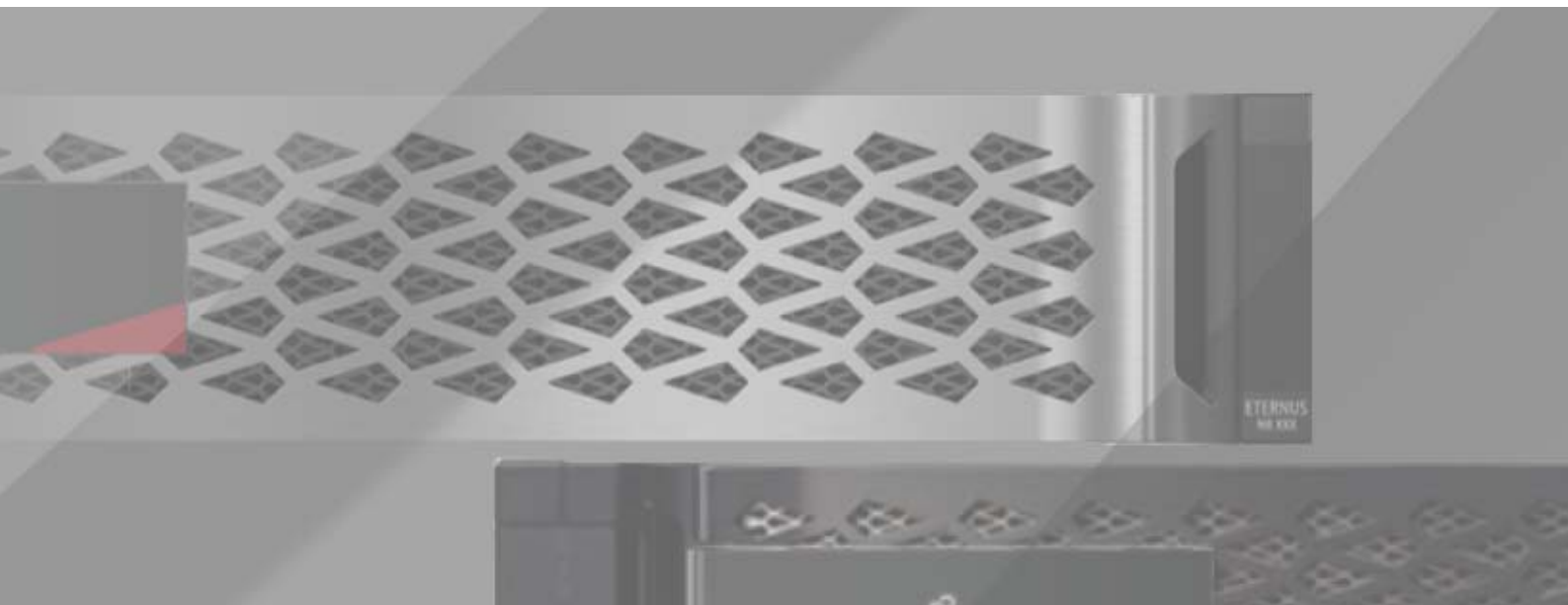


Fujitsu Storage
ETERNUS AB series All-Flash Arrays,
ETERNUS HB series Hybrid Arrays

Reference Architecture and Storage Best Practices with
Veeam Backup & Replication 12



In partnership with Veeam

Table of Contents

1. Executive Summary	8
Introduction	9
About Veeam	9
2. Reference Architecture Overview	10
ETERNUS AB/HB series as Veeam Backup & Replication Repositories for Backup and Archiving	10
ETERNUS AB/HB series as a Veeam Backup & Replication Backup Repository and an Off-Site Cloud Repository	11
ETERNUS AB/HB series as a Veeam Backup & Replication Backup Repository for the ETERNUS AX/HX series Production Storage	12
Deployment Scenarios	13
Simple Deployment	13
Advanced Deployment	14
Distributed Deployment	15
3. Veeam Backup & Replication 12	17
Overview	17
Solution Architecture	17
Veeam Backup Server	17
Backup Proxy	18
Backup Repository	19
4. Veeam Backup & Replication 12 Requirements	20
VMware System Requirements	20
Veeam Backup Server	20
VMware Backup Proxy Server	20
VMware Backup Repository Server	20
Hyper-V System Requirements	21
Veeam Backup Proxy Server (Hyper-V)	21
Off-Host Backup Proxy Server (Hyper-V)	21
Backup Repository Server (Hyper-V)	21
Veeam Sizing Requirements	21

5. Veeam Backup & Replication 12 Design Considerations	22
Direct SAN Access Mode	22
Requirements for the Direct SAN Access Transport Mode	22
Limitations for the Direct SAN Access Transport Mode	22
Data Restore in Direct SAN Access Mode	23
Veeam Backup & Replication 12 Components	24
6. ETERNUS AB/HB series Volume Configuration Guidelines	26
ETERNUS AB/HB series Storage Configuration Guidelines for Backup & Replication 12 Backup Repositories	26
7. ETERNUS AB/HB series Host Configuration Guidelines	27
Host Connectivity	27
Host Connectivity for the ETERNUS HB1000/HB2000	27
Host Connectivity for the ETERNUS AB3100/AB5100/AB6100 and the ETERNUS HB5100/HB5200	27
ETERNUS AB/HB series Host Mapping Configuration for Direct SAN Access	28
8. CPU and Memory Sizing for Veeam and the ETERNUS AB/HB series	29
CPU and Memory Sizing of Backup Server	29
CPU and Memory Sizing of Backup Proxy	29
CPU and Memory Sizing of Backup Repository	30
Example for CPU and Memory Sizing	30
9. Network Planning and Sizing for Veeam and the ETERNUS AB/HB series	31
Performance with Veeam and the ETERNUS AB/HB series	32
Test Environment and Setup	32
Volume Configuration for Performance Testing	33
Backup Performance Results	33
Performance Results with the ETERNUS HB1000/HB2000	33
Performance Best Practices	35
10. SANtricity Plug-Ins for VMware	38
SANtricity Plug-In for VMware vCenter	38

11. Summary 39

List of Figures

Figure 1	ETERNUS AB/HB series as Veeam Backup & Replication repositories for backup and archiving	10
Figure 2	ETERNUS AB/HB series as a Veeam Backup & Replication backup repository and an off-site cloud repository.....	11
Figure 3	ETERNUS AB/HB series as a Veeam Backup & Replication backup repository and off-premises backup repository for the ETERNUS AX/HX series production storage	12
Figure 4	Simple deployment.....	13
Figure 5	Advanced deployment	14
Figure 6	Distributed deployment	15
Figure 7	Data restore in Direct SAN Access mode	23
Figure 8	Backup server mapping.....	28
Figure 9	Network planning tool.....	31
Figure 10	Test environment diagram	32
Figure 11	Processing Speeds with Veeam and the ETERNUS HB1000/HB2000	34
Figure 12	Restricting concurrent tasks per backup proxy	36
Figure 13	Restricting concurrent tasks per backup repository	37

List of Tables

Table 1	Veeam Backup & Replication 12 components and their description.....	24
---------	---	----

Preface

This document outlines the reference architecture and best practices when using the ETERNUS AB/ HB series storage system in a Veeam Backup & Replication 12 environment.

Copyright 2023 Fujitsu Limited

First Edition
October 2023

Trademarks

Third-party trademark information related to this product is available at:

<https://www.fujitsu.com/global/products/computing/storage/eternus/trademarks.html>

Trademark symbols such as ™ and ® are omitted in this document.

About This Manual

Intended Audience

This manual is intended for system administrators who configure and manage operations of the ETERNUS AB/HB, or field engineers who perform maintenance. Refer to this manual as required.

Related Information and Documents

The latest information for the ETERNUS AB/HB is available at:

<https://www.fujitsu.com/global/support/products/computing/storage/manuals-list.html>

Document Conventions

■ Notice Symbols

The following notice symbols are used in this manual:

Caution

Indicates information that you need to observe when using the ETERNUS AB/ HB. Make sure to read the information.

Note

Indicates information and suggestions that supplement the descriptions included in this manual.

1. Executive Summary

■ The Challenge

With data growing at astounding rates, IT managers depend more and more on reliable data backup and recovery. High-growth businesses require a complete data protection solution that is reliable, flexible, and easy to use. Virtualizing an environment provides increased levels of data availability, but meeting aggressive recovery point objectives (RPOs) and recovery time objectives (RTOs) becomes increasingly difficult.

Traditional backup tools were not created for virtualized environments. That fact makes it hard for many organizations to take full advantage of their virtualized environment, and many IT managers struggle with:

- Unreliable backups
- Recovery that takes too long
- High costs that are associated with managing backup data and secondary storage
- An inability to provide reliable and true backups for compliance purposes
- Lost productivity because of management complexity
- The need to scale backup operations for growth

■ The Solution

To meet these challenges, Veeam and Fujitsu collaborated to offer high-performance storage with reliable data protection that is designed for virtualized environments.

Veeam and Fujitsu help you modernize your data protection strategy with a solution that is designed to manage large data volumes and to handle the increasing performance and availability demands of a 21st-century infrastructure.

Veeam Backup & Replication unifies backup and replication in a single solution, increasing the value of backup and reinventing data protection for VMware vSphere and Microsoft Hyper-V virtual environments. The Veeam agentless design provides multiple backup options to meet your needs. Features such as source-side deduplication and compression, change block tracking, parallel processing, and automatic load balancing provide fast and efficient backups.

The ETERNUS AB/HB series provides simple and reliable SAN storage that integrates seamlessly with most application environments. Its modular design helps decrease operating expenses while offering many options for connectivity, capacity, and performance that easily scale to meet the demands of a growing backup environment.

