this is not the original machine, skip this step, otherwise, before the restore of System State or Shadow Copy Components starts, run `w2koption.exe` with the following command syntax:

```
C:\Program_Files\VERITAS\NetBackup\bin\w2koption -restore -same_hardware 1
```

- B. Restore the System State or Shadow Copy Components. **DO NOT REBOOT.**

- C. Repeat the `w2koption` command as performed earlier:

```
C:\Program_Files\VERITAS\NetBackup\bin\w2koption -restore -same_hardware 1
```

- D. Upon completion of the restore, check the tar log again for any problems. Once again, **DO NOT REBOOT.**



5. **[Optional]** Restore other data

Perform restores of other drive letters (non-system Drives) before rebooting.
(Alternatively, perform this step after the reboot.)

6. Stop NetBackup Client Service (bpinetd) and Reboot.

It is now prudent to reboot the server; however, the NetBackup client should be stopped prior to the reboot to ensure the registry information is pushed. The following command can be used to stop the NetBackup Client Service from the command line:

```
net stop "NetBackup Client Service"
```

Figure 5.4.3.2-5: Stopping NetBackup Client displays the output of stopping the NetBackup Client Service from the Microsoft Windows command line.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.BR-W2K8-AD>net stop "NetBackup Client Service"
The NetBackup Client Service service is stopping..
The NetBackup Client Service service was stopped successfully.

C:\Users\Administrator.BR-W2K8-AD>_
```

Figure 5.4.3.2-5: Stopping NetBackup Client



Verify Functionality

Once the server completes the reboot after restoring, verify functionality by checking if users can login. **Figure 5.4.3.2-6: Validating User Login** displays user *Jane* logged into the example.com Windows Domain post restore to the domain controller, *br-w2k8-ad*.

```
Z:\>net user jane
User name                jane
Full Name                Jane Tyndall
Comment
User's comment
Country code             000 (System Default)
Account active           Yes
Account expires          Never

Password last set        5/17/2011 12:07:23 PM
Password expires         6/28/2011 12:07:23 PM
Password changeable      5/18/2011 12:07:23 PM
Password required         Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory            \\br-w2k8-ad\home\jane
Last logon               5/24/2011 3:57:08 PM

