Veeam Backup & Replication 4.0 for VMware

Evaluator's Guide
November, 2009

Copyright © 2005-2009 Veeam Software Inc. All rights reserved worldwide.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software Inc (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Important: Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

CONTENTS

What's New in v4.0

Veeam Backup & Replication 4.0 is a major update to Veeam's industry-leading data protection and disaster recovery solution for VMware vSphere that combines backup and replication in a single product. Improvements in version 4.0 have been made in the following areas:

Enterprise management. A new Enterprise Management Server allows distributed enterprises to manage multiple Veeam Backup & Replication installations from a single web console. The ability to easily manage multiple instances of Veeam Backup & Replication allows you to deploy the backup solution and manage backups and restores according to your administrative, business, geographical and security requirements and boundaries.

Native vSphere and vStorage support.

- Native support for thin-provisioned disks for faster full VM backups and restores, to reduce the amount of storage required to host your production VMs.
- Ability to leverage ESX4 changed block tracking for lightning-fast incremental backup.
- Support for the new vStorage API. The VMware vStorage API for Data Recovery is VMware Consolidated Backup (VCB) successor and the preferred API for VMware vSphere backup.
- Support for virtual applications (vApp).

Near-real-time replication. Veeam Backup & Replication 4.0 now leverages the new vSphere ESX(i) 4 functionality to provide much faster replication cycles. You can now schedule replication jobs to run as often as every few minutes, allowing you to achieve very low recovery point objectives in case of disaster, thus providing near-CDP (continuous data protection) at a fraction of the cost.

Other Enhancements. v4 offers numerous additional enhancements requested by our customers that make Veeam Backup & Replication even easier and more convenient to use, such as: hot VM copy, PowerShell access, safe snapshot removal, backup storage disk space monitoring, replica seeding and a lot more. Learn more about new features in Veeam Backup & Replication v.4.

Reference Environment

This section describes minimum hardware and software requirements to a test environment that will be used for evaluation of Veeam Backup & Replication.

Virtual Infrastructure Platform

VMware vSphere 4 or VMware Infrastructure 3 (VI3)

VMware Infrastructure

(Optional) Virtual Center 2.x or 4.0.
(Optional) VMware Consolidated Backup (VCB) framework 1.0 or later (required if you are planning to perform VCB-enabled backup). Ensure that your VCB framework is compatible with your ESX server version (refer to the official compatibility matrix).

ESX Hosts

ESX(i) 3.x or higher. ESXi free is not supported.

Virtual Machines

Hardware	All types and versions of virtual hardware are supported, except physical RDM (raw device mapping) and Independent disks.
OS	Virtual machines running any operating system supported by VMware.
Software	(Optional) For Microsoft Windows VSS option, VMware Tools and all latest service packs and patches installed.

Backup Target

Hardware	Processor: x86/x64. Memory 256 MB RAM. Sufficient hard disk space required to store backup files.
OS	Microsoft Windows. All major Linux distributions. ESX 3.0 or later. ESXi is not supported.

Replication Target

ESX Server 3.x or later. Replication to ESXi is supported in v4.1.

Veeam Backup & Replication Console

Hardware	Processor: x86/x64. Memory: 1024 MB (2048 MB RAM when using local SQL Express installation). Hard disk space: 100 MB.
OS	Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 or Windows 7. All latest security updates should be installed.
Software	Microsoft Installer 3.1 VMware Player 2.5 (if you are planning to use FLR plug-in to restore files from VMs using other guest file systems than NTFS, FAT and FAT32)

GETTING STARTED

Before you start evaluating Veeam Backup & Replication, make sure that your test lab meets requirements outlined above, Veeam Backup & Replication is properly installed and ports used by Veeam Backup & Replication are open.

