

StarWind Virtual Tape Library

Best Practices

APRIL, 2019

BEST PRACTICES



Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the [Technical Papers](#) webpage or in [StarWind Forum](#). If you need further assistance, please [contact us](#) .

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company’s core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

Copyright ©2009-2018 StarWind Software Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

INTRODUCTION

Companies involved in sensitive data handling are required to adhere to regulatory requirements for secure data storage and archival. This document provides information on how to configure [StarWind Virtual Tape Library \(VTL\)](#) for high data security and resilience to malicious software or activities.

StarWind Virtual Tape Library (VTL) eliminates the need for physical tapes by emulating industry-standard tape hardware and keeping data on directly attached spinning disks as well as replicating and tiering it in object storage arrays and cloud storage. VTL is designed for organizations that want to either get rid of physical tapes completely or to accelerate the backup process, add an extra level of protection and automate the DR process by offloading tapes to the cloud. This document describes the best practices for setting up the StarWind Virtual Tape Library (VTL) environment.

A full set of up-to-date technical documentation can be accessed [here](#), or by pressing the **Help** button in the StarWind Management Console.

For any technical inquiries please visit our [online community](#), [Frequently Asked Questions](#) page, or use the [support form](#) to contact our technical support department.

Design Principles

Most administrators are familiar with backups and some of them are required to backup onto tapes. StarWind Virtual Tape Library (VTL) can be used to store backups (Storage Repository) and it is also possible to offload Virtual Tapes to the cloud or object storage arrays. Such method guarantees redundancy of backups and fits the 3-2-1 backup rule. It can be useful in DR scenarios or for restoring after a ransomware attack. If there is a requirement to store the backups for a long period of time, offloading to the cloud maximizes the security and minimizes the cost of maintaining a physical tape-based infrastructure.

Main configuration scenarios

There are several configuration scenarios:

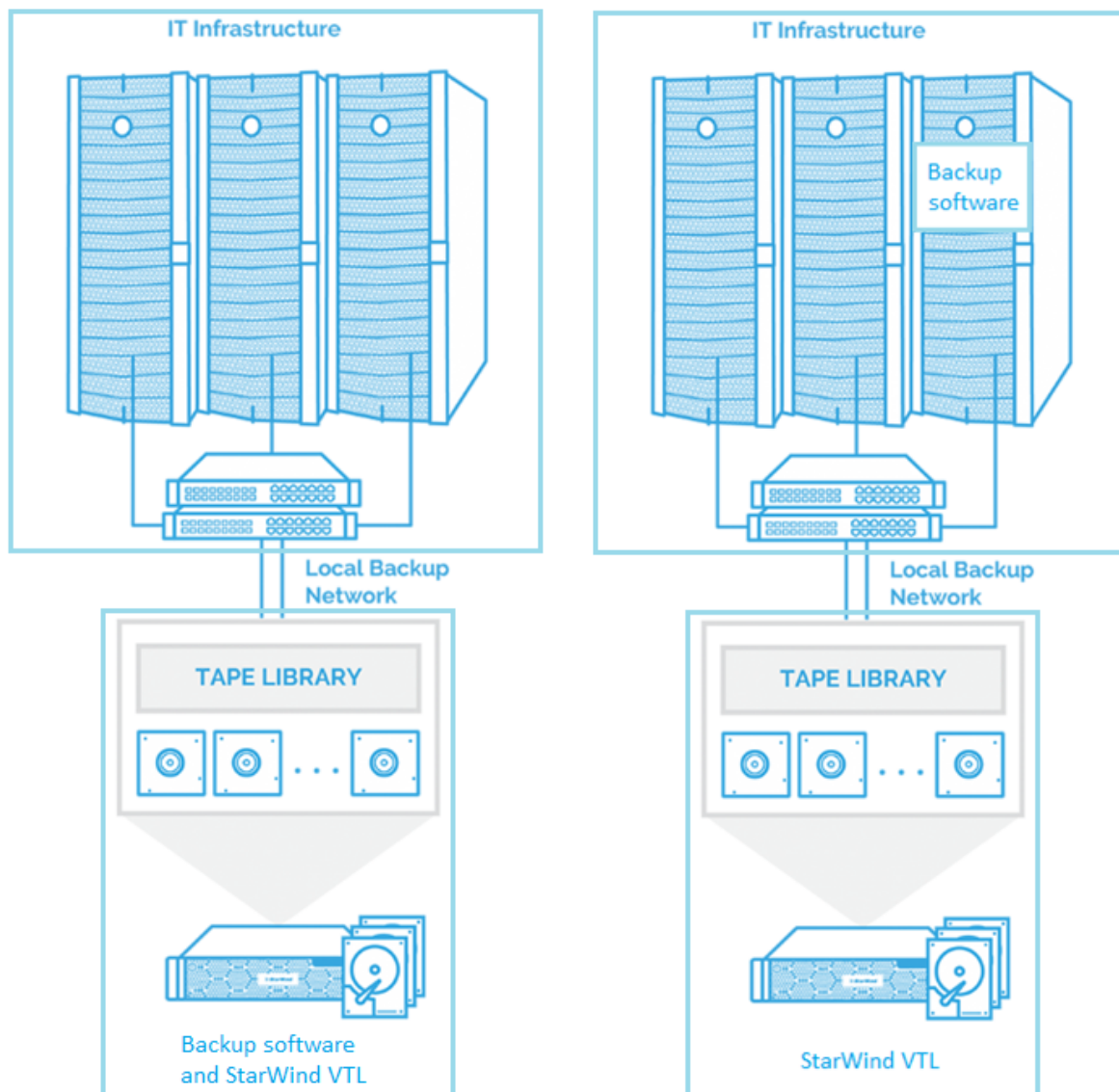
- Backup software and VTL are installed on the physical server with Storage Repository connected (all in one box);
- Backup software is installed inside the VM in (or outside) the Cluster, VTL is installed inside the physical server with Storage Repository connected (separated scenario).

