White paper

EMC VIPR SRM: VAPP BACKUP AND RESTORE USING VMWARE VSPHERE® DATA PROTECTION™ ADVANCED

Abstract

This white paper provides a working example of how to back up and restore an EMC ViPR SRM vApp using VMware vSphere Data Protection Advanced 5.8.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit www.emc.com, or explore and compare products in the EMC Store

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.
For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

VMware and are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number H14603

Table of Contents

Executive summary

There are many ways to perform backup and many applications to do so. This document provides general guidelines on how to perform backup for your existing EMC ViPR SRM deployment.

Generally, you do not want files to be changed while being backed up. Configuration files are not modified while EMC ViPR SRM is running, as they are loaded in RAM. However, the databases, log files and temporary files are constantly modified.

You will find below some indications on how to avoid these issues. Most importantly, you should periodically test data restoration to make sure backup works better and prepare yourself when a disaster really occurs and you need to recover data quickly.

About EMC ViPR SRM

EMC ViPR SRM leverages state-of-the-art visibility and forecasting from various devices and technologies processing and storing millions of indicators. When designing an EMC ViPR SRM solution it should be taken into consideration how to avoid common availability pitfalls and in the case of a failure how to gracefully reestablish the services to maintain consistency and performance. This white paper is applicable to all current versions of ViPR SRM.

Audience

This white paper is intended for anyone (e.g. system and storage administrators), system implementers (e.g. solution architects), support, and EMC partners interested in knowing the current recommended guidelines for backup and recovery solutions.

Terminology

Term	Definition
Backup Policy	The methods, procedures, policies and rules that are used as guidelines to safeguard data. Typically involves detailed information on how a backup should proceed, what systems should the data be saved to, schedule for a backup window and to what sort of media and destination a backup should be delivered.
Backup Window	The time period required to finish a backup process.
Recovery Point Objective	Recovery Point Objective (RPO) is the maximum amount of data that an organization can tolerate to lose.
Recovery Time Objective	After a service disruption, the Recovery Time Objective (RTO) is the maximum period of time a business or process can endure for restoring data accesses.
Snapshots	A snapshot is the state of a system in a specific point in time. In a virtual environment, this could mean the state and data of a virtual machine, including the files that make the virtual machine disk and information about the state of the virtual machine (i.e.: powered off or powered on).

Data protection strategies

Backup and restore strategy

Your backup and restore strategy should take into account your organization's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in order to comply with expected Service Level Agreements (SLA) and other regulatory components. Often, the lack of clear guidelines on a SLA contract will drive a backup and restore policy into a costly upward spiral. Understanding your RTO and RPO are key to avoiding this situation.

Assumptions

The methods and strategies described in this white paper are accompanied by some basic assumptions. Results may vary if these same conditions are not in effect in the customer's environment.

- Backup and restore should only be done using the same version of EMC ViPR SRM. Mixing versions can lead to unknown results.
- These guidelines adhere to the *EMC ViPR SRM Support Matrix*.
- Specific components leveraged in this solution may require additional licensing to enable and use the full feature set of capabilities necessary for the multi-tiered data protection strategy outlined in this document.

Additionally, the implementation and test procedures outlined in this document do not give exact instructions for each step. It is assumed that the audience is familiar enough with the tools and interfaces of the different products in this solution to perform them without explicit guidance.

Case Study – Using VMware vSphere® Data Protection™ Advanced

For this example, we will examine VMware vSphere Data Protection Advanced (VDPA) and how it leverages a robust, easy to use and scalable option when it comes to backup and restore. VMware makes it available one virtual appliance, the VMware vSphere Data Protection (VDP) appliance, free of charge. When more advanced requirements are needed, a license can be acquire and deployed to the VDP appliance, upgrading it to a fully workable VDPA instance, unlocking many advanced features such as the integration with EMC Data Domain and EMC Avamar.

VDP and VDPA both make use of a key technology known as Changed Block Tracking (CBT). CBT allows the appliance to only backup or restore the blocks that were changed since the last backup operation, being very effective on the network resources.

For more information on the feature-set and differences between VMware vSphere Data Protection and VMware vSphere Data Protection Advanced please visit:

http://www.vmware.com/products/vsphere-data-protection-advanced

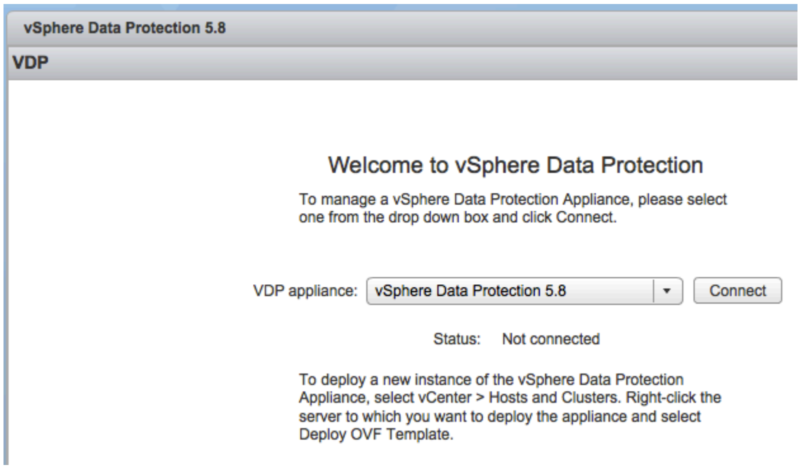
Now that we know what VDPA provides, let's see an example on how to setup the Backup and Restore task. The procedural details on how to setup and license VDPA are beyond the scope of this white paper. For more information on how to do the initial setup please refer to the *vSphere Data Protection Administration Guide* found at http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vmware-data-protection-administration-guide-580.pdf

