vRealize Suite 7.0 Backup and Restore by Using Symantec NetBackup 7.6

vRealize Suite 7.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002059-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

vRealize Suite 7.0 Backup and Restore by Using Symantec NetBackup 7.6

vRealize Suite 7.0 Backup and Restore by Using Symantec Netbackup 7.6 provides information about how to back up and restore vRealize components by using Symantec NetBackup™.

Intended Audience

This information is intended for anyone who wants to back up and restore vRealize Suite 7.0 components by using NetBackup. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

1 Backup and Restore Introduction

You can successfully back up and restore the vRealize Suite 7.0 components by using Symantec NetBackup 7.6.

You can back up and restore the following versions of vRealize Suite 7.0 components with NetBackup 7.6.

- VMware vRealize ™ Automation 7.0.1
- VMware vRealize ™ Orchestrator ™ 7.0.1
- vRealize Operations Manager 6.2.0
- vRealize Log Insight 3.3.0
- vRealize Business 7.0.1

When to Back Up Components

You should back up vRealize Suite components for the following reasons:

- To prepare for major maintenance of any of the system components
- To implement scheduled maintenance backup
- To prepare for updating certificates
- To protect certificates after updating them

Preparing to Back Up vRealize Components

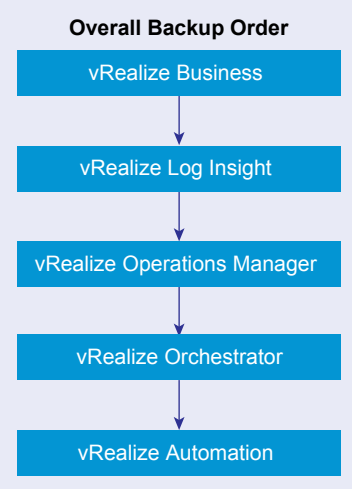
2

You can successfully prepare the vRealize Suite components for backup by planning and observing some basic guidelines.

This chapter includes the following topics:

vRealize Components Backup Order

You should back up the VMs for vRealize Suite components in a specific order.



Depending on the vRealize Suite components that you have configured and your requirements, schedule backups for your vRealize Suite components in the following order. If you do not have a particular component, you can move to the next component in the specified order. The order of the VMs can be also defined in the backup tools.

1 vRealize Business. Back up the VM for vRealize Business.

2 vRealize Log Insight. If the resources are not an issue, it is recommended to enable concurrent cluster node backups to speed up the backup process. Back up all the nodes at the same time.

3 vRealize Operations Manager. All nodes are backed up at the same time.

4 vRealize Orchestrator. You can take backups of the vRealize Orchestrator VMs, individually and in cluster mode, in no particular order.

- If vRealize Orchestrator is a standalone component, back it up before vRealize Automation components in no particular order.
- If vRealize Orchestrator is embedded with in the vRealize Automation deployment, back it up as part of the vRealize Appliance.

5 vRealize Automation. Back up the vRealize Automation components in the following order:

a Proxy Agents

b DEM Workers

c DEM Orchestrator

d Manager Services

e Websites

f vRealize Automation Appliances

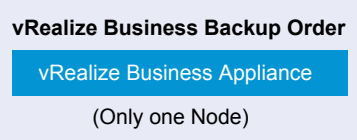
g PostgreSQL, if applicable

h MS SQL

If you have multiple components on a VM, select the order considering the latter component on the VM from the list.

vRealize Business Preparations for Backing Up

To minimize system downtime and data loss when failures occur, administrators back up the vRealize Business Standard installation on a regular basis. If your system fails, you can recover it by restoring the last known working backup. You back up vRealize Business by exporting or cloning the virtual appliance and use backups to restore the virtual appliance.



Guidelines for Backing Up

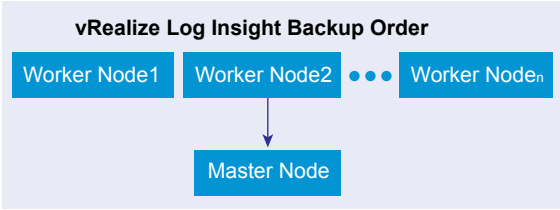
Use the following guidelines to plan backups:

- Verify that vRealize Business is up and running and vRealize Automation is registered with it.
- Verify that you can view the **Business Management** tab in your vRealize Automation deployment.
- Verify that vRealize Business is calculating the correct cost of the VMs.
- Verify that the VMs provisioned for vRealize Automation and vRealize Orchestrator are visible in vRealize Business and that vRealize Business can calculate the cost for the VMs.

vRealize Log Insight Preparations for Backing Up

You can perform full, differential, and incremental backups and restores of vRealize Log Insight VMs.

If resources are not a problem back up all the nodes at the same time, to speed up the backup process. Verify that you are increasing the number of concurrent backups from one, which is the default. Linear backup is also supported but it slows down the restore operation.



Guidelines for Planning Backups

You can use the following information for backing up vRealize Log Insight 3.3 clusters in a new environment.

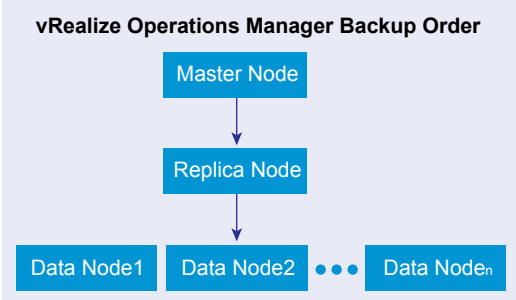
- Ensure that you have no configuration problems on source and target sites before performing the backup and restore operations.
- During the backup operation, the memory usage can increase due to the vRealize Log Insight cluster usage. In some cases, the worker nodes might be disconnected for 1 to 3 minutes due to high memory usage. To reduce the memory throttling on vRealize Log Insight nodes, follow these guidelines:
  - Allocate additional memory over the vRealize Log Insight recommended configuration.
  - Schedule the recurring backups during off-peak hours.
- Disable quiesced snapshots, because vRealize Log Insight does not support them.
- The vRealize Log Insight server supports Linux and Windows agents.
  - If the agent configuration is created on the server side, a separate backup of the agent node is not required.
  - If you use the agent nodes for more than installing the agent software and if these nodes need a full backup, follow the same backup procedure as for any VM.
  - If the agent configuration is done on the client side, on the agents, and if the agent nodes are used only to install vRealize Log Insight agent software, scheduling a backup of the agent configuration file is sufficient. Back up the `liagent.ini` file and replace the file on the recovered agent or Linux or Windows machine with the backup file.
- If concurrent backup is not possible, ensure that the vRealize Log Insight master node is backed up first before the worker nodes. Worker nodes can be backed up in any order.
- Ensure that the backup frequency and backup types are selected based on the available resources and customer-specific requirements.
- Use the following guidelines when scheduling recurring backups.
  - For a reasonable loaded cluster setup, it might take a while for the first backup to finish irrespective of the tool.

    - The first backup is usually a full backup. Successive backups can be incremental or full backups, Successive backups finish relatively fast, compared to the first backup operation.
- Use static IP addresses for all nodes in a vRealize Log Insight cluster.
    - Using static IP addresses eliminates the need to update the IP addresses of vRealize Log Insight cluster nodes each time the IP address of a vRealize Log Insight node changes.
    - vRealize Log Insight includes all node IP addresses in each cluster node configuration file at `/storage/core/loginsight/config/loginsight-config.xml#<n>` where `<n>` is the largest number.
    - Some products that integrate with vRealize Log Insight to feed their logs, use a fully qualified domain name (FQDN) or IP address as the syslog target. For example, vSphere ESXi, vSphere, and vRealize Operations Manager use the nodes of the cluster master's or the load balancer's (if configured) FQDN or IP address as the syslog target.
- Use an FQDN for all nodes in the vRealize Log Insight cluster.
    - For the master node, when you use a load balancer, a fully resolvable FQDN is required. Otherwise, the ESXi hosts fail to feed the syslog messages to vRealize Log Insight or to any remote target.
    - Using an FQDN saves time on post-restore and recovery configuration changes, assuming that the same FQDN can be resolved on the recovery site.
    - For system alerts, vRealize Log Insight uses FQDN host names if available instead of IP addresses.
    - Assuming that only underlying IP addresses change post-backup and recovery or disaster recovery operations, using FQDN eliminates the need to change the syslog target address (master node FQDN or internal load balancer FQDN) on all the external devices feeding logs to the vRealize Log Insight cluster.
    - With vRealize Log Insight 2.5, you must update the configuration file, located at `/storage/core/loginsight/config/loginsight-config.xml#<n>` where `<n>` is the largest number. This configuration file replaces the worker node IP address with the new IP address used for the restored nodes because the FQDN is not used for worker node addresses in the configuration file. You need to make this change only on the master node to synchronize the changes with all the worker nodes.
- Join requests from a vRealize Log Insight worker node should use the FQDN of the vRealize Log Insight master node.
    - Beginning in vRealize Log Insight 2.5, the master node host value in the configuration file on each of the nodes, located at `/storage/core/loginsight/config/loginsight-config.xml#<n>`, is based on the value used by the first worker node sending a join request. Using the FQDN of the master node for the join request prevents making any manual changes to the master node host value post-disaster recovery. Otherwise, the worker nodes cannot rejoin the master node until the master node host name is updated in the configuration files on all restored cluster nodes.
- Provide static IP addresses as well as optional virtual IP addresses for the load balancer.
    - When configuring an integrated load balancer, provide the optional FQDN for the virtual IP address. This optional FQDN enables vRealize Log Insight to revert to the FQDN when an IP address is not reachable for any reason.

vRealize Operations Manager Preparations for Backing Up

To minimize vRealize Operations Manager downtime and data loss if a failure occurs, back up on a regular basis. If your system fails, you can recover it by restoring to the last full or incremental backup.

You can backup and restore vRealize Operations Manager single-node or multi-node clusters by using backup tools. You can perform full or incremental backups and restores of virtual machines.



NOTE All nodes are backed up and restored at the same time. You cannot back up and restore individual nodes.

Guidelines for Planning Backups

Verify that the following prerequisites are met before you back up vRealize Operations Manager systems by using any tool:

- Do not quiesce the file system.
- Use a resolvable host name and a static IP address for all nodes.
- All nodes must be powered on and accessible during backup.
- Back up the entire VM. You must back up all VMDK files that are part of the virtual appliance.
- Do not stop the cluster while performing the backup.

NOTE Do not perform a backup while dynamic threshold (DT) calculations are running because this backup might lead to performance problems or loss of nodes. DT calculations run at 2 a.m. by default. The initial backup might take longer to complete depending on the cluster size and number of nodes, so you should turn off the DT. Schedule the differential or incremental backups so that they end before the DT calculations begin.

If you are using backup tools, such as NetBackup and vSphere Data Protection, and have manually created vSphere snapshots of any of the VMs to be backed up, be aware that the tools delete all existing snapshots at the time of the backup or restore.

Common Backup Scenarios

The common backup scenarios for vRealize Operations Manager systems include a full backup of a single node virtual appliance system and a full backup of a multiple node virtual appliance cluster.

Single-Node Virtual Appliance

This scenario backs up a single-node system on the same host.

1. Assign a static IP address.
2. Ensure that the power is on for the entire backup process.
3. If the system is a Linux or Windows installation, you need to prepare the system before you start the backup. For more information, see *Preparing for vRealize Operations Manager Installation* in the VMware vRealize Operations Manager Documentation Center.

Multiple-Node Virtual Appliance Clusters

This scenario backs up a multiple-node virtual appliance clusters.

1 Assign a static IP address for each node.

2 Ensure that all nodes that are configured with high availability are accessible and are enabled for high availability.

3 Ensure that the power remains on during the entire backup process.

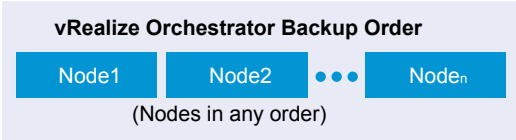
4 If the system is a Linux or Windows installation, you must prepare the system before you start the backup. For more information, see *Preparing for vRealize Operations Manager Installation* in the VMware vRealize Operations Manager Documentation Center.

vRealize Orchestrator Preparations for Backing Up

You can backup your vRealize Orchestrator VMs in no particular order. You can also back up the vRealize Orchestrator elements that you modified.

If vRealize Orchestrator is embedded within the vRealize Automation appliance, perform its backup along with Manager Services for vRealize Automation.

If vRealize Orchestrator is a standalone component, perform its backup before backing up vRealize Automation components in no particular order.



Each vRealize Orchestrator server instance has unique certificates, and each vCenter Server plug-in instance has a unique ID. The certificates and the unique ID identify the vRealize Orchestrator server and the vCenter Server plug-in. If you do not back up the vRealize Orchestrator elements or export the vRealize Orchestrator configuration for backup purposes, make sure that you change these identifiers.

All components of the vRealize Orchestrator must be backed up together and at the same time including the database components. You must back up the vRealize Orchestrator database and VMs (custom workflows and packages).

vRealize Orchestrator Database

You can take full database backups of the database in your environment before a full VM backup. The main purpose is to ensure consistency of the data when you have to restore.

Follow your in-house procedures to back up the vRealize Orchestrator database outside of the vRealize Suite framework.

vRealize Automation Preparations for Backing Up

A system administrator backs up the full vRealize Automation installation on a regular basis. Plan the backup around efficiencies and periods of low activity.

You can use several strategies, singly or in combination, to back up vRealize Automation system components. For virtual machines (VMs), you can use the Snapshot function to create snapshot images of critical components or use tools like Symantec NetBackup and vSphere Data Protection. If a system failure occurs, you can use these images to restore components to their state when the images were created. Alternatively, and for non-virtual machine components, you can create copies of critical configuration files for system components, which can be used to restore these components to a customer configured state following reinstallation.

