VEEAM

10 Best Practices for VMware vSphere Backups

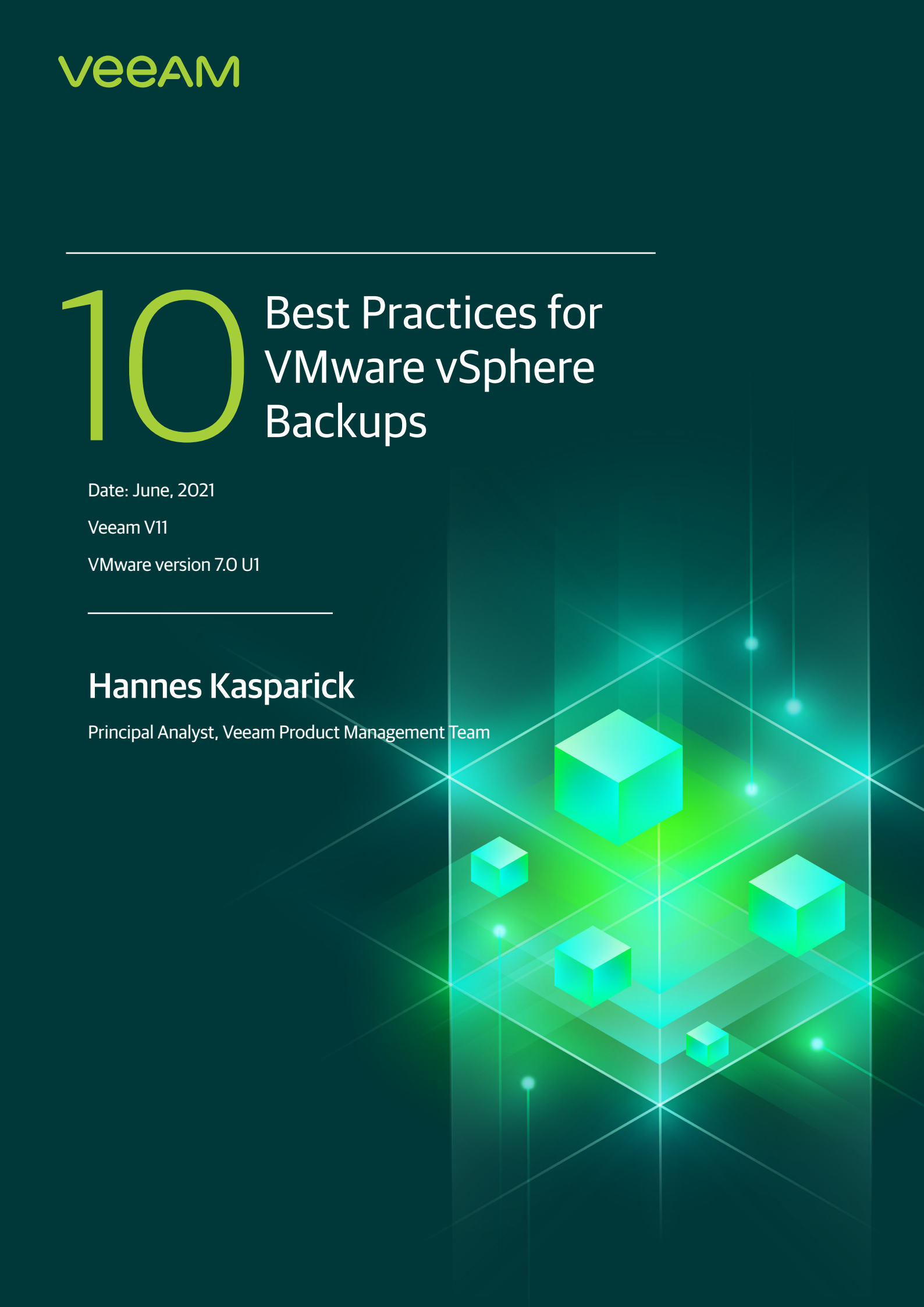
Date: June, 2021

Veeam V11

VMware version 7.0 U1

Hannes Kasparick

Principal Analyst, Veeam Product Management Team



Contents

Executive summary

Server virtualization has seen extensive adoption globally and remains a foundation for cloud computing. VMware remains the most popular hypervisor and many Veeam® customers use VMware vSphere as their preferred virtualization platform. This white paper describes the best practices that are specific to the backup and availability of VMware vSphere with Veeam Backup & Replication™ v11. In this guide, you will find tips and recommendations regarding VMware backup from experienced Veeam community members, which should help you augment your backup strategy and ensure your data is protected. This paper does not address data protection recommended practices for hypervisors other than VMware or physical servers.

Introduction

To maintain service levels, performance and availability, backup and recovery of virtual machines (VMs) on vSphere is fundamental to avoiding and minimizing outages. The most important general best practice for backups is the 3-2-1 Rule.

This means having at least three copies of your data, including a first and second line of backup. This rule also recommends storing backup copies on at least two independent types of media. The "independent" part of this cannot be overemphasized. Here, independent media means that these pieces of media have no dependency from a technology perspective. Finally, another copy should be off site and offline so it's out of reach of natural disasters, malicious software and unauthorized people. As an example, Veeam added support for S3 object lock in Veeam Backup & Replication v10 and Hardened (immutable) repositories in V11. Of course, tape is still an option for off-site storage for backups.

