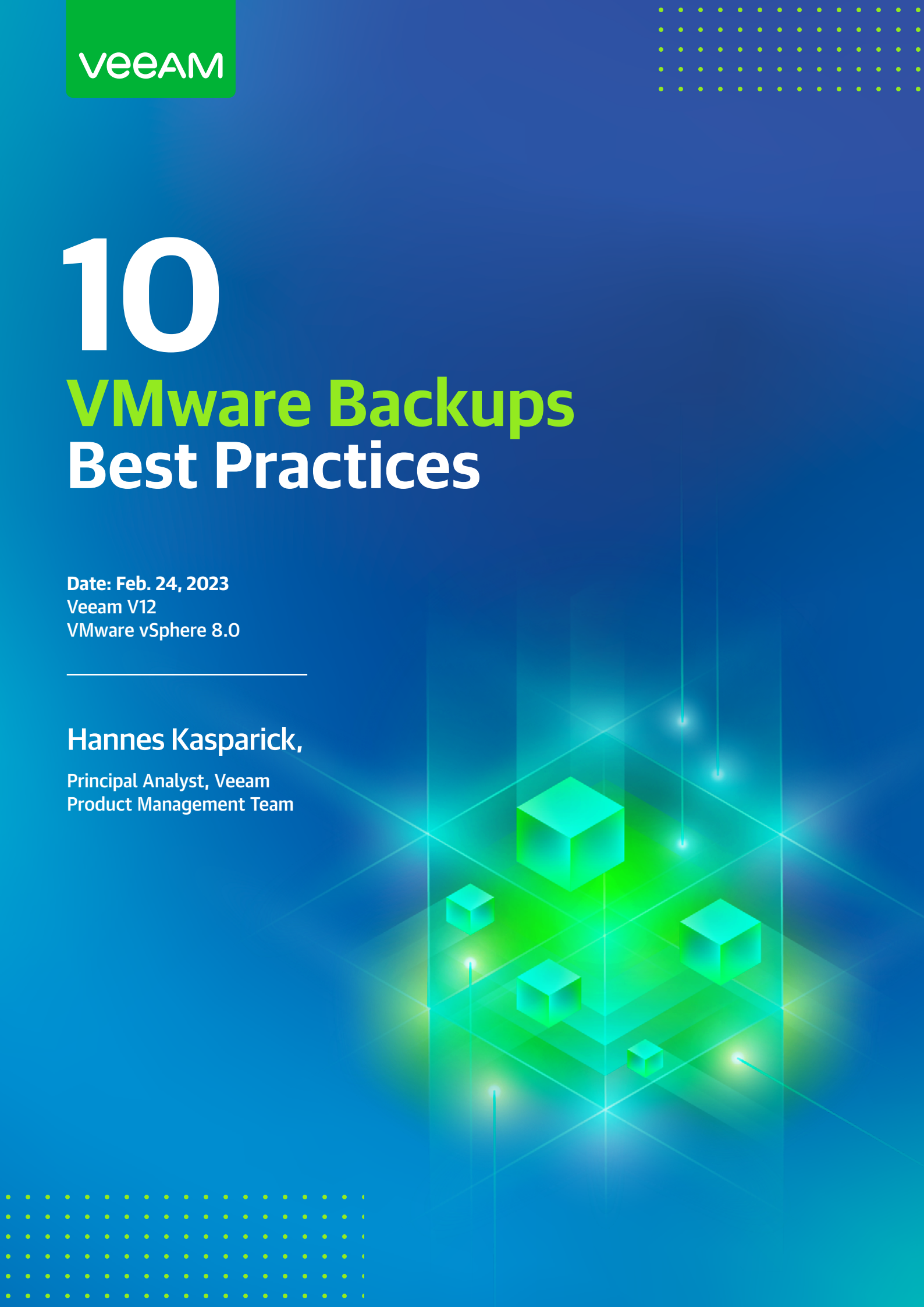
10 VMware Backups Best Practices

Date: Feb. 24, 2023
Veeam V12
VMware vSphere 8.0

Hannes Kasparick,

Principal Analyst, Veeam
Product Management Team



Contents

Executive summary 3
Introduction 3
One: Use current versions of Veeam Backup & Replication and vSphere 4
Two: Choose your backup mode wisely. 6
Three: Plan how to restore 9
Four: Integrate Veeam Continuous Data Protection into your disaster recovery concept 11
Five: Install VMware Tools 13
Six: Integrate storage-based snapshots into your backup concept. 14
Seven: VMware vSAN backup 15
Eight: Security. 17
Nine: Use Veeam ONE and Recovery Orchestrator to optimize backups and recoveries 18
Ten: Application-aware backup via VIX API 20
Conclusion 22
About the Author 23

Executive summary

Server virtualization has seen extensive adoption globally and remains a foundation for cloud computing. VMware vSphere remains the most popular hypervisor, and many Veeam® customers use it 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™ v12. 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. Specifically, this paper addresses data protection recommendations for VMware vSphere (no other hypervisors, cloud, SaaS or physical servers are covered here).

Introduction

Maintaining service levels, performance, 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 in backups. The backups must be stored on at least two independent types of media. The "independent" part of this cannot be overemphasized. Here, independent media refers to pieces of media that have no dependency from a technological perspective. Finally, another copy must be air-gapped, such that it's out of reach of malware, ransomware, natural disasters and unauthorized people.

