Control Server
Backup and Restore User Guide

June 2019
These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: June 2019
Issued: April 2018


* Indicates a trademark of General Electric Company and/or its subsidiaries. All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation. Please send comments or suggestions to controls.doc@ge.com
Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Restore HC1 VM (Alternative Instructions)</td>
<td>New section</td>
</tr>
</tbody>
</table>

Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Controller</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>EWS</td>
<td>Engineering Workstation</td>
</tr>
<tr>
<td>MC</td>
<td>Management Computer</td>
</tr>
<tr>
<td>PDH</td>
<td>Plant Data Highway</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
</tbody>
</table>

Related Documents

<table>
<thead>
<tr>
<th>Doc #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6844</td>
<td>Control Server System Overview</td>
</tr>
<tr>
<td>GEH-6845</td>
<td>Control Server - Domain Services Maintenance Guide</td>
</tr>
</tbody>
</table>

Safety Symbol Legend

- **Warning**: Indicates a procedure or condition that, if not strictly observed, could result in personal injury or death.

- **Caution**: Indicates a procedure or condition that, if not strictly observed, could result in damage to or destruction of equipment.

- **Attention**: Indicates a procedure or condition that should be strictly followed to improve these applications.
Control System Warnings

To prevent personal injury or damage to equipment, follow all equipment safety procedures, Lockout Tagout (LOTO), and site safety procedures as indicated by Employee Health and Safety (EHS) guidelines.

Warning

This equipment contains a potential hazard of electric shock, burn, or death. Only personnel who are adequately trained and thoroughly familiar with the equipment and the instructions should install, operate, or maintain this equipment.

Warning

Isolation of test equipment from the equipment under test presents potential electrical hazards. If the test equipment cannot be grounded to the equipment under test, the test equipment’s case must be shielded to prevent contact by personnel.

To minimize hazard of electrical shock or burn, approved grounding practices and procedures must be strictly followed.

Warning

To prevent personal injury or equipment damage caused by equipment malfunction, only adequately trained personnel should modify any programmable machine.

Warning

Always ensure that applicable standards and regulations are followed and only properly certified equipment is used as a critical component of a safety system. Never assume that the Human-machine Interface (HMI) or the operator will close a safety critical control loop.
1 Overview

The Control Server Backup and Restore package adds the hardware and software required to periodically back up both the definition and contents of the Virtual Machines (VMs) running on the Control Server. The resulting backup archives can be used to restore the entire VM (definition and contents), or recover individual files from the archive. The standard configuration backs up daily archives for one week, weekly archives for one month, and monthly archives for one year.

There are two versions of the package available: one for the Simplex Control Server and one for the High Availability (HA) Control Server. The appropriate package can be purchased with a new Control Server, or purchased for upgrade into an existing system.

The package consists of one or more hard disk drives (HDD) to hold the archives, the software used to create and restore the archives, and the licenses required for the host system (HA or Simplex). The licensing is based upon the number of host servers and the number of CPUs they contain. Additional VMs can be added to the servers without requiring a license upgrade.
2 Theory of Operation

The Veeam® Backup & Replication package is a hypervisor-based backup scheme. It contacts the hypervisor that is hosting the VM and uses it to collect the contents of the VM virtual drives. A hypervisor-based backup scheme has some advantages, such as:

- It can back up the VM definition so the entire VM can be recovered or recreated instead of just the contents that are running within the VM.
- It does not require an agent running within the VM; it accesses the VM virtual disk contents through the hypervisor. This allows it to back up any type of VM, not just VMs running an operating system with an available backup agent. This also means it can be used to back up limited access VMs (sometimes called appliances) where there is no option to run an additional program (such as a backup agent) inside the VM.

To implement the backup scheme, the backup subsystem includes:

- **Backup Drives**: These hard drives hold the backups. Normal spinning metal HDDs are used to hold the backups; they do not require high-performance Solid State Drives (SSDs), which may be cost prohibitive at the large capacities required for backups.
- **Backup Program**: This program communicates with the hypervisor to collect the information and write it to the backup drives. The Backup Program must run within a VM.
- **Backup User Interface**: This user interface (UI) allows users to schedule backups, see the results of the backups, and initiate restore. This typically runs in the same VM as the Backup Program.

2.1 Backup Architecture

There are two configurations used for the backups: one for the HA system and one for the Simplex system. These differ in the types and locations of the hard drives and the VM that hosts the Backup Program.

2.1.1 HA Backup Architecture

The HA architecture consists of two servers (HS1, HS2) in a cluster configuration that run the site-specific VMs, and one server (MC2) for managing the cluster. The Management Computer (MC2) hypervisor hosts a Management VM (MC3) that contains the cluster management tools.

The backup hard drive (or drives) are added to the MC2 computer and exposed as a large virtual drive to the MC3 VM. The MC3 VM has the Backup Program and Backup User Interface installed and is the focal point for defining, running, and restoring from the backups.
2.1.2 Simplex Backup Architecture

The Simplex architecture consists of a single server (HS1) running all of the site VMs. One of the existing Windows®-based VMs is chosen to host the Backup Program and Backup User Interface. While this does not provide a completely separate system to back up the running VMs, storing the backups on a separate hard drive (sometimes called a separate spindle solution) does provide the ability to recover VMs from that hard drive alone.

