Veeam Hypervisor Migration to Proxmox Virtual Environment Guide

Ver 1.0

Olivier Rossi — Veeam Sr. Solutions Architect

Rich Brambley — Veeam Sr. Solutions Architect

Table of Contents

1. Introduction

Virtualization technology has become an integral part of modern IT infrastructures, providing incredible flexibility, scalability, and cost-efficiency to businesses of all sizes. Several hypervisor options have gained momentum in recent years. Solutions such as VMware, Microsoft Hyper-V, Proxmox VE (Virtual Environment), and Nutanix AHV Virtual Environment have evolved into robust and reliable choices for virtualization needs. Recognizing that business requirements are dynamic; virtualization platform selection must also be appropriately dynamic.

Migrating away from one hypervisor to another introduces a complex decision-making process for businesses. A non-exhaustive list includes application dependencies, migration timeline, identifying workload criticality, and application downtime impact to the business.

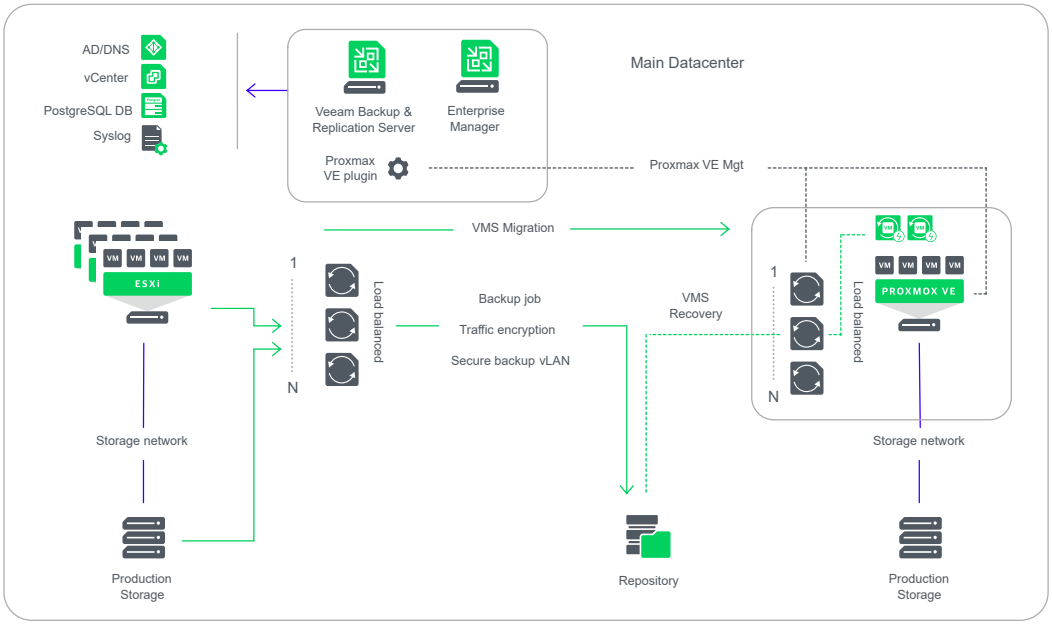
This guide will provide step by step instruction to leverage Veeam's unique abilities to restore VMware VM backups, with on-the-fly conversion, to the selected target hypervisor, in this guide: Proxmox VE, for migration purposes. This guide will also describe how to leverage Instant VM Recovery to migrate back from Proxmox VE to VMware.

Make sure you understand the application and the component dependencies prior to performing the migration.

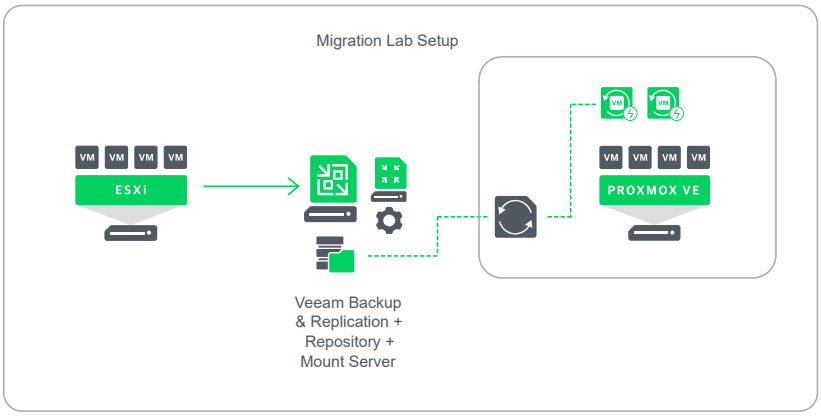
2. VM Recovery (Migrate from VMware to Proxmox VE)