Veeam has many options to store air-gapped backups, Such options include classic (WORM) tapes, the Veeam Hardened Repository (immutable backup storage based on a Linux server), immutable backups via object-lock support for AWS S3 object storage and Microsoft Azure blob storage, and finally immutability for HPE StoreOnce Catalyst stores.

This document describes several best practices with Veeam Backup & Replication and VMware vSphere that help eliminate data loss and ensure fast recovery. These best practices are dedicated to Veeam and VMware only!

These general best practices include:

- Having a backup and restore strategy that fits your business needs
- Having proper sizing
- Making sure Volume Shadow Copy Service (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, Red Hat Virtualization, cloud 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, businesses create requirements and tell their IT team which recovery point objectives (RPO) and recovery time objectives (RTO) are 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 (CDP) or storage snapshots? In the past, disaster recovery was mainly planned for natural disasters. With the rise of ransomware in recent years, this has changed. The most likely case for a full restore today is ransomware. Ransomware is a disaster, and disaster orchestration has become more important than ever.

With RPO and RTO defined, it is possible to accurately size up the required hardware. This includes the number of CPU cores, the amount of memory needed and the bandwidth requirements for WAN, LAN and SAN. Finally, you need a source and a backup storage unit that is fast enough to achieve the required speeds.

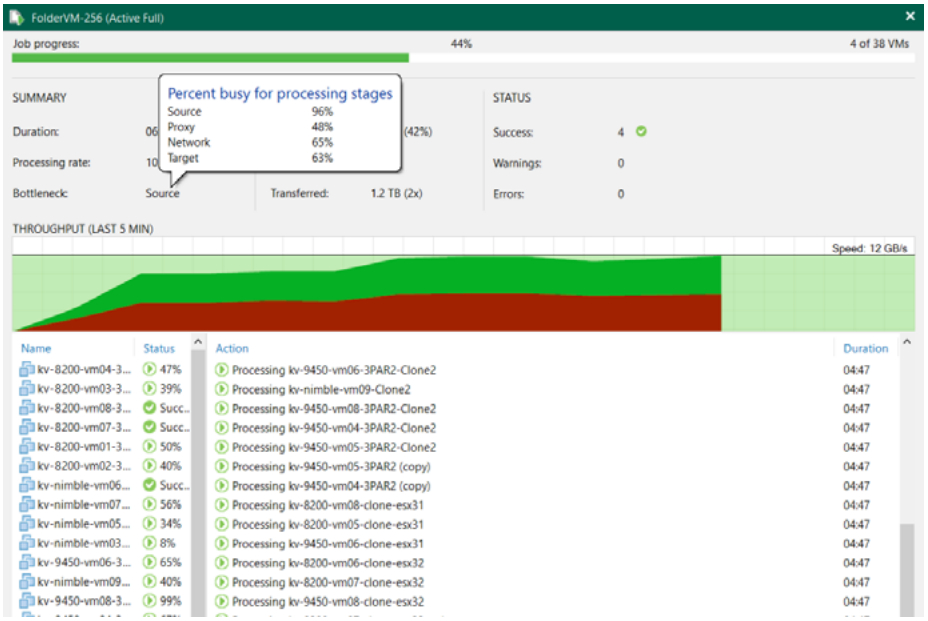
The next step is the backup itself. Veeam's application-aware image processing uses Microsoft VSS to achieve application-consistent backup of Windows virtual machines (VMs). This mechanism does not use VMware Tools quiescing.

To ensure application-aware image processing works reliably, it is necessary that the VSS writers located on the VMs are working properly.

One: Use current versions of Veeam Backup & Replication and vSphere

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

In Veeam Backup & Replication v11, Veeam laid the foundation for massive performance improvements. With "asynchronous read everywhere" and "unbuffered writes" for writing backups to the storage system, Veeam started maxing out 100Gbit/s links on one standard x86 four rack-units server. The screenshot below shows a backup job with 38 vSphere VMs running at 12GB/s to one 56 NL-SAS repository server.



100Gbit/s maxed out on one repository server

In Veeam Backup & Replication v12, there are many background improvements that allow the software to scale more efficiently. One of the most significant changes is the improved "per-machine backup chains" function, which allows customers to create jobs at a much larger scale than earlier versions (as well as many other functionalities, such as moving backups easily between repositories). Until V11, Veeam recommended having up to 300 VMs in one backup job. Customers extended that recommendation up to 500 – 700 VMs successfully. In V12, Veeam tested backup jobs up to 5,000 VMs in one job. That should be enough for most scenarios.

Improving security is a permanent topic for VMware and Veeam. The most notable security features in V12 are the following:

- Multi-factor authentication (MFA)
- Support for group Managed Service Accounts (gMSA) for application-aware processing
- Support for Kerberos-only environments
- Updates for the Hardened Repository without SSHor the need for credentials

Using the latest version of the products ensures that security improvements are implemented.

