

Protecting Nutanix Environments with Quest Rapid Recovery

Rapid Recovery with Nutanix hosted Hypervisor solutions

Quest Technical Marketing

August 2017



© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

| | |
|---|-----------|
| Introduction | 6 |
| The Benefits of Protecting Nutanix using Rapid Recovery | 6 |
| Nutanix Architecture | 7 |
| Nutanix Deployment Options | 9 |
| VMware on Nutanix Features and Benefits | 9 |
| Rapid Recovery Protection Options | 10 |
| Agentless Protection | 10 |
| Agent Based Protection | 11 |
| This Tech Brief | 12 |
| Rapid Recovery Agentless Protection of Nutanix Hosted Virtual Machines | 14 |
| Example Configuration Details | 14 |
| Creating a Protection Policy: | 15 |
| Rapid Recovery Agent Protection of Nutanix Hosted Virtual Machines | 19 |
| Example Configuration Details | 19 |
| Creating a Protection Policy: | 20 |
| Rapid Recovery-Recovery of Nutanix Hosted Virtual Machines | 23 |
| Example Configuration Details | 23 |
| Virtual Machine Recovery - Virtual Export | 24 |
| Virtual Machine Recovery – Live Recovery | 26 |
| Rapid Recovery Protection of Nutanix provided Virtual Machines with a Clustered Applications | 30 |
| Example Configuration Details | 30 |
| Protecting the entire cluster: | 31 |

| | |
|--|-----------|
| Rapid Recovery Replication of Nutanix Hosted Virtual Machines | 33 |
| Example Configuration Details | 33 |
| Setting up Replication: | 34 |
| Appendix..... | 36 |

Executive Summary

As Information Technology professionals invest in providing Hypervisor hosted virtual machine applications, Quest customers know that Nutanix is able to host and scale VMs massively. However, by leveraging Quest Rapid Recovery backup and recovery software, critical Nutanix-hosted virtual machines can be protected from failure, and can be recovered in minutes in the event of a disaster. Rapid Recovery provides the ability to protect virtual machines from disasters, media failure and data corruption. It allows users to protect their entire hypervisor environment without the need for complex scripting or deep understanding of software internals.

This white paper examines how to protect Nutanix-hosted virtual machines using Rapid Recovery. Protection is a simple process that only takes moments. Once Rapid Recovery is configured, you can be rest assured that Nutanix provided virtual machines are securely and correctly protected.

Introduction

This document is intended to be an explanation of how to use Rapid Recovery to protect Nutanix environments.

Common terms:

- **Rapid Recovery core:** The primary Rapid Recovery component which coordinates and orchestrates backups. Rapid Recovery Core integrates with the VMware and Hyper-V API's, deduplicates, compresses and encrypts backups then sends them to a designated disk repository.
- **Dell XC Series appliance with Nutanix:** Appliance that provides enterprise compute and storage through the deployment of commodity computing servers (called nodes) which each run a standard hypervisor and the Nutanix Operating System (NOS). Each server contains x86-64 processors, memory, solid-state drives and traditional hard drives, and when added into a cluster, aggregates storage resources into a single storage pool. Both capacity and compute power is increased by adding a node to the Nutanix cluster.
- **Nutanix Controller Virtual Machine (CVM):** The Nutanix CVM runs the Nutanix software and serves all I/O operations for the hypervisor and VMs running on that host.

The Benefits of Protecting Nutanix using Rapid Recovery

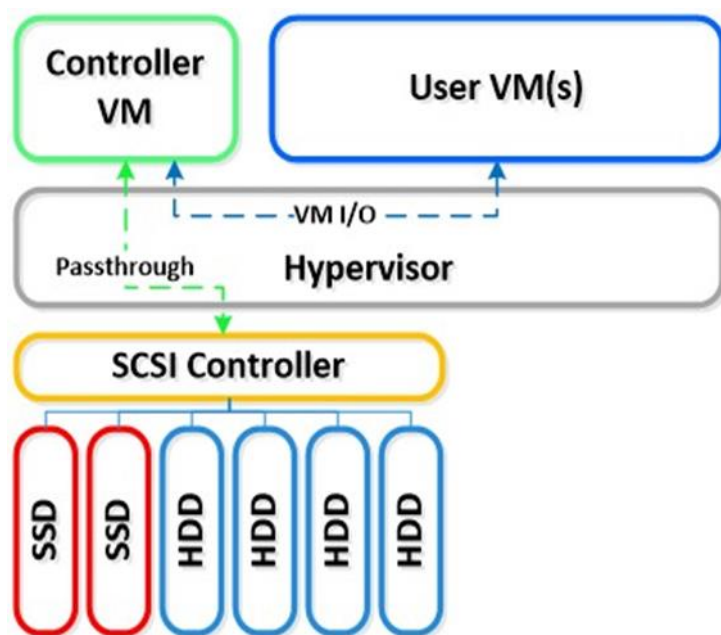
Data Protection is the process of safeguarding important information from corruption and/or loss. Rapid Recovery enables users to protect servers, applications and data by maintaining an up-to-date copy that can be accessed and recovered from at a moment's notice. For example, replicas can be stored on a virtualization hypervisor in standby mode for near immediate disaster recovery. Users only need to power on the remote virtual machine (VM) to bring up the last replicated state of the protected machine — there is no need for a long recovery process from a backup file.

Rapid Recovery agents protect and manage the backup and recovery of individual machines in a variety of environments. Each agent allows for block tracking, data volume grouping and the creation of application aware backups.

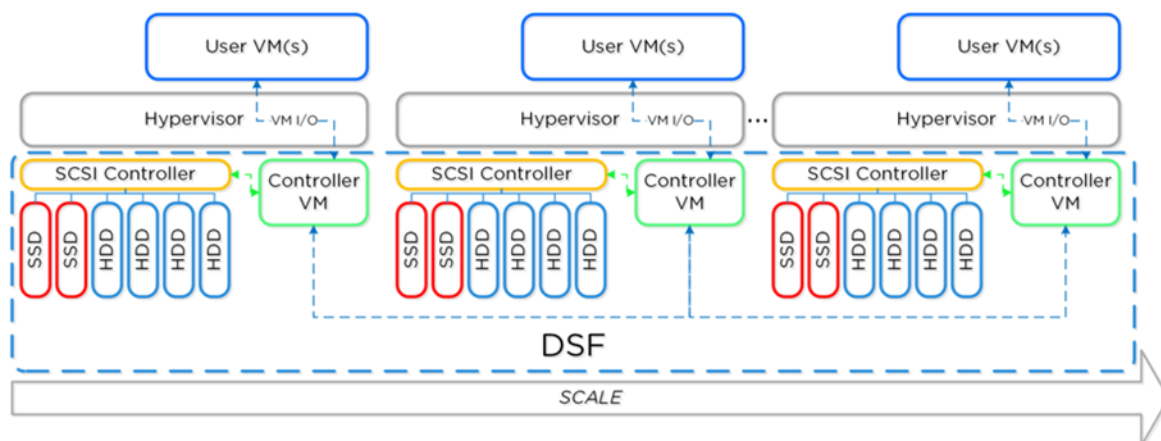
Rapid Recovery provides recoverability confidence with Microsoft Exchange, SQL Server and Power Point applications as recovery points are inspected using mountability and attachability testing along with Microsoft Virtual Shadow Copy Services (VSS) for consistency backup.

