Windows and Physical Servers

Backup Best Practices

Matthias Mehrtens,

Sr. Solutions Architect,
Veeam Software

Contents

Most organizations today rely on virtualized IT infrastructures. Veeam® helps them to provide and increase availability of critical workloads running on their systems. Due to various factors, including complex hardware configurations and compliance regulations, some workloads cannot be virtualized, along with endpoints (workstations and notebook computers) that might not be protectable in their entirety by leveraging back-up solutions built for virtualized systems. Thus, everyday occurrences such as lapses in connectivity, hardware failures, file corruption, ransomware or even theft can leave an organization's data at risk.

Veeam Agents solve these issues by closing the gap that some enterprises face with large, heterogeneous environments and further enabling workload mobility by delivering availability for cloud-based workloads. Of course, Veeam Agents can also handle virtual machines and applications that do not support a hypervisor snapshot, or for any other reason cannot be protected on the virtualization layer.

This paper describes the main concepts behind Veeam Agent *for Microsoft Windows*, how agents can be managed centrally by integration into Veeam Backup & Replication, and more. It is an updated version of the paper that was released in 2021 to accommodate new features and changes that have become available with Veeam Agent *for Microsoft Windows* v6 (alongside Veeam Backup & Replication™ v12) in February 2023. We've also included some quotes from experienced community members to provide a peer perspective, which should give you confidence in developing the best backup strategy.

1. Where to look when choosing backup for physical workloads?

Nowadays, physical workload protection might be considered a no-brainer with so many vendors who have had established solutions for years. However, not every choice provides the same quality. There are many key aspects to quality data protection and it's hard to provide protection when some of those aspects are missing. Here at Veeam, we believe that organizations must have multiple options, not only when it comes to backup modes, but also for recovery options. The ability to create backups to any suitable medium and restore them with best possible granularity when needed is crucial for businesses of any size.

Here we will dive deeper into Veeam's backup and recovery technologies we believe are crucial for timely and reliable physical server backups.

> *"What I love most about Veeam Agent features is how the scenarios we can create when combining them really change the game with endpoint data protection. We can create a single backup job that can be run not just on schedule but triggered by supported business applications and scripts. If internet connectivity is missing, we can store these backups locally, ready and waiting to send back the moment we get internet connectivity. With Veeam Cloud Connect integrated we don't need to worry about USBs being lost either, we take the data straight from the user to a trusted data center, meeting the 3-2-1-1 capabilities offered by Veeam Agent. Then when the time comes that backup recovery is necessary, this can be sent straight to the user, wherever they are, securely, without IT needing physical access to the device. Whether it's a single file that's been accidentally deleted or imaging a new device with all the previous applications and configurations, Veeam Agent delivers."*
>
> **— Michael Paul,**
> Technical Consultant,
> Veeam Legend, VMCA, VCP

1.1. Benefits of an application-aware image-based backups

Veeam Agents are leveraging, in principle, the same technology used by Veeam for backing up virtual workloads: image-based backups that create backup copies of each disk attached to a protected computer. This benefit enables very fast and simple backups, as well as fast restores to bare-metal systems such as, restoring to replaced hardware due to some sort of malfunction of the original computer.

Another benefit of an image-based approach is portability of backup files because they can be restored almost anywhere. This proven Veeam technology provides unique mobility of backups, which allows for moving workloads from physical to virtual or to cloud and back, simply by leveraging one of the many restore options provided. The backup files created by Veeam Agent *for Microsoft Windows* are self-contained. Even without an existing backup infrastructure, restores are still feasible.

For application awareness, Veeam Agent *for Microsoft Windows* adds the same proven guest processing engine found in Veeam Backup & Replication, which helps bring the power and flexibility you need to ensure Availability for your physical Windows workstations and servers. It also:

- Ensures that enterprise applications are discovered during backup
- Provides simple log backup for enterprise databases (MS-SQL and Oracle)
- Allows granular restores of files and applications.

NOTE: *Application-aware processing is available in the server edition only.*

> *"Veeam Agents are a great way to have a unified backup strategy, where all your workloads are backed up with Veeam regardless of being virtual or physical. It is possible to do application aware backup of an SQL server for example to create consistent backups. If the server does indeed run database or heavy workloads, it is best to install Veeam's CBT Driver (Changed Block Tracking Driver) which works more efficiently and boosts backup performance. For added security you should enable backup encryption."*
>
> **— Nico Stein**,
> AVP of IT, Veeam Vanguard,
> vExpert, Cisco Champion

1.2. Incremental backup forever with change block tracking

To avoid transferring all the data on all disks every time a backup is performed (such as daily), which would essentially be required if taking bare images of the computer's disks without any added intelligence, Veeam Agent *for Microsoft Windows* leverages change block tracking on each of the computer's disks. This ensures that, after an initial full backup, only blocks that have changed since the last backup run will be read and transferred to the new incremental backup file (see **Figure 1-1**).

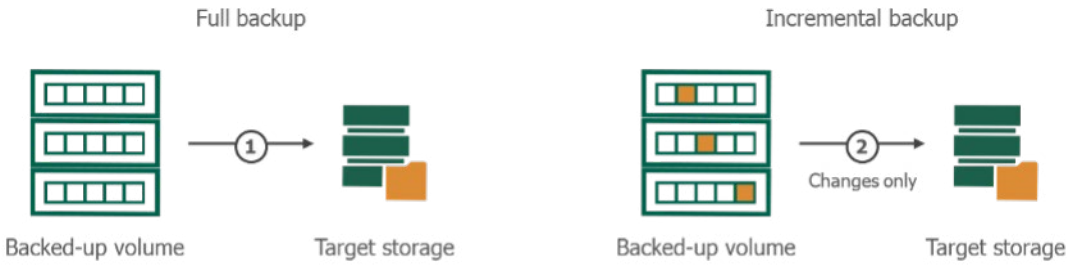

Figure 1-1: Change block tracking

This technology allows for the creation of powerful incremental backup chains where only one initial full backup is required. Additionally, required full backups (e.g., once per week) can be created as "synthetic full backups" which re-use already existing backup data blocks, eliminating the need to again transfer the full amount of data (which would be referred as "active full" and can of course be scheduled as well if desired).

Another option would be a "forever forward incremental" chain which also starts with an active full backup. Then, all subsequent backup runs are incremental, and process changes only. As soon as the first full backup expires due to the chosen retention, the oldest incremental backup file will automatically be merged into the existing full backup file, overwriting the expired blocks (if any) within.

1.3. Simple yet powerful recovery options

Any backup solution would be useless if there was no way of restoring from backups. Veeam Agent *for Microsoft Windows* provides a comprehensive set of recovery options, including:

- Bare metal restore
  Restores the whole system to existing/replaced/new hardware or "empty" virtual machines
- Volume level restore
  Restores single or multiple volumes to an existing (same or different) computer or virtual machine
- Export as virtual disk
  Exports single disks as virtual disks that can be attached to virtual machines (Microsoft Hyper-V or VMware vSphere)

- Instant VM recovery to Microsoft Hyper-V[1]
  Run a Hyper-V virtual machine directly from the backup files created by the agent
- Instant VM recovery to VMware vSphere[1]
  Run a vSphere virtual machine directly from the backup files created by the agent
- Restore to Microsoft Azure[1], Amazon EC2[1] and Google CE[1]
  Restores the computer as a virtual machine to the IaaS environment of the chosen cloud provider
- Application item recovery[1]
  Restore single-application items (Microsoft SQL, Oracle, Microsoft Exchange, Active Directory, SharePoint)
- File level recovery
  Restores single files or folders back to the original computer or another location

And all these options are just a few clicks away as shown in **Figure 1-2**:

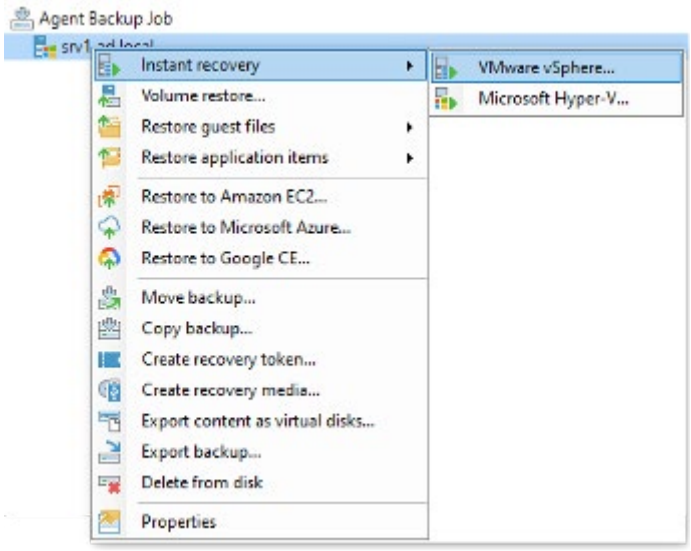

Figure 1-2: Restore options in context menu of **Agent Backup** in Veeam Backup & Replication Console

1 Only available in conjunction with Veeam Backup & Replication

1.4. Automatic Physical-To-Virtual Conversion (P2V)

Have you noticed the "Instant Recovery" option above? Yes, it's true: You can restore a backup of a physical computer taken with Veeam Agent *for Microsoft Windows* as a virtual machine on either Microsoft Hyper-V or VMware vSphere. All the required P2V conversion work (e.g. converting the boot disk image into a bootable virtual disk, exchanging device drivers for storage and network within the Windows OS, etc.) will be done automatically. These are not only great restoring options but may also be very helpful when migrating physical computers to virtual machines!

"What I like most about the Veeam Agent are the restore options which you get in combination with Veeam Backup & Replication. Of course, you're able to do standard restores, like file-level, application-level or bare-metal, but with Veeam Backup & Replication you also get more advanced restore capabilities:

1. *Instant VM Recovery to VMware vSphere or Microsoft Hyper-V*
2. *Restore to Amazon EC2 or Microsoft Azure*

Being able to start your backup on a virtualization host or in the cloud extends your possibilities for many scenarios.

If your physical server or workstation has an hardware error and you can't wait for replacement, then why not use your existing virtualization resources or upload it as a EC2 or Azure machine to the cloud?

And this is not only useful during outages; using Veeam as a migration utility from physical to virtual or the cloud keeps both the downtime and the admin stress-level low.

Last but not least, if you need to do any critical maintenance or update tasks, you can first evaluate them virtually in your lab environment, before doing them on your production hardware."

— Maximilian Maier,
Sr. IT Consultant,
Veeam Legend, VMCE, VCP

1.5. Multiple backup modes

Figure 1-3 shows the backup mode selection dialog of Veeam Agent *for Microsoft Windows*.

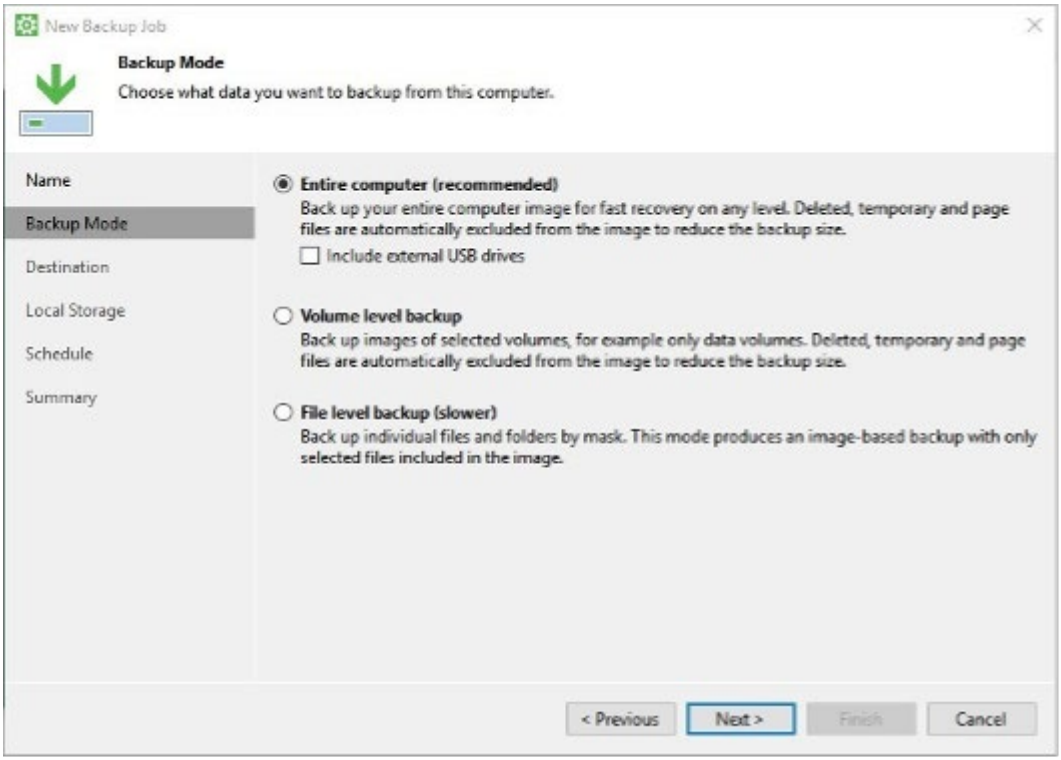

Figure 1-3: Backup modes of **Agent Backup** job

1.5.1. Entire computer

This is the recommended mode to create an image-based backup of all disks while deleted, temporary and page files are automatically excluded from the image to reduce the backup size. It also includes an option to back up external USB drives connected to the computer (compatible only with drives that support Microsoft VSS).