The backup hard drive(s) are added to the HS1 computer and exposed as a large virtual drive added to the VM chosen to host the Backup Program. The chosen VM has the Backup Program and Backup User Interface installed and is the focal point for defining, running, and restoring from the backups.

2.1.3 Common Backup Architecture

Both the HA and the Simplex architectures handle the additional hard drives in the same way:

- The hard drive(s) are placed into a BIOS RAID array (even if there is only one drive) to make use of some of the performance benefits provided by the RAID controller. If there are multiple drives, a RAID-0 array is used so the multiple drives all add capacity, not redundancy.
- A new hypervisor datastore is created and the backup drive is added to it. A separate datastore is used to isolate the main system storage and the backup storage. This datastore is typically named XXX Backup where XXX is the name of the computer to which the drives were added. This typically translates to MC2 Backup on an HA system, and HS1 Backup on a Simplex system.
- The VM where the Backup Program is running (typically MC3 on an HA system and a chosen VM on a Simplex system) has an additional virtual hard drive added to it, where the size of the virtual hard drive is just under the full size of the XXX Backup datastore. The size of this virtual drive is set to 0.02 TB less than the size of the datastore to account for overhead, rounding in sizing calculations, and to leave a small portion of the datastore (and hard drive[s]) available for diagnostics and testing.
- The additional hard drive is given the drive letter D: and a D:\Backup directory is created to store the backups. The use of the drive letter D: is not a requirement, just a convention.
2.2 Backup Concepts

Several concepts are used to define the backup scheme. Most of these concepts are not requirements, but they are decisions made about the frequency and types of backups, as well as what is to be backed up and what should be skipped. This section defines some of those concepts and what items should be taken into account when modifying the backup settings.

2.2.1 Short Term and Long Term Repositories

The backup software uses the concept of a Repository to hold the backups. In the original configuration, this is nothing more than a directory in D:\Backup. These repositories can be moved off of the local drive and onto a network drive to store copies of the backups outside of the system. Additional repositories can also be created (instead of moving the existing one) to store additional copies to a location off of the server and rack.

There are two types of repositories used in the backup scheme:

- The **Short Term Repository** is configured to maintain one full backup and collect an incremental backup every day for one week. The last incremental backup is typically the one used for a full VM restore operation as it will be the most current backup of the VM. In cases where the latest is not desired, any of the incremental or the full backup can be used as the source for a recovery operation. The Short Term Repository is stored in D:\Backup\ShortTerm, with each VM in a subdirectory named with the VM name.

  *Example:* The Short Term backups for the EWS VM are located in D:\Backup\ShortTerm\EWS.

- The **Long Term Repository** is configured to maintain one full backup each week for one month, and one full backup each month for one year. The Long Term Repository is stored in D:\Backup\LongTerm, with each VM in a subdirectory named Copy_<VMname>, where <VMname> is the name of the VM.

  *Example:* The Long Term backups for the DC1 VM are located in D:\Backup\LongTerm\Copy_DC1.

If additional copies of the backups are needed (such as on a network drive), an additional copy job can be created that is similar to the existing copy job but with the destination being a repository on the remote drive. The scheduling of how often to save backups can be customized to match the site's desired frequency of backups.

A similar remote backup scheme can be achieved by copying the files in the Short Term or Long Term Repository to a remote location. An example of this is copying the last monthly full backup off-site for emergency purposes. The backup subsystem does not place any limitations on external file copies; nothing special is required. Upon restoring a remote archive file to the local repository, the files copied back will show as imported archives that can be selected for restore operations just like any other archive in the repository. This simple file copy method is also suitable for copying local archive files onto a portable USB drive for remote storage.

2.2.2 Backup Jobs

Users can define backup jobs using the Veeam tool. Backup software determines what and when to back up based on scheduling. Each backup job defines which VM(s) to back up, when to run the backup, what type of backup to run (full or incremental), and where to place the backup (repository). In standard configurations, a separate backup job is created for each VM. The VM name describes the job name, the directory name, and the backup name. Multiple VMs can be combined into a single backup job but the default configuration is one VM per job.

The Short Term backups use a job type of **Backup**. These jobs read information from the VM and create the incremental or full backups in the Short Term Repository. To gain efficiency, when it is time to create a new full backup, the Backup Program does not necessarily collect all files from the VM. It can get an incremental backup, then integrate the last full backup plus all the intermediate incremental backups to create a new full backup. This is called a synthesized backup. Use of synthesized backups is enabled by default, but can be disabled on a job-by-job basis.

