



# Configuration Guide: Protecting Virtual Machines with HP Storage and Veeam

## Table of contents

<b>Intended Audience</b>	<b>3</b>
<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>3</b>
Data Protection Trade-offs	4
Instant Restore Testing: 40 GB	
Exchange vSphere VM	4
<b>Planning your Virtual Data Protection</b>	
<b>Infrastructure</b>	<b>5</b>
Design Goals	5
Backup Methodology and Optimization	7
Architectural Overview: Veeam Backup	9
Architectural Overview: Veeam	
Replication	10
Configuring Veeam Backup Servers and	
Backup Proxies	10
Configuring Backup Repositories	11
Design Guidelines for Backup Jobs	11
<b>Configuration Guidelines for the</b>	
<b>StoreOnce Backup System</b>	<b>12</b>
Configuring Multiple CIFS Shares to	
Increase Backup Throughput	12
Replicating Backup Repositories with	
StoreOnce Backup Systems	12
Replicating VMs with Veeam Backup &	
Replication	12
Configuring Veeam Backup Jobs for	
StoreOnce B6200 Autonomic Node	
Failover	12
Backup Job Settings: Using a StoreOnce	
Backup System as a Backup Repository	13
Setting Block Size for Backup Jobs	13
Backup Repository Settings: Using	
StoreOnce Backup Systems	14

Additional StoreOnce Backup System Capabilities	15
<b>Configuration Guidelines for Primary Storage Devices</b>	<b>16</b>
Backup Repository Settings: Using Primary Storage as a Backup Repository	16
Backup Job Settings: Using Primary Storage for Backup and Restore	17
<b>Summary</b>	<b>19</b>
Primary and Secondary Storage Comparison	19
Conclusion	19
<b>Resources</b>	<b>20</b>

## Intended Audience

This guide is intended for anyone involved in the design, acquisition and implementation of data protection solutions for vSphere and Hyper-V virtual machines on shared SAN and NAS storage. This guide was written for IT generalists and specialists alike whether you need to back up a dozen or hundreds of virtual machines. The audience includes but is not limited to: Systems Administrators responsible for servers, hypervisors, storage and backup; Sales Engineers; Systems Engineers; Solution Architects; Professional Services Engineers and Consultants. The technical information in this guide is intended to be a starting point for designing and implementing a virtual machine data protection solution. This backup and replication solution has been tested and certified jointly by HP and Veeam.

## Executive Summary

Today's backup environments include physical servers in addition to virtual machines and their associated disk images. When virtual machines (VMs) are included in a backup strategy, deploying backup software agents on guest virtual machines increases cost and complexity. The use of traditional host agent backup methods for guest VMs places a significant burden on physical host servers by requiring additional CPU cycles and I/O bandwidth during the guest backup process as well. Backing up VM images, in an agentless fashion, can reduce costs while dramatically reducing the performance impact that backing up guest virtual machines has on the physical host server.

Data protection software and hardware need to provide an effective solution that protects vSphere and Hyper-V files, images, templates and applications running on virtual machines by integrating directly into the rich feature sets of vSphere and Hyper-V while offering features such as backup, data deduplication and replication. Ideally, this data protection solution will be able to manage multiple hypervisor environments from one management console.

HP and Veeam Software offer VMware vSphere- and Microsoft® Hyper-V-optimized protection solutions for virtual data center administrators. HP and Veeam have teamed up to solve the problems inherent in the traditional agent-based backup model with a solution that is simple to license and simple to implement at a low price point. The HP-Veeam solution has been tested and proven to optimize VM backup when used in conjunction with HP Storage disk arrays and the StoreOnce Backup System family of disk-to-disk backup appliances. The HP and Veeam data protection solution is complimentary to existing physical system backup tools.

## Introduction

This technical brief provides an overview of the latest VMware and Hyper-V data protection technologies available and their recommended best practices when configuring disk-to-disk backup appliances and primary disk systems from HP Storage.

HP Storage disk-based systems consist of primary storage arrays (i.e., P2000/MSA, P4000/LeftHand, EVA, 3PAR, P9000) as well as secondary disk-to-disk backup solutions represented by the StoreOnce Backup System deduplication appliance family. HP primary disk arrays and the StoreOnce Backup System appliances offer highly available, disaster-tolerant storage solutions with hardware RAID and remote volume and share replication.

Veeam Backup & Replication compliments the HP Storage infrastructure by providing fast recovery and application object-level restoration by running a VM directly from its backup image on disk. This fast and granular recovery is enabled by Veeam's patent-pending vPower technology used in conjunction with disk backup storage that can handle random read I/O activity well. With vPower, it is possible to restore a VM in minutes with object-level granularity. This unique restoration capability enables you to quickly restore VMs and individual files as well as application objects such as Exchange mailbox messages and SQL tables.

In addition to VM backup and fast recovery, Veeam Replication can create point-in-time copies of VMs in separate locations across IP networks. These replicas are bit-for-bit copies of production VMs, which are registered to a standby Hyper-V or ESX host, not compressed and deduplicated VM backup images. These standby virtual machine replicas are ready to power-on with a moment's notice. These backup, recovery and replication tools allow you to manage both Hyper-V and vSphere environments from one console, providing efficient "single pane of glass" management.

## Data Protection Trade-offs

The type of backup and recovery problem that you're trying to solve will depend a great deal on the type of disk system used for backup. Common questions to consider when you begin your virtualization data protection strategy include:

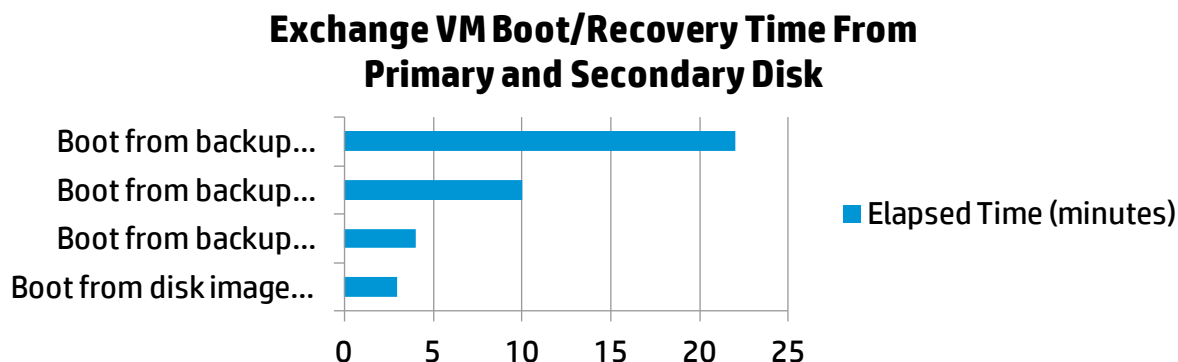
- Is fast virtual machine recovery required and, if so, which VMs?
- Is the fast recovery of individual files or application-level items such as mail messages or database objects important?
- Is it necessary to retain backup copies for a period of several months or even a year?
- Is dense and efficient storage required for maximum capacity at the lowest cost per GB?

The first two recovery criteria will likely require the type of random I/O performance typically found in a primary storage device. The best solution for a backup target that can provide the fastest granular recovery would be an HP Storage disk array; for example, P2000 MSA or P4000 LeftHand, or locally attached storage (DAS) in a SAN-attached physical backup proxy server. If the answer to the previous questions about long retention, high capacity and low cost per GB is "yes," then the best solution is a StoreOnce backup appliance.

The following chart compares the boot times of a 40 GB VM running a simple Exchange 2007 instance from both primary production storage and the boot time using Veeam's vPower Instant Restore technology from different backup targets. The comparison begins by measuring the boot time when using a P4300 LeftHand array as primary production storage. Once this baseline is established, we compare the virtual machine's native boot time to the time required to boot the VM, using vPower, from its backup image on a P4300 LeftHand array used as a backup target. The boot time of the VM, again using vPower technology, from its backup image on a StoreOnce backup appliance was tested and measured as well.