Together, Veeam and Fujitsu create an optimal staging area for backups, reducing backup ingest bottlenecks and providing faster backups through parallel processing.

In addition, Veeam Backup & Replication provides:

- Granular recovery of virtual machines (VMs) and files, including Microsoft Exchange and SharePoint application items
- The ability to automatically verify every backup, VM, and replica every time
- Self-service recovery of VMs and guest files without direct network connection to the VM, user permissions, or the need to deploy costly agents
- Instant VM recovery to recover a failed VM in as little as two minutes
- A choice to back up and recover what you need, where you need it, and when you need it, whether it is on site, on tape, or in the cloud

Veeam and Fujitsu offer the right solution for performance, flexibility, and reliability, providing an impressive modern disaster recovery solution for your vSphere or Hyper-V environment.

This document is a reference architecture for enabling a collaborative backup and recovery solution on the ETERNUS AB/HB series with Veeam Backup & Replication 12 data protection software.

Introduction

This reference architecture guides successful Backup & Replication 12 deployments with the ETERNUS AB/HB series and enables data and application availability.

The ETERNUS AB/HB series and Veeam Backup & Replication 12 combine to offer a data protection and availability solution through this tested reference architecture from industry leaders Fujitsu and Veeam. This solution is optimized for virtual environments, providing drive-to-drive backup and recovery on high-capacity, flexible, performance-oriented ETERNUS AB/HB series storage systems. This solution provides you with superior data management for virtual environments and high availability while also making your data highly available.

The ETERNUS AB/HB series storage systems provide a high-performing backup repository to house Veeam-created backups. With this capability, the recovery technologies that are enabled through Veeam can satisfy stringent RTOs. Recovery technologies such as instant VM recovery, SureBackup, and on-demand sandbox can leverage backup repositories that are capable of high I/O to achieve their full potential.

These technologies enable you to restore from your backups faster and also enable capabilities such as automated recovery verification. The technologies can also leverage backup data as an ad hoc testing environment. This capability changes the way that users have used backups in the past because more benefits are associated with having backups. No longer do backups sit idle, waiting for an emergency restore; you can apply your backups for many creative uses.

Features include:

- Instant VM Recovery of failed VMs in as little as two minutes
- Continuous data protection with the replication function
- Agentless item recovery for Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange, or Oracle
- Transaction-level recovery of SQL Server, Oracle, and PostgreSQL databases
- Automatic recoverability testing of every backup and every replica
- Off-site backups made up to 50 times faster than the speed of standard file copy with built-in WAN acceleration
- Deduplication and compression to minimize storage consumption
- Off-site recovery with one-click site failover and support for facilitated data center migrations with zero data loss

About Veeam

Veeam recognizes the new challenges that companies across the globe face in enabling the always-on business, a business that must operate 24/7/365. To address this challenge, Veeam delivers availability for the modern data center by helping to make sure of recovery time and point objectives (RTPOs) of less than 15 minutes for all applications and data. Information about Veeam is available at www.veeam.com. Veeam's corporate headquarters is in Ohio, U.S.A.

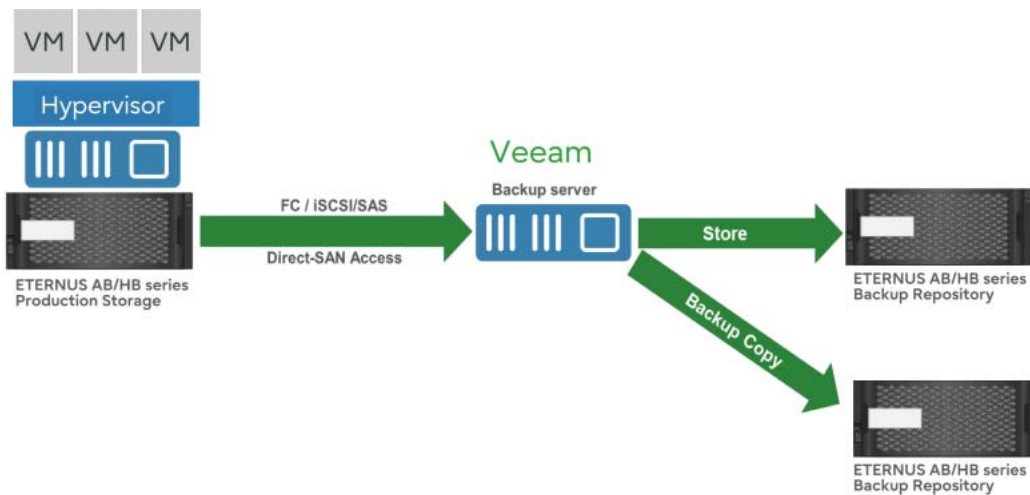
2. Reference Architecture Overview

This chapter details reference architectures that range from those of small environments that protect a few terabytes of data to those in enterprise-size environments with petabytes of data under management.

ETERNUS AB/HB series as Veeam Backup & Replication Repositories for Backup and Archiving

[Figure 1](#) gives us a graphical representation of an ETERNUS AB/HB series and Veeam setup. Veeam provides a backup copy job. This job can be leveraged for backups off the premises or for long-term archiving by using Veeam's built-in grandfather-father-son (GFS)-type retention.

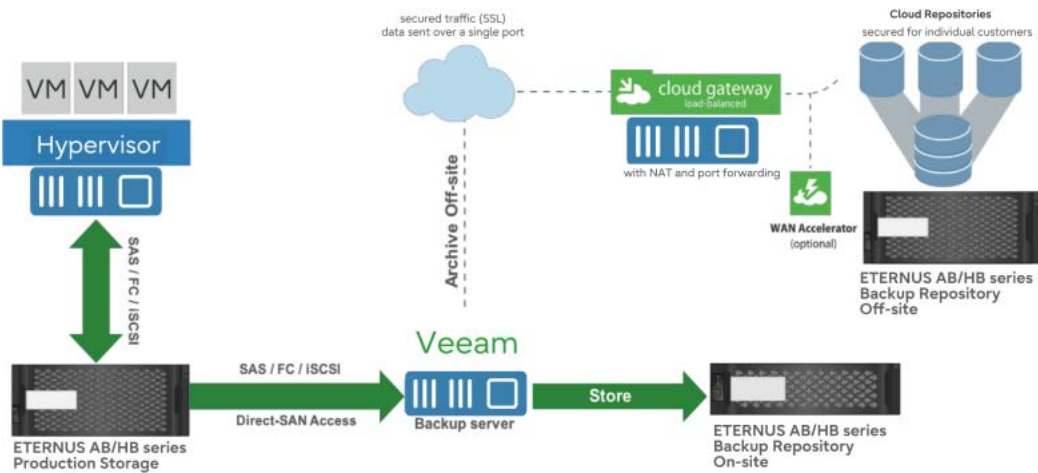
Figure 1 ETERNUS AB/HB series as Veeam Backup & Replication repositories for backup and archiving



ETERNUS AB/HB series as a Veeam Backup & Replication Backup Repository and an Off-Site Cloud Repository

Figure 2 shows the ETERNUS AB/HB series as a Veeam Backup & Replication backup repository and an off-site cloud repository.

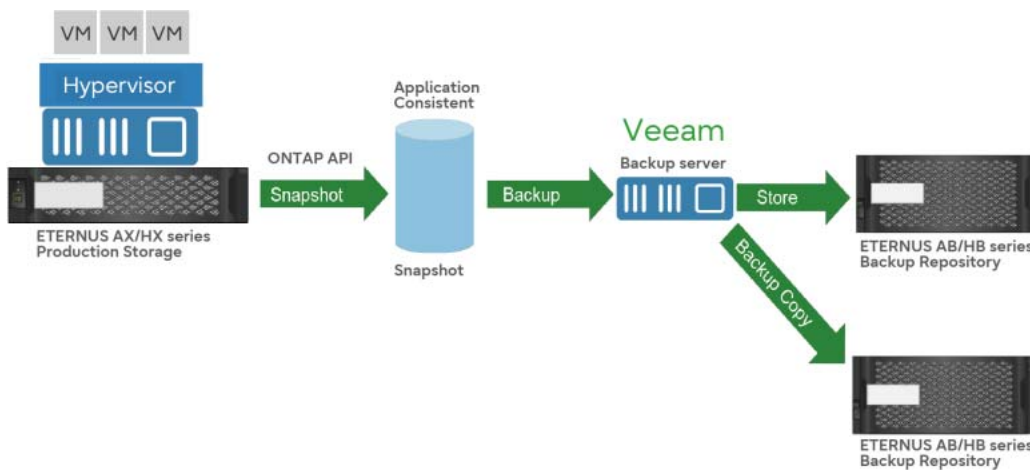
Figure 2 ETERNUS AB/HB series as a Veeam Backup & Replication backup repository and an off-site cloud repository



ETERNUS AB/HB series as a Veeam Backup & Replication Backup Repository for the ETERNUS AX/HX series Production Storage

Figure 3 illustrates Veeam integration with an ETERNUS AX/HX series production storage, with newly created backups going to an ETERNUS AB/HB series for storage. To provide disaster recovery, backups can also be sent off the premises to another backup repository (another ETERNUS AB/HB series). Veeam provides a backup copy job for such scenarios; this job can be leveraged for backups off the premises or for long-term archiving by using Veeam's built-in grandfather-father-son (GFS)-type retention.

Figure 3 ETERNUS AB/HB series as a Veeam Backup & Replication backup repository and off-premises backup repository for the ETERNUS AX/HX series production storage



Note that this function is available only when VMware is used.