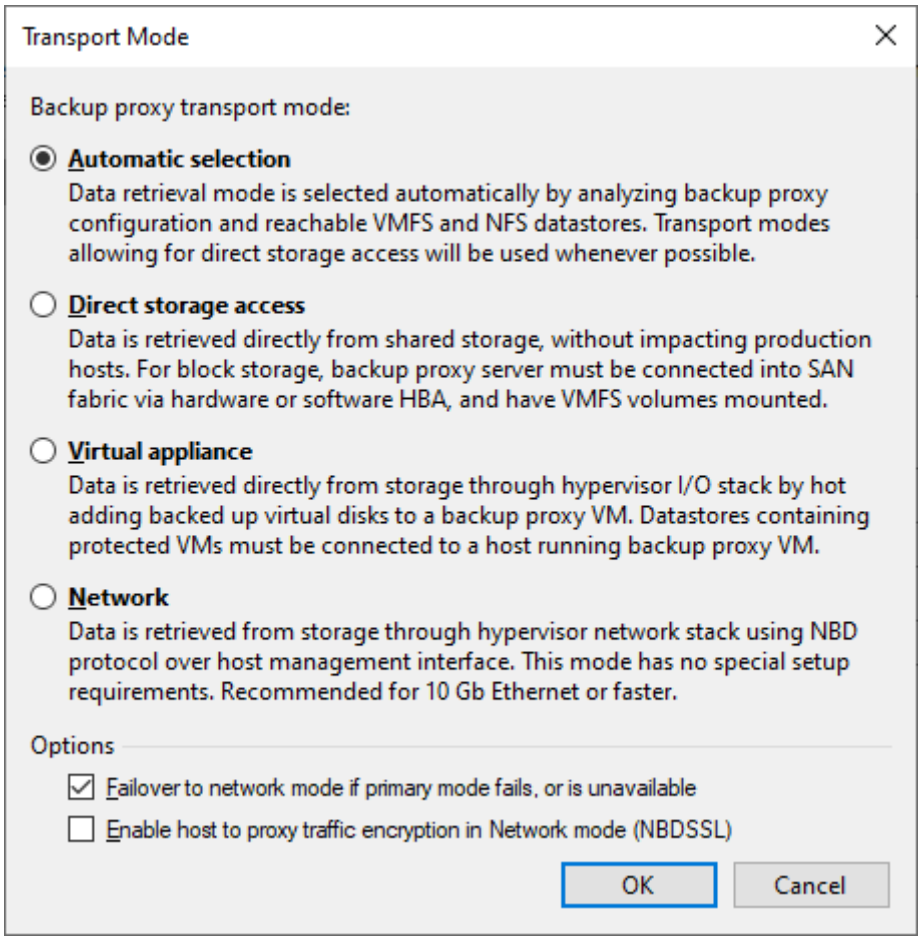
The best practice: Look out for improvements in the latest versions of Veeam Backup & Replication and VMware vSphere.

Two: Choose your backup mode wisely

With Veeam Backup & Replication, there are three different transport modes to back up VMs on vSphere. Starting with V12, Veeam supports all backup modes for Linux proxies as well. If you prefer Linux, 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:

- Network mode (NBD)
- Direct storage access, including Backup from Storage Snapshots
- Virtual appliance (Hot-Add)

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



Transport mode options

The network mode, or NBD mode, is the easiest way to conduct vSphere backups. Here, the Veeam proxy server uses 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 scales directly with the number of ESXi hosts in use. 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 especially for incremental backups. 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 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 on a 1Gbit interface. However, with 10Gbit 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 a Fibre Channel or iSCSI. Direct storage access mode also has an advantage over Hot-Add: There's no time-consuming Hot-Add operation.

NBD and direct storage access (excluding Backup from Storage Snapshot) both use vSphere Storage APIs – Data Protection (formerly known as vStorage API for Data Protection, or VADP). This API is VMware's snapshot-based framework that enables backup and restore of VMs. As it can impact backup performance, Veeam Backup & Replication does have the ability to bypass the API in three scenarios. These three scenarios are:

- Backup from Storage Snapshots
- Direct NFS (Network File System), like direct storage access
- Virtual appliance or Hot-Add

By having the ability to bypass the Data Protection API, Veeam can significantly improve backup performance. This is one of the reasons why Hot-Add became popular. However, there are many more advantages with 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. This is especially true with 1Gbit 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 simply 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. For vSphere backup, there are many options and it's best to check in your environment.

Three: Plan how to restore

After defining your optimal backup mode, it's important to look at the restore mode too. The restore test needs to satisfy the RTO. Veeam offers a variety of recovery scenarios to restore VMs from on-premises or cloud providers, physical machines, files and application objects. For many years, one can instantly recover any image-based backup to VMware vSphere (including physical servers).

First, it's important to know that file- and item-level restores differ from VM or disk restores. Veeam restores files, or items such as 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 Veeam persistent guest agent.

Since VM backup is snapshot-based and 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. Restore modes are identical to the restore modes for backup (i.e., direct storage access, virtual appliance and network). Additionally, there is Instant VM Recovery combined with Storage vMotion or quick migration.