### Instant Restore Testing: 40 GB Exchange vSphere VM

The following chart compares the boot times of a minimally configured 40 GB vSphere Exchange VM in a lab environment. This test was conducted in a controlled environment and is merely intended to serve as a guideline for comparing boot times across different disk storage environments. The test measures the interval from VM power-on from the primary VMFS volume or Instant Restore from the backup image until log-in to Outlook Web Access is complete. The boot time in the first row below is from the native VM image booted from a P4300 LeftHand disk array used as primary storage. The second row features the P4300 used as a backup target while the third and fourth columns represent VM boot times using a StoreOnce Backup appliance.



The 3-minute native boot time on the P4000 production volume increases to 4 minutes when booting the VM's backup image from a P4000 primary disk array used as a backup target with vPower Instant Restore. The third and final columns compare the boot times when the VM is started from the backup image on a StoreOnce backup appliance using vPower Instant Restore with different compression settings. The boot times when starting the VM from a backup image on a StoreOnce appliance increase to 10 and 22 minutes, depending on the compression setting. Contrast this to the 4-minute boot time when the same VM was started from a backup image residing on a P4000 LeftHand disk array.

The relative difference in boot times of a VM backup image started from a disk array versus a backup appliance is consistent across most storage vendors' platforms. With few exceptions, disk arrays, when used as backup targets, outperform backup appliances for fast and granular recovery of a VM from its backup image. On the other hand, disk arrays typically cannot store as many backups with the high capacity and increased utilization of a backup appliance with target-side deduplication at the hardware level.

# Planning your Virtual Data Protection Infrastructure

HP and Veeam provide flexibility in allowing customers to choose the best backup policies for the network and the type of backup target. Backup images can be stored on local as well as remote backup repositories in a compressed and deduplicated format. In addition to backup, Veeam's replication technology can be used to copy production VMs to a separate location where they're inventoried with a host and powered off.

Veeam brings both forward and reversed incremental backup options to the HP Storage customer. Customers can choose between reversed incremental backups ("incremental forever") or forward incremental backups. Forward incremental backup is typically the best option when backing up to a StoreOnce Backup System or with a scripted offload of a backup image to tape. Reversed incremental, on the other hand, may be better suited to customers backing up VM images using primary storage as the disk target because of the higher workload created by this backup mode.

## Design Goals

Backup and recovery decisions must be based on business priorities. Once business priorities are defined, backup policies can be created. Backup policies should define the value of data and map that value to backup targets and methods. These policies can then be applied as appropriate, given the business importance of the data.

Some of the major considerations for a data protection strategy include:

- Fast Recovery of critical VMs or select VM files (that is, VMDK or .VHD files)
- Length of retention periods
- Off-site replication of backup repositories (for example, CIFS shares)
- Off-site replication of VMs
- Off-site archiving of backup jobs
- Meeting or exceeding Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) or Service Level Agreements (SLAs)
- The duration of your backup window

Your design should also consider whether some VMs have a lower RTO than others. Do you have SLA commitments with different levels of service depending on a VM's role?

The type of storage and the network resources that you have available greatly impact the effectiveness of your backup policies. Do you have SAN-attached primary disk arrays, Network-Attached Storage, disk-to-disk deduplication appliances or a combination of all of these? Do you need to replicate or archive offsite? How will your current LAN and WAN infrastructure affect your backup design?

The answers to these questions go a long way toward dictating the design of your backup solution. The fastest, most granular recovery is achieved when using SAN-based primary disk arrays. Although primary disk arrays feature fast VM recovery characteristics due to their fast random read performance, they don't have the high capacity utilization that disk-based deduplicating backup appliances offer.

Not all VMs have equal business priority for an organization. A backup policy using fast SAN-attached or direct-attached storage (DAS) in the backup proxy server itself can provide much faster restore capability for business-critical or mission-critical VMs. Consequently, if a backup policy for less critical VMs is put in place using a deduplication appliance, more backup images can be stored more efficiently with longer retention periods.

## Meeting Backup Objectives

In order to meet backup objectives it may be necessary to have more than a single backup job type, proxy and repository. The most common mistake in virtual machine backup design is to have a single job regardless of VM size, OS, applications and the overall importance of the virtual machine to the organization's mission. By using a combination of proxy types with repositories that can provide fast recovery and repositories that have good capacity utilization you can scale virtual data protection while meeting RTO and RPO commitments.

## Technology Overview

The technologies covered include vSphere and Hyper-V Change Block Tracking, VSphere vStorage and Hyper-V APIs, Veeam Backup & Replication inline source-side deduplication, HP StoreOnce D2D appliance target-side deduplication and HP StoreOnce replication. When used together, these technologies deliver a data protection solution that can be implemented in any VSphere and Hyper-V environment.

### VMware vStorage APIs and Changed Block Tracking

Changed Block Tracking (CBT) is a feature that was introduced in VMware vSphere 4.0 that keeps track of blocks of data stored on a virtual disk that have been changed since a certain point in time. CBT is a VMkernel feature. Access is via the VMware vStorage APIs. By default, CBT is not enabled due to the slight (1–2%) overhead incurred when using this feature. The vStorage APIs are a set of interfaces exposed for third-party hardware and software integration with the VMware storage features. A subset of these is specifically for backup and recovery software vendors to optimize VMware data protection. These are known as the vStorage APIs for Data Protection (VADP).

The VMware-recommended method of backup and recovery is to use products that support VADP. Veeam Backup & Replication fully supports VADP. Veeam Backup & Replication queries the VMkernel through the VADP to identify the blocks of data that have changed on the virtual disk since the last backup—a process that greatly improves the performance of incremental backups. The first full backup of any virtual machine results in all of the data being transferred to the HP StoreOnce D2D appliance, but all incremental data consists of only the changed blocks as identified by CBT. Veeam uses VMware Tools to create an application-consistent snapshot from which to replicate VM files or create a compressed, deduplicated backup image.

### Microsoft Hyper-V APIs and Changed Block Tracking

To perform an incremental backup, Veeam Backup & Replication needs to know which data blocks have changed since the previous job run. This becomes an issue with Microsoft Hyper-V, as Microsoft has not released this feature with its hypervisor. To solve the problem of keeping track of changing data blocks, Veeam has developed a custom Hyper-V changed block tracking mechanism that is implemented as a file system driver. Veeam uses Microsoft VSS to create an application-consistent snapshot from which to replicate VM files or create a compressed, deduplicated backup image. For more detail, please refer to the Veeam Backup & Replication User Guide for Hyper-V under the **Documentation** section on the Veeam website.

### HP StoreOnce D2D Appliance Target-side Deduplication

Target-side deduplication is performed on the HP StoreOnce D2D appliance that has been configured as an NAS share and is presented to the backup application. A major benefit of target-side deduplication is that the backup storage appliance uses finer deduplication chunking (4 KB on average), which improves deduplication ratios and storage utilization. The HP StoreOnce D2D appliance uses smaller blocks to identify repeated data across multiple backups produced by different Veeam backup jobs. This further reduces the amount of data to be physically stored, thus greatly improving storage utilization. In addition to using a more granular 4 KB chunk size, StoreOnce deduplication works across an entire backup repository containing multiple Veeam backup jobs to bring even more storage savings.

### Veeam Backup & Replication Source-side Deduplication

Veeam Backup & Replication performs deduplication processing during backup before writing data to the StoreOnce appliance. Once again, this reduces the amount of data sent across a network while also increasing storage efficiency and utilization. The scope of the deduplication is the data in the backup job. Deduplication is a configurable option for was previously backed up. Duplicate data is skipped while unique data is sent to the StoreOnce appliance. Veeam's source-side inline deduplication block sizes are configurable from 256 KB to 1 MB. These block sizes are optimized to accommodate the distance from the backup repository to the virtual machine. Configuring the storage target setting as a WAN target will result in a block size of 256 KB. A block size of 512 KB is automatically configured for the LAN target selection while a 1 MB block size is created for locally attached targets.