Install Veeam Backup & Replication

Prerequisites

- You should have Local Administrator permissions on the server where Veeam Backup & Replication is installed.
- Veeam Backup & Replication uses an SQL Server instance installed locally or remotely. If you do not have one, the setup will install SQL Server 2005 Express SP3.
- Veeam Backup & Replication 4.0 requires .NET Framework 2.0 SP1. If it is not available, the setup will install it.

Procedure

1. Download the latest version of Veeam Backup & Replication from: http://www.veeam.com/vmware-esx-backup/download.html.
2. Run the *VeeamBackup_x86/x64.exe* setup file. If you are planning to perform VCB-enabled backup, install Veeam Backup & Replication on the VCB proxy server. If you are planning to back up VMs residing on NFS, install Veeam Backup & Replication on a virtual machine within the same ESX cluster.
3. Follow the steps of the installation wizard.
4. At the **Provide License** step of the wizard, specify a path to the license file that was sent to you after you downloaded the product from the web site.
5. At the **SQL Server Instance** step of the wizard, choose to install a new instance of SQL Server or use an existing one (either local or remote). If you select to use an existing SQL server, provide credentials of a user who has database owner rights.
6. Once installation is complete, select **Programs > Veeam > Veeam Backup and FastSCP** from the **Start** menu to make sure Veeam Backup & Replication is properly installed.

BACKUP

This section outlines recommended steps you should take to successfully perform backup of VMs or VM containers.

Overview

Designed specifically for virtualization, Veeam Backup & Replication performs an image-level backup of VMs running in VMware ESX or ESXi environment. Working through VMware APIs, Veeam Backup & Replication can conduct full and incremental backups of VMs residing on SAN, NFS, or Local Storage. Three backup modes are available: vStorage APIs, VCB, or in-built network mode.

Backup from SAN

For backup of VMs residing on SAN, the SAN mode of VMware vStorage API mode is a recommended method. In this mode, Veeam Backup & Replication uses VMware vStorage APIs for Data Protection to access VMware virtual disk storage and copy virtual disk data to the target directly through SAN, and thus enable LAN-free backup.

To be able to perform backup in the VMware vStorage API mode, you should have the Veeam Backup & Replication server directly connected to SAN.

Use of vStorage API mode along with Changed Block Tracking results in extremely fast backup performance (above 600-700 MB/s) according to the customers' feedback on 4.0.

Backup from NFS

Customers using NFS shared storages can achieve greater performance with the new Virtual Appliance transport mode available in Veeam Backup & Replication. In this mode, VM data is retrieved directly from storage through the ESX I/O stack, instead of going through the network, which improves performance.

This mode is recommended and can only be used if Veeam Backup & Replication is installed on a VM running on an ESX within the same cluster. Only one appliance is needed per cluster.

Backup from Local Storage

For environments that do not have shared storages, network backup is a recommended method. At network backup, data of a VM is retrieved directly from the ESX host through the local area network bypassing the Veeam Backup & Replication server.

By default, Veeam Backup & Replication uses a service console agent to achieve the best performance. If you are not using a shared storage or need to perform backup to a remote server, Veeam service console agent backup mode is the most efficient approach due to empty block removal, network traffic compression and "direct-to-target" architecture.

If the service console is not available, Veeam Backup & Replication uses an agentless mode. Agentless backup requires support of ESXi that has service console access restricted, and provides better stability with full ESX due to no 3rd party agents running in the service console.

Backup in the VCB Environment

If you have invested in VCB infrastructure, Veeam Backup & Replication offers full VCB support for backing up or replicating from both ESX and ESXi servers.

In case the VCB-enabled backup method is used, Veeam Agents are deployed on the VCB proxy server — a physical server running Windows 2003/2008. As a result, backup processes are moved to the VCB proxy, offloading the ESX server. Due to its proprietary "VCB on-the-fly" technology, Veeam Backup & Replication 4.0 doesn't require extra space on the VCB proxy for VM images.