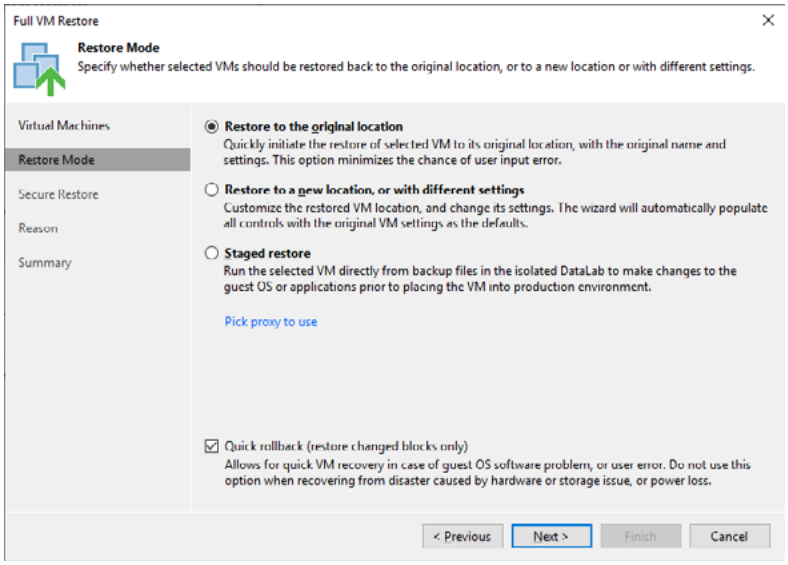
Both Hot-Add and NBD can restore thick- and thin-provisioned VMs. As already mentioned, the virtual appliance transport, or Hot-Add, has very good backup performance. This is also true for full VM or disk restores with Hot-Add. In many scenarios, it makes sense to have at least one Hot-Add proxy available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

Network mode is often the slowest way to restore.

Direct storage access mode works 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 VMware's vStorage API for restores, this is usually not the fastest option. An exception to this is when restoring with direct NFS, where Veeam Backup & Replication bypasses VADP.

Note: *With direct storage access, one can try to disable WRITE_SAME on the ESXi host(s). The impact is hard to predict, so there is no general recommendation. For more details, please see: https://kb.vmware.com/s/article/2146566.*

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, though the quick rollback option must be manually enabled during restore.



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. There are two options to transfer the VM data from the repository NFS datastore back to the production datastore:

- Veeam Quick Migration
- vSphere Storage vMotion

Note: *Keep in mind that Storage vMotion has a low priority in vSphere, so it will take more time to finish.*

Another thing independent from vSphere or Veeam: If you use synchronously mirrored storage, then restore will be faster by deactivating the synchronous mirror on the volumes where you restore. No matter how fast the storage is, the speed of light is limited. The second storage array must acknowledge that it has received data, which takes time. Restore performance can double (or even more if the distance between the arrays is large). Depending on your storage vendor, it may make sense to break the mirror for restore and then resync afterwards.

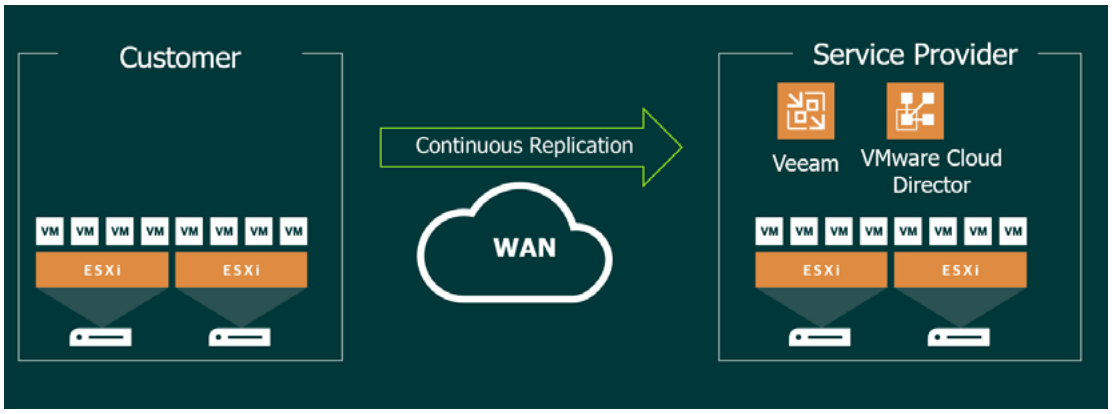
Since there are diverse options for full VM restores, you can use the following table to quantify the results of each mode and decide which one is best for you.

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. If you use synchronously mirrored storage, think about breaking the mirror for faster restore temporarily.

Four: Integrate Veeam Continuous Data Protection into your disaster recovery concept

With Veeam Backup & Replication, you can replicate VMware VMs every few seconds without vSphere snapshots. The feature is called Continuous Data Protection (CDP), which allows you 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 (which is snapshot-based). CDP can be used within your own data center or to a Veeam Cloud & Service Provider (VCSP).