A complete backup includes the following components:

- IaaS components
  - Proxy Agents
  - DEM Workers
  - DEM Orchestrator
  - Manager Services
  - Websites
- vRealize Automation appliance
- PostgreSQL database. Applicable only for legacy installations that do not use an embedded appliance database
- Infrastructure MSSQL database
- (Optional) Software load balancers
- (Optional) Load balancers that support your distributed deployment. Consult the vendor documentation for your load balancer for information about backup considerations

Guidelines for Planning Backups

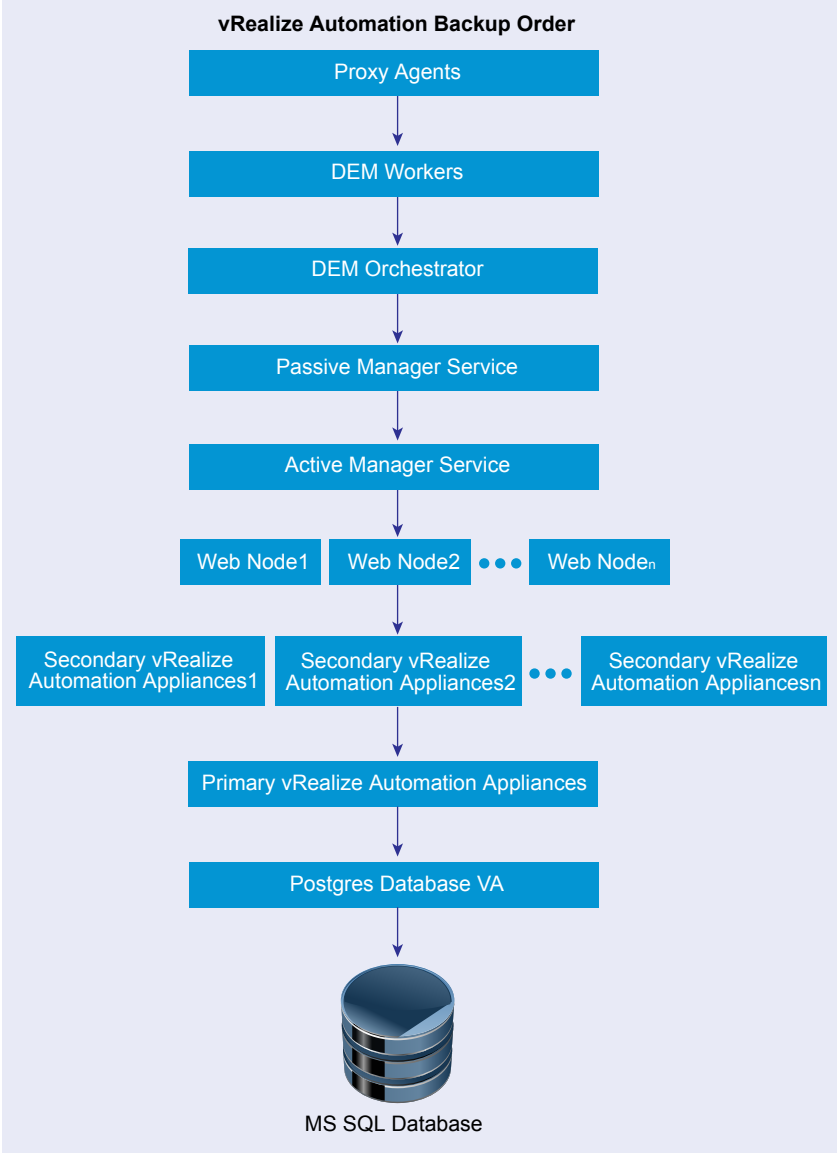
Use the following guidelines to plan backups:

- When you back up a complete system, back up all instances of the vRealize Automation appliance and databases as near simultaneously as possible, preferably within seconds.
- Minimize the number of active transactions before you begin a backup. Schedule your regular backup to when your system is least active.
- Back up all databases at the same time.
- Create a backup of instances of the vRealize Automation appliance and the IaaS components when you update certificates.

vRealize Automation Backup Order

You must back up the VMs for vRealize Automation components in a specific order.

When you use backup tools to schedule backups for your vRealize Automation deployment, you must back up the components in the following order:



If you have multiple components on a VM, select the order considering the latter component on the VM from the list.

If vRealize Orchestrator is a standalone component, then it should be backed up in no particular order before vRealize Automation components.

Backing Up vRealize Automation Certificates

A system administrator backs up certificates and certificate chains at installation time or when a certificate is replaced.

Back up the following certificates:

- vRealize Automation appliance certificates and the entire corresponding certificate chain.
- IaaS certificates and the entire corresponding certificate chain.

Backing Up vRealize Automation Databases

The database administrator backs up the Infrastructure MSSQL Server and Appliance Database.

As a best practice, back up the Infrastructure MSSQL and Appliance Database or legacy PostgreSQL databases as nearly simultaneously as possible to prevent or minimize data loss. Also, when applicable, back up databases with Point-in-Time enabled. By using Point-in-Time recovery, you ensure that the two databases are consistent with each other.

NOTE If only one database fails, you must restore the running database to the most recent backup so that the databases are consistent.

Infrastructure MSSQL Database

Back up the Infrastructure MSSQL and Appliance Database or legacy PostgreSQL databases as nearly simultaneously as possible to prevent or minimize data loss. Also, when applicable, back up databases with Point-in-Time enabled. By using point-in-time recovery, you ensure that the two databases are consistent with each other. If only one database fails, you must restore the running database to the most recent backup so that the databases are consistent.

Follow your in-house procedures to back up the Infrastructure MSSQL database outside of the vRealize Suite framework.

Use the following guidelines when creating a backup:

- If possible, check that all IaaS workflows are complete and that all IaaS services are stopped or that activity is minimized.
- Back up with Point-in-Time enabled.
- Back up the MSSQL database at the same time that you back up the other components.
- Back up the passphrase for your database.

NOTE Your database is protected by a passphrase. Have the passphrase available when you restore the database. Typically, you record the passphrase in a safe and accessible location at install time.

Appliance Database or Legacy PostgreSQL Database

If you are using an Appliance Database or a legacy PostgreSQL database embedded in a vRealize Automation appliance, you can back up the database by backing up the entire appliance.

If you are using a standalone legacy PostgreSQL appliance, you must back up the appliance.

If you are using a legacy PostgreSQL database, you can also backup the database separately. For more information, see the VMware Knowledge Base article *Migrating from external vPostgres appliance to vPostgres instance located in the vCAC appliance (2083562)* at http://kb.vmware.com/kb/2083562 for more information.

Backing Up Load Balancers

Load balancers distribute work among servers in high-availability deployments. The system administrator backs up the load balancers on a regular basis at the same time as other components.

Follow your site policy for backing up load balancers, keeping in mind the preservation of network topology and vRealize Automation backup planning.

Backing Up IaaS Components

The system administrator backs up the IaaS components in a specific order.

You can back up IaaS components by taking a snapshot of the VMs in the following order:

- Proxy Agents and DEMs
- Manager Service
- Websites

Backing Up vRealize Automation Appliance

You must back up secondary vRealize Automation appliance nodes, followed by the master node.

The primaryvRealize Automation appliance instance contains the writeable Appliance Database, if applicable, and is the last appliance that you shut down in an ordered shutdown procedure.

(Optional) Shut Down vRealize Automation

Shutting down vRealize Automation is optional. If you decide to shut down your vRealize Automation system, use the specified order.

If you are using vCenter Server to manage your virtual machines, use the guest `shutdown` command to shut down vRealize Automation.

Procedure

1. Shut down the DEM Orchestrator and Workers and all vRealize Automation agents in any order and wait for all components to finish shutting down.
2. Shut down the VMs that are running the Manager Service and wait for the shutdown to finish.
3. (Optional) For distributed deployments, shut down all secondary Web nodes and wait for the shutdown to finish.
4. Shut down the primary Web node, and wait for the shutdown to finish.
5. (Optional) For distributed deployments, shut down all secondary vRealize Automation appliance instances and wait for the shutdown to finish.
6. Shut down the primary vRealize Automation appliance and wait for the shutdown to finish.

   If applicable, the primary vRealize Automation appliance is the one that contains the master, or writeable, Appliance Database. Make a note of the name of the primary vRealize Automation appliance. You use this information when you restart vRealize Automation.
7. If you are using a legacy standalone PostgreSQL database, also shut down that machine.

You have shut down your vRealize Automation deployment.

Backing Up vRealize Components by Using NetBackup 7.6

3

To minimize system downtime and data loss when failures occur, back up all components in the vRealize Suite on a regular basis. If your system fails, you can recover it by restoring the last known working backup and reinstalling some components.

You can back up the vRealize Suite VMs with NetBackup 7.6 by creating a backup policy and executing it.

You must create the backup policy before you start the backup process for any VM. For more information about creating a backup policy, go to www.symantec.com and see *Symantec NetBackup 7.6 for VMware Administrator's Guide*.

Create a Backup Policy for vRealize Suite

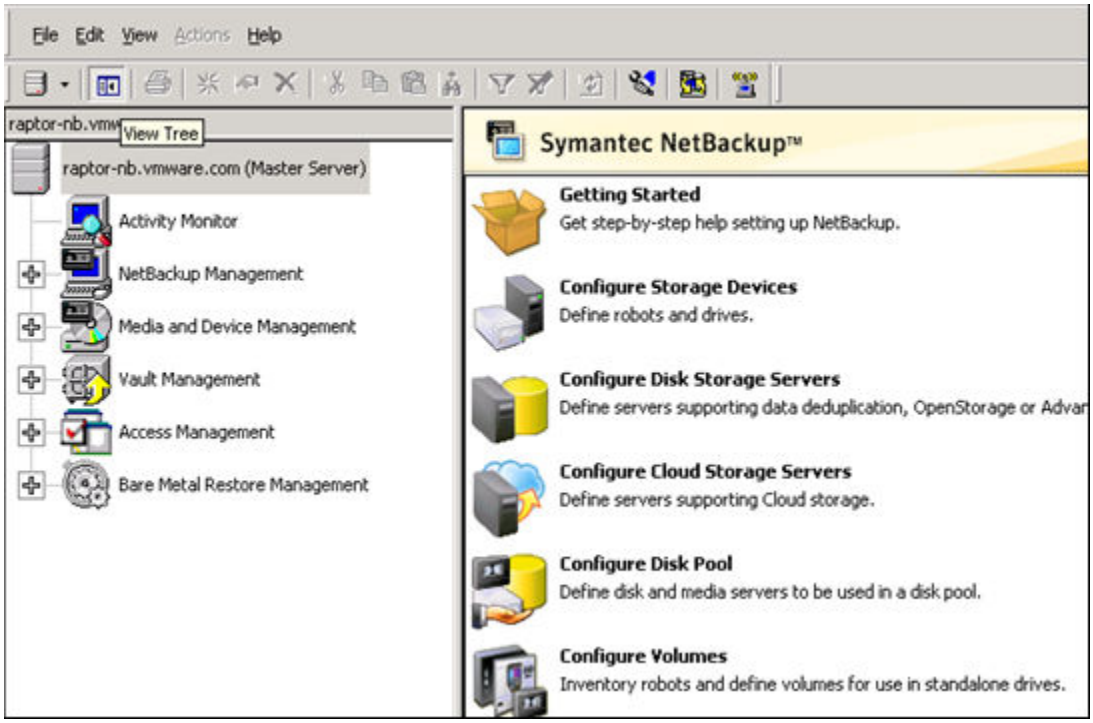
You can create a backup policy for vRealize Suite components by using the Policy Configuration Wizard.

Prerequisites

- Verify that your NetBackup is fully configured.
- You can include VMs that use the same datastore in a single NetBackup policy to control the amount of backup-related I/O that occurs per datastore and to limit the backup effect on the target VMs.
- You can use combination of full and incremental backups to reduce the time needed for the execution of the backup policy and required resources.

