Veeam Hypervisor Migration Guide

Ver 1.0

Douglas Cheung | Veeam Solutions Architect
Olivier Rossi | Veeam Sr. Solutions Architect

Contents

1. Introduction 3

2. Instant VM Recovery 3

2.1. What is IVMR? 3

2.2. Should you use IVMR for all migrations? 4

2.3. Hyper-V IVMR 4

3. Migrating from VMware to Hyper-V 5

3.1. Lab Setup 5

3.2. Considerations 5

3.3. Step by Step IVMR to Hyper-V 7

3.3.1 Windows VM 7

3.3.2 Linux VM 7

3.4. How to scale 7

3.4.1 Scripting 7

3.4.2 Considerations and Optimizations 8

3.4.3 Performance from the field and Sizing guidance 9

4. Summary 10

5. Appendix A: Migration Tools and Scripts 11

5.1. Reduce final backup duration 11

5.2. Migration to Hyper-V script 15

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, 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 Instant VM Recovery capabilities to migrate workloads, with on-the-fly conversion, to the selected target hypervisor. Make sure you understand the application and the component dependencies prior to performing the migration.

2. Instant VM Recovery

2.1. What is IVMR?

Instant VM Recovery is a feature supported for virtualization platforms, including VMware, Hyper-V, Nutanix AHV, Oracle Linux Virtualization Manager and Red Hat Virtualization. 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 on-the-fly.

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

2.2. Should you use IVMR for all migrations?

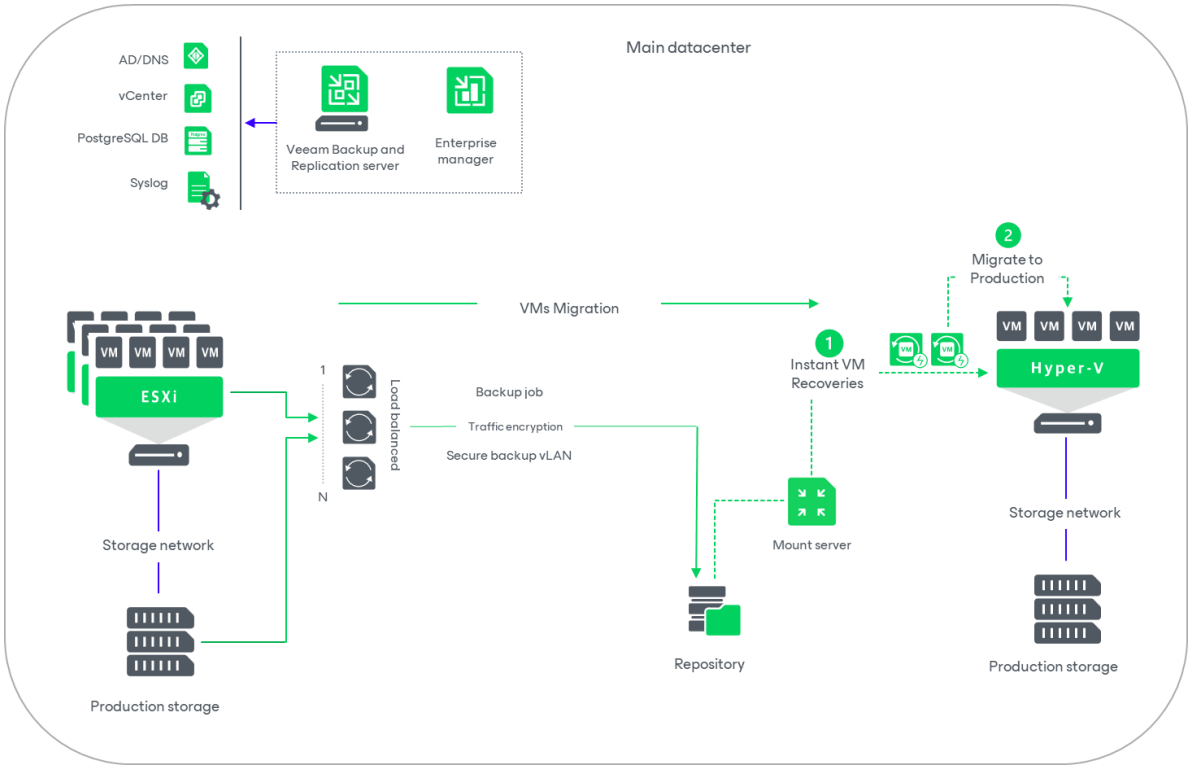
While Veeam's IVMR capabilities are quite extensive, IVMR may not always be the best method for migrating 24/7 sensitive application workloads.