Typical Veeam Backup performance in VCB SAN mode on FC4 hardware is 100-150MB/s, allowing for significantly smaller backup window (*note that backup speed heavily depends on your virtual infrastructure*).

Add Source and Target Servers

Before you start creating a backup job, you should add to the Veeam Backup & Replication console source and target servers that will be involved in backup.

You can perform backup from/to the next sources/targets:

Backup source: ESX/ESXi version 3.x and higher.

Backup target:

- Storage Area Network devices (the Veeam Backup server must be connected directly into SAN fabric).
- Network Attached Storage devices able to represent itself as CIFS (direct operation) or NFS share (storage must be mounted on ESX host or Linux server).
- Direct Attached Storage connected to the Veeam Backup server, including USB drives.
- Any x86/x64 Windows or Linux based computer (or ESX host).

If you are planning to use an ESX server being a part of VirtualCenter hierarchy, we recommend that you add VirtualCenter instead of separate ESX servers to provide more flexibility at work.

Procedure

1. Run Veeam Backup & Replication by selecting **Programs > Veeam > Veeam Backup and FastSCP** from the **Start** menu.
2. Click the **Add Server** button on the toolbar.
3. Select a necessary type of server (ESX, VirtualCenter or Linux) and follow the wizard steps.
4. At the last step of the wizard, select **Connect when I click Finish** and click **Finish**.
5. Expand the **Servers** node in the management tree to check if the server is added successfully.

Create a Backup Job

To perform backup of a VM, you should create a backup job. A backup jog aggregates all settings and policies of backup to be performed such as backup mode and type of data transport, backed up objects, destination, scheduling settings, retention policy and so on.

Procedure

1. Click the **Backup** button on the toolbar.
2. Specify a name for the created backup job and job details.
3. Click **Next**.

Select Backup Mode

Depending on the type of storage you use, select a backup mode and an appropriate data transport method.

Exclude VMs, VM Disks and VM Templates from Backup

Veeam Backup & Replication provides the ability to exclude specific VMs or VI objects, VM templates from your container-based backup jobs, and select what VM disks should be backed up.

Procedure

1. Click the **Exclusions** button.
2. On the **Excludes** tab, click the **Add** button to select objects that should be excluded from backup (for example, to exclude some VMs from a container that you want to back up).
3. On the **VM disks** tab, select VM disks that should be backed up. This functionality may be useful if you are performing an application's backup using legacy agents, and thus only want to perform VM's system drive backup, or in similar scenarios.
4. If you exclude some VM disks from backup, select the **Remove excluded disks from VM configuration** to automatically modify VMX file with regard to selected VM disks. With this option selected, you will be able to power on a restored VM without a necessity to edit its configuration.
5. On the **VM Templates** tab, select the **Backup VM Templates** check box to include VM templates into backup. Select the **Exclude VMs from incremental backup** check box to include VM templates into full backup only – this will fasten backup process and reduce size of incremental backups.
6. Click **OK**.
7. Click the **Recalculate** button to get the total size of backed up objects. When multiple machines are backed up, Veeam Backup & Replication uses the deduplication technique. De-duplication brings significant storage costs savings by providing up to 90% reduction of backup size when backing up VMs made from the same template. De-duplication is performed on the source host automatically during backup.
8. Click **Next**.

Specify Backup Destination

You can store a created backup to the following targets: Storage Area Network devices; Network Attached Storage devices; Direct Attached Storage, including USB drives and x86/x64 Windows or Linux based computer (or ESX host).

Procedure

1. From the **Destination** list, select a backup target. Check if you have sufficient space on the target: click the **Host Properties…** button. On the **General** tab, click the **Populate** button to see storage details.
2. Click the **Browse…** button next to **Path to folder** field and select a folder where created backup should be stored.
3. Click the **Check Space** button on the right to see how much free space is available on the backup destination, and how much space you will require to store a full backup and its increments.
4. Enter a name of the backup file.