Solution	Storage Type	Backup	vCenter Snapshot	Backup	Restore
VDPA	LVM + Additional Disk	Hot	Yes	Ok	Ok
VDPA	LVM + Additional Disk	Hot	No	Ok	Ok
VDPA	LVM	Hot	No	Ok	Ok
VPDA	LVM	Hot	Yes	Ok	Ok
VPDA	LVM + Additional Disk	Cold	Yes	Ok	Ok
VPDA	LVM + Additional Disk	Cold	No	Ok	Ok
VPDA	LVM	Cold	Yes	Ok	Ok
VDPA	LVM	Cold	No	Ok	Ok

Backup

Before you start, make sure that none of you vSphere objects (i.e.: virtual machines, cluster names, datastore, folders, etc.) have any special characters such as %, &, *, $, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ' on their name or the backup will fail. For more information on this topic please refer to the VMware KB: *Backup job fails for all virtual machines after VMware vSphere Data Protection 5.x deployment (2038597)* at http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2038597&sliceId=1&docTypeID=DT_KB_1_1&dialogID=483824194&stateId=1%200%20483826604

1. On the vCenter home display navigate to the vSphere Data Protection Advanced by clicking on its icon found on the left side menu.
2. Connect to the VDPA by clicking **Connect**.



vSphere Data Protection 5.8

VDP

Welcome to vSphere Data Protection

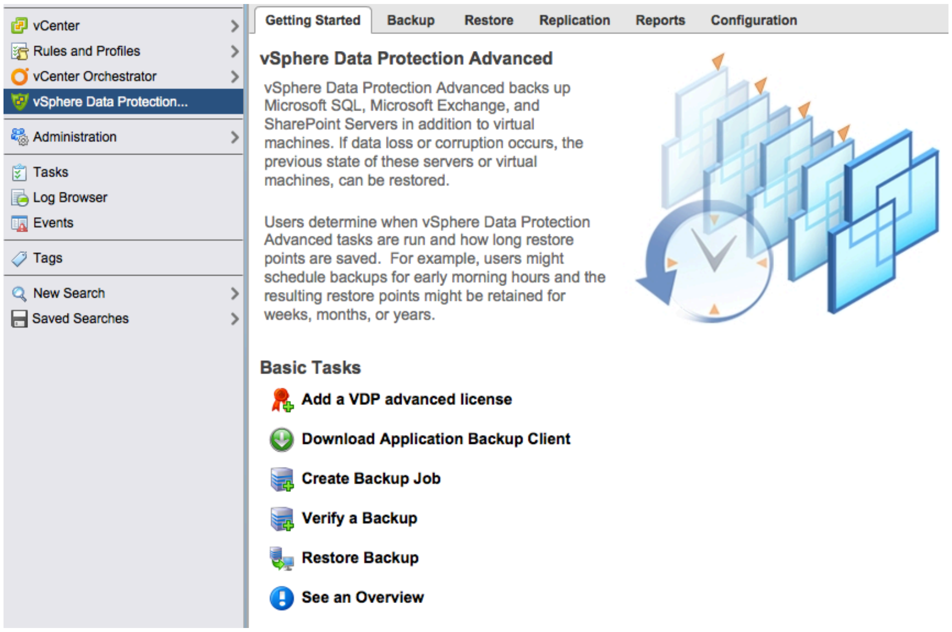
To manage a vSphere Data Protection Appliance, please select one from the drop down box and click Connect.

VDP appliance: vSphere Data Protection 5.8 ▾ Connect

Status: Not connected

To deploy a new instance of the vSphere Data Protection Appliance, select vCenter > Hosts and Clusters. Right-click the server to which you want to deploy the appliance and select Deploy OVF Template.

3. On the Getting Started tab click **Create Backup Job.**



vSphere Data Protection Advanced

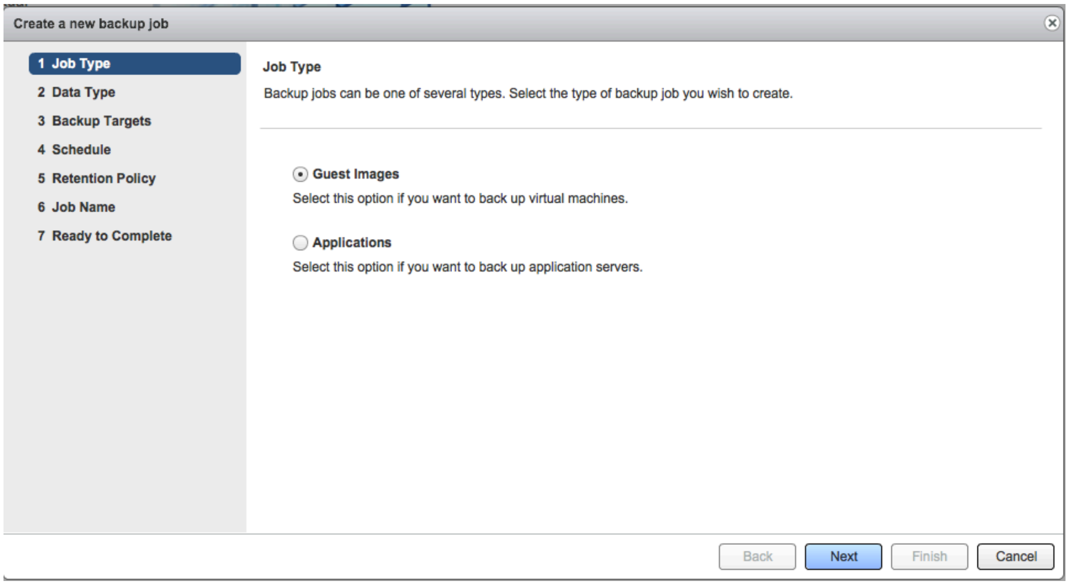
vSphere Data Protection Advanced backs up Microsoft SQL, Microsoft Exchange, and SharePoint Servers in addition to virtual machines. If data loss or corruption occurs, the previous state of these servers or virtual machines, can be restored.

Users determine when vSphere Data Protection Advanced tasks are run and how long restore points are saved. For example, users might schedule backups for early morning hours and the resulting restore points might be retained for weeks, months, or years.