1.5.2. Volume-level backup

The image-level approach still applies when selecting volume-level backup and explicitly selecting the volumes to back up. An example would be if you want to back up only specific data volumes, but not the boot volume on which Windows resides (or vice versa). However, keep in mind that when the boot volume is excluded from backup, a bare metal restore of the computer from such backup will not be available. On the opposite, whenever the boot volume is included, the "System Reserved" or the EFI volume alongside with a recovery partition (if there is such) will be included in the backup automatically to enable bare-metal recovery.

1.5.3. File-level backup and Changed Block Tracking

For situations where it is not required or not possible to follow the image-level backup approach at all, Veeam Agent *for Microsoft Windows* can be configured to create file-level backups instead. In prior versions of the Agent, this approach used to reduce backup performance as the file system's file table needed to be checked for changed files to create incremental backups. However, Veeam Agent *for Microsoft Windows* v6 introduces enhancements to the optional Changed Block Tracking (CBT) driver, which is installable via the Agent's settings dialog as shown in **Figure 1-4**. It's now also available in the Workstation edition and supports tracking changed blocks of files when using file-level backups. More details and considerations can be found on this page of the Veeam help center.

NOTE: *When using centrally managed Agents, there is of course an option to control whether CBT driver should be installed — we will cover this topic in section 5 below.*

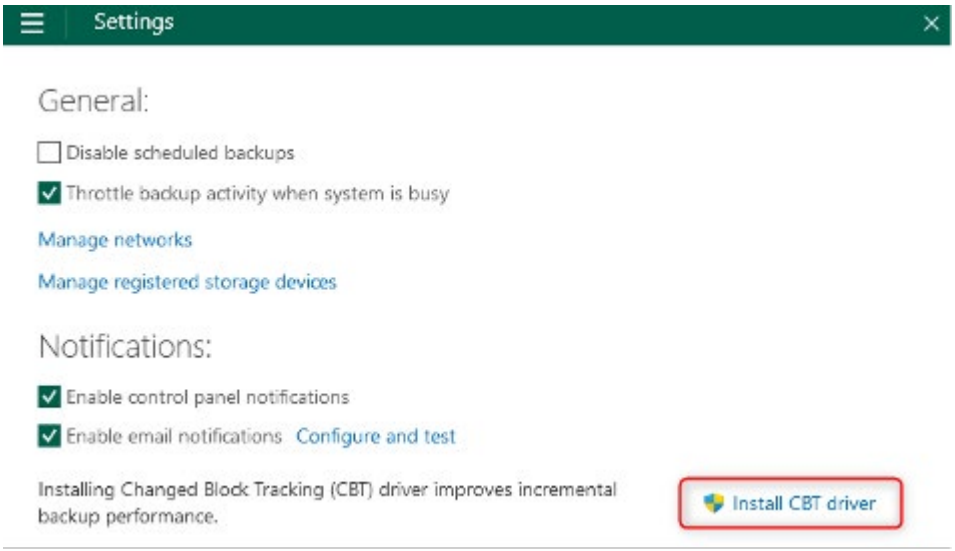

Figure 1-4: Optional CBT driver installation in settings dialog

File-level backup adds the ability to include/exclude specific files or folders by specifying file masks (like, for example, ***.log**) or system environment variables. This Veeam knowledge base article explains the variety of combinations when using wildcards and/or environment variables: https://www.veeam.com/kb3236

NOTE: *If you just want to exclude specific folders on NTFS volumes from backup, you can still use the volume-level backup, as it also supports the exclusion of folders including those based on wildcards (only after last backslash of path) or system environment variables (e.g., %WINDIR%, which typically points to the **C:\Windows** folder).*

For managed agents (see section 3), there is an additional option to exclude users' local OneDrive folders from backup. As these folders are typically synced to OneDrive cloud storage you possibly want them to be excluded from backup. You'll find the option when clicking on the "Advanced" button as shown in **Figure 1-5**.

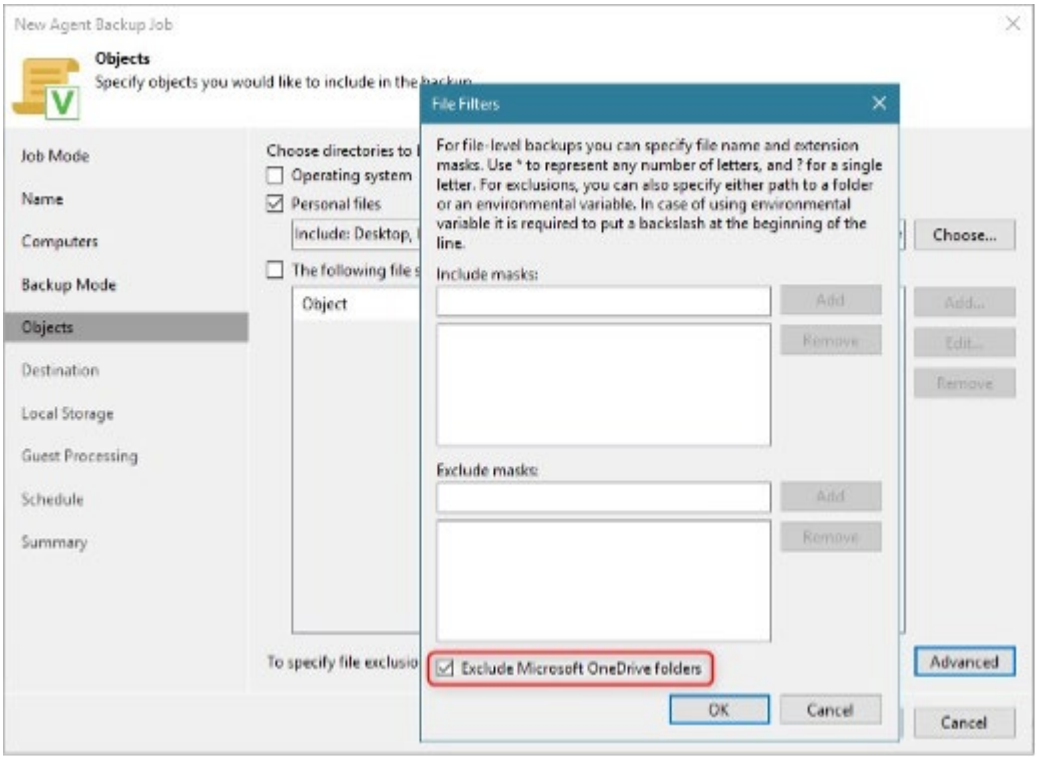

Figure 1-5: Exclude OneDrive folders

1.5.4. Parallel disk processing

Veeam Agent *for Microsoft Windows* is using parallel disk processing which helps drastically reduce backup processing time of computers with multiple disks, as all disks will be backed up simultaneously instead of one after another.

Parallel disk processing is available and enabled by default in "entire computer" and "volume-level" backup modes and will be effective only when using a Veeam backup repository or a Veeam Cloud Connect repository as the backup target. It is possible to tune the level of parallelism or completely disable the feature if needed (see https://www.veeam.com/kb3157 for details).

1.6. Optional application awareness

There might sometimes be reasons to disable application awareness within the Veeam Agent *for Microsoft Windows* configuration. This results in applications on the computer not being brought to a consistent state (quiesced) before the actual backup starts and will create a crash consistent backup only. Please be aware that, although this approach still creates recoverable backups, some restore options will not be available. Some applications (especially databases) might suffer from corrupt or inconsistent application data after being restored from such a backup and some might not even start at all for the same reason.

1.7. Focus on simple recovery

As a result, it is advised to always think twice before bypassing any of the basic concepts by not using the entire computer backup mode. In most cases, such a configuration will reduce the number and/or simplicity of restore options you probably need in case there has been an outage or failure that requires recovering from backup. As time is always short in such emergency situations, the more restore options that are available and the simpler they are, the easier and faster the whole recovery process will be.

Now that we have reviewed the basic concepts of physical workload protection with Veeam, let's dive deeper into Veeam Agent *for Microsoft Windows*: licensing options, centralized agent management and deployment and several best practices for your environment.

2. License editions

Veeam Agents are available in three different license editions, named.

Free: Provides a simple solution for backing up Windows-based desktops and laptops. Ideal for, but not limited to, personal use.

Workstation: Entitles you for 24.7.365 technical support and adds features for mobile user protection and support for remote management; adds the ability to create synthetic full backups and use Veeam Cloud Connect repositories as backup targets. Starting with V6, Veeam's Changed Block Tracking (CBT) driver is available for Workstation edition running on any supported Windows edition.

Server: All features of Workstation edition, plus full server support via application-aware processing and server-focused job-scheduler; unlimited amount of backup jobs to any supported target and Veeam Volume Change Tracking (CBT driver) for Windows Server operating systems.

Table 2-1 provides a quick feature comparison of these editions:

	Free	Workstation	Server
Instant recovery to Hyper-V or vSphere VM	✓[2]	✓	✓
Restore to Azure or Amazon EC2	✓[2]	✓	✓
Source-side encryption	✓[3]	✓[3]	✓[3]
Synthetic full backups		✓	✓
Remote configuration and management		✓	✓
CBT driver		✓	✓
24.7.365 technical support		✓	✓
Object storage support		✓	✓
Application-aware processing			✓
File indexing and catalog search			✓
Transaction log processing			✓

Table 2-1: Editions overview

Depending on deployment and management requirements, there are different sets of software components being installed on a workstation or server to be protected by Veeam Agent *for Microsoft Windows*. For this reason, there are three different modes of operation for how Veeam Agent *for Microsoft Windows* can be deployed and managed to provide flexibility for many different use cases.

2 To perform instant recovery to Hyper-V or vSphere and Restore to Azure or Amazon, specific license of Veeam Backup & Replication may be required.

3 If a Veeam backup repository is used as a backup target in **standalone** mode, source side encryption is not available. However, encryption of backup data can be enabled on the Veeam repository instead

3. Management modes

Veeam Backup & Replication allows you to centrally manage every aspect of Veeam Agent *for Microsoft Windows* installations. This means that local configuration management components (backup job management, user interface, restore options, etc.) will not be available locally on the protected machine because these tasks will be controlled centrally by the Veeam Backup & Replication backup server. This is referred to as the ***managed by backup server*** mode.

On the other hand, if the Veeam Agent *for Microsoft Windows* installation package is installed manually on a physical or virtual computer not being managed by Veeam Backup & Replication, more components need to be available and configurable on the local computer. This is referred to as the ***standalone*** mode.

A third option, called ***managed by agent*** *mode*, resembles a special mix of the two modes above and is the only available mode for the workstation edition combined with central management.

Technically, you are free to choose one of the modes described above individually for each protected computer. But there are certain scenarios where a specific mode should be the preferred choice. Here is a summary and a list of use cases for each mode:

3.1. Standalone

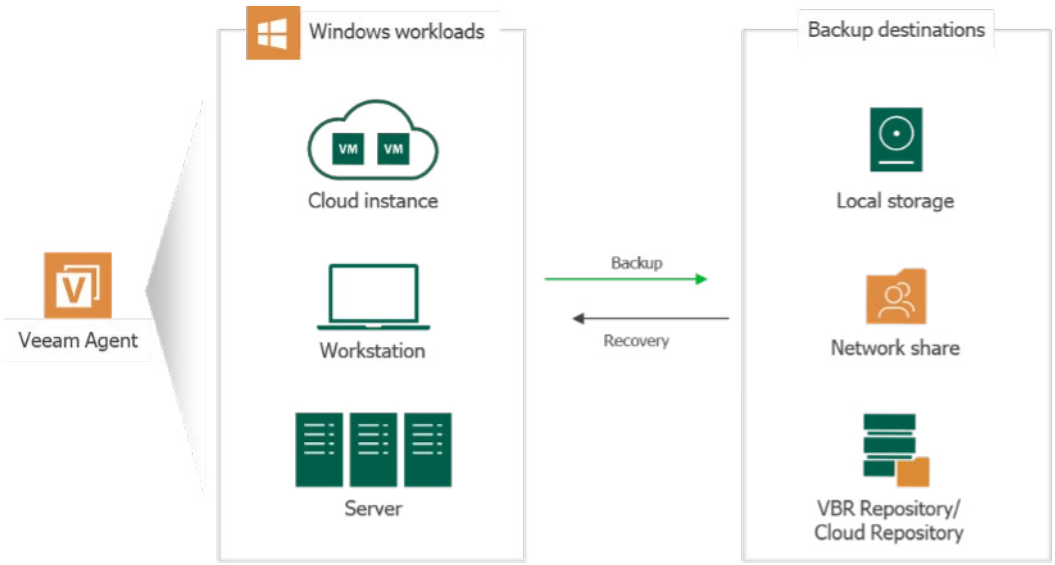

Figure 3-1: Standalone mode without central management

This mode is obviously targeted at protecting standalone computers, both physical and virtual, which are not part of a centrally managed backup infrastructure. Any user with local administrative permissions will be able to configure backups and restores as required. Use case examples:

- Personal physical or virtual workstation or server computers at home
- Physical or virtual corporate servers/workstations, which are managed individually
- Virtual computers in public clouds, which are managed individually

Standalone mode is available for all editions of Veeam Agent *for Microsoft Windows*. Although there is obviously no central management available for this mode, locally configured backup jobs on an agent computer in **standalone** mode can write their backup data into backup repositories managed by Veeam Backup & Replication.