Logon hours allowed      All

Local Group Memberships
```

Figure 5.4.3.2-6: Validating User Login



5.4.3.3 Bare Metal Restore

There are a multitude of ways to protect machines in the event of a disaster. Symantec offers a Bare Metal Restore¹⁴ option within NetBackup that provides a single step recovery capability. This greatly streamlines disaster recovery scenarios and can perform multiple DR operations at the same time for multiple machines. The following components comprise the Bare Metal Restore environment:

- **BMR Main Server**
 - Responsible for BMR administrative functions and provides the appropriate services to other BMR servers and BMR clients. It maintains the BMR database that describes the total BMR environment, methods, and utilities that implement the services requested by other BMR servers or BMR clients.
- **BMR File Server**
 - Maintains the recovery environment referred to as the Shared Resource Tree (SRT). Each SRT contains the operating system and additional utilities (such as VERITAS Volume Manager) needed to rebuild and restore the BMR Client.
 - Operating System Image via Shared Resource Tree (SRT)
- **BMR Boot Server**
 - Maintains the Unix boot images and kernels required for Unix BMR clients to perform a diskless network boot. Windows BMR clients do not use a network based boot image to initiate the recovery, but rather boot from a single BMR floppy disk.
 - Pre-execution (PXE) environment
 - Dynamic Host Control Protocol (DHCP)
- **BMR Client**
 - Primary function is to save an up-to-date snapshot of the system's configuration each time a scheduled backup executes. This snapshot is referred to as the client's "meta-data". The meta-data is required to rebuild the machine during BMR system recovery. On a Windows platform, the BMR Client is also responsible for the creation/modification of the SRT and creating the bootable floppy disk.
 - Within each backup policy configured, an option exists to enable Bare Metal Recovery during execution as shown in **Figure 5.4.3.3-1: Bare Metal Restore Policy Option**.

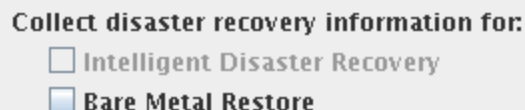


Figure 5.4.3.3-1: Bare Metal Restore Policy Option

Note: For this reference architecture, there was not a focus on utilizing Symantec BMR capabilities as additional deployment/re-deployment methods were configured and used via Red Hat Network Satellite Server, Cobbler, and templates within RHEV. Integrating these services with Symantec BMR are beyond the scope of this guide.



6 Backup and Restore of Red Hat Enterprise Virtualization Manager

The focus of this section is the backup and recovery for Red Hat Enterprise Virtualization Manager¹⁵. Actions include using the NetBackup client to perform file level backup and restore for the Windows operating system and the Microsoft SQL database which provides back-end support for RHEV-M.

6.1 NetBackup Client Installation

The NetBackup client installation for RHEV-M mirrors the same process noted in section 5.2: **Microsoft Windows Client Installation**. The configuration of the client differs in the need to backup the Microsoft SQL database in support of Red Hat Enterprise Virtualization outlined in the following section.

6.2 NetBackup Microsoft SQL Agent Configuration

Once the NetBackup client has been installed, configure the MS SQL client¹⁶ to allow for database backups. The following steps need to be completed prior to configuring the MS SQL backup policy within the NetBackup Administrator Console.

1. Attach to SQL database
2. Configure backup batch file

Attach to SQL Database

Click *Start*, highlight NetBackup MS SQL Client, right-click and select *Run as administrator* as depicted in **Figure 6.2-1: Open NetBackup MS SQL Client**.

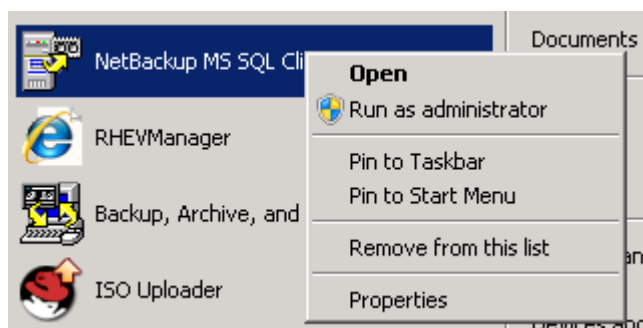


Figure 6.2-1: Open NetBackup MS SQL Client



Input the *Host*, *Instance*, *Userid* and *Password* for the SQL database as displayed in **Figure 6.2-2: SQL Server Agent Properties**. The password required is the same as was provided during the installation of Red Hat Enterprise Virtualization Manager and may differ from the RHEV-M administrator login.

SQL Server connection properties

Database management system: SQL Server
Your Windows account: Administrator

SQL Server properties

Host
br-rhevnm

Instance
SQLEXPRESS

SQL Server version: 2005 Security: Mixed Host type: local

NetBackup for SQL Server is installed on selected host? ☒ Yes

Userid and Password for SQL Server Standard or Mixed Security

Userid: sa Password: ***** Reenter password: *****

Apply Close Help

Figure 6.2-2: SQL Server Agent Properties



Configure Backup Batch File

With a successful connection established with the SQL database, objects can be selected for backup and a subsequent backup batch file can be created. From the NetBackup MS SQL client, click *File* and *Backup SQL Server objects* as shown in **Figure 6.2-3: Backup SQL Server Objects**.

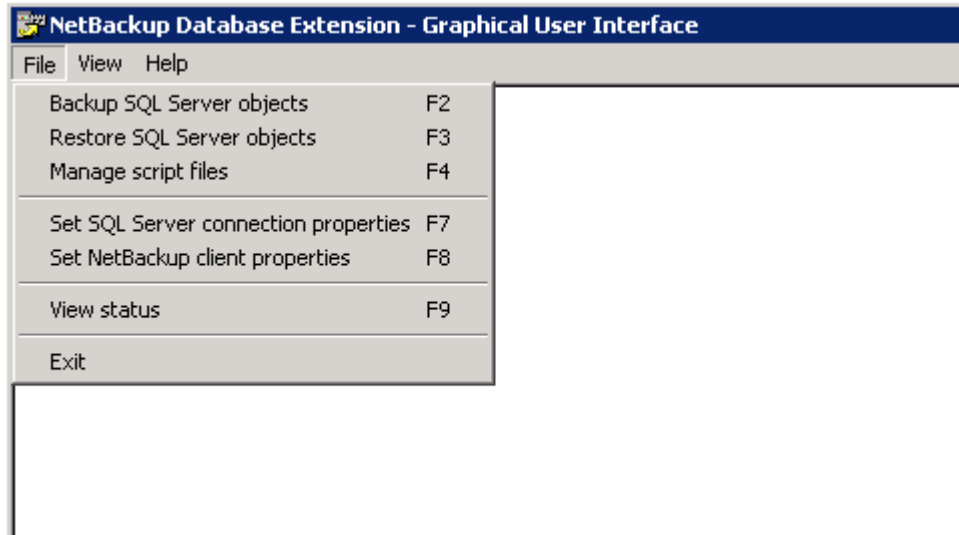


Figure 6.2-3: Backup SQL Server Objects



Highlight the SQL instance under the *Expand Database* left window pane and then select all databases on the *Select database(s) for backup from instance* right window pane as displayed in **Figure 6.2-4: SQL Database Backup Selection**.

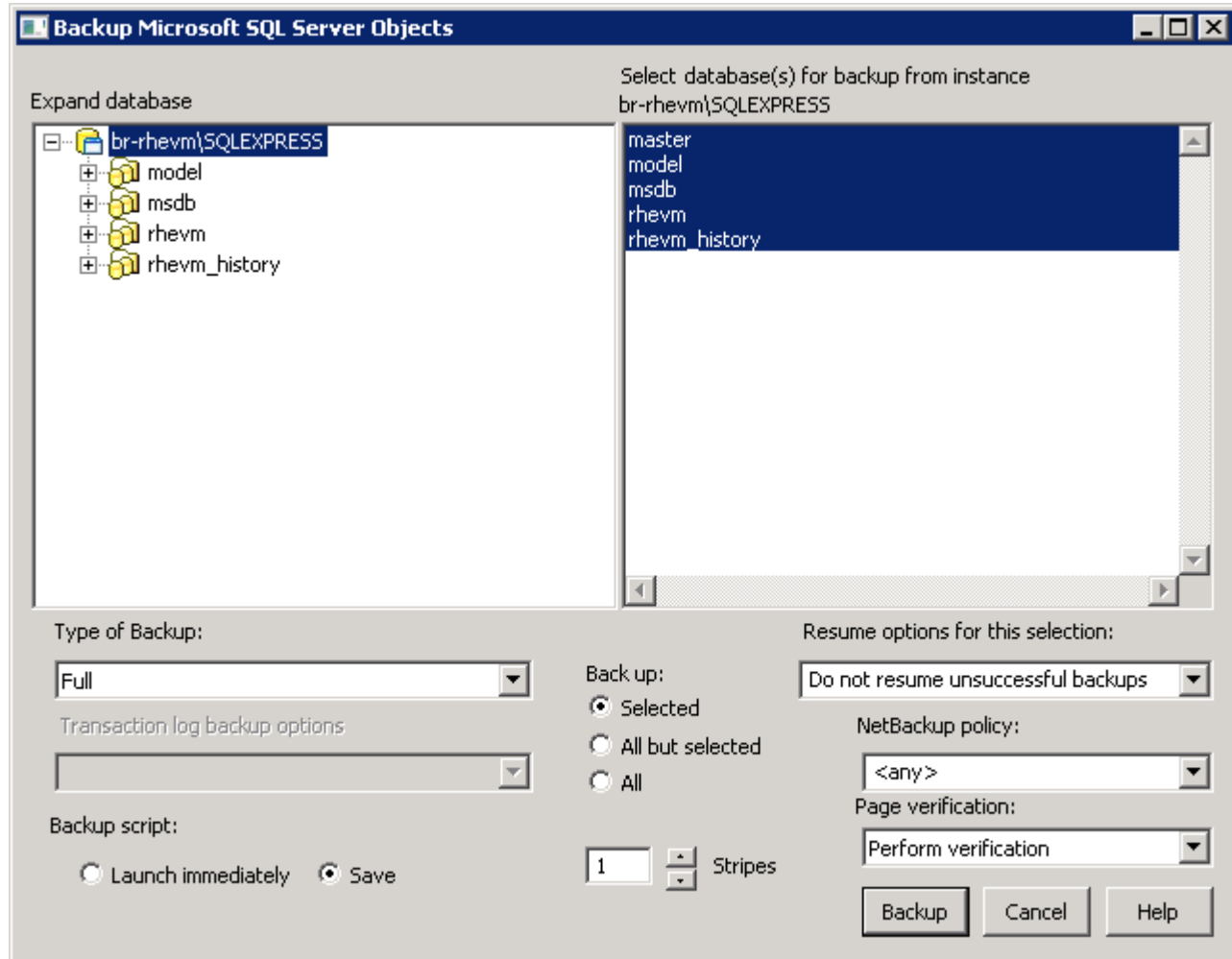


Figure 6.2-4: SQL Database Backup Selection

Ensure that *Type of Backup* is set to Full, *Resume options for this selection* are set as desired as-well-as *Page verification*. Ensure *Backup script* is checked for Save. Once complete, click on *Backup*. Additional details on creating Microsoft SQL backup scripts with the NetBackup client can be found in: *Symantec NetBackup for Microsoft SQL Server Administrator's Guide 7.0*¹⁷