Nutanix Architecture

Nutanix converged infrastructure is a scale out cluster of high performance cluster nodes. Each node runs a standard hypervisor and contains processors, memory, and local storage consisting of high performance solid-state drives (SSD) and high capacity hard disk drives (HDD). Each node runs workloads in virtual machines on industry standard hypervisors like VMware ESXi, Microsoft Windows Hyper-V or Nutanix's own hypervisor Acropolis. Figure 1 provides a general overview of how Nutanix works.



In addition, local storage from all nodes is virtualized into a unified pool by the Nutanix Distributed Storage Fabric (DSF). In effect, DSF uses local SSDs and HDDs from all nodes to store virtual machine data. Virtual machines running on the cluster write data to DSF as if they were writing to shared storage. An NFS data store based on a Nutanix container is created for ESXi and Hyper-V hosts. The image below provides a general overview of how a Nutanix clustering works.



Nutanix Deployment Options

Nutanix is available in three versions. Each version appeals to different customer needs. For customers requiring proven Enterprise Hypervisor support, Nutanix nodes with VMware preinstalled are available. For customers that have an extensive Microsoft infrastructure investment and would like to continue using their preferred hypervisor of choice, Nutanix can provide nodes preinstalled with Hyper-V. Nutanix offers a native hypervisor called Acropolis at an attractive price point.

Note: Rapid Recovery does not support the interoperability with the Nutanix hypervisor called Acropolis, and any Rapid Recovery function that relies on Acropolis services will not function. Currently these features are: agentless protection and Export. The rest of the Rapid Recovery feature set such as file level recovery, Live Recovery, backup verification, VSS, replication, etc. will function when protecting Acropolis virtual machines while using an agent and a specific VirtIO driver provided by Nutanix. [KB192255](#). Acropolis examples will not be covered within this document.

In the sections below, specific features and benefits of each configuration are described in more detail.

VMware on Nutanix Features and Benefits

- **Native Support for all virtualization capabilities:** VMware includes support for Enterprise VMware features such as vMotion, High Availability (HA), Dynamic Resource Scheduling (DRS) and Fault Tolerance (FT).
- **VMware Integration:** Provides full integration of VMware snapshot and cloning capabilities by supporting both the VMware API for Array Integration (VAAI) and View Composer for Array Integration (VCAI) standards.
- **Converged Infrastructure:** Eliminates the cost and complexity of SAN and NAS-based storage.
- **Better than PC performance:** Leverages NOS features, including elastic-deduplication to eliminate IOPS bottlenecks resulting in fast application response and boot/login experience.
- **Eliminate project risk:** Enables users to start small and expand as needed, utilizing the latest advances in CPU, memory and flash.

- **Eliminate the need for dedicated infrastructure:** Provides each node with its own storage controller localizing application/database I/O and prevents requests from competing with other virtual machines running on different nodes.
- **Linear and seamless scale-out:** Enables customers to independently scale storage capacity and compute resources, and increases the number and size of application/database instances without expensive scale-up investments.
- **Resilient and high-performance infrastructure:** Provides pooled storage (HDD, SSD, and Flash) from all nodes in a cluster, while leveraging strong data protection and resiliency by replicating data across all nodes in a Nutanix cluster.

Rapid Recovery Protection Options

Rapid Recovery Protection is available in two general formats: Agentless and Agent based protection styles. Agentless protection functions by backing up and restoring VMware and Hyper-V hosted VMs without an agent being installed on the VM to be protected. This is accomplished by integrating into the hypervisor API and asking that it either provide a snapshot of a specific virtual machine to Rapid Recovery or to create (restore) a specific virtual machine that Rapid Recovery is providing. Because Rapid Recovery is interfacing with VMware or Hyper-V rather than a specific virtual machine, there is no need to deploy an agent. The benefit of this type of protection is that it scales quickly and does not require that virtual machines be rebooted when an agent is updated. Agent based protection of virtual machines also has its benefits as it offers important protection and restoration abilities such as Live Recovery, and application mountability and attachability checks.

Agentless Protection

Rapid Recovery's "Rapid Snap for Virtual" protects virtual machines on VMware ESXi & Hyper-V hosts without installing a Rapid Recovery Agent.

i **Note:** For Hyper-V virtual machine agentless protection, a Rapid Recovery agent is required to be installed on each Hyper-V host.

To protect a VM without the Rapid Recovery Agent, the Rapid Recovery Core works with the snapshot technology native to the hypervisor.

Rapid Recovery agentless protection uses an application program interface (API) to protect selected VMs without installing Rapid Recovery Agent software in them.



Note: Rapid Recovery recommends that VMware Tools be installed on virtual machines that will be protected on vSphere or ESXi hosts. It is also recommended that Hyper-V Integration Services be installed on protected Hyper-V VM's. When VMware Tools are installed on a VM using Windows operating systems, Rapid Recovery triggers Microsoft Volume Shadow Services (VSS) to create application consistent snapshots

Agentless protection use VMware Changed Block Tracking (CBT) native to the hypervisor to reduce the time needed for incremental snapshots.

There are multiple benefits to using agentless protection. Some of the most useful attributes include the following characteristics:

- Agentless protection allows automatic protection of new VMs.
- A restart is not required during the protection process.
- Credentials are not required for each individual VM.
- Powered down virtual machines are protected.
- Agentless protection lets you restore to disks.
- Agentless protection does not require free space on a volume during transfers.
- Support for all guest operating systems (that do not have a compatible Rapid Recovery agent).
- Export dynamic disks or volumes.

Agent Based Protection

To protect data using Rapid Recovery agents, users install an agent on the virtual machines to be protected. In the Rapid Recovery Core Console, using Protect Machine wizards, users can identify machines they would like to protect by performing the following.

- Protection of a single machine using the Protect Machine wizard, which connects to the machine using network hostname or IP address. Users can protect a network cluster using the Protect Cluster function, which connects to the cluster and its nodes using network hostname or IP address.
- Protection of multiple machines simultaneously using the Protect Multiple Machines wizard, which connects to the machines using Microsoft Active Directory, or to a vCenter or ESXi host; or you can specify the network hostname or IP addresses for a list of machines you enter manually.



NOTE: Quest recommends limiting the number of machines users protect simultaneously to 50 or fewer, to preclude experiencing resource constraints that may cause the protect operation to fail.

When identifying protection requirements for a single machine in the wizard, users can specify which volumes to protect. When using protect multiple machines, all volumes are protected by default. (This can be changed later on an individual machine basis).

Using advanced options, users can add additional security measures by specifying or applying an encryption key to backups for the machines they would like to protect.