3.2. Managed by backup server

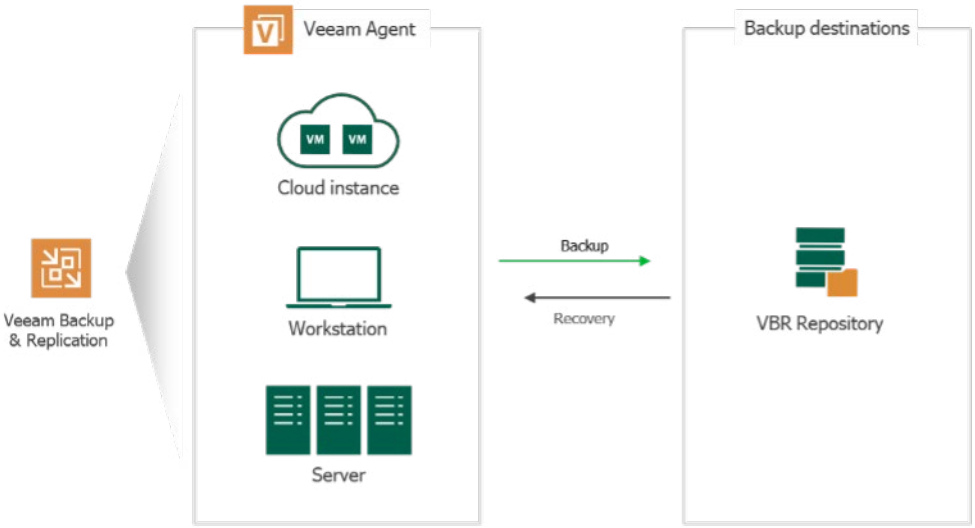

Figure 3-2: Managed by ***backup server*** mode

This mode requires a Veeam Backup & Replication infrastructure to be in place for agent deployment, configuration, and management. Local users of computers protected by Veeam Agent *for Microsoft Windows* in this mode have no option to perform or configure backups or restores (there is no UI available locally). Everything will be under the control of the Veeam Backup & Replication backup server that the computer is managed by.

Figure 3-2 shows that only backup repositories of the Veeam Backup & Replication infrastructure can be used as targets. This looks like a limitation compared to standalone mode, but instead it enables a lot more target options, because Veeam Backup & Replication supports a huge variety of backup targets (many more than the agent in standalone mode is capable of).

Use case examples:

- Physical or virtual corporate servers/clusters, centrally managed
- Public cloud virtual machines or clusters with central management
- Virtual machines that cannot be protected via virtualization-focused backup solutions due to unsupported Hypervisor technology (i.e., Veeam Agent *for Microsoft Windows* picks up where Veeam Backup & Replication VM backups might not be suitable).

Managed by ***backup server*** mode is available for the Server edition only and is the only mode that supports protection of Microsoft Failover Clusters (see https://www.veeam.com/kb2463 for details).

3.3. Managed by agent

Being a mix of the two previous modes, this mode is built for protection of computers that require central backup/restore capabilities and management, but equally require a local user to be able to have some control. It's also suitable for computers that do not have a permanent network connection to the central backup infrastructure.

Although all agent configuration options are required to be defined centrally on a Veeam Backup & Replication backup server, it is the local computer that executes the scheduled backups (even if the backup server is not available at the time), using its own configuration database and scheduling engine after having pulled its configuration from the backup server. A local user has a limited UI, which enables the creation of on-demand backups (in addition to regular backups created based on a centrally defined schedule), as well as performing file- or volume-level restores. Use case examples include:

- Corporate physical or virtual application or database servers (on-premises or in the public cloud) managed by dedicated application/database administrators who need the ability to perform on-demand backups/restores without help from infrastructure/backup operations staff
- Corporate workstations
- Mobile endpoint computers without continuous connection to the corporate network

Managed by agent mode is available for server and workstation editions and can be leveraged by the "Protection Group with flexible scope" which is covered in section 5.2 of this paper.

4. Agent installation types

As the ***standalone*** mode obviously handles all management and configuration tasks locally on the protected computer, it requires the complete installation of all Veeam Agent *for Microsoft Windows* components. This includes a local database to store configuration and job information by leveraging an embedded SQLite engine and is referred to as the ***full agent*** installation type. In versions prior to Veeam Agent *for Microsoft Windows* v6, Microsoft's SQL LocalDB was included for this purpose.

If, in contrast to the above, configuration and management are conducted centrally as described in the ***managed by backup server*** mode, only a smaller set of components is required, referred to as the ***lightweight agent*** installation type.

Eventually for ***managed by agent*** mode, all components of the ***full agent*** installation type plus a small setup/maintenance service (Veeam Installer Service) will be installed. However, all local UI components will be disabled in this mode (i.e., configuration options can be reviewed but not changed on the local computer), and Veeam Agent *for Microsoft Windows* will regularly pull its configuration from a central Veeam Backup & Replication backup server. Additionally, the ability to manually start an on-demand (out of schedule) backup as well as several restore options are available via the local agent GUI/CLI and do not require access to the central Veeam Backup & Replication console.

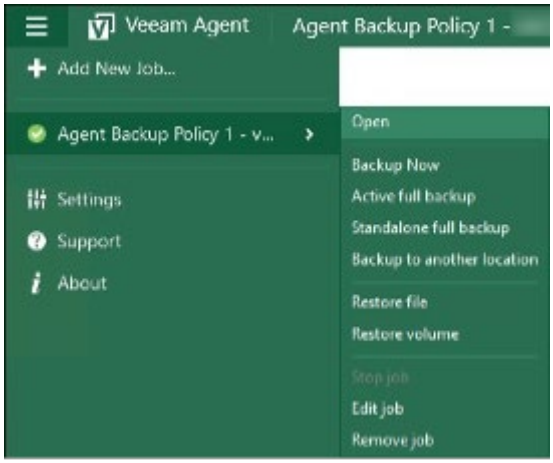

Figure 4-1: Locally available backup and restore options in managed by agent mode

Regarding installed components, the only difference between ***managed by agent*** and ***standalone*** mode is the Veeam Installer Service not being installed in the latter. The installation of Veeam Agent *for Microsoft Windows* is, therefore, still referred to as being of the ***full agent*** type.

Table 4-1 provides a quick overview of the two agents' installation types and included components related to the three management modes.

	Full agent	Lightweight agent
Standalone	Veeam Agent *for Microsoft Windows* • Full local UI and scheduling engine • Local database (embedded SQLite engine) CBT driver (optional)	✖
Managed by backup server	✖	Veeam Installer Service Veeam Agent *for Microsoft Windows* • No local UI • No local database CBT driver (optional)

Managed by agent	Veeam Installer Service
	Veeam Agent *for Microsoft Windows*
	• Local scheduling engine, limited GUI
	  • Configuration options read-only in local GUI
	  • Configuration and schedules pulled from central backup server
	• Local database (embedded SQLite engine)
	CBT driver (optional)
		✖

Table 4-1: Installed components based on management mode

5. Central agent management and deployment

Veeam Backup & Replication offers complete control over protection of computers using Veeam Agent *for Microsoft Windows*, covering deployment of the agent software, as well as management of agent configurations, schedules, backup targets and, of course, recoveries.

5.1. Protection Groups

Two of the main goals of any central management effort in IT is to standardize configurations across many computers and to deploy, manage, control, and enforce these standards in a simple way. In Veeam Backup & Replication, **Protection Groups** are the starting point to execute standardization tasks for all computers using Veeam Agent *for Microsoft Windows* or Veeam Agent *for Linux*, both physical and virtual.

A **Protection Group (PG)** configures a scope of computers (= members of the PG) and defines if a Veeam Agent should be installed on these members. The scope of a PG can be based on different sources as shown in **Figure 5-1**.

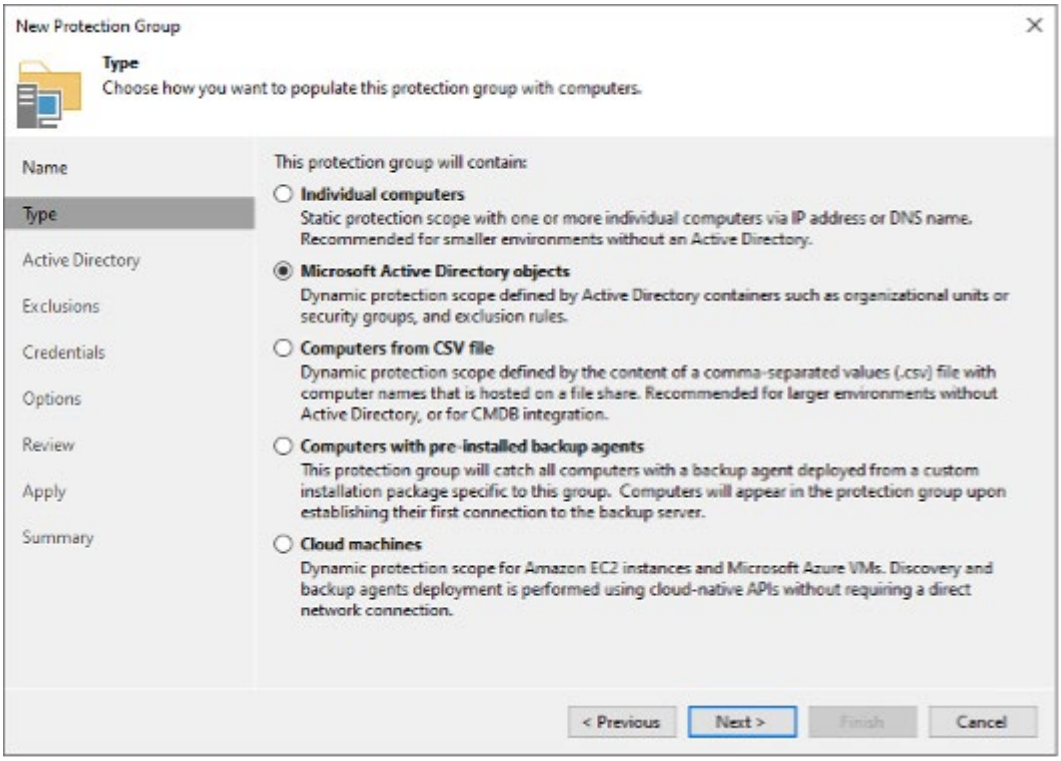

Figure 5-1: **Protection Group** types

When using Active Directory objects as a PG source, it is possible to select container objects such as organizational units or security groups instead of (or in addition to) individual computer objects. This is a very powerful option as it follows the dynamics of the chosen container object:

- Whenever a computer is added to the selected container within Active Directory, the PG will respect the change and the new members of the container will be processed automatically.

The same applies when removing computer objects from Active Directory containers:

- Processing of these computers by the PG will cease automatically based on the PG's schedule.

To add even more flexibility, exclusions can be defined within the PG to skip certain computers and/or containers from PG processing. Exclusions can also be defined for virtual machines in general (if the PG's intended scope is physical computers only), or for computers that have been offline for more than 30 days.

To enable installation of Veeam Agent *for Microsoft Windows* on the resulting set of members of a **PG**, credentials with local admin privileges on these members will be required. These credentials can be configured to be the same (**master account**) for all PG members, as well as individually per container, group, or individual computers.

A schedule can be configured in the PG's configuration dialog to define when the computers in the scope of the PG should be scanned for changes. It also allows to select a **Distribution server** as part of the Veeam Backup & Replication infrastructure, which will be responsible for pushing the agent binaries to the PG's member computers in case the central backup server cannot or should not be uploading these binaries to the computers directly. The automatic installation and updating of the Veeam Agent *for Microsoft Windows* software components can also be disabled if needed **(Figure 5-2)**.