Basic Tasks

- Add a VDP advanced license
- Download Application Backup Client
- Create Backup Job
- Verify a Backup
- Restore Backup
- See an Overview

4. Choose **Guest Images** and click **Next.**



Create a new backup job

Job Type

Backup jobs can be one of several types. Select the type of backup job you wish to create.

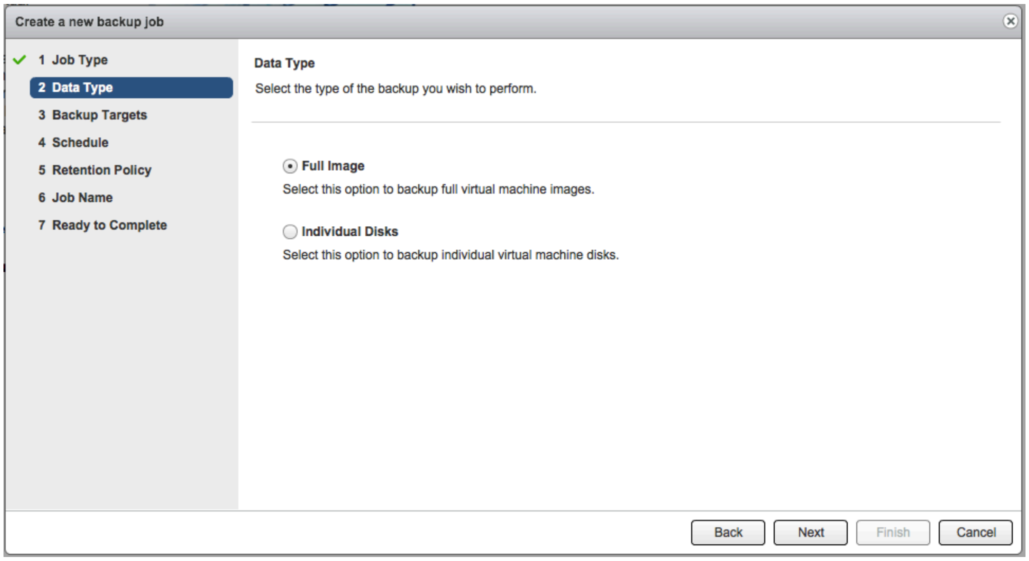
● Guest Images

Select this option if you want to back up virtual machines.

○ Applications

Select this option if you want to back up application servers.

5. Under Data Type you can choose either to backup the full image or individual disks. In this example we will choose to back up the full image of the virtual machines. Select that option and click **Next**.



Create a new backup job

Data Type

Select the type of the backup you wish to perform.

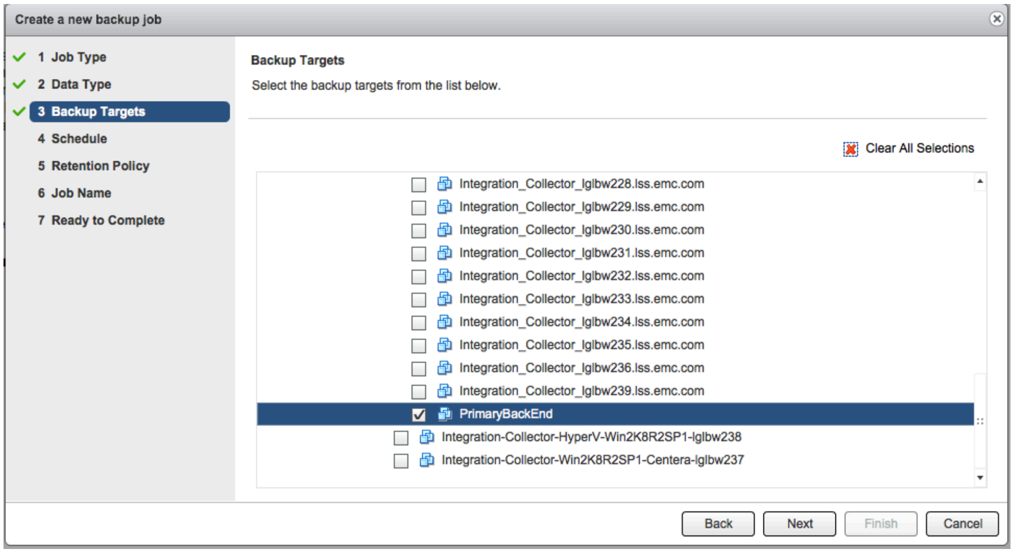
● Full Image

Select this option to backup full virtual machine images.

○ Individual Disks

Select this option to backup individual virtual machine disks.

6. Select the backup targets. This is where you will specify the virtual machine that needs to be backed up. It is possible to choose more than one virtual machine or even an entire cluster. Please be aware that by choosing an entire cluster or many virtual machines at once one can put extra burden on the system. As an example we will choose the primary backend virtual machine.



Create a new backup job

- ✓ 1 Job Type
- ✓ 2 Data Type
- ✓ 3 Backup Targets
- 4 Schedule
- 5 Retention Policy
- 6 Job Name
- 7 Ready to Complete