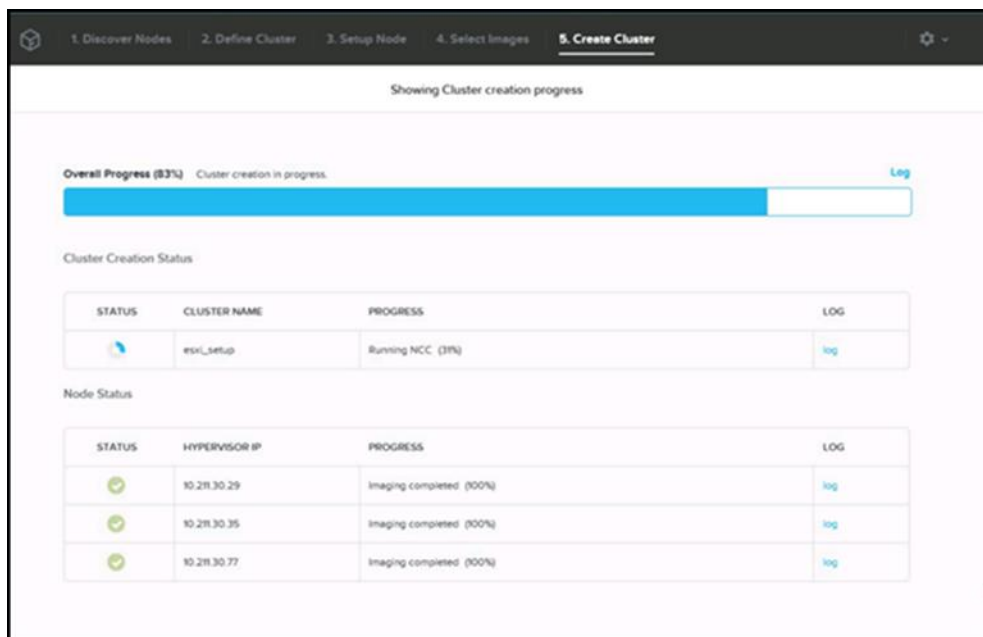
Agent based protection offer many benefits compared to agentless protection:

- Limited support for dynamic volumes (spanned, striped, mirrored and RAID) at the volume level. Please select the following link for more information.
- Live Recovery
- SQL attachability checking & log truncation
- Exchange mountability and checksum checking including log truncation.

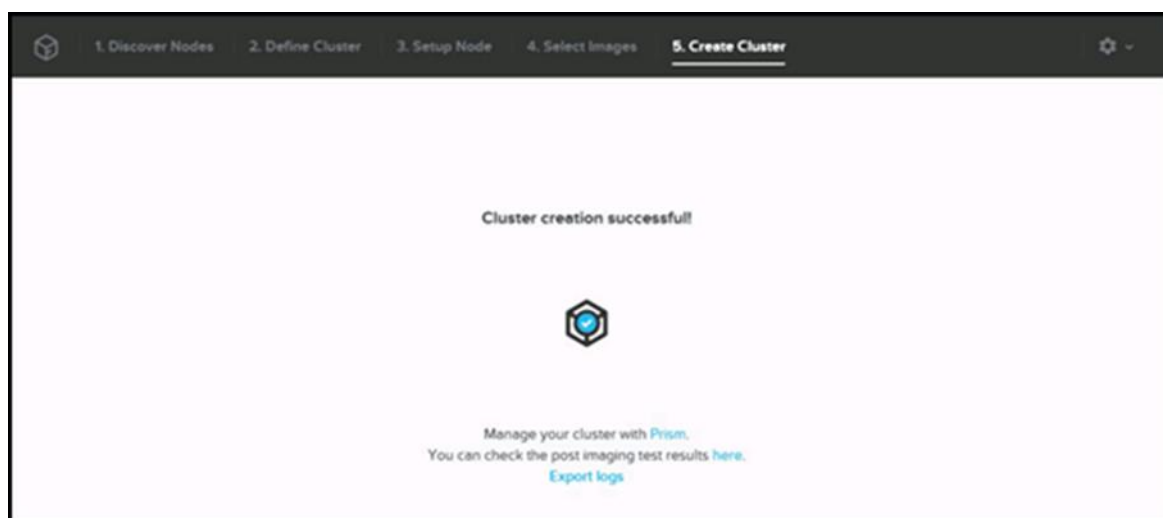
This Tech Brief

This tech brief provides step-by-step examples for using Rapid Recovery 6.1.2 to protect virtual machines running on a hypervisor hosted by Nutanix. Choice of hypervisor is defined by user needs. For simplicity, all examples in this document are run on VMware.

Nutanix nodes are expected to be run as a cluster. While the screenshots below provide a general overview of how to add new Nutanix nodes to a Nutanix cluster, please contact Support for more detailed instruction. (Usually clusters are defined by a professional services engineer on initial install.) Once all Nutanix nodes have been added to the Nutanix, customer administration is achieved through the hypervisor.



Nutanix cluster creation takes approximately 20 minutes for a three-node cluster.



A Nutanix cluster has been successfully created.

Rapid Recovery Agentless Protection of Nutanix Hosted Virtual Machines

This section describes how to use Rapid Recovery to backup Nutanix clusters running a VMware hypervisor agentlessly. If available (using a VMware hypervisor) most customers will agentlessly protect VMs. Reasons for this include ease of use (no need for agent management), and no need to reboot protected clients when installing an agent. Recall, agentless protection does not offer all of Rapid Recovery features such as Live Recovery and mountability/attachability integrity checking. Quest recommends that VMware tools be installed on every VMware virtual machine that is agentlessly protected.

Example Configuration Details

Table 1: Component table example

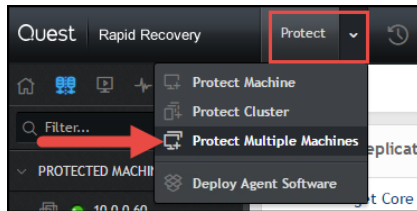
| Component | Description |
|--------------------------|--|
| Nutanix Operating System | NOS 4.6 (or greater) on a Dell XC Series appliance |
| Rapid Recovery version | 6.01 (or greater) running on its own hardware |
| ESXi version | 5.0.0 build 623860 (or greater) |

Test notes:

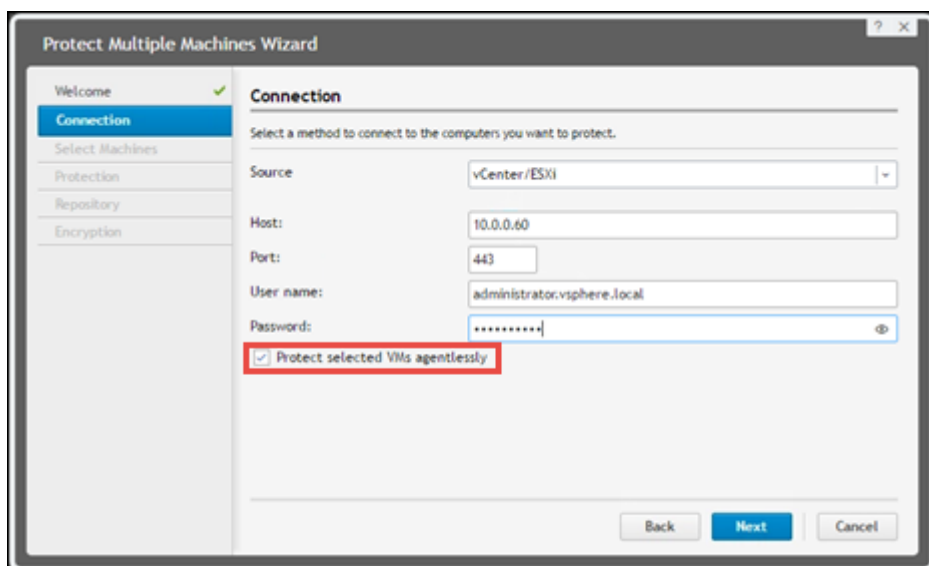
- ESXi 5.0.0 build 623860 (Running within Nutanix).
- VMware Tools installed on each VM to be protected.
- Rapid Recovery Core running on its own hardware.