Specify General Backup Settings

Procedure

1. Click the **Advanced…** button.
2. Select the **Enable email notification for this job** check box. You will receive an e-mail with details on job performance when it completes. To specify e-mail notification settings, select **Tools > Options** from the main menu.
3. Select the **Enable VMware tools quiescence** check box. This option helps create a transactionally consistent backup of running VMs. If VMs runs highly transactional applications clear the check box to avoid risks of application failure. For applications like MS Exchange, SQL, Active Directory we recommend using the VSS option rather than VMware tools quiescence.
4. Select the **Enable automatic backup integrity checks** check box to periodically verify integrity of a backup file and avoid a situation when a full backup is corrupted, making all further increments corrupted, too.
5. Veeam Backup & Replication provides tape integration via a post-job script option. Select the **Run the following command** check box and specify a path to an executable script file. Schedule execution of scripts on specific days or at some time interval.

Specify Compression Settings

Veeam Backup & Replication provides traffic compression and empty block removal, allowing for dramatic reduction of network traffic. Backup compression is offloaded to the Linux-based backup storage file servers, which reduces workload on production ESX hosts.

Procedure

1. Click the **Compression** tab.
2. Select one of three compression levels: *Low* - for low load on ESX CPU; *Optimal* – for the best compression to performance ratio; *Best* – if Veeam Backup & Replication is installed on a computer with multi-core CPU; If backup files are to be stored on devices with hardware deduplication, select *None*.

Specify Changed Block Tracking Settings

Veeam Backup & Replication leverages Changed Block Tracking — a feature of vStorage APIs that minimizes CPU and memory resource consumption on the ESX host up to several times. Veeam Backup & Replication tracks and processes only changed data blocks, thus making the process of incremental backup much faster. For example, if a VM only had 5 percent change since the last backup, the incremental backup time will be 20 times faster.

Procedure

1. Click the **vSphere** tab.
2. Select the **Use changed block tracking data** check box.
3. Select the **Enable changed block tracking for all processed VMs** to use this option for VMs for which changed block tracking is disabled on the ESX server.

Specify Backup Policies and Attributes

Procedure

1. Click the **Backup** tab.
2. Specify backup retention policy - number of reverse increments (restore points) that should be stored.
3. Select the **Perform full backup on these days** option to configure a job for performing full backups instead of forever-incremental synthetic backup. This option will help you obey regulations and policies requiring that full backup is performed every time, or with certain periodicity. Creating new full backup resets the chain of rollback files, so all subsequent incremental backups processing will use the new full backup. A previously used synthetic full backup file will remain on storage until it is automatically deleted by backup retention policy, just like rollback files.
4. Select the **Safe snapshot removal** option to prevent production applications from timing out during helper snapshot commit. This option will allow you to perform hot image-level backups of large VMs with high disk I/O loads without affecting production applications. Veeam Backup & Replication offers a procedure of safe snapshot removal which includes creating an additional snapshot in cases when the "main" snapshot size is above the specified threshold. An additional snapshot is used to host writes while the "main" snapshot is being deleted. This ensures that a consolidation helper snapshot does not grow large.
5. Veeam Backup & Replication can optionally update backup information in a VM's custom attribute upon successful backup. Information includes backup date and time, backup console name, and path to the backup file containing the specific VM. Select the **Set successful backup details to this VM attribute** check box to write to a VM custom attribute information about successfully performed backup and data on backup results. Enter the name of an attribute to the field below: if it does not exist, it will be created.
6. Click **Next**.

Enable VSS Integration

Veeam Backup & Replication utilizes the Windows Volume Shadow Copy Service (VSS) that ensures consistent backup of VSS-aware application running within your virtual machines (domain controllers, databases and other applications) without shutting them down. This option allows creating a transactionally consistent backup image of a VM, which, in contrast to a crash-consistent backup image, ensures successful VM recovery, as well as proper recovery of all applications installed on the VM without any data loss.