This document describes several best practices with Veeam Backup & Replication and VMware vSphere that help eliminate data loss and ransomware. These best practices are dedicated to Veeam and VMware only; other hypervisors are not covered in this document.

These general best practices include:

- Having a backup and restore strategy that fits your business needs
- Having proper sizing
- Making sure VSS works within Windows machines
- Having enough backup space

These apply in any case, regardless of whether the backup is a VMware, Hyper-V, Nutanix AHV, cloud provider or physical server backup.

The first and most important thing to do before planning or implementing any solution is to be certain about its requirements. In an ideal world, the business will create the requirements and tell IT which recovery point objective (RPO) and recovery time objective (RTO) is needed. For example, do they only need backup, or is disaster recovery (DR) also a requirement? Does a small RTO enforce additional configuration of Veeam replication, Veeam Continuous Data Protection or storage snapshots?

With this information, it is possible to better size the required hardware. That includes the number of CPU cores and the amount of memory and bandwidth requirements for WAN, LAN and SAN. Finally, you need a source and backup storage that is fast enough to achieve the required speed.

The next step is the backup itself. Veeam's application-aware image processing uses Microsoft VSS to achieve application-consistent backup of Windows VMs. This mechanism does not use VMware tools quiescing. To ensure application-aware image processing works reliably, it is necessary that the VSS writers located on the VMs are working properly.

No. 1: Use current versions of Veeam and vSphere

The latest versions of Veeam Backup & Replication improve performance and security along with VMware vSphere.

Veeam Backup & Replication v11 introduces asynchronous read everywhere and unbuffered writes for writing backups to the storage system. Asynchronous read improves all kinds of reads. In version 10, Veeam already used asynchronous read for Windows file-level restore, Instant VM Recovery™ and creating virtual synthetic full backups for backup-to-tape jobs. In version 11, Veeam uses this for all other kinds of reads like backup copy jobs and backup-to-tape jobs.

Unbuffered writes help improve backup write performance. With version 10, we have seen around 4 GB backup speed to a single server with 56 NL-SAS disks. With version 11, we more than doubled that speed again and maxed out 100 GB connections.

Improving security is a permanent topic for VMware and Veeam. Using the latest version of the products ensures that security improvements are implemented.

> *Your engineering did an amazing job with optimizing V11 code; with 10 GiB/s in a single server, Veeam on Apollo 4510 is a record-breaking solution. V10 was already one of the fastest data protection solutions, but V11 redefines the concept of enterprise-class performance. I have never seen any company doubling its performance from one release to the next.*
>
> — Federico Venier, HPE Engineer

The best practice: Look out for improvements in the latest versions of Veeam Backup & Replication and vSphere.

No. 2: Choose your backup mode wisely

With Veeam Backup & Replication, there are three different transport modes to back up VMs on vSphere. Starting with version 11, Veeam will support almost all backup modes for Linux proxies as well. If you prefer Linux, then this is the first decision you'll make. All backup modes have their own pros and cons and there is no general rule as to which is the best. Your environment and requirements will determine which one of the following three modes you should choose:

1. Network mode or NBD
2. Direct storage access, including Backup from Storage Snapshots
3. Virtual appliance or "Hot-Add"

The properties of each proxy allow the configuration of the above options in the transport mode section.