Creating a Protection Policy:

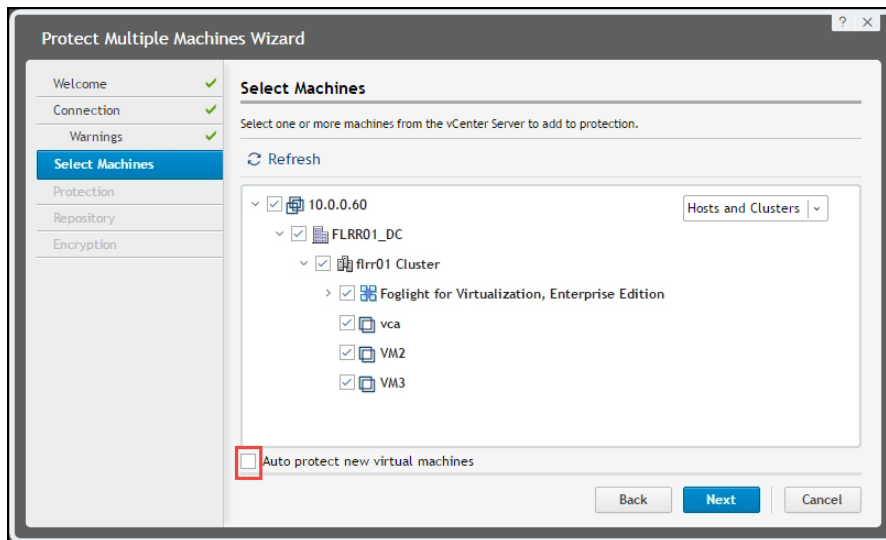
- 1 On the Rapid Recovery core console, click on the “Protect” pull down, then click “Protect Multiple Machines”.



- 2 In the Welcome screen, check “Advanced (show optional steps)”.
- 3 Click **Next**.
- 4 In the Connection window to the right of Source, select “vCenter/ESXi” (or Hyper-V).
- 5 Define the vCenter host IP address, Username and Password.
- 6 Ensure the ‘Protect selected VMs agentlessly’ checkbox is selected. Click **Next**.



- 7 In the Select Machines window, make sure the VMs you would like to backup are checked. If automatic Rapid Recovery protection is desired for all future newly created virtual machines, enable the check box ‘Auto protect new virtual machines.’ Click **Next**.



- 8 In the Protection window, choose the default protection schedule or choose Custom protection to define a new one. Click **Next**.
- 9 In the Repository window, define the repository where you would like the protection stored then click **Next**.
- 10 In the Encryption window, leave default (not encrypted) and click **Next**.
- 11 In the “Events” tab, monitor the job to confirm that it’s running successfully.

The following figure shows a three node Nutanix cluster displayed within the Rapid Recovery Core Protected Machine View. Rapid Recovery is running externally from a standalone server. Rapid Recovery protection is ongoing for all the server nodes. Each of the node has multiple VMs. Protection is agentless.

| Type | Status | Display Name | Last Snapshot | Next Snapshot | Repository Name | Recovery Points | Version | Actions |
|----------------------|--------|---------------------|-----------------------|----------------------|--------------------|-----------------|-----------|---------|
| 10.211.32.42 | | 10.211.32.42 | 3/31/2016 12:01:14 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 193 (86.43 GB) | 6.0.1.609 | |
| 10.211.34.145 | | 10.211.34.145 | | | | | (none) | |
| NG-source2 | | NG-source2 | 3/17/2016 10:40:18 AM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 1 (500 GB) | (none) | |
| NG-source4 | | NG-source4 | 3/31/2016 12:00:58 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 336 (500 GB) | (none) | |
| NG-source6 | | NG-source6 | 3/31/2016 12:01:43 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 333 (500 GB) | (none) | |
| NG-source7 | | NG-source7 | 3/31/2016 12:00:59 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 334 (500 GB) | (none) | |
| NTNX-GL7CC42-A-C... | | NTNX-GL7CC42-A-C... | Not yet performed | No schedule | Repository 2 (DVM) | 0 (0 bytes) | (none) | |
| 10.211.34.148 | | 10.211.34.148 | | | | | (none) | |
| NG-10.211.34.14... | | NG-10.211.34.148... | 3/31/2016 8:01:19 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 24 (30.01 GB) | (none) | |
| NG-source4_Replic... | | NG-source4_Replica | 3/31/2016 8:41:46 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 24 (11.72 TB) | (none) | |
| NG-source5 | | NG-source5 | 3/31/2016 8:02:25 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 167 (500 GB) | (none) | |
| NTNX-GL9CC42-A-C... | | NTNX-GL9CC42-A-C... | Not yet performed | No schedule | Repository 2 (DVM) | 0 (0 bytes) | (none) | |
| W_VM10 | | W_VM10 | 3/31/2016 8:01:54 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 167 (500 GB) | (none) | |
| W_VM16 | | W_VM16 | 3/31/2016 8:01:21 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 167 (500 GB) | (none) | |
| W_VM5 | | W_VM5 | 3/24/2016 8:02:59 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 146 (497 GB) | (none) | |
| W_VM6 | | W_VM6 | 3/31/2016 8:02:01 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 167 (500 GB) | (none) | |
| WVM_VM_1 | | WVM_VM_1 | 3/31/2016 8:02:01 AM | 3/31/2016 4:00:00 PM | Repository 2 (DVM) | 168 (500 GB) | (none) | |
| 10.211.34.152 | | 10.211.34.152 | | | | | (none) | |
| NG-vRanger install | | NG-vRanger install | 3/31/2016 12:02:56 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 337 (1.06 TB) | (none) | |
| NTNX-GLBFC42-A-C... | | NTNX-GLBFC42-A-C... | Not yet performed | No schedule | Repository 2 (DVM) | 0 (0 bytes) | (none) | |
| W_VM11 | | W_VM11 | 3/31/2016 12:00:41 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 325 (501.89 GB) | (none) | |
| W_VM14 | | W_VM14 | 3/31/2016 12:00:23 PM | 3/31/2016 1:00:00 PM | Repository 2 (DVM) | 331 (500 GB) | (none) | |
| W_VM15 | | W_VM15 | | | | | (none) | |

The following figure shows the Rapid Recovery summary screen from an individual virtual machine in the Nutanix VMware environment.

| Name | File System | Allocated Space | Schedule | Current Schedule | Next Snapshot |
|-----------------------|-------------|-----------------------|----------------------|------------------------------|---------------|
| V:\Hard disk 1\Vol... | NTFS | 500 GB used of 500 GB | Su Mo Tu We Th Fr Sa | 12:00 AM - 11:59 PM (60 min) | |



NOTE: When VMware virtual machines are protected agentlessly by Rapid Recovery, disk allocation is incorrectly reported due to a limitation between VMware and NFS datastores. (Figure 6 shows a Rapid Recovery allocation space warning with 100% allocation). The allocation warning message can be ignored and the 'Refresh Disk Information' command is not required to be run. For additional information regarding this issue, examine the following articles [KB192255](#), [KB195086](#).

Rapid Recovery Agent Protection of Nutanix Hosted Virtual Machines

This section describes how to use Rapid Recovery to protect Nutanix clusters with an agent. Agent based Rapid Recovery protection is supported in both VMware and Hyper-V. Reasons for installing an agent include the ability to provide Live Recovery, attachability and mountability checks and the ability to provide bare metal recovery (BMR) protection. For example, the use of a Rapid Recovery agent for the protection of a SQL server implemented within a virtual machine may be desirable because SQL attachability checks and log truncation are now possible which results in improved reliability and availability.

Although the Configuration Details example below outlines SQL protection only, Rapid Recovery agent supports all protection and recovery features for all supported applications when running on Nutanix.

