SUSE® Enterprise Storage Implementation Guide for Veeam Archive

Veeam Certified Deployment

Table of Contents

Introduction ................................................................. 2
Business Problem and Business Value ......................... 2
Requirements ............................................................... 3
Deployment ................................................................. 4
Additional Resources .................................................... 6
Introduction

The objective of this document is to present a guide on implementing Veeam connectivity with SUSE® Enterprise Storage as a backup target. It is suggested that the document be read in its entirety, along with the supplemental appendix information before attempting the process.

The final outcome of use of this document should provide a working Veeam backup environment leveraging block storage provided by SUSE Enterprise Storage (SES) using the SES iSCSI Gateway (IGW). This document will illustrate a single IGW connection and if multiple IGW's are rational, then the included diagram already reflects this model. This architecture assumes an understanding of SUSE Enterprise Storage as presented in the SUSE Enterprise Storage Technical Overview document available online which presents the concepts behind software defined storage and Ceph. It is also assumed that the reader has familiarity with the concepts and architecture of Veeam and cloud storage as described in the Veeam documentation.

Target Audience
The target audience for this document is IT staff or consultants responsible for implementing SUSE Enterprise Storage as a backup target for Veeam. Reasonable administrative knowledge of Linux and SUSE Enterprise Storage and operational knowledge of Veeam is assumed.

Business Problem and Business Value
Businesses are confronted by ever expanding production storage environments that require timely backups. Coupled with the need for a short Recovery Time Objective (RTO) and concerns involving data durability of traditional media, the interest in disk-to-disk backup mechanisms continues to increase. Many of these requirements are dictated by external threats (such as ransomware or security breaches) or regulatory changes such General Data Protection Regulation (GDPR).

Business Problem
The challenge of providing a valid backup and recovery service to IT is a multi-faceted issue. Ever expanding datacenter landscapes are filled with applications spread across multiple servers and operating systems. Combine this with the always-on requirements of a digital economy—the result is a need for fast backup, faster recovery, and application aware backup software. These issues are compounded by the external threats. When a virus or a ransomware hits an enterprise, the administrator must be able to recover the data quickly.

Business Value
The solution outlined in this guide enables a customer to deploy a disk-to-disk target that is orchestrated through Veeam. SUSE Enterprise Storage can be utilized as an iSCSI Block Storage target over a common network. The result is a high performing and flexible backup target with exabyte scalability.

SUSE Enterprise Storage delivers savings for a Veeam disk-to-disk backup solution with:

- Commodity hardware and open source software for greatly reduced TCO.
- Open source software, for minimal software cost and maximum flexibility
- A self-managing, self-healing architecture for reduced management overhead.
- A flexible, cluster-based design for graceful and inexpensive upgrade and innovative licensing model that avoids...
per-gigabyte software licensing charges, resulting in much lower TCO at scale.

- With minimal acquisition cost, management overhead, and upgrade expense, SUSE Enterprise Storage is the lowest-price and most highly scalable solution for enterprise archive and backup implementations.

Requirements

Enterprise backup environments require stability, long term data durability, scalability, and simple management. Establishing these requirements enables the business to consistently meet their data protection needs and comply with data recovery requirements that can be mandated by operational needs or governmental regulations.

This guide requires that a functional SUSE Enterprise Storage cluster with one or more RADOS Block Devices (RBD) already deployed. The process for deploying this environment can be found in the SUSE Enterprise Storage deployment guide.

Software:
- SUSE Enterprise Storage 5
- Windows 2016 Tenant VM
- Veeam Backup & Replication 9.5 Update 2

Functional Requirements

A SUSE Enterprise Storage solution is:

- Simple to setup and deploy, within the documented guidelines of system hardware, networking and environmental prerequisites.
- Adaptable to the physical and logical constraints needed by the business, both initially and as needed over time for performance, security, and scalability concerns.
- Resilient to changes in physical infrastructure components, caused by failure or required maintenance.
- Capable of providing optimized object and block services to client access nodes, either directly or through gateway services.
- Data protection is configurable to meet the customer’s individual needs at a granular level.

SUSE Enterprise Storage (SES) iSCSI Gateway (IGW) target for Veeam

**iSCSI Initiator-Target relationship between Veeam Application VM and IGW uses Multipath**

*Figure 1. iSCSI Gateway (IGW) target for Veeam*

Servers send backup data to Veeam application server VM

ESX Servers

Veeam application VM uses Windows iSCSI client to connect to SES iSCSI Gateways (IGW), which present storage from the SES cluster.
Solution Architecture—Block
SUSE Enterprise Storage can be used as a Veeam Local Disk Repository. This document covers the certified method of attaching one or more iSCSI LUNs to a Windows server running the Veeam application, thus appearing as a local Windows disk when adding a backup repository through the Veeam console.