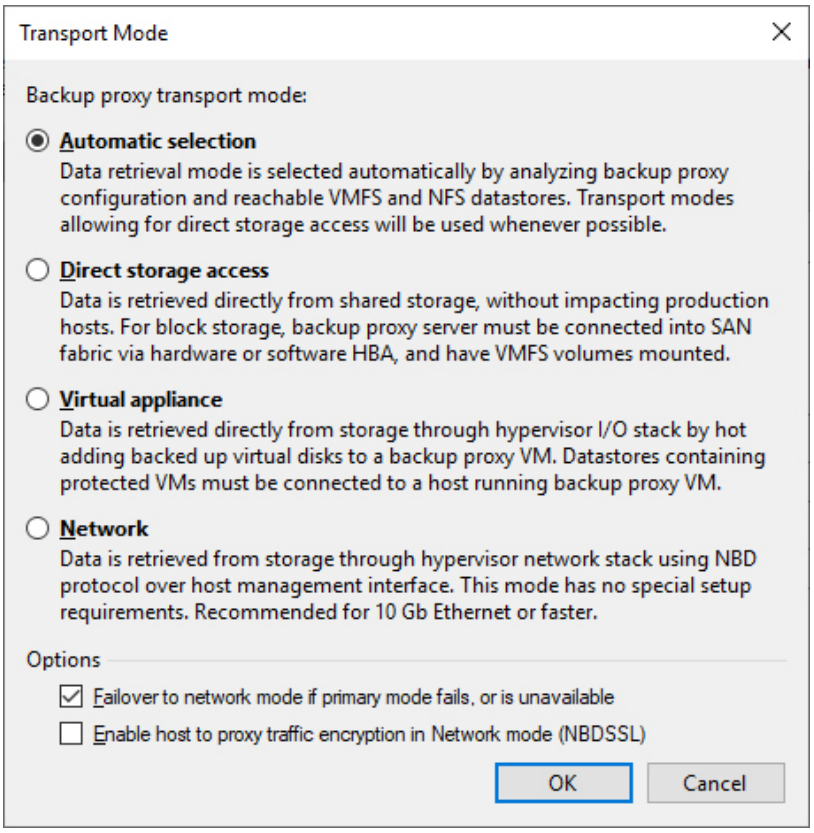


Figure 1: Transport mode options

The network mode or NBD mode is the easiest way to do VMware backups. Here, the Veeam proxy server will use the ESXi management port of each ESXi-host to transfer backup data. This makes setup very simple as it requires no additional storage or VM configuration, plus it also scales with the number of ESXi hosts. Additionally, it has very low overhead, which is another advantage. Compared to Hot-Add mode, it does not need any additional Hot-Add mount operations, which saves time. It also does not create additional storage snapshots like Backup from Storage Snapshots with integrated storage systems. The coordination of VM and storage snapshots takes time, so network mode can even be the fastest option for incremental backups in environments with many VMs and a low data change rate.

The ESXi management port can become a bottleneck, especially if it is only on a 1 Gbit interface. However, with 10 Gbit and better network interface cards this usually isn't a problem.

Direct storage access mode backup traffic goes directly from the storage system to the Veeam backup proxy. Here, the backup traffic does not need to go through the ESXi hypervisor, and the protocol depends on the storage environment. Usually, this is FibreChannel or iSCSI. Direct storage access mode also has an advantage over Hot-Add as network mode; there's no time-consuming Hot-Add operation. On the other hand, both modes use VMware vStorage API for Data Protection (VADP).

VADP is VMware's snapshot-based framework that enables backup and restore of VMs. As VADP can impact backup performance, Veeam Backup & Replication does have the ability to bypass VADP in three scenarios. These three scenarios are:

- Backup from Storage Snapshots
- Direct NFS (like direct storage access)
- Virtual appliance/Hot-Add

By having the ability to bypass VADP, Veeam can significantly improve backup performance. This is one of the reasons why Hot-Add became popular. However, there are more advantages in using Hot-Add mode. With Hot-Add, the Veeam backup proxy runs as an additional VM for backups; it mounts the snapshots of the VMs to backup and sends the traffic over the normal VM network.

This mode also does not use the ESXi management interface, resulting in Hot-Add as a great alternative, especially with 1 Gbit networks where direct storage access backup modes are not possible.

> ***The flexibility and wide range of transport modes make Veeam a perfect fit for all types of VMware vSphere environments. The network mode for SMB, Hot-Add for HCI and general purposes, direct storage access and storage integration have huge change rates and minimize impact to the production environment.***
>
> — Markus Kraus, Veeam Vanguard and VMware vExpert

In general, Hot-Add is not recommended when using NFS datastores. With NFS, the recommendation is to use direct storage access, which results in the direct NFS mode. Direct NFS has no separate option in the UI, it's just a flavor of direct storage access. The reason for this recommendation is that Hot-Add often results in VM stuns if the Veeam proxy does not run on the same ESXi host as the VM. Veeam KB1681 provides more details in the section titled "For environments with NFS datastores." However, if you do plan to use Hot-Add mode on NFS datastores, please apply the following rules and settings:

- One Hot-Add proxy per ESXi host
- Set EnableSameHostHotAddMode = 1 in HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication

Note: Direct NFS backup can only back up VMs without existing snapshots. VMware recommends removing snapshots as soon as possible. In case a VM snapshot is present, Veeam will failover to alternative backup modes.

As there are diverse options to do backups, you can use the following table to quantify the results of each mode and decide which one is best for you.

Mode	Operation	Time	Speed
Direct Storage Access	Full backup		
Direct Storage Access	Incremental backup		
Backup from Storage Snapshots	Full backup		
Backup from Storage Snapshots	Incremental backup		
Virtual Appliance	Full backup		
Virtual Appliance	Incremental backup		
Network	Full backup		
Network	Incremental backup		

The best practice: Test which backup mode fits your environment best.

No. 3: Plan how to restore

After defining your optimal backup mode, it's important to look at the restore mode too. No matter what your restore test results are, they need to satisfy the recovery time objective (RTO) and hardware with more performance capacity may be required. Veeam offers a variety of recovery scenarios to restore VMs from on-premises or cloud providers, physical machines, files and application objects. Since version 10, you can even instantly recover any image-based backup to VMware vSphere.

First, it's important to know that file and object restores differ from VM or disk restores. Veeam restores files or objects like Microsoft Exchange emails or Microsoft Active Directory objects over the network. "Over the network" means an RPC (i.e., Windows) or SSH (i.e., Linux) connection plus data mover ports are required to transfer the data into the VM. The reason behind this is that Veeam is agentless for VM backups per default. If you want to reduce port requirements for Windows backup and restore, then you can use the new Veeam persistent guest agent in version 11.