Veeam VMware VM backup can be restored directly to Proxmox VE with on-the-fly conversion.Provided that the proper Storage Types are in place, it is possible to convert the VM's disk types to RAW, QCOW2 and VMDK when restoring to Proxmox VE.

It is recommended to install the appropriate Qemu-guest-agent prior to restoring to ensure proper VM connectivity out of the gate.



2.1 Scenario Setup



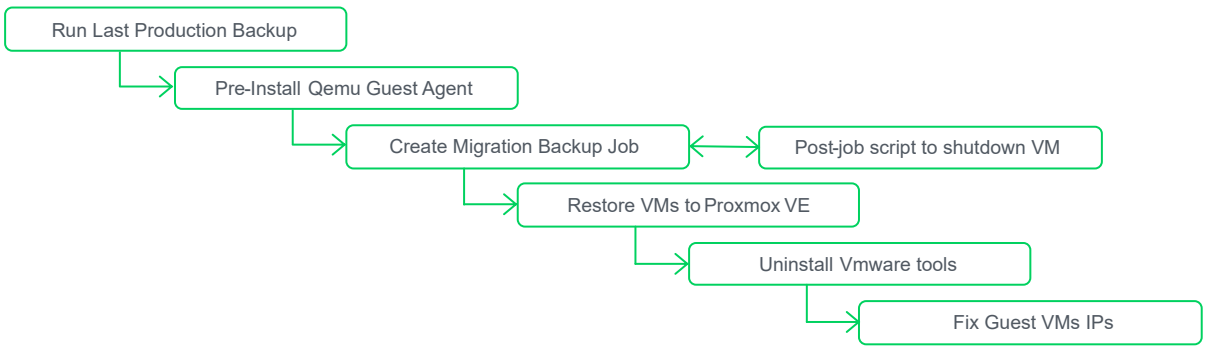
The lab is comprised of an all-in-one VBR/Repo server. VMware ESX Windows and Linux VMs are backed up. The target Hypervisor is Proxmox VE.

2.2 Considerations

For this migration document, we will assume that separate migration specific backup jobs have been created and that the source VMware VMs have been turned off prior to recovering to Proxmox VE.

Migration Maintenance Window: Minimize Production Downtime

With this first version of Veeam Backup for Proxmox VE, the only option to migrate to Proxmox VE is to perform a full VM recovery. To minimize production downtime, it is recommended to recover VMs to Proxmox VE in small batches and stagger them. A maintenance window should be scheduled per batch to:



Note that all above steps can be scripted except for the “Restore VMs to Proxmox”.

Select the appropriate Qemu-guest-agent.

Destination Hypervisor vCPUs considerations

Proxmox VE has a hard vCPUs limit equals to the [number of cores] x [number of sockets]. Trying to restore an "oversubscribed" will fail with a "TASK ERROR: MAX X vcpus allowed per VM on this node" error.

The rule of thumb is to ensure that none of the source VMware VMs have more vCPUs than the weakest Proxmox VE node in the target cluster. It is possible, (though not recommended) to override that limit by editing the QemuServer.pm file (look for $allowed_vcpus). The preferred workaround is to reduce the vCPU count of the VMware VM prior to creating the migration specific backup job.

Destination Hypervisor Storage options

Veeam Backup for Proxmox supports 3 disk types: RAW, QCOW2 and VMDK. Conversion to the desired disk type will only work provided that the proper Storage Types are in place on the target Proxmox cluster nodes. Regardless of the Proxmox Storage Type, you will have the option to select the target disk type at the "Select Storage" step of the restore wizard. If the disk type is unsupported, you get a warning and Veeam Backup for Proxmox will make the necessary background adjustments to a supported disk type.