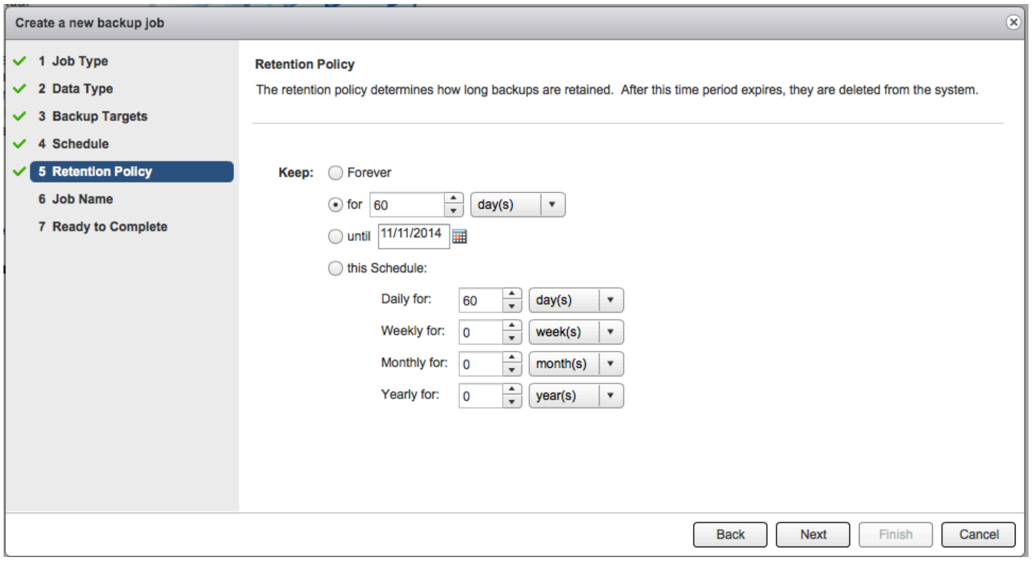
Backup Targets

Select the backup targets from the list below.

☒ Clear All Selections

- □ Integration_Collector_lglbw228.lss.emc.com
- □ Integration_Collector_lglbw229.lss.emc.com
- □ Integration_Collector_lglbw230.lss.emc.com
- □ Integration_Collector_lglbw231.lss.emc.com
- □ Integration_Collector_lglbw232.lss.emc.com
- □ Integration_Collector_lglbw233.lss.emc.com
- □ Integration_Collector_lglbw234.lss.emc.com
- □ Integration_Collector_lglbw235.lss.emc.com
- □ Integration_Collector_lglbw236.lss.emc.com
- □ Integration_Collector_lglbw239.lss.emc.com
- ☑ PrimaryBackEnd
- □ Integration-Collector-HyperV-Win2K8R2SP1-lglbw238
- □ Integration-Collector-Win2K8R2SP1-Centera-lglbw237

7. Set up a backup schedule followed by when to start the backup.



Create a new backup job

- ✓ 1 Job Type
- ✓ 2 Data Type
- ✓ 3 Backup Targets
- ✓ 4 Schedule
- ✓ 5 Retention Policy
- 6 Job Name
- 7 Ready to Complete

Retention Policy

The retention policy determines how long backups are retained. After this time period expires, they are deleted from the system.

Keep: ○ Forever

● for 60 day(s)

○ until 11/11/2014

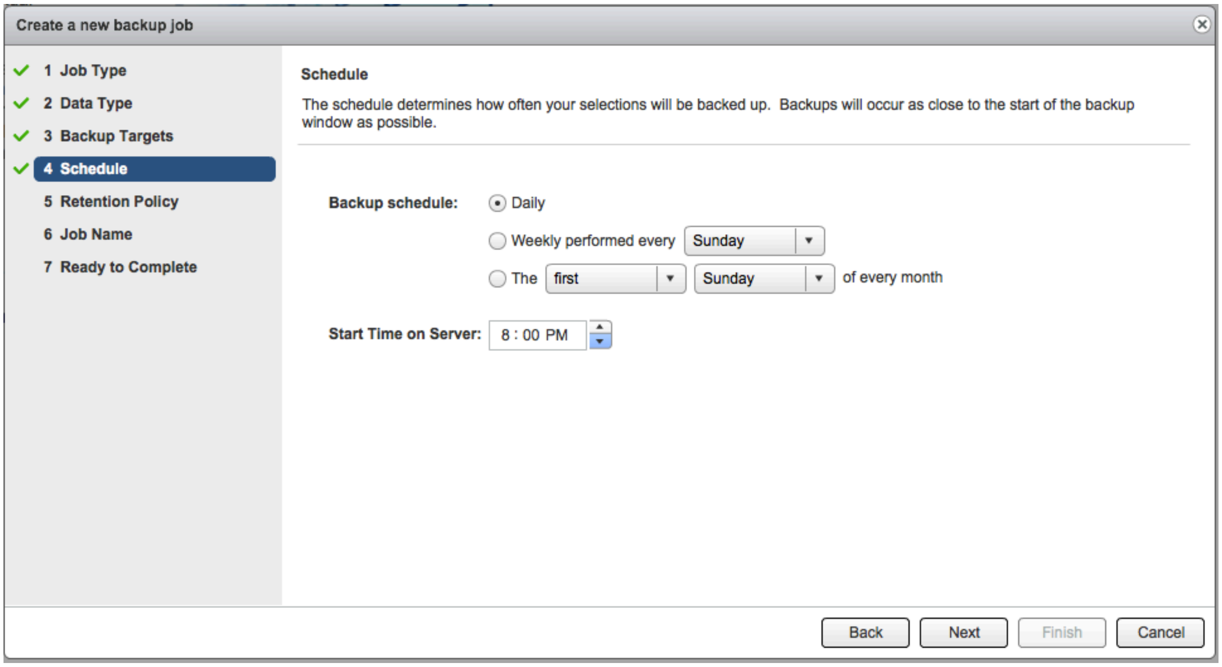
○ this Schedule:

Daily for: 60 day(s)

Weekly for: 0 week(s)

Monthly for: 0 month(s)

Yearly for: 0 year(s)



Schedule

The schedule determines how often your selections will be backed up. Backups will occur as close to the start of the backup window as possible.