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.

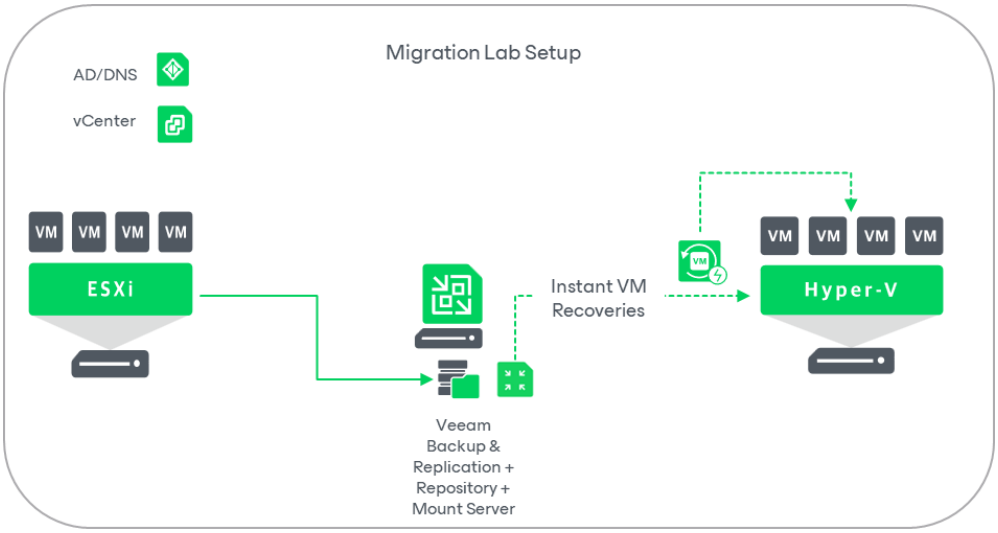
2.3. Hyper-V IVMR



During instant recovery, Veeam Backup & Replication runs workloads directly from compressed and deduplicated backup files. When an IVMR session starts, Veeam creates a temporary empty VM on the target Hyper-V host with a protective snapshot. The VM's disks are directly mounted from backup files via the mount server to the temporary VM and the VM is booted.
Writes are redirected to the instant recovery write cache area before engaging the final step, which is to migrate to production.

3. Migrating from VMware to Hyper-V

3.1. Lab 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 Hyper-V.

3.2. 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 VMware 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.

Destination Hypervisor RAM Considerations:

Hyper-V has a feature called dynamic memory, which allows the hypervisor to handle RAM consumption by VMs on the host in a flexible way. As part of this feature, a memory buffer setting can be configured. The memory buffer setting designates a percentage of memory that Hyper-V should allocate to the VM as a buffer. The default is 20%.

A Hyper-V host uses the current VM demand for memory to figure out how much memory for the buffer it should be reserving. For example, for a VM with a current RAM consumption at 1TB, Hyper-V is keeping a 20% buffer and allocating the VM 1.2TB of RAM. Not accounting for the buffer for each VM being migrated risks the chance of exceeding the RAM available on the host.

Understanding Hyper-V VM Generations:

Veeam Backup & Replication reads the workload configuration from the backup file in the backup repository and creates a temporary VM with empty disks on the target host. Before creating the temporary VM, Veeam Backup & Replication performs an analysis of the workload configuration and decides on the generation for this VM:

- If the workload is a Hyper-V VM, Veeam Backup & Replication creates the temporary VM of the same generation.
- If Veeam Backup & Replication detects an EFI system partition, it creates a generation 2 VM.
- If Veeam Backup & Replication detects BIOS boot partition, it creates a generation 1 VM.
- If Veeam Backup & Replication detects at least one GPT partition, it creates a generation 2 VM.
- In other cases, Veeam Backup & Replication creates a generation 1 VM.

SMB3 Shared Folder

If a SMB3 share is used for the cluster volume, the host or cluster on which you register VMs must have access to the specified SMB3 shared folder. If you are using SCVMM 2012 or later, the server hosting the Microsoft SMB3 shared folder must be registered in SCVMM as a storage device.