The Long Term backups use a job type of **Backup Copy**. These jobs copy the information from the Short Term Repository instead of retrieving the information from the VM. Backup Copy jobs are typically not scheduled; they run continuously in that they are triggered whenever a backup job completes. There can be multiple Backup Copy jobs defined for each backup job. You can create a new Backup Copy job to copy the backups to a location off of the server and rack in addition to the existing Long Term Backup Copy job. By default, the Backup Copy jobs are named Copy_<VMname>, where <VMname> is the name of the VM.
In the default configuration, each VM has two jobs associated with it, as follows:

- A **Backup** job named `<VMname>` reads the files from the VM and populates the Short Term Repository. This job is scheduled to run at midnight each night.
- A **Backup Copy** job named `Copy_<VMname>` copies the files from the Short Term Repository to the Long Term Repository. This job is **Continuous** in that it will run each time the backup job completes.

### 2.2.3 Backup Scheduling

By default, each backup job (default is one per VM) is scheduled to run at midnight. The Short Term Repository definition has an attribute that defines the number of concurrent jobs that are allowed to run. In the default configuration, this is set to 1 so that each VM job will run to completion, then the next VM job will start. This scheme works well to address issues such as the difference in time it takes to do a full backup versus an incremental backup. VM jobs do not need to be staggered in time so that they do not overlap, yet the backups will be completed as soon as possible. The total amount of time it takes to do all backups can be quickly determined by looking at the time the last backup completed.

The Backup Copy jobs are not scheduled; they run after each Backup job completes. Because these jobs involve copying files from the Short Term Repository to the Long Term Repository, they do not impact the original VM.

### 2.2.4 Performance and Throttles

The act of backing up the contents of a VM virtual drive moves a lot of data. The movement and processing of this data may overwhelm portions of the system if care is not taken to prevent it. There are several ways that data can be **throttled** to achieve a reasonable balance between backup performance and normal system performance.

One method of throttling has already been mentioned: limiting the backup program to only run one Short Term Backup job at once. This helps limit the loading on the VM that is running the Backup job, the loading on the hypervisor that is supplying the information, and the bandwidth used to collect the data. Having only one Short Term Backup job active at one time is the simplest way to avoid performance holdups.

In the HA system, the backup program running in MC3 must communicate over the Plant Data Highway (PDH) to the hypervisor to collect the contents of the VM's virtual drives. Even with only backing up one VM at a time, the backup program will attempt to take up as much of the PDH bandwidth as it can to copy the data from the VM to the Short Term Repository. Initial testing showed that this can take up to 85% of the PDH bandwidth, leaving very little bandwidth available for other use. While this does not necessarily create a problem (all programs will fight for the available bandwidth), it may visibly slow down the data flow between the Thin Client terminals and their host VMs. This may impact the speed at which the displays are updated. To limit the impact of the backups, a throttle has been created to limit the backup data to use no more than 20% of the PDH bandwidth. This throttle is actually implemented by the hypervisor, not the backup program. In case of emergencies (such as restoring all VMs before the site is at full performance again), this throttle can be removed to improve the recovery time. Once the site is operational again, the throttle should be reinstated. (This is done using the Traffic Shaping settings on the hypervisor vmk1 interface, setting it to 200000 Kbits/s, about 20% of a 1Gb link.)

In the Simplex system, the backup program is running under the same hypervisor as the VMs that it is backing up. In this situation, the backup program recognizes that it does not need to use the PDH to obtain the VM virtual drive contents; it can map a drive of its own to the virtual drive and simply read it. If you are logged into the VM running the backup program you will see an extra hard drive display when it is backing up one of the other VMs. The backup program then populates the Short Term Repository from this extra hard drive, and removes the hard drive when it is done. This scheme provides for faster backups and it does not use any network bandwidth.

The VM that is running the backup program can run low on memory while attempting to do the backups due to the amount of data and disk caches used while copying the data. For that reason, the memory used by the VM is increased by 2 GB when the backup program is installed into the VM. This applies to the MC3 VM on an HA system, as well as the selected VM on a Simplex system. The increase in memory is the only setting that is modified on the VM when the backup package is installed.
2.2.5 Backup Exclusions

There are some portions of the system that the backup subsystem will not try to backup. This includes the virtual drive used with the Large Historian option, as well as the HDD that is used to hold the backup repositories.

To prevent these virtual drives from being backed up, you must first understand how the backup program collects the data from the hypervisor. When the backup program wants to read the contents of the VM's virtual drive, it determines if the VM is running. If the VM is not running, then it can simply read the contents of the virtual hard drive. If the VM is running, then it must handle with the fact that the VM is changing the contents on the virtual drive as the backup is being done. To address this, the backup program works with the hypervisor to create a snapshot of the disk contents, then backs up the (static) contents within the snapshot. The VM can be running and changing disk content during the backup, but it is the content of the snapshot that is actually stored in the backup repository. When the backup is complete, the hypervisor is commanded to remove the snapshot and the VM continues running, unaware that a backup was done.

When a snapshot is made of a running VM, the backup program notifies the VM to flush its disk buffers to the virtual drive before it makes the snapshot. This is called asking the VM to quiesce. Occasionally, a warning message is displayed concerning the inability to quiesce the VM prior to taking the backup. If this becomes troublesome, there is an option available to attempt to quiesce the VM or to proceed if it does not. This option is located in the Backup job definition as follows: Guest Processing, Enable application-away processing, Applications, and General tab.