Both scenarios above can be used depending on the administrator's requirements.

The first one is easier to manage and helps avoiding bottlenecks when connecting VTL devices. This scenario can be used for greenfield environments.

The second one is more flexible on the permissions configuration which allows enhancing the security of the entire setup. This scenario can be used for brownfield environments.

The general configuration schemes are presented in the pictures below. The Virtual Tape Library server is connected to the IT infrastructure, but not joined into the domain, to enhance security.



All in the box StarWind VTL scheme

Separated scenario StarWind VTL scheme

Storage considerations

A common design for backup storage is to use an applicable number of spindle disks

given that they deliver huge capacity at a very low cost. To obtain data redundancy and the best price-per-GB ratio, it is recommended to configure RAID 5, 50, 6 and 60 for VTL storage. In order to minimize the recovery process time, all-flash or hybrid storage can be used.

Networking

Considering that backup runs over the network, the network throughput becomes one of the most important parts of any backup environment. Network throughput between the IT infrastructure and the VTL server has to be sufficient to ensure that it will not bottleneck the backup performance. For example, if backups are done with the speed up to 100 MB/s, 1GbE network is required, while for bigger loads, 10 GbE network should be in use.

It is strongly recommended to have dedicated network interfaces and a separate VLAN to achieve the expected performance.

Security recommendations


There are several recommendations to improve VTL host security:

- Don't join the VTL server to the domain;
- Assign a separate user to access the backup server;
- Create a dedicated service user for backup software;
- In order to fit the ransomware resiliency into the local environment, the Virtual Tape Library should be located on the dedicated storage that is isolated from the production environment;
- Disable file shares for the StarWind Virtual Tape Library (VTL) host or Storage Repository;
- Additionally, CHAP authentication and access rights have to be configured for iSCSI connections in StarWind Virtual Tape Library (VTL);
- Enable firewall and keep antivirus and OS updated;
- Configure VTL cloud replication to have at least one copy of your backups off-site. This guarantees protection and restores in case of a ransomware attack.

CONCLUSION

Following the best practices for VTL and backups, and proper design of the network topology, storage and security allows to get fast, resilient and protected backup copies. Such method warrants the main objective of backups – 100% restore of the latest backup copy.

Contacts

US Headquarters	EMEA and APAC
 1-617-449-77 17	 +44 203 769 18 57 (UK)
 1-617-507-58 45	 +34 629 03 07 17
 1-866-790-26 46	(Spain and Portugal)

Customer Support Portal: <https://www.starwind.com/support>

Support Forum: <https://www.starwind.com/forums>

Sales: sales@starwind.com

General Information: info@starwind.com



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA

www.starwind.com

©2020, StarWind Software Inc. All rights reserved.