Prerequisites

- Microsoft Windows VSS option is supported on Windows XP, Windows 2003, Windows 2008, Windows 2008 R2 and Windows 7.
- VM guest OS should have VMware Tools and all latest service packs and patches installed.

Procedure

1. Select the **Enable Veeam VSS integration** check box. Select **Continue backup even if Veeam VSS quiescence fails** check box. In case VSS fails, VMs will be processed with the **VMware tools quiescence** option (if it is enabled). If VMware tools quiescence is not enabled, Veeam Backup & Replication will create a crash-consistent backup.
2. Specify VSS agent credentials – user name and password.
3. Click **Next**.

Schedule a Backup Job

You can perform a backup job manually or schedule it.

Procedure

1. Select the **Run this job automatically** check box to specify job schedule. If you do not select this check box, the job will be saved and you will have to run it manually.
2. Select the schedule type: on specific week days or at some time interval.
3. Select the **Retry VM processing** check box. During the retry cycle, only VMs failed during the main backup cycle are processed. In case of agentless network backup retry, alternate data access mechanism featuring granular block-level retry is leveraged, allowing you to perform network backup over unreliable network connections.
4. Click **Next**.
5. Select the **Run the job when I click Finish** check box and click **Finish**. The job will be started.

View Real-Time Job Statistics

When the job is being run, Veeam Backup & Replication allows viewing job statistics in the real-time mode. Job statistics provides detailed data on a job that is currently running: job status, start and end time, total number of processed and failed objects, size, performance rate and details of the session performance (for example, errors that have occurred in the process of operation).

Procedure

1. Click the **Jobs** node in the management tree.
2. Right-click the job you created and select **Realtime Statistics** from the shortcut menu. Now you can track the job performance as it runs.

Check Backup Results

When full backup is performed, the resulting backup .vbk file is written to the target host.

Procedure

1. Open the folder on the target host that you selected to store a backup file.
2. Check if it has a .vbk file.
3. Click the **Backups** node in the management tree. Right-click a necessary backup in the list and select **Properties**. Check properties of a created backup file: initial data size, backup size, compression and de-duplication ratios.

Perform Incremental Backup

When incremental backup is performed, Veeam Backup & Replication 4.0 rebuilds this full backup to the most recent state of a VM and uses historical data to calculate a reverse increment. Obtained changes are backed up and saved as a service .vrb file next to the rebuilt full backup .vbk file.

Procedure

1. Click the **Jobs** node in the management tree.
2. Select the job that you created.
3. Click the **Start** button on the toolbar. The job will be started.
4. After the job is completed, open the folder on the target host that you selected to store a backup file.
5. Check if it has a .vbr file next to the full .vbk file.

RESTORE FROM BACKUP

Veeam Backup & Replication offers three methods of restore: entire VM, specific VM files only (VMX, VMDK) or individual guest files. This section outlines recommended steps you should take to perform restore from a created backup.

Restore VM Guest Files (FAT, FAT32, NTFS)

You can perform Windows file-level restore with built-in file-level restore functionality. In contrast to competitive solutions, Veeam does not have to uncompress the entire VM to restore VM guest files, which makes the restore process much faster.

Prerequisites

- You can restore VM guest files from a backup that has been successfully run at least once. Click **Backups** in the management tree; expand a necessary backup job and check if there is at least one restore point available for a backed up VM.
- Built-in file-level restore option supports Microsoft Windows file systems only (NTFS, FAT and FAT32). Dynamic disks support is limited for built-in file level restore. To restore VMs from other file systems, use the Veeam File Level Restore wizard.
- You cannot restore files from a replica that is currently running, or in case the replication or backup job with the VM from which you want to restore files is being performed.