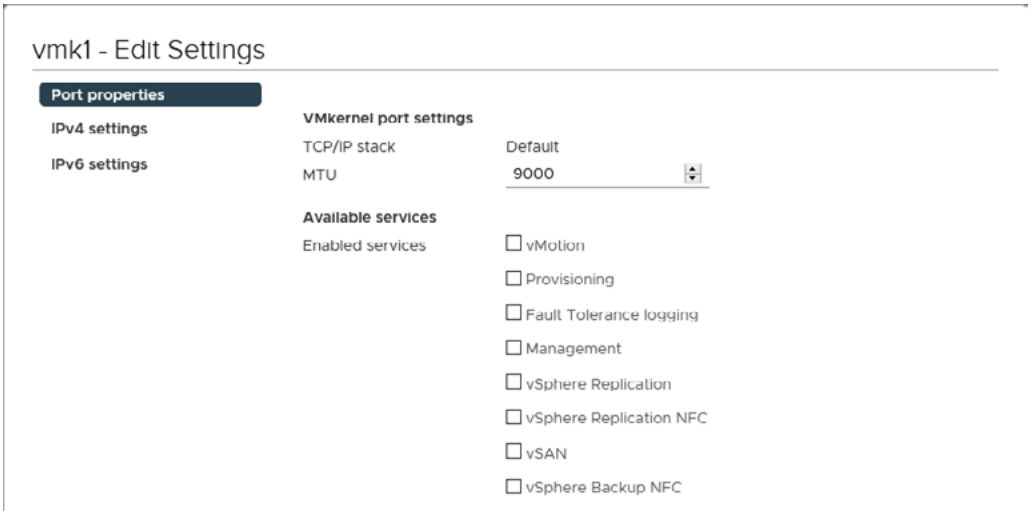


Overview of "disaster recovery as a service" with Veeam CDP

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 changed data. While classic backups happen every eight, 12 or 24 hours, and only use network bandwidth a few times per day, CDP has a constant stream of data to transfer. Bandwidth estimations 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 slightly lower than what you see on the storage.

For the vSphere datastore destination, you will 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 or more RPO time. Two seconds of RPO time is possible, but this uses more disk space and creates more I/O on the target datastore, as 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 I/O load and RPO time, the network traffic for CDP can be significant. MTU 9000 increases the performance by 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 screenshot below). Existing distributed virtual switches can be used, and there is no need to configure a dedicated vSwitch for CDP traffic.



No services enabled for VMkernel port that handles CDP traffic

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 host 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.

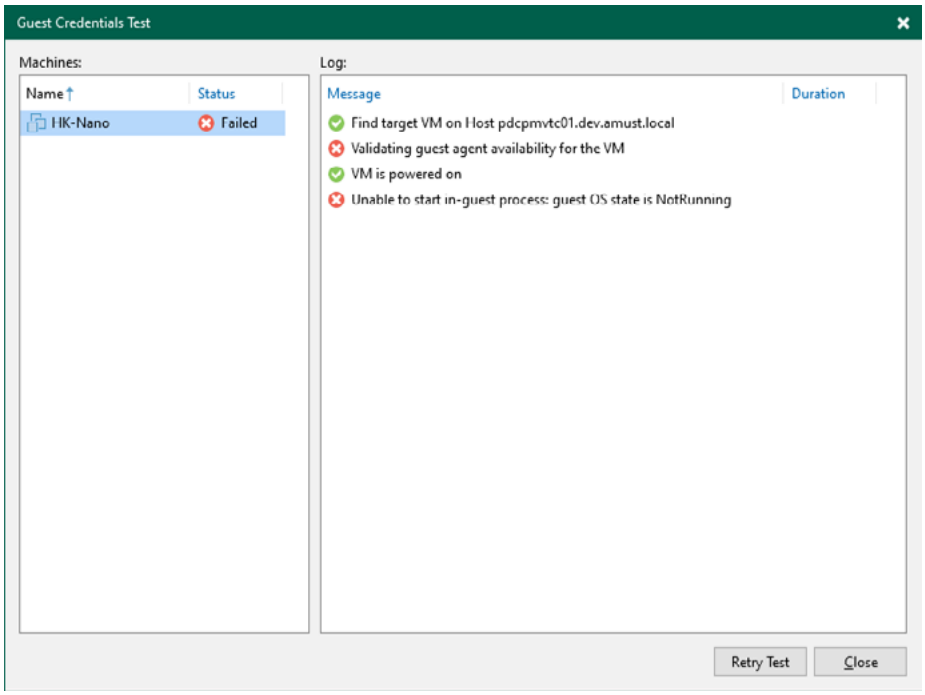
When implementing CDP, there are several important infrastructure requirements that apply only when CDP replication is used. Specifically, the backup server, CDP proxies, the vCenter Server and ESXi hosts must be able to resolve each other's DNS names. For additional requirements, please consult the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

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

Five: Install VMware Tools

In many situations, Veeam Backup & Replication relies on the existence of VMware Tools that run within the VMs. For example, without VMware Tools, Veeam Backup & Replication cannot see IP addresses or operating system versions. 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 best practice number 10 for more information on VIX). The screenshot below shows an example of failed guest credentials test due to missing VMware Tools:



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.

Six: 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.

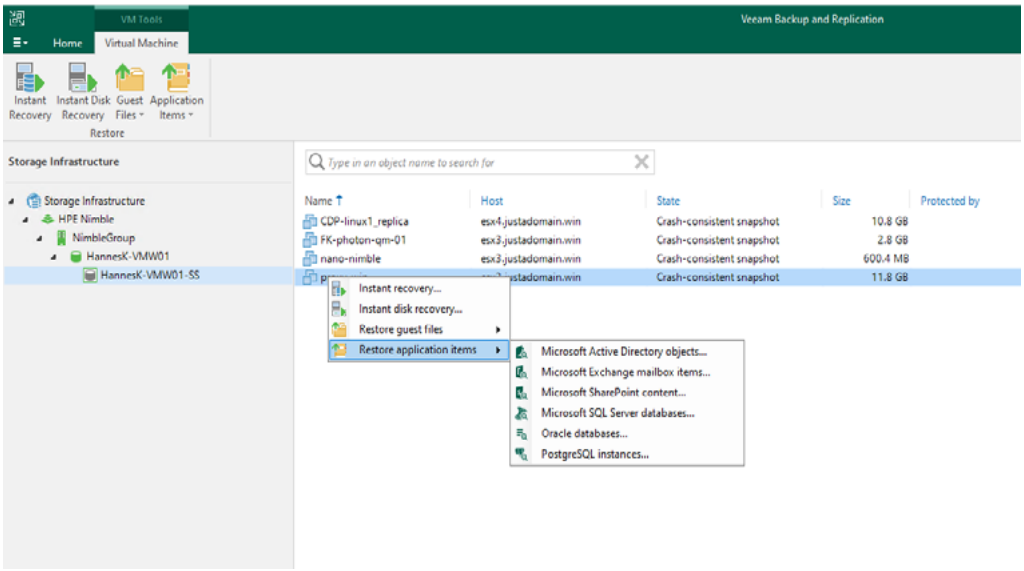
The first option is that Veeam Backup & Replication can open storage snapshots and restore files and objects directly from the storage snapshot. This allows you, for example, to schedule storage snapshots every 15 minutes without being required to create VM snapshots as well. Though a snapshot every 15 minutes is not a real backup (as 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 vSphere snapshot before the storage snapshot.*