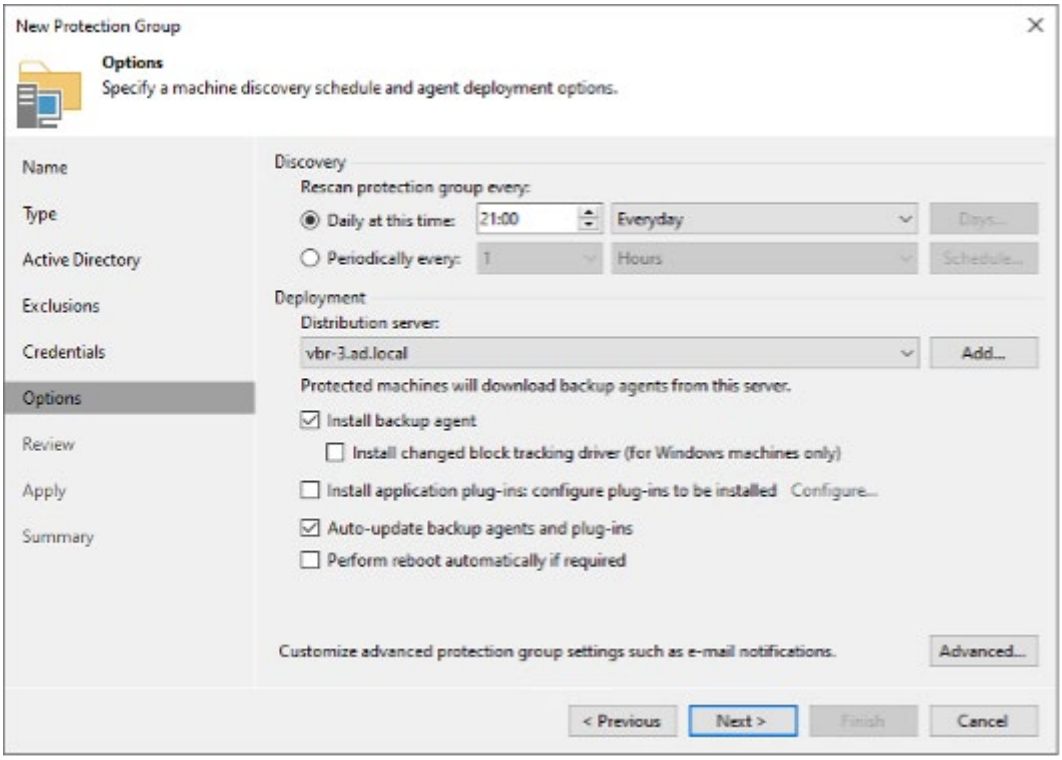

Figure 5-2: **Protection Group** discovery and deployment options

For environments where the deployment of Agents should not be handled by the Veeam backup server at all, Veeam Backup & Replication provides PG for "Computers with pre-installed backup agents" (see **Figure 5-1**), also called ***"Protection Group with a Flexible Scope"***.

5.2. Protection Group with a flexible scope

The main use cases for this type of PG are the following:

- You already have a working solution for software distribution and want to also use it to install the Veeam Agent software, instead of establishing "yet another software distribution" just for the sake of backup agent installation.
- Security and compliance rules prevent you from storing the passwords of local administrator accounts (which are required to install software on any computer) in the credential manager of Veeam Backup & Replication.

- You don't have the full list of computers that you want to protect at the time you are creating the PG, and this list can neither be provided by Active Directory nor via CSV file (e.g. by third party CMDB).
- You want to create a PG for computers running Apple MacOS, IBM AIX or Oracle Solaris; Veeam Agents for these operating systems cannot be deployed by the other PG types and therefore have to be pre-installed.

PGs of this type will create an installation package of the Veeam Agent you choose (see **Figure 5-3**), and it will also create a configuration file containing all information the agent needs to find and authenticate against the backup server. Once this package is installed and configured with this configuration file, the agent will synchronize with the backup server and pull the configuration of the backup policy that targets this protection group on a regular basis. The installation will always be of type ***full agent*** as described in section 4, and these protection groups can only be used in backup jobs of type ***managed by agent*** (see section 3.3).

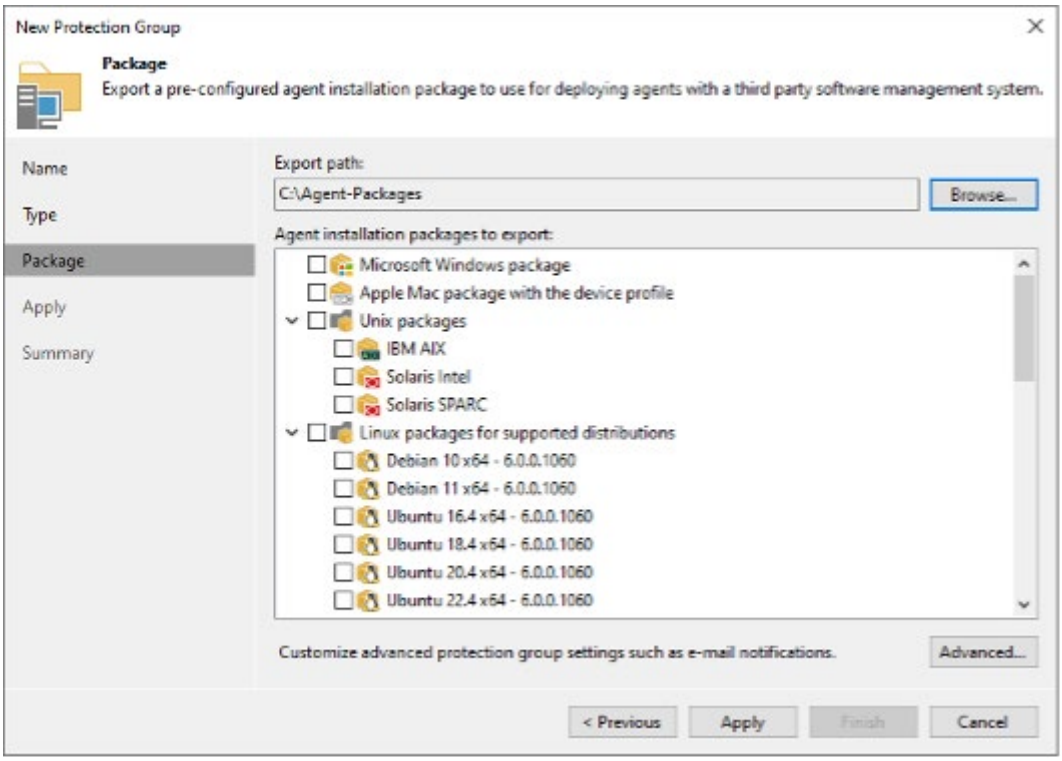

Figure 5-3: Agent installation packages available in Protection Group of flexible scope

5.3. Protection Group for cloud machines

Veeam Backup & Replication v12 introduced a new type of Protection Groups for "cloud machines", and the description in the dialog shown in **Figure 5-1** says it all. It defines a protection scope for either Amazon EC2 instances or Microsoft Azure virtual machines that enables discovery and backup agents deployment via cloud-native APIs without requiring a direct network connection between the Veeam backup server and the agent computers.

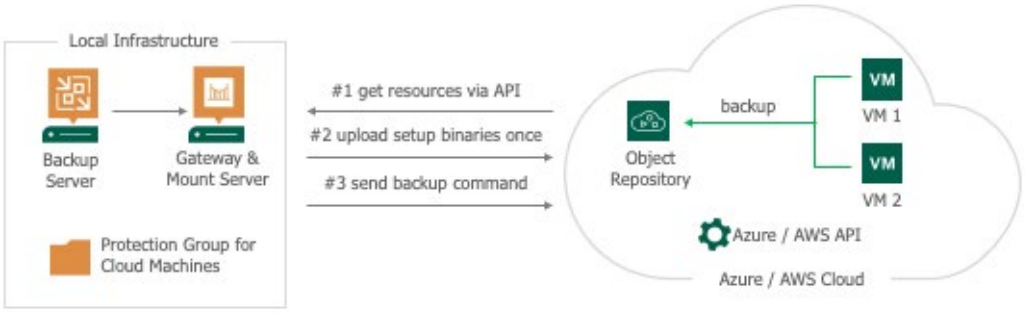

Figure 5-4: Protection Group for cloud machines — setup/management/backup

How does it work? The Veeam backup server communicates directly (or via optional gateway server) with the AWS or Microsoft Azure cloud API to discover virtual machines as shown in **Figure 5-4**. All setup files required to install the Veeam Agents to the discovered cloud VMs are uploaded to a selected destination object storage of the chosen cloud provider (AWS S3 bucket or Azure Blob storage account) by the backup server **only once**. To perform installation of the agent software on the cloud VMs, a service called "Veeam Cloud Message service" is injected into the VMs by leveraging the AWS/Azure APIs for controlling/accessing the VMs and the selected object storage as a source. This service is then also used to manage the installed Veeam Agents to perform backups, detect update requirements, etc.

It is important to recognize in this scenario that all backup traffic (i.e., "high volume traffic") generated by these Agents stays within the AWS or Azure cloud — there is no transfer of backup data between the managing Veeam backup server and the VM agents performing the backups. Only "low volume traffic" required for management is exchanged between the backup server and the AWS/Azure cloud API, and this control traffic does not involve any direct or VPN connection between backup server and agent VMs.

This also applies when it comes to file-level restores from backups created this way. The Veeam backup server communicates with the Azure/AWS APIs to manage restore processing, but the restore traffic does not traverse the cloud boundary, as shown in **Figure 5-5**.

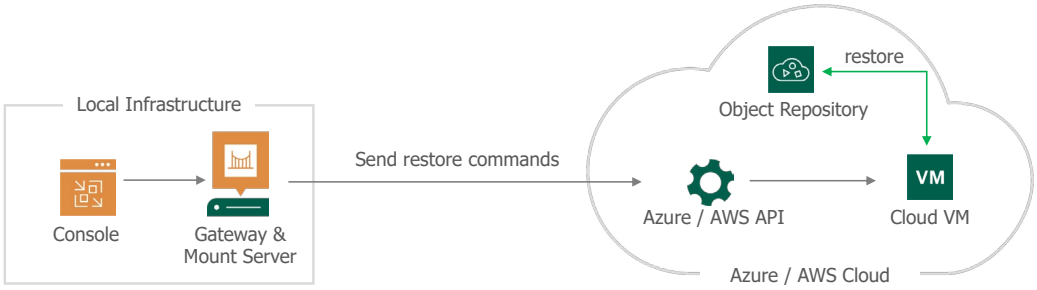

Figure 5-5: Protection Group for cloud machines — file-level restore

A backup job using a PG group for cloud machines can only use an object storage repository of the cloud the protected VMs are running in as backup target — because this guarantees that backup data will not traverse between cloud and on-premises, or between separate clouds, possibly introducing an unwanted egress cost. But this does not at all prevent from creating a "cross-cloud" or "cloud-to-on-prem" backup solution. Veeam Backup & Replication can be configured to regularly copy these backups from the object storage repository to any other repository, completely independent of the target's location. Additionally, most of the restore options are directly available from these backups as well, including Instant Recovery (see example in **Figure 5-6**)!

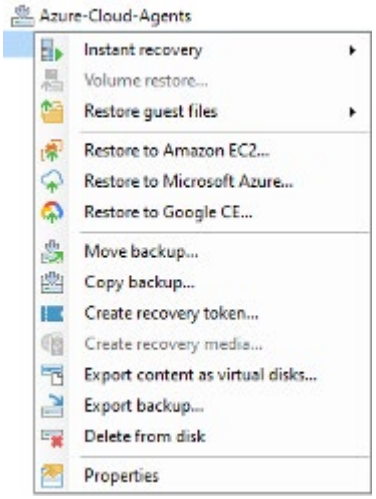

Figure 5-6: Cloud machine restore options (Azure VM in this example)

5.4. Agent backup jobs

To create backups of computers that have been added to **PGs**, at least one agent backup job is required, because the backup job defines the backup scope, schedule as well as the target where the backup data will be stored.

Centrally managed agent backup jobs are created and configured on the Veeam Backup & Replication backup server. These jobs let you choose between the already discussed ***managed by backup server*** and ***managed by agent*** modes as shown in **Figure 5-7**.

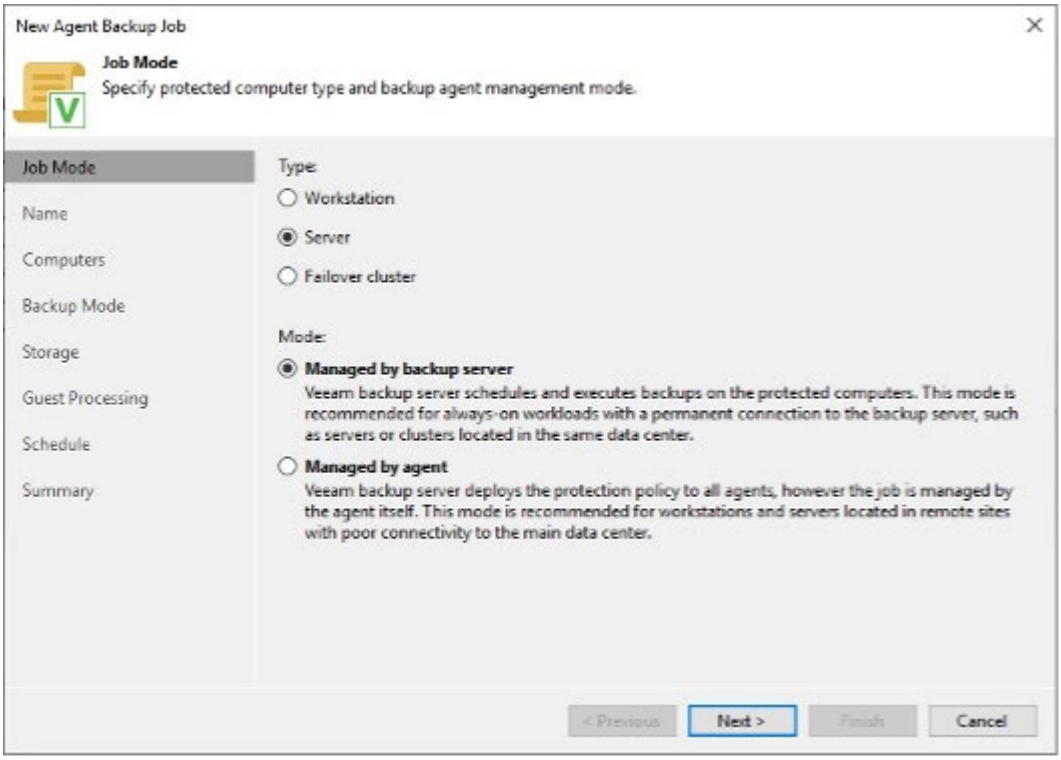

Figure 5-7: New Agent Backup Job dialog in Veeam Backup & Replication console

Note that only jobs of type ***Server*** or ***Failover cluster*** (i.e., for agents with Server edition license) provide the ability to enable application-aware processing, shown on the **Guest Processing** page of the wizard dialog.