Leveraging Veeam's backup copy job architecture is important for achieving that last level of protection. The off-site copy provides safeguards for an entire data center-level disaster. Veeam also provides an optional WAN acceleration component that can help reduce bandwidth utilization. This component can play a huge role in environments that have active-active sites or that have low available bandwidth to start with. The forever-incremental nature of the backup copy job enables only incremental change data to be transmitted off site after the initial copy. Preseeding options are available for the initial transfer of data for environments that need it.

Deployment Scenarios

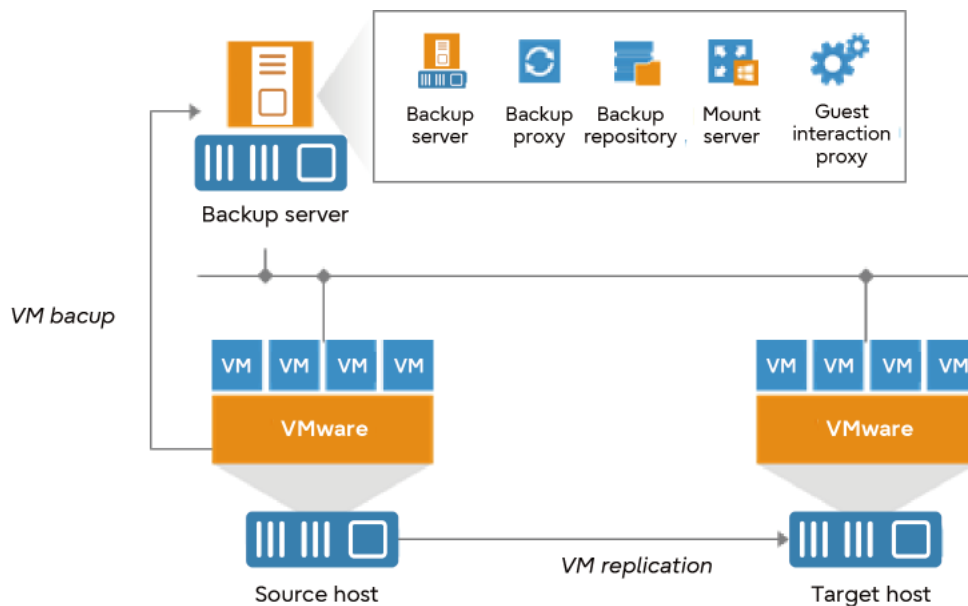
Simple Deployment

In a simple deployment scenario, one instance of Veeam Backup & Replication is installed on a physical or virtual Windows-based machine. This installation is referred to as a Veeam backup server.

Simple deployment (Figure 4) implies that the Veeam backup server fills three major roles:

- It functions as a management point, coordinates all jobs, controls job scheduling, and performs other administrative activities.
- It acts as the default backup proxy for handling job processing and for transferring backup traffic. All services that are necessary for the backup proxy functionality are installed on the Veeam backup server locally.
- It is used as the default backup repository. During installation, Veeam Backup & Replication checks volumes of the machine on which you install the product and identifies a volume with the greatest amount of free drive space. On this volume, Veeam Backup & Replication creates the backup folder that is used as the default backup repository.

Figure 4 Simple deployment



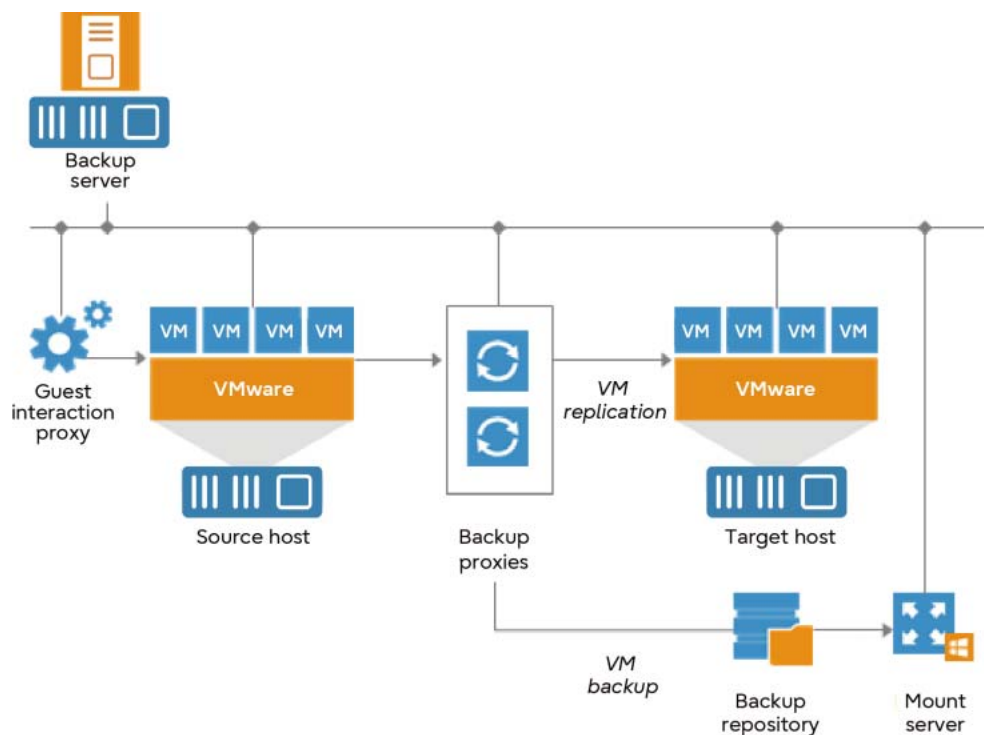
If you plan to back up and replicate only a few VMs or evaluate Veeam Backup & Replication, this configuration is enough to get you started. Veeam Backup & Replication is ready for use right out of the box; as soon as it is installed, you can start using the solution to perform backup and replication operations. To balance the load of backing up and replicating your VMs, you can schedule jobs at different times.

Advanced Deployment

In large-scale virtual environments with numerous jobs, the load on the Veeam backup server is heavy. In this case, it is recommended to use the advanced deployment scenario (Figure 5), which moves the backup workload to dedicated backup proxies and backup repositories.

The essence of the advanced deployment is that the backup proxy takes off part of Veeam backup server activities (namely, it collects and processes data and moves backup traffic from the source to the target). In addition, the Veeam backup server no longer acts as a storage location. The backup proxy transports VM data to a dedicated backup repository that keeps backup files, VM copies, metadata, and so on. The Veeam backup server in this scenario functions as a manager for deploying and maintaining backup proxies and repositories.

Figure 5 Advanced deployment



To deploy a backup proxy or a backup repository, add a server to Veeam Backup & Replication and assign a proxy or a repository role to it, as applicable. Veeam Backup & Replication automatically installs lightweight components and services on these servers. A backup proxy does not require a separate database. All settings are stored centrally, within the database that the Veeam backup server uses. From Veeam Backup & Replication 12 and later, a database can be selected from PostgreSQL or SQL Server.

With the advanced deployment scenario, you can easily meet your current and future data protection requirements. You can expand your backup infrastructure horizontally in a matter of minutes to match the amount of data that you want to process and the available network throughput. Instead of growing the number of backup servers or constantly tuning job scheduling, you can install multiple backup proxies and repositories and distribute the backup workload among them. The installation process is fully automated, which simplifies deploying and maintaining the backup infrastructure in your virtual environment.

In virtual environments with several proxies, Veeam Backup & Replication dynamically distributes backup traffic among those proxies. You can explicitly map a job to a specific proxy, or you can let Veeam Backup & Replication choose the most suitable proxy. If you opt for the latter, Veeam Backup & Replication checks the settings of available proxies and selects the most appropriate one for the job. The proxy server to be used should have access to the source and target hosts as well as to the backup repository to which files are written.

The advanced deployment scenario can be a good choice for backing up and replicating off site. You can deploy a backup proxy in the production site and another one in the disaster recovery (DR) site, closer to the backup repository. When a job is performed, backup proxies on both sides establish a stable connection, so this architecture also allows efficient data transport over a slow network connection or WAN.

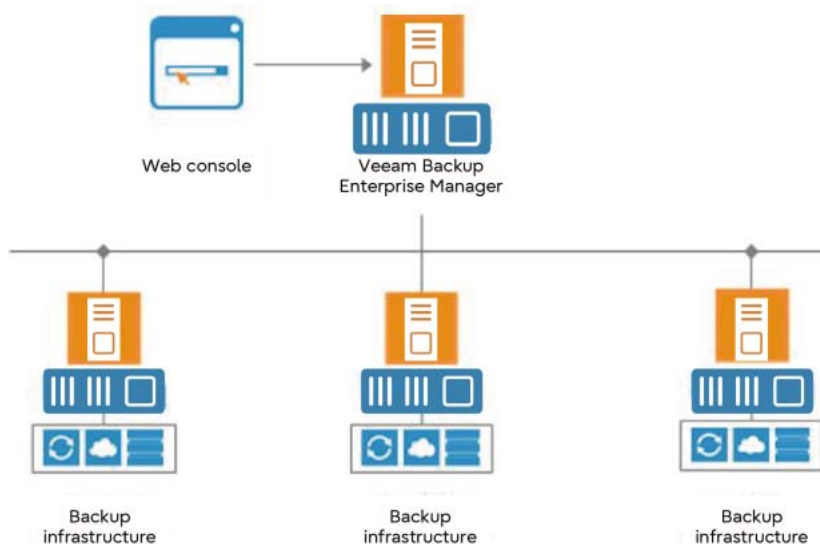
To regulate backup load, you can specify the maximum number of concurrent tasks per proxy and set up throttling rules to limit proxy bandwidth.

Another advantage of the advanced deployment scenario is that it contributes to high availability. Jobs can migrate between proxies if one of them becomes overloaded or unavailable.