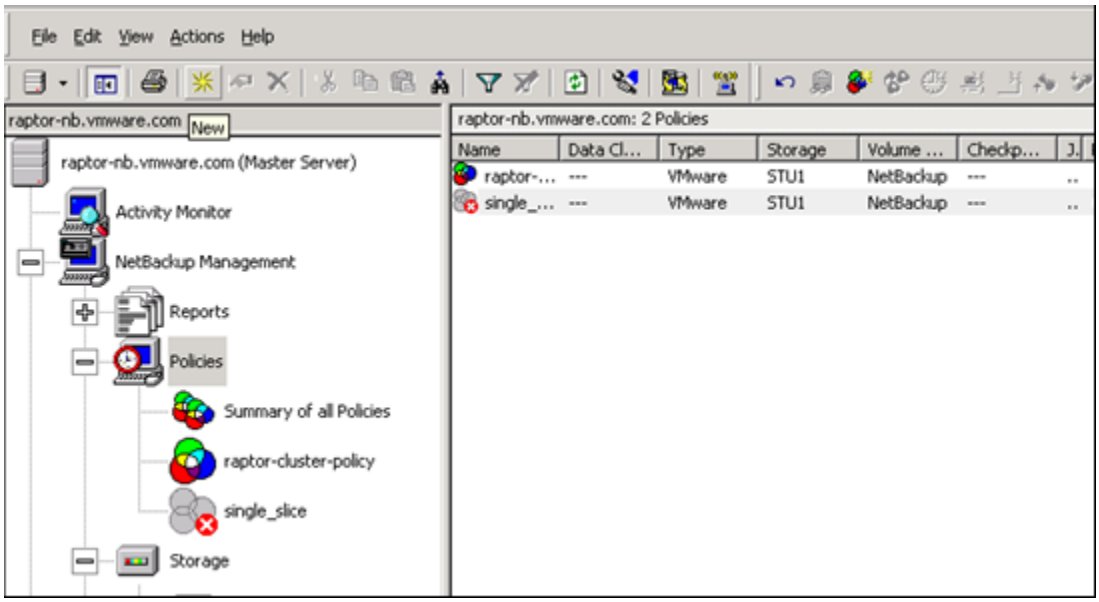
Procedure

1 Start NetBackup Administration Console and click the **View Tree** icon.

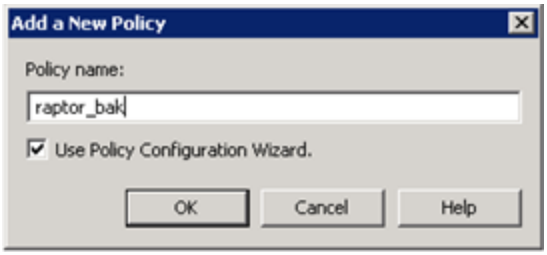


2 Select **NetBackup Management** > **Policies** in the navigation pane.

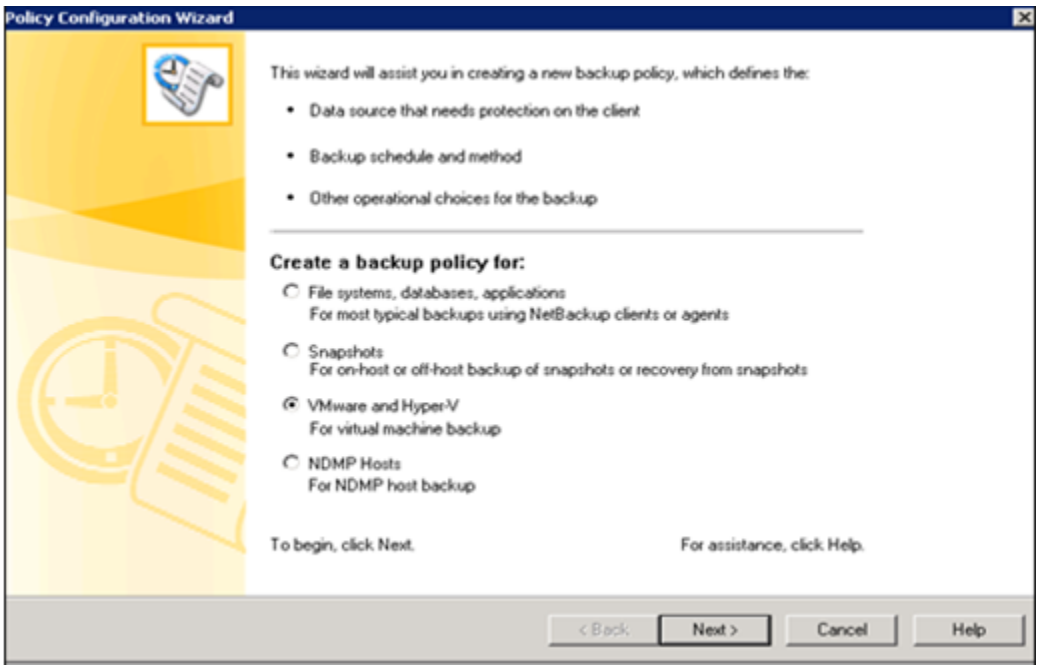
3 Click the **New** icon from the toolbar.



4 In the Add a New Policy window, enter a name for the new policy. Select the **Use Policy Configuration Wizard** check box, and click **OK**.



5 In the **Policy Configuration Wizard** window, under **Create a backup policy for**, select **VMware and Hyper-V** and click **Next**.

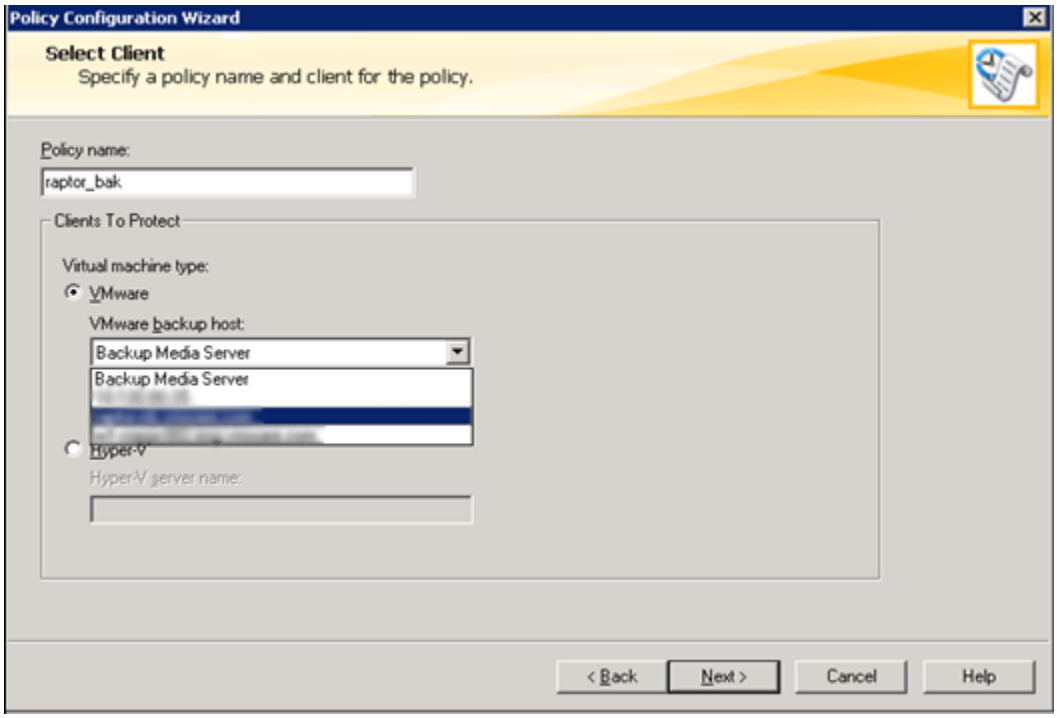


6 In the **Select Client** window, verify that the **Policy Name** is the same as you have entered and click **VMware** as the virtual machine type.

7 Select a backup host from the drop-down menu and click **Next**.

Instead of a particular host, you can select Backup Media Server. This option enables the use of one or more media servers as the backup host, for host redundancy and faster backups.

The individual backup hosts (not the media servers) are defined in the **Administration Console** in the following location: **Host Properties > Master servers**. Double-click the master server and click **Master Server Properties > VMware Access Hosts**.



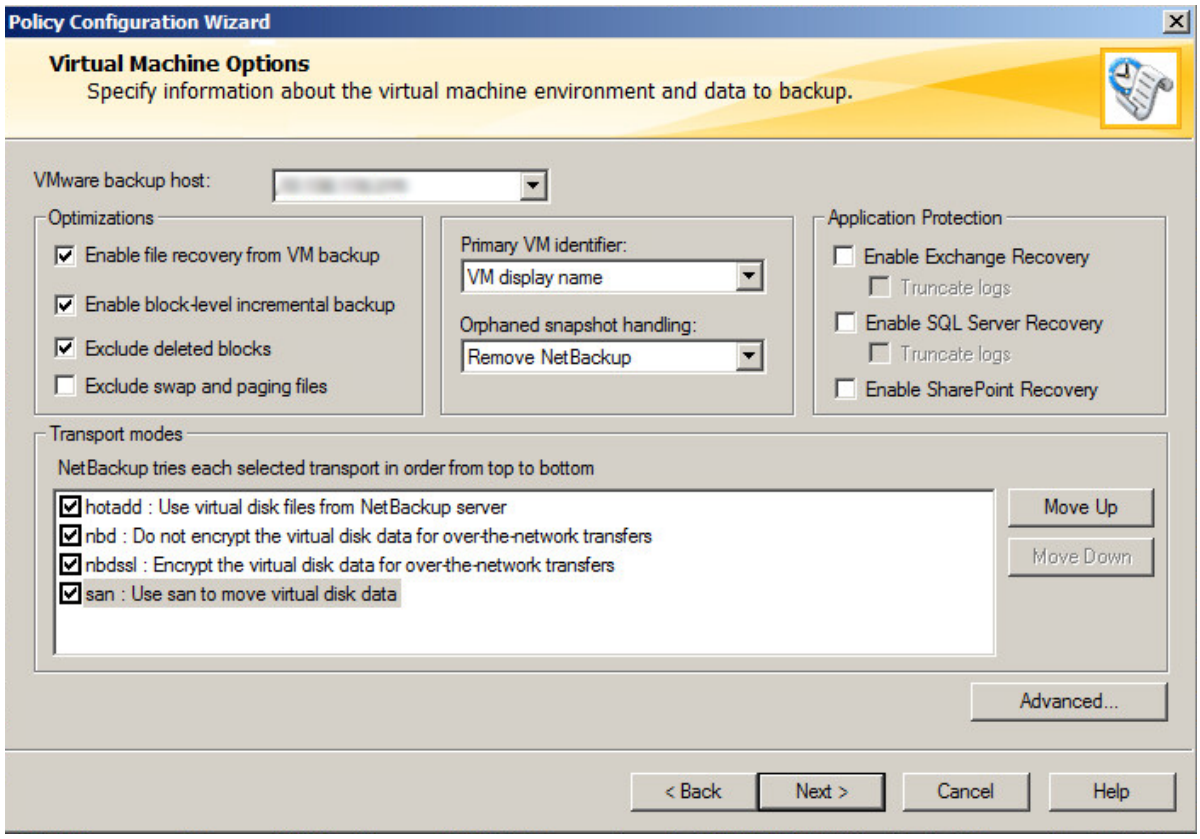
8 In the Virtual Machine Options window, specify information about the virtual machine environment.

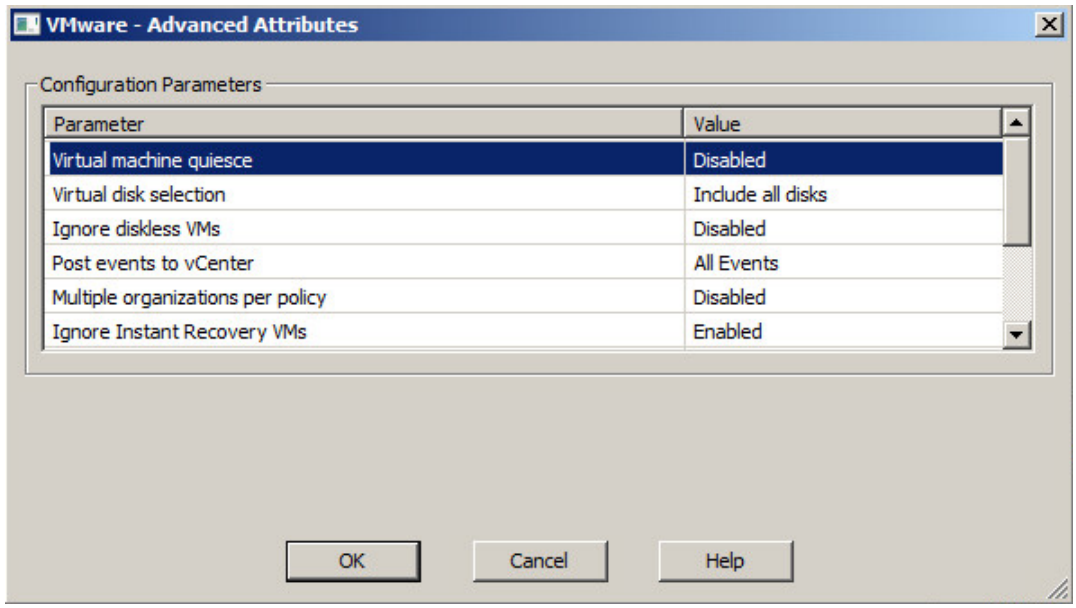
a Select options under **Optimizations**, **Appication Protection**, and **Transport modes** or use the default.

b Select **Primary VM identifier** as **VM display name**.

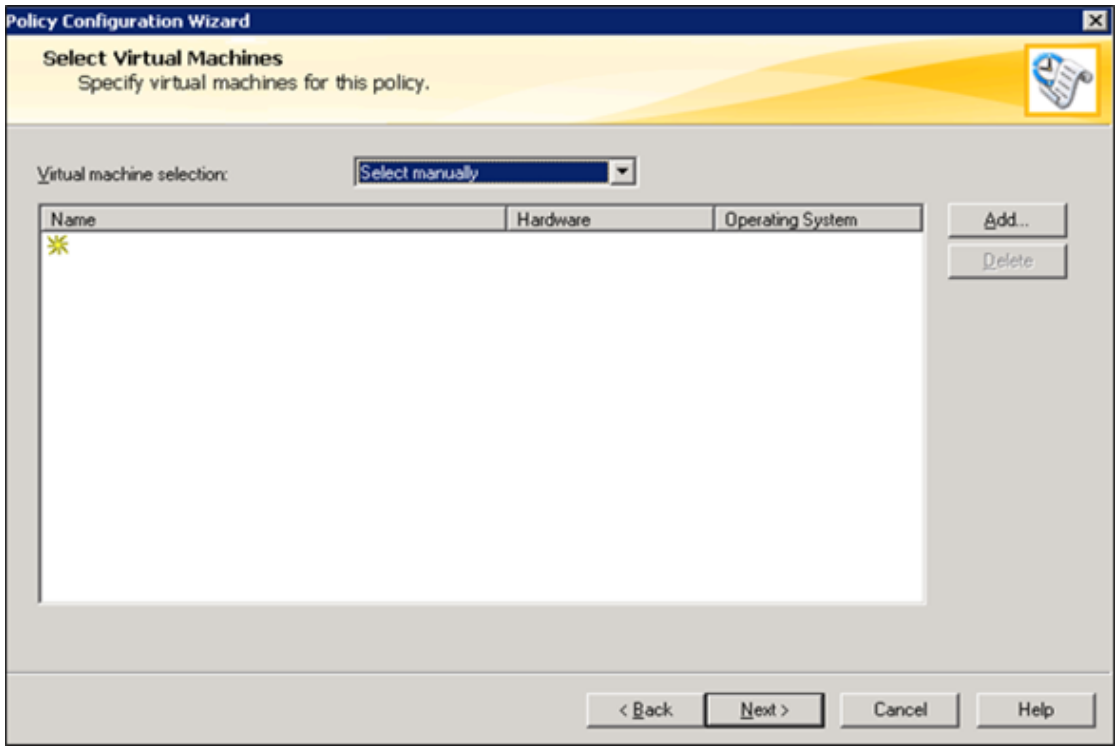
c Click **Advanced**. In the VMWare - Advanced Attributes window verify that the **Virtual machine quiesce** parameter is **Disabled** for all the VMs and click **OK**.

d In the Virtual Machine Options window and click **Next**.