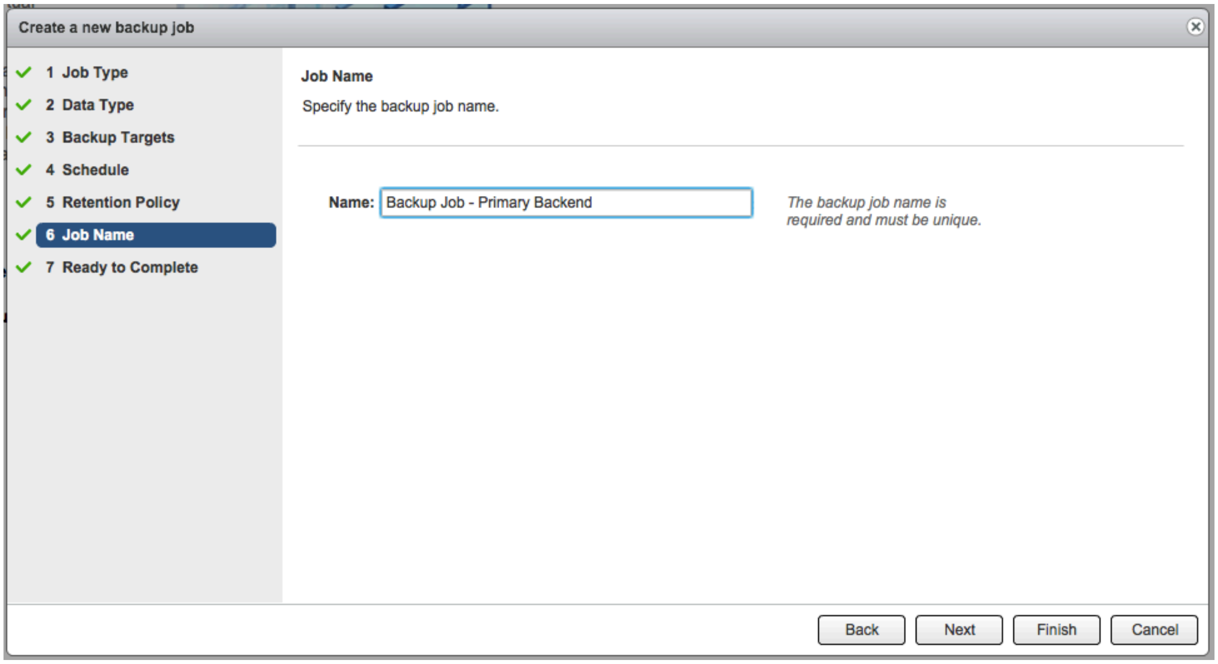
Backup schedule: ● Daily

○ Weekly performed every Sunday

○ The first Sunday of every month

Start Time on Server: 8 : 00 PM

8. Define a retention policy choosing for how long backups should be retained. We will leave the default option of 60 days. Lastly name the specific backup job and click **Finish**.



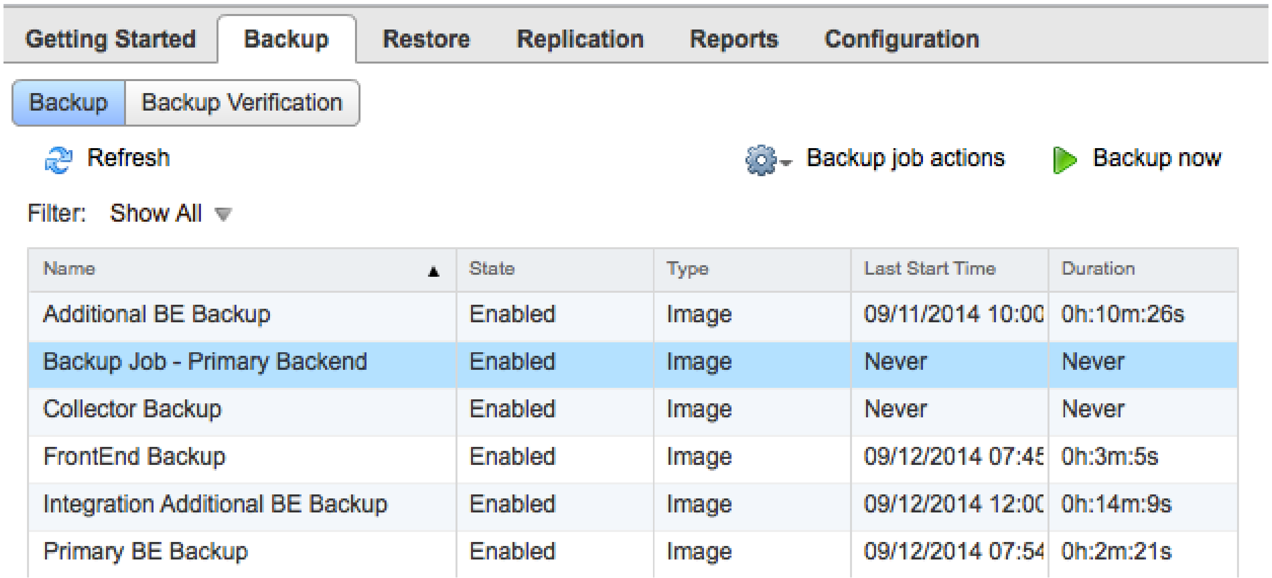
Job Name

Specify the backup job name.

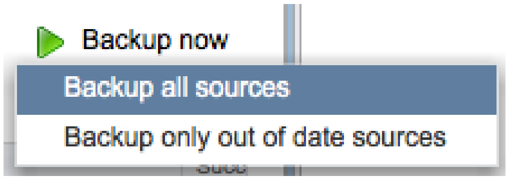
Name: Backup Job - Primary Backend

The backup job name is required and must be unique.

1. Returning to the appliance main window, click on the **Backup** tab to verify all of the currently available backup jobs. Here you can see at a glance all of the information available for the current jobs, including the last time it was executed and how long it took for the job finish.