Because the backup subsystem uses VM snapshots, it follows the settings that are used when creating virtual drives in a VM to determine if those virtual drives should be included in the snapshots of the VM or not. This is the easiest way to exclude an entire virtual drive from being included in a backup of that VM. This is how both the Large Historian option (which adds a new virtual drive for the long term history) and the Backup and Restore option (which adds a new virtual drive to hold the backups) excludes those drives from the backups. By defining the virtual drives to be independent, they will not be included in the snapshot and therefore will not be backed up. Likewise, you can restore the system disk of these VMs and the contents of these data drives will not be touched.

Note The Short Term backup jobs that back up these VMs may display a message notification that these drives were not backed up with the VM.
2.2.6 Backup Progress Messages and Job Duration Reporting

During most operations, the Backup User Interface indicates the current status of the operation in progress and provides estimates as to the percentage complete and estimated time remaining for these operations. These estimates and projections can be discouraging as they assume that all virtual drives are full (all blocks are used and need to be backed up).

For example, it is not uncommon to see a percent complete bar for a backup operation start at zero and slowly move forward until it hits a certain point, then jump to 100% complete. This is because it assumes that the entire disk is used and estimates the percent complete (and time to completion, if provided) based upon that assumption. When it hits the point where it has backed up all the used portions of the virtual drive and only unused portions remain, it will jump to 100% complete because it has nothing left to read.

The default backup scheme is to launch all Short Term backup jobs at midnight. The Short Term job queue is configured to only run one job at a time, starting a new job after the previous job has completed. The status reports for the Short Term backups display the Start Time as midnight for all Short Term jobs. The job’s End Time is the time that each job completes; however, because each job does not start performing the backup operation until the previous job has completed, the end times for the duration of each job (End Time minus Start Time) increases for each subsequent VM. Thus, direct comparison of the duration of one VM to another may be misleading. To get an accurate representation, determine the duration of a job as the end time of the previous job to the end time of the current job. This calculation represents the actual time that is taken to perform the backup.

Job Duration Report
2.2.7 Hypervisor Integration

In a Simplex system, there is only one hypervisor element. The backup subsystem is configured to communicate directly with that hypervisor at its PDH IP address, which is all that is required. Both backup and restore operations use that one ESXi host as the source or destination of the operation.

In an HA system, multiple elements are involved and special information is required. Because VMs can move from one server to the other at any time, the backup program communicates with the Hypervisor Control VM (HC1), which is the VMware vCenter Appliance. This VM keeps track of the cluster, including the list of hypervisors, and which VMs are currently running on each hypervisor. By contacting the HC1 VM, the backup subsystem can determine where the VM is running and retrieve the server address of the server currently hosting the VM.

Using the HC1 VM for coordination works well for backing up an HA system, but it can run into a problem when it is time to restore a VM. If the HC1 VM is running, it can be used to restore a VM to one of the servers running in the server cluster. If the HC1 VM is not running, there is a problem since it was the central point of contact for the backup system. To get around this, not only is the HC1 VM defined in the backup system (and used for most all operations) but the two individual servers (HS1 and HS2) are also defined to act as a target to be able to restore the HC1 VM during a rebuild operation. In this case, one server (HS1 or HS2) is chosen as the destination for restoring the HC1 VM, then the HC1 VM is started and used to restore any additional VMs.

This scheme of defining both HC1 access as well as direct HS1 and HS2 access can be confusing in the backup program UI. Each VM is displayed twice: once in the HC1 master list, and once under the HSn server where it is currently running. Backup operations should always be defined to capture their images from the HC1 address so it will continue to function as the VM migrates from one host to the other. Likewise, restore operations should always be defined to restore the VM to the HC1 address so that it automatically reestablishes the redundancy across the cluster servers. The only exception to these rules is that when the HC1 VM itself must be restored, it must be restored directly to a selected server.
### 2.2.8 Deleting Backup Jobs

When you delete the definition of a backup job, by default only the definition of the backup job is removed; the archives that have already been created are not removed. Archives that are no longer referenced by the backup job are listed in the backup list as *Imported* backups. These archives can be restored just like any other archive.

When you delete a backup job, old archives remain in the repositories and display as *(Imported)* archives. If a new backup job is created for that same VM, a new directory is created for the VM by appending `<n>` to the end of the VM for the directory name. This allows the archives created from the original backup job and the archives created from the current backup job to coexist in the repositories. Make sure you select from the proper directory during restore operations for both the Short Term and Long Term Repository.

➢➢ To remove the archives from the repositories: expand the Backups item in the Tree View to access the following items:

- Select the **Disk** item to view and remove current Short Term archives.
- Select the **Disk (copy)** item to view and remove current Long Term archives.
- Select the **Disk (imported)** item to view and remove archives that are not associated with a current backup job (Short Term and Long Term).