Below, you can see Veeam Explorer™ for Storage Snapshots, which follows a similar concept to all other Veeam Explorer platforms. The left side shows the storage snapshots (i.e., the logical unit numbers (LUNs) or volumes and the snapshots of one volume). 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 items.

Now imagine the storage creates snapshots of critical LUNs or volumes every 15 minutes and deletes them after four hours. This would mean it's possible to restore data from 15 minutes ago, rather than older data from much older backups.

> *"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.



Item-level restore from a 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 snapshot consolidation. Although the situation is much better with current vSphere versions, it is still the main reason why customers want to use storage snapshots.

Finally, Backup from Storage Snapshots allows Veeam to use its proprietary data-fetcher mechanisms to outperform classic vSphere vStorage API-based 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 array that has snapshot support for Veeam Backup & Replication.

Seven: VMware vSAN backup

As adoption of VMware vSAN continues to grow, there are a few considerations to keep in mind 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. Testing which mode fits your needs best is recommended. With NBD, there is no Hot-Add overhead, which usually results in faster incremental backups.

On the other hand, the Hot-Add mode has some optimizations. 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 best, there needs to 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.

These optimizations can result in faster backups since there is less network traffic and latency. If most of the VM data is on one host and the proxy is on a different host, then there is more traffic over the network, which adds latency and reduces speed.

Deploying one backup proxy per ESXi host can result in overhead management and resource usage (CPU, disk, RAM), as there are many proxy VMs. With enough bandwidth, the overhead of having one proxy per ESXi host usually does not pay off. Having only a few Hot-Add proxies per vSAN cluster is better in most situations.

There are up to 32 VM snapshots in parallel per default on vSAN

Per default, Veeam creates a maximum of four snapshots per datastore. With hundreds of VMs on one VMware vSAN datastore, there would be a negative impact on performance. This is why Backup & Replication creates up to 32 snapshots in parallel on vSAN datastores. If this is not enough, the value can be changed with the VSANMaxSnapshotsNum (DWORD) registry value under the "HKLM\SOFTWARE\Veeam\Veeam Backup and Replication" key on the backup server.

```
Key Location:         HKLM\SOFTWARE\Veeam\Veeam Backup and Replication

Value Name:           VSANMaxSnapshotsNum

Value Type:           DWORD (32-Bit) Value

Value Default Data:   32
```

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.

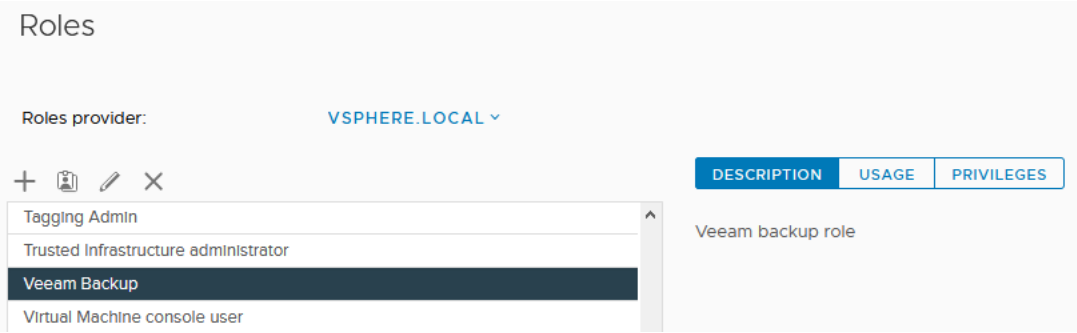
> *"We are backing up our vSAN infrastructure with one dedicated virtual proxy for each ESXi host. There are many proxies because of this, but they're quite small (4vCPUs). We also have a stretched vSAN cluster configuration with long distances between data centers. One proxy per ESXi host ensures that Veeam always assigns the 'nearest' proxy to each VM that needs to be 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 host reduces vSAN network traffic but is usually overkill. Hot-Add in general has higher throughput, and NBD has less overhead.

Eight: 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. The figure below shows a dedicated role that has limited permissions suitable for backup.