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 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 VMware, see: https://knowledge.broadcom.com/external/article/315639/uninstalling-vmware-tools-in-a-windows-v.html
- For AHV, see: https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_8:mul-ngt-bulk-uninstall-c.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)
- Power On VM(s) in original hypervisor
- Verify VM(s) and Applications
- Perform cleanup i.e. storage, jobs of failed VM(s)

3.3. Step by Step IVMR to Hyper-V

3.3.1 Windows VM

NOTE: When migrating VMs to a Hyper-V failover cluster, the VMs must be registered on the cluster to run. You must select the Hyper-V host in the cluster that owns the Cluster Shared Volume. DO NOT select the cluster resource itself. If a selected host does not own the chosen Cluster Shared Volume, the restore will fail.

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 Hyper-V. The following should be considered before starting an Instant Recovery to Hyper-V:

- Ensure that the "Disable changed block tracking for this host" is not selected for a host to which you plan to recover(migrate) a workload. If this option is selected for the host, the driver required for work of Instant Recovery will be disabled.

3.3.2 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 Linux-based 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.

3.4. How to scale

3.4.1 Scripting

The proper way to scale is to automate the process by scripting the Instant VM Recoveries to Hyper-V.
The list below only represents some of the main considerations when automating IVMR to Hyper-V:

- List of VMs and their associated backup job name to move to Hyper-V.
- The target Hyper-V hosts, paths and folders, Hyper-V target datastores (available space).
- The networks mappings rules, whether to preserve MAC addresses or not, Re-IP'ing (scripts for Linux).
- The VM's source OS as with Linux VMs, a Hyper-V helper appliance is required.
- Concurrency of restores to adequately size the Mount Server.

The core of the script uses 3 cmdlets:

- Getting the VM's restore points: `Get-VBRRestorePoint`
- Starting the IVMR: `Start-VBRHvInstantRecovery`
- Finalizing migration by moving to production: `Start-VBRHvInstantRecoveryMigration`

First, we need to obtain the latest available restore point to start the IVMR process from.

```
$VMrestorepoint = Get-VBRBackup -Name [Backup-Name] Backup | Get-VBRRestorePoint
-Name [VM-Name] | Sort-Object –Property CreationTime –Descending | Select-Object
-First 1
```

Second, we can start the IVMR:

```
Start-VBRHvInstantRecovery -RestorePoint $VMrestorepoint -Server [Hyper-V-
ServerName] -Path [TargetPath] -PowerUp $true -NICsEnabled $true -PreserveMACs
$true -NetworkMapping [NetworkMappingRules[]] [-HelperAppliance
<VBRHvInstantRecoveryHelperAppliance>] -DisableDiskAllocation
```

Last, we need to migrate to production:

```
Start-VBRHvInstantRecoveryMigration | Get-VBRInstantRecovery
```

Please refer to Appendix A: Migration Tools and Scripts for a more complete scripting example.

3.4.2 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:

- Depending on the backup methodology, understanding of the network architecture is required.
- If VMware virtual proxies are used, ensure backup traffic is not going out the management network.
- 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 Hyper-V host.
- Total VM-assigned RAM cannot exceed available disk space on the Hyper-V host’s C:\ drive.
- 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.

3.4.3 Performance from the field and Sizing guidance

The following sizing guidance is based on test data gathered in a lab as well as in the field. Note: your mileage may vary depending on a multitude of factors. Adjust the values for your environment accordingly.

- Backup Server: 8 CPU / 24 GB RAM
    - This configuration for the backup server allows for up to 40 VMs to be included per batch migration.
- Proxy Server: 8 CPU/ 16 GB RAM
    - Proxy per cluster depends on number of VMs to be migrated. The number of VMs processed by a proxy server is dependent on a multitude of factors including VM size, full or incremental backup, network, source and target storage performance, transport mode, and proxy resources.
- Mount Server (Hyper-V Host): 16 CPU / 32 GB RAM
    - A VM on the Hyper-V host should be designated as the mount server.
    - In this scenario, this size host was able to mount 42 VMs effectively.
- Gateway Server:
    - The gateway server is required if the VMs backed up reside on object storage or file storage on a storage array.
    - The resources required are dependent on a multitude of factors, however the CPU and RAM resources required should at a minimum match the proxy resources.
- Repository:
    - The repository for the migrating VMs should be as close to production storage as possible.
    - No deduplication devices, object storage in the cloud, or low-end storage/CIFS/SMB/NFS should be used as repository storage as these do not provide high performance for migration and will significantly increase migration time.
    - Design of the repository should ideally focus on providing the best read and write performance possible. This may influence RAID/volume design on the storage.
    - If using a scale-out repository, consider using a separate gateway server for each extent to maximize performance.
    - Consider using a portion of the primary storage (SAN) or other performant storage as swing space for better performance.
- Physical Servers:
    - For the best performance possible, consider leveraging physical servers for the Veeam Infrastructure.
- Network:
    - Leverage the fastest networking possible. At least a 10 Gbps network is recommended.