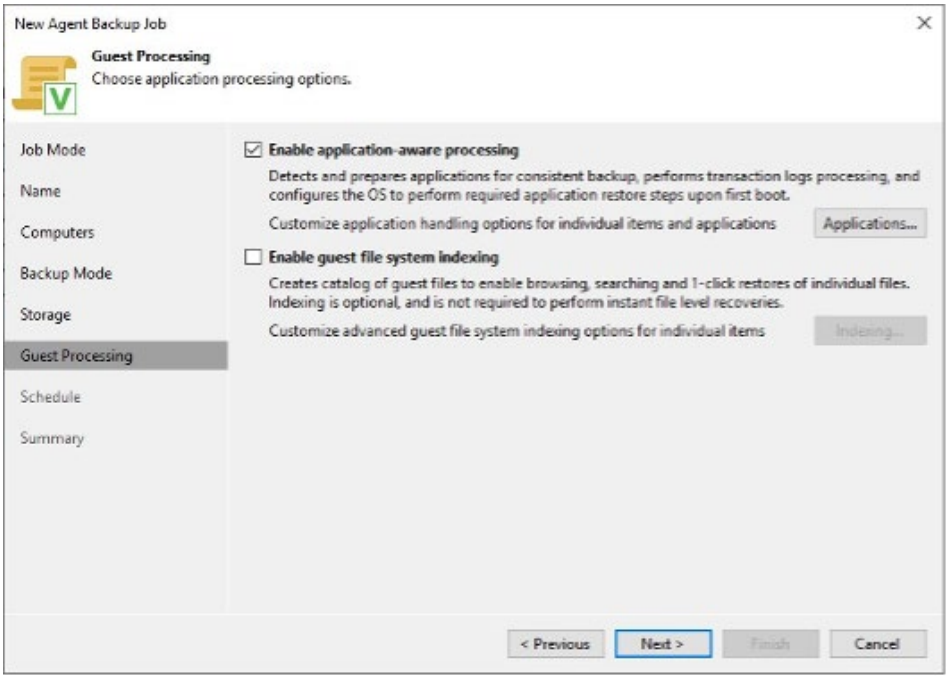

Figure 5-8: Guest processing options of a Server job

Starting with Veeam Agent *for Microsoft Windows* v6 and Veeam Backup & Replication v12, the application aware processing can leverage "Active Directory Group Managed Service Accounts" (gMSA) for authentication against the target Windows machine as shown in **Figure 5-9**.

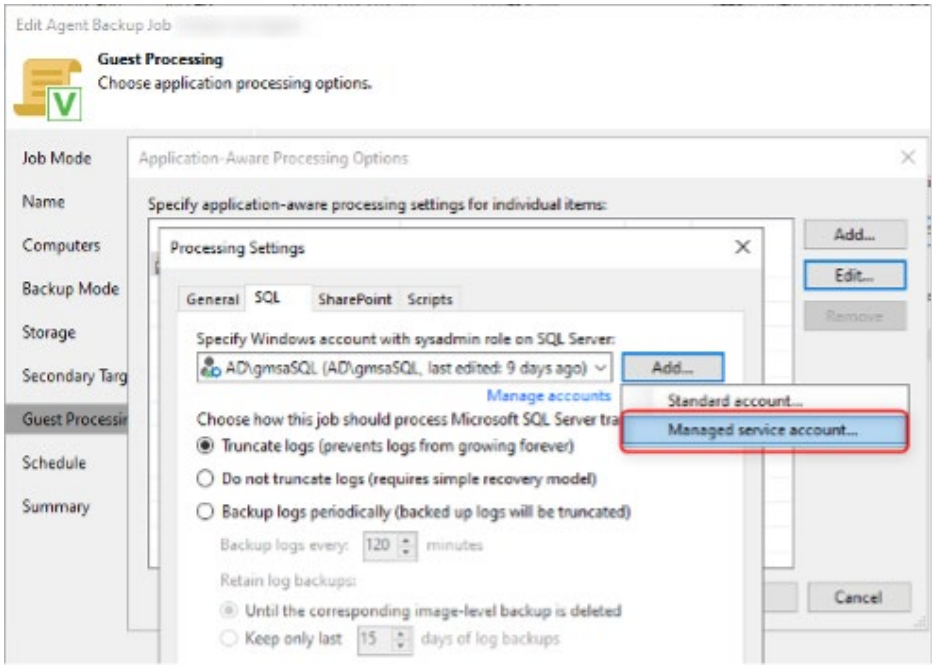

Figure 5-9: Configuring Group Managed Service Account for guest processing

To enable this Active Directory feature and leverage these managed service accounts for guest processing, some preparations are required within AD. For details, please see [this Help Center page](#).

The last step of the backup job configuration wizard shows the powerful scheduling options available in backup jobs managed by Veeam Backup & Replication (**Figure 5-10**).

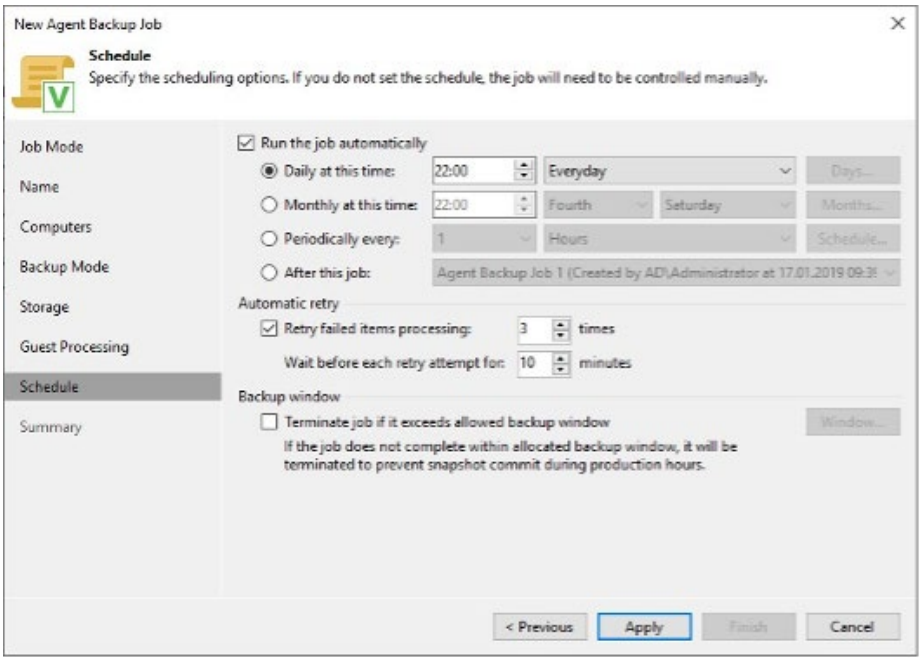

Figure 5-10: Job scheduling options for managed by backup server jobs

(Please note that there are different options available for standalone or managed by agent jobs, see **Figure 9-2**)

6. Backup targets

If you are familiar with Veeam Backup & Replication, you already know that many different targets can be used to store your valuable backup data. Veeam Agent *for Microsoft Windows* also supports a variety of configurable backup targets, depending on the management mode, as shown in **Table 6-1**.

	Standalone	Managed by Backup Server	Managed by Agent
Local storage	✔	✖	✔
Object storage	✔	✔	✔
Shared folder	✔	✔[4]	✔[3]
Veeam backup repository	✔	✔	✔
Veeam Cloud Connect repository[5]	✔	✔	✔
Deduplication appliance[6]	✔	✔	✔

Table 6-1: Backup targets

4 If configured as **backup repository** in Veeam Backup & Replication

5 For limitations and requirements regarding Cloud Connect repositories read more here: https://helpcenter.veeam.com/docs/agentforwindows/userguide/cloud_connect.html

6 Only if configured as **backup repository** in Veeam Backup & Replication. Read more about supported systems and configuration requirements here: https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html

6.1. Object Storage Support

Veeam Backup & Replication v12 introduced a feature called "Direct Object Storage Support". This allows object storages such as Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage and many other S3-compatible storage solutions to be used as primary backup repositories — regardless of being in public cloud or on-premises. The good news is that this feature is also included in the new Veeam Agent versions that have been released alongside Veeam Backup & Replication v12.

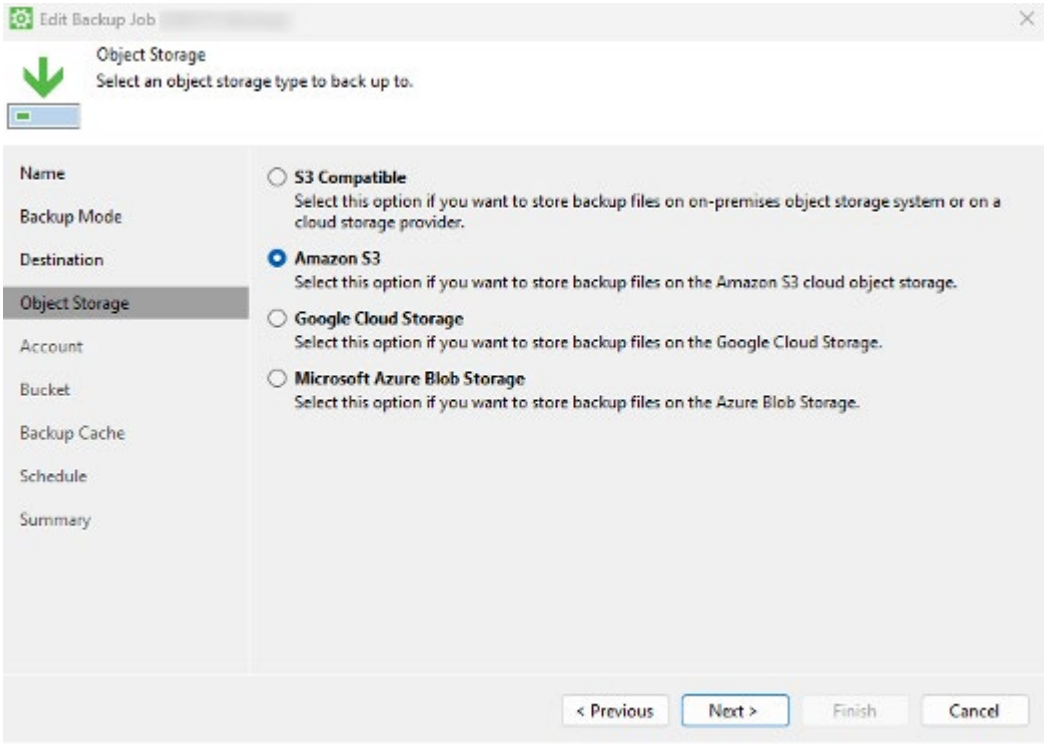

Figure 6-1: Object storage selection in Veeam Agent *for Microsoft Windows* (standalone)

You can leverage object storage either directly as the target of an Agent's backup job (only Agents for Windows, for Linux, and for Mac) or by using a Veeam Backup & Replication v12 backup repository that has been configured as an object storage repository (available for all Veeam Agents).

NOTE: *If you plan to store backups on an IBM or Wasabi cloud storage, use the S3 compatible storage option.*

A very important detail here is: If a Veeam Backup & Replication backup repository is used, you have the choice of whether backups of Agents should either directly be transferred to the configured object storage or if a (set of) gateway server(s) should be used as an intermediate hop before data arrives at the object storage. This provides a lot of flexibility for centrally managed agents as described in section 5. For example, you can back up remote office computers directly via a local internet link to a public cloud object storage provider, while still managing all agents from a central data center that might have a bandwidth-limited VPN link to the remote office. **Figure 6-2** illustrates this example.