Distributed Deployment

It is recommended to use the distributed deployment scenario ([Figure 6](#)) for large geographically dispersed virtual environments with multiple Veeam backup servers that are installed across different sites. These backup servers are federated under Veeam Backup Enterprise Manager, an optional component that provides centralized management and reporting for these servers through a web interface.

Figure 6 Distributed deployment



Veeam Backup Enterprise Manager collects data from Veeam backup servers and enables you to run backup and replication jobs across the entire backup infrastructure through a single interface. You can also edit those jobs and clone jobs by using a single job as a template. Enterprise Manager also provides reporting data for various areas (for example, all jobs that were performed within the past 24 hours or 7 days, all VMs that were engaged in these jobs, and so on).

By using indexing data that is consolidated on one server, Veeam Backup Enterprise Manager provides advanced capabilities to search for VM guest OS files in VM backups that are created on all Veeam backup servers. You can search even if the files are stored in repositories on different sites, and you can recover them in a single click. Searching for VM guest OS files is enabled through Veeam Backup Enterprise Manager; to streamline the search process, you can optionally deploy a Veeam Backup Search server in your backup infrastructure.

With flexible delegation options and security roles, IT administrators can delegate the necessary file restore or VM restore rights to authorized personnel in your organization. For example, they can allow database administrators to restore Oracle or SQL Server VMs. Note that delegation of restore rights is a VMware only function.

If you use Veeam Backup Enterprise Manager in your backup infrastructure, you do not need to install licenses on every Veeam backup server that you deploy. Instead, you can install one license on the Veeam Backup Enterprise Manager server, and it is applied to all servers across your backup infrastructure. This approach simplifies tracking license usage and license updates across multiple Veeam backup servers.

In addition, VMware administrators can benefit from the Veeam plug-in for vSphere Web Client, which can be installed by using Veeam Backup Enterprise Manager. Administrators can analyze cumulative information about used and available storage space; view statistics on processed VMs; and review success, warning, and failure counts for all jobs. Administrators can also easily identify unprotected VMs and perform capacity planning for repositories, all directly from vSphere.

3. Veeam Backup & Replication 12

Overview

Veeam Backup & Replication is a data protection and disaster recovery solution for VMware vSphere and Microsoft Hyper-V virtual environments of any size or complexity. By combining all the necessary functions in one intuitive interface, Veeam Backup & Replication solves the most critical problems of virtualized infrastructure management. The solution also protects mission-critical VMs from both hardware and software failures.

Solution Architecture

Veeam Backup & Replication is composed of the following three elements:

- Backup server
- Backup proxy
- Backup repository

Veeam Backup Server

The Veeam backup server is a Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component in the backup infrastructure that fills the role of the configuration and control center. The Veeam backup server performs all types of administrative activities. This server:

- Coordinates backup, replication, recovery verification, and restore tasks
- Controls job scheduling and resource allocation
- Is used to set up and manage backup infrastructure components and to specify global settings for the backup infrastructure

In addition to its primary functions, a newly deployed Veeam backup server also acts as a default backup proxy and the backup repository (it manages data handling and data storing tasks).

The Veeam backup server uses the following services and components:

- **Veeam Backup Service** is a Windows service that coordinates all the operations that Veeam Backup & Replication performs, such as backup, replication, recovery verification, and restore tasks. The Veeam Backup Service runs under the local system account or an account that has the local administrator permissions on the backup server.
- **Veeam Broker Service** interacts with the virtual infrastructure to collect and cache the virtual infrastructure topology. It jobs and tasks query information about the virtual infrastructure topology from the Broker Service, which accelerates job and task performance.
- **Veeam Guest Catalog Service** manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files. Index data is stored in the Veeam Backup Catalog, which is a folder on the backup server. The Veeam Guest Catalog Service running on the backup server works in conjunction with search components that are installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft Search Server.
- **Veeam Mount Service** mounts backups and replicas for file-level access, browsing the VM guest file system and restoring VM guest OS files and application items to the original location.
- **Veeam backup proxy services:** In addition to dedicated services, the backup server runs a set of data mover services. For details, see ["Backup Proxy" \(page 18\)](#).

- **Veeam Backup & Replication Configuration database** stores data about the backup infrastructure, jobs, sessions, and so on. The database instance can be on a SQL Server that is installed either locally (on the same machine where the backup server is running) or remotely.
- **Veeam Backup & Replication console** provides the application UI and allows user access to the application's functionality.
- **Veeam Backup PowerShell snap-in** is an extension for Microsoft Windows PowerShell 5.1. Veeam Backup PowerShell adds a set of cmdlets that enable you to perform backup, replication, and recovery tasks through the PowerShell CLI or run custom scripts to fully automate Veeam Backup & Replication operation.

Backup Proxy

When Veeam Backup & Replication is first installed, the Veeam backup server coordinates all job activities and handles data traffic. So, when you run a backup, replication, VM copy, or VM migration job or perform restore operations, VM data is moved from the source to the target through the Veeam backup server. This scenario is acceptable for virtual environments in which few backup jobs are performed. In large-scale environments, however, the workload on the Veeam backup server is significant.

To take the workload off the Veeam backup server, Veeam Backup & Replication uses backup proxies. A backup proxy is an architecture component that sits between the data source and the target and is used to process jobs and to deliver backup traffic. In particular, the backup proxy tasks include retrieving VM data from the production storage. The tasks also include compressing the data and sending it to the backup repository (for example, if you run a backup job) or to another backup proxy (for example, if you run a replication job). As the data handling task is assigned to the backup proxy, the Veeam backup server becomes the point of control for dispatching jobs to proxy servers.

The role of a backup proxy can be assigned to a dedicated Windows Server or Linux (physical or virtual) in your virtual environment. You can deploy backup proxies both in the primary site and in remote sites. To optimize the performance of several concurrent jobs, you can use a number of backup proxies. In this case, Veeam Backup & Replication distributes the backup workload between available backup proxies.

By using backup proxies, you can easily scale your backup infrastructure up and down based on your demands. Backup proxies run lightweight services that take a few seconds to deploy. Deployment is fully automated: Veeam Backup & Replication installs the necessary components on a Windows-based server when you add it to the product console. As soon as you assign the role of a backup proxy to the added server, Veeam Backup & Replication starts the required services on it.

The primary role of the backup proxy is to provide an optimal route for backup traffic and to enable efficient data transfer. Therefore, when deploying a backup proxy, you must analyze the 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 (starting with the most efficient):

- A machine used as a backup proxy should have direct access to the storage on which VMs reside or to the storage to which VM data is written. In this way, the backup proxy retrieves data directly from the datastore, bypassing the LAN.
- The backup proxy can be a VM with HotAdd access to VM drives on the datastore. This type of proxy also enables LAN-free data transfer.
- If neither of the preceding scenarios is possible, you have alternatives. You can assign the role of the backup proxy to a machine on the network that is closer to the source or closer to the target storage with which the proxy works. In this case, VM data is transported over the LAN by using the Network Block Device (NBD) protocol.

Depending on the type of backup proxy and your backup architecture, the backup proxy can use one of the following data transport modes: Direct SAN Access, Virtual Appliance, or Network. If the VM drives are on the SAN storage and the SAN storage is added to the Veeam Backup & Replication console, the backup proxy can also use the Backup from Storage Snapshots mode. You can select the transport mode or let Veeam Backup & Replication automatically choose it.

The backup proxy uses the following services and components:

- **Veeam Installer Service** is an auxiliary service that is installed and started on any Windows Server after it is added to the list of managed servers in the Veeam Backup & Replication console. This service analyzes the system and installs and upgrades necessary components and services depending on the role that is selected for the server.
- **Veeam Transport** is responsible for deploying and coordinating executable modules that act as data movers and that perform the main job activities on behalf of Veeam Backup & Replication. These activities include communicating with VMware Tools, copying VM files, performing data deduplication and compression, and so on.

Backup Repository

A backup repository is a location that Veeam Backup & Replication jobs use to store backup files, copies of VMs, and metadata for replicated VMs. Technically, a backup repository is a folder on the backup storage. By assigning different repositories to jobs and by limiting the number of parallel jobs for each one, you can balance the load across your backup infrastructure.

4. Veeam Backup & Replication 12 Requirements

VMware System Requirements

Veeam Backup Server

For the specifications and requirements of the Veeam backup server with VMware, refer to the following website.

https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120#backup-server

Note

- You might plan to back up VMs that are running Microsoft Windows Server 2016, and data deduplication is enabled for some VM volumes. In that case, it is recommended to deploy Veeam Backup & Replication on a machine that is running Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2016 with data deduplication enabled. Otherwise, some types of restore operations for these VMs (such as Microsoft Windows File Level Recovery) might fail.
 - Because of its limitations, Microsoft SQL Server Express Edition can be used only for evaluation purposes or for a small-scale production environment. For environments with several VMs, you must install a fully functional commercial version of Microsoft SQL Server.
-

VMware Backup Proxy Server

For the specifications and requirements of the VMware backup proxy server, refer to the following website.

https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120#vmware-backup-proxy

VMware Backup Repository Server

For the specifications and requirements of the VMware backup repository server, refer to the following website.

https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120#backup-repository

Hyper-V System Requirements

Veeam Backup Proxy Server (Hyper-V)

For the specifications and requirements of the Veeam backup proxy server with Microsoft Hyper-V, refer to the following website.

https://helpcenter.veeam.com/docs/backup/hyperv/system_requirements.html?ver=120#hyper-v-off-host-backup-proxy-hyper-v-host-as-backup-proxy

Note

- You might plan to back up VMs that are running Microsoft Windows Server 2016, and data deduplication is enabled for some VM volumes. In that case, it is recommended to deploy Veeam Backup & Replication on a machine that is running Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2016 with data deduplication enabled. Otherwise, some types of restore operations for these VMs (such as Microsoft Windows File Level Recovery) might fail.
- Because of its limitations, Microsoft SQL Server Express Edition can be used only for evaluation or in a small-scale production environment. For environments with several VMs, you must install a fully functional commercial version of Microsoft SQL Server.