- Testing Environment

Storage	SSD Storage Array
Windows VM Size (Average)	50 GB
Linux VM Size (Average)	66 GB

- Results

Protect VMware Windows VMs (23)	Average Process 300 – 600 MB/s
Protect VMware Linux VMs (19)	Average Process 300 – 600 MB/s
Instant Recovery to Hyper-V Windows (1)	~ 3 Minutes
Instant Recovery to Hyper-V Windows (5)	~ 3 Minutes
Instant Recovery to Hyper-V Windows (10)	~ 3 Minutes
Instant Recovery to Hyper-V Linux (1)	~ 5 Minutes
Instant Recovery to Hyper-V Linux (5)	~ 5 Minutes
Instant Recovery to Hyper-V Linux (10)	~ 5 Minutes
Migrate Windows VMs to Hyper-V (1)	~ 7 Minutes
Migrate Linux VMs to Hyper-V (1)	~ 14 Minutes
Migrate Windows VMs to Hyper-V (23)	~ 56 Minutes
Migrate Linux VMs to Hyper-V (19)	~ 2 Hours 45 Minutes
Total Storage on Hyper-V Host (Windows)	1.23 TB
Total Storage on Hyper-V Host (Linux)	2.93 TB
Windows Restore Rate	366.1 MB/s
Linux Restore Rate	295.96 MB/s

4. Summary

In this comprehensive guide, we have provided step by step instructions to leverage Veeam's unique Instant VM Recovery capabilities to perform migrations to Hyper-V.

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.

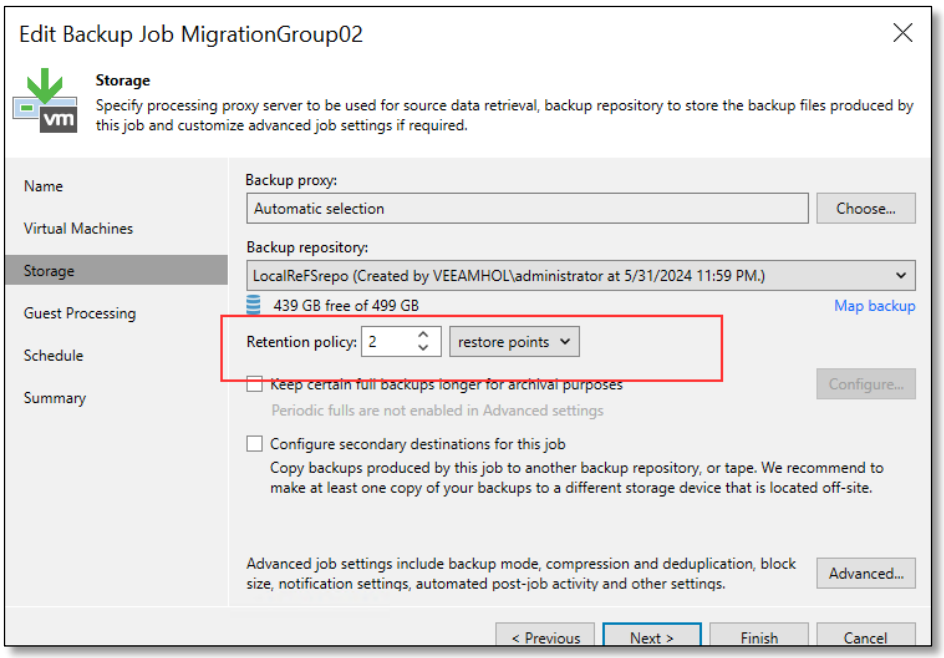
You should now be well equipped to go forth on your Hypervisor migration journey.