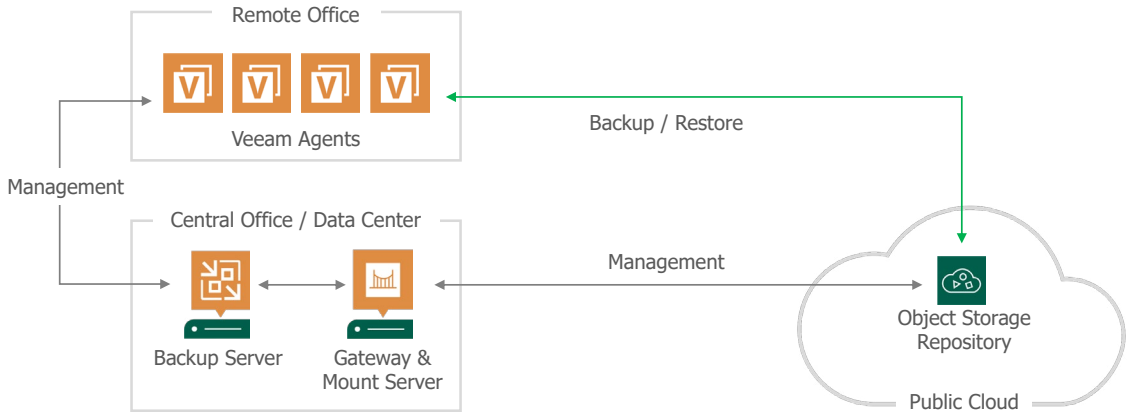

Figure 6-2: Remote office example using "direct to object storage" with central management

In such a scenario, you must configure the "direct to object" feature not within the Agent backup job, but within the repository's settings instead as show in **Figure 6-3**.

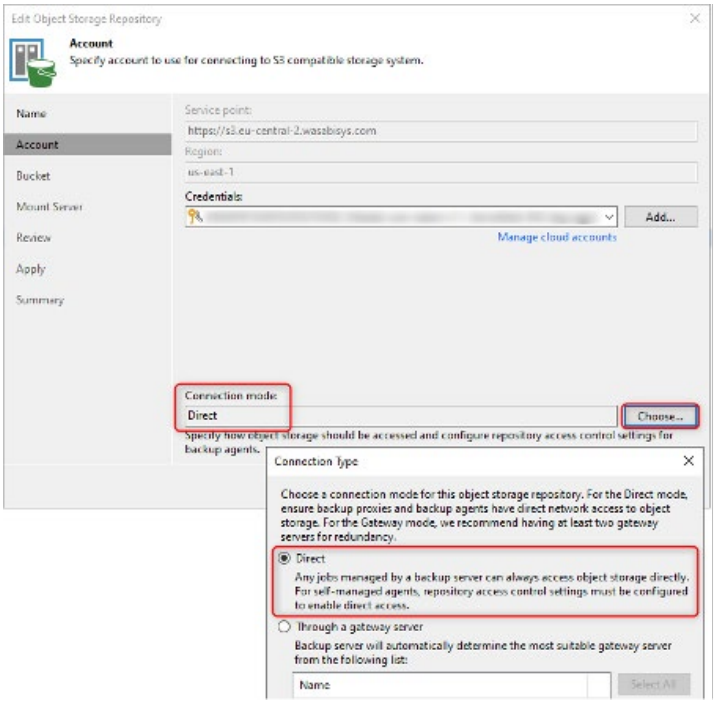

Figure 6-3: Direct connection mode in object storage repository settings

This example shows a configuration of an "S3-compatible" object storage (Wasabi in this case). The same configuration can of course be applied when using S3-compatible **on-premises object storage** located at your data center, so no traffic would leave your corporate LAN. Please have a look at this page to find a current list of on-premises and cloud object storage solutions known to be usable as a Veeam backup target — some of them also support immutability as an additional security feature!

6.2. Immutability

Many object storage solutions provide an additional immutability feature to prevent data from being changed or deleted for a predefined period of time. Veeam Backup & Replication has already been supporting this feature for quite some time already when using such a storage as a "capacity tier" in a Veeam scale-out backup repository (see here for details). Veeam Backup & Replication v12 now supports immutability for the "performance tier" as well as object storage repositories which are not part of a scale-out backup repository.

The same applies to the Veeam agents that have been released alongside Veeam Backup & Replication v12: When configuring an object storage as an agent's backup target, you can select to activate immutability and define the immutability period as shown in **Figure 6-4**.

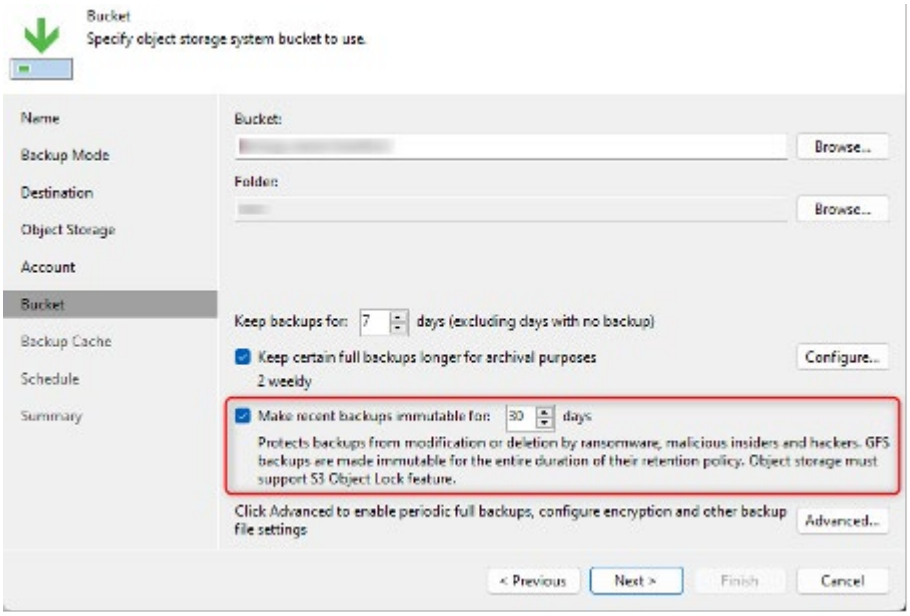

Figure 6-4: Immutability settings of backup target in Veeam Agent *for Microsoft Windows*

NOTE: *Veeam Backup & Replication additionally offers an immutability feature for storing backups on a so-called hardened repository which can also be used to store agent backup data!*

7. Encryption

To add extra protection to the backup data created by Veeam Agent *for Microsoft Windows* to comply with legal regulations or corporate policies. You can choose to encrypt backup files in the **Advanced Settings** of the job's backup target configuration as shown in **Figure 7-1**.

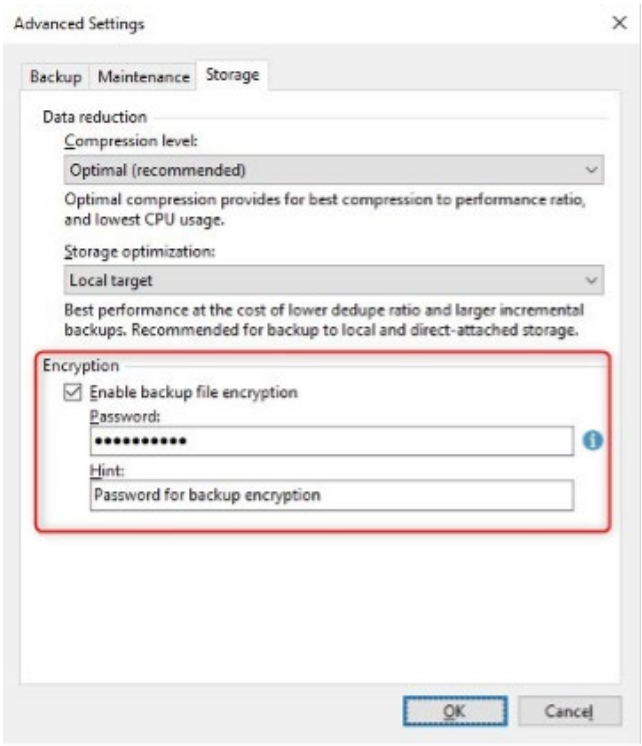

Figure 7-1: **Encryption** setting

All that's required is a password, which you need to remember for decrypting and restoring encrypted backup data. An optional hint phrase can be stored along with the password itself, which can help you recall the password when you need it most.

If a Veeam backup repository is selected as the backup target of a Veeam Agent *for Microsoft Windows* backup job in **standalone** mode. Encryption cannot be configured in the agent's job settings (**Figure 7-2**). This is because encryption of data located in Veeam backup repositories is managed by the administrators working with Veeam Backup & Replication.

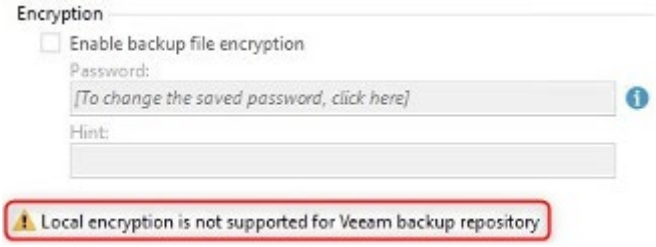

Figure 7-2: Local encryption is not available for Veeam backup repositories

That said, encryption can still be enabled for these agent backup files, but it must be configured by the backup administrator within the repository's "Access Permissions" settings (**Figure 7-3**).

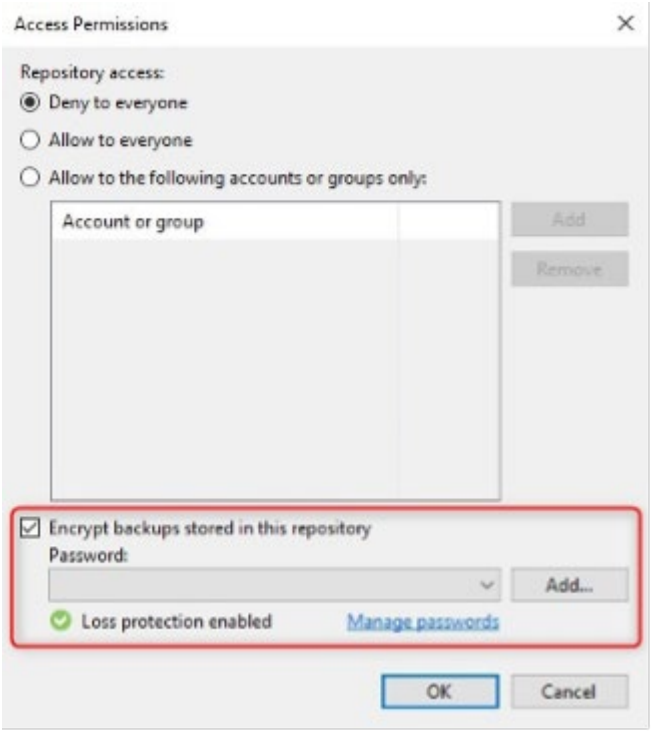

Figure 7-3: Encryption settings in a Veeam backup repository

NOTE: *The setting highlighted in* ***Figure 7-3*** *only applies to backups of agents in the* **standalone** *mode. When using* **managed by agent** *or* **managed by backup server** *jobs, this setting will be ignored and only the encryption settings in the job configuration will apply.*

8. Taking backups off-site: Following the 3-2-1 Rule

You are very likely already familiar with the 3-2-1 Rule of data protection:

Always create **3** copies of your data.

Store these copies on **2** different media types.

Move **1** copy off-site.

To help you follow this rule with Veeam Agent *for Microsoft Windows*, Veeam Backup & Replication provides backup copy jobs, which enable copying of any backup data to a secondary Veeam repository.