Example Configuration Details

Table 2: Component table example

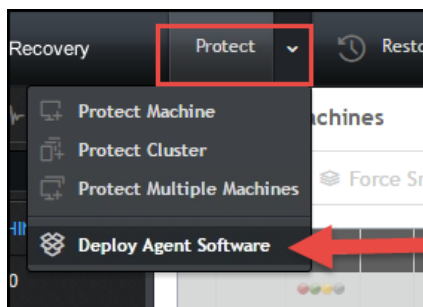
| Component | Description |
|--------------------------|---|
| Nutanix Operating system | NOS 4.6 (or greater) on a Dell XC Series appliance |
| Rapid Recovery version | 6.01 (or greater) running on its own hardware |
| ESXi version | 5.0.0 build 623860 (or greater) |
| Hyper-V version | Server 2008 SP, 2008 R2 SP1, 2012 R2, 2016 Windows 8, 8.1 with Hyper-V, Windows 10 |

Test Notes:

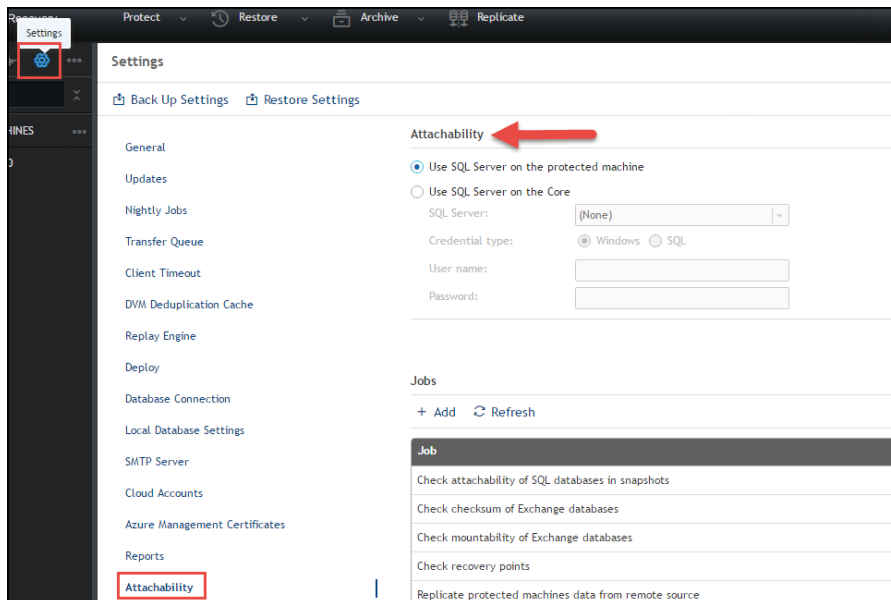
- Rapid Recovery supported SQL instance installed on a VM hosted by Nutanix (VMware or Hyper-V).
- Rapid Recovery agent installed on the system running SQL.
- Rapid Recovery Core running on its own hardware.

Creating a Protection Policy:

- 1 Deploy an Agent to one or more Windows or Linux Servers by selecting 'Deploy Agent Software Wizard' under the Rapid Recovery Core Console Protect menu. Select the following links for [Windows](#) and [Linux](#) agent installation details.




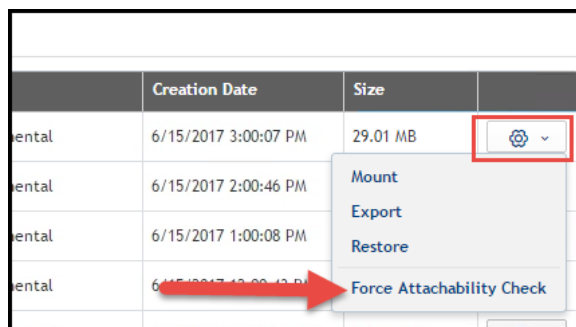
- 2 Now select the "Settings" tab, then click on "Attachability". This is where you define where the SQL attachability check will occur, and what SQL versions to use.



- 3 Nightly Rapid Recovery SQL Attachability jobs occur on the SQL server already installed on the protected machine, or on the Rapid Recovery Core machine (The instance of SQL Server installed on the Core

must be equal to or higher than the highest version of SQL being protected. It must also be licensed). If attachability jobs occur on the Core, select the appropriate SQL version and instance. For additional information about Rapid Recovery SQL attachability test settings and configuration, select the following [link](#) for additional information.)

- 4 Define the SQL administrator user name and password.
- 5 SQL attachability jobs occur nightly which tests the latest recovery point in SQL backup chain. To adjust the nightly job's scheduled time, select the 'Jobs' option within the 'Settings' tab of options.
- 6 Forcing a SQL attachability check.
 - a In the left navigation area of the Rapid Recovery Core Console, select the protected SQL Server machine for which you want to force the attachability check, and then click the Recovery Points menu.
 - b Scroll down to the Recovery Points pane.
 - c Navigate through the recovery points to find the desired recovery point. Optionally, click the ► arrow to the right of a recovery point in the list to expand the view.
 - d In the expanded recovery point information, you can see volumes included in the recovery point.
 - e In the Recovery Points pane, from the row representing the correct recovery point, click , and from the drop-down menu, select **Force Attachability Check**.



- f In the resulting dialog box, click to confirm that you want to force an attachability check.
- g The dialog box closes. The system performs the attachability check.

The following figure displays an Exchange server within a Nutanix environment, implemented within a VMware virtual machine. An agent is installed within the Exchange virtual machine so all recovery points are automatically checked using Recovery Points mountability checking.

For additional information on Rapid Recovery Exchange mountability checks, select the following [link](#).

Quest Rapid Recovery

Protect - Restore - Archive - Replicate

Running tasks: 1 - Help - 12:09 PM

10.211.32.42 Summary Recovery Points Events Settings Reports - More -

Filter...

PROTECTED MACHINES

- 10.211.32.42
- 10.211.34.145
- MG-source2
- MG-source4
- MG-source6
- MG-source7
- HTM1-GL9CCQ-A...
- 10.211.34.148
- MG-10.211.34.14...
- MG-source5
- HTM1-GL9CCQ-A...
- W_VW10
- W_VW16
- W_VW3
- W_VW6
- WV1_VM_1
- 10.211.34.152
- MG-vRanger Intel
- HTM1-GL9CCQ-A...
- W_VW11

Recovery Points Summary

Total Recovery Points: 191

Total Protected Data: 86.43 GB

Repository: Repository 2

Repository Status

67.87 GB used of 3.71 TB 2%

Recovery Points

Refresh Delete Range Delete All

| | Contents | Space Usage | File System | Type | Creation Date | Size | |
|--|-------------------------|------------------------|-------------|-------------|---------------|----------|--|
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 9.59 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.51 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.8 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.57 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 8.62 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.59 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 16.98 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.32 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 8.5 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.84 MB | |
| | (Volume Labeled Syst... | 64.9 GB used of 500 GB | NTFS | Incremental | | 7.88 MB | |

Rapid Recovery-Recovery of Nutanix Hosted Virtual Machines

This section describes how to use Rapid Recovery to recover protected virtual machines. While Rapid Recovery offers multiple methods to restore virtual machines, the most simple and quick method is a Virtual Export. Using the Rapid Recovery Virtual Export, both agent and agentless protected machines can be near instantly recovered to either Hyper-V or ESXi. Another method called Live Recovery, which requires an agent, allows for non-system Windows volume recovery in near-zero time.