Installing Proxmox VE guest VM agents

VirtIO drivers should be pre-installed on most Linux distributions. For Windows, the VirtIO drivers must be installed manually.

The Qemu-guest-agent is used to exchange information between the Proxmox host and guest VM, and to execute command in the guest VM.

When to Shut Down source ("old") VMs As Part Of The Migration Process

VMs scheduled to be migrated should be shut down immediately prior to a final, successful backup. This process can easily be automated as part of the final backup job. (See this Help Center page for reference:

https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_advanced_scripts_vm.html?ver=120.)
In this case, the first checkbox labelled "Run the following script before the job:" on the Scripts tab must be enabled and the field for the path to the script location must be populated appropriately. Note that these scripts will execute as the service account configured on the Veeam Backup and Replication server; if this is not appropriate or available in a specific environment, then alternate means of script execution must be explored and considered.

Removal of Hypervisor Specific Guest-Tools

At scale, removal of prior/old hypervisor-specific guest tools/drivers should be done via scripting; both in-guest and remotely executed methods may be appropriate. Do not remove prior/old hypervisor agents until the migration of the VM is complete.

Removal of the hypervisor agent prior to the migration may result in the loss of IP address, MAC address, and other networking information in the VM during the migration.

- For VMware, see: https://knowledge.broadcom.com/external/article/315639/uninstalling-vmware-tools-in-a-windowsv.html

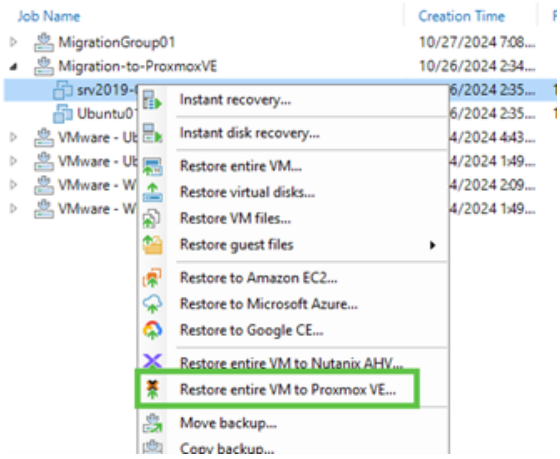
Rollback Plan

In the event of a failure, there may be a need to rollback a migration attempt. The rollback plan should include the following steps:

- Gather necessary logs (open cases)
- Power OFF failed VM(s)
- Restore Production VMs from the last Production backup and Power On VM(s) in original hypervisor
- Verify VM(s) and Applications
- Perform cleanup i.e. storage, jobs of failed VM(s)

2.3. Recover VMs to Proxmox VE

The recovery to Proxmox VE is straight forward: Simply select and right-click the VM you wish to restore and follow the wizard. Please note that in version 1, recoveries cannot be scripted.



3. Instant VM Recovery (Migrate to VMware)

3.1. What is IVMR?

Instant VM Recovery is a feature supported for most virtualization platforms, including VMware, Hyper-V, Nutanix AHV, Oracle Linux Virtualization Manager, Red Hat Virtualization and Proxmox VE. This feature allows IT administrators to quickly recover virtual machines (VMs) in the event of a failure or disaster.

When a VM fails, the traditional recovery process involves restoring the VM from a backup. This process can be time-consuming and disrupt the normal operations of an organization.

With IVMR, the recovery process is expedited and simplified. IVMR allows administrators to rapidly restore a failed VM by booting it directly from the backup storage, without the need to restore the entire VM data to the primary storage environment to gain access to the data. This significantly reduces the downtime and ensures a swift recovery of critical services and applications. Ultimately, the data may need to be moved on to production storage, so Veeam orchestrates that process too, combining any changed data from the instantly recovered VM with restored data to minimize data loss.

The list of supported source backup types and cross platform/hypervisor instant recovery options is extensive. While the instant recovery process is specific to each virtualization platform, Veeam will handle cross-hypervisor conversion onthe-fly.