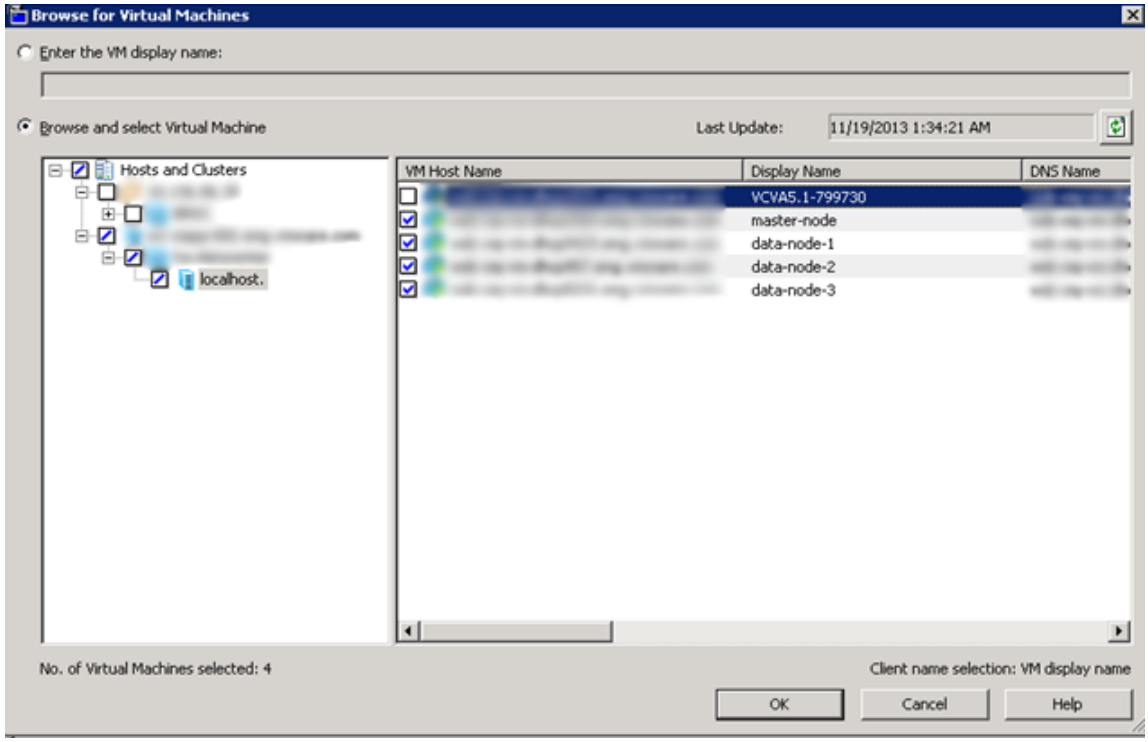


9 In the **Select Virtual Machines** window, click **Add** to browse and select VMs.

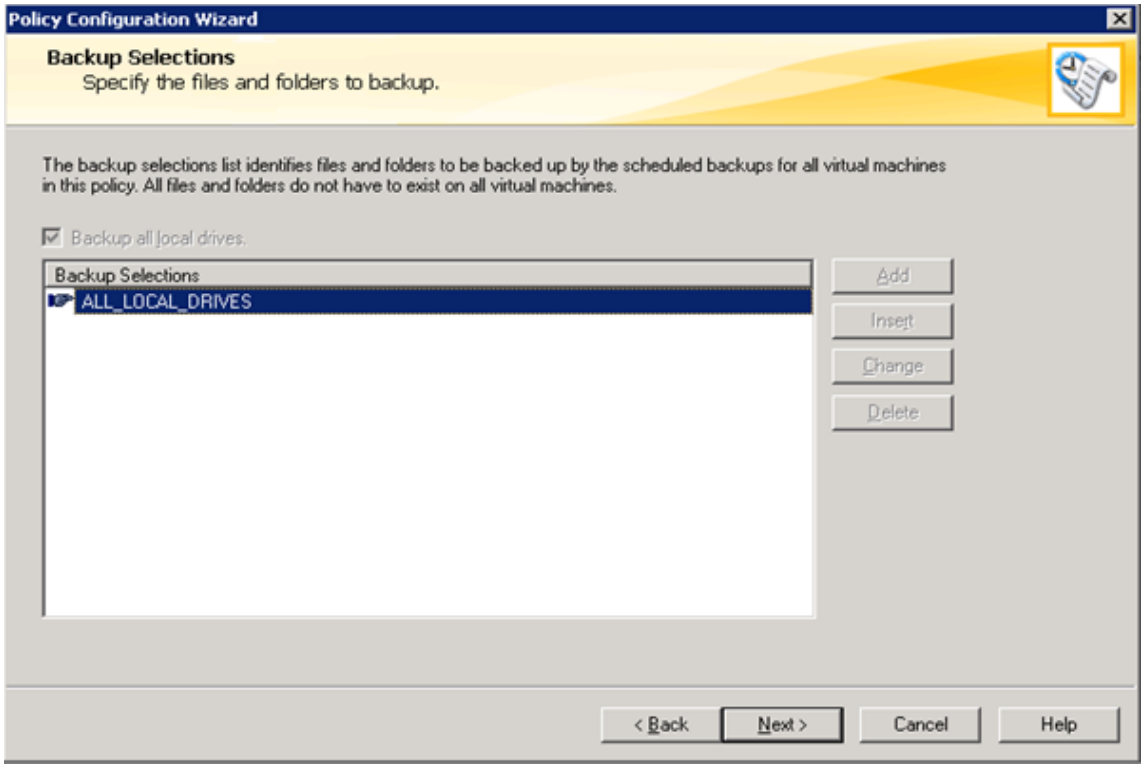


NOTE You can add VMs as per the lists in the respective vRealize Suite components. If you do not add the VMs in the correct order, you do not have to remove the VMs, because NetBackup allows you to change the order of the VMs by dragging the VMs to the correct order.

10 Select the VMs that you want to add, click **OK**, and click **Next**.



11 In the **Backup Selections** window, select **ALL_LOCAL_DRIVES** to get a full backup of each VM and click **Next**.

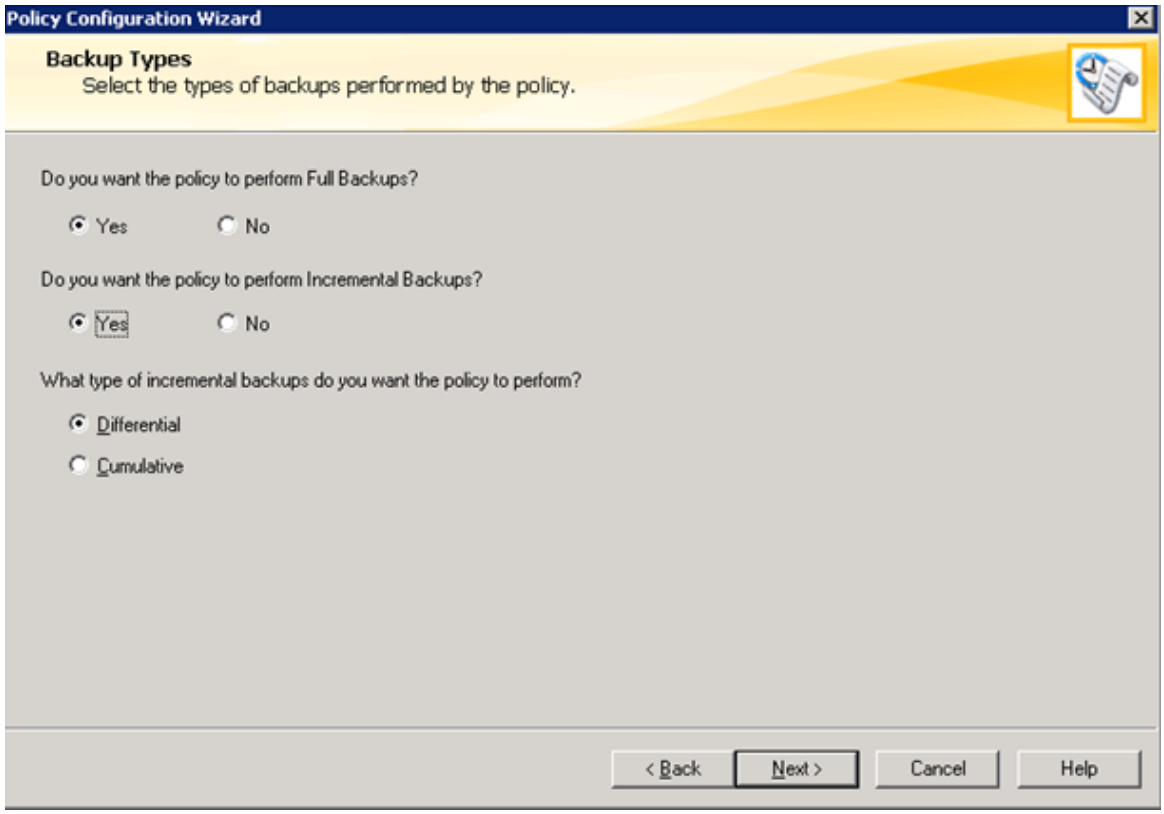


12 On the **Backup Types** window, select the types of backups.

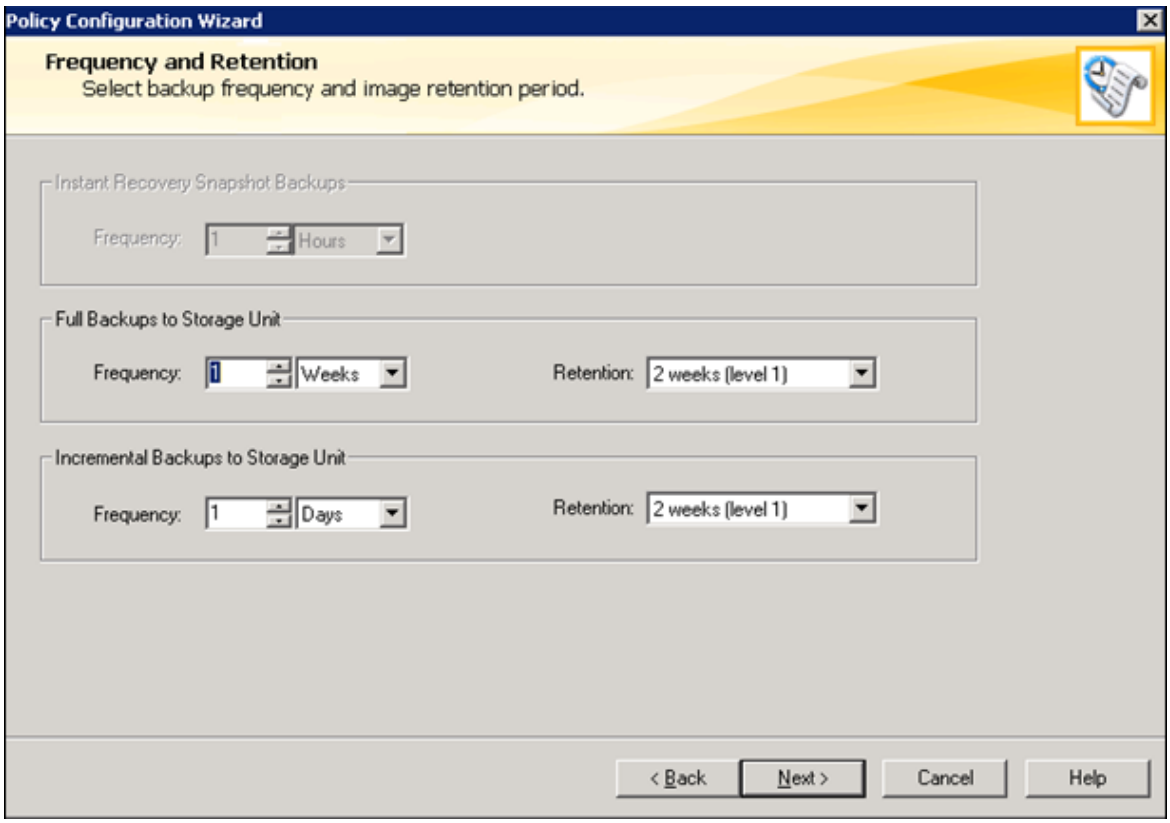
a Selct if you want the policy to perform full backups and incremental backups.

b Select **Differential** to perform incremental backups to optimize the overall backup process.

c Click **Next**.


Policy Configuration Wizard
Backup Types
Select the types of backups performed by the policy.
Do you want the policy to perform Full Backups?
Yes
No
Do you want the policy to perform Incremental Backups?
Yes
No
What type of incremental backups do you want the policy to perform?
Differential
Cumulative
< Back
Next >
Cancel
Help

13 In the **Frequency and Retention** window, select the backup frequency, the image retention period, and click **Next**.