Off-Host Backup Proxy Server (Hyper-V)

For the specifications and requirements of an off-host backup proxy server with Hyper-V, refer to the following website.

https://helpcenter.veeam.com/docs/backup/hyperv/system_requirements.html?ver=120#hyper-v-off-host-backup-proxy-hyper-v-host-as-backup-proxy

Backup Repository Server (Hyper-V)

For the specifications and requirements of a backup repository server with Hyper-V, refer to the following website.

https://helpcenter.veeam.com/docs/backup/hyperv/system_requirements.html?ver=120#backup-repository

Veeam Sizing Requirements

For Veeam sizing requirements, refer to the following websites.

- VMware vSphere
https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=120
- Microsoft Hyper-V
https://helpcenter.veeam.com/docs/backup/hyperv/system_requirements.html?ver=120

5. Veeam Backup & Replication 12 Design Considerations

Direct SAN Access Mode

Veeam proxy servers directly connect to the storage fabric because it is the fastest way to perform backups with Backup & Replication. That approach allows a LAN-free backup and provides the possibility to leverage storage Snapshot copies on supported storage systems such as ETRENUS HX series. Fast backup speed is critical for low RPOs.

An often-discussed point about Direct SAN Access for the Veeam proxy is the possibility that the Veeam proxy can mount VMware Virtual Machine File System (VMFS) LUNs and write a Windows signature onto the LUN. Doing so results in an inaccessible VMFS, which requires VMware support to fix the issue. Veeam Knowledge Base (KB) article #1446 provides instructions on how to configure SAN access for use with Veeam Backup & Replication.

The SAN policy is set to Offline Shared by default. However, even if an administrator changed the policy to Online All, Veeam reverts the policy back to Offline Shared. The result is that Windows does not mount and resignature VMFS LUNs unless an administrator changes this setting again or manually mounts VMFS LUNs while ignoring Windows warnings. It is recommended to use the Direct SAN Access transport mode for VMs whose drives are on shared VMFS SAN LUNs that are connected to ESXi hosts through FC or iSCSI.

In the Direct SAN Access transport mode, Veeam Backup & Replication leverages VMware VADP to transport VM data directly from and to FC and iSCSI storage over the SAN. VM data travels over the SAN, bypassing ESXi hosts and the LAN. The Direct SAN Access transport method provides the fastest data transfer speed and produces no load on the production network.

You can use the Direct SAN Access transport mode for all operations in which the backup proxy is engaged, including:

- Backup
- Replication
- Full VM restore
- VM drive restore
- Replica failback
- Quick migration
- VMcopy

Requirements for the Direct SAN Access Transport Mode

For the requirements for the Direct SAN Access transport mode, refer to the following website.
https://helpcenter.veeam.com/docs/backup/vsphere/direct_san_access.html?ver=120#requirements-for-the-direct-san-access-mode

Limitations for the Direct SAN Access Transport Mode

For the limitations for Direct SAN Access transport mode, refer to the following website.
https://helpcenter.veeam.com/docs/backup/vsphere/direct_san_access.html?ver=120#limitations-for-the-direct-san-access-mode

Data Restore in Direct SAN Access Mode

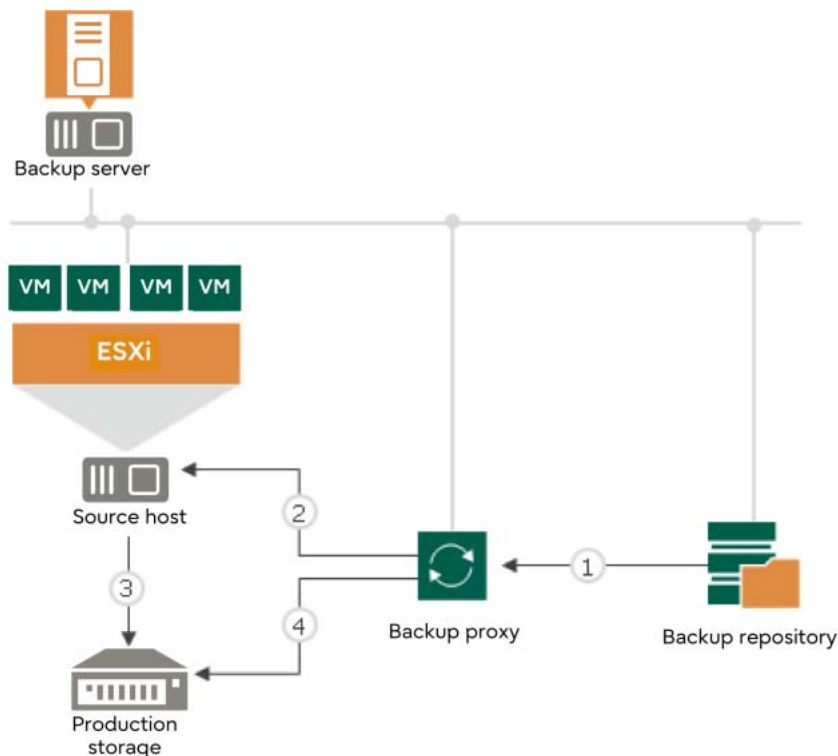
Data restore in the Direct SAN Access transport mode includes the following steps (see [Figure 7](#)):

Procedure ▶▶▶

- 1 The backup proxy retrieves data blocks from the backup repository or a datastore in the target site.
- 2 The backup proxy sends a request to the ESXi host on the source site to restore data to a necessary datastore.
- 3 The ESXi host on the source site allocates space on the datastore.
- 4 Data blocks that are obtained from the backup proxy are written to the datastore.



Figure 7 Data restore in Direct SAN Access mode



You can use the Direct SAN Access transport mode to restore VMs only with thick drives. Before VM data is restored, the ESXi host must allocate space for the restored VM drive on the datastore:

- When thick drives are restored, the ESXi host allocates space on the drive before writing VM data.
- When thin drives are restored, the ESXi host attempts to allocate space dynamically as requests for data block restores are received.

As a result, restoring thin drives involves extra allocation overhead when compared with restoring thick drives, which results in decreased performance.

To restore VMs with thin drives, you can use the Virtual Appliance mode or the Network mode. If you plan to process a VM that has both thin and thick drives, select the Direct SAN Access transport mode and choose to fail over to the Network mode if the SAN becomes inaccessible. In that case, Veeam Backup & Replication uses the Direct SAN Access transport mode to restore thick drives and uses the Network transport mode to restore thin drives. Alternatively, you can restore all VM drives as thick.

Veeam Backup & Replication 12 Components

[Table 1](#) describes each component in Veeam Backup & Replication 12.

Table 1 Veeam Backup & Replication 12 components and their description

Component	Description
Veeam backup server	<p>The Veeam backup server is a Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component in the backup infrastructure that fills the role of the configuration and control center. The Veeam backup server performs all types of administrative activities:</p> <ul style="list-style-type: none"> • Coordinates backup, replication, recovery verification, and restore tasks • Controls job scheduling and resource allocation • Is used to set up and manage backup infrastructure components and to specify global settings for the backup infrastructure <p>In addition to its primary functions, a newly deployed Veeam backup server also performs the roles of the default backup proxy and the backup repository (it manages data handling and data storing tasks).</p>
Veeam Backup Service	<p>This Windows service coordinates all the operations that are performed by Veeam Backup & Replication, such as backup, replication, recovery verification, and restore tasks. The Veeam Backup Service runs under the local system account or the account that has the local administrator permissions on the Veeam backup server.</p>
Veeam Backup Shell	<p>The Veeam Backup Shell provides the application UI and enables user access to the application's functionality.</p>
Veeam Backup Catalog Service	<p>This Windows service manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files. Index data is stored in the Veeam Backup Catalog, a folder on the Veeam backup server. The Veeam Backup Catalog Service running on the Veeam backup server works with search components that are installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft Search Server.</p>
Veeam Backup Configuration Server database	<p>This database is used by Veeam Backup Service, Veeam Backup Shell, and Veeam Backup Catalog Service to store data about the backup infrastructure, jobs, sessions, and so on. The database instance can be on a SQL Server installed either locally (on the same machine where the Veeam backup server runs) or remotely.</p>

5. Veeam Backup & Replication 12 Design Considerations
 Veeam Backup & Replication 12 Components

Component	Description
Veeam Backup PowerShell snap-in	This snap-in is an extension for Microsoft Windows PowerShell 5.1. Veeam Backup PowerShell adds a set of cmdlets to enable you to perform backup, replication, and recovery tasks through the PowerShell CLI or run custom scripts to fully automate Veeam Backup & Replication operation.
Backup proxy services	In addition to dedicated services, the Veeam backup server runs a set of Data Mover Services.
Backup proxy	A backup proxy is an architecture component that sits between the data source and the target and is used to process jobs and deliver backup traffic. The backup proxy retrieves VM data from the production storage. It also compresses the retrieved data and sends it to the backup repository (for example, if you run a backup job) or to another backup proxy (for example, if you run a replication job). As the data handling task is assigned to the backup proxy, the Veeam backup server becomes the point of control for dispatching jobs to proxy servers.
Backup repository	A backup repository is a location that Veeam Backup & Replication jobs use to store backup files, copies of VMs, and metadata for replicated VMs. Technically, a backup repository is a folder on the backup storage. By assigning different repositories to jobs and by limiting the number of parallel jobs for each one, you can balance the load across your backup infrastructure.