Procedure

1. Click the **Restore** button on the toolbar.
2. Select **Individual guest files**.
3. Expand a necessary backup job and select a VM that should be restored. Click **Next**.
4. Select a necessary restore point.
5. Click **Next**, then click **Finish**.
6. After the restore process is completed, Veeam Backup & Replication will display a file browser displaying the file system tree of the restored virtual machine. Note that the names of the restored machine drives may differ from the original ones.
7. Right–click a necessary node in the file system tree and select the **Copy To...** command from the shortcut menu to save restored VM guest OS files.
8. Open the folder on the target host that you selected to restore VM guest OS files and check if the files have been successfully saved.

Restore VM Guest Files (Linux, Unix, BSD, Mac File Systems)

You can restore Linux-, Unix-, BSD- and Mac-based file systems with the File Level Restore wizard that is installed together with Veeam Backup & Replication. The Veeam File Level Restore wizard uses the virtual appliance image that is copied to your computer at the product installation process. You can then copy the individual files and folders from VM disks to your local machine drive, network share or to a remote host.

Prerequisites

- The Veeam File Level Restore wizard uses VMware Player. Make sure that VMware Player is installed on your computer.
- Panned/striped/raid-5 volumes and GPT disks are not supported.
- Encrypted LVM volumes are not supported.
- DHCP server should be presented to perform successful FLR.

Procedure

1. Select **Programs > Veeam > File Level Restore Wizard** from the **Start** menu or **Tools > File Level Restore Wizard** from the main menu of Veeam Backup & Replication.
2. The wizard will be displayed. Click **Next**.
3. Expand a necessary backup job and select a VM that should be restored. Click **Next**.
4. Select a necessary restore point.
5. Click **Next**, then click **Finish**. Note that file-level restore appliance may take about 30-40 seconds to boot.
6. After the restore process is completed, file browser displaying the file system tree of the restored virtual machine will be opened. Right–click a necessary file or folder and select the **Copy to...** command from the shortcut menu and select a necessary destination and folder on the local or remote host.
7. Open the folder on the target host that you selected to restore VM guest OS files and check if the files have been successfully saved.

Restore VM Files (VMX, VMDK, etc)

The ability to restore VM files (VMDK, VMX) to a custom location allows restoring specific files only as opposed to the full VM.

Prerequisites

You can restore VM files from a backup that has been successfully run at least once. Click **Backups** in the management tree; expand a necessary backup job and check if there is at least one restore point available for a backed up VM.

Procedure

1. Click the **Restore** button on the toolbar.
2. Select **Specific VM files only (VMX, VMDK)**.
3. Expand a necessary backup job and select a VM that should be restored. Click **Next**.
4. Select a necessary restore point.
5. From the **Destination** list, select where to store VM files: to an ESX host or the local machine. Use the **Host Summary…** button to view information on storage resources.
6. Specify the path to the folder on the selected host where files should be restored.
7. In the **VM files to restore** section, select check boxes next to files that should be restored.
8. Click **Next**; then click **Finish** to restore VM files.
9. Open the folder on the target host that you selected to restore VM files and check if the files have been successfully restored.

Restore Entire VM from Backup

Veeam Backup & Replication provides the shortest possible restore time due to latest VM state always available as an image in the latest VM state.

Prerequisites

- You can restore a VM from a backup that has been successfully run at least once. Click **Backups** in the management tree; expand a necessary backup job and check if there is at least one restore point available for a backed up VM.
- You can restore a VM to the ESX server of the same or later version than the server on which the backup was created. For instance, if you created a backup of a VM running on ESX 3.0, you can restore this VM to ESX 3.0, 3.0.1, 3.0.2 and 3.5 or ESXi.