Since backup is VM snapshot-based as a block-level backup, the restore of full VMs or virtual disks is also block based. Depending on the restore mode, it makes a difference whether the VM is thick or thin provisioned. The restore modes are the same as the ones for backup (i.e., direct storage access, virtual appliance and network). Additionally, there is Instant VM Recovery combined with Storage vMotion or quick migration.

Hot-Add and network mode can restore both thick- and thin-provisioned VMs. As already mentioned, the virtual appliance or Hot-Add transport has very good performance for backup. This is also true for full VM or disk restores with "Hot-Add." In many scenarios, it makes sense to have at least one Hot-Add proxy available for VM or disk restores.

Network mode is often the slowest way to restore.

Direct storage access mode works very well, but it can only restore thick-provisioned disks. Thin-provisioned disks would be converted on-the-fly to thick disks when using this option. Since direct storage access mode uses VADP for restores, this is usually not the fastest option. An exception is restoring with direct NFS where Veeam Backup & Replication bypasses VADP.

To restore a VM or virtual disk, you're not required to fully transfer all data. If the change block tracking information on the production storage is correct, then a restore that's based on change block tracking is possible. Setting this option can reduce restore time, and the quick rollback option to do this must be manually enabled during restore.

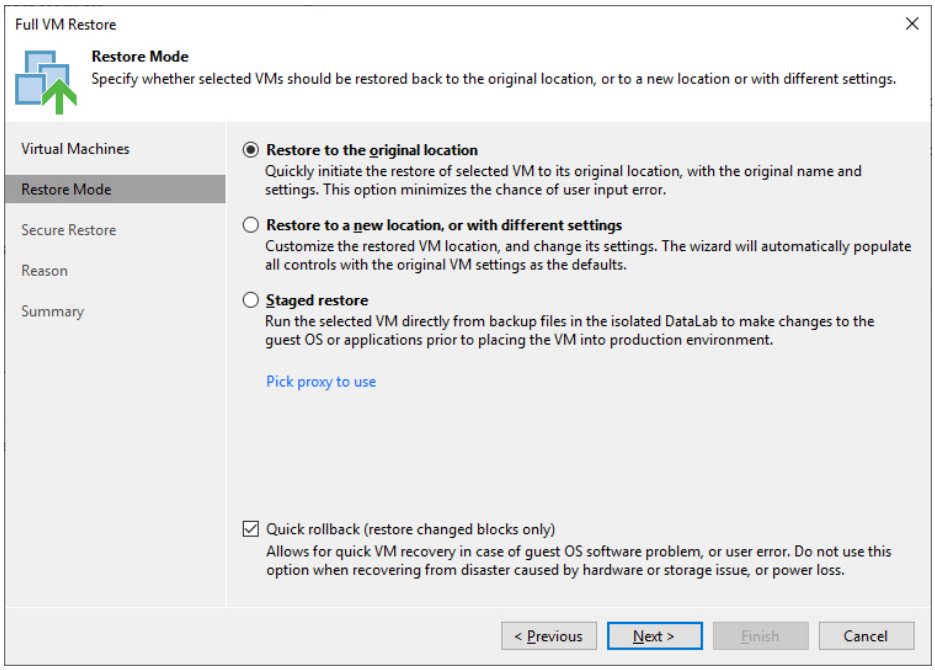


Figure 2: Quick rollback based on change block tracking information

Instant VM Recovery is an alternative way to perform a full VM restore (this is the same for instant VM disk recovery instead of full disk recovery). Instant VM Recovery allows you to instantly boot a VM directly from the backup repository. The backup repository acts as an NFS datastore that is mounted to an ESXi host. Instant VM Recovery performance was massively improved in version 10. There are two options to transfer the VM data from the repository NFS datastore back to the production datastore:

- Veeam Quick Migration
- VMware Storage vMotion

Since there are diverse options for full VM restores, you can use the following table to quantify the results of each mode and decide which one is best for you.

Mode	Operation	Time	Speed
Direct Storage Access	Full VM restore		
Direct Storage Access	Full VM restore CBT		
Virtual Appliance	Full VM restore		
Virtual Appliance	Full VM restore CBT		
Network	Full VM restore		
Network	Full VM restore CBT		
Instant VM recovery + Storage Vmotion	Full VM restore		
Instant VM recovery + Quick Migration	Full VM restore		

The best practice: Plan and test restore options depending on your storage and transport modes. If you do not use NFS datastores, have at least one "Hot-Add" proxy installed as a spare.

No. 4: Integrate Veeam Continuous Data Protection into your disaster recovery concept

With Veeam Backup & Replication, you can replicate VMware VMs every few seconds without VMware snapshots. The feature is called Continuous Data Protection (CDP) and allows to reduce RPO and RTO times for disaster recovery. CDP is based on the vSphere APIs for I/O Filtering (VAIO) and can be used very similarly to classic Veeam replication.

When planning CDP, there are a few things you need to consider. As always, you need to allocate hardware resources for the data transfer and for storing the changed data. While classic backups happen every eight, 12 or 24 hours and only uses network bandwidth a few times per day, CDP has a constant stream of data to transfer. Estimations on the bandwidth can be done by monitoring the storage write traffic. Veeam will apply compression and filter out unnecessary blocks (i.e., only transfer the latest version of a block that was changed multiple times within the RPO window). Because of this, the bandwidth required will be a little bit lower than what you see on the storage.