* Note that currently for Proxmox VE backup Version 1.0, the cross-hypervisor on-the-fly conversion only works with Proxmox VE as the source hypervisor.

For example, it is possible to use a VMware VM backup as a source to instantly recover to Hyper-V and/or Nutanix AHV.

The various supported source types and instant recoveries hypervisor destinations can be found in our Help Center user guides:

- VMware vSphere
- Hyper-V
- Nutanix AHV
- oVirt and RHV
- Proxmox VE

3.2. Should you use IVMR for all migrations?

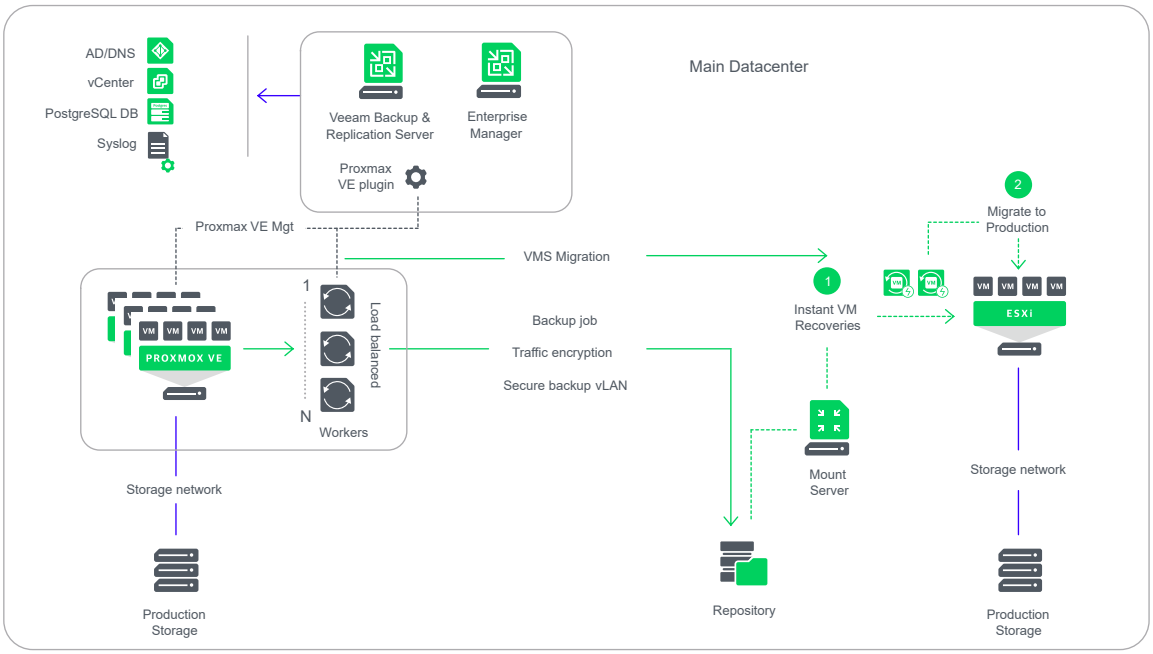
While Veeam's IVMR capabilities are quite extensive, IVMR may not always be the best method for migrating 24/7 sensitive application workloads.

IVMR drastically shortens the RTO by essentially reducing VM boot time and cross-hypervisor conversion time, however, minimal downtime is still required.

For applications that require consistency across multiple systems, please also consider native HA capabilities within the application. Use this in conjunction with IVMR.

Always check with application owners for application SLAs and application documentation for any application-level migration.

3.3. Proxmox VE IVMR



During instant recovery, Veeam Backup & Replication runs workloads directly from compressed and deduplicated backup files. When an IVMR session starts, the VMs are directly mounted from backup files via the mount server to the target ESXi host and the VMs are booted.

Writes are redirected to the instant recovery write cache area before engaging the final step, which is to migrate to production.

3.4. Considerations

IVMR offers several advanced scanning capabilities including AV, Malware, and YARA with the opportunity for remediation. For this migration document, we will assume that all backups are free of infections and will forego any scanning. We will also assume that all source Proxmox VE VMs have been powered off. Lastly, we will assume that our backup jobs have been designed for the purpose of migration and align with the restore priorities and concurrency we want to achieve.