Procedure

1. Click the **Restore** button on the toolbar.
2. Select **Entire VM (including registration)**. Click **Next**.
3. Expand a necessary backup job and select a VM that should be restored. Click **Next**.
4. Select a necessary restore point.
5. If you want to power on a VM after it is restored, select the **Power on VM after restoring** check box. Click **Next**.
6. From the **Host** list, select a host on which a restored VM should be started. To learn how much space is available on storage devices, click the **Host Summary…** button and click the **Populate** button.
7. In the **Virtual machine name**, enter the name under which a restored VM shall be registered.
8. Select a datastore and resource pool to which the virtual machine should be restored.
9. If you restore a VM using virtual hardware version 7, from the **Restore disks** list, select the type of disks for a restored VM: you can restore a VM in the original state, force all VM disks thin or thick.
10. Click **Next**; then click **Finish** to restore and power on a VM.
11. Open vSphere Client and check if the VM you restored is available in the inventory tree, and is powered on.

Specify General Replication Settings

Procedure

1. Click the **Advanced…** button.
2. Select the **Enable email notification for this job** check box. You will receive an e-mail with details on job performance when it completes. To specify e-mail notification settings, select **Tools > Options** from the main menu.
3. Select the **Enable VMware tools quiescence** check box if you are performing the replication job for running virtual machines, and want it to be performed correctly. If VMs runs highly transactional applications, clear the check box to avoid risks of application failure. For applications like MS Exchange, MS SQL, Active Directory we recommend using the VSS option rather than VMware tools quiescence.
4. Select the **Enable automatic replication integrity checks** check box to periodically verify integrity of a replica and avoid a situation when a replica is corrupted, making all further increments corrupted, too.
5. Veeam Backup & Replication provides tape integration via a post-job script option. Select the **Run the following command** check box and specify a path to an executable script file. Schedule execution of scripts on specific days or at some time interval.

Specify Compression Settings

Veeam Backup & Replication provides traffic compression and empty block removal, allowing for dramatic reduction of network traffic.

Procedure

1. Click the **Compression** tab.
2. Select one of three compression levels: *Low* - for low load on ESX CPU; *Optimal* – for the best compression to performance ratio and *Best* – if Veeam Backup & Replication is installed on a computer with multi-core CPU. If replica's files are to be stored on devices with hardware deduplication, select *None*.

Specify Changed Block Tracking Settings

Veeam Backup & Replication leverages Changed Block Tracking — a feature of vStorage APIs that minimizes CPU and memory resource consumption on the ESX host up to several times. Veeam Backup & Replication tracks and processes only changed data blocks, thus making the process of incremental replication much faster. For example, if a VM only had 5 percent change since the last replication, the incremental replication time will be 20 times faster.

Procedure

1. Click the **vSphere** tab.
2. Select the **Use changed block tracking data** check box.
3. Select the **Enable changed block tracking for all processed VMs** to use this option for VMs for which changed block tracking is disabled on the ESX server.

Specify Backup Policies and Attributes

Procedure

1. Click the **Backup** tab.
2. Specify replica retention policy - number of reverse increments that should be stored.
3. Select the **Safe snapshot removal** option to prevent production applications from timing out during helper snapshot commit. This option will allow you to perform hot image-level replication of large VMs with high disk I/O loads without affecting production applications. Veeam Backup & Replication offers a procedure of safe snapshot removal which includes creating an additional snapshot in cases when the "main" snapshot size is above the specified threshold. An additional snapshot is used to host writes while the "main" snapshot is being deleted. This ensures that a consolidation helper snapshot does not grow large.
4. Click **Next**.

Enable VSS Integration

Veeam Backup & Replication utilizes the Windows Volume Shadow Copy Service (VSS) that ensures consistent replication of VSS-aware application running within your virtual machines (domain controllers, databases and other applications) without shutting them down. This option allows creating a transactionally consistent VM image, which, in contrast to a crash-consistent image, ensures successful VM replication, as well as proper replication of all applications installed on the VM without any data loss.

Prerequisites

- Microsoft Windows VSS option is supported on Windows XP, Windows 2003, Windows 2008, Windows 2008 R2 and Windows 7.
- VM guest OS should have VMware Tools and all latest service packs and patches installed.