6. ETERNUS AB/HB series Volume Configuration Guidelines

ETERNUS AB/HB series Storage Configuration Guidelines for Backup & Replication 12 Backup Repositories

It is recommended to avoid thin volumes while setting up the ETERNUS AB/HB series with Veeam.

For **optimal performance**, Fujitsu recommends that you follow these guidelines:

- Use RAID 6 (8+2) volume groups.
- Create multiple volume groups, having an even number when possible so that you can achieve balance between owning controllers. Make sure of drawer loss protection (DLP) when applicable to reduce the risk of data unavailability and/or data loss.
- Create a single standard (not thin) volume per volume group.
- When creating the volumes, select a 512KB segment size to match the 512KB transfer size that Veeam Backup & Replication presents as a sequential write to the system after sequencing I/O.
- Run multiple backup jobs to each repository.

Note

The preceding setup can be configured without any hot spares too, to achieve better performance in case of drive failure. A caveat is that data loss might occur if more than two drives fail at once.

For a **large configuration**, Fujitsu recommends that you follow these guidelines:

- Use Dynamic Disk Pools (DDP) technology to maximize ease of use and for fast rebuild times.
- Create multiple Dynamic Disk Pools (DDP), having an even number when possible so that you can achieve balance between owning controllers. Make sure of DLP when applicable to reduce the risk of data unavailability and/or data loss.
- Create a single standard (not thin) volume per DDP.
- When creating the volumes with DDP, the default segment size is 128KB. No additional selection is required.
- Run multiple backup jobs to each repository.

Note

RAID 10 was also tested. It can also be considered as an option for volume configuration, but it is not recommended due to a single parity and capacity penalty. Also, write throughput performance of RAID 6 and DDP is better in comparison to RAID 10.

7. ETERNUS AB/HB series Host Configuration Guidelines

Host Connectivity

The ETERNUS AB/HB series provides multiple options for connectivity.

Host Connectivity for the ETERNUS HB1000/HB2000

The ETERNUS HB1000/HB2000 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Either two optical FC/iSCSI or two RJ-45 iSCSI baseboard ports for host connection
- SAS drive expansion ports to attach expansion drive shelves

Note

Adding an optional HIC is only needed if you want to use the SAS protocol, need more than two host ports per controller, or want to use both FC and iSCSI protocols.

Host Connectivity for the ETERNUS AB3100/AB5100/AB6100 and the ETERNUS HB5100/HB5200

The ETERNUS AB3100/AB5100/AB6100 and the ETERNUS HB5100/HB5200 controllers have the following base hardware features:

- Dual Ethernet ports for management-related activities
- Dual optical 16/32Gbps FC or 10/25Gbps iSCSI baseboard ports for host connection
- Dual 12Gb SAS drive expansion ports to attach expansion drive shelves

Note

Adding the optional HICs for the ETERNUS HB5100/HB5200 controller provides faster host interfaces for iSCSI, FC, and IB.

For an overview about the different host I/O interfaces for the ETERNUS HB series controllers, refer to the following websites.

- ETERNUS HB2100
<https://www.fujitsu.com/global/products/computing/storage/disk/eternus-hb/hb2100/index.html#specs>
- ETERNUS HB2200
<https://www.fujitsu.com/global/products/computing/storage/disk/eternus-hb/hb2200/index.html#specs>
- ETERNUS HB2300
<https://www.fujitsu.com/global/products/computing/storage/disk/eternus-hb/hb2300/index.html#specs>
- ETERNUS HB5100
<https://www.fujitsu.com/global/products/computing/storage/disk/eternus-hb/hb5100/index.html#specs>

- ETERNUS HB5200
<https://www.fujitsu.com/global/products/computing/storage/disk/eternus-hb/hb5200/index.html#specs>

This configuration might not be ideal for larger environments in which Veeam's distributed architecture is implemented and in which multiple proxy servers process backup data. Having a dedicated network for backup targets might make more sense in those cases. Either way, the options are there for any environment, and Veeam provides a bottleneck detector to help optimize the backup data flow as you progress through your implementation.

ETERNUS AB/HB series Host Mapping Configuration for Direct SAN Access

On the ETERNUS AB/HB series that hosts the virtual environment's storage, verify that the Veeam backup server is associated with the same host group as the host of the virtual environment. See the example shown for SANtricity in [Figure 8](#).

Host_Cluster_Veeam is the host cluster that has the ESXi Server (Host_ESXi_Server) and the Veeam Server (Host_Veeam_Server). As seen, all 16 volumes are shared between both the host members.

Figure 8 Backup server mapping

Name	Type	Associated Objects	Total Assigned Volumes	Reported Capacity (GiB)	Host Type	Edit
- Default Cluster	Default Cluster	1 Host Cluster(s) 2 Host(s)	16	23600.00	Windows	
- Host_Cluster_Veeam	Cluster	Default Cluster 2 Host(s)	16	23600.00	Windows	
Host_ESXi_Server	Host Member	Host_Cluster_Veeam	16	23600.00	Windows	
Host_Veeam_Server	Host Member	Host_Cluster_Veeam	16	23600.00	Windows	

Total rows: 4

As a result of hosting both the virtual environment and the backup repository on the ETERNUS AB/HB series, Veeam Backup & Replication has resource location awareness in the environment. The resulting data transfers take place over the SAN.

8. CPU and Memory Sizing for Veeam and the ETERNUS AB/HB series

This section covers the CPU and memory considerations when setting up Veeam with the ETERNUS AB/HB series. Three components need to be considered during this sizing: backup server, repository, and proxy.

The backup server is the core component. Features and component requirements affect your decision how to install the backup server (for example, one data center or multiple locations). It could mean that you choose to install additional backup servers or services in remote locations to optimize the data streams.

Sizing with Veeam is cumulative in respect to configurations. If you want to create an all-in-one appliance (appliance model), add all the resource requirements together (CPU + memory) for backup server, repository, and proxy to understand what in total you will need. The same goes if you only want to have proxy and repository in one host and server independently.

CPU and Memory Sizing of Backup Server

Recommended Veeam backup server configuration is 1 CPU core (physical or virtual) and 4GB RAM per 10 concurrently running jobs. Concurrent jobs include any running backup or replication jobs as well as any job with a continuous schedule such as backup copy jobs and tape jobs. (Concurrent job is a job that processes a single VM with a single virtual drive.) The minimum recommendation is 2 CPU cores and 8GB RAM.

It is recommended to group multiple virtual machines into a single job for better efficiency and resource usage. With default configuration, it is recommended to configure at minimum a VM with a single drive up to around 30 VMs per job.

CPU and Memory Sizing of Backup Proxy

Getting the right amount of processing power is essential to achieving the RTPO defined by the business.

It is a best practice to plan for 1 physical core or 1 vCPU and 2GB of RAM for each of the tasks. A task processes 1 VM drive at a time, and CPU/RAM resources are used for inline data deduplication, compression, encryption and other features that are running on the proxy itself. A task as described earlier should ideally have around 30 VMs.

CPU and Memory Sizing of Backup Repository

In midsized or enterprise environments, the recommended amount of CPU for a repository is 1 core per concurrent job and 4GB RAM per core that processes data on a repository server. At least 2 cores allow for the operating system to be more responsive.

Example for CPU and Memory Sizing

Consider an all-in-one configuration (physical) set up for 10TB of data or 100 VMs:

- Total number of jobs is 100 VMs; 30 VMs per job = 4 (rounding it up to a higher number)
- CPU and memory for backup server = 1 CPU core and 4GB of RAM (refer to "[CPU and Memory Sizing of Backup Server](#)" (page 29))
- CPU and memory for backup proxy = 4 CPU core and 8GB of RAM (refer to "[CPU and Memory Sizing of Backup Proxy](#)" (page 29))
- CPU and memory for backup repository = 4 CPU core and 16GB of RAM (refer to "[CPU and Memory Sizing of Backup Repository](#)" (page 30))

Total is sum of the three, which gives us 10 CPU cores (rounded up to 10, because 9 is not possible) and around 32GB of RAM (including a couple of gigabytes for operating system and so on, hence 32GB instead of 29GB).

Note

Refer to <https://bp.veeam.expert/> for further details.

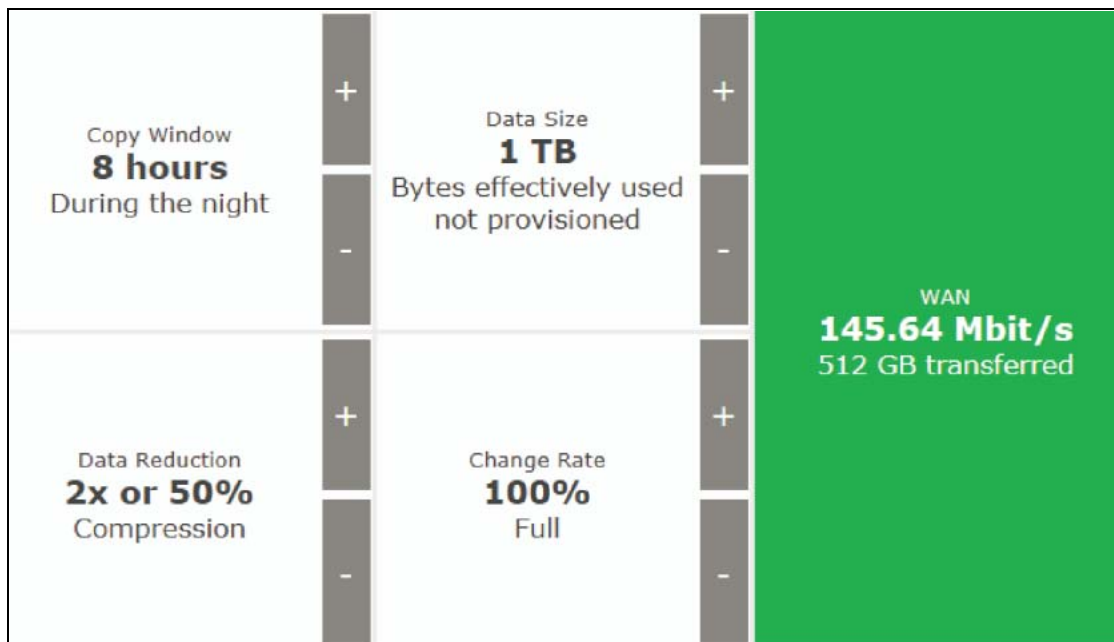
9. Network Planning and Sizing for Veeam and the ETERNUS AB/HB series

Veeam has an unofficial tool that can assist in network planning. It can be accessed at <http://rps.dewin.me/bandwidth/>.