Name	State	Type	Last Start Time	Duration
Additional BE Backup	Enabled	Image	09/11/2014 10:00	0h:10m:26s
Backup Job - Primary Backend	Enabled	Image	Never	Never
Collector Backup	Enabled	Image	Never	Never
FrontEnd Backup	Enabled	Image	09/12/2014 07:45	0h:3m:5s
Integration Additional BE Backup	Enabled	Image	09/12/2014 12:00	0h:14m:9s
Primary BE Backup	Enabled	Image	09/12/2014 07:54	0h:2m:21s

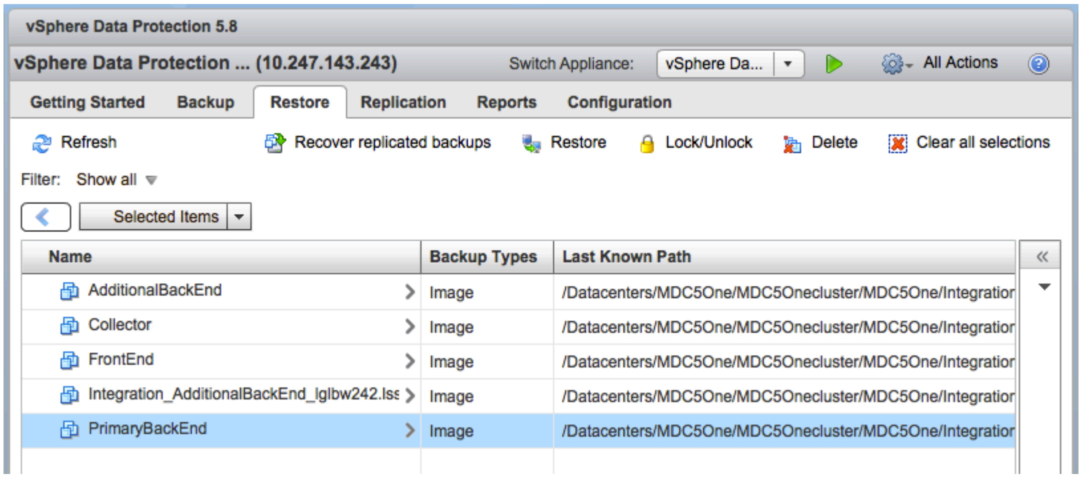


2. With all of the settings in place we can now run the backup by clicking on **Backup now** than choosing **Backup all sources**.

The VDPA will create a snapshot of the virtual machine vmdk while the backup procedure is running. After the backup is completed the VDPA will go ahead and delete this snapshot, committing any changes made to the snapshot back to the original vmdk. From this point on whenever a backup happens for this specific backup job, only the blocks that were changed will be sent to the backup destination. This is known as the Changed Block Tracking technology and when it's implemented it will save network resources as well as disk space on the backup destination. VDPA has also a very tight integration with Data Domain, leveraging technology such as de-duplication and compression.

Restore

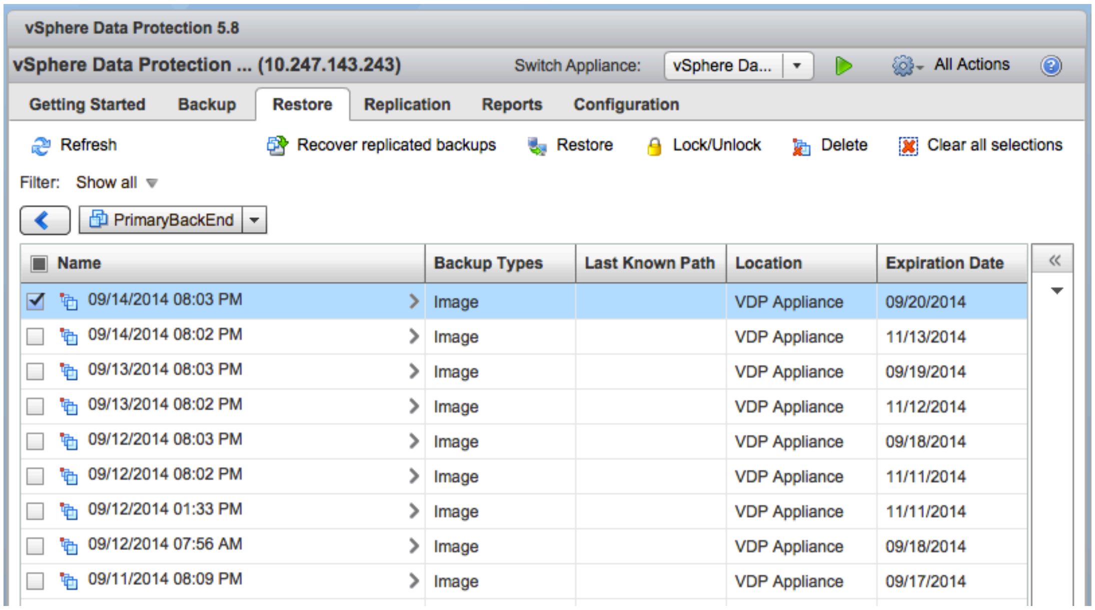
1. Navigate to the **Restore** tab and then choose instance that you wish to restore from the window containing the list of available images.



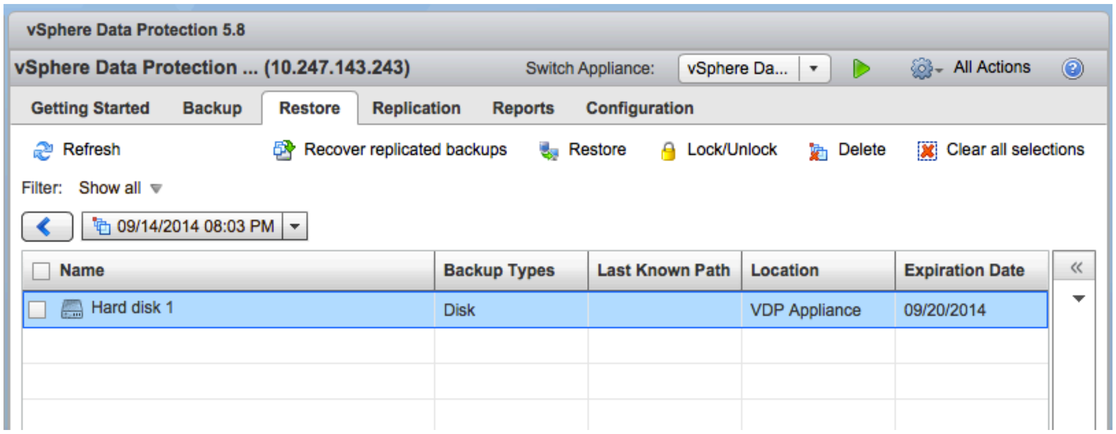
Name	Backup Types	Last Known Path
AdditionalBackEnd	Image	/Datacenters/MDC5One/MDC5Onecluster/MDC5One/Integratior
Collector	Image	/Datacenters/MDC5One/MDC5Onecluster/MDC5One/Integratior
FrontEnd	Image	/Datacenters/MDC5One/MDC5Onecluster/MDC5One/Integratior
Integration_AdditionalBackEnd_lglbw242.lss	Image	/Datacenters/MDC5One/MDC5Onecluster/MDC5One/Integratior
PrimaryBackEnd	Image	/Datacenters/MDC5One/MDC5Onecluster/MDC5One/Integratior