NOTE: To reduce the time of the final incremental backup consider performing backups so that the incremental time frame is as short as possible. Please refer to Appendix A: Migration Tools and Scripts.

Migration Maintenance Window: Minimize Downtime and Duration

A maintenance window to perform the migration should be scheduled to start right after the last increment backup. Allocate at least 2 hours of hands-on time to perform, monitor, and verify the migration of the VMs. To reduce the duration of the maintenance window, increase the frequency of increments prior to migration. This will reduce the amount of changed data that will be stored and applied during migration.

When to Shut Down source ("old") VMs As Part Of The Migration Process

VMs scheduled to be migrated should be shut down immediately prior to a final, successful backup. This process can easily be automated as part of the final backup job. (See this Help Center page for reference: https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_advanced_scripts_vm.html?ver=120.) In this case, the first checkbox labelled "Run the following script before the job:" on the Scripts tab must be enabled and the field for the path to the script location must be populated appropriately. Note that these scripts will execute as the service account configured on the Veeam Backup and Replication server; if this is not appropriate or available in a specific environment, then alternate means of script execution must be explored and considered.

Removal of Hypervisor Specific Guest-Tools / Agents

At scale, removal of prior/old hypervisor-specific guest tools/drivers should be done via scripting; both in-guest and remotely executed methods may be appropriate. Do not remove prior/old hypervisor agents until the migration of the VM is complete.

Removal of the hypervisor agent prior to the migration may result in the loss of IP address, MAC address, and other networking information in the VM during the migration.

- For Proxmox, see: https://pve.proxmox.com/wiki/Qemu-guest-agent

Rollback Plan

In the event of a failure, there may be a need to rollback a migration attempt. The rollback plan should include the following steps:

- Gather necessary logs (open cases)
- Power OFF failed VM(s)
- Power On VM(s) in original hypervisor
- Verify VM(s) and Applications
- Perform cleanup i.e. storage, jobs of failed VM(s)

3.5 Step by Step IVMR to VMware

3.5.1 Windows VM

Restoring a Windows based VMware VM is a straightforward process. Using the Instant Recovery Wizard, one can easily select multiple Windows-based VMs to restore to VMware.

3.5.2 Linux VM

The same process used to Instant Recover a Windows VM is used to restore a Linux VM. Additional points must be considered when restoring a Linux VM.

- We strongly recommend having dracut and mkinitrd installed on workloads that will be restored. Otherwise, they may not boot after restore.

- Open the /etc/fstab/ file and check that all file systems are mounted using UUID. If any filesystems are mounted using block device name, the restored VM may not boot.
- A Helper Appliance will be used to assist the restoration of Linux VMs to Hyper-V. This appliance will help patch Linuxbased machines so they can start on a new host or with different settings. When configuring the helper appliance, the following should be considered:
  - Select the same network where the backup server and mount server reside.
  - Select the same VLAN where the backup server and mount server reside. A value of 0 means the VLAN is not set.

3.5.3 Considerations and Optimizations

Source Environment Performance Considerations

When performing the migration, source environment performance considerations include:

- Impact on source storage operating environment (latency, performance impact)
- Impact on source hypervisor hosts when performing backups.
- The storage that will become the swing space should be configured for the highest performance possible. Storage type should be considered, and configuration of the storage should be optimized for highest performance of both write and read operations.
- Swing space storage should be virtually/physically directly connected. (DAS/FC/iSCSI)
- In a brownfield environment, disable existing backup jobs and create new backup jobs using "restore points" for the Retention Policy — See Appendix-A
- Consider shorter incremental backup intervals leading up to cutover, days to hours, or hours to minutes. — See Appendix-A
- Consider concurrency of processes running in existing virtual environment
  - Leverage throttling and/or storage I/O control as necessary to reduce impact on the source environment.

Network Tips and Considerations

The following networking considerations should be considered:

- Minimum networking speed of 10 Gbps is recommended to ensure enough bandwidth is available for the migration of the data.
- If a dedicated backup network exists, it is ideal to leverage this for the migration. Consider leveraging the preferred networks option in Veeam or configure a static route for migration if a dedicated backup network does not exist.