The Rapid Recovery bare metal (BMR) restore process is another to recover protected virtual machines.

i **NOTE:** Nutanix Acropolis is not a supported hypervisor for virtual export (and is not covered in this document), but bare metal recovery should work for restore. [KB192256](#).

Example Configuration Details

Table 3: Component table example

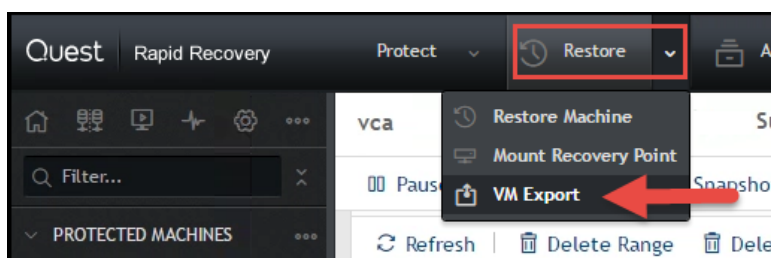
| Component | Description |
|--------------------------|---|
| Nutanix Operating system | NOS 4.6 (or greater) on a Dell XC Series appliance |
| Rapid Recovery version | 6.01 (or greater) running on its own hardware |
| ESXi version | 5.0.0 build 623860 (or greater) |
| Hyper-V version | Server 2008 SP, 2008 R2 SP1, 2012 R2, 2016 Windows 8, 8.1 with Hyper-V, Windows 10 |

Test Notes:

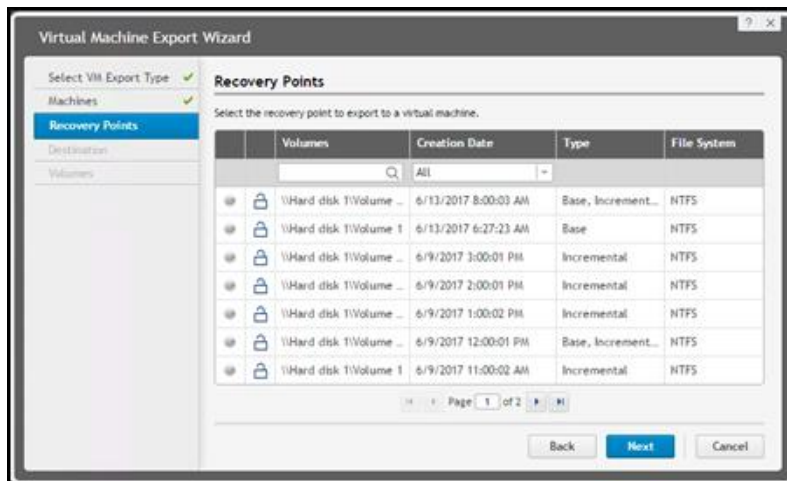
- Live Recovery - Rapid Recovery Agent required.
- Test will be performed on VMware.
- Rapid Recovery Core running on its own hardware.

Virtual Machine Recovery - Virtual Export

- 1 In the Rapid Recovery Core Console, within the button bar, click the Restore drop-down menu, and select VM Export.



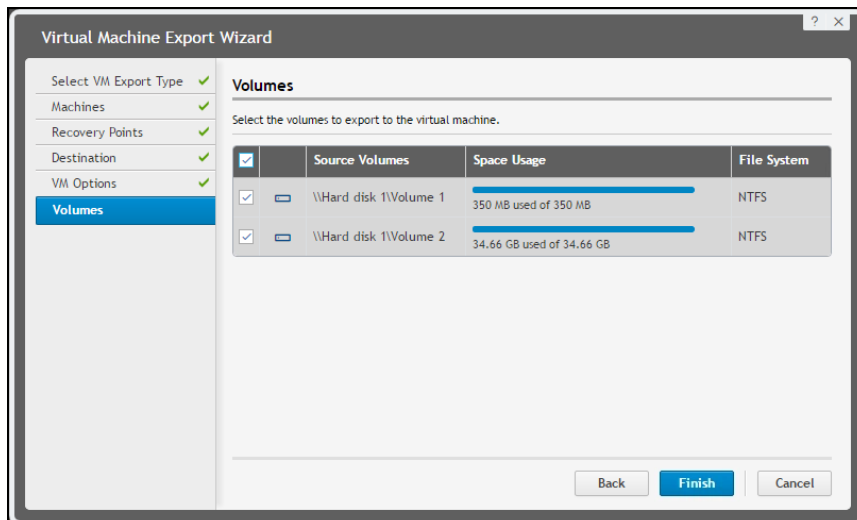
- 2 In the Virtual Machine Export Wizard, select One-time Export. Click **Next**.
 - For near immediate recovery of a protected virtual machine, Continuous (Virtual Standby) would be selected. Select the following [link](#) for additional Virtual Standby details.
- 3 On the Machines page, select the protected machine that you want to export. Click **Next**.
- 4 On the Recovery Points page, choose the desired recovery point for export. Click **Next**.



- 5 Within the Export to Virtual machine drop-down menu, select vCenter/ESXi (or Hyper-V).

- 6 Enter the required information to connect to the ESXi server. Click **Next**.
- 7 Within the Virtual Machine Options, enter the appropriate information needed to run the virtual machine export. Click **Next**.

- 8 Select the Volumes of the virtual machine to export. Click **Finish**.

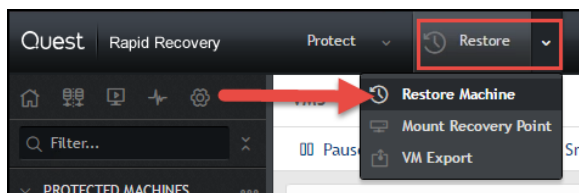


- 9 For additional information on the Rapid Recovery Export feature for Hyper-V and ESXi virtual machines, select the following [link](#).

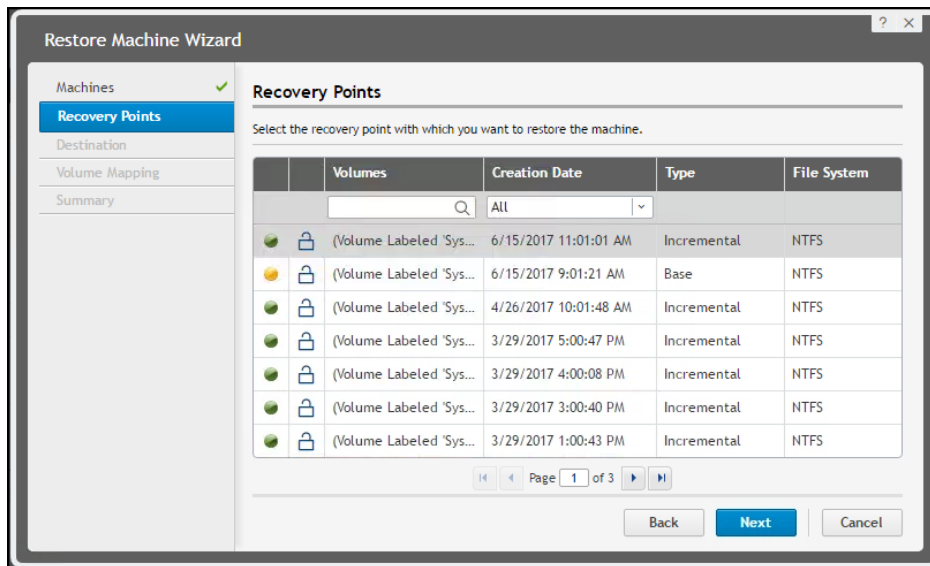
Virtual Machine Recovery – Live Recovery

Select the following [link](#) for additional Live Recovery details.