2. In this example we will select the Primary Backend by clicking on its name. A window containing all of the backup images displays.

3. Choose from one of the available options by clicking on the checkbox on the left side. Optionally you could also restore individual virtual hard drives.

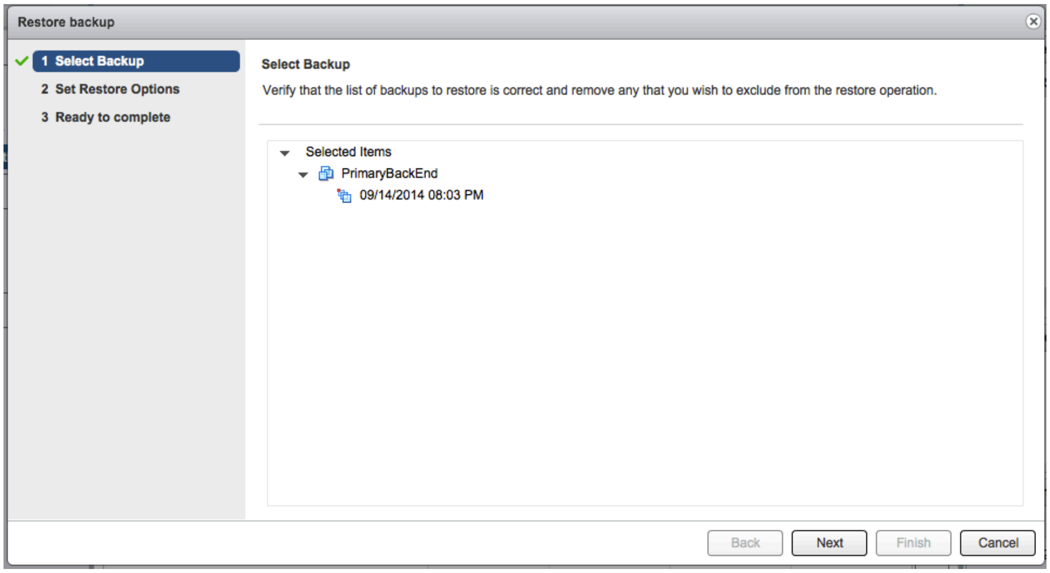


Name	Backup Types	Last Known Path	Location	Expiration Date
☑ 09/14/2014 08:03 PM	Image		VDP Appliance	09/20/2014
□ 09/14/2014 08:02 PM	Image		VDP Appliance	11/13/2014
□ 09/13/2014 08:03 PM	Image		VDP Appliance	09/19/2014
□ 09/13/2014 08:02 PM	Image		VDP Appliance	11/12/2014
□ 09/12/2014 08:03 PM	Image		VDP Appliance	09/18/2014
□ 09/12/2014 08:02 PM	Image		VDP Appliance	11/11/2014
□ 09/12/2014 01:33 PM	Image		VDP Appliance	11/11/2014
□ 09/12/2014 07:56 AM	Image		VDP Appliance	09/18/2014
□ 09/11/2014 08:09 PM	Image		VDP Appliance	09/17/2014



Name	Backup Types	Last Known Path	Location	Expiration Date
Hard disk 1	Disk		VDP Appliance	09/20/2014

4. Click **Restore.**

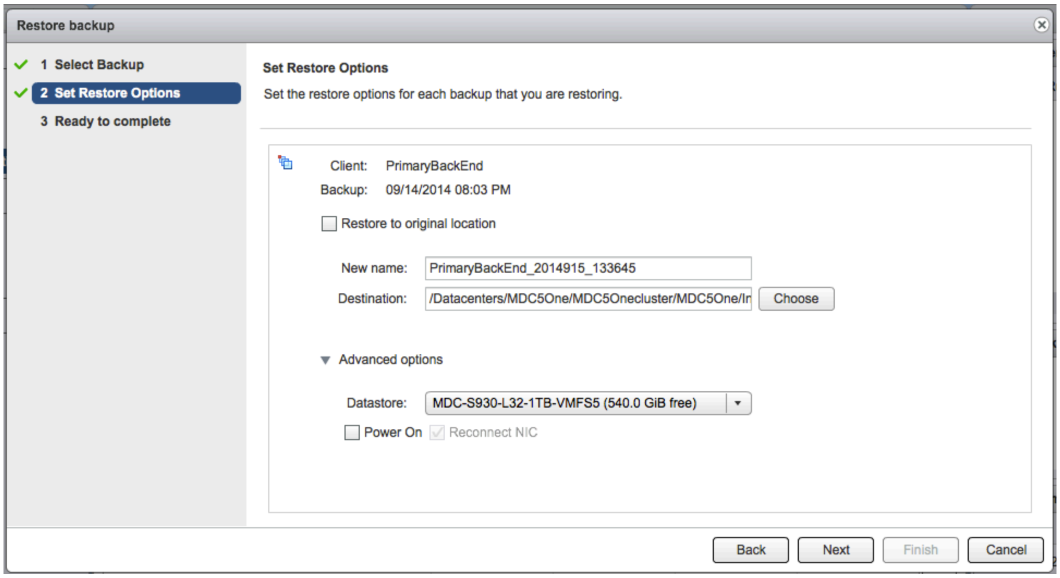


Select Backup

Verify that the list of backups to restore is correct and remove any that you wish to exclude from the restore operation.