#### Example:

- If a backup job is created for DC1:
  - Short Term archives are stored in the directory `D:\Backup\ShortTerm\DC1`. Archives in this directory are located within the Backups, Disk item in the Tree View.
  - Long Term archives are stored in the directory `D:\Backup\LongTerm\Copy_DC1`. Archives in this directory are located within the Backups, Disk (copy) item in the Tree View.
- If the backup job DC1 is deleted (without removing the archives):
  - Short Term archives already created remain in the directory `D:\Backup\ShortTerm\DC1`. Archives in this directory are located within the Backups, Disk (imported) item named DC1.
  - Long Term archives already created remain in the directory `D:\Backup\LongTerm\Copy_DC1`. Archives in this directory are located within the Backups, Disk (imported) item named Copy_DC1.
- If a new backup job is created for DC1:
  - Short Term archives already created remain in the directory `D:\Backup\ShortTerm\DC1`. Archives in this directory are located within the Backups, Disk (imported) item named DC1.
  - Long Term archives already created remain in the directory `D:\Backup\LongTerm\Copy_DC1`. Archives in this directory are located within the Backups, Disk (imported) item named Copy_DC1.
  - New Short Term archives are stored in the directory `D:\Backup\ShortTerm\DC1_1`. Archives in this directory are located within the Backups, Disk.
  - New Long Term archives are stored in the directory `D:\Backup\LongTerm\Copy_DC1_1`. Archives in this directory are located within the Backups, Disk (copy).
3 Procedures

The procedures provided in this chapter are required to set up the backup jobs that back up a VM, and are used to recover a VM from one of the previously created backup archives.

Note The Veeam Backup & Replication UI often provides multiple methods to initiate these actions (such as toolbar icons, tree view items, menu items, and so forth). Any of these methods can be used to launch the procedure.

3.1 Create Backup Jobs for VM

Each VM uses two backup jobs to create the backup archives. The first collects the file changes from the VM and integrates them into the Short Term Repository. The second creates periodic copies of the Short Term Repository and places them in the Long Term Repository to save longer duration backups (weekly, monthly). The supplied Microsoft® PowerShell script creates both jobs at once and binds them together with the default schedule (backups are run at midnight every day, and weekly and monthly backups are saved on Sunday).

➢➢➢ To create backup jobs for a VM

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. Open an Administrator Mode PowerShell window.
3. Enter the command `CD D:\Backup` to change the directory and press `[Enter]`.
4. Enter the command `.\Create-BackupJob <VMname>` (where `<VMname>` is the name of the VM to backup) and press `[Enter]`.
   For example: `Create-BackupJob DC1`

Tip • Backup jobs preserve the case of the VM name (case sensitive); we recommend using all capital letters.
   • If the job already exists and you want to delete the old one and create a new one, add the `-Force` option to the command line.
     - The `-Force` option removes the old job, then creates a new job.
     - The `-Force` option takes a couple of minutes to remove the old job, and it may seem suspended, showing 00:00:00 remaining. This is normal behavior so wait for it to complete.
   • Type `help\Create-BackupJob.ps1` and press `[Enter]` to display a help screen that explains the available parameters, such as defining the time-of-day or day-of-week the backups should be performed. With no parameters, it defaults to midnight each day for incremental backups, and Sunday for full backups (weekly and monthly).
3.2 Open Veeam Backup & Replication Console

➢ To open the Veeam Backup & Replication console

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. From the desktop, double-click the Veeam Backup & Replication Console icon.

3. When the Veeam Backup & Replication connection dialog box displays, accept the defaults (to connect to the version running on the local computer) and click Connect.
4. The *Veeam Backup & Replication Console* window displays. From the Tree View, use the Backup & Replication item to monitor the status of backup jobs and archives, and initiate restore operations.
3.3 Launch Unscheduled Backup of VM

Use the following procedure to trigger an immediate backup of a VM outside of its normal schedule. The resulting archive displays in the Short Term Repository. Use this procedure to create an incremental backup or a full backup.

➢➢ To launch an unscheduled backup of a VM

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.

2. Open the Veeam Backup & Replication console.

3. From the Tree View, expand the Jobs item and select the Backup item.

4. Select the appropriate VM(s).
   a. Press [Ctrl] and click to toggle the selection of a VM.
   b. Select one entry then press [Shift] and click on another entry to select both entries and every entry between them.

5. Initiate the backup job.
   a. To initiate an incremental backup, select Start icon from the toolbar.
   b. To initiate a full backup that collects the files from the VM, select the Active Full icon from the toolbar.

The backup will immediately begin and the console window displays the backup status.
3.4 **Restore Entire VM from Archive (Except HC1)**

Use the following procedure to recover an entire VM from an archive.

➢ **To restore an entire VM from an archive (except HC1)**

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. *Open the Veeam Backup & Replication console.*
3. From the toolbar, click the **Restore** icon.