### Combining Deduplication at the Source and Target

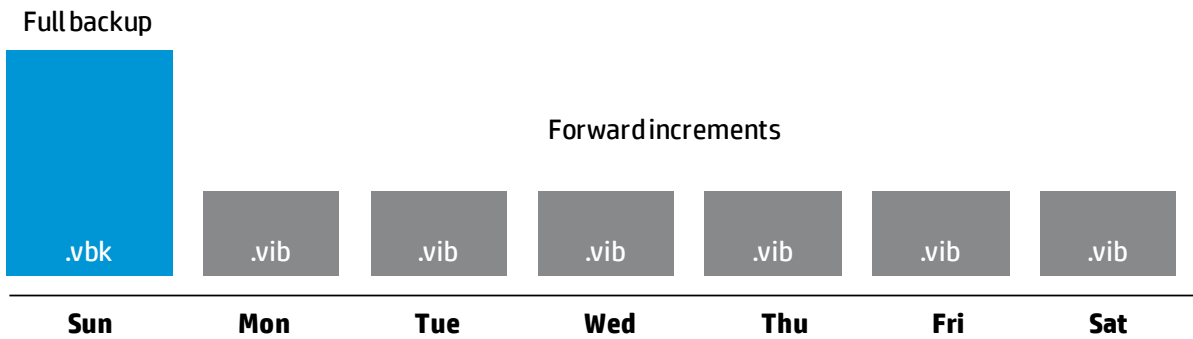
The HP and Veeam recommendation is to enable Veeam Backup & Replication's inline deduplication along with HP StoreOnce D2D appliance target-side deduplication. Veeam Backup & Replication deduplicates across a backup job while the HP StoreOnce Backup System deduplicates further, across an entire repository containing multiple Veeam backup jobs. Both deduplication techniques provide complementary benefits. Source-side deduplication (Veeam) generates less LAN traffic while target-side dedupe (StoreOnce) reduces the size of the backup image on disk.

# Backup Methodology and Optimization

## Forward Incremental Backup

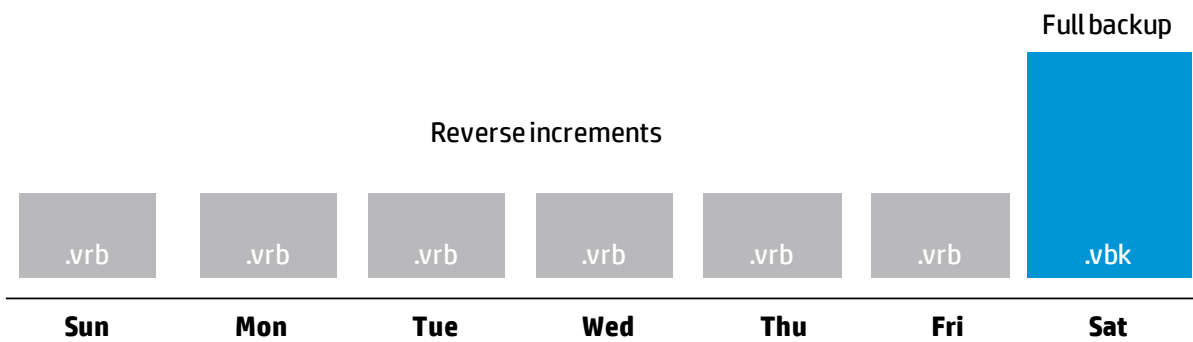
For customers utilizing disk backup appliances like the HP StoreOnce Backup System, a forward incremental backup mode is the recommend backup job setting. With a forward incremental backup more space is required for backups; however, there is less of a performance impact on the backup target. A forward incremental backup requires a periodic synthetic backup or active full backups. A synthetic backup simply creates a new full backup from the last full backup and its subsequent incremental backups.

Using forward incremental backup mode generally produces a three-fold reduction of the workload in terms of the number of I/O operations that the disk backup target has to process when compared to a reversed incremental backup job.



## Reversed Incremental Backup

For customers utilizing primary disk arrays as disk-to-disk backup targets, the reversed incremental backup mode is recommended. With reversed incremental backup, less space is used for backups and the customer can have a more granular retention policy. Reversed incremental backups do require more I/O performance from the backup target.



### Impact of Backup Modes on Target Storage

The creation of periodic synthetic or active full backups (the recommended method) will generate additional I/O load on the backup target as well. The following guidelines should be considered when designing virtual backup infrastructure:

- Full and forward incremental backup modes represent the baseline I/O load on the backup target (100% write)
- Reverse incremental backup mode creates a 3X workload increase on the backup target, relative to the baseline (66% write/33% read)
- When using incremental backup mode it is necessary to schedule occasional full backups. These can be either active full backups or synthetic backups created by consolidating previous full and incremental backups into a new full backup. These backups will have the following impact on the target storage:
  - Active full backup is the same as an original full backup (100% write)
  - Synthetic full backup will generate a 2X increase in the baseline I/O load (50% read/50% write)
  - Synthetic full backup with transform will generate a 4X I/O load increase on the backup target (50% read/50% write)

### Compression

Compression technology is employed by Veeam Backup & Replication to reduce the disk space and network bandwidth requirements of VM image backup. Compression of the VM backup image results in additional disk savings while requiring less network bandwidth when used on a primary storage array. When used with backup appliances, disabling compression can enhance the appliance's target-side deduplication at the expense of increased network traffic. It is possible to configure a backup repository to decompress data blocks before they are deduped and written to disk on the StoreOnce appliance. The backup image in this scenario is compressed prior to being transmitted over the network, reducing backup traffic, then decompressed and written to disk when it reaches the StoreOnce Backup System. The steps to decompress a backup file prior to being written to its disk target are outlined later in this guide.

### Off-site Backup & Replication for Archiving and Disaster Recovery

There are two levels of replication available to vSphere and Hyper-V customers deploying HP Storage with Veeam data protection. The HP Storage disk arrays and StoreOnce appliances have the capability to replicate entire LUNs or shares to remote sites. Consolidation benefits can be achieved by implementing a many-to-one “fan-in” replication where multiple virtualized environments are backed up to a local StoreOnce appliance and then the entire repository (example, a CIFS share or NFS Export) can be replicated to a centralized StoreOnce appliance.

At the Virtual Machine level, Veeam Backup & Replication can be used to replicate VM images to remote ESX (i) or Hyper-V hosts as well as to write VM backup images to remote repositories. A replication job can be configured to include one or more VMs as well as objects such as folders, clusters and even entire datastores.

With Veeam Backup & Replication a snapshot is taken before a VM's files are copied from the snapshot by a proxy server and sent to another proxy server at a target location where they are registered in the virtual environment and then powered off. Virtual machine files that have been replicated to another vSphere or Hyper-V host using Veeam Backup & Replication can be recovered by powering on from hypervisor tools such as vCenter or Microsoft System Center. Once this VM is powered on it can be failed over into the production environment. A compressed and deduplicated VM backup image, on the other hand, must be recovered from the backup repository and powered on using the Veeam console or Veeam recovery tools.

Veeam repositories can also be configured in remote locations, enabling backup over a WAN link for off-site archiving if fast recovery is not a design goal for the VMs in question. Whether deploying remote backup or remote replication, a minimum WAN link of 1 Mbps is recommended. High latency links are tolerated as long as the TCP/IP connection does not drop.