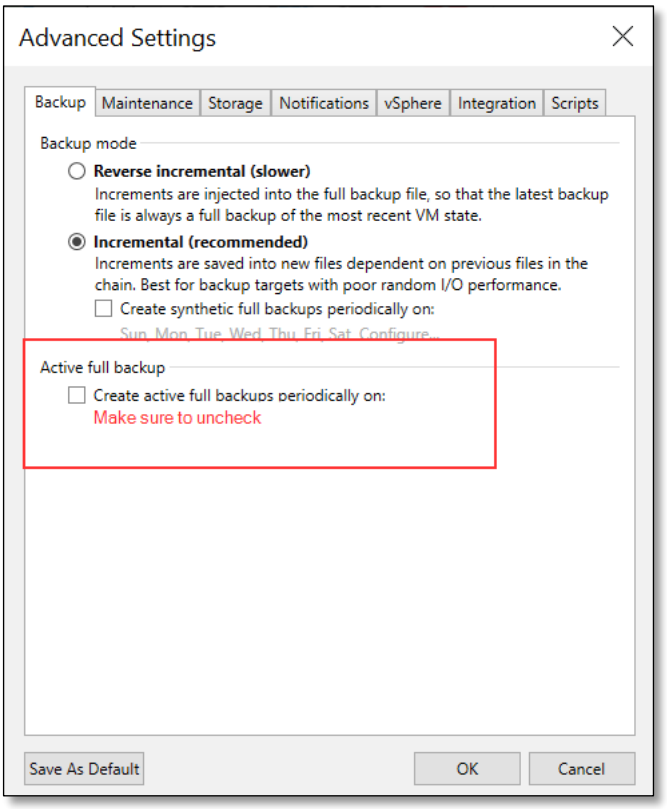
5. Appendix A: Migration Tools and Scripts

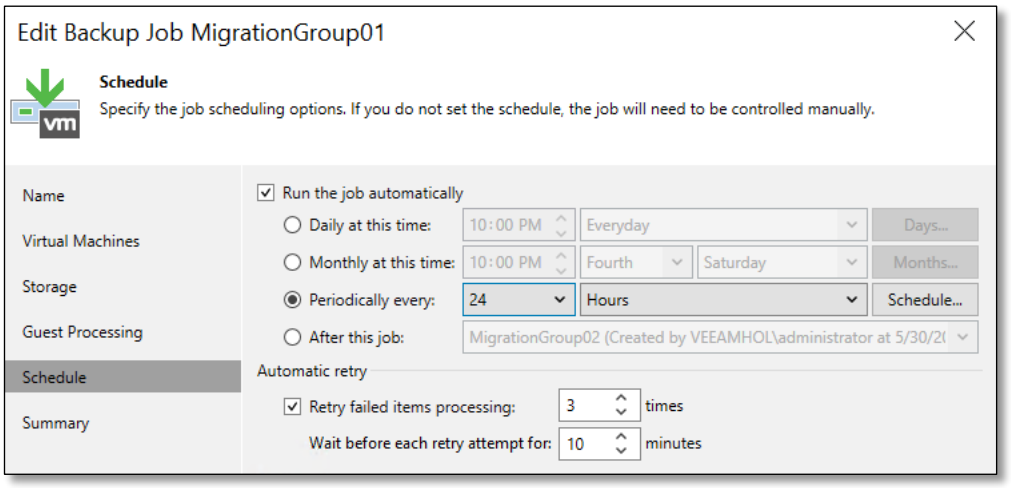
5.1. Reduce final backup duration

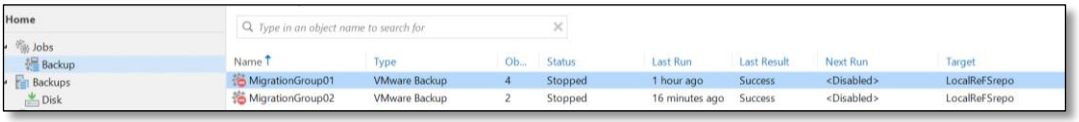
To meet your maintenance window and reduce downtime consider performing backups so that the incremental time frame of the final incremental is as short as possible.