![Veeam Console Toolbar Icons](image)

4. Accept the default **Entire VM (including registration)** and click **Next**.
5. Add the VMs.
   a. From the *Virtual Machine* dialog box, click **Add VM** and select **From backup...**
   b. Select the appropriate VM and click **Add**.
      i. To select multiple VMs, press and hold **[Ctrl]** while selecting the appropriate VMs. The **[Ctrl]** key toggles the selection state of the VM.
      ii. Normally the Job Name with the name of the VM should be used, but if you want to restore to a point in the Long Term storage, click the **Copy_<VMname>** job instead.
   c. To add additional VMs, click **Add VM**.
   d. To remove VMs, select the VM and click **Remove**.
   e. To restore something other than the latest backup, perform the following steps:
      i. Select the VM and click **Point...** to display a list of the available Short Term (<VMname>) and Long Term (Copy_<VMname>) backups.
      ii. Expand the list of backups and select the backup to restore.
      iii. Click **OK**.
   f. When the selection of the VMs to restore is complete, click **Next**.
6. From the *Restore Mode* dialog box, accept the defaults for **Restore to the original location** and **Restore VM tags**, then click **Next**.
7. From the *Reason* dialog box, you may optionally enter the reason for the restore, then click **Next**.
8. From the *Summary* dialog box:
   a. For the VM to power up immediately once the restore is completed, select (to enable) the **Power on target VM after restoring** checkbox.
   b. Click **Finish**.
9. The VM Restore status dialog box displays with updates during the restore process.
   a. Do not be alarmed by the initial time estimates on the Statistics tab; the initial estimates include the setup time. Once
      the actual transfer starts, the Time Remaining estimate will quickly update to something reasonable.
   b. To cancel the restore operation, select **Cancel restore task**.

10. When the restore task has completed, click **Close**.

On an HA system, the VM will be recovered to one of the servers in the cluster, and the Virtual SAN subsystem will copy the
VM information and the VM hard drive(s) to the other server. Perform a compliance check to verify that the VM has been
copied. If not, reapply the compliance policy.

➢➢ **To check or correct the compliance policy**

1. Open the vCenter Appliance Web Interface using an account with administrative privileges.
2. Select **Hosts and Clusters** and expand **Datacenter1** and **Cluster1** to view the list of cluster VMs.
3. Select the restored VM and select the **Summary** tab.
4. Verify that the **VM Storage Policies** area displays the following:
   a. **VM Storage Policies** field displays **Virtual SAN Default Storage Policy**.
   b. **VM Storage Policy Compliance** field displays **Compliant**.
5. If the fields in step 4 are not displayed correctly, click **Check Compliance** to retest the compliance and wait for it to
   refresh the screen.
6. If the **VM Storage Policies** field still does not display as **Virtual SAN Default Storage Policy**, perform the
   following steps:
   a. From the Tree View, right-click the VM and select **VM Policies**, then select **Edit VM Storage Policies**.
      i. From the **VM Storage Policy** drop-down list, select **Virtual SAN Default Storage Policy**.
      ii. Click **Apply to all**.
      iii. Click **OK**.
   b. Wait for the **Recent Tasks** pane to indicate that the **Reconfigure virtual machine** task has completed, then click
      **Check Compliance**.
7. If the **VM Storage Policy Compliance** field does not display as **Compliant**, perform the following steps:
   a. From the Tree View, right-click the VM and select **VM Policies**, then select **Reapply VM Storage Policy**.
   b. Wait for the **Recent Tasks** pane to indicate that the task has completed, then click **Check Compliance**.
3.5 Restore HC1 VM from Archive (Special Instructions)

➢ To restore the HC1 VM from an archive

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. Open the Veeam Backup & Replication console.
3. From the toolbar, click the Restore icon.
4. Accept the default Entire VM (including registration) and click Next.
5. Add the VMs as follows:
   a. From the Virtual Machine dialog box, click Add VM and select From backup....
   b. Select the HC1 VM and click Add.
   c. To restore something other than the latest backup, select the HC1 VM and click Point....
      i. A list of the available Short Term (<VMname>) and Long Term (Copy_<VMname>) backups is displayed.
      ii. Expand the list of backups and select the backup to restore.
      iii. Click OK.
   d. When the selection of VMs to restore is complete, click Next.
6. From the Restore Mode dialog box, select Restore to a new location... and Restore VM tags, then click Next.
   (Note: Wait for the Loading VM data... dialog message to clear (~ 3-5 minutes). The vCenter Appliance will be unavailable during this time frame.)
7. From the Host dialog box, select Restore to a new location... and Restore VM tags, then click Next.
8. Select the HC1 VM and click Host....

   Selecting the host is required, even if it looks like the correct host is already selected:
   - The displayed default host is the host from which the backup was taken.
   - The backup was taken through the vCenter Appliance; therefore, the displayed host is reached through the vCenter Appliance, which will fail because the vCenter Appliance is not available.
   - The HS1 server address at the top of the Tree View (parallel to the vCenter Appliance address) is reached directly, which is required for the following step.

   a. Select the HS1 address (standard is 172.16.199.8) displayed in the initial Tree View.
   (Note: Do not attempt to expand the HC1 address (standard is 172.16.199.7) as the vCenter Appliance is not available as a recovery host and it will not be able to expand. It will take a long time before it allows you to continue.

   b. Click OK.