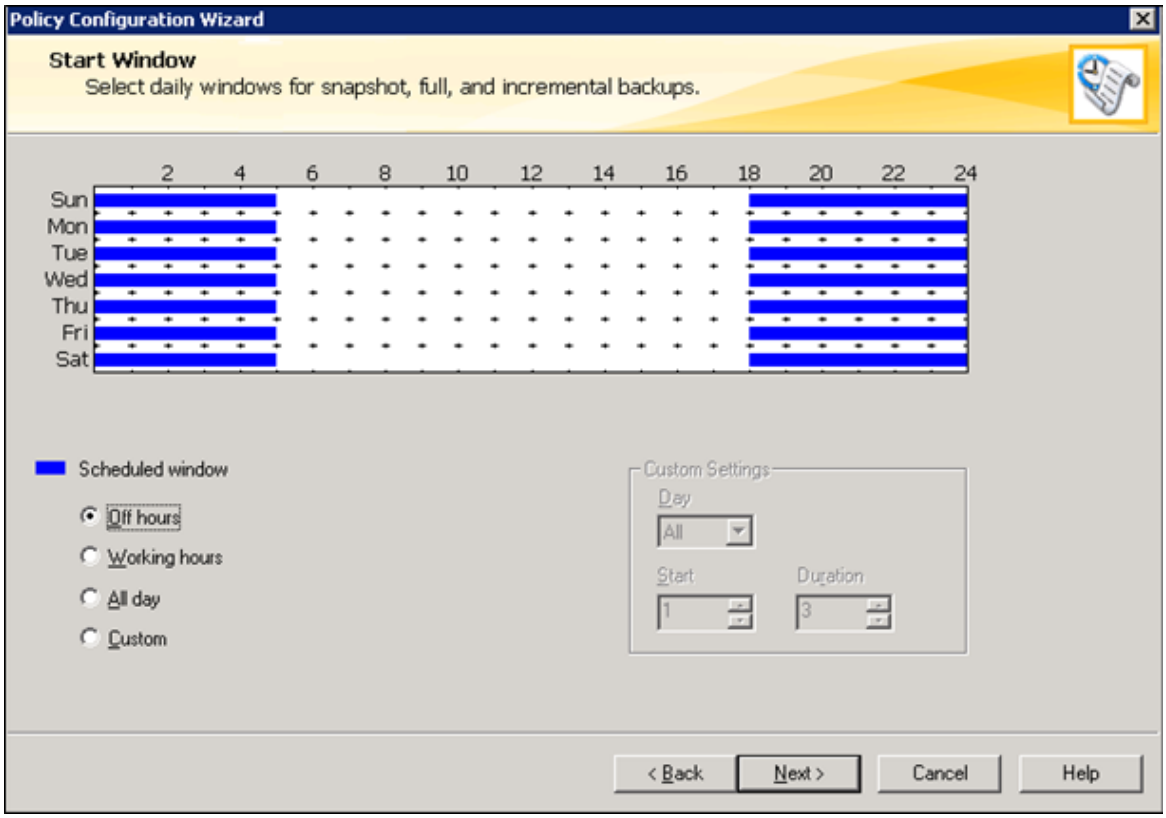


14 In the **Start Window**, select daily windows for snapshot, full, and incremental backups.

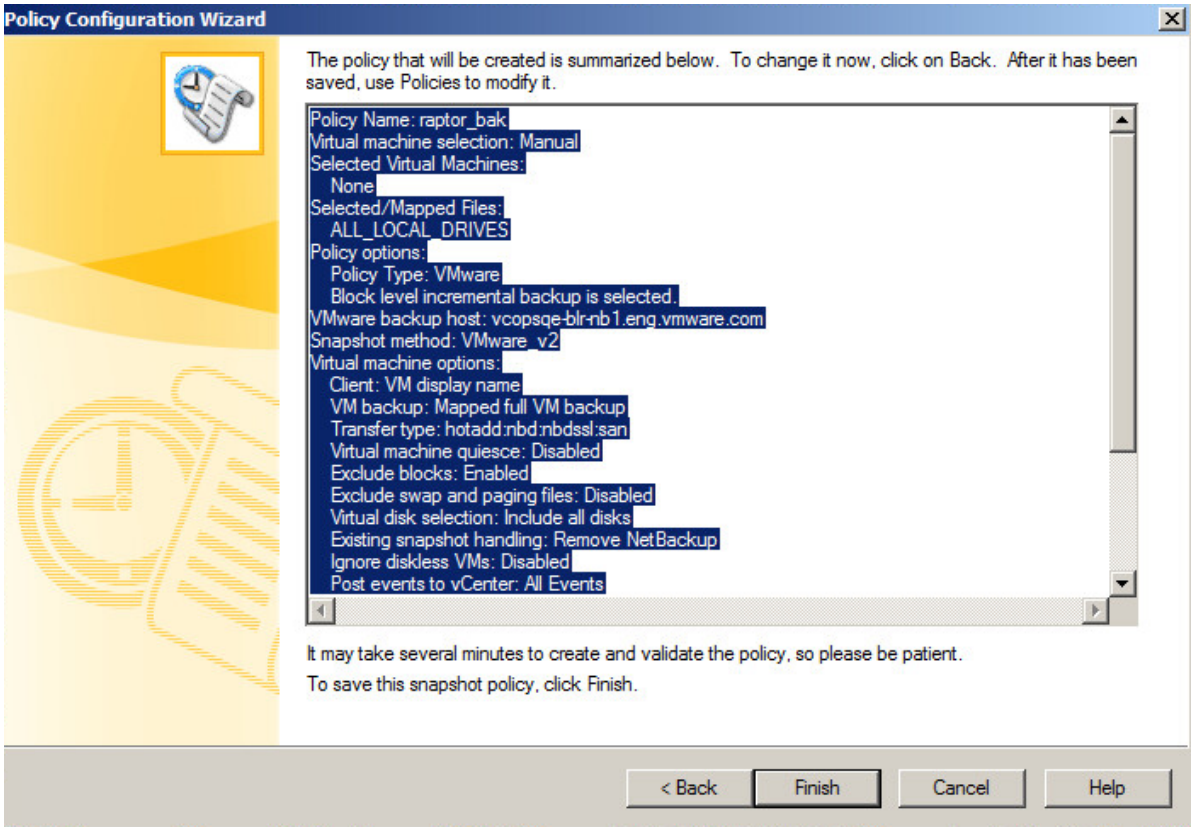
a Select **Off hours** as the **Scheduled window**, because an active backup process can add a overhead to the client-system setup.

b Click **Next**.

NOTE For vRealize Operations Manager, the **Scheduled window** must not interfere with the Dynamic Threshold (DT). Schedule the backups when the DT is not running. DT runs at 2 a.m. by default.



15 Review the summary of the policy. Click **Back** to make any change or click **Finish** to save the backup policy.



The backup policy is configured and is ready for execution.

Executing a Backup Policy

You can execute the backup policy manually after you create the backup policy.

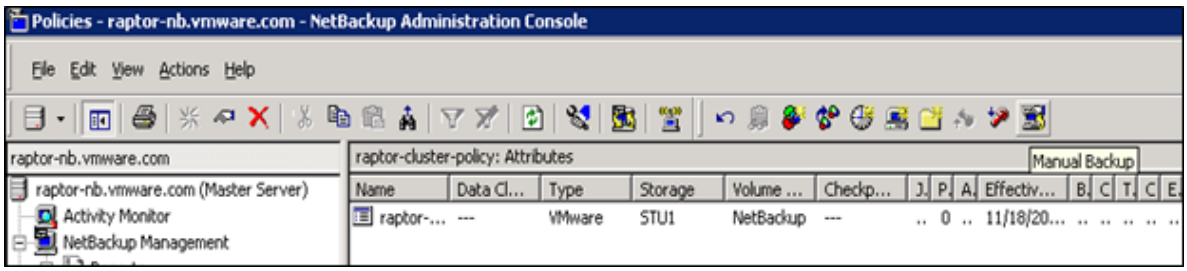
Prerequisites

"Create a Backup Policy for vRealize Suite," on page 19 components

Procedure

1 To manually execute a backup policy, select the policy on the Netbackup Administration Console window and click the **Manual Backup** icon from the toolbar.

The backup is executed to the schedule specifications that you created in the backup policy.



2 The backup runs in the background and you can monitor it in **Activity Montor**.

Restoring, Powering On, and Validating vRealize Suite

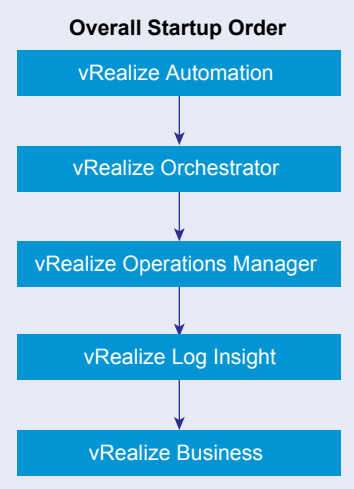
4

You can restore, power on, and validate that the vRealize Suite components are restored correctly by using the following information.

This chapter includes the following topics:

vRealize Suite Startup Order

You should start up the VMs for vRealize Suite components in a specific order.



Depending on the vRealize Suite components that you have backed up, restore your vRealize Suite components in the specified order. If you have taken any snapshots, you must remove the snapshots before you restore.

1 vRealize Automation. Start up the vRealize Automation components in the following order:

   a MS SQL

b PostgreSQL, if applicable

c vRealize Automation Appliances

d Websites

e Manager Services

f DEM vRealize Orchestrator

g DEM Workers

h Proxy Agents

2 vRealize Orchestrator. You can take start up the vRealize Orchestrator VMs in no particular order.

3 vRealize Operations Manager. All nodes can start at the same time.

4 vRealize Log Insight. Start up the master node, followed by VMs with the worker nodes in any order.

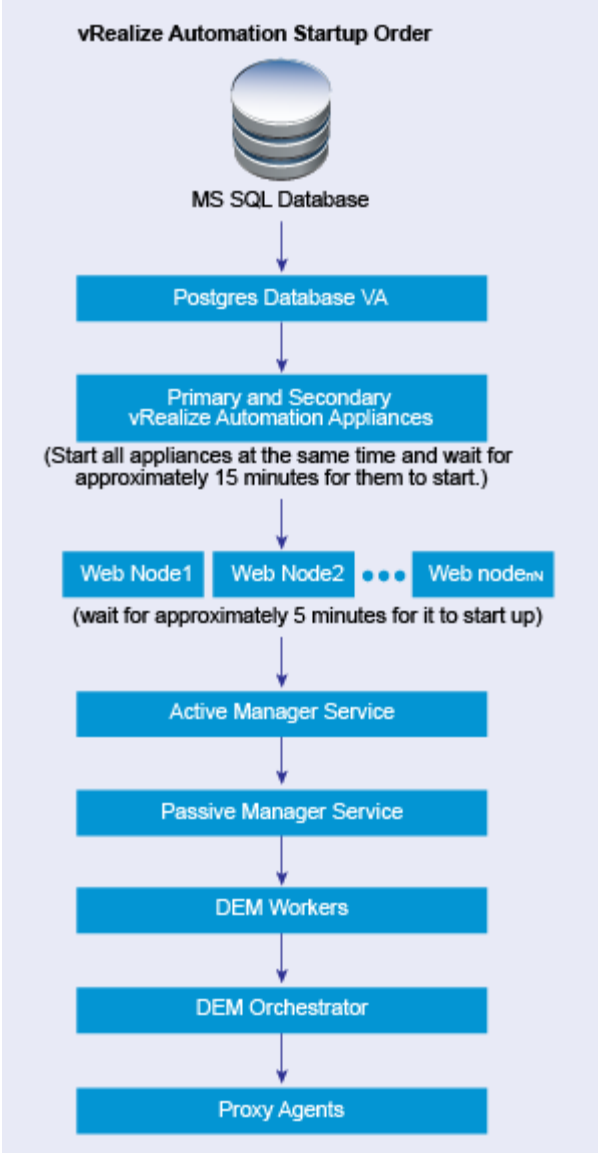
5 vRealize Business. Start up the VM for vRealize Business.

vRealize Automation System Recovery

A system administrator uses backups to restore vRealize Automation to a functional state after a system failure. If IaaS components such as Manager Service machines fail, you must reinstall them.

If you restore from a backup, machines that were provisioned after the backup still exist, but are not managed by vRealize Automation. For example, they do not appear in the items list for the owner. Use the Infrastructure Organizer to import virtual machines and bring them back under management.

You must start up your vRealize Automation components in a specified order.



Restoring vRealize Automation Databases

A system administrator restores the IaaS MSSQL database and the PostgreSQL database.

Recover a database in the following situations:

- If both databases fail, restore them from the last known time when both databases were backed up.
- If one database fails, restore it and revert the functional database to the version that was in use when the backup used to restore the failed database was created.

The backup time for each database can differ. The greater the gap between the last working time of the databases, the greater the potential for data loss.

You should back up full VMs of databases, instead of backing up PostgreSQL database directly. For information about how to restore a PostgreSQL database, see the VMware Knowledge Base article *Migrating from external vPostgres appliance to a vPostgres instance located in the vCAC appliance (2083562)*..

Database Passphrases

IaaS MSSQL database security requires a security passphrase to generate an encryption key that protects the data. You specify this passphrase when you install vRealize Automation.

If you lose the passphrase, or want to change the passphrase, consult VMware technical support for more information.

Restoring the vRealize Automation Appliance and Load Balancer

If a failure occurs, a system administrator restores the vRealize Automation appliance. If a load balancer is used, the administrator restores the load balancer and the virtual appliances that it manages. For vRealize Automation 7.0, you cannot change the host names during restoration.

You might need to restore a failed virtual appliance in the following circumstances:

- You are running a minimal deployment and your only vRealize Automation appliance fails or becomes corrupted.
- You are running a distributed deployment and some, but not all, virtual appliances fail.
- You are running a distributed deployment and all virtual appliances fail.

How you restore a vRealize Automation appliance or virtual appliance load balancer depends on your deployment type and on which appliances failed.

- If you are using a single virtual appliance whose name is unchanged, restore the virtual appliance, or redeploy it and restore a set of backed up files. No further steps are required.
- If you are running a distributed deployment that uses a load balancer, and you change the name of the virtual appliance or the virtual IP address of the load balancer, you must redeploy the appliance and restore its backed up VMs or files. Also, you must regenerate and copy certificates for your deployment.