Target Environment Considerations

- Storage type and performance should be the equivalent of production storage to ensure optimal performance for a production environment.
- Do not over-subscribe total CPU and RAM resources available on the VMware host.
- Reserve enough space on target hypervisor datastore to continue operations.
- Reserve enough Veeam licensing to continue data protection operations.

New Installations and Existing Deployments Considerations

- **New Installations —** Ability to design migration infrastructure and architecture specifically for migrating workloads targeting the highest performance possible.
  - Design leveraging and optimize available resources without existing environment constraints.
  - New jobs designed and optimized for migrations.
- **Existing Deployments —** Cannot guarantee performance due to existing infrastructure and design. Modifications to improve performance may include additional infrastructure, reconfiguration, and other tuning operations.
  - Modify the backup server with additional CPU and RAM resources.
  - Add a mount server or separate the mount server from the backup server.
  - Consider using swing space on performant storage (SAN) instead of the existing backup repository.
    - If deduplication storage or object storage in cloud is used for the repository, local swing space is a requirement.

4. Summary

In this comprehensive guide, we have provided step by step instructions to leverage Veeam's unique VM Recovery and Instant VM Recovery capabilities to perform migrations from VMware to Proxmox VE and back to VMware.

We have highlighted when Application-level migration is preferred to minimize downtime.

Lastly, we have demonstrated how to scale the migration by using Veeam PowerShell scripts and wizardry to address both greenfield and brownfield environments.

You should now be well equipped to go forth on your Hypervisor migration journey.

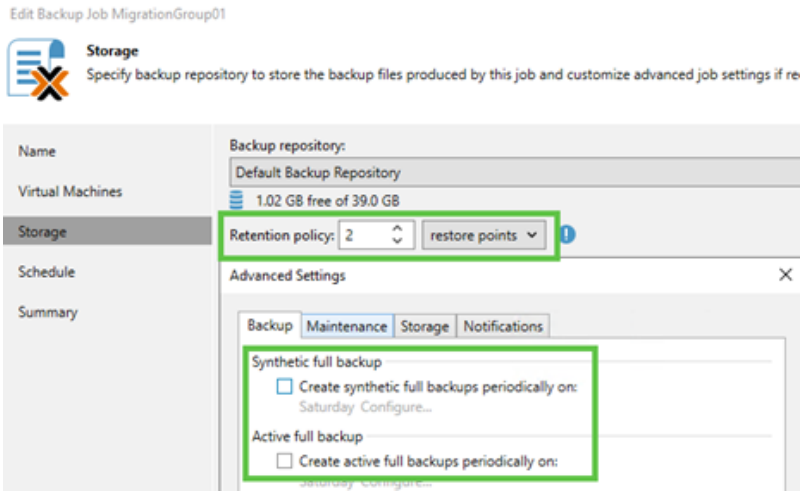
5. Appendix A: Migration Tools

5.1. Reduce final backup duration

To meet your maintenance window and reduce downtime consider performing backups so that the incremental time frame of the final incremental is as short as possible.

1. Ensure migration backups do not overlap or contend for production backup resources. (**IMPORTANT:** when a temporary VBR server and storage is being used ensure production backup job is disabled before final conversion backup is performed)

2. Create Backup Migration Groups using Incremental for ever Backup mode — (For the Retention policy use “restore points” to minimize the number of incremental restore points prior to maintenance window



3. Perform Full backup of VM Migration Group
4. Enable Migration Group Backup Jobs and Perform Incremental backups
(**IMPORTANT:** to minimize resource contention perform backup with enough time to meet the conversion maintenance/outage window)
5. Adjusting schedule Eg. Reduce to 12-hrs, 8-hrs, 4-hrs, etc.
(**NOTE:** this will depend on the environment and change rate so adjust accordingly)
6. Disable backups and Shutdown system(s)
7. Perform Final backup and verify the minimal number of restore points are met
8. Perform Veeam IR to VMware using preferred method (eg. UI or script)