For the VMware datastore destination, you need to have enough free space and I/O capacity for the restore points. The lower the RPO time and the longer the retention, the more disk space is required. We recommend using 10 seconds and more RPO time. Two seconds of RPO time is possible, but it uses more disk space and creates more I/O on the target datastore and writes to the target datastore are unthrottled. If there are also production VMs on the target storage system, it is recommended that you use a dedicated datastore for the replica VMs.

Depending on the IO load and RPO time, the network traffic for CDP can be significant. MTU 9000 increases the performance about 25% in 10Gbit/s networks. A dedicated VMkernel adapter with a dedicated physical uplink (or multiple uplinks) is also recommended. This ensures that CDP traffic does not interfere with other traffic types (i.e., management traffic). No services need to be enabled on these VMkernel adapters (see figure 3). Existing (distributed) virtual switches can be used, and there is no need to configure a dedicated vSwitch for CDP traffic.

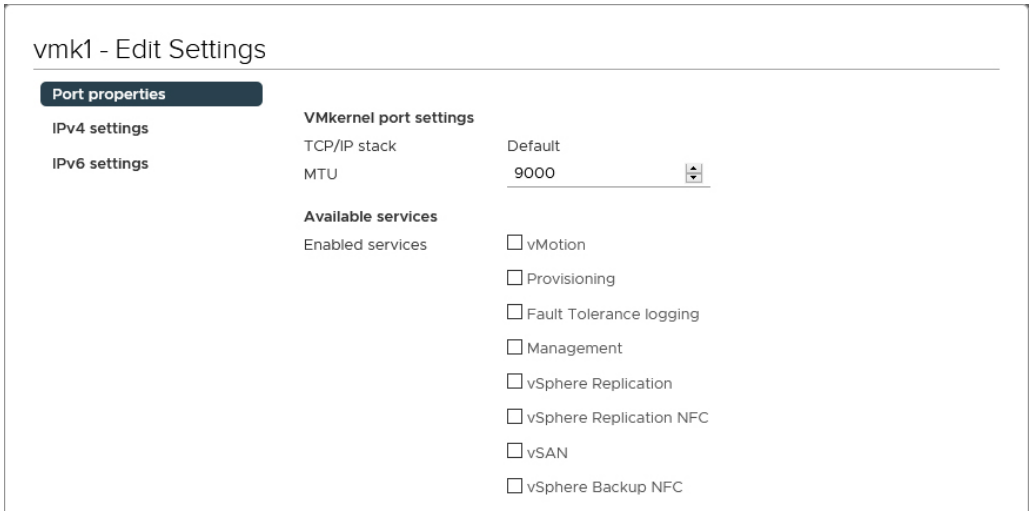


Figure 3: No services enabled for VMkernel port

The proxy design questions are similar for backup:

- Few big (physical) proxies
- Many small (virtual) proxies

There should be at least two source and destination proxies for redundancy. If virtual proxies are used, one proxy per ESXi is the best way to optimize network traffic flow. It is also recommended that you use dedicated proxies for source and target. For the proxy cache, fast SSDs for mixed workloads are recommended.

When implementing CDP, there are several important infrastructure requirements that apply only when CDP replication is used. Specifically, backup server, CDP proxies, vCenter Server and ESXi hosts must be able to resolve each other's DNS names. For additional requirements, please consult the Veeam Backup & Replication User Guide for VMware vSphere.

The best practice: Use Veeam Continuous Data Protection for disaster recovery if you do not have storage-based replication in place.

No. 5: Install VMware tools

In many situations, Veeam Backup & Replication relies on the existence of VMware tools that run in the VMs. Without VMware tools, Veeam Backup & Replication cannot find out, for example, the IP addresses or the operating system version. As a result, application-aware image processing will fail.

This is because Veeam Backup & Replication cannot detect the IP address, and without the IP address, Veeam cannot connect to the VM over the network. The fallback mechanism VIX or vSphere API for guest interaction also doesn't work due to the lack of VMware tools (see No. 10 for more information on VIX). Figure 4 shows this in an example of a failed guest credentials test because of missing VMware tools:

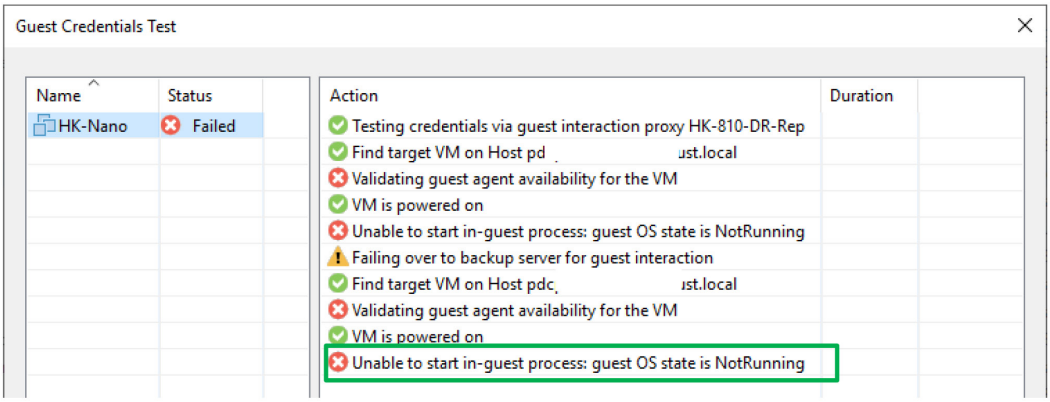


Figure 4: Failed application-aware processing test

The second example is SureBackup tests. Heartbeat and ping tests will fail if VMware tools are not present. For VMware tools, the first rule applies: Keep them up to date.