Figure 9 gives a snapshot of the tool. Overall it has four parameters that need input, based on which it gives an approximate bandwidth required.

- Copy Window: This parameter is divided into four categories; select the input based on the expected copy window:
 - Short Slot: Your copy window is below 6 hours.
 - During the night: Your copy window is below 8 to 9 hours.
 - During business hours: Your copy window is below 24 hours.
 - Over multiple days: Your copy window can span multiple days.
- Data Size: Make sure you input the bytes effectively used, not provisioned.
- Data Reduction: This parameter is divided into four categories:
 - Reduction Disabled: No compression or data reduction is carried out.
 - Compression: From 40% to 80% data is transferred after compression and reduction.
 - Extreme Compression: From 33% to 36% data is transferred after compression and reduction.
 - Veeam WAN Acceleration: WAN acceleration is used to reduce the data transferred below 30%.
To learn more about WAN acceleration, visit the following website.
https://bp.veeam.expert/resource_planning/wan_acceleration.html
- Change Rate: This parameter should be selected based on the data change rate expected. Average is ~10%. Databases have a change rate ~20% to 50%.

Figure 9 Network planning tool

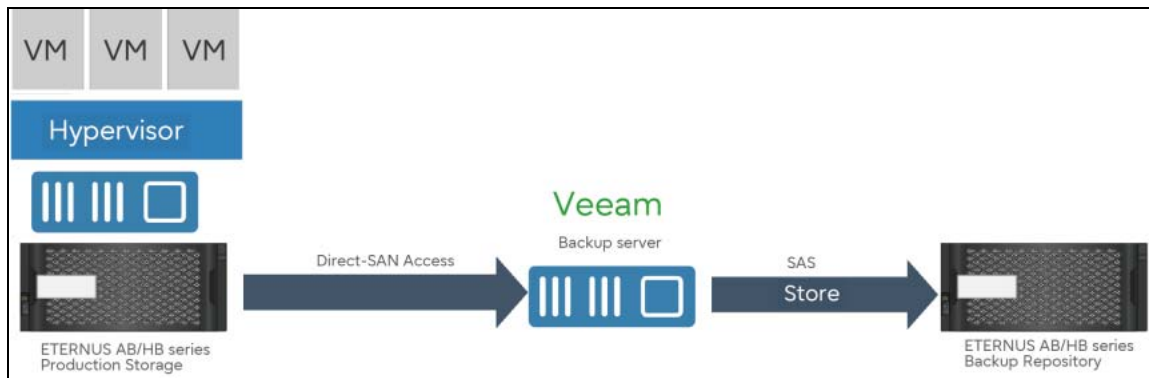


Performance with Veeam and the ETERNUS AB/HB series

The performance testing carried out with the ETERNUS HB2000 and Veeam proved to be a robust solution that meets the backup and restore needs of modern data centers. The testing objective was to determine the best practices in addition to those highlighted in "[5. Veeam Backup & Replication 12 Design Considerations](#)" (page 22).

Test Environment and Setup

Figure 10 Test environment diagram



The test setup is divided into the following components:

- The ETERNUS AB/HB production storage
 - Production storage was on an ETERNUS HB5100 with 24 SSDs.
 - Four PRIMERGY ESXi servers hosted a total of 96 VMs.
 - Each server has 24 VMs with 60GB of capacity.
 - All VMs had a test file to make sure that real-world test scenarios were replicated.
- Veeam Backup Server:
 - One PRIMERGY server was used to run Veeam Backup & Replication. This server was also used as a backup proxy.
- The ETERNUS AB/HB backup repository:
 - The ETERNUS HB2000 was used to host the backup repositories.
 - System consisted of a mix of 4TB and 8TB drives.
 - The ETERNUS HB2000 was directly connected to the Veeam Backup Server using SAS.

Note

FC or iSCSI could have been used instead of SAS.

Volume Configuration for Performance Testing

["6. ETERNUS AB/HB series Volume Configuration Guidelines" \(page 26\)](#) highlights the various recommended configuration options. During our performance testing, it was decided to run spot tests on each of the potential configuration options:

- RAID 6, RAID 10, and DDP were tested.
- An even number of volume groups was used per test as per ["6. ETERNUS AB/HB series Volume Configuration Guidelines" \(page 26\)](#).
- One volume per volume group was created for each of the RAID levels to have an equal number of volumes per controller.

Backup Performance Results

The following were the observations made from the testing we carried out:

- Spot checks on each of the configuration options showed consistent performance between all RAID levels, including DDP.
- The RAID level the customer chooses should be based on the level of data protection and availability desired. The amount of usable capacity varies based on the RAID level selected.

Performance Results with the ETERNUS HB1000/HB2000

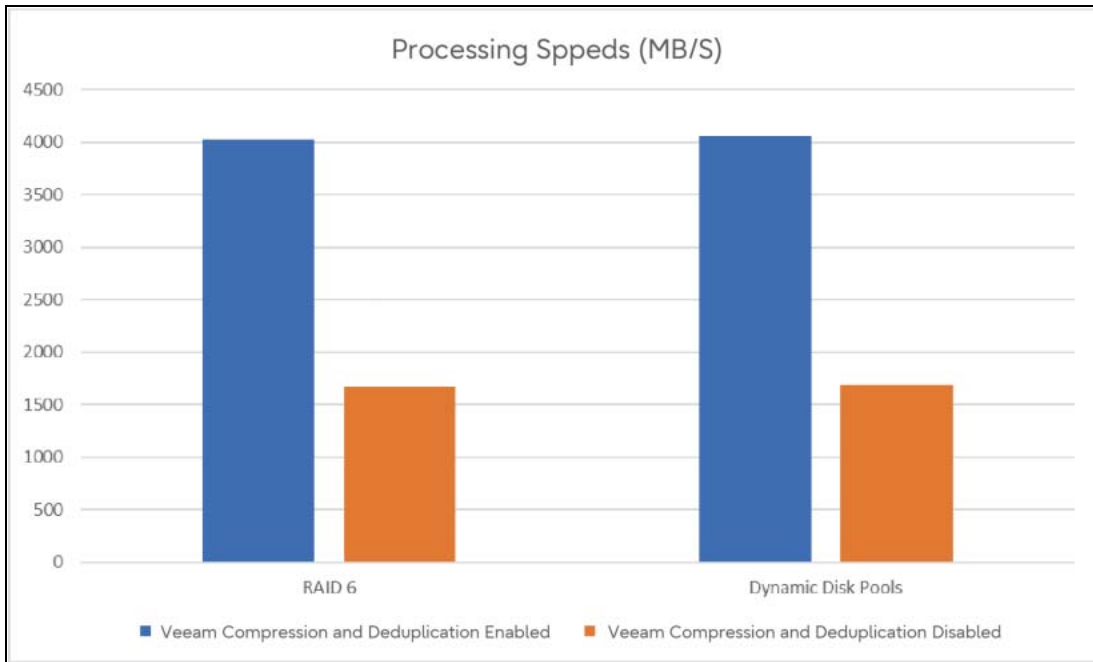
[Figure 11](#) shows the processing speeds achieved when the ETERNUS HB1000/HB2000 is used for backup repositories with Veeam Backup & Replication:

- The chart shows speeds for RAID 10, RAID 6, and Dynamic Disk Pools (DDP) with compression/deduplication enabled and disabled.
- Consistent performance is achieved with all three volume configurations.
- With compression and deduplication enabled, processing speeds of ~4GBps were achieved. This result is not the actual throughput achieved because it includes Veeam compression and deduplication.
- The processing speeds achieved with compression and deduplication disabled are ~1.6GBps. This result can be considered as the actual throughput achieved with this solution because it only accounts for the actual data transferred.

Note

Processing speeds vary depending on the compression and deduplication ratio achieved with Veeam. It is fair to assume it will be greater than ~1.6GB/s as that was achieved without compression and deduplication. Note that deduplication and compression of Veeam are used.

Figure 11 Processing Speeds with Veeam and the ETERNUS HB1000/HB2000



Note

Scale out backup repository can be used with Veeam to take advantage of the ETERNUS HB series capability. To learn more about scale out backup repository use the [link](#).

Performance Best Practices

Based on the performance tests carried out, a list of best practices was created. These help setup and tune the system to achieve excellent backup/restore performance.

- (1) When you start a data protection or disaster recovery job, Veeam Backup & Replication analyzes the list of VMs added to the job, and creates a separate task for every drive of every VM to be processed. Veeam Backup & Replication then defines what backup infrastructure components must be used for the job, checks what backup infrastructure components are currently available, and assigns necessary components to process the created job tasks.