SUSE recommends utilizing SSD journal devices within the Object Storage Daemon (OSD) configuration, which is part of the SES architecture and represents a single instance of the distributed storage target. While solid state devices are not required, these devices may significantly reduce latency for some workloads, resulting in higher performance of write operations. This is particularly true with smaller block writes of less than 64KB. This configuration must be done at the time of cluster node deployment and is described in the SUSE Enterprise Storage 5 Deployment Guide.

iSCSI must utilize iSCSI Gateways to convert from iSCSI to the native RBD protocol for interaction with the SES cluster. While this process nominally impacts performance, it enables the use of SUSE Enterprise Storage with the Microsoft Windows VM tenant running the Veeam application. SUSE recommends configuring iSCSI with multipath software enabled with a policy of round-robin among two or more IGW nodes. Refer to the Windows multipath configuration in the Connecting to lrbd-managed targets section of the SUSE Enterprise Storage Administration Guide. This enables the best performance and availability for iSCSI. An iSCSI scenario is described above in Figure 1. At a high level, the admin will create the iSCSI LUN presentation from SES using the iSCSI client within Windows and then map the LUN on the Windows VM running within the ESX cluster. Finally, the mapped drive letter will be presented as a new repository within Veeam. This will be illustrated further on.

Pool Configuration
When configuring the SUSE Enterprise Storage cluster for use as a backup target, the data protection scheme is an important consideration. There are two main options for data protection, each with advantages and disadvantages.

1. Replication
   This data protection scheme works by replicating each data chunk on the specified number of unique devices.

   The default is 3. If the failure domain is assumed to be at the storage host level, this means that the cluster could survive the loss of two storage servers without data loss. The downside of replication is the space overhead, which is 200% or two-thirds of the total cluster capacity.

2. Erasure Coding (EC)
   EC works by splitting the data into the specified number of chunks (k) and then performing a mathematical calculation to create the requested number of EC chunks (m). Again, assuming the failure domain is at the host level, a system using an EC scheme of k=6,m=3 has an overhead of only 50%, or one-third of the total cluster capacity. Because EC actually writes less data, it is sometimes faster than replication for writes, but slower on the reads due to the requirement to reassemble the data from multiple nodes.

   Another aspect to consider is the total cluster size. In general, it is not recommended to use EC with a cluster of fewer than seven storage nodes. When using EC with SUSE Enterprise Storage, it is recommended that the data chunks + (2x erasure coding chunks) is less than or equal to the cluster node count. Expressed in a formula:

   \[
   \text{data chunks} \times k + (\text{coding chunks} \times m) \times 2 \leq \text{cluster node count}
   \]

   A cluster size of seven would thus allow for 3 data chunks + 2 erasure coding chunks + 2 spare nodes to allow for device failures. In a larger cluster, EC profiles of 8+3, 6+4, 9+3, etc. are not uncommon.

Deployment
This section is a bridge document between SUSE Enterprise Storage and Veeam. The intent is to highlight the steps required to properly setup the Veeam environment to utilize the IGW.

Veeam Configuration Procedure—Local Disk Library over iSCSI
Create a Windows Disk volume locally from within Windows Disk Manager using the ISG nodes. See Veeam Backup & Replication 9.5 User Guide for VMware vSphere. In this guide, we will refer to it as “LocalDisk.”
1. Create, export, and mount an iSCSI LUN as described in the SUSE Enterprise Storage 5 Deployment Guide.

2. Within the Veeam Console, click **Backup Infrastructure** on the left-hand menu bar. Right-click on **Backup Repositories** followed by **Add Backup Repository**.

3. Provide a friendly name to distinguish the multiple repositories.

4. Select Windows Server as the repository type. This option will be used for iSCSI LUN’s presented directly to the Veeam application Host. Leverage the Windows Drive letter mapping as a Veeam Repository.

5. Click Finish.
You should now be able backup directly to the new repository. Consult the resources linked below for additional understanding and configuration options.

**Additional Resources**

- Veeam HCL—SUSE Enterprise Storage v5 SDS:  
  [www.veeam.com/kb2373](http://www.veeam.com/kb2373)
- Veeam Documentation:  
  [www.veeam.com/documentation-guides-datasheets.html](http://www.veeam.com/documentation-guides-datasheets.html)

- SUSE Enterprise Storage Technical Overview:  
- SUSE Enterprise Storage v5—Deployment Guide:  
- SUSE Enterprise Storage v5—Administration Guide:  