9. Click Next.
10. From the Resource Pool dialog box, accept the default and click Next.
11. From the Datastore dialog box, accept the defaults and click Next.
12. From the Folder dialog box, accept the defaults and click Next. If prompted to overwrite an existing folder with the same name, select Yes.
13. From the Network dialog box, accept the defaults and click Next.

14. From the Reason dialog box, you may optionally enter the reason for the restore, then click Next.

15. From the Summary dialog box:
   a. For the VM to power up immediately once the restore is completed, select (to enable) the Power on target VM after restoring checkbox.
   b. Click Finish.

16. The VM Restore status dialog box displays with updates during the restore process.
   a. Do not be alarmed by the initial time estimates on the Statistics tab; the initial estimates include the setup time and assume that all hard drives were completely filled. Once the actual transfer starts, the Time Remaining estimate will quickly update to something reasonable. A typical restore operation takes ~15-20 minutes.
   b. The restore operation can be canceled by selecting the Cancel restore task option.

17. When the restore task is complete, click Close.
3.6  **Restore Individual Files from Windows VM**

Use the following procedure to recover individual files from an archive. This procedure is useful when files have been inadvertently deleted or if changes made to files need to be undone. You can choose to copy the files to the computer running the Backup User Interface, or restore them to the original VM.

➢ **To restore individual files from a Windows VM**

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. *Open the Veeam Backup & Replication console.*
3. From the toolbar, click the **Restore** icon.
4. From the **Restore Wizard** dialog box **Restore from backup** column, select **Guest files (Microsoft Windows)** and click **Next**.
5. From the **Virtual Machine** dialog box, expand the backup job that contains the archive to use as the source for the file recovery, select the archive, then click **Next**.
   a. For a backup from the Short Term Repository, select the Job Name that matches the VM name.
   b. For a backup from the Long Term Repository, select the Job Name **Copy_<VMname>**.
6. From the **Restore Point** dialog box, select the archive to use as the source of the restored files and click **Next**.
7. From the **Reason** dialog box, you may optionally enter the reason for the restore, then click **Next**.
8. From the **Summary** dialog box, click **Finish**. Wait for the system to open the archive and display a list of files that are available for restore. This can take ~10-30 seconds, depending on the archive size and complexity (how many incremental backups need to be integrated into the final selection).
9. From the **Backup Browser** dialog box, select one or more files to be restored as follows:
   • Clicking on a file selects that file and only that file.
   • To select additional files, press and hold [Ctrl] while clicking on a file. This toggles the selection state of that file without impacting other files that are selected.
   • To select a block of files, select the first file then press and hold [Shift] and click on a second file. All files between the first and the second (inclusive) file will be selected.
   • Selecting a directory causes all contents of the directory to be restored.
10. To obtain a **local** copy of the file(s) and restore them to the VM running the Veeam UI, perform the following steps:
    a. Right-click a selected file and select **Copy-To**.
    b. The default location is the user’s current desktop. To change where the file(s) are copied, click **Browse ...** and select the local directory as the target for the restore.
    c. Click **OK**.
    d. When the file(s) have been copied, it returns to the **Backup Browser** window where additional files can be selected or the files can be copied back to the original VM.
11. To restore the files to the original VM, perform the following steps:
    a. Right-click on a selected file and select **Restore**.
    b. To overwrite existing files in the VM with files from the archive, select **Overwrite**.
    c. To keep existing files in the VM and rename the files from the archive, select **Keep**. The restored file(s) will be named **RESTORED-_<filename>**.
12. From the **Credentials** dialog box, check the credentials as follows:
    a. If the account is present in the **Credentials** drop-down list, select it and click **OK**.
b. If the account is not present in the Credentials drop-down list, perform the following steps to add it:
   i. Click Add....
   ii. Enter the Username of an account with write access to the VM where the files are to be restored.
   iii. Enter the Password.
   iv. (Optional) Enter a Description for the account credentials.
   v. Click OK.

13. After the restore is complete, the Backup Browser window is displayed, where additional files may be selected for restore.

14. After file restoration is complete, close the Backup Browser window.
3.7 Restore Individual Files from Non-Windows VM

To restore files from a non-Windows VM, the backup program creates a new (temporary) VM from the contents of the archive. The backup program reads the files from the (temporary) copy of the VM, then deletes the temporary VM after the restore is complete. Because a temporary VM is created, make sure a host with sufficient resources to host an additional VM is available.

Use the following procedure to recover individual files from an archive. Use this procedure when files have been inadvertently deleted or if changes made to the files need to be undone. You can choose to copy the files to the computer running the Backup User Interface, or restore the files to the original VM.