The best practice: Install VMware tools and keep them up to date.

No. 6: Integrate storage-based snapshots into your backup concept

Storage snapshots do not replace backup, but they can help minimize data loss in many situations. Veeam Backup & Replication has integrations with various storage vendors in conjunction with VMware vSphere. Storage integration adds more options for data protection. A list of storage systems with integration is available here.

The first is that Veeam Backup & Replication can open storage snapshots and restore files and objects directly from the storage snapshot. This allows you, for example, to schedule storage snapshots every 15 minutes without being required to create VM snapshots too. Although a snapshot every 15 minutes is not a real backup since it does not meet the 3-2-1 Rule, it does help to decrease RPO times.

Note: You can choose between crash-consistent and application-consistent snapshots. Only application-consistent snapshots create a VMware snapshot before the storage snapshot.

Figure 5 shows Veeam Explorer™ *for Storage Snapshots*, which follows a similar concept. The left side shows the storage snapshots (i.e., the LUNs and the snapshots of one LUN). The right side shows the VMs of each storage snapshot. From there, you can restore VMs with Instant VM Recovery or restore files and application objects.

Now imagine the storage does snapshots of critical LUNs or volumes every 15 minutes and deletes them after four hours. This means it's possible to restore data from 15 minutes ago, instead of older data from the last night's backup.

> ***I use storage integration with Veeam, combining storage snapshot orchestrations with my backup jobs, in which I use Backup from Storage Snapshots. Enabling both features within Veeam allows me to have a single-pane-of-glass for my storage snapshot management and coincides storage snapshot retention with my backup schedule. This was crucial when recently I had to recover our most critical data that was deleted, allowing full restore of our data with minimal data loss.***
>
> — Shane Williford, Systems Architect, North Kansas City School District

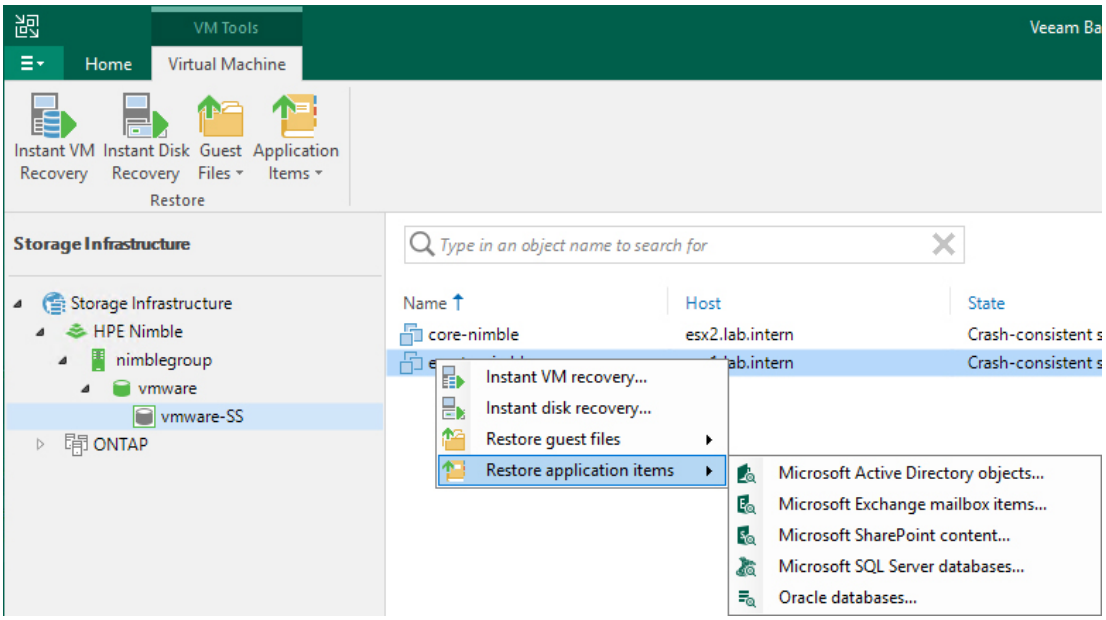


Figure 5: Object restore from Storage Snapshot

The second advantage of having a storage integration is the possibility to back up from Storage Snapshots. Backup from Storage Snapshots allows you to back up highly transactional VMs like database servers without the risk of VM stuns during VMware snapshot consolidation. Although the situation is much better with current vSphere versions, it is still the main reason why you want to use storage snapshots.