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

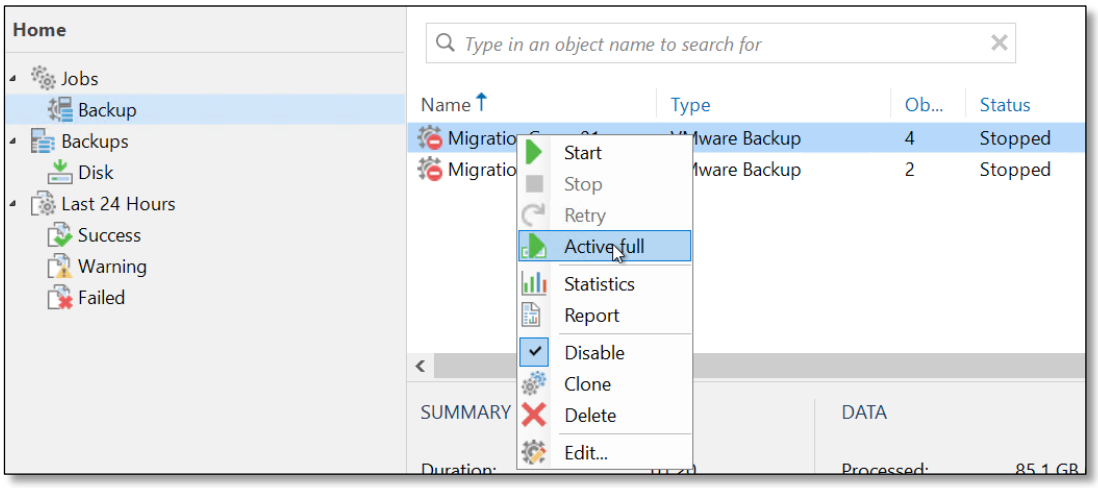




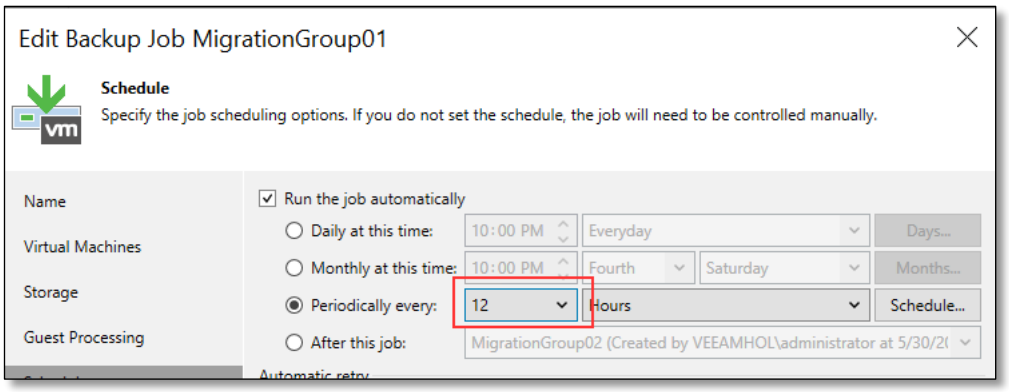


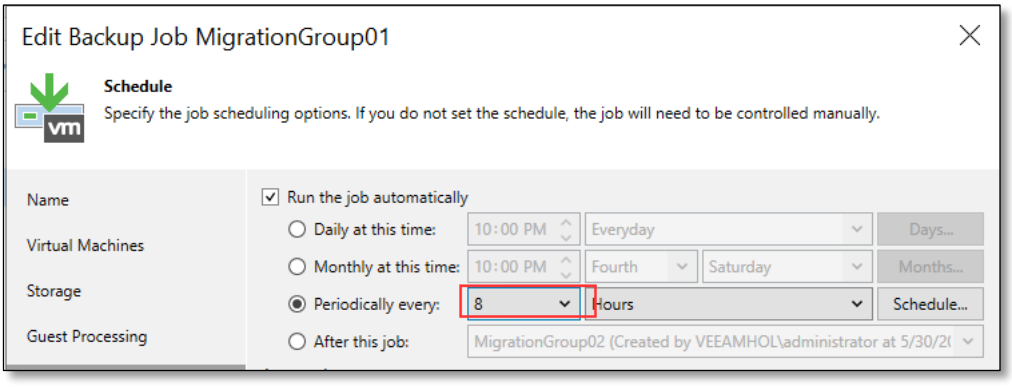


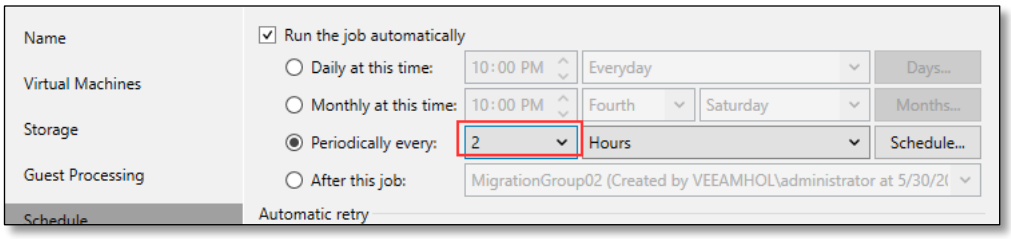
3. Perform Full backup of VM Migration Group