If you use the parallel data processing mode and/or schedule several jobs to run in parallel, backup infrastructure components typically process several tasks at the same time. You can limit the number of tasks that backup infrastructure components must process concurrently. Task limitations help you balance the workload across the backup infrastructure and avoid performance bottlenecks. Veeam Backup & Replication lets you limit the number of concurrent tasks for the following backup infrastructure components:

Note

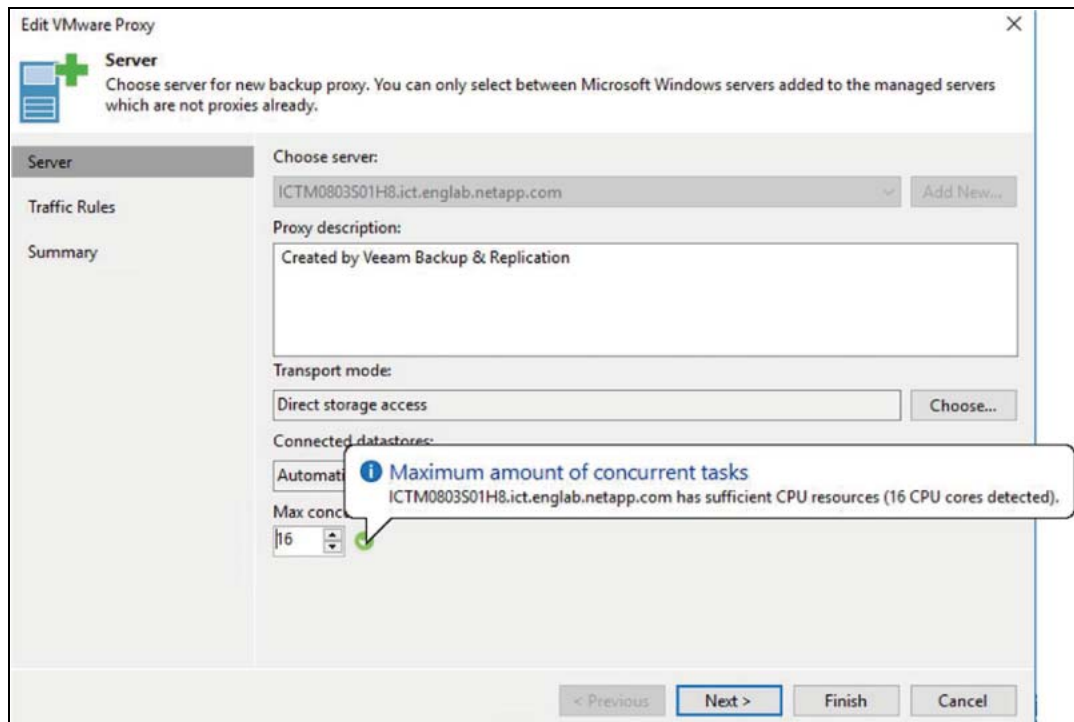
Task limits set for backup infrastructure components influence the job performance. For example, you add a VM with 4 drives to a job and assign a backup proxy that can process maximum 2 tasks concurrently for the job. In this case, Veeam Backup & Replication will create 4 tasks (1 task per each VM drive) and start processing 2 tasks in parallel. The other 2 tasks will be pending.

a Backup Proxies

To limit the number of concurrent tasks on a backup proxy, you must define the Max concurrent tasks setting for the backup proxy. For on host backup, you must define the Task limit setting for the source Microsoft Hyper-V host.

The maximum number of concurrent tasks depends on the number of CPU cores available on the backup proxy. It is strongly recommended that you define task limitation settings using the following rule: 1 task = 1 CPU core. For example, if a backup proxy has 4 CPU cores, it is recommended that you limit the number of concurrent tasks for this backup proxy to 4.

Figure 12 Restricting concurrent tasks per backup proxy



b Backup Repositories

To limit the number of concurrent tasks on a backup repository, you must enable the Limit maximum concurrent tasks to <N> option on the backup repository and define the necessary task limit.

The maximum number of concurrent tasks depends on the number of CPU cores available on the backup repository. It is strongly recommended that you define task limitation settings using the following rule: 1 task = 1 CPU core.

It is recommended to configure 2GB RAM per core. In case of shared folder backup repositories, the same amount of resources is required for gateway servers.

Synthetic operations performed on the backup repository (such as synthetic full backup, backup files merge and transform) are also regarded as tasks. The number of tasks performed during these operations depends on the type of backup chains stored on the backup repository:

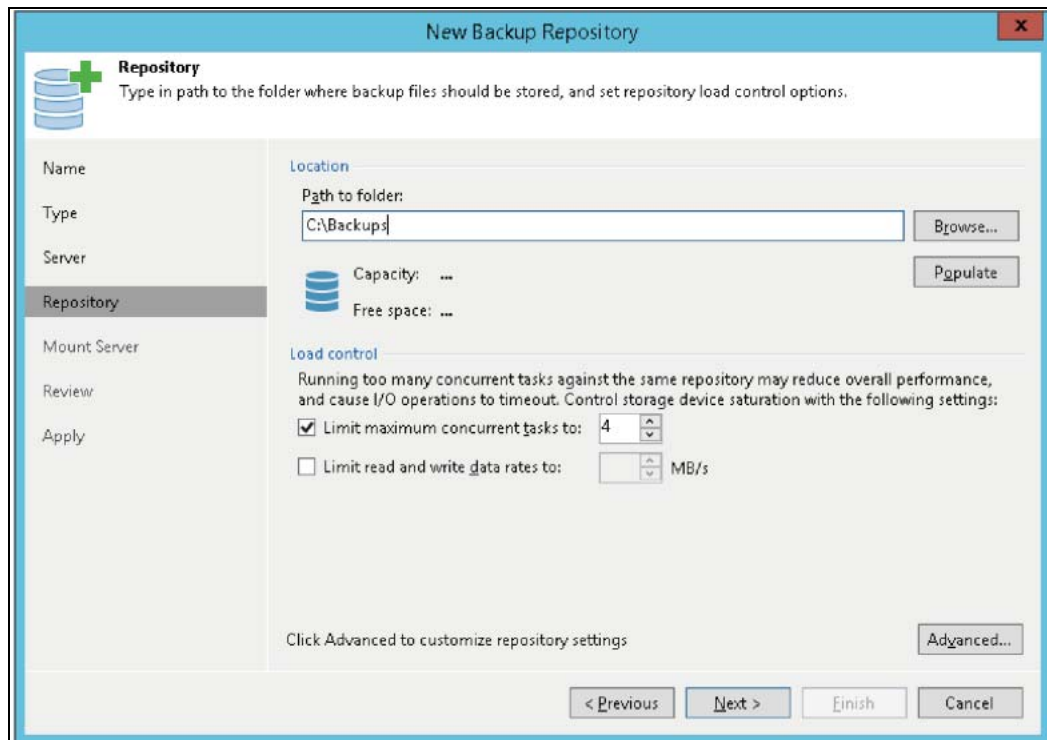
- For regular backup chains, Veeam Backup & Replication creates 1 task per job.
- For per-VM backup chains, Veeam Backup & Replication creates 1 task per every VM chain (that is, every VM added to the job).

If you use backup repositories for backup copy jobs, you must also consider tasks for read operations.

Note

When you limit the number of tasks for the backup repository, bear in mind the storage throughput. If the storage system is not able to keep up with the number of tasks that you have assigned, it will be the limiting factor. It is recommended that you test components and resources of the backup infrastructure to define the workload that they can handle.

Figure 13 Restricting concurrent tasks per backup repository



- (2) Adjust the number of active snapshots per datastore, to be in line with the number of concurrent tasks per backup repository. By default, it is restricted to 4 as a "protection method" in order to avoid filling up a datastore. If left at default value, your number of tasks per backup repository will be restricted to 4.
 - The default 4 active snapshot per datastore value can be modified by creating a registry DWORD value in "HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\" called MaxSnapshotsPerDatastore and use the appropriate hex or decimal value.
 - Any number can be selected but ensure you have enough capacity on your backup repository.
- (3) Use the recommended guidelines with regards to Direct SAN Access Mode. This is the recommended transfer mode.

10. SANtricity Plug-Ins for VMware

SANtricity Plug-In for VMware vCenter

The SANtricity Plug-In for VMware vCenter is a VMware vCenter Server plug-in that provides integrated management of ETERNUS AB/HB series storage systems from within a VMware vSphere Web Client. The vSphere Web Client is a single management interface that you can use to manage the VMware infrastructure and all your day-to-day storage needs.

The plug-in enables you to perform the following tasks:

- Configure ESXi hosts to ETERNUS AB/HB series storage systems.
- Provision new and existing storage system volumes.
- Map storage system volumes to ESXi hosts and host groups.
- Manage synchronous and asynchronous mirroring and storage system snapshots.
- View vCenter datastores that are on the ETERNUS AB/HB series volumes.

11. Summary

Veeam Backup & Replication offers powerful and cutting-edge capabilities in the data protection industry, but without a proper repository, backup windows and recoveries can be negatively affected. Veeam provides more recovery options and faster restoration capabilities, but to realize these benefits, the storage system must have the necessary performance profile. With technologies such as instant VM recovery, you can run an application directly from your backup file, but how is that application going to perform? The ETERNUS AB/HB series storage systems offer the performance that you need when recovering one or more applications and give you confidence that the data that you backed up is protected and is available when you need it.

Fujitsu Storage
ETERNUS AB series All-Flash Arrays,
ETERNUS HB series Hybrid Arrays
Reference Architecture and Storage Best Practices
with Veeam Backup & Replication 12

C140-0050-01ENZ3

Date of issuance: October 2023
Issuance responsibility: Fujitsu Limited

- The content of this manual is subject to change without notice.
- This manual was prepared with the utmost attention to detail. However, Fujitsu shall assume no responsibility for any operational problems as the result of errors, omissions, or the use of information in this manual.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- The content of this manual may not be reproduced or distributed in part or in its entirety without prior permission from Fujitsu.


FUJITSU