Dedicated vSphere roles for Veeam Backup & Replication

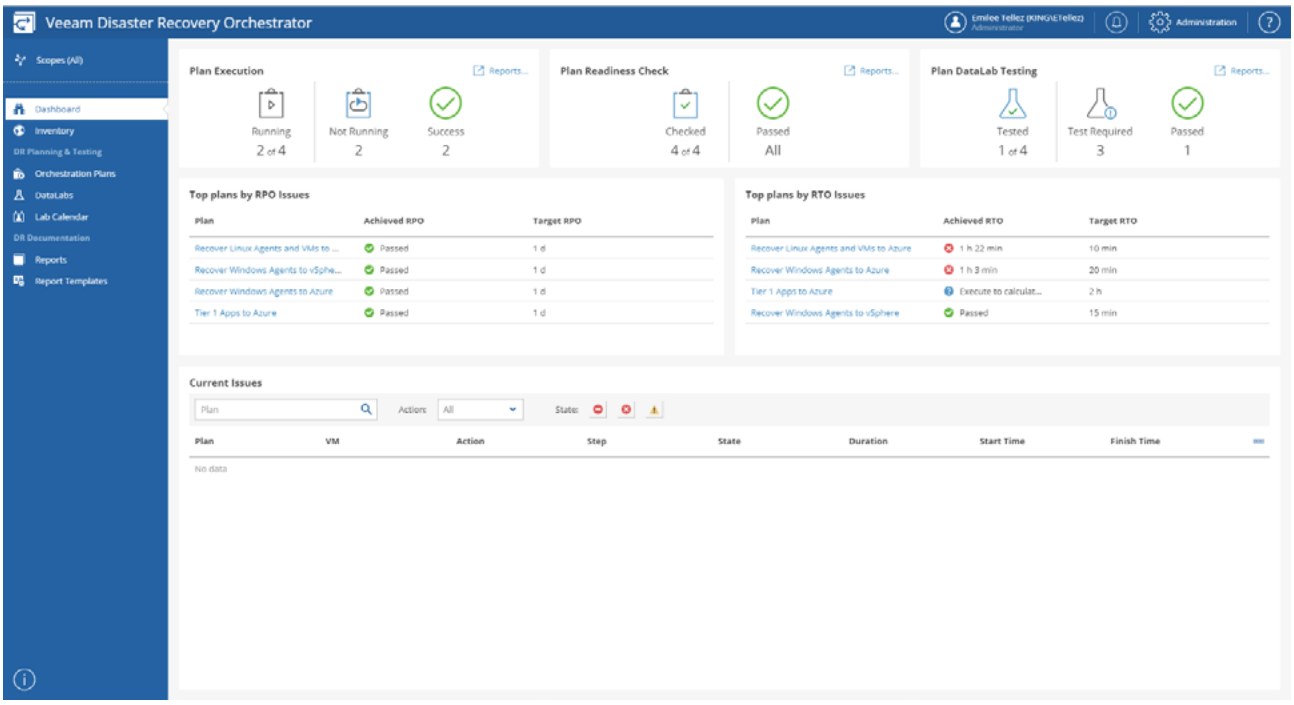
These security considerations can influence the choice of the backup mode. It's also possible to restrict specific backup servers (if you have multiple) to specific locations or objects in vCenter.

As attacks on the backup servers are becoming more and more popular, the backup environment itself should be hardened by following the Veeam Backup & Replication best practices guide. The Veeam Hardened Repository, or any other immutable storage option, is also something to consider.

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

Nine: Use Veeam ONE and Recovery Orchestrator to optimize backups and recoveries

Veeam Data Platform Premium (new since 2023) contains a powerful planning tool for Veeam Backup & Replication deployments called Veeam ONE™ and a recovery orchestration tool called Veeam Recovery Orchestrator. Veeam Recovery Orchestrator (formerly known as Veeam Disaster Recovery Orchestrator) helps orchestrate all kinds of VM recovery scenarios.