➢➢ To restore individual files from a non-Windows VM

1. Log in to the VM running the Veeam Backup & Replication software using an administrative account.
2. Open the Veeam Backup & Replication console.
3. From the toolbar, click the Restore icon.
4. From the Restore Wizard dialog box Restore from backup column, select Guest files (other OS) and click Next.
5. From the Virtual Machine dialog box, expand the backup job that contains the archive to use as the source for the file recovery, select the archive, then click Next.
   a. For a backup from the Short Term Repository, select the Job Name that matches the VM name.
   b. For a backup from the Long Term Repository, select the Job Name Copy_<VMname>.
6. From the Restore Point dialog box, select the archive to use as the source of the restored files and click Next.
7. From the Reason dialog box, you may optionally enter the reason for the restore, then click Next.
8. From the Summary dialog box, click Finish. Wait for the system to open the archive and display a list of files that are available for restore. This can take ~10-30 seconds, depending on the archive size and complexity (how many incremental backups need to be integrated into the final selection).
9. From the Helper Appliance dialog box, select a host for the temporary VM.
   a. Click Customize.
   b. From the FLR Appliance Configuration dialog box, locate the Host section and click Choose.
   c. For an HA system, select the host for the temporary VM as follows:
      i. Expand the vCenter Appliance, Datacenter1, and Cluster1 items.
      ii. Select one of the listed hosts to use for the temporary VM.
      iii. Click OK.
   d. For a Simplex system, select the host for the temporary VM as follows:
      i. Select the top-level host (typically HS1).
      ii. Click OK.
   e. Click OK.
   f. Click Finish. Wait for the system to create the temporary VM from the archive files and display a list of files that are available for restore. This can take ~20-60 seconds, depending on the archive size and complexity (how many incremental backups need to be integrated into the final selection).
10. From the File Level Restore dialog box, select one or more files to be restored as follows:
   • Clicking on a file selects that file and only that file.
   • To select additional files, press and hold [Ctrl] while clicking on a file. This toggles the selection state of that file without impacting other files that are selected.
• To select a block of files, select the first file then press and hold [Shift] and click on a second file. All files between the first and the second (inclusive) file will be selected.
• Selecting a directory causes all contents of the directory to be restored.

11. To obtain a **local** copy of the file(s) and restore them to the VM running the Veeam UI, perform the following steps:
   a. Right-click a selected file and select **Copy-To**.
   b. Accept the default **Server** (the computer running the UI).
   c. Click **Browse ...** and select the local directory where the files are to be restored.
   d. Click **Restore**.
   e. When the file(s) have been copied, the *File Level Restore* window is displayed, where additional files can be selected or the files can be copied back to the original VM.

12. To restore the files to the original VM, perform the following steps:
   a. Right-click on a selected file and select **Restore**.
   b. To overwrite any existing files in the VM with files from the archive, select **Overwrite**.
   c. To keep existing files in the VM and rename the files from the archive, select **Keep**. The restored file(s) will be named RESTORED-<filename>.

13. From the *Credentials* dialog box, check the credentials as follows:
   a. If the account is present in the **Credentials** drop-down list, select it and click **OK**.
   b. If the account is not present in the **Credentials** drop-down list, perform the following steps to add it:
      i. Click **Add...**.
      ii. Enter the Username of an account with write access to the VM where the files are to be restored.
      iii. Enter the Password.
      iv. (Optional) Enter a Description for the account credentials.
      v. Click **OK**.

14. After the restore is complete, the *File Level Restore* window is displayed, where additional files may be selected for restore.

15. After file restoration is complete, close the *File Level Restore* window.
3.8 Restore HC1 VM (Alternative Instructions)

Use the following instructions as an alternative procedure to recover an HC1 VM.

➢ To restore an HC1 VM

1. Log in to the VM running the Veeam Backup & Replication software on MC3 using an administrative account.
2. Open the Veeam Backup & Replication console on MC3.
3. From the toolbar, click the Restore icon to open the Restore Wizard.
4. Select VM file (VMDK, VMX) from the Restore from backup options and click Next.

5. From the Virtual Machine dialog box, select the HC1 VM with the appropriate date for recovery, then click Next.
6. From the *Restore Point* dialog box, select **Full** backup, then click **Next**.

![Restore Point dialog box]

7. From the *Restore Destination* dialog box, click **Browse**, and navigate to and select the path on the local machine (MC3) where the files will be stored.

8. Click **Select All** to select all of the files, then click **Next**.

![Restore Destination dialog box]
9. The *VM Restore* dialog box displays and the **Log** tab provides the status of the restore process. The restore process takes approximately two to three hours to complete.

   ![VM Restore dialog box](image)

   a. Do not be alarmed by the initial time estimates on the Statistics tab; the initial estimates include the setup time. Once the actual transfer starts, the Time Remaining estimate will quickly update to something reasonable.

   b. To cancel the restore process, select **Cancel restore task**.
10. When the restore process has completed, click **Close**.

11. Upload the restored VM folder to the HS1 (172.16.199.8) datastore.

   **Note**  
   Upload time depends on the network bandwidth.

   a. Right-click the HS1 Datastore and select **Browse Datastore**.

   b. Select the **HC1 recovery** folder location and click **OK** to upload the files.
12. Once upload is complete, double-click the uploaded folder to open it.

13. Right-click on the **HC1.VMX** file, and select **Add to inventory**.
14. Enter the VM Name as HC1 and click **Next**.
15. Select the resource pool within which to run the VM and click **Next**.

16. Click **Finish**.
17. Power on the VM from HS1 through the vSphere client and wait for all services to start.

18. Verify successful login to HC1 and check for any errors.