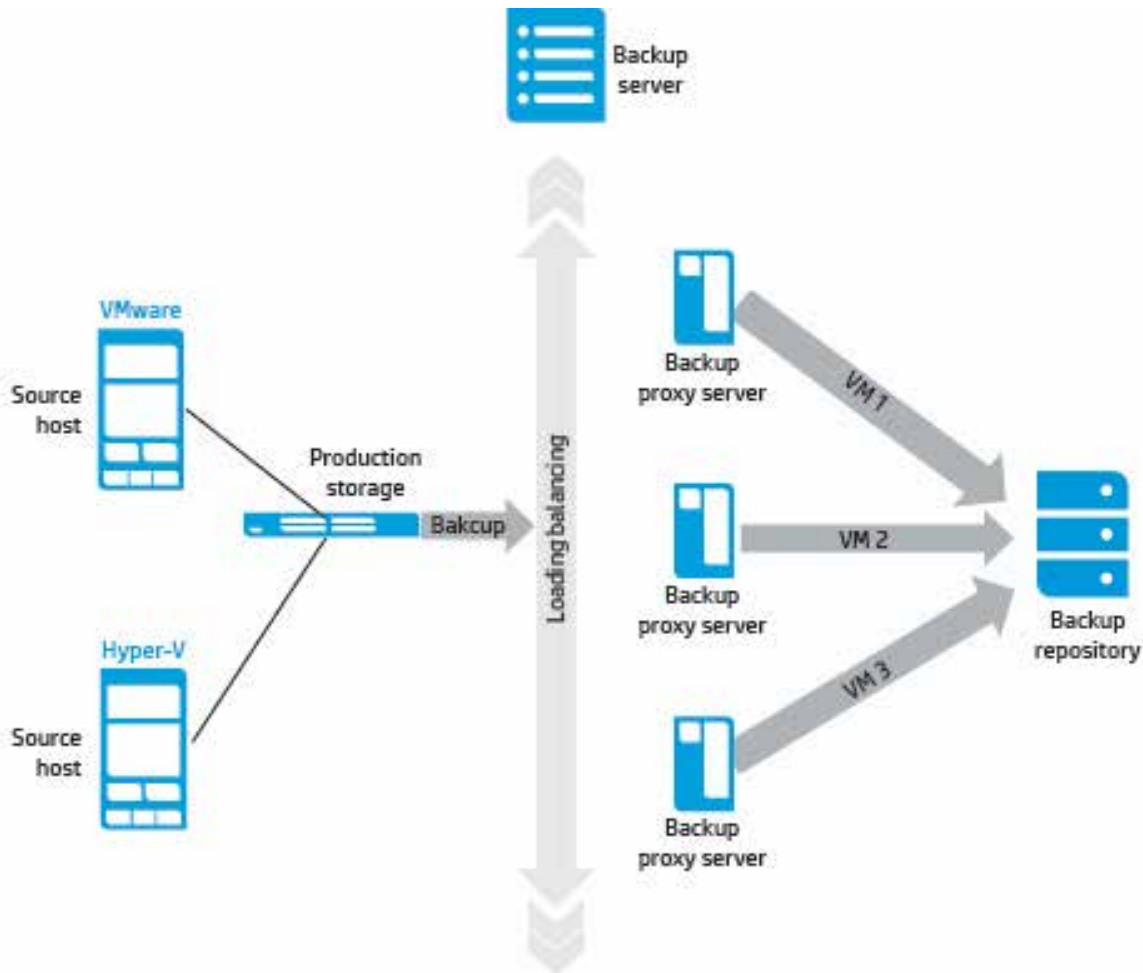


## Increase DR Flexibility and Lower Cost

Veeam Backup & Replication occurs from proxy to proxy. The source datastores and the target disk repositories do not communicate directly and do not have to be compatible. With Veeam Backup & Replication, a VM stored on production 3PAR datastore can be replicated to a lower-cost MSA or LeftHand disk array deployed in a DR location. The HP-Veeam virtual infrastructure protection solution offers a great deal of flexibility and cost savings in Business Continuity and Disaster Recovery.

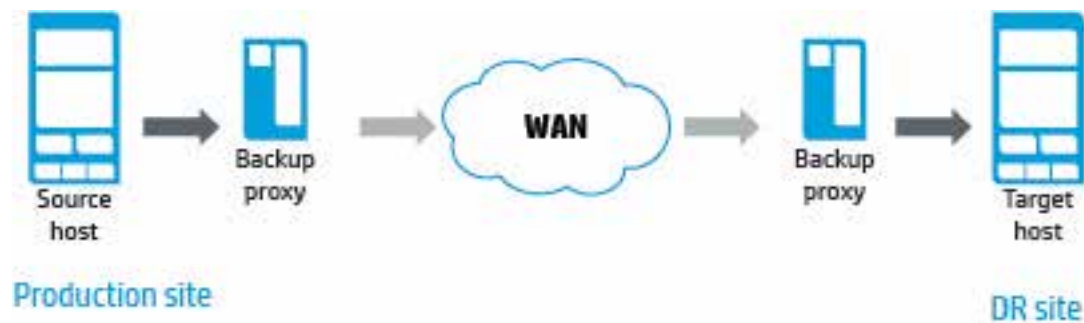
## Architectural Overview: Veeam Backup

This configuration is an example of the Veeam Backup architecture with distributed backup proxies.



## Architectural Overview: Veeam Replication

This configuration is an example of the Veeam Replication architecture with distributed proxies at the source (production) and target (recovery) locations.



## Configuring Veeam Backup Servers and Backup Proxies

The Veeam backup server is the “brain” of Veeam Backup & Replication. The backup server is responsible for job scheduling and management as well as the orchestration of the overall solution.

### Minimum Guidelines for Sizing backup Servers

- The recommended minimum is two processor cores. Faster processors and additional cores will generally improve backup performance; it is recommended that at least one CPU core or vCPU be provisioned for every eight to ten concurrent jobs
- 4 GB of RAM is the recommended minimum for local SQL installation
- 2 GB of RAM is the recommended minimum for remote SQL installation

For more detail on sizing, please refer to the User Guides for VMware or Hyper-V under the **Documentation** section on the Veeam website.

The proxy server or servers can be thought of as the “muscle” of the backup architecture. The proxy has the CPU-intensive task of reading the backup snapshot, deduplicating and compressing the data and sending it on to disk. The primary role of the backup proxy is to provide an optimal route for backup traffic and to enable efficient data transfer. The virtual infrastructure data protection architecture scales with additional distributed proxies. When deploying backup proxies, you need to analyze a connection between the backup proxy and the storage with which it is working. Depending on the type of connection, the backup proxy can be configured in one of the following ways:

- A server used as a backup proxy should have direct access to the storage on which VMs reside or the storage where VM data is written. This way, the backup proxy will retrieve directly from/to the storage, bypassing the LAN.
- The backup proxy can be a virtual machine with ‘Hot Add’ access to VM disks on the storage. This type of proxy also enables LAN-free data transfer.
- If neither of the above scenarios is feasible, you can assign the role of the backup proxy to a physical or virtual machine on the network, closer to the source or the target storage with which the proxy will be working. In this case the backup data will be transmitted over the LAN.
- A virtual infrastructure can benefit from deploying both physical and virtual proxies.

The best backup throughput and fastest recovery often results from having physical proxy servers. For the fastest backups, a proxy should use Direct SAN Backup where the proxy reads the VM files directly from VMFS, NFS or NTFS volumes residing on a Fibre Channel or iSCSI SAN. With Direct SAN Backup, the proxy can create backup images faster by reading virtual machine files directly from the volumes containing the production VMs.

For the fastest possible VM recovery, we recommend a ProLiant-based physical proxy with local Direct Attached Storage or an inexpensive disk array. Low-cost primary disk arrays, SAN-attached or local to a server (i.e., P2000/MSA, P4000/LeftHand or P6300/EVA) can also provide fast, granular VM recovery with longer retention periods. Direct Attached Storage on a backup proxy and entry-level disk arrays can be used to complement a StoreOnce Backup appliance. Using faster DAS or SAN backup repositories in conjunction with high-capacity StoreOnce appliances allows you to meet multiple objectives. Different backup jobs targeted at different repositories can be deployed to conform to specific backup policies.