If you are redeploying, reconfiguring, or adding virtual appliances to a cluster, see *Installation and Configuration* documentation for vRealize Automation appliance in the vRealize Automation Documentation Center for more information.

Restoring the IaaS Website, Manager Services, and Their Load Balancers

A system administrator restores the IaaS Website and Manager Service and their associated load balancers. For vRealize Automation 7.0, host name or IP address changes are not supported.

Restoring the DEM Orchestrator and the DEM Workers

If a failure occurs, a system administrator restores all DEMs from the available backups.

Restoring the IaaS Agents

The system administrator restores all the IaaS agents from the available backups.

If you reinstall vSphere agents, use the same endpoint name used at backup.

(Optional) Change the IP Addresses of vRealize Automation Appliances After Restore

You should perform these steps, only if you have changed the IP addresses of the vRealize Automation appliances after the restore of vRealize Automation has started. This is a workaround in order to get the vRealize Automation up and running after the restore, if you have changed the IP addresses during the restore process.

If you have changed the IP addresses of the vRealize Automation appliances during the restore process, you must perform the following steps in order to have the vRealize Automation operational after the restore.

Procedure

1 Change the DNS server so that the FQDNs of all the vRealize Automation machines points to the new IP addresses.

2 Add the new IP addresses in the load balancer pools, such as virtual appliances, web, and manager.

3 Update the `/etc/hosts` file for each of the vRealize Automation VA nodes with the new IP addresses.

4 Update the `/etc/sysconfig/elasticsearch` for each of the vRealize Automation VA nodes with the new IP addresses.

5 Restart all the vRealize Automation VA Nodes.

You should now be able to startup vRealize Automation.

Start Up vRealize Automation

When you start vRealize Automation from the beginning, such as after a power outage or a controlled shutdown, you must start its components in a specified order.

Prerequisites

Verify that the load balancers that your deployment uses are running.

Procedure

1 Start the MS SQL database machine. If you are using a legacy PostgreSQL standalone database, start that machine as well.

2 (Optional) If you are running a deployment that uses load balancers with health checks, disable the health check before you start the vRealize Automation appliance. Only ping health check should be enabled.

3 Start all instances of vRealize Automation appliance at the same time.

4 Start the primary Web node and wait for the startup to finish.

5 (Optional) If you are running a distributed deployment, start all secondary Web nodes and wait 5 minutes.

6 Start the primary Manager Service node and wait for 2 to 5 minutes, depending on your site configuration.

7 Start the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation proxy agents.

   You can start these components in any order and you do not need to wait for one startup to finish before you start another.

8 If you disabled health checks for your load balancers, reenable them.

9 Verify that the startup succeeded.

a Navigate to the vRealize Automation appliance management console by using its fully qualified domain name, https://*vra-va-hostname.domain.name*:5480/.

b Click the **Services** tab.

c Click the **Refresh** tab to monitor the progress of service startup.

When all services are listed as registered, the system is ready to use.

Validate vRealize Automation

After the restore is complete and you power on the VMs, you must validate that the environment and application functionality is restored.

Procedure

1 Verify that the Messaging server is connected.

a Log in to vRealize Automation appliance Web Interface on https://<*IP of VM*>:5480/ by using root credentials.

b Click the vRealize Automation **Settings > Messaging** tab to verify that the status of the Messaging Server is `Connected`.

2 Verify that the vRealize Automation services are registered.

a Log in to the vRealize Automation appliance Web Interface on https://<*IP of VM*>:5480/ by using root credentials.

b Click the **Services** tab to verify that the vRealize Automation services, except for the IaaS service, have the status of `Registered`.

3 If RabbitMQ fails to register correctly, see KB 2106969 to reset RabbitMQ.

Click vRealize Automation **Settings > Messaging** tab to reset RabbitMQ for every virtual appliance node in the cluster.

4 Verify that your IaaS database host and MSSQL are running.

5 Start the IaaS Website hosts and ensure that IIS server is running.

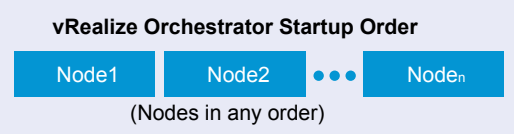
6 Start the IaaS Manager Service hosts and ensure that the VMware Manager Service and Windows service are running on the active node only.

7 Verify that the vRealize Automation IaaS Web Appliance is functioning properly. Enter the following address in the Web browser:
`https://<IP-of-VM-or-LB>/repository/data/managementmodelentities.svc/` and ensure that it is working.

vRealize Orchestrator Restore Process

A system administrator uses backups to restore vRealize Orchestrator to a functional state after a system failure.

After you restore the images from the backup, you must power the nodes on in any order.



The vRealize Orchestrator server status appears as `Service is starting`. The first boot can take 5 to 10 minutes because the server is installing the vRealize Orchestrator plug-in's content in the database tables.

A message states that the service has started successfully.

Validate vRealize Orchestrator

After the restore is complete and you power on the VMs, you must validate that the environment and application functionality is restored.

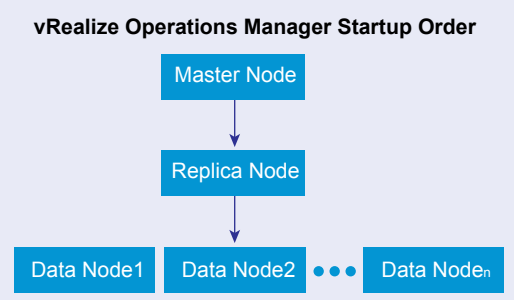
Procedure

1. Log in to the vRealize Orchestrator node 1 appliance configuration Web interface at https://*vRO_node1*:8283.
2. Restart the vRealize Orchestrator service from the Startup options page and wait for the service to start.
3. Log in to the vRealize Orchestrator node 2 appliance configuration Web interface at https://*vRO_node2*:8283.
4. Restart vRealize Orchestrator service from the Startup options page and wait for the service to start.
5. Ensure that your MSSQL database host server is running.
6. Ensure that the two vRealize Orchestrator nodes are working in a cluster mode.
7. Verify that every tab in the configuration is green.
8. Log in to the vRealize Orchestrator server and verify that all the running tasks, policies, and workflows appear and continue running on the home page.

vRealize Operations Manager Restore Process

A system administrator uses backups to restore vRealize Operations Manager to a functional state after a system failure.

You must start the vRealize Operations Manager components in a specifiedd order after the restore is complete.



Common Restore Scenarios

The common restore scenarios for vRealize Operations Manager systems include a full restore of a single-node virtual appliance system and restore of multiple-node virtual appliance clusters.

Single-Node Virtual Appliance

This scenario restores a single node system on the same host.

1. After the restore is complete, power on the VM.

2 Verify that you have set up a static IP address for the node and that the IP address is restored.

3 Log in to the node to verify that all your data is preserved and that all vmware-vcops services are running.

4 If your root password was reset, you must change it now.

For incremental backups, a user must create a cumulative differential policy. Every backup after a full backup is an incremental backup.

NOTE If you restore to another host, you must power off the environment at the original location and start the environment on the new host.

Multiple-Node Virtual Appliance Clusters

This scenario restores multiple-node virtual appliance clusters.

1 After the restore is complete, you must power on the nodes in the following order:

   a master

   b replica

   c data

   d remote collector

   Ensure that each node is online before attempting to start the next component.

2 Verify that you have set up a static IP address for the node and that the IP address is restored.

3 Log in to the administrator interface of the master node and verify that all the nodes are online and running. Log in to each node to verify that all your data is preserved and all of the vmware-vcops services are up and running by using the **`vmware-vcops status`** command.

4 Log in to the administrator interface of the master node.

   a Verify that high availability is enabled. If the **Enable High Availability** button appears, high availability was disabled during the backup and restore process. Enable high availability.

   b Verify that all nodes are collecting metrics.

5 If your root password was reset, you must change it now.

6 (Optional) If a node in a non-high availability cluster does restart, you must take it offline with the administrator interface.

7 (Optional) If the replica node in a high availability cluster does not restart, you must assign a new master-replica node.

8 (Optional) You can execute an incremental backup only if a full backup already exists. After an incremental backup, you can choose to restore to either the full or incremental backup.

NOTE If you restore to another host, you must power off the environment at the original location before starting the environment on the new host.

Verify the Restore of vRealize Operations Manager Systems

After the restore operation of the VM is finished, verify that vRealize Operations Manager is in a functional state.

NOTE Do not power on any vRealize Operations Manager nodes during the restore operation. Wait until the entire cluster restore has finished before you power on any node.

1 For a non-HA cluster, power on the master node followed by the data nodes. For an HA environment, power on the master node followed by the replica node, data nodes, and remote collectors.

2 Use SSH to log in to the vRealize Operations Manager master node to verify the vRealize Operations Manager service status.

   a Use SSH to switch to the vRealize Operations Manager master node and enter the `service vmware-vcops status` command.

```
# service vmware-vcops status
Slice Online-true
admin Role Enabled-true
        vRealize Operations vPostgres Replication Database is running (31810).
        vRealize Operations Gemfire Locator is running (31893).
data Role Enabled-true
        vRealize Operations vPostgres Database is running (32013).
        vRealize Operations Cassandra Distributed Database is running (21062).
        vRealize Operations Analytics is running (32142).
        vRealize Operations Collector is running (32225).
        vRealize Operations API is running (32331).
ui Role Enabled-true
remote collector Role Enabled-false
```

   b Confirm that the admin, data, and UI roles are running.

3 Log in to the administration UI of the master node and verify that all nodes in the cluster are up and collecting data.

   a Open a browser and go to the administration UI of the master node: https://<*Master_Node_IP*>/admin/login.action.

   b Log in as administrator.

   c Verify that each node is in the Online status.

   d Click each node and verify that adapter instances are in the Data receiving status.

4 If the High Availability state indicates **Enabled, degraded** after the restore, one or more nodes are inaccessible, and you must power on the nodes or you must restart the cluster.

   a Open a browser and go to the administration UI of the master node: https://<*Master_Node_IP*>/admin/login.action.

   b Verify that all nodes are in Running state and Online .

      1 If a node is not in Running state and Online, power on the node and start it online.

      2 If all nodes are in Running state and Online, but HA is still **Enabled, degraded**, restart the cluster.

Checking the Restore of vRealize Operations Manager Systems

After you have restored a vRealize Operations Manager system, verify that the system nodes are up and running.

Procedure

1 Power on the master node for a simple cluster, and the master node and replica node for HA clusters.

2 Use SSH to log into the vRealize Operations Manager master node to check the vRealize Operations Manager service status, and run `service vmware-vcops status`.

```
# service vmware-vcops status
Slice Online-true
admin Role Enabled-true
        vRealize Operations vPostgres Replication Database is running (31810).
        vRealize Operations Gemfire Locator is running (31893).
data Role Enabled-true
        vRealize Operations vPostgres Database is running (32013).
        vRealize Operations Cassandra Distributed Database is running (21062).
        vRealize Operations Analytics is running (32142).
        vRealize Operations Collector is running (32225).
        vRealize Operations API is running (32331).
ui Role Enabled-true
remote collector Role Enabled-false
```

3 Confirm that the `admin`, `data`, and `ui` roles are running.

4 Verify that all the nodes in the cluster are up and collecting data. If you have an HA-enabled cluster, verify that HA mode is enabled.

   a In a Web browser, navigate to the vRealize Operations Manager administration interface at https://<*Master_Node_IP*>/admin/login.action.

   b Log in with the admin username and password.

   c Verify that each node is online.

   d Click each node, and verify that the status of adapter instances is Data receiving.

   e Verify that HA mode is enabled. If the cluster is running in degraded mode, restart the cluster.

Change the IP Address of Nodes After Restoring a Cluster on a Remote Host

After you have restored a vRealize Operations Manager cluster to a remote host, change the IP address of the master nodes and data nodes to point to the new host.

Prerequisites

- Verify that the restore job has completed successfully.
- Verify that the datastore on the new host has sufficient capacity for the new cluster.

Procedure

1 Shut down the vRealize Operations Manager cluster at the original location.

2 In the Virtual Appliance Management Interface (VAMI), access the machine from the vCenter console and run the `/opt/vmware/share/vami/vami_set_network eth0 STATICV4` *new IP netmask gateway* to change the IP address for each node in the cluster.

   For example:

```
/opt/vmware/share/vami/vami_set_network
                eth0 STATICV4 10.145.152.170 255.255.252.0 10.145.155.253
```

3 After the command runs successfully, restart the network, reboot each node, and power on the remote collector node.

4 Use SSH to access the master, data, and remote collector nodes, and run the `$VMWARE_PYTHON_BIN /usr/lib/vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsConfigureRoles.py --action=bringSliceOffline --offlineReason=restore cluster` command to take the cluster offline.

5 Update the CaSA database with the new IP address first on the master nodes, and then on the data nodes.

   a Run the `vmware-casa stop` command to stop the CaSA service.

   b Open the `/storage/db/casa/webapp/hsqldb/casa.db.script` file for editing, and replace all instances of the old IP address and with the new IP address.

   c Run the `vmware-casa start` command to start the CaSA service.

6 In the following configuration files, use a text editor to replace all instances of the old IP address with the new IP address.

   - `/usr/lib/vmware-vcopssuite/utilities/sliceConfiguration/data/roleState.properties`.
   - `/usr/lib/vmware-vcops/user/conf/gemfire.properties`.
   - `/usr/lib/vmware-vcops/user/conf/gemfire.locator.properties`. This configuration file only runs on the master node. Edit the `locater` parameter.
   - `/usr/lib/vmware-vcops/user/conf/gemfire.native.properties`.
   - `/usr/lib/vmware-vcops/user/conf/persistence/persistence.properties`.

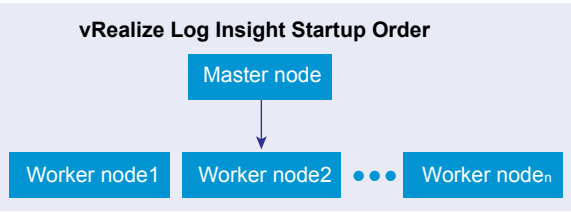
7 Navigate to the `/usr/lib/vmware-vcops/user/conf/cassandra/` directory, and edit the `cassandra.yaml` file so that the `seeds` parameter points to the new IP address of the master node, and the `listen_address` and `broadcast_rpc_address` point to the IP addresses of the data nodes.

8 Log in to the vRealize Operations Manager administration interface, and bring the cluster online.

vRealize Log Insight Restore Process

A system administrator uses backups to restore vRealize Log Insight to a functional state after a system failure.

You must start the master node for the vRealize Log Insight, followed by worker nodes in any order after the restore is complete.



Restore Guidelines

Use the following information for restoring and validating after a restore operation.

- Verify that restored nodes are in a powered-off state. Restore the nodes in a specific order and apply manual configuration changes where applicable.
- Verify that the vRealize Log Insight master node is restored first before restoring worker nodes. Worker nodes can be restored in any order.
- You can restore the VMs to the same host, to a different host on the same data center, or to a different host on a target remote data center, depending on the backup tool used.
  - Unless the vRealize Log Insight cluster is completely shut down and inaccessible, the cluster instances are powered off before you restore the cluster to a new site.
  - Verify that split-brain behavior does not occur when the same IP addresses and FQDNs are used on the recovery site. Verify that no one is unintentionally using a partially working cluster on the primary site.
- During an outage, recover the vRealize Log Insight cluster as soon as possible.
- When a successful restoration is finished, perform a quick spot check of the cluster that was restored.

Post-Recovery Configuration Change Guidelines

Depending on the recovery target and IP customizations applied during the backup configuration, manual configuration changes are required to one or more vRealize Log Insight nodes before the restored site can become fully functional.

Recovering to the Same Host

You can restore vRealize Log Insight cluster to the same host by using any back up tool.

- All network, IP, and FQDN settings that are used for the production environment should be preserved in the restored site.
- The original copy of the cluster is overwritten with the restored version unless a new name is provided to the virtual machine, during the restore process.
- If the same IP addresses and FQDNs are used for the restored cluster nodes as per the default settings, power down the existing cluster before beginning the restore.
- After a successful restoration and validation, delete the old copy to conserve resources and to prevent potential issues.

Recovering to a Different Host

You must perform manual configuration on vRealize Log Insight, if you are restoring to a different host cluster. For information about changes that are specific to vRealize Log Insight 3.3.0 versions, see "Restoring to a Different Host," on page 43. It is assumed that the restored vRealize Log Insight nodes have been assigned different IP addresses and FQDNs than their source counterparts from which a backup was taken.

Recovering vRealize Log Insight Forwarders

The manual instructions for recovering vRealize Log Insight forwarders are the same as that of the vRealize Log Insight server as described above.

Recovering vRealize Log Insight Agents

If the complete agent OS is backed up, follow the tool-specific workflow to recover the agent OS.

- If agent configuration is made on the client side, that is on agent OS, replace the agent.ini using the backup copy.
- If configuration changes are made on the server side, that is vRealize Log Insight master node , no backup and recovery is required for the agent virtual machines.

Confirming the Restoration

You must confirm that all restored vRealize Log Insight clusters are fully functional.

- Verify that you can access the vRealize Log Insight user interface using the Internal Load Balancer (ILB) IP address or FQDN (if configured) as well as access all individual cluster nodes using respective IP addresses or FQDNs.
- From the vRealize Log Insight Administration page:
  - Verify the status of cluster nodes from the cluster page and make sure the ILB, if configured, is also in an active state.
  - Verify the vSphere integration. If required, reconfigure the integration. This occurs when the ILB and/or the master node IP address or FQDN is changed post-recovery.
  - Verify the vRealize Operations Manager integration and reconfigure again if needed.
  - Verify that all content packs and UI features are functioning correctly.
  - Verify that vRealize Log Insight forwarders and agents, if configured, are functioning correctly.
- Verify that other key features of vRealize Log Insight are functioning as expected.

Restoring to a Different Host

When you restore your system to a different host, you should make some configuration changes on the vRealize Log Insight cluster.

The configuration changes listed are specific to vRealize Log Insight 2.5 and 3.0. It is assumed that the restored vRealize Log Insight nodes are assigned different IP addresses and FQDNs than their source counterparts from which the backup was taken.

Procedure

1 List all new IP addresses and FQDNs that were assigned to each vRealize Log Insight node.

2 Perform the following configuration changes on the master node:

a Power on the master node, if it is not ON.

NOTE Steps b through e are applicable for vRealize Log Insight 2.5. You can not make changes to the configuration files directly from the appliance console for vRealize Log Insight 3.0 and higher. To make changes to the internal configuration options by using the web UI interface for vRealize Log Insight 3.0 and higher, refer to the Knowledge Base article KB 2123058.

---

b Use SSH to connect as a root user to the node's virtual appliance.

c If the vRealize Log Insight service is running, stop the service first by running this command `service loginsight stop`.

d Run `cd /storage/core/loginsight/config`

e Run `cp loginsight-config.xml#<n> backup-loginsight-config.xml` where <n> represents the largest number that is automatically suffixed to `loginsight-config.xml` during configuration changes.

f Open the copied version of the configuration file in your favorite editor or in the vRealize Log Insight 3.0 web UI and look for lines that resemble the following lines. This configuration change is applicable to both vRealize Log Insight 2.5 and 3.0.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

In this code snippet, there are three nodes. The first one is the master node which shows `<service-group name=standalone>` and the remaining two nodes are worker nodes and show `<service-group name="workernode">`.

g For the master node, in the newly recovered environment, veerify if the DNS entry that was used in the pre-recovery environment can be reused.

- If the DNS entry can be reused, you only need to update the DNS entry to point to the new IP address of the master node.
- If the DNS entry cannot be reused, replace the master node entry with the new DNS name, pointing to the new IP address.
- If the DNS name cannot be assigned, as a last option, update the configuration entry with the new IP address.

h Update the worker node IP addresses to reflect the new IP addresses.

i In the same configuration file, look for entries that represent NTP, SMTP and database, and appenders sections.

This applies to vRealize Log Insight 2.5 and 3.0.

NOTE The <logging><appenders>...</appenders></logging> section is applicable only to the vRealize Log Insight 2.5 and is not available for vRealize Log Insight 3.0.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>

<logging>
  <appenders>
    <appender name="REMOTE"
class="com.vmware.loginsight.commons.logging.ThriftSocketAppender">
      <param name="RemoteHost" value="vdli-node1.domain.com" />
    </appender>
  </appenders>
</logging>
```

- If the configured NTP server values are not valid in the new environment, update these in the <ntp>...</ntp> section.
- If the configured SMTP server values are not valid in the new environment, update these in the <smtp>...</smtp> section.
- Optionally, change the default-sender value in the SMTP section. The value can be any value, but as a good practice, you should represent the source from where the email was sent.
- In the <database>..</database> section, change the host value to point to the master node FQDN or IP address.
- In the <logging><appenders>...</appenders></logging> section, change the parameter value for RemoteHost to reflect the new master node FQDN or IP address.

j In the same configuration file, update the vRealize Log Insight ILB configuration section

For a vRealize Log Insight 3.0 appliance,

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

For a vRealize Log Insight 2.5 appliance,

```
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="192.168.1.75" />
  <layer4-enabled value="true" />
</load-balancer>
```

k Under the `<load-balancer>...</load-balancer>` section, update the `high-availability-ip` value if it is different from the current setting.

l In the vRealize Log Insight 3.0, make sure to also update the FQDN of the load balancer.

m Rename the updated configuration file to finish the changes.

NOTE This step is applicable for vRealize Log Insight 2.5 only. In vRealize Log Insight 3.0 the changes are made through web UI.

Run : `mv backup-loginsight-config.xml loginsight-config.xml#<n+1>` where `n` represents the current maximum number suffixed to the `loginsight-config.xml` files.

n For vRealize Log Insight 2.5, restart the vRealize Log Insight service and run : `service loginsight start`.

NOTE For vRealize Log Insight 3.0, this can be achieved from the web UI by going to the Cluster tab on the Administration page. For each node listed, select its hostname or IP address to open the details panel and click **Restart Log Insight**. The configuration changes are automatically applied to all cluster nodes.

---

o Wait for two minutes after the vRealize Log Insight service starts in order to give enough time for Cassandra services to come up before bringing other worker nodes online.

NOTE You can skip steps 3 to 9 for vRealize Log Insight 3.0. These steps are only applicable for vRealize Log Insight 2.5.

---

3 SSH onto the first worker node using root credentials.

4 Stop the vRealize Log Insight service and run : `service loginsight stop`.

5 Copy the latest `loginsight-conig.xml` file from the master node to the worker node.

6 On the worker node, run : `scp root@[master-node-ip]:/storage/core/loginsight/config/loginsight-config.xml#<n> /storage/core/loginsight/config/`

7 Run : `service loginsight start`.

8 Wait for 2 minutes after the vRealize Log Insight service starts in order to give enough time for Cassandra service to start completely.

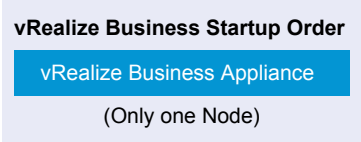
9 Repeat the steps for each worker node.

vRealize Business Restore Process

You can restore vRealize Business to the last full or incremental backup.

If a failure occurs, a system administrator must restore vRealize Business Standard to a functional state.

Verify that the vRealize Automation system is running before you start the vRealize Business VM.



NOTE If you change the certificate of vRealize Automation, you must reregister vRealize Business with vRealize Automation.

Validate vRealize Business

1 Log in to https://<VRB IP>:5480/ by using root credentials and ensure that no configuration has changed after the restore.

2 Verify that vRealize Automation is in the Registered status in vRealize Business.

3 Log in to vRealize Automation and verify that the cost profiles that are set to Automatic continue to pull the rates from vRealize Business.

4 Log in to vRealize Automation and verify that the **Business Management** tab appears.

5 Log in to vRealize Automation and verify that vRealize Business is collecting data after the restore and that the cost of the VMs is correctly calculated. This cost should be the same as before the backup.

6 Provision any VM by using vRealize Orchestrator or vRealize Automation and validate that vRealize Business is able to calculate the VM costs

7 If you are adding more endpoints to vRealize Automation, vRealize Business should be able to calculate these endpoints managed VM cost.

Restore vRealize Suite by Using NetBackup

5

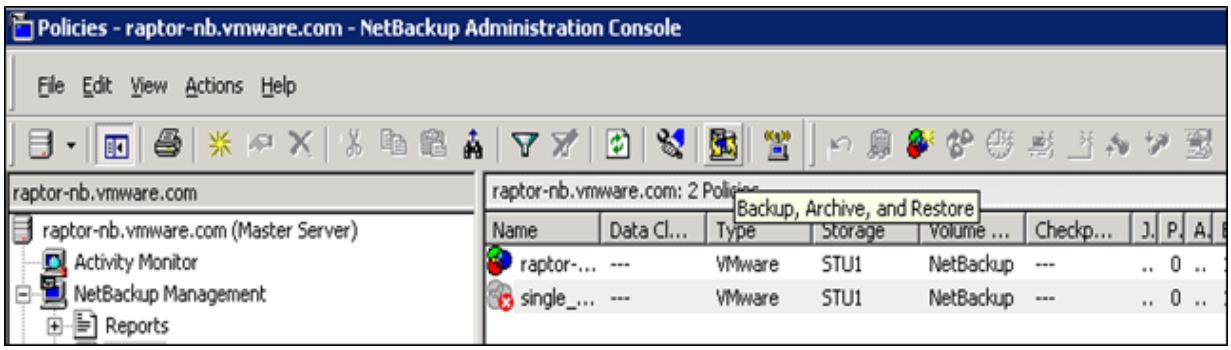
You can restore the backed up data for vRealize Suite components by using NetBackup.

Prerequisites

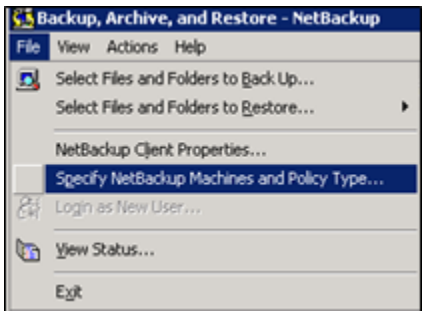
Verify that a backup of the vRealize Suite components is available.

Procedure

1 Start **NetBackup Administration Console** and click the **Backup, Archive, and Restore** icon from the toolbar.



2 In the Backup, Archive, and Restore utility window, select **File > Specify NetBackup Machines and Policy Types**.



3 In the Specify NetBackup Machines and Policy Type window, configure the NetBackup machines and policy type.

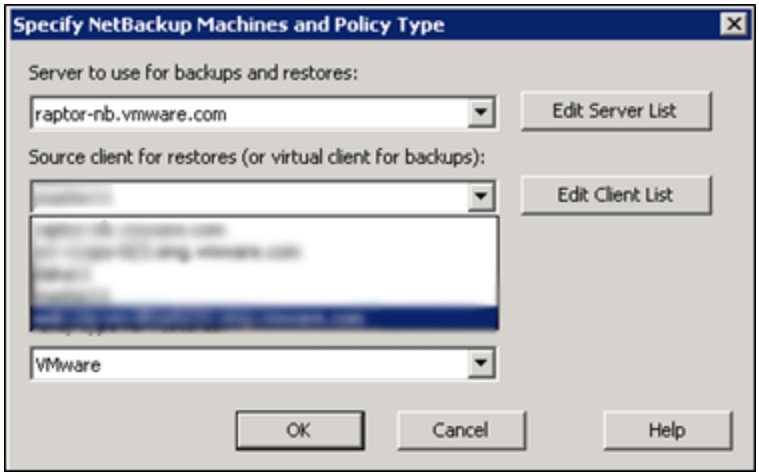
a In **Server to use for backups and restores**, select the IP address or FQDN of the system that hosts NetBackup Master server. If the IP address or FQDN you want is not listed, click **Edit Server List**, add the IP address or FQDN, and select it.

b In **Source client for restores (or virtual client for backups)**, select the client name from the drop-down menu. If the client that was backed up is not listed, click **Edit Client List**, add the VM name, and select it.

c In **Destination client for restores**, enter the destination server name on which the VMs should be restored. This destination selection is not final.

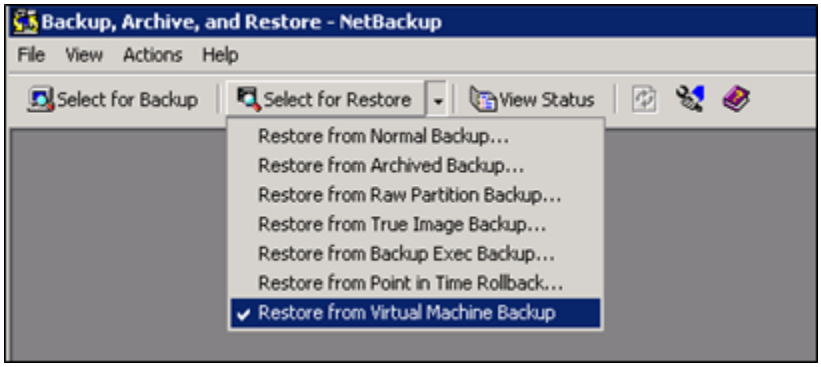
d In **Policy type**, select the same policy type that you configured for backup. To restore a VM configured with VMware policy, select **VMware**.

e Click **OK**.

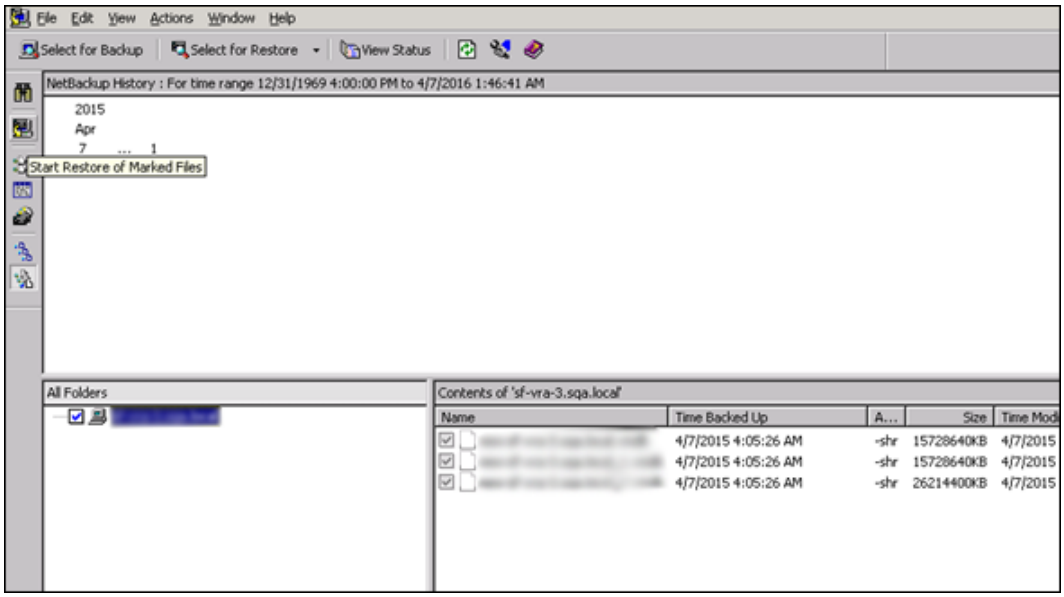


4 In the Backup, Archive, and Restore window, click **Select for Restore > Restore from Virtual Machine Backup**.

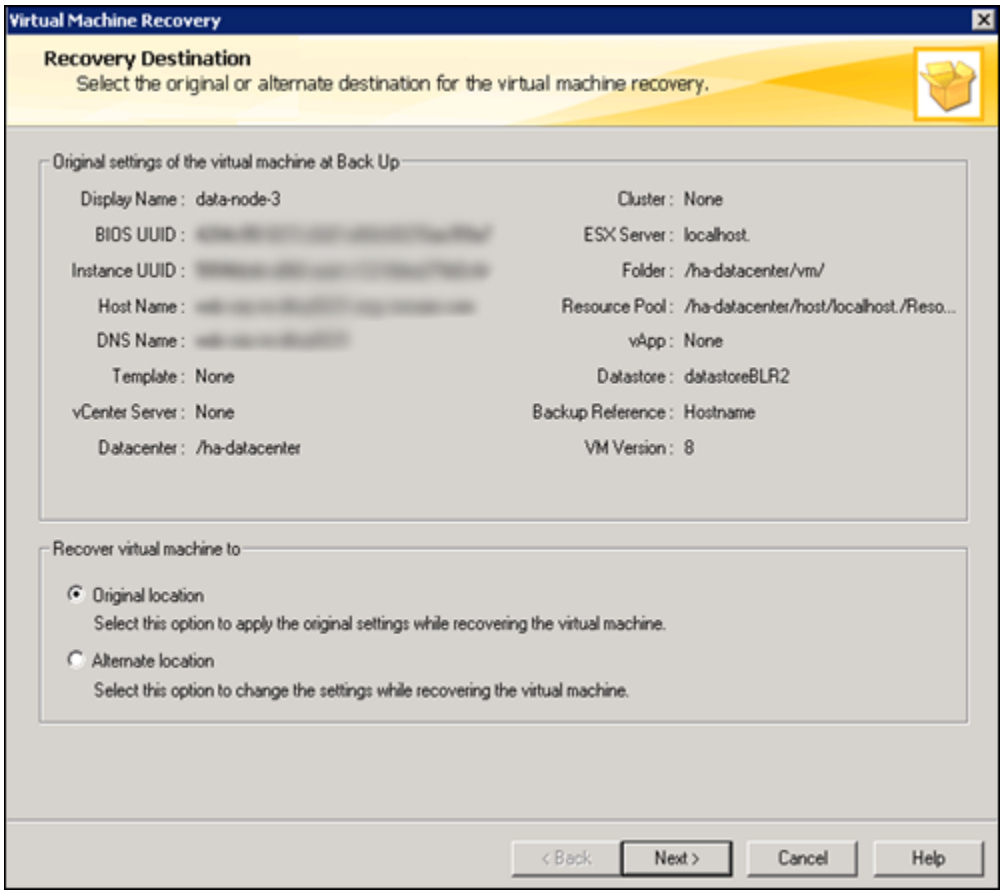
The **NetBackup History** is displayed.



5 Select the file that you want to restore and click the **Start Restore of Marked Files** icon from the left toolbar. To restore a complete VM, select all files listed in the lower-right panel.



6 In the **Recovery Destination** window, select the original or alternate location for the VM to restore and click **Next**.



7 Select the **NetBackup Recovery Host** and the **Transport modes** you want, and click **Next**.

8 In the Virtual Machine Options window, select the virtual machine and disk provisioning options and click **Next**.

a For **Virtual machine options**, select the **Restore BIOS UUID "<exisiting UUID>" instead of creating a new UUID** option.

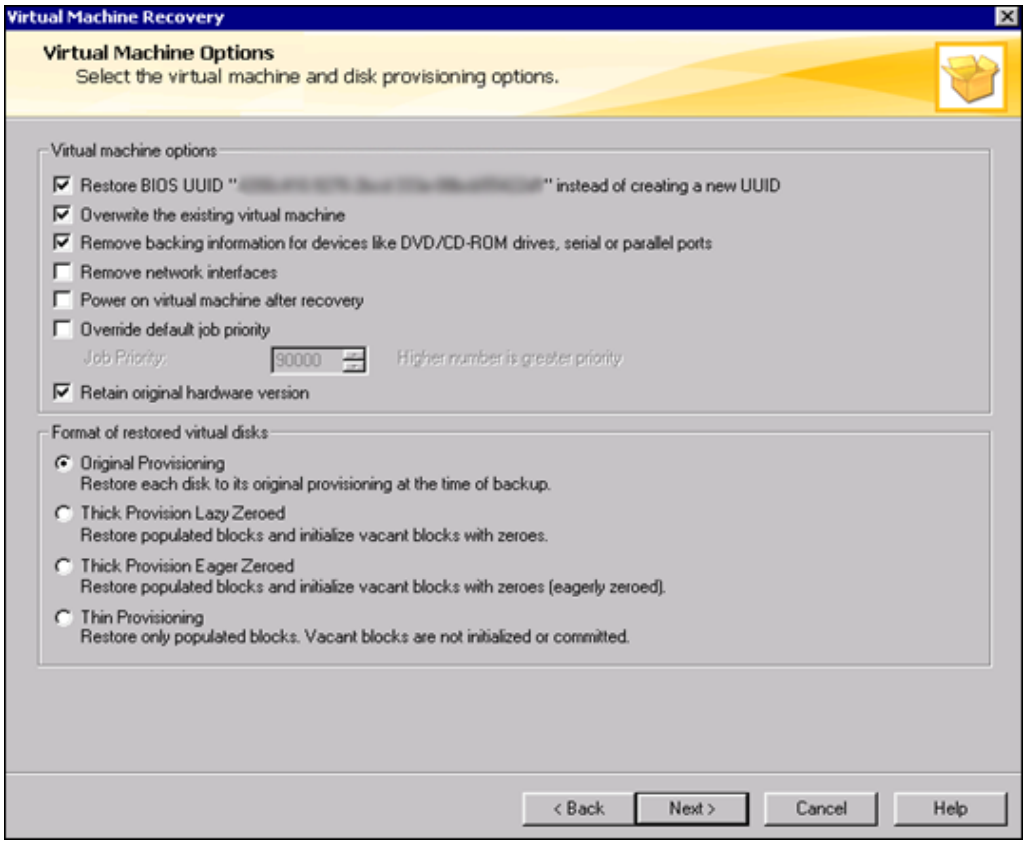
b Select the **Overwrite the existing virtual machine** option.

c Select the **Remove backing information for devices like DVD/CD-ROm drives, serial or parallel ports** option.

d Ensure that **Power on virtual machine after recovery** option is not selected.

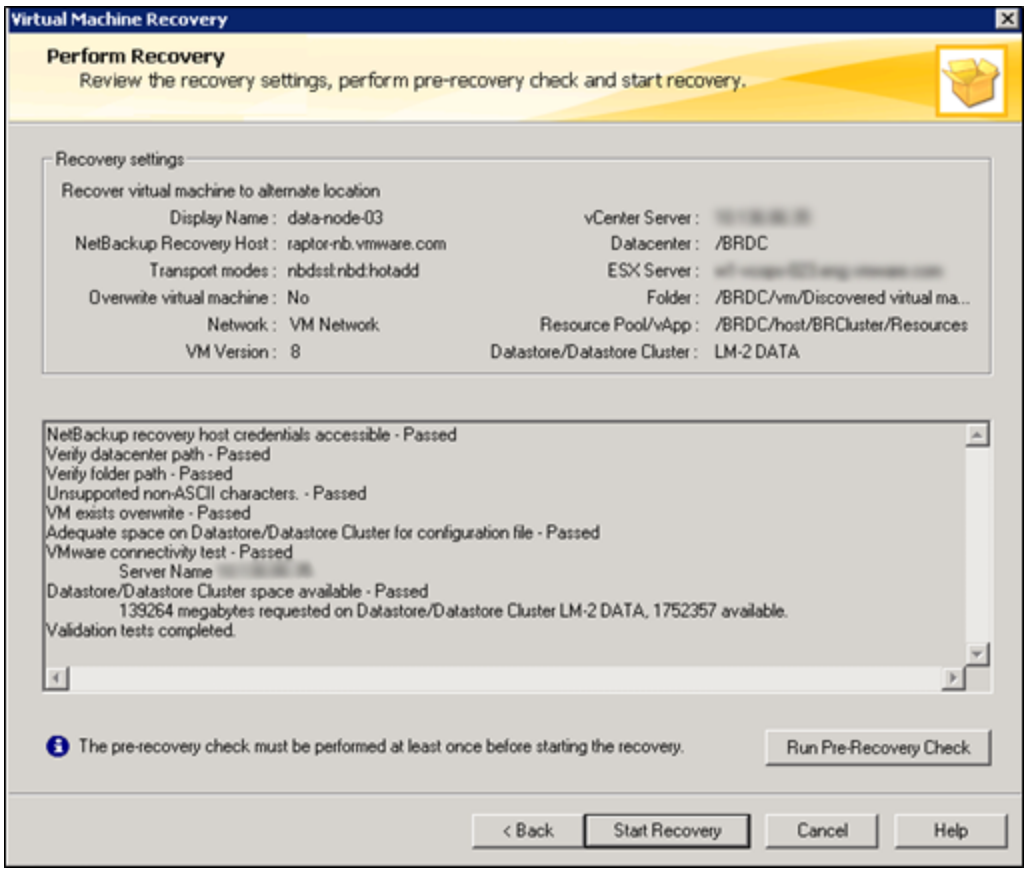
e For **Format of restored virtual disks**, select **Original Provisioning** to restore each disk to its original provisioning at the time of backup.

f Click **Next**.



9 In the **Perform Recovery** window, review the **Recovery settings** that you configured and click **Run Pre-Recovery Check**.

10 After the pre-recovery check is finished, click **Start Recovery** to restore the backup of the VMs.



11 Repeat the restore process for every VM that you want to restore.

The time it takes to restore can vary from a few minutes to hours, depending on the environment settings. After the restore is finished, start the cluster and verify that the system is working correctly. After you restore your vRealize Suite components, refer to the validation process for each component in Chapter 4, “Restoring, Powering On, and Validating vRealize Suite,” on page 31 to verify that your system is working correctly.

Index