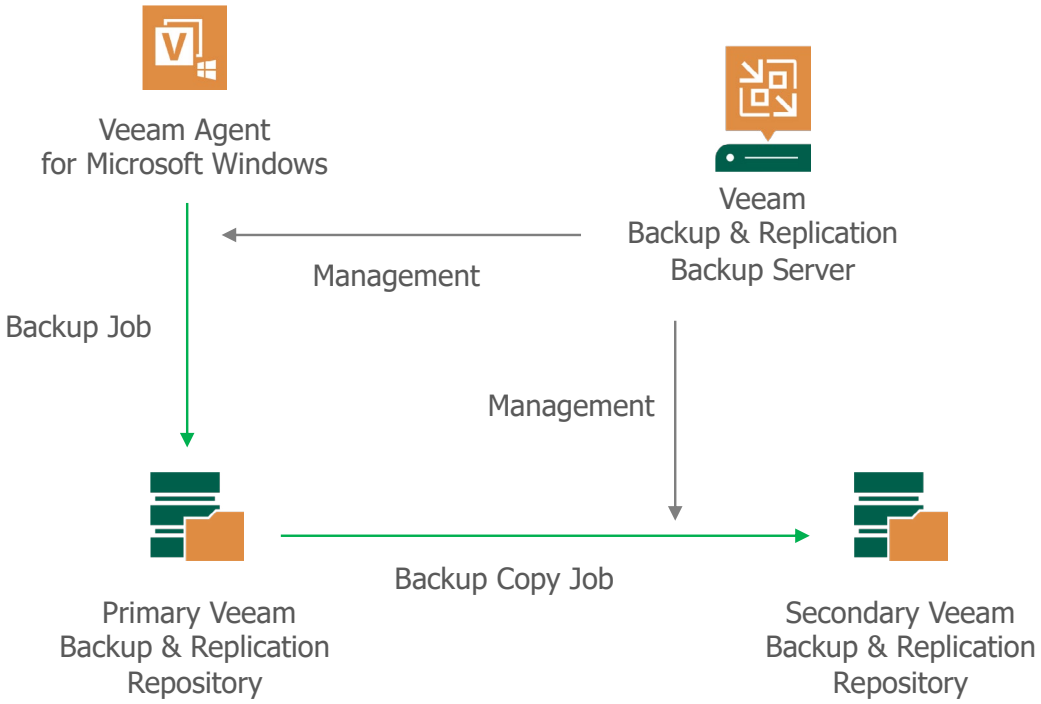

Figure 8 1: Backup copy

9. Protecting workstations

It is always a challenge to protect users' workstations as soon as they are not located directly beside your central backup infrastructure, i.e., if they are not well connected to your data center or sometimes are even completely offline during prolonged periods of time. This is a very common situation these days when you think of home office workers, travelling notebook users or even remote corporate locations which might have some local infrastructure, but backups still need to be stored centrally (e.g., because of corporate or legal requirements, lack of backup storage in the remote office, etc.).

For the deployment of Veeam Agent *for Microsoft Windows* on such remote computers, we already mentioned the possibility of using **distribution servers** in the section about **PGs** to create a distributed deployment infrastructure. But what are the options for workstations with an unreliable or sometimes unavailable connection to the central backup target? Well, let's have a look at what Veeam Agent *for Microsoft Windows* is offering in such situations for ***standalone*** workstation agents as well as for ***managed by agent*** policies!

9.1. Automatic resume of interrupted backups

If the network connection to the backup target is lost during the processing of a backup job, Veeam Agent *for Microsoft Windows* will try to resume its work as soon as the connection has been re-established. These resume operations will be retried over a maximum period of 23 hours (for scheduled job launches only); i.e., after this time the workstation agent will give up and mark the job as failed.

This "resume the backup" processing works automatically in the background and it will of course only transfer backup data which hasn't been transferred already, by keeping track of each transferred block (updating the local "block map" once per minute). If the backup job is targeting local storage or a shared folder, it will also resume automatically on returning from power saving modes (sleep, hibernate) which may have interrupted the backup run (for details and prerequisites, please see https://helpcenter.veeam.com/docs/agentforwindows/userguide/scheduled_backup_retry.html).

This feature is also available in Veeam Agent *for Mac* (version 2 or newer), you can find the corresponding details on this Veeam help center page.

9.2. Backup cache

If the backup target is not reachable when a backup job starts, an optional local cache can be used as a staging location for the backup data. This enables the job to run normally, and the cache will be synchronized to the original backup target as soon as connectivity resumes. The cache synchronization process works very similar to the "resume the backup" process described above, i.e., it will try to resume in case of intermittent connections or when returning from power save modes.

A suitable location of the cache can be selected automatically by Veeam Agent *for Microsoft Windows*, but it is also possible to manually configure a folder where backup data should be cached. Be aware that for agents managed by Veeam Backup & Replication via ***backup by agent*** policy, the manual selection must be available for all workstations the policy will be applied to! That's why the automatic selection might be a better choice, as it will select the best suitable volume for each workstation individually. **Figure 9-1** shows the cache configuration options of such a policy (for more details about the automatic cache placement, please visit https://helpcenter.veeam.com/docs/backup/agents/backup_cache.html).

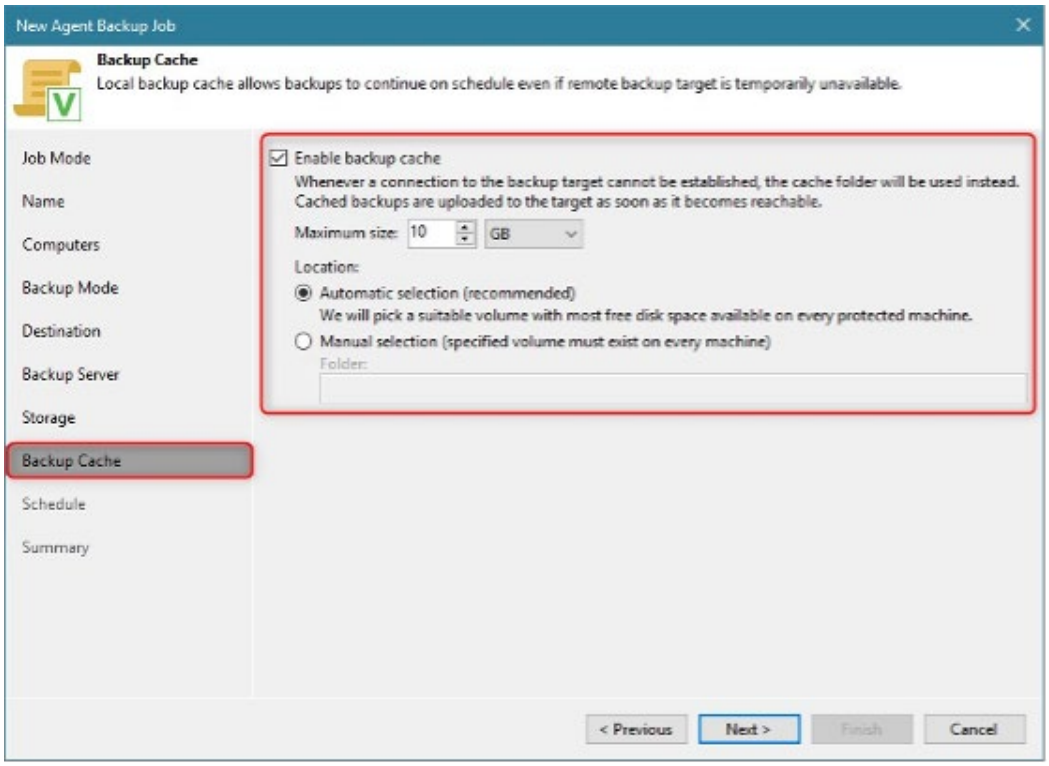

Figure 9-1: Backup Cache options of a managed by agent policy

Please note that for ***standalone*** agents the Backup Cache option is available for all supported backup targets except "local storage" (where it wouldn't make any sense). However, for agents being controlled via a ***managed by agent*** policy, caching is available only when targeting a Veeam repository or a Veeam Cloud Connect repository. Cache cannot be used with file-level backup mode (unless it's configured for image-based processing as described in section "Multiple backup modes").

9.3. Event-based scheduling

Taking a closer look at the scheduling options for either ***standalone*** agents or jobs/policies of type "Workstation," you will notice there are more settings available to create a much more flexible backup schedule that not only depends on time of day, weekdays, etc.

Figure 9-2 shows all selectable scheduling options of agents with a workstation license (i.e., using backup jobs of type "workstation." This also applies to free standalone agents).

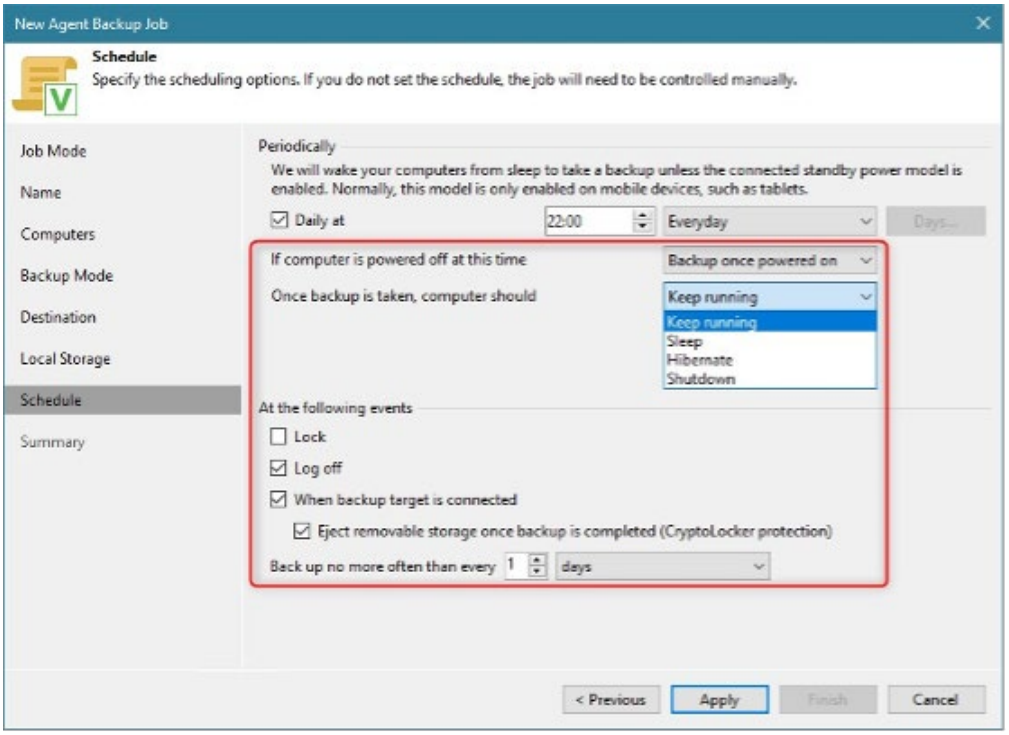

Figure 9 2: Scheduling options of a ***managed by agent*** policy or ***standalone*** agent

These settings provide great flexibility for travelling users or home office workers, because usually such users have very individual working schedules and a "static" backup schedule (e.g., daily at a fixed time of day) is most likely not suitable.

Most of the options shown in **Figure 9-2** are self-explaining, but let's have a closer look at the setting "When backup target is connected." This simply means that Veeam Agent *for Microsoft Windows* will start the backup job as soon as the configured backup target becomes available, and this just works for local storage (e.g. plugging in an external USB storage device) as well as for targets reachable via network (e.g. a shared folder on a NAS or file server, a backup repository that requires a VPN connection to be reachable, etc.). Imagine a travelling user who is working on documents while offline: The backup of his computer will start immediately as soon as he gets connected to the corporate network where the backup target is reachable!

9.4. Ransomware Protection

Removable storage devices being used as a backup target should be physically disconnected from the computer after backup processing finishes — this means the backup data will be safe off-line and cannot be tampered with by any malicious software. Veeam Agent *for Microsoft Windows* can help you with following this recommendation by automatically ejecting the removable storage device when it completes the backup (see the optional setting "Eject removable storage once backup is completed" in **Figure 9-2** above).

Combined with the "When backup target is connected" scheduling option, the task to back up your remote or travelling workstation becomes as easy as it can be. Backup starts when the device is plugged in, and the device will be automatically ejected after the backup completes. Even if you forget to physically unplug the device, its contents will be no longer available to the operating system (it's in a dismounted state), and thus will be protected from any ransomware or crypto locker attack.

Another way is of course to combine these options with the setting "Once backup is taken, computer should Sleep/Hibernate/Shutdown", and that's how I use it to create a daily backup of my home workstation:

1. At the end of my workday, I close all my documents/applications and plug-in the USB key I configured as the backup target. The backup starts immediately.
2. I lock the screen and leave the computer running.
3. Veeam Agent *for Microsoft Windows* creates a backup on my USB key and ejects it afterwards.
4. Veeam Agent *for Microsoft Windows* shuts down the computer.
5. First thing on the next morning: Unplug the USB key before starting the computer.

Now, that's easy, isn't it?

10. Integration with Storage Snapshots

A feature that was introduced with Veeam Backup & Replication v11 is the capability to create "off-host" backups of SAN based storage snapshots of volumes mounted to computers running Veeam Agent *for Microsoft Windows* v5 and newer.

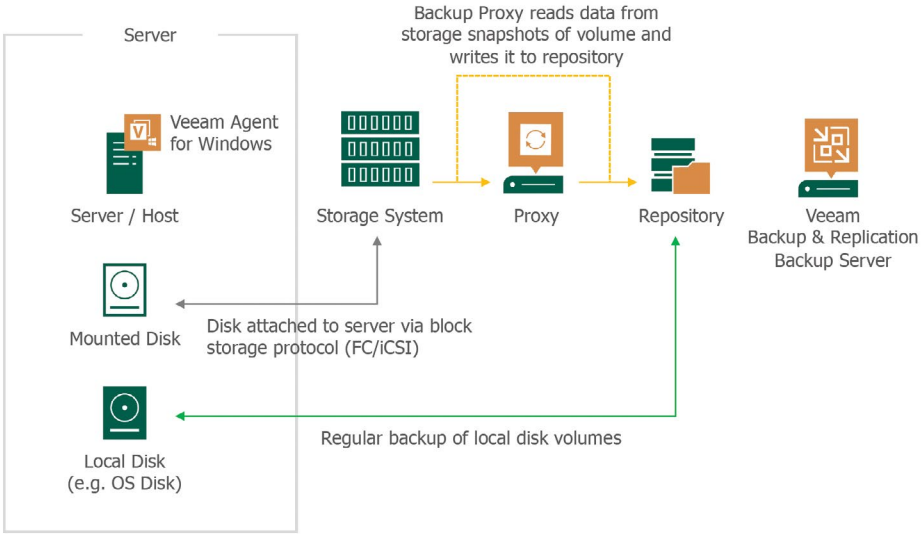

Figure 10-1: Veeam Agent *for Microsoft Windows* storage snapshot integration

Figure 10-1 illustrates how the integration works: The server on the upper left runs Veeam Agent *for Microsoft Windows* and has a volume mounted from an external storage system, in addition to its local, directly attached volumes (e.g., the OS volume). The storage system has been integrated into Veeam Backup & Replication's storage infrastructure, and the check box "Block storage for Microsoft Windows servers" has been enabled in the settings as shown in the NetApp example in **Figure 10-2**.