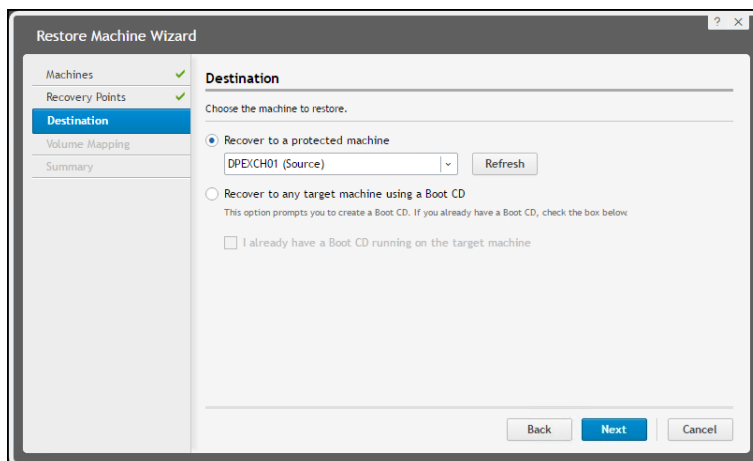
- 1 Volumes protected on a server without a Rapid Recovery agent cannot be recovered using Live Recovery. Ensure the data source you desire to be recovered has been protected by an agent. Additionally, an agent is required on the target server that you are recovering to. Only non-system Windows volumes can be recovered with Live Recovery.
- 2 Select the Restore option in the Rapid Recovery Core console button bar.



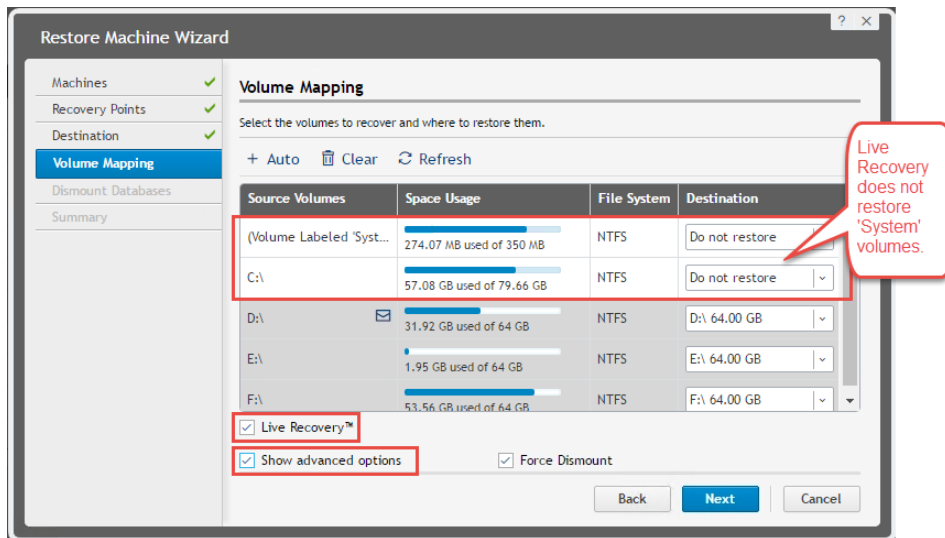
- 3 From the Protected Machines page, select the protected machine for which you want to restore data. Click **Next**.
- 4 From the list of recovery points, select the snapshot you want to restore to the agent machine. Click **Next**.



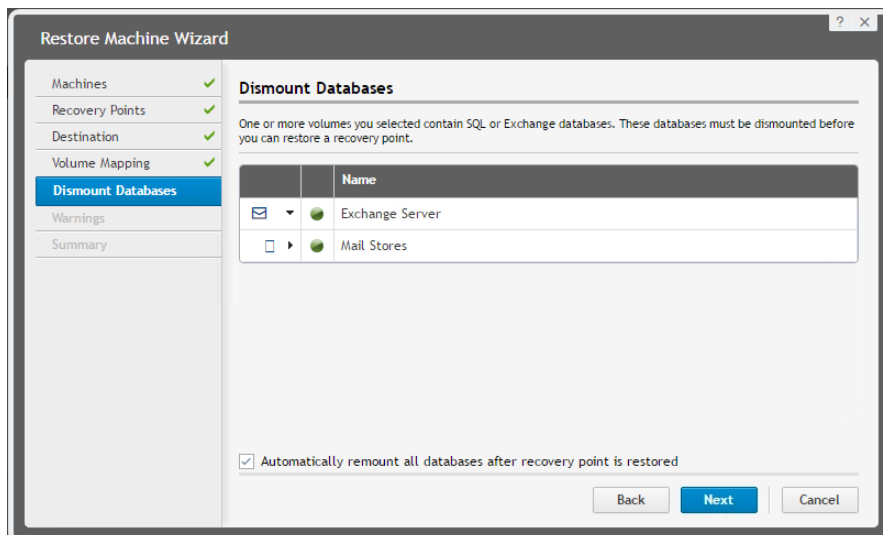
- 5 On the Destination page, choose the machine to which you want to restore data. (In the following image, data will be recovered to the original or source machine.) Click **Next**.



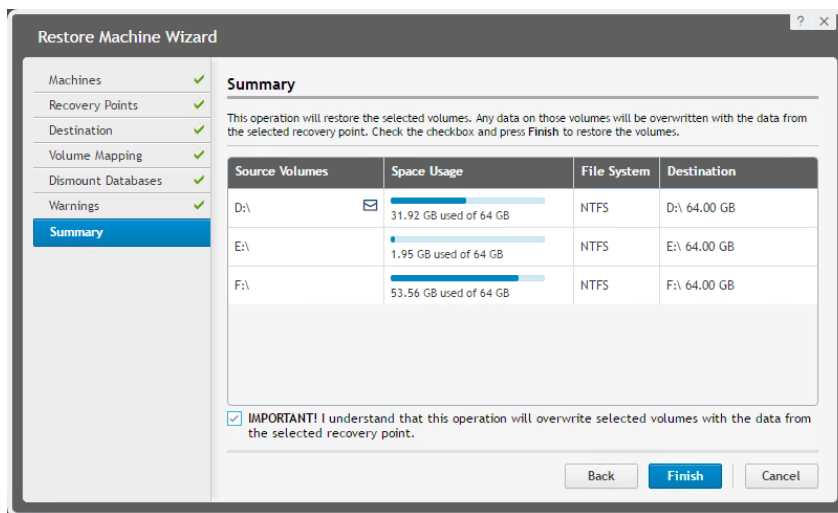
- 6 Within the Volume Mapping page, select the proper destination volume to restore data to.
- 7 Select Show advanced options and select the Live Recovery Checkbox. Click **Next**.



- 8 On the Dismount Databases page, if the volumes you want restored contain SQL or Microsoft Exchange databases, you are notified that the databases will be dismounted. Click **Next**.



- 9 The Warning page may appear and prompt you to close all programs on the volumes that you want to restore. If it does, click **Next** again.
- 10 On the summary page, select the **IMPORTANT!** option and click **Finish**.



Rapid Recovery Protection of Nutanix provided Virtual Machines with a Clustered Applications

Rapid Recovery protects clusters when each of the cluster node has Agent software installed. Rapid Recovery protects all cluster nodes as if they were one composite machine. Cluster protection requires an agent which also adds protection benefits such as, Live Recovery, attachability and mountability checks and the ability to provide BMR protection.