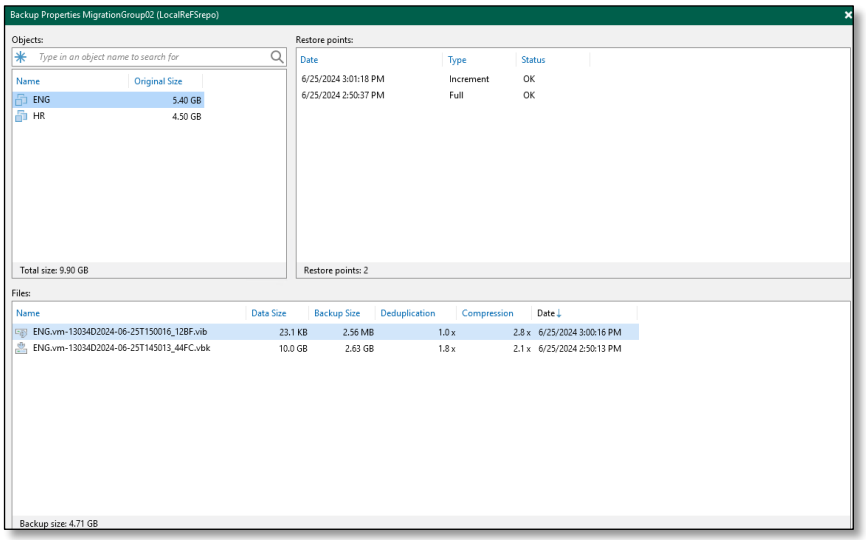
4. Enable Migration Group Backup Jobs and Perform Incremental backups (**IMPORTANT**: to minimize resource contention perform backup with enough time to meet the conversion maintenance/outage window)
5. Adjusting schedule Eg. Reduce to 12-hrs, 8-hrs, 4-hrs, etc. (**NOTE**: this will depend on the environment and change rate so adjust accordingly)



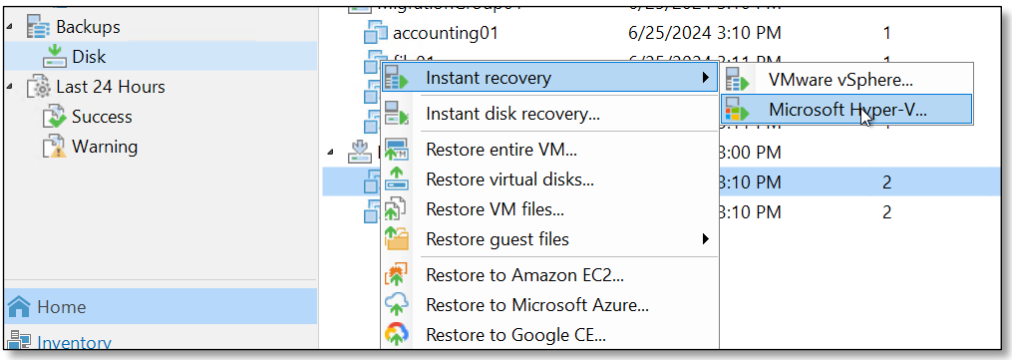




6. Disable backups and Shutdown system(s)
7. Perform Final backup and verify the minimal number of restore points are met