## Guidelines for Sizing Proxies

- Multi-core processors can run more simultaneous jobs resulting in fewer proxies to manage
- 2 CPUs per active job (two cores per physical proxy, 2 vCPUs per virtual proxy)
- For virtual proxies, 4 vCPUs is the recommended minimum

For more detail on sizing, please refer to the User Guides for VMware or Hyper-V under the **Documentation** section on the Veeam website.

Deciding between physical or virtual proxies or a combination of both requires an understanding of your organization's operational priorities and the available network, storage and compute resources. A distributed backup and replication model gives you the agility to build an infrastructure that provides full virtual machine data protection to complement existing physical machine data protection methods.

## Configuring Backup Repositories

A backup repository is a location used by Veeam Backup & Replication jobs to store backup files, copies of VMs and metadata for replicated VMs. A backup repository is a volume, share or export that is accessible by the backup proxy. By assigning different repositories to jobs and balancing the number of parallel jobs for each one, you can balance the load across your backup infrastructure. In the Veeam backup infrastructure, you can use one of the following repository types:

- A Windows® server with local or directly attached storage. The storage can be a local disk, directly attached disk-based storage or, in cases where the server is connected into the SAN fabric, an iSCSI or Fibre Channel SAN LUN.
- A Linux server with local or directly attached storage. The storage can be a local disk, directly attached disk-based storage (DAS) or, in cases where the server is connected into the SAN fabric, an iSCSI or Fibre Channel SAN LUN formatted with NFS. A Linux/NFS repository can, in many cases, provide up to a 25% increase in the Instant Restore performance for a VM.
- A CIFS share via a Windows proxy server.

## Repository Sizing Guidelines

- Estimate disk space by calculating the total size of the VMs being backed up
- Determine the frequency of backups and the retention period
- The type of disk target, primary array or backup appliance will determine the correct usage of forward or reverse incremental backup modes
- Use a baseline ratio of 2:1 for a conservative estimate of dedupe/compression savings until you can verify the actual savings in your production environment
- Use a baseline data change rate of 2–5% per day if you are unsure of your rate of change
- Include disk space for additional growth and functions like ad hoc full backups or any exceptions to the guidelines

For more detail on sizing, please refer to the User Guides for VMware or Hyper-V under the **Documentation** section on the Veeam website.

## Design Guidelines for Backup Jobs

The most common mistake in production environments is to rely on a single backup job, proxy and repository. If your backups exceed the backup window after testing the various job settings, you may need to add more proxies and repositories and then distribute the jobs across all proxies and repositories. You can often increase backup throughput, thus reducing the backup duration by assigning different repositories to different jobs.

In order to reduce backup image size and duration, consider including virtual machines created from the same template or clone in a backup job. Virtual machines created from the same source will have higher deduplication ratios.

# Configuration Guidelines for the StoreOnce Backup System

StoreOnce deduplication appliances are well-suited for nearline storage of VM backup images when a customer requires long retention periods and maximum disk space savings. The trade-offs for increased disk capacity utilization and the longer retention periods allowed by this efficiency are potentially slower restore times and less granular recovery of VM data for larger environments. The trade-off of slower RTOs vs. increased capacity and efficiency is inherent in nearly all disk-based backup appliances.

## Configuring Multiple CIFS Shares to Increase Backup Throughput

The StoreOnce Backup system can be configured with multiple CIFS shares or NFS Exports, which can then be used for backup repositories that can be accessed by the Veeam Backup Server. Multiple StoreOnce shares can be used to load balance the workload of the Veeam proxy servers.

## Replicating Backup Repositories with StoreOnce Backup Systems

The StoreOnce Backup System can be configured to replicate shares or exports from one location to another over an IP network. This replication is performed via hardware by the StoreOnce storage node to a Disaster Recovery target node at a remote location. The storage hardware on the source (production) and target (recovery site) must be compatible. Multiple StoreOnce Backup Systems can be deployed to replicate in a many-to-one “fan-in” architecture from remote locations to a large central StoreOnce repository.

## Replicating VMs with Veeam Backup & Replication

In addition to StoreOnce hardware replication at the repository level, the files associated with a running virtual machine can be quiesced and replicated at the software level to a secondary physical host or cluster (recommended), registered in the host's or cluster's inventory and powered off until needed. Veeam's replication feature creates a point-in-time replica of the actual VM files from a running virtual machine, not a compressed and deduplicated backup image.

This replication occurs between two Veeam proxy servers (physical or virtual), which can be VMs in different locations on an IP network. Replication occurs between two Veeam proxies at the source and target locations. The replica of the VM can then be powered on through a hypervisor tool like the vSphere client, vCenter, Hyper-V Manager or Microsoft System Center Virtual Machine Manager.

A Veeam proxy server can also be used to back up a running VM to a remote repository. This backup process has a different outcome than replication. In this scenario the files are read from a VM that has been quiesced before being compressed and deduplicated into backup images with .vbk and .vib file extensions. A .vbk or .vib file must be read and powered on by the Veeam proxy server, not vSphere or Hyper-V management tools, before being converted into native VM files. This is accomplished via the vPower Instant Recovery process or via a restore job. Recovery and restoration times will vary with network link speed and latency.

## Configuring Veeam Backup Jobs for StoreOnce B6200 Autonomic Node Failover

The StoreOnce B6200 Backup System has a high availability failover capability between the NAS nodes. The StoreOnce B6200 Backup System has been tested with Veeam Backup & Replication to assure compatibility and to test the job restart capability of Veeam Backup & Replication.

### Managing B6000 StoreOnce Node Failover

A StoreOnce CIFS share typically requires a minimum of three minutes for a failover from one node of a two-node B6200 couplet to the other. Begin failover testing by setting a backup job to retry five times at four-minute intervals. The failover and failback commands for the StoreOnce B6200 Backup System can be found in the StoreOnce B6200 Backup System User Guide and the CLI guide, which are available from the [HP Business Support Center](#).

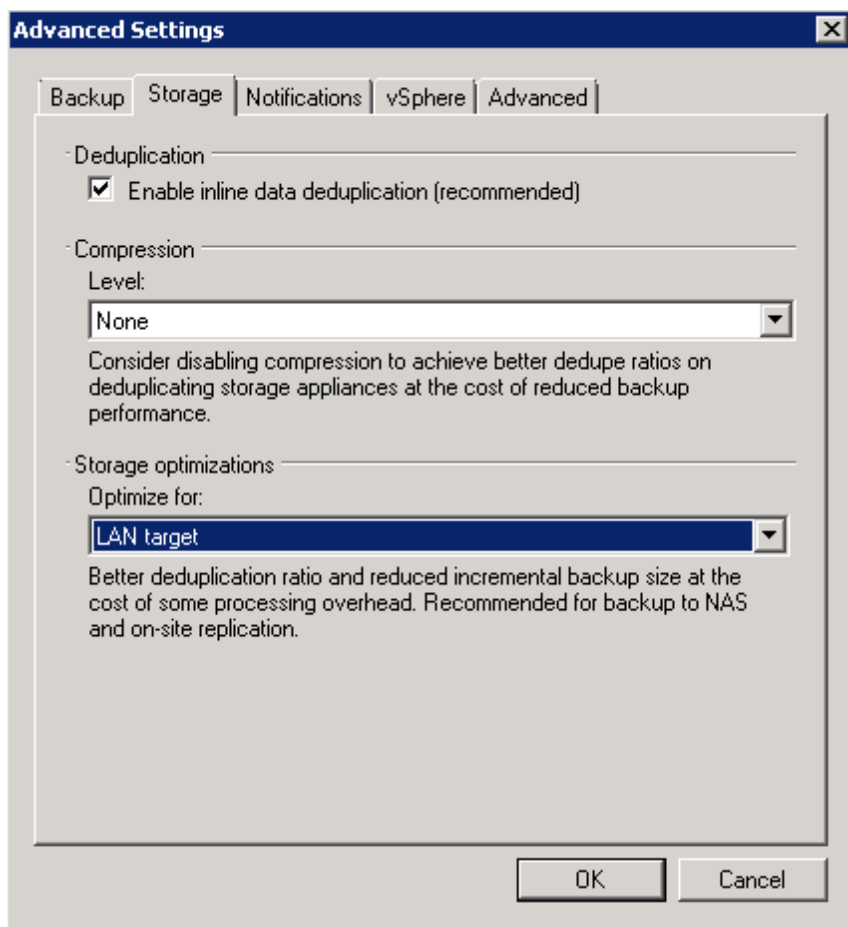
## Backup Job Settings: Using a StoreOnce Backup System as a Backup Repository