For Rapid Recovery cluster abilities and details, please select the following [link](#).

Example Configuration Details

Table 4: Component table example

| Component | Description |
|--------------------------|---|
| Nutanix Operating System | NOS 4.6 (or greater) Dell XC Series appliance |
| Rapid Recovery version | 6.01 (or greater) running on its own hardware |
| ESXi version | 5.0.0 build 623860 (or greater) |
| Hyper-V version | Server 2008 SP, 2008 R2 SP1, 2012 R2, 2016 Windows 8, 8.1 with Hyper-V, Windows 10 |

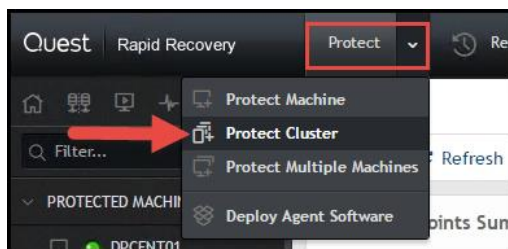
SQL Cluster Support:

Application Version / Cluster Configuration Windows Failover Cluster

- 2005 / 2008, 2008 R2
- 2008, 2008 R2 SCC / 2008, 2008 R2, 2012, 2012 R2
- 2012, 2014 SCC 2008 / 2008 R2, 2012, 2012 R2
- 2012, 2014 Availability Groups 2012, 2012 R2

Protecting the entire cluster:

- 1 In the Rapid Recovery Core Console, click the **Protect** button drop-down, then click **Protect Cluster**.



- 2 In window that pops up, define the IP address of the cluster, the cluster application or one of the cluster nodes.
- 3 Define the cluster application type.
- 4 Define the user name (domain_name\administrator).
- 5 Define the password.
- 6 Click **Connect**.
- 7 Select a repository for the cluster.
- 8 Optionally, select an encryption key.
- 9 If you do not want protection to begin immediately after completing this procedure, select **Initially pause protection**.
- 10 To protect the cluster based on default settings, select the nodes for default protection, and then go to Step 13.

i | **NOTE:** The default settings schedule a snapshot of all volumes every 60 minutes.

- 11 To enter custom settings for the cluster (for example, to customize the protection schedule for the shared volumes), do one of the following, and then see [Creating custom protection schedules](#).
 - To customize settings for an individual node, next to the node that you want to customize, click **Settings**, and then click **Function** next to the relevant volume.

- To customize settings for the cluster, click the Settings button at the bottom of the dialog box, and then click Function next to the relevant volume.

For more information about customizing nodes, click the following link.

12 When you have made all necessary changes, click **Save**.

13 In the **Protect Cluster** dialog box, click **Protect**.

Rapid Recovery Replication of Nutanix Hosted Virtual Machines

This section describes how to use Rapid Recovery to Replicate Nutanix hypervisor hosted virtual machine protected data from one Rapid Recovery Core to another. Replication is the process of copying recovery points from selected protected machines and transmitting them to a Rapid Recovery Core residing at another location for disaster recovery purposes. The replication configuration requires a paired source-target relationship between two or more Cores.

Example Configuration Details

Table 5: Component table example

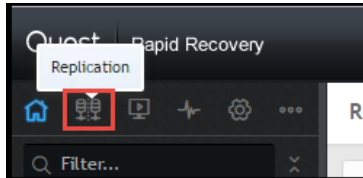
| Component | Description |
|--------------------------|---|
| Nutanix Operating System | NOS 4.6 (or greater) on a Dell XC Series appliance |
| Rapid Recovery | 6.01 (or greater) running on its own hardware |
| ESXi version | 5.0.0 build 623860 (or greater) |
| Hyper-V version | Server 2008 SP, 2008 R2 SP1, 2012 R2, 2016 Windows 8, 8.1 with Hyper-V, Windows 10) |

Test Notes:

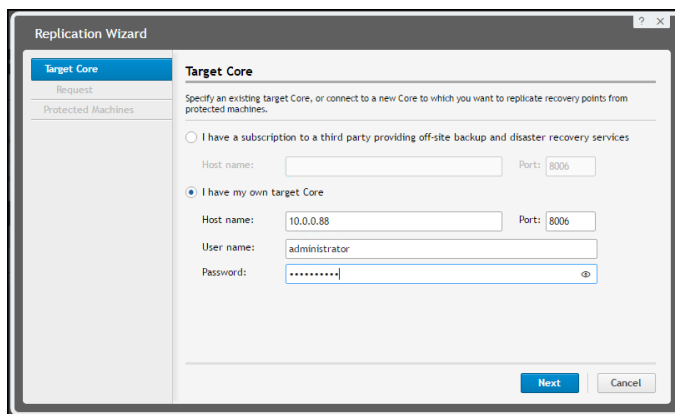
- Two Rapid Recovery Core running on its own hardware.
- Data/Protections defined in the local Rapid Recovery core server.

Setting up Replication:

- 1 Navigate to the Rapid Recovery Core console of the source Core.
- 2 On the button bar, click **Replicate**.



- 3 On the Outgoing Replication portion of the Replication screen, select Add Target Core if the target Core is not already listed. The Replication Wizard is launched.
- 4 In the Target Core portion of the Replication Wizard, select **I have my own remote Core** when your target Core is managed by you on your network.



- 5 Enter the IP address or host name of the remote Rapid Recovery core server and click **Next**.
- 6 Enter the User name and Password of the remote Rapid Recovery core server (servername/administrator). Click **Next**.
- 7 On the Requests Page, enter a name for this replication configuration. This name will be displayed for the Incoming Replication pane on the target Core's Replication page. Click **Next**.
- 8 On the Protected Machines page, select the protected machines to be replicated, then use the drop-down list in the Repository column to select a repository for each protected machine.
- 9 Click **Finish**.

For additional replication information including seeding, select the following [link](#).

Summary

Because Nutanix is built for flexible and scalable virtual environments that quickly adapt to daily IT demands, most backup and recovery offerings fall behind as they do not offer technologies that can adapt and change. Rapid Recovery successfully complements Nutanix environments as it has the flexibility, features and technologies to meet and exceed the most demanding SLA's, RPO and RTO's in an easy to manage and affordable solution. Additionally, Rapid Recovery includes unique testing of protected applications to ensure restorations are successful and reliable.

Rapid recovery brings a complete backup and recovery solution to Nutanix environments as virtual machine, application and data protection abilities are seamlessly applied and managed. From restoring entire virtual machines to granular recovery of applications or files, Rapid Recovery recovers Nutanix VMware and Hyper-V environments with near-zero RTO's further minimizing business interruptions.

Appendix

The following list of items offer additional information and depth to areas discussed in this paper.

- [Rapid Recovery Website](#)
- [Rapid Recovery System Requirements](#)
- [Rapid Recovery Sizing Guide](#)
- [The Nutanix Bible](#)
- [VMware and Nutanix](#)
- [Hyper-V and Nutanix](#)
- [Rapid Recovery – agent and agentless protection](#)
- [Protecting multiple machines on a VMware vCenter/ESXi virtual host](#)
- [Protecting multiple machines on a Hyper-V virtual host](#)
- [Virtual Machine Recovery – VM Export](#)
- [Virtual Machine Recovery – Live Recovery](#)
- [Restoring Data from Recovery Points](#)
- [Rapid Recovery Server Cluster Protection](#)
- [Rapid Recovery Replication](#)