- Selected Items
  - PrimaryBackEnd
    - 09/14/2014 08:03 PM

5. Under **Set Restore Options** you will be prompted to choose whether or not you want to restore to original location or into a new destination. Other advanced options enable you to pick a different datastore for the restore or if the virtual machine will be powered on.



Restore backup

✓ 1 Select Backup
✓ 2 Set Restore Options
3 Ready to complete

Set Restore Options

Set the restore options for each backup that you are restoring.

Client: PrimaryBackEnd
Backup: 09/14/2014 08:03 PM

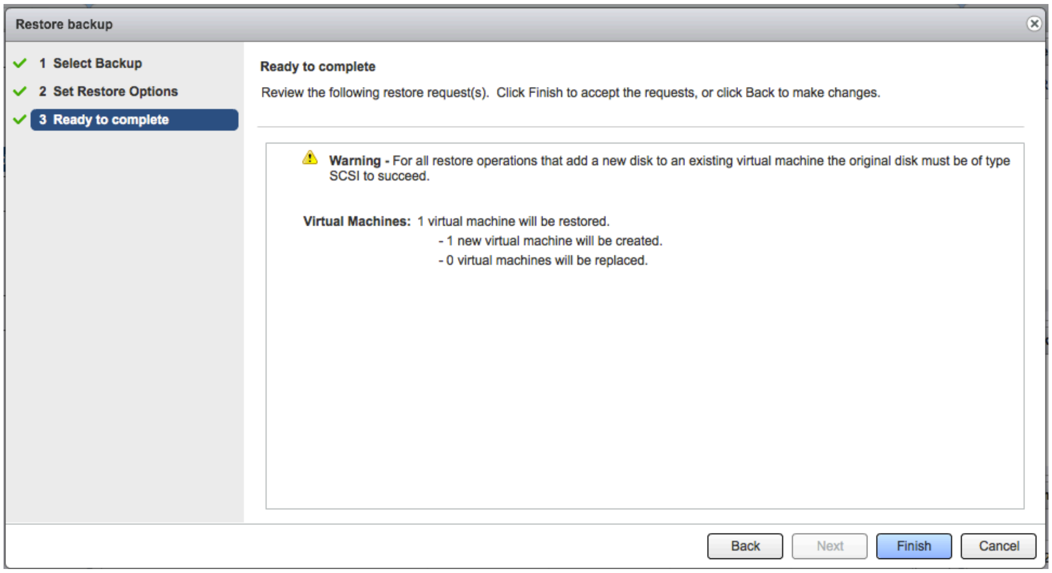
□ Restore to original location

New name: PrimaryBackEnd_2014915_133645
Destination: /Datacenters/MDC5One/MDC5Onecluster/MDC5One/In

▼ Advanced options

Datastore: MDC-S930-L32-1TB-VMFS5 (540.0 GiB free)
□ Power On ☑ Reconnect NIC

6. Select the desired options and click **Finish**.



Restore backup

✓ 1 Select Backup
✓ 2 Set Restore Options
✓ 3 Ready to complete

Ready to complete

Review the following restore request(s). Click Finish to accept the requests, or click Back to make changes.

⚠ **Warning -** For all restore operations that add a new disk to an existing virtual machine the original disk must be of type SCSI to succeed.

Virtual Machines: 1 virtual machine will be restored.
- 1 new virtual machine will be created.
- 0 virtual machines will be replaced.

You should now have your virtual machine and it restored state.

Patching the Guest-OS

As a guideline, patching up an EMC ViPR SRM virtual machine is not different than patching up another Tier 1 application running on a VM. Deploying a guest-OS level patch is the same as when doing it in the physical world.

When using virtual machines, you could make use of snapshots. As handy as they are, it is very important to understand that snapshots are not a backup solution. Do not rely on them as a backup.

You could use a snapshot prior to a new patch, allowing the VM a period of testing. VMware recommends the use of up to 3 snapshots and for not more than 24-72 hours. Snapshots grow in size and an excessive number of snapshots in a chain could cause a decrease in the VM and overall host performance. We adhere to the official recommendations of VMware.

The following is a procedural overview of the above:

1. Snapshot the VM
2. Apply the new patch
3. Allow the VM to run with the new patch (burn-in)
4. Remove the nth snapshot

Additional resources

For more information please refer to:

Best practices for virtual machine snapshots in the VMware environment (1025279). http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1025279

Best Practices for Applying Service Packs, Hotfixes and Security Patches. http://technet.microsoft.com/en-us/library/cc750077.aspx

VMware vSphere 5.1 Documentation Center, Using Snapshots to Manage Virtual Machines. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vm_admin.doc/GUID-E0080795-C2F0-4F05-907C-2F976433AC0D.html

References

1. EMC Inc., (n.d). *Using EMC VNX Storage with VMware vSphere*.

   Retrieved August 28, 2014, from https://www.emc.com/collateral/hardware/technical-documentation/h8229-vnx-vmware-tb.pdf

2. EMC ViPR SRM deployment documentation available on https://community.emc.com/community/products/vipr

3. VMware Inc., (n.d.). *VMware vSphere 5.1 Documentation Center, Using Snapshots to Manage Virtual Machines*. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vm_admin.doc/GUID-E0080795-C2F0-4F05-907C-2F976433AC0D.html

4. VMware Inc., (Aug 11, 2014). *Best practices for virtual machine snapshots in the VMware environment (1025279)*: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1025279

5. Microsoft Corporation, (n.d.). *Best Practices for Applying Service Packs, Hotfixes and Security Patches*. Retrieved August 28, 2014 from http://technet.microsoft.com/en-us/library/cc750077.aspx