Finally, Backup from Storage Snapshots allows Veeam to use its proprietary data fetcher mechanisms to outperform classic VADP backups. This is especially relevant for full backups or any backup that has high change rates.

The best practice: Use storage integration if you have a storage that has snapshot support for Veeam Backup & Replication.

No. 7: VMware vSAN backup

Adoption of VMware vSAN continues to grow, and there are a few considerations when determining how to best back up workloads residing on VMware HCI. VMware vSAN does not use traditional storage protocols, which means that there is no direct storage access or Backup from Storage Snapshots option available.

The supported backup modes are virtual appliance/Hot-Add and network mode. Network mode is recommended since the Hot-Add process isn't required, which can result in faster incremental backups. With Hot-Add mode, Veeam Backup & Replication backs up VMs relative to the proximity to the VM data. That means the backups occur through the proxy on the host that has the most VM-specific data. To make this work properly, there must be one Hot-Add proxy per ESXi host. Host affinity for the proxy VM rules prevent the VMware Distributed Resource Scheduler (DRS) from moving those VMs to other ESXi hosts.

That means shorter backup windows, since there is less network traffic and latency. If a VM was on one host and the proxy on a different host, then there is more traffic over the network, which adds latency and reduces speed. With version 10, Veeam has added support for Linux proxies that support Hot-Add mode. Version 11 added support for new backup modes for Linux proxies, like:

- Network mode (NBD) that can be used with vSAN
- Direct SAN (NFS, iSCSI and FC)
- Backup from Storage Snapshot (iSCSI, FC)

Veeam Backup & Replication is certified as VMware-Ready for vSAN within the Data Protection and File Services category. The VMware Compatibility Guide (VCG) provides further information including support for vSAN in VMware Cloud on AWS.

> *We are backing up our vSAN infrastructure with one dedicated virtual proxy for each ESXi host. There are many proxies because of this, but they're quite small (4vCPUs). We also have a stretched VSAN cluster configuration with long distances between data centers. One proxy per ESXi host ensures that Veeam always assigns the "nearest" proxy to each VM that needs backed up. This avoids unnecessary traffic on data center interconnects.*
>
> — Manuel Aigner - Porsche Informatik

The best practice: Test which backup mode is fastest in your environment. One Hot-Add proxy per ESXi reduces vSAN network traffic. Hot-Add in general has higher throughput and network mode has less overhead.

No. 8: Security

Veeam Backup & Replication connects to VMware vCenter to manage backup and restores of VMs. From a security point of view, it is recommended that you leverage the principle of least privilege. VMware vCenter offers granular permissions for backups.

The required permissions reference guide contains a detailed description of permissions necessary for each backup mode. Different backup modes require different permissions. A security-relevant permission for the virtual appliance backup mode is that it requires the "remove disk" permission. Figure 6 shows a dedicated role that has limited permissions suitable for backup.

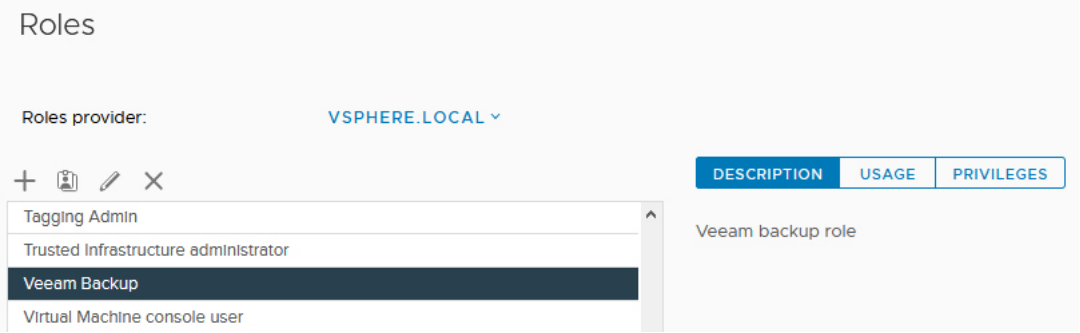


Figure 6: Dedicated vSphere roles for Veeam Backup & Replication

These security considerations can influence the choice of the backup mode. It's also possible to restrict specific backup servers (if you have multiple) to specific locations or objects in vCenter.

As attacks on the backup servers are becoming more and more popular, the backup environment itself should be hardened by following the best practices guide. The Veeam Hardened Repository is also something to consider for storing immutable backups.

The best practice: Work within the boundaries of the principal of least privilege.

No. 9: Plan your Veeam Backup & Replication deployment with Veeam ONE

Veeam Availability Suite™ contains a powerful planning tool for Veeam Backup & Replication deployments called Veeam ONE™.

The Veeam ONE monitor shows the actual status and current issues of the vSphere environment. Relevant issues around backup could be, for example, a high storage latency or old, large, many or orphaned VM snapshots.

The Veeam ONE reporter includes the VM configuration assessment report that shows potential backup issues. Typical issues the report shows are:

- VMware tools not installed
- Hardware version 4 or earlier
- Disks that cannot be backed up (i.e., independent disks)
- Datastores with less than 10% free space
- Raw device mappings in VMs

Fixing these issues before running backups prevents further backup issues.