### Setting Compression for Backup Jobs using a StoreOnce Backup System

The settings for compression are selected from the **Advanced** tab of the **New/Edit Backup Jobs** wizard's **Storage** screen. A compression setting of **Optimal** balances the CPU load on the proxy server vs. the backup size and the amount of network bandwidth used. A setting of **Best** will yield the fastest backup; however, six processor cores are recommended for the backup proxy per the recommendation that appears under the **Storage optimizations** drop-down list. In this example, the **Compression** is set to **None**, which optimizes the StoreOnce deduplication ratio at the expense of increased network traffic during backup. The following section explains how to reduce network traffic while optimizing StoreOnce deduplication.

### Setting Block Size for Backup Jobs

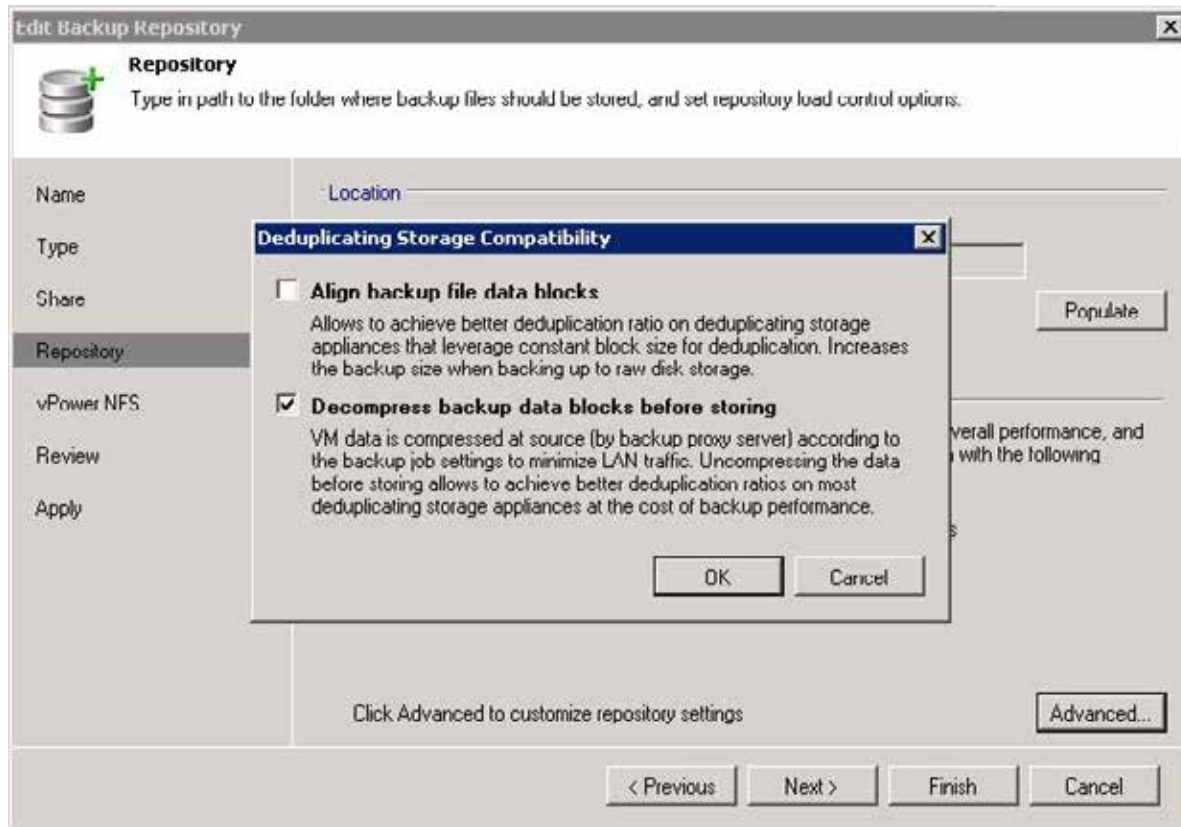
For StoreOnce Backup Systems presenting CIFS shares or NFS Exports (NAS) use the **LAN target** setting under **Advanced Settings**.



## Backup Repository Settings: Using StoreOnce Backup Systems

### Data Block Decompression and Data Block Alignment Settings for StoreOnce Backup Systems

This section describes how to enable source-side compression to reduce network traffic and then disable it prior to writing the backup image to the target. The decompression and alignment settings are found in the **New Backup Repository** wizard (click the **Advanced** button on the **Edit Backup Repository** wizard). For StoreOnce Backup Systems, select the checkbox for **Decompress backup data blocks before storing**. Leave the **Align backup file data blocks** checkbox unselected, as StoreOnce deduplication uses a variable block size.



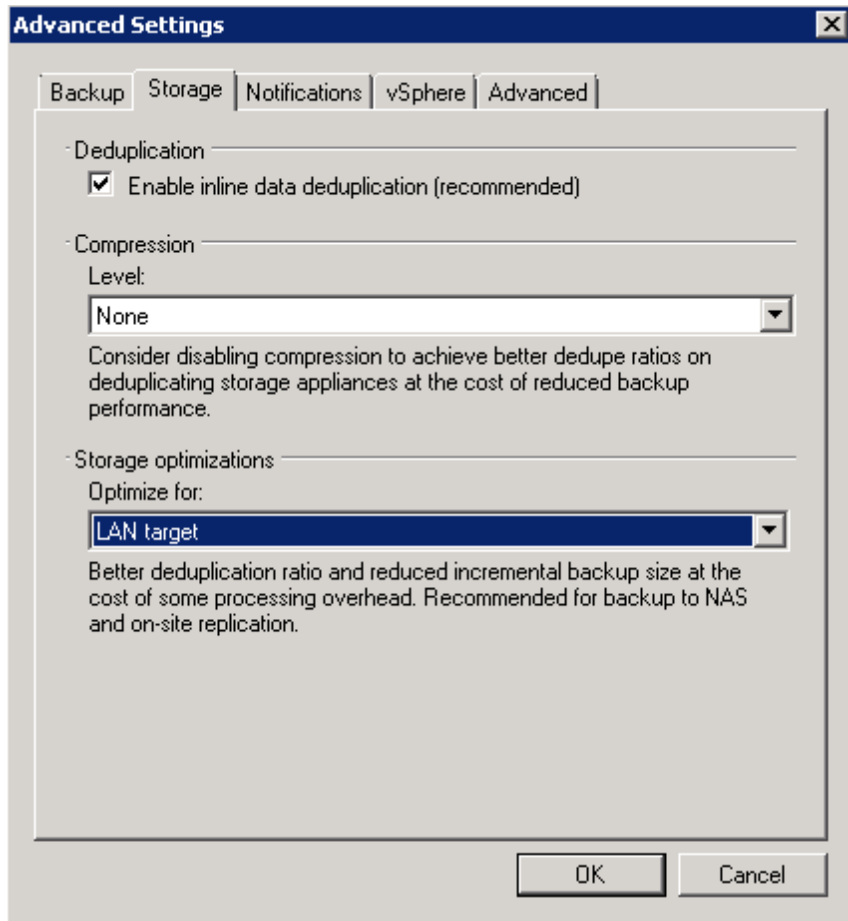
### Best Practices for Maximizing VM Backup Capacity and Retention with HP StoreOnce

Enable deduplication for both Veeam Backup & Replication and the StoreOnce appliance to achieve maximum network throughput.