Choose a location and name for the newly created backup batch file as shown in **Figure 6.2-5: Save SQL Database Backup Selection**.

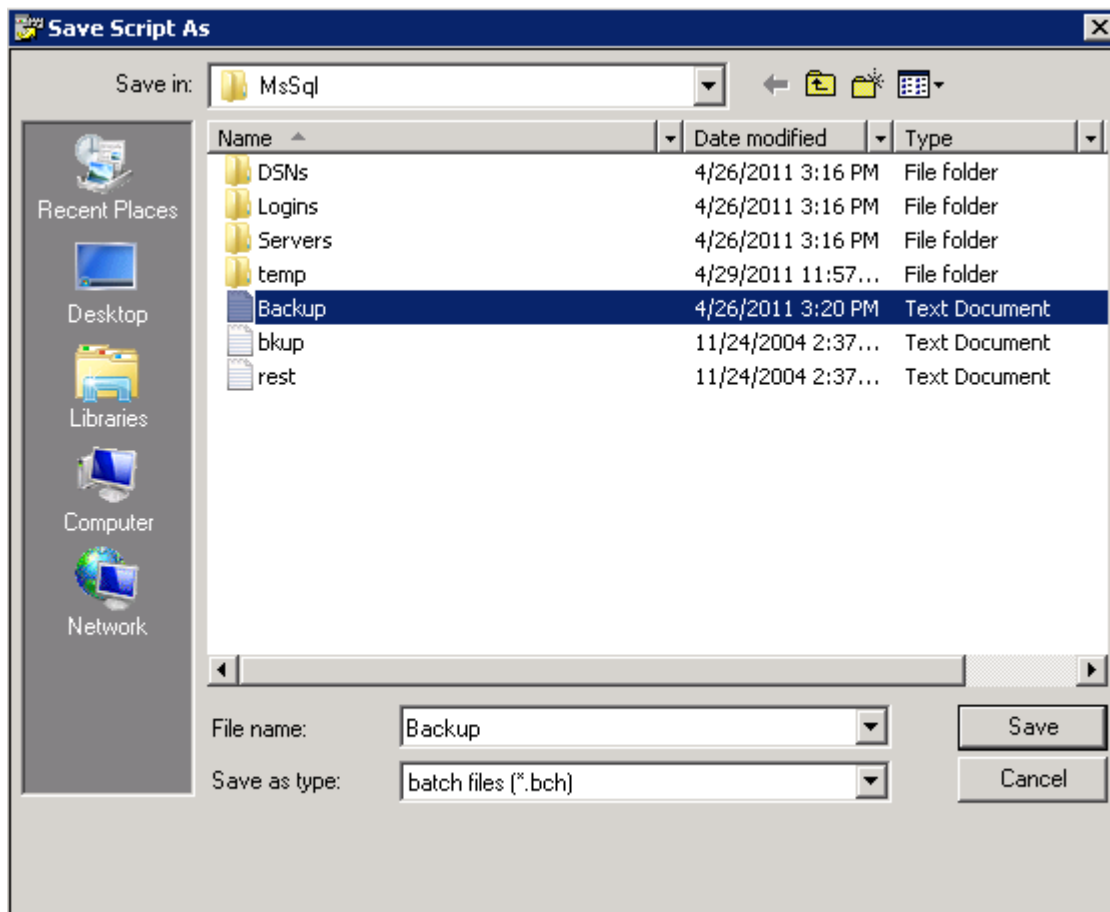


Figure 6.2-5: Save SQL Database Backup Selection

Take note of the path and file name for the batch file as it is later used to create the policy within the NetBackup Administration Console.



6.2.1 Backup Policy Creation

Setup a new backup policy within the NetBackup Administration Console. Set the policy type to *MS-SQL-Server* as listed in **Figure 6.2.1-1: MS SQL Policy Type**.

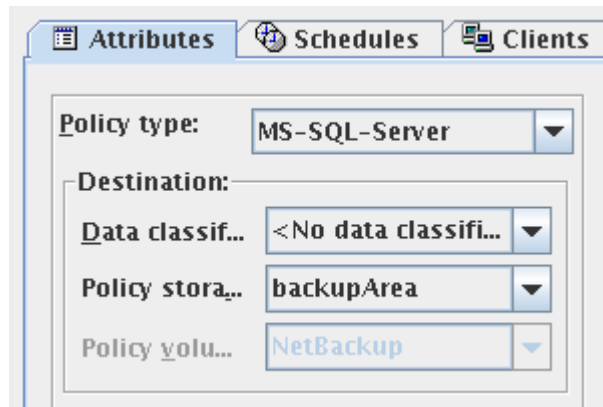


Figure 6.2.1-1: MS SQL Policy Type

Add the client machine, define the schedule and input the selection. In the case of creating a MS SQL policy, the backup selection will be the full file system path to the backup batch file created on the target machine. For this reference environment the path is:

C:\Program Files\Veritas\NetBackup\DbExt\MsSql\Backup.bch as depicted in **Figure 6.2.1-2: MSSQL Backup Policy Selection**.

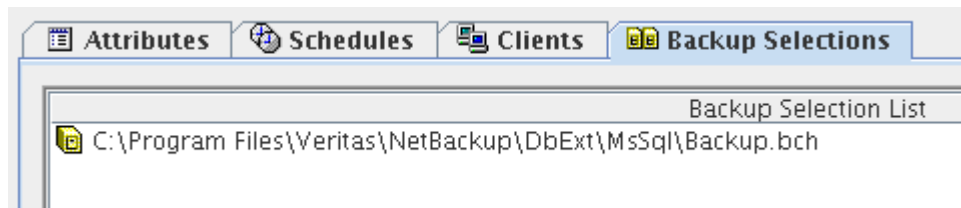


Figure 6.2.1-2: MSSQL Backup Policy Selection

6.3 Backup

Perform manual test backups using the newly created policies to ensure functionality. Any issues encountered should be resolved before relying on automated scheduled backup integrity. Based on industry best practices, it is highly recommended to perform periodic test restores to verify and validate backup and restore procedures and functionality. Refer to section **5.3 Backup** as a reference for performing test backups using the NetBackup Administration Console.



6.4 Restore

Performing file level restores for RHEV-M can involve operating system and database recovery depending on the nature of the issue or requirement that may impact the environment. Partial (select restore such as a database, application, or operating system) or a full system restore (complete to include database, application and operating system) may become necessary. The following sub-sections outline procedures for recovery in various scenarios.

6.4.1 Partial

6.4.1.1 RHEV-M Application Failure

In this scenario, the RHEV-M application has become unresponsive and repeated attempts to access the Admin Console have failed. The machine has been rebooted and it is noted that the *RHEV Manager* service attempts to start and fails. The following steps are taken to resolve this scenario:

1. Restore operating system
2. Restore system state and shadow copy components
3. Verify functionality

Restore Operating System

The operating system restore can be initiated from the client or from the NetBackup Administration Console. For this scenario, the Administration Console is used. First, specify the backup server, source, destination and policy type as displayed in **Figure 6.4.1.1-1: Specify Backup, Destination and Policy**.

Specify NetBackup Machines and Policy Type

Server to use for backups and restores:
bkup Edit Server List

Source client for restores:
br-rhev-m-bkup Browse

Destination client for restores:
br-rhev-m-bkup Browse

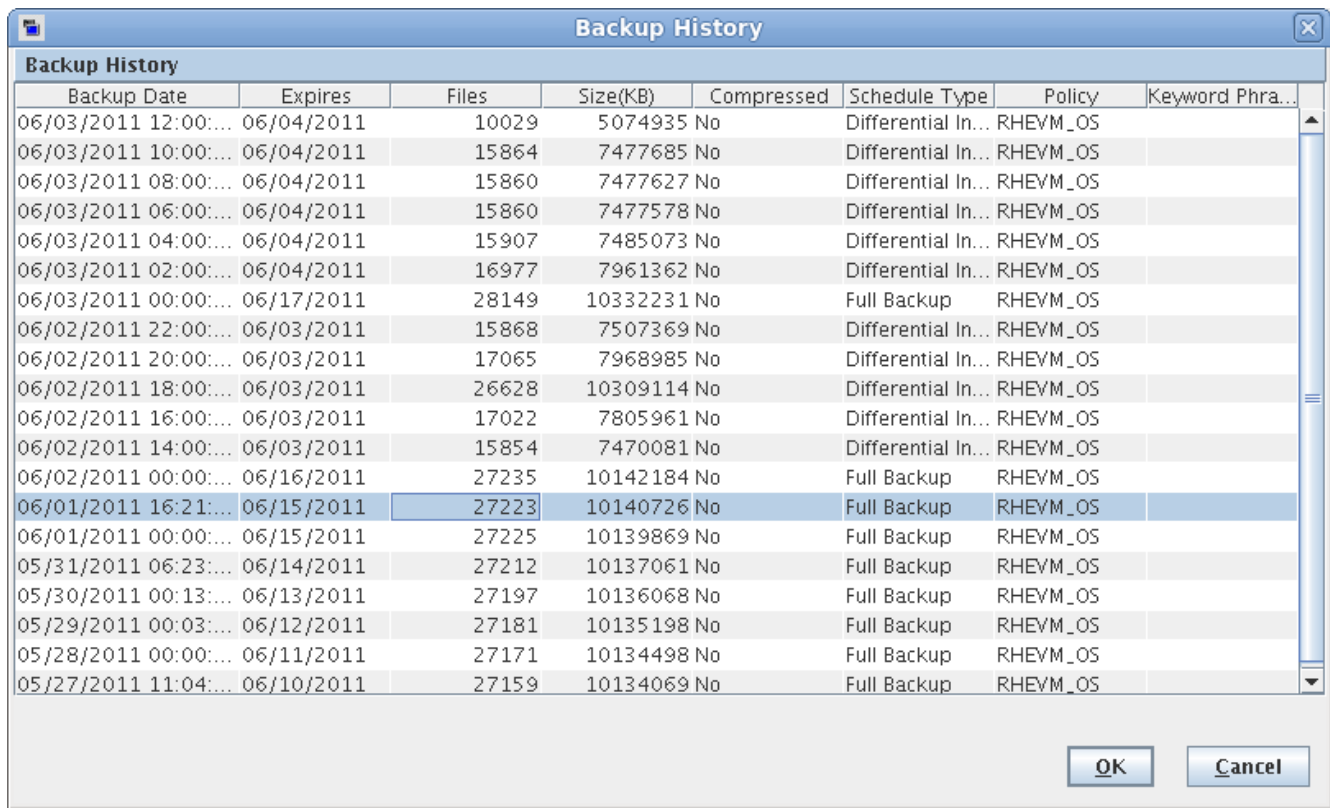
Policy type for restores:
MS-Windows

OK Cancel Help

Figure 6.4.1.1-1: Specify Backup, Destination and Policy



Next, select the date to restore from backup as shown in **Figure 6.4.1.1-2: RHEV-M Restore Date Range**.



Backup Date	Expires	Files	Size(KB)	Compressed	Schedule Type	Policy	Keyword Phra...
06/03/2011 12:00:...	06/04/2011	10029	5074935	No	Differential In...	RHEVM_OS	
06/03/2011 10:00:...	06/04/2011	15864	7477685	No	Differential In...	RHEVM_OS	
06/03/2011 08:00:...	06/04/2011	15860	7477627	No	Differential In...	RHEVM_OS	
06/03/2011 06:00:...	06/04/2011	15860	7477578	No	Differential In...	RHEVM_OS	
06/03/2011 04:00:...	06/04/2011	15907	7485073	No	Differential In...	RHEVM_OS	
06/03/2011 02:00:...	06/04/2011	16977	7961362	No	Differential In...	RHEVM_OS	
06/03/2011 00:00:...	06/17/2011	28149	10332231	No	Full Backup	RHEVM_OS	
06/02/2011 22:00:...	06/03/2011	15868	7507369	No	Differential In...	RHEVM_OS	
06/02/2011 20:00:...	06/03/2011	17065	7968985	No	Differential In...	RHEVM_OS	
06/02/2011 18:00:...	06/03/2011	26628	10309114	No	Differential In...	RHEVM_OS	
06/02/2011 16:00:...	06/03/2011	17022	7805961	No	Differential In...	RHEVM_OS	
06/02/2011 14:00:...	06/03/2011	15854	7470081	No	Differential In...	RHEVM_OS	
06/02/2011 00:00:...	06/16/2011	27235	10142184	No	Full Backup	RHEVM_OS	
06/01/2011 16:21:...	06/15/2011	27223	10140726	No	Full Backup	RHEVM_OS	
06/01/2011 00:00:...	06/15/2011	27225	10139869	No	Full Backup	RHEVM_OS	
05/31/2011 06:23:...	06/14/2011	27212	10137061	No	Full Backup	RHEVM_OS	
05/30/2011 00:13:...	06/13/2011	27197	10136068	No	Full Backup	RHEVM_OS	
05/29/2011 00:03:...	06/12/2011	27181	10135198	No	Full Backup	RHEVM_OS	
05/28/2011 00:00:...	06/11/2011	27171	10134498	No	Full Backup	RHEVM_OS	
05/27/2011 11:04:...	06/10/2011	27159	10134069	No	Full Backup	RHEVM_OS	

Figure 6.4.1.1-2: RHEV-M Restore Date Range

Select the system drive to restore as seen in **Figure 6.4.1.1-3: System Drive Selection**.

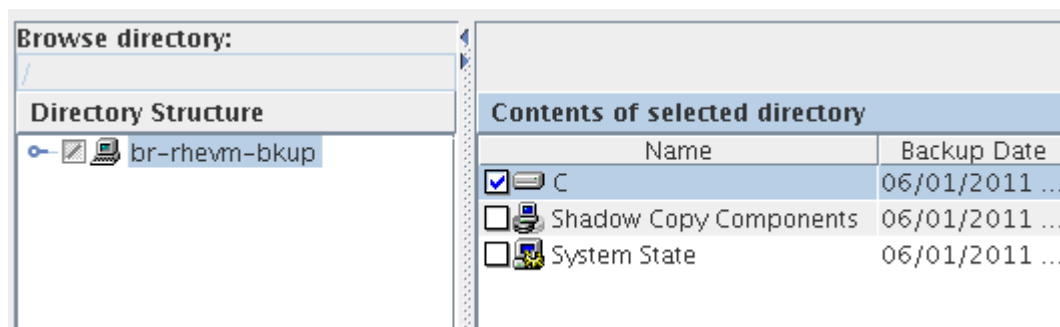


Figure 6.4.1.1-3: System Drive Selection

Do not elect to restore the System State/Shadow Copy Components at the same time as the system drive. Monitor the restore progress and ensure it completes successfully.

Note: DO NOT REBOOT after the system drive(s) restore is completed.



Restore System State and Shadow Copy Components

With the system drive restored, the system state and shadow copy components follow. Execute the following command on the system prior to initiating the system state and shadow volume copy restore:

```
C:\Program_Files\VERITAS\NetBackup\bin\w2koption -restore -same_hardware  
1
```

Once complete, select the *Shadow Copy Components* and *System State* as depicted in **Figure 6.4.1.1-4: System State and Shadow Copy Selection**.

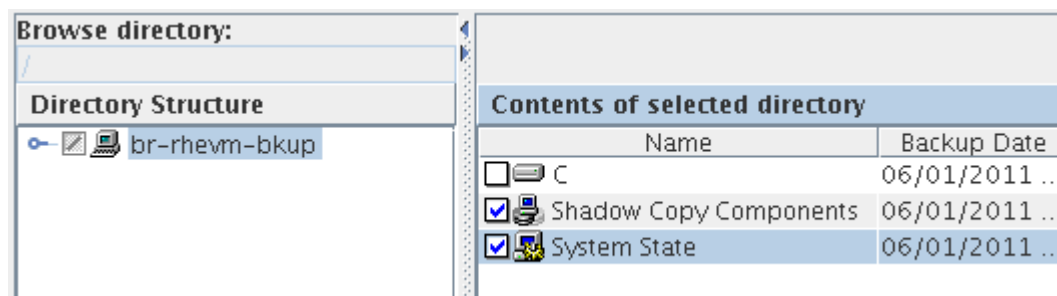


Figure 6.4.1.1-4: System State and Shadow Copy Selection

Monitor the restore progress and ensure it completes successfully. Repeat the w2koption command as performed earlier:

```
C:\Program_Files\VERITAS\NetBackup\bin\w2koption -restore -same_hardware  
1
```

It is now prudent to reboot the server, however, the NetBackup client should be stopped prior to the reboot as shown in **Figure 6.4.1.1-5: Post Restore NetBackup Client Stop**.

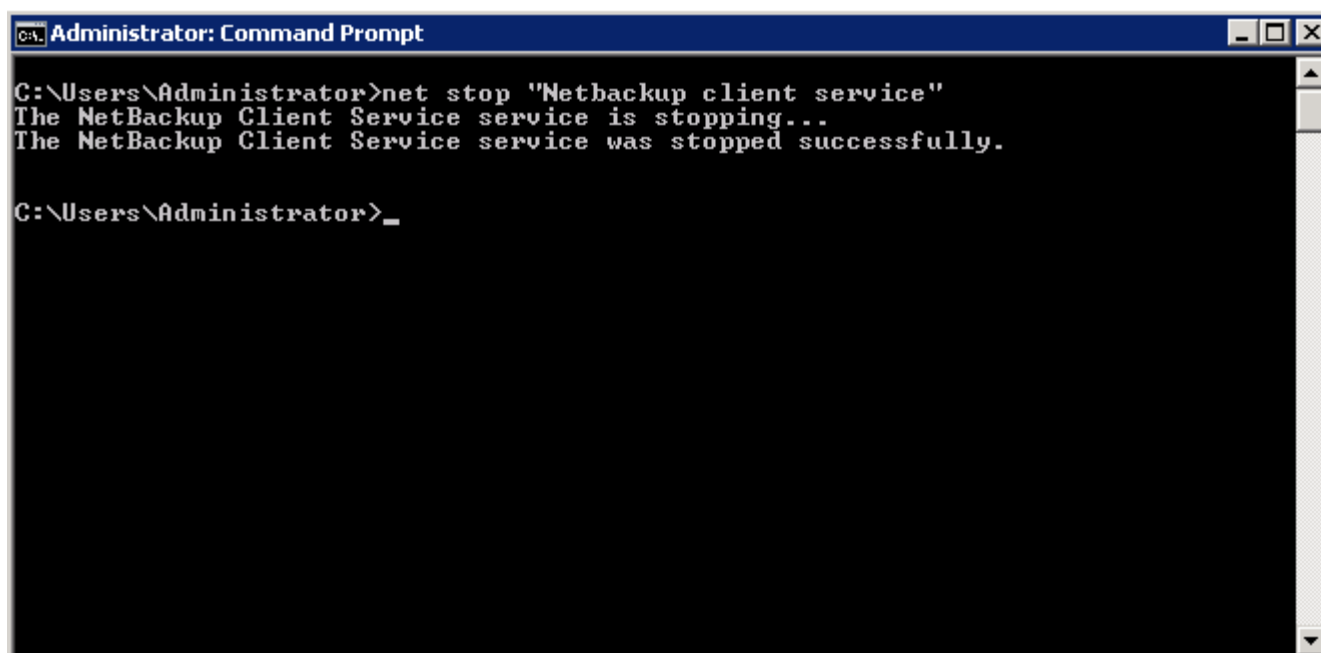


Figure 6.4.1.1-5: Post Restore NetBackup Client Stop



Verify Functionality

With the system restore and reboot complete, access the RHEV-M Admin Portal to verify functionality. In this scenario, access to the portal was restored and the RHEV environment able to be managed as depicted in **Figure 6.4.1.1-6: RHEV-M Portal Access**.

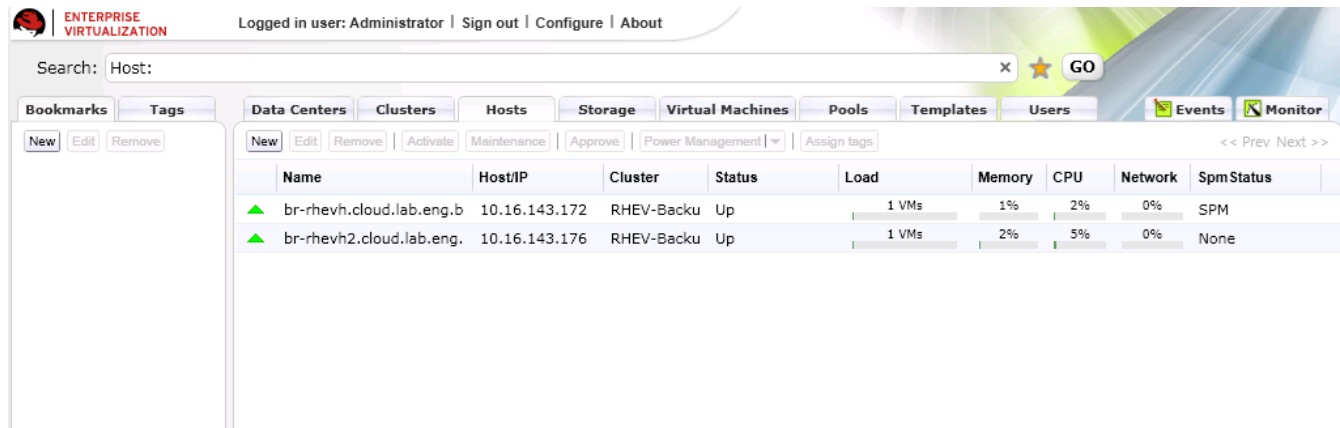


Figure 6.4.1.1-6: RHEV-M Portal Access

6.4.1.2 RHEV-M DB Corruption

The next scenario involves having a corrupted RHEV database on the RHEV-M host. Upon login to the RHEV Admin Portal, an event is generated advising that there is a database error. Upon troubleshooting, it has been determined that the *rhev* database experienced corruption and a restore of the RHEV database from a previous backup is the best solution to resolve the error. The following steps are taken to recover:

1. Stop the RHEV-M services
2. Restore database from a selected backup
3. Verify Functionality

Stop RHEV-M Services

Within Windows, open the Services management console by clicking *Start*, type *services.msc* in the *Search programs and files* dialogue box and hit *Enter*. Stop the following services:

- RHEV Manager
- RHEV Net Console
- RHEV Notification Service

Figure 6.4.1.2-1: RHEV-M Services displays a list of the services within the management console.

	RHEV Manager	Red Hat En...	Automatic
	RHEVM History Ser...	RHEVM Dat...	Manual
	RHEVM Net Console	RHEVM Net...	Automatic
	RHEVM Notification ...	Red Hat En...	Automatic

Figure 6.4.1.2-1: RHEV-M Services



Restore Database

With the RHEV-M services stopped, open the NetBackup MS SQL Client by clicking *Start* and selecting from the Start Menu. Click *File* and choose *Restore SQL Server Objects* as shown in **Figure 6.4.1.2-2: Restore SQL Objects**.

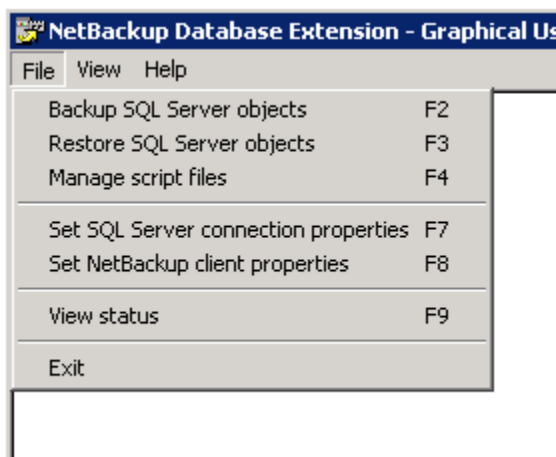


Figure 6.4.1.2-2: Restore SQL Objects

Choose the SQL host and date range for the backup files as displayed in **Figure 6.4.1.2-3: SQL Backup History**.

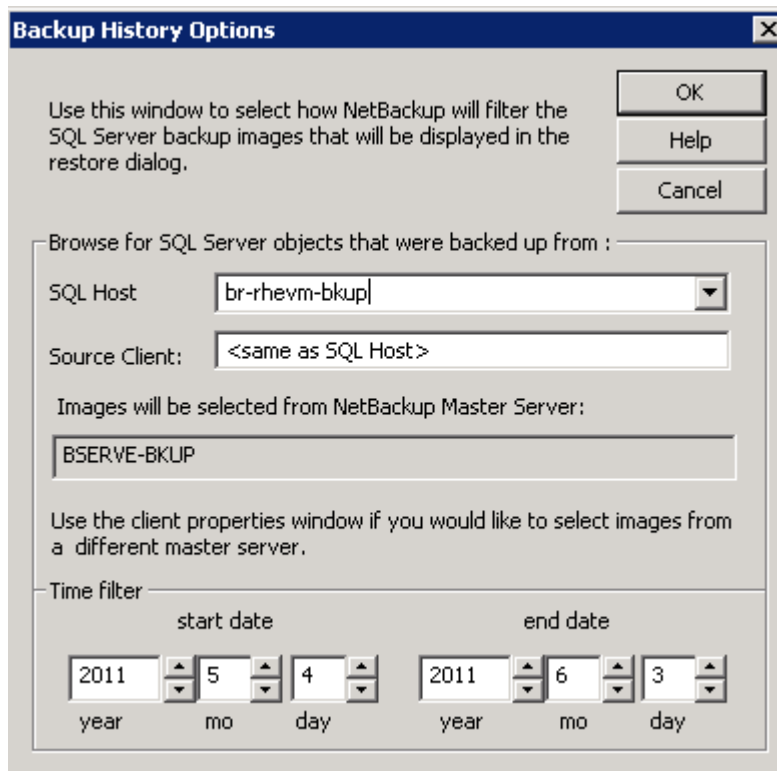


Figure 6.4.1.2-3: SQL Backup History



Expand the *rhev*m database and choose a date to restore from. Set the restore parameters to the following:

Option	Parameter	Description
Scripting	Restore selected object	Restore selected database
Recovery	Recovered	Allows database to be usable after restore
Consistency Check	Full check, including indexes	Verify database consistency after a restore including indexes
Page Verification	Perform verification	Used for SQL Server 2005 or later where torn page detection ¹⁸ and checksum are supported
Restore Script	Launch immediately	Execute job immediately

Table 6.4.1.2-A: SQL Restore Settings

Figure 6.4.1.2-4: SQL Restore Options displays the restore job settings.

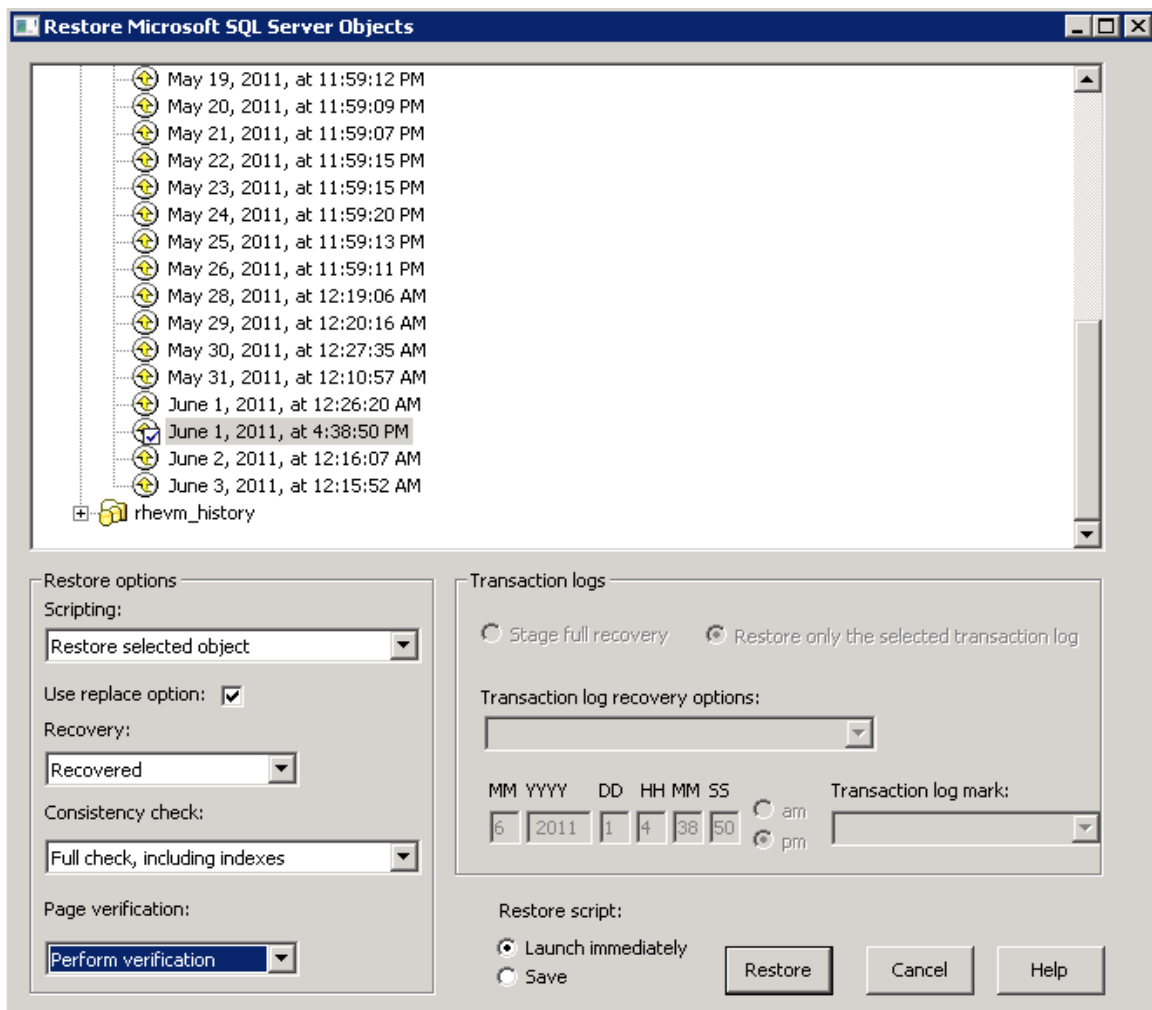


Figure 6.4.1.2-4: SQL Restore Options



Click *Restore* to begin the database recovery. Progress for the running job can be viewed via the NetBackup Administration Console under *Activity Monitor*. Monitor the job for completion. Upon success, start the RHEV-M services as shown in **Figure 6.4.1.2-5: RHEV-M Service Start**.

	RHEV Manager	Red Hat En...	Started	Automatic
	RHEVM History Ser...	RHEVM Dat...		Manual
	RHEVM Net Console	RHEVM Net...	Started	Automatic
	RHEVM Notification ...	Red Hat En...	Started	Automatic

Figure 6.4.1.2-5: RHEV-M Service Start

Verify Functionality

Open the RHEV-M Admin Portal and view the *Events* tab for any database related errors as displayed in **Figure 6.4.1.2-6: RHEV-M Portal Events**.

	Time	Message	Event ID	User	Host	Virtual Machine	Template	Storage
✓	Jun 03, 17:11	User Administrator logged in.	30	Administratc				
✓	Jun 03, 17:07	Storage Pool Manager runs on Host br-rhev.cloud.lab.eng.bos.redhat.com (IP Address: 10.16.143.172).	204		br-rhev.cloud			
✓	Jun 03, 17:07	Detected new Host br-rhev2.cloud.lab.eng.bos.redhat.com. Host state was set to Up .	13		br-rhev2.cl			
✓	Jun 03, 17:07	Detected new Host br-rhev.cloud.lab.eng.bos.redhat.com. Host state was set to Up .	13		br-rhev.cloud			
!	Jun 03, 17:07	Error getting Data Center RHEV-Backup status - setting status to Non-Responsive.	980		br-rhev.cloud			
!	Jun 03, 17:06	VM br-rhel6-rcvr was set to the Unknown status.	142		br-rhev2.cl	br-rhel6-rcvr	RHEL6	
!	Jun 03, 17:06	VM br-rhel56 was set to the Unknown status.	142		br-rhev.cloud	br-rhel56	Blank	
✓	Jun 03, 17:06	Starting RHEV Manager.	1					

Figure 6.4.1.2-6: RHEV-M Portal Events



6.4.2 Full RHEV-M Machine Crash

The final scenario deals with recovering a machine running RHEV-M. The machine has experienced disk corruption and will no longer boot to the operating system. Utilizing NetBackup, the backup administrator will recover the machine back to an operational state. The following steps are taken to restore the machine:

1. Install base operating system
2. Configure networking
3. Install and configure the NetBackup Client
4. Install RHEV-M
5. Restore operating system
6. Restore system state and shadow copy components
7. (Optional) Restore database to a specific point in time
8. Verify functionality

Install Base Operating System