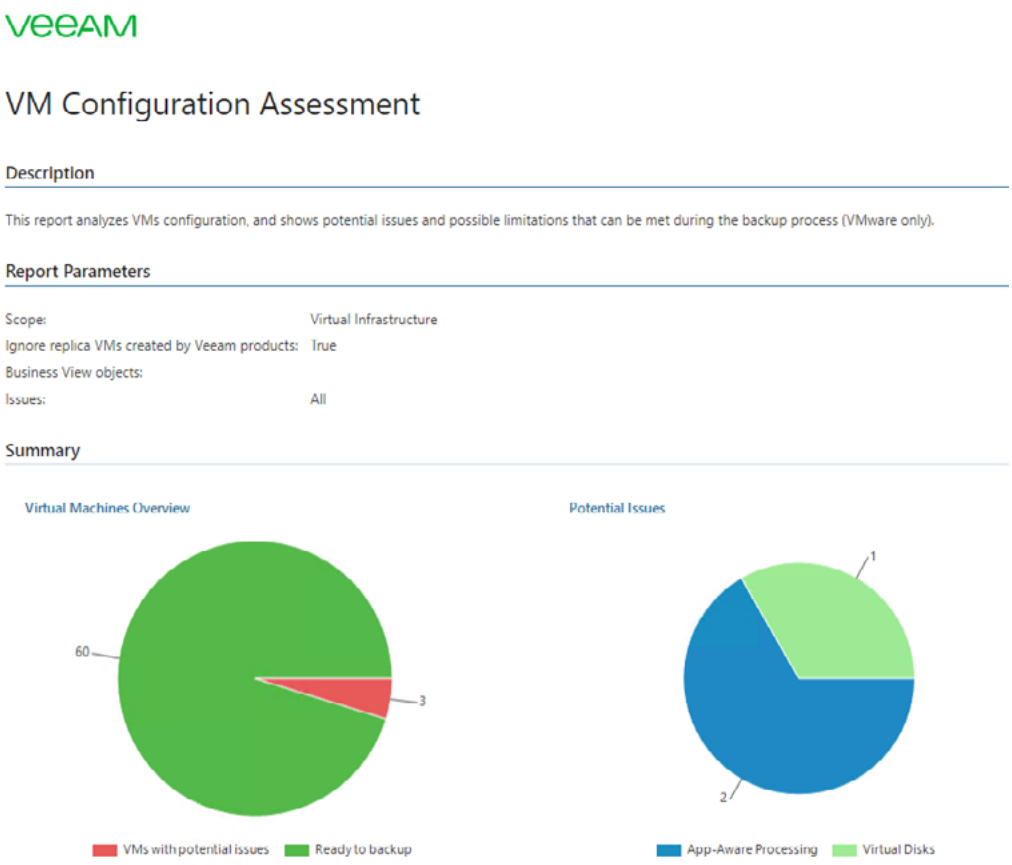


Veeam Recovery Orchestrator dashboard

In the past, Veeam Recovery Orchestrator was mainly addressing use cases around natural disasters such as fire, floods and earthquakes. For many customers, however, the most common large-scale data recovery operation occurs after a ransomware attack — not a natural disaster. Veeam Recovery Orchestrator provides many ways to help orchestrate restores in VMware environments:

- Orchestrated failover for snapshot-based Veeam replication
- Orchestrated failover for snapshot-less CDP replication
- Orchestrated restore from a repository to vSphere, including scans for ransomware during recovery
- Orchestrated restore to Azure (physical and VMs)
- Orchestrate failover from storage systems

Veeam ONE provides monitoring and reporting of Veeam backup products and the connected environment. For example, this could be high-storage latency, or old, large, many or orphaned VM snapshots. However, there are also some useful features regarding vSphere backup specifically.



Veeam ONE: VM configuration assessment report for VMware

Veeam ONE includes the "VM Configuration Assessment" report, which shows potential backup issues. Typical issues the report shows are:

- VMware Tools not installed
- Hardware version four or earlier (should not happen in 2023)
- Disks cannot be backed up (i.e., independent disks)
- Datastores with less than 10% free space
- Raw device mappings in VMs

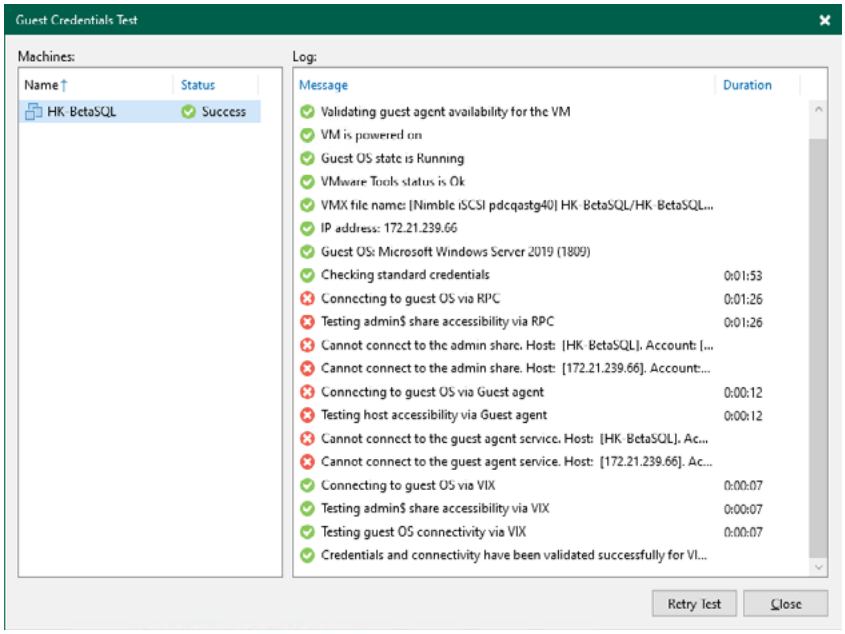
Fixing these issues before running backups prevents further backup issues.

The best practice: Use Veeam Recovery Orchestrator and Veeam ONE to be prepared for the worst case and to optimize your backup strategy.

Ten: Application-aware backup via VIX API

Best practice number four 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 remote procedure call (RPC) or persistent guest agent to the VM. This is the fastest way. If network segmentation or firewalls prevent 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. The figure below shows the login via VIX marked in green.



Guest credentials test via VIX API

VIX or vSphere API for guest interaction does not work out of the box. Further detail is available via Veeam KB 1788, but two key requirements are:

- The user account used by Veeam Backup & Replication must be a member of the local administrator's 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. This is because Veeam Backup & Replication always attempts 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 not application items. This means it is not possible to restore Microsoft Active Directory, Exchange or other similar objects this way, as it requires a network connection for restores. It should also be noted that file restores are much slower when performed over 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 Data Platform provides the data resiliency and confidence required to keep your business running. Designing infrastructure and implementing tools that provide secure and reliable backups, advanced monitoring and analytics, and robust and orchestrated recovery is critical when it comes to keeping enterprises online.

VMware vSphere is the de facto standard virtualization platform in businesses across the globe today. While Veeam Data Platform itself is highly optimized, it is still important to regularly review your environment to achieve the best possible performance. Applying the best practices covered in this guide will help ensure optimum results when it comes to protecting your data.

Try Veeam for free 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.