Set your backup repository to decompress backup images before they are written to disk or disable compression for the backup job. Compressing VM images prior to backing them up to a deduplication appliance reduces backup traffic on the network; however, it will negatively impact the appliance's ability to deduplicate the backup image on disk.

Recommended Backup Mode = Forward Incremental

The type of incremental backup as well as source-side deduplication and compression can be configured in the backup job wizard (click the **Advanced** button). Deduplication is always recommended regardless of the choice of backup target device. Select a setting from the drop-down list (**Storage** tab) to display a detailed description for particular use cases. The following example shows the recommendation for disabling compression on a backup/dedupe appliance.



The selection for the type of incremental backup mode is made in the **Backup** tab of the **Advanced Settings** dialog box. Incremental backup mode is the recommended configuration when backing up to a StoreOnce Backup appliance as shown below.

Incremental backup mode, also known as forward incremental, can be configured for forever incremental backup using synthetic full backups or you can elect to run periodic full backups. A synthetic backup is simply a series of incremental backups rolled into a previous full backup to create a current synthetic “full” backup.

**Best Practices for Maximizing VM Backup Capacity and Retention with HP StoreOnce while Offering Fast Recovery of Critical VMs:** Fast recovery of a VM is predicated on a backup target’s ability to handle random I/O and whether or not “rehydration” of deduplicated data is required. If critical VMs need quick and granular recovery capability, consider backing up to a physical backup proxy server with locally attached disks or a primary storage array to complement the StoreOnce appliance. Direct Attached Storage in a proxy or a disk array can provide a low-cost repository with a much lower RTO than a backup appliance.

## Additional StoreOnce Backup System Capabilities

In addition to presenting highly available CIFS shares and NFS exports for use as backup repositories, the StoreOnce appliances can emulate Virtual Tape Libraries in addition to presenting iSCSI LUNs as backup targets for backing up physical servers using existing backup tools. When deploying B6200 StoreOnce Backup Systems a high availability pair of “active-active” storage controllers, referred to as a couplet, are deployed to increase the fault tolerance level of your high-capacity, highly efficient backup appliance.



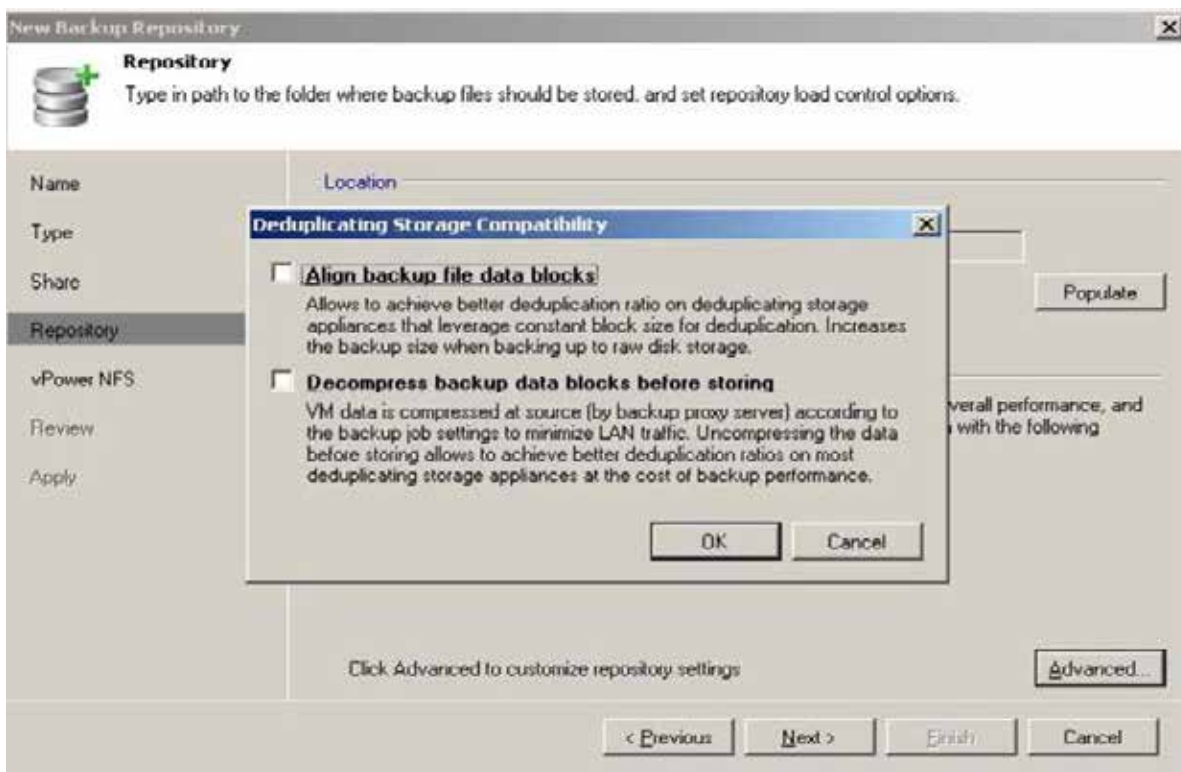
## Configuration Guidelines for Primary Storage Devices

In addition to primary storage of production data from virtual as well as physical servers, disk arrays have benefits when used as secondary storage for backing up and recovering virtual machines. Primary storage arrays, HP Storage solutions beginning with the “P” designation, offer good random I/O performance characteristics required for recovering VMs fast with object-level granularity. The array doesn’t have to be a large mid-range or enterprise array. Arrays such as the P2000/MSA, P4000/LeftHand and the P6300/EVA families have sufficient I/O capability to serve as an adequate backup target in most environments. The trade-off with an online primary storage array, in general, versus a nearline backup appliance with deduplication is fast recovery and granular restoration at the expense of lower storage efficiency and shorter retention periods. Backup appliances are purpose-built to offer a lot of bulk storage for longer retention and overall lower cost per GB at the expense of longer recovery times when compared to general-purpose primary disk arrays.

### Backup Repository Settings: Using Primary Storage as a Backup Repository

#### Data Block Decompression and Data Block Alignment

These settings are found in the **New Backup Repository** wizard (click the **Advanced** button on the Repository step in the wizard). For primary storage arrays, leave these settings unchecked.



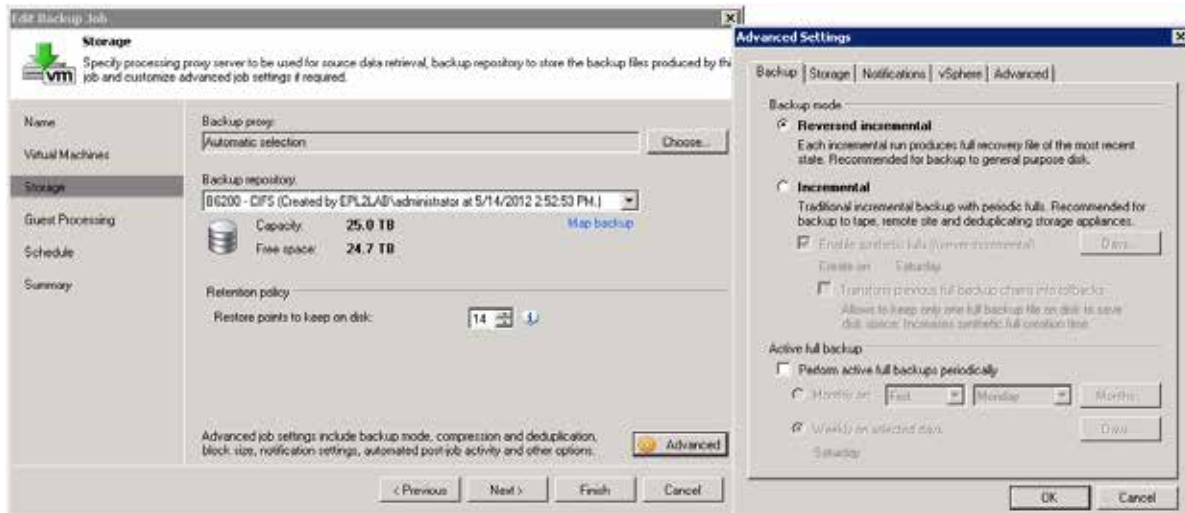


## Backup Job Settings: Using Primary Storage for Backup and Restore

The mode of incremental backup, source-side deduplication and compression can all be configured by clicking the Advanced button in the Storage step of the New Backup Job or Edit Backup Job wizards. Deduplication is always recommended regardless of the choice of backup target device to minimize the backup image size and reduce network traffic. The settings in the drop-down lists under the Backup and Storage tabs display detailed descriptions for particular use cases when selected.