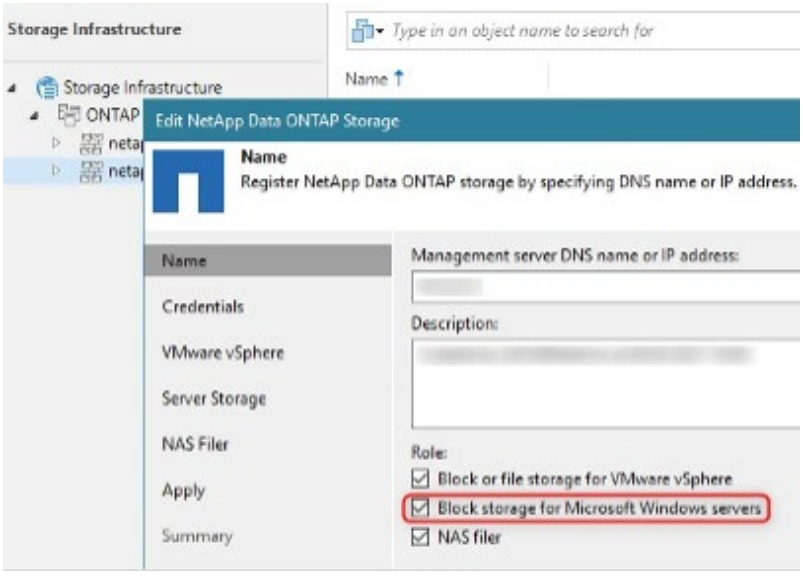

Figure 10-2: Storage settings for NetApp system integrated into Veeam Backup & Replication

Additionally, a Veeam backup proxy server has been added/configured to the Veeam backup infrastructure which has access to the storage system (**Figure 10-3**).

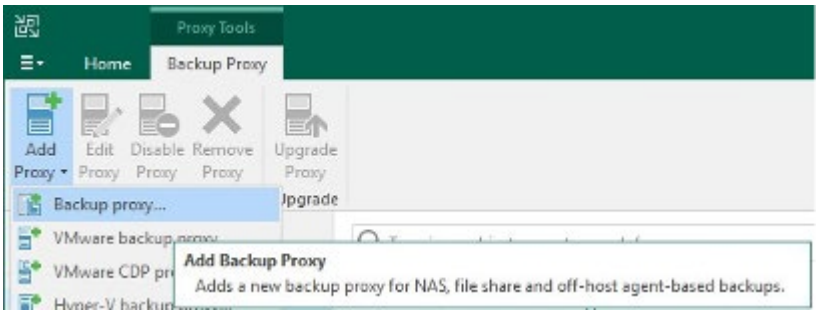

Figure 10-3: Backup Proxy to access the storage system integrated into Veeam Backup & Replication

The final bit must be configured within the ***managed by backup server*** backup job. Here, you have to enter the advanced settings of the "Storage" step of the configuration wizard and check the box "Enable backup from storage snapshots" as shown in **Figure 10-4**. Select whether proxies should be assigned automatically during each job run, or if you want to restrict the job to utilize only a set of proxies of your choice, and what to do in case the snapshot processing fails (either failover to "normal" mode or end job with a status of "failed").

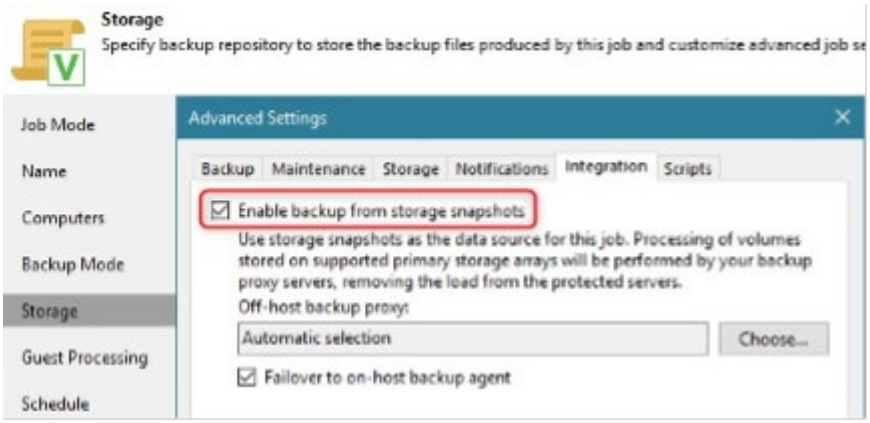

Figure 10-4: Backup job setting to enable storage snapshot integration

When running the job, the log will show whether everything works as desired, as you can see in **Figure 10-5**. This screenshot was taken from the run of a 2-node failover cluster job where a SAN-based volume was used as a cluster disk, and you can see that it works just fine (taking the storage volume snapshot while processing the current owner node).

Figure 10-5: While processing the owner node, SAN based cluster disk E:
has been backed up via off-host storage snapshot while system volume C: was backed up "the usual way".

11. Recovery tokens

When a restore process is initiated directly from an agent computer with the intention to restore from backup data that has been stored on a repository managed by Veeam Backup & Replication, it is required to authenticate against the backup server. This guarantees that the user performing the restore will only be able to see the backup data (i.e., the computer's restore points) the user is authorized to access. Usually, the installed Veeam Agent performs this authentication task in the background, not visible to the user. But what happens if this isn't possible because the user wants to perform a bare metal restore of a selected computer's backup to a totally different hardware that has nothing installed (no OS and no Agent)? Well, this requires booting from a recovery media and selecting either bare metal restore or volume restore. During this process, the user needs to authenticate via username/password credentials before being allowed access to the backups. So, the user needs to know the correct credentials to be able to proceed, and this sometimes means sharing sensitive credential information with users who usually should not have access to these credentials.

To avoid such situations Veeam Backup & Replication v12 introduced a new feature called "Recovery Tokens" which works with Veeam Agent *for Microsoft Windows* and Veeam Agent *for Linux* v6 or newer. The process of leveraging these tokens follows these steps:

1. User wants to start a recovery process and submits a request that arrives at the Veeam backup administration staff or at the organization's helpdesk.
2. An administrative Veeam or helpdesk user ("Restore Operator" role required) creates a recovery token, either manually via the Veeam console (see **Figure 1-2**) or automated via PowerShell or Rest API.

a. The token is built as a 16-digit alphanumeric string (allowing >1024 combinations)

b. The token by default expires 24 hours after creation.

3. The token is sent to the requesting user (by email, text message, on the phone, ...).
4. The token is used by the restore user during the authentication step of the restore process instead of entering credentials, as shown in **Figure 11-1**.
5. A list of restore points associated with this recovery token is presented to the user.
6. The user selects a restore point and proceeds with the restore process.

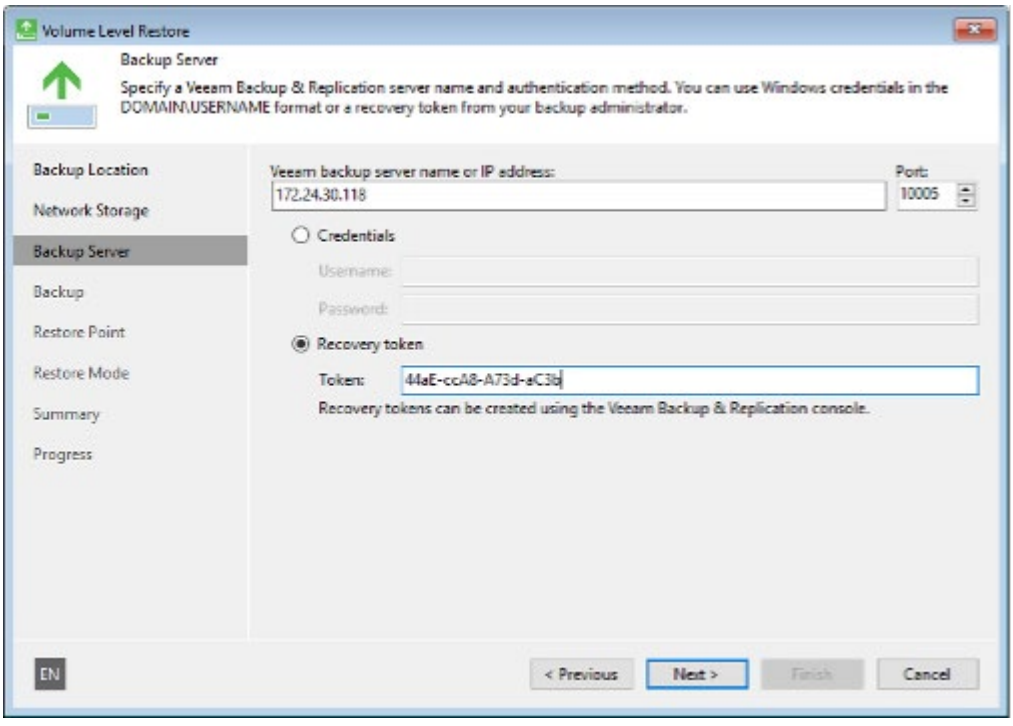

Figure 11-1: Entering recovery token during volume restore in Veeam Agent *for Microsoft Windows*

It's a very easy process to follow and eliminates sharing of sensitive access credentials with the user performing the restore.

As mentioned above, recovery tokens are also available for Veeam Agent *for Linux* restores as shown in **Figure 11-2**.

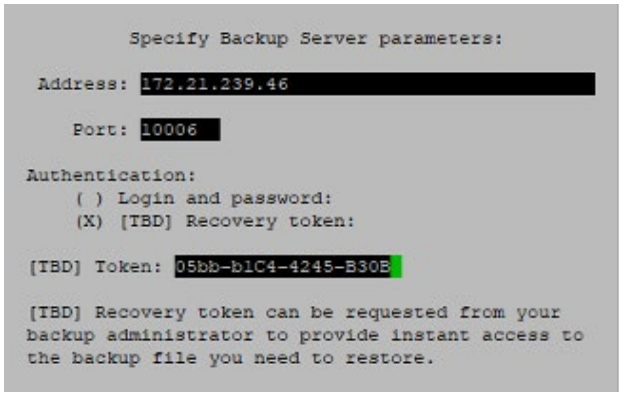

Figure 11-2: Entering recovery token during bare metal restore in Veeam Agent *for Linux*

12. Conclusion

Ensuring timely and reliable backups for ALL workloads is a must but is challenging with the many possible configurations when it comes to virtual AND physical environments.

Veeam Agents offer a great solution because they

- Significantly reduce deployment and management operations with simple to organize, automate and deploy Veeam Agents at scale in protection groups designed to be customized and flexible.
- Reduce production impact by combining change block tracking (CBT), parallel disk processing and storage snapshot integrations to provide the performance needed to process server-extensive data sets.
- Stay agile and highly available without sacrificing your data protection. Flexibility is key in recovery from bare metal to applications and all the way down to files — Veeam has what you need to succeed.

To see all these best practices in action, start a free 30-day trial.

Finally, please remember that this paper is focused on **Veeam Agent *for Microsoft Windows***. But as mentioned a few times in this document, Veeam provides agents for other platforms/OSes, too! Here's a current list of all the available Veeam Agents:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Mac
- Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris

Each list item above is linked to the corresponding product page on veeam.com, so please go and give them a try!

About the Author

As a Senior Solutions Architect at Veeam, Matthias is helping customers and partners with planning, designing, and implementing strategies and solutions to protect mission-critical workloads. Matthias holds an advanced degree in physics and has been in the IT industry for more than 25 years in several operations, management, and consultancy positions.

About Veeam Software

Veeam provides organizations with resiliency through data security, data recovery and data freedom for their hybrid cloud. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments that give businesses the peace of mind their apps and data are protected and always available so that they can keep their businesses running. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 82% of the Fortune 500 and 69% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers, service providers, and alliance partners. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeam-software and Twitter @veeam.

Please leave your feedback at our dedicated Veeam Community Forum or the Veeam Community Resource Hub!

Protect your Windows backups against hardware failures, file corruption and ransomware with Veeam Data Platform. Get a free 30-day trial!