8. Perform Veeam IR to Hyper-V using preferred method (eg. UI or script)



Or

```
© Veeam Software Group GmbH. All rights reserved.

PS C:\Users\Administrator.VBR> cd C:\Scripts\
PS C:\Scripts> .\IVMR2HyperV624.ps1
WARNING: Source OS is not Unix-based. Parameter HelperAppliance will be skipped.


Id              : 487d964f-6156-4c66-9fec-cab78803bfe8
BackupName      : MigrationGroup01
RestorePoint    : 6/25/2024 12:48:54 PM
Platform        : EVmware
RestorePlatform : EHyperV
SourcePlatform  : EVmware
TargetPlatform  : EHyperV
MountState      : Mounting
JobType         : InstantRecovery
StateString     : Mounting...
PlatformString  : vi
EsxName         : HYPERV-01
HostName        : HYPERV-01
VMName          : sql

WARNING: Source OS is not Unix-based. Parameter HelperAppliance will be skipped.
Id              : 2ba354b1-8b66-4390-83c1-12d2fcc48530
BackupName      : MigrationGroup01
RestorePoint    : 6/25/2024 12:48:58 PM
Platform        : EVmware
RestorePlatform : EHyperV
SourcePlatform  : EVmware
TargetPlatform  : EHyperV
MountState      : Mounting
JobType         : InstantRecovery
StateString     : Mounting...
PlatformString  : vi
EsxName         : HYPERV-01
HostName        : HYPERV-01
VMName          : accounting01
```

5.2. Migration to Hyper-V script

The following PowerShell script can be used to automate VMware to Hyper-V Instant VM Recoveries and subsequent Migration to Production at scale.
It leverages backups carefully crafted for the purpose of migration to control the VM migration concurrency.

```
##############################################################################################
#
# VMware VMs Instant Recoveries to Hyper-V Migration
# Author: Olivier Rossi
# 06/20/2024
# version 1.0
# ---------------------------------------------------------------------------------------------
#
# Synopsis:
# ---------
# This script assumes that jobs have been organized with the purpose of migration to
# Hyper-V in mind.
# It assumes that source VMware VMs have been turned off.
# The script uses the job as the unit of migration to control the number of concurrent
# IVMRs.
# The script is run on the VBR server itself (or adjust Connect-VBRServer statement)
#
##############################################################################################

# connect to the VBR server
Connect-VBRServer

# Get VMware Backups for Jobs labeled MigrationXXX only
$MigrationBackups = Get-VBRBackup -Name 'Migration*' | Where-Object {$_.TypeToString -eq 'VMware Backup'};

# Define target Hyper-V hosts
$hvhost = 'HYPERV-01';
$hvnetwork = 'extvsw01';
$hvcsvpath = 'C:\ClusterStorage\Volume1';

# Migrate VMs 1 group (aka job) at a time
foreach ($mb in $MigrationBackups){

    # Get the VM list for the current backup
    $job = $mb.GetJob();
    $VMs = $job.GetObjectsInJob().Name;

    foreach ($vm in $VMs){
        # Get the latest restore point for all VMs to migrate
```

```
        $rp = $mb | Get-VBRRestorePoint -Name $vm | Sort-Object -Property CreationTime -Descending | Select-Object -First 1;

        # New helper appliance (only used for unix VMs)
        $server = Get-VBRServer -Name $hvhost;
        $network = Get-VBRHvServerNetworkInfo -Server $server;
        $helperappliance = New-VBRHvInstantRecoveryHelperAppliance -Network $network;

        # Create the network mapping rule
        $sourcenetwork = Get-VBRComputerNetworkInfo -RestorePoint $rp;
        $targetnetwork = Get-VBRHvServerNetworkInfo -Server $server | Where-Object { $_.NetworkName -eq $hvnetwork };
        $nmr = New-VBRHvInstantRecoveryNetworkMappingRule -SourceNetwork $sourcenetwork -TargetNetwork $targetnetwork;

        # Start the IVMR session (helper appliance is ignored for windows VMs)
        $csvpath = $hvcsvpath + '\' + $vm;
        Start-VBRHvInstantRecovery -RestorePoint $rp -Server $server -Path $csvpath -HelperAppliance $helperappliance -
NetworkMapping $nmr -NICsEnabled $true -PowerUp $true -PreserveVmID $true -PreserveMACs $true;
    }

    # Wait for all IVMR sessions to be mounted
    $mountstate = 'Mounting';
    $HvInstantRecovery = Get-VBRInstantRecovery;
    while ($mountstate -eq 'Mounting'){
        $mountstate = 'Mounted';
        foreach ($IR in $HvInstantRecovery){
            if ($IR.MountState -eq 'Mounting'){
                $HvInstantRecovery = Get-VBRInstantRecovery;
                $mountstate = 'Mounting';
                Start-Sleep -Seconds 5;
            }
        }
    }

    # Migrate to production
    Start-VBRHvInstantRecoveryMigration -InstantRecovery $HvInstantRecovery;
}

# disconnect from the VBR server
Disconnect-VBRServer
```