### Backup Mode Settings

Screen Shot: Reversed Incremental Backup Mode

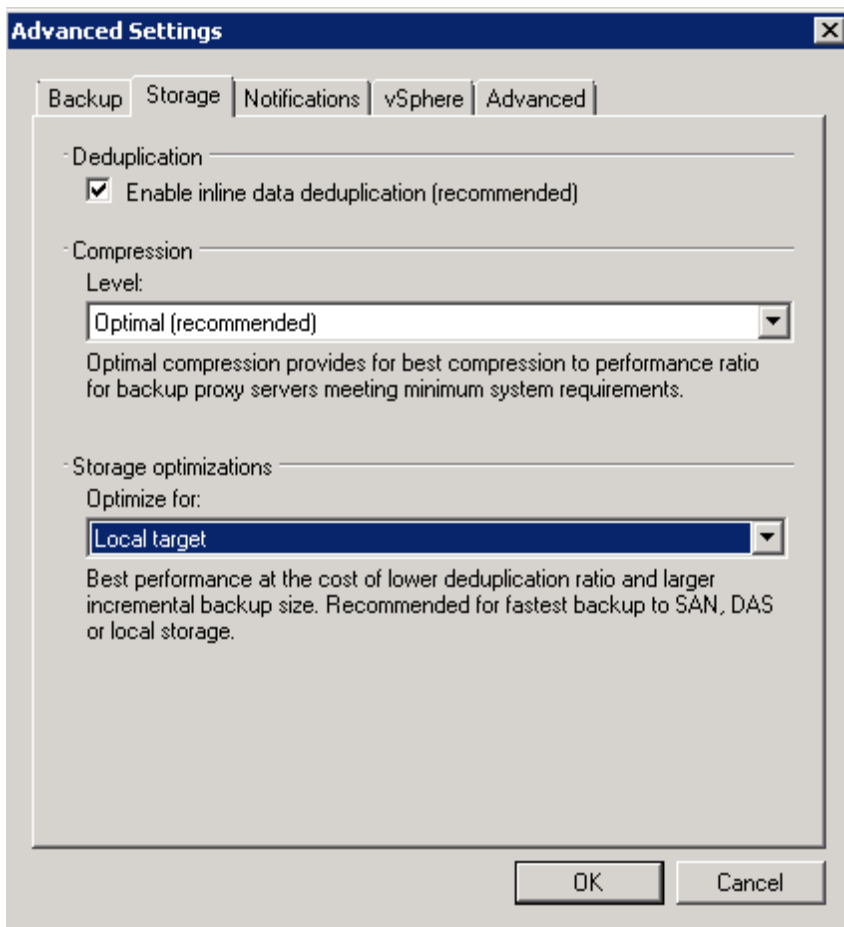


### Setting Compression for Backup Jobs using Primary Storage Arrays

The Edit Backup Jobs wizard Storage tab provides the configuration settings for compression. The following example shows compression enabled, which is the recommendation for backing up to primary disk arrays. The setting in this example is for optimal compression, which strikes a balance between compression, which reduces network traffic during backup, and the CPU load on the backup proxy. A compression setting of “best” yields the smallest backup image and uses less network bandwidth; however, the wizard recommends a six-core processor in the backup proxy.

### Setting Block Size for Backup Jobs using Primary Storage Arrays

The Storage tab optimizations, configured for a local target in this example, determine the block size used for backup and deduplication. The block sizes can be: 256 KB for a backup target over a WAN; 512 KB for backup over a LAN; and 1024 KB for backup targets located directly on the backup server. For a primary storage array the local setting is recommended.



**Note:** If you have closed the Advanced Settings dialog, you can launch it by clicking on the **Advanced** button in the **Edit Backup Jobs** wizard. Open the **Storage** tab in the Advanced Settings dialog to see the configuration options. When you select an option from the drop-down list, a detailed description of the appropriate use case is displayed, ensuring a simple and successful deployment experience.

#### **Best Practices for Maximizing VM Recovery with HP Storage Primary Storage Subsystems**

Design your disk array for fast random read I/O profiles to better enable vPower Instant Restore. Mounting NFS exports on a Linux proxy can improve Instant Restore RTOs by up to 25% in many cases. Enable deduplication and compression with Veeam Backup & Replication in order to reduce backup traffic on the network and to achieve maximum space savings of the backup images.

Recommended Backup Mode = Reversed Incremental

## Summary

Protecting virtual machines requires a fundamentally different approach from legacy physical machine backup. Agentless VM image backup solutions offer lower-cost backup and fast recovery with the appropriate backup target. If the main objectives are longer retention periods and maximum capacity utilization, then a purpose-built StoreOnce backup appliance with deduplication is the best solution. If the main objective is the ability to quickly recover a VM, a file or an application-level object, then DAS in a physical ProLiant proxy or a primary storage solution such as the P4000 LeftHand or P2000 MSA will yield the best RTO.

When using multiple tiers of virtual machine backup repositories, the backup images can be copied or moved from fast disk arrays to high-capacity deduplication appliances (or off-loaded to tape) using post-job activity scripts that can be added via the Backup Job wizard. **Veeam Community Forums** contain examples of how to script the off-loaded VM backup images from one backup target to another, using common third-party copy utilities.

## Primary and Secondary Storage Comparison

Feature	HP P4000 LeftHand	HP StoreOnce Backup Appliance
Fastest recovery, lowest RTO	✓	
Fast application object-level recovery	✓	
SureBackup verification capability	✓	
Longest retention period for backups		✓
Highest deduplication ratio		✓
Lowest capacity overhead		✓
Backup to CIFS shares and tape emulation		✓

## Conclusion

Backup appliances can be deployed with primary disk storage or direct-attached storage in a physical backup server to provide quick recovery down to the application object-level for higher priority VMs. This two-tiered approach provides the long retention and efficient space utilization of a deduplication appliance while providing the lower recovery time (RTO) and granular restoration of a disk array.

It is important to select an agentless backup solution for Hyper-V and VMware environments that will complement your legacy backup environment. HP Storage solutions powered by Veeam allow you to recover VMs quickly at a granular level, while reducing network traffic, and provide space savings on disk.

## Resources

### HP Storage

#### HP StoreOnce Backup System

#### HP-Veeam on Veeam.com

- Download free white papers
- Register for your 60-day trial of Veeam Backup & Replication

### HP Business Support Center

- StoreOnce B6000 Backup System User Guide and the CLI guide

### Veeam Backup & Replication User Guides for Hyper-V or VMware

- Documentation Section

### Veeam Community Forums—Backup & Replication

### Veeam Community Forums—PowerShell Forum

### Veeam Community Forums—Script for copying backup images



---

### Get connected

[hp.com/go/getconnected](http://hp.com/go/getconnected)

Current HP driver, support, and security alerts  
delivered directly to your desktop

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

4AA4-4136ENW, Created November 2012