The best practice: Use Veeam ONE to plan the Veeam Backup & Replication installation.

No. 10: Application-aware backup via VIX API

Best practice No. 4 recommends having VMware tools always installed and up to date. VMware tools offer Veeam administrators the opportunity to perform application-aware backups for Windows VMs without a direct network connection.

The preferred way to perform application-aware backups is to connect the application proxy via RPC or persistent guest agent to the VM. This is the fastest way. If network segmentation or firewalls prevent a network communication to the VM, Veeam can use the VIX API or in newer vSphere versions (version 6.5 and newer) the vSphere API for guest interaction. Figure 6 shows the login via VIX marked in green.

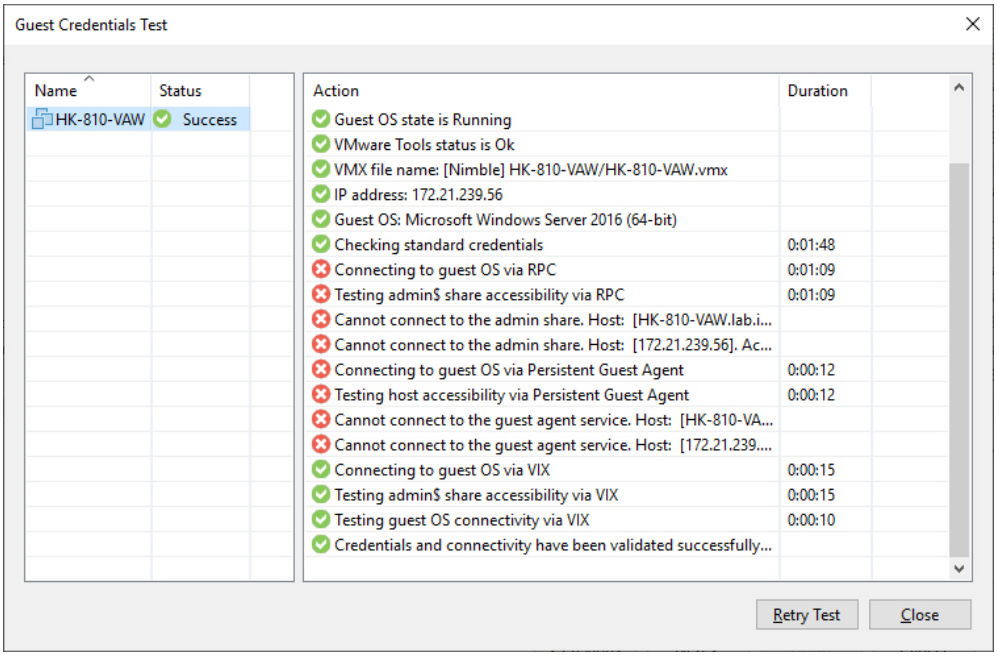


Figure 6: Guest credentials test via VIX API

VIX or vSphere API for guest interaction does not work out of the box. Though there are two requirements, further detail is available via Veeam KB 1788.

- The user account used by Veeam must be a member of the local administrators' group.
- If the account is not titled "administrator," then Windows User Account Control (UAC) must be disabled.

VIX or vSphere API for guest interaction is the fallback mode if RPC does not work. The result for the environment, where most VMs are not reachable via RPC, is that the backup will take longer because Veeam always tries RPC first. For those environments, it is possible to change the order to "VIX first" with the following registry key on the backup server or guest interaction proxy:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veeam\Veeam Backup and
Replication\ DWORD: InverseVssProtocolOrder
Value = 1
To disable (default behavior), value is 0 (false)
```

It is important to know that VIX or vSphere API for guest interaction has some limitations on restore operations. It is only possible to restore files but no application items. That means it is not possible to restore Microsoft Active Directory, Exchange or other similar objects this way; it requires network connection for restores. It should also be noted that the file is much slower when you go through the network.

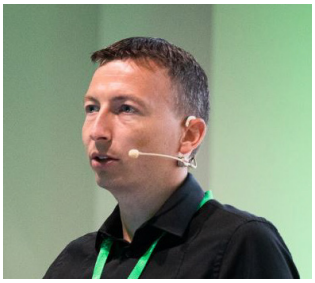
Speaking of speed, the VeeamLogShipper service that does SQL log-shipping can also use VIX as a fallback mechanism if it cannot reach the repository through the network. This can be too slow for most environments. That said, it is recommended that SQL log-shipping is done through the network.

The best practice: Keep in mind the limitations of VIX or vSphere API for guest interaction.

Conclusion

Veeam Backup & Replication ensures your data is backed up and recoverable with various backup and granular recovery options for VMware vSphere. Though Veeam Backup & Replication is engineered to work right out of the box with VMware vSphere, incorporating best practices from this guide will ensure optimum performance. To learn more, watch a demonstration or download a 30-day FREE trial today!

About the Author



Hannes Kasparick is a member of the Veeam product management team. Before that, he was senior systems engineer at Veeam in CEMEA. There he helped customers and partners design effective and efficient backup and DR solutions with Veeam products.

He managed Linux and Windows environments as well as infrastructure services like storage, network, firewalls and VMware. He has more than 15 years of experience in the IT business.