There are multiple ways to redeploy the operating system onto a machine. Some environments may use Bare Metal Restore, Windows Deployment Services, or other automated and non-automated methods. For this reference architecture, install from DVD was the chosen method. For additional options, refer to **Appendix D.4 Additional RHEV-M Backup and Recovery**.

Configure Networking

Once the operating system has been deployed, configuration of the network interfaces may be needed to assign static IP addresses to selected network interface controllers (NIC). This will vary depending on environmental configuration and needs. For this reference architecture, it involves assigning a static IP address to the second NIC for the dedicated backup network as depicted in **Figure 6.4.2-1: NIC Static IP Address Assignment**.

The screenshot shows a network configuration window with two radio buttons at the top. The first radio button, labeled 'Obtain an IP address automatically', is unselected. The second radio button, labeled 'Use the following IP address:', is selected. Below this, there are three text input fields. The first field is labeled 'IP address:' and contains the text '192 . 168 . 77 . 171'. The second field is labeled 'Subnet mask:' and contains the text '255 . 255 . 255 . 0'. The third field is labeled 'Default gateway:' and contains three dots separated by spaces.

Figure 6.4.2-1: NIC Static IP Address Assignment

Note: If using host files to redirect backup traffic over specific networks, update the file as needed located at `C:\Windows\System32\drivers\etc\hosts`.



Install and Configure NetBackup Client

For specifics regarding the installation and configuration of the NetBackup Client, refer to section **5.2 Microsoft Windows Client Installation**.

Install RHEV-M

With the operating system, network configuration and NetBackup Client installed and configured, the next step is to install RHEV-M. Perform a full install to include installing the RHEVM Database as shown in **Figure 6.4.2-2: RHEV-M Database Selection** and **Figure 6.4.2-3: RHEV-M Install SQL**.

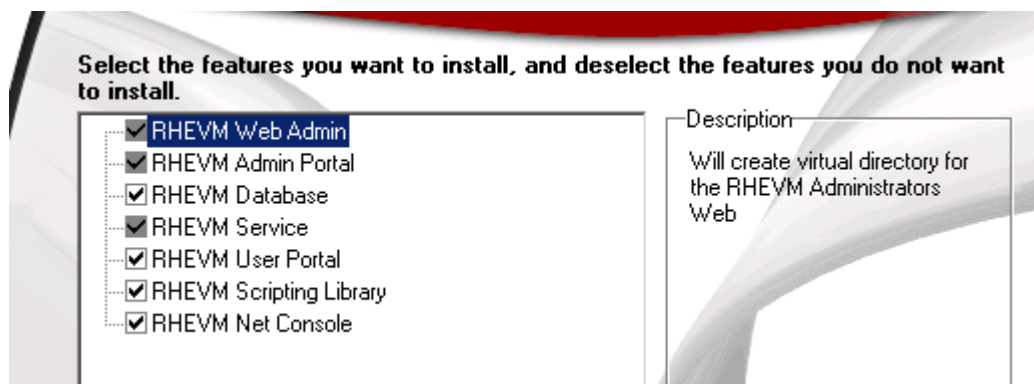


Figure 6.4.2-2: RHEV-M Database Selection



Figure 6.4.2-3: RHEV-M Install SQL

Reboot the server once the installation completes. Before proceeding with restoring the operating system and system state, stop the running RHEV-M services. Refer to section **6.4.1.2 RHEV-M DB Corruption** for a list of services.

Restore Operating System

For specifics regarding the operating system restore, refer to section **6.4.1.1 RHEV-M Application Failure**.

Restore System State and Shadow Copy Components

For specifics regarding the system state and shadow volume copy restore, refer to section **6.4.1.1 RHEV-M Application Failure**.

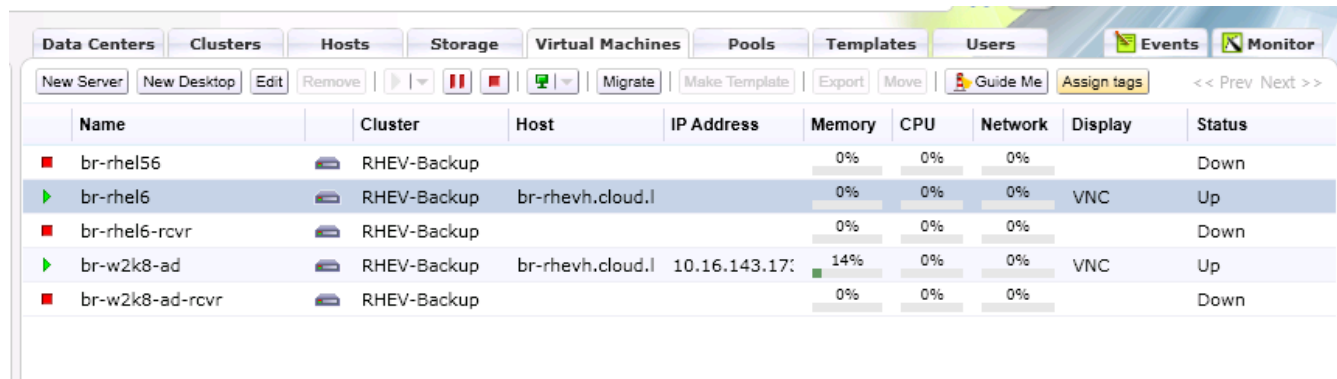


(Optional) Restore Database

It may be desired to restore the *rhev* database from a specific point in time. Refer to section **6.4.1.2 RHEV-M DB Corruption** for specific database recovery details.

Verify Functionality

With the operating, system state and optionally the database restore complete, reboot the server and RHEV-M was restored to a previously working state. Login to the RHEV-M Admin Portal and verify RHEV-M displays the correct information as shown in **Figure 6.4.2-4: RHEV-M Post Full Restore**.



Name	Cluster	Host	IP Address	Memory	CPU	Network	Display	Status
br-rhel56	RHEV-Backup			0%	0%	0%		Down
br-rhel6	RHEV-Backup	br-rhevcloud.l		0%	0%	0%	VNC	Up
br-rhel6-rcvr	RHEV-Backup			0%	0%	0%		Down
br-w2k8-ad	RHEV-Backup	br-rhevcloud.l	10.16.143.17	14%	0%	0%	VNC	Up
br-w2k8-ad-rcvr	RHEV-Backup			0%	0%	0%		Down

Figure 6.4.2-4: RHEV-M Post Full Restore

Note: For all restore operations, it may be desirable to disable any backup policies for the affected machine until the restore is complete to prevent backup jobs from running during the restore operation.



7 Conclusion

This paper demonstrated the ability to backup and recover a Red Hat Enterprise Virtualization environment using Symantec NetBackup to maintain business continuity. The following steps were successfully performed:

- Symantec NetBackup setup and configuration within a Red Hat Enterprise Virtualization environment
- Virtual Machine file level backup and recovery
- Virtual Machine operating system backup and recovery
- Red Hat Enterprise Virtualization Manager application backup and recovery
- Red Hat Enterprise Virtualization Manager database backup and recovery
- Red Hat Enterprise Virtualization full system backup and recovery

There are almost endless possibilities in regards to maintaining business continuity. When planning for backup and recovery, many considerations need to be taken into account and will vary based on specific business needs. This drives the ultimate list of requirements for IT departments to plan for. Some requirements may include:

- Data deduplication¹⁹
- Off-site storage
- Data retention policies
- Data encryption
- Reporting
- Scalability

In conclusion, business continuity is of utmost importance for business operations. It is critical to maintain and operate successful backup and recovery procedures and plans regardless of the tools used. Requirements for each environment and businesses will vary however the need to recover from unplanned disasters never changes.



Appendix A: NetBackup SQL Backup and Restore Batch Files

Contents of *Backup.bch* file:

```
GROUPSIZE 5
OPERATION BACKUP
DATABASE "master"
SQLHOST "br-rheVM"
SQLINSTANCE "SQLEXPRESS"
NBSERVER "BSEVER-BKUP"
MAXTRANSFERSIZE 6
BLOCKSIZE 7
NUMBUFS 2
VERIFYOPTION STOPONERROR
ENDOPER TRUE
```

```
OPERATION BACKUP
DATABASE "model"
SQLHOST "br-rheVM"
SQLINSTANCE "SQLEXPRESS"
NBSERVER "BSEVER-BKUP"
MAXTRANSFERSIZE 6
BLOCKSIZE 7
NUMBUFS 2
VERIFYOPTION STOPONERROR
ENDOPER TRUE
```

```
OPERATION BACKUP
DATABASE "msdb"
SQLHOST "br-rheVM"
SQLINSTANCE "SQLEXPRESS"
NBSERVER "BSEVER-BKUP"
MAXTRANSFERSIZE 6
BLOCKSIZE 7
NUMBUFS 2
VERIFYOPTION STOPONERROR
ENDOPER TRUE
```

```
OPERATION BACKUP
DATABASE "rheVM"
SQLHOST "br-rheVM"
SQLINSTANCE "SQLEXPRESS"
NBSERVER "BSEVER-BKUP"
MAXTRANSFERSIZE 6
BLOCKSIZE 7
NUMBUFS 2
```



```
VERIFYOPTION STOPONERROR  
ENDOPER TRUE
```

```
OPERATION BACKUP  
DATABASE "rheVM_history"  
SQLHOST "br-rheVM"  
SQLINSTANCE "SQLEXPRESS"  
NBSERVER "BSEVE-BKUP"  
MAXTRANSFERSIZE 6  
BLOCKSIZE 7  
NUMBUFS 2  
VERIFYOPTION STOPONERROR  
ENDOPER TRUE
```

Example *Restore.bch* file:

```
OPERATION RESTORE  
OBJECTTYPE DATABASE  
DATABASE "rheVM"  
# The following image is type: Full  
NBIMAGE "br-rheVM.MSSQL7.BR-  
RHEVM\SQLEXPRESS.db.rheVM.~.7.001of001.20110601163850..C"  
SQLHOST "br-rheVM"  
SQLINSTANCE "SQLEXPRESS"  
NBSERVER "BSEVE-BKUP"  
BROWSECLIENT "br-rheVM-bkup"  
MAXTRANSFERSIZE 6  
BLOCKSIZE 7  
CONSISTENCYCHECK FULLINCLUDINGINDICES  
RESTOREOPTION REPLACE  
RECOVEREDSTATE RECOVERED  
NUMBUFS 2  
VERIFYOPTION STOPONERROR  
ENDOPER TRUE
```



Appendix B: Host Configuration Files

bkup

/etc/hosts

```
10.16.x.x bkup.cloud.....
192.168.66.170 bserve-mgmt
192.168.77.170 bserve-bkup bserve
192.168.66.171 br-rheVM-mgmt
192.168.77.171 br-rheVM-bkup
192.168.66.172 br-rhevh-mgmt
192.168.77.172 br-rhevh-bkup
192.168.66.176 br-w2k8-ad-mgmt
192.168.77.176 br-w2k8-ad-bkup
192.168.66.177 br-rhel56-mgmt
192.168.77.177 br-rhel56-bkup
192.168.66.178 br-rhel6-mgmt
192.168.77.178 br-rhel6-bkup
```

br-rheVM

C:\Windows\System32\drivers\etc\hosts

```
192.168.66.170 bserve-mgmt
192.168.77.170 bserve-bkup bserve
192.168.77.171 br-rheVM-bkup
```

br-w2k8-ad

C:\Windows\System32\drivers\etc\hosts

```
192.168.66.170 bserve-mgmt
192.168.77.170 bserve-bkup bserve
```

br-rhel56

/etc/hosts

```
10.16.x.x br-rhel56.cloud.....
192.168.77.170 bserve-bkup bserve
192.168.66.170 bserve-mgmt
```

br-rhel6

/etc/hosts

```
192.168.66.170 bserve-mgmt
192.168.77.170 bserve-bkup bserve
```




Appendix C: Iptables

NetBackup master server – **bkup**

/etc/sysconfig/iptables

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 13724 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 13720 -j ACCEPT
-A RH-Firewall-1-INPUT -j LOG --log-prefix "firewall dropped packet: "
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Red Hat Enterprise Linux client – **br-rhel6**

/etc/sysconfig/iptables

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [28:2992]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.77.0/24 -i eth2 -p tcp -m tcp --dport 13724 -j ACCEPT
-A INPUT -s 192.168.77.0/24 -i eth2 -p tcp -m tcp --dport 13782 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```



/etc/sysconfig/iptables

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [125:15387]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.77.0/255.255.255.0 -i eth2 -p tcp -m tcp --dport 13724 -j
ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.77.0/255.255.255.0 -i eth2 -p tcp -m tcp --dport 13782 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```



Appendix D: RHEV-M Backup and Recovery Boot from SAN

The following scenario describes a boot from SAN Red Hat Enterprise Virtualization Manager machine performing a block level backup of the LUN hosting the operating system from a secondary machine. This can be used as a recovery point used in case of a machine, disk or operating system failure preventing operation.

D.1 Environment Setup

This configuration consists of two physical machines, attached to a Storage Area Network, configured to access the source and destination LUN's for backup as displayed in **Figure D.1-1: Boot from SAN Environment**.

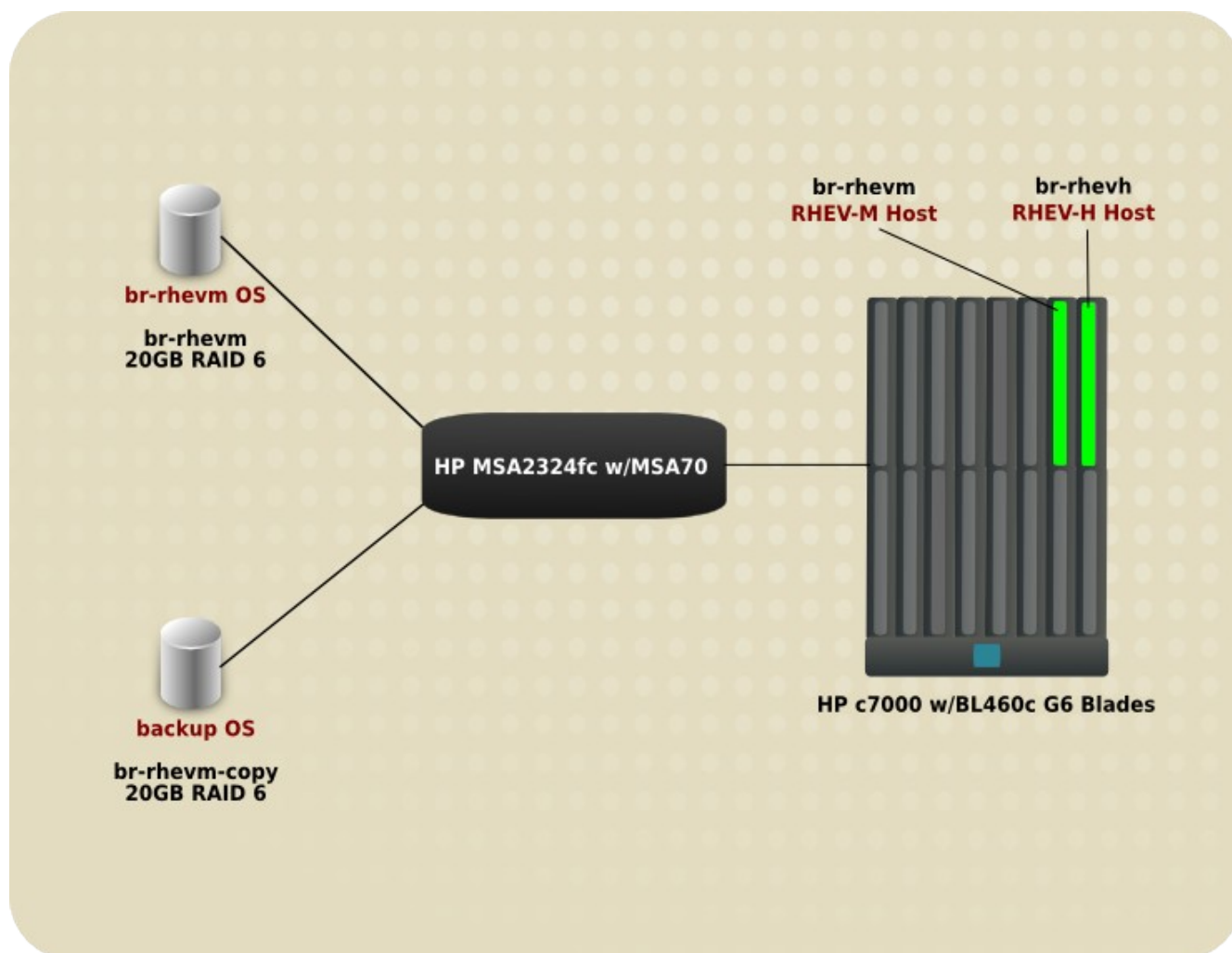


Figure D.1-1: Boot from SAN Environment



Configuring the machine to boot from SAN versus local storage will vary depending on the server and storage equipment manufactures. For this reference environment, the following items were configured to allow boot from SAN:

- On board HP SmartArray RAID controller disabled via the server BIOS
- LUN configured and explicitly mapped to a designated machine
- QLogic host bus adapter BIOS enabled and the configured LUN assigned to boot from

D.2 Snapshot of RHEV-M OS LUN

The following steps are performed to perform a block level snap-shot of the RHEVM-M LUN:

1. Power down the RHEV-M host
2. Configure the secondary host so that it has access to both source and destination LUNs
3. Determine the WWID of each LUN
4. Perform block level copy between the source and destination LUN

Power Down RHEV-M Host

Gracefully power down the RHEV-M machine.

Configure LUN Access

On a secondary Red Hat Enterprise Linux host, configure LUN access so that both *br-rhevm* and *br-rhevm-copy* are zoned for access. For this environment, this is performed by setting explicit mappings from within the HP MSA Storage Management Utility interface for each configured LUN as shown in **Figure D.2-1: Explicit LUN Mapping**.

Maps for Volume br-rhevm						
	Type	Host ID	Name	Ports	LUN	Access
<input type="radio"/>	Default	50060B0000C2860A	br-rhevh2-2			not-mapped
<input type="radio"/>	Default	50060B0000C28608	br-rhevh2-1			not-mapped
<input type="radio"/>	Explicit	50060B0000C28644	br-rhevh-1	A1,A2,B1,B2	58	read-write
<input type="radio"/>	Explicit	50060B0000C28646	br-rhevh-2	A1,A2,B1,B2	58	read-write

Figure D.2-1: Explicit LUN Mapping

Once complete, reboot the secondary host. Alternately, if the *sg3_utils* package is installed, execute `rescan-scsi-bus.sh` to dynamically rescan for added storage.

Note: Refer to the storage vendor for multiple host mapping to the same LUN support.



Determine WWID of Each LUN

With the reboot complete, it is necessary to determine the World Wide Identifier for each LUN. This information is needed to determine the source and destination devices used for the block level copy. Perform the following command on the secondary host:

```
# blkid

[ ... output truncated ... ]

/dev/mapper/3600c0ff000d8d18b293daf4c01000000p1: TYPE="ntfs"
/dev/mapper/3600c0ff000d8d18b9518b74c01000000p1: TYPE="ntfs"

[ ... output truncated ... ]
```

Correlate the `blkid` output to the serial number associated to each LUN. Refer to your storage vendors management interface as needed. For this reference environment, the information is located within the MSA Storage Management Utility interface under the *Volume Overview* information page as depicted in **Figure D.2-2: LUN Serial Number**.

Volume Overview				
Details about a specific volume				
Volume Overview				
	Component	Count	Capacity	Storage Space
<input checked="" type="radio"/>	Volume		20.0GB	<div></div>
<input type="radio"/>	Maps	47		
<input type="radio"/>	Schedules	0		
Properties for br-rhev-m-copy				
Property		Value		
Vdisk Name		BKUPRA		
Name		br-rhev-m-copy		
Size		19.9GB		
Preferred Owner		B		
Current Owner		B		
Serial Number		00c0ffd8d18b00009518b74c01000000		

Figure D.2-2: LUN Serial Number



Once the WWID's for each LUN have been mapped, perform the block level copy using the following command:

```
# dd if=/dev/mapper/3600c0ff000d8d18b293daf4c01000000 \
of=/dev/mapper/3600c0ff000d8d18b9518b74c01000000
```

Command options:

- **if** – source LUN
- **of** – destination LUN

The amount of time for the copy to complete will vary depending on the size of the source and destination. For this configuration, it took approximately 11 minutes to perform a 20GB copy between the source and destination LUNs using defaults.

The Fibre Channel connection speed between the host bus adapters, interconnect switches and connected storage were configured for 8Gb/sec.

Note: The destination LUN must be of equal or greater value than the source LUN.

With the LUN copy complete, a third party backup utility could be used to perform a raw backup of the newly copied data for archive purposes. Access to the LUN must be restricted to a single host to prevent corruption during such processes.

Additionally, some SAN manufactures provide utilities third party backup software providers are able to integrate with to perform SAN LUN copies, snapshots and data replication. Refer to the backup software and SAN hardware vendors for additional information for compatibility with these features.



D.3 Recovering RHEV-M from Snapshot LUNs

When complete, unmap both LUNs from the secondary machine, map the *br-rhevm-bkup* destination LUN to the RHEV-M host machine.

Note: Only map one of the *br-rhevm** LUNs to the RHEV-M machine at a time. Mapping both at the same time may cause corruption on boot.

With the mappings complete, boot *br-rhevm* and verify functionality. **Figure D.3-1: RHEV-M Backup LUN Functionality** displays machine *br-rhevm* booted into the operating system with the RHEV-M Admin Portal open.

Enterprise Virtualization
Logged in user: Administrator | Sign out | Configure | About

Search: Host:

Bookmarks Tags Data Centers Clusters Hosts Storage Virtual Machines Pools Templates

New Edit Remove New Edit Remove Activate Maintenance Approve Power Management Assign tags

Name	Host/IP	Cluster	Status	Load
br-rhevh.cloud.lab.eng.b	10.16.143.172	RHEV-Backu	Up	0 VMs
br-rhevh2.cloud.lab.eng.	10.16.143.176	RHEV-Backu	Up	0 VMs

General Virtual Machines Network Interfaces

OS Version: RHEV Hypervisor - 5.6 - 10.2.el5_6
Kernel Version: 2.6.18 - 238.9.1.el5
KVM Version: 83 - 224.el5
VDSM Version: 2.2.63.25
SPICE Version: 0.3.0 - 54.el5_5.2

Active VMs: 0
KSM Feature: Inactive
Number of CPUs: 16
CPU Name: Intel Xeon Core i7
CPU Type: Intel(R) Xeon(R) CPU

Figure D.3-1: RHEV-M Backup LUN Functionality

Note: This same procedure can be used as a method to backup a RHEV Storage Domain. The RHEV environment needs to be brought into an off-line status with all virtual machines powered off and the Data Center hosts powered down so that access to the storage is limited to a single machine preventing possible data corruption.



In the event of a machine failure, it is possible to map the recovery boot-from-SAN LUN to another machine. There are some hardware considerations that need to be taken into account and may affect the ability to boot. It is recommended to utilize like hardware where the processor, network interface controllers and host bus adapters are of the same make and model²⁰. The risk associated with running RHEV-M on physical hardware can be alleviated through the use of virtualization. Kernel Virtual Machine, discussed in section **2.1 Kernel Virtual Machine**, provides an easy and cost effective method to host a RHEV-M instance.

D.4 Additional RHEV-M Backup and Recovery

Additional continuity options include:

- Logical Volume Management snapshots, in conjunction with KVM²¹
- High Availability through Red Hat Cluster Services²²
- Symantec Ghost²³
- Clonezilla
- SAN vendor LUN snapshot and replication between multiple datacenters
- Duplicity
- rsync
- Bacula



Appendix E: Contributors

The following contributors provided technical input, guidance and overall content review.

Contributor	Title	Contribution
Vinny Valdez, RHCA	Principle Software Engineer, Red Hat	Content, Review
Steve Reichard, RHCE	Principle Software Engineer, Red Hat	Content, Review
John Herr, RHCA	Sr. Software Engineer, Red Hat	Content

Table E-A: Contributors

Appendix F: References

- 1 <http://www.slideshare.net/CAinc/north-american-businesses-lose-265-billion-annually-from-avoidable-downtime-according-to-new-ca-technologies-study>
- 2 <http://www.soxlaw.com/>
- 3 <http://www.redhat.com/promo/qumranet/>
- 4 <http://www.symantec.com/business/netbackup>
- 5 <http://www.symantec.com/business/support/index?page=content&id=TECH136090>
- 6 <http://technet.microsoft.com/en-us/network/bb545423>
- 7 <http://www.symantec.com/business/support/index?page=content&id=TECH127083>
- 8 <http://www.symantec.com/business/support/index?page=content&id=TECH127084>
- 9 http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/DOCUMENTATION/3000/DOC3647/en_US/NetBackup_Install_UNIX.pdf
- 10 <http://www.symantec.com/business/support/index?page=content&id=TECH127081>
- 11 <http://www.symantec.com/business/support/index?page=content&id=TECH56473>
- 12 <http://www.symantec.com/business/support/index?page=content&id=TECH56473>

Appendix F: References

- 13 <http://www.symantec.com/business/support/index?page=content&id=TECH22365>
- 14 <http://www.symantec.com/connect/articles/whitepaper-veritas-netbackup-bare-metal-restore-symantec-best-breed-server-recovery-using-v>
- 15 <https://access.redhat.com/kb/docs/DOC-40846>
- 16 <http://www.symantec.com/connect/articles/how-backup-and-restore-microsoft-sql-server-backup-netbackup>
- 17 <http://www.symantec.com/business/support/index?page=content&id=TECH127055>
- 18 <http://social.msdn.microsoft.com/forums/en-US/sqldatabaseengine/thread/6d45e4a9-2c9b-451d-b7c2-1fa96c6cd03a>
- 19 http://www.symantec.com/business/resources/articles/article.jsp?aid=power_of_disk
- 20 <http://support.microsoft.com/kb/249694>
- 21 http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Logical_Volume_Manager_Administration/snapshot_volumes.html
- 22 <https://engage.redhat.com/forms/private-iaas-clouds-v2>
- 23 <http://www.symantec.com/themes/theme.jsp?themeid=ghost>