Procedure

1. Select the **Enable Veeam VSS integration** check box.
2. Select **Continue backup even if Veeam VSS quiescence fails** check box. In case VSS fails, VMs will be processed with the **VMware tools quiescence** option (if it is enabled). If VMware tools quiescence is not enabled, Veeam Backup & Replication will create a crash-consistent backup.
3. Specify VSS agent credentials – user name and password.
4. Click **Next**.

Schedule a Replication Job

You can perform a replication job manually or schedule it.

Procedure

1. Select the **Run this job automatically** check box to specify job schedule. If you do not select this check box, the job will be saved and you will have to run it manually.
2. Select the schedule type: on specific week days or at some time interval.
3. Select the **Retry VM processing** check box. During the retry cycle, only VMs failed during the main replication cycle are processed.

4. Click **Next**.
5. Select the **Run the job when I click Finish** check box and click **Finish**. The job will be started.

View Real-Time Job Statistics

When the job is being run, Veeam Backup & Replication allows viewing job statistics in the real-time mode. Job statistics provides detailed data on a job that is currently running: job status, start and end time, total number of processed and failed objects, size, performance rate and details of the session performance (for example, errors that have occurred in the process of operation).

Procedure

1. Click the **Jobs** node in the management tree.
2. Right-click the job you created and select **Realtime Statistics** from the shortcut menu. Now you can track the job performance as it runs.

Check VM Replica

At replication, VM files are placed on the selected datastore in */Veeam Backup/VMname(vm-ID)* folder.

Procedure

1. Open vSphere Client and check if the VM you replicated is available in the inventory tree.
2. Check if */Veeam Backup/VMname(vm-ID)* folder has been created on the target host.

Perform Incremental Replication

When incremental replication is performed, Veeam Backup & Replication 4.0 'injects' changed data to a VM replica and uses historical data to calculate a reverse increment. Obtained changes are saved as a service .vrb file next to a VM replica.

Procedure

1. Click the **Jobs** node in the management tree.
2. Select the job that you created.
3. Click the **Start** button on the toolbar. The job will be started.
4. After the job is completed, open the folder on the target host that you selected to store a replica.
5. Check if it has a .vbr file next to a created replica.

REPLICA FAILOVER

With the virtual machine replica failover option, you can recover a corrupted VM in case of software or hardware malfunction to its replicated version. Do not power on a replicated VM manually - use the **Perform failover** option in the Restore wizard instead. If you power on a VM manually (for example, using vSphere Client), the replicated VM will be working as a usual one; however, the replication 'chain' will be broken and incremental replication sessions will be failing.

Prerequisites

The failover option can be used for any virtual machine replica that was successfully created at least once. Click **Replicas** in the management tree; expand a necessary replication job and check if there is at least one restore point available for replicated VM.

Procedure

1. Power off the original virtual machine on the source host before starting failover. To avoid unwanted interference with the replica files, stop the corresponding replication job, too.
2. Click the **Restore** button on the toolbar.
3. Select **Perform failover.** Click **Next**.
4. Expand a necessary replication job and select a VM that you want to fail over to its replicated version. Click **Next**.
5. Select a necessary restore point.
6. Click **Next**.
7. Open vSphere Client and check if the replicated VM is powered on.

Undo Failover

When the Undo failover option is performed, Veeam Backup & Replication powers off a replica on the target host, and rolls back to replica's initial state.

When replica failover is performed, Veeam Backup & Replication creates a snapshot of a replica to protect a replicated VM from user's changes. When the undo failover operation is performed, the replica reverts to the created snapshot.

Procedure1.

1. Click the **Restore** button on the toolbar.
2. Select **Undo previously performed failover.** Click **Next**.
3. Expand a necessary replication job and select a VM for which failover was performed.
4. Click **Next**. Veeam Backup & Replication will rebuild a replica to the state it was at the point of failover and discard any data changes that